The How To Pass on Your First Try Certification Study Guide

CEH

Certified Ethical Hacker Certification Exam Preparation

Course in a Book for Passing the CEH Certified Ethical Hacker Exam

William Manning

CEH Certified Ethical Hacker Certification Exam Preparation Course in a Book for Passing the CEH Certified Ethical Hacker Exam:

The 'How to Pass on Your First Try' Certification Study Guide

***Notice of Rights**: Copyright © The Art Of Service. All rights reserved. No part of this book may be reproduced or transmitted in any form by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.*

***Notice of Liability**: The information in this book is distributed on an "As Is" basis without warranty. While every precaution has been taken in the preparation of the book, neither the author nor the publisher shall have any liability to any person or entity with respect to any loss or damage caused or alleged to be caused directly or indirectly by the instructions contained in this book or by the products described in it.*

***Trademarks**: Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this book, and the publisher was aware of a trademark claim, the designations appear as requested by the owner of the trademark. All other product names and services identified throughout this book are used in editorial fashion only and for the benefit of such companies with no intention of infringement of the trademark. No such use, or the use of any trade name, is intended to convey endorsement or other affiliation with this book.*

Foreword

The Art of Service is an Accredited Training Organization and has been training IT professionals since 1998. The strategies and content in this book are a result of experience and understanding of the Certified Ethical Hacker methods, and the exam requirements.

This Exam Preparation book is intended for those preparing for the Certified Ethical Hacker Exam. This book is ***not*** *a replacement for completing the course. This is a study aid to assist those who have completed an accredited course and preparing for the exam. Do not underestimate the value of your own notes and study aids. The more you have, the more prepared you will be.*

While it is not possible to pre-empt every question and content that MAY be asked in the CEH exam, this book covers the main concepts covered within the Certified Ethical Hacker discipline.

The CEH exam certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective. The Certified Ethical Hacker certification will fortify the application knowledge of security officers, auditors, security professionals, site administrators, and anyone who is concerned about the integrity of the network infrastructure. A Certified Ethical Hacker is a skilled professional who understands and knows how to look for the weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker.

Due to licensing rights, we are unable to provide actual CEH Exam. However, the study notes and sample exam questions in this book will allow you to appropriately prepare for the CEH exam.

The Art of Service
http://www.theartofservice.com/

Write a Review and Receive a Bonus Emereo eBook of Your Choice

Up to $99 RRP – Absolutely Free

If you recently bought this book we would love to hear from you – submit a review of this title and you'll receive an additional free ebook of your choice from our catalog at http://www.emereo.org.

How Does it Work?

Submit your review of this title via the online store where you purchased it. For example, to post a review on Amazon, just log in to your account and click on the 'Create Your Own Review' button (under 'Customer Reviews') on the relevant product page (you'll find plenty of example product reviews on Amazon). If you purchased from a different online store, simply follow their procedures.

What Happens When I Submit my Review?

Once you have submitted your review, send us an email via review@emereo.org, and include a link to your review and a link to the free eBook you'd like as our thank-you (from http://www.emereo.org – choose any book you like from the catalog, up to $99 RRP). You will then receive a reply email back from us, complete with your bonus ebook download link. It's that simple!

2 Table of Contents

Copyright The Art of Service

Copyright The Art of Service

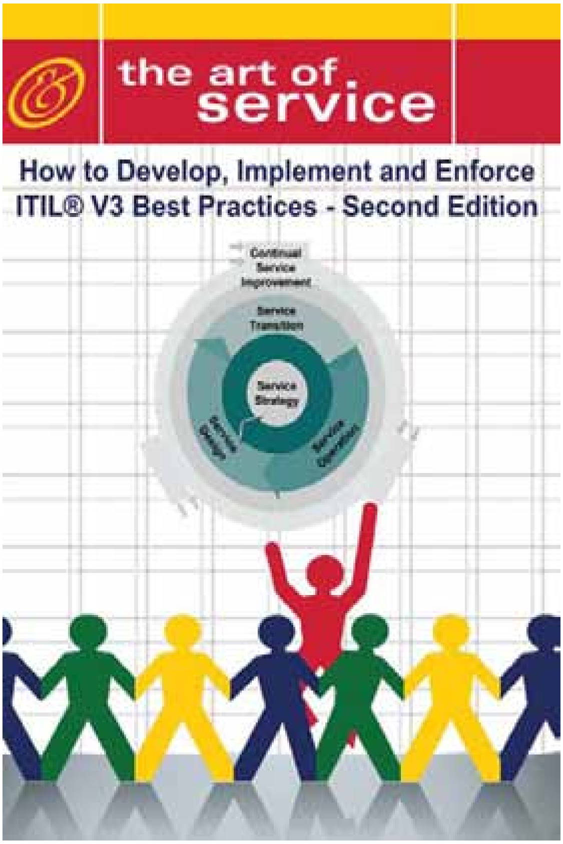
Copyright The Art of Service

Copyright The Art of Service

Copyright The Art of Service

Copyright The Art of Service

Also from Emereo Publishing and The Art of Service:


the art of service
How to Develop, Implement and Enforce ITIL® V3 Best Practices - Second Edition
Continual Service Improvement
Service Transition
Service Strategy
Service Design
Service Operation

How to Develop, Implement and Enforce ITIL V3's Best Practices:

2009 Edition

2009 Revised Edition: ITIL® V3 comprehensive walk-though of the 5 Critical Lifecycle Steps, core principles, best practices and support materials for adoption and implementation of the ITIL® V3 IT Service Management Framework.

Also from Emereo Publishing and The Art of Service:

the art of service
ITIL® V3 Foundation
Complete Certification Kit:
2009 Edition
Study Guide Book and Online Course

ITIL V3 Foundation Complete Certification Kit:

2009 Edition Study Guide Book and Online Course

2009 Edition ITIL V3 Foundation Certification exam prep guide, including refreshed study guide, online eLearning program, new examples, instructions, and cautionary advice.

3 Cisco Certified Entry Networking Technician

An Ethical Hacker is a person employed and trusted by an organization to penetrate the network and computer systems using the same methods as a hacker. Similar to a penetration tester, the goal of the ethical hacker is to assist the organization in taking preemptive measures against malicious attacks by hacking the system.

Hacking is a felony crime within most countries, including the United States. As an Ethical Hacker, the activities are performed on request and under contract with the organization; therefore bypassing any legal consequences for the activities performed.

The challenge and benefit of the Ethical Hacking is the same: to catch the criminal, one must think like the criminal. This requires a level of creativity and thinking “outside the box” to ensure that organizations have adequately protected their information assets from the numerous methods of attacks that can be perpetrated against them.

A Certified Ethical Hacker is a skill professional who understands and can identify weaknesses and vulnerabilities in target systems. The purpose of the certification is to strengthen the applicable knowledge and trust of security officers, auditors, security professionals, and site administrators.

Specific topics of CCENT cover:

- Fundamentals of Ethical Hacking
- Footprinting
- Scanning technologies
- Enumeration
- Trojans, backdoors, worms, and viruses
- Session Hijacking
- Denial of Service
- Hacking of Systems, Web Services, and Linux
- Cryptography
- Penetration Testing

Copyright The Art of Service

4 Exam Specifics

The certification for Ethical Hacker is administered by the EC-Council. The candidate must attend a prerequisite source and show proof of attendance in order to take the exam.

Exams are delivered by Prometric and Vue testing centers. The cost of the exam, 312-50, is $250 USD.

Specifics on the exam -

Duration:	4 hours
Number of Questions:	150
Passing Score:	70%
Type of Questions:	Multiple choice – single answer Multiple choice – multiple answer Fill in the Blank

For more information, see the EC-Council's website: www.eccouncil.org.

5 Exam Prerequisites

A candidate for Certified Ethical Hacker must attend the Ethical Hacking and Countermeasures Course. After completing the training, the candidate must successfully complete the Ethical Hacking and Countermeasures Exam (312-50 or ECO-350).

In addition to the course, it is recommended that a candidate has at least 2 years of experience. The candidate must also sign an Ethics Agreement.

6 Ethics

Ethical Hacking is about providing security to business assets.
Reasons for security:

- Impact of hacking on business assets and reputation
- Technology development making computers easier to use
- Complexity of administration and management of computer infrastructures increasing
- Malicious hacking can be performed with reducing skill levels
- Increasing requirements on networking

6.1 Terminology

Hacker – a person who is enthusiastic about the details of computer systems, and build their capabilities.

Hacking – to write of refine computer programs skillfully, usually associated with gaining unlawful or malicious access.

Cracker – a person who attempts to break into a network computer system or software, as in “cracking the code.”

Ethical Hacker – a person who attacks a security system on behalf of its owners with the intent of discovering vulnerabilities that can be exploited by a malicious hacker.

Threat – an action or event can has the potential of adversely affecting security. Threats are sought after and prioritized during security analysis.

Vulnerability – the real existence of a weakness, design, or implementation error that can allow the security of the system to be compromised unexpectedly.

Target of Evaluation – An IT system, product, or component that has been identified as requiring an evaluation of its security.

Copyright The Art of Service

Attack – an direct assault on computer systems to compromise the system based on a vulnerability.

Exploit – Taking advantage of a vulnerability, bug, or glitch for the purpose of breaching the security of an IT system.

Remote exploit – exploits security vulnerabilities without any prior access to the vulnerable system.

Local exploit – exploits security vulnerabilities with prior access to the vulnerable system.

6.2 The Ethical Hacker

- Typically consists of security professionals and network penetration testers.
- Utilizes hacking skills and technologies to protect the system and defend against intrusions.
- Activities include testing the network and systems security for vulnerabilities.
- Uses the same tools and technologies as a malicious hacker.

6.3 Security and Hacking

Security speaks to the well-being of information and infrastructure. Security looks to mitigate or prevent undetected theft, tampering, and disruption to information and services.

6.3.1 Foundation of Security – C.A.I.A

Confidentiality protects information or resources from unauthorized access.
Authentication is the identification and control of access to computer systems.
Integrity ensures the trustworthiness of data or resources through the management and control of changes.
Availability refers to continual accessibility of information and resources.

Hacking events will affect one or more of these security elements.

6.3.2 Phases of Ethical Hacking

Processes for malicious and ethical hacking are similar.
Includes;

- Reconnaissance
- Scanning
- Gaining Access
- Maintaining Access
- Covering Tracks

6.4 Hacking Technologies

Tools and methods are used to:

- Locate vulnerabilities
- running exploits
- Compromising systems

Areas where weaknesses are commonly exploited:

- Operating systems
- Applications
- Shrink-wrap code
- Misconfigurations

Installing operating systems with defaults settings can lead to vulnerabilities, when patches are not well installed.
Lack of vulnerability testing in application codes, can be exploited through programming flaws.
Extra features in off-the-shelf applications can be used to exploit a system.
Ease of use being balanced with security concerns can contribute to opening vulnerabilities in the configurations.

Copyright The Art of Service

Technologies used to hack networks or systems include:

- Trojans
- Backdoors
- Sniffers
- Rootkits
- Exploits
- Buffer overflows
- SQL injection

Hacking activities are classified as passive or active.
Activities can also be classified as inside or outside attacks.

Passive attacks are breaches of confidentiality as they seek information only.
Active attacks affect the availability, integrity, and authenticity of the system with the intent to change the system or network.

An inside attack refers to attacks which originate from within the organization's security perimeter and is often caused by an “insider.”
An outside attack originates from outside the security perimeter.

6.5 Phase of Ethical Hacking

6.5.1 Reconnaissance

- Preparatory phase
- Focuses on information gathering
- Activities can be external or internal to the computer systems
- Attempts to identify vulnerabilities related to ease of entry are found.

External reconnaissance methods include:

- Surveillance
- Social engineering
- Dumpster diving
- Internet searches
- Googling individuals and companies

Copyright The Art of Service

Internal reconnaissance methods include:

- Sniffing the network (passive)
- “Rattling the doorknobs” (active)

Active reconnaissance involves probing the network to detect:

- Accessible hosts
- Open ports
- Router locations
- Details on operating systems and services

6.5.2 Scanning

The pre-attack phase when the network is scanned using the information gained in the reconnaissance stage. Attempts to identify “high” business risks.
High risks are single points of entry for attack and exploitation when the system vulnerability is detected.

Utilizes:

- Dialers
- Port scanners
- Network mapping
- Sweeping
- Vulnerability scanners

6.5.3 Gaining Access

Attack phase:
Vulnerabilities are exploited. The purpose is to gain access or “owning” the system.

Methods of connection for exploitation include:

- Local Area Network (LAN)
- Wireless connections
- Direct access to a PC
- The Internet
- Offline

Copyright The Art of Service

Exploits can be perceived as a deception or theft, and include:

- Buffer overloads
- Denial of service
- Session hijacking
- Password filtering

Factors that can influence the situation:

- Architecture of the target system
- Configuration of the target system
- Skill level of the perpetrator
- Initial level of access obtained

Identifies the “highest” business risks
The highest risks are unauthorized access to the operating systems, application or network.

6.5.4 Maintaining Access

Focuses on retaining 'ownership' of the system:
A vulnerability has been exploited. The system can be tampered with and compromised.

Exclusive access to the system is secured, using:

- Backdoors
- RootKits
- Trojans
- Trojan Horse Backdoors

May involve several hackers to harden the system.

Data, applications, and configurations can be uploaded, downloaded, or manipulate.

Owned systems are sometimes referred to as “zombie” systems.

6.5.5 Covering Tracks

Focuses on activities to continue without detection
Purpose for hiding:

- Prolonging stay within the system
- Continue use of resources

Copyright The Art of Service

- Removing evidence
- Avoiding countermeasures
- Avoiding legal action

Methods for covering tracks:

- Steganography
- Tunneling
- Alteration of log files

Another use for covering tracks to begin reconnaissance to a related system.

6.6 Hacker Classes

6.6.1 Black Hats

- Also known as “crackers”
- Highly competent computer skills
- Resorts to malicious or destructive activities

6.6.2 White Hats

- Also known as 'Security Analysts'
- Knowledge of hacking and hacking toolsets
- Skills are used for defensive purposes to identify weaknesses and implement countermeasures

6.6.3 Gray Hats

Will work offensively and defensively depending on the situation

Copyright The Art of Service

6.7 Hacktivism

Hacking with or for a cause.
The cause is typically routed in a social or political agenda.
Hacking activities are meant to deliver a message.
Purpose is to gain visibility for the cause or themselves.

Common targets include:

- Government agencies
- MNCs
- Entities who hackers perceive are 'bad'

6.8 Skills of an Ethical Hacker

May also be called a “penetration tester.”

6.8.1 Focus of an Ethical Hacker

Ethical hackers try to answer:

- What can the intruder see on the target system?
- What can an intruder do with that information?
- Does anyone at the target notice the intruder’s successful attempts of failures?

Within an organization: the questions are:

- What should be protected?
- From whom should the protection be?
- What resources are required to protect?

6.8.2 Profile of an Ethical Hacker

Adept at technical domains
In-depth knowledge about target platforms:

- Windows
- Unix
- Linux

Copyright The Art of Service

Extraordinary knowledge in networking and related hardware / software.
Knowledgeable about security areas and related issues.
Ideally, would have the highest level of security clearance, but often does not.

6.8.3 Actions of an Ethical Hacker

- Relies on penetration testing
- Used to test the security of a system or network
- Relies on persistence and repetition over intelligence

Looks to secure the elements of the system:

- Confidentiality
- Authenticity
- Integrity
- Availability

6.8.4 Skills of an Ethical Hacker

Must be computer system experts.
Be knowledgeable about:

- Computer programming
- Networking
- Operating systems

Possesses in-depth knowledge about operating platforms.

