CCNA Cyber Ops

SECFND 210-250

Official Cert Guide

OMAR SANTOS, CISSP No. 463598
JOSEPH MUNIZ, CISSP No. 344594
STEFANO DE CRESCENZO CCIE No. 26025, CISSP 406579

Cisco Press
800 East 96th Street
Indianapolis, IN 46240

CCNA Cyber Ops SECFND 210-250 Official Cert Guide

Omar Santos
Joseph Muniz
Stefano De Crescenzo

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

1 17

Library of Congress Control Number: 2017931952

ISBN-10: 1-58714-702-5

ISBN-13: 978-1-58714-702-9

Warning and Disclaimer

This book is designed to provide information about the CCNA Cyber Ops SECFND #210-250 exam. Every effort has been made to make this book as complete and accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, 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 authors 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 United States, 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: Ron Fligge

Product Line Manager: Brett Bartow

Executive Editor: Mary Beth Ray

Managing Editor: Sandra Schroeder

Technical Editors: Pavan Reddy, Ron Taylor

Development Editor: Christopher Cleveland

Copy Editor: Bart Reed

Project Editor: Mandie Frank

Designer: Chuti Prasertsith

Composition: Tricia Bronkella

Editorial Assistant: Vanessa Evans

Indexer: Ken Johnson

Proofreader: The Wordsmithery LLC

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 Authors

Omar Santos is an active member of the cyber security community, where he leads several industry-wide initiatives and standards bodies. His active role helps businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of their critical infrastructures.

Omar is the author of over a dozen 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 cyber security vulnerabilities. Additional information about Omar's current projects can be found at omarsantos.io, and you can follow Omar on Twitter @santosomar.

Joseph Muniz is an architect at Cisco Systems and security researcher. He has extensive experience in designing security solutions and architectures for the top Fortune 500 corporations and the U.S. government. Joseph's current role gives him visibility into the latest trends in cyber security, from both leading vendors and customers. Examples of Joseph's research include his RSA talk titled "Social Media Deception," which has been quoted by many sources (search for "Emily Williams Social Engineering"), as well as his articles in *PenTest Magazine* regarding various security topics.

Joseph runs The Security Blogger website, a popular resource for security, hacking, and product implementation. He is the author and contributor of several publications covering various penetration testing and security topics. You can follow Joseph at www.thesecurityblogger.com and @SecureBlogger.

Stefano De Crescenzo is a senior incident manager with the Cisco Product Security Incident Response Team (PSIRT), where he focuses on product vulnerability management and Cisco products forensics. He is the author of several blog posts and white papers about security best practices and forensics. He is an active member of the security community and has been a speaker at several security conferences.

Stefano specializes in malware detection and integrity assurance in critical infrastructure devices, and he is the author of integrity assurance guidelines for Cisco IOS, IOS-XE, and ASA.

Stefano holds a B.Sc. and M.Sc. in telecommunication engineering from Politecnico di Milano, Italy, and an M.Sc. in telecommunication from Danish Technical University, Denmark. He is currently pursuing an Executive MBA at Vlerick Business School in Belgium. He also holds a CCIE in Security #26025 and is CISSP and CISM certified.

About the Technical Reviewers

Pavan Reddy serves as a Security Principal in Cisco Security Services. Pavan has 20+ years of security and network consulting experience in Financial Services, Healthcare, Service Provider, and Retail arenas. Recent projects cover Technical Security Strategy and Architecture, Network Segmentation Strategy, Threat Intelligence Analytics, Distributed Denial-of-Service Mitigation Architectures, and DNS Architecture and Security. Pavan holds multiple CCIEs and BS in Computer Engineering.

Ron Taylor has been in the Information Security field for almost 20 years. Ten of those years were spent in consulting where he gained experience in many areas. In 2008, he joined the Cisco Global Certification Team as an SME in Information Assurance. In 2012, he moved into a position with the Security Research & Operations group (PSIRT), where his focus was mostly on penetration testing of Cisco products and services. He was also involved in developing and presenting security training to internal development and test teams globally. Additionally, he provided consulting support to many product teams as an SME on product security testing. In his current role, he is a Consulting Systems Engineer specializing in Cisco's security product line. Certifications include GPEN, GWEB, GCIA, GCIH, GWAPT, RHCE, CCSP, CCNA, CISSP, and MCSE. Ron is also a Cisco Security Blackbelt, SANS mentor, Cofounder and President of the Raleigh BSides Security Conference, and a member of the Packet Hacking Village team at Defcon.

Dedications

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.

I also dedicate this book to my father, Jose, and to the memory of my mother, Generosa. Without their knowledge, wisdom, and guidance, I would not have the goals that I strive to achieve today.

—Omar Santos

I would like to dedicate this book to the memory of my father, Raymond Muniz. He never saw me graduate from college or accomplish great things, such as writing this book. I would also like to apologize to him for dropping out of soccer in high school. I picked it back up later in life, and today play in at least two competitive matches a week. Your hard work paid off. Hopefully you somehow know that.

—Joseph Muniz

This book is dedicated to my wife, Nevena, and my beautiful daughters, Sara and Tea, who supported and inspired me during the development of this book. Specifically, Tea was born a few weeks before I started writing my first chapter, so she is especially connected with this book.

I would also like to mention my whole family: my mother, Mariagrazia, and my sister, Francesca, who supported my family and me while I was away writing. I also dedicate this book to the memory of my father, Cataldo.

—Stefano De Crescenzo

Acknowledgments

I would like to thank the technical editors, Pavan Reddy and Ron Taylor, for their time and technical expertise. They verified our work and contributed to the success of this book. I would also like to thank the Cisco Press team, especially Mary Beth Ray, Denise Lincoln, and Christopher Cleveland, for their patience, guidance, and consideration. Their efforts are greatly appreciated. Finally, I would like to acknowledge the Cisco Security Research and Operations teams, Cisco Advanced Threat Analytics, and Cisco Talos. Several leaders in the network security industry work there, supporting our Cisco customers, often under very stressful conditions, and working miracles daily. They are truly unsung heroes, and I am honored to have had the privilege of working side by side with them in the trenches while protecting customers and Cisco.

—Omar Santos

I would first like to thank Omar and Stefano for including me on this project. I really enjoyed working with these guys and hope we can do more in the future. I also would like to thank the Cisco Press team and technical editors, Pavan Reddy and Ron Taylor, for their fantastic support in making the writing process top quality and easy for everybody. Hey, Ron, you got this and the CTR comic. 2016 was great for you, Mr. Green.

I would also like to thank all the great people in my life who make me who I am.

Finally, a message for Raylin Muniz (age 7): Hopefully one day you can accomplish your dreams like I have with this book.

—Joseph Muniz

I would like to thank Omar and Joey for being fantastic mates in the development of this book. A special mention goes to my wife as well, for supporting me throughout this journey and for helping me by reviewing my work.

Additionally, this book wouldn't have been possible without the help of the Cisco Press team and in particular of Chris Cleveland. His guidance has been very precious. A big thanks goes to the technical reviewers, Pavan and Ron. Thanks for keeping me honest and to the point! A big thanks also to Eric Vyncke for his numerous suggestions.

—Stefano De Crescenzo

Contents at a Glance

Introduction xxv

Part I Network Concepts

Chapter 1 Fundamentals of Networking Protocols and Networking Devices 3

Chapter 2 Network Security Devices and Cloud Services 109

Part II Security Concepts

Chapter 3 Security Principles 159

Chapter 4 Introduction to Access Controls 185

Chapter 5 Introduction to Security Operations Management 241

Part III Cryptography

Chapter 6 Fundamentals of Cryptography and Public Key Infrastructure (PKI) 309

Chapter 7 Introduction to Virtual Private Networks (VPNs) 339

Part IV Host-Based Analysis

Chapter 8 Windows-Based Analysis 357

Chapter 9 Linux- and Mac OS X–Based Analysis 379

Chapter 10 Endpoint Security Technologies 403

Part V Security Monitoring and Attack Methods

Chapter 11 Network and Host Telemetry 419

Chapter 12 Security Monitoring Operational Challenges 487

Chapter 13 Types of Attacks and Vulnerabilities 499

Chapter 14 Security Evasion Techniques 523

Part VI Final Preparation

Chapter 15 Final Preparation 545

Part VII Appendixes

Appendix A Answers to the "Do I Know This Already?" Quizzes and Q&A Questions 551

Glossary 571

Index 586

Elements Available on the Book Website

Appendix B Memory Tables

Appendix C Memory Tables Answer Key

Appendix D Study Planner

Contents

Introduction xxv

Part I Network Concepts

Chapter 1 Fundamentals of Networking Protocols and Networking Devices 3

"Do I Know This Already?" Quiz 3

Foundation Topics 6

TCP/IP and OSI Model 6

TCP/IP Model 6

TCP/IP Model Encapsulation 9

Networking Communication with the TCP/IP Model 10

Open System Interconnection Model 12

Layer 2 Fundamentals and Technologies 16

Ethernet LAN Fundamentals and Technologies 16

Ethernet Physical Layer 16

Ethernet Medium Access Control 17

Ethernet Frame 19

Ethernet Addresses 19

Ethernet Devices and Frame-Forwarding Behavior 20

LAN Hubs and Bridges 20

LAN Switches 22

Link Layer Loop and Spanning Tree Protocols 26

Virtual LAN (VLAN) and VLAN Trunking 31

Cisco VLAN Trunking Protocol 33

Inter-VLAN Traffic and Multilayer Switches 33

Wireless LAN Fundamentals and Technologies 35

802.11 Architecture and Basic Concepts 37

802.11 Frame 39

WLAN Access Point Types and Management 40

Internet Protocol and Layer 3 Technologies 43

IPv4 Header 45

IPv4 Fragmentation 47

IPv4 Addresses and Addressing Architecture 48

IP Network Subnetting and Classless Interdomain Routing (CIDR) 50

Variable-Length Subnet Mask (VLSM) 52

Public and Private IP Addresses 54

Special and Reserved IPv4 Addresses 56

IP Addresses Assignment and DHCP 57
IP Communication Within a Subnet and Address Resolution Protocol (ARP) 60
Intersubnet IP Packet Routing 61
Routing Tables and IP Routing Protocols 64
Distance Vector 65
Advanced Distance Vector or Hybrid 67
Link-State 67
Using Multiple Routing Protocols 69
Internet Control Message Protocol (ICMP) 69
Domain Name System (DNS) 71
IPv6 Fundamentals 75
IPv6 Header 78
IPv6 Addressing and Subnets 79
Special and Reserved IPv6 Addresses 82
IPv6 Addresses Assignment, Neighbor Discovery Protocol, and DHCPv6 83
Transport Layer Technologies and Protocols 89
Transmission Control Protocol (TCP) 90
TCP Header 91
TCP Connection Establishment and Termination 92
TCP Socket 94
TCP Error Detection and Recovery 95
TCP Flow Control 97
User Datagram Protocol (UDP) 98
UDP Header 98
UDP Socket and Known UDP Application 99
Exam Preparation Tasks 100
Review All Key Topics 100
Complete Tables and Lists from Memory 103
Define Key Terms 103
Q&A 103
References and Further Reading 106

Chapter 2 Network Security Devices and Cloud Services 109

"Do I Know This Already?" Quiz 109

Foundation Topics 112

Network Security Systems 112

Traditional Firewalls 112

Packet-Filtering Techniques 113

Application Proxies 117

Network Address Translation 117

Port Address Translation 118

Static Translation 119

Stateful Inspection Firewalls 120

Demilitarized Zones 120

Firewalls Provide Network Segmentation 120

High Availability 121

Firewalls in the Data Center 123

Virtual Firewalls 124

Deep Packet Inspection 125

Next-Generation Firewalls 126

Cisco Firepower Threat Defense 126

Personal Firewalls 128

Intrusion Detection Systems and Intrusion Prevention Systems 128

Pattern Matching and Stateful Pattern-Matching Recognition 130

Protocol Analysis 131

Heuristic-Based Analysis 131

Anomaly-Based Analysis 131

Global Threat Correlation Capabilities 132

Next-Generation Intrusion Prevention Systems 133

Firepower Management Center 133

Advance Malware Protection 133

AMP for Endpoints 133

AMP for Networks 136

Web Security Appliance 137

Email Security Appliance 140

Cisco Security Management Appliance 142

Cisco Identity Services Engine 143

Security Cloud-based Solutions 144
Cisco Cloud Web Security 145
Cisco Cloud Email Security 146
Cisco AMP Threat Grid 147
Cisco Threat Awareness Service 147
OpenDNS 148
CloudLock 148
Cisco NetFlow 149
What Is the Flow in NetFlow? 149
NetFlow vs. Full Packet Capture 151
The NetFlow Cache 151
Data Loss Prevention 152
Exam Preparation Tasks 153
Review All Key Topics 153
Complete Tables and Lists from Memory 154
Define Key Terms 154
Q&A 154

Part II Security Concepts

Chapter 3 Security Principles 159
"Do I Know This Already?" Quiz 159
Foundation Topics 162
The Principles of the Defense-in-Depth Strategy 162
What Are Threats, Vulnerabilities, and Exploits? 166
Vulnerabilities 166
Threats 167
Threat Actors 168
Threat Intelligence 168
Exploits 170
Confidentiality, Integrity, and Availability: The CIA Triad 171
Confidentiality 171
Integrity 171
Availability 171
Risk and Risk Analysis 171
Personally Identifiable Information and Protected Health Information 173
PII 173
PHI 174

Principle of Least Privilege and Separation of Duties 174
Principle of Least Privilege 174
Separation of Duties 175
Security Operation Centers 175
Runbook Automation 176
Forensics 177
Evidentiary Chain of Custody 177
Reverse Engineering 178
Exam Preparation Tasks 180
Review All Key Topics 180
Define Key Terms 180
Q&A 181

Chapter 4 Introduction to Access Controls 185
"Do I Know This Already?" Quiz 185
Foundation Topics 189
Information Security Principles 189
Subject and Object Definition 189
Access Control Fundamentals 190
Identification 190
Authentication 191
Authentication by Knowledge 191
Authentication by Ownership 191
Authentication by Characteristic 191
Multifactor Authentication 192
Authorization 193
Accounting 193
Access Control Fundamentals: Summary 194
Access Control Process 195
Asset Classification 195
Asset Marking 196
Access Control Policy 197
Data Disposal 197
Information Security Roles and Responsibilities 197
Access Control Types 199
Access Control Models 201
Discretionary Access Control 203
Mandatory Access Control 204

Role-Based Access Control 205
Attribute-Based Access Control 207
Access Control Mechanisms 210
Identity and Access Control Implementation 212
Authentication, Authorization, and Accounting Protocols 212
RADIUS 212
TACACS+ 214
Diameter 216
Port-Based Access Control 218
Port Security 218
802.1x 219
Network Access Control List and Firewalling 221
VLAN Map 222
Security Group–Based ACL 222
Downloadable ACL 222
Firewalling 223
Identity Management and Profiling 223
Network Segmentation 223
Network Segmentation Through VLAN 224
Firewall DMZ 225
Cisco TrustSec 225
Intrusion Detection and Prevention 227
Network-Based Intrusion Detection and Protection System 229
Host-Based Intrusion Detection and Prevention 230
Antivirus and Antimalware 231
Exam Preparation Tasks 233
Review All Key Topics 233
Complete Tables and Lists from Memory 234
Define Key Terms 234
Q&A 234
References and Additional Reading 237

Chapter 5 Introduction to Security Operations Management 241
"Do I Know This Already?" Quiz 241
Foundation Topics 244
Introduction to Identity and Access Management 244
Phases of the Identity and Access Lifecycle 244
Registration and Identity Validation 245
Privileges Provisioning 245

Access Review 246
Access Revocation 246
Password Management 246
Password Creation 246
Password Storage and Transmission 248
Password Reset 249
Password Synchronization 249
Directory Management 250
Single Sign-On 252
Kerberos 253
Federated SSO 255
Security Assertion Markup Language 256
OAuth 258
OpenID Connect 259
Security Events and Logs Management 260
Logs Collection, Analysis, and Disposal 260
Syslog 262
Security Information and Event Manager 264
Assets Management 265
Assets Inventory 266
Assets Ownership 267
Assets Acceptable Use and Return Policies 267
Assets Classification 268
Assets Labeling 268
Assets and Information Handling 268
Media Management 269
Introduction to Enterprise Mobility Management 269
Mobile Device Management 271
Cisco BYOD Architecture 272
Cisco ISE and MDM Integration 274
Cisco Meraki Enterprise Mobility Management 276
Configuration and Change Management 276
Configuration Management 276
Change Management 278

Vulnerability Management 281
Vulnerability Identification 281
Finding Information about a Vulnerability 282
Vulnerability Scan 284
Penetration Assessment 285
Product Vulnerability Management 286
Vulnerability Analysis and Prioritization 290
Vulnerability Remediation 294
Patch Management 295
References and Additional Readings 299
Exam Preparation Tasks 302
Review All Key Topics 302
Complete Tables and Lists from Memory 303
Define Key Terms 303
Q&A 303

Part III Cryptography

Chapter 6 Fundamentals of Cryptography and Public Key Infrastructure (PKI) 309

"Do I Know This Already?" Quiz 309
Foundation Topics 311
Cryptography 311
Ciphers and Keys 311
Ciphers 311
Keys 312
Block and Stream Ciphers 312
Symmetric and Asymmetric Algorithms 313
Symmetric Algorithms 313
Asymmetric Algorithms 313
Hashes 314
Hashed Message Authentication Code 316
Digital Signatures 317
Digital Signatures in Action 317
Key Management 320
Next-Generation Encryption Protocols 321
IPsec and SSL 321
IPsec 321
SSL 322

Fundamentals of PKI 323
Public and Private Key Pairs 323
RSA Algorithm, the Keys, and Digital Certificates 324
Certificate Authorities 324
Root and Identity Certificates 326
Root Certificate 326
Identity Certificate 327
X.500 and X.509v3 Certificates 328
Authenticating and Enrolling with the CA 328
Public Key Cryptography Standards 330
Simple Certificate Enrollment Protocol 330
Revoking Digital Certificates 330
Using Digital Certificates 331
PKI Topologies 331
Single Root CA 332
Hierarchical CA with Subordinate CAs 332
Cross-certifying CAs 333
Exam Preparation Tasks 334
Review All Key Topics 334
Complete Tables and Lists from Memory 334
Define Key Terms 335
Q&A 335

Chapter 7 Introduction to Virtual Private Networks (VPNs) 339
"Do I Know This Already?" Quiz 339
Foundation Topics 341
What Are VPNs? 341
Site-to-site vs. Remote-Access VPNs 341
An Overview of IPsec 343
IKEv1 Phase 1 343
IKEv1 Phase 2 345
IKEv2 348
SSL VPNs 348
SSL VPN Design Considerations 351
User Connectivity 351
VPN Device Feature Set 351
Infrastructure Planning 352
Implementation Scope 352

Exam Preparation Tasks 353
Review All Key Topics 353
Complete Tables and Lists from Memory 353
Define Key Terms 353
Q&A 353

Part IV Host-Based Analysis

Chapter 8 Windows-Based Analysis 357
"Do I Know This Already?" Quiz 357
Foundation Topics 360
Process and Threads 360
Memory Allocation 362
Windows Registration 364
Windows Management Instrumentation 366
Handles 368
Services 369
Windows Event Logs 372
Exam Preparation Tasks 375
Review All Key Topics 375
Define Key Terms 375
Q&A 375
References and Further Reading 377

Chapter 9 Linux- and Mac OS X–Based Analysis 379
"Do I Know This Already?" Quiz 379
Foundation Topics 382
Processes 382
Forks 384
Permissions 385
Symlinks 390
Daemons 391
UNIX-Based Syslog 392
Apache Access Logs 396
Exam Preparation Tasks 398
Review All Key Topics 398
Complete Tables and Lists from Memory 398
Define Key Terms 398
Q&A 399
References and Further Reading 400

Chapter 10 Endpoint Security Technologies 403
"Do I Know This Already?" Quiz 403
Foundation Topics 406
Antimalware and Antivirus Software 406
Host-Based Firewalls and Host-Based Intrusion Prevention 408
Application-Level Whitelisting and Blacklisting 410
System-Based Sandboxing 411
Exam Preparation Tasks 414
Review All Key Topics 414
Complete Tables and Lists from Memory 414
Define Key Terms 414
Q&A 414

Part V Security Monitoring and Attack Methods

Chapter 11 Network and Host Telemetry 419
"Do I Know This Already?" Quiz 419
Foundation Topics 422
Network Telemetry 422
Network Infrastructure Logs 422
Network Time Protocol and Why It Is Important 423
Configuring Syslog in a Cisco Router or Switch 424
Traditional Firewall Logs 426
Console Logging 427
Terminal Logging 427
ASDM Logging 427
Email Logging 427
Syslog Server Logging 427
SNMP Trap Logging 428
Buffered Logging 428
Configuring Logging on the Cisco ASA 428
Syslog in Large Scale Environments 430
Splunk 430
Graylog 434
Elasticsearch, Logstash, and Kibana (ELK) Stack 436
Next-Generation Firewall and Next-Generation IPS Logs 437
NetFlow Analysis 445
Commercial NetFlow Analysis Tools 447
Open Source NetFlow Analysis Tools 449
Counting, Grouping, and Mating NetFlow Records with Silk 453

Big Data Analytics for Cyber Security Network Telemetry 453
Configuring Flexible NetFlow in Cisco IOS and Cisco IOS-XE Devices 455
Cisco Application Visibility and Control (AVC) 469
Network Packet Capture 470
tcpdump 471
Wireshark 473
Cisco Prime Infrastructure 474
Host Telemetry 477
Logs from User Endpoints 477
Logs from Servers 481
Exam Preparation Tasks 483
Review All Key Topics 483
Complete Tables and Lists from Memory 483
Define Key Terms 483
Q&A 484

Chapter 12 Security Monitoring Operational Challenges 487
"Do I Know This Already?" Quiz 487
Foundation Topics 490
Security Monitoring and Encryption 490
Security Monitoring and Network Address Translation 491
Security Monitoring and Event Correlation Time Synchronization 491
DNS Tunneling and Other Exfiltration Methods 491
Security Monitoring and Tor 493
Security Monitoring and Peer-to-Peer Communication 494
Exam Preparation Tasks 495
Review All Key Topics 495
Define Key Terms 495
Q&A 495

Chapter 13 Types of Attacks and Vulnerabilities 499
"Do I Know This Already?" Quiz 499
Foundation Topics 502
Types of Attacks 502
Reconnaissance Attacks 502
Social Engineering 504
Privilege Escalation Attacks 506
Backdoors 506

Code Execution 506
Man-in-the Middle Attacks 506
Denial-of-Service Attacks 507
Direct DDoS 507
Botnets Participating in DDoS Attacks 508
Reflected DDoS Attacks 509
Attack Methods for Data Exfiltration 510
ARP Cache Poisoning 511
Spoofing Attacks 512
Route Manipulation Attacks 513
Password Attacks 513
Wireless Attacks 514
Types of Vulnerabilities 514
Exam Preparation Tasks 518
Review All Key Topics 518
Define Key Terms 518
Q&A 518

Chapter 14 Security Evasion Techniques 523
"Do I Know This Already?" Quiz 523
Foundation Topics 526
Encryption and Tunneling 526
Key Encryption and Tunneling Concepts 531
Resource Exhaustion 531
Traffic Fragmentation 532
Protocol-Level Misinterpretation 533
Traffic Timing, Substitution, and Insertion 535
Pivoting 536
Exam Preparation Tasks 541
Review All Key Topics 541
Complete Tables and Lists from Memory 541
Define Key Terms 541
Q&A 541
References and Further Reading 543

Part VI Final Preparation

Chapter 15 Final Preparation 545

Tools for Final Preparation 545

Pearson Cert Practice Test Engine and Questions on the Website 545

Accessing the Pearson Test Prep Software Online 545

Accessing the Pearson Test Prep Software Offline 546

Customizing Your Exams 547

Updating Your Exams 547

Premium Edition 548

The Cisco Learning Network 548

Memory Tables 548

Chapter-Ending Review Tools 549

Suggested Plan for Final Review/Study 549

Summary 549

Part VII Appendixes

Appendix A Answers to the "Do I Know This Already?" Quizzes and Q&A Questions 551

Glossary 571

Index 586

Elements Available on the Book Website

Appendix B Memory Tables

Appendix C Memory Tables Answer Key

Appendix D Study Planner

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:

- **Bold** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), bold 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

Congratulations! If you are reading this, you have in your possession a powerful tool that can help you to:

- Improve your awareness and knowledge of cyber security fundamentals
- Increase your skill level related to the implementation of that security
- Prepare for the CCNA Cyber Ops SECFND certification exam

Whether you are preparing for the CCNA Cyber Ops certification or just changing careers to cyber security, this book will help you gain the knowledge you need to get started and prepared. When writing this book, we did so with you in mind, and together we will discover the critical ingredients that make up the recipe for a secure network and how to succeed in cyber security operations. By focusing on covering the objectives for the CCNA Cyber Ops SECFND exam and integrating that with real-world best practices and examples, we created this content with the intention of being your personal tour guides as we take you on a journey through the world of network security.

The CCNA Cyber Ops: Understanding Cisco Cybersecurity Fundamentals (SECFND) 210-250 exam is required for the CCNA Cyber Ops certification. This book covers all the topics listed in Cisco's exam blueprint, and each chapter includes key topics and preparation tasks to assist you in mastering this information. Reviewing tables and practicing test questions will help you practice your knowledge in all subject areas.

About the 210-250 CCNA Cyber Ops SECFND Exam

The CCNA Cyber Ops: Understanding Cisco Cybersecurity Fundamentals (SECFND) 210-250 exam is the first of the two required exams to achieve the CCNA Cyber Ops certification and is aligned with the job role of associate-level security operations center (SOC) security analyst. The SECFND exam tests candidates' understanding of cyber security's basic principles, foundational knowledge, and core skills needed to grasp the more advanced associate-level materials in the second required exam: Implementing Cisco Cybersecurity Operations (SECOPS).

The CCNA Cyber Ops: Understanding Cisco Cybersecurity Fundamentals (SECFND) 210-250 exam is a computer-based test that has 55 to 60 questions and a 90-minute time limit. Because all exam information is managed by Cisco Systems and is therefore subject to change, candidates should continually monitor the Cisco Systems site for exam updates at http://www.cisco.com/c/en/us/training-events/training-certifications/exams/current-list/secfnd.html.

You can take the exam at Pearson VUE testing centers. You can register with VUE at www.vue.com/cisco.

210-250 CCNA Cyber Ops SECFNC Exam Topics

Table I-1 lists the topics of the 210-250 SECFND exam and indicates the chapter in the book where they are covered.

Table I-1 *210-250 SECFND Exam Topics*

Exam Topic	Chapter
1.0 Network Concepts	
1.1 Describe the function of the network layers as specified by the OSI and the TCP/IP network models	Chapter 1
1.2 Describe the operation of the following:	
1.2.a IP	Chapter 1
1.2.b TCP	Chapter 1
1.2.c UDP	Chapter 1
1.2.d ICMP	Chapter 1
1.3 Describe the operation of these network services:	
1.3.a ARP	Chapter 1
1.3.b DNS	Chapter 1
1.3.c DHCP	Chapter 1
1.4 Describe the basic operation of these network device types:	
1.4.a Router	Chapter 1
1.4.b Switch	Chapter 1
1.4.c Hub	Chapter 1
1.4.d Bridge	Chapter 1
1.4.e Wireless access point (WAP)	Chapter 1
1.4.f Wireless LAN controller (WLC)	Chapter 1
1.5 Describe the functions of these network security systems as deployed on the host, network, or the cloud:	
1.5.a Firewall	Chapter 2
1.5.b Cisco Intrusion Prevention System (IPS)	Chapter 2
1.5.c Cisco Advanced Malware Protection (AMP)	Chapter 2
1.5.d Web Security Appliance (WSA) / Cisco Cloud Web Security (CWS)	Chapter 2
1.5.e Email Security Appliance (ESA) / Cisco Cloud Email Security (CES)	Chapter 2
1.6 Describe IP subnets and communication within an IP subnet and between IP subnets	Chapter 1
1.7 Describe the relationship between VLANs and data visibility	Chapter 1
1.8 Describe the operation of ACLs applied as packet filters on the interfaces of network devices	Chapter 2
1.9 Compare and contrast deep packet inspection with packet filtering and stateful firewall operation	Chapter 2

Exam Topic	Chapter
1.10 Compare and contrast inline traffic interrogation and taps or traffic mirroring	Chapter 2
1.11 Compare and contrast the characteristics of data obtained from taps or traffic mirroring and NetFlow in the analysis of network traffic	Chapter 2
1.12 Identify potential data loss from provided traffic profiles	Chapter 2
2.0 Security Concepts	
2.1 Describe the principles of the defense-in-depth strategy	Chapter 3
2.2 Compare and contrast these concepts:	
2.2.a Risk	Chapter 3
2.2.b Threat	Chapter 3
2.2.c Vulnerability	Chapter 3
2.2.d Exploit	Chapter 3
2.3 Describe these terms:	
2.3.a Threat actor	Chapter 3
2.3.b Runbook automation (RBA)	Chapter 3
2.3.c Chain of custody (evidentiary)	Chapter 3
2.3.d Reverse engineering	Chapter 3
2.3.e Sliding window anomaly detection	Chapter 3
2.3.f PII	Chapter 3
2.3.g PHI	Chapter 3
2.4 Describe these security terms:	
2.4.a Principle of least privilege	Chapter 3
2.4.b Risk scoring/risk weighting	Chapter 3
2.4.c Risk reduction	Chapter 3
2.4.d Risk assessment	Chapter 3
2.5 Compare and contrast these access control models:	
2.5.a Discretionary access control	Chapter 4
2.5.b Mandatory access control	Chapter 4
2.5.c Nondiscretionary access control	Chapter 4
2.6 Compare and contrast these terms:	
2.6.a Network and host antivirus	Chapter 4
2.6.b Agentless and agent-based protections	Chapter 4

Exam Topic	Chapter
2.6.c SIEM and log collection	Chapter 5
2.7 Describe these concepts:	
2.7.a Asset management	Chapter 5
2.7.b Configuration management	Chapter 5
2.7.c Mobile device management	Chapter 5
2.7.d Patch management	Chapter 5
2.7.e Vulnerability management	Chapter 5
3.0 Cryptography	
3.1 Describe the uses of a hash algorithm	Chapter 6
3.2 Describe the uses of encryption algorithms	Chapter 6
3.3 Compare and contrast symmetric and asymmetric encryption algorithms	Chapter 6
3.4 Describe the processes of digital signature creation and verification	Chapter 6
3.5 Describe the operation of a PKI	Chapter 6
3.6 Describe the security impact of these commonly used hash algorithms:	
3.6.a MD5	Chapter 6
3.6.b SHA-1	Chapter 6
3.6.c SHA-256	Chapter 6
3.6.d SHA-512	Chapter 6
3.7 Describe the security impact of these commonly used encryption algorithms and secure communications protocols:	
3.7.a DES	Chapter 6
3.7.b 3DES	Chapter 6
3.7.c AES	Chapter 6
3.7.d AES256-CTR	Chapter 6
3.7.e RSA	Chapter 6
3.7.f DSA	Chapter 6
3.7.g SSH	Chapter 6
3.7.h SSL/TLS	Chapter 6
3.8 Describe how the success or failure of a cryptographic exchange impacts security investigation	Chapter 6
3.9 Describe these items in regard to SSL/TLS:	
3.9.a Cipher-suite	Chapter 6

Exam Topic	Chapter
3.9.b X.509 certificates	Chapter 6
3.9.c Key exchange	Chapter 6
3.9.d Protocol version	Chapter 6
3.9.e PKCS	Chapter 6
4.0 Host-based Analysis	
4.1 Define these terms as they pertain to Microsoft Windows:	
4.1.a Processes	Chapter 8
4.1.b Threads	Chapter 8
4.1.c Memory allocation	Chapter 8
4.1.d Windows Registry	Chapter 8
4.1.e WMI	Chapter 8
4.1.f Handles	Chapter 8
4.1.g Services	Chapter 8
4.2 Define these terms as they pertain to Linux:	
4.2.a Processes	Chapter 9
4.2.b Forks	Chapter 9
4.2.c Permissions	Chapter 9
4.2.d Symlinks	Chapter 9
4.2.e Daemon	Chapter 9
4.3 Describe the functionality of these endpoint technologies in regard to security monitoring:	
4.3.a Host-based intrusion detection	Chapter 10
4.3.b Antimalware and antivirus	Chapter 10
4.3.c Host-based firewall	Chapter 10
4.3.d Application-level whitelisting/blacklisting	Chapter 10
4.3.e Systems-based sandboxing (such as Chrome, Java, Adobe Reader)	Chapter 10
4.4 Interpret these operating system log data to identify an event:	
4.4.a Windows security event logs	Chapter 8
4.4.b Unix-based syslog	Chapter 9
4.4.c Apache access logs	Chapter 9
4.4.d IIS access logs	Chapter 8

Exam Topic	Chapter
5.0 Security Monitoring	
5.1 Identify the types of data provided by these technologies:	
5.1.a TCP Dump	Chapter 11
5.1.b NetFlow	Chapter 11
5.1.c Next-gen firewall	Chapter 11
5.1.d Traditional stateful firewall	Chapter 11
5.1.e Application visibility and control	Chapter 11
5.1.f Web content filtering	Chapter 11
5.1.g Email content filtering	Chapter 11
5.2 Describe these types of data used in security monitoring:	
5.2.a Full packet capture	Chapter 11
5.2.b Session data	Chapter 11
5.2.c Transaction data	Chapter 11
5.2.d Statistical data	Chapter 11
5.2.e Extracted content	Chapter 11
5.2.f Alert data	Chapter 11
5.3 Describe these concepts as they relate to security monitoring:	
5.3.a Access control list	Chapter 12
5.3.b NAT/PAT	Chapter 12
5.3.c Tunneling	Chapter 12
5.3.d TOR	Chapter 12
5.3.e Encryption	Chapter 12
5.3.f P2P	Chapter 12
5.3.g Encapsulation	Chapter 12
5.3.h Load balancing	Chapter 12
5.4 Describe these NextGen IPS event types:	
5.4.a Connection event	Chapter 11
5.4.b Intrusion event	Chapter 11
5.4.c Host or endpoint event	Chapter 11
5.4.d Network discovery event	Chapter 11
5.4.e NetFlow event	Chapter 11

Exam Topic	Chapter
5.5 Describe the function of these protocols in the context of security monitoring:	
5.5.a DNS	Chapter 12
5.5.b NTP	Chapter 12
5.5.c SMTP/POP/IMAP	Chapter 12
5.5.d HTTP/HTTPS	Chapter 12
6.0 Attack Methods	
6.1 Compare and contrast an attack surface and vulnerability	Chapter 13
6.2 Describe these network attacks:	
6.2.a Denial of service	Chapter 13
6.2.b Distributed denial of service	Chapter 13
6.2.c Man-in-the-middle	Chapter 13
6.3 Describe these web application attacks:	
6.3.a SQL injection	Chapter 13
6.3.b Command injections	Chapter 13
6.3.c Cross-site scripting	Chapter 13
6.4 Describe these attacks:	
6.4.a Social engineering	Chapter 13
6.4.b Phishing	Chapter 13
6.4.c Evasion methods	Chapter 13
6.5 Describe these endpoint-based attacks:	
6.5.a Buffer overflows	Chapter 13
6.5.b Command and control (C2)	Chapter 13
6.5.c Malware	Chapter 13
6.5.d Rootkit	Chapter 13
6.5.e Port scanning	Chapter 13
6.5.f Host profiling	Chapter 13
6.6 Describe these evasion methods:	
6.6.a Encryption and tunneling	Chapter 14
6.6.b Resource exhaustion	Chapter 14
6.6.c Traffic fragmentation	Chapter 14
6.6.d Protocol-level misinterpretation	Chapter 14

Exam Topic	Chapter
6.6.e Traffic substitution and insertion	Chapter 14
6.6.f Pivot	Chapter 14
6.7 Define privilege escalation	Chapter 13
6.8 Compare and contrast a remote exploit and a local exploit	Chapter 13

About the CCNA Cyber Ops SECFND 210-250 Official Cert Guide

This book maps to the topic areas of the 210-250 SECFND 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. So, this book does not try to help you pass the exams only by memorization, but by truly learning and understanding the topics. This book is designed to help you pass the SECFND 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:

- **"Do I Know This Already?" quiz:** Each chapter begins with a quiz that helps you determine how much time you need to spend studying that chapter.
- **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. Each chapter includes the activities that make the most sense for studying the topics in that chapter:
  - **Review All the Key Topics:** The Key Topic icon appears next to the most important items in the "Foundation Topics" section of the chapter. The "Review All the 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.

- **Complete the Tables and Lists from Memory:** To help you memorize some lists of facts, many of the more important lists and tables from the chapter are included in a document on the companion website. This document lists only partial information, allowing you to complete the table or list.
- **Define Key Terms:** Although the exam is unlikely to ask you to define a term, the CCNA Cyber Ops exams do require that you learn and know a lot of networking 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.
- **Q&A:** Confirm that you understand the content you just covered.

- **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 14 core chapters—Chapters 1 through 14. Chapter 15 includes some preparation tips and suggestions for how to approach the exam. Each core chapter covers a subset of the topics on the CCNA Cyber Ops SECFND exam. The core chapters are organized into parts. They cover the following topics:

Part I: Network Concepts

- **Chapter 1: Fundamentals of Networking Protocols and Networking Devices** covers the networking technology fundamentals such as the OSI model and different protocols, including IP, TCP, UDP, ICMP, DNS, DHCP, ARP, and others. It also covers the basic operations of network infrastructure devices such as routers, switches, hubs, wireless access points, and wireless LAN controllers.
- **Chapter 2: Network Security Devices and Cloud Services** covers the fundamentals of firewalls, intrusion prevention systems (IPSs), Advance Malware Protection (AMP), and fundamentals of the Cisco Web Security Appliance (WSA), Cisco Cloud Web Security (CWS), Cisco Email Security Appliance (ESA), and the Cisco Cloud Email Security (CES) service. This chapter also describes the operation of access control lists applied as packet filters on the interfaces of network devices and compares and contrasts deep packet inspection with packet filtering and stateful firewall operations. It provides details about inline traffic interrogation and taps or traffic mirroring. This chapter compares and contrasts the characteristics of data obtained from taps or traffic mirroring and NetFlow in the analysis of network traffic.

Part II: Security Concepts

- **Chapter 3: Security Principles** covers the principles of the defense-in-depth strategy and compares and contrasts the concepts of risks, threats, vulnerabilities, and exploits. This chapter also defines threat actor, runbook automation (RBA), chain of custody

(evidentiary), reverse engineering, sliding window anomaly detection, personally identifiable information (PII), protected health information (PHI), as well as the principle of least privilege and how to perform separation of duties. It also covers the concepts of risk scoring, risk weighting, risk reduction, and how to perform overall risk assessments.

- **Chapter 4: Introduction to Access Controls** covers the foundation of access control and management. It provides an overview of authentication, authorization, and accounting principles, and introduces some of the most used access control models, including discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), and attribute-based access control (ABAC). Also, this chapter covers the actual implementation of access control, such as AAA protocols, port security, 802.1x, Cisco TrustSec, intrusion prevention and detection, and antimalware.
- **Chapter 5: Introduction to Security Operations Management** covers the foundation of security operations management. Specifically, it provides an overview of identity management, protocol and technologies, asset security management, change and configuration management, mobile device management, event and logging management, including Security Information and Event Management (SIEM) technologies, vulnerability management, and patch management.

Part III: Cryptography

- **Chapter 6: Fundamentals of Cryptography and Public Key Infrastructure (PKI)** covers the different hashing and encryption algorithms in the industry. It provides a comparison of symmetric and asymmetric encryption algorithms and an introduction of public key infrastructure (PKI), the operations of a PKI, and an overview of the IPsec, SSL, and TLS protocols.
- **Chapter 7: Introduction to Virtual Private Networks (VPNs)** provides an introduction to remote access and site-to-site VPNs, different deployment scenarios, and the VPN solutions provided by Cisco.

Part IV: Host-based Analysis

- **Chapter 8: Windows-Based Analysis** covers the basics of how a system running Windows handles applications. This includes details about how memory is used as well as how resources are processed by the operating system. These skills are essential for maximizing performance and securing a Windows system.
- **Chapter 9: Linux- and Mac OS X–Based Analysis** covers how things work inside a UNIX environment. This includes process execution and event logging. Learning how the environment functions will not only improve your technical skills but can also be used to build a strategy for securing these systems.
- **Chapter 10: Endpoint Security Technologies** covers the functionality of endpoint security technologies, including host-based intrusion detection, host-based firewalls, application-level whitelisting and blacklisting, as well as systems-based sandboxing.

Part V: Security Monitoring and Attack Methods

- **Chapter 11: Network and Host Telemetry** covers the different types of data provided by network and host-based telemetry technologies, including NetFlow, traditional and next-generation firewalls, packet captures, application visibility and control, and web

and email content filtering. It also provides an overview of how full packet captures, session data, transaction logs, and security alert data are used in security operations and security monitoring.

- **Chapter 12: Security Monitoring Operational Challenges** covers the different operational challenges, including Tor, access control lists, tunneling, peer-to-peer (P2P) communication, encapsulation, load balancing, and other technologies.
- **Chapter 13: Types of Attacks and Vulnerabilities** covers the different types of cyber security attacks and vulnerabilities and how they are carried out by threat actors nowadays.
- **Chapter 14: Security Evasion Techniques** covers how attackers obtain stealth as well as the tricks used to negatively impact detection and forensic technologies. Topics include encryption, exhausting resources, fragmenting traffic, manipulating protocols, and pivoting within a compromised environment.

Part VI: Final Preparation

- **Chapter 15: Final Preparation** identifies the tools for final exam preparation and helps you develop an effective study plan. It contains tips on how to best use the web-based material to study.

Part VII: Appendixes

- **Appendix A: Answers to the "Do I Know This Already?" Quizzes and Q&A Questions** includes the answers to all the questions from Chapters 1 through 14.
- **Appendix B: Memory Tables** (a website-only appendix) contains the key tables and lists from each chapter, with some of the contents removed. You can print this appendix and, as a memory exercise, complete the tables and lists. The goal is to help you memorize facts that can be useful on the exam. This appendix is available in PDF format at the book website; it is not in the printed book.
- **Appendix C: Memory Tables Answer Key** (a website-only appendix) contains the answer key for the memory tables in Appendix B. This appendix is available in PDF format at the book website; it is not in the printed book.
- **Appendix D: Study Planner** is a spreadsheet, available from the book website, with major study milestones, where you can track your progress throughout your study.

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 authors that provide further insight into the more troublesome topics on the exam. 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 9781587147029.
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 the 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 containing 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 software.

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, simply follow these steps:

1. Go to http://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 or CiscoPress.com, you will need to 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.
6. The product will now be listed in your My Products page. Click the **Exams** button to launch the exam settings screen and start your exam.

Accessing the Pearson Test Prep Software Offline

If you wish 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 just enter the following link in your browser:

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

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

1. Register your book by going to PearsonITCertification.com/register and entering the ISBN 9781587147029.
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. Once the software finishes downloading, 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. Once the installation is complete, launch the application and select **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 the **Finish** button to download the exam data to your application.
12. You can now 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 synch together, so saved exams and grade results recorded on one version will be available to you on the other as well.

Customizing Your Exams

Once 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 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 will not provide the detailed score reports that the other two modes will, so it should not be used 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 a specific part in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters 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, it will check to see if there are any updates to your exam data and automatically download any changes that were made since the last time you used the software. This requires that you are connected to the Internet at the time you launch 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 exam.

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

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

This chapter covers the following topics:

- Describe the principles of the defense-in-depth strategy.
- What are threats, vulnerabilities, and exploits?
- Describe Confidentiality, Integrity, and Availability.
- Describe risk and risk analysis.
- Define what personally identifiable information (PII) and protected health information (PHI) are.
- What are the principles of least privilege and separation of duties?
- What are security operation centers (SOCs)?
- Describe cyber forensics.

CHAPTER 3

Security Principles

This chapter covers the principles of the defense-in-depth strategy and compares and contrasts the concepts of risk, threats, vulnerabilities, and exploits. This chapter also defines what are threat actors, run book automation (RBA), chain of custody (evidentiary), reverse engineering, sliding window anomaly detection, Personally Identifiable Information (PII), Protected Health Information (PHI), as well as what is the principle of least privilege, and how to perform separation of duties. It also covers concepts of risk scoring, risk weighting, risk reduction, and how to perform overall risk assessments.

"Do I Know This Already?" Quiz

The "Do I Know This Already?" quiz helps you identify your strengths and deficiencies in this chapter's topics. The 11-question quiz, derived from the major sections in the "Foundation Topics" portion of the chapter, helps you determine how to spend your limited study time. You can find the answers in Appendix A Answers to the "Do I Know This Already?" Quizzes and Q&A Questions.

Table 3-1 outlines the major topics discussed in this chapter and the "Do I Know This Already?" quiz questions that correspond to those topics.

Table 3-1 "Do I Know This Already?" Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions Covered in This Section
The Principles of the Defense-in-Depth Strategy	1–2
What Are Threats, Vulnerabilities, and Exploits?	3–6
Risk and Risk Analysis	7
Personally Identifiable Information and Protected Health Information	8
Principle of Least Privilege and Separation of Duties	9
Security Operation Centers	10
Forensics	11

1. What is one of the primary benefits of a defense-in-depth strategy?
   - **a.** You can deploy advanced malware protection to detect and block advanced persistent threats.
   - **b.** You can configure firewall failover in a scalable way.
   - **c.** Even if a single control (such as a firewall or IPS) fails, other controls can still protect your environment and assets.
   - **d.** You can configure intrusion prevention systems (IPSs) with custom signatures and auto-tuning to be more effective in the network.

2. Which of the following planes is important to understand for defense in depth?
   a. Management plane
   b. Failover plane
   c. Control plane
   d. Clustering
   e. User/data plane
   f. Services plane
3. Which of the following are examples of vulnerabilities?
   a. Advanced threats
   b. CVSS
   c. SQL injection
   d. Command injection
   e. Cross-site scripting (XSS)
   f. Cross-site request forgery (CSRF)
4. What is the Common Vulnerabilities and Exposures (CVE)?
   a. An identifier of threats
   b. A standard to score vulnerabilities
   c. A standard maintained by OASIS
   d. A standard for identifying vulnerabilities to make it easier to share data across tools, vulnerability repositories, and security services
5. Which of the following is true when describing threat intelligence?
   a. Threat intelligence's primary purpose is to make money by exploiting threats.
   b. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats.
   c. With threat intelligence, threat actors can become more efficient to carry out attacks.
   d. Threat intelligence is too difficult to obtain.
6. Which of the following is an open source feed for threat data?
   a. Cyber Squad ThreatConnect
   b. BAE Detica CyberReveal
   c. MITRE CRITs
   d. Cisco AMP Threat Grid

7. What is the Common Vulnerability Scoring System (CVSS)?
   a. A scoring system for exploits.
   b. A tool to automatically mitigate vulnerabilities.
   c. A scoring method that conveys vulnerability severity and helps determine the urgency and priority of response.
   d. A vulnerability-mitigation risk analysis tool.

8. Which of the following are examples of personally identifiable information (PII)?
   a. Social security number
   b. Biological or personal characteristics, such as an image of distinguishing features, fingerprints, x-rays, voice signature, retina scan, and geometry of the face
   c. CVE
   d. Date of birth

9. Which of the following statements are true about the principle of least privilege?
   a. Principle of least privilege and separation of duties can be considered to be the same thing.
   b. The principle of least privilege states that all users—whether they are individual contributors, managers, directors, or executives—should be granted only the level of privilege they need to do their job, and no more.
   c. Programs or processes running on a system should have the capabilities they need to "get their job done," but no root access to the system.
   d. The principle of least privilege only applies to people.

10. What is a runbook?
    a. A runbook is a collection of processes running on a system.
    b. A runbook is a configuration guide for network security devices.
    c. A runbook is a collection of best practices for configuring access control lists on a firewall and other network infrastructure devices.
    d. A runbook is a collection of procedures and operations performed by system administrators, security professionals, or network operators.

11. Chain of custody is the way you document and preserve evidence from the time you started the cyber forensics investigation to the time the evidence is presented at court. Which of the following is important when handling evidence?
    a. Documentation about how and when the evidence was collected
    b. Documentation about how evidence was transported
    c. Documentation about who had access to the evidence and how it was accessed
    d. Documentation about the CVSS score of a given CVE

Foundation Topics

In this chapter, you will learn the different cyber security principles, including what threats, vulnerabilities, and exploits are. You will also learn details about what defense in depth is and how to perform risk analysis. This chapter also provides an overview of what runbooks are and how to perform runbook automation (RBA).

When you are performing incident response and forensics tasks, you always have to be aware of how to collect evidence and what the appropriate evidentiary chain of custody is. This chapter provides an overview of chain of custody when it pertains to cyber security investigations. You will learn the details about reverse engineering, forensics, and sliding window anomaly detection. You will also learn what personally identifiable information (PII) and protected health information (PHI) are, especially pertaining to different regulatory standards such as the Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA).

In this chapter, you will also learn the concepts of principle of least privilege. It is important to know how to perform risk scoring and risk weighting in the realm of risk assessment and risk reduction. This chapter provides an overview of these risk assessment and risk reduction methodologies.

The Principles of the Defense-in-Depth Strategy

If you are a cyber security expert, or even an amateur, you probably already know that when you deploy a firewall or an intrusion prevention system (IPS) or install antivirus or advanced malware protection on your machine, you cannot assume you are now safe and secure. A layered and cross-boundary "defense-in-depth" strategy is what is needed to protect your network and corporate assets. One of the primary benefits of a defense-in-depth strategy is that even if a single control (such as a firewall or IPS) fails, other controls can still protect your environment and assets. Figure 3-1 illustrates this concept.

The following are the layers illustrated in Figure 3-1 (starting from the top):

- Nontechnical activities such as appropriate security policies and procedures, and end-user and staff training.
- Physical security, including cameras, physical access control (such as badge readers, retina scanners, and fingerprint scanners), and locks.
- Network security best practices, such as routing protocol authentication, control plane policing (CoPP), network device hardening, and so on.
- Host security solutions such as advanced malware protection (AMP) for endpoints, antiviruses, and so on.
- Application security best practices such as application robustness testing, fuzzing, defenses against cross-site scripting (XSS), cross-site request forgery (CSRF) attacks, SQL injection attacks, and so on.
- The actual data traversing the network. You can employ encryption at rest and in transit to protect data.

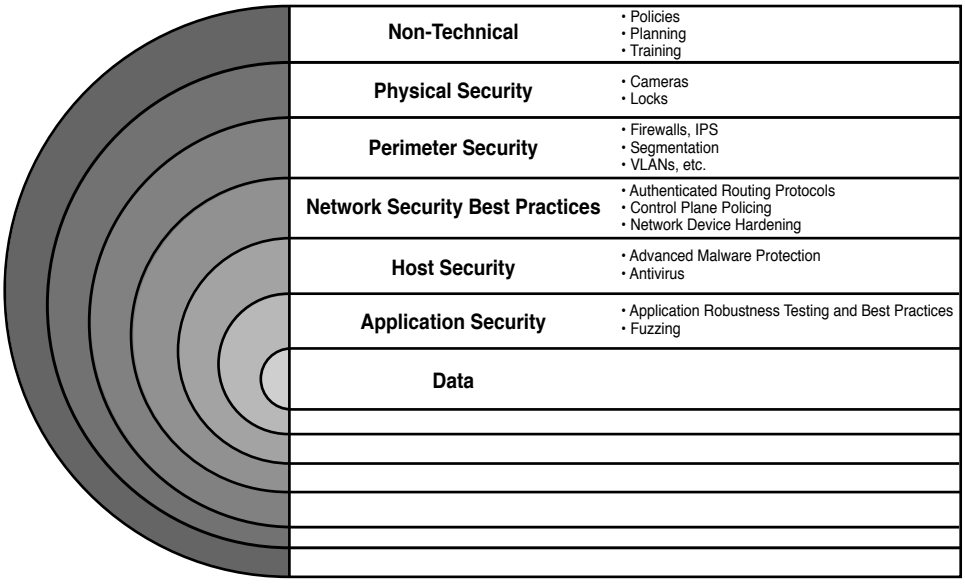

Figure 3-1 *Defense in Depth*

TIP Each layer of security introduces complexity and latency, while requiring that someone manage it. The more people are involved, even in administration, the more attack vectors you create, and the more you distract your people from possibly more important tasks. Employ multiple layers, but avoid duplication—and use common sense.

The first step in the process of preparing your network and staff to successfully identify security threats is achieving complete network visibility. You cannot protect against or mitigate what you cannot view/detect. You can achieve this level of network visibility through existing features on network devices you already have and on devices whose potential you do not even realize. In addition, you should create strategic network diagrams to clearly illustrate your packet flows and where, within the network, you could enable security mechanisms to identify, classify, and mitigate the threats. Remember that network security is a constant war. When defending against the enemy, you must know your own territory and implement defense mechanisms.

In some cases, onion-like diagrams are used to help illustrate and analyze what "defense-in-depth" protections and enforcements should be deployed in a network. Figure 3-2 shows an example of one of these onion diagrams, where network resources are protected through several layers of security.

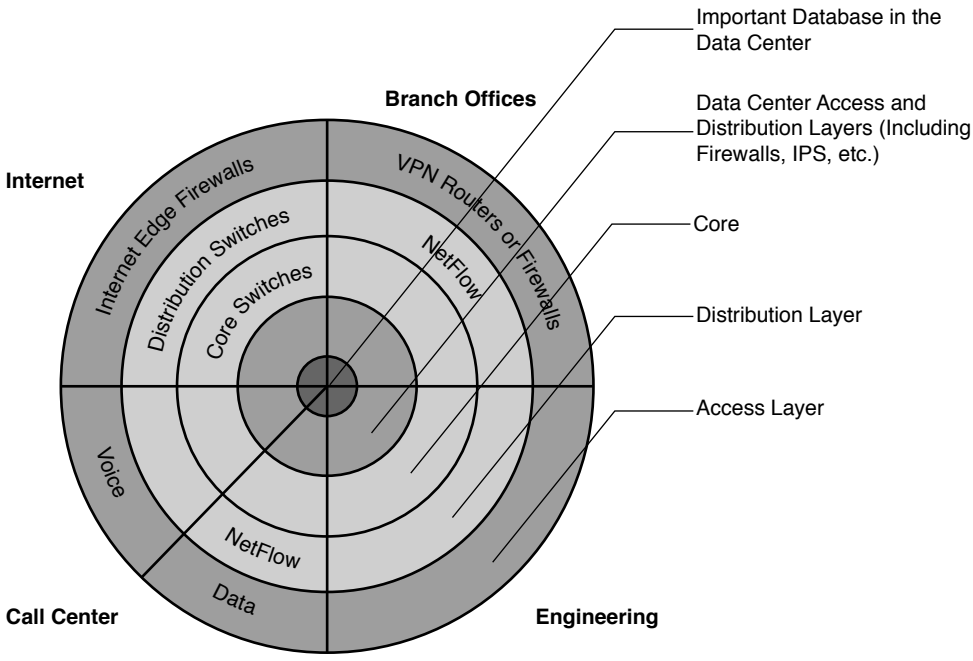

Figure 3-2 *Layered Onion Diagram Example*

You can create this type of diagram, not only to understand the architecture of your organization, but also to strategically identify places within the infrastructure where you can implement telemetry mechanisms such as NetFlow and identify choke points where you can mitigate an incident. Notice that the access, distribution, and core layers/boundaries are clearly defined.

These types of diagrams also help you visualize operational risks within your organization. The diagrams can be based on device roles and can be developed for critical systems you want to protect. For example, identify a critical system within your organization and create a layered diagram similar to the one in Figure 3-2. In this example, an "important database in the data center" is the most critical application/data source for this company. The diagram includes the database in the center.

You can also use this type of diagram to audit device roles and the types of services they should be running. For example, you can decide in what devices you can run services such as Cisco NetFlow or where to enforce security policies. In addition, you can see the life of a packet within your infrastructure, depending on the source and destination. An example is illustrated in Figure 3-3.

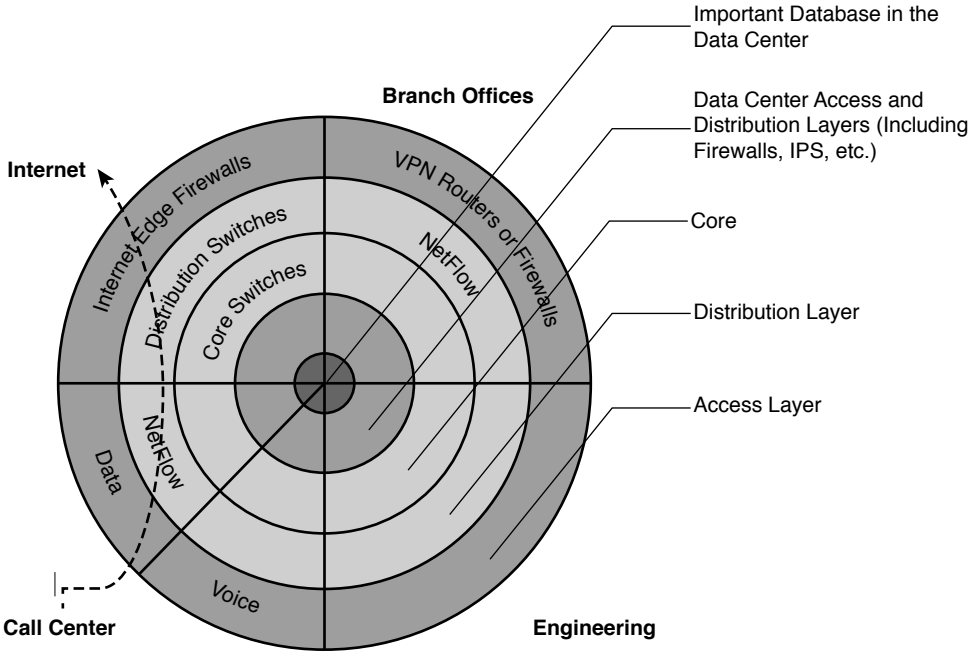

Figure 3-3 *Layered Onion Diagram Example*

In Figure 3-3, you can see a packet flow that occurs when a user from the call center accesses an Internet site. You know exactly where the packet is going based on your architecture as well as your security and routing policies. This is a simple example; however, you can use this concept to visualize risks and to prepare your isolation policies.

When applying defense-in-depth strategies, you can also look at a roles-based network security approach for security assessment in a simple manner. Each device on the network serves a purpose and has a role; subsequently, you should configure each device accordingly. You can think about the different planes as follows:

- **Management plane**: This is the distributed and modular network management environment.
- **Control plane**: This plane includes routing control. It is often a target because the control plane depends on direct CPU cycles.
- **User/data plane**: This plane receives, processes, and transmits network data among all network elements.
- **Services plane**: This is the Layer 7 application flow built on the foundation of the other layers.
- **Policies**: The plane includes the business requirements. Cisco calls policies the "business glue" for the network. Policies and procedures are part of this section, and they apply to all the planes in this list.

You should also view security in two different perspectives, as illustrated in Figure 3-4:

- Operational (reactive) security
- Proactive security

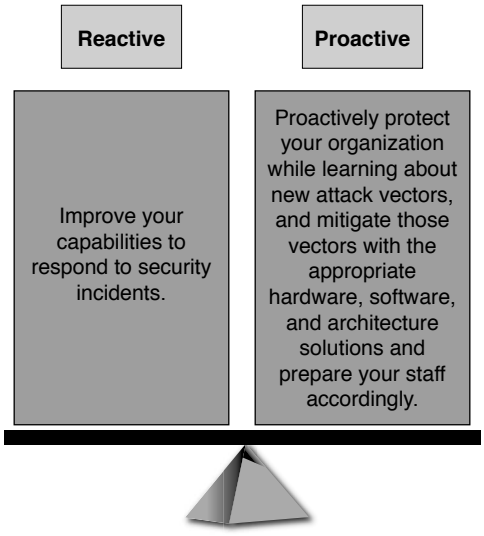

Figure 3-4 *Reactive vs. Proactive Security*

You should have a balance between proactive and reactive security approaches. Prepare your network, staff, and organization as a whole to better identify, classify, trace back, and react to security incidents. In addition, proactively protect your organization while learning about new attack vectors, and mitigate those vectors with the appropriate hardware, software, and architecture solutions.

What Are Threats, Vulnerabilities, and Exploits?

In this section, you will learn the difference between vulnerabilities, threats, and exploits.

Vulnerabilities

Key Topic

A *vulnerability* is an exploitable weakness in a system or its design. Vulnerabilities can be found in protocols, operating systems, applications, hardware, and system designs. Vulnerabilities abound, with more discovered every day. You will learn many examples of vulnerability classifications in Chapter 13, "Types of Attacks and Vulnerabilities." However, the following are a few examples:

- SQL injection vulnerabilities
- Command injections
- Cross-site scripting (XSS)
- Cross-site request forgery (CSRF)
- API abuse vulnerabilities

- Authentication vulnerabilities
- Privilege escalation vulnerabilities
- Cryptographic vulnerabilities
- Error-handling vulnerabilities
- Input validation vulnerabilities
- Path traversal vulnerabilities
- Buffer overflows
- Deserialization of untrusted data
- Directory restriction error
- Double free
- Password management: hardcoded password
- Password plaintext storage

Vendors, security researchers, and vulnerability coordination centers typically assign vulnerabilities an identifier that's disclosed to the public. This identifier is known as the *Common Vulnerabilities and Exposures (CVE)*. CVE is an industry-wide standard. CVE is sponsored by US-CERT, the office of Cybersecurity and Communications at the U.S. Department of Homeland Security. Operating as DHS's Federally Funded Research and Development Center (FFRDC), MITRE has copyrighted the CVE List for the benefit of the community in order to ensure it remains a free and open standard, as well as to legally protect the ongoing use of it and any resulting content by government, vendors, and/or users. MITRE maintains the CVE list and its public website, manages the CVE Compatibility Program, oversees the CVE Naming Authorities (CNAs), and provides impartial technical guidance to the CVE Editorial Board throughout the process to ensure CVE serves the public interest.

The goal of CVE is to make it easier to share data across tools, vulnerability repositories, and security services.

More information about CVE is available at http://cve.mitre.org.

Threats

Key Topic

A *threat* is any potential danger to an asset. If a vulnerability exists but has not yet been exploited—or, more importantly, it is not yet publicly known—the threat is latent and not yet realized. If someone is actively launching an attack against your system and successfully accesses something or compromises your security against an asset, the threat is realized. The entity that takes advantage of the vulnerability is known as the *malicious actor*, and the path used by this actor to perform the attack is known as the *threat agent* or *threat vector*.

A *countermeasure* is a safeguard that somehow mitigates a potential risk. It does so by either reducing or eliminating the vulnerability, or it at least reduces the likelihood of the threat agent to actually exploit the risk. For example, you might have an unpatched machine on your network, making it highly vulnerable. If that machine is unplugged from the network and ceases to have any interaction through exchanging data with any other device, you have

successfully mitigated all those vulnerabilities. You have likely rendered that machine no longer an asset, though—but it is safer.

Threat Actors

Key Topic

Threat actors are the individuals (or group of individuals) who perform an attack or are responsible for a security incident that impacts or has the potential of impacting an organization or individual. There are several types of threat actors:

- **Script kiddies**: People who uses existing "scripts" or tools to hack into computers and networks. They lack the expertise to write their own scripts.
- **Organized crime groups**: Their main purpose is to steal information, scam people, and make money.
- **State sponsors and governments**: These agents are interested in stealing data, including intellectual property and research-and-development data from major manufacturers, government agencies, and defense contractors.
- **Hacktivists**: People who carry out cyber security attacks aimed at promoting a social or political cause.
- **Terrorist groups**: These groups are motivated by political or religious beliefs.

Threat Intelligence

Key Topic

Threat intelligence is referred to as the knowledge about an existing or emerging threat to assets, including networks and systems. Threat intelligence includes context, mechanisms, indicators of compromise (IoCs), implications, and actionable advice. Threat intelligence is referred to as the information about the observables, indicators of compromise (IoCs) intent, and capabilities of internal and external threat actors and their attacks. Threat intelligence includes specifics on the tactics, techniques, and procedures of these adversaries. Threat intelligence's primary purpose is to inform business decisions regarding the risks and implications associated with threats.

Converting these definitions into common language could translate to threat intelligence being evidence-based knowledge of the capabilities of internal and external threat actors. This type of data can be beneficial for the security operations center (SOC) of any organization. Threat intelligence extends cyber security awareness beyond the internal network by consuming intelligence from other sources Internet-wide related to possible threats to you or your organization. For instance, you can learn about threats that have impacted different external organizations. Subsequently, you can proactively prepare rather than react once the threat is seen against your network. Providing an enrichment data feed is one service that threat intelligence platforms would typically provide.

Forrester defines a five-step threat intelligence process (see Figure 3-5) for evaluating threat intelligence sources:

Step 1. Planning and direction

Step 2. Collection

Step 3. Processing

Step 4. Analysis and production

Step 5. Dissemination

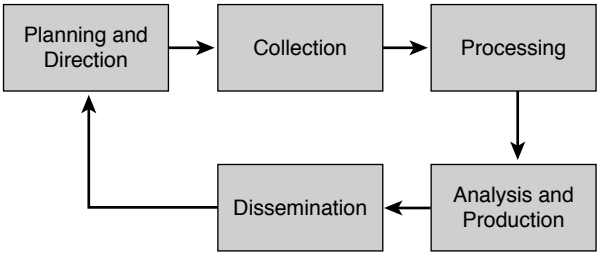

Figure 3-5 *Threat Intelligence*

Many different threat intelligence platforms and services are available in the market nowadays. Cyber threat intelligence focuses on providing actionable information on adversaries, including indicators of compromise (IoCs). Threat intelligence feeds help you prioritize signals from internal systems against unknown threats. Cyber threat intelligence allows you to bring more focus to cyber security investigation because instead of blindly looking for "new" and "abnormal" events, you can search for specific IoCs, IP addresses, URLs, or exploit patterns. The following are a few examples:

- **Cyber Squad ThreatConnect:** An on-premises, private, or public cloud solution offering threat data collection, analysis, collaboration, and expertise in a single platform. You can obtain more details at http://www.threatconnect.com.
- **BAE Detica CyberReveal:** A multithreat monitoring, analytics, investigation, and response product. CyberReveal brings together BAE Systems Detica's heritage in network intelligence, big-data analytics, and cyber threat research. CyberReveal consists of three core components: platform, analytics, and investigator. Learn more at http://www.baesystems.com.
- **Lockheed Martin Palisade:** Supports comprehensive threat collection, analysis, collaboration, and expertise in a single platform. Learn more at http://www.lockheedmartin.com.
- **MITRE CRITs:** Collaborative Research Into Threats (CRITs) is an open source feed for threat data. Learn more at https://crits.github.io.
- **Cisco AMP Threat Grid:** Combines static and dynamic malware analysis with threat intelligence into one unified solution.

A number of standards are being developed for disseminating threat intelligence information. The following are a few examples:

- **Structured Threat Information eXpression (STIX):** An express language designed for sharing of cyber attack information. STIX details can contain data such as the IP address of command-and-control servers (CnC), malware hashes, and so on. STIX was originally developed by MITRE and is now maintained by OASIS. You can obtain more information at http://stixproject.github.io.

- **Trusted Automated eXchange of Indicator Information (TAXII):** An open transport mechanism that standardizes the automated exchange of cyber threat information. TAXII was originally developed by MITRE and is now maintained by OASIS. You can obtain more information at http://taxiiproject.github.io.
- **Cyber Observable eXpression (CybOX):** A free standardized schema for specification, capture, characterization, and communication of events of stateful properties that are observable in the operational domain. CybOX was originally developed by MITRE and is now maintained by OASIS. You can obtain more information at https://cyboxproject.github.io.
- **Open Indicators of Compromise (OpenIOC):** An open framework for sharing threat intelligence in a machine-digestible format. Learn more at http://www.openioc.org.

It should be noted that many open source and non-security-focused sources can be leveraged for threat intelligence as well. Some examples of these sources are social media, forums, blogs, and vendor websites.

Exploits

Key Topic

An *exploit* is software or a sequence of commands that takes advantage of a vulnerability in order to cause harm to a system or network. There are several methods of classifying exploits; however, the most common two categories are remote and local exploits. A *remote exploit* can be launched over a network and carries out the attack without any prior access to the vulnerable device or software. A *local exploit* requires the attacker or threat actor to have prior access to the vulnerable system.

NOTE Exploits are commonly categorized and named by the type of vulnerability they exploit.

There is also the concept of exploit kits. An *exploit kit* is a compilation of exploits that are often designed to be served from web servers. Their main purpose is identifying software vulnerabilities in client machines and then exploiting such vulnerabilities to upload and execute malicious code on the client. The following are a few examples of known exploit kits:

- Angler
- MPack
- Fiesta
- Phoenix
- Blackhole
- Crimepack
- RIG

NOTE Cisco Talos has covered and explained numerous exploit kits in detail, including Angler. You can obtain more information about these type of threats at Talos's blog, http://blog.talosintel.com, and specifically for Angler at http://blog.talosintel.com/search/label/angler.

Confidentiality, Integrity, and Availability: The CIA Triad

Key Topic

Confidentiality, integrity and availability, is often referred to as the CIA triad. This is a model that was created to define security policies. In some cases, you may also see this model referred to as the AIC triad (availability, integrity and confidentiality) to avoid confusion with the United States Central Intelligence Agency.

The idea is that confidentiality, integrity and availability should be guaranteed in any system that is considered secured.

Confidentiality

The ISO 27000 standard has a very good definition: "confidentiality is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes." One of the most common ways to protect the confidentiality of a system or its data is to use encryption. The Common Vulnerability Scoring System (CVSS) uses the CIA triad principles within the metrics used to calculate the CVSS base score.

NOTE You will learn more about CVSS throughout the following chapters, and you can obtain more information about CVSS at: https://www.first.org/cvss/specification-document

Integrity

Integrity is the ability to make sure that a system and its data has not been altered or compromised. It ensures that the data is an accurate and unchanged representation of the original secure data. Integrity applies not only to data, but also to systems. For instance, if a threat actor changes the configuration of a server, firewall, router, switch or any other infrastructure device, it is considered that he or she impacted the integrity of the system.

Availability

Availability refers that a system or application must be "available" to authorized users at all times. According to the CVSS version 3 specification, the availability metric "measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability. While the Confidentiality and Integrity impact metrics apply to the loss of confidentiality or integrity of data (e.g., information, files) used by the impacted component, this metric refers to the loss of availability of the impacted component itself, such as a networked service (e.g., web, database, email). Since availability refers to the accessibility of information resources, attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of an impacted component."

A common example of an attack that impacts availability is a denial of service (DoS) attack.

Risk and Risk Analysis

Key Topic

According to the Merriam-Webster dictionary, risk is "the possibility that something bad or unpleasant will happen." In the world of cyber security, risk can be defined as the possibility of a security incident (something bad) happening. There are many standards and methodologies for classifying and analyzing cyber security risks. The Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool (Assessment)

to help financial institutions identify their risks and determine their cyber security preparedness. This guidance/tool can be useful for any organization. The FFIEC tool provides a repeatable and measurable process for organizations to measure their cyber security readiness.

According to the FFIEC, the assessment consists of two parts:

- **Inherent Risk Profile and Cybersecurity Maturity**: The Inherent Risk Profile identifies the institution's inherent risk before implementing controls. The Cybersecurity Maturity includes domains, assessment factors, components, and individual declarative statements across five maturity levels to identify specific controls and practices that are in place. Although management can determine the institution's maturity level in each domain, the Assessment is not designed to identify an overall cyber security maturity level.
- **The International Organization for Standardization (ISO) 27001:** This is the international standard for implementing an information security management system (ISMS). ISO 27001 is heavily focused on risk-based planning to ensure that the identified information risks (including cyber risks) are appropriately managed according to the threats and the nature of those threats. ISO 31000 is the general risk management standard that includes principles and guidelines for managing risk. It can be used by any organization, regardless of its size, activity, or sector. Using ISO 31000 can help organizations increase the likelihood of achieving objectives, improve the identification of opportunities and threats, and effectively allocate and use resources for risk treatment.

  The ISO/IEC 27005 standard is more focused on cyber security risk assessment. It is titled "Information technology—Security techniques—Information security risk management."

  The following is according to ISO's website:

  "The standard doesn't specify, recommend or even name any specific risk management method. It does however imply a continual process consisting of a structured sequence of activities, some of which are iterative:

  - Establish the risk management context (e.g. the scope, compliance obligations, approaches/methods to be used and relevant policies and criteria such as the organization's risk tolerance or appetite);
  - Quantitatively or qualitatively assess (i.e. identify, analyze and evaluate) relevant information risks, taking into account the information assets, threats, existing controls and vulnerabilities to determine the likelihood of incidents or incident scenarios, and the predicted business consequences if they were to occur, to determine a 'level of risk;'
  - Treat (i.e. modify [use information security controls], retain [accept], avoid and/or share [with third parties]) the risks appropriately, using those 'levels of risk' to prioritize them;
  - Keep stakeholders informed throughout the process; and
  - Monitor and review risks, risk treatments, obligations and criteria on an ongoing basis, identifying and responding appropriately to significant changes."

There are also standards to score the overall "risk" of a vulnerability. The most commonly used is the Common Vulnerability Scoring System (CVSS) developed by the Forum of Incident Response and Security Teams (FIRST). CVSS is a standards-based scoring method

that conveys vulnerability severity and helps determine the urgency and priority of response. CVSS is used by many Product Security Incident Response Teams (PSIRTs), vulnerability coordination centers, security researchers, and consumers of security vulnerability information.

NOTE You will learn about CVSS in more detail in Chapter 5, "Introduction to Security Operations Management," and can obtain more information at FIRST's website, https://www.first.org/cvss.

There are also several additional scoring systems:

- **Common Weakness Scoring System (CWSS):** A methodology for scoring software weaknesses. CWSS is part of the Common Weakness Enumerator (CWE) standard. More information about CWSS is available at http://cwe.mitre.org/cwss.
- **Common Misuse Scoring System (CMSS):** A standardized way to measure software feature misuse vulnerabilities. More information about CMSS is available at http://scap.nist.gov/emerging-specs/listing.html#cmss.
- **Common Configuration Scoring System (CCSS):** More information about CCSS can be found at http://csrc.nist.gov/publications/nistir/ir7502/nistir-7502_CCSS.pdf.

Personally Identifiable Information and Protected Health Information

Many regulations as well as the United States government require organizations to identify personally identifiable information (PII) and protected health information (PHI) and handle them in a secure manner. Unauthorized release or loss of such data could result in severe fines and penalties for the organization. Given the importance of PII and PHI, regulators and the government want to oversee the usage more efficiently. This section explains what PII and PHI are.

PII

Key Topic

According to the Executive Office of the President, Office of Management and Budget (OMB) and the U.S. Department of Commerce, Office of the Chief Information Officer, PII refers to "information which can be used to distinguish or trace an individual's identity." The following are a few examples:

- The individual's name
- Social security number
- Biological or personal characteristics, such as an image of distinguishing features, fingerprints, x-rays, voice signature, retina scan, and the geometry of the face
- Date and place of birth
- Mother's maiden name
- Credit card numbers
- Bank account numbers

- Driver license number
- Address information, such as email addresses or street addresses, and telephone numbers for businesses or personal use

PHI

Key Topic

The Health Insurance Portability and Accountability Act (HIPAA) requires health care organizations and providers to adopt certain security regulations for protecting health information. The Privacy Rule calls this information "protected health information," or PHI. This information includes, but is not limited to, the following:

- Individual's name (that is, patient's name)
- All dates directly linked to an individual, including date of birth, death, discharge, and administration
- Telephone and fax numbers
- Email addresses and geographic subdivisions such as street addresses, ZIP Codes, and county.
- Medical record numbers and health plan beneficiary numbers
- Certificate numbers or account numbers
- Social security number
- Driver license number
- Biometric identifiers, including voice or fingerprints
- Photos of the full face or recognizable features
- Any unique number-based code or characteristic
- The individual's past, present, and future physical or mental health or condition
- The provision of health care to the individual, or the past, present, or future payment for the provision of health care to the individual

Principle of Least Privilege and Separation of Duties

Key Topic

Two additional key concepts in information security are the principle of least privilege and separation of duties. This section defines these two key concepts.

Principle of Least Privilege

The principle of least privilege states that all users—whether they are individual contributors, managers, directors, or executives—should be granted only the level of privilege they need to do their jobs, and no more. For example, a sales account manager really has no business having administrator privileges over the network, or a call center staff member over critical corporate financial data.

The same concept of principle of least privilege can be applied to software. For example, programs or processes running on a system should have the capabilities they need to "get their job done," but no root access to the system. If a vulnerability is exploited on a system that runs "everything as root," the damage could extend to a complete compromise of the

system. This is why you should always limit users, applications, and processes to access and run as the least privilege they need.

TIP Somewhat related to the principle of least privilege is the concept of "need to know," which means that users should get access only to data and systems that they need to do their job, and no other.

Separation of Duties

Separation of duties is an administrative control that dictates that a single individual should not perform all critical- or privileged-level duties. Additionally, important duties must be separated or divided among several individuals within the organization. The goal is to safeguard against a single individual performing sufficiently critical or privileged actions that could seriously damage a system or the organization as a whole. For instance, security auditors responsible for reviewing security logs should not necessarily have administrative rights over the systems. Another example is that a network administrator should not have the ability to alter logs on the system. This is to prevent such individuals from carrying out unauthorized actions and then deleting evidence of such action from the logs (in other words, covering their tracks).

Think about two users having two separate keys in order to open a safety deposit box. Separation of duties is similar to that concept, where the safety deposit box cannot be opened by a user without the other key.

Security Operation Centers

Key Topic

Security operation centers (SOCs) are facilities where an organization's assets, including applications, databases, servers, networks, desktops, and other endpoints, are monitored, assessed, and protected. Establishing SOC capabilities requires careful planning. The planning phase helps you decide on and formalize yourself with the objectives that justify having an SOC, and to develop a roadmap you can use to track your progress against those predefined objectives. The success of any security program (including the SOC) depends on proper planning. There are always challenges that are specific to an organization, and these challenges are introduced because of issues related to governance, collaboration, lack of tools, lack of automation, lack of threat intelligence, skill sets, and so on. Such challenges must be identified and treated, or at least acknowledged, at an early stage of an SOC establishment program. SOCs are created to be able to address the following challenges:

- How can you detect a compromise in a timely manner?
- How do you triage a compromise to determine the severity and the scope?
- What is the impact of the compromise to your business?
- Who is responsible for detecting and mitigating a compromise?
- Who should be informed or involved, and when do you deal with the compromise once detected?
- How and when should you communicate a compromise internally or externally, and is that needed in the first place?

To build and operate an effective SOC, you must have the following:

- Executive sponsorship.
- SOC operating as a program. Organizations should operate the SOC as a program rather than a single project. Doing so depends on the criticality and the amount of resources required to design, build, and operate the various services offered by the SOC. Having a clear SOC service strategy with clear goals and priorities will shape the size of the SOC program, timeline, and the amount of resources required to deliver the program objectives.
- A governance structure. Metrics must be established to measure the effectiveness of the SOC capabilities. These metrics should provide sufficient and relevant visibility to the organization's management team on the performance of the SOC and should identify areas where improvements and investments are needed.
- Effective team collaboration.
- Access to data and systems.
- Applicable processes and procedures.
- Team skill sets and experience.
- Budget (for example, will it be handled in-house or outsourced?).

Runbook Automation

Organizations need to have capabilities to define, build, orchestrate, manage, and monitor the different operational processes and workflows. This is achieved by implementing runbooks and runbook automation (RBA). A *runbook* is a collection of procedures and operations performed by system administrators, security professionals, or network operators. According to Gartner, "the growth of RBA has coincided with the need for IT operations executives to enhance IT operations efficiency measures." Gartner, Inc. is an American research and advisory firm providing information technology related insight for IT and other business leaders.

Here are some of the metrics to measure effectiveness:

- Mean time to repair (MTTR)
- Mean time between failures (MTBF)
- Mean time to discover a security incident
- Mean time to contain or mitigate a security incident
- Automating the provisioning of IT resources

Many different commercial and open source RBA solutions are available in the industry. An example of a popular open source RBA solution is Rundeck (http://rundeck.org/). Rundeck can be integrated with configuration management platforms such as Chef, Puppet, and Ansible. A commercial RBA example is the Cisco Workload Automation (CWA), which can manage different business processes across a comprehensive set of applications and systems. You can obtain more information about Cisco CWA at http://www.cisco.com/c/en/us/products/analytics-automation-software/tidal-enterprise-scheduler/index.html.

Forensics

The United States Computer Emergency Response Team (CERT) defines cyber forensics as follows:

> "If you manage or administer information systems and networks, you should understand cyber forensics. Forensics is the process of using scientific knowledge for collecting, analyzing, and presenting evidence to the courts. (The word forensics means 'to bring to the court.') Forensics deals primarily with the recovery and analysis of latent evidence. Latent evidence can take many forms, from fingerprints left on a window to DNA evidence recovered from blood stains to the files on a hard drive."

Cyber forensics is often referred to as "computer forensics." However, "cyber forensics" is a more appropriate term than "computer forensics."

The two primary objectives in cyber forensics are to find out what happened and to collect data in a manner that is acceptable to the court. Any device that can store data is potentially the object of cyber forensics, including, but not limited to, the following:

- Computers (servers, desktop machines, and so on)
- Smartphones
- Tablets
- Network infrastructure devices (routers, switches, firewalls, intrusion prevention systems)
- Network management systems
- Printers
- Even vehicle GPSs

Chain of custody is critical to forensics investigations. The following section describes chain of custody in detail.

Evidentiary Chain of Custody

Key Topic

Chain of custody is the way you document and preserve evidence from the time that you started the cyber forensics investigation to the time the evidence is presented at court. It is extremely important to be able to show clear documentation of the following:

- How the evidence was collected
- When it was collected
- How it was transported
- How is was tracked
- How it was stored
- Who had access to the evidence and how it was accessed

TIP If you fail to maintain proper chain of custody, it is likely you cannot use that evidence in court. It is also important to know how to dispose of evidence after an investigation.

When you collect evidence, you must protect its integrity. This involves making sure that nothing is added to the evidence and that nothing is deleted or destroyed (this is known as *evidence preservation*).

TIP A method often used for evidence preservation is to only work with a copy of the evidence—in other words, not directly working with the evidence itself. This involves creating an image of any hard drive or any storage device.

Several forensics tools are available on the market. The following are two of the most popular:

- Guidance Software's EnCase (https://www.guidancesoftware.com/)
- AccessData's Forensic Toolkit (http://accessdata.com/)

Another methodology used in evidence preservation is to use write-protected storage devices. In other words, the storage device you are investigating should immediately be write-protected before it is imaged and should be labeled to include the following:

- Investigator's name
- The date when the image was created
- Case name and number (if applicable)

Additionally, you must prevent electronic static or other discharge from damaging or erasing evidentiary data. Special evidence bags that are antistatic should be used to store digital devices. It is very important that you prevent electrostatic discharge (ESD) and other electrical discharges from damaging your evidence. Some organizations even have cyber forensic labs that control access to only authorized users and investigators. One method often used involves constructing what is called a "Faraday cage." This "cage" is often built out of a mesh of conducting material that prevents electromagnetic energy from entering into or escaping from the cage. Also, this prevents devices from communicating via Wi-Fi or cellular signals.

What's more, transporting the evidence to the forensics lab or any other place, including the courthouse, has to be done very carefully. It is critical that the chain of custody be maintained during this transport. When you transport the evidence, you should strive to secure it in a lockable container. It is also recommended that the responsible person stay with the evidence at all times during transportation.

Reverse Engineering

Key Topic

Reverse engineering is the methodology for acquiring architectural information about anything originally created by someone else. Reverse engineering has been around since long before computers or modern technology. Nowadays, reverse engineering is not only used to steal or counterfeit technology and to "reverse" cryptographic algorithms, but also to perform malware analysis and cyber security forensics. Reverse engineering can even be useful to software developers to discover how to interoperate with undocumented or partially documented software, or even to develop competing software (which in some cases may be illegal).

Reverse engineering can be used for exploit development to locate vulnerabilities in a system and compromise the system, but it also can be used on malware. Security researchers and forensics experts can trace every step the malware takes and assess the damage it could cause, the expected rate of infection, how it could be removed from infected systems, and how to potentially proactively defend against such a threat. Malware analysis extends to identifying whether malware is present on a given system and studying the malware to understand how it functions. Doing this can reveal the purpose of the malware, and even its author.

Two additional uses of reverse engineering are to "reverse" cryptographic algorithms to decrypt data as well as Digital Rights Management (DRM) solutions. Threat actors use DRM reverse-engineering techniques to steal music, movies, books, and any other content protected by DRM solutions.

Many tools are available for performing reverse engineering. The following are a few examples:

- **System-monitoring tools**: Tools that sniff, monitor, explore, and otherwise expose the program being reversed.
- **Disassemblers**: Tools that take a program's executable binary as input and generate textual files that contain the assembly language code for the entire program or parts of it.
- **Debuggers**: These tools allow reverse engineers to observe the program while it is running and to set breakpoints; they also provide the ability to trace through code. Reverse engineers can use debuggers to step through the disassembled code and watch the system as it runs the program, one instruction at a time.
- **Decompilers**: Programs that take an executable binary file and attempt to produce readable high-level language code from it.

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 3-2 lists a reference of these key topics and the page numbers on which each is found.

Key Topic

Table 3-2 Key Topics

Key Topic Element	Description	Page
Summary	Describe what are vulnerabilities	166
Summary	Define what are threats	167
Summary	Define threat actors	168
Summary	Describe what is threat intelligence and why is it useful	168
Summary	Define what are exploits	170
Summary	Describe confidentiality, integrity, and availability	171
Summary	Describe risk and risk analysis	171
Summary	Define and provides examples of PII	173
Summary	Define and provides examples of PHI	174
Summary	Decribe the principle of least privilege	174
Summary	Define what is a security operations center	175
Summary	Describe runbook automation	176
Summary	Define and describe chain of custody	177
Summary	Describe what is reverse engineering	178

Define Key Terms

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

Vulnerabilities, threats, threat actors, exploits

Q&A

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

1. Which of the following statements are true about vulnerabilities?
   a. A vulnerability is a threat on a system.
   b. A vulnerability is an exploitable weakness in a system or its design.
   c. Vulnerabilities can be found in protocols, operating systems, applications, hardware, and system designs.
   d. Vulnerabilities are exploits that are discovered every day in software and hardware products.
2. On which of the following can exploit kits be run from?
   a. Web servers
   b. Email servers
   c. NTP servers
   d. Firewalls
3. Which of the following are examples of exploit kits?
   a. Angler
   b. Mangler
   c. Blackhole
   d. Black ICE
4. Which of the following describe what a threat is?
   a. Threats and vulnerabilities are the same.
   b. A threat is an exploit against a patched vulnerability.
   c. A threat is any potential danger to an asset.
   d. A threat is a piece of software aimed at exploiting a vulnerability.
5. What is an IoC?
   a. An indicator of compromise
   b. An indicator of containment
   c. An intrusion operating control
   d. An intrusion of compromise
6. Which of the following are provided by threat intelligence feeds?
   a. Indicators of compromise
   b. IP addresses of attacking systems
   c. The overall risk score of all vulnerabilities in the corporate network
   d. The overall risk score of threats in the corporate network

7. The way you document and preserve evidence from the time you start the cyber forensics investigation to the time the evidence is presented in court is referred to as which of the following?
   a. Chain of compromise
   b. Custody of compromise
   c. Chain of forensics
   d. Chain of custody
8. What are decompilers?
   a. Programs that take an executable binary file and attempt to produce readable high-level language code from it
   b. Programs that take a non-executable binary file and attempt to produce compiled code from it
   c. Programs that take a non-executable binary file and attempt to produce encrypted code from it
   d. Programs that execute a binary file and attempt to crack the encryption of it
9. Which of the following are metrics that can measure the effectiveness of a runbook?
   a. Mean time to repair (MTTR)
   b. Mean time between failures (MTBF)
   c. Mean time to discover a security incident
   d. All of the above
10. What is PHI?
   a. Protected HIPAA information
   b. Protected health information
   c. Personal health information
   d. Personal human information

Index

Numbers

802.1Q tags, VLAN, 33

802.1x, 219-221, 512

802.11

frames, 39-40

IBSS, 37-38

A

AAA (Authentication, Authorization and Accounting)

Diameter protocol, 216-217, 220

RADIUS, 212-214, 220

revoking digital certificates, 331

TACACS+, 214

ABAC (Attribute-Based Access Control), 202, 207-210

acceptable asset use/return policies, 266-267

access

ACL, 512

delegation of access (OAuth), 258

directories

DAP, 251

LDAP, 252

IAM

access review phase, 244-246

access revocation phase, 244-246

account provisioning, 244-246

directories, 250-252

passwords, 246-249

privileges provisioning phase, 244-245

registration/identity validation phase, 244-245

SSO, 252-260

access controls

AAA protocols, 212

Diameter, 216-217, 220

RADIUS, 212-214, 220

TACACS+, 214

ABAC, 202, 207-210

access control policy, 195-197

access policy definition, 195-197

accounting, 193-194

ACL, 210, 221-223

ACM, 211

administrative (management) controls, 199

antimalware technologies, 231

antivirus technologies, 231

assets

classifying, 195, 266-268

marking, 195-196

authentication, 191-194

authorization, 193-194

availability, 189

capability tables, 210

Cisco Attack Continuum, mapping access controls to, 201

compensating controls, 200

confidentiality, 189

content-dependent access controls, 211

context-dependent access controls, 212

corrective controls, 200

DAC, 202-203
data disposal, 195-197
defined, 185, 189
detective controls, 200
deterrent controls, 200
Diameter protocol, 216-217, 220
identification, 190-194
identity/profile management, 223
IDS
deploying IDS, 227-228
false negative/positive events, 229
HIDS, 230
IPS versus, 229
NIDS, 229-230
true negative/positive events, 229
information security roles/responsibilities, 197
auditors, 199
data custodians, 198
data owners, 198
end users, 198
executives (senior management), 198
information system security professionals, 198
security administrators, 198
security officers, 198
system owners, 198
integrity, 189
IPS
deploying IPS, 227-228
false negative/positive events, 229
HIPS, 230
IDS versus, 229
NIPS, 229-230
true negative/positive events, 229
MAC, 202-205
network ACL, 221
dACL, 222
firewalls, 223
SGACL, 222
VLAN maps, 222
network segmentation
firewall DMZ, 225
TrustSec, 225-226
VLAN, 224
objects, defined, 189
physical controls, 199
port-based access control, 218
802.1x, 219-221
port security, 218-219
preventive controls, 200
process of, 195-197
RADIUS, 212-214, 220
RBAC, 202-207
recovery controls, 200
restricted interfaces, 211
subjects, defined, 189
TACACS+, 214
technical (logical) controls, 199
access policy definition (access controls), 195-197
account provisioning (IAM), 244-246
accounting
access controls, 193-194
revoking digital certificates, 331
TACACS+, 214
ACE (Access Control Entries), 113-114
ACI (Application Centric Infrastructure), 124
ACK packets, TCP three-way handshakes, 93
ACL (Access Control Lists), 210, 512
ACE, 113-114
ASA versus, 114-115
controlled plane ACL, 115
EtherType ACL, 116
example of, 116
extended ACL, 115-116

network ACL, 221
dACL, 222
firewalls, 223
SGACL, 222
VLAN maps, 222
standard ACL, 115
Webtype ACL, 116
ACM (Access Control Matrix), 211
ACS (Access Control Server), identity management, 223
actions (UNIX-based syslog), 394
active scans, reconnaissance attacks, 502
active-active failover, stateful inspection firewalls, 122
active/passive scanners, 284
active-standby failover, stateful inspection firewalls, 121
ad-hoc wireless networks. *See* IBSS
administration, security administrator role in information security, 198
administrative controls (access controls), 199
administrative distance, defined, 69
advanced distance vector/hybrid protocols, IP routing, 67
age of passwords, 247
AH (Authentication Headers), IPsec, 321, 346
AI (Asset Identification), vulnerability management, 288
AIC (Availability, Integrity, Confidentiality) triad, 171, 189
alert logs (UNIX-based syslog), 393
algorithms
encryption
asymmetric algorithms, 313-314, 324
block ciphers, 312
IPsec, 321
stream ciphers, 312
symmetric algorithms, 313
thumbprint, root certificates, 327
AMP (Advanced Malware Protection), 231
AMP for Endpoints, 133-136, 408
AMP for Networks, 136-137
AMP Threat Grid, 147, 408
anomaly-based analysis, IDS, 131
antimalware technologies, 231, 406-408
antiphishing defenses, 506
antivirus technologies, 406-407, 506
ClamAV, 135
ESA, 231
Immunet, 135
anycast addresses, IPv6 addressing, 80
AnyConnect NVM (Network Visibility Module), user endpoint logs, 479
AnyConnect Secure Mobility Client, BYOD architectures, 273
AP (Access Points)
autonomous AP, 40-41
BYOD architectures, 273
LAP, 40-41
rogue AP, 514
WLAN AP, 40-43
Apache access logs, 396-397
apache daemon, 392
API (Application Program Interface)
API abuse, 515
PSIRT openVuln API, 283
APIC (Application Policy Infrastructure Controller), 124
Application ID field (Diameter protocol), 216
application layer
OSI model, 12
TCP/IP model, 8
application-level blacklisting, 410-411
application-level graylisting, 410
application-level whitelisting, 410
application proxies (proxy servers), 117
ARF (Asset Reporting Format), vulnerability management, 288

ARP (Address Resolution Protocol)
cache poisoning, 511
Dynamic ARP inspection, 512
IP subnet communication, 60
spoofing attacks, 512
AS (Autonomous Systems), IP routing, 65
ASA (Adaptive Security Appliances)
ACL versus, 114-115
ASAv, 124
deep packet inspection, 125
DHCP, 126
DMZ, 120
FirePOWER Services, 126, 129
firewall logs, 426
ASDM logs, 427
buffered logs, 428
configuring, 428-430
console logs, 427
email logs, 427
SNMP trap logs, 428
Syslog server logs, 427
terminal logs, 427
high availability
active-active failover, 122
active-standby failover, 121
clustering firewalls, 122
IPsec, 345-346
logs, severity logging levels, 422
MPF, 125
next generation firewall features, 126
PAT, 119
SSL VPN, 352
static NAT, 119, 126
virtual contexts, 125
ASDM logs, 427
ASR (Aggregation Services Routers), BYOD architectures, 273
assets
acceptable use/return policies, 266-267
ARF, vulnerability management, 288
classifying, 195, 266-268
handling, 266-268
inventory, 266-267
labeling, 266-268
managing, 266-269
marking, 195-196
ownership, 266-267
asymmetric algorithms
defined, 313
DH, 314
DSA, 314
ECC, 314
ElGamal, 314
examples of, 314
RSA, 314, 324
AsyncOS
ESA features, 141
WSA features, 140
attachments (email) as malware, 140
attack continuum, 137
auditor role in information security, 199
auscert.org.au, 284
authentication
access controls, 194
authentication by characteristic, 191-192
authentication by knowledge, 191-192
authentication by ownership, 191
behavioral authentication, 191
biometric authentication, 191-192
multifactor authentication, 192
authentication server role (802.1x), 219
bypass vulnerabilities, 515
CA, 329-330
Diameter protocol, 216-217, 220
EAP, 802.1x port-based access control, 220
HMAC, 316. *See also* hash verification (hashing)

IPsec, 321
Kerberos, 254
passwords, 246-248
RADIUS, 212-214, 220
revoking digital certificates, 331
SAML, 256
SSO, 252
federated SSO, 253-256
Kerberos, 253-254
OAuth, 253, 258-259
OpenID Connect, 253, 259-260
SAML, 253, 256-258
TACACS+, 214
two-factor authentication, 505
Windows-based analysis, 361
authenticator role (802.1x), 219
authorization
access controls, 193-194
authorization (privilege) creep, 203
bypass vulnerabilities, 515
Kerberos, 254
OAuth and SSO, 253, 258-259
OpenID Connect, 259-260
revoking digital certificates, 331
SAML, 256
TACACS+, 214
automation and vulnerability management
SCAP, 288-290
TMSAD, 290
autonomous AP, 40-41
autonomous architectures, 41
Autorun, Windows registration, 366
availability, CIA triad, 171, 189
AVC (Application Visibility and Control), 469-470

B

backdoors, 134, 406, 506
background daemons, 389
backoff time, 18, 36
BAE Detica CyberReveal, 169
baseline configurations, 276
behavioral authentication, 191
BGP (Border Gateway Protocol) and TCP, 95
BID (Bridge ID)
root BID, 28
root elections, 28
STP, 27
binlogd, 392
biometric authentication, 191-192
black box penetration assessments, 286
blacklisting applications, 410-411
block ciphers, 312
blocking state (STP port state), 30
Bluejacking, 514
botnets and DDoS attacks, 508
BPDU (Bridge PDU)
BPDU Guard, 512
STP, 28
bridges, Ethernet LAN, 22
broadcast domains (Ethernet), 23
broadcast MAC addresses, 20
broadcast network addresses, 50
broadcast storms, 27
browsers (web), launching via SSL VPN, 348
BSS (Basic Service Set), IBSS, 37-38
buffer overflows, 132, 515
buffered logging, 428
BYOD (Bring-Your-Own-Device) architecture, 269-274

C

CA (Certificate Authorities), 324-326
authentication/enrolling with, 329-330
cross-certifying CA topology, 333
hierarchical PKI topology, 332
ISE and, 144
revoking certificates, 330-331
root certificates, 327
SCEP (Simple Certificate Enrollment Protocol), 330
single root CA topology, 332
cache poisoning (ARP), 511
caches (NetFlow), 152
capability tables, 210
capturing
packets
encryption, 470
sniffers, 470
tcpdump, 471-473
Wireshark, 473
passwords, 514
CAPWAP, LAP and WLC, 41
carrier sense, 36
carriers, 21
CCE (Common Configuration Enumeration), vulnerability management, 289
CCSS (Common Configuration Scoring System)
vulnerability management, 289
web resources, 173
centralized architectures, split-MAC, 42
CERT (Computer Emergency Response Team) and cyber forensics, 177
CERT-EU, 284
cert.europa.eu, 284
certificates (digital)
CA, 324-326
authenticating/enrolling with, 329-330
cross-certifying CA topology, 333
hierarchical PKI topology, 332
ISE and, 144
revoking certificates, 330
root certificates, 327
SCEP, 330
single root CA topology, 332
elements of, 328
identity certificates, 327-329
PKI
CA, 324-333
identity certificates, 327-329
root certificates, 326-327
uses for certificates, 331
X.500 certificates, 328
X.509v3 certificates, 328
root certificates, 326-327
uses for, 331
X.500 certificates, 328
X.509v3 certificates, 328
certificates (SSL), 322
CES (Cloud Email Security), 146
chain of custody (evidentiary)
defined, 177
evidence preservation, 178
chaining vulnerabilities, 285
change management, 276, 281, 506
ITIL Service Transition, 278-279
RFC, 279
chapter-ending review tools, 549
characteristic, authentication by, 191-192
child processes, defined, 383
chmod command, modifying permissions, 386-388
Chromium, sandboxing, 413

CI (Configuration Items), 276
CIA (Confidentiality, Integrity, Availability) triad, 171, 189
CIDR (Classless Interdomain Routing), 50-52
ciphers
block ciphers, 312
defined, 311
digit streams, 312
polyalphabetic method, 311
stream ciphers, 312
substitution method, 311
transposition method, 311
Cisco AMP Threat Grid, 169
Cisco Attack Continuum, mapping access controls to, 201
Cisco Learning Network, 548
ClamAV antivirus software, 135, 407
classful addressing, 48-49
classifying
assets (access controls), 195, 266-268
information, 506
client-based remote-access VPN (Virtual Private Networks), 343
client-based SSL VPN
clientless SSL VPN versus, 351
full tunnel mode, 350
thin client mode, 350
client-based VPN, 526
client mode (VTP), 33
clientless remote-access VPN (Virtual Private Networks), 342
clientless SSL VPN, 350-351
clientless VPN, 528
cloud-based architectures, 41
cloud-based security, 144
AMP Threat Grid, 147
CES, 146
CloudLock, 148, 152
CTAS, 147
CWS, 145
Hybrid Email Security, 146, 152
OpenDNS, 148
clustering
firewalls, 122
WSA, 140
CMDB (Configuration Management Database), 276
CMSS (Common Misuse Scoring System)
vulnerability management, 289
web resources, 173
code execution, 506
collision domains
bridges and, 22
defined, 20-21
collision resistance, 315
compensating controls (access controls), 200
computer viruses, defined, 133
confidentiality
CIA triad, 171, 189
ISO 27000, 171
configuring
baseline configurations, 276
CCSS
vulnerability management, 289
web resources, 173
CI, 276
configuration management
baseline configurations, 276
change control phase, 278
CI, 276
CMDB, 276
identifying/implementing configuration phase, 278
monitoring phase, 278
planning phase, 277
records, 276
SecCM, 277
logs, ASA configuration, 428-430
NTP, 423

routers
NTP configuration, 423
Syslog configuration, 424-426
switches, Syslog configuration, 424-426
Syslog, 424-426
console logging, 427
constraint RBAC (Role-Based Access Control), 206
content-dependent access controls, 211
context-dependent access controls, 212
Control plane (roles-based network security), 165
controlled plane ACL, 115
converged architectures, split-MAC, 43
core RBAC (Role-Based Access Control), 206
corond, 391
corrective controls (access controls), 200
countermeasures, defined, 167
CPE (Common Platform Enumeration), vulnerability management, 289
cracking passwords, 513
CreateProcessWithTokenW function, Windows-based analysis, 361
crime (organized) as threat actors, 168
CRITs (MITRE), 169
CRL (Certificate Revocation List), 331
cross-certifying CA topology, 333
cryptanalysis, defined, 311
cryptography
asymmetric algorithms
defined, 313
DH, 314
DSA, 314
ECC, 314
ElGamal, 314
examples of, 314
RSA, 314, 324
ciphers
block ciphers, 312
defined, 311
polyalphabetic method, 311
stream ciphers, 312
substitution method, 311
transposition method, 311
defined, 311
digital signatures
benefits of, 317
example of, 317-320
RSA digital signatures and PKI, 324
SSL, 322
ECC, 314
hash verification (hashing)
collision resistance, 315
defined, 314
example of, 314-316
IPsec, 321
MD5, 316
SHA-1, 316
SHA-2, 316
hash verification (hashing), 316
HMAC, 316
IPsec
AH, 321, 346
ASA, 346
defined, 321
DH, 346
elements of, 321
ESP, 321, 346
IKEv1, Phase 1, 343-345, 348
IKEv1, Phase 2, 345-347
IKEv2, 348
IPsec pass-through, 345
NAT-T, 345
transport mode, 347
tunnel mode, 347
keys
asymmetric algorithms, 313-314, 324
defined, 312
key management, 320-322

keyspace, 321
OTP, 312
private key cryptography, 313-314, 324
public key cryptography, 313-314, 324, 327, 330
stream ciphers, 312
symmetric algorithms, 313
NGE, examples of, 321
private key cryptography, 313-314, 324
public key cryptography, 313
ECC, 314
PKCS, 330
PKI and public key pairs, 324
root certificates, 327
quantum computing, 316
SSL, 322
symmetric algorithms, 313
vulnerabilities, 516
CSRF (Cross-Site Request Forgery) vulnerabilities, 516
CTAS (Cisco Threat Awareness Service), 147
customizing practice exams, 547
CustomLog directive (Apache access logs), 396
CVE (Common Vulnerabilities and Exposures), 282, 515
vulnerability management, 289
web resources, 167
cve.mitre.org, 283
CVRF (Common Vulnerability Reporting Framework), 283
CVSS (Common Vulnerability Scoring System), 172, 291-294
vulnerability management, 289
web resources, 171
CWA (Cisco Workload Automation), web resources, 176
CWE (Common Weakness Enumerator), 173
CWS (Cloud Web Security), 145, 273
CWSS (Common Weakness Scoring System)
vulnerability management, 289
web resources, 173
cyber forensics
chain of custody (evidentiary)
defined, 177
evidence preservation, 178
defined, 177
objectives of, 177
reverse engineering
debuggers, 179
decompilers, 179
defined, 178
disasemblers, 179
DRM, 179
system-monitoring tools, 179
tools, 178
write-protected storage devices, 178
Cyber Squad ThreatConnect, 169
cyber threat intelligence, 169-170
Cybersecurity Maturity (risk analysis), 172
CybOX (Cyber Observable eXpression), 170

D

DAC (Discretionary Access Control), 202-203
dACL (downloadable ACL), 222
daemons
background daemons, 389
defined, 391
Linux-based analysis, 391-392
Mac OS X-based analysis, 391-392
UNIX-based analysis, 391-392
DAP (Directory Access Protocol), 251

data-at-rest
access control policy, 197
defined, 530
data centers
ACI and, 124
firewalls, 123-124
lateral traffic, 123
data classification (access controls), 195
data custodian role in information security, 198
data disposal (access controls), 195-197
data exfiltration attacks, 510-511
data in motion (access control policy), 197
data integrity
hash verification (hashing)
defined, 314
example of, 314-316
IPsec, 321
MD5, 316
SHA-1, 316
SHA-2, 316
HMAC, 316
data in use (access control policy), 197
data link layer (OSI model), 12
data owner role in information security, 198
databases
routing databases, 44
views as restricted interfaces, 212
Data/User plane (roles-based network security), 165
DDoS (Distributed denial-of-Service) attacks, 132
botnets and, 508
Direct DDoS, 507
Radware DefensePro DDoS mitigation software, 127
Reflected DDoS, 509
debuggers, reverse engineering, 179
decapsulation, TCP/IP model, 9
decompilers, reverse engineering, 179
deep packet inspection, stateful inspection firewalls, 125
default routes, defined, 44
defense-in-depth strategy
benefits of, 162
multi-layered approach, 163
network visibility, 163
onion diagrams, 163-165
proactive versus reactive security, 166
roles-based network security, 165
delegation of access (OAuth), 258
denial-of-service attacks, 531
deploying
firewalls, 112
patches, 298
deserialization of untrusted data vulnerabilities, 516
destination addresses (Ethernet frames), 19
Destination Unreachable messages (ICMP), 71
destroying documents, 506
detective controls (access controls), 200
deterrent controls (access controls), 200
DH (Diffie-Hellman key exchange protocol), 314
IPsec, 345-346
PFS, 346
DHCP (Dynamic Host Configuration Protocol)
ASA, 126
DHCPACK messages, 58
DHCPDECLINE messages, 58
DHCPDISCOVERY messages, 58
DHCPINFORM messages, 59
DHCPNACK messages, 58
DHCPOFFER messages, 58
DHCPRELEASE messages, 59
DHCPREQUEST messages, 58
DHCP snooping, 512
DHCPv6 and IPv6 addressing, 87-88

IPv4 dynamic address assignments, 58-59
relays, 59
Diameter protocol
Application ID field, 216
capability exchange/communication termination, 217
Diameter exchange for network access services, 217, 220
DIB (Directory Information Bases), 250
digital certificates
CA, 324-326
authenticating/enrolling with, 329-330
cross-certifying CA topology, 333
hierarchical PKI topology, 332
revoking certificates, 330
root certificates, 327
SCEP, 330
single root CA topology, 332
elements of, 328
identity certificates, 327-329
PKI
CA, 324-333
identity certificates, 327-329
root certificates, 326-327
uses for certificates, 331
X.500 certificates, 328
X.509v3 certificates, 328
root certificates, 326-327
uses for, 331
X.500 certificates, 328
X.509v3 certificates, 328
digital signatures
benefits of, 317
DSA, 314
example of, 317-320
RSA digital signatures and PKI, 324
SSL, 322
Direct DDoS attacks, 507
directories
DAP, 251
DIB, 250
directory services, 250-252
DIT, 250
DN, 251
DSA, 251
DUA, 251
ITU-T X.500, 250-252
LDAP, 252
managing, 250
RDN, 251
disabled state (STP port state), 30
disassemblers, reverse engineering, 179
disk storage, memory versus, 363
DIT (Directory Information Trees), 250
DITKA questions (final review/study plans), 549
DLP (Data Loss Prevention), 152
DMZ (Demilitarized Zones), 120, 225
DN (Distinguished Names), 251
DNS (Domain Name System)
FQDN, 71
IP addressing, 71
OpenDNS, 148
resolution, 74-75
resolvers, 74
resource names, 72
root domains, 72
RR
common RR, 73
defined, 72
SLD, 72
spoofing attacks, 512
subdomains, 72
TCP and, 95
TLD, 72
tunneling, 491-492, 510-511
zones, 73

DNS2TCP, 510
DNScat-P, 510
document handling/destruction, 506
DoS (Denial-of-Service) attacks, 127, 132, 171, 189, 507-509
double free vulnerabilities, 516
downloaders, defined, 134, 406
DP (Designated Ports), port roles (STP), 29
DRM (Digital Rights Management), reverse engineering threats, 179
DSA (Digital Signature Algorithm), 314
DSA (Directory Service Agents), 251
DSoD (Dynamic Separation of Duty), Constraint RBAC, 206
DUA (Directory User Agents), 251
duties, separation of, 175
DV (Distance Vectors), IP routing, 65-67
dynamic address assignments, IPv4, 57
Dynamic ARP inspection, 512
dynamic memory allocation, Windows-based analysis, 363
dynamic routes, IP routing, 64

E

EAP (Extensible Authentication Protocol), 802.1x port-based access control, 220
EAPoL (EAP over LAN), 802.1x port-based access control, 220
ECC (Elliptic Curve Cryptography), 314
Echo Reply messages (ICMP), 70
Echo Request messages (ICMP), 70
EIGRP (Enhanced Interior Gateway Routing Protocol), IP routing, 67
Elasticsearch ELK stack, 436-437, 453
ElGamal asymmetric encryption system, 314
email
attachments as malware, 140
CES, 146
encryption, 409
ESA, 140, 231
AsyncOS, 141
SMTP and, 142
Hybrid Email Security, 146, 152
logs, 427
mail gateways. *See* MX (Mail Exchangers)
MX, 142
phishing attacks, 140
SenderBase, 141
SMTP
ESA and, 142
TCP and, 95
spam, 140
spear-phishing attacks, 141
whaling attacks, 141
EMM (Enterprise Mobility Management)
BYOD architecture, 269-270, 273
lifecycle of, 270-271
MDM, 271
BYOD architectures, 272-274
ISE and MDM integration, 274
Meraki EMM, 276
Meraki EMM, 276
encapsulation
ESP, IPsec, 321, 346
OSI model, 13-14
TCP, 91
TCP/IP model, 9-10
encryption, 531
algorithms
asymmetric algorithms, 313-314, 324
block ciphers, 312
IPsec, 321
stream ciphers, 312
symmetric algorithms, 313
data-at-rest, 530
defined, 526
email encryption, 409
file encryption, 409

Hak5 LAN Turtle USB adaptor, 529
LAN Turtle SSH Tunnel, 530
NGE, examples of, 321
packet captures, 470
security monitoring, 490
end user role in information security, 198
endpoints
AMP for Endpoints, 133-136
AMP for Networks, 136-137
security
antimalware software, 406-408
antivirus software, 406-407
blacklisting applications, 410-411
email encryption, 409
file encryption, 409
firewalls, 408
graylisting applications, 410
HIPS, 408
sandboxing, 411-413
whitelisting applications, 410
user endpoint logs, 477-481
enrollment, CA, 329-330
entropy vulnerabilities (insufficient), 517
enumeration
CCE, 289
CPE, 289
CVE, 289
Error events (Windows event logs), 373
ErrorLog directive (Apache access logs), 396
ESA (Email Security Appliance), 140, 231
AsyncOS, 141
SMTP and, 142
ESD (Electrostatic Discharge), evidence preservation, 178
ESP (Encapsulating Security Payloads), IPsec, 321, 346
ESS (Extended Service Sets), 38
Ethernet LAN
bridges, 22
broadcast domains, 23
frames, 19
hubs, 20-21
link layer loops, 26
LLC, 16
MAC, 16
address tables, 23-25
broadcast MAC addresses, 20
dynamic MAC address learning, 23-24
flooding, 24
full duplex mode, 18, 22
half-duplex mode, 17
multicast MAC addresses, 20
unicast MAC addresses, 20
physical layer, 16-17
STP, 27-30
switches, 22-25
VLAN
benefits of, 31
frame-forwarding, 31
IEEE 802.1Q tags, 33
multilayer switches and inter-VLAN traffic, 33-35
tagging, 32
VTP, 33
EtherType ACL, 116
ethical hacking. *See* penetration assessments
EUI-64 method, IPv6 addressing, 83
evasion techniques, 523
encryption, 526, 531
data-at-rest, 530
Hak5 LAN Turtle USB adaptor, 529
LAN Turtle SSH Tunnel, 530
Lockheed Martin kill chain, 536

pivoting, 536
defensive strategies, 538-539
example of, 537
privilege escalation, 536
protocol misinterpretation attacks, 533-534
resource exhaustion attacks
defensive strategies, 532
Slowloris, 531
throttling, 532
traffic fragmentation attacks, 532-533
traffic substitution and insertion attacks, 535
traffic timing attacks, 535
TTL manipulation attacks, 534
tunneling, 531
Hak5 LAN Turtle USB adaptor, 529
LAN Turtle SSH Tunnel, 530
Event Viewer (Windows), 372
events
event correlation time synchronization, 491
log collection, 260-261, 265
managing, 260-265
SEM, user endpoint logs, 478
SIEM, 264-265
Syslog, 262-264
evidence preservation, defined, 178
evidentiary chain of custody, 177-178
evil twin attacks, 514
exams (practice), Pearson Test Prep software, 549
Cisco Learning Network, 548
customizing exams, 547
Flash Card mode, 547
offline access, 546-547
online access, 545-547
Practice Exam mode, 547
Premium Edition, 548
Study mode, 547
updating exams, 547
executing code, 506
executive (senior management) role in information security, 198
exfiltration attacks (data), 510-511
exploits. *See also* threats; vulnerabilities, 167
defined, 134, 170, 406
exploit kits, 170
local exploits, defined, 170
remote exploits, defined, 170
extended ACL, 115-116

F

facilities (UNIX-based syslog), 392-393
Failure Audit events (Windows event logs), 373
false negative/positive events, 229
false negatives (pattern matching), 130
false positives (pattern matching), 130
FAR (False Acceptance Rates), 192
Faraday cages, evidence preservation, 178
FCS (Frame Check Sequences), Ethernet frames, 19
federated SSO, 253-256
FFIEC (Federal Financial Institutions Examination Council), Cybersecurity Assessment Tool, 172
fibers, defined, 361
file encryption, 409
file permissions
group permissions, 388-389
list of permission values, 387
Mac OS X-based analysis, 385
group permissions, 388-389
limiting processes in permissions, 389
list of permission values, 387
modifying permissions via chmod command, 386-388
rwx statements, 386

modifying via
chmod command, 386-388
su command, 389
sudo command, 389
processes and, 389
rwx statements, 386
subdirectories/files, 388
UNIX-based analysis, 385
group permissions, 388-389
limiting processes in permissions, 389
list of permission values, 387
modifying permissions via chmod command, 386-388
modifying permissions via su command, 389
modifying permissions via sudo command, 389
rwx statements, 386
subdirectories/files, 388

final review/study plans, 549

FirePOWER 7000 Series NGIPS, 133

FirePOWER 8000 Series NGIPS, 133

FirePOWER Security Intelligence Blacklisting, 411

FirePOWER Services, 126
FirePOWER 4100 Series, 127
FirePOWER 5500 Series, 129
FirePOWER 9300 Series, 127

firewalls
firewall DMZ, network segmentation, 225
FTD, 119, 126
FirePOWER 4100 Series, 127
FirePOWER 5500 Series, 129
FirePOWER 9300 Series, 127
ISR routers, 127-128
host-based firewalls, 408
Internet edge firewalls, 112
logs, 426
ASA configuration, 428-430
ASDM logs, 427
buffered logs, 428
console logs, 427
email logs, 427
SNMP trap logs, 428
Syslog server logs, 427
terminal logs, 427
network ACL, 223
next-generation firewalls, 119, 126-129, 223, 437-444
personal firewalls, 113, 128, 135, 408
stateful inspection firewalls, 117
ASA, 114-115, 119-126, 129
data centers and, 123-124
deep packet inspection, 125
DMZ, 120
high availability, 121-122
network segmentation, 120
virtual firewalls, 124-125
traditional firewalls
deploying, 112
packet-filtering techniques, 113-117
virtual firewalls, 124-125

FIRST (Forum of Incident Response and Security Teams), CVSS, 172

five-tuple (flow), 150

Flash Card mode (practice exams), 547

Flexible NetFlow, 455-468

flooding (MAC addresses), 24

flow
defined, 149
example of, 150
five-tuple, 150

FMC (FirePOWER Management Center), 133, 437-444

forensics
chain of custody (evidentiary)
defined, 177
evidence preservation, 178
objectives of, 177

reverse engineering
debuggers, 179
decompilers, 179
defined, 178
disassemblers, 179
DRM, 179
system-monitoring tools, 179
tools, 178
write-protected storage devices, 178
forks
defined, 383-384
Linux-based analysis, 383-385
Mac-OS X-based analysis, 383-385
processes, verifying, 385
UNIX-based analysis, 383-385
forwarding state (STP port state), 30
FQDN (Fully Qualified Domain Names), DNS, 71
fragmentation, IPv4, 47-48
frame-forwarding
Ethernet LAN
bridges, 22
broadcast storms, 27
carriers, 21
flooding, 24
hubs, 20-21
MAC addresses, 23
MAC address tables, 25
switches, 22-25
VLAN, 31
WLAN, 36
frames
defined, 7
Ethernet frames, 19
FRR (False Rejection Rates), 192
FS750 appliances (FMC), 133
FS2000 appliances (FMC), 133
FS4000 appliances (FMC), 133
FTD (FirePOWER Threat Defense), 119, 126
FirePOWER 4100 Series, 127
FirePOWER 5500 Series, 129
FirePOWER 9300 Series, 127
ISR routers, 127-128
ftdp, 392
FTP (File Transfer Protocol) and TCP, 95
full disclosure approach (PSIRT), 288
full duplex mode (Ethernet MAC), 18, 22
full packet capture versus Netflow, 151
full tunnel mode (SSL VPN), 350

G

global correlation and NGIPS, 132
global unicast addresses, IPv6 addressing, 80
gray box penetration assessments, 286
graylisting applications, 410
Graylog, 434
group permissions, 388-389

H

hacking (ethical). *See* penetration assessments
hacktivists, defined, 168
half-duplex mode (Ethernet MAC), 17
handles
defined, 368
example of, 369
handle leak, defined, 369
hash verification (hashing). *See also* HMAC
collision resistance, 315
defined, 314
example of, 314-316
IPsec, 321
MD5, 316
SHA-1, 316
SHA-2, 316

HCU (HKEY_CURRENT_CONFIG) hive (Windows registry), 366
headers
IPv4 headers, 45-47
IPv6, 78-79
TCP, 91-92
UDP, 98-99
HeapAlloc, defined, 364
heaps, defined, 363
heuristic-analysis and IDS, 131
HIDS (Host-based IDS), 230
hierarchical PKI topology, 332
hierarchical RBAC (Role-Based Access Control), 206
high availability, stateful inspection firewalls
active-active failover, 122
active-standby failover, 121
clustering firewalls, 122
HIPAA (Health Insurance Portability and Accountability Act), 174
HIPS (Host Intrusion Prevention Systems), 230, 408
hives (Windows registry), 365
HKCR (HKEY_CLASSES_ROOT) hive (Windows registry), 365
HKCU (HKEY_CURRENT_USER) hive (Windows registry), 366
HKLM (HKEY_LOCAL_MACHINE) hive (Windows registry), 366
HKU (HKEY_USERS) hive (Windows registry), 366
HMAC (Hashed Message Authentication Code), 316. *See also* hash verification (hashing)
hop count, defined, 65
host-based firewalls, 408
host telemetry
server logs, 481-482
user endpoint logs, 477-481
HTTP (Hypertext Transfer Protocol)
SSL VPN, 349
TCP and, 95
HTTPS (Hypertext Transfer Protocol Secure), SSL VPN, 349
hubs, Ethernet LAN, 20-21
Hunk, 430
hybrid/advanced distance vector protocols, IP routing, 67
Hybrid Email Security, 146, 152

I

IAM (Identity Access Management)
access review phase, 244-246
access revocation phase, 244-246
account provisioning, 244-246
directories
DAP, 251
DIB, 250
directory services, 250-252
DIT, 250
DN, 251
DSA, 251
DUA, 251
ITU-T X.500, 250-252
LDAP, 252
RDN, 251
passwords
age of passwords, 247
authentication, 246-248
creating, 246-248
OTP, 247-248
resetting passwords, 249
reusability of passwords, 247
storing passwords, 248
strength of passwords, 247
synchronizing passwords, 249
system-generated passwords, 247-248

tokens, 247-248
transmitting passwords, 248
user-generated passwords, 247-248
privileges provisioning phase, 244-245
registration/identity validation phase, 244-245
SSO, 252
federated SSO, 253-256
Kerberos, 253-254
OAuth, 253, 258-259
OpenID Connect, 253, 259-260
SAML, 253, 256-258
IBSS (Independent BSS), 37-38
ICMP (Internet Control Message Protocol)
ICMPv6 and IPv6 addressing, 85
IP routing, 70
identification (access controls), 190-194
identifying vulnerabilities, 281
analyzing, 290
CVRF, 283
CVSS, 291-294
information repositories/ aggregators, 283-284
OVAL, 282
penetration assessments, 285-286
prioritizing, 291
PSIRT, 286-288
PSIRT openVuln API, 283
remediation, 294-295
scanning, 284-286
SCAP, 288-290
vendor vulnerability announcements, 282-283
identity
IAM
access review phase, 244-246
access revocation phase, 244-246
account provisioning, 244-246
directories, 250-252
passwords, 246-249
privileges provisioning phase, 244-245
registration/identity validation phase, 244-245
SSO, 252-260
identity certificates, 327-329
ISE
security, 143-144
user endpoint logs, 480-481
managing
ACS, 223
ISE, 223, 538
Prime Access Registrar, 223
security, ISE
BYOD support, 144
CA and, 144
installing, 144
MDM and, 144
NAC features, 143
pxGrid and, 144
IDS (Intrusion Detection Systems)
access controls, 227-228
false negative/positive events, 229
HIDS, 230
NIDS, 229-230
true negative/positive events, 229
anomaly-based analysis, 131
DDoS attacks, 132
deploying, 227-228
disadvantages of, 132
example of, 128
false negative/positive events, 229
heuristic-analysis, 131
HIDS, 230
IPS versus, 229
NIDS, 131, 229-230
pattern matching, 130
protocol analysis, 131
protocol-based analysis, 131

stateful pattern-matching recognition, 130
traffic fragmentation attacks, 532
true negative/positive events, 229
zero-day attacks, 132
IEEE 802.1Q tags, VLAN, 33
IEEE 802.1x, 219-221, 512
IEEE 802.11
frames, 39-40
IBSS, 37-38
IKE (Internet Key Exchange), IPsec
IKEv1
Phase 1, 343-345, 348
Phase 2, 345-347
IKEv2, 348
immediate cache (NetFlow), 152
Immunet antivirus software, 135, 407
implicit denial (authorization), 193
information classification policies, 506
Information events (Windows event logs), 373
information security
availability, 189
confidentiality, 189
integrity, 189
roles/responsibilities, 197
auditors, 199
data custodians, 198
data owners, 198
end users, 198
executives (senior management), 198
information system security professionals, 198
security administrators, 198
security officers, 198
system owners, 198
Inherent Risk Profiles (risk analysis), 172
init processes, defined, 383
insufficient entropy vulnerabilities, 517
integrity
CIA triad, 171, 189
hash verification (hashing), 314-316, 321
HMAC, 316
interference attacks (wireless), 514
Internet edge firewalls, 112
Internet layer (TCP/IP model)
networking nodes, 7
packets, 8
routers/routing, 8
inter-VLAN traffic with multilayer switches, 33-35
inventories (assets), 266-267
IoC (Indicators of Compromise), 168-170
Iodine Protocol v5.00, 510
Iodine Protocol v5.02, 510
IOS
Flexible NetFlow, 455-468
logs, severity logging levels, 422
IOS-XE
Flexible NetFlow, 455-468
logs, severity logging levels, 422
IOS-XR, severity logging levels, 422
IP (Internet Protocol)
DNS
FQDN, 71
resolution, 74-75
resolvers, 74
resource names, 72
root domains, 72
RR, 72-73
SLD, 72
subdomains, 72
TLD, 72
zones, 73
ICMP, 70
IPv4
addresses, 44, 48
addresses, ARP, 60

addresses, broadcast network addresses, 50
addresses, CIDR, 50-52
addresses, classful addressing, 48-49
addresses, DHCP, 58-59
addresses, DNS, 71
addresses, dynamic address assignments, 57
addresses, mapped addresses, 491
addresses, network addresses, 50
addresses, network masks, 50-52
addresses, network subnetting, 50-54
addresses, private IP addresses, 54-56
addresses, public IP addresses, 54-56
addresses, real IP addresses, 491
addresses, reserved IP addresses, 56-57
addresses, special IP addresses, 56-57
addresses, spoofing attacks, 512
addresses, static address assignments, 57
addresses, VLSM, 52-54
default routes, 44
fragmentation, 47-48
headers, 45-47
intersubnet packet routing, 61-63
IP gateways, 44
IPv6 versus, 43, 75-77
packet routing, 44
routers, 44
routing, advanced distance vector/ hybrid protocols, 67
routing, AS, 65
routing databases, 44
routing, DV, 65-67
routing, dynamic routes, 64
routing, EIGRP, 67
routing, ICMP, 70
routing, LSA, 67-69
routing, routed protocol, 64
routing, routing protocol, 64
routing, static routes, 64
routing tables, 44
routing, using multiple routing protocols, 69
subnet communication, 60

IPv6

addresses, 44, 79
addresses, anycast addresses, 80
addresses, DHCPv6, 87-88
addresses, EUI-64 method, 83
addresses, finding network ID, 80
addresses, global unicast addresses, 80
addresses, ICMPv6, 85
addresses, LLA, 81
addresses, multicast addresses, 80-81
addresses, NDP, 84-86
addresses, reserved IP addresses, 82-83
addresses, SeND, 86
addresses, SLAAC, 84-87
addresses, special IP addresses, 82-83
addresses, static address assignments, 83
addresses, unicast addresses, 80-81
default routes, 44
headers, 78-79
IP gateways, 44
IPv4 versus, 43, 75-77
packet routing, 44
routers, 44
routing databases, 44
routing tables, 44
subnets, 79-81

IP Source Guard, 512
IPFIX (Internet Protocol Flow Information Export), 149, 446

IPS (Intrusion Prevention Systems)
access controls, 227-228
false negative/positive events, 229
HIPS, 230
NIPS, 229-230
true negative/positive events, 229
DDoS attacks, 132
deploying, 227-228
disadvantages of, 132
example of, 128
false negative/positive events, 229
HIPS, 230
IDS versus, 229
next-generation IPS logs, 437-444
NGIPS, 129
FirePOWER 7000 Series appliances, 133
FirePOWER 8000 Series appliances, 133
FMC, 133
global correlation, 132
NGIPSv, 133
Talos, 132
NIPS, 129, 229-230
traffic fragmentation attacks, 532
true negative/positive events, 229
IPsec (IP Security)
AH, 321, 346
ASA, 346
defined, 321
DH, 346
elements of, 321
ESP, 321, 346
IKEv1
Phase 1, 343-345, 348
Phase 2, 345-347
IKEv2, 348
IPsec pass-through, 345
NAT-T, 345
transport mode, 347
tunnel mode, 347
ISE (Identity Services Engine), 538
BYOD
architectures, 273
support, 144
CA and, 144
identity management, 223
installing, 144
MDM and, 144, 274
NAC features, 143
pxGrid and, 144
user endpoint logs, 480-481
island hopping. *See* pivoting
ISO 27000, confidentiality, 171
ISO 27001, risk analysis, 172
ISO 27005, risk analysis, 172
ISO 31000, risk analysis, 172
ISR (Integrated Services Routers)
BYOD architectures, 273
FTD and, 127-128
issuers (CA), root certificates, 327
ITIL Service Transition, change management, 278-279
ITU-T X.500, directory services, 250-252
IV (Initialization Vector) attacks, 514

J-K

jamming wireless signals, 514
job objects, defined, 361
jpcert.or.jp, 284

Kerberos
KDC and, 253
SSO and, 253-254
key loggers, defined, 134, 407

keys
asymmetric algorithms
defined, 313
DH, 314
DSA, 314
ECC, 314
ElGamal, 314
examples of, 314
RSA, 314, 324
defined, 312
key management, 320-322
keyspace, 321
OTP, 312
private key cryptography, 313-314, 324
public key cryptography, 313
ECC, 314
PKCS, 330
PKI and public key pairs, 324
root certificates, 327
stream ciphers, 312
symmetric algorithms, 313
Kibana, 436
kill chain (Lockheed Martin), 536
knowledge, authentication by, 191-192

L

labeling assets, 266-268
Lancope Stealthwatch, NAT stitching, 491
LAN (Local Area Networks)
bridges, 22
defined, 16
EAPoL, 802.1x port-based access control, 220
Ethernet LAN
bridges, 22
frames, 19
hubs, 20-21
link layer loops, 26
LLC, 16
MAC, 16-17, 20
physical layer, 16-17
STP, 27-30
switches, 22-25
VLAN, 31-35
hubs, 20-21
switches, 22-25
VLAN
benefits of, 31
frame-forwarding, 31
IEEE 802.1Q tags, 33
multilayer switches and inter-VLAN traffic, 33-35
network segmentation, 224
tagging, 32
VLAN maps, 222
VTP, 33
WLAN, 35
802.11, 37-40
AP, 40-43
architecture of, 37-38
frame-forwarding, 36
WLC, 273
LAP (Lightweight AP), 40-41
LastWrite time, 366
lateral traffic (data centers), 123
Layer 2
ACL, 512
security best practices, 511
Layer 3
ACL, 512
DNS
FQDN, 71
IP addressing, 71
resolution, 74-75
resolvers, 74
resource names, 72
root domains, 72
RR, 72-73

SLD, 72
subdomains, 72
TLD, 72
zones, 73
forwarding, 44
ICMP, 70
IPv4
addresses, 44, 48
addresses, ARP, 60
addresses, broadcast network addresses, 50
addresses, CIDR, 50-52
addresses, classful addressing, 48-49
addresses, DHCP, 58-59
addresses, DNS, 71
addresses, dynamic address assignments, 57
addresses, network addresses, 50
addresses, network masks, 50-52
addresses, network subnetting, 50-54
addresses, private IP addresses, 54-56
addresses, public IP addresses, 54-56
addresses, reserved IP addresses, 56-57
addresses, special IP addresses, 56-57
addresses, static address assignments, 57
addresses, VLSM, 52-54
default routes, 44
fragmentation, 47-48
headers, 45-47
intersubnet packet routing, 61-63
IP gateways, 44
IPv6 versus, 43, 75-77
packet routing, 44
routers, 44
routing, advanced distance vector/hybrid protocols, 67
routing, AS, 65
routing databases, 44
routing, DV, 65-67
routing, dynamic routes, 64
routing, EIGRP, 67
routing, ICMP, 70
routing, LSA, 67-69
routing, routed protocol, 64
routing, routing protocol, 64
routing, static routes, 64
routing tables, 44
routing, using multiple routing protocols, 69
subnet communication, 60
IPv6
addresses, 44, 79
addresses, anycast addresses, 80
addresses, DHCPv6, 87-88
addresses, EUI-64 method, 83
addresses, finding network ID, 80
addresses, global unicast addresses, 80
addresses, ICMPv6, 85
addresses, LLA, 81
addresses, multicast addresses, 80-81
addresses, NDP, 84-86
addresses, reserved IP addresses, 82-83
addresses, SeND, 86
addresses, SLAAC, 84-87
addresses, special IP addresses, 82-83
addresses, static address assignments, 83
addresses, unicast addresses, 80-81
default routes, 44
headers, 78-79
IP gateways, 44
IPv4 versus, 43, 75-77
packet routing, 44
routers, 44

routing databases, 44
routing tables, 44
subnets, 79-81
switches. *See* multilayer switches
Layer 4 (transport layer) protocols/technologies
connection oriented protocols, 90
connectionless protocols, 90
TCP
ACK packets, 93
applications and port numbers, 94-95
BGP, 95
connection establishment/termination, 91-93
DNS, 95
encapsulation, 91
error detection/recovery, 95-97
flow control, 91, 97-98
FTP, 95
headers, 91-92
HTTP, 95
multiplexing, 89-91
reliability, 91
SMTP, 95
sockets, 94-95
SSH, 95
SYN-ACK packets, 93
SYN packets, 93
three-way handshakes, 93
UDP, 89
applications and port numbers, 99
headers, 98-99
multiplexing, 90
sockets, 99
layered onion diagrams, defense-in-depth strategy, 163-165
LDAP (Lightweight Directory Access Protocol), 252
learning state (STP port state), 30
least privilege, principle of, 174. ***See also*** **need to know**
Length/Type field (Ethernet frames), 19
link layer (Layer 2)
Ethernet LAN
bridges, 22
frames, 19
hubs, 20-21
link layer loops, 26
LLC, 16
MAC, 16-17, 20
physical layer, 16-17
STP, 27-30
switches, 22-25
VLAN, 31-35
link layer loops, 26
WLAN, 35
802.11, 37-40
AP, 40-43
architecture of, 37-38
frame-forwarding, 36
link layer (TCP/IP model), frames, 7
Linux-based analysis
daemons, 391-392
forks
defined, 383-384
verifying processes, 385
processes
child processes, 383
defined, 382
init processes, 383
orphan processes, 384
parent processes, 383
PID, 383
scheduling, 382
terminating, 384
zombie processes, 384
shell, 382
symlinks, 390-391

listening state (STP port state), 30
LLA (Link-Local Addresses), IPv6 addressing, 81
LLC (Logical Link Control), 16
local exploits, defined, 170
Lockheed Martin kill chain, 536
Lockheed Martin Palisade, 169
LogFormat (Apache access logs), 396-397
logic bombs, defined, 134, 406
logical (technical) controls (access controls), 199
logs
alert logs (UNIX-based syslog), 393
Apache access logs, 396-397
ASDM logs, 427
buffered logs, 428
collection, 260-261, 265
console logs, 427
email logs, 427
firewall logs, 426
ASA configuration, 428-430
ASDM logs, 427
buffered logs, 428
console logs, 427
email logs, 427
SNMP trap logs, 428
Syslog server logs, 427
terminal logs, 427
log parsers, 374
managing, 260-265
network infrastructure logs, 422
NTP, 423-424
Syslog configuration, 424-426
next-generation IPS logs, 437-444
server logs, 481-482
session logs (UNIX-based syslog), 393
SIEM, 264-265
SNMP trap logs, 428
Syslog, 262-264
Elasticsearch ELK stack, 436-437
Graylog, 434
large scale environments, 430-437
router configuration, 424-426
server logs, 427
server topologies, 423
severity logging levels, 422
Splunk, 430-433
switch configuration, 424-426
terminal logs, 427
threat logs (UNIX-based syslog), 393
transaction logs (UNIX-based syslog), 393
UNIX-based syslog, managing logs, 394-395
user endpoint logs, 477-481
Windows event logs
Error events, 373
Failure Audit events, 373
Information events, 373
log parsers, 374
Success Audit events, 373
Warning events, 373
Windows Event Viewer, 372
Logstash, 436
lpd, 392
LSA (Link-State Algorithms)
IP routing, 67-69
LSA flooding, 68

M

MAC (Mandatory Access Control), 202-205
MAC (Medium Access Control)
addresses
address tables, 23-25
dynamic MAC address learning, 23-24

MAC moves, 219
port security, 218-219
Ethernet MAC, 16
address tables, 23-25
broadcast MAC addresses, 20
dynamic MAC address learning, 23-24
flooding, 24
full duplex mode, 18, 22
half-duplex mode, 17
multicast MAC addresses, 20
unicast MAC addresses, 20
flooding, 24
split MAC, 41-43
MAC Client Data and Pad field (Ethernet frames), 19
Mac OS X-based analysis
daemons, 391-392
forks
defined, 383-384
verifying processes, 385
multitasking, defined, 385
multiusers, defined, 385
permissions, 385
group permissions, 388-389
limiting processes in permissions, 389
list of permission values, 387
modifying via chmod command, 386-388
rwx statements, 386
processes
child processes, 383
defined, 382
init processes, 383
orphan processes, 384
parent processes, 383
PID, 383
scheduling, 382
terminating, 384
zombie processes, 384
symlinks, 390-391
MACSec (Media Access Control Security), TrustSec and network segmentation, 225
mail gateways. *See* MX (Mail Exchangers)
mailer worms, defined, 134, 406
malicious actors, defined, 167
Malloc, defined, 364
malvertising, 505
malware
AMP, 231
AMP for Endpoints, 133-136
AMP for Networks, 136-137
antimalware technologies, 231, 406-408
backdoors, 134, 406
downloaders, 134, 406
email attachments, 140
exploits, 134
key loggers, 134, 407
logic bombs, 134, 406
ransomware, 134, 407
rootkits, 134
spammers, 134, 406
Trojan horses, 134, 406
viruses, 133, 406-407
worms, 134, 406
man-in-the-middle attacks, 506-507
management (administrative) controls (access controls), 199
Management plane (roles-based network security), 165
managing
assets
acceptable asset use/return policies, 266-267
classifying, 266-268
handling assets, 266-268
inventories, 266-267
labeling assets, 266-268

media management, 266, 269
owning, 266-267
changes, 276, 281, 506
ITIL Service Transition, 278-279
RFC, 279
configurations
baseline configurations, 276
change control phase, 278
CI, 276
CMDB, 276
identifying/implementing configuration phase, 278
monitoring phase, 278
planning phase, 277
records, 276
SecCM, 277
directories
DAP, 251
DIB, 250
directory services, 250-252
DIT, 250
DN, 251
DSA, 251
DUA, 251
ITU-T X.500, 250-252
LDAP, 252
RDN, 251
events
log collection, 260-261, 265
SIEM, 264-265
Syslog, 262-264
IAM
access review phase, 244-246
access revocation phase, 244-246
account provisioning, 244-246
directories, 250-252
passwords, 246-249
privileges provisioning phase, 244-245
registration/identity validation, 244-245
SSO, 252-260
identity, ISE, 538
keys, 320
logs
collection, 260-261, 265
SIEM, 264-265
Syslog, 262-264
UNIX-based syslog, 394-395
media, 266, 269
mobile devices
MDM, 144, 271-276
OTA device management, 271
passwords, 505
age of passwords, 247
authentication, 246-248
creating passwords, 246-248
OTP, 247-248
resetting passwords, 249
reusability of passwords, 247
storage, 248
strength of passwords, 247
synchronization, 249
system-generated passwords, 247-248
tokens, 247-248
transmitting passwords, 248
user-generated passwords, 247-248
patches, 295-296
deploying patches, 298
prioritizing patches, 297
SMA, 142
vulnerabilities
analyzing vulnerabilities, 290
CVSS, 291-294
identifying vulnerabilities, 281-290
prioritizing vulnerabilities, 291
remediation, 294-295

mapped IP addresses, 491
marking assets (access controls), 195-196
Marvel (Elasticsearch ELK stack), 436
mass-mailer worms, defined, 134, 406
MD5 (Message Digest 5) and hash verification (hashing), 316
MDM (Mobile Device Management), 271
BYOD architectures, 272-274
ISE and, 144, 274
Meraki EMM, 276
user endpoint logs, 480
media
managing, 266, 269
removable media, 269
sanitizing, 269
memory
buffer overflow, 132
disk storage versus, 363
dynamic memory allocation, defined, 363
HeapAlloc, defined, 364
heaps, defined, 363
Malloc, defined, 364
memory tables, 548-549
NVRAM, defined, 363
stacks, defined, 363
static memory allocation, defined, 363
virtual address space
defined, 363-364
working sets, 364
VirtualAlloc, defined, 364
volatile memory, defined, 362
Meraki EMM (Enterprise Mobility Management), 276
Metron, 454
misuses, CMSS
vulnerability management, 289
web resources, 173
mitigations, 295
MITRE
CRITs, 169
CVE, 282
cve.mitre.org, 283
mobile devices
BYOD architectures, 269-270, 272-274
EMM
BYOD architecture, 269-270, 273
lifecycle of, 270-271
MDM, 271-276
Meraki EMM, 276
managing
MDM, 144, 271-276
OTA device management, 271
MDM, 271
BYOD architectures, 272-274
ISE and, 144, 274
Meraki EMM, 276
OTA device management, 271
monitoring
security
DNS tunneling, 491-492
encryption, 490
event correlation time synchronization, 491
NAT, 491
P2P communication, 494
Tor, 493
system-monitoring tools, reverse engineering, 179
MPF (Modular Policy Framework) and ASA, 125
MRU (Most Recently Used) lists, Windows registration, 366
multicast addresses
IPv6 addressing, 80-81
MAC addresses, 20
multifactor authentication, 192
multilayer switches, inter-VLAN traffic with, 33-35

multiplexing, 8
TCP multiplexing, 89
UDP multiplexing, 90
multitasking, defined, 385
multiusers, defined, 385
MX (Mail Exchangers), 142
mysqld, 392

N

NA (Neighbor Advertisement) messages (ICMPv6), 85
NAC (Network Admission Control) and ISE, 143
NAT (Network Address Translation)
example of, 118
mapped IP addresses, 491
NAT stitching, 491
PAT, 118-119
real IP addresses, 491
security monitoring, 491
static NAT, 117-119
NAT-T (NAT Traversal), IPsec, 345
NDP (Neighbor Discovery Protocol), IPv6 addressing, 84-86
need to know (authorization), 193. ***See also*** **principle of least privilege**
neighbors
defined, 65
NA messages (ICMPv6), 85
NDP, IPv6 addressing, 84-86
NS messages (ICMPv6), 85
SeND, IPv6 addressing, 86
NetFlow, 132, 445
big data analytics for cyber security, 453-455
caches, 152
commercial analysis tools, 447-448
Flexible NetFlow, 455-468
flow
defined, 149
example of, 150
full packet capture versus, 151
IPFIX, 149, 446
open source analysis tools, 449-453
pivoting defensive strategies, 539
UDP messages, 149
versions of, 150
network layer (OSI model), 12
networking
devices, defined, 10
nodes, defined, 7
TCP/IP model, 10-12
networks
ACL, 221
dACL, 222
firewalls, 223
SGACL, 222
VLAN maps, 222
basic network topology, 44
broadcast network addresses, 50
Ethernet LAN
bridges, 22
frames, 19
hubs, 20-21
link layer loops, 26
LLC, 16
MAC, 16-17, 20
physical layer, 16-17
STP, 27-30
switches, 22-25
VLAN, 31-35
ID, IPv6 addressing, 80
infrastructure logs, 422
NTP, 423-424
Syslog configuration, 424-426
IP networks, subnetting, 50-54

LAN
defined, 16
EAPoL, 220
Ethernet LAN, 16-35
VLAN, 31-35
WLAN, 35-43
network addresses, 50
network masks, 50-52
security
AMP, 133-137
application proxies (proxy servers), 117
ESA, 140-142
extended ACL, 116
firewalls, 112-129, 135
FTD, 119, 126-129
IDS, 128-132
IPS, 128-133
ISE, 143-144
NAT, 117-119
packet-filtering techniques, 113-117
roles-based network security, 165
SMA, 142
WSA, 137-140
segmentation, 536
firewall DMZ, 225
stateful inspection firewalls, 120
TrustSec, 225-226
VLAN, 224
telemetry
AVC, 469-470
firewall logs, 426-430
firewalls, 437-444
FMC, 437-444
NetFlow, 445-468
network infrastructure logs, 422-426
next-generation IPS logs, 437-444
packet capturing, 470-473
Prime Infrastructure, 474-477
Syslog, 430-437
visibility, defense-in-depth strategy, 163
VLAN
benefits of, 31
frame-forwarding, 31
IEEE 802.1Q tags, 33
multilayer switches and inter-VLAN traffic, 33-35
tagging, 32
VTP, 33
VPN
client-based VPN, 526
clientless VPN, 528
defined, 341, 526
Hak5 LAN Turtle USB adaptor, 529
IPsec, IKEv1 Phase 1, 343-345, 348
IPsec, IKEv1 Phase 2, 345-347
IPsec, IKEv2, 348
LAN Turtle SSH Tunnel, 530
protocols, 341
remote-access VPN, 342-343, 526
site-to-site VPN, 341, 526
SSH VPN, 528-530
SSL VPN, 348-352
Tor, 341
vulnerability scanners, 284
WAN, defined, 16
WLAN, 35
802.11, 37-40
AP, 40-43
architecture of, 37-38
frame-forwarding, 36
next generation firewalls, 119, 126-129, 223, 437-444
next-generation IPS logs, 437-444
NFdump, 449-452
NGE (Next Generation Encryption), examples of, 321
NGIPS (Next-Generation IPS), 129
FirePOWER 7000 Series appliances, 133
FirePOWER 8000 Series appliances, 133

FMC, 133
global correlation, 132
NGIPSv, 133
Talos, 132
NIDS (Network-based Intrusion Detection Systems), 131, 229-230
NIPS (Network-based Intrusion Prevention Systems), 129, 229-230
Nmap scans, reconnaissance attacks, 503-504
non-designated ports, port roles (STP), 29
non-preemptive scheduling, 383
normal cache (NetFlow), 152
NS (Neighbor Solicitation) messages (ICMPv6), 85
NTP (Network Time Protocol), 423-424
NVD (National Vulnerability Database), 515
nvd.nist.gov, 283
NVRAM (Nonvolatile Memory), defined, 363
NX-OS, severity logging levels, 422

O

OAuth (Security Assertion Markup Language) and SSO, 253, 258-259
objects (access controls), defined, 189
OCIL (Open Checklist Interactive Language), vulnerability management, 288
OCRL (Open Checklist Reporting Language), vulnerability management, 289
OCSP (Online Certificate Status Protocol), revoking digital certificates, 331
onion diagrams, defense-in-depth strategy, 163-165
online resources
CCSS, 173
CMSS, 173
CVE, 167
CVSS, 171
CWA, 176
CWSS, 173
exploit kits, 170
Rundeck, 176
OpenDNS, 148
OpenID Connect and SSO, 253, 259-260
OpenIOC (Open Indicators of Compromise), 170
OpenSOC (Open Security Operations Center), 454
organized crime as threat actors, 168
orphan processes, defined, 384
orphan symlinks, defined, 390
OSI model
application layer, 12
data link layer, 12
encapsulation, 13-14
network layer, 12
physical layer, 12
presentation layer, 12
session layer, 12
TCP/IP model, mapping to, 13-15
transport layer, 12
OSR (Asset Summary Reporting), vulnerability management, 289
OTA (Over-The-Air) device management, 271
OTP (One-Time Pads), 312
OTP (One-Time Passwords), 247-248
OVAL (Open Vulnerability and Assessment Language), 282, 288
OWASP Foundation, 517
ownership, authentication by, 191
owning assets, 266-267
OzymanDNS, 510

P

P2P (Peer-to-Peer) communication, security monitoring, 494
PA (Permission Assignments), RBAC, 205
packets
ACK packets, TCP three-way handshakes, 93
capturing
encryption, 470
full packet capturing versus NetFlow, 151
sniffers, 470
tcpdump, 471-473
Wireshark, 473
deep packet inspection, stateful inspection firewalls, 125
defined, 8
filtering, 113
controlled plane ACL, 115
EtherType ACL, 116
extended ACL, 115-116
limitations of, 117
standard ACL, 115
Webtype ACL, 116
routing, 44
ICMP, 70
IP intersubnet packet routing, 61-63
SYN packets, TCP three-way handshakes, 93
SYN-ACK packets, TCP three-way handshakes, 93
parent processes, defined, 383
passive/active scanners, 284, 502
passwords
age of, 247
authentication, 246-248
capturing, 514
cracking, 513
creating, 246-248
managing, 505
OTP, 247-248
password-guessing attacks, 513
password-resetting attacks, 513
resetting, 249
reusability of, 247
sniffing, 514
storing, 248
strength of, 247
synchronizing, 249
system-generated passwords, 247-248
tokens, 247-248
transmitting, 248
user-generated passwords, 247-248
PAT (Port Address Translation), 118-119, 345
patches
deploying, 298
managing, 295-296
deploying patches, 298
prioritizing patches, 297
pattern matching, 130
Pearson Cert Practice Test Engine and practice exams, 549
customizing exams, 547
Flash Card mode, 547
offline access, 546-547
online access, 545-547
Practice Exam mode, 547
Premium Edition, 548
Study mode, 547
updating exams, 547
penetration assessments, vulnerabilities, 285-286
per-user ACL. *See* dACL
permanent cache (NetFlow), 152
permissions
group permissions, 388-389
list of permission values, 387

Mac OS X-based analysis, 385
group permissions, 388-389
limiting processes in permissions, 389
list of permission values, 387
modifying permissions via chmod command, 386-388
rwx statements, 386
modifying via
chmod command, 386-388
su command, 389
sudo command, 389
PA, RBAC, 205
processes and, 389
rwx statements, 386
UNIX-based analysis, 385
group permissions, 388-389
limiting processes in permissions, 389
list of permission values, 387
modifying permissions via chmod command, 386-388
modifying permissions via su command, 389
modifying permissions via sudo command, 389
rwx statements, 386
subdirectories/files, 388
Windows-based analysis, 361
personal firewalls, 113, 128, 135, 408
personal information
PHI, defined, 174
PII, defined, 173
PFS (Perfect Forward Secrecy), DH, 346
pharming, 505
PHI (Protected Health Information), defined, 174
phishing, 505-506
defined, 140
spear-phishing, 141
whaling, 141
physical carrier sense, 36
physical controls (access controls), 199
physical layer (Ethernet LAN), 16-17
physical layer (OSI model), 12
physical security, social engineering attacks, 506
PID (Processor Identifiers)
daemons, 391
defined, 383
PII (Personally Identifiable Information), defined, 173
pivoting, 536
defensive strategies
ISE, 538
NetFlow, 539
Stealthwatch, 539
example of, 537
PKCS (Public Key Cryptography Standards), 330
PKI (Public Key Infrastructure)
CA, 324-326
authenticating/enrolling with, 329-330
cross-certifying CA topology, 333
hierarchical PKI, 332
revoking certificates, 330
root certificates, 327
SCEP, 330
single root CA topology, 332
defined, 323
digital certificates
CA, 324-333
elements of, 328
identity certificates, 327-329
root certificates, 326-327
uses for, 331
X.500 certificates, 328
X.509v3 certificates, 328
identity certificates, 327-329
PKCS, 330

private key pairs, 324
public key pairs, 324
root certificates, 326-327
RSA digital signatures, 324
topologies
cross-certifying CA, 333
hierarchical PKI, 332
single root CA, 332
X.500 certificates, 328
X.509v3 certificates, 328
Policies plane (role-based network security), 165
policy enforcement, ISE, 538
polyalphabetic method and ciphers, 311
ports
access control
802.1x, 219-221
port security, 218-219
costs (STP), 28
numbers
TCP applications, 94-95
UDP applications, 99
roles (STP), 29
scans, reconnaissance attacks, 503
security, 218-219, 512
state (STP), 30
practice exams
Cisco Learning Network, 548
Pearson Test Prep software, 549
customizing exams, 547
Flash Card mode, 547
offline access, 546-547
online access, 545-547
Practice Exam mode, 547
Premium Edition, 548
Study mode, 547
updating exams, 547
preambles (Ethernet frames), 19
preemptive scheduling, 383
preparation (test-taking) tools
chapter-ending review tools, 549
Cisco Learning Network, 548
DITKA questions, 549
final review/study plans, 549
memory tables, 548-549
Pearson Cert Practice Test Engine, 549
offline access, 546-547
online access, 545
practice exams, 545
customizing, 547
Flash Card mode, 547
Practice Exam mode, 547
Premium Edition, 548
Study mode, 547
updating, 547
presentation layer (OSI model), 12
preserving evidence, defined, 178
preventive controls (access controls), 200
primary thread, defined, 360
Prime Access Registrar, identity management, 223
Prime Infrastructure, 474-477
principle of least privilege, 174. ***See also*** **need to known**
priorities (UNIX-based syslog), 393
prioritizing patches, patch management, 297
Privacy Rule (HIPAA), 174
private IP addresses, 54-56
private key cryptography, 313-314, 324
privileges
creep, 203
escalation, 506, 536
principle of least privilege, 174. *See also* need to know
privileges provisioning phase (IAM), 244-245
proactive security versus reactive security, 166

processes
background daemons, 389
child processes, 383
defined, 360, 382
forks, verifying processes, 385
init processes, 383
Linux-based analysis
child processes, 383
defined, 382
init processes, 383
orphan processes, 384
parent processes, 383
PID, 383
scheduling processes, 382
terminating processes, 384
zombie processes, 384
Mac OS X-based analysis
child processes, 383
defined, 382
init processes, 383
orphan processes, 384
parent processes, 383
PID, 383
scheduling processes, 382
terminating processes, 384
zombie processes, 384
orphan processes, 384
parent processes, 383
scheduling, 382
terminating, 384
UNIX-based analysis
child processes, 383
defined, 382
init processes, 383
orphan processes, 384
parent processes, 383
PID, 383
scheduling processes, 382
terminating processes, 384
zombie processes, 384
verifying, 385
Windows-based analysis
example of, 360
job objects, 361
threads, 360
virtual address space, 363-364
zombie processes, 384
profile management, 223
protocols
analysis, IDS, 131
misinterpretation attacks, 533-534
per level in TCP/IP model, 8
proxy servers (application proxies), 117
PSIRT (Product Security Incident Response Team), 286-287
CVSS, 173
full disclosure approach, 288
responsible disclosure approach, 288
PSIRT openVuln API, 283
public IP addresses, 54-56
public key cryptography, 313
ECC, 314
PKCS, 330
PKI and public key pairs, 324
root certificates, 327
pxGrid (Platform Exchange Grid) and ISE, 144
PySiLK, 453

Q-R

quantum computing and cryptography, 316

RA (Router Advertisement) messages (ICMPv6), 85
RADIUS (Remote Authentication Dial-In User Service), 212-214, 220
Radware DefensePro DDoS mitigation software, 127

RAM (Random Access Memory) as volatile memory, 362
ransomware, defined, 134, 407
RBA (Runbook Automation), defined, 176
RBAC (Role-Based Access Control), 202, 205-207
RDN (Relative Distinguished Names), 251
reactive security versus proactive security, 166
real IP addresses, 491
reconnaissance attacks
active scans, 502
Nmap scans, 503-504
passive scans, 502
port scans, 503
stealth scans, 503
strobe scans, 503
TCP ACK scans, 503
TCP scans, 503
TCP SYN scans, 503
UDP scans, 503
recovery controls (access controls), 200
Redirect messages (ICMPv6), 85
Reflected DDoS attacks, 509
registration
registration/identity validation phase (IAM), 244-245
Windows registration, 364
Autorun, 366
bives, 365
LastWrite time, 366
MRU lists, 366
Registry Editor, 365
relays (DHCP), 59
remediating vulnerabilities, 294-295
remote exploits, defined, 170
remote-access VPN (Virtual Private Networks)
client-based remote-access VPN, 343
clientless remote-access VPN, 342
defined, 526
removable media, 269
reserved IP addresses
IPv4, 56-57
IPv6, 82-83
resetting passwords, 249
resolvers (DNS), 74
resource exhaustion attacks
defensive strategies, 532
Slowloris, 531
throttling, 532
resource names, defined, 72
responsible disclosure approach (PSIRT), 288
restricted interfaces (access controls), 211
return policies (assets), 266-267
reusability of passwords, 247
reverse engineering
debuggers, 179
decompilers, 179
defined, 178
disassemblers, 179
DRM, 179
system-monitoring tools, 179
reverse proxy technology, SSL VPN, 350
review tools (test-taking strategies), 549
revoking
access revocation phase (IAM), 244-246
digital certificates, 330-331
RFC (Requests for Change), change management, 279
risk
analysis, 172-173
countermeasures, defined, 167
defined, 171
rlogind, 392
roaming, defined, 38
ROAS (Router On A Stick), 34
roles-based network security, 165
root BID, 28

root certificates, 326-327
root costs (STP), 28
root domains, defined, 72
root elections, 28-29
Root Guard, 512
root switches, STP, 28
rootkits, defined, 134, 407
rouge AP (Access Points), 514
routers/routing
administrative distance, 69
ASR, BYOD architectures, 273
CIDR, 50-52
default routes, 44
defined, 8
hop count, 65
IP routing
AS, 65
DV, 65-67
dynamic routes, 64
EIGRP, 67
ICMP, 70
LSA, 67-69
routed protocol, 64
routing protocol, 64
static routes, 64
using multiple routing protocols, 69
ISR
BYOD architectures, 273
FTD and, 127-128
neighbors, 65
NTP configuration, 423
packet routing, 44
ICMP, 70
IP intersubnet packet routing, 61-63
ROAS, 34
route manipulation attacks, 513
routing databases, 44
routing tables, 44, 62-63
Syslog configuration, 424-426
RP (Root Ports), port roles (STP), 29
RR (Resource Records)
common RR, 73
defined, 72
RS (Router Solicitation) messages (ICMPv6), 85
RSA asymmetric algorithm, 314, 324
rshd, 392
runbooks, defined, 176
Rundeck, web resources, 176
RVRM (Risk Vulnerability Response Model), 297
rwx statements, 386

S

S/MIME email encryption, 409
SAML (Security Assertion Markup Language) and SSO, 253, 256-258
sandboxing, 411-413
sanitizing media, 269
scanning vulnerabilities, 284-286
Sc.exe (Service Control utility), 371
SCAP (Security Content Automation Protocol), vulnerability management, 288-290
SCEP (Simple Certificate Enrollment Protocol), 330
scheduling
non-preemptive scheduling, 383
preemptive scheduling, 383
processes, 382
script kiddies, defined, 168
SecCM (Security-focused Configuration Management), 277
secure identities, 190-191
secure portal. *See* clientless VPN

security
administrator role in information security, 198
evasion techniques, 523
encryption, 526, 529-531
Lockheed Martin kill chain, 536
pivoting, 536-539
privilege escalation, 536
protocol misinterpretation attacks, 533-534
resource exhaustion attacks, 531-532
traffic fragmentation attacks, 532-533
traffic substitution and insertion attacks, 535
traffic timing attacks, 535
TTL manipulation attacks, 534
tunneling, 529-531
monitoring
DNS tunneling, 491-492
encryption, 490
event correlation time synchronization, 491
NAT, 491
P2P communication, 494
Tor, 493
officer role in information security, 198
proactive security versus reactive security, 166
segmenting networks, 536
firewall DMZ, 225
stateful inspection firewalls and, 120
TrustSec, 225-226
VLAN, 224
segments, defined, 8
selectors (UNIX-based syslog), 394
SEM (Security Event Management), user endpoint logs, 478
SeND (Secure Neighbor Discovery), IPv6 addressing, 86
SenderBase, 141
senior management (executive) role in information security, 198
separation of duties, 175, 206
serial numbers, root certificates, 327
server logs, 481-482
server mode (VTP), 33
Service Transition (ITIL), change management, 278-279
Services (Windows)
disabling, 371-372
enabling, 372
Sc.exe, 371
Services Control Manager, 369
Services snap-in, 370
Services plane (roles-based network security), 165
session layer (OSI model), 12
session logs (UNIX-based syslog), 393
SFD (Start-Frame Delimiters), Ethernet frames, 19
SGACL (Security Group-based ACL), 222
SGT (Security Group Tags)
security group-based access control, 225
SXP and, 226
TrustSec and network segmentation, 225
SHA-1 (Secure Hash Algorithm-1) and hash verification (hashing), 316
SHA-2 (Secure Hash Algorithm-2) and hash verification (hashing), 316
shell (UNIX), defined, 382
Shield (Elasticsearch ELK stack), 436
SIEM (Security Information and Event Manager), 264-265, 478
signatures (digital)
benefits of, 317
DSA, 314
example of, 317-320
RSA digital signatures and PKI, 324
SSL, 322
SiLK, 452-453

SIM (Security Information Management), user endpoint logs, 478
single root CA topology, 332
site-to-site VPN (Virtual Private Networks), 341, 526
SLAAC (Stateless Address Autoconfiguration), IPv6 addressing, 84-87
SLD (Second-Level Domains), defined, 72
Slowloris, 531
SMA (Security Management Appliance), 142
SMTP (Simple Mail Transfer Protocol)
ESA and, 142
TCP and, 95
sniffers, 470, 514
SNMP (Simple Network Management Protocol), trap logging, 428
SOC (Security Operation Centers), 175-176
social engineering attacks, 504
malvertising, 505
pharming, 505
phishing, 505-506
sockets
TCP, 94-95
UDP, 99
source addresses (Ethernet frames), 19
spam, defined, 140
spammers, defined, 134, 406
spear-phishing, defined, 141
special IP addresses
IPv4, 56-57
IPv6, 82-83
split MAC, 41-43
SplitBrain, 510
Splunk, 430-433
spoofing attacks, 512
SQL injection vulnerabilities, 517
SSH (Secure Shell)
SSH VPN, 528-530
TCP and, 95
SSL (Secure Sockets Layer)
certificates, 322
defined, 322
digital signatures, 322
example of, 322
SSL VPN
administrative privileges, 352
ASA placement, 352
client-based SSL VPN, 350-351
clientless SSL VPN, 350-351
HTTP, 349
HTTPS, 349
implementation scope, 352
infrastructure planning, 352
infrastructure requirements, 352
launching browsers, 348
reverse proxy technology, 350
user accounts, 352
user connectivity, 351
VPN device feature set, 351
SSO (Single Sign-On), 252
federated SSO, 253-256
Kerberos, 253-254
OAuth, 253, 258-259
OpenID Connect, 253, 259-260
SAML, 253, 256-258
SSoD (Static Separation of Duty), Constraint RBAC, 206
stacks, defined, 363
standard ACL, 115
state sponsors/governments as threat actors, 168
stateful DHCPv6, IPv6 addressing, 87
stateful inspection firewalls, 117
ASA
ACL versus, 114-115
ASAv, 124
deep packet inspection, 125
DHCP, 126

DMZ, 120
FirePOWER Services, 126, 129
high availability, 121-122
MPF, 125
next generation firewall features, 126
PAT, 119
static NAT, 119, 126
virtual contexts, 125
data centers and, 123-124
deep packet inspection, 125
DMZ, 120
high availability
active-active failover, 122
active-standby failover, 121
clustering firewalls, 122
network segmentation, 120
virtual firewalls, 124-125
stateful pattern-matching recognition, 130
stateless DHCPv6, IPv6 addressing, 87-88
static addresses
IPv4 addressing, 57
IPv6 addressing, 83
static memory allocation, Windows-based analysis, 363
static NAT, 117-119
static routes, IP routing, 64
stealth techniques, 523
encryption, 526, 531
data-at-rest, 530
Hak5 LAN Turtle USB adaptor, 529
LAN Turtle SSH Tunnel, 530
Lockheed Martin kill chain, 536
pivoting, 536
defensive strategies, 538-539
example of, 537
privilege escalation, 536
protocol misinterpretation attacks, 533-534
resource exhaustion attacks
defensive strategies, 532
Slowloris, 531
throttling, 532
stealth scans, reconnaissance attacks, 503
traffic fragmentation attacks, 532-533
traffic substitution and insertion attacks, 535
traffic timing attacks, 535
TTL manipulation attacks, 534
tunneling, 531
Hak5 LAN Turtle USB adaptor, 529
LAN Turtle SSH Tunnel, 530
Stealthwatch, 447-448, 539
STIX (Structured Threat Information eXpression), 169
storage
disk storage versus memory, 363
password storage, 248
write-protected storage devices, evidence preservation, 178
storm control, 512
STP (Spanning Tree Protocols)
BID, 27
BPDU, 28
port costs, 28
port roles, 29
port state, 30
root costs, 28
root elections, 29
root switches, 28
stream ciphers, 312
strength of passwords, 247
strobe scans, reconnaissance attacks, 503
Study mode (practice exams), 547
study plans, 549
su command, modifying permissions, 389
subdomains, defined, 72
subjects (access controls), defined, 189

subnets, 23
IP intersubnet packet routing, 61-63
IP networks
CIDR, 50-52
VLSM, 52-54
IP subnet communication, 60
IPv6 addressing, 79-81
substitution method and ciphers, 311
Success Audit events (Windows event logs), 373
sudo command, modifying permissions, 389
supplicant role (802.1x), 219
switches
Ethernet LAN, 22-25
Layer 3 switches. *See* multilayer switches
multilayer switches, inter-VLAN traffic with, 33-35
root switches, STP, 28
Syslog configuration, 424-426
SXP (SGT Exchange Protocol), TrustSec and network segmentation, 226
symlinks, 390-391
symmetric algorithms, defined, 313
symmetric key ciphers. *See* stream ciphers
SYN packets, TCP three-way handshakes, 93
SYN scans, reconnaissance attacks, 503
SYN-ACK packets, TCP three-way handshakes, 93
synchronizing
event correlation time synchronization, 491
passwords, 249
Syslog, 262-264
Elasticsearch ELK stack, 436-437
Graylog, 434
large scale environments
Elasticsearch ELK stack, 436-437
Graylog, 434
Splunk, 430-433
router configuration, 424-426
server logs, 427
server topologies, 423
severity logging levels, 422
Splunk, 430-433
switch configuration, 424-426
UNIX-based analysis, 396
actions, 394
alert logs, 393
example of, 394
facilities, 392-393
managing logs, 394-395
priorities, 393
selectors, 394
session logs, 393
threat logs, 393
transaction logs, 393
syslogd, 394
systems
monitoring tools, reverse engineering, 179
owner role in information security, 198
system-generated passwords, 247-248
updates, patch management, 295

T

tables
capability tables, 210
memory tables, 548-549
routing tables, 44, 62-63
TACACS+ (Terminal Access Controller Access Control System Plus), 214
Talos and NGIPS, 132
TAXII (Trusted Automated eXchange of Indicator Information), 170
TCP (Transmission Control Protocol)
ACK packets, 93
ACK scans, reconnaissance attacks, 503
applications and port numbers, 94-95

BGP, 95
connection establishment/termination, 91-93
DNS, 95
encapsulation, 91
error detection/recovery, 95-97
flow control, 91, 97-98
FTP, 95
headers, 91-92
HTTP, 95
multiplexing, 89-91
reconnaissance attacks, 503
reliability, 91
SMTP, 95
sockets, 94-95
SSH, 95
SYN-ACK packets, 93
SYN packets, 93
SYN scans, reconnaissance attacks, 503
SYN-ACK packets, 93
three-way handshakes, 93
TCP/IP model, 6
application layer, 8
decapsulation, 9
encapsulation, 9-10
Internet layer
networking nodes, 7
packets, 8
routers/routing, 8
layer interactions, 11-12
link layer, 7
networking communication, 10-12
networking devices, 10
OSI model, mapping to, 13-15
protocols per level, 8
transport layer, 8
TCP/IP suite, traffic fragmentation attacks, 532
TCP-Over-DNS, 511
tcpdump, 471-473
technical (logical) controls (access controls), 199
telemetry
host telemetry
server logs, 481-482
user endpoint logs, 477-481
network telemetry
AVC, 469-470
firewall logs, 426-430
FMC, 437-444
NetFlow, 445-468
network infrastructure logs, 422-426
next-generation firewalls, 437-444
next-generation IPS logs, 437-444
packet capturing, 470-473
Prime Infrastructure, 474-477
Syslog in large scale environments, 430-437
telnetd, 392
terminal logging, 427
terminating processes, 384
terrorist groups as threat actors, 168
tests (practice)
Cisco Learning Network, 548
Pearson Test Prep software, 549
customizing tests, 547
Flash Card mode, 547
offline access, 546-547
online access, 545-547
Practice Exam mode, 547
Premium Edition, 548
Study mode, 547
updating tests, 547
thin client mode (SSL VPN), 350
threads
defined, 360
example of, 360
fibers, defined, 361
primary thread, defined, 360
thread pools, defined, 361

threat logs (UNIX-based syslog), 393
threats. *See also* exploits; vulnerabilities
countermeasures, defined, 167
defined, 167
DRM reverse engineering, 179
threat actors, defined, 168
threat agents, defined, 167
threat intelligence
cyber threat intelligence, 169-170
defined, 168
feeds, 169
five-step process, 168
IoC, 168
IoC, OpenIOC, 170
standards, 169
threat vectors, defined, 167
throttling, resource exhaustion, 532
thumbprint algorithms, root certificates, 327
Time Exceeded messages (ICMP), 71
TLD (Top-Level Domains), defined, 72
TMSAD (Trust Model for Security Automation Data), vulnerability management, 290
tokens
password tokens, 247-248
Windows-based analysis, 361
Tor (The Onion Router)
security monitoring, 493
Tor exit node, 493
VPN, 341
traditional firewalls
deploying, 112
packet-filtering techniques, 113
controlled plane ACL, 115
EtherType ACL, 116
extended ACL, 115-116
limitations of, 117
standard ACL, 115
Webtype ACL, 116
traffic fragmentation attacks, 532-533
traffic substitution and insertion attacks, 535
traffic timing attacks, 535
transaction logs (UNIX-based syslog), 393
transmitting passwords, 248
transparent mode (VTP), 33
transport layer (Layer 4) protocols/technologies
connectionless protocols, 90
connection oriented protocols, 90
TCP
ACK packets, 93
applications and port numbers, 94-95
BGP, 95
connection establishment/termination, 91-93
DNS, 95
encapsulation, 91
error detection/recovery, 95-97
flow control, 91, 97-98
FTP, 95
headers, 91-92
HTTP, 95
multiplexing, 89-91
reliability, 91
SMTP, 95
sockets, 94-95
SSH, 95
SYN-ACK packets, 93
SYN packets, 93
three-way handshakes, 93
UDP, 89
applications and port numbers, 99
headers, 98-99
multiplexing, 90
sockets, 99
transport layer (OSI model), 12
transport layer (TCP/IP model), 8

transport mode (IPsec), 347
transposition method, ciphers and, 311
Trojan horses, defined, 134, 406
true negative/positive events, 229
TrustSec, network segmentation, 225-226
TTL manipulation attacks, 534
tunnel mode (IPsec), 347
tunneling, 531
Hak5 LAN Turtle USB adaptor, 529
LAN Turtle SSH Tunnel, 530
two-factor authentication, 505

U

UA (User Assignments), RBAC, 205
UDP (User Datagram Protocol), 89
applications and port numbers, 99
headers, 98-99
multiplexing, 90
NetFlow and, 149
reconnaissance attacks, 503
sockets, 99
unicast addresses
IPv6 addressing, 80-81
unicast MAC addresses, 20
unique local addresses, 76
UNIX-based analysis
Apache access logs, 396-397
daemons, 391-392
forks
defined, 383-384
verifying processes, 385
multitasking, defined, 385
multiusers, defined, 385
orphan symlinks, 390
permissions, 385
group permissions, 388-389
limiting processes in permissions, 389
list of permission values, 387
modifying via chmod command, 386-388
modifying via su command, 389
modifying via sudo command, 389
rwx statements, 386
subdirectories/files, 388
processes
child processes, 383
defined, 382
init processes, 383
orphan processes, 384
parent processes, 383
PID, 383
scheduling, 382
terminating, 384
zombie processes, 384
shell, 382
symlinks, 390-391
syslog, 396
actions, 394
alert logs, 393
example of, 394
facilities, 392-393
managing logs, 394-395
priorities, 393
selectors, 394
session logs, 393
threat logs, 393
transaction logs, 393
untrusted data, deserialization of, 516
updates
patch management, 295-296
deploying patches, 298
prioritizing patches, 297
practice exams, 547
system updates, 295
us-cert.gov, 284

User/Data plane (roles-based network security), 165
users
capability tables, 210
endpoint logs, 477-481
principle of least privilege, 174
separation of duties, 175
user-generated passwords, 247-248

V

validation, registration/identity validation phase (IAM), 244-245
validity dates (root certificates), 327
verifying processes, 385
virtual address space, defined, 363-364
virtual carrier sense, 36
virtual contexts, ASA, 125
virtual firewalls, 124-125
virtual FMC appliances, 133
virtual NGIPS, 133
VirtualAlloc, defined, 364
viruses
antivirus technologies, 231, 406-407, 506
defined, 133, 406
ESA, 231
worms, defined, 406
VLAN (Virtual Local Area Networks)
benefits of, 31
frame-forwarding, 31
IEEE 802.1Q tags, 33
multilayer switches and inter-VLAN traffic, 33-35
network segmentation, 224
tagging, 32
VLAN maps, 222
VTP, 33
VLSM (Variable-Length Subnet Masks), 52-54
VM (Virtual Machines), virtual firewalls, 124-125
volatile memory, defined, 362
VPN (Virtual Private Networks)
client-based VPN, 526
clientless VPN, 528
defined, 341, 526
Hak5 LAN Turtle USB adaptor, 529
IPsec
IKEv1, Phase 1, 343-345, 348
IKEv1, Phase 2, 345-347
IKEv2, 348
LAN Turtle SSH Tunnel, 530
protocols, 341
remote-access VPN
client-based remote-access VPN, 343
clientless remote-access VPN, 342
defined, 526
site-to-site VPN, 341, 526
SSH VPN, 528-530
SSL VPN
administrative privileges, 352
ASA placement, 352
client-based SSL VPN, 350-351
clientless SSL VPN, 350-351
HTTP, 349
HTTPS, 349
implementation scope, 352
infrastructure planning, 352
infrastructure requirements, 352
launching browsers, 348
reverse proxy technology, 350
user accounts, 352
user connectivity, 351
VPN device feature set, 351
Tor, 341
VTP (VLAN Trunking Protocol), 33

vulnerabilities, 514. ***See also*** **exploits; threats**
analyzing, 290
API abuse, 515
authentication bypass vulnerabilities, 515
authorization bypass vulnerabilities, 515
buffer overflows, 515
chaining, 285
countermeasures, defined, 167
cryptography vulnerabilities, 516
CSRF vulnerabilities, 516
CVE, 167, 282, 515
CVSS, 171-172, 291-294
defined, 166
deserialization of untrusted data vulnerabilities, 516
double free vulnerabilities, 516
examples of, 166-167
identifying, 281
CVRF, 283
information repositories/ aggregators, 283-284
OVAL, 282
PSIRT openVuln API, 283
vendor vulnerability announcements, 282-283
insufficient entropy vulnerabilities, 517
malicious actors, defined, 167
managing
analyzing vulnerabilities, 290
CVSS, 291-294
identifying vulnerabilities, 281-290
prioritizing vulnerabilities, 291
remediation, 294-295
misuses, CMSS, 173
mitigations, 295
NVD, 515
OWASP Foundation, 517
penetration assessments, 285-286
prioritizing, 291
PSIRT, 286-288
remediation, 294-295
RVRM, 297
scanning, 284-286
SCAP, 288-290
SQL injection vulnerabilities, 517
workarounds, 295
XSS vulnerabilities, 516

W

WAN (Wide Area Networks), defined, 16
war driving, 514
Warning events (Windows event logs), 373
WCCP (Web Cache Communication Protocol), WSA registration, 138-139
weaknesses, CWSS
vulnerability management, 289
web resources, 173
web browsers, launching via SSL VPN, 348
web proxies. ***See*** **application proxies (proxy servers)**
web resources
CCSS, 173
CMSS, 173
CVE, 167
CVSS, 171
CWA, 176
CWSS, 173
exploit kits, 170
Rundeck, 176
web security
CWS, 145
WSA
AsyncOS, 140
attack continuum, 137
clustering, 140
explicit proxy configuration, 138
transparent proxy configuration, 139
WCCP registration, 138-139

web vulnerability scanners, 284
Webtype ACL, 116
WEP attacks, 514
whaling, defined, 141
white box penetration assessments, 285
whitelisting applications, 410
Windows-based analysis
authentication, 361
CreateProcessWithTokenW function, 361
fibers, 361
handles
defined, 368
example of, 369
handle leak, 369
job objects, 361
memory allocation
dynamic memory allocation, 363
HeapAlloc, 364
heaps, 363
Malloc, 364
NVRAM, 363
stacks, 363
static memory allocation, 363
virtual address space, 363-364
VirtualAlloc, 364
volatile memory, 362
working sets, 364
permissions, 361
processes
defined, 360
example of, 360
job objects, 361
virtual address space, 363-364
threads
defined, 360
example, 360
fibers, 361
primary thread, 360
thread pools, 361
tokens, 361
Windows event logs, 372
Error events, 373
Failure Audit events, 373
Information events, 373
log parsers, 374
Success Audit events, 373
Warning events, 373
Windows Event Viewer, 372
Windows registration, 364
Autorun, 366
hives, 365
LastWrite time, 366
MRU lists, 366
Registry Editor, 365
Windows Services
disabling, 371-372
enabling, 372
Sc.exe, 371
Services Control Manager, 369
Services snap-in, 370
WMI, 366-368
Windows event logs, 372
Error events, 373
Failure Audit events, 373
Information events, 373
log parsers, 374
Success Audit events, 373
Warning events, 373
Windows Event Viewer, 372
Windows registration, 364
Autorun, 366
hives, 365
LastWrite time, 366
MRU lists, 366
Registry Editor, 365
Windows Services
disabling, 371-372
enabling, 372
Sc.exe, 371

Services Control Manager, 369
Services snap-in, 370
wireless AP (Access Points), BYOD architectures, 273
wireless attacks, 514
Wireshark, 473
WLAN (Wireless Local Area Networks), 35, 273
802.11
frames, 39-40
IBSS, 37-38
AP, 40-43
architecture of, 37-38
frame-forwarding, 36
WLC (Wireless LAN Controllers), 40-41, 273
WMI (Windows Management Instrumentation), 366-368
workarounds (vulnerability), 295
working sets, defined, 364
worms, defined, 134, 406
WPA attacks, 514
WPS attacks, 514
write-protected storage devices, evidence preservation, 178
WSA (Web Security Appliance)
AsyncOS, features of, 140
attack continuum, 137
clustering, 140
explicit proxy configuration, 138
transparent proxy configuration, 139
WCCP registration, 138-139

X

X.500 certificates, 328
X.509v3 certificates, 328
XCCDF (Extensible Configuration Checklist Description Format), vulnerability management, 288
xinetd, 391
XSS (Cross-Site Scripting) vulnerabilities, 516

Y-Z

YourFreedom, 511

zero-day attacks and IDS, 132
zombie processes, defined, 384
zones (DNS), 73

Connect, Engage, Collaborate

The Award Winning Cisco Support Community

Attend and Participate in Events

Ask the Experts
Live Webcasts

Knowledge Sharing

Documents
Blogs
Videos

Top Contributor Programs

Cisco Designated VIP
Hall of Fame
Spotlight Awards

Multi-Language Support

https://supportforums.cisco.com