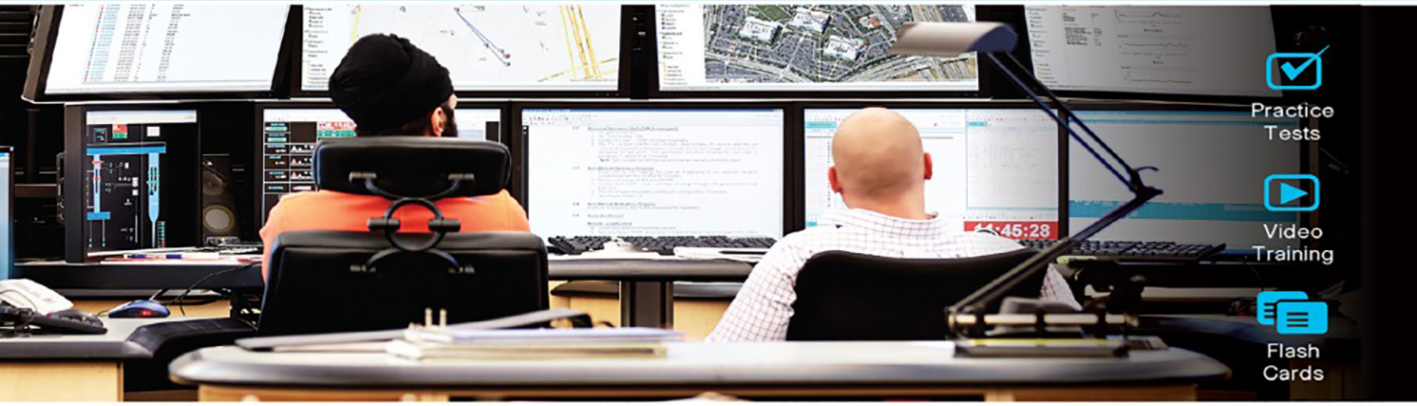

Study
Planner

Review
Exercises

Official Cert Guide

Advance your IT career with hands-on learning

Cisco CyberOps Associate

CBROPS 200-201

ciscopress.com

Omar Santos

Cisco CyberOps Associate

CBROPS 200-201

Official Cert Guide

OMAR SANTOS

Cisco Press

Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

Omar Santos

Published by:
Cisco Press
Hoboken, NJ

ScoutAutomatedPrintCode

Library of Congress Control Number: 2020944691

ISBN-13: 978-0-13-680783-4

ISBN-10: 0-13-680783-6

Warning and Disclaimer

This book is designed to provide information about the Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS 200-201) exam. 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 is provided on an "as is" basis. The author, Cisco Press, and Cisco Systems, Inc. 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 discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., 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.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book, or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Editor-in-Chief: Mark Taub

Alliances Manager, Cisco Press: Arezou Gol

Director, ITP Product Management: Brett Bartow

Executive Editor: James Manly

Managing Editor: Sandra Schroeder

Development Editor: Christopher A. Cleveland

Senior Project Editor: Tonya Simpson

Copy Editor: Chuck Hutchinson

Technical Editor: John Stuppi

Editorial Assistant: Cindy Teeters

Cover Designer: Chuti Prasertsith

Composition: codeMantra

Indexer: Timothy Wright

Proofreader: Donna E. Mulder

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

About the Author

Omar Santos is an active member of the security community, where he leads several industrywide initiatives. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of the critical infrastructure. Omar is the chair of the OASIS Common Security Advisory Framework (CSAF) technical committee, the co-chair of the Forum of Incident Response and Security Teams (FIRST) Open Source Security working group, and the co-lead of the DEF CON Red Team Village.

Omar is the author of more than 20 books and video courses as well as numerous white papers, articles, and security configuration guidelines and best practices. Omar is a principal engineer of the Cisco Product Security Incident Response Team (PSIRT), where he mentors and leads engineers and incident managers during the investigation and resolution of security vulnerabilities.

Omar has been quoted by numerous media outlets, such as TheRegister, Wired, ZDNet, ThreatPost, CyberScoop, TechCrunch, Fortune Magazine, Ars Technica, and more. You can follow Omar on Twitter @santosomar.

About the Technical Reviewer

John Stuppi, CCIE No. 11154, is a technical leader in the Customer Experience Security Programs (CXSP) organization at Cisco, where he consults Cisco customers on protecting their networks against existing and emerging cybersecurity threats, risks, and vulnerabilities. Current projects include working with newly acquired entities to integrate them into the Cisco PSIRT Vulnerability Management processes. John has presented multiple times on various network security topics at Cisco Live, Black Hat, as well as other customer-facing cybersecurity conferences. John is also the co-author of the *Official Certification Guide for CCNA Security 210-260* published by Cisco Press. Additionally, John has contributed to the Cisco Security Portal through the publication of white papers, security blog posts, and cyber risk report articles. Prior to joining Cisco, John worked as a network engineer for JPMorgan and then as a network security engineer at Time, Inc., with both positions based in New York City. John is also a CISSP (No. 25525) and holds AWS Cloud Practitioner and Information Systems Security (INFOSEC) Professional Certifications. In addition, John has a BSEE from Lehigh University and an MBA from Rutgers University. John lives in Ocean Township, New Jersey (down on the “Jersey Shore”), with his wife, two kids, and his dog.

Dedication

I would like to dedicate this book to my lovely wife, Jeannette, and my two beautiful children, Hannah and Derek, who have inspired and supported me throughout the development of this book.

Acknowledgments

I would like to thank the technical editor and my good friend, John Stuppi, for his time and technical expertise.

I would like to thank the Cisco Press team, especially James Manly and Christopher Cleveland, for their patience, guidance, and consideration.

Finally, I would like to thank Cisco and the Cisco Product Security Incident Response Team (PSIRT), Security Research, and Operations for enabling me to constantly learn and achieve many goals throughout all these years.

Contents at a Glance

Reader Services

In addition to the features in each of the core chapters, this book has additional study resources on the companion website, including the following:

Practice exams: The companion website contains an exam engine that enables you to review practice exam questions. Use these to prepare with a sample exam and to pinpoint topics where you need more study.

Interactive exercises and quizzes: The companion website contains hands-on exercises and interactive quizzes so that you can test your knowledge on the spot.

Glossary quizzes: The companion website contains interactive quizzes that enable you to test yourself on every glossary term in the book.

The companion website contains 30 minutes of unique test-prep video training.

To access this additional content, simply register your product. To start the registration process, go to www.ciscopress.com/register and log in or create an account.* Enter the product ISBN 9780136807834 and click Submit. After the process is complete, you will find any available bonus content under Registered Products.

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

Contents

Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the IOS Command Reference. The Command Reference describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS) exam is a 120-minute exam that includes 95 to 105 questions. This exam and curriculum are designed to prepare the cybersecurity analysts of the future! The CyberOps Associate certification provides a path to prepare individuals pursuing a cybersecurity career and associate-level job roles in security operations centers (SOCs). The exam covers the fundamentals you need to prevent, detect, analyze, and respond to cybersecurity incidents.

TIP You can review the exam blueprint from the Cisco website at https://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/200-201-cbrops.html.

This book gives you the foundation and covers the topics necessary to start your CyberOps Associate certification journey.

The Cisco CyberOps Associate Certification

The Cisco CyberOps Associate certification is one of the industry's most respected certifications. There are no formal prerequisites for the CyberOps Associate certification. In other words, you do not have to pass any other exams or certifications to take the 200-201 CBROPS exam. On the other hand, you must have a good understanding of basic networking and IT concepts.

Cisco considers ideal candidates to be those who possess the following:

- Knowledge of fundamental security concepts
- An understanding of security monitoring
- An understanding of host-based and network intrusion analysis
- An understanding of security policies and procedures related to incident response and digital forensics

The Exam Objectives (Domains)

The Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS 200-201) exam is broken down into five major domains. The contents of this book cover each of the domains and the subtopics included in them, as illustrated in the following descriptions.

The following table breaks down each of the domains represented in the exam.

Domain	Percentage of Representation in Exam
1: Security Concepts	20%
2: Security Monitoring	25%
3: Host-based Analysis	20%
4: Network Intrusion Analysis	20%
5: Security Policies and Procedures	15%
	Total 100%

Here are the details of each domain:

Domain 1: Security Concepts: This domain is covered in Chapters 1, 2, 3, and 4.

1.1 Describe the CIA triad

1.2 Compare security deployments

1.2.a Network, endpoint, and application security systems

1.2.b Agentless and agent-based protections

1.2.c Legacy antivirus and antimalware

1.2.d SIEM, SOAR, and log management

1.3 Describe security terms

1.3.a Threat intelligence (TI)

1.3.b Threat hunting

1.3.c Malware analysis

1.3.d Threat actor

1.3.e Run book automation (RBA)

1.3.f Reverse engineering

1.3.g Sliding window anomaly detection

1.3.h Principle of least privilege

1.3.i Zero trust

1.3.j Threat intelligence platform (TIP)

1.4 Compare security concepts

1.4.a Risk (risk scoring/risk weighting, risk reduction, risk assessment)

1.4.b Threat

1.4.c Vulnerability

1.4.d Exploit

- 1.5 Describe the principles of the defense-in-depth strategy
- 1.6 Compare access control models
  - 1.6.a Discretionary access control
  - 1.6.b Mandatory access control
  - 1.6.c Nondiscretionary access control
  - 1.6.d Authentication, authorization, accounting
  - 1.6.e Rule-based access control
  - 1.6.f Time-based access control
  - 1.6.g Role-based access control
- 1.7 Describe terms as defined in CVSS
  - 1.7.a Attack vector
  - 1.7.b Attack complexity
  - 1.7.c Privileges required
  - 1.7.d User interaction
  - 1.7.e Scope
- 1.8 Identify the challenges of data visibility (network, host, and cloud) in detection
- 1.9 Identify potential data loss from provided traffic profiles
- 1.10 Interpret the 5-tuple approach to isolate a compromised host in a grouped set of logs
- 1.11 Compare rule-based detection vs. behavioral and statistical detection

Domain 2: Security Monitoring: This domain is covered primarily in Chapters 5, 7, 10, 12, 14, and 15.