Characteristics required include:

- Patience
- Persistence
- Perseverance

Copyright The Art of Service

6.9 Vulnerability Research

A process of discovering vulnerabilities and design weaknesses.
The intent is to identify areas of potential attacks.

Current lists of known vulnerabilities and possible exploits for systems and networks are often provided through websites and tools used by the ethical hacker.

Maintaining current knowledge of existing Trojans, viruses, and common exploits are required to protect system.

Discovering threats aid in the detection, prevention, and recovery of an attack.

6.10 Methods of a Ethical Hacker

Ethical Hacking is structured and organized.
Often part of a “Tiger Team,” a group of individuals hired to conduct security audits.

Steps for performing a security audit include:

- Discussing testing needs with the client
- Preparing and signing nondisclosure agreements (NDA) with client
- Organize an team
- Prepare a testing schedule
- Conduct the test
- Analyze results
- Present findings

Security evaluations involve three components:

- Preparation
- Conducting
- Conclusion

6.10.1 Preparation

A formal contract is signed, including:

- Nondisclosure agreement
- Immune to prosecution

Contract agrees on:

- Infrastructure perimeter
- Evaluation activities
- Time schedules
- Available resources
- Scope of the test

6.10.2 Conduct Security Evaluation

- Creates a evaluation technical report
- Tests potential vulnerabilities

Modes of Ethical Hacking:

- Remote networking – simulated attempt to launch an attack over the Internet
- Remote Dial-up – simulated attempt to launch an attack through the organization'[s modem pool
- Local networking – simulated attempt to gaining unauthorized access over the network using an employee's access rights
- Stolen equipment – simulates theft of resource for critical information, such as a laptop
- Social engineering – works to compromise the integrity of the organization's employees
- Physical entry – works to compromise the organization's physical IT infrastructure

Two approaches to security testing:

- Black-box approach is used when no prior knowledge of the testing infrastructure is available.
- White-box approach has complete knowledge of the network knowledge.

Copyright The Art of Service

Internal testing is sometimes referred to as Gray-box testing. Focuses on the extent of access by insiders within the network.

Forms of security testing include:

- Vulnerability testing
- Ethical hacking
- Penetration testing

6.10.3 Conclusion

Results of evaluation are communicated.
Corrective action is advised or taken if needed.
Usually works in cooperation with the organization or sponsor.

Deliverables include:

- Ethical Hacking Report
- Result details of hacking activities
- Detail information on vulnerabilities
- Recommended avoidance measures

6.10.4 Issues for Ethical Hacking

Nondisclosure agreement:

- Ensure the right information is available to conduct security testing
- The integrity of the evaluation team
- The sensitivity of the information

6.11 Legal Implications

6.11.1 Crime Statistics

CSI/FBI 2002 Computer Crime and Security Survey had 90% of respondents acknowledge security breaches, with only 34% reported to law enforcement agencies.

85% to 97% of computer intrusions are not even detected, according to the FBI computer crimes squad.

6.11.2 United States Federal Code on Computer Crimes

Cyber Security Enhancement Act 2002
Enforces life sentences for hackers who recklessly endanger the lives of others, specifically transportation systems, power companies, or other public services or utilities.

18 U.S.C. § 1029 Fraud and Related Activity in Connection with Access Devices

18 U.S.C. § 1030 Fraud and Related Activity in Connection with Computers

18 U.S.C. § 1362 Communication Lines, Stations, or Systems

18 U.S.C. § 2510 Wire and Electronic Communications Interception and Interception of Oral Communications

18 U.S.C. § 2701 Stored Wire and Electronic Communications and Transactional Records Access

6.11.3 Crimes and Criminal Procedure Section 1029

Subsection (a)
Whoever -

(1) Knowingly and with intent to defraud produces, uses, or traffics in one or more counterfeit access devices;
(2) Knowingly and with intent to defraud traffic in or uses one or more unauthorized access devices during any one-year period, and by such conduct obtains anything of value aggregating $1,000 or more during that period;
(3) Knowingly and with intent to defraud possesses fifteen or more devices which are counterfeit or unauthorized access devices;
(4) Knowingly, and intent to defraud, produces, traffics in, has

Copyright The Art of Service

control or custody of, or possesses device-making equipment;

(5) Knowingly and with intent to defraud effects transactions, with 1 or more access devices issued to another person or persons, to receive payment of any other thing of value during any 1-year period the aggregate value of which is equal to or greater than $1,000;

(6) Without the authorization of the issuer or the access device, knowingly and with intent to defraud solicits a person for the purpose of -

A) Offering an access device; or

B) Selling information regarding or an application to obtain an access device;

(7) Knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;

(8) Knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a scanning receiver;

(9) Knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization; or

(10) Without the authorization of the credit card system member or its agent, knowingly and with intent to defraud causes or arranges for another person to present to the member or its agent, for payment, one or more evidences or records of transactions made by an access device.

Penalties:

A) In the case of an offense that does not occur after a conviction for another offense under this section - -

(i) If the offense is under paragraph (1), (2), (3), (6), (7), or (10) of subsection (a), a fine under this title or imprisonment for not more than 10 years, or both; and

(ii) If the offense is under paragraph (4), (5), (8), or (9) of subsection (a), a fine under this title or imprisonment

Copyright The Art of Service

for not more than 15 years, or both;

B) In the case of an offense that occurs after a conviction for another offense under this section, a fine under this title or imprisonment for not more than 20 years, or both; and

C) In either case, forfeiture to the United States of any personal property used or intended to be used to commit the offense.

6.11.4 Crimes and Criminal Procedure Section 1030

Subsection (a)
Whoever--

(1) Having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) Intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

A) Information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

B) Information from any department or agency of the United States; or

C) Information from any protected computer if the conduct involved an interstate or foreign communication;

Copyright The Art of Service

(3) Intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) Knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)

A)

(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and

B) By conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--

(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more

individuals;
(iii) physical injury to any person;
(iv) a threat to public health or safety; or
(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;

(6) Knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--
A) Such trafficking affects interstate or foreign commerce; or
B) Such computer is used by or for the Government of the United States;

(7) With intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer;

Penalties

(1)
A) A fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
B) A fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(8)
A) Except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
B) A fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection

Copyright The Art of Service

(a)(2), or an attempt to commit an offense punishable under this subparagraph, if--

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortuous act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000;

C) A fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(9)

A) A fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

B) A fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4), (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(10)

A) A fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

B) A fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;

C) A fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section.

Copyright The Art of Service

7 Footprinting

- Part of the Reconnaissance phase
- Used to gather as much information as possible
- Involves network scanning without authorization
- Can be done internally or externally

7.1 Defining Footprinting

- The blueprinting of the security profile of an organization
- A methodological technique

- Results in a unique organization profile of the networks and systems involved.

- One of three pre-attack phases
- Other phases include scanning and enumeration

Begins with the determination of the target system, application, and/or the location of the target.
Nonintrusive methods are used to gather specific information, such as:

- Access an organization's web directory or employee bios
- Google or Yahoo! People search
- Blogs
- Newsgroups
- Press releases
- Job postings

Copyright The Art of Service

7.1.1 Google Hacking

Using the Google search engine to perform information gathering.

Uses commands in conjunction to perform searches to locate certain types of vulnerable web applications.
Commands often used include:

Site: – to search a specific website or domain
Filetype: - to search for text within a specific type of file
Link – to search and identify linked pages for a specific term
Cache: - identifies the version of a web page
Intitle – to search for a term within a title of a document
Inurl: – to search for a term within the web address

7.2 Gathering Information

7.2.1 The Information Gathering Methodology

- Uncover initial information
- Locate the network range
- Identify active machines
- Discover open ports / access points
- Detect operating systems
- Uncover services on ports
- Map the network

Footprinting involves uncovering initial information and locating the network range.

7.2.2 Uncovering Initial Information

Utilizes:

- Domain name lookup
- Locations

Copyright The Art of Service

- Telephone contacts
- Mail contacts
- Scanning IP addresses for open ports

Information typically is easy and legal to obtain

Sources of Information

- Open source
- Whois
- Nslookup

Tools used by hackers:

- Sam Spade – a website with a collection of tools such as Whois, nslookup, and traceroute

Ethical hackers should have a thorough understanding of DNS and name resolution on the Internet.

7.2.3 Locating Network Ranges

Includes:

- Finding the range of IP addresses
- Discerning the subnet mask

Sources of information:

- ARIN (American Registry of Internet Numbers)
- Traceroute

Tools used by hackers:

- NeoTrace
- Visual Route

7.3 Competitive Intelligence

Information about a company's:

- Products
- Marketing
- Technologies

Information gathering is typically nonintrusive
Often found in:

- Product comparisons
- Sales and marketing strategies

7.4 DNS Enumeration

A process of locating all DNS services and corresponding records for an organization.
External and internal DNS servers may exist with the appropriate information.
Information sought after include:

- Usernames
- Computer names
- IP addresses

Common Tools utilized:

- Whois
- Nslookup
- DNSstuff
- American Registry for Internet Numbers (ARIN)

Copyright The Art of Service

7.5 Lookups

7.5.1 Whois

Queries the Internet Corporation for Assigned Names and Numbers (ICANN).

Includes information on the Registrant:

- Target company
- Address
- Domain name

Includes information on administrative and technical contacts:

- Name
- Email address
- Physical company address
- Telephone number
- Fax number

Includes information on domain servers:

- Web address
- IP address

7.5.2 Nslookup

A program to query Internet domain name servers.
Included in Unix, Linux, and Windows operating systems
Used to display information to diagnose the Domain Name System (DNS) infrastructure.
Reveals specific users and zone transfers that can compromise DNS security.

Additional IP addresses can be found from authoritative DNS listed in whois.

MX (mail server) record reveals the IP of the mail server.

Third party clients exist, such as

- Sam Spade
- DNSstuff.com

7.5.3 ARIN

A database which includes information on the ownership of static IP addressses.

Allows search on whois database.
Locates information on network autonomous system numbers (ASNs), network-related handles and related point of contact (POC).
allows querying of IP address to identify subnet addressing strategies.
Used for social engineering.

For other regions, the equivalent to ARIN is:

- Europe, the Middle East, and parts of Central Asia (RIPE NCC)
- Latin American and Caribbean Internet Addresses Registry (LACNIC)
- Asia Pacific Network Information Center (APNIC)

7.5.4 SmartWhois

Network information utility to find information about an IP address, host name, of domain.
Information includes:

- Country
- State or province
- City
- Network provider
- Administrative contact information
- Technical support contact information

Differences with standard Whois includes:

- Ability to locate computers in any part of the world
- Queries the right database intelligently
- Delivers output faster

Copyright The Art of Service

7.6 Types of DNS Records

Common DNS record types:

- A (address) – maps a host name to IP address
- SOA (Start of Authority) – identifies the DNS server responsible for domain information
- CNAME (canonical name) – provides additional names or aliases
- MX (mail server) – identifies all domain mail services
- SRV (service) – identifies services like directory services
- PTR (pointer) – maps IP addresses to host names
- NS (name server) – identifies other name servers for the domain

7.7 Using traceroute

A packet-tracking tool available on most operating systems.
Operates by sending an Internet Control Message Protocol (ICMP) echo to each hop along a communication path.
A hop can consist of a router or gateway.

Works by exploiting a feature of TTL, or Time To Live.
TTL is an Internet Protocol.

Reveals the path IP packets travel between two systems.
Path is derived by sending out consecutive UDP packets with ever-increasing TTLs.
Used to target specific IP addresses and aids in IP spoofing.

Each router which processes an IP packet decrements the TTL.
When the TTL reaches zero, a “TTL exceeded” message is sent back to the originator.
Can identify the number of hops between two systems.

Copyright The Art of Service

Routers with DNS entries reveal:

- The name of routers
- Network affiliations
- Geographic locations

Can identify a firewall or packet-filtering router when traceroute times out. Timeouts are indicated by a asterisk in the record.

7.7.1 NeoTrace (McAfee Visual Trace)

Shows traceroute output visually:

- Map views
- Node views
- IP views

7.7.2 VisualLookout

Provides different views to traffic information, including:

- High level views
- Detailed views
- Historical views

Will provide real-time and historical information.

Ability to provide a view of active network connections identifying:

- Who is connected
- What services are being used
- Inbound and outbound connections
- The number of active connections
- Time lapse of active connections

Copyright The Art of Service

7.8 E-mail Tracking

Allows the sender of an e-mail to know if the recipient reads, forwards, modifies, or deletes an e-mail.

Works by appending a domain address to the e-mail address.
A single-pixel graphic file is attached to the e-mail.
The graphic file connects back to the server when action is performed on the e-mail.

7.8.1 emailTrackerPro

An e-mail analysis tool.
Enables automatic analysis of an e-mail and its headers.
Provides graphical results.

7.8.2 Mail Tracking

An e-mail tracking service.
Allows users to track when mail is read, for how long and how many times.
Records forwards and passing of sensitive information.

7.9 Web Spiders

Combs websites which collect information such as e-mail addresses.
Uses syntax characters such as @ symbol to locate desired information.
Information is found and copied into a list.

Can automate the information gathering process.

Web spiders can be prevented by creating a robots.txt file in the root of the website.
A list of directories to protect must accompany the file.

Copyright The Art of Service

8 Social Engineering

A nontechnical approach to breaking into a system of network.
Typically involves deception or coercion.
Attacks the human element of the system.

8.1 Defining Social Engineering

The influence and persuasion of individuals for the purpose of obtaining information or coercing the victim to perform some act.
Common tools for social engineering:

- Internet
- Telephone

Used to exploit the natural tendencies and trust of a person.
Includes the gathering of sensitive information or access privileges.
Often involves appearing as a part of the organization.

8.2 Common Types of Attacks

Human-based attacks – person-to-person interaction to retrieve desired information.
Computer-based attacks – having computer software retrieve the desired information, also known as phishing.

8.2.1 Human-Based Attacks

- Impersonation of employee or user
- Pose as an executive or manager and use intimidation on lo-level employee
- Pretend to have permission from an authorized source
- Calling technical support for assistance
- Shoulder surfing, typically for gathering passwords
- Looking through trash for information, or dumpster diving

Copyright The Art of Service

8.2.2 Computer-Based Attacks

- E-mail attachments
- Fake websites
- Popup windows
- SPAM

8.3 Insider Attacks

Infiltrate the organization by:

- Getting hired as employee
- Finding a disgruntled employee

Powerful because of the physical access to the organization and freedom to move inside.

8.4 Identity Theft

Poses as an employee or steals the identify of the employee to perpetrate an attack.
Goal is to create a persona that can enter the organization unchallenged.

8.5 Phishing

Involves sending an e-mail.
The sender poses as a financial organization.
Types of phishing:

- Requests the confirmation of banking information, passwords, or PIN numbers
- Need assistance moving large amounts of money out of the country

Copyright The Art of Service

8.6 Online Scams

Poses as websites with free or special offers.
Victim enters a username and password.
The hope is the username and password is the same for accessing work systems.

Sending malicious code to the system as e-mail attachments.

Use of popup windows with free or special offers.
Entices users to take action, which inadvertently installs malicious software.

8.7 URL Obfuscation

Used in phishing attacks.
Some online frauds make the method seem legitimate.

The intent is to lead the user to a hidden or fake URL (Uniform Resource Locator) which appears to be legitimate.

Obfuscation typically uses hexadecimal or decimal notation.

