

Save 10%
on Exam
Voucher

See Inside



Practice
Tests



Flash
Cards



Review
Exercises



Study
Planner

Cert Guide

Advance your IT career with hands-on learning

CompTIA®

Security+

SY0-601



OMAR SANTOS
RON TAYLOR
JOSEPH MLODZIANOWSKI

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



CompTIA[®] Security+ SY0-601 Cert Guide

Omar Santos

Ron Taylor

Joseph Mlodzianowski



Pearson

CompTIA® Security+ SY0-601 Cert Guide

Copyright © 2022 by Pearson Education, Inc.

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

ISBN-13: 978-0-13-677031-2

ISBN-10: 0-13-677031-2

Library of Congress Control Number: 2021935686

ScoutAutomatedPrintCode

Trademarks

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

Warning and Disclaimer

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

Special Sales

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

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

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

Editor-in-Chief

Mark Taub

Product Line Manager

Brett Bartow

Executive Editor

Nancy Davis

Development Editor

Christopher A. Cleveland

Managing Editor

Sandra Schroeder

Senior Project Editor

Tonya Simpson

Copy Editor

Chuck Hutchinson

Indexer

Erika Millen

Proofreader

Abigail Manheim

Technical Editor

Chris Crayton

Publishing Coordinator

Cindy Teeters

Cover Designer

Chuti Prasertsith

Compositor

codeMantra

Contents at a Glance

Introduction xliv

Part I: Threats, Attacks, and Vulnerabilities

- CHAPTER 1 Comparing and Contrasting Different Types of Social Engineering Techniques 3
- CHAPTER 2 Analyzing Potential Indicators to Determine the Type of Attack 29
- CHAPTER 3 Analyzing Potential Indicators Associated with Application Attacks 61
- CHAPTER 4 Analyzing Potential Indicators Associated with Network Attacks 95
- CHAPTER 5 Understanding Different Threat Actors, Vectors, and Intelligence Sources 117
- CHAPTER 6 Understanding the Security Concerns Associated with Various Types of Vulnerabilities 133
- CHAPTER 7 Summarizing the Techniques Used in Security Assessments 171
- CHAPTER 8 Understanding the Techniques Used in Penetration Testing 193

Part II: Architecture and Design

- CHAPTER 9 Understanding the Importance of Security Concepts in an Enterprise Environment 209
- CHAPTER 10 Summarizing Virtualization and Cloud Computing Concepts 227
- CHAPTER 11 Summarizing Secure Application Development, Deployment, and Automation Concepts 253
- CHAPTER 12 Summarizing Authentication and Authorization Design Concepts 285
- CHAPTER 13 Implementing Cybersecurity Resilience 311
- CHAPTER 14 Understanding the Security Implications of Embedded and Specialized Systems 335
- CHAPTER 15 Understanding the Importance of Physical Security Controls 367
- CHAPTER 16 Summarizing the Basics of Cryptographic Concepts 391

Part III: Implementation

- CHAPTER 17 Implementing Secure Protocols 423
- CHAPTER 18 Implementing Host or Application Security Solutions 447
- CHAPTER 19 Implementing Secure Network Designs 483
- CHAPTER 20 Installing and Configuring Wireless Security Settings 547

- CHAPTER 21** Implementing Secure Mobile Solutions 567
- CHAPTER 22** Applying Cybersecurity Solutions to the Cloud 595
- CHAPTER 23** Implementing Identity and Account Management Controls 619
- CHAPTER 24** Implementing Authentication and Authorization Solutions 651
- CHAPTER 25** Implementing Public Key Infrastructure 685

Part IV: Operations and Incident Response

- CHAPTER 26** Using the Appropriate Tool to Assess Organizational Security 703
- CHAPTER 27** Summarizing the Importance of Policies, Processes, and Procedures for Incident Response 755
- CHAPTER 28** Using Appropriate Data Sources to Support an Investigation 781
- CHAPTER 29** Applying Mitigation Techniques or Controls to Secure an Environment 819
- CHAPTER 30** Understanding the Key Aspects of Digital Forensics 837

Part V: Governance, Risk, and Compliance

- CHAPTER 31** Comparing and Contrasting the Various Types of Controls 865
- CHAPTER 32** Understanding the Importance of Applicable Regulations, Standards, or Frameworks That Impact Organizational Security Posture 875
- CHAPTER 33** Understanding the Importance of Policies to Organizational Security 893
- CHAPTER 34** Summarizing Risk Management Processes and Concepts 913
- CHAPTER 35** Understanding Privacy and Sensitive Data Concepts in Relation to Security 935

Part VI: Final Preparation

- CHAPTER 36** Final Preparation 953
 - Glossary of Key Terms 955
- APPENDIX A** Answers to the “Do I Know This Already?” Quizzes and Review Questions 1023
- APPENDIX B** *CompTIA Security+ (SY0-601) Cert Guide* Exam Updates 1087
 - Index 1089

Online Elements:

- APPENDIX C** Study Planner
 - Glossary of Key Terms

Table of Contents

Introduction xliv

Part I: Threats, Attacks, and Vulnerabilities

Chapter 1 Comparing and Contrasting Different Types of Social Engineering Techniques 3

“Do I Know This Already?” Quiz 3

Foundation Topics 7

Social Engineering Fundamentals 7

Phishing and Spear Phishing 9

Smishing 12

Vishing 12

Spam and Spam over Internet Messaging (SPIM) 13

Dumpster Diving 13

Shoulder Surfing 14

Pharming 14

Piggybacking or Tailgating 15

Eliciting Information 15

Whaling 16

Prepending 17

Identity Fraud 17

Invoice Scams 17

Credential Harvesting 18

Reconnaissance 18

Hoaxes 19

Impersonation or Pretexting 19

Eavesdropping 19

Baiting 20

Watering Hole Attack 20

Typo Squatting 20

Influence Campaigns, Principles of Social Engineering,
and Reasons for Effectiveness 21

User Security Awareness Education	22
Chapter Review Activities	24
Review Key Topics	24
Define Key Terms	25
Review Questions	26
Chapter 2 Analyzing Potential Indicators to Determine the Type of Attack	29
“Do I Know This Already?” Quiz	29
Foundation Topics	33
Malicious Software (Malware)	33
Ransomware and Cryptomalware	33
Trojans	35
Remote Access Trojans (RATs) and Rootkits	35
Worms	36
Fileless Virus	37
Command and Control, Bots, and Botnets	37
Logic Bombs	39
Potentially Unwanted Programs (PUPs) and Spyware	40
Keyloggers	42
Backdoors	43
Malware Delivery Mechanisms	43
You Can’t Save Every Computer from Malware!	45
Password Attacks	45
Dictionary-based and Brute-force Attacks	45
Password Spraying	46
Offline and Online Password Cracking	46
Rainbow Tables	47
Plaintext/Unencrypted	47
Physical Attacks	48
Malicious Flash Drives	48
Malicious Universal Serial Bus (USB) Cables	48
Card Cloning Attacks	48
Skimming	49

Adversarial Artificial Intelligence	50
Tainted Training Data for Machine Learning	50
Security of Machine Learning Algorithms	50
Supply-Chain Attacks	51
Cloud-based vs. On-premises Attacks	52
Cloud Security Threats	52
Cloud Computing Attacks	54
Cryptographic Attacks	55
Collision	55
Birthday	56
Downgrade	56
Chapter Review Activities	57
Review Key Topics	57
Define Key Terms	58
Review Questions	59
Chapter 3 Analyzing Potential Indicators Associated with Application Attacks	61
“Do I Know This Already?” Quiz	61
Foundation Topics	67
Privilege Escalation	67
Cross-Site Scripting (XSS) Attacks	68
Injection Attacks	70
Structured Query Language (SQL) Injection Attacks	70
SQL Injection Categories	73
Dynamic Link Library (DLL) Injection Attacks	74
Lightweight Directory Access Protocol (LDAP) Injection Attacks	74
Extensible Markup Language (XML) Injection Attacks	74
Pointer/Object Dereference	75
Directory Traversal	76
Buffer Overflows	77
Arbitrary Code Execution/Remote Code Execution	78
Race Conditions	79
Error Handling	79

	Improper Input Handling	80
	Compile-Time Errors vs. Runtime Errors	81
	Replay Attacks	82
	Request Forgeries	85
	Application Programming Interface (API) Attacks	86
	Resource Exhaustion	87
	Memory Leaks	88
	Secure Socket Layer (SSL) Stripping	88
	Driver Manipulation	89
	Pass the Hash	89
	Chapter Review Activities	90
	Review Key Topics	90
	Define Key Terms	92
	Review Questions	92
Chapter 4	Analyzing Potential Indicators Associated with Network Attacks	95
	“Do I Know This Already?” Quiz	95
	Foundation Topics	98
	Wireless Attacks	98
	Evil Twin Attacks	98
	Rogue Access Points	99
	Bluesnarfing Attacks	99
	Bluejacking Attacks	100
	Disassociation and Deauthentication Attacks	101
	Jamming Attacks	102
	Radio Frequency Identifier (RFID) Attacks	102
	Near-Field Communication (NFC) Attacks	102
	Initialization Vector (IV) Attacks	103
	On-Path Attacks	103
	Layer 2 Attacks	105
	Address Resolution Protocol (ARP) Poisoning Attacks	105
	Media Access Control (MAC) Flooding Attacks	106
	MAC Cloning Attacks	106
	Best Practices to Protect Against Layer 2 Attacks	106

	Domain Name System (DNS) Attacks	107
	Domain Hijacking Attacks	108
	DNS Poisoning Attacks	108
	Uniform Resource Locator (URL) Redirection Attacks	110
	Domain Reputation	110
	Distributed Denial-of-Service (DDoS) Attacks	111
	Malicious Code or Script Execution Attacks	113
	Chapter Review Activities	114
	Review Key Topics	114
	Define Key Terms	115
	Review Questions	115
Chapter 5	Understanding Different Threat Actors, Vectors, and Intelligence Sources	117
	“Do I Know This Already?” Quiz	117
	Foundation Topics	120
	Actors and Threats	120
	Attributes of Threat Actors	122
	Attack Vectors	122
	Threat Intelligence and Threat Intelligence Sources	123
	Structured Threat Information eXpression (STIX) and the Trusted Automated eXchange of Indicator Information (TAXII)	125
	Research Sources	127
	The MITRE ATT&CK Framework	128
	Chapter Review Activities	129
	Review Key Topics	129
	Define Key Terms	130
	Review Questions	131
Chapter 6	Understanding the Security Concerns Associated with Various Types of Vulnerabilities	133
	“Do I Know This Already?” Quiz	133
	Foundation Topics	137
	Cloud-based vs. On-premises Vulnerabilities	137
	Other “Cloud”-based Concerns	143
	Server Defense	144

	<i>File Servers</i>	144
	<i>Network Controllers</i>	144
	<i>Email Servers</i>	145
	<i>Web Servers</i>	146
	<i>FTP Server</i>	147
	Zero-day Vulnerabilities	149
	Weak Configurations	150
	Third-party Risks	155
	Improper or Weak Patch Management	160
	Patches and Hotfixes	161
	Patch Management	163
	Legacy Platforms	165
	The Impact of Cybersecurity Attacks and Breaches	165
	Chapter Review Activities	166
	Review Key Topics	166
	Define Key Terms	167
	Review Questions	168
Chapter 7	Summarizing the Techniques Used in Security Assessments	171
	“Do I Know This Already?” Quiz	171
	Foundation Topics	175
	Threat Hunting	175
	Security Advisories and Bulletins	177
	Vulnerability Scans	180
	Credentialed vs. Noncredentialed	182
	Intrusive vs. Nonintrusive	182
	Common Vulnerability Scoring System (CVSS)	182
	Logs and Security Information and Event Management (SIEM)	186
	Security Orchestration, Automation, and Response (SOAR)	188
	Chapter Review Activities	189
	Review Key Topics	189
	Define Key Terms	190
	Review Questions	190

Chapter 8 Understanding the Techniques Used in Penetration Testing 193

“Do I Know This Already?” Quiz	193
Foundation Topics	197
Penetration Testing	197
Bug Bounties vs. Penetration Testing	202
Passive and Active Reconnaissance	203
Exercise Types	205
Chapter Review Activities	206
Review Key Topics	206
Define Key Terms	207
Review Questions	207

Part II: Architecture and Design**Chapter 9 Understanding the Importance of Security Concepts in an Enterprise Environment 209**

“Do I Know This Already?” Quiz	209
Foundation Topics	213
Configuration Management	213
Data Sovereignty and Data Protection	214
Secure Sockets Layer (SSL)/Transport Layer Security (TLS) Inspection	215
API Considerations	216
Data Masking and Obfuscation	216
Encryption at Rest, in Transit/Motion, and in Processing	218
Hashing	218
Rights Management	219
Geographical Considerations	220
Data Breach Response and Recovery Controls	220
Site Resiliency	221
Deception and Disruption	222
Fake Telemetry	223
DNS Sinkhole	223
Chapter Review Activities	224

Review Key Topics	224
Define Key Terms	225
Review Questions	225
Chapter 10 Summarizing Virtualization and Cloud Computing Concepts	227
“Do I Know This Already?” Quiz	227
Foundation Topics	231
Cloud Models	231
Public, Private, Hybrid, and