- 2.1 Compare attack surface and vulnerability
- 2.2 Identify the types of data provided by these technologies
  - 2.2.a TCP dump
  - 2.2.b NetFlow
  - 2.2.c Next-gen firewall
  - 2.2.d Traditional stateful firewall
  - 2.2.e Application visibility and control
  - 2.2.f Web content filtering
  - 2.2.g Email content filtering

2.3 Describe the impact of these technologies on data visibility

2.3.a Access control list

2.3.b NAT/PAT

2.3.c Tunneling

2.3.d TOR

2.3.e Encryption

2.3.f P2P

2.3.g Encapsulation

2.3.h Load balancing

2.4 Describe the uses of these data types in security monitoring

2.4.a Full packet capture

2.4.b Session data

2.4.c Transaction data

2.4.d Statistical data

2.4.e Metadata

2.4.f Alert data

2.5 Describe network attacks, such as protocol-based, denial of service, distributed denial of service, and man-in-the-middle

2.6 Describe web application attacks, such as SQL injection, command injections, and cross-site scripting

2.7 Describe social engineering attacks

2.8 Describe endpoint-based attacks, such as buffer overflows, command and control (C2), malware, and ransomware

2.9 Describe evasion and obfuscation techniques, such as tunneling, encryption, and proxies

2.10 Describe the impact of certificates on security (includes PKI, public/private crossing the network, asymmetric/symmetric)

2.11 Identify the certificate components in a given scenario

2.11.a Cipher-suite

2.11.b X.509 certificates

2.11.c Key exchange

2.11.d Protocol version

2.11.e PKCS

Domain 3: Host-based Analysis: This domain is covered primarily in Chapter 11.

3.1 Describe the functionality of these endpoint technologies in regard to security monitoring

3.1.a Host-based intrusion detection

3.1.b Antimalware and antivirus

3.1.c Host-based firewall

3.1.d Application-level whitelisting/blacklisting

3.1.e Systems-based sandboxing (such as Chrome, Java, Adobe Reader)

3.2 Identify components of an operating system (such as Windows and Linux) in a given scenario

3.3 Describe the role of attribution in an investigation

3.3.a Assets

3.3.b Threat actor

3.3.c Indicators of compromise

3.3.d Indicators of attack

3.3.e Chain of custody

3.4 Identify type of evidence used based on provided logs

3.4.a Best evidence

3.4.b Corroborative evidence

3.4.c Indirect evidence

3.5 Compare tampered and untampered disk image

3.6 Interpret operating system, application, or command line logs to identify an event

3.7 Interpret the output report of a malware analysis tool (such as a detonation chamber or sandbox)

3.7.a Hashes

3.7.b URLs

3.7.c Systems, events, and networking

Domain 4: Network Intrusion Analysis: This domain is covered primarily in Chapters 10, 13, and 15.

4.1 Map the provided events to source technologies

4.1.a IDS/IPS

4.1.b Firewall

- 4.1.c Network application control
- 4.1.d Proxy logs
- 4.1.e Antivirus
- 4.1.f Transaction data (NetFlow)

4.2 Compare impact and no impact for these items

- 4.2.a False positive
- 4.2.b False negative
- 4.2.c True positive
- 4.2.d True negative
- 4.2.e Benign

4.3 Compare deep packet inspection with packet filtering and stateful firewall operation

4.4 Compare inline traffic interrogation and taps or traffic monitoring

4.5 Compare the characteristics of data obtained from taps or traffic monitoring and transactional data (NetFlow) in the analysis of network traffic

4.6 Extract files from a TCP stream when given a PCAP file and Wireshark

4.7 Identify key elements in an intrusion from a given PCAP file

- 4.7.a Source address
- 4.7.b Destination address
- 4.7.c Source port
- 4.7.d Destination port
- 4.7.e Protocols
- 4.7.f Payloads

4.8 Interpret the fields in protocol headers as related to intrusion analysis

- 4.8.a Ethernet frame
- 4.8.b IPv4
- 4.8.c IPv6
- 4.8.d TCP
- 4.8.e UDP
- 4.8.f ICMP
- 4.8.g DNS
- 4.8.h SMTP/POP3/IMAP

- 4.8.i HTTP/HTTPS/HTTP2
- 4.8.j ARP

4.9 Interpret common artifact elements from an event to identify an alert

- 4.9.a IP address (source/destination)
- 4.9.b Client and server port identity
- 4.9.c Process (file or registry)
- 4.9.d System (API calls)
- 4.9.e Hashes
- 4.9.f URI/URL

4.10 Interpret basic regular expressions

Domain 5: Endpoint Protection and Detection: This domain is covered primarily in Chapters 7, 8, 9, 14, and 15.

5.1 Describe management concepts

- 5.1.a Asset management
- 5.1.b Configuration management
- 5.1.c Mobile device management
- 5.1.d Patch management
- 5.1.e Vulnerability management

5.2 Describe the elements in an incident response plan as stated in NIST.SP800-61

5.3 Apply the incident handling process (such as NIST.SP800-61) to an event

5.4 Map elements to these steps of analysis based on the NIST.SP800-61

- 5.4.a Preparation
- 5.4.b Detection and analysis
- 5.4.c Containment, eradication, and recovery
- 5.4.d Post-incident analysis (lessons learned)

5.5 Map the organization stakeholders against the NIST IR categories (CMMC, NIST.SP800-61)

- 5.5.a Preparation
- 5.5.b Detection and analysis

- 5.5.c Containment, eradication, and recovery
- 5.5.d Post-incident analysis (lessons learned)

5.6 Describe concepts as documented in NIST.SP800-86

- 5.6.a Evidence collection order
- 5.6.b Data integrity
- 5.6.c Data preservation
- 5.6.d Volatile data collection

5.7 Identify these elements used for network profiling

- 5.7.a Total throughput
- 5.7.b Session duration
- 5.7.c Ports used
- 5.7.d Critical asset address space

5.8 Identify these elements used for server profiling

- 5.8.a Listening ports
- 5.8.b Logged in users/service accounts
- 5.8.c Running processes
- 5.8.d Running tasks
- 5.8.e Applications

5.9 Identify protected data in a network

- 5.9.a PII
- 5.9.b PSI
- 5.9.c PHI
- 5.9.d Intellectual property

5.10 Classify intrusion events into categories as defined by security models, such as Cyber Kill Chain Model and Diamond Model of Intrusion

5.11 Describe the relationship of SOC metrics to scope analysis (time to detect, time to contain, time to respond, time to control)

Steps to Pass the 200-201 CBROPS Exam

There are no prerequisites for the 200-201 CBROPS exam; however, students must have an understanding of networking and cybersecurity concepts.

Signing Up for the Exam

The steps required to sign up for the 200-201 CBROPS exam are as follows:

1. Create an account at https://home.pearsonvue.com/cisco.
2. Complete the Examination Agreement, attesting to the truth of your assertions regarding professional experience and legally committing to the adherence of the testing policies.
3. Submit the examination fee.

Facts About the Exam

The exam is a computer-based test. The exam consists of multiple-choice questions only. You must bring a government-issued identification card. No other forms of ID will be accepted.

TIP Refer to the Cisco Certification site at https://cisco.com/go/certifications for more information regarding this, and other, Cisco certifications.

About the Cisco CyberOps Associate CBROPS 200-201 Official Cert Guide

This book covers the topic areas of the 200-201 CBROPS exam and uses a number of features to help you understand the topics and prepare for the exam.

Objectives and Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. This book does not try to help you pass the exam only by memorization; it seeks to help you truly learn and understand the topics. This book is designed to help you pass the Implementing and Understanding Cisco Cybersecurity Operations Fundamentals (200-201 CBROPS) exam by using the following methods:

- Helping you discover which exam topics you have not mastered
- Providing explanations and information to fill in your knowledge gaps
- Supplying exercises 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 companion website

Book Features

To help you customize your study time using this book, the core chapters have several features that help you make the best use of your time:

- **Foundation Topics:** These are the core sections of each chapter. They explain the concepts for the topics in that chapter.
- **Exam Preparation Tasks:** After the "Foundation Topics" section of each chapter, the "Exam Preparation Tasks" section lists a series of study activities that you should do at the end of the chapter:
  - **Review All Key Topics:** The Key Topic icon appears next to the most important items in the "Foundation Topics" section of the chapter. The Review All Key Topics activity lists the key topics from the chapter, along with their page numbers. Although the contents of the entire chapter could be on the exam, you should definitely know the information listed in each key topic, so you should review these.
  - **Define Key Terms:** Although the Understanding Cisco Cybersecurity Operations Fundamentals (200-201 CBROPS) exam may be unlikely to ask a question such as "Define this term," the exam does require that you learn and know a lot of cybersecurity terminology. This section lists the most important terms from the chapter, asking you to write a short definition and compare your answer to the glossary at the end of the book.
  - **Review Questions:** Confirm that you understand the content you just covered by answering these questions and reading the answer explanations.
- **Web-Based Practice Exam:** The companion website includes the Pearson Cert Practice Test engine, which allows you to take practice exam questions. Use it to prepare with a sample exam and to pinpoint topics where you need more study.

How This Book Is Organized

This book contains 15 core chapters—Chapters 1 through 15. Chapter 16 includes preparation tips and suggestions for how to approach the exam. Each core chapter covers a subset of the topics on the Understanding Cisco Cybersecurity Operations Fundamentals (200-201 CBROPS) exam. The core chapters map to the Cisco CyberOps Associate topic areas and cover the concepts and technologies you will encounter on the exam.

The Companion Website for Online Content Review

All the electronic review elements, as well as other electronic components of the book, exist on this book's companion website.

To access the companion website, which gives you access to the electronic content with this book, start by establishing a login at www.ciscopress.com and registering your book.

To do so, simply go to www.ciscopress.com/register and enter the ISBN of the print book: 9780136807834. After you have registered your book, go to your account page and click the **Registered Products** tab. From there, click the **Access Bonus Content** link to get access to the book's companion website.

Note that if you buy the *Premium Edition eBook and Practice Test* version of this book from Cisco Press, your book will automatically be registered on your account page. Simply go to your account page, click the **Registered Products** tab, and select **Access Bonus Content** to access the book's companion website.

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.