8.8 Countermeasures

- Documenting and enforcing security policies
- Conducting security awareness programs
- Continual communication and education

Security policies should involve:

- How and when accounts are set-up and terminated
- Password changes
- Identifying who can access what information
- How violations to policies will be handled
- Destruction of paper documents
- Physical access restrictions
- Control of modem access
- Virus controls

Copyright The Art of Service

9 Scanning

Another pre-attack activity.
Typically involves making request to systems and networking elements to determine what services are being offered or filtering.
Used to detect 'live' systems on a target network:

- Determines the perimeter of the target network or system
- Facilitates network mapping
- Builds an inventory of accessible systems

Tools used:

- War Dialers
- Ping Utilities

9.1 Define Scanning

Scanning is used to determine the availability of a system on the network.

Scanning tools gather information about a system such as IP addresses, operating systems and services, which may be running on the system.

'Live' is a term referring to networked devices that are available, responsive, and open to attack.

Countermeasures are the processes and tools sets used to detect and prevent malicious activity.

9.1.1 Port Scanning

Port scanning refers to gathering information about open TCP/IP ports and services on the system.

Port numbers are associated with services or applications on a machine.

Copyright The Art of Service

Port scanning tools allow hackers to learn about the services available on a given system.

The most commonly known ports are:

20	FTP data
21	FTP controlled
22	Secure Shell (SSH)
23	Telnet
25	SMTP
39	RLP
53	DNS
80	HTTP
88	Kerberos
110	POP3
115	SFTP
118	SQL
137	NetBIOS Name Servive
138	NetBIOS Datagram Service
139	NetBIOS Session Service
143	IMAP
156	SQL Service
161	SNMP
194	IRC
443	HTTP over TLS/SSL
444	SNPP
445	SMB over TCP/IP
593	HTTP RPC

9.1.2 Network Scanning

Network scanning focuses on identifying IP addresses.

Looks for active hosts on the network for purposes of security assessments or attack.

Network hosts are identified by their IP addresses.

Network scanning tools look for all live or hosts on the network and their IP addresses.

Copyright The Art of Service

9.1.3 Vulnerability Scanning

Vulnerability scanning attempts to identify weaknesses within the current system.

Typically, will identify the operating system and version number, including any installed service packs.

With this information, the vulnerability scanning looks for any weaknesses in the operating system, which can be exploited later.

9.1.4 Detection of Scanning

Active port-scanning activity can be detected using an intrusion detection system (IDS).

Scans can be recognized when they probe TCP/IP ports.

9.1.5 Passive Scans

A passive scan to identify open application ports on remote systems.
Happens during communication setup.
A SYN packet is sent to the target system on a specific application port.
The desired result is a response.

- An acknowledgment indicates the port is open and the service is accepting connections.
- A reset identifies the port as closed or being filtered
- No response typically means the port is being blocked, especially when other ports are responding.

The reply is dropped with no acknowledgment of receipt.

9.1.6 Active Scans

Similar to passive scans.
Used to discover ghost open ports, such as a firewall or load-balancing system.

Copyright The Art of Service

The reply is not dropped and an acknowledgment of the reply is sent. The purpose is to test the ability to establish communications with the remote system.

9.1.7 Interactive Scans

Connects to the service.
Exchanges commands and response.

Used to learn about the system.

9.2 CEH Scanning Methodology

The process which a hacker scans the network.

Ensures nothing is overlooked.

9.2.1 Method

- Check for live systems
- Check for open ports
- Identify services
- Banner grabbing and OS fingerprinting
- Vulnerability scanning
- Draw network diagrams of vulnerable hosts
- Prepare probes
- Attack

9.3 Ping Sweeps

Checks for systems, which are live on the network.
Simple technique, but not the most accurate.

Sends an ICMP request to all hosts on the network.

Copyright The Art of Service

Multiple requests can be done in parallel.
Intent is to obtain a response indicating a live system.

Ping sweeps allow network mapping by polling network blocks and/or IP address ranges.

Ping Utilities used by hackers:

- WS_Ping ProPack
- NetScan Tools
- Hping
- icmpenum

Ping Sweep Detection Utilities include:

- Network-based IDS
- Genius
- BlackICE
- Scanlogd

9.3.1 Technique Used

An ICMP Echo Request packet is sent out and waits for an ICMP Echo Reply message to return from an active machine.
Alternatively, TCP/UDP packets are sent if ICMP messages are blocked.
The network traffic is assessed by time stamping each packet.

Ping can also resolve host names.

Ping Sweeps are most effective after a home is based within the network has been established.

9.3.2 Detecting Ping Sweeps

Any IDS or intrusion prevention system (IPS) will detect a ping sweep and alert the security administrator.

Most firewalls and proxy services block ping responses.

9.3.3 Identifying Open Ports and Services

If ping sweeps are blocked, the next step is port scanning.

Involves probing each port on a host to identify which are open.
Generally provides more information than a ping sweep

Service identification is the next step.
Uses the same tools as port scanning.
The services available are associated with the port, which are open.

9.3.4 Countering Port Scans

Proper security architectures including:

- IDS
- firewalls

Firewalls should perform stateful inspections: examination of the data of the packet and not just the header to identify authority.
Network IDS used to identify OS detection activities.

Only required ports should remain open; the rest blocked or filtered.
Continual testing of scanning countermeasures.
Continual security awareness training.

9.4 Nmap Command Switches

Nmap is an open source tool, which is quick and efficient.
Performs:

- Ping sweeps
- Port scans
- Service identification
- IP address detection
- Operating system detection

Can scan large numbers of hosts in a single session

Copyright The Art of Service

9.4.1 Port States

Nmap determines the state of the port:

- Open – the target is accepting incoming requests on the port
- Filtered – a firewall or network filter is in place
- Unfiltered – no firewall or network filter exists and the port is closed

9.4.2 Common Scan Methods

- TCP connect – a full TCP connection is made with the target system
- XMAS tree scan – TCP services are checked by sending XMAS-tree packets: all "lights" are on with the FIN, URG and PSH flags set
- SYN stealth scan – known as "half-open scanning" because a full TCP connection is not opened. A SYN packet is sent and a SYN-ACK is received
- Null scan – all flags are off or not set which allows passing through UNIX firewalls undetected of modified
- ACK scan – used in the UNIX environment to map out firewall rules
- Windows scan - similar to the ACK scan in the Windows environment, but also detects open ports

9.4.3 Common NMAP Commands

Used to perform different types of scans:

-sT	TCP connect scan
-sS	SYN scan
-sF	FIN scan
-sX	XMAS tree scan
-sN	Null scan
-sP	Ping scan
-sU	UDP scan
-sO	Protocol scan
-sA	ACK scan
-sW	Windows scan
-sR	RPC scan

Copyright The Art of Service

-sL	List / DNS scan
-sI	Idle scan
-Po	Don't ping
-PT	TCP ping
-PS	SYN ping
-PI	ICMP ping
-PB	TCP and ICMP ping
-PB	ICMP timestamp
-PM	ICMP netmask
-oN	Normal output
-oX	XML output
-oG	Greppable output
-oA	All output
-T Paranoid	Serial scan; 300 sec between scans
-T Sneaky	Serial scan; 15 sec between scans
-T Polite	Serial scan; .4 sec between scans
-T Normal	Parallel scan
-T Aggressive	Parallel, 300 sec timeout, 1.25 sec/probe
-T Insane	Parallel, 75 sec timeout, .3 sec/probe

9.5 Types of Scans

CEH should be familiar with SYN, Stealth, XMAS, NULL, IDLE and FIN scans.

9.5.1 SYN scans

Also referred to as stealth or half-open scan.
Does not complete the TCP three-way handshake.

A SYN packet is sent to a target.
If a SYN/ACK frame is sent back, the connection is assumed and the port is listening.
If a RST frame is sent back, the post is assumed inactive or closed.

Fewer IDS system log SYN scans as an attempted attack.

Copyright The Art of Service

9.5.2 XMAS scans

Sends packets with the FIN, URG, and PSH flags sets.
If there is no response, the port is open.
If the response is a RST/ACK packet, the port is closed.

Works only on UNIX.
Works only on systems following the TCP/IP implementation of RFC793.

9.5.3 FIN scans

Similar to XMAS scans.
Receives the same response and limitations as XMAS.

The packet sent contains only the FIN flag set.

9.5.4 NULL scans

Similar to XMAS and FIN scans.
Sends out a packet with no flags set.

9.5.5 IDLE scans

Send a SYN packet using a spoofed IP address.
Port scan response is determined through the monitoring of IT header sequence numbers.
Through this, the port can be identified as open or closed.

Copyright The Art of Service

9.6 TCP Communication Flag Types

TCP scans are built on the TCP three-way handshake.
A three-way handshake is required before a connection is made and data is transferred.

The handshake consists of:

- Sender sending a TCP packet with a synchronized (SYN) bit set
- Receiver responds with a SYN bit set and an acknowledgment (ACK) bit set
- Sender responds with an ACK bit set to complete the connection

TCP is a connection-oriented protocol, used to:

- Establish a connection
- Restart a failed connection
- Finish a connection

Uses flags to manipulate the TCP protocol with the intent to bypass detection.

9.6.1 TCP Flag Types

SYN – Synchronize	initiates a connection
ACK – Acknowledge	establishes a connection
PSH – Push	forwarding buffered data
URG – Urgent	data must be processed quickly
FIN – Finish	no more transmissions
RST – Reset	resets a connection

9.6.2 TCP Scan Types

XMAS scan	All flags set (SYN, ACK, PSH, URG, FIN, RST)
FIN scan	FIN set
NULL set	No flags set

Copyright The Art of Service

TCP connect	SYN, then ACK
SYN scan	SYN, then RST

9.6.3 Hacking Tools

IPEye is a TCP port scanner that performs SYN, FIN, Bull, and XMAS scans.
Probes the target ports and responds with either:

- Closed – computer exists but is not listening
- Reject – firewall is rejecting the port connection
- Drop – no computer exists or the firewall is dropping everything to the port
- Open – some service is listening at the port

IPSecScan is a tool, which can scan a single IP address, or a range of addresses that are IPSec enabled.

Scanning tools that can be used to fingerprint the operating system include:

- Netscan Tools Pro 2000
- Hping2
- KingPingIcmpenum
- SNMP Scanner

Hping2 has additional capabilities such as TCP, UDP, ICMP, and raw-IPping protocols, traceroute, and can send files between hosts.

Icmpenum will probe the network using ICBM Echo packets, ICMP timestamp and ICMP Information packets and supports spoofing and sniffing.

SNMP Scanner allows a range of hosts to be scanned using ping, DNS, and SNMP queries.

9.7 War Dialers

Process of dialing modem numbers to find an open modem connection.
Purpose is to gain remote access to a network.

A war dialer is used to scan large pools of telephone numbers with the intent to detect vulnerable modems as a means to access the system.
A demon dialer is used to monitor a specific phone number and target its modem to gain access to the system.

Highly advantageous against poorly configured remote access products.
Works on the assumption that organization's have weaker security mechanisms in place for remote systems.
Many servers still utilize telephone connections as backups in case the primary Internet connection is disrupted.

9.7.1 Tools Used

Tools used by hackers:

- THC-Scan
- ToneLoc
- TBA

9.8 Banner Grabbing and OF Fingerprinting Techniques

Often called “fingerprinting” the TCP/IP stack.
Fourth step of the CEH scanning methodology.

Allows vulnerable or high value targets on the network to be identified.

Copyright The Art of Service

9.8.1 Banner Grabbing

The process of opening a connection and reading the response, or banner, sent by an application.
Email, FTP, and web servers will respond to a telnet connection with the name and version of the software.
This information aids in fingerprinting the OS and application software.

9.8.2 Fingerprinting

Two forms of fingerprinting found:

- Active stack
- Passive stack

Active stack fingerprinting involves sending data to a system to see how the response is.
Various operating system vendors implement the TCP stack differently which results in different responses from the system.
The responses are connected to different operating systems.
Is detectable because the same target repeatedly receives connect attempts.

Passive stack fingerprinting examines the traffic on the network.
Uses sniffing techniques rather than scanning.
Usually is undetected but is less accurate than active fingerprinting.

9.9 Proxy Servers

The last step in the CEH scanning methodology.

Proxy server – a computer acting as an intermediary between the hacker and the target.

Allows a hacker to become anonymous on the network.
Makes a connection with the proxy server.

Requests a connection to the target through the proxy server.

9.9.1 Tools for Hackers

SocksChain provides the ability to attack through a chain of proxy servers.
The more proxy servers used in series, the harder to detect the hacker.
The chain is broken when one of the log files is lost or broken.

9.10 Anonymizers

Services that utilizes a website to make web surfing anonymous.
Acts as a proxy service for the web client.
Removes all identifying information from a computer while the Internet is surfer to ensure privacy.

The address of the target website is entered into the anonymizer software.
The software makes the request to the target website.
All subsequent requests and web pages are relayed through the anonymizer.

9.11 HTTP Tunneling Techniques

Used to bypass a firewall or IDS.
A blocked protocol is tunneled through an allowed protocol.

Most IDS and firewalls act as proxies between the client and the Internet.
Traffic using HTTP protocol is typically allowed because web access is benign.
The proxy can be subverted using a HTTP tunneling tool to hide destructive protocols.

Copyright The Art of Service

9.11.1 Hacking Tools Used

Common HTTP Tunnelers include:

- HTTPort
- Tunneld
- BackStealth

Will allow potentially destructive protocols to be used, such as:

- e-mail
- IRC
- ICQ
- News
- AIM
- FTP

9.12 IP Spoofing Techniques

Used during scanning to minimize the chance of detection.
Spoofing an IP address does not allow TCP sessions to be completed successfully.

Source routing allows a route to be specified for the packet through the Internet.
Firewalls and IDS, which can block or detect an attack, can be bypassed because of this specification.
A reply address is used in the IP header to return the packet to a spoofed address instead of a real address.

IP address spoofing is detectable by comparing the time to live (TTL) values of the real and spoofed addresses.

10 Enumeration

Happens after scanning.
A process for gathering and compiling:

- Usernames
- Machine names
- Network resources
- Shares
- Services

Refers also to the active connecting and querying of a target system to information gathering.

10.1 Define Enumeration

The object is to identify a user or system account for use during a potential attack.
Used to identify each domain present within the LAN.
Most account privileges can be escalated to allow the account more access than originally granted.

Hacking tools are designed to locate NetBIOS name information, which includes:

- IP address
- NetBIOS computer name
- Username logged under
- MAC address information

Net View is a built-in tool for Windows 2000 used for NetBIOS enumeration.
To enumerate NetBIOS names:

- net view / domain
- nbtstat -A IP address

Copyright The Art of Service

10.1.1 Hacking Tools Used

DumpSec is a NetBIOS enumeration tool connecting to target systems as a null user

Hyena enumerates NetBIOS shares and will exploit null session vulnerabilities to change the share path or edit the registry on the target system.

SMB Auditing Tool is a password-auditing tool for Windows and SMB (Server Message Block) platforms to identify usernames and crack passwords on systems.

NetBIOS Auditing Tool is an enumeration tool used to perform various security checks on remote services using NetBIOS file sharing services.

10.2 Null Sessions

A null session exists when a systems is logged into using no username or password.
Capitalizes on vulnerabilities found in the CIFS (Common Internet File System) or SMB based on the operating system.

Allow s full dumps of large amounts of information including:

- Lists of usernames
- Lists of groups
- Lists of machines
- Lists of shares
- Lists of permissions
- Lists of policies
- Lists of services

SMB and NetBIOS standards in Windows include APIs, which returns information about a system through TCP port 139.

