EXAM CRAM

CEH

Certified Ethical Hacker


Cram Sheet


Flash Cards


Practice Tests

Dr. CHUCK EASTTOM

FREE SAMPLE CHAPTER

SHARE WITH OTHERS

EXAM CRAM

CEH Certified Ethical Hacker Exam Cram

Dr. Chuck Easttom

CEH Certified Ethical Hacker Exam Cram

ISBN-13: 978-0-13-751344-4
ISBN-10: 0-13-751344-5

Library of Congress Control Number: 2021921550

ScoutAutomatedPrintCode

Editor-in-Chief
Mark Taub

Director, ITP Product Management
Brett Bartow

Executive Acquisitions Editor
James Manly

Development Editor
Ellie Bru

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Kitty Wilson

Indexer
Timothy Wright

Proofreader
Donna Mulder

Technical Editor
Akhil Behl

Publishing Coordinator
Cindy Teeters

Designer
Chuti Prasertsith

Compositor
codeMantra

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where:

- Everyone has an equitable and lifelong opportunity to succeed through learning.
- Our educational products and services are inclusive and represent the rich diversity of learners.
- Our educational content accurately reflects the histories and experiences of the learners we serve.
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview).

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

- Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

Credits

Figure	Attribution/Credit
Figure 1-1	Screenshot of Google Search © 2021 Google LLC
Figure 1-2	Screenshot of Google Advanced Search © Google LLC
Figure 1-3	Screenshot of Google Hacking Database © OffSec Services Limited 2021
Figure 1-4	Screenshot of netcraft.com Scan © 1995 - 2021 Netcraft Ltd
Figure 1-5	Screenshot of Shodan Search © Shodan
Figure 1-6	Screenshot of Archive.org Search © The Internet Archive
Figure 1-7	Screenshot of OSINT Page © Osintframework.com
Figure 1-8	Screenshot of Neustar Geolocation ©2021 Neustar, Inc.
Figure 1-9	Screenshot of https://mxtoolbox.com/DNSLookup.aspx DNS Results © Copyright 2004-2021, MXToolBox, Inc
Figure 1-10	Screenshot of tracert Results © Microsoft 2021
Figure 1-11	Screenshot of recon-ng © OffSec Services Limited 2021
Figure 1-12	Screenshot of UPnP SSDP M-SEARCH © Rapid7
Figure 1-13	Screenshot of Zenmap Tool © Insecure.Org
Figure 2-1	Screenshot of Colasoft Main Screen © 2001 - 2021 Colasoft
Figure 2-2	Screenshot of Colasoft Packet Editing © 2001 - 2021 Colasoft
Figure 2-3	Screenshot of Ping Scan © Microsoft 2021
Figure 2-4	Screenshot of Network Pinger Main Screen © Gonçalo Ferreira
Figure 2-5	Screenshot of Network Pinger Results © Gonçalo Ferreira
Figure 2-7	Screenshot of Lan Helper © 2021 Dan.com
Figure 2-8	Screenshot of nbtstat © Microsoft 2021
Figure 2-9	Screenshot of net view © Microsoft 2021
Figure 2-10	Screenshot of Zone Transfer © Microsoft 2021
Figure 2-11	Screenshot of tcpdump © OffSec Services Limited 2021
Figure 2-12	Screenshot of Wireshark Main Screen © Wireshark Foundation
Figure 2-13	Screenshot of Wireshark Color Coding © Wireshark Foundation
Figure 2-14	Screenshot of Nessus Main Screen © 2021 Tenable®, Inc
Figure 2-15	Screenshot of Nessus Scan Results © 2021 Tenable®, Inc
Figure 3-2	Screenshot of Winrtgen © Massimiliano Montoro
Figure 3-3	Screenshot of pwdump7 © Andres and Miguel Tarasco
Figure 3-4	Screenshot of RainbowCrack © 2020 RainbowCrack Project
Figure 3-5	Screenshot of ADS © Microsoft 2021
Figure 3-6	Screenshot of DeepSound © 2012-2021 Jpinsoft | Jozef Bátora

Figure 3-7	Screenshot of QuickStego © 2020 cybernescence ltd Pictorial Press Ltd / Alamy Stock Photo
Figure 3-8	Screenshot of OpenStego © 2017-2021 Samir Vaidya
Figure 3-9	Screenshot of ClearLogs © Microsoft 2021
Figure 3-10	Screenshot of Launching Metasploit in Kali Linux © OffSec Services Limited 2021
Figure 3-11	Screenshot of Launching Metasploit © OffSec Services Limited 2021
Figure 3-12	Screenshot of SMB Scan © OffSec Services Limited 2021
Figure 3-13	Screenshot of Getting a reverse Shell © Microsoft 2021
Figure 4-1	Screenshot of eLiTeWrap © Microsoft 2021
Figure 4-2	Screenshot of DarkHorse Trojan Maker © Trojan virus maker 1.2
Figure 4-3	Screenshot of TeraBIT Virus Maker © TeraBIT Virus Maker
Figure 4-4	Screenshot of BlackHost Virus Maker © 2021 - BlackHost
Figure 4-5	Screenshot of Internet Worm Maker Thing © Internet Worm Maker Thing
Figure 4-6	Screenshot of BinText © 2021 McAfee, LLC
Figure 4-7	Screenshot of IDA Decompiler © 2021 Hex-Rays
Figure 4-8	Screenshot of Sysinternals Process Explorer © Microsoft 2021
Figure 5-4	Screenshot of Antivirus System PRO © Antivirus System Pro
Figure 5-5	Screenshot of Netcraft Anti-phishing © 1995 - 2021 Netcraft Ltd
Figure 5-6	Screenshot of Social Engineer Toolkit © 2021 by TrustedSec
Figure 5-8	Screenshot of macof © OffSec Services Limited 2021
Figure 5-9	Screenshot of Changing a MAC Address in Windows 10 © Microsoft 2021
Figure 5-10	Screenshot of Technitium MAC Spoofer © Technitium
Figure 6-1	Screenshot of LOIC © 2021 Slashdot Media
Figure 6-2	Screenshot of DoSHTTP © Socketsoft LLC
Figure 6-3	Screenshot of XOIC © 2008-2038 of AppNee Freeware Group
Figure 6-4	Screenshot of HOIC © 2021 Slashdot Media
Figure 6-5	Screenshot of Burp Suite © 2021 PortSwigger Ltd.
Figure 7-1	Screenshot of Snort Installation: Choose Components Screen ©2021 Cisco
Figure 7-2	Screenshot of Executing Snort ©2021 Cisco
Figure 7-4a	Studio_G/Shutterstock
Figure 7-5a	
Figure 7-6a	
Figure 9-7c	

Contents at a Glance

Table of Contents

About the Author

Dr. Chuck Easttom is the author of 34 books, including several on computer security, forensics, and cryptography. He holds a doctor of science degree in cybersecurity, a Ph.D. in nanotechnology, a Ph.D. in computer science, and three master's degrees (one in applied computer science, one in education, and one in systems engineering). He is also an inventor with 23 patents. He is a senior member of both the IEEE and the ACM. He is also a Distinguished Speaker of the ACM and a Distinguished Visitor of the IEEE. Dr. Easttom is currently an adjunct professor for Georgetown University and for University of Dallas.

Dedication

For my wife, Teresa, who is always so supportive of my work.
—Chuck Easttom

Acknowledgments

Thanks are due to Eleanor (Ellie) Bru for working on this title once more and making it as strong as it can be.