How to Access the Pearson Test Prep (PTP) App

You have two options for installing and using the Pearson Test Prep application: a web app and a desktop app. To use the Pearson Test Prep application, start by finding the registration code that comes with the book. You can find the code in these ways:

- **Print book:** Look in the cardboard sleeve in the back of the book for a piece of paper with your book's unique PTP code.
- **Premium Edition:** If you purchase the *Premium Edition eBook and Practice Test* directly from the Cisco Press website, the code will be populated on your account page after purchase. Just log in at www.ciscopress.com, click **account** to see details of your account, and click the **digital purchases** tab.
- **Amazon Kindle:** For those who purchased a Kindle edition from Amazon, the access code will be supplied directly from Amazon.
- **Other bookseller e-books:** Note that if you purchase an e-book version from any other source, the practice test is not included because other vendors to date have not chosen to provide the required unique access code.

NOTE Do not lose the activation code because it is the only means with which you can access the QA content with the book.

Once you have the access code, to find instructions about both the PTP web app and the desktop app, follow these steps:

Step 1. Open this book's companion website, as was shown earlier in this Introduction under the heading "The Companion Website for Online Content Review."

Step 2. Click the **Practice Exams** button.

Step 3. Follow the instructions listed there both for installing the desktop app and for using the web app.

Note that if you want to use the web app only at this point, just navigate to www.pearsontestprep.com, establish a free login if you do not already have one, and register this book's practice tests using the registration code you just found. The process should take only a couple of minutes.

NOTE Amazon e-book (Kindle) customers: It is easy to miss Amazon's email that lists your PTP access code. Soon after you purchase the Kindle e-book, Amazon should send an email. However, the email uses very generic text and makes no specific mention of PTP or practice exams. To find your code, read every email from Amazon after you purchase the book. Also, do the usual checks for ensuring your email arrives, such as checking your spam folder.

NOTE Other e-book customers: As of the time of publication, only the publisher and Amazon supply PTP access codes when you purchase their e-book editions of this book.

Customizing Your Exams

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

- **Study mode:** Allows you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you would use first to assess your knowledge and identify information gaps.
- **Practice Exam mode:** Locks certain customization options, as it is presenting 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 do, so you should not use it if you are trying to 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 well as 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.

There are several other customizations you can make to your exam from the exam settings screen, such as the time of the exam, the number of questions served up, whether to randomize questions and answers, whether to show the number of correct answers for multiple-answer questions, and 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 while connected to the Internet, it checks if there are any updates to your exam data and automatically downloads any changes that were made since the last time you used the software.

Sometimes, due to many factors, the exam data may not fully download when you activate your exam. If you find that figures or exhibits are missing, you may need to manually update your exams. To update a particular exam you have already activated and downloaded, simply click the **Tools** tab and click the **Update Products** button. Again, this is an issue only with the desktop Windows application.

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

Credits List

Figure 1-2: Screenshot of a Cisco security advisory © The MITRE Corporation

Figure 1-3: Screenshot of The National Vulnerability Database © National Institute of Standards and Technology

Figure 1-4: Screenshot of the Exploit Database © OffSec Services Limited

Figure 4-1: Screenshot of Shodan search engine results example © Shodan

Figure 5-5: Screenshot of Mac OS X System Roots © Apple, Inc

Figure 8-2: Screenshot of sample security events and confirmed incident © Bamm Visscher

Figure 8-9: Screenshot of logs from a Cisco switch in ELK © Wireshark

Figure 8-10: Screenshot of following in the TCP stream in Wireshark © Wireshark

Figure 8-13: Screenshot of example of security events in Sguil © Bamm Visscher

Figure 8-14: Screenshot of Kibana dashboard overview © 2020. Elasticsearch B.V.

Figure 8-15: Screenshot of NIDS alert count, categories, and classification statistics © 2020. Elasticsearch B.V.

Figure 8-16: Screenshot of NIDS alert severity, the top source and destination ports © 2020. Elasticsearch B.V.

Figure 8-17: Screenshot of the top source and destination IP addresses that generated NIDS alerts in Snort © 2020. Elasticsearch B.V.

Figure 8-18: Screenshot of ELK map visualization example © 2020. Elasticsearch B.V.

Figure 8-23: Screenshot of examples of a packet capture of an exploit against a Windows vulnerability © Microsoft 2019

Figure 9-1: Screenshot of acquiring a disk image using Guymager © Guymager

Figure 9-2: Screenshot of the CAINE distribution © CAINE

Figure 9-3: Screenshot of making a disk image with the dd Linux command © 2020 The Linux Foundation

Figure 9-5: Screenshot of the Ghidra reverse engineering platform © Ghidra

Figure 10-2: Screenshot of logs from a Cisco switch in ELK © 2020. Elasticsearch B.V.

Figure 10-3: Screenshot of security alert visualization in Kibana © 2020. Elasticsearch B.V.

Figure 10-4: Screenshot of NDIS alerts in Kibana © 2020. Elasticsearch B.V.

Figure 10-5: Screenshot of visualization of different NIDS alerts categories © 2020. Elasticsearch B.V.

Figure 11-1: Screenshot of Windows Task Manager © Microsoft 2019

Figure 11-2: Screenshot of running the tasklist command on the Windows command line © Microsoft 2019

Figure 11-3: Screenshot of using the ps -e command on a macOS system © Apple, Inc

Figure 11-5 Screenshot of Windows Task Manager showing applications by user © Microsoft 2019

Figure 11-6: Screenshot of macOS activity monitor © Apple Inc

Figure 11-12: Screenshot of Windows Registry Editor © Microsoft 2019

Figure 11-13: Screenshot of Windows computer showing the WMI service © Microsoft 2019

Figure 11-15: Screenshot of Windows Services Control Manager © Microsoft 2019

Figure 11-16: Screenshot of Windows Event Viewer example © Microsoft 2019

Figure 11-17: Screenshot of running the ps aux command © Microsoft 2019

Figure 11-21: Screenshot of Permissions Calculator online tool © Dan's Tools

Figure 11-23: Screenshot of NGINX access logs tool © Nginx, Inc

Chapter 13 quote, "VERIS is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner. The overall goal is to lay a foundation on which we can constructively and cooperatively learn from our experiences to better manage risk." VERIS OVERVIEW, http://veriscommunity.net/veris-overview.html

Figure 14-5: Screenshot of MITRE ATT&CK malware example © The MITRE Corporation

Figure 14-6: Screenshot of MITRE ATT&CK Navigator © The MITRE Corporation

Figure 14-7: Screenshot of adding metadata to the MITRE ATT&CK Navigator © The MITRE Corporation

Figure 14-11: Screenshot of querying for insecure protocol exposure in Shodan © Shodan

Figure 15-8: Screenshot of Mimikatz example in the MITRE ATT&CK Navigator © The MITRE Corporation

Figure 15-16: Screenshot of Mimikatz example in the MITRE ATT&CK Navigator © The MITRE Corporation

CHAPTER 12

Challenges in the Security Operations Center (SOC)

This chapter covers the following topics:

Security Monitoring Challenges in the SOC

Additional Evasion and Obfuscation Techniques

There are several security monitoring operational challenges, including encryption, Network Address Translation (NAT), time synchronization, Tor, and peer-to peer communications. This chapter covers these operational challenges in detail. Attackers try to abuse system and network vulnerabilities to accomplish something; however, there is another element that can make or break the success of the attack. Attackers need to be *stealthy* and be able to evade security techniques and technologies. Attackers must consider the amount of exposure an attack may cause as well as the expected countermeasures if the attack is noticed by the target's defense measures. They need to cover their tracks.

In this chapter, you learn how attackers obtain stealth access and the tricks used to negatively impact detection and forensic technologies.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz allows 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 12-1 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 12-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
Security Monitoring Challenges in the SOC	1–10
Additional Evasion and Obfuscation Techniques	11–20

1. Which of the following are benefits of encryption?
   - **a.** Malware communication
   - **b.** Privacy and confidentiality
   - **c.** Malware mitigation
   - **d.** Malware identification

2. Why can encryption be challenging to security monitoring?
   a. Encryption introduces latency.
   b. Encryption introduces additional processing requirements by the CPU.
   c. Encryption can be used by threat actors as a method of evasion and obfuscation, and security monitoring tools might not be able to inspect encrypted traffic.
   d. Encryption can be used by attackers to monitor VPN tunnels.
3. Network Address Translation (NAT) introduces challenges in the identification and attribution of endpoints in a security victim. The identification challenge applies to both the victim and the attack source. What tools are available to be able to correlate security monitoring events in environments where NAT is deployed?
   a. NetFlow
   b. Cisco Stealthwatch System
   c. Intrusion prevention systems (IPS)
   d. Encryption protocols
4. If the date and time are not synchronized among network and security devices, logs can become almost impossible to correlate. What protocol is recommended as a best practice to deploy to mitigate this issue?
   a. Network Address Translation
   b. Port Address Translation
   c. Network Time Protocol (NTP)
   d. Native Time Protocol (NTP)
5. What is a DNS tunnel?
   a. A type of VPN tunnel that uses DNS.
   b. A type of MPLS deployment that uses DNS.
   c. DNS was not created for tunneling, but a few tools have used it to encapsulate data in the payload of DNS packets.
   d. An encryption tunneling protocol that uses DNS's UDP port 53.
6. Which of the following are examples of DNS tunneling tools? (Select all that apply.)
   a. DeNiSe
   b. dns2tcp
   c. DNScapy
   d. DNStor
7. What is Tor?
   a. A blockchain protocol
   b. A hashing protocol
   c. A VPN tunnel client
   d. A free tool that enables its users to surf the Internet anonymously

8. What is a Tor exit node?
   a. The encrypted Tor network
   b. The last Tor node or the gateways where the Tor-encrypted traffic exits to the Internet
   c. The Tor node that performs encryption
   d. The Tor browser installed in your system to exit the Internet
9. What is a SQL injection vulnerability?
   a. An input validation vulnerability where an attacker can insert or inject a SQL query via the input data from the client to the application or database
   b. A type of vulnerability where an attacker can inject a new password to a SQL server or the client
   c. A type of DoS vulnerability that can cause a SQL server to crash
   d. A type of privilege escalation vulnerability aimed at SQL servers
10. Which of the following is a distributed architecture that partitions tasks or workloads between peers?
   a. Peer-to-peer networking
   b. P2P NetFlow
   c. Equal-cost load balancing
   d. None of these answers are correct.
11. Which of the following describes when the attacker sends traffic more slowly than normal, not exceeding thresholds inside the time windows the signatures use to correlate different packets together?
   a. Traffic insertion
   b. Protocol manipulation
   c. Traffic fragmentation
   d. Timing attack
12. Which of the following would give an IPS the most trouble?
   a. Jumbo packets
   b. Encryption
   c. Throughput
   d. Updates
13. In which type of attack does an IPS receive a lot of traffic/packets?
   a. Resource exhaustion
   b. DoS (denial of service)
   c. Smoke and mirrors
   d. Timing attack
14. Which of the following is *not* an example of traffic fragmentation?
   a. Modifying routing tables
   b. Modifying the TCP/IP in a way that is unexpected by security detection devices
   c. Modifying IP headers to cause fragments to overlap
   d. Segmenting TCP packets

15. What is the best defense for traffic fragmentation attacks?
    a. Deploying a passive security solution that monitors internal traffic for unusual traffic and traffic fragmentation
    b. Deploying a next-generation application layer firewall
    c. Configuring fragmentation limits on a security solution
    d. Deploying a proxy or inline security solution
16. Which of the following is a TCP-injection attack?
    a. Forging a TCP packet over an HTTPS session
    b. Replacing legitimate TCP traffic with forged TCP packets
    c. Adding a forged TCP packet to an existing TCP session
    d. Modifying the TCP/IP in a way that is unexpected by security detection
17. A traffic substitution and insertion attack does which of the following?
    a. Substitutes the traffic with data in a different format but with the same meaning
    b. Substitutes the payload with data in the same format but with a different meaning, providing a new payload
    c. Substitutes the payload with data in a different format but with the same meaning, not modifying the payload
    d. Substitutes the traffic with data in the same format but with a different meaning
18. Which of the following is *not* a defense against a traffic substitution and insertion attack?
    a. De-obfuscating Unicode
    b. Using Unicode instead of ASCII
    c. Adopting the format changes
    d. Properly processing extended characters
19. Which of the following is *not* a defense against a pivot attack?
    a. Content filtering
    b. Proper patch management
    c. Network segmentation
    d. Access control
20. Which security technology would be best for detecting a pivot attack?
    a. Virtual private network (VPN)
    b. Host-based antivirus
    c. NetFlow
    d. Application layer firewalls

Foundation Topics

Security Monitoring Challenges in the SOC

Analysts in the security operations center (SOC) try to have complete visibility into what's happening in a network. However, that task is easier said than done. There are several challenges that can lead to false negatives (where you cannot detect malicious or abnormal activity in the network and systems). The following sections highlight some of these challenges.

Security Monitoring and Encryption

Encryption has great benefits for security and privacy, but the world of incident response and forensics can present several challenges. Even law enforcement agencies have been fascinated with the dual-use nature of encryption. When protecting information and communications, encryption has numerous benefits for everyone from governments and militaries to corporations and individuals.

Key Topic

On the other hand, those same mechanisms can be used by threat actors as a method of evasion and obfuscation. Historically, even governments have tried to regulate the use and exportation of encryption technologies. A good example is the Wassenaar Arrangement, which is a multinational agreement with the goal of regulating the export of technologies like encryption.

Other examples include events around law enforcement agencies such as the U.S. Federal Bureau of Investigation (FBI) trying to force vendors to leave certain investigative techniques in their software and devices. Some folks have bought into the idea of "encrypt everything." However, encrypting everything would have very serious consequences, not only for law enforcement agencies, but also for incident response professionals. Something to remember about the concept of "encrypt everything" is that the deployment of end-to-end encryption is difficult and can leave unencrypted data at risk of attack.

Many security products (including next-generation IPSs and next-generation firewalls) can intercept, decrypt, inspect, and re-encrypt or even ignore encrypted traffic payloads. Some people consider this a man-in-the-middle (MITM) matter and have many privacy concerns. On the other hand, you can still use metadata from network traffic and other security event sources to investigate and solve security issues. You can obtain a lot of good information by leveraging NetFlow, firewall logs, web proxy logs, user authentication information, and even passive DNS (pDNS) data. In some cases, the combination of these logs can make the encrypted contents of malware payloads and other traffic irrelevant. Of course, this is as long as you can detect their traffic patterns to be able to remediate an incident.

It is a fact that you need to deal with encrypted data, whether in transit or "at rest" on an endpoint or server. If you deploy web proxies, you'll need to assess the feasibility in your environment of MITM secure HTTP connections.

TIP It is important to recognize that from a security monitoring perspective, it's technically possible to monitor some encrypted communications. However, from a policy perspective, it's an especially different task depending on your geographical location and local laws around privacy. Cisco has a technology that allows you to detect malicious activity even if the communication is being encrypted. That technology is called Encrypted Traffic Analytics (ETA), and it is integrated into the Stealthwatch and Cognitive Security solution, as shown in Figure 12-1.

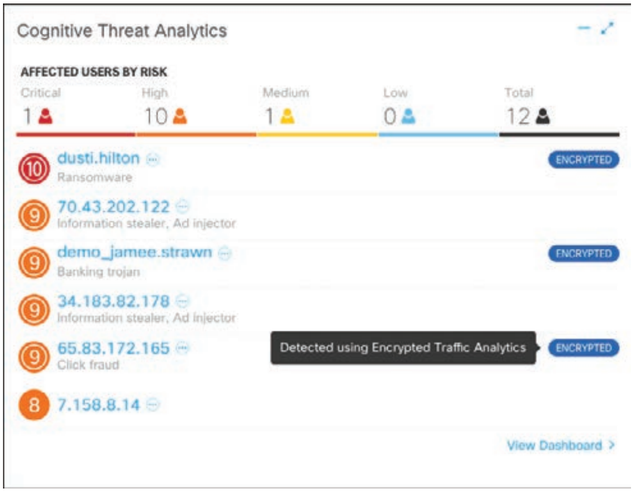

Figure 12-1 *Encrypted Traffic Analytics*

Security Monitoring and Network Address Translation

In Chapter 10, "Network Infrastructure Device Telemetry and Analysis," you learned that Layer 3 devices, such as routers and firewalls, can perform Network Address Translation (NAT). The router or firewall "translates" the "internal" host's private (or real) IP addresses to a publicly routable (or mapped) address. By using NAT, the firewall hides the internal private addresses from the unprotected network and exposes only its own address or public range. This enables a network professional to use any IP address space as the internal network. A best practice is to use the address spaces that are reserved for private use (see RFC 1918, "Address Allocation for Private Internets").

NOTE Cisco uses the terminology of *real* and *mapped* IP addresses when describing NAT. The real IP address is the address that is configured on the host before it is translated. The mapped IP address is the address that the real address is translated to.

Static NAT allows connections to be initiated bidirectionally, meaning both to the host and from the host.

Key Topic

NAT can present a challenge when you're performing security monitoring and analyzing logs, NetFlow, and other data, because device IP addresses can be seen in the logs as the "translated" IP address versus the "real" IP address. In the case of Port Address Translation (PAT), this could become even more problematic because many different hosts can be translated to a single address, making the correlation almost impossible to achieve.

Security products, such as the Cisco Stealthwatch system, provide features that can be used to correlate and "map" translated IP addresses with NetFlow. This feature in the Cisco Stealthwatch system is called *NAT stitching*. This accelerates incident response tasks and eases continuous security monitoring operations.

Security Monitoring and Event Correlation Time Synchronization

Server and endpoint logs, NetFlow, syslog data, and any other security monitoring data are useless if they show the wrong date and time. This is why as a best practice you should configure all network devices to use Network Time Protocol (NTP). Using NTP ensures that the correct time is set and all devices within the network are synchronized. Also, another best practice is to try to reduce the number of duplicate logs. This is why you have to think and plan ahead as to where exactly you will deploy NetFlow, how you will correlate it with other events (like syslog), and so on.

DNS Tunneling and Other Exfiltration Methods

Threat actors have been using many different nontraditional techniques to steal data from corporate networks without being detected. For example, they have been sending stolen credit card data, intellectual property, and confidential documents over DNS using tunneling. As you probably know, DNS is a protocol that enables systems to resolve domain names (for example, cisco.com) into IP addresses (for example, 72.163.4.161). DNS is not intended for a command channel or even tunneling. However, attackers have developed software that enables tunneling over DNS. These threat actors like to use protocols that traditionally are not designed for data transfer because they are less inspected in terms of security monitoring. Undetected DNS tunneling (otherwise known as *DNS exfiltration*) represents a significant risk to any organization.

In many cases, malware can use Base64 encoding to put sensitive data (such as credit card numbers, personal identifiable information [PII], and so on) in the payload of DNS packets to cyber criminals. The following are some examples of encoding methods that could be used by attackers:

- Base64 encoding
- Binary (8-bit) encoding
- NetBIOS encoding
- Hex encoding

Several utilities have been created to perform DNS tunneling (for the good and also for the bad). The following are a few examples:

- **DeNiSe:** This Python tool is used for tunneling TCP over DNS.
- **dns2tcp:** Written by Olivier Dembour and Nicolas Collignon in C, this tool supports KEY and TXT request types.
- **DNScapy:** Created by Pierre Bienaimé, this Python-based Scapy tool for packet generation even supports SSH tunneling over DNS, including a SOCKS proxy.
- **DNScat or DNScat-P:** This Java-based tool created by Tadeusz Pietraszek supports bidirectional communication through DNS.
- **DNScat (DNScat-B):** Written by Ron Bowes, this tool runs on Linux, Mac OS X, and Windows. DNScat encodes DNS requests in NetBIOS encoding or hex encoding.
- **Heyoka:** This tool, written in C, supports bidirectional tunneling for data exfiltration.

- **Iodine:** Written by Bjorn Andersson and Erik Ekman in C, this tool runs on Linux, Mac OS X, and Windows, and can even be ported to Android.
- **Nameserver Transfer Protocol (NSTX):** This tool creates IP tunnels using DNS.
- **OzymanDNS:** Written in Perl by Dan Kaminsky, this tool is used to set up an SSH tunnel over DNS or for file transfer. The requests are Base32 encoded, and responses are Base64-encoded TXT records.
- **psudp:** Developed by Kenton Born, this tool injects data into existing DNS requests by modifying the IP/UDP lengths.
- **Feederbot and Moto:** Attackers have used this malware using DNS to steal sensitive information from many organizations.