10.2.1 Connecting a Null Session

One method is to use the IPC$ (Inter-Process Communications) share.
Used to share data between applications and computers.

Connecting to the IPC$ share can be done using the net use command:

```
net use \\IP\IPC$ “” /u:””
where 'IP' is the actual IP address used
```

10.2.2 Countermeasures Available

Specific port numbers are used on target machines:

- 135 – MS-RPC Endmapper
- 137 – NetBIOS Name Service
- 138 – NetBIOS Datagram Service
- 139 – NetBIOS Session Service
- 445 – SMB over TCP/IP

Closing these ports will prevent enumeration.

To close ports on client:

- Open the properties of the network connection
- Click TCP/IP
- Click Properties button
- Click Advanced button
- In the WINS tab, select disable NetBIOS over TCP/IP

Restricting anonymous users from logging in, a security administrator can edit the registry:

- Open regedit32
- Navigate to HKLM\SYSTEM\CurrentControlSet\LSA
- Choose Edit > Add Value
- Enter the values:

Value Name:	Restrict Anonymous
Data Type:	REG_WORD
Value:	2

Upgrading to Windows XP and the latest Microsoft security patches will mitigate null session vulnerabilities.

Copyright The Art of Service

10.2.3 SNMP Enumeration

Uses SNMP to enumerate user accounts on a target system.
Two major types of software components used for communication:

- the SNMP agent located on the networking device
- the SNMP management station with communicates with the agent

Most network infrastructure devices have a SNMP agent.
SNMP agents manage the system or devices.
The management station sends requests to the agent who sends back replies.
Configuration variables used by the agent are within the requests and replies.
On the network device is a database of configuration variables, called the Management Information Base (MIB).

Traps let the management station know of any significant events in the agent's software such as an interface failure or reboot.

Two passwords are used to access and configuration the SNMP agent from the management station:

- The read community string allows the configuration to be viewed
- The read/write community string allows the configuration to be changed

The default of the first password is public and the second, private.
A common security loophole is where the default settings are maintained.

10.2.4 Hacking Tools Used

SNMPUtil is a SNMP enumeration tool.
Gathers Windows user account information such as:

- Routing tables
- ARP tables
- IP addresses
- MAC addresses
- TCP and UDP open ports
- User accounts
- Shares

IP Network Browser uses SNMP to gather more information about a device containing a SNMP agent.

10.2.5 SNMP Countermeasures

To prevent SNMP enumeration:

- Remove the SNMP agent on potential target systems
- Turn off the SNMP service
- Change the default passwords for the read and read/write communities
- Implement the Group Policy option “Additional Restrictions For Anonymous Connection

10.3 Windows 2000 DNS Zone Transfer

Service (SRV) records are used to locate Windows 2000 domain services, such as Active Directory and Kerberos.
Every Windows 2000 Active Directory domain must have a DNS server in place to operate properly.

A zone transfer can enumerate network information using nslookup.
The command to enumerate:

nslookup ls -d *domainname*

Copyright The Art of Service

Additional information available using tags, such as:

gc,tcp	Global Catalog service
_ldap._tcp	Domain controllers
_kerberos._tcp	Kerberos authentication

10.3.1 Zone Transfer Countermeasures

Zone transfers can be blocked in the properties of the Windows DNS server.

10.3.2 LDAP Enumeration

An Active Directory database is based in a Lightweight Directory Access Protocol (LDAP).
Existing users and groups in the database can be enumerated with a simple LDAP query by creating an authenticated session.

A Windows 2000 LDAP client called the Active Directory Administration Tool (ldp.exe) connects to an Active Directory service and exposes the contents.

An enumeration attack is performed by:

- Connect to any Active Directory service using ldp.exe on port 389.
- Server information will be displayed when the connection is complete.
- Choose to authenticate on the Connection Menu.
- Type in username, password, and domain name
- Choose the Search option from the Browse menu to enumerate users and groups.

Copyright The Art of Service

10.4 Performing Enumeration

- Extract usernames using enumeration.
- Gather information about the host during a null session
- Perform Windows enumeration using the Superscan tool
- Acquire the user accounts using the GetAcct tool
- Perform SNMP port scanning

10.4.1 System Hacking

The system hacking cycle consists of six steps:

- Enumeration
- Cracking passwords
- Escalating privileges
- Executing applications
- Hiding files
- Covering tracks

System hacking is the point where information gathering ends and the efforts can be considered breaking and entering,
It is achieved through an administrative connection of an enumerated share.

10.5 Password Cracking Techniques

Passwords are a key component to access a system.
Most passwords are prone to be cracked, due to:

- Users keeping them simple to remember
- Making them relevant to their lives
- Reusing passwords

Accounts where password cracking is focused on include:

- Account that have not change passwords
- Accounts the user never logged in
- Accounts with information in the comment field that may compromise security

Copyright The Art of Service

- Service accounts
- Shared accounts

Passwords can be cracked manually or through automated tools.

Manual password cracking involves:

- Find a valid user account
- Create a list of possible passwords
- Rank probability of passwords
- Key in each password
- Try again until successful

A script file can be created to try each password.

An efficient method of cracking passwords is to gain access to the password file on the system.
Passwords are stored:

- In the Security Accounts Manager (SAM) file on a Windows system
- In a password shadow file on a Linux system

Hacking tools used to crack passwords include Legion, NTInfoScan, LOphtCrack, Jack the Ripper, and KerbCrack.

10.5.1 LanManager Hash

Windows 2000 uses NT Lan Manager (NTLM) hashing to secure passwords in transit.
The weaker the password, the weaker the NTLM hashing and the easier the password is to break.

The password is encrypted with the NTLM algorithm:

- Converted to all uppercase
- Padded with blank characters to be a minimum of 14 characters
- Split in half with each string being 7 characters long
- Each string is individually encrypted
- Each string is concatenated

If the password is fewer than seven characters, the second half will be all blanks and always be AAD3B4B51404EE.

10.5.2 Windows 2000 Passwords

The username and hashed passwords are stored in the Windows SAM file.
The SAM file is located in Windows\systems32\config directory.

When Windows is running, the file is locked.
To obtain the file:

- Boot to an alternate operating system and copy the file
- From the repair directory, extract a compressed copy called SAM._ which was created when the system was backed up.

The file can be uncompressed with the command:

```
C:\>expand sam._ sam
```

Tools used to crack Windows 2000 passwords include the Win32CreateLocalAdminUser and Offline NT Password Resetter.

10.5.3 SMB Logon Redirection

The Server Message Block (SMB) logon can be redirected to an attacker's computer as a means to discovering passwords.
The process includes:

- sniffing out the NTLM responses from the authentication server
- tricking the victim into attempting Windows authentication with the attacker's computer

A popular trick is sending an e-mail message with an embedded hyperlink to a fraudulent SMB server, which will have the victim sending their credentials.

Some tools that utilize SMB redirection is SMBRelay, SMBRelay2, pwdump2, Samdump, C2MYAZZ.

Copyright The Art of Service

10.5.4 SMB Relay MITM Attacks

The attacker creates a fraudulent server with a relay address.
The victim client attempts to connect to the server.
A MITM server intercepts the call, hashes the password, and passes the connection to the server.

MITM stands for Man-In-The-Middle.

The countermeasure used against SMB relays is configuring Windows 2000 to use SMB signing which cryptographically each block of SMB communications.

Hacking Tools used in SMB relays are SMBGrind, SMBDle, and NBTdeputy.

10.5.5 NetBIOS DoS Attacks

Denial of Service (DoS) attacks sends NetBIOS Name Release messages to the NetBIOS Name Service on the target Windows system.
The system is forced to place its name in conflict.
When the name is in conflict, the name can't be used, blocking the client from participating in the NetBIOS network.

10.5.6 Countermeasures Against Password Cracking

Users should create “strong” passwords, which have 8-12 alphanumeric characters.

Physically isolating the server will protect against cracking the hashing algorithm.
The SYSKEY utility can be used to add greater protection to hashes.
Monitoring of server logs against brute force attacks on user accounts is recommended.

The effectiveness of brute force attacks can be decreased by:

- Never using the default password
- Never using a password that can be found in a dictionary

- Never use a password that can be found with whois like the host name or domain name
- Never use a password tied to family, important dates, pats, or hobbies

Passwords should be changed and expire after a certain period.
If the time interval is too short, users are prone to forgetting.
If the time interval is too long, security has a greater risk of compromise.
The recommended time interval is thirty days.
Users should not be allowed to reuse the last three passwords.

Monitoring Event Viewer logs can identify intrusion attempts before when they are in progress.
Typically, several failed attempts will occur before being successful.

In windows, the event logis located:

```
c:\\windows\system32\config\Sec.Event.Evt
```

10.6 Types of Passwords

Passwords can be formed using:

- Only letters
- Only numbers
- Only special characters
- Letters and numbers
- Letters and special characters
- Numbers and special characters
- Letters, numbers and special characters

The stronger the password, the less susceptible to attack.

Recommended password creation includes:

- Not including any part of the user's account name
- Having a minimum of eight characters
- Containing characters from at least three categories
    - special characters
    - numbers
    - uppercase characters

Copyright The Art of Service

- lowercase characters

10.6.1 Types of Password Attacks

Passive online – listening in on network password exchanges using sniffing, MITM, and replay attacks.

Active online – guessing the administrator password and typically involves automated password guessing.

Offline – Dictionary, hybrid, and brute-force attacks.

Nonelectronic – shoulder surfing, keyboard sniffing, and social engineering.

10.6.2 Passive Online Attacks

Sniffing can be performed on wired and wireless networks.
Will not be detectable to the end user.
The password is captured when it is being authenticated.
It is compared to against a dictionary file or word list.
It is typically encrypted or hashed.
Special tools can be used to break the encryption algorithm.

MITM attacks intercept the authentication request and forward it to the server.
Inserting a sniffer between client and server will sniff both connections and capture passwords.

A reply attack intercepts the password to the authentication server and captures the authentication packet to be resent later.
Breaking or learning the password is not required because the actual authentication packet is still in place.

10.6.3 Active Online Attacks

Password guessing is the easiest method of gaining Administrator-level access to a system.

Typically involves connected to an enumerated share and attempting different account and password combinations.
The most commonly used Administrator account and password combinations include words like:

- Admin
- Administrator
- Sysadmin
- Password
- or no password at all

Generating dictionary files, word lists, and multiple combinations for possible passwords can be done quickly using automated programs.

An easy method for automating password guessing uses the standard NET USE syntax within the Windows shell commands.
A simple script can be built:

- Using Windows notepad, create a username and password file.
- Save the file as c:\> credentials.txt.
- Pipe this file using the FOR command:
  C:\> FOR /F “token=1, 2*” %i in (credentials.txt)
- To use the credentials.txt file, type:
  net use \\targetIP\IPC$ %i /u: %j
  where targetIP is the IP addresses of the target

Most systems prevent password guessing by setting the maximum number of login attempts possible.

Other forms of defense against of password guessing include:
Biometrics – using the characteristics such as fingerprints, hand geometry scans, and retinal scans.
Two-factor authentication – requires two forms of identification, typically sometimes physical like a smart card and something known by the user such as a password.

Copyright The Art of Service

10.6.4 Offline attacks

Performed at a location other than the actual computer where the password is used or resides.
Typically involves gaining physical access to the computer and copying the password file to removable media.
The password file is taken to another computer to crack.

Types of offline attacks include:

- Dictionary attack – uses passwords from a list of dictionary words
- Hybrid attack – substitutes numbers or symbols for password characters
- Brute-force attack – tries all possible combinations of letters, numbers,and special characters

A dictionary attack is the simplest and quickest offline attack.
Used when the password is an actual word which can be found int eh dictionary.
Typically, the word is derived from a list and run through the same algorithm used by the authentication process.
The hashed dictionary words are compared with the passwords in the file as the user logs on.

A hybrid attack starts with the dictionary files and substitutes numbers and symbols for characters in the password.
Many users already use common substitutions to create stronger passwords, substituting:

- One (1) for the letter L
- Three (3) for the letter E
- Zero (0) for the letter O
- 1 at the end of a password

The brute-force attack takes the most time to perform.
Tries every combination of letters, numbers, and symbols.

Copyright The Art of Service

10.6.5 Non-electronic Attacks

Utilizes:

- Social engineering - one-on-one interaction to obtain information
- Shoulder surfing – looking over someone's shoulder as they type a password
- Dumpster diving – looking through trash for information

10.7 Escalating Privileges

A method that adds more rights and permissions to a user account. Can turn a regular account into an administrator account.

Administrative accounts typically have stricter password requirements and protected more.
Administrative access is required to install programs.

Tools to escalate administrative privileges include GetAdmin.com and Hk.exe.

10.7.1 Executing Applications

With administrative access, a hacker can install:

- Backdoors
- Keystroke loggers
- Copy files
- Cause other problems

Once applications can be executed, the system is considered “owned.”

Hacking tools that aid in executing applications on target systems include PsExec and Remoxec.

Copyright The Art of Service

10.7.2 Buffer Overflows

Used to exploit a flaw in an application's code.
Forces an application error by sending a field variable more information than it can handle.

The application will either executes a command in the overflow data or provides a command prompt to have the user enter the next command.
The goal of the hacker is to obtain the command prompt or shell.

Access to the command shell allows the hacker to execute other applications.

10.8 Spyware Technologies

For cracking passwords, keystroke loggers are a popular alternative when other attempts fail.
Also called keyloggers.
Can be hardware or software.
Sit between the keyboard and the operating system.
Records every keystroke made by the user.

To install hardware, physical access to the computer is required.
To install software, keyloggers are typically deployed by Trojans or viruses.

10.8.1 Other Spyware Technologies

Spector records everything that is done by a system on the Internet by taking snapshots of what is on the computer screen.

Anti-spector is used to detect and remove Spector.

eBlaster captures incoming and outgoing e-mails and forwards them to another e-mail address. Can also be used to capture IM conversations, perform keylogging, and record visited websites.

SpyAnywhere views system and user activities as well as control open programs and windows from a remote system.

Invisible KeyLogger Stealth (IKS) Software Logger records all keystrokes in a binary keystroke file.

Fearless Key Logger is a Trojan, which resides in memory to capture all user heystrokes.

E-mail Keylogger logs all e-mails sent and received on a target system.

10.9 Hiding Files

To prevent detection, hiding files is critical.
Methods for hiding files include:

- Using the attrib command in the command prompt.
- Using NTFS alternate data streaming

10.9.1 Alternate Data Streams

Allows data to be stored in hidden files, which are linked to a normal, visible file.

To create and use a NTFS file stream:

- enter notepad test.txt at the command line
- add data, save and close Notepad
- enter dir test.txt at the command line (note the file size)
- enter test.txt:hidden.txt at the command line
- add data, save and close
- ensure the file size is the same as step three
- open test.txt to see that only the original data is shown
- enter test.txt:hidden.txt at the command line should provide a syntax error message

Copyright The Art of Service

10.9.2 Countermeasures to NTFS Streaming

To delete a stream file:

- Copy the first file to a FAT partition
- Copy the file back to a NTFS partition

This will lose the stream since they only work on the NTFS partition.

10.10 Rootkits

Used to hide utilities on a compromised system.
Typically includes back doors to access the system easily later.

Types of rootkits that exist include:

- Kernel-level
- Library-level
- Application-level

Kernel-level rootkits will add code to replace a portion of the kernel code to hide a back door.
The added code is done through a device driver or loadable module.
Highly difficult to detect without the appropriate software.

