MICHAEL GREGG

Cert Guide

Learn, prepare, and practice for exam success

CEH

Certified Ethical Hacker

PEARSON IT CERTIFICATION

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

Certified Ethical Hacker (CEH) Cert Guide

Michael Gregg

PEARSON

800 East 96th Street
Indianapolis, Indiana 46240 USA

Certified Ethical Hacker (CEH) Cert Guide

Copyright © 2014 by Pearson Education, Inc.

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-7897-5127-0

ISBN-10: 0-7897-5127-5

Library of Congress Control Number: 2013953303

Printed in the United States of America

Second Printing: May 2014

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Pearson IT Certification cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the CD or programs accompanying it.

Bulk Sales

Pearson IT Certification offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales. For more information, please contact

U.S. Corporate and Government Sales
1-800-382-3419
corpsales@pearsontechgroup.com

For sales outside of the U.S., please contact

International Sales
international@pearsoned.com

Associate Publisher
Dave Dusthimer

Acquisitions Editor
Betsy Brown

Development Editor
Ellie C. Bru

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Keith Cline

Indexer
Tim Wright

Proofreader
Kathy Ruiz

Technical Editors
Brock Pearson
Tatyana Zidarov

Publishing Coordinator
Vanessa Evans

Media Producer
Lisa Matthews

Book Designer
Alan Clements

Compositor
Jake McFarland

Contents at a Glance

Table of Contents

About the Author

Michael Gregg (CISSP, SSCP, CISA, MCSE, MCT, CTT+, A+, N+, Security+, CCNA, CASP, CISA, CISM, CEH, CHFI, and GSEC) is the founder and president of Superior Solutions, Inc., a Houston, Texas-based IT security consulting firm. Superior Solutions performs security assessments and penetration testing for Fortune 1000 firms. The company has performed security assessments for private, public, and governmental agencies. Its Houston-based team travels the country to assess, audit, and provide training services.

Michael is responsible for working with organizations to develop cost-effective and innovative technology solutions to security issues and for evaluating emerging technologies. He has more than 20 years of experience in the IT field and holds two associate's degrees, a bachelor's degree, and a master's degree. In addition to co-authoring the first, second, and third editions of *Security Administrator Street Smarts*, Michael has written or co-authored 14 other books, including *Build Your Own Security Lab: A Field Guide for Network Testing* (Wiley, 2008); *Hack the Stack: Using Snort and Ethereal to Master the 8 Layers of an Insecure Network* (Syngress, 2006); *Certified Ethical Hacker Exam Prep 2* (Que, 2006); and *Inside Network Security Assessment: Guarding Your IT Infrastructure* (Sams, 2005).

Michael has been quoted in newspapers such as the *New York Times* and featured on various television and radio shows, including NPR, ABC, CBS, Fox News, and others, discussing cyber security and ethical hacking. He has created more than a dozen IT security training security classes. He has created and performed video instruction on many security topics, such as cyber security, CISSP, CISA, Security+, and others.

When not consulting, teaching, or writing, Michael enjoys 1960s muscle cars and has a slot in his garage for a new project car.

You can reach Michael by email at MikeG@thesolutionfirm.com.

Dedication

In loving memory of my mother-in-law, Elvira Estrello Cuellar, who always stood behind me, encouraged me, and prayed that all my dreams would come true.

Acknowledgments

I would like to offer a big "thank you" to Christine, for her help and understanding during the long hours that such a project entails. I also want to thank Curley, Betty, Gen, Alice, and all of my family. A special thanks to the people of Pearson IT Certification, who helped make this project a reality, including Betsy Brown. I would also like to thank my technical editors, Brock Pearson and Tatyana Zidarov.

Finally, I would like to acknowledge all the dedicated security professionals who contributed "In the Field" elements for this publication. They include Darla Bryant, Guy Bruneau, Ron Bandes, Jim Cowden, Laura Chappell, Rodney Fournier, Pete Herzog, Bryce Gilbrith, George Mays, Mark "Fat Bloke" Osborn, Donald L. Pipkin, Shondra Schneider, and Allen Taylor.

We Want to Hear from You!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

We welcome your comments. You can email or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

Please note that we cannot help you with technical problems related to the topic of this book.

When you write, please be sure to include this book's title and author as well as your name and email address. We will carefully review your comments and share them with the author and editors who worked on the book.

Email:	feedback@pearsonitcertification.com
Mail:	Pearson IT Certification ATTN: Reader Feedback 800 East 96th Street Indianapolis, IN 46240 USA

Reader Services

Visit our website and register this book at www.pearsonitcertification/register for convenient access to any updates, downloads, or errata that might be available for this book.

Introduction

The EC-Council Certified Ethical Hacker (CEH) exam has become the leading ethical hacking certification available today. CEH is recognized by both employers and the industry as providing candidates with a solid foundation of hands-on security testing skills and knowledge. The CEH exam covers a broad range of security concepts to prepare candidates for the technologies that they are likely to be working with if they move into a role that requires hands-on security testing.

Let's talk some about what this book is. It offers you a one-stop shop for what you need to know to pass the exam. You do not have to take a class in addition to buying this book to pass the exam. However, depending on your personal study habits or learning style, you might benefit from buying this book *and* taking a class.

Cert Guides are meticulously crafted to give you the best possible learning experience for the particular characteristics of the technology covered and the actual certification exam. The instructional design implemented in the Cert Guides reflects the nature of the CEH certification exam. The Cert Guides provide you with the factual knowledge base you need for the exams, and then take it to the next level with exercises and exam questions that require you to engage in the analytic thinking needed to pass the CEH exam.

EC-Council recommends that the typical candidate for this exam have a minimum of 2 years of experience in IT security. In addition, EC-Council recommends that candidates have preexisting knowledge of networking, TCP/IP, and basic computer knowledge.

Now let's briefly discuss what this book is not. It is not a book designed to teach you advanced hacking techniques or the latest hack. This book's goal is to prepare you for the CEH 312-50 exam, and it is targeted to those with some networking, OS, and systems knowledge. It provides basics to get you started in the world of ethical hacking and prepare you for the exam. Those wanting to become experts in this field should be prepared for additional reading, training, and practical experience.

Goals and Methods

The most important and somewhat obvious goal of this book is to help you pass the CEH exam (312-50). In fact, if the primary objective of this book was different, the book's title would be misleading; however, the methods used in this book to help you pass the CEH exam are designed to also make you much more knowledgeable about how penetration testers do their job. While this book and the accompanying CD together have more than enough questions to help you prepare for the actual exam, the method in which they are used is not to simply make you memorize as many questions and answers as you possibly can.

One key methodology used in this book is to help you discover the exam topics and tools that you need to review in more depth. Remember that the CEH exam will not only expect you to understand hacking concepts but also common tools. So, this book does not try to help you pass by memorization, but helps you truly learn and understand the topics and when specific tools should be used. This book will help you pass the CEH exam by using the following methods:

- Helping you discover which test topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises and scenarios that enhance your ability to recall and deduce the answers to test questions
- Providing practice exercises on the topics and the testing process via test questions on the CD

Who Should Read This Book?

This book is not designed to be a general security book or one that teaches network defenses. This book looks specifically at how attackers target networks, what tools attackers use, and how these techniques can be used by ethical hackers. Overall, this book is written with one goal in mind: to help you pass the exam.

So, why should you want to pass the CEH exam? Because it's one of the leading entry-level hacking certifications. It is also featured as part of DoD 8570, and having the certification might mean a raise, a promotion, or other recognition. It's also a chance to enhance your resumé and to demonstrate that you are serious about continuing the learning process and that you're not content to rest on your laurels. Or one of many other reasons.

Strategies for Exam Preparation

Although this book is designed to prepare you to take and pass the CEH certification exam, there are no guarantees. Read this book, work through the questions and exercises, and when you feel confident, take the practice exam and additional exams provided in the test software. Your results should tell you whether you are ready for the real thing.

When taking the actual certification exam, make sure that you answer all the questions before your time limit expires. Do not spend too much time on any one question. If you are unsure about the answer to a question, answer it as best as you can, and then mark it for review.

Remember that the primary objective is not to pass the exam but to understand the material. When you understand the material, passing the exam should be simple. Knowledge is a pyramid; to build upward, you need a solid foundation. This book and the CEH certification are designed to ensure that you have that solid foundation.

Regardless of the strategy you use or the background you have, the book is designed to help you get to the point where you can pass the exam with the least amount of time required. For instance, there is no need for you to practice or read about scanning and Nmap if you fully understand the tool already. However, many people like to make sure that they truly know a topic and therefore read over material that they already know. Several book features will help you gain the confidence that you need to be convinced that you know some material already, and to also help you know what topics you need to study more.

How This Book Is Organized

Although this book could be read cover to cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with. Chapter 1 provides an overview of ethical hacking and reviews some basics. Chapters 2 through 13 are the core chapters. If you do intend to read them all, the order in the book is an excellent sequence to use.

The core chapters, Chapters 2 through 13, cover the following topics:

- **Chapter 2, "The Technical Foundations of Hacking"**—This chapter discusses basic techniques that every security professional should know. This chapter reviews TCP/IP and essential network knowledge.
- **Chapter 3, "Footprinting and Scanning"**—This chapter discusses the basic ideas behind target selection and footprinting. The chapter reviews what type of information should be researched during footprinting and how passive and active footprinting and scanning tools should be used.
- **Chapter 4, "Enumeration and System Hacking"**—This chapter covers enumeration, and it is a final chance to uncover more detailed information about a target before system hacking. System hacking introduces the first step at which the hacker is actually exploiting a vulnerability systems.
- **Chapter 5, "Linux and Automated Assessment Tools"**—This chapter examines the role of Linux in the hacking community and how Linux distributions such as Backtrack are used. This chapter also reviews automated security tools such as Metasploit and Canvas.

- **Chapter 6, "Trojans and Backdoors"**—This chapter covers the ways in which Trojans and backdoors function. It reviews the methods in which the tools are deployed and used.
- **Chapter 7, "Sniffers, Session Hijacking, and Denial of Service"**—This chapter covers sniffing tools such as Wireshark. The chapter examines the difference in passive and active sniffing. It also reviews session hijacking and DoS, DDoS, and botnet techniques.
- **Chapter 8, "Web Server Hacking, Web Applications, and Database Attacks"**—This chapter covers the basics of web hacking, application attacks, and how SQL injection works.
- **Chapter 9, "Wireless Technologies, Mobile Security, and Attacks"**—This chapter examines the underlying technology of wireless technologies, mobile devices, Android, IOS, and Bluetooth.
- **Chapter 10, "IDS, Firewalls, and Honeypots"**—This chapter discusses how attackers bypass intrusion detection systems and firewalls. This chapter also reviews honeypots and honeynets and how they are used to jail attackers.
- **Chapter 11, "Buffer Overflows, Viruses, and Worms"**—This chapter covers the fundamentals of buffer overflows. The chapter also examines basic types of malware such as viruses and worms, and examines static and active analysis of malicious code.
- **Chapter 12, "Cryptographic Attacks and Defenses"**—This chapter covers the fundamentals of attacking cryptographic systems and how tools such as encryption can be used to protect critical assets.
- **Chapter 13, "Physical Security and Social Engineering"**—This chapter covers the fundamentals of social engineering attacks and introduces the concept that not all attacks are technical in nature. Attacks can be technical, social, or even physical. Finally, this chapter reviews important concepts of penetration testing.

This page intentionally left blank

This chapter covers the following topics:

- **Enumeration:** The process of counting off or listing what services, applications, and protocols are present on each identified computer.
- **System Hacking:** The process of gaining access, escalating privileges, maintaining control, and covering tracks.

CHAPTER 4

Enumeration and System Hacking

This chapter introduces Windows enumeration and system hacking. It gives you the knowledge you need to prepare for the Certified Ethical Hacker exam, and it broadens your knowledge of Windows security controls and weaknesses. However, this chapter addresses only the basic information, as it would require an entire book to cover all Windows hacking issues. If you are seriously considering a career as a penetration tester, this chapter should whet your appetite for greater knowledge.

The chapter begins by introducing enumeration and discusses what kind of information can potentially be uncovered. Enumeration is the final pre-attack phase in which you probe for usernames, system roles, account details, open shares, and weak passwords. This chapter also reviews some basics of Windows architecture. A review of Windows users and groups is discussed. The last topic is system hacking. This section discusses the tools and techniques used for gaining access to computer systems. Although many of the tools introduced are specific to Windows systems, the steps are the same no matter what the platform, as evident in Chapter5, "Linux and Automated Assessment Tools," when Linux is discussed.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz enables you to assess whether you should read this entire chapter thoroughly or jump to the "Exam Preparation Tasks" section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 4-1 lists the major headings in this chapter and their corresponding "Do I Know This Already?" quiz questions. You can find the answers in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions."

Table 4-1 "Do I Know This Already?" Section-to-Question Mapping

Foundation Topics Section	Questions
Enumeration	2, 3, 4, 5, 10
System Hacking	1, 6, 7, 8, 9

CAUTION The goal of self-assessment is to gauge your mastery of the topics in this chapter. If you do not know the answer to a question or are only partially sure of the answer, you should mark that question as wrong for purposes of the self-assessment. Giving yourself credit for an answer you correctly guess skews your self-assessment results and might provide you with a false sense of security.

1. Which of the following is considered a nontechnical attack?
   a. Password sniffing
   b. Dumpster diving
   c. Password injection
   d. Software keylogger

2. A RID of 500 is associated with what account?
   a. A user account
   b. The first users account
   c. The guest account
   d. The administrator account

3. During enumeration what ports may specifically indicate SMB on a Windows computer?
   a. 110
   b. 111
   c. 389
   d. 445

4. During enumeration what ports may specifically indicate portmapper on a Linux computer?
   a. 110
   b. 111
   c. 389
   d. 445

5. Which of the following is a tool commonly used for enumeration?
   a. GetAcct
   b. John

c. LCP
d. IAM tool kit

6. Which type of password cracking makes use of the space/time memory trade-off?
   a. Dictionary attack
   b. Rainbow table
   c. Rule
   d. Hybrid

7. The second layer of security on the SAM file is known as what?
   a. Encoding
   b. Obscuring
   c. SYSKEY
   d. Salting

8. Windows passwords that are stored in seven-character fields are known as what?
   a. NTLMv2
   b. Kerberos
   c. Salted
   d. LAN Manager

9. Which of the following matches the common padding found on the end of short Windows passwords?
   a. 1404EE
   b. EE4403
   c. EEEEEE
   d. 1902DD

10. If you were going to enumerate DNS, which of the following tools could be used?
    a. Route print
    b. ARP -A
    c. Nslookup
    d. IPconfig

Foundation Topics

Key Topic

Enumeration

Enumeration can be described as an in-depth analysis of targeted computers. Enumeration is performed by actively connecting to each system to identify the user accounts, system accounts, services, and other system details. Enumeration is the process of actively querying or connecting to a target system to acquire information on: NetBIOS/LDAP, SNMP, UNIX/Linux operation, NTP servers, SMTP servers, and DNS servers. These topics are discussed next.

Windows Enumeration

The object of Windows enumeration is to identify a user account or system account for potential use. You might not have to find a system administrator account because escalation of privilege may be possible. At this point, we are simply seeking the knowledge to gain some level of access.

To better target Microsoft Windows computers, you should understand how they function. Windows ships with both client and server versions. Client systems that are still being supported as of this writing include the following: Windows XP, Vista, 7, and 8. On the server side, Microsoft supports Windows 2003, 2008, and 2012. Each of these operating systems shares a somewhat similar kernel. The kernel is the most trusted part of the operating system. How does the operating system know who and what to trust? The answer is by implementing rings of protection. The protection ring model provides the operating system with various levels at which to execute code or restrict its access. It provides a level of access control and granularity. As you move toward the outer bounds of the model, the numbers increase, and the level of trust decrease. Figure 4-1 shows the basic model that Windows uses for protective rings.

With the Windows architecture, you can see that there are two basic modes: user mode (ring 3) and kernel mode (ring 0). User mode has restrictions, whereas kernel mode allows full access to all resources. This is an important concept for the ethical hacker to contemplate because antivirus and analysis tools can detect hacking tools and code that run in user mode. However, if code can be deployed on a Windows system to run in kernel mode, it can hide itself from user mode detection and will be harder to detect and eradicate. All the code that runs on a Windows computer must run in the context of an account. The system account has the capability to perform kernel mode activities. The level of the account you hold determines your ability to execute code on a system. Hackers always want to run code at the highest possible privilege. Windows uses the following two things to help keep track of a user's security rights and identity:

- Security identifiers (SIDs)
- Relative identifiers (RIDs)

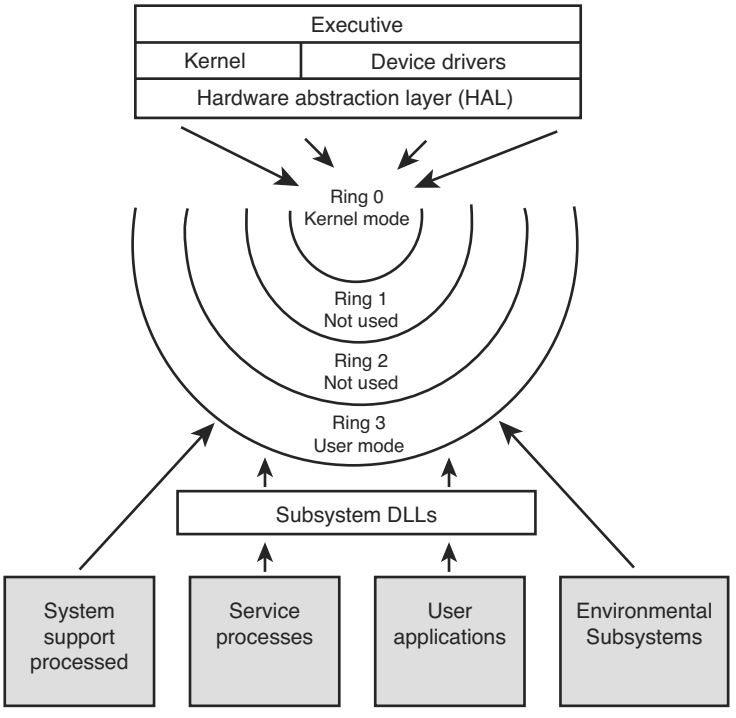


Figure 4-1 Windows architecture.

SIDs are a data structure of variable length that identifies user, group, and computer accounts. For example, a SID of S-1-1-0 indicates a group that includes all users. Closely tied to SIDs are RIDs. A RID is a portion of the SID that identifies a user or group in relation to the authority that user has. Let's look at an example:

```
S-1-5-21-1607980848-492894223-1202660629-500
     S for security id
     1 Revision level
     5 Identifier Authority (48 bit) 5 = logon id
     21 Sub-authority (21 = nt non unique)
     1607980848       SA
     492894223        SA domain id
     1202660629       SA
     500               User  id
```

Focus your attention on the last line of text in this example. The user ID specifies the specific user, as shown in Table 4-2.

Key Topic

Table 4-2 User ID and Corresponding RID Code

User ID	Code
Admin	500
Guest	501
Kerberos	502
First user	1000
Second user	1001

This table shows that the administrator account has a RID of 500 by default, the guest has a RID 501, and the first user account has a RID of 1000. Each new user gets the next available RID. This information is important because simply renaming an account will not prevent someone from discovering key accounts. This is similar to the way that Linux controls access for users and system processes through an assigned user ID (UID) and a group ID (GID) that is found in the /etc/passwd file. On a related topic, let's look at some other important security components of Microsoft Windows that will help you understand the enumeration process.

TIP Be able to correlate specific user accounts and RIDs for the exam, such as 501 = guest.

Windows Security

On a standalone Windows computer, user information and passwords are stored in the Security Account Manager (SAM) database. If the system is part of a domain, the domain controller stores the critical information in Active Directory (AD). On standalone systems not functioning as domain controllers, SAM contains the defined local users and groups, along with their passwords and other attributes. The SAM database is stored in Windows/System32/config folder in a protected area of the Registry under HKLM\SAM.

AD is a directory service, which contains a database that stores information about objects in a domain. AD keeps password information and privileges for domain users and groups that were once kept in the domain SAM. Unlike the old NT trust model, a domain is a collection of computers and their associated security groups

that are managed as a single entity. AD was designed to be compatible to Lightweight Directory Access Protocol (LDAP); you can get more background information from RFC 2251.

Another important Windows security mechanism is Local security authority subsystem (Lsass). It might sound familiar to you: Lsass is what the Sasser worm exploited by buffer overflow in 2004. Lsass is a user mode process that is responsible for the local system security policy. This includes controlling access, managing password policies, user authentication, and sending security audit messages to the event log.

NetBIOS and LDAP Enumeration

NetBIOS was a creation of IBM. It is considered a legacy protocol today but may still be found on some older systems. On local-area networks (LANs), NetBIOS systems usually identify themselves by using a 15-character unique name. Because NetBIOS is nonroutable by default, Microsoft adapted it to run over Transmission Control Protocol/Internet Protocol (TCP/IP). NetBIOS is used in conjunction with Server Message Blocks (SMBs). SMB allows for the remote access of shared directories and files. These services are provided through the ports shown in Table 4-3.

Table 4-3 Microsoft Key Ports and Protocols

Key Topic

Port	Protocol	Service
135	TCP	MS-RPC endpoint mapper
137	UDP	NetBIOS name service
138	UDP	NetBIOS datagram service
139	TCP	NetBIOS session service
445	TCP	SMB over TCP

This table lists key ports and protocols that Microsoft systems use. When performing a port scan or attempting to identify a system, finding these open ports will signal that you might be dealing with a Microsoft system. After these ports have been identified, you can begin to further enumerate each system.

TIP Make sure that you can identify key Windows ports.

SMB was designed to make it possible for users to share files and folders, although InterProcess Communication (IPC) offers a default share on Windows systems.

This share, the IPC$, was used to support named pipes that programs use for interprocess (or process-to-process) communications. Because named pipes can be redirected over the network to connect local and remote systems, they also enable remote administration. As you might think, this can be a problem.

A null session occurs when you log in to a system with no user ID and password at all. In legacy Windows versions 2000, XP, and Windows 2003, a null session could be set up using the `net` command.

There's an entire host of `net` commands. A few are discussed here, but for a more complete list, just type **net** from the command line and the **/?** syntax after any of the commands you see that you would like more information on.