Some of these tools were not created with the intent of stealing data, but cyber criminals have used them for their own purposes.

The examples in Figure 12-2 and Figure 12-3 demonstrate how DNS tunneling can be achieved with the Iodine tool. Figure 12-2 shows the Iodine server listening for any connections from clients using DNS resolution for the domain h4cker.org.

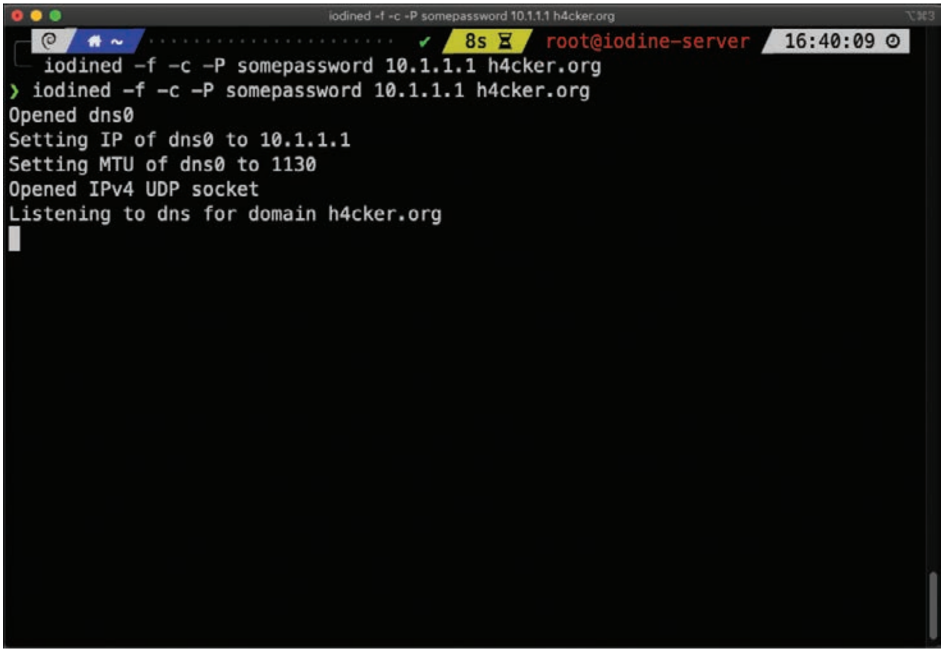

Figure 12-2 *Iodine DNS Tunneling Server*

Figure 12-3 shows the Iodine client (assume that this is a compromised system). The client successfully established a connection to the Iodine server. The 192.168.88.207 IP address is the address configured in the network interface card (NIC) of the server. The 10.1.1.1 is the IP address used by Iodine to communicate with the clients over the tunnel. In this example, the client IP address is 10.1.1.2, and the server tunnel IP address is 10.1.1.1. All data is now sent over the DNS tunnel, and the domain h4cker.org is used for DNS resolution.

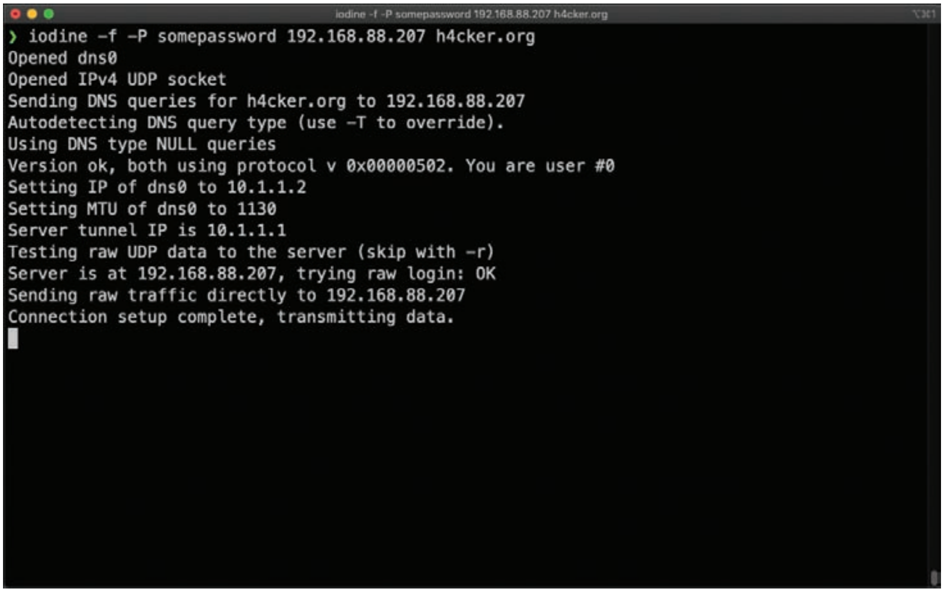

Figure 12-3 *Iodine DNS Tunneling Client*

Key Topic

Security Monitoring and Tor

Many people use tools such as Tor for privacy. Tor is a free tool that enables its users to surf the web anonymously. Tor works by routing IP traffic through a free, worldwide network consisting of thousands of Tor relays. Then it constantly changes the way it routes traffic to obscure a user's location from anyone monitoring the network.

NOTE Tor is an acronym of the software project's original name, "The Onion Router."

The use of Tor also makes security monitoring and incident response more difficult because it's hard to attribute and trace back the traffic to the user. Different types of malware are known to use Tor to cover their tracks.

This "onion routing" is accomplished by encrypting the application layer of a communication protocol stack that's nested just like the layers of an onion. The Tor client encrypts the data multiple times and sends it through a network or circuit that includes randomly selected Tor relays. Each of the relays decrypts a layer of the onion to reveal only the next relay so that the remaining encrypted data can be routed on to it.

Figure 12-4 shows the Tor browser. You can see the Tor circuit when the user accessed h4cker.org from the Tor browser. The packets first went to a host in the Netherlands, then to hosts in Norway and Germany, and finally to h4cker.org.

A Tor exit node is basically the last Tor node or the gateway where the Tor encrypted traffic exits to the Internet. A Tor exit node can be targeted to monitor Tor traffic. Many organizations block Tor exit nodes in their environment. The Tor project has a dynamic list of Tor exit nodes that makes this task a bit easier. This Tor exit node list can be downloaded from https://check.torproject.org/exit-addresses.

12

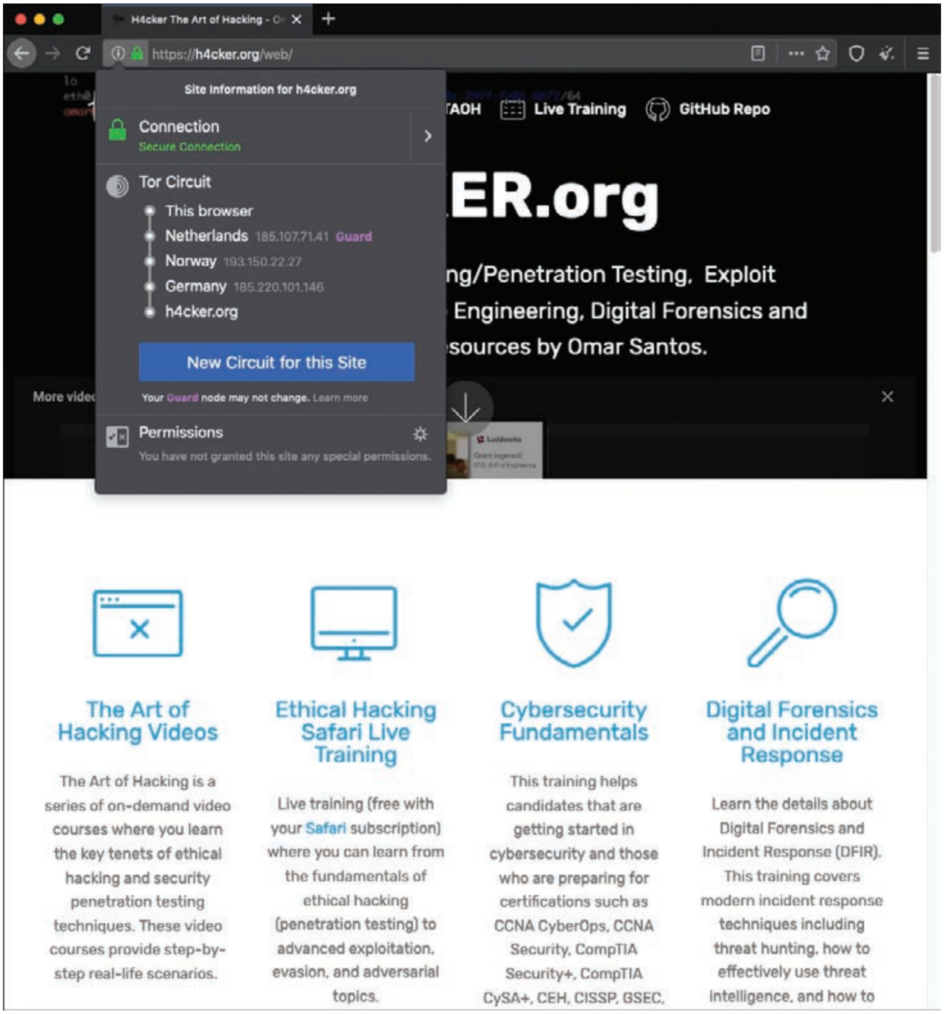

Figure 12-4 *The Tor Browser*

NOTE Security products such as the Cisco Next-Generation Firepower software provide the capability to dynamically learn and block Tor exit nodes.

Security Monitoring and Peer-to-Peer Communication

Key Topic

Peer-to-peer (P2P) communication involves a distributed architecture that divides tasks between participant computing peers. In a P2P network, the peers are equally privileged, which is why it's called a *peer-to-peer* network of nodes.

P2P participant computers or nodes reserve a chunk of their resources (such as CPU, memory, disk storage, and network bandwidth) so that other peers or participants can access those resources. This is all done without the need of a centralized server. In P2P networks, each peer can be both a supplier as well as a consumer of resources or data. A good example was the music-sharing application Napster back in the 1990s.

P2P networks have been used to share music, videos, stolen books, and other data; even legitimate multimedia applications such as Spotify use a peer-to-peer network along with streaming servers to stream audio and video to their clients. There's even an application called Peercoin (also known as PPCoin) that's a P2P crypto currency that utilizes both proof-of-stake and proof-of-work systems.

Universities such as MIT and Penn State have even created a project called LionShare, which is designed to share files among educational institutions globally.

From a security perspective, P2P systems introduce unique challenges. Malware has used P2P networks to communicate and also spread to victims. Many "free" or stolen music and movie files usually come with the surprise of malware. Additionally, like any other form of software, P2P applications are not immune to security vulnerabilities. This, of course, introduces risks for P2P software because it is more susceptible to remote exploits, due to the nature of the P2P network architecture.

Additional Evasion and Obfuscation Techniques

Attackers can use SSH to hide traffic, such as creating a reverse SSH tunnel from a breached system back to an external SSH server, hiding sensitive data as the traffic leaves the network. Figure 12-5 provides an example of how a typical SSH session functions.

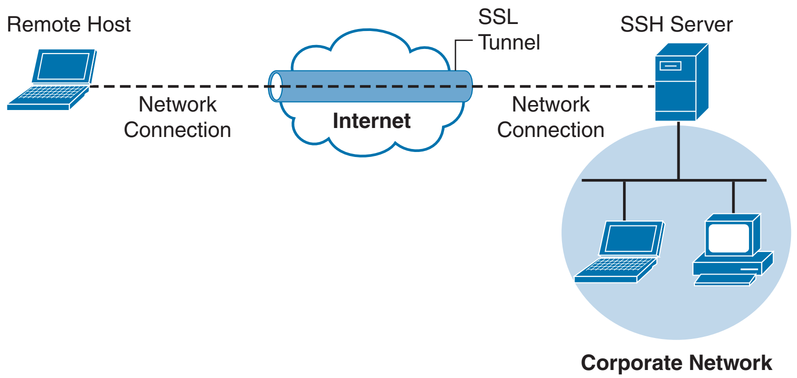

Figure 12-5 *SSH VPN Example*

You can use SSH tunnels over other tunnels such as VPNs, DNS tunnels, and so on. For instance, you can create a DNS tunnel and then have an SSH tunnel over it.

There are many use cases where an attacker breaches a network and launches some form of a VPN session. An example is using Hak5's LAN Turtle USB adapter, which can be configured to auto-launch a reverse SSH tunnel to a cloud storage server, essentially creating a cloud-accessible backdoor to a victim's network.

It is challenging for an administrator to identify the LAN Turtle because it sits on a trusted system and does not require an IP address of its own to provide the reverse-encrypted tunnel out of the network.

Figure 12-6 shows an example of a LAN Turtle plugged into a server, providing an encrypted tunnel to an attacker's remote server. This would represent a physical attack that leads to a backdoor for external malicious parties to access.

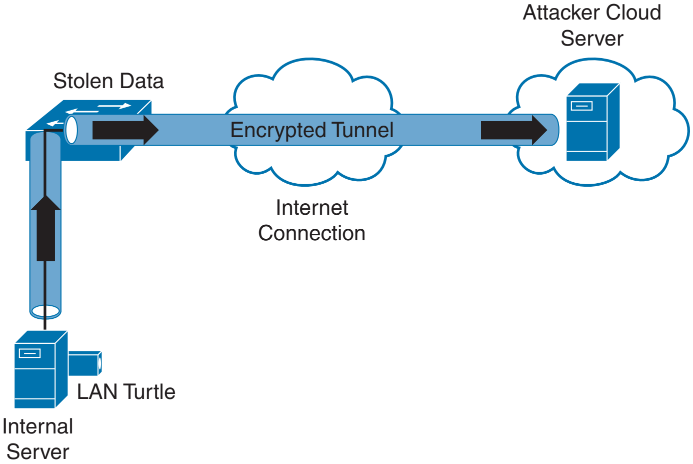

Figure 12-6 *LAN Turtle SSH Tunnel*

The LAN Turtle is just one example of the many tools available that can be planted on a network to create an unauthorized backdoor. The Packet Squirrel is another device that can be deployed to give an attacker remote access to a target network. All of these tools are available to the public on websites like hak5.org.

Another encryption concept is hiding the actual data. There are many techniques for doing this, such as enterprise file encryption technologies that encrypt files and control access to opening them. An example is having a software agent installed on a server that specifies which files should be encrypted. When a file is removed that should be encrypted, it is tagged and encrypted, with access provided only to people within a specific authentication group. People within that group can use a host-based agent that auto-logs them in to the file, or they could be sent to an online portal to authenticate to gain access to the file.

The term *data at rest* means data that is placed on a storage medium. Data-at-rest security requirements typically refer to the ability to deny all access to stored data that is deemed sensitive and at risk of being exposed. Typically, this is done by encrypting data and later removing all methods to unencrypt the data. Examples include hard disk encryption where a hard drive is encrypted, making it impossible to clone. The same concept can be applied to file encryption technology, where the data owner can expire access to the file, meaning all users won't be able to unencrypt it.

Many attackers abuse encryption concepts such as file and protocol encryption to hide malicious code. An example would be an attack happening from a web server over SSL encryption to hide the attack from network intrusion detection technologies. This works because a network intrusion detection tool uses signatures to identify a threat, which is useless if the traffic being evaluated is encrypted. Another example would be encoding a malicious file with a bunch of pointless text, with the goal of confusing an antivirus application. Antivirus applications also use signatures to detect threats, so adding additional text to malicious code could possibly change the code enough to not be tied to a known attack when evaluated by a security tool.

The following list highlights several key encryption and tunneling concepts:

Key Topic

- A VPN is used to hide or encode something so the content is protected from unwanted parties.
- Encryption traffic can be used to bypass detection, such as by an intrusion prevention system (IPS).
- The two forms of remote-access VPNs are client based and clientless.
- A site-to-site VPN connects two or more networks.
- SSH connects a host to an SSH server and uses public-key cryptography to authenticate the remote computer and permit it to authenticate the user.
- File encryption technology protects files from unauthorized users.

Next, we look at exhausting resources to bypass detection and gain unauthorized access to systems and networks.

Resource Exhaustion

Resource exhaustion is a type of denial-of-service attack; however, it can also be used to evade detection by security defenses. A simple definition of *resource exhaustion* is "consuming the resources necessary to perform an action." An example of a denial-of-service attack tool that can exhaust the available resources of web applications and other systems is called Slowloris, which can be found at https://github.com/gkbrk/slowloris. This tool holds connections by sending partial HTTP requests to the website. The tool continues sending several hundred subsequent headers at regular intervals to keep sockets from closing, thus overwhelming the target's resources. This causes the website to be caught up with existing requests, thus delaying responses to legitimate traffic. Figure 12-7 shows the Slowloris tool being used against the h4cker.org website.

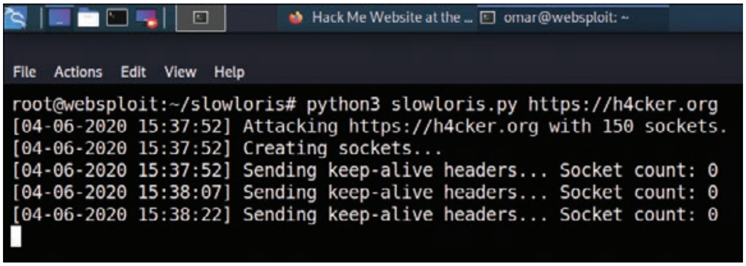

Figure 12-7 *Slowloris Attack Example*

When it comes to bypassing access-control security, resource exhaustion attacks can consume all processes to force a system to fail open, meaning to permit access to unauthorized systems and networks. This attack can be effective against access-control technologies that administrators typically configure to fail open if a service failure is detected. The same approach could be used to exhaust systems that have tracking capabilities, such as intrusion detection tools or other network sensors, causing a blackout period for an attacker to abuse without being recorded. Attackers will use resource exhaustion attacks against logging systems they identify during an attack, knowing many administrators do not have the skills or understanding to defend against resource exhaustion attacks and therefore will be unable to prevent the monitoring blackouts from occurring. This also prevents the evidence required for a forensic investigation from being collected, thus legally protecting the attacker from being incriminated by a future post-breach investigation. The most common example of a resource exhaustion attack involves sending a bunch of traffic directly at the IPS.

Defensive strategies should be implemented to prevent resource exhaustion attacks. The first defense layer, which involves having checks for unusual or unauthorized methods of requesting resources, is usually built in by the vendor. The idea is to recognize when an attack is being attempted and to deny the attacker further access for a specific amount of time so that the system resources can sustain the traffic without impacting service. One simple method to enforce this effect involves using *throttling*, which is limiting the amount of service a specific user or group can consume, thus enforcing an acceptable amount of resource consumption. Sometimes these features need to be enabled before they can be enforced, so best practice is to validate whether resource exhaustion defenses exist within a security solution.

The list that follows highlights the key resource exhaustion concepts:

Key Topic

- Resource exhaustion refers to consuming the resources necessary to perform an action.
- Attackers use resource exhaustion to bypass access control and security detection capabilities. A common example is sending a ton of traffic at an IPS.
- Resource exhaustion can be used to render logging unusable.
- Throttling is a method to prevent resource exhaustion by limiting the number of processes that can be consumed at one time.

Now let's look at dicing up and modifying the traffic to bypass detection. This is known as *traffic fragmentation*.

Traffic Fragmentation

Network technologies expect traffic to move in a certain way. This is known as the *TCP/IP suite*. Understanding how this works can help you identify when something is operating in an unusual manner. Fragmenting traffic is a method of avoiding detection by breaking up a single Internet Protocol (IP) datagram into multiple, smaller-size packets. The goal is to abuse the fragmentation protocol within IP by creating a situation where the attacker's intended traffic is ignored or let through as trusted traffic. The good news is that most modern intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) are aware of this attack and can prevent it. Best practice is to verify that your version of IDS/IPS has traffic fragmentation detection capabilities.

IPS products should be able to properly reassemble packets to evaluate whether there is malicious intent. This includes understanding the proper order of the packets. Unfortunately, attackers have various techniques they can use to confuse an IPS solution during its reassembly process. An example of this involves using a TCP segmentation and reordering attack that is designed to confuse the detection tool by sending traffic in an uninspected method with the hope it can't properly reassemble the traffic and identify it as being malicious. Security devices that can't perform traffic reassembly will automatically fail to prevent this attack. Some security devices will fail when the attacker reorders or fragments the traffic with enough tweaks to accomplish the bypass.

Another example of a fragmentation attack involves using overlapping fragments. This attack works by setting the offset values in the IP header so that they do not match up, thus causing one fragment to overlap another. The confusion could cause the detection tool to ignore some traffic, letting malicious traffic slip through.

Best practice for avoiding traffic fragmentation attacks is verifying with your security solution provider that the solution is capable of detecting traffic fragmentation. Solutions that operate in full proxy type modes are not susceptible to this type of attack (for example, content filters and inline security devices).

The following list highlights the key traffic fragmentation concepts:

Key Topic

- Traffic fragmentation attacks modify the TCP/IP traffic in a way that is unexpected by security detection devices; the goal is to confuse the detection functions.
- Using TCP segmentation and reordering attacks is one way to modify traffic to bypass detection.
- Causing fragments to overlap by modifying IP headers is another type of traffic fragmentation attack.
- Proxies and inline security devices can help prevent traffic fragmentation attacks.

Like with TCP/IP traffic, protocols can also be modified to bypass security devices. Let's look at how this works.

Protocol-Level Misinterpretation

A *protocol* is a set of rules or data structures that governs how computers or other network devices exchange information over a network. Protocols can be manipulated to confuse security devices from properly evaluating traffic since many devices and applications expect network communication to follow the industry-defined rules when a protocol is used. The key is understanding how the protocol should work and attempting to see if the developer of the receiving system defined defenses such as limitations on what is accepted, a method to validate what is received, and so on. The second key piece is identifying what happens when a receiving system encounters something it doesn't understand (meaning seeing the outcome of a failure). A security device misinterpreting the end-to-end meaning of network protocols could cause traffic to be ignored, dropped, or delayed, all of which could be used to an attacker's advantage.

Another example of a protocol-level misinterpretation is abusing the "time to live" (TTL) of traffic. TTL is a protocol within a packet that limits the lifespan of data in a computer network. This prevents a data packet from circulating indefinitely. Abusing TTL works by first sending a short TTL value with the goal of passing the security receiver, assuming it will be dropped by a router later. This dropping occurs after the security device (meaning between the target and the security device) due to the TTL equaling a value of zero before the packet can reach its intended target. The attacker follows up the first packet with a TTL that has too high a value, with the goal of looking like duplicate traffic to the security device so that the security device will ignore it. By having the longer TTL, the packet will make it all the way to the host because now it has a high enough TTL value while being ignored by the network security solutions. Figure 12-8 shows an example of how this attack works. The first packet has a TTL value of 1, meaning it will hop past the security device but be dropped by the router due to having a value equal to 0. The second packet has a large enough TTL to make it to the host, yet if it's the same data, the security device will assume it's a duplicate, thus giving the attacker the ability to sneak in data.

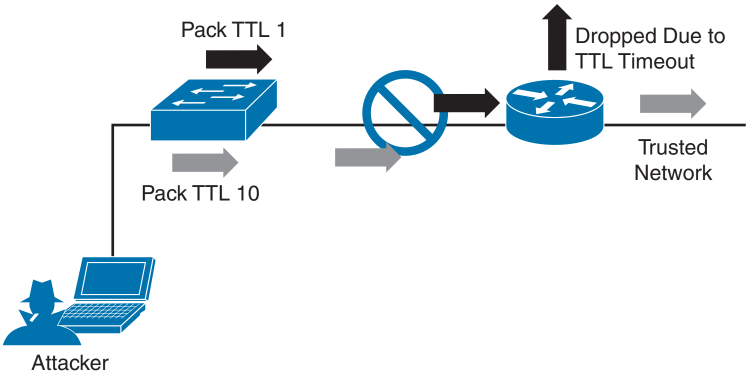

Figure 12-8 *TTL Manipulation Attack*

Like with IP fragmentation attacks, the good news is that many security solutions are aware of this form of attack and have methods to validate and handle protocol manipulation. Best practice is to verify with your security solution providers whether their products are aware of protocol-level misinterpretation attacks.

The following list highlights the key protocol misinterpretation concepts:

Key Topic

- Protocols can be manipulated to confuse security devices from properly evaluating traffic.
- TCP checksum and time-to-live protocols can be manipulated to first look like one thing and later to look like something else, with the goal of tricking the security defenses.

Now let's look at another evasion technique that takes a different approach to modifying network traffic.

Traffic Timing, Substitution, and Insertion

In a traffic timing attack, the attacker evades detection by performing his or her actions more slowly than normal while not exceeding thresholds inside the time windows the detection signatures use to correlate different packets together. A traffic timing attack can be mounted against any correlating engine that uses a fixed time window and a threshold to classify multiple packets into a composite event. An example of this attack would be sending packets at a slower rate than the detection system would be tuned to alarm to via sampling, making the attack unacceptably long in the eyes of the detection system.

A *traffic substitution and insertion attack* involves substituting the payload data with data in a different format but that has the same meaning, with the goal of it being ignored due to not being recognized by the security device. Some methods for changing the format include exchanging spaces with tabs, using Unicode instead of ASCII strings or characters in HTTP requests, modifying legitimate shell code with exploit code, and abusing case-sensitive communication. Most security devices can decode traffic; however, this attack is successful when a flaw is found in the decoding process. An example of a traffic substitution and insertion attack would be hiding malicious code by using Latin characters, knowing that the receiver will translate the code into ASCII. If this vulnerability exists, the security device will translate the text without verifying whether it is a threat, thus permitting the attack into the environment.

Defending against traffic timing attacks as well as substitution and insertion attacks once again requires features typically found in many security products offered by leading security vendors. Security features need to include the ability to adapt to changes in the timing of traffic patterns as well as changes in the format, to properly process extended characters, and to perform Unicode de-obfuscation. Unicode decoding examples include identifying ambiguous bits, double-encoding detection, and multidirectory delimiters. It is recommended that you verify with your trusted security solution provider whether your security solution has these detection capabilities.

The following list highlights the key traffic substitution and insertion concepts:

Key Topic

- Traffic timing attacks occur when the attacker evades detection by performing his or her actions more slowly than normal while not exceeding thresholds inside the time windows the detection signatures use to correlate different packets together.
- A traffic substitution and insertion attack substitutes the payload with data that is in a different format but has the same meaning.
- Some methods to accomplish a traffic substitution and insertion attack include exchanging spaces with tabs, using Unicode instead of ASCII, and abusing case-sensitive communication.
- Security products can stop this type of attack by being able to adapt to format changes, properly processing extended characters, and providing Unicode de-obfuscation.

One final evasion technique to cover is pivoting inside a network.

Pivoting

Although cyber attacks can vary in nature, one common step in the attack process, according to the cyber kill chain model first introduced by Lockheed Martin, is the idea of establishing a foothold in the target network and attempting to pivot to a more trusted area of the network. Establishing a foothold means breaching the network through exploiting a vulnerability and creating access points into the compromised network. The challenge for the attacker is the level of access granted with the exploit. For example, breaching a guest system on a network would typically mean gaining access to a guest network that is granted very limited access to network resources. An attacker would want to pivot from the guest network to another network with more access rights, such as the employee network. In regard to the kill chain, a pivot would be an action taken to start the sequence over once the attacker reached the "action" point. As illustrated in Figure 12-9, the attacker would first perform reconnaissance on other systems on the same network as the compromised system, weaponize an attack, and eventually move through the attack kill chain with the goal of gaining command and control abilities on other systems with greater network access rights.

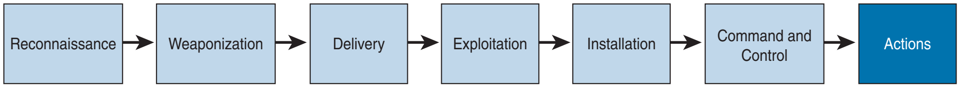

Figure 12-9 *The Lockheed Martin Kill Chain*

Usually, privileges and available resources on a network are grouped together into silos; this is known as *network segmentation*. Access to each network segment is typically enforced through some means of network access control. Figure 12-10 demonstrates the concept of segmentation and access control, where printers, guests, and a trusted network are on different network segments.

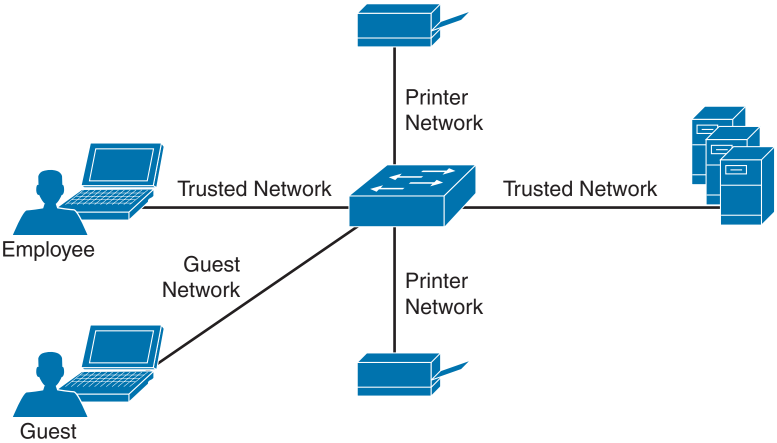

Figure 12-10 *Example of Basic Network Segmentation*

Pivoting, also known as *island hopping*, means to attack other systems on the same network. The idea is to identify a system with higher-level access rights, such as administrator. This is also known as a form of *privilege escalation*. Other systems with different levels of network access privileges can also be identified to provide more doorways into the network in the event the original breach is closed, to identify systems to leverage for another form or attack, to hide data by using multiple systems as exit points from the network, and so on. It is also important to understand that privilege escalation can occur within a system. This involves breaching a server with a guest account and then later obtaining root access to provide more resource rights on that system. Figure 12-11 shows an attacker pivoting through a vulnerable system sitting on a trusted network. This could be accomplished by identifying a vulnerability on the employee's laptop, placing a remote-access tool (RAT) on it, and then remotely connecting to the system to use it to surf inside the trusted network. The pivot occurs when the threat actor first gains access to the employee computer and "pivots" from that system to another system on the same network to gain further access to the target network.

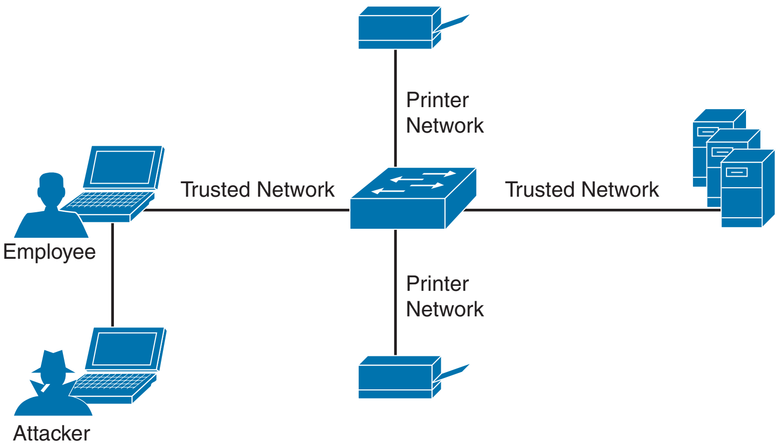

Figure 12-11 *Example of Pivoting*

There are different methods for pivoting across a network. The first involves using the existing network connections and ports available on the compromised system, essentially turning that system into a proxy pivot point. Although this provides some access, the attacker would be limited to the available TCP and UDP ports on the compromised system. A second approach that provides full access is setting up a VPN connection from the compromised system to the trusted network, giving the attacker full access by having all ports available from the attacker's system to the point of VPN termination.

Figure 12-12 shows an example of using a system connected to two networks as a pivot point for a remote attack.

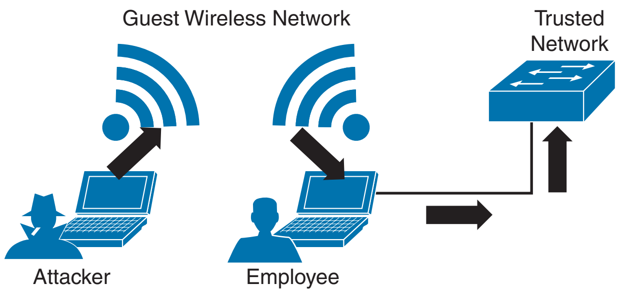

Figure 12-12 *Pivoting Through a Compromised Host*

Defending against pivoting can be addressed a few ways. The first method is to enforce proper network access control and segmentation by limiting what can access specific network segments and filtering access to only what is required to operate the business within those segments. This approach limits the available systems an attacker can pivot to as well as what new network services would become available by breaching other systems on the same network. For example, if all printers are limited to a specific network segment and one printer is breached, the attacker could only attack other printers and access printer-related traffic. We find pivoting occurs when a poor security architecture is implemented, such as putting all devices on the same network segment and not validating what can plug into a network. There are many penetration-testing stories about organizations that forgot about an older, vulnerable system sitting on the same network as the administrators and critical servers.

Cisco Identity Services Engine (ISE) is the Cisco flagship identity management and policy enforcement solution designed for address pivoting risks. An example is providing an employee named Hannah limited access to specific resources due to her device being an iPhone, which doesn't require the same access as her laptop. Figure 12-13 represents how ISE would identify user Hannah and limit her access to only specific resources. Different access would be provisioned to her printer, laptop, and desk phone, depending on each device's posture status and how the administrators configured the ISE solution. This is just one of the many ways ISE dramatically simplifies enforcing segmentation through a centralized policy.

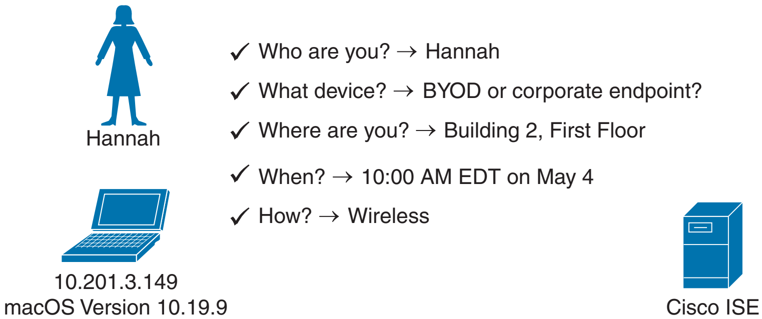

Figure 12-13 *Cisco Identity Services Engine (ISE) Device and User Interrogation*

Another defense strategy is to provide proper endpoint security practices such as patch management, antivirus, breach detection technologies, and so on. Typically, systems are breached though a vulnerability, where a payload such as a remote-access tool is delivered to give access to an unwanted remote party. Preventing the breach stops the attacker from having access to the network.

NetFlow security products such as Cisco Stealthwatch can be used to identify unusual traffic, giving you a "canary in the coal mine" defense. An example of this concept in regard to Stealthwatch would be an attacker compromising an employee's system and using it to pivot into the network. If Hannah is in the sales department and she starts scanning the network and accessing critical systems for the first time, it probably means something bad is happening, regardless of whether she is authorized to do so. Although NetFlow might not be able to tell you *why* the situation is bad at first, it can quickly alarm you that something bad is happening so that you can start to investigate the situation—just like miners would do when they noticed the canary had died in the coal mine.

NetFlow security doesn't require a lot of storage, is supported by most vendors, and can be enabled on most device types (routers, switches, wireless apps, virtual switching traffic, data center traffic, and so on). It essentially turns the entire network into a security sensor grid. Figure 12-14 shows the Cisco Stealthwatch host status for the system with the IP address 10.201.3.149.

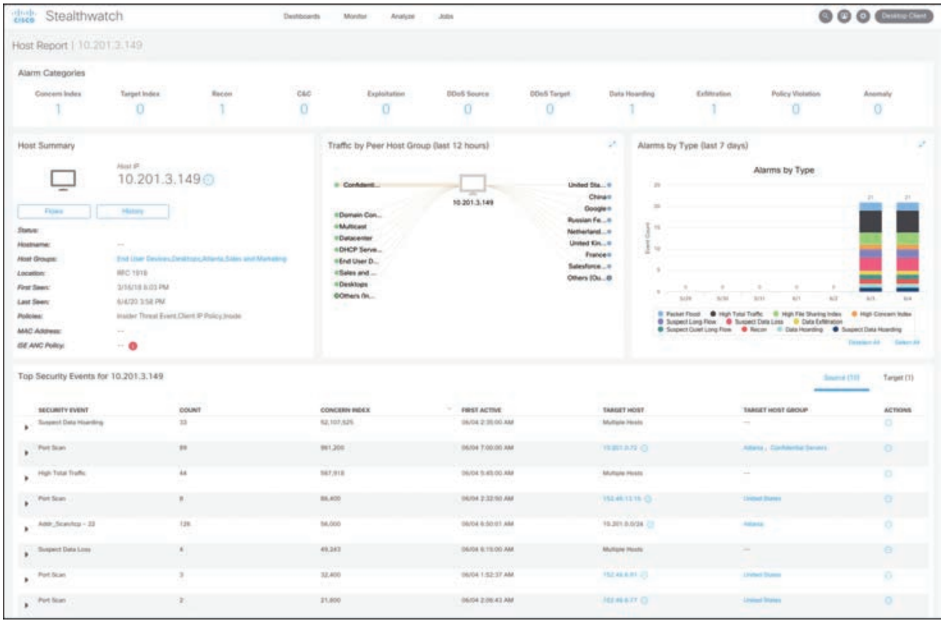

Figure 12-14 *Cisco Stealthwatch Host Report for 10.201.3.149*

The following list highlights the key pivot concepts:

Key Topic

- Pivoting in terms of cyber attacks (also known as *island hopping*) means to attack other systems on the same network with the goal of gaining accessing to that system.
- Best practice is to have networks segmented and to control access between each segment.
- A common goal for a pivot attack is to escalate the attacker's privileges. This is commonly accomplished by jumping from one system to another system with greater network privileges.
- Defending against pivoting can be accomplished by providing proper access control, network segmentation, DNS security, reputation security, and proper patch management.
- NetFlow is a great sensor-based tool for detecting unauthorized pivoting occurring within the network.

Exam Preparation Tasks

Review All Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. Table 12-2 lists these key topics and the page numbers on which each is found.

Key Topic

Table 12-2 Key Topics for Chapter 12

Key Topic Element	Description	Page
Paragraph	Understanding the challenges that encryption introduces to security monitoring	500
Paragraph	Understanding the challenges that NAT introduces to security monitoring	501
Section	Security Monitoring and Tor	504
Summary	Understanding the challenges that peer-to-peer communication introduces to security monitoring	505
List	Key encryption and tunneling concepts	508
List	Key resource exhaustion concepts	509
List	Key traffic fragmentation concepts	510
List	Key protocol misinterpretation concepts	511
List	Understanding traffic substitution and insertion concepts	512
List	Understanding pivoting (lateral movement)	516

Define Key Terms

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

Tor, Tor exit node, peer-to-peer (P2P) communication, virtual private network (VPN), remote-access VPN, traffic timing attack, clientless VPN, Secure Shell (SSH), resource exhaustion attack, traffic fragmentation attack, protocol misinterpretation attack, traffic substitution and insertion attack, pivoting, site-to-site VPN

Review Questions

The answers to these questions appear in Appendix A, "Answers to the 'Do I Know This Already?' Quizzes and Review Questions." For more practice with exam format questions, use the exam engine on the website.

1. Why does NAT present a challenge to security monitoring?
2. What is a Tor exit node?
3. Iodine is a tool that attackers use to obfuscate their techniques and _________ information from an organization using DNS tunnels.
4. Base64 is an example of one of the most popular _________ mechanisms used by threat actors.
5. Why should NTP be enabled in infrastructure devices and for security monitoring?

6. What is SSH used for?
7. What is the best explanation of an overlapping fragment attack?
8. Describe a timing attack.
9. What technology is used to create a circuit of computers that exchange encrypted data and is typically used by attackers to avoid being detected from a specific geographical location?
10. What term describes when the threat actor first gains access to the employee computer and "moves" from that system to another system on the same network to gain further access to the target network?

This page intentionally left blank

Index

Numerics

A

D

E

F

G

H

I

J-K

L

M

N

O

P

Q-R

T

U

V

W

X-Y-Z