Library-level rootkits will patch, hook, or replace system calls with versions that hide information.

Application-level rootkits will either replace regular application binaries with fake Trojans or modify the behavior of the application using hooks, patches, or injected code.

10.10.1 Rootkits on Windows 2000 and NP

Rootkits are typically kernel mode drivers.
Loaded dynamically at runtime.
Has access to all the resources of the operating system.

Also aids the hacker by:

- Hiding processes
- Hiding files
- Hiding registry entries
- Intercepting keystrokes
- Cause system errors
- Redirects executable files

The kernel mode device driver is called _root_.sys.
A launcher program is called DEPLOY.EXE.

Once a target system is accessed, the files are copied.
DEPLOY.EXE is executed and the device driver is installs.
DEPLOY.EXE is deleted to hide the hacker's activities.
The rootkit can be stopped and restarted whenever desired.

10.10.2 Rootkits Embedded TCP/IP Stack

- Provides a stateless TCP/IP stack.
- Determins the state of the connection based on data from the incoming packet.
- Used raw Ethernet connections to the system's network card.
- Any port on the system can be telneted.

10.10.3 Countermeasures to Rootkits

A rootkit requires administrator access, so securing passwords is critical.

If a rootkit is detected, critical data should be backed up and the operating system and application reinstalled.

The MD5 checksum utility can aid in detecting changes to files.
Acts as a fingerprint to the file.
When a file is changed by even one bit, the checksum value changed.
Comparing files can determine the integrity of the file/
Tripwire is a helpful tool to check the MD5 checksum.

Copyright The Art of Service

10.11 Steganography

A process of hiding data in other types of data.
The most popular method uses graphics as hiding places.

Detection is difficult.
Done by analyzing patterns and changes to the color palette.

10.11.1 Stenography Tools

- ImageHide will hide large amounts of text in an image.
- Blindside hides information inside Bitmap images.
- MP3Stego will hide information in MP3 files during compression.
- Snow will conceal messages in ASCII text using whitespace.
- Camera.Shy will use GIF files to hide information.
- Stealth will hide information in PGP files.

10.11.2 Countermeasures to Stegnography

Stegdetect works to find hidden text in images.

Dskprobe is a low-level harddisk scanner

10.12 Covering Tracks

The longer detection can be avoided, the longer the attack can persist.

10.12.1 Disabling Audits

Auditing records certain events in a log file stored in the Windows Event Viewer.
Logging in to the system, applications, or the event log are crucial events to be found in the Event Viewer.
The administrator can choose the level of logging on the system. This level should be determined to identify whether events should be cleared which could identify any presence of hacking.

AuditPol in the Windows NT Resource Kit can enable or disable auditing.

10.12.2 Clearing the Event Log

Even with disabling audits, the event log should be cleared of some events.
Too many events cleared can indicate intrusion.

Tools used to clear the log include:

- elsave.exe utility
- winZapper
- Evidence Eliminator

Copyright The Art of Service

11 Trojans and Backdoors

Methods for gaining access to a system.
Must be installed by another program or by the user without their knowledge.

Backdoor – a program or set of related programs to allow access to a system at a later time.
They allow:
remove evidence of initial entry
retain access to a penetrated machine even after detection

Backdoors are often disguised by adding a new service.

Remote administration Trojans (RATs) are a class of backdoor that allows remote control over a compromised machine.
RATs hook into the victim's operating system.
The infected machine becomes a server to the intruder's client.

11.1 Defining Trojans

A malicious program disguised as benign.
Often downloaded along with another program or software package.
Once installed, they allow:

- Data theft
- Data loss
- System crashes
- System slowdowns
- Launch other attacks

Trojans are often used to:

- Manipulate files
- Manage processes
- Run commands remotely
- Intercept keystrokes
- Watch screen images
- Shut down or restart machines

The most sophisticated Trojans will connect to the originator using an Internet Relay Chat (IRC) channel.

The distinguishing point of Trojans is they accompany other programs and install without the user's knowledge.

Trojans can be sent to a machine as:

- Instant message attachment
- E-mail attachment
- NetBIOS file sharing
- IRC

Trojans can be contained in:

- Freeware
- Spyware-removal tools
- System optimizers
- Screen savers
- Music
- Pictures
- Games
- Videos

Common Trojan Programs include:

- BackOrifice
- Deep Throat
- NetBus
- Whack-a-mole
- NetBus 2
- GirlFriend
- Masters Paradise

11.2 Overt and Covert Channels

Overt channel – the legitimate method for programs to communicated within a computer system.

Covert channel – uses programs and communication paths in unintended ways.

Copyright The Art of Service

Trojans use covert channels.
Can send instructions to the server component, which can make Trojan communication difficult to detect and decipher.

Covert channels rely on tunneling techniques

11.3 Types of Trojans

Trojans are created and used to perform different types of attacks.

Common types of Trojans include:

- Remote Access Trojans (RATs) – obtains remote access to system
- Data-Sending Trojans – find data and delivers to the hacker
- Destructive Trojans – used to delete or corrupt files
- Denial of Service Trojans – causes services to be attacked or denied
- Proxy Trojans – tunnels traffic or launches attacks though another system
- FTP Trojans – creates a FTP server to copy files on the system
- Security Software Disabler Trojans – used to stop antivirus software

11.4 Netcat Trojans

Uses a command-line interface to open TCP and UDP ports on a target system.

Hackers can then telnet to the open port to gain shell access.

11.5 Wrapping

Software packages used to deliver Trojans.
The legitimate file and Trojan file are binded into s single executable file.

Games and animated installations are common wrappers.
The Trojans are installed without the user's knowledge, only the legitimate file.

11.6 Reverse-Connecting Trojans

Allows an attacker to access an internally networked machine from outside the network.

A simple Trojan program is installed, such as a reverse WWW shell server.
In regular time intervals, the internal machine will access the external master system to find commands.
Any new commands will be retrieved and executed.
WWW shell server uses standard HTTP, so all communications appear to be regular web browsing.

11.7 Preventing Trojans

Most antivirus programs can detect and remove Trojans and spyware.
Hard drives are scanned on startup before damage is done.

It is best to use commercial products, not freeware.

Copyright The Art of Service

11.8 Trojan Evading Techniques

The best prevention is education.
Users should know not to install Internet downloads or open e-mails from unknown sources.

12 Virus and Worms

Used to infect a system and modify the system to allow access.
Many carry Trojans and backdoors.

12.1 Differences Between Viruses and Worms

Both are malicious software, or malware.

A virus will infect another program and use it to spread.
Virus code is injected into a benign program and spreads when it is executed.
Virus carrier programs include:

- Macros
- Games
- E-mail attachments
- Visual Basic scripts
- Animations

A worm is like a virus, but it self-replicates.
It can go from system to system without assistance from another program.

12.2 Types of Viruses

Viruses are classified based on:

- What they infect
- How they infect

12.2.1 What Can Be Infected

The components often infected by a virus include:

- Files
- System sectors
- Macros

Copyright The Art of Service

- Companion files
- Disk clusters
- Batch files
- Source code

12.2.2 How Viruses Infect

Different infection techniques include:

- Polymorphic viruses – encrypt code differently with each infection
- Stealth viruses – will hide normal virus characteristics to prevent detection
- Fast and slow infectors – prevents detection by infecting either very quickly or very slowly
- Sparse infectors – will infect only a few systems or applications
- Armored viruses – encrypted to prevent detection
- Multipartite viruses – create multiple infections
- Cavity viruses – attach themselves to empty parts of a file
- Tunneling viruses – sent through a different protocol or encrypted to prevent detection through a firewall
- Camouflage viruses – appear as another program
- NTFS virus – specifically attacks the NT file system
- Active Directory viruses – specifically attacks the Windows system's Active Directory

12.3 Antivirus Evasion Techniques

Virus detection and removal is based on the program's signature.

A virus can evade as long as it is not detected and antivirus companies have no chance to update virus definitions.

12.4 Virus Detection Methods

Viruses can be detected using:

- Scans
- Integrity checking of checksums
- Interception based on virus signatures

Detection and removal of virus happens by:

- Detecting the attack as a virus
- Tracing processes using utilities like
  - handle.exe
  - listdlls.exe
  - fport.exe
  - natstat.exe
  - pslist.exe.
- Map commonalities between affected systems
- Detect virus payload by looking for:
  - altered files
  - replaced files
  - deleted files
  - new files
  - changed file attributes
  - shared library files
- Acquire and isolate the infection vector
- Update virus definitions
- Rescan all systems

Copyright The Art of Service

13 Sniffers

Intercepts traffic on the network.
Can be a packet-capturing or frame-capturing tool.
The traffic can be viewed in a command-line or GUI format.

Can be used to obtain usernames, passwords, and confidential information.

13.1 Susceptible Protocols

Normal operation for a system is to read and respond only to traffic sent directly to the MAC address.
Promiscuous mode has a system read all traffic and sent it to the sniffer for processing.
Promiscuous mode is enabled through the installation of special driver software.

Protocols that do not encrypt are easily sniffed:

- HTTP
- POP3
- FTP
- SMTP

13.2 Defining Sniffing

Sniffing can be of two types: passive and active.

Passive sniffing will listen and capture traffic.
Best used in networks which have hubs.
All hosts can see all traffic in networks using hubs or wireless media.

Active sniffing will launch an Address Resolution Protocol (ARP) spoofing or traffic-flooding attack on a switch with the intent to capture traffic.

Networks using switches will read data sent to it and forward the data to the appropriate segment of a network.
Forwarding is possible because the switch maintains a table of MAC addresses and port numbers for all systems on the network.
Switch networks have greater security and improved throughput.

13.3 ARP Poisoning

ARP is used to translate IP addresses into MAC addresses.
A TCP/IP host must have the MAC address of the target host to connect on a network.

The ARP cache is searched to find the MAC address.
If the MAC address does not exist, the requesting host sends a broadcast ARP request, asking who has the right IP address.
The host with the request IP address hears the ARP query and responds with the correct MAC address.

ARP poisoning attacks the Ethernet network to:

- Sniff data frames on a switched LAN
- Stop traffic completely

Utilizes ARP spoofing, where fake ARP messages are sent to the Ethernet LAN.
The frames contain false MAC addresses and confuse the network devices resulting in:

- Frames being sent to an unintended host
- Frames being sent to an unreachable host

ARP spoofing can be used for MITM attacks

13.3.1 Preventing ARP Spoofing

Permanently add MAC addresses of the gateway to the ARP cache of the system.
The command to add MAC address in Windows is ARP -s.
The gateway's IP and MAC addresses require appending...

Port-based security will allow only one MAC address per switch port.

Copyright The Art of Service

13.4 Ethereal Filters

Ethereal is a freeware sniffer used to capture packets from LAN connections over a wired and wireless LANs.

They capture only one type of protocol traffic or traffic from a specific source IP or MAC address.

13.5 MAC Flooding

Packet sniffers on a switched network will only capture traffic going to and from a system.
To capture all traffic on a switched network:

- Perform ARP spoofing
- MAC flooding

MAC flooding is a process of flooding the switch with so much information that it stops working as a switch and start working as a hub.
Once the switch starts acting like a hub, all traffic on the network can be read.

13.6 DNS Spoofing

Also called DNS poisoning.
A technique that tricks the DNS server into believing it has received authentic information, which it has not.
The information is typically cached and its effect is spread to the users of the server.
The result will redirect the user to a fake website whenever a specific website URL is requested from the DNS server.

13.6.1 How DNS Spoofing Works

A DNS attack is effective because it exploits a flaw in the DNS server software where it can accept incorrect information.
Incorrect information can be cached locally until the DNS response is validated to come from an authorized source.
While the information is cached, it is provided to users who make subsequent requests.

This allows users to be redirected to the IP address of a server the attacker controls.
The controlled servers can have fake entries for the files that match those of the actual server.
Within the fake files, the attacker can embed viruses or worms.

13.6.2 Types of DNS Spoofing

Different types of DNS spoofing include:

- Intranet spoofing – acts as a device within the same internal network
- Internet spoofing – acts as a device on the Internet
- Proxy server DNS poisoning – modifies the DNS entries on a proxy server to redirect to a different host system
- DNS cache poisoning – modifying the DNS entries on any system to redirect to a different host

13.7 Sniffing Countermeasures

Encryption is the best defense against sniffing.
Encryption renders any data captured during the sniffing attack useless.
Common encryptions used against sniffing include:

- AES
- RC4
- RCS

Copyright The Art of Service

14 Denial of Service

The system is rendered unusable or significantly slowed down.
Are performed against individual systems or the entire network.
Are usually successful.

14.1 Types of DoS Attacks

An attempt to flood the system of a user or organization.

Types of DoS attacks include:

- DoS - sent by a single system to a single target
- DDoS – sent by multiple systems to a single target

The purpose of DoS attacks is to prevent legitimate use of a system.
An attack may:

- Flood the network with traffic
- Disrupt connections between two machines
- Prevent a specific individual from access services
- Disrupt a service to a specific system or person

Different types of traffic can be used to flood a system.
The service or system is kept busy responding to a massive amount of requests to be usable.

Typically, DoS attacks are a last resort.

14.2 DDoS Attacks

An advanced version of DoS attack, originating from multiple systems.
A coordinated attack from multiple systems, which have been compromised.

The compromised systems are considered secondary victims.
They are sometimes called zombies or BOTs.
Tracking the source of the attack is difficult since several IP addresses are in use.

Copyright The Art of Service

The systems under attack are considered the primary system.

DdoS attacks have three parts:

- Master/handler
- Slave/secondary victim/zombie/agent/BOT/BOTNET
- Victim/primary victim

The attacker launcher is the master.
The slave is a compromised host controlled by the master.
The target system is the victim.

DDoS is done in two phases:

- The intrusion phase compromises weak systems to act as slaves.
- The DDoS attack phase initiates the slave systems to attack the primary victim.

14.3 BOTs/BOTNETS

BOT is short for web robot.
An automated software program, which behaves intelligently.

14.3.1 Using BOTs

BOTs are used to:

- Post spam messages on newsgroups
- Send spam messages through e-mail
- As remote attack tools
- Web agents that interface with web pages (spiders)
- Install themselves on computers for malicious purposes

BOTs can use different types of communication, such as:

- Instant messaging
- Internet Relay Chat (IRC)
- Web interfacing

Copyright The Art of Service

BOTS can handle:

- Reporting weather
- Providing zip codes
- Listing sports scores
- Converting units of measure

14.3.2 Using BOTNETs

A group of BOT systems.

BOTNETS are used to:

- Conduct DDoS attacks
- Creation of SMTP mail relays for spam
- Internet Marketing fraud
- application serial number theft
- Theft of login IDs
- Theft of financial information

14.4 Smurf Attacks

Large amounts of ICMP echo traffic sent to a broadcast IP address with a spoofed source address.

A secondary victim on an IP network will perform an echo reply to an ICMP echo request.
The secondary victims on the network, the more responses made.
A magnified DoS attack of ping replies floods the primary victim.

14.5 SYN Flooding

Sends TCP connection requests faster than can be processed.
A random source address is created for each packet.
The SYN flag is set to request a new connection from the spoofed IP address.

The victim responds to the spoofed IP address and waits for a TCP confirmation that never arrives.
In the meantime, the victim's connection table continues to fill up until all new connections are ignored.
The server can no longer be accessed.