Even though you may not see the IPC$ share when looking for shared drives and folders, that doesn't mean that it is not there. For example, if you have identified open ports of 135, 139, and 445 on some targeted systems, you might attempt the `net view /domain` command:

```
C:\>net view /domain
Domain
SALES
MARKETING
ACCOUNTING
The command completed successfully.
```

Notice that these `net` commands are quite handy. They have identified the sales, marketing, and accounting groups. To query any specific domain group, just use the net command again in the form of `net view /domain:`*`domain_name`*:

```
C:\>net view /domain:accounting
Server Name             Remark
\\Mickey
\\Pluto
\\Donald
The command completed successfully.
```

You can take a closer look at any one system by using the `net view \ \`*`system_name`* command:

```
C:\net view \\donald
Shared resources at \\DONALD
Sharename     Type          Comment
-------------------------------------------------------
CDRW          Disk
D             Disk
Payroll       Disk
```

```
Printer       Disk
Temp          Disk
The command was completed successfully.
```

Now that you have completed some basic groundwork, let's move on to enumerating user details, account information, weak passwords, and so on. `IPC$` is further exploited for these activities. Specifically, you will need to set up a null session. You can do so manually with the `net` command:

```
C:\net use \\donald\ipc$ "" /u:""
```

NOTE Setting up a null session to take advantage of Windows underlying communication protocols has been secured with newer operating systems such as Server 2012, Windows 7, and Windows 8, but you might still find a few old systems on which this is possible.

NetBIOS Enumeration Tools

With a `net use \\` *`computer name`*`\ ipc$ "" /u:""` command executed, you're primed to start hacking at the system. The tools discussed in this section, such DumpSec and GetAcct, require that you have a null session established before you attempt to use them.

DumpSec is a Windows-based graphical user interface (GUI) enumeration tool from SomarSoft. It enables you to remotely connect to Windows machines and dump account details, share permissions, and user information. It is shown in Figure 4-2. Its GUI-based format makes it easy to take the results and port them into a spreadsheet so that holes in system security are readily apparent and easily tracked. It can provide you with usernames, SIDs, RIDs, account comments, account policies, and dial-in information.

GetAcct enables you to input the IP address or NetBIOS name of a target computer and extract account information. It can extract SID, RID, comments, full name, and so on. From our discussion earlier about SIDs on Windows machines, you know that the administrator account on the machine ends in 500. Therefore, you can use GetAcct to discover the SID for the usernames found in your enumeration and discover who has administrative access.

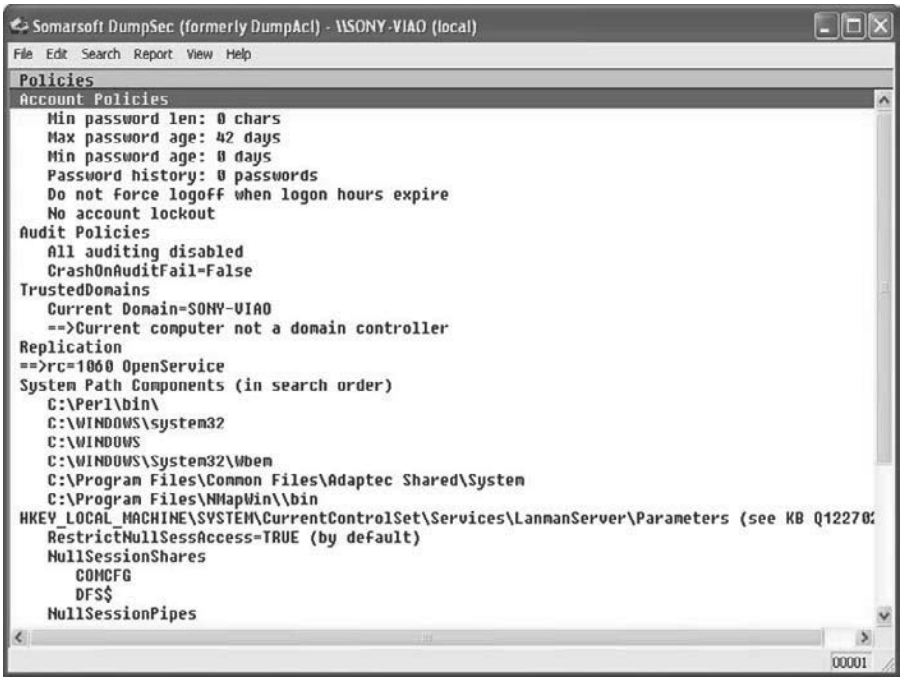


Figure 4-2 DumpSec.

Many tools can be used for enumeration. The ones listed here should give you an idea of what this category of tool can do. Listed here are some other tools that perform the same type of enumeration:

- **SuperScan:** Released by Foundstone, SuperScan retrieves all available information about any known user from any vulnerable Windows system.
- **GetUserInfo:** Created by JoeWare, this command-line tool extracts user info from a domain or computer.
- **Ldp:** This executable is what you need if you're working with AD systems. After you find port 389 open and authenticate yourself using an account (even guest will work), you will be able to enumerate all the users and built-in groups.
- **User2sid:** This program can retrieve a SID from the SAM from the local or a remote machine. Sid2user.exe can then be used to retrieve the names of all the user accounts and more. For example, typing `user2sid \\ computer name` returns the name and corresponding SID.

Other tools are available to enumerate a Windows system. For example, if you are local to the system, you can also use NBTStat. Microsoft defines NBTStat as a tool

designed to help troubleshoot NetBIOS name resolution problems. It has options such as local cache lookup, WINS server query, broadcast, LMHOSTS lookup, Hosts lookup, and DNS server query. Typing **nbtstat** at a Windows command prompt will tell you all about its usage:

```
C:\ nbtstat
Displays protocol statistics and current TCP/IP connections using
NBT(NetBIOS over TCP/IP).
NBTSTAT [-a RemoteName] [-A IP address] [-c] [-n]
         [-r] [-R] [-s] [S] [interval] ]
```

One of the best ways to use NBTstat is with the `-A` option. Let's look at what that returns:

```
C:\ >NBTstat -A 192.168.13.10

            NetBIOS Remote Machine Name Table

       Name                 Type          Status
    ---------------------------------------------
    DONALD          <00>    UNIQUE        Registered
    WORKGROUP       <00>    GROUP         Registered
    DONALD          <20>    UNIQUE        Registered
    WORKGROUP       <1E>    GROUP         Registered
    WORKGROUP       <1D>    UNIQUE        Registered
    ..__MSBROWSE__. <01>    GROUP         Registered

    MAC Address = 00-19-5D-1F-26-68
```

A name table that provides specific hex codes and tags of unique or group is returned. These codes identify the services running on this specific system. For example, do you see the code of `1D UNIQUE`? This signifies that the system Donald is the master browser for this particular workgroup. Other common codes include the following:

Title	Hex Value	User/Group	Service
domain	1B	U	Domain master browser
domain	1C	G	Domain controllers
domain	1D	U	Master browser
domain	1E	G	Browser service elections

You can find a complete list of NetBIOS name codes at www.cotse.com/nbcodes.htm or by searching for NetBIOS name codes.

SNMP Enumeration

Simple Network Management Protocol (SNMP) is a popular TCP/IP standard for remote monitoring and management of hosts, routers, and other nodes and devices on a network. It works through a system of agents and nodes. SNMP is designed so that requests are sent to agents, and the agents send back replies. The requests and replies refer to configuration variables accessible by agent software. Traps are used to signify an event, such as a reboot or interface failure. SNMP makes use of the Management Information Base (MIB). The MIB is the database of configuration variables that resides on the networking device.

SNMP version 3 offers data encryption and authentication, but version 1 and 2 are still in use. Both version 1 and 2 are clear-text protocols that provides only weak security through the use of community strings. The default community strings are public and private and are transmitted in clear text. If the community strings have not been changed or if someone can sniff the community strings, that person then has more than enough to enumerate the vulnerable devices.

NOTE SNMP version 1 and 2 use default community strings of public and private.

Devices that are SNMP enabled share a lot of information about each device that probably should not be shared with unauthorized parties. SNMP enumeration tools can be found in both Windows and Linux. Several are mentioned here:

- **snmpwalk:** A Linux command-line SNMP application that uses SNMP GETNEXT requests to query a network entity for a tree of information.
- **IP Network Browser:** A GUI-based network discovery tool from www.solarwinds.net that enables you to perform a detailed discovery on one device or an entire subnet.
- **SNScan:** A free GUI-based SNMP scanner from Foundstone, shown in Figure 4-3.

The best defense against SNMP enumeration is to turn it off if it is not needed. If it is required, make sure that you block ports 161 and 162 at network chokepoints, and ensure that an upgrade to SNMPv3 is possible. Changing the community strings is another defensive tactic as is making them different in each zone of the network.

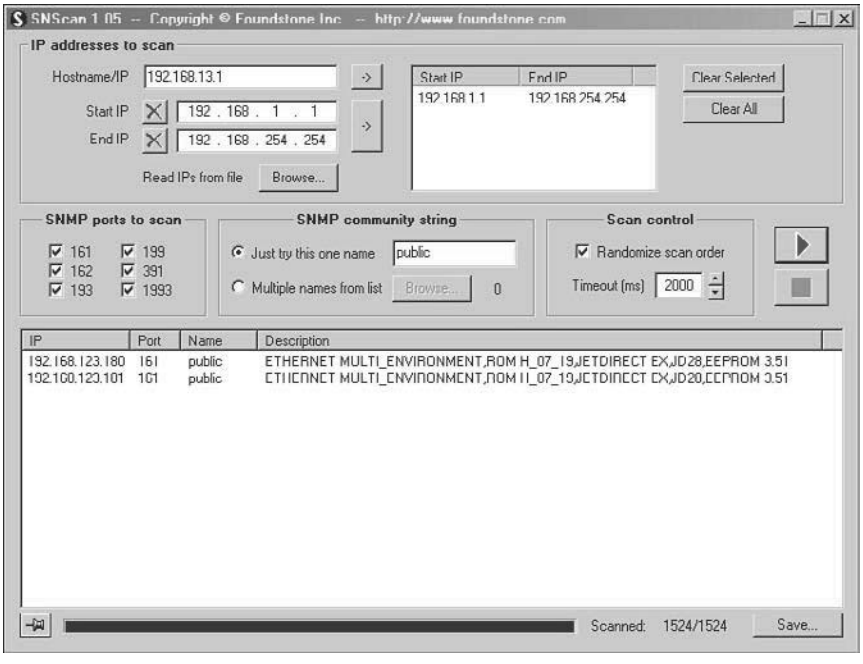


Figure 4-3 SNScan.

Linux/UNIX Enumeration

Even though Linux might not offer the opportunities that Windows systems do, there are still some enumeration techniques you can perform. Tools such as rpcclient can be used to enumerate usernames on those operating systems just like on a Windows system. Some other tools are shown here:

- **Rpcclient:** Using the `rpcclient` command, the attacker can enumerate usernames (for example, `rpcclinet $> netshareenum`).
- **Showmount:** The `showmount` command displays a list of all clients that have remotely mounted a file system from a specified machine in the host parameter.
- **Finger:** The `finger` command enumerates the user and the host. It enables the attacker to view the user's home directory, login time, idle times, office location, and the last time they both received or read mail.
- **Rpfinfo:** The `rpfinfo` command helps to enumerate Remote Procedure Call (RPC) protocol. It makes an RPC call to an RPC server and reports what it finds.

- **Enum4linux:** The `enum4linux` command is used for enumerating information from Windows and Samba systems. The application basically acts as a wrapper around the Samba commands `smbclient`, `rpclient`, `net`, and `nmblookup`.

NTP Enumeration

Network Time Protocol (NTP) is a protocol designed to synchronize clocks of networked computers. Networks using Kerberos or other time-based services need a time server to synchronize systems. NTP uses UDP port 123. Basic commands that can be attempted include the following:

- **Ntpdate:** Used to collect time samples
- **Ntptrace:** Follows time servers back up the chain to primary time server
- **Ntpdc:** Used to query about the state of the time server
- **Ntpq:** Used to monitor performance

NTP enumeration tools include the following:

- PresenTense Time Server
- NTP Server Scanner
- LAN Time Analyzer

SMTP Enumeration

Simple Mail Transfer Protocol (SMTP) is used for the transmission of email messages. SMTP operates on TCP port 25. SMTP is something that a hacker will be interested in because it can potentially be used to perform username enumeration via the `EXPN`, `RCPT`, and `VRFY` commands. Penetration testers can also leverage the usernames that have been obtained from this enumeration to conduct further attacks on other systems. SMTP enumeration can be performed with utilities like Netcat. From the command line, you type the following:

```
nc -v -z -w 2 IP Address 1-1024
```

Other common SMTP enumeration tools include the following:

- NetScan Tools Pro
- Nmap
- Telnet

DNS Enumeration

Domain Name System (DNS) enumeration is the process of locating all information about DNS. This can include identifying internal and external DNS servers and performing lookups of DNS records for information such as usernames, computer names, and IP addresses of potential target systems and performing zone transfers. Much of this activity was done in Chapter 3, "Footprinting and Scanning." The most straightforward way is to use Nslookup, but you can also use other tools. Tools for enumeration include the following:

- DigDug
- WhereIsIP
- NetInspector
- Men and Mice Management Console

System Hacking

Key Topic

System hacking is a big step in the fact that you are no longer simply scanning and enumerating a system. At this point, you are attempting to gain access. Things start to change because this stage is about breaking and entering into the targeted system. Previous steps, such as footprinting, scanning, and enumeration, are all considered pre-attack stages. As stated, before you begin, make sure that you have permission to perform these activities on other people's systems.

The primary goal of the system hacking stage is to authenticate to the remote host with the highest level of access. This section covers some common nontechnical and technical password attacks against authentication systems.

Nontechnical Password Attacks

Attackers are always looking for easy ways to gain access to systems. Hacking authentication systems is getting harder because most organizations have upped their game, using strong authentication and improving auditing controls. That is one reason why nontechnical attacks remain so popular. Basic techniques include the following:

- **Dumpster diving:** Dumpster diving is the act of looking through a company's trash to find information that may help in an attack. Access codes, notes, passwords, and even account information can be found.
- **Social engineering:** We spend much more time discussing social engineering later in the book, but for now what is important to know is that social engineering is the manipulation of people into performing actions or divulging confidential information.

- **Shoulder surfing:** The act of watching over someone's shoulder to get information such as passwords, logins, and account details.

Technical Password Attacks

Technical password attacks require some use of technology. These attacks also build on the information you have obtained in the previous steps. Tools used during enumeration, such as Getacct, IP Network Browser, and net view, may have returned some valuable clues about specific accounts. By now, you may even have account names, know who is the administrator, know whether there is a lockout policy, and even know the names of open shares. Technical password attack techniques discussed here include the following:

- Password guessing
- Automated password guessing
- Password sniffing
- Keyloggers

Many of today's most successful attacks involve both technical and nontechnical elements.

Password Guessing

Guessing usernames and passwords requires that you review your findings. Remember that good documentation is always needed during a penetration test, so make sure that you have recorded all your previous activities. When password guessing is successful, it is usually because people like to use easy to remember words and phrases. A diligent penetration tester or attacker will look for subtle clues throughout the enumeration process to key in on—probably words or phrases the account holder might have used for a password. What do you know about this individual, what are his hobbies? If the account holder is not known to you, focus on accounts that

- Haven't had password changes for a long time
- Have weakly protected service accounts
- Have poorly shared accounts
- Indicate the user has never logged in
- Have information in the comment field that might be used to compromise password security

If you can identify such an account, you can issue the `net use` command from the command line to attempt the connection:

```
net use * \\IP_address\share * /u:name
```

You'll be prompted for a password to complete the authentication:

```
C:\ >net use * \\192.188.13.10\c$ * /u:jack
Type the password for \\172.20.10.79\c$:
The command completed successfully
```

Automated Password Guessing

Because you may want to set up a method of trying each account once or twice for weak passwords, you might consider looping the process. Automated password guessing can be performed by constructing a simple loop using the Windows command shell. It is based on the standard `net use` syntax. The steps are as follows:

1. Create a simple username and password file.
2. Pipe this file into a `FOR` command as follows:

```
C:\ > FOR  /F "token=1, 2*" %i in (credentials.txt) do net use \\target\IPC$
        %i /u:%j
```

Many dedicated software programs automate password guessing. Some of the more popular free tools include NAT, Brutus, THC Hydra, and Venom. NetBIOS Auditing Tool (NAT) is a command-line automated password guessing tool. Just build a valid list of users from the tools discussed during enumeration. Save the usernames to a text file. Now create a second list with potential passwords. Feed both of these into NAT, as follows:

```
nat [-o filename] [-u userlist] [-p passlist] <address>
```

NAT attempts to use each name to authenticate with each password. If it is successful, it halts the program at that point. Then you want to remove that name and start again to find any additional matches. You can grab a copy of NAT at www.tux.org/pub/security/secnet/tools/nat10/.

NOTE Make sure that you identify whether there is a password lockout policy, because you might have only two or three tries before the account is locked. Otherwise, you might inadvertently cause a denial of service (DoS) if you lock out all the users.

Password Sniffing

If your attempts to guess passwords have not been successful, sniffing or keystroke loggers might offer hope. Do you ever think about how much traffic passes over a typical network every day? Most networks handle a ton of traffic, and a large portion of it might not even be encrypted. Password sniffing requires that you have physical or logical access to the device. If that can be achieved, you can simply sniff the credentials right off the wire as users log in.

One such tool is Pass-The-Hash. This application allows an attacker to authenticate to a remote server using the LM/NTLM hash of a user's password, eliminating the need to crack/brute-force the hashes to obtain the clear-text password. Because Windows does not salt passwords, they remain static from session to session until the password is changed. If an attacker can obtain a password hash, it can be functionally equivalent to obtaining the clear-text password. Rather than attempting to crack the hash, attackers can simply replay them to gain unauthorized access. You can download Pass-The-Hash at http://corelabs.coresecurity.com/index.php?module=Wiki&action=view&type=tool&name=Pass-The-Hash_Toolkit. ScoopLM is another tool designed to sniff password hashes; it sniffs for Windows authentication traffic. When passwords are detected and captured, it features a built-in dictionary and brute-force cracker.

Besides capturing Windows authentications, there are also tools to capture and crack Kerberos authentication. Remember that the Kerberos protocol was developed to provide a secure means for mutual authentication between a client and a server. It enables the organization to implement single sign-on (SSO). You should already have a good idea if Kerberos is being used, as you most likely scanned port 88, the default port for Kerberos, in an earlier step.

KerbCrack, a tool from NTSecurity.nu, can be used to attack Kerberos. It consists of two separate programs. The first portion is a sniffer that listens on port 88 for Kerberos logins, and the second portion is used as a cracking program to dictionary or brute-force the password. If all this talk of sniffing has raised your interest in the topic, you'll enjoy Chapter 7, "Sniffers, Session Hijacking, and Denial of Service," which covers sniffers in detail.

TIP If none of the options discussed previously are feasible, there is still keystroke logging, which is discussed next.

Keystroke Loggers

Keystroke loggers can be software or hardware devices used to monitor activity. Although an outsider to a company might have some trouble getting one of these devices installed, an insider is in a prime position.

Hardware keystroke loggers are usually installed while users are away from their desks and are completely undetectable, except for their physical presence. When was the last time you looked at the back of your computer? Even then, they can be overlooked because they resemble a keyboard extension cable or adapter; www.keyghost.com has a large collection. Some hardware keyloggers use WiFi, which means that once it is deployed the attacker does not have to retrieve the device and can communicate with it remotely via wireless or Bluetooth connection.

Software keystroke loggers sit between the operating system and the keyboard. Most of these software programs are simple, but some are more complex and can even email the logged keystrokes back to a preconfigured address. What they all have in common is that they operate in stealth mode and can grab all the text a user enters. Table 4-4 shows some common keystroke loggers.

Table 4-4 Software Keystroke Loggers

Product	URL
ISpyNow	www.ispynow.net
PC Activity Monitor	PCActivityMonitor.org
RemoteSpy	www.remotespy.com
Spector	www.spectorsoft.com
KeyStrokeSpy	www.keylogger-software.com

TIP Keystroke loggers are one way to obtain usernames and passwords.

Privilege Escalation and Exploiting Vulnerabilities

If the attacker can gain access to a Windows system as a standard user, the next step is privilege escalation. This step is required because standard user accounts are limited; to be in full control, administrator access is needed. This might not always be an easy task because privilege-escalation tools must be executed on the victim's

system. How do you get the victim to help you exploit a vulnerability? Common techniques include the following:

- Exploiting an application
- Tricking the user into executing the program
- Copying the privilege escalation tool to the targeted system and schedule the exploit to run at a predetermined time, such as the `AT` command
- Gaining interactive access to the system, such as Terminal Server, pcAnywhere, and so on

Exploiting an Application

Sometimes a hacker can get lucky and exploit a built-in application. For example, when you press the Shift key five or more times Windows opens StickyKeys options for you. The resulting dialog box that appears is an interface to enable the use of StickyKeys, which is a Windows feature to aid handicapped users. There is nothing wrong with the use of this feature. The only problem is how it is implemented. If an attacker can gain access, it mght be possible to replace sethc.exe with cmd.exe. After replacing the file, you can invoke the command prompt and execute explorer.exe and commands with full access to the computer.

The reason this attacks works is because it slips through all of Windows protection checks. Windows first checks whether the .exe is digitally signed, which cmd.exe is. Next, it checks that the .exe is located in the system directory (%systemroot%\system32), thus validating integrity level and administrator permissions. Windows then checks to make sure the executable is on its internal list of Windows protected system files and known to be part of the OS, which cmd.exe is and therefore passes. Therefore, Windows thinks that it is launching the accessibility feature StickyKeys, but instead it is launching shellcode running as LocalSystem.

Exploiting a Buffer Overflow

It's important to realize that buffer overflows, memory corruption, heap attacks are patched over time. Therefore, these exploits work only for specific versions of operating system or application. An example of this can be seen with the Aurora exploit. This exploit was used to gain access on vulnerable Windows systems running Internet Explorer 6. The exploit caused a memory corruption flaw in Internet Explorer. This flaw was found in the wild and was a key component of the Operation Aurora attacks used against Google and others. The attack works by spraying the heap with a large amount of data. Heap spraying is the act of loading a large amount of data in the heap along with some shellcode. The aim of placing all of this data onto the

heap is to create the right conditions in memory to allow the shellcode to be executed.

Java is another application that has been exploited in several attacks. One example is the Java watering hole attacks in 2013. Stack-based buffer overflows in the Java Stored Procedure infrastructure allows remotely authenticated users to execute arbitrary code by leveraging certain CONNECT and EXECUTE privileges. Some well-known privilege-escalation tools are shown here:

- **Billybastard.c:** Windows 2003 and XP
- **ANI Exploit:** Windows Vista
- **Getad.exe:** Windows 2003 and XP
- **ERunAs2X.exe:** Windows 2000

TIP Keeping systems and applications patched is one of the best countermeasures you can do to defend against privilege-escalation tools.

Owning the Box

One of the first activities an attacker wants to do after he owns the box is to make sure that he has continued access and that he has attempted to cover his tracks. One way to ensure continued access is to compromise other accounts. Stealing SAM is going to give the attacker potential access to all the passwords. SAM contains the user account passwords stored in their hashed form. Microsoft raised the bar with the release of NT Service Pack 3 by adding a second layer of encryption called SYSKEY. SYSKEY adds a second layer of 128-bit encryption. After being enabled, this key is required by the system every time it is started so that the password data is accessible for authentication purposes.