—Chuck Easttom

About the Technical Editor

Akhil Behl, CCIE Emeritus No. 19564, is a passionate IT executive with key focus on cloud and security. He has 18+ years of experience in the IT industry, working across several leadership, advisory, consultancy, and business development profiles with various organizations. His technology and business specializations include cloud, security, infrastructure, data center, and business communication technologies. Currently he leads business development for cloud for a global systems integrator.

Akhil is a published author. Over the span of the past few years, he has authored multiple titles on security and business communication technologies. He has contributed as technical editor for over a dozen books on security, networking, and information technology. He has published four books with Pearson Education/Cisco Press.

He has published several research papers in national and international journals, including *IEEE Xplore*, and presented at various IEEE conferences, as well as other prominent ICT, security, and telecom events. Writing and mentoring are his passion.

He holds CCIE Emeritus (Collaboration and Security), Azure Solutions Architect Expert, Google Professional Cloud Architect, Azure AI Certified Associate, Azure Data Fundamentals, CCSK, CHFI, PMP, ITIL, VCP, TOGAF, CEH, ISM, CCDP, and many other industry certifications. He has a bachelor's degree in technology and a master's in business administration.

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: community@informit.com

*Be sure to check the box indicating that you would like to hear from us to receive exclusive discounts on future editions of this product.

Introduction

Welcome to CEH *Certified Ethical Hacker Exam Cram*. This book is designed to prepare you to take—and pass—the CEH exam. The CEH exam has become the leading introductory-level network certification available today. It is recognized by both employers and industry giants as providing candidates with a solid foundation of networking concepts, terminology, and skills.

About *CEH Exam Cram*

Exam Crams are designed to give you the information you need to know to prepare for a certification exam. They cut through the extra information, focusing on the areas you need to get through the exam. With this in mind, the elements within Exam Crams are aimed at providing the exam information you need in the most succinct and accessible manner.

This book is organized to closely follow the actual EC-Council objectives for exam CEH v11. As such, it is easy to find the information required for each of the specified EC-Council CEH v11 objectives. The objective focus design used by this Exam Cram is an important feature because the information you need to know is easily identifiable and accessible.

Within the chapters, potential exam hot spots are clearly highlighted with Exam Alerts. They have been carefully placed to let you know that the surrounding discussion is an important area for the exam. To further help you prepare for the exam, a Cram Sheet is included that you can use in the final stages of test preparation. Be sure to pay close attention to the bulleted points on the Cram Sheet because they pinpoint the technologies and facts you will probably encounter on the test.

Finally, great effort has gone into the questions that appear throughout the chapter and the practice tests to ensure that they accurately represent the look and feel of the ones you will see on the real CEH v11 exam. Be sure, before taking the exam, that you are comfortable with both the format and content of the questions provided in this book.

About the CEH v11 Exam

The CEH v11 exam is the newest iteration of several versions of the exam. The new CEH v11 objectives are aimed toward those who have at least two years of experience in cybersecurity and some exposure to penetration testing.

You will have a maximum of four hours to answer the 125 questions on the exam. The allotted time is quite generous, so when you finish, you will probably have time to double-check a few of the answers you were unsure of. Time is not typically an issue for this exam. The issue is ensuring that you fully understand the material in this book! Note that the exam includes 20 practical challenges. So when you see tools and techniques in this book, make sure you practice with them!

You need a minimum score of 70% to pass the CEH v11 exam. This means you can miss some questions and still pass. Your goal should be to get as many correct as you can, but if you feel like you don't really know the answers to a few questions, don't panic. Even if you get a few wrong, you can still pass the exam. The 70% is actually an estimate. CEH uses an adaptive format, described at https://cert.eccouncil.org/faq.html?_ga=2.167294973.253704694.1632148579-1175590966.1632148579.

EC-Council CEH v11 Exam Topics

Table I.1 lists general exam topics (that is, objectives) and specific topics under each general topic (that is, subobjectives) for the CEH v11 exam. This table also lists the chapter in which each exam topic is covered.

TABLE I.1 **Certified Ethical Hacker Exam Topics**

Chapter	CEH Exam Objective
Chapter 1: Reconnaissance and Scanning	Introduction to ethical hacking/concepts
Chapter 1: Reconnaissance and Scanning	Footprinting and reconnaissance
Chapter 2: Enumeration and Vulnerability Scanning	Enumeration
Chapter 2: Enumeration and Vulnerability Scanning	Vulnerability analysis
Chapter 3: System Hacking	System hacking
Chapter 4: Malware	Malware threats

Chapter	CEH Exam Objective
Chapter 5: Packet Sniffing and Social Engineering	Sniffing
Chapter 5: Packet Sniffing and Social Engineering	Social engineering
Chapter 6: Denial of Service and Session Hacking	Denial of service
Chapter 6: Denial of Service and Session Hacking	Session hijacking
Chapter 7: Evading Security Measures	Evading IDS, firewalls, and honeypots
Chapter 8: Hacking Web Servers and Applications	Hacking web servers
Chapter 8: Hacking Web Servers and Applications	Hacking web applications
Chapter 8: Hacking Web Servers and Applications	SQL injection
Chapter 9: Hacking Wireless	Hacking wireless
Chapter 10: Hacking Mobile	Hacking mobile
Chapter 11: IoT and OT Hacking	IoT and OT hacking
Chapter 12: Cloud Computing and Hacking	Cloud computing
Chapter 13: Cryptography	Cryptography

Booking and Taking the CEH v11 Exam

In order to be considered for the EC-Council CEH exam without attending official network security training, a candidate must have at least two years of work experience in the information security domain. A candidate who has the required work experience can submit an eligibility application form (see https://cert.eccouncil.org/application-process-eligibility.html) along with a nonrefundable fee of US$100. The exam itself costs $850.

When booking the exam, you need to provide the following information:

- Your name as you would like it to appear on your certificate
- Your Social Security or social insurance number
- Contact phone numbers (to be called in the event of a problem)
- Mailing address to which you want your certificate mailed

- Exam number and title
- Email address for contact purposes
- Credit card information so that you can pay online (You can redeem a voucher by calling the respective testing center.)

What to Expect from the Exam

If you haven't taken a certification test, the process can be a little unnerving. Even if you've taken numerous tests, it is not much better. Mastering the inner mental game often can be as much of a battle as knowing the material. Knowing what to expect before heading in can make the process a little more comfortable.

Certification tests are administered on a computer system at a Pearson VUE authorized testing center. The format of the exams is straightforward: For each question you have several possible answers to choose from. The questions in this book provide a good example of the types of questions you can expect on the exam. If you are comfortable with the questions provided in the book, the test should hold few surprises. The questions vary in length. Some of them are longer scenario questions, whereas others are short and to the point. Carefully read each question; a longer question typically has a key point that will lead you to the correct answer.

Most of the questions on the CEH v11 exam require you to choose a single correct answer, but a few require multiple answers. When there are multiple correct answers, a message at the bottom of the screen prompts you with the message "Choose all that apply." Be sure to read these messages.

Also make sure you are prepared for practical questions. These questions ask you to actually use tools and techniques described in this book. This is often done as a separate test with six hours to do 20 practical problems. As you can imagine, these questions are very involved. So practice, practice, practice,….

A Few Exam-Day Details

It is recommended that you arrive at the examination room at least 15 minutes early, although a few minutes earlier certainly would not hurt. This will give you time to prepare and will give the test administrator time to answer any questions you might have before the test begins. Many people suggest that you

review the most critical information about the test you're taking just before the test. (Exam Cram books provide a reference—the Cram Sheet, located inside the front of the book—that lists the essential information from the book in distilled form.) Arriving a few minutes early will give you some time to compose yourself and mentally review this critical information.