14.5.1 Preventing SYN Floods

Some methods to prevent SYN floods include;

- SYN cookies
- RST cookies
- Micro Blocks
- Stack Tweaking

14.6 DoS/DDoS Countermeasures

Some common security features used to detect, halt, or prevent DoS attacks include:

- net-ingress filtering – stops downstream networks from injecting packets with faked or spoofed addresses
- rate-limiting network traffic – allows traffic shaping or limitation of the bandwidth some types of traffic can consume
- intrusion detection systems – can detect attackers who are communicating with slave, master, or agent machines
- host-auditing tools – file-scanning tools used to identify known DDoS tool client and server binaries
- network-auditing tools – network scanning tools used to detect DDoS agents running on hosts in the network
- automated network-tracing tools – Traces streams of packets with spoofed addresses through the network.

Copyright The Art of Service

15 Session Hijacking

A method, which creates a temporary DoS for an end-user while the attacker takes over a session. Generally, performed after a user establishes an authenticated session and used to conduct a MITM attack.

15.1 Spoofing vs. Hijacking

With spoofing, the hacker will perform use the information obtained to use an address of a legitimate receiver.

In hijacking, the user is made offline to perform the attack.
The hacker relies on the legitimate user to make a connection and authenticate.
The hacker then takes over the session.

Three steps are involved to hijack a session:

- Tracking the Session
- Desynchronizing the connection
- Injecting the attacker's packet

An open session is identified and the sequence number for the next packet is predicted.
The user's system is sent a TCP reset or finish packet to close the session.
The server is sent a TCP packet with the predicted sequence number that the server will think is the systems next packet.

15.2 Types of Session Hijacking

Two types of session hijacking exist: active and passive.

Active hijacking will find an active session and take it over.
Passive hijacking will find an active session and watch all the traffic being sent by the legitimate user.

15.3 Sequence Prediction

TCP is responsible for reassembling streams of packets into an intended order.
TCP is a connection-oriented protocol.

Each packet must have a unique number to enable reassembly with other packets in the stream.
The number is called a sequence number.
Packets typically arrive out of order, so the sequence number ensures that they are assembled correctly.

15.3.1 Sequence Numbering

In a three way TCP handshake, a device initiates a session by transmit a packet to a receiving device.
The original packet with a SYN bit set is called a synchronize packet.
The synchronize packet contains an Initial Sequence Number (ISN).
The ISN is a pseudo-random generated number from over 4 billion combinations.

When the receiving device sends an acknowledgment (ACK) packet, the sequence number from the original packet is used with an increment added.
The ACK packet confirms receipt and provides the sender the next expected TCP packet sequence number.

Within a three-way handshake, the increment value is one.
In normal data communications, the increment value equals the size of the data in bytes being transmitted.

15.3.2 Sequence Predictions

The traffic between two systems is sniffed.
Using a hacking tool, the ISN must be located to calculate the next sequence number or the number needs to be guessed.

Packets with the guessed sequence number are issued, but must arrive at the target system before the actual packet arrives.

Copyright The Art of Service

To ensure that false packet arrives first, the trusted system is either flooded with packets or sent a reset packet.

15.4 Dangers Posed By Session Hijacking

TCDP/IP is a primary communication protocol, so most systems are vulnerable to session hijacking.
In addition:

- Few countermeasures are available
- Hijacking attacks are simple to launch
- Systems are completely exposed during a hijack

15.5 Prevent Session Hijacking

Several measures should be in place to defend against session hijacking.
The most effective protection is encryption.
Reducing the potential methods of gaining access to the network will reduce the possible entry points to launch a session hijacking attack.

Additional countermeasures are:

- Using a secure protocol
- Minimizing remote access
- Using encryption
- Limiting incoming connections
- Strong authentication
- Educating employees
- Requiring different username and passwords for different accounts

16 Hacking Web Servers

16.1 Types of Web Server Vulnerabilities

Most commonly exploited vulnerabilities on a web server include:

- Misconfiguration of web serve4r software
- Bugs or flaws in programming code in the operating system of applications
- Default installation of operating system of web server software
- Lack of patch management to update operating systems or web server software
- Lack of or disregard for proper security policies and procedures

As web services devices are located in a publicly accessible area between two packet-filtering devices.
This publicly accessible area is often called a Demilitarized Zone (DMZ).
A device in the DMZ is easily accessible by an organization's client system, therefore providing easier access to internal systems or databases by a hacker.

16.2 Attacks Against Web Servers

Defacement is the most visible type of attack against a web server. Defacing a website requires exploiting vulnerability so that the website files can be altered to show that the site has been hacked.

Common website attacks that allow defacement are:

- Obtaining administrator credentials through MITM attacks
- Obtaining an administrator password through a brute-force attack
- Redirecting users to a different web server using a DNS attacker
- Compromising a e-mail or FTP server

Copyright The Art of Service

- Exploiting vulnerabilities caused by web application bugs
- Misconfiguring web shares
- Exploiting weak permissions
- Rerouting clients after an attack on the firewall or router
- Using SQL injection attacks
- Intrusion using Telnet or Secure Shell (SSH)
- URL poisoning
- Intrusion using web server extensions or remote services
- Intercepting communications between client and server and changing the cookies

16.3 IIS Unicode Exploits

IIS has vulnerability that opens Windows 2000 systems to a directory traversal attack, commonly referred to as the Unicode exploit.
The vulnerability occurs in unpatched Windows 2000 systems and affects CGI scripts and ISAPI extensions.
The ISS parser does not properly interpret unicode, making systems running IIS to open system level access to hackers.

Unicode converts characters of any language to universal hex code specifications.
Unicode must be interpreted twice, but the IIS parser only interprets once.
This allows hackers to sneak file requests through IIS.

The vulnerability allows files to be added, changed, or deleted by hackers.
Code can be uploaded and run, including Trojans or backdoors.

16.4 Patch Management

A process of updating appropriate patches or hotfixes required by a system vendor.
The process involves:

- Choosing how patches are installed
- How patches are verified
- Testing patches prior to installation

A log of all patches applied to each system should be maintained. Automated patch-management systems are available which assess the system and decides which patches to deploy.

16.5 Web Application Scanners

Scanners allow a web application to be assessed for a large number of vulnerabilities including:

- Cross-site scripting
- SQL injection
- Buffer overflow
- Parameter-tampering attacks

16.6 Metasploit Framework

A freeware tool for testing or hacking operating systems or web server software.
Exploits can be used as plug-ins.
Testing can be performed on either a UNIX or Windows platform.

Copyright The Art of Service

16.7 Web Server Hardening

Hardening a server means increasing its security.

Increase the security of the web server by:

- Renaming the administrator account
- Using a strong password
- Disable default websites and FTP sites
- Remove unused applications
- Disable directory browsing in configuration settings
- Add a legal notice to provide notice of implications for illegal activities specifically the most current patches, hotfixes, and service packs
- Perform bounds-checking on input to prevent buffe3r overflow or malicious input
- Disable remote administration
- Map unused file extension to a 404 error message (File not Found)
- Enable auditing and logging
- Use a firewall between the web server and the Internet
- Allow only necessary ports through the firewall
- Replace the GET with POST methods when sending data to a web server.

Copyright The Art of Service

17 Web Application Vulnerabilities

17.1 Web Applications

Web applications are programs that reside o a web server and gives users functionality beyond just a website.
Web applications can provide:

- Database queries
- Webmail
- Discussion groups
- Blogs

A web application builds on the client/server architecture, with the web browser as the client and the web server as the application server.
JavaScript is a popular language for creating web applications.

17.2 Web Application Hacking

Hacking web application is driven by obtaining confidential data.

Web applications are typically connected to a database that has personal identify, financial, and passwords residing.

Web application vulnerabilities increase the threat of exploitation.

Because of their purpose and accessibility to critical information, security for web applications is critical.

Copyright The Art of Service

17.3 Anatomy of an Attack

Hacking web applications is similar to hacking any other system.

The five-step process consists of:

- Scanning a network
- Gathering information
- Testing attack scenarios
- Planning the attack
- Launching the attack

17.4 Web Application Threats

Threats to a web application exist on a web server.

The most common threats are:

- Cross-site scripting – a parameter entered into a web form is processes by the web application which can lead to an arbitrary command execution
- SQL injection – SQL commands are inserted into the URL which causes the database to dump, alter, delete, or create information in the database
- Command injection – programming commands are inserted into a web form
- Cookie poisoning and snooping – cookies are stolen or corrupted
- Buffer overload – huge amounts of data are sent to a web application through a web form
- Authentication hijacking – a session is stolen ponce a user has been authenticated
- Directory traversal/Unicode – folders on a system are browsed using a web browser

Copyright The Art of Service

17.5 Google Hacking

Google's search engine can be used to locate high-value targets and valuable information such as passwords.
Using the search engine maliciously in this manner is referred to as Google hacking.

Many times, Google will pull information directly out of private documents or databases.

17.6 Web Application Countermeasures

Countermeasures for each of the vulnerabilities include:

- Cross-site scripting – validation of cookies, query strings, form fields, and hidden fields
- SQL injection – validation user variables
- Command injection – language-specific languages used for the programming language
- Cookie poisoning and snooping – implement cookie time-outs, authenticate cookies, and don't store passwords in a cookie
- Buffer overload – validation of user input length and performing bounds checking
- Authentication hijacking – use SSL to encrypt traffic
- Directory traversal/Unicode – define the access rights to private folders on the web servers, as well as apply patches and hotfixes

Copyright The Art of Service

18 Web Based Password Cracking Techniques

18.1 Authentication Types

Web applications and web servers support several authentication types.

The most common authentication type is HTTP authentication.
Two types of HTTP authentication exist: basic and digest.
Basic HTTP authentication sends the username and password in cleartext.
Digest authentication hashes credentials and used a challenge-response model of authentication.

Other authentication supports include:

- NTLM – using Internet Explorer and IIS web servers and suitable for internal authentication on an intranet
- Certificate-based – uses x.509 certificates for public/private key technology
- Token-based – a hardware device that displays an authentication code, like SecurID, for a prescribed time limit
- Biometric – uses a physical characteristic such as a fingerprint, eye iris, or handprint

18.2 Password Cracker

A program designed to decrypt passwords or disable password protection.

Dictionary searches or brute-force methods are required for a password cracker to be successful.

Copyright The Art of Service

18.3 Using a Password Cracker

A dictionary attack is performed by:

- Generating a list of potential passwords that can be found in a dictionary, using a dictionary generator program or downloading a dictionary from the Internet
- Encrypting, or hashing, the list of words
- Comparing the hash list against the hashed passwords obtained from sniffing the network

Strong passwords require brute-force attacks.
Brute-force attacks attempt every combination of letters, numbers, and special characters.

18.4 Password Attacks - Classification

Types of password attacks are:

- Dictionary
- Brute force
- Hybrid

18.5 Password Cracking Countermeasures

Countermeasures should include:

- Strong passwords of at least eight characters
- Different usernames and passwords, since usernames are transmitted in cleartext
- Strong authentication mechanism

Copyright The Art of Service

19 SQL Injection

SQL server injections are delivered through a user-input field.
The input field is used to:

- Enter a username and password
- Add data to a URL
- Perform a search

19.1 SQL Injection

During a SQL injection attack:

- Malicious code is inserted into a web form field or the website's code
- The intent of the malicious code is to make the system execute a command shell or other arbitrary commands

SQL servers are very common and used to store confidential information.

19.2 Conducting SQL Injection

To determine the SQL server's vulnerability:

- Using a web browser, search for a website that uses a login page or other database input or query field
- Check the site's source code for the POST or GET HTML commands
- Test the SQL server using single quotes
  (identifies if user input is sanitized or interpreted literally)
- An error message, *use 'a'='a'* or similar, will determine whether the SQL server is susceptible to attack
- Use SELECT command to retrieve data or INSERT command to add information to the database

Copyright The Art of Service

19.3 SQL Server Vulnerabilities

The vulnerabilities of SQL servers are a result of:

- Poor coding practices
- Lack of input validation
- Services not being updated or patched

The two primary vulnerabilities are:

- Unpatched systems
- Blank SA password

19.4 SQL Injection Countermeasures

Countermeasures against SQL injection attacks include:

- Minimize the privileges of users' connections to the database
- Enforce strong passwords for SA and Administrator accounts
- Disable verbose of explanatory error messages
- Review source code for programming weaknesses:
  - single quotes
  - lack of input validation
- Rejecting known bad input
- Checking input bounds

Copyright The Art of Service

20 Buffer Overflows

Buffer Overflows have the same causes as SQL Injection attacks

20.1 Types of Buffer Overflows

Causes a system to fail by:

- Overloading memory
- Executing a command shell
- Executing arbitrary code

Vulnerabilities to buffer overflows are caused by:

- A lack of bounds checking
- Lack of input validation sanitizing

Buffer overloads are memory-based: affect either the stack or head storage locations for user-supplied variables

Two types of buffer overflows exist:

- Stack-based – impacts static memory locations
- Heap-based – impacts dynamic memory locations

20.2 Stack-Based Buffer Overflows

To execute a stack-based buffer overflow:

- A variable is entered into the buffer to exhaust the amount of memory in the stack
- Continue entering more data than allocated in memory for that variable.
- Add another variable
- Overwrite the return pointer which instructs the program where to return after executing the variable
- The malicious code variable will be executed and the return pointer will move to the next line of executable code.
- If the pointer is successfully overwritten, the hacker's code will be executed instead of the program code.

Hackers can use a No Operation (NOP) instruction to aid in redirecting the return pointer.

An IDS looks for a series of NOPs to identify the existence of a potential buffer overflow.

To bypass the IDS, the hacker can randomly replace the NOPs with equivalent code.

Copyright The Art of Service

21 Wireless Hacking

Most wireless LANs are based on the IEEE 802.11 standard and amendments, like

- 802.11a
- 802.11b
- 802.11g
- 802.11i
- 802.11n

802.11i comprises the latest security solution to address the weaknesses of 802.11.

The Wi-Fi Alliance, known as WPA (Wi-Fi Protected Access) and WPA2 create additional security certifications.

21.1 WEP, WPA Authentication Systems

Wireless LAN clients authenticate to access points using:

- Open system
- Shared key authentication

Open system is a simple request to make a connection to the network and has no security measures in place.

Shared key authentication provides a string of challenge text with a Wired Equivalent Privacy (WEP) key to authenticate to the network.

21.1.1 Wired Equivalent Privacy (WEP)

WEP was the first security option for 802.11 WLANs and used to encrypt data.
Uses anRC4 64-bit or 128-bit encryption key to encrypt payloads out of layer 2.
A WEP key is comprised of a user defined 40-bit or 104-bit key combined with a 24-bit Initialization Vector (IV).

How RC4 utilizes IVs is a weakness, allowing the WEP key to be cracked.

The method for cracking the key uses encrypted output bytes to determine the most probable key bytes.
The method is called the FMS attack.

21.1.2 Wi-Fi Protected Access (WPA)

WPA uses Temporal Key Integrity Protocol (TKIP)
TKIP is safer than RC4 for data encryption.
WPA Personal or WPA Enterprise is used for authentication.

WPA Personal uses an ASCII passphrase for authentication.
WPA Enterprise uses a RADIUS server to authenticate users.
From a security standpoint, SPA Enterprise is a better option but requires the creation and complex setup of a RADIUS server.
The data encryption key is rotated by TKIP to overcome the vulnerabilities of WEP.

WPA2 is similar to 802.11i.
Advanced Encryption Standard (AES) is used to encrypt the data payload.
AES is considered to be an uncrackable encryption algorithm.
WPA2 will also use TKIP during a transitional period called mixed mode security where both TKIP and AES are used.