Attackers can steal the SAM through physical or logical access. If physical access is possible, the SAM can be obtained from the NT ERD (Emergency Repair Disk) from C:\winnt\repair\sam. Newer versions of Windows place a backup copy in C:\winnt\repair\regback\sam, although SYSKEY prevents this from easily being cracked. One final note here is that you can always just reset the passwords. If you have physical access, you can simply use tools such as LINNT and NTFSDOS to gain access. NTFSDOS can mount any NTFS partition as a logical drive. NTFSDOS is a read-only network file system driver for DOS/Windows. If loaded onto a CD or thumb drive, it makes a powerful access tool. Logical access presents some easier possibilities. The Windows SAM database is a binary format, so it's not

easy to directly inspect. Tools such as PWdump and LCP can be used to extract and crack SAM. Before those programs are examined, let's briefly review how Windows encrypts passwords and authenticates users.

Authentication Types

Windows supports many authentication protocols, including those used for network authentication, dialup authentication, and Internet authentication. For network authentication and local users, Windows supports Windows NT Challenge/Response, also known as NTLM. Windows authentication algorithms have improved over time. The original LAN Manager (LM) authentication has been replaced by NTLMv2. Windows authentication protocols include the following:

- **LM authentication:** Used by 95/98/Me and is based on DES
- **NTLM authentication:** Used by NT until Service Pack 3 and is based on DES and MD4
- **NTLM v2 authentication:** Used post-NT Service Pack 3 and is based on MD4 and MD5
- **Kerberos:** Implemented first in Windows 2000 and can be used by all current versions of Windows, including Server 2012 and Windows 8

Because of backward compatibility, LM can still be used. These encrypted passwords are particularly easy to crack because an LM password is uppercased, padded to 14 characters, and divided into two 7-character parts. The two hashed results are concatenated and stored as the LM hash, which is stored in SAM. To see how weak this system is, consider the following example. Let's say that an LM password to be encrypted is Dilbert!:

1. When this password is encrypted with an LM algorithm, it is converted to all uppercase: DILBERT!
2. Then the password is padded with null (blank) characters to make it a 14-character length: DILBERT!_ _ _ _ _ _
3. Before encrypting this password, the 14-character string is divided into two seven character pieces: DILBERT and !_ _ _ _ _ _
4. Each string is encrypted individually, and the results are concatenated together.

With the knowledge of how LM passwords are created, examine the two following password entries that have been extracted from SAM with PWdump:

```
Bart:  1001:
B79135112A43EC2AAD3B431404EE:
DEAC47322ABERTE67D9C08A7958A:

Homer: 1002:
B83A4FB0461F70A3B435B51404EE:
GFAWERTB7FFE33E43A2402D8DA37:
```

Notice how each entry has been extracted in two separate character fields? Can you see how the first half of each portion of the hash ends with 1404EE? That is the padding, and this is how password-cracking programs know the length of the LM password. It also aids in password-cracking time. Just consider the original Dilbert! example. If extracted, one seven-character field will hold Dilbert, whereas the other only has one character (!).

Cracking 1 character or even 7 is much easier than cracking a full 14. Fortunately, Windows has moved on to more secure password algorithms. Windows can use six levels of authentication now, as shown in Table 4-5. Using longer passwords, greater than 14 characters, and using stronger algorithms is one of the best defenses against cracking passwords.

Table 4-5 LM, NTLM, and NTLM2

Attribute	LM	NTLM	NTLMv2
Password	Yes	No	No
Hash	DES	MD4	MD5
Algorithm	DES	DES	HMAC

TIP Kerberos authentication started with Windows 2000 and is the default authentication on all current versions of Microsoft Windows products. Kerberos is considered a strong form of authentication.

Cracking the Passwords

One direct way to remove the passwords from a local or remote system is by using L0phtcrack. L0phtcrack is a Windows password-cracking tool. LC6 is the current version. It can extract hashes from the local machine, a remote machine, and can sniff passwords from the local network if you have administrative rights.

Tools like FGdump and PWdump are other good password-extraction tools. You can get a copy of this tool at www.openwall.com/passwords/nt.shtml. This command-line tool can bypass SYSKEY encryption if you have administrative access. PWdump works by a process of dynamic link library (DLL) injection. This allows the program to hijack a privileged process. PWdump7, the current version, was expanded to allow remote access to the victim system. The program is shown here:

```
C:\ pwdump>pwdump7 192.168.13.10 password.txt
Completed.
```

For PWdump7 to work correctly, you need to establish a session to an administrative share. The resulting text file reveals the hashed passwords:

```
C:\ pwdump>type password.txt
Jack:       500:       A34A4329AAD3MFEB435B51404EE:
                       FD02A1237LSS80CC22D98644FE0:
Ben:       1000:       466C097A37B26C0CAA5B51404EE:
                       F2477A14LK4DFF4F2AC3E3207FE0:
Guest:      501:       NO PASSWORD*********************:
                       NO PASSWORD*********************:
Martha:    1001:       D79135112A43EC2AAD3B431404EE:
                       EEAC47322ABERTE67D9C08A7958A:
Curley:    1002:       D83A4FB0461F70A3B435B51404EE:
                       BFAWERTB7FFE33E43A2402D8DA37
```

With the hashed passwords safely stored in the text file, the next step is to perform a password crack. Historically, three basic types of password cracking exist: dictionary, hybrid, and brute-force attacks.

A dictionary password attack pulls words from the dictionary or word lists to attempt to discover a user's password. A dictionary attack uses a predefined dictionary to look for a match between the encrypted password and the encrypted dictionary word. Many times, dictionary attacks will recover a user's password in a short period of time if simple dictionary words are used.

A hybrid attack uses a dictionary or a word list and then prepends and appends characters and numbers to dictionary words in an attempt to crack the user's password. These programs are comparatively smart because they can manipulate a word and use its variations. For example, take the word *password*. A hybrid password audit would attempt variations such as 1password, password1, p@ssword, pa44w0rd, and so on. Hybrid attacks might add some time to the password-cracking process, but they increase the odds of successfully cracking an ordinary word that has had some variation added to it.

A brute-force attack uses random numbers and characters to crack a user's password. A brute-force attack on an encrypted password can take hours, days, months, or years, depending on the complexity and length of the password. The speed of success depends on the speed of the CPU's power. Brute-force audits attempt every combination of letters, numbers, and characters.

Tools such as L0phtcrack, LCP, Cain and Abel, and John the Ripper can all perform dictionary, hybrid, and brute-force password cracking. The most popular are explained in the following list:

- Cain and Abel is a multipurpose tool that can perform a variety of tasks, including password cracking, Windows enumeration, and Voice over IP (VoIP) sniffing. The password-cracking portion of the program can perform dictionary/brute-force attacks and can use precomputed rainbow tables. It is shown in Figure 4-4. Notice the many types of password cracking it can perform.

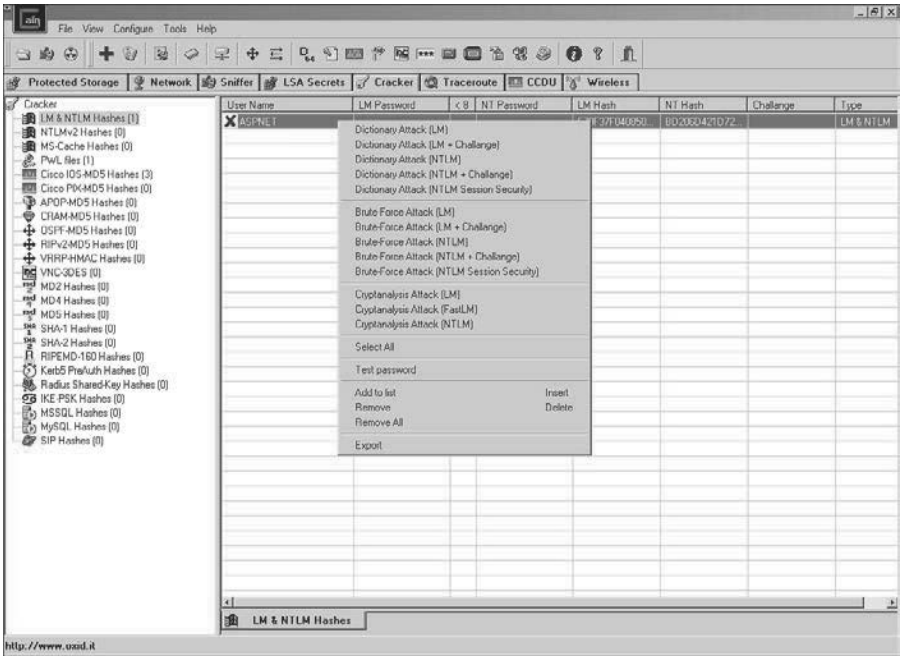


Figure 4-4 Cain and Abel.

- John the Ripper is another great password-auditing tool. It is available for 11 types of UNIX systems, plus Windows. It can crack most common passwords, including Kerberos AFS and Windows hashes. Also, a large number of add-on modules are available for John the Ripper that can enable it to crack OpenVMS passwords, Windows credentials cache, and MySQL passwords. Just

remember that the cracked passwords are not case sensitive and might not represent the real mixed-case password. A determined attacker can overcome this small hindrance.

Years ago, dictionary, hybrid, and brute-force attacks were the primary methods used to recover passwords or attempt to crack them. Many passwords were considered secure just because of the time it would take to crack them. This time factor was what made these passwords seem secure. If given enough time, the password could be cracked, but it might take several months. A relatively new approach to password cracking has changed this belief. It works by means of a rainbow table. The RainbowCrack technique is the implementation of Philippe Oechslin's faster time-memory trade-off technique. It works by precomputing all possible passwords in advance. After this time-consuming process is complete, the passwords and their corresponding encrypted values are stored in a file called a rainbow table. An encrypted password can be quickly compared to the values stored in the table and cracked within a few seconds. RainbowCrack and Ophcrack are examples of two such programs.

Ophcrack is a password-cracking tool that implements the rainbow table techniques previously discussed. What's most important to note here is that if a password is in the rainbow table, it will be cracked quickly. Its website also lets you enter a hash and reveal the password in just a few seconds.

Hiding Files and Covering Tracks

Before moving on to other systems, the attacker must attend to a few unfinished items. According to Locard's exchange principle, "Whenever someone comes in contact with another person, place, or thing, something of that person is left behind." This means that the attacker must disable logging, clear log files, eliminate evidence, plant additional tools, and cover his tracks. Listed here are some of the techniques that an attacker can use to cover his tracks.

- **Disabling logging:** Auditpol was originally included in the NT Resource Kit for administrators. It works well for hackers, too, as long as they have administrative access. Just point it at the victim's system as follows:

```
C:\ >auditpol \\ 192.168.13.10 /disable
Auditing Disabled
```

- **Clear the log file:** The attacker will also attempt to clear the log. Tools such as Winzapper, Evidence Eliminator, and ELSave can be used. ELSave will remove all entries from the logs, except one entry that shows the logs were cleared. It is used as follows:

```
elsave -s \\192.168.13.10 -l "Security" -C
```

One way for attackers to cover their tracks is with rootkits. Rootkits are malicious codes designed to allow an attacker to get expanded access and hide his presence. Rootkits were traditionally a Linux tool, but they are now starting to make their way into the Windows environment. Rootkits such as FU, Vanquish, Hacker Defender, and AFX are all available for Windows systems.

Rootkits can be classified as hypervisor, kernel level, application level, hardware/firmware, boot loader, and library level. Some of these rootkits, such as kernel level, are particularly dangerous because they take control of the operating system kernel. If you suspect that a computer has been rootkitted, you need to use an MD5 hashing utility or a program, such as Tripwire, to determine the viability of your programs. The only other alternative is to rebuild the computer from known good media.

File Hiding

Various techniques are used by attackers to hide their tools on the compromised computer. Some attackers might just attempt to use the `attribute` command to hide files, whereas others might place their files in low traffic areas. A more advanced method is to use NTFS alternate data streams (ADS). NTFS ADS was developed to provide for compatibility outside of the Windows world with structures, such as the Macintosh Hierarchical File System (HFS). These structures use resource forks to maintain information associated with a file, such as icons and so on.

The streams are a security concern because an attacker can use these streams to hide files on a system. ADS provides hackers with a means of hiding malware or hacking tools on a system to later be executed without being detected by the systems administrator. Because the streams are almost completely hidden, they represent a near-perfect hiding spot on a file system. It allows the attacker the perfect place to hide his tools until he needs to use them at a later date. An ADS stream is essentially files that can be executed. To delete a stream, its pointer must be deleted first (or copy the pointer file to a FAT file system). That will delete the stream because FAT cannot support ADS. To create an ADS, issue the following command:

```
Type certguide.zip > readme.txt:certguide.zip
```

This command streamed certguide.zip behind readme.txt. This is all that is required to stream the file. Now the original secret file can be erased:

```
Erase certguide.zip
```

All the hacker must do to retrieve the hidden file is to type the following:

```
Start c:\readme.txt:certguide.zip
```

This will execute ADS and open the secret file. Tools that can detect streamed files include the following:

- **Streams:** A Microsoft tool
- **Sfind:** A Foundstone forensic tool for finding streamed files
- **LNS:** Another tool used for finding streamed files, developed by ntsecurity.nu

Linux does not support ADS, although an interesting slack space tool is available called Bmap, which you can download from www.securityfocus.com/tools/1359. This Linux tool can pack data into existing slack space. Anything could be hidden there, as long as it fits within the available space or is parsed up to meet the existing size requirements.

One final step for the attacker is to gain a command prompt on the victim's system. This allows the attacker to actually be the owner of the box. Tools that allow the attacker to have a command prompt on the system include Psexec, Remoxec, and Netcat. Netcat is covered in detail in Chapter 6, "Trojans and Backdoors." After the attacker has a command prompt on the victim's computer, he will usually restart the methodology, looking for other internal targets to attack and compromise. At this point, the methodology is complete. As shown in Figure 4-5, you can see that the attacker has come full circle.

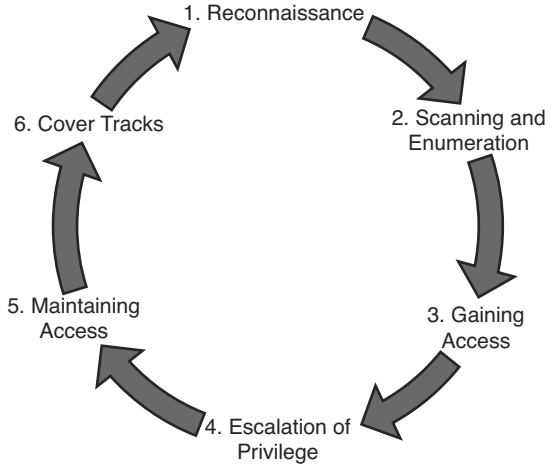


Figure 4-5 Methodology overview.

Chapter Summary

In this chapter, you learned about Windows enumeration and system hacking. Enumeration of Windows systems can be aided by SMB, the `IPC$` share, SMTP, SNMP, and DNS. Each offers opportunities for the attacker to learn more about the network and systems he is preparing to attack. The goal of enumeration is to gather enough information to map the attack surface, which is a collection of potential entry points. It might be a buffer overflow, an unsecure application, such as SNMPv1 or 2, or even a weak password that is easily guessed.

System hacking represents a turning point, which is the point at which the attacker is no longer probing but is actually attacking the systems and attempting to break in. System hacking might start with a low-level account. One key component of system hacking is escalation of privilege, which is the act of exploiting a bug, design flaw, or configuration oversight to gain elevated access. The attacker's overall goal is to own the system. After spending time gaining access, the attacker will want long-term control of the computer or network. After an attacker penetrates and controls one computer, he rarely stops there. He will typically work to cover his tracks and remove any log entries. Besides redirecting sensitive information, stealing proprietary data, and establishing backdoors, attackers will most likely use the compromised system to spread their illegal activities to other computers. If any one system is compromised, the entire domain is at risk. The best defense is a good offense. Don't give the attacker any type of foothold.

Exam Preparation Tasks

As mentioned in the section "How to Use This Book" in the Introduction, you have a couple of choices for exam preparation: the exercises here; Chapter 14, "Final Preparation"; and the exam simulation questions on the CD-ROM.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 4-6 lists a reference of these key topics and the page numbers on which each is found.

Table 4-6 Key Topics for Chapter 4

Key Topic

Key Topic Element	Description	Page Number
Section	Explains how enumeration works	140
Table 4-2	User ID and corresponding RID code	142

Key Topic Element	Description	Page Number
Table 4-3	Microsoft key ports and protocols	143
Section	Explains how system hacking works	151
Section	Explains how ADS works	163

Define Key Terms

Define the following key terms from this chapter and check your answers in the glossary:

Active Directory, brute-force attack, dictionary attack, hybrid attack, Inter-Process Communication, kernel, kernel mode, keystroke loggers, local security authority subsystem, NetBIOS, RainbowCrack techniques, relative identifiers, Security Accounts Manager, security identifiers, Server Message Block, Simple Network Management Protocol, and user mode

Command Reference to Check Your Memory

The CEH exam focuses on practical, hands-on skills that are used by a security professional. Therefore, you should be able to identify common `net use` commands.

Table 4-7 `net use` Commands

Task	Command Syntax
Null session	`net use \\ip address\ipc$ "" /u:""`
Map a drive	`net use * \\ip address\share * /u:username`
View open shares	`net view \\ipaddress`

Exercise

4.1 NTFS File Streaming

By using NTFS file streaming, you can effectively hide files in an NTFS environment.

Estimated Time: 15 minutes.

1. Download Sfind and LNS—two good NTFS file streaming programs. Sfind is at www.antiserver.it/Win%20NT/Security/download/ForensicToolkit14.exe, and LNS is at www.ntsecurity.nu/toolbox/lns/.
2. Create a temporary folder on the root of your NTFS drive. Name the folder **test**, or give it another suitable name.
3. Copy notepad.exe into the test folder and rename it **hack.exe**. You will use this file to simulate it as the hacking tool.
4. Next, create a text file called **readme.txt**. Place some text inside the readme file, something like hello world will work.
5. Open a command prompt and change directories to place yourself in the test folder. By performing a directory listing, you should see two files: hack.exe and readme.txt. Record the total free space shown after the directory listing:

   _____
6. From the command line, issue the following command:

```
Type hack.exe > readme.txt:hack.exe
```

7. Now run a directory listing again and record the free space results:

   _____
8. Has anything changed? You should have noticed that free space has been reduced. That is because you streamed hack.exe behind readme.txt.
9. Execute the following from the command line:

```
Start c:\ test\ readme.txt:hack.exe
```

10. Did you notice what happened? Your hacked file, notepad.exe, should have popped open on the screen. The file is completely hidden, as it is streamed behind readme.txt.
11. Finally run both Sfind and LNS from the command line. Both programs should detect the streamed file hack.exe. File streaming is a powerful way to hide information and make it hard to detect.

Review Questions

1. How can you determine whether an LM hash you extracted contains a password that is fewer than eight characters long?
   a. There is no way to tell because a hash cannot be reversed.
   b. The rightmost portion of the hash is always the same.

c. The hash always starts with AB923D.

d. The leftmost portion of the hash is always the same.

2. Which of the following is a well-known password-cracking program?

a. L0phtcrack

b. Netcat

c. Jack the Ripper

d. NetBus

3. What did the following commands determine?

```
C:\  user2sid \ \ truck guest
S-1-5-21-343818398-789336058-1343024091-501
C:\ sid2user 5 21 343818398 789336058 1343024091 500
Name is Joe
Domain is Truck
```

a. These commands demonstrate that the Joe account has a SID of 500.

b. These commands demonstrate that the guest account has not been disabled.

c. These commands demonstrate that the guest account has been disabled.

d. These commands demonstrate that the true administrator is Joe.

4. What is the RID of the true administrator?

a. 0

b. 100

c. 500

d. 1000

5. What is the best alternative if you discover that a rootkit has been installed on one of your computers?

a. Copy the system files from a known good system.

b. Perform a trap and trace.

c. Delete the files and try to determine the source.

d. Rebuild from known good media.

6. To increase password security, Microsoft added a second layer of encryption. What is this second later called?
   a. Salt
   b. SYSKEY
   c. SYS32
   d. SAM

7. SNMP is a protocol used to query hosts and other network devices about their network status. One of its key features is its use of network agents to collect and store management information, such as the number of error packets received by a managed device. Which of the following makes it a great target for hackers?
   a. It's enabled by all network devices by default.
   b. It's based on TCP.
   c. It sends community strings in cleartext.
   d. It is susceptible to sniffing if the community string is known.

8. Which of the following is the best way to prevent the use of LM authentication of your legacy Windows 2003 servers?
   a. Use the LMShut tool from Microsoft.
   b. Use the NoLMHash Policy by Using Group Policy.
   c. Disable Lsass in Windows 2003.
   d. Use a password that is at least 10 characters long.

9. Which of the following tools can be used to clear the Windows logs?
   a. Auditpol
   b. ELSave
   c. PWdump
   d. Cain and Abel

10. What is one of the disadvantages of using John the Ripper?
    a. It cannot crack NTLM passwords.
    b. It separates the passwords into two separate halves.
    c. It cannot differentiate between uppercase and lowercase passwords.
    d. It cannot perform brute-force cracks.

11. You found the following command on a compromised system:

```
Type nc.exe > readme.txt:nc.exe
```

What is its purpose?

a. This command is used to start a Netcat listener on the victim's system.
b. This command is used to stream Netcat behind readme.txt.
c. This command is used to open a command shell on the victim with Netcat.
d. This command is used to unstream Netcat.exe.