You will be asked to provide two forms of ID, one of which must be a photo ID. Each of the IDs you present should have a signature. You also might need to sign in when you arrive and sign out when you leave.

Be warned: The rules are clear about what you can and cannot take into the examination room. Books, laptops, note sheets, and so on are not allowed in the examination room. The test administrator will hold these items, to be returned after you complete the exam. You might receive either a wipe board or a pen and a single piece of paper for making notes during the exam. The test administrator will ensure that no paper is removed from the examination room.

After the Test

Whether you want it or not, as soon as you finish your test, your score displays on the computer screen. In addition to the results appearing on the computer screen, a hard copy of the report prints for you. Like the onscreen report, the hard copy displays your exam results and provides a summary of how you did on each section and on each technology. If you were unsuccessful, this summary can help you determine the areas you need to brush up on.

When you pass the CEH v11 exam, you will have earned the CEH certification, and your certificate will be mailed to you within a few weeks. Should you not receive your certificate and information packet within five weeks of passing your exam, contact feedback@eccouncil.org.

Last-Minute Exam Tips

Studying for a certification exam is no different than studying for any other exam, but a few hints and tips can give you the edge on exam day:

- **Read all the material:** EC-Council has been known to include material not expressly specified in the objectives. This book includes additional information not reflected in the objectives to give you the best possible preparation for the examination.

- **Watch for the Exam Alerts:** The CEH v11 objectives include a wide range of technologies. Exam Tips and Notes throughout each chapter are designed to highlight exam-related hot spots. They can be your best friends when preparing for the exam.
- **Use the questions to assess your knowledge:** Don't just read the chapter content; use the exam questions in each chapter to find out what you know and what you don't. If you struggle, study some more, review, and then assess your knowledge again.
- **Review the exam objectives:** Develop your own questions and examples for each topic listed. If you can develop and answer several questions for each topic, you should not find it difficult to pass the exam.

Good luck!

Companion Website

Register this book to get access to the Pearson Test Prep practice test software and other study materials plus additional bonus content. Check this site regularly for new and updated postings written by the author that provide further insight into the more troublesome topics on the exams. Be sure to check the box that you would like to hear from us to receive updates and exclusive discounts on future editions of this product or related products.

To access this companion website, follow these steps:

1. Go to **www.pearsonITcertification.com/register** and log in or create a new account.
2. Enter the ISBN **9780137513444**.
3. Answer the challenge question as proof of purchase.
4. Click the **Access Bonus Content** link in the Registered Products section of your account page to be taken to the page where your downloadable content is available.

Please note that many of our companion content files can be very large, especially image and video files.

If you are unable to locate the files for this title by following these steps, please visit **www.pearsonITcertification.com/contact** and select the **Site Problems/ Comments** option. Our customer service representatives will assist you.

Pearson Test Prep Practice Test Software

As noted previously, this book comes complete with the Pearson Test Prep practice test software and two full exams. These practice tests are available to you either online or as an offline Windows application. To access the practice exams that were developed with this book, please see the instructions in the card inserted in the sleeve in the back of the book. This card includes a unique access code that enables you to activate your exams in the Pearson Test Prep practice test software.

> **Note**
>
> The cardboard sleeve in the back of this book includes a piece of paper. The paper lists the activation code for the practice exams associated with this book. Do not lose the activation code. On the opposite side of the paper from the activation code is a unique, one-time-use coupon code for the purchase of the Premium Edition eBook and Practice Test.

Accessing the Pearson Test Prep Software Online

The online version of this software can be used on any device with a browser and connectivity to the Internet, including desktop machines, tablets, and smartphones. To start using your practice exams online, follow these steps:

1. Go to **www.PearsonTestPrep.com**.
2. Select **Pearson IT Certification** as your product group.
3. Enter your email/password for your account. If you don't have an account on PearsonITCertification.com, establish one by going to **PearsonITCertification.com/join**.
4. In the My Products tab, click the **Activate New Product** button.
5. Enter the access code printed on the insert card in the back of your book to activate your product. The product is now listed in your My Products page.
6. Click the **Exams** button to launch the exam settings screen and start a practice exam.

Accessing the Pearson Test Prep Software Offline

If you want to study offline, you can download and install the Windows version of the Pearson Test Prep software. There is a download link for this software on the book's companion website, or you can enter the following link in your browser:

www.pearsonitcertification.com/content/downloads/pcpt/engine.zip

To access the book's companion website and the software, follow these steps:

1. Register your book by going to **PearsonITCertification.com/register** and entering the ISBN **9780137513444**.
2. Respond to the challenge questions.
3. Go to your account page and select the **Registered Products** tab.
4. Click the **Access Bonus Content** link under the product listing.
5. Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to download the software.
6. After the software downloads, unzip all the files on your computer.
7. Double-click the application file to start the installation and follow the onscreen instructions to complete the registration.
8. When the installation is complete, launch the application and click the **Activate Exam** button on the My Products tab.
9. Click the **Activate a Product** button in the Activate Product Wizard.
10. Enter the unique access code found on the card in the sleeve in the back of your book and click the **Activate** button.
11. Click **Next** and then click **Finish** to download the exam data to your application.
12. Start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

Note that the offline and online versions will sync together, so saved exams and grade results recorded in one version will be available to you on the other as well.

Customizing Your Exams

When you are in the exam settings screen, you can choose to take exams in one of three modes:

- Study mode
- Practice Exam mode
- Flash Card mode

Study mode allows you to fully customize an exam and review answers as you are taking the exam. This is typically the mode you use first to assess your knowledge and identify information gaps. Practice Exam mode locks certain customization options in order to present a realistic exam experience. Use this mode when you are preparing to test your exam readiness. Flash Card mode strips out the answers and presents you with only the question stem. This mode is great for late-stage preparation, when you really want to challenge yourself to provide answers without the benefit of seeing multiple-choice options. This mode does not provide the detailed score reports that the other two modes provide, so it is not the best mode for helping you identify knowledge gaps.

In addition to these three modes, you will be able to select the source of your questions. You can choose to take exams that cover all of the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. The two exams printed in the book are available to you, as are two additional exams of unique questions. You can have the test engine serve up exams from all four banks or just from one individual bank by selecting the desired banks in the exam bank area.

You can make several other customizations to your exam from the exam settings screen, such as the time of the exam, the number of questions, whether to randomize questions and answers, whether to show the number of correct answers for multiple answer questions, or whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if there are any updates to your exam data and automatically download any changes made since the last time you used the software. This requires that you be connected to the Internet at the time you launch the software.

Sometimes, due to a number of factors, the exam data might not fully download when you activate your exam. If you find that figures or exhibits are missing, you might need to manually update your exams.

To update a particular exam you have already activated and downloaded, simply select the Tools tab and click the Update Products button. Again, this is only an issue with the desktop Windows application.

If you wish to check for updates to the Windows desktop version of the Pearson Test Prep exam engine software, simply select the Tools tab and click the Update Application button. Doing so allows you to ensure that you are running the latest version of the software engine.

Assessing Exam Readiness

Exam candidates never really know whether they are adequately prepared for the exam until they have completed about 30% of the questions. At that point, if you are not prepared, it is too late. The best way to determine your readiness is to work through all of the quizzes in each chapter and review the foundation and key topics presented in each chapter. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

Premium Edition eBook and Practice Tests

This book also includes an exclusive offer for 70% off the Premium Edition eBook and Practice Tests edition of this title. Please see the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.