Low-end devices like PDAs utilize only TKIP because AES requires a faster processor.
WPA Personal and WPA2 Personal authenticate WLAN clients with a passphrase.
WPA Enterprise and WPA2 Enterprise will authenticate WLAN users through a RADIUS server using 802.1x/extensible Authentication Protocol (EAP) standards.

WPA uses the same encryption and authentication mechanisms used by 802.11i and WPA2.
WPA2 does not require preauthorization, which enables fast, secure roaming necessary in very mobile environments using time-sensitive applications.

Copyright The Art of Service

21.2 Wireless Sniffers and SSID, MAC Spoofing

Eavesdropping or sniffing is a common attack on WLANs.
Usually happens in hotspots or default installation access point (AP).
Packets are sent unencrypted across the WLAN s for protocols such as FTP, POP3, or SMTP to be captured.

The SSID is the name of the WLAN.
The WLAN can be located in a beacon.
SSIDs are used to identify and differentiate between WLANs.

Most access points allow the WLAN administrator to hide the SSID.
The SSID can be read from data or probe packets.

Early WLAN technologies used MAC address filters to allow systems to associate with the access point.
MAC filters prove to be cumbersome to configure and did not support the scalability required for network enterprises.
MAC headers are never encrypted allowing valid MAS addresses to be easy obtained.

21.3 Rogue Access Points

WLAN access points, which are not authorized to connect to a target, network creating a wireless hole in the network.
A rogue AP can be planted or inadvertently created by plugging an access point into the network to gain mobile access.
Any rogue AP can be used by any person to connect to the AP and have access to a wired LAN.

Copyright The Art of Service

21.4 Wireless Hacking Techniques

Wireless hacking activities are categorized as:

- Cracking encryption and authentication mechanisms
- Eavesdropping or sniffing
- Denial or Service
- AP masquerading or spoofing
- MAC spoofing

21.5 Securing Wireless Networks

Fewer security options are available because wireless networking is a relatively new technology.
Categories of security methods are based on the OSI model.

Layer 2 options are:

- WPA
- WPA2
- 802.11i

Layer 3 options are

- IPSec or SSL VPN

Layer 7 options are secure application like:

- Secure Shell (SSH)
- HTTP Over SSL (HTTPS)
- FTP/SSL (FTPS)

Copyright The Art of Service

22 Physical Security

22.1 Physical Security Breach Incidents

Equipment theft is the most common physical security attack.

Physical security breaches lead to most insider attacks.

Most security breaches caused by insufficient physical security consist of:

- installation of malware like
    - Keyloggers
    - Viruses
    - Trojans
    - Backdoors
    - Rootkits
- Identification and capture of passwords and certificates
- Physical connection to the wired network to sniff confidential information
- Access to systems to collect data
- Planting of rogue access points
- Theft of documents in paper of electronic format
- Theft of sensitive fax information
- Dumpster diving

22.2 Physical Security

Security measures are categorized by:

- Physical
- Technical
- Operational

Copyright The Art of Service

22.2.1 Physical Measures

Access prevention to systems includes:

- Security guards
- Lighting
- Fencing
- Locks
- Alarms

Access points should be limited and monitored by CCTV (closed-circuit television) and alarms

Entrance should restrict access to authorized personnel.
Laptops and removable media should be limited, restricted, and protected.
Computer screens should be positioned to avoid shoulder surfing.

Policies should require users to lock down their systems when they leave their workstations

Computer systems with highly sensitive data should be enclosed in a credential-access room

22.2.2 Technical Measures

Technical solutions include

- Firewalls
- IDS
- Spyware content filtering
- Virus scanning
- Trojan scanning

Implemented on all remote client systems, networks, and servers.

Copyright The Art of Service

22.2.3 Operational Measures

Well defined and documented Security Policy and processes, specifically dealing with:

- Analyzing threats
- Performing risk assessments

22.3 Need for Physical Security

Physical security is designed to prevent:

- Access to a computer system by unauthorized personnel
- Stealing data from systems
- Corruption of data stored on a system
- Loss of data or damage to systems caused by natural causes.

22.4 Accountability for Physical Security

Accountability for physical security falls on:

- The Security Officer of the organization
- Information system professionals
- Chief information officer
- Employees

The enforcement of physical security policies is the responsibility of everyone.

Copyright The Art of Service

22.5 Factors Affecting Physical Security

Physical security can be affected by:

- Vandalism
- Theft
- Natural causes
    - Earthquake
    - Fire
    - Flood

Copyright The Art of Service

23 Linux Hacking

Linux is a popular operation system because of its open source code and its flexibility.
Being open source, Linux can be modified by anyone.
Different versions of Linux are called distributions, or distros.

Linux had tighter security controls than Windows operating systems.

23.1 Linux Kernels Compilation

23.1.1 Linux Basics

Linux is similar to UNIX.
All distributions of Linux include all standard commands and utilities.

Several text editors are available within the Linux system.

GNU software provides most basic Linux utilities.
GNU utilities support advanced features not found in standard versions of UNIX and BSD.

Several types of shells are available for Linux.
The differences between the shells are the command languages used.
A shell is a command-line program interface allowing users to enter and execute commands.
Many shells provide additional features such as:

- Input and output redirection
- Command language for writing shell scripts
- Multiple process management
- Job control

Copyright The Art of Service

23.1.2 Linux Kernels

Linus source code is freely distributed and available as binary files, or Linus kernels.
Binary files must be compiled to operate properly as an operating system.
Anyone can use a binary file, downloading them and adding or changing functionality.

A Linus kernel may need to be recompiled because:

- New hardware with no kernel module in the distribution CD
- A bug which has been fixed with a revision to the operating system
- New software application requiring a newer version or the operating system

Sites which source code can be downloaded from may have and or infected code, Trojans, or other backdoors added to the source code. Any download of source code should be done from a known and trusted Internet website or purchased from a commercial distribution.

23.1.3 Compiling Linux Kernels

To download, configure, and compile Linux kernel:

- Locate the file for the latest version of the operating system
- Download the file to the /usr/src directory on the Linux system
- Use the command, tar zxf, to unpack the file
- Configure the kernel
  - Change the directory to /usr/src/Linux
  - Type make menuconfig
  - Use the window menu to alter any aspects of the kernel configuration
  - Save the configuration
  - Type make dep; make clean
- Compile the kernel by using the commands:
  - Make zimage
  - Make modules

Copyright The Art of Service

- install the new kernel
    - cp /usr/Linux/src/arch/1386/boot/zimage /boot/newkernel
- Install the modules in /lib/ modules
    - use the command, make modules_install
- Edit /etc/lilo.conf to add a section like this:

```
image = /boot/kernel
label = new
read-only
```

- At the next reboot, select the new kernel in lilo to load the new kernel
- If the kernel works, move it to the first position in the lilo.conf to boot it every time by default

23.2 Understand GCC Compilation Commands

GNU Compiler Collection (GCC) is a command-line compiler that takes source code and makes it executable.

GCC can be used to compile and execute applications written in C, C++, and Fortran to run on Linux systems

The GCC can be downloaded from http://gcc.gnu.org

23.3 LKM modules

Linux Kernel Modules (LKM) adds functionality to the operating system without recompiling the operating system.
To load a LKM, use the command:

- Modprobe LKM

LKMs should be downloaded from a trusted source, since rootkits can be easily created as LKM.

23.4 Linux Hardening Methods

Hardening is the process of improving security on a system

Steps to hardening a system:

- Store in a secure physical location
- Create and maintain strong passwords
- Do not communicate usernames and passwords unsecured
- Ensure null passwords do not exist
    - Check the /etc/shadow file on Linux systems
- Use the default security stance of deny all
- Provide access to only those users that need access
- Remove unused services
- Patch the system with the latest bug fixes
- Use a widely recognized and known Linux distribution
- Don't install unnecessary applications or services
- Change default passwords
- Disable remote root login
- Setup and enable IP tables
- Install host-based IDS
- Utilize and review log files

Copyright The Art of Service

24 Evading IDS, Honeypots and Firewalls

24.1 Intrusion Detection Systems and Evasion Techniques

Intrusion Detection Systems (IDS) inspect traffic and look for known signatures of attacks or unusual behavior patterns.
Packet sniffers view and monitor traffic and a built-in component of an IDS.

An alert is sent from IDS when an event on the security event list is triggered.
The alert can be sent to either a command center or system administrator.
The alert can take the form of a page, a phone call, or e-mail.

Intrusion Prevention Systems (IPS) will initiate countermeasures when suspected traffic is identified.
An IPS has automated responses to an intrusion attempt, including deny-access capability.

24.1.1 Types of IDS

Main types of IDS include:

- Host-based
- Network-based

Host-based IDSs (HIDSs) reside on a single system or host.
HIDS filter traffic or events based on a known signature list for the specific operating system.
HIDS are susceptible to being turned off by Trojans and worms.

HIDS are applications and NIDS are software-based appliances.

Network-based IDSs (NIDS) reside on the networking.
They are used solely for intrusion detection purposes to d etect all types of malicious activity not found by a conventional firewall.

Copyright The Art of Service

NIDS are passive systems: the IDS sensor detects a potential security breach, logs the required information and signals an alert on the monitoring console.

24.1.2 Using IDS

A possible attack is determined by performing:

- Signature analysis
- Anomaly detection

A signature is a pattern used to identify either a single packet or a series of packets that execute an attack.
Signature detection IDSs matches traffic with known signatures and patterns of misuse.

Anomaly detection IDS searches for intrusion attempts, which are outside the normal business patterns and alerts.

An Ids can be evades by changing the traffic behavior to be something other than known signatures.
Popular methods of evading:

- Using a different protocol
- Breaking an attack into smaller packets to pass through the IDS (session slicing)
- Inserting extra data
- Obfuscating addresses or data
- Desynchronization
- Session hijacking

Copyright The Art of Service

24.2 Firewall and Honeypot Evasion Techniques

A firewall is a software application or hardware appliance that controls access to a network through rules set by an administrator.

A perimeter hardware firewall appliance is set up near a network edge where a trusted network connects to an untrusted network.

A software firewall will protect a personal computer, system, or host from unwanted or malicious packets entering the network interface card (NIC).

A honeypot is a decoy machine within the Demilitarized Zone, which is in place as a trap or aid in locating hackers, or to draw them away from a critical target.
A honeypot looks like a real production server.

24.2.1 Evading Firewalls and Honeypots

The easiest method to bypass a firewall is to compromise a system on the internal side of the firewall.
The compromised system can connect through the firewall.

A reverse SSS shell has the compromised system connect to the hacker using port 80 to make it look like a web client connecting to a web server.

Tunneling allows a hacker to bypass the firewall, such as:

- HTTP tunneling
- Internet Control Message Protocol (ICMP)
- TCP acknowledgment

Anti-honeypot software is used to evade honeypot traps.

25 Cryptography

Cryptography is the study of encryption and encryption algorithms.

Encryption is the conversion of messages from a comprehensible form to an incomprehensible form and back.

The purpose of encryption is to prevent data from being read or used by unauthorized persons or systems.

25.1 Cryptography and Encryption Techniques

Encryption can be applied to data in storage or in transit.

Encryption happens by mathematically scrambling the data so it cannot be deciphered.
To decipher the encrypted text, knowledge of the mathematical formula is required.
The mathematical formula is known as the encryption algorithm.

Encryption uses mathematical calculations based on:

- Substitution – replacing characters with other characters
- Transposition – changing the order of characters

Two types of encryption are:

- Symmetric key encryption
- Asymmetric key encryption

Symmetric key encryption has both the sender and receiver uses the same secret key to encrypt and decrypt the data.
Sharing the key between multiple systems is not very secure.
Typically, an offline method of transporting keys between systems is required.

Asymmetric (or public) key cryptography addresses the weaknesses of symmetric key encryption and distribution.

Copyright The Art of Service

25.2 Public and Private Keys

Using asymmetric cryptography, the client and server will each create a pair of keys:

- The server's public key
- The server's private key
- The client's public key
- The client's private key

A key pair has a relationship that allows data to be encrypted with one key and decrypted with the other key.
The relationship is mathematical based on factoring prime numbers.

When a client and server what to share information, the both send their public key yo the remote system.
The private keys are never shared.

A message is encrypted with the receiver's public key.
The message is decrypted with the receiver's private key.

25.3 Algorithms

Algorithms can have a length from 40 bits to 448 bits.
The longer the key length, the stronger the encryption algorithm.

A 40-bit algorithm takes, 2 seconds to 1.4 minutes to crack using a brute-force attack.
A 64-bit algorithm takes 37 days to 50 years to crack using a brute-force attack.
Any algorithm over 256 bits is considered uncrackable.

Copyright The Art of Service

25.3.1 Types of Algorithm

MD5 – a hashing algorithm that creates a random-length input to generate a 128-bit digest.
A digital signature is created to accompany documents and e-mails to prove the integrity of the source.
The MD5 message digests are encrypted by a private key in the digital signature process.

SHA – a message digest generating a 160-bit digest of encrypted data.
Most commonly used by the government.

RC4 – a symmetric key algorithm using streaming cipher, or encrypting one bit at a time.
Uses random mathematical permutations and variable key sizes.

RC5 – uses a variable block size and variable key size.

Blowfish – a 64-bit block cipher: encrypting chunks of data.
Consists of variable key length between 32 and 448 bits.

Copyright The Art of Service

26 Penetration Testing Methodologies

A penetration test attempts to recreate the probable process that an intruder will take to gain unauthorized access to the network and systems.

The purpose of the penetration test is to test the implementation of the security policy within the organization.

26.1 Security Assessments

Security assessments can be categorized as:

- Security audits
- Vulnerability assessments
- Penetration testing

Different skills are required to fulfill the scope of the security assessments

Security audits scan IP networks and hosts for any known security weaknesses with tools designed to:

- Locate live systems
- Enumerate users
- Identify applications
- Identify operating systems
- Look for common security configuration mistakes
- Look for common security vulnerabilities

Vulnerability assessments only identify the potential vulnerabilities.

Penetration tests, or pen tests, attempts to gain access to the network.

26.2 Penetration Testing Methodologies

Security assessments fall into two types: external and internal assessments.

An external assessment tests and analyzes:

- Available information
- Conducts network scanning
- Enumeration

Exploits are run from outside the network perimeter, usually through the Internet.

An internal assessment is performed within the network.
The tester acts as an employee with some access either to the4 network or as a black hat with non-knowledge of the network.

Assessments are often outsourced when qualified or experienced testers are lacking in the organization.
Outsourced assessors are often required when audit requirements need to be meeting, such as the Health Insurance Portability and Accountability Act (HIPAA).

The scope of the assessment must be specified.
A code of conduct for the assessment team should be specified.

Penetration tests can be conducted using:

- Freeware
- Shareware
- Automated tools

26.3 Penetration Testing Steps

Penetration testing involves three steps:

- Pre-attack phase
- Attack phase
- Post-attack phase

Copyright The Art of Service

26.3.1 Pre-Attack Phase

Involves reconnaissance and data gathering, using:

- Whois
- DNS scanning
- Network scanning
- Locating IP blocks
- Enumerating information

Other testing in the pre-attack phase includes:

- Testing network filtering devices
- Stress-testing proxy servers
- Check for default installations of firewalls
- Checking restrictions on remote login

26.3.2 Attack Phase

Activities include but not limited to:

- Penetrating the perimeter
- Acquiring the target
- Escalating privileges
- Executing, implanting, and retracting

When penetrating the perimeter, the tester looks at:

- Error reports
- Access Control Lists by forging responses
- Evaluating protocol filtering rules using various protocols like
    - SSH
    - FTP
    - Telnet
- Buffer overflows
- SQL injections
- Bad input validation
- Output sanitization
- DoS attacks

Copyright The Art of Service

Some areas of testing should include:

- Software
- Web applications
- Wireless configurations

When acquiring the target, the tester is more intrusive than a vulnerability scan or audit.
To acquire the target:

- An automated exploit tool can be used
- Attempt to access the system using information obtained from social engineering
- Test the enforcement of the security policy
- Using brute-force password crackers
- Attempt to use get admin tools to access protected resources

Escalating privileges typically gives users and systems more rights and privileges than originally set

Executing, implanting and retracting are the final phase of testing and focuses on gaining control of the system or network without disrupting business processes.