12. Which of the following uses the faster time-memory trade-off technique and works by precomputing all possible passwords in advance?

a. Rainbow tables
b. Dictionary cracks
c. Hybrid cracks
d. Brute-force crack

13. Why would an attacker scan for port 445?

a. To attempt to DoS the NetBIOS SMB service on the victim system
b. To scan for file and print sharing on the victim system
c. To scan for SMB services and verify that the system is Windows 2000 or greater
d. To scan for NetBIOS services and verify that the system is truly a Windows NT server

14. You have downloaded a tool called SYSCracker, and you plan to use it to break SYSKEY encryption. The first thing the tool prompts you for is to set the level of SYSKEY encryption. How many bits are used for SYSKEY encryption?

a. 40 bits
b. 64 bits
c. 128 bits
d. 256 bits

15. You are trying to establish a null session to a target system. Which is the correct syntax?

    a. `net use \\ IP_address\ IPC$ "" /u:""`

    b. `net use //IP_address/IPC$ "" \ u:""`

    c. `net use \\ IP_address\ IPC$ * /u:""`

    d. `net use \\ IP_address\ IPC$ * \ u:""`

Suggested Reading and Resources

www.bindview.com/Services//RAZOR/Utilities/Windows/enum_readme.cfm: Enum website

www.systemtools.com/cgi-bin/download.pl?DumpAcl: DumpSec home page

http://evgenii.rudnyi.ru/programming.html#overview: SID2USER enumeration tools

www.securityfocus.com/infocus/1352: Enumerating Windows systems

www.microsoft.com/resources/documentation/Windows/2000/server/reskit/en-us/Default.asp?url=/resources/documentation/Windows/2000/server/reskit/en-us/cnet/cnbd_trb_gtvp.asp: NBTStat overview and uses

www.governmentsecurity.org/articles/ExploitingTheIPCShare.php: Exploiting the `IPC$` share

www.netbus.org/keystroke-logger.html: Keystroke loggers

www.theregister.co.uk/2003/03/07/windows_root_kits_a_stealthy: Windows rootkits

www.hnc3k.com/hackingtutorials.htm: Hacking Windows

www.antionline.com/showthread.php?threadid=268572: Privilege/escalation tools

45. Which of the following tools is used for web-based password cracking?
    a. ObiWan
    b. SQLSmack
    c. Wikto
    d. N-Stealth
46. The initialization vector for WEP was originally how long?
    a. 8 bits
    b. 16 bits
    c. 24 bits
    d. 40 bits
47. This version of 802.11 wireless operates at the 5.725 to 5.825GHz range.
    a. 802.11a
    b. 802.11b
    c. 802.11g
    d. 802.1x
48. Although WEP is a good first start at securing wireless LAN communication, it has been widely reported as having vulnerabilities. Which of the following is one of the primary reasons that WEP is vulnerable?
    a. The encryption method used is flawed.
    b. The 24-bit IV field is too small.
    c. The encryption is too weak since it only used a 40-bit key.
    d. Tools such as WEPCrack have been optimized to crack WEP in only a few minutes.
49. WEP uses which of the following types of encryption?
    a. Symmetric
    b. Asymmetric
    c. Public key encryption
    d. SHA-1

50. Ron would like your advice on a wireless WEP cracking tool that can save him time and get him better results with fewer packets. Which of the following tools would you recommend?

    a. Kismet

    b. Aircrack

    c. WEPCrack

    d. AirSnare

51. While scanning, you have not been able to determine what is in front of 192.168.13.10, which you believe to be some type of firewall. Your Nmap scan of that address seems to hang without response. What should you do next?

    a. Perform an Nmap stealth scan.

    b. Perform an Nmap OS scan.

    c. Run Hping with Null TCP settings.

    d. Attempt to banner grab from the device.

52. What does an ICMP type 3 code 13 denote?

    a. Subnet mask request

    b. TTL failure

    c. Administratively prohibited

    d. Redirect

53. During a penetration test, you saw a contractor use the tool ACKCMD. Which of the following best describes the purpose of the tool?

    a. It is being used as a Windows exploit.

    b. It is being used as a covert channel.

    c. It is being used as a honeypot.

    d. It is being used to exploit routers.

54. You have been asked to enter the following rule into Snort: `Alert tcp any any -> any 23(msg: "Telnet Connection Attempt")`. What is its purpose?

    a. This is a logging rule designed to notify you of the use of Telnet in either direction.

    b. This is a logging rule designed to notify you of the use of Telnet in one direction.

c. This is an alert rule designed to notify you of the use of Telnet in either direction.

d. This is an alert rule designed to notify you of the use of Telnet in one direction.

55. Snort is a useful tool. Which of the following best describes Snort's capabilities?

a. Proxy, IDS, and sniffer

b. IDS and sniffer

c. IDS, packet logger, and sniffer

d. Firewall, IDS, and sniffer

56. You are visiting a client site and have noticed a sheep dip system. What is it used for?

a. A sheep dip system is used for integrity checking.

b. A sheep dip system is another name for a honeypot.

c. A sheep dip system is used for virus checking.

d. A sheep dip system is used to find buffer overflows.

57. Which of the following is Melissa considered?

a. MBR infector

b. Macro infector

c. File infector

d. True worm

58. Which type of virus or worm has the capability to infect a system in more than one way?

a. Appenders

b. Polymorphic

c. Prependers

d. Multipartite

59. Which portion of the virus is responsible for copying the virus and attaching it to a suitable host?

a. Infection routine

b. Search routine

c. Antidetection routine

d. Trigger routine

60. In the Intel architecture, which of the following instructions is one byte long and is represented in assembly language by the hex value 0X90?

a. Add

b. Mov

c. NOP

d. Sub

61. Management has become concerned that too many people can access the building and would like you to come up with a solution that only allows one person at a time entry and can hold them there if they fail authentication. Which of the following best describes what they are asking for?

a. A turnstile

b. A mantrap

c. A piggyback

d. Biometric authentication

62. Electrical fires are classified as which of the following?

a. Class A

b. Class B

c. Class C

d. Class D

63. Your company has become serious about security and has changed the rules. They will no longer let you control access to company information and resources. Now, your level of access is based on your clearance level and need to know. Which of the following systems have been implemented?

a. Discretionary access control

b. Mandatory access control

c. Role-based access control

d. Rule-based access control

64. Frequent password changes have made it hard for you to remember your current password. New help desk policies require them to ask you several questions for proper identification. They would like to know your mother's maiden name and your first pet's name. What is this type of authentication called?

- **a.** Biometric authentication
- **b.** Complex password
- **c.** Cognitive password
- **d.** Security token

65. Pedro has heard about a biometric trick in which he can use a gummy bear to fool a fingerprint scanner into providing him access even though he is not a legitimate user. Which of the following terms is most closely associated?

- **a.** False acceptance rate
- **b.** False positives
- **c.** False rejection rate
- **d.** Crossover error rate

66. Review the Wireshark TCP data flow shown here:

```
Host A          -- SYN -->              Host B Seq = 0 Ack = 919412342
Host A          <-- SYN, ACK ---          Host B Seq = 0 Ack = 1
Host A        -- ACK -->                  Host B Seq = 1 Ack = 1
Host A        --- PSH, ACK Len: 512 --->      Host B Seq = 1 Ack = 1
Host A        <--- ACK ---                  Host B Seq = 1 Ack = 901
Host A        <--- ACK Len: 1460 ---          Host B Seq = 1 Ack = 901
Host A        --- ACK --->                   Host B Seq = 901 Ack =
  1342
Host A      <--- ACK Len: 1452 ---     Host B Seq = 1342 Ack = 701
Host A        --- ACK --->              Host B Seq = 901 Ack = 2992
Host A      <--- ACK Len: 1452 ---     Host B Seq = 2992 Ack = 901
```

Which of the following statements is correct and represents the next appropriate acknowledgment from Host A?

- **a.** Sequence Number 901, Acknowledgment Number 3689
- **b.** Sequence Number 2992, Acknowledgment Number 901
- **c.** Sequence Number 2992, Acknowledgment Number 2993
- **d.** Sequence Number 901, Acknowledgment Number 4444

67. You have configured Wireshark to capture network traffic. You all looking specifically for ISNs. What type of attack are you a planning to perform?

    a. XSRF

    b. Sniffing

    c. Session hijacking

    d. XSS

68. Which of the following correctly describes Tripwire?

    a. Session hijacking

    b. Antivirus

    c. NIDS

    d. Integrity verification

69. An attacker has gone to a website that has an order entry field and entered the following: `mike@thesolutionfirm.com ; drop table users`

    What might the attacker be attempting?

    a. LDAP injection

    b. SQL injection

    c. XSRF

    d. XSS

70. While performing a security assessment on an organization's web application, you identify a web page that has a "search" text form entry designed to allow users to search for items on the site. Instead of a search you enter `<script> Your Hacked <script>` in the search box and press Enter. Afterward a pop-up appears that states, "You're Hacked." What kind of test has been performed?

    a. Directory traversal

    b. SQL injection

    c. XSRF

    d. XSS

71. While performing a security assessment on an organizations web application, you notice that if you enter `www.knowthetrade.com/../../../../Windows` you can view the folder contents. What type of attack does this describe?

    a. Directory traversal

    b. SQL injection

c. XSRF

d. XSS

72. While performing a security assessment on an organizations web application, you notice that if you enter `anything OR 1=1` into an search form on the website that you get an error returned that says "Microsoft OLE DB Provider for SQL Server error 80040e14." What kind of attack does this indicate?

a. Directory traversal

b. SQL injection

c. XSRF

d. XSS

73. You have been asked to review some code that was found on a compromised system.

```
/*
  attack.c
*/

#pragma check_stack(off)

#include <string.h>
#include <stdio.h>

void foo(const char* input)
{
    char buf[10];

    printf("Display this data:\n%p\n%p\n%p\n%p\n%p\n%p\n% p\n\n");

    strcpy(buf, input);
    printf("%s\n", buf);

    printf("Now display this:\n%p\n%p\n%p\n%p\n%p\n%p\n%p\n\n");
}

void bar(void)
{
    printf("Augh! I've been hacked!\n");
}
```

```
int main(int argc, char* argv[])
{
      printf("Address of foo = %p\n", foo);
    printf("Address of bar = %p\n", bar);
    if (argc != 2)
 {
        printf("Please supply a input value as an argument!\n");
        return -1;
 }
foo(argv[1]);
    return 0;
}
```

Based on your analysis of the code, what issue might arise from its use?

a. Exploit code

b. Buffer overflow

c. Parameter tampering

d. Cookie exploitation

74. You have configured Netcat as follows: `nc -v -l -p 80`. Which of the following is the best example of what you may be using Netcat for?

a. Low interaction honeypot

b. Port scanner

c. Banner grabber

d. File transfer

75. Which of the following DNS records is used for IPv6?

a. MX

b. AAAA

c. SOA

d. PTR

76. You are setting up your own network security lab and want to install Wireshark on a Windows 7 VM. What do you need to install first?

a. libPcap

b. winPcap

c. Ettercap

d. Etherape

77. Which of the following commands will allow you to capture traffic between two hosts when using TCPdump?

a. `tcpdump -i eth0 port 22`

b. `tcpdump -w test.pcap -i eth0 dst 192.168.201.166 and port 22`

c. `tcpdump -i eth0 not arp and not rarp`

d. `tcpdump -i eth0 arp`

78. You are on a high-speed network or you want to log the packets into a more compact form for later analysis. Which of the following is the correct syntax?

a. `snort -l ./log -b`

b. `snort -dev -l ./log`

c. `snort -v`

d. `snort dev -l log -1`

79. You are reviewing the following log file from TCPdump. What can you determine from the captured data?

```
12:54:28.378321 arp who-has w732 tell XP63
12:54:28.379323 arp duplicate address detected
12:54:28.379319 arp who-has XP63 tell w732
12:54:28.386982 arp who-has w733 tell XP63
12:54:28.387577 arp who-has XP63 tell w733
12:54:28.417102 arp who-has w735 tell XP63
12:54:28.418467 arp who-has XP63 tell w735
12:54:28.441782 arp who-has w736 tell XP63
12:54:28.443088 arp who-has XP63 tell w736
12:54:28.464739 arp who-has w738 tell XP63
12:54:28.465819 arp who-has XP63 tell w738
12:54:28.497036 arp who-has w740 tell XP63
12:54:28.498279 arp who-has XP63 tell w740
12:54:28.498381 arp duplicate address detected
12:54:28.512120 arp who-has stud1 tell XP63
12:54:28.513094 arp who-has XP63 tell stud1
12:54:28.541941 arp who-has w743 tell XP63
12:54:28.543183 arp who-has XP63 tell w743
12:54:28.566591 arp who-has w744 tell XP63
12:54:28.568011 arp who-has XP63 tell w744
```

```
12:54:28.568134 arp duplicate address detected
12:54:28.574582 arp who-has w745 tell XP63
```

a. Etherflood is being used.

b. A ping sweep is being performed.

c. ARP poisoning is being attempted.

d. Firesheep is being used.

80. Examine the following Snort capture and choose the correct answer.

```
12:55:28.586591: IDS181/nops-x86: 192.168.201.199:1903 ->
  192.168.201.164:53
```

a. The capture is a UDP connection to DNS.

b. The capture is a DNS reply.

c. The capture is a DNS query.

d. The capture indicates a buffer overflow attack.

81. You have just run a command that provided the following output:

```
Active Connections
  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:135            0.0.0.0:0              ESTABLISHED
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:554            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:2869           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:10243          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:12025          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:12110          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:12119          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:12143          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:12465          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:12563          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:12993          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:12995          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:27275          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING
```

Which of the following commands produced this output?

a. `TCPdump`

b. `Netstat -an`

c. `WinDump`

d. `Netstat -r`

82. A friend has been discussing Firewalking. Which of the following is true?

a. It alters TTLs.

b. It alters IP packets.

c. It alter RIP and OSPF packets.

d. It alters UDP packets.

83. Which of the following is not one of the three IP protocols that Snort supports?

a. UDP

b. BGP

c. TCP

d. ICMP

84. Examine the following rule:

```
log TCP any any -> 192.168.123.0/24 !6000:6010
```

Which of the following is not true?

a. This rule applies to any source port.

b. This rule applies to any source IP address.

c. This rule does not apply to port 6000.

d. This rule does apply to port 6000.

85. You have just run a port scan on an edge device and found ports 1745 and 1080 open. Which of the following is true?

a. It is most likely Microsoft's proxy server.

b. It is most likely a router.

c. It is most likely Check Point FireWall-1.

d. It is most likely Snort.

86. Which of the following properly describes an insertion attack?

- **a.** An IDS blindly believes and accepts a packet that an end system has rejected.
- **b.** Splits data between several packets that the IDS cannot detect.
- **c.** An end system accepts a packet that an IDS rejects.
- **d.** Uses polymorphic shell code to avoid detection.

87. Which of the following is an example of a honeypot?

- **a.** KFSensor
- **b.** Nessus
- **c.** Traffic Q Professional
- **d.** Hping

88. Which of the following is considered a low-powered protocol, supports close range, and has low bandwidth?

- **a.** 802.16
- **b.** 802.11b
- **c.** Bluetooth
- **d.** 802.11a

89. Which wireless standard has a frequency of 2.4GHz and 54Mbps?

- **a.** 802.11n
- **b.** 802.11b
- **c.** 802.11i
- **d.** 802.11a

90. Which of the following is an AirPcap adaptor used with?

- **a.** NetStumbler
- **b.** Aircrack
- **c.** John the Ripper
- **d.** Wireshark

91. How long are WEP IVs?

- **a.** 16 bits
- **b.** 24 bits

c. 30 bits

d. 32 bits

92. Which of the following will extract an executable from an NTFS stream?

a. `Start c:\legit.txt: hack.exe`

b. `Type hack.exe > legit.txt:`

c. `Start c:\hack.exe`

d. `Type hack.exe`

93. You have just sent an unsolicited message to a Bluetooth device. What is this called?

a. Bluejacking

b. Bluesnarfing

c. Bluesniffing

d. Bluesmacking

94. Which of the following correctly describes the war chalking symbol shown here?

a. Open

b. WEP

c. Nonbroadcast

d. None of the above

95. Which of the following is designed for MANs?

a. 802.16

b. 802.11b

c. 802.11i

d. 802.11a

96. Which of the following properly describes an evasion attack?

- **a.** An IDS blindly believes and accepts a packet that an end system has rejected.
- **b.** Splits data between several packets that the IDS cannot detect.
- **c.** An end system accepts a packet that an IDS rejects.
- **d.** Uses polymorphic shell code to avoid detection.

97. What is Loki used for?

- **a.** Honeypot detection
- **b.** Personal firewall
- **c.** OS identification
- **d.** Tunneling traffic via ICMP

98. Which of the following is not an example of a honeypot detection tool?

- **a.** Hunter
- **b.** Nessus
- **c.** Traffic Q Professional
- **d.** Hping

99. You have just run a port scan on an edge device and found ports 256, 257, 258, and 259 open. Which of the following it true?

- **a.** It is most likely Microsoft's proxy server.
- **b.** It is most like a router.
- **c.** It is most likely Check Point FireWall-1.
- **d.** It is most likely Snort.

100. You have been asked to review a segment of code and set a counter to stop at a specific value. You want to verify a buffer overflow cannot occur. Which of the following code entries will stop input at 50 characters?

- **a.** `if (I > 50) then exit (1)`
- **b.** `if (I < 50) then exit (1)`
- **c.** `if (I <= 50) then exit (1)`
- **d.** `if (I >= 50) then exit (1)`

Answers to Practice Exam 2

Answers at a Glance

1. B	**26.** D	**51.** C	**76.** B
2. B	**27.** D	**52.** C	**77.** B
3. C	**28.** A	**53.** B	**78.** A
4. B	**29.** A	**54.** D	**79.** C
5. A	**30.** D	**55.** C	**80.** D
6. C	**31.** D	**56.** C	**81.** B
7. C	**32.** A	**57.** B	**82.** A
8. B	**33.** D	**58.** D	**83.** B
9. D	**34.** B	**59.** A	**84.** C
10. A	**35.** C	**60.** C	**85.** A
11. A	**36.** C	**61.** B	**86.** A
12. C	**37.** A	**62.** C	**87.** A
13. A	**38.** A	**63.** B	**88.** C
14. C	**39.** B	**64.** C	**89.** A
15. D	**40.** B	**65.** A	**90.** D
16. C	**41.** B	**66.** D	**91.** B
17. D	**42.** B	**67.** C	**92.** A
18. C	**43.** B	**68.** D	**93.** A
19. C	**44.** C	**69.** B	**94.** A
20. C	**45.** A	**70.** D	**95.** A
21. D	**46.** C	**71.** A	**96.** C
22. D	**47.** A	**72.** B	**97.** D
23. D	**48.** B	**73.** B	**98.** C
24. C	**49.** A	**74.** A	**99.** C
25. B	**50.** B	**75.** B	**100.** D

Answers with Explanations

1. Answer: B.

   Explanation: Firewalk is a network security tool that attempts to determine what the rule set is on a firewall. It is a technique used to discover what rules are configured on the gateway. It works by sending out TCP and UDP packets with a TTL configured one greater than the targeted firewall. Answers A, C, and D are incorrect because Firewalk is not used to determine NIC settings, used for buffer overflows, or used for mapping wireless networks. For more information, see Chapter 10.

2. Answer: B.

   Explanation: With steganography, messages can be hidden in image files, sound files, or even the whitespace of a document before being sent. Answers A, C, and D are incorrect because they do not describe steganography. For more information, see Chapter 12.

3. Answer: C.

   Explanation: This rule detects if someone attempts to use SSH. Snort is a popular open source IDS service. The rule shown in the question is used to detect if SSH is being used. Locating the target port of 22 should have helped in this summation. Therefore, answers A, B, and D are incorrect because FTP is port 21, Telnet is port 22, and TFTP is port 69. For more information, see Chapter 10.

4. Answer: B.

   Explanation: Snort can be a powerful IDS. The rule shown in the question triggers on detection of a NetBus scan. NetBus defaults to port 12345. Answers A, C, and D are incorrect. SubSeven, BackOrifice, and Donald Dick do not use that port by default. For more information, see Chapter 6.

5. Answer: A.

   Explanation: An access control list implemented on a router is the best choice for a stateless firewall. Most organizations already have the routers in place to perform such services, so this type of protection can be added for little additional cost. Answers B, C, and D are incorrect because they represent more expensive options and offer more than stateless inspection. For more information, see Chapter 3.

6. Answer: C.

   Explanation: Worms are replicating programs that can run independently and travel from system to system. Answer A is incorrect because a Trojan usually gives someone else control of the system. Answer B is incorrect because

viruses do not run independently. Answer D is incorrect because a dropper is used with a virus.

7. Answer: C.

   Explanation: SYSKEY was added in Windows NT (SP3) to add a second-layer ID 128-bit encryption. Therefore, answers A, B, and D are incorrect. For more information, see Chapter 4.

8. Answer: B.

   Explanation: SQL injection is a subset of an unverified/unsanitized user input vulnerability. The idea is to convince the application to run SQL code that was not intended. Therefore, answers A, C, and D are incorrect because they do not describe SQL injection. For more information, see Chapter 8.

9. Answer: D.

   Explanation: Archive.org maintains the Wayback Machine that preserves copies of many websites from months or years ago. Answers A, B, and C are incorrect because none of these methods offer much hope in uncovering the needed information. For more information, see Chapter 8.

10. Answer: A.

    Explanation: Snow is used to conceal messages in ASCII text by appending whitespace to the end of lines. Spaces and tabs are not usually visible in document viewer programs; therefore, the message is effectively hidden from casual observers. Answer B is incorrect because Wget is used to copy web pages. Answer C is incorrect because Blindside is used to hide text in graphics files, and answer D is incorrect because a wrapper is used with Trojans to make their installation easy.

11. Answer: A.

    Explanation: Most versions of Linux, such as Red Hat, use MD5 by default. If you choose not to use MD5, you can choose DES, although it limits passwords to eight alphanumeric characters. Therefore, answer B is incorrect. Answers C and D are incorrect because Linux does not use AES or Diffie-Hellman for password encryption. For more information, see Chapter 5.

12. Answer: C.

    Explanation: Adore is a loadable kernel module (LKM) rootkit. A loadable kernel module runs in kernel space but can be loaded separately after the system is running. Answers A and B are incorrect because Flea and T0rm are not LKM rootkits. Answer D is incorrect because Chkroot is a rootkit detector. For more information, see Chapter 5.

13. Answer: A.

Explanation: Tripwire works with a database that maintains information about the byte count of files. If the byte count has changed, it will identify the finding and set a notification flag. Answers B, C, and D are incorrect because Tripwire does not harden applications, it does not scan source code, and it does not build a jail that limits the access of attackers. For more information, see Chapter 12.

14. Answer: C.

Explanation: The command for file and folder permissions is `chmod`, and the proper setting is `764`. Answer A is incorrect because a setting of `746` would give read, write, and execute rights to the owner, read to the group, and read and write to all others. Answers B and D are incorrect because chroot is not used for file permissions. For more information, see Chapter 5.

15. Answer: D.

Explanation: Chrooting is one of the hardening procedures that can be performed to a Linux system. It creates additional borders in case of zero-day threats so that hackers are jailed in specific folders. Answer A is incorrect because Tripwire is used to verify no changes have occurred to files and folders without your knowledge. Answer B, chmod, is incorrect because it is used to set file and folder permissions. Answer C is incorrect because loadable kernel modules are used by rootkits. For more information, see Chapter 5.

16. Answer: C.

Explanation: The first packet is the first step of the three-step startup. During the second step with the SYN ACK flags set, the acknowledgment value is set to 0BAA5002. Answers A, B, and D are incorrect because the second step will always have a value of the initial sequence number (ISN)+1. For more information, see Chapter 3.

17. Answer: D.

Explanation: A Ping of Death can occur in some older systems when data is broken down into fragments and could add up to more than the allowed 65,536 bytes. Answers A, B, and C are incorrect because a Smurf attack uses ICMP, SYN attacks target TCP, and Land is characterized by identical source and target ports. For more information, see Chapter 7.

18. Answer: C.

Explanation: A DoS attack targets availability. Answers A, B, and D are incorrect because DoS attacks do not target authentication, integrity, or confidentiality. For more information, see Chapter 7.

19. Answer: C.

Explanation: For hijacking to be successful, several things must be accomplished: 1) Identify and find an active session; 2) Predict the sequence number; 3) Take one of the parties offline; and 4) Take control of the session. Answers A and B are incorrect because MAC flooding or ARP poisoning would have already been started before the attack if the attacker were on a switched network. Answer D is incorrect because session control is the final step according to EC-Council documentation. For more information, see Chapter 7.

20. Answer: C.

Explanation: DNS spoofing can be thwarted by using DNS Security Extensions (DNSSEC). DNSSEC act as an antispoofer because it digitally signs all DNS replies to ensure their validity. Answers A, B, and D are incorrect because disabling zone transfers or blocking TCP 53, which is the port and protocol used for zone transfers, cannot stop spoofing. Disabling DNS timeouts would also not help because it would only cause the spoofing to persist. For more information, see Chapter 7.

21. Answer: D.

Explanation: Tunneling software acts as a socks server, allowing you to use your Internet applications safely despite restrictive firewalls. Answer A is incorrect because systems infected with spyware would not behave in this manner. Spyware-infected systems usually run slower and tend to go to URLs not requested or suffer from a barrage of pop-up ads. Answer B is incorrect because seeing that Dale watches his firewall closely, it is unlikely that they successfully attacked his firewall. Answer C is incorrect because backdoor programs are used to bypass authentication. For more information, see Chapter 6.

22. Answer: D.

Explanation: An ICMP ping request is a type 8. Answer A is incorrect because a type 0 is a ping reply. Answer B is incorrect because a type 3 is a destination unreachable, and answer C is incorrect because a type 5 is a redirect. For more information, see Chapter 2.

23. Answer: D.

Explanation: Fpipe is used for port redirection: a technique that is useful behind a firewall. This command redirects traffic from UDP port 69 to port 53. The syntax is -l listen, -r redirect -u UDP, and the IP address is the IP address to bind to this command. Answers A, B, and C, are incorrect because they do not properly define the syntax of the command. For more information, see Chapter 6.

24. Answer: C.

Explanation: The command `nc -u -v -w 1 10.2.2.2 135-139` performs a UDP port scan, in verbose mode, and waits 1 second between scanning ports 135 to 139 on IP address 10.2.2.2. Answers A, B, and D are incorrect because they do not properly define the syntax that is given. For more information, see Chapter 6.

25. Answer: B.

Explanation: Gil should primarily be concerned that he has proper policy and procedures in place that address keystroke logging. He must also make sure that employees understand that they have no expected level of privacy when using company computers and might be monitored. Answers A and C are incorrect because most of these programs are hard to detect. Answer D is incorrect because these programs can allocate a buffer big enough to store millions of keystrokes, so storage should not be a problem. For more information, see Chapter 6.

26. Answer: D.

Explanation: Beast uses port 6666 and is considered unique because it uses injection technology. Answer A is incorrect because SubSeven uses port 6711. Answer B is incorrect because NetBus uses port 12345, and Answer C is incorrect because Amitis uses port 27551. For more information, see Chapter 6.

27. Answer: D.

Explanation: Wrappers are used to package covert programs with overt programs. They act as a type of file joiner program or installation packager program. Answer A is incorrect because wrappers do not tunnel programs. An example of a tunneling program is Loki. Answer B is incorrect because wrappers are not used to cause a Trojan to execute when previewed in email; the user must be tricked into running the program. Answer C is incorrect because wrappers are not used as backdoors. A backdoor program allows unauthorized users to access and control a computer or a network without normal authentication. For more information, see Chapter 6.

28. Answer: A.

Explanation: Loki is a Trojan that opens and can be used as a backdoor to a victim's computer by using ICMP. Answer B is incorrect because Loki does not use UDP port 69 by default. Answer C is incorrect because Loki does not use TCP port 80 by default. Answer D is incorrect because Loki does not use IGRP. For more information, see Chapter 6.

29. Answer: A.

Explanation: `Netstat -an` would be the proper syntax. `-a` displays all connections and listening ports. `-n` displays addresses and port numbers in numeric

form. Answer B is incorrect because `-r` displays the routing table. Answer C is incorrect because `-p` shows connections for a specific protocol, yet none was specified in the answer. Answer D is incorrect because `-s` displays per-protocol statistics. By default, statistics are shown for TCP, UDP, and IP. For more information, see Chapter 6.

30. Answer: D.

Explanation: NetBus uses port 12345 by default. Answers A, B, and C are incorrect because Donald Dick uses 23476, BOK uses port 31337, and SubSeven uses port 6711. For more information, see Chapter 6.

31. Answer: D.

Explanation: The transport layer is the correct answer. TCP can be the target for SYN attacks, which are a form of DoS. Answer A is incorrect because the network layer is not associated with TCP. Answer B is incorrect because the data link layer is responsible for frames. Answer C is incorrect because the physical layer is the physical media on which the bits or bytes are transported. For more information, see Chapter 6.

32. Answer: A.

Explanation: ARP spoofing is used to redirect traffic on a switched network. Answer B is incorrect because setting this MAC address to be the same as the coworker would not be effective. Answer C is incorrect because DNS spoofing would not help in this situation because DNS resolves FQDNs to unknown IP addresses. Answer D is incorrect because ARP poisoning requires a hacker to set his MAC address to be the same as the default gateway, not his IP address. For more information, see Chapter 7.

33. Answer: D.

Explanation: The Start of Authority record gives information about the zone, such as the administrator contact. Answer A is incorrect because CNAME is an alias. Answer B is incorrect because MX records are associated with mail server addresses, and answer C is incorrect because an A record contains IP addresses and names of specific hosts. For more information, see Chapter 7.

34. Answer: B.

Explanation: Source routing was designed to allow individuals the ability to specify the route that a packet should take through a network or to allow users to bypass network problems or congestion. Answer A is incorrect because routing is the normal process of moving packets from node to node. Answer C is incorrect because RIP is a routing protocol. Answer D is incorrect because traceroute is the operation of sending trace packets to determine node information and to trace the route of UDP packets for the local host to a remote

host. Normally, traceroute displays the time and location of the route taken to reach its destination computer. For more information, see Chapter 7.

35. Answer: C.

Explanation: The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private networks: Class A network IP address range = 10.0.0.0–10.255.255.255, Class B network IP address range = 172.31.0.0–172.31.255.255, and Class C network IP address range = 192.168.255.0–192.168.255.255. Check out RFC 1918 to learn more about private addressing. Answers A, B, and D are incorrect because they do not fall within the ranges shown here. For more information, see Chapter 7.

36. Answer: C.

Explanation: UDP scanning is harder to perform because of the lack of response from open services and because packets could be lost due to congestion or a firewall blocking ports. Answer A is incorrect because a stealth scan is a TCP-based scan and is much more responsive than UDP scans. Answer B is incorrect because an ACK scan is again performed against TCP targets to determine firewall settings. Answer D is incorrect because FIN scans also target TCP and seek to elicit a RST from a Windows-based system. For more information, see Chapter 3.

37. Answer: A.

Explanation: A full connect or SYN scan of a host will respond with a SYN/ACK if the port is open. Answer B is incorrect because an ACK is not the normal response to the first step of a three-step startup. Answer C is incorrect because an RST is used to terminate an abnormal session. Answer D is incorrect because an RST/ACK is not a normal response to a SYN packet. For more information, see Chapter 3.

38. Answer: A.

Explanation: An ICMP type 3 code 13 is administrative filtered. This type response is returned from a router when the protocol has been filtered by an ACL. Answer B is incorrect because the ACK scan only provides a filtered or unfiltered response; it never connects to an application to confirm an open state. Answer C is incorrect because port knock requires you to connect to a certain number of ports in a specific order. Answer D is incorrect because, again, an ACK scan is not designed to report a closed port; its purpose it to determine the router or firewall's rule set. Although this might appear limiting, the ACK scan can characterize the capability of a packet to traverse firewalls or packet filtered links. For more information, see Chapter 3.

39. Answer: B.

Explanation: Regional registries maintain records from the areas from which they govern. ARIN is responsible for domains served within North and South America, and therefore is the logical starting point for that .com domain. Answer A is incorrect because AfriNIC is the RIR proposed for Africa. Answer C is incorrect because APNIC is the RIR for Asia and Pacific Rim countries. Answer D is incorrect because RIPE is the RIR for European-based domains. For more information, see Chapter 3.

40. Answer: B.

Explanation: TCP port 53 is used for zone transfers; therefore, if TCP 53 is open on the firewall, there is an opportunity to attempt a zone transfer. Answer A is incorrect because UDP 53 is typically used for DNS lookups. Answer C is incorrect because UDP 161 is used for SNMP. Answer D is incorrect because TCP 22 is used for SSH. For more information, see Chapter 3.

41. Answer: B.

Explanation: Password Authentication Protocol (PAP) allows the client to authenticate itself by sending a username and password to the server in clear text. The technique is vulnerable to sniffers who might try obtaining the password by sniffing the network connection. Answer A is incorrect because message digest is secured by using hashing algorithms such as MD5 in combination with a random nonce. Answer C is incorrect because certificate authentication uses PKI. Answer D is incorrect because forms authentication can use a cookie to store the encrypted password. For more information, see Chapter 4.

42. Answer: B.

Explanation: Converting 2605306123 base10 to octet reveals 203.2.4.5. For example, to convert the number 155.73.209.11 to base 10, first convert to binary 10011011010010011101000100001011, and then divide into 4 bytes:

10011011 = 155

01001001 = 73

11010001 = 209

00001011 = 11

Then, convert each back to decimal, 155.73.209.11. Therefore, answers A, C, and D are incorrect. For more information, see Chapter 8.

43. Answer: B.

Explanation: Cross-site scripting (XSS) lets you assume a user's identity at a dynamically generated web page or site by exploiting the stateless architecture of the Internet. It works by performing cookie theft. The attacker tricks

the victim into passing him the cookie through XSS. After the attacker gains the cookie, he sends the cookie to the web server and spoofs the identity of the victim. To get the cookie using a script attack, the attacker needs to craft a special form, which posts back the value of document cookie to his site. Answer A is incorrect because the question does not define a buffer overflow attack. Answer C is incorrect because the question does not define a SQL attack, and Answer D is not a possibility. File-traversal attacks occur when the attacker can move from one directory to another with valid permissions. For more information, see Chapter 8.

44. Answer: C.

Explanation: The Nimda worm modifies all web content files it finds and bases its attack on the same vulnerability that is seen in the Unicode vulnerability. Answers A, B, and D are incorrect because the log entry does not indicate the Morris worm, Blaster, or a double-decode attack. Identifying admin.dll is one way to identify this as a Nimda attack. For more information, see Chapter 8.

45. Answer: A.

Explanation: ObiWan is used for password cracking. Answers B, C, and D are incorrect because SQLSmack is a Linux SQL hacking tool, Wikto is a web assessment tool, and N-Stealth is a web vulnerability tool. Knowing which tools are used in each step of the web hacking methodology is an important goal of the CEH exam. You should spend a portion of your time preparing for the test practicing with the tools and learning to understand their output. For more information, see Chapter 8.

46. Answer: C.

Explanation: WEP is the original version of wireless protection. It was based on RC4 and used a 24-bit IV. Answers A, B, and D are incorrect because they do not specify the correct length. For more information, see Chapter 9.

47. Answer: A.

Explanation: Three popular standards are in use for WLANs, along with a new standard, 802.11n, which is due for release. Of these four types, only 802.11a operates at the 5.725 to 5.825GHz range. Answers B and C are incorrect because 802.11b and 802.11g operate at the 2.4000 to 2.2835GHz range. Answer D is incorrect because 802.1x deals with authentication. For more information, see Chapter 9.

48. Answer: B.

Explanation: The 24-bit IV field is too small because of this, and key reusage WEP is vulnerable. Answer A is incorrect because RC4 is not flawed. Answer C is incorrect because although 40 bits is not overly strong, that is not the primary weakness in WEP. Answer D is incorrect because tools such as

WEPCrack must capture 5 hours of traffic or more to recover the WEP key. For more information, see Chapter 9.

49. Answer: A.

Explanation: WEP uses a shared key, which is a type of symmetric encryption. Answer B is incorrect because WEP does not use asymmetric encryption. Answer C is incorrect because public key encryption is the same as asymmetric encryption. Answer D is incorrect because SHA-1 is a hashing algorithm. For more information, see Chapter 9.

50. Answer: B.

Explanation: In 2004, the nature of WEP cracking changed when a hacker named KoreK released a new piece of attack code that sped up WEP key recovery by nearly two orders of magnitude. Instead of the need to collect 10 million packets to crack the WEP key, it now took less than 200,000 packets. Aircrack is one of the tools that have implemented this code. Answer A is incorrect because Kismet is a wireless sniffer. Answer C is incorrect because WEPCrack does not use the fast WEP cracking method. Answer D is incorrect because AirSnare is a wireless IDS. For more information, see Chapter 9.

51. Answer: C.

Explanation: Running a Null TCP with Hping should tell you whether packet filter is in use. Answer A is incorrect because running an Nmap stealth scan will not help. Answer B is incorrect because an OS scan most likely will not provide any details to help you determine the packet filtering status of the device. Answer D is incorrect because banner grabbing is not a valid option without knowing open ports. For more information, see Chapter 3.

52. Answer: C.

Explanation: An ICMP type 3 code 13 is an unreachable message that is generated because the communication is administratively prohibited. Answers A, B, and D are incorrect because they do not describe an ICMP 3-13. For more information, see Chapter 2.

53. Answer: B.

Explanation: ACKCMD is a covert channel tool that can be used to send and receive information and potentially bypass a firewall and IDS. Answer A is incorrect because it is not a Windows exploit. Answer C is incorrect because it is not a honeypot. Answer D is incorrect because it is not used to exploit routers. For more information, see Chapter 6.

54. Answer: D.

Explanation: This is an alert rule designed to notify you of the use of Telnet in one direction. The rule means that any IP address on any port that attempts to

connect to any IP address on port 23 will create an alert message. The arrow points one direction, so the alert will not apply to both directions. Answers A and B are incorrect because this is not a logging rule. Answer C is incorrect because the rule applies to only one direction. For more information, see Chapter 10.

55. Answer: C.

Explanation: Snort can best be described as an IDS, packet logger, and sniffer. Answer A is incorrect because Snort is not a proxy. Answer B is incorrect because Snort is not only an IDS and sniffer, but also a packet logger. Answer D is incorrect because Snort is not a firewall. For more information, see Chapter 10.

56. Answer: C.

Explanation: A sheepdip system is used for checking media, file, disks, or CD-ROMs for viruses and malicious code before they are used in a secure network or computer. Answers A, B, and D are incorrect because a sheep dip system is not specifically for an integrity checker, honeypot, or to detect buffer overflows. For more information, see Chapter 11.

57. Answer: B.

Explanation: Melissa is a good example of a macro infector. Answer A is incorrect because Melissa is not an MBR infector. Answer C is incorrect because Melissa is not a file infector. Answer D is incorrect because a true worm requires no interaction from the end user, and Melissa requires no interaction from a user. Melissa needed to trick the victim into opening an attachment to execute its payload. For more information, see Chapter 11.

58. Answer: D.

Explanation: A multipartite virus can use more than one propagation method. Answer A is incorrect because an appender is a virus that adds its code to the end of a file. Answer B is incorrect because a polymorphic virus is one that has the capability to mutate. Answer C is incorrect because a prepender is a virus that adds its code to the beginning of a file. For more information, see Chapter 11.

59. Answer: A.

Explanation: The infection routine is the portion of the virus responsible for copying the virus and attaching it to a suitable host. Answers B, C, and D are incorrect because the search routine is responsible for locating new files, disk space, or RAM to infect. The antidetection routine is designed to make the virus more stealth like and avoid detection. The trigger routine's purpose is to launch the payload at a given date and time. For more information, see Chapter 11.

60. Answer: C.

Explanation: NOP, which stands for no operation, is a 1-byte-long instruction and is represented in assembly language by the hex value 0X90? Answer A is incorrect because Add is 03 hex. Answer B is incorrect because Mov is 8B, and answer D is incorrect because Sub is 2B. For more information, see Chapter 10.

61. Answer: B.

Explanation: A mantrap is a set of two doors. The idea behind a mantrap is that one or more people must enter the mantrap and shut the outer door before the inner door will open. Some mantraps lock both the inner and outer door if authentication fails so that the individual cannot leave until a guard arrives to verify the person's identity. Answer A is incorrect because a turnstile controls the flow of human traffic and is similar to a one-way gate. Answer C is incorrect because piggybacking is the act of riding in on someone's coattails. Answer D is incorrect because biometric authentication would not prevent more than on person at a time from entering. For more information, see Chapter 13.

62. Answer: C.

Explanation: Electrical fires are classified as class C fires. Answers A, B, and D are incorrect because class A fires have elements of common combustibles such as wood and paper. Class B fires are composed of flammable liquids, and class D fires are caused by flammable metals. For more information, see Chapter 13.

63. Answer: B.

Explanation: Your company has implemented mandatory access control. Mandatory access control features a static model and is based on a predetermined list of access privileges. This means that with a MAC model, access is determined by the system rather than the user. Answer A is incorrect because discretionary access control places control with the end user or resource owner. Answer C is incorrect because role-based access control is considered a nondiscretionary access control because such a system allows users to access systems based on the role they play in an organization. Answer D is incorrect because rule-based access control is based on a predetermined set of rules. For more information, see Chapter 13.

64. Answer: C.

Explanation: Cognitive passwords function by asking a series of questions about facts or predefined responses that only the user should know. Answer A is incorrect because biometric authentication uses a physical attribute. Answer

B is incorrect because a complex password uses uppercase or lowercase letters, numbers, and special characters. Answer D is incorrect because a security token would be something you have (a SecurID, for example). For more information, see Chapter 13.

65. Answer: A.

Explanation: A false acceptance rate measures the percentage of individuals gaining entry who should not be authorized. Answer B is incorrect because false positive is a term associated with intrusion detection to indicate something that triggered the system, yet was not an attack. Answer C is incorrect because the false rejection rate, also known as the insult rate, is the number of legitimate users denied access. Answer D is incorrect because the crossover error rate is used to measure the accuracy of the biometric system. For more information, see Chapter 13.

66. Answer: D.

Explanation: Sequence and acknowledgment numbers follow a predictable pattern. You will need to add the previous sequence number 1452 to the current packet length to get a total of 4444 to determine what values should be acknowledged next. Answers A, B, and C do not show the correct sequence number. For more information, see Chapter 7.

67. Answer: C.

Explanation: You are attempting to gather information for a session hijacking attack. For a session-hijacking attack to be successful you must successfully capture the ISN. Remember that sequence numbers move up in a predictable pattern and by capturing this value you will have the information you need to attempt session hijacking. Answers A, B, and D are incorrect because ISNs are not used with XSS, XSRF, and sniffing. For more information, see Chapter 7.

68. Answer: D.

Explanation: Tripwire is an integrity verification tool and can be used to verify the integrity of files, folders, or entire hard drives. Tripwire can be used to detect unauthorized changes to files or other data alterations. Answers A, B, and C are incorrect because Tripwire is not an antivirus, IDS, or session-hijacking tool. For more information, see Chapter 7.

69. Answer: B.

Explanation: The example is an attempt of some type of SQL injection attack. SQL injection attacks occur because of poor input sanitization. They should be some input validation that says: "Hey, I don't expect this here. Maybe I should delete everything after the semicolon." Answer A, C, and D are incorrect because this question does not describe a XSS, XSRF, or LDAP injection

attack. LDAP injection attacks target LDAP statements that construct LDAP statements. For more information, see Chapter 8.

70. Answer: D.

Explanation: The question describes a basic example of XSS. An XSS attempt is to insert malicious script into an input field and see if the site will actually execute it. Answers A, B, and C are incorrect as SQL injection attack would inject basic SQL commands and attempt to execute them. XSRF exploits an existing connection to a legitimate site while also connected to an attacker. A file-traversal attack seeks to move from one location to another. For more information, see Chapter 8.

71. Answer: A.

Explanation: This question describes a directory-traversal attack. This technique was prevalent when IIS made the move from ASCII to Unicode. This technique sends HTTP requests asking the web server to back out of the folder it is in and up to the root directory thereby giving access to other folders. Answers B, C, and D are incorrect as SQL injection attack would inject basic SQL commands and attempt to execute them. XSRF exploits an existing connection to a legitimate site while also connected to an attacker. XSS is about dynamic content and the executing of malicious scripts. For more information, see Chapter 8.

72. Answer: B.

Explanation: The results of that input indicates that a successful SQL injection attack may be launched. A SQL injection attack consists of inserting either a partial or complete SQL statement query via a data input field. Answers A, C, and D are incorrect as XSS is about dynamic content and the executing of malicious scripts, XSRF exploits an existing connection to a legitimate site while also connected to an attacker, and a file traversal attack seeks to move from one location to another. For more information, see Chapter 8.

73. Answer: B.

Explanation: A buffer overflow is the result of stuffing more data into a buffer than it can handle. Some functions that do not perform good bounds testing and can result in a buffer flow include the following: `strcat()`, `sprintf()`, `vsprint()`, `bcopy()`, `gets()`, and `scanf()`. Answers A, C, and D are incorrect because the code example is not exploit code, parameter tampering is carried out in the browser bar or URL, and cookie exploitation would require modification of the cookie. For more information, see Chapter 11.

74. Answer: A.

Explanation: Running Netcat as shown in the question would setup a Netcat listener on port 80 and would allow it to be used as a low interaction honey-

pot. Low-interaction honeypots somewhat appear as a legitimate service but would not reply with banners or other details. Answers B, C, and D are incorrect because that is not the correct syntax for a port scan, banner grab, or a file transfer. For more information, see Chapter 10.

75. Answer: B.

Explanation: AAAA records map to a FQDN to an IPv6 address. It is the equivalent to the A record. Answers A, C, and D are incorrect as an MX record is tied to mail servers. The SOA record is used to associate how the zone propagates to secondary name servers. Finally, PTR records are used for the configuration for reverse DNS. For more information, see Chapter 4.

76. Answer: B.

Explanation: WinPcap acts as an application interface for the use of sniffer tools such as Wireshark. Answers A, C, and D are incorrect. LibPcap has the same function but is used for Linux computers. Ettercap is a session-hijakacking and sniffing tool. Etherape allows users to monitor network traffic in a graphical manner. For more information, see Chapter 7.

77. Answer: B.

Explanation: The proper syntax is `tcpdump -w test.pcap -i eth0 dst 192.168.201.166 and port 22`. Answers A, C, and D are incorrect. Answer A, `tcpdump -i eth0 port 22`, captures a specific port only. Answer C, `tcpdump -i eth0 not arp and not rarp`, captures ARP traffic. Answer D, `tcpdump -i eth0 arp`, captures traffic only. For more information, see Chapter 7.

78. Answer: A.

Explanation: Answer A configures the logs for binary mode. Binary mode should always be used on high-speed networks when large amounts of data must be collected. Answer B is the correct syntax for logging but does not use binary mode. Answer C simply shows the switch for verbose. Answer D is an incorrect syntax. For more information, see Chapter 7.

79. Answer: C.

Explanation: ARP poisoning is being attempted and can been seen by the pattern of replies listed with duplicate addresses. All other answers are incorrect as Etherflood is used for flooding and sends random MAC addresses. If a ping sweep were being performed, we would see ICMP (ping) data. Firesheep is a session-hijacking tools that targets session (cookie) information from sites like Facebook and LinkedIn. For more information, see Chapter 7.

80. Answer: D.

Explanation: The capture indicates a buffer overflow attack, specifically against DNS. The buffer overflow is making use of a NOP. Answer A, B, and C are incorrect. The capture is not a UDP connection to DNS. The capture is not a DNS reply because the traffic is the wrong direction. The capture is not a DNS query because the NOP indicates a buffer overflow. For more information, see Chapter 11.

81. Answer: B.

Explanation: The output shown is for `netstat -an`. For the exam, you will be expected to know the output of Netstat and it various switches. Answers A, C, and D are incorrect because the output is not `TCPdump`, `Windump`, or `Netstat -r`.

82. Answer: A.

Explanation: Firewalking uses a traceroute-like IP packer analysis using ICMP packets to determine what type of traffic can pass through the firewall. Answers B, C, and D are incorrect because it does not alter IP packets, OSPF, RIP, or UDP. For more information, see Chapter 6.

83. Answer: B.

Explanation: Snort only supports TCP, UDP, and ICMP. Knowledge of Snort and the protocols it supports is required knowledge for the exam. For more information, see Chapter 7.

84. Answer: C.

Explanation: The answer does not apply to port 6000 because it has the negation symbol in front of it. What is true about this rule is that it applies to any source port, and the rule shown applies to any source IP address. For more information, see Chapter 7.

85. Answer: A.

Explanation: Ports 1745 and 1080 are used by Microsoft's proxy server; therefore, all other answers are incorrect. For more information, see Chapter 10.

86. Answer: A.

Explanation: An insertion attack sends packets to an end system (victim) that will be rejected but that the IDS will think are valid, thus giving different streams to the IDS and target hosts. Answers B, C, and D do not match this description and so are incorrect. For more information, see Chapter 10.

87. Answer: A.

Explanation: Answer A is correct as KFSensor is an example of a Windows-based honeypot. It acts as a honeypot to attract and detect hackers and worms

by simulating vulnerable system services and Trojans. By acting as a decoy server, it can divert attacks from critical systems and provide a higher level of information than can be achieved by using firewalls and NIDS alone. For more information, see Chapter 10.

88. Answer: C.

Explanation: Bluetooth is a short-range wireless technology standard for exchanging data in the 2400 to 2480MHz range. For more information, see Chapter 9.

89. Answer: A.

Explanation: The 802.11n standard operates in 2.4GHz band, with a maximum raw data rate of 54Mbps. Answers B, C, and D do not operate on those frequencies. For more information, see Chapter 9.

90. Answer: D.

Explanation: AirPcap is an adapter that captures all or a filtered set of WLAN frames and delivers the data to the Wireshark platform. It does not work with NetStumbler, Aircrack, or John the Ripper. For more information, see Chapter 9.

91. Answer: B.

Explanation: WEP IVs are 24 bits long. They suffer from the fact that they are too small and repeat over time. For more information, see Chapter 9.

92. Answer: A.

Explanation: An example of starting an NTFS stream would look like this: `"Start c:\legit.txt: hack.exe"`. The other examples would not start an NTFS stream. For more information, see Chapter 4.

93. Answer: A.

Explanation: Sending an unsolicited text message is known as Bluejacking. Bluesnarfing is unauthorized access of information. Bluesniffing is war driving for Bluetooth. Bluesmacking is a DoS attack. For more information, see Chapter 9.

94. Answer: A.

Explanation: The CEH exam may have one or more questions on warchalking symbols. The example shown is of an open network. For more information, see Chapter 9.

95. Answer: A.

Explanation: The 802.16 family of standards is known as WiMAX and is designed for MANs. Answers B, C, and D are all used for short range communication. For more information, see Chapter 9.

96. Answer: C.

Explanation: An evasion attack sends packets that the IDS rejects but that the target host accepts, again giving different streams to the IDS and target. All other answers are incorrect because they do not describe an evasion attack. For more information, see Chapter 10.

97. Answer: D.

Explanation: Loki is an ICMP tunneling tool. It is not used for honeypot detection, firewall, or OS identification. For more information, see Chapter 6.

98. Answer: C.

Explanation: Hping is an example of a honeypot detection tool. This versatile tool can be used to detect honeypots by sending ICMP packets containing shellcode and analyzing their response. For more information, see Chapter 10.

99. Answer: C.

Explanation: If you have fond ports 256, 257, 258, and 259 open, there is a high probability that you are scanning Check Point's FireWall-1. For more information, see Chapter 10.

100. Answer: D.

Explanation: Some functions in C do a better job of bounds testing than others. Answers A, B, and C are incorrect because none of the options will stop at an input of 50 characters. For more information, see Chapter 11.

Index

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y-Z

Answers to the "Do I Know This Already?" Quizzes and Review Questions

Chapter 1

"Do I Know This Already?" Quiz

1. A
2. A
3. C
4. A
5. D
6. B
7. A
8. C
9. D
10. B

Review Questions

1. B. Section 1029 is one of the main federal statutes that address computer hacking under U.S. federal law. All other answers are incorrect. Sections 2510 and 2701 are part of the Electronic Communication Privacy Act and address information as storage and information in transit. Section 1028 is incorrect because it deals with fraud and related activity in connection with identification documents.
2. B. Confidentiality addresses the secrecy and privacy of information. Physical examples of confidentiality include locked doors, armed guards, and fences. Logical examples of confidentiality can be seen in passwords, encryption, and firewalls. Answer A is incorrect because integrity deals with the correctness of the information. Answer C is incorrect because availability deals with the issue that services and resources should be available when legitimate users need them. Answer D is incorrect because authentication is the means of proving someone is who he says he is. Authentication is usually verified by passwords, PINs, tokens, or biometrics.

3. B. A threat is any agent, condition, or circumstance that could potentially cause harm, loss, damage to or could compromise an IT asset or data asset. All other answers are incorrect because risk is the probability or likelihood of the occurrence or realization of a threat. A vulnerability is a weakness in the system design, implementation, software, code, or other mechanism. An exploit refers to a piece of software, tool, or technique that takes advantage of a vulnerability, leading to privilege escalation, loss of integrity, or denial of service on a computer system.
4. A. Gray hat hackers are individuals who vacillate between ethical and unethical behavior. Answer B is incorrect because ethical hackers do not violate ethics or laws. Answer C is incorrect because crackers are criminal hackers, and answer D is incorrect because white hat hackers is another term for ethical hackers.
5. B. Obtain written permission to hack. Ethical hackers must always obtain legal, written permission before beginning any security tests. Answers A, C, and D are incorrect because ethical hackers should not hack web servers. They should gather information about the target, but this is not the most important step; obtaining permission is not enough to approve the test and should come in written form.
6. D. Ethical hackers use the same methods but strive to do no harm. Answers A, B, and C are incorrect because malicious hackers might use the same tools and techniques that ethical hackers do. Malicious hackers might be less advanced, as even script kiddies can launch attacks; ethical hackers try not to bring down servers, and they do not steal credit card databases.
7. C. A stolen equipment test is performed to determine what type of information might be found. The equipment could be the CEO's laptop or the organization's backup media. Answer A is incorrect because insider attacks seek to determine what malicious insiders could accomplish. Answer B is incorrect because physical entry attacks seek to test the physical controls of an organization such as doors, locks, alarms, and guards. Answer D is incorrect because outsider attacks are focused on what outsiders can access and, given that access, what level of damage or control they can command.
8. A. Integrity provides for the correctness of information. Integrity allows users of information to have confidence in its correctness. Integrity can apply to paper documents as well as electronic ones. Answer B is incorrect because an attack that exposes sensitive information could be categorized as an attack on confidentiality. Answer C is incorrect because availability deals with the issue that services and resources should be available when legitimate users need them. Answer D is incorrect because authentication is the means of proving someone is who he says he is. Authentication is usually verified by passwords, PINs, tokens, or biometrics.

9. D. Hactivists seek to promote social change; they believe that defacing websites and hacking servers is acceptable as long as it promotes their goals. Regardless of their motives, hacking remains illegal, and they are subject to the same computer crime laws as any other criminal. Answer A is incorrect because ethical hackers work within the boundaries of laws and ethics. Answer B is incorrect because gray hat hackers are those individuals who cross the line between legal and questionable behavior. Answer C is incorrect because black hat hackers are criminal hackers and might be motivated to perform illegal activities for many different reasons.
10. C. The attack was considered DoS, which targets availability. Although it does not provide the attacker access, it does block legitimate users from accessing resources. Answer A is incorrect because integrity provides for the correctness of information. Answer B is incorrect because the confidentiality of information and data was not exposed. Answer D is incorrect because authentication is the means to prove a person's identity. Authentication is usually verified by passwords, PINs, tokens, or biometrics.
11. A. A penetration test can be described as an assessment in which the security tester takes on an adversarial role and looks to see what an outsider can access and control. Answer B is incorrect because a high-level evaluation examines policies and procedures. Answer C is incorrect because a network evaluation consists of policy review, some scanning, and execution of vulnerability-assessment tools. Answer D is incorrect because a policy assessment is another name for a high-level evaluation.
12. B. There are three components to a security evaluation: preparation, conducting the evaluation, and the conclusion. The conclusion is the post-assessment period when reports are written and recommendations are made. Because the evaluation process is composed of three components, answers A, C, and D are incorrect.

Chapter 2

"Do I Know This Already?" Quiz

1. C
2. D
3. A
4. C
5. D
6. B
7. D

8. A
9. A
10. C

Review Questions

1. C. Each zone is a collection of structured resource records. Answer A is incorrect because it is not a collection of domains; zones are a collection of resource records that can include an SOA record, A record, CNAME record, NS record, PTR record, and the MX record. Answer B is incorrect because it does not describe a zone namespace; that is the purpose of the SOA record. Answer D is incorrect because a collection of aliases is a CNAME.
2. B. Reconnaissance includes the act of reviewing an organization's website to gather as much information as possible. Answer A is incorrect because scanning and enumeration is not a passive activity. Answer C is incorrect because fingerprinting is performed to identify a systems OS. Answer D is incorrect because gaining access is the equivalent of breaking and entering.
3. D. Dumpster diving is the act of going through someone's trash. All other answers are incorrect because they do not describe dumpster diving. Reconnaissance is information gathering, intelligence gathering is another name for reconnaissance, and social engineering is the art of manipulating people.
4. B. The format for an Ethernet II frame is target MAC address, source MAC address, and Type field. The second 6 bytes equal FF FF FF FF FF FF, which indicates that they are from a broadcast address. Answer A is incorrect because the information shown does not indicate an ARP packet. ARP packets can be identified by the hex value 08 06 in the Type field. Answer C is incorrect because the destination is not set to a broadcast address. Answer D is incorrect because the packet is not from a multicast address.
5. C. TFTP was used by the Nimda worm to move the infected file to the victim's web server, admin.dll. Answer A is incorrect because Nimda does not use Telnet. Answer B is incorrect because Nimda did not use FTP. Answer D is incorrect because Nimda targeted IIS, not Apache.
6. D. SNMP is UDP based and uses two separate ports: 161 and 162. It is vulnerable because it can send the community strings in clear text. Answer A is incorrect because port 69 is TFTP. Answer B is incorrect because SNMP is not TCP based. Answer C is incorrect because TCP 69 is not used for SNMP.
7. B. A Teardrop attack is considered a type of overlapping fragment attack. It targets the IP header. Answer B is incorrect because Smurf alters an ICMP ping packet. Answer C is incorrect because the Ping of Death is also an ICMP

attack. Answer D is incorrect because a LAND attack is not an overlapping fragment attack; it alters the port numbers.

8. B. The second step of the three-step handshake sets the SYN ACK flags. Answer A is incorrect because the SYN flag is set on the first step. Answer C is incorrect because the ACK flag occurs to acknowledge data. Answer D is incorrect because the ACK PSH flags are not set on the second step of the handshake.

9. D. RST is used to terminate a session that is abnormal or is nonresponsive. Answer A is incorrect because the default flag sequence to terminate is not RST FIN. Answer B is incorrect because FIN PSH is not used to terminate an abnormal session. Answer C is incorrect because FIN is used to shut down a normal session.

10. A. Deny all means that by default all ports and services are turned off; then only when a service or application is needed to accomplish a legitimate function of the organization is the service turned on. Answer B is incorrect because the principle of least privilege means that you give employees only the minimum services needed to perform a task. Answer C is incorrect because an access control list is used for stateless inspection and can be used to block or allow approved services. Answer D is incorrect because defense in depth is the design of one security mechanism layered on top of another.

11. D. The last fragmented packet will have the more bit set to 0 to indicate that no further packets will follow. Answer A is incorrect as it must be the last packet in the series if the more bit is set to 0. Answer B is incorrect as the more bit indicates that it must be the last packet. Answer C is incorrect as it cannot be the first packet with the more bit set to 0.

12. C. ICMP type 11 is the correct code for time exceeded. All other answers are incorrect because type 3 is for destination unreachable, type 5 is for redirects, and type 13 is for time stamp requests. RFC 792 is a good resource for information on ICMP.

13. B. ARP poisoning occurs at the data link layer. Answer A is incorrect because the network layer is associated with IP addresses. Answer C is incorrect because the session layer is in charge of session management. Answer D is incorrect because the transport layer is associated with TCP and UDP.

14. B. DNS cache poisoning is a technique that tricks your DNS server into believing it has received authentic information when in reality, it has been deceived. Answer A is incorrect because a DoS attack's primary goal is to disrupt service. Answer C is incorrect because DNS pharming is used to redirect users to an incorrect DNS server. Answer D is incorrect because an illegal zone transfer is an attempt to steal the zone records, not to poison them.

15. D. The transport layer is the correct answer. TCP can be the target for SYN attacks, which are a form of DoS. Answer A is incorrect because the network layer is not associated with TCP. Answer B is incorrect because the data link layer is responsible for frames. Answer C is incorrect because the physical layer is the physical media on which the bits or bytes are transported.
16. A. ARP spoofing is used to redirect traffic on a switched network. Answer B is incorrect because setting this MAC address to be the same as the co-worker would not be effective. Answer C is incorrect because DNS spoofing would not help in this situation because DNS resolves FQDNs to unknown IP addresses. Answer D is incorrect because ARP poisoning requires a hacker to set his MAC address to be the same as the default gateway, not his IP address.
17. D. The Start of Authority record gives information about the zone, such as the administrator contact. Answer A is incorrect because CNAME is an alias. Answer B is incorrect because MX records are associated with mail server addresses, and answer C is incorrect because an A record contains IP addresses and names of specific hosts.
18. B. Source routing was designed to enable individuals to specify the route that a packet should take through a network or to allow users to bypass network problems or congestion. Answer A is incorrect because routing is the normal process of moving packets from node to node. Answer C is incorrect because RIP is a routing protocol. Answer D is incorrect because traceroute is the operation of sending trace packets to determine node information and to trace the route of UDP packets for the local host to a remote host. Normally, traceroute displays the time and location of the route taken to reach its destination computer.
19. C. The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private networks: Class A network IP address range = 10.0.0.0–10.255.255.255, Class B network IP address range = 172.31.0.0–172.31.255.255, and Class C network IP address range = 192.168.255.0–192.168.255.255. Check out RFC 1918 to learn more about private addressing. Answers A, B, and D are incorrect because they do not fall within the ranges shown here.
20. B. The presentation layer is responsible for encryption. Answer A is incorrect because the application layer is responsible for program support. Programs are usually accessed by port number. Answer C is incorrect because the session layer handles such functions as the TCP startup and TCP shutdown. Answer D is incorrect because the transport layer is the home of TCP and UDP, which are connection and connectionless protocols.

Chapter 3

"Do I Know This Already?" Quiz

1. C
2. C
3. C
4. B
5. A
6. B
7. D
8. B
9. C
10. A

Review Questions

1. D. Running `nmap -O` would execute OS guessing. Answer A is incorrect because `nmap -P0` means do not ping before scanning. Answer B is incorrect because `nmap -sO` would perform an IP scan. Answer C is incorrect because `nmap -sS` would execute a TCP stealth scan. Keep in mind that scanning IPv4 networks is much easier than IPv6 because of the much greater number of IP addresses.
2. C. Passive information gathering should be the first step performed in the penetration test. The EC-Council defines seven steps in the pre-attack phase: include passive information gathering, determining the network range, identifying active machines, finding open ports and access points, OS fingerprinting, fingerprinting services, and mapping the network. Answer A is incorrect because social engineering is not the first step in the process. Answer B is incorrect because Nmap port scanning would not occur until after passive information gathering. Answer D is incorrect because OS fingerprinting is one of the final steps, not the first.
3. B. Ping is the most common ICMP type. A ping request is a type 8, and a ping reply is a type 0. All other answers are incorrect because a request is always a type 8 and a reply is always a type 0. An ICMP type 5 is redirect, and a type 3 is destination unreachable. For a complete listing of ICMP types and codes, see RFC 792.
4. C. RFC 1191 specifies that when one IP host has a large amount of data to send to another host the data is transmitted as a series of IP datagrams. IP is

designed so that these datagrams be of the largest size that does not require fragmentation anywhere along the path from the source to the destination. The specified range is from 68 to 65535 bytes. Answer A is incorrect because 1500 bytes is the MTU for Ethernet. Answer B is incorrect because 576 bytes is the default MTU for IP. Answer D is incorrect because that value is the frame size for Ethernet.

5. A. Nmap requires one open and one closed port to perform OS identification. Answers B, C, and D are incorrect because none of these answers list one open and one closed port, which is the minimum required for OS identification.
6. D. The proper syntax for a UDP scan using Netcat is `netcat -u -v -w2 <host> 1-1024`. Netcat is considered the Swiss army knife of hacking tools because it is so versatile. Answers A, B, and C are incorrect because they do not correctly specify the syntax used for UDP scanning with Netcat.
7. B. A DMZ is a separate network used to divide the secure inner network from the unsecure outer network. Services such as HTTP, FTP, and email may be placed there. Answer A is incorrect because a proxy is simply a system that stands in place of and does not specifically define a DMZ. Answer C is incorrect because an IDS is used to detect intrusions or abnormal traffic. Answer D is incorrect because a bastion host is a computer that is fully on the public side of the demilitarized zone and is unprotected by a firewall or filtering router.
8. B. A null scan is a TCP-based scan in which all flags are turned off. Answer A is incorrect because it describes a XMAS scan. Answer C is incorrect because this could describe a TCP full connect of a stealth scan. Answer D is incorrect because it describes a TCP WIN scan.
9. B. Active fingerprinting works by examining the unique characteristics of each OS. One difference between competing platforms is the datagram length. On a Linux computer, this value is usually 84, whereas Microsoft computers default to 60. Therefore, answers A, C, and D are incorrect because they are all Windows operating systems.
10. B. P0f is a passive OS fingerprinting tool. Answers A, C, and D are incorrect because Queso was the first active fingerprinting tool, Nmap is probably the most well known, and Xprobe 2 is the next generation of OS fingerprinting tools. These active tools have the capability to look at peculiarities in the way that each vendor implements the RFCs. These differences are compared with its database of known OS fingerprints. Then a best guess of the OS is provided to the user.
11. C. UDP scanning is harder to perform because of the lack of response from open services and because packets could be lost due to congestion or a firewall blocking ports. Answer A is incorrect because a stealth scan is a TCP-based scan and is much more responsive than UDP scans. Answer B is incorrect

because an ACK scan is again performed against TCP targets to determine firewall settings. Answer D is incorrect because FIN scans also target TCP and seek to elicit an RST from a Windows-based system.

12. A. A full connect or SYN scan of a host will respond with a SYN/ACK if the port is open. Answer B is incorrect because an ACK is not the normal response to the first step of a three-step startup. Answer C is incorrect because an RST is used to terminate an abnormal session. Answer D is incorrect because an RST/ACK is not a normal response to a SYN packet.
13. A. An ICMP type 3 code 13 is administrative filtered. This type response is returned from a router when the protocol has been filtered by an ACL. Answer B is incorrect because the ACK scan only provides a filtered or unfiltered response; it never connects to an application to confirm an open state. Answer C is incorrect because port knock requires you to connect to a certain number of ports in a specific order. Answer D is incorrect because again, an ACK scan is not designed to report a closed port; its purpose it to determine the router or firewall's rule set. Although this might appear limiting, the ACK scan can characterize the capability of a packet to traverse firewalls or packet-filtered links.
14. B. Regional Internet registries (RIR) maintain records from the areas from which they govern. ARIN is responsible for domains served within North and South America, and therefore is the logical starting point for that .com domain. Answer A is incorrect because AfriNIC is the RIR proposed for Africa. Answer C is incorrect because APNIC is the RIR for Asia and Pacific Rim countries. Answer D is incorrect because RIPE is the RIR for European-based domains.
15. B. TCP port 53 is used for zone transfers; therefore, if TCP 53 is open on the firewall, there is an opportunity to attempt a zone transfer. Answer A is incorrect because UDP 53 is usually used for DNS lookups. Answer C is incorrect because UDP 161 is used for SNMP. Answer D is incorrect because TCP 22 is used for SSH.

Chapter 4

"Do I Know This Already?" Quiz

1. B
2. D
3. D
4. B
5. A

6. B
7. C
8. D
9. A
10. C

Review Questions

1. B. When looking at an extracted LM hash, you will sometimes observe that the rightmost portion is always the same. This is padding that has been added to a password fewer than eight characters long. The usual ending is 1404EE. Answer A is incorrect because even though a hash cannot be reversed, it is possible to recognize the padding in the hash. Answer C is incorrect because the hash will not always start with AB923D. Answer D is incorrect because the leftmost portion of the hash might not always be the same.
2. A. L0phtcrack is a well-known password-cracking program. Answer B is incorrect because even though Netcat is considered the Swiss army knife of hacking tools, it is not used for password cracking. Answer C is incorrect because John the Ripper is the password-hacking tool. Answer D is incorrect because NetBus is a Trojan program.
3. D. One important goal of enumeration is to determine the true administrator. In the question, the true administrator is Joe. Answer A is incorrect because the Joe account has a RID of 500. Answer B is incorrect because the commands issued do not show that the account is disabled, which is not the purpose of the tool. Answer C is incorrect because the commands do not show that the guest account has been disabled.
4. C. The administrator account has a RID of 500. Therefore, answers A, B, and D are incorrect. RIDs of 0 and 100 are not used, although 1000 is the first user account.
5. D. If a rootkit is discovered, you will need to rebuild the OS and related files from known good media. This usually means performing a complete reinstall. Answers A, B, and C are incorrect because copying system files will do nothing to replace infected files; performing a trap and trace might identify how the attacker entered the system, but will not fix the damage done; and deleting the files will not ensure that all compromised files have been cleaned. You will also want to run some common rootkit detection tools such as chkrootkit and rkhunter.
6. B. SYSKEY is the second layer of encryption used to further obfuscate Windows passwords. It features 128-bit encryption. Answer A is incorrect because

a salt is used by Linux for password encryption. Answer C is incorrect because SYS32 is an executable used by the Flux.e Trojan. Answer D is incorrect because SAM stores password and account information.

7. C. Most SNMP devices are configured with public and private as the default community strings. These are sent in clear text. Answer A is incorrect because it is not enabled on all devices by default. Answer B is incorrect because it is not based on TCP; it is UDP based. Answer D is incorrect because anyone can sniff it while in cleartext. The community strings are required to connect.
8. B. There are several ways to prevent the use of LM authentication in your Windows 2003 environment. The easiest is to use the NoLMHash Policy by Using Group Policy. Although you could edit the Registry, if this is done incorrectly it can cause serious problems that might require you to reinstall your operating system. Answer A is incorrect because the LMShut tool does not accomplish the required task. Answer C is incorrect because Lsass generates the process responsible for authenticating users for the Winlogon service. Answer D is incorrect because passwords would need to be at least 15 characters long, not 10.
9. B. ELSave is used to clear the log files. Other tools used to remove evidence and clear logs include MRU-Blaster and CCleaner. Answers A, C, and D are incorrect because Auditpol is used to disable auditing, PWdump is used to extract the hash, and Cain and Abel is used for a host of activities, such as password cracking, although clearing the logs is not one of them.
10. C. John the Ripper cannot differentiate between uppercase and lowercase passwords. Answer A is incorrect because it can crack NTLM passwords. Answer B is incorrect because separating the NTLM passwords into two halves actually speeds cracking. Answer D is incorrect because John the Ripper can perform brute-force cracks.
11. B. Alternate data streams are another type of named data stream that can be present within each file. The command streams Netcat behind readme.txt on an NTFS drive. Answers A, C, and D are incorrect because the command does not start a Netcat listener, it does not open a command shell, and it is not used to unstream Netcat.
12. A. Rainbow tables use the faster time-memory trade-off technique and work by precomputing all possible passwords in advance. Answers B, C, and D are all incorrect because they are the traditional methods used to crack passwords.
13. C. The SMB protocol is used for file sharing in Windows 2000. In 2000 and newer systems, Microsoft added the capability to run SMB directly over TCP port 445. Answer A is incorrect because a scan probably will not DoS the server. Answer B is incorrect because it is not the most correct answer. Answer D is incorrect because Windows NT systems do not run port 445 by default.

14. C. After Windows NT, SYSKEY was no longer optional, it's enabled by default at installation time. After being activated, the hashes are encrypted yet another time before being stored in SAM. SYSKEY offers 128-bit encryption. Answer A is incorrect because SYSKEY does not offer 40-bit encryption. Answer B is incorrect because SYSKEY does not offer 64-bit encryption. Answer D is incorrect because SYSKEY does not offer 256-bit encryption.
15. A. The proper syntax is net use `\\ IP_address\ ipc$ "" /u:""`. Therefore, answers B, C, and D are incorrect.

Chapter 5

"Do I Know This Already?" Quiz

1. B
2. D
3. B
4. A
5. D
6. D
7. C
8. A
9. D
10. C

Review Questions

1. D. The `ps` command gives a snapshot of the currently running processes, including ps itself. Answer A is incorrect because `netstat` is a command-line tool that displays a list of the active connections a computer currently has. Answer B is incorrect because `ls` only provides a directory listing. Answer C is incorrect because `echo` displays entered characters on the screen.
2. C. SARA is a system-level scanner that can scan various ports and attempt to verify what is running on each and what vulnerabilities are present. Answer A is incorrect because Flawfinder is a source code scanner. Answers B and D are incorrect because both N-Stealth and Whisker are web application scanners and do not perform system-level scans.

3. B. Lynx is a basic browser that can be used to pull down the needed code. Answer A is incorrect because TFTP is not used for web browsing. Answer C is incorrect because Explorer is a Windows-based web browser. Answer D is incorrect because Firefox is a GUI tool.
4. B. The password has been shadowed. You can determine this because there is an *x* in the second field. Answer A is incorrect because the password has been shadowed. Answer C is incorrect because the password is not being stored in the passwd file. You might or might not be able to see it, depending on whether you are logged in as root. Answer D is incorrect because the SAM is only used in Windows. There is no SAM file in Linux.
5. C. The command for file and folder permissions is `chmod`, and the proper setting would be `740`. Answer A is incorrect because a setting of `777` would give read, write, and execute rights to the owner, group, and all others. Answers B and D are incorrect because `chroot` is not used for file permissions.
6. D. Absolute mode will require the use of octal values, such as `chmod 320`. Answers A, B, and C are incorrect. The `chroot` command is not used to set file permissions; `chmod a+rwx` is a valid command but is in symbolic form.
7. C. The three valid groups in Red Hat Linux are super users, system users, and normal users. Therefore, answers A, B, and D are incorrect. Guest is a default group found in the Windows environment.
8. D. The /etc/host file stores IP addresses and is used for hostname-to-IP address resolution. Answers A, B, and C are incorrect because subnet masks, default gateways, and `allow` or `deny` statements are not found there.
9. C. The structure of the passwd file is such: Account Name:Password:UID:GID:User Information:Directory:Program. In this case, the 100 falls under the GID. Answers A, B, and D are therefore incorrect because they do not specify the correct field.
10. B. The shadow file is used to prevent hackers and ordinary users from viewing encrypted passwords. Answer A is incorrect because the host file is used for name resolution. Answer C is incorrect because the passwd file is not restricted to root. Answer D is incorrect because inetd is a configuration file and not related to passwords.

Chapter 6

"Do I Know This Already?" Quiz

1. D
2. B
3. C

4. B
5. C
6. A
7. C
8. B
9. B
10. B

Review Questions

1. B. BOK uses port 31337 by default. All other answers are incorrect because Donald Dick uses port 23476, SubSeven uses port 6711, and NetBus uses port 12345.
2. D. FPipe is a source port forwarder/redirector. It can create a TCP or UDP stream with a source port of your choice. Answer A is incorrect because Loki is a covert channel program. Answer B is incorrect because Recub is a Trojan. Answer C is incorrect because Girlfriend is also a Trojan.
3. C. Covert communications can be described as sending and receiving unauthorized information or data between machines without alerting any firewalls and IDSes on a network. Answer A is incorrect because it describes a Trojan. Answer B is incorrect because it describes a backdoor. Answer D is incorrect because it more accurately describes a virus or worm.
4. B. Netcat is a network utility for reading from and writing to network connections on either TCP or UDP. Because of its versatility, Netcat is also called the TCP/IP Swiss army knife. Modified versions of Netcat can be found on some systems. One example is socat. Answers A, C, and D are incorrect because Netcat is not a more powerful version of Snort and can be used on both Windows and Linux.
5. B. Watching.dll is one of the files that is loaded when SubSeven is installed. Answers A, C, and D are incorrect because none of the other Trojans install that file. NetBus installs KeyHook.dll, Poison Ivy installs pmss.exe, and Loki is a Linux-based program that does not run on Windows.
6. B. Jane should use a third-party tool that is in a known good state. One way to ensure this is to download the file only from the developer's website and to verify that the fingerprint, hash or MD5Sum of the tool has remained unchanged. Answer A is incorrect because patch.exe is known malware. Loading this on her computer will only compound her problems. Answer C is incorrect because if the computer does have a Trojan, it might be hard to determine when the point of infection occurred. Therefore, the recent backup might also

be infected or corrupt. Answer D is incorrect because although the Trojan might have installed something in the Startup folder, there are many other places that the hacker could hide elements of the tool, including the Registry, system folders, and INI files.

7. D. FakeGina captures login usernames and passwords that are entered at system startup. Answers A, B, and C are incorrect because FakeGina does not send out passwords by email, is not a hardware keystroke capture program (it is software based), and only captures username and login information at startup.
8. B. ACKCMD uses TCP ACK packets to bypass ACLs that block incoming SYN packets. Answer A is incorrect because Loki uses ICMP. Answer C is incorrect because Stealth Tools is used to alter the signature of a known Trojan or virus. Answer D is incorrect because Firekiller 2000 is used to disable Norton antivirus or software firewall products.
9. D. `Nc -n -v -l -p 25` opens a listener on TCP port 25 on the local computer. Answers A, B, and C are incorrect because it does not allow the hacker to use a victim's mail server to send spam, it does not forward email, and it will not block traffic on port 25. (Actually, it listens on the port for incoming connections.)
10. D. Datapipe is a Linux redirector. It can be used for port redirections. This form of tool is useful when certain ports are blocked at the firewall. Answer A is incorrect because it is not a virus. Answer B is incorrect because it is not a remote-control Trojan. Answer C is incorrect because, as it does not report open processed.

Chapter 7

"Do I Know This Already?" Quiz

1. B
2. C
3. C
4. A
5. D
6. B
7. B
8. C
9. C
10. C

Review Questions

1. B. The ARP process is a two-step process that consists of an ARP request and an ARP reply. Answers A, C, and D are incorrect because the ARP process is not one, three, or four steps.
2. D. Passive sniffing is all that is required to listen to traffic on a hub. Answer A is incorrect because active sniffing is performed on switches. Answers B and C are incorrect because ARP poisoning and MAC flooding are both forms of active sniffing, and these activities are not required when using a switched network.
3. C. A Smurf attack uses ICMP to send traffic to the broadcast address and spoof the source address to the system under attack. Answer A is incorrect because a SYN attack would not be indicated by traffic to a broadcast address. Answer B is incorrect because a Land attack is to and from the same address. Answer D is incorrect because a Chargen attack loops between Chargen and Echo.
4. A. Here is what the command-line option flags do: `-T` tells Ettercap to use the text interface; `-q` tells Ettercap to be quieter; `-F` tells Ettercap to use a filter (in this case, `cd.ef`); `-M` tells Ettercap the MITM (man-in-the-middle) method of ARP poisoning. Answers B, C, and D are incorrect because this command is not logging sniffed passwords, it is not checking to see if someone else is performing ARP poisoning, and it is not used to place the NIC into promiscuous mode.
5. C. MAC flooding is the act of attempting to overload the switches content-addressable memory (CAM) table. By sending a large stream of packets with random addresses, the CAM table of the switch will evenly fill up and the switch can hold no more entries; some switches might divert to a "fail open" state. This means that all frames start flooding out all ports of the switch. Answer A is incorrect because active sniffing is not the specific type requested in the question. Answer B is incorrect because ARP poisoning is characterized by spoofing address in the ARP request or response. Answer D is incorrect because passive sniffing is usually performed only on hubs.
6. A. Trinity uses TCP port 6667. Trinoo and Shaft do not use port 6667, and DDoSPing is a scanning tool; therefore, answers B, C, and D are incorrect.
7. D. DDoSPing is a Windows GUI scanner for the DDoS agents Wintrinoo, Trinoo, Stacheldraht, and TFN. Answers A, B, and C are incorrect because MStream, Trinoo, and Shaft are all DDoS programs.
8. B. Stacheldraht is a DDoS program. All other answers are incorrect because they are DoS programs (Smurf, Land, and Fraggle).

9. A. A SYN flood disrupts TCP by sending a large number of fake packets with the SYN flag set. This large number of half open TCP connections fills the buffer on victim's system and prevents it from accepting legitimate connections. Answer B is incorrect because this describes a Land attack. Answer C is incorrect because a large number of SYN ACK packets would not be present. Answer D is incorrect because ACK packets would not be the signature of this attack.
10. C. The optimum time to perform a session hijack is after authentication. Answers A, B, and D are incorrect because if performed at the point of the three-step handshake, the attacker would not have an authenticated session—anytime before authentication would not do the hacker much good. If performed right before shutdown, any misstep would mean that the user would log out and the attacker might have missed his chance to steal user's credentials.

Chapter 8

"Do I Know This Already?" Quiz

1. C
2. A
3. B
4. D
5. C
6. D
7. D
8. B
9. A
10. D

Review Questions

1. D. The purpose of the entry was an attempt to install Netcat as a listener on port 8080 to shovel a command shell back to the attacker. Answers A, B, and C are incorrect. The attack is not attempting to replace cmd.exe, it is not exploiting double decode, and it is not attempting to execute the Linux `xterm` command.
2. D. Although HTTP uses TCP as a transport, it is considered a stateless connection because the TCP session does not stay open waiting for multiple

requests and their responses. Answer A is incorrect because HTTP is not based on UDP; it is TCP based. Answer B is incorrect because HTTP is considered stateless. Answer C is incorrect because HTTP is not based on ICMP.

3. C. A brute-force attack attempts every single possibility until you exhaust all possible combinations of words and characters or discover the password. Answer A is incorrect because it describes a dictionary attack. Answer B is incorrect because using a rainbow table created from a dictionary is not an example of a brute-force attack. Answer D is incorrect because threatening someone with bodily harm is not a brute-force attack.
4. D. This command returns the banner of the website specified by IP address. Answers A, B, and C are incorrect because this command does not open a backdoor Telnet session on the client, it does not start a Netcat listener, and it does not return a banner from a URL because an IP address is specified in the command.
5. A. 0xde.0xaa.0xce.0x1a hexadecimal converted to base10 gives 222.170.206.26. Answers B, C, and D are therefore incorrect.
6. A. It uses the username, the password, and a nonce value to create an encrypted value that is passed to the server. Answer B is incorrect because Password Authentication Protocol (PAP) sends information in clear text. Answer C is incorrect because certificate authentication uses the PKI infrastructure. Answer D is incorrect because forms-based authentication is based on the use of a cookie.
7. B. When attackers discover the hidden price field, they might attempt to alter it and reduce the price. To avoid this problem, hidden price fields should not be used. However, if they are used, the value should be confirmed before processing. Answer A is incorrect because the value in the name field will not affect the fact that someone might attempt to lower the price of the item. Answer C is incorrect because, again, the PID has no effect on this price-altering possibility. Answer D is incorrect because the hidden field should not be expanded. If attackers can change the hidden field to a larger value and submit a long string, there is a possibility that they can crash the server.
8. A. File traversal will not work from one logical drive to another; therefore, the attack would be unsuccessful. Answer B would not prevent an attacker from exploiting the Unicode vulnerability. Answer C is incorrect because no TFTP server is required on the IIS system for the attack to be successful. Answer D is a possibility, and renaming the file would slow down the attacker; however, there is still the chance that he might guess what it has been renamed. Security by obscurity should never be seen as a real defense.
9. D. SQL injection is a type of exploit whereby hackers are able to execute SQL statements via an Internet browser. You can test for it using logic such as 1=1

or inserting a single '. Answer A is incorrect because this is not an Oracle database. Answer B is incorrect because it is not a MySQL database. Answer C is incorrect because 80004005 indicates a potential for SQL injection.

10. B. Changing the hidden tag value from a local copy of the web page would allow an attacker to alter the prices without tampering with the SQL database and without any alerts being raised on the IDS. Therefore, answers A, C, and D are incorrect.

Chapter 9

"Do I Know This Already?" Quiz

1. C
2. B
3. B
4. D
5. C
6. B
7. D
8. C
9. A
10. B

Review Questions

1. B and D. Toby should provide employee awareness activities to make sure that employees know about the new policy and perform periodic site surveys to test for rogue access points. Answer A is incorrect because disabling SNMP would have no effect because SNMP is used for network management. Answer C is incorrect because using a magnetron to build an 802.11 wireless jamming device could jam more than just wireless network devices, be a danger to those around it, and have an uncontrolled range.
2. B. Airsnarf is a rogue access point program that can be used to steal usernames and passwords from public wireless hotspots. Answers A, C, and D are incorrect because he is not attempting a DoS attack, Airsnarf will not detect rogue access points, and it is not used to perform site surveys.
3. D. Frequency-hopping spread spectrum hops between subchannels and sends out short bursts of data on each subchannel for a short period of time. Answer A is incorrect because direct-sequence spread spectrum uses a stream of

information that is divided into small pieces and transmitted—each of which is allocated across to a frequency channel across the spectrum. Answer B is incorrect because plesiochronous digital hierarchy is a technology used in telecommunications networks to transport large quantities of data over digital transport equipment such as fiber-optic cable. Answer C is incorrect because time-division multiplexing is used in circuit switched networks such as the Public Switched Telephone Network.

4. C. Bluetooth operates at 2.45GHz. It is available in three classes: 1, 2, and 3. It divides the bandwidth into narrow channels to avoid interference with other devices that use the same frequency. Answers A, B, and D are incorrect because they do not specify the correct frequency.

5. A. MAC addresses can be spoofed; therefore, used by itself, it is not an adequate defense. Answer B is incorrect because MAC addresses can be spoofed. Answer C is incorrect because IP addresses, like MAC addresses, can be spoofed. Answer D is incorrect because MAC filtering will not prevent unauthorized devices from using the wireless network. All a hacker must do is spoof a MAC address.

6. D. The SSID is still sent in packets exchanged between the client and WAP; therefore, it is vulnerable to sniffing. Tools such as Kismet can be used to discover the SSID. Answer A is incorrect because turning off the SSID will make it harder to find wireless access points, but ad hoc or infrastructure will not make a difference. Answer B is incorrect because the SSID has been changed, and therefore, the default will no longer work. Answer C is incorrect because running DHCP or assigning IP address will not affect the SSID issue.

7. A. Void11 is a wireless DoS tool. Answer B is incorrect because RedFang is used for Bluetooth. Answer C is incorrect because THC-Wardrive is used to map wireless networks, and answer D is incorrect because Kismet is used to sniff wireless traffic.

8. A. Strong password authentication protocols, such as Kerberos, coupled with the use of smart card and the secure remote password protocol are good choices to increase security on wired networks. The secure remote password protocol is the core technology behind the Stanford SRP Authentication Project. Answer B is incorrect because PAP, passwords, and Cat 5 cabling are not the best choices for wired security. PAP sends passwords in clear text. Answer C is incorrect because 802.1x and WPA are used on wireless networks. Answer D is also incorrect because WEP, MAC filtering, and no broadcast SSID are all solutions for wireless networks.

9. D. EAP-MD5 does not provide server authentication. Answers A, B, and C are incorrect because they do provide this capability. EAP-TLS does so by public key certificate or smart card. PEAP can use a variety of

types, including CHAP, MS-CHAP and public key. EAP-TTLS uses PAP, CHAP, and MS-CHAP.

10. C. WPA2 uses AES, a symmetric block cipher. Answer A is incorrect because WPA2 does not use RC4 although WEP does use it. Answer B is incorrect because WPA2 does not use RC5. Answer D is incorrect because MD5 is a hashing algorithm and is not used for encryption.

Chapter 10

"Do I Know This Already?" Quiz

1. D
2. C
3. B
4. B
5. A
6. B
7. D
8. A
9. A
10. C

Review Questions

1. A. Pattern matching is the act of matching packets against known signatures. Answer B is incorrect because anomaly detection looks for patterns of behavior that are out of the ordinary. Answer C is incorrect because protocol analysis analyzes the packets to determine if they are following established rules. Answer D is incorrect because stateful inspection is used firewalls.
2. C. Snort cannot analyze IGMP, a routing protocol. Answers A, B, and D are incorrect because Snort can analyze IP, TCP, UDP, and ICMP.
3. C. Session splicing works by delivering the payload over multiple packets, which defeats simple pattern matching without session reconstruction. Answer A is incorrect because evasion is a technique that might attempt to flood the IDS to evade it. Answer B is incorrect because IP fragmentation is a general term that describes how IP handles traffic when faced with smaller MTUs. Answer D is incorrect because session hijacking describes the process of taking over an established session.

4. D. `Snort -ix -dev -l\ snort\ log` is the correct entry to run Snort as an IDS on a Windows computer. The syntax in answers A B, and C are invalid, although it is the correct syntax to start up Snort on a Linux computer.
5. C. Filtering data on the source port of a packet isn't secure because a skilled hacker can easily change a source port on a packet, which could then pass through the filter. Therefore answers A, B, and D are incorrect.
6. D. In a NetBus scan, port 12345 is scanned as can be seen in the trace. Answers A, B, and C are incorrect because an ACK scan would show an ACK flag. A XMAS scan would show as Urgent, Push, and FIN flag.
7. B. WinPcap is a program that will allow the capture and sending of raw data from a network card. Answer A is incorrect because LibPcap is used by Linux, not Windows. Answer C is incorrect because IDSCenter is a GUI for Snort, not a packet driver. Answer D is incorrect because AdMutate is a tool for bypassing IDS.
8. B. A XMAS scans as the Urgent, Push, and FIN flags are set. Answer A is not correct because an ACK scan would show an ACK flag. Answer C is incorrect because 27444 would be displayed; answer D is incorrect because a NetBus scan port 12345 is scanned.
9. C. Cisco uses a proprietary Vigenere cipher to encrypt all passwords on the router except the enable secret password, which uses MD5. The Vigenere cipher is easy to break. Answers A, B, and D are incorrect because the password is not MD5, DES, or AES.
10. B. Proxy servers have the capability to maintain state. Answer A is incorrect because packet filters do not maintain state. Answers C and D are incorrect because honeypots and bastion servers do not maintain a state table or answer the question.

Chapter 11

"Do I Know This Already?" Quiz

1. A
2. C
3. A
4. B
5. B
6. D
7. A

8. C
9. D
10. D

Review Questions

1. B. Nimda had the capability to infect in many different ways, including malformed MIME header and IFrame exploit within email propagation, placing an infected riched20.dll in the document, prepending itself to target executable files, and by attempting to connect to open shares and copy itself to these locations. Answer A is incorrect because the Brain virus is an MBR virus. Answer C is incorrect because Sasser exploited a buffer overflow, and answer D is incorrect because Staog was a single infector Linux virus.
2. D. The `strncat` function accepts a length value as a parameter, which should be no larger than the size of the destination buffer. Answers A, B, and C are incorrect as `gets`, `memcpy`, and `strcpy` do not perform automatic bounds checking and should be avoided.
3. A. Virus programs have two required components: search routines and infection routines. The infection routine is the portion of the virus responsible for copying the virus and attaching it to a suitable host. Answers B, C, and D are incorrect because the payload routine, antidetection routine, and trigger routine are all considered optional.
4. B. Anna Kournikova was created in only a few hours using a tool called the VBS Worm Generator. Answers A, C, and D are incorrect because they were not created with the VBS Worm Generator. While malware generation tool kits are typically not illegal using them to create and release malware can result in criminal charges.
5. C. Tripwire provides integrity assurance. Tripwire looks for changes that may have occurred from hackers or malicious software. By monitoring attributes of files that typically do not change, such as binary signatures, size, changes in size, or integrity scans, Tripwire can be useful for detecting intrusions, attacks, and the corruption of data. Answer A is incorrect because Tripwire is not used to guard the stack against buffer overflow. Answer B is incorrect because heuristic scanning looks for actions that programs or applications would not typically perform. Answer D is incorrect because signature scanning is performed to look for known signatures of viruses and worms.
6. C. The stack is a last-in, first-out (LIFO) mechanism that computers use to pass arguments to functions as well as reference local variables. Answer A is incorrect because a first-in, first-out mechanism is useful for buffering a stream of data between a sender and receiver, which are not synchronized but is not

used in stack operations. Answers B and D are incorrect; push refers to the act of pushing elements onto the stack, and pop refers to removing elements off the stack.

7. C. Heap-based buffer overflows differ from stack-based buffer overflows in that stack-based buffer overflows are dependent on overflowing a fixed-length buffer. This makes answers A, B, and D incorrect. In heap-based buffer-overflow attacks, the attacker overflows a buffer that is placed in the lower part of the heap.
8. A. Answers B, C, and D are incorrect because the question asks which of the following is not a defense, and each of those items is a defense. Defenses against buffer overflows include manual auditing of code, disabling stack execution, safer C library support, and better compiler techniques. Answer A is the correct choice because enabling stack execution is something you would not want to do.
9. B. A macro virus is designed to be embedded in a document. After being embedded, the virus writer can have the macro execute each time the document is opened. Many applications, such as Microsoft Word and Excel, support powerful macro languages. Answer A is incorrect because an MBR infector targets the boot sector of a disk. Answer C is incorrect because a file infector typically targets files or applications and can append or prepend themselves to the infected item. Answer D is incorrect because a mass mailer is a type of virus or worm that sends itself to many or all the individuals listed in your address book.
10. A. The Sasser worm targets a security issue with the Local Security Authority Subsystem Service. Answer B is incorrect because Sobig does not exploit LSASS. Sobig activates from infected emails when a victim clicks the infected attachment. After this, the worm will install itself and start to spread further. Answer C is incorrect because Netsky spreads via email as a .pif or .zip attachment. Answer D is incorrect because Code Red exploits an idq.dll buffer overflow.

Chapter 12

"Do I Know This Already?" Quiz

1. D
2. C
3. B
4. C
5. B

6. A
7. D
8. C
9. A
10. C

Review Questions

1. C. With DES electronic codebook (ECB), the identical plain text encrypted with the same key will always produce the same cipher text. Answer A is incorrect because DES cipher block chaining is considered more secure because it chains the blocks together. Answer B is incorrect because MD5 is a hashing algorithm. Answer D is incorrect because Diffie-Hellman is an asymmetric algorithm.
2. B. Asymmetric encryption can provide users both confidentiality and authentication. Authentication is usually provided through digital certificates and digital signatures. Answer A is incorrect because steganography is used for file hiding and provides a means to hide information in the whitespace of a document, a sound file, or a graphic. Answer C is incorrect because it can provide integrity but not confidentiality. Answer D is incorrect because symmetric encryption only provides confidentiality.
3. D. Jake should compare the tools hash value to the one found on the vendor's website. Answer A is incorrect because having a copy of the vendor's digital certificate only proves the identity of the vendor; it does not verify the validity of the tool. Answer B is incorrect because having the digital certificate of his friend says nothing about the tool. Digital certificates are used to verify identity, not the validity of the file. Answer C is incorrect and the worst possible answer because loading the tool could produce any number of results, especially if the tool has been Trojaned.
4. B. When a standalone file is encrypted with EFS, a temp file is created named efs0.tmp. DiskProbe or a hex editor can be used to recover that file. All other answers are incorrect because DiskProbe is not used for spoofing a PKI certificate; it can only recover the last file encrypted, not an entire folder of encrypted files. DiskProbe is not used to crack an MD5 hash.
5. C. Because the question asks what the RA cannot do, the correct answer is that the RA cannot generate a certificate. All other answers are incorrect because they are functions the RA can provide, including reducing the load on the CA, verifying an owner's identity, and passing along the information to the CA for certificate generation.

6. B. The known plain-text attack requires the hacker to have both the plain text and cipher text of one or more messages. For example, if a WinZip file is encrypted and the hacker can find one of the files in its unencrypted state, the two form plain text and cipher text. Together, these two items can be used to extract the cryptographic key and recover the remaining encrypted zipped files. Answer A is incorrect because cipher-text attacks don't require the hacker to have the plain text; they require a hacker to obtain encrypted messages that have been encrypted using the same encryption algorithm. Answer C is incorrect because a chosen cipher-text attack occurs when a hacker can choose the cipher text to be decrypted and can then analyze the plain-text output of the event. Answer D is incorrect because an attack occurs when the attacker tries to repeat or delay a cryptographic transmission.
7. C. The secring.skr file contains the PGP secret key. PGP is regarded as secure because a strong passphrase is used and the secret key is protected. The easiest way to break into an unbreakable box is with the key. Therefore, anyone who wants to attack the system will attempt to retrieve the secring.skr file before attempting to crack PGP itself. Answer A is incorrect because the Windows passwords are kept in the SAM file. Answer B is incorrect because Linux passwords are generally kept in the passwd or shadow file. Answer D is incorrect because secring.skr is a real file and holds the user's PGP secret key.
8. D. Examples of symmetric algorithms include DES, 3DES, and Rijndael. All other answers are incorrect because ElGamal, ECC, and Diffie-Hellman are all asymmetric algorithms.
9. B. 3DES has a key length of 168 bits. Answer A is incorrect because 3DES does not have a key length of 192 bits. Answer C is incorrect because 3DES does not have a key length of 64 bits. Answer D is incorrect because 56 bits is the length of DES not 3DES.
10. D. A digital certificate binds a user's identity to a public key. Answers A, B, and C are incorrect because a digital signature is electronic and not a written signature, a hash value is used to verify integrity, and a private key is not shared and does not bind a user's identity to a public key.
11. A. An inference attack involves taking bits of nonsecret information, such as the flow of traffic, and making certain assumptions from noticeable changes. Answer B is incorrect because cipher-text attacks don't require the hacker to have the plain text; they require a hacker to obtain messages that have been encrypted using the same encryption algorithm. Answer C is incorrect because a chosen cipher-text attack occurs when a hacker can choose the cipher text to be decrypted and then analyze the plain-text output of the event. Answer D is incorrect because an attack occurs when the attacker tries to repeat or delay a cryptographic transmission.

12. C. DES processes 64 bits of plain text at a time. Answer A is incorrect because 192 bits is not correct. Answer B is incorrect, but it does specify the key length of 3DES. Answer D is incorrect because 56 bits is the key length of DES.
13. B. Collisions occur when two message digests produce the same hash value. This is a highly undesirable event and was proven with MD5 in 2005 when two X.509 certificates were created with the same MD5Sum in just a few hours. Answer A is incorrect because collisions address hashing algorithms, not asymmetric encryption. Answer C is incorrect because collisions address hashing algorithms, not symmetric encryption. Answer D is incorrect because the goal of steganography is to produce two images that look almost identical, yet text is hidden in one.
14. C. John is a password-cracking tool available for Linux and Windows. Answer A is incorrect because John is not used to crack PGP public keys. Also, because the key is public, there would be no reason to attempt a crack. Answer B is incorrect because John is not a PGP-cracking tool. Answer D is incorrect because John is not used to crack EFS files.
15. B. DES uses a 56-bit key, and the remaining 8 bits are used for parity. Answer A is incorrect as 32 bits is not the length of the DES key. Answer C is incorrect as 64 bits is not the length of the DES key, because 8 bits are used for parity. Answer D is incorrect as 128 bits is not the length of the DES key; it is 56 bits.

Chapter 13

"Do I Know This Already?" Quiz

1. A
2. B
3. A
4. C
5. A
6. B
7. C
8. A
9. D
10. B

Review Questions

1. A and B. Paper shredders are the number one defense that can be used to prevent dumpster divers from being successful. By keeping the trash in a secured location, you make it much harder for individuals to obtain information from the trash. Answer C is incorrect because strong passwords will not prevent dumpster diving. Answer D is incorrect because dumpster divers might not have even seen the CCTV camera and because CCTV is primarily a detective control. Replaying a tape later to find that someone has gone through the trash will not have prevented the attack.
2. A. A cipher lock is one in which a keypad is used for entering a PIN number or password. These are commonly used on secured doors to control access. Answer B is incorrect because a device lock is used to secure a piece of equipment such as a laptop. Answer C is incorrect because a warded lock is a basic low-end padlock that is easily picked. Answer D is incorrect because a tumbler lock is just an improved version of a warded lock. Instead of wards, they use tumblers that make it harder for the wrong key to open the wrong lock.
3. B. By stationing a guard by the door, you could monitor and make sure that piggybacking is not occurring. Answer A is incorrect because although installing a CCTV camera would allow you to see who piggybacked, it might not prevent it. Answer C is incorrect because a fingerprint reader would not prevent more than one person entering at a time. Answer D is incorrect because installing a cipher lock would be no different from the fingerprint reader and would not prevent piggybacking.
4. B. Shoulder surfing is to look over someone's shoulder to get information. Shoulder surfing is an effective way to get information in crowded places because it's relatively easy to stand next to someone and watch as that person enters a password or PIN number. Answer A is incorrect because dumpster diving is performed by digging through the trash. Answer C is incorrect because tailgating is similar to piggybacking; it's done at a parking facility or where there is a gate that controls the access of vehicles. Answer D is incorrect because social engineering is the art of manipulating people to gain insider information.
5. D. A retina scan examines the blood vessel patterns of the retina; it offers a unique method of identification. It's a form of biometric authentication used for high-security areas, such as military and bank facilities. Answer A is incorrect because a pupil scan does not specifically define how a retina scan works. Answer B is incorrect because blood vessels are not specific to the type of scan. Answer C is incorrect because a facial shape scan does not look specifically at the eye. Facial scans are routinely done in places such as casinos.

6. D. Sensitive is the second-to-lowest level of security in the commercial data classification system. The commercial system is categorized from lowest to highest level as public, sensitive, private, and confidential. Answers A, B, and C are incorrect because secret and top secret are both from the governmental classification system and because confidential is the highest rating in the commercial system.
7. D. Tumbler locks are more complex than a basic warded lock. Instead of wards, they use tumblers that make it harder for the wrong key to open the wrong lock. Answer A is incorrect because a cipher lock does not use a key. It requires that you input a PIN or code. Answer B is incorrect because a combination lock is also like a cipher lock and does not require a key. Answer C is incorrect because a warded lock is considered the cheapest and easiest lock to pick.
8. C. Guards can make a decision and judgment call in situations that require discernment. Answer A is incorrect because CCTV can only record events for later analysis. Answer B is incorrect because dogs are not capable of making a judgment call and might bite or injure the wrong person. Answer D is incorrect because a biometric system cannot make a judgment call; it will either allow or block access based on the results of analysis of the individual's biometric attribute.
9. C. The false rejection rate measures the number of legitimate users who should have gotten in but didn't. Answer A is incorrect because the false acceptance rate is the measurement of unauthorized individuals who are allowed access. Answer B is incorrect because a false positive measures the number of alarms issued by and IDS, indicating an attack that is not occurring. Answer D is incorrect because the crossover error rate indicates the overall effectiveness of a biometric device. The lower this number, the more accurate the device.
10. B. Reciprocation is the technique of giving someone a token or small gift to make them more willing to give something in return. Answers A, C, and D are incorrect: Scarcity works by attempting to make someone believe something is in short supply and so immediate action is required, social validation works on the angle of a need to do something to fit in with your peers, and authority is the act of acting as someone's boss or superior and demanding action.

Memory Tables

Chapter 2

Table 2-3 IPv4 Addressing

Address Class	Address Range Number of Networks	Number of Networks	Number of Hosts
A		126	16,777,214
B		16,384	65,534
C		2,097,152	254
D		N/A	N/A
E		N/A	N/A

Table 2-5 ICMP Types and Codes

Type	Code	Function
	0/8	Echo response/request (ping)
	0–15	Destination unreachable
	0	Source quench
	0–3	Redirect
	0–1	Time exceeded
	0	Parameter fault
	0	Time stamp request/response
	0	Subnet mask request/response

Table 2-6 Some Common Type 3 Codes

Code	Function
	Net unreachable
	Host unreachable
	Protocol unreachable
	Port unreachable
	Fragmentation needed and Don't Fragment was set
	Source route failed
	Destination network unknown
	Destination host unknown
	Source host isolated
	Communication with destination network administratively prohibited
	Communication with destination host administratively prohibited
	Destination network unreachable for type of service
	Destination host unreachable for type of service
	Communication administratively prohibited

Table 2-8 Layers and Responsibilities

Layer	Layer Responsibility	Protocols or Ports	Potential Attacks
Application			
Host-to-host			
Internet			
Network access			

Chapter 3

Table 3-5 Common Ports and Protocols

Port	Protocol	Service/Transport
20/21	FTP	TCP
	SSH	TCP
	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
69		UDP
80	HTTP	TCP
	POP3	TCP
135		TCP
161/162		UDP
	MSSQL	TCP

Table 3-7 The Seven Steps of the Pre-Attack Phase

Step	Title	Active/Passive	Common Tools
One			www.domaintools.com, ARIN, IANA, Whois, Nslookup
Two			RIPE, APNIC, ARIN
Three			Ping, traceroute, SupersScan, Angry IP Scanner
Four			Nmap, Hping, AngryIPScanner, SuperScan
Five			Nmap, WinFingerprint, P0f, Xprobe2
Six			Telnet, FTP, Netcat
Seven			CartoReso, traceroute, LANsurveyor

Table 3-9 Nmap Commands

Task	Command Syntax
TCP full connect scan	
TCP stealth scan	
UDP scan	
Switch to adjust scan time	
Idle scan switch	
Decoy switch	

Table 3-10 Passive Information Gathering

Domain Name	IP Address	Location	Contact Person	Address and Phone Number
Redriff.com				
Examcram.com				
	72.3.246.59			
Rutgers.edu				

Chapter 4

Table 4-7 `net use` Commands

Task	Command Syntax
	`net use \\`*`ip address`*`\ipc$ "" /u:""`
	`net use * \\`*`ip address\share`*` * /u:`*`username`*
	`net view \\ipaddress`

Chapter 6

Table 6-3 Common Netcat Switches

Netcat Switch	Purpose
	Used to detach Netcat from the console.
	Used to create a simple listening TCP port. Adding `-u` will place it into UDP mode.
	Used to redirect stdin/stdout from a program to Netcat.
	Used to set a timeout before Netcat automatically quits.
	Used to pipe output of program to Netcat.
	Used to pipe output of Netcat to program.
	Used to display help options.
	Used to put Netcat into verbose mode.
	Used to specify source routing flags. `-g` is gateway source routing, `-G` is numeric source routing.
	Used for Telnet negotiation `DON'T` and `WON'T`.
	Used to hex dump traffic to file.
	Used for port scanning.

Table 6-6 Netcat Commands

Task	Command Syntax
`Nc -d`	
`Nc -l -p [port]`	
`Nc -e [program]`	
`Nc -w [timeout]`	
`Nc -d`	

Memory Tables Answer Key

Chapter 2

Table 2-3 IPv4 Addressing

Address Class	Address Range Number of Networks	Number of Networks	Number of Hosts
A	1–127	126	16,777,214
B	128–191	16,384	65,534
C	192–223	2,097,152	254
D	224–239	N/A	N/A
E	240–255	N/A	N/A

Table 2-5 ICMP Types and Codes

Type	Code	Function
0/8	0/8	Echo response/request (ping)
3	0–15	Destination unreachable
4	0	Source quench
5	0–3	Redirect
11	0–1	Time exceeded
12	0	Parameter fault
13/14	0	Time stamp request/response
17/18	0	Subnet mask request/response

Table 2-6 Some Common Type 3 Codes

Code	Function
0	Net unreachable
1	Host unreachable
2	Protocol unreachable
3	Port unreachable
4	Fragmentation needed and Don't Fragment was set
5	Source route failed
6	Destination network unknown
7	Destination host unknown
8	Source host isolated
9	Communication with destination network administratively prohibited
10	Communication with destination host administratively prohibited
11	Destination network unreachable for type of service
12	Destination host unreachable for type of service
13	Communication administratively prohibited

Table 2-8 Layers and Responsibilities

Layer	Layer Responsibility	Protocols or Ports	Potential Attacks
Application	Communication with FTP	SNMP, Telnet, DNS, SSH, SMTP	Password capture
Host-to-host	Connection and connectionless communication	TCP and UDP	Session hijacking, connectionless, scanning communication
Internet	Deliver of data, error detection, and routing	IP and ICMP	Routing attacks, man-in-the-middle attacks
Network access	Physical layer delivery	PPP	Sniffing, MAC address spoofing

Chapter 3

Table 3-5 Common Ports and Protocols

Port	Protocol	Service/Transport
20/21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP
135	RPC	TCP
161/162	SNMP	UDP
1433/1434	MSSQL	TCP

Table 3-7 The Seven Steps of the Pre-Attack Phase

Step	Title	Active/Passive	Common Tools
One	Information gathering	Passive	www.domaintools.com, ARIN, IANA, Whois, Nslookup
Two	Determining network range	Passive	RIPE, APNIC, ARIN
Three	Identify active machines	Active	Ping, traceroute, SupersScan, Angry IP Scanner
Four	Finding open ports and applications	Active	Nmap, Hping, AngryIPScanner, SuperScan
Five	OS fingerprinting	Active/passive	Nmap, WinFingerprint, P0f, Xprobe2
Six	Fingerprinting services	Active	Telnet, FTP, Netcat
Seven	Mapping the network	Active	CartoReso, traceroute, LANsurveyor

Table 3-9 Nmap Commands

Task	Command Syntax
TCP full connect scan	`-sT`
TCP stealth scan	`-sS`
UDP scan	`-sU`
Switch to adjust scan time	`-T`
Idle scan switch	`-sI`
Decoy switch	`-d`

Table 3-10 Passive Information Gathering

Domain Name	IP Address	Location	Contact Person	Address and Phone Number
Redriff.com	64.235.246.143	Los Angeles, CA	Admin	213-683-9910 5482 Wilshire Blvd
Examcram.com	63.240.93.157	Old Tappan, NJ	Administrator	201-784-6187 123 Old Tappan Rd
Theregister.com	72.3.246.59	Southport	Philip	+44-798-089-8072 19 Saxon Road
Rutgers.edu	128.6.72.102	Piscataway, NJ	Net Manager	732-445-2293 110 Frelinghuysen Road

Chapter 4

Table 4-7 `net use` Commands

Task	Command Syntax
Null session	`net use \\`*`ip address`*`\ipc$ "" /u:""`
Map a drive	`net use * \\`*`ip address\share`*`* /u:`*`username`*
View open shares	*`net view \\ipaddress`*

Chapter 6

Table 6-3 Common Netcat Switches

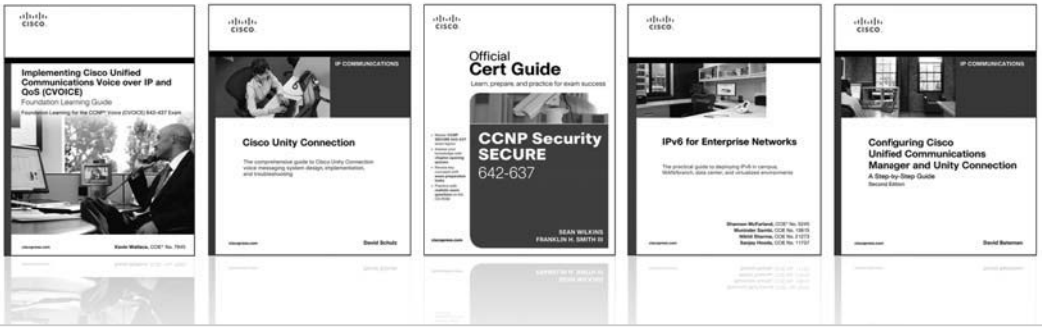
Netcat Switch	Purpose
`Nc -d`	Used to detach Netcat from the console.
`Nc -l -p [port]`	Used to create a simple listening TCP port. Adding `-u` will place it into UDP mode.
`Nc -e [program]`	Used to redirect stdin/stdout from a program to Netcat.
`Nc -w [timeout]`	Used to set a timeout before Netcat automatically quits.
`Program | nc`	Used to pipe output of program to Netcat.
`Nc | program`	Used to pipe output of Netcat to program.
`Nc -h`	Used to display help options.
`Nc -v`	Used to put Netcat into verbose mode.
`Nc -g` or `nc -G`	Used to specify source routing flags. `-g` is gateway source routing, `-G` is numeric source routing.
`Nc -t`	Used for Telnet negotiation `DON'T` and `WON'T`.
`Nc -o [file]`	Used to hex dump traffic to file.
`Nc -z`	Used for port scanning.

Table 6-6 Netcat Commands

Task	Command Syntax
`Nc -d`	Used to detach Netcat from the console
`Nc -l -p [port]`	Used to create a simple listening TCP port; adding `-u` places it into UDP mode
`Nc -e [program]`	Used to redirect stdin/stdout from a program
`Nc -w [timeout]`	Used to set a timeout before Netcat automatically quits
`Nc -d`	Used to detach Netcat from the console

Try Safari Books Online FREE for 15 days

Get online access to Thousands of Books and Videos



Safari Books Online

FREE 15-DAY TRIAL + 15% OFF*
informit.com/safaritrial

Feed your brain

Gain unlimited access to thousands of books and videos about technology, digital media and professional development from O'Reilly Media, Addison-Wesley, Microsoft Press, Cisco Press, McGraw Hill, Wiley, WROX, Prentice Hall, Que, Sams, Apress, Adobe Press and other top publishers.

See it, believe it

Watch hundreds of expert-led instructional videos on today's hottest topics.

WAIT, THERE'S MORE!

Gain a competitive edge

Be first to learn about the newest technologies and subjects with Rough Cuts pre-published manuscripts and new technology overviews in Short Cuts.

Accelerate your project

Copy and paste code, create smart searches that let you know when new books about your favorite topics are available, and customize your library with favorites, highlights, tags, notes, mash-ups and more.

* Available to new subscribers only. Discount applies to the Safari Library and is valid for first 12 consecutive monthly billing cycles. Safari Library is not available in all countries.

Addison Wesley · Adobe Press · Alpha · Cisco Press · FT Press · IBM Press · Microsoft Press · New Riders · O'Reilly · Peachpit Press · Prentice Hall · Que · Redbooks · Sams · SAS Publishing · Wharton School Publishing · Wiley · Wrox