This page intentionally left blank

CHAPTER 6

Denial of Service and Session Hijacking

This chapter covers the following CEH exam objectives:

- Understand various DoS attacks
- Be able to implement DoS countermeasures
- Use common DoS tools
- Comprehend session hijacking techniques
- Implement session hijacking countermeasures

Denial of Service

Denial of service (DoS) attacks, as the name suggests, are not about breaking into a system but rather about denying legitimate users the opportunity to use the system. In most cases, a DoS attack is easy to execute. This makes DoS attacks a very serious problem. Every technology has limits; if you can exceed those limits, then you can make a system unusable.

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. Sharia has detected an attack on her company web server. In this attack, the message body is sent quite slowly. What best describes this attack?
   - **A.** Slowloris
   - **B.** HTTP post
   - **C.** Smurf
   - **D.** PDoS
2. Todd is concerned about DoS attacks against his network. He is particularly worried about attacks that used malformed ICMP packets. What type of attack is Todd concerned about?
   - **A.** PoD
   - **B.** Teardrop
   - **C.** PDoS
   - **D.** Smurf
3. How does SPI help mitigate DoS?
   - **A.** By detecting anomalies in the stream such as too many SYN packets from the same IP source
   - **B.** By blocking fake IP addresses and sending their traffic to a black hole
   - **C.** By carefully examining each packet and tracing back its origin
   - **D.** By encrypting traffic, preventing many attacks

Answers

1. **B.** This is an HTTP post attack. Slowloris involves partial HTTP requests.
2. **A.** This is a PoD (ping of death) attack.
3. **A.** SPI (stateful packet inspection) looks at not just the individual packet but all the packets that came before it in the session. It can detect a range of DoS attacks.

Protocol Attacks

A protocol attack tries to exploit some vulnerability in the protocol being used. Exploiting such vulnerabilities can cause a system to become unresponsive. The magnitude of a protocol attack is measured in packets per second (pps).

ExamAlert

Objective For the CEH exam, make certain you know the categories of attacks as well as how the magnitude is measured for each category.

TCP SYN Flood Attacks

A TCP SYN flood attack is an older type of DoS attack, but it illustrates the concepts of denial of service quite well. This particular type of attack depends on the hacker's knowledge of how connections to a server are made. When a session is initiated between a client and a server in a network using TCP, a packet is sent to the server with a 1-bit flag called a SYN flag set. (SYN is short for synchronize.) This packet is asking the target server to synchronize communications. The server allocates appropriate resources and then sends to the client a packet with both the SYN (synchronize) and ACK (acknowledge) flags set. The client machine is then supposed to respond with an ACK flag set. This process, called a three-way handshake, is summarized as follows:

1. The client sends a packet with the SYN flag set.
2. The server allocates resources for the client and then responds with the SYN and ACK flags set.
3. The client responds with the ACK flag set.

There have been a number of well-known SYN flood attacks on web servers. This attack type is popular because any machine that engages in TCP communication is vulnerable to it—and all machines connected to the Internet engage in TCP communications. Such communication is obviously the entire reason for web servers. The easiest way to block DoS attacks is via firewall rules.

Teardrop Attacks

Fragmentation attacks in general try to prevent targets from being able to reassemble packet fragments. They usually involve sending a large number of fragmented packets to the target. A teardrop attack is a specific type of fragmentation attack. In a teardrop attack, the attacker sends a fragmented message, where the two fragments overlap in ways that make it impossible to reassemble them properly without destroying the individual packet headers. Therefore, when the victim attempts to reconstruct the message, the message is destroyed. This causes the target system to halt or crash. There are a number of variations on the basic teardrop attack, such as TearDrop2, Boink, targa, Nestea Boink, NewTear, and SYNdrop.

ACK Flood Attacks

As the name suggests, an ACK flood attack involves sending a flood of TCP ACK packets. Normally an ACK packet is an acknowledgment of something being received, be it data or a synchronization request. Some devices or services are stateful, which means they process each packet. When a target receives a flood of ACK packets, it tries to process it but, because it is not actually an acknowledgment of anything, it can overwhelm the target.

TCP State Exhaustion Attacks

There are a variety of state exhaustion attacks, and the idea behind them all is essentially the same. They attack weaknesses in Layers 3 and 4 of the protocol stack and overconsume resources. Invalid name queries to a DNS server are a type of state exhaustion attack. TCP state exhaustion attacks operate on some aspect of the TCP handshake. For example, a SYN flood attack is a type of TCP state exhaustion.

Application Layer Attacks

Application layer DoS attacks work to consume a given application's resources. The magnitude is usually measured in requests per second (rps). Basically, overwhelming a target server with too many requests is the basis for most application layer attacks.

HTTP Post DoS Attacks

An HTTP post DoS attack involves sending a legitimate HTTP post message. Part of the post message is the content length, which indicates the size of the message to follow. In this type of attack, the attacker sends the actual message body at an extremely slow rate. The web server is then hung as it waits for the message to complete. For more robust servers, the attacker needs to use multiple HTTP post attacks simultaneously.

Slowloris Attacks

A Slowloris attack is another attack against web servers. The attacker sends partial HTTP requests. When the target receives these requests, it opens a connection and waits for the requests to complete. But rather than complete a request, the attacker continues to send multiple partial requests. Eventually, the

server has opened so many connections that it exhausts its maximum connection pool limit and can no longer respond to legitimate requests.

Volumetric Attacks

All volumetric attacks seek to overwhelm the target with an overwhelming number of packets. These attacks are not particularly sophisticated or difficult. They simply overwhelm the target. The magnitude of a volumetric attack is usually measured in bits per second (bps).

Smurf IP Attacks

A UDP attack is a type of volumetric attack, and a Smurf attack is a very popular version of a DoS attack. An ICMP (Internet Control Message Protocol) packet is sent out to the broadcast address of the network. The network responds by echoing the packet out to the network hosts, which then send it to the spoofed source address. Also, the spoofed source address can be anywhere on the Internet, not just on the local subnet. A hacker who can continually send such packets can cause the network itself to perform a DoS attack on one or more of its member servers. This attack is clever and rather simple. The only problem for the hacker is getting the packets started on the target network. This task can be accomplished via some software, such as a virus or Trojan horse, that begins sending the packets.

In a Smurf attack, there are three people/systems involved: the attacker, the intermediary (who can also be a victim), and the victim. The attacker first sends an ICMP echo request packet to the intermediary's IP broadcast addresses. Since this is sent to the IP broadcast address, many of the machines on the intermediary's network receive this request packet and send back an ICMP echo reply packet. If all the machines on a network are responding to this request, the network becomes congested, and there may be outages.

The attacker impacts the third party—the intended victim—by creating forged packets that contain the spoofed source address of the victim. Therefore, when all the machines on the intermediary's network start replying to the echo request, those replies flood the victim's network. Thus, another network becomes congested and could become unusable. This type of attack is illustrated in Figure 4.4 in Chapter 4, "Malware."

UDP Flood Attacks

The UDP flood attack is another example of a volumetric attack. Keep in mind that UDP (User Datagram Protocol) is a protocol that does not verify each packet's delivery. In a UDP flood attack, the attacker sends a UDP packet to a random port on a target system. When the target system receives a UDP packet, the attacker determines what application is listening on the destination port. Then, if the attacker wants to attack that application, he or she just starts a flood of UDP packets to the IP address and port. If enough UDP packets are delivered to ports on the target, the system becomes overloaded trying to determine awaiting applications (which do not exist) and then generating and sending packets back.