26.3.3 Post-Attack Phase

Usually involves restoring the system to normal pre-test configurations, requiring:

- Removing files
- Cleaning registry entries
- Removing shares
- Removing connections

Results are analyzed and presented to management in a comprehensive report.

Copyright The Art of Service

26.4 Pen-Test Legal Framework

When conducting a penetration test, the legal implications must be considered.
The documents of great interest and must be signed include:

- Scope of work
- Nondisclosure agreements
- Liability release

26.5 Pen-Test Deliverables

The goal of a penetration test is the report, containing:

- List of findings based on risk
- Analysis of findings
- Explanation of findings
- Recommendation measures for findings
- Log files to provide evidence
- Executive summary of security posture
- Name of tester and date of testing
- Positive findings and security implementations

Copyright The Art of Service

26.6 Automated Penetration Testing Tools

The most popular automatic penetration testing tools consist of:

- Nessus – freeware network vulnerability scanner
- GFI LANguard – commercial network security scanner for WIndows
- Retina - commercial vulnerability assessment scanner
- CORE IMPACT – automated penetration tester focusing on exploitation
- ISS Internet Scanner – application-level vulnerability assessor
- X-Scan – multithreaded plug-in supported network vulnerability scanner
- SARA - vulnerability assessment tool
- QualysGuard - web-based vulnerability scanner
- SAINT – commercial vulnerability assessment tool
- MBSA – Microsoft Baseline Security Analyzer

Copyright The Art of Service

27 Practice Exam

27.1 Refresher “Warm up Questions”

The following multiple-choice questions are a refresher from the Foundation level as a prelude.

Question 1

Why would a hacker use a proxy server?

A. To create a stronger connection with the target.
B. To create a ghost server on the network.
C. To obtain a remote access connection.
D. To hide malicious activity on the network.

Question 2

What type of symmetric key algorithm using a streaming cipher to encrypt information?

A. RC4
B. Blowfish
C. SHA
D. MD5

Question 3

Which of the following is not a factor in securing the environment against an attack on security?

A. The education of the attacker
B. The system configuration
C. The network architecture
D. The business strategy of the company
E. The level of access provided to employees

Copyright The Art of Service

Question 4

What type of attack uses a fraudulent server with a relay address?

A. NTLM
B. MITM
C. NetBIOS
D. SMB

Question 5

What port is used to connect to the Active Directory in Windows 2000?

A. 80
B. 445
C. 139
D. 389

Question 6

To hide information inside a picture, what technology is used?

A. Rootkits
B. Bitmapping
C. Steganography
D. Image Rendering

Question 7

Which phase of hacking performs actual attack on a network or system?

A. Reconnaissance
B. Maintaining Access
C. Scanning
D. Gaining Access

Copyright The Art of Service

Question 8

Attempting to gain access to a network using an employee's credentials is called the _____________ mode of ethical hacking.

A. Local networking
B. Social engineering
C. Physical entry
D. Remote networking

Question 9

Which Federal Code applies the consequences of hacking activities that disrupt subway transit systems?

A. Electronic Communications Interception of Oral Communications
B. 18 U.S.C. § 1029
C. Cyber Security Enhancement Act 2002
D. 18 U.S.C. § 1030

Question 10

Which of the following is not a typical characteristic of an ethical hacker?

A. Excellent knowledge of Windows.
B. Understands the process of exploiting network vulnerabilities.
C. Patience, persistence and perseverance.
D. Has the highest level of security for the organization.

Question 11

What is the proper command to perform an Nmap XMAS scan every 15seconds?

A. nmap -sX -sneaky
B. nmap -sX -paranoid
C. nmap -sX -aggressive
D. nmap -sX -polite

Question 12

What type of rootkit will patch, hook, or replace the version of system call in order to hide information?

A. Library level rootkits
B. Kernel level rootkits
C. System level rootkits
D. Application level rootkits

Question 13

What is the purpose of a Denial of Service attack?

A. Exploit a weakness in the TCP/IP stack
B. To execute a Trojan on a system
C. To overload a system so it is no longer operational
D. To shutdown services by turning them off

Question 14

What are some of the most common vulnerabilities that exist in a network or system?

A. Changing manufacturer, or recommended, settings of a newly installed application.
B. Additional unused features on commercial software packages.
C. Utilizing open source application code
D. Balancing security concerns with functionality and ease of use of a system.

Question 15

What is the sequence of a TCP connection?

A. SYN-ACK-FIN
B. SYN-SYN ACK-ACK
C. SYN-ACK
D. SYN-SYN-ACK

Copyright The Art of Service

Question 16

What tool can be used to perform SNMP enumeration?

A. DNSlookup
B. Whois
C. Nslookup
D. IP Network Browser

Question 17

Which ports should be blocked to prevent null session enumeration?

A. Ports 120 and 445
B. Ports 135 and 136
C. Ports 110 and 137
D. Ports 135 and 139

Question 18

The first phase of hacking an IT system is compromise of which foundation of security?

A. Availability
B. Confidentiality
C. Integrity
D. Authentication

Question 19

How is IP address spoofing detected?

A. Installing and configuring a IDS that can read the IP header
B. Comparing the TTL values of the actual and spoofed addresses
C. Implementing a firewall to the network
D. Identify all TCP sessions that are initiated but does not complete successfully

Copyright The Art of Service

Question 20

Why would a ping sweep be used?

A. To identify live systems
B. To locate live systems
C. To identify open ports
D. To locate firewalls

Question 21

What are the port states determined by Nmap?

A. Active, inactive, standby
B. Open, half-open, closed
C. Open, filtered, unfiltered
D. Active, closed, unused

Question 22

What port does Telnet use?

A. 22
B. 80
C. 20
D. 23

Question 23

Which of the following will allow footprinting to be conducted without detection?

A. PingSweep
B. Traceroute
C. War Dialers
D. ARIN

Copyright The Art of Service

Question 24

Performing hacking activities with the intent on gaining visibility for an unfair situation is called ________.

A. Cracking
B. Analysis
C. Hacktivism
D. Exploitation

Question 25

What is the most important activity in system hacking?

A. Information gathering
B. Cracking passwords
C. Escalating privileges
D. Covering tracks

Question 26

A packet with no flags set is which type of scan?

A. TCP
B. XMAS
C. IDLE
D. NULL

Question 27

Sniffing is used to perform ______________ fingerprinting.

A. Passive stack
B. Active stack
C. Passive banner grabbing
D. Scanned

Copyright The Art of Service

Question 28

Phishing is a form of ____________________.

A. Spamming
B. Identify Theft
C. Impersonation
D. Scanning

Question 29

Why would HTTP Tunneling be used?

A. To identify proxy servers
B. Web activity is not scanned
C. To bypass a firewall
D. HTTP is a easy protocol to work with

Question 30

Which Nmap scan is does not completely open a TCP connection?

A. SYN stealth scan
B. TCP connect
C. XMAS tree scan
D. ACK scan

Question 31

What protocol is the Active Directory database based on?

A. LDAP
B. TCP
C. SQL
D. HTTP

Copyright The Art of Service

Question 32

Services running on a system are determined by _____________.

A. The system's IP address.
B. The Active Directory
C. The system's network name
D. The port assigned

Question 33

What are the types of scanning?

A. Port, network, and services
B. Network, vulnerability, and port
C. Passive, active, and interactive
D. Server, client, and network

Question 34

Enumeration is part of what phase of ethical hacking?

A. Reconnaissance
B. Maintaining Access
C. Gaining Access
D. Scanning

Question 35

Keyloggers are a form of ______________.

A. Spyware
B. Shoulder surfing
C. Trojan
D. Social engineering

Question 36

What are hybrid attacks?

A. An attempt to crack passwords using words that can be found in dictionary.
B. An attempt to crack passwords by replacing characters of a dictionary word with numbers and symbols.
C. An attempt to crack passwords using a combination of characters, numbers, and symbols.
D. An attempt to crack passwords by replacing characters with numbers and symbols.

Question 37

Which form of encryption does WPA use?

A. Shared key
B. LEAP
C. TKIP
D. AES

Question 38

What is the best statement for taking advantage of a weakness in the security of an IT system?

A. Threat
B. Attack
C. Exploit
D. Vulnerability

Question 39

Which database is queried by Whois?

A. ICANN
B. ARIN
C. APNIC
D. DNS

Copyright The Art of Service

Question 40

Having individuals provide personal information to obtain a free offer provided through the Internet is considered what type of social engineering?

A. Web-based
B. Human-based
C. User-based
D. Computer-based

Copyright The Art of Service

28 Answer Guide

28.1 Answers to Questions

Question 1
Answer: D
Reasoning: Proxy servers exist to act as an intermediary between the hacker and the target and servces to keep the hacker anonymous tot he network.

Question 2
Answer: A
Reasoning: RC$ uses streaming ciphers.

Question 3
Answer: D
Reasoning: All of the answers are factors supporting the exploitation or prevention of an attack. The business strategy may provide the motivation for a potential attack, but by itself will not influence the outcome.

Question 4
Answer: B
Reasoning: MITM (Man in the Middle) attacks create a server with a relay address. It is used in SMB relay attacks.

Question 5
Answer: D
Reasoning: The Active Directory Administration Tool used for a Windows 2000 LDAP client uses port 389 to connect to the Active Directory service.

Question 6
Answer: C
Reasoning: Steganography is the right answer and can be used to hide information in pictures, music, or videos.

Copyright The Art of Service

Question 7

Answer: D

Reasoning: In the process of hacking, actual attacks are performed when gaining access, or ownership, of the network or system. Reconnaissance and Scanning are information gathering steps to identify the best possible action for staging the attack. Maintaining access attempts to prolong the attack.

Question 8

Answer: A

Reasoning: Local networking uses an employee's credentials, or access rights, to gain access to the network. Physical entry uses credentials to gain access to the physical IT infrastructure.

Question 9

Answer: C

Reasoning: The Cyber Security Enhancement Act 2002 deals with life sentences for hackers who recklessly endanger the lives of others, specifically transportation systems.

Question 10

Answer: D

Reasoning: Each answer has validity as a characteristic of an ethical hacker. Though having the highest security clearance is ideal, it is not always the case in an organization.

Question 11

Answer: A

Reasoning: SX is used to identify a xmas scan, while sneaky performs scans 15 seconds apart.

Question 12

Answer: A

Reasoning: Library leve rootkits is the correct answer. Kerel level focuses on replaceing specific code while application level will concentrate on modifying the behavior of the application or replacing application binaries. The type, system level, does not exist for rootkits.

Question 13
Answer: C
Reasoning: DoS attacks force systems to stop responding by overloading the processing of the system.

Question 14
Answer: B
Reasoning: Linux is an open source code and considered to have greater security than the commercial Windows environment. Balancing security. Ease of use and functionality can open vulnerabilities that already exist. Manufacturer settings, or default settings, may provide basic protection against hacking threats, but need to change to provide advance support. The unused features of application code provide an excellent opportunity to attack and cover the attack.

Question 15
Answer: B
Reasoning: A three-handed connection of TCP will start with a SYN packet followed by a SYN-ACK packet. A final ACK packet will complete the connection.

Question 16
Answer: D
Reasoning: SNMPUtil and IP Network Browser is SNMP enumeration tool

Question 17
Answer: D
Reasoning: Port 139 is the NetBIOS Session port typically can provide large amounts of information using APIs to connect to the system. Other ports that can be blocked in 135, 137,138, and 445.

Question 18
Answer: B
Reasoning: Reconnaissance is about gathering confidential information, such as usernames and passwords.

Copyright The Art of Service

Question 19
Answer: B
Reasoning: IP address spoofing is detectable by comparing TTL values of the actual and spoofed IP addresses.

Question 20
Answer: A
Reasoning: A ping sweep is intended to identify live systems. Once an active system is found on the network, other information may be distinguished, including location. Open ports and firewalls.

Question 21
Answer: C
Reasoning: Nmap determines that ports are open, filtered, or unfiltered.

Question 22
Answer: D
Reasoning: Telnet uses port 23.

Question 23
Answer: D
Reasoning: ARIN is a publicly accessible database, which has information that could be valuable. Because it is public, any attempt to obtain information in the database would go undetected.

Question 24
Answer: C
Reasoning: Hacktivism is the act of malicious hacking for a cause or purpose.

Question 25
Answer: B
Reasoning: Passwords are a key component to access a system, making cracking the password the most important part of system hacking.

Question 26
Answer: D
Reasoning: A NULL scan has no flags set.

Question 27
Answer: A
Reasoning: Passive stack fingerprinting uses sniffing technologies instead of scanning.

Question 28
Answer: C
Reasoning: Phishing is typically a potential attacker posing, or impersonating, a financial institution

Question 29
Answer: C
Reasoning: HTTP Tunneling is used to bypass the IDS and firewalls present on a network.

Question 30
Answer: A
Reasoning: Also known as a “half-open scanning,” SYN stealth scan will not complete a full TCP connection.

Question 31
Answer: A
Reasoning: Active4 direction in Windows 200 is based on a Lightweight Directory Access Protocol (LDAP).

Question 32
Answer: D
Reasoning: Hackers can identify services running on a system by the open ports that are found.

Question 33
Answer: B
Reasoning: The three types of accepted scans are port, network, and vulnerability.

Question 34
Answer: C
Reasoning: Enumeration is a process of gaining access to the network by obtaining information on a user or system to be used during an attack.

Copyright The Art of Service

Question 35
Answer: A
Reasoning: Keyloggers are a form of hardware or software spyware installed between the keyboard and operating system.

Question 36
Answer: B
Reasoning: Hybrid attacks do crack passwords that are created with replaced characters of dictionary type words

Question 37
Answer: C
Reasoning: TKIP is used by WPA

Question 38
Answer: C
Reasoning: A weakness in security is exploited. An attack does the exploitation. A weakness is vulnerability. A threat is a potential vulnerability.

Question 39
Answer: A
Reasoning: Who utilizes the Internet Corporation for Assigned Names and Numbers.

Question 40
Answer: D
Reasoning: Whether using email, a fake website, or popup to entice the used, obtaining information from an individual over the Internet is a computer-based type of social engineering

29 References

Tiller, James S. *The Ethical Hack*. Boca Raton: Auerbach Publications, 2005.
Certified Ethical Hacker Mega Guide. Tampa:PreLogic, Inc. wwww.preplogic.com.
Graves, Kimberly. *Official Certified Ethical Hacker Review Guide*. Indianapolis: Wiley Publishing, Inc, 2007.

CEH information: www.eccouncil.com

Websites

www.artofservice.com.au
www.theartofservice.org
www.theartofservice.com

Copyright The Art of Service

INDEX*

Copyright The Art of Service

Copyright The Art of Service

Copyright The Art of Service

Copyright The Art of Service

Copyright The Art of Service

Copyright The Art of Service

Copyright The Art of Service

Copyright The Art of Service

Copyright The Art of Service

Copyright The Art of Service

Copyright The Art of Service