ICMP Flood Attacks

The ICMP flood attack is another volumetric attack. ICMP flood attacks are usually accomplished by broadcasting a large number of either pings or UDP packets. Like other flood attacks, the idea is to send so much data to the target system that the system slows down. If it can be forced to slow down enough, the target will time out (i.e., not send replies fast enough) and be disconnected from the Internet. This type of attack is far less effective against modern computers than it was against older ones. Even a low-end desktop PC now has 4 GB (or more) of RAM and a dual-core processor, making it difficult to generate enough pings to knock the machine offline. However, at one time, this was a very common form of DoS attack.

Ping of Death Attacks

A ping of death attack, often simply called a PoD attack, is accomplished by sending malformed ICMP packets (e.g., sending a packet that is 65,536 bytes in size). RFC 791 specifies a maximum packet size of 65,535 bytes. A PoD attack can cause a vulnerable system to crash.

Other DoS Attacks

Some DoS attack types don't fit neatly into one of the previously discussed categories. These attacks can nonetheless be quite effective against target systems.

Multi-Vector Attacks

As the name suggests, a multi-vector attack is a combination of two or more of the other attacks (e.g., launching a SYN flood attack and a teardrop attack at the same time). Another method is to launch one type of attack and then, after a time, to shift to a different attack vector. This method can overcome DoS countermeasures the target may have implemented.

DHCP Starvation Attacks

DHCP (Dynamic Host Configuration Protocol) is used to dynamically assign IP addresses to systems on a network. If an attacker floods a target network with DHCP requests for dynamic IP addresses, the attacker can completely exhaust the address space allocated by the DHCP server. Then legitimate users cannot get an IP address assigned and thus cannot connect to the network. There are tools such as gobblers that can do this for an attacker.

PDoS Attacks

Though not terribly common, it is possible to have a DoS attack that leaves the system either inoperable or needing the operating system completely reinstalled. These are referred to as *permanent denial of service* (*PDoS*) *attacks*, or phlashing. Such attacks usually involve DoS attacks on a device's firmware.

Registration DoS Attacks

A registration DoS attack is a very simplistic attack used against websites. The attacker creates a script or program that just keeps registering fake users on a website. This is one reason many registration websites use CAPTCHA.

Login DoS Attacks

Login DoS attacks are similar to registration DoS attacks and also frequently use scripts or programs. The attacker tries to overload the login process by continually sending login information. This can overwhelm the target system or at least slow it down. Many websites use CAPTCHA to prevent automated login attempts.

DDoS Attacks

Perhaps the most common form of DoS attack today is the *DDoS attack*. This type of attack is accomplished by getting various machines to attack the target. This is commonly done by sending out a Trojan horse that causes infected computers to attack a specified target at a particular date and time—which is a very effective way to execute a DDoS attack on any target. In this form of DDoS attack, the attacker does not have direct control of the various machines used in the attack. These machines are simply infected by some malware that causes them to participate in the attack on a particular date and at a particular time.

Another method is to use a botnet to orchestrate a DDoS attack. A *botnet* is a network of computers that have been compromised by an attacker so that the attacker has control of the computers. This is often accomplished via delivery of a Trojan horse. However, unlike in the previous DDoS example, the attacker has direct control over the attacking machines in the botnet.

A botnet usually has a command and control (C&C) that controls the various compromised machines. Then the botnet can be used for whatever the attacker wishes. DDoS is only one application of a botnet. Password cracking and sending phishing emails are other uses. The compromised systems can be attacked in any of the ways that malware is usually distributed: via phishing emails, compromised websites, vulnerable target systems, etc.

Peer-to-Peer Attacks

While peer-to-peer (P2P) apps have become quite popular, so have P2P DoS attacks. One method is to force the client to disconnect from the legitimate P2P hub and get the client to connect to the attacker's fake hub. There have also been massive DDoS attacks on peer-to-peer networks. In addition, attackers attempt to exploit flaws in the protocols used, such as the Direct Connect (DC++) protocol that is used to share files between peer-to-peer clients.

Distributed Reflection DoS Attacks

As previously stated, DDoS attacks are becoming more common. Most such attacks rely on getting various machines (i.e., servers or workstations) to attack the target. A distributed reflection DoS attack is a special type of DoS attack. As with all such attacks, it is accomplished by the hacker getting a number of machines to attack the selected target. However, this attack works a bit differently than other DoS attacks. Rather than getting computers to attack the target, this method tricks Internet routers into attacking a target.

Many of the routers on the Internet backbone communicate on port 179, particularly using BGP (Border Gateway Protocol) to exchange routing information. A distributed reflection DoS attack exploits that communication line and gets routers to attack a target system. What makes this attack particularly wicked is that it does not require the routers in question to be compromised in any way. The attacker does not need to get any sort of software on a router to get it to participate in the attack. Instead, the hacker sends a stream of packets to the various routers, requesting a connection. The packets have been altered so that they appear to come from the target system's IP address. The routers respond by initiating connections with the target system. What occurs is a flood of connections from multiple routers, all hitting the same target system. This has the effect of rendering the target system unreachable.

ExamAlert

Objective For the CEH exam, you must be able to fully describe each of the attacks discussed in this section. It is worth your time to memorize these attacks.

Common Tools Used for DoS Attacks

As with any of the other security issues discussed in this book, you will find that hackers have at their disposal a vast array of tools in the DoS arena. While it is certainly well beyond the scope of this book to begin to categorize or discuss all of these tools, a brief introduction to just a few of them will prove useful.

LOIC

LOIC (Low Orbit Ion Cannon) is one of the most widely known DoS tools available. It has a very easy-to-use graphical user interface, shown in Figure 6.1.

This tool is very easy to use. As you can see in Figure 6.1, it simply requires the user to enter the target URL or IP address and then begin the attack. Fortunately, this tool also does nothing to hide the attacker's address and thus makes it relatively easy to trace the attack back to its source. It is an older tool but still widely used today. There is a tool similar to this named HOIC, which we discuss later in this section.

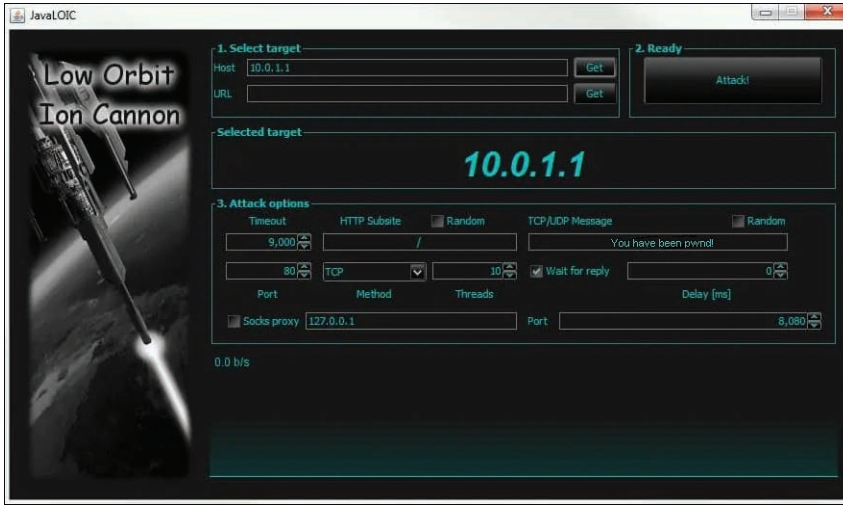

FIGURE 6.1 **LOIC**

DoSHTTP

DoSHTTP is another tool that is simple to use. You select the target, the agent (i.e., the browser type to simulate), the number of sockets, and the requests and then start the flood. You can see this in Figure 6.2.

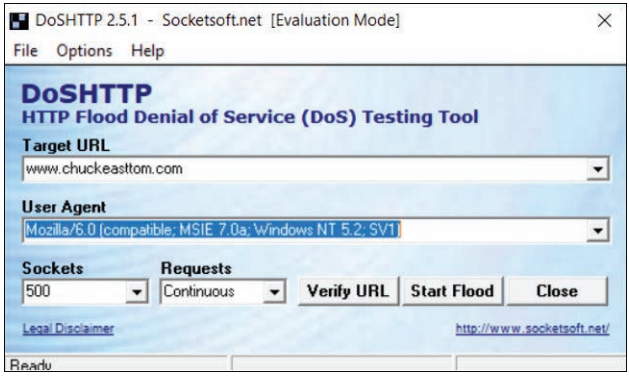

FIGURE 6.2 **DoSHTTP**

XOIC

XOIC, which is similar to LOIC, has three modes: send a message, execute a brief test, or start a DoS attack. You can see these options in Figure 6.3.

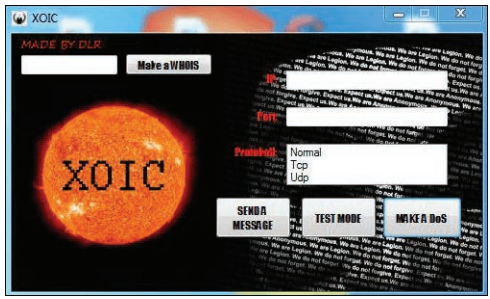

FIGURE 6.3 **XOIC**

Like LOIC, XOIC is very easy to use. It is just a point-and-click graphical user interface. Even attackers with minimal skill can launch a DoS attack using XOIC.

HOIC

HOIC (High Orbit Ion Cannon) was developed by the Anonymous collective as an improvement on LOIC. It is available at https://sourceforge.net/projects/highorbitioncannon/. Although HOIC was meant to be more powerful than LOIC, it still has a very simple user interface, which can be seen in Figure 6.4.

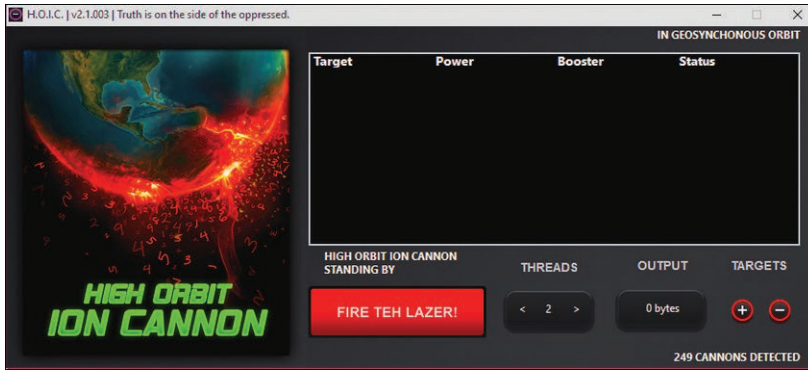

FIGURE 6.4 **HOIC**

Other Tools for DoS and DDoS Attacks

There are many other tools for DoS and DDoS. A few are listed here:

- **Hulk:** A Python script, available at https://github.com/grafov/hulk
- **DAVOSET:** A command line tool for DoS attacks, available at https://github.com/MustLive/DAVOSET
- **R-U-Dead-Yet (RUDY):** Tool that uses POST attacks, available at https://sourceforge.net/projects/r-u-dead-yet/
- **AnDOSid:** An Android tool for DoS, available at https://www.hackingtools.in/free-download-andosid/

Countermeasures to DoS and DDoS Attacks

The CEH exam will ask you about countermeasures to DoS and DDoS attacks. A few of them have already been discussed. For example, CAPTCHA can mitigate web DoS attacks. In general, three categories can be used in the case of overwhelming attacks:

- Simply shut down the targeted service. This is usually not a good choice, as it essentially means capitulating to the attack.
- Keep the critical services functioning by stopping noncritical services and use those resources for the critical services.
- Absorb the attack. This method is popular with internet service providers (ISPs; for an added charge). When the ISP detects a DoS or DDoS attack in progress, it allocates additional bandwidth to absorb that attack.

A good antivirus approach coupled with regular system updates can prevent one of your systems from becoming compromised and becoming part of a botnet. Filtering incoming and outgoing traffic to your network can also mitigate DoS attacks. Rate limiting any service or IP address so that it can consume only a finite percentage of resources also helps mitigate DoS attacks.

Honeypots are gaining popularity in deflecting all sorts of attacks, including DoS attacks. A *honeypot* is a fake system set up for the sole purpose of attracting hackers. Essentially, if a honeypot looks realistic enough, the attacker may go after it rather than after a real system.

Robust network configuration can also help mitigate DoS attacks. Load balancing critical services is a very good first step in helping mitigate DoS attacks. Throttling or limiting traffic for a given service can also help. Being able to drop incoming requests when a certain threshold is reached is also helpful.

There is actually a standard for filtering. RFC 3704, "Ingress Filtering for Multihomed Networks," is a standard to help limit the impact of DDoS attacks by blocking any traffic with spoofed IP addresses.

Black hole filtering is another common technique. A *black hole* is a network location where traffic is simply discarded/dropped, typically by sending traffic to an IP address that is not in use. When a DoS attack is detected, suspected DoS traffic can be forwarded to the network black hole.

As mentioned earlier in this book, the CEH exam has a strong emphasis on Cisco. You therefore need to be familiar with a couple Cisco commands that can help mitigate DoS attacks:

- **access-list access-list-number {deny | permit} tcp any destination destination-wildcard:** Defines an IP extended access list
- **ip tcp Intercept list access-list-number:** Enables TCP intercept

There are also a number of devices that can be added to a network to help mitigate DoS attacks, including:

- FortiDDoS-1200B
- Cisco Guard XT 5650
- Cisco IP reputation filtering
- Check Point DDoS Protector
- Active Reach DDoS mitigation device https://activereach.net/solutions/network-security/protect/ddos-mitigation/perimeter-ddos-mitigation/
- Verizon DDoS Shield https://www.verizon.com/business/products/security/network-cloud-security/ddos-shield/
- Netscout DDoS protection https://www.netscout.com/solutions/ddos-protection
- F5 DDoS protection https://www.f5.com/solutions/application-security/ddos-protection
- DDoS Mitigation https://www.a10networks.com/products/thunder-tps/

There are also software solutions that can help mitigate DoS attacks:

- **Anti DDoS Guardian:** http://www.beethink.com
- **DOSarrest's DDoS Protection Service:** https://www.dosarrest.com
- **DDoS-GUARD:** https://ddos-guard.net

SPI (stateful packet inspection) is an excellent way to mitigate DoS attacks. Many modern firewalls use SPI. These types of firewalls not only apply rules to each packet but maintain the state of communication between the client and the server. As an example of how this mitigates attacks, the firewall realizes that multiple SYN packets are coming from the same IP address and then blocks those packets. This is one major reason SYN floods are not seen much today. In addition, next-generation firewalls (NGFWs) combine traditional firewall capabilities and other functions, such as those of an application firewall or an intrusion detection system/prevention system (IDS/IPS). Using a modern advanced firewall is an excellent way to mitigate DoS and DDoS attacks.

ExamAlert

Objective For the CEH exam, be sure you are very familiar with the DoS/DDoS countermeasures.

DoS in the Real World

According to the security consulting firm Calyptix Security, the first quarter of 2018 set records for DoS and DDoS attacks. This included a massive DDoS attack against the GitHub site on February 28, 2018, peaking at 1.3 Tbps. This illustrates how effective and damaging these attacks can be, for the amount of data sent in DoS attacks is growing all the time.

One creative example comes from 2017. In February 2017, a new DDoS attack vector emerged. Attackers used memcache, a database caching system, to amplify traffic volume. A request could be amplified by a factor of several thousand by using this method. The aforementioned GitHub attack involved memcaching. This illustrates that new methods of DoS are being developed, and you should expect to see them out in the real world (though not on the CEH exam).

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. What Cisco command enables TCP intercept?
   - ❍ **A. access-list access-list-number {deny | permit} tcp any destination destination-wildcard**
   - ❍ **B. ip tcp Intercept list access-list-number**
   - ❍ **C. ip tcp Intercept-enable**
   - ❍ **D. access-list access-list-number intercept-enable**

2. Which attack is based on an ICMP (Internet Control Message Protocol) packet sent to the broadcast address of the network?
   - ❍ **A.** Teardrop attack
   - ❍ **B.** Slowloris attack
   - ❍ **C.** Smurf attack
   - ❍ **D.** PDoS attack

3. What is the most effective countermeasure for registration DoS attacks?
   - ❍ **A.** Using an SPI firewall
   - ❍ **B.** Using CAPTCHA
   - ❍ **C.** Encrypting traffic
   - ❍ **D.** Using Cisco configuration

Answers

1. **C.** If you are not familiar with Cisco router/switch commands, this can be one of the more challenging parts of the CEH exam.
2. **B.** A Smurf attack works by sending a flood of broadcast messages to the target system router, impersonating the target machine's IP address.
3. **B.** This is one reason so many sites use CAPTCHA: It prevents scripts from running registration DoS attacks.

Session Hijacking

Conceptually, session hijacking is quite simple. The goal is to find an authentic TCP session and to take over that session. This is possible because, generally speaking, the session is authenticated at the beginning. Clearly, session hijacking is easier with some systems than with others.

CramSaver

If you can correctly answer these CramSaver questions, save time by skimming the Exam Alerts in this section and then completing the Cram Quiz at the end of the section. If you are in any doubt at all, read everything in this chapter.

1. What type of session hijacking begins with the attacker attempting to get the user to authenticate to the target server, using a session ID prechosen by the attacker?
   - **A.** Man-in-the-browser
   - **B.** Session fixation
   - **C.** Session replay
   - **D.** Man-in-the-middle
2. Mohanned has discovered malware on a machine. This malware has an interface like a web browser library and appears to be intercepting browser calls. What type of attack is this?
   - **A.** Trojan horse
   - **B.** Session fixation
   - **C.** Man-in-the-middle
   - **D.** Man-in-the-browser
3. Gerard, who is a web developer, is concerned about session hijacking and is using the HTTPOnly flag. What does this flag do?
   - **A.** Permits only HTTP and not HTTPS
   - **B.** Only allows cookies to be accessed via HTTP
   - **C.** Prevents scripts running on the client
   - **D.** Logs all HTTP request queries and nothing else

Answers

1. **B.** This is a classic description of session fixation.
2. **D.** This is a man-in-the-browser attack. A man-in-the-browser attack is a special type of man-in-the-middle attack, and it is possible that the malware was delivered via a Trojan horse, but the best answer is man-in-the-browser.
3. **B.** Allowing cookies to be accessible only via HTTP prevents client-side scripts or malware from manipulating cookies.

Several factors can make a system more vulnerable to session hijacking. Having a weak session ID generation algorithm is a common issue. This makes predicting or guessing session IDs much easier. Having no expiration or having a very long expiration on a session also increases the possibilities for an attacker.

There are two types of session hijacking:

- **Active:** In active session hijacking, the attacker identifies an active session and takes over that session.
- **Passive:** In passive hijacking, the attacker just sniffs the traffic. This is not true session hijacking but is identified as passive session hijacking by the CEH exam.

The Session Hijacking Process

The CEH exam defines a process of five steps for session hijacking. An attacker won't always follow this process, but you should know it for the CEH exam:

1. Sniff the traffic going to the target so you can learn about how sessions are handled. This involves using a packet sniffer such as Wireshark or tcpdump (discussed in Chapter 2, "Enumeration and Vulnerability Scanning") to see what is being sent between a client and a server.
2. Monitor the traffic to determine if you can predict the next valid sequence number or session ID.
3. Break the connection to the legitimate client.
4. Take over the session, posing as that client using a session and/or sequence ID that will appear legitimate to the target server.
5. Perform command injection, or inject packets into the target server.

Specific Session Hijacking Methods

There are a number of mechanisms for getting a session token in order to take over a session. If data is unencrypted, you may be able to derive this information through packet sniffing. Or if the target uses a simple session ID, such as a date/time stamp, it is easy to predict the next session ID. However, there are other methods, as described in the following subsections.

Web Session Hijacking

If the target is a web server, cross-site scripting (XSS) might be able to derive a token. XSS uses malicious JavaScript. The most typical method of XSS is to

insert the JavaScript into a website in a place where users normally enter text for other users to read, such as product reviews. However, it is also possible to send malicious scripts as part of an email. Or a phishing email may be able to get a user to a website that has malicious JavaScript built in.

Cross-site request forgery (CSRF) attacks an active session with a trusted site. The attacker might have a malicious link on some compromised site. Often users have more than one browser open at a time. If a user visits a compromised site and clicks on the link while they also have an active session open, the attacker can get the user's session ID for the target site. Then the attacker sends requests to the target website, posing as the user. Both XSS and CSRF are listed as OWASP (Open Web Application Security Project) top 10 vulnerabilities.

Session fixation is another method of session hijacking. The attacker tries to get the user to authenticate to the target server, using a session ID prechosen by the attacker. This works only if the server has a very weak session ID generation scheme—one that the attacker can readily emulate to produce a session ID that appears legitimate to the server.

Session replay attacks are still covered on the CEH exam, but they rarely work today. Such an attack involves simply intercepting authentication packets and re-sending them to the target. Although modern authentication methods make such attempts ineffective, you should be aware of this type of attack for the CEH exam.

Variations of the man-in-the-middle attack work whether the target is a web server or not. The attacker sits between the client and server, via a fake access point, a fake website, or using one of many other methods. One variation of the man-in-the-middle attack is the forbidden attack. This is targeted to older, flawed implementations of TLS. Older TLS versions would sometimes reuse a nonce (short for *number only used once*) during the TLS handshake, which made them vulnerable. The attacker would sniff the nonce and then use it to authenticate to the server. (Remember that TLS [Transport Layer Security] is the successor to SSL [Secure Sockets Layer] since 1999. However, many people still simply say SSL when they mean TLS.)

With a man-in-the-browser attack, malicious software is on the client machine and behaves like a software library or component that the browser uses. Then that malware intercepts data going out from the browser. This is a variation of a man-in-the-middle attack. A number of malicious Chrome extensions and Firefox add-ins have been man-in-the-browser malware.

Other attacks specifically target flaws in protocols such as SSL/TLS. CRIME (Compression Ratio Info-Leak Made Easy) is one such attack. Essentially, the compression used in earlier versions of TLS was flawed and could lead to data leaks. There have been similar issues such as the BREACH attack. BREACH (Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext) is an improvement over CRIME that attacks an issue with the gzip compression algorithm.

Network Session Hijacking

TCP/IP hijacking is the process of taking over a TCP connection between a client and a target machine. It often uses spoofed packets. If the attacker can cause the client machine to pause or hang, the attacker can pretend to be the client and send spoofed packets. To do this, the attacker must know the packet sequence number and be able to use the next sequence number. Modern authentication methods periodically re-authenticate, often rendering this type of attack unsuccessful.

RST hijacking is another method. The attacker uses an RST (reset) packet to spoof the client's IP address, but also uses the correct sequence number to cause the connection to reset. This resets the connection and allows the attacker to take over that session. A number of tools help craft custom packets, such as Packet Builder from Colasoft.

Some attackers simply inject forged packets into a data stream, spoofing the source IP address. With this method, the attacker cannot see the response, and it is thus called *blind hijacking*.

UDP hijacking is similar to TCP/IP hijacking, but using UDP packets. The attacker spoofs the server, sending the client a forged UDP reply, so the client connects to the attacker's machine.

There are a number of tools that can help perform any of these attacks. One of the most widely used—and heavily emphasized on the CEH exam—is Burp Suite. Burp Suite can be downloaded from https://portswigger.net/burp. There is a free community edition, and there are professional and enterprise editions. Using the default settings, the main screen of the Burp Suite community edition looks as shown in Figure 6.5.

The CEH exam won't test you on all the uses of Burp Suite, but it is probably a good idea to get familiar with this tool as it is very helpful in conducting penetration tests. Fortunately, the internet is replete with tutorials for Burp Suite.

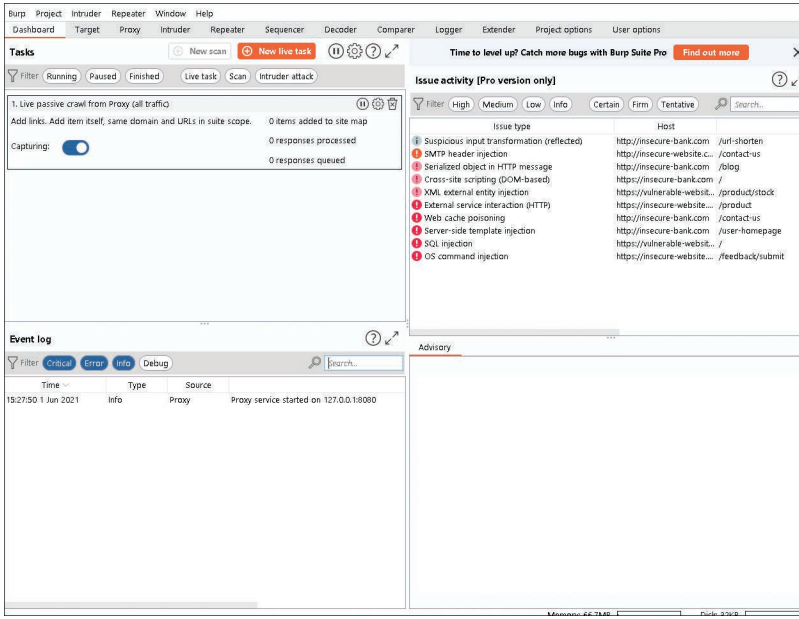

FIGURE 6.5 **Burp Suite**

There are other tools that can accomplish similar tasks:

- **OWASP ZAP:** A tool often touted as a website vulnerability scanner, which also allows you to intercept and alter packets, available at www.owasp.org
- **WebSploit Framework:** A tool explicitly designed for man-in-the-middle attacks, available at https://sourceforge.net/projects/websploit/
- **Bettercap:** A tool that is also useful for Bluetooth hacking, available at https://www.bettercap.org
- **DroidSheep:** A session hijacking tool that runs on Android, available at https://droidsheep.info
- **DroidSniff:** An Android tool designed for security scanning that can also be used for man-in-the-middle attacks, available at https://github.com/evozi/DroidSniff

Countermeasures for Session Hijacking

There are many different methods for mitigating session hijacking. One of the easiest is to encrypt all data in transit. This includes using SSH for any secure communications. In addition to ensuring that communications are encrypted,

you should ensure that you are using up-to-date methods. Earlier in this chapter, we discussed attacks against TLS vulnerabilities. Using the latest TLS version (which is 1.3 as of this writing) will mitigate or eliminate most of them.

Never use session ID numbers that are easy to predict. They should be random numbers generated by a robust random number generation algorithm. Also ensure that session IDs are transmitted securely and that sessions time out.

Strong authentication techniques such as Kerberos will prevent at least some session hijacking attacks. Also ensure that you are using the normal antimalware protections, such as antivirus and intrusion prevention systems.

Web developers can combat session hijacking attacks on their websites by using a variety of additional techniques. For example, cookies with session information should be stored securely (encrypted), and a website should use the HTTPOnly attribute. HTTPOnly means the cookie can only be accessed with the HTTP protocol; any script or malware on the client computer cannot access it.

Websites should check to see that all traffic for a given session is coming from the same IP address that initiated the session. This will at least detect many session hijacking techniques. Always have timeouts for cookies, sessions, and so on. The shorter, the better—but, of course, it is important to keep user satisfaction in mind.

HTTP Strict-Transport-Security (HSTS) can also help mitigate session hijacking attacks. HSTS is a server setting that requires browsers to connect with HTTPS rather than HTTP. This makes all traffic encrypted. HTTP Public Key Pinning (HPKP) allows a web client to associate a specific public key with a specific server, so it is harder for an attacker to spoof a legitimate web server.

Always use secure protocols. Table 6.1 summarizes them.

TABLE 6.1 **Secure Protocol Replacement**

Insecure Protocol	Secure Replacement
HTTP	HTTPS
Telnet, rlogin	SSH
Any TCP/IP traffic	Encrypt with a VPN
FTP	SFTP or FTPS

ExamAlert

Objective For the CEH exam, make certain you are very familiar with all of these secure protocols.

Cram Quiz

Answer these questions. The answers follow the last question. If you cannot answer these questions correctly, consider reading this section again until you can.

1. John is logged into his company web portal using a secure session. However, he is simultaneously logged into a site that he did not realize has been compromised. What attack might John be vulnerable to?
   - ❍ **A.** Session fixation
   - ❍ **B.** Man-in-the-middle
   - ❍ **C.** Cross-site scripting
   - ❍ **D.** Cross-site request forgery

2. What is the key aspect of RST hijacking?
   - ❍ **A.** Intercepting RST packets
   - ❍ **B.** Spoofing RST packets to pretend to be the client
   - ❍ **C.** Spoofing RST packets from the client to reset the session
   - ❍ **D.** Blocking RST packets to force the session to stay active

3. What is the basis of a CRIME attack?
   - ❍ **A.** Flaws in TLS compression
   - ❍ **B.** Flaws in gzip compression
   - ❍ **C.** Flaws in TLS authentication nonces
   - ❍ **D.** Flaws in cryptographic key generation

Answers

1. **D.** This is a very good description of cross-site request forgery.
2. **C.** Causing the session to reset, making it seem like the client sent the reset, can allow the attacker to attempt to hijack the session.
3. **A.** CRIME (Compression Ratio Info-Leak Made Easy) is an attack that targets flaws in TLS compression. The compression used in earlier versions of TLS was flawed and could lead to data leaks.

What Next?

If you want more practice on this chapter's exam objectives before you move on, remember that you can access all of the Cram Quiz questions on the book web page. The next chapter covers specific methods for avoiding security measures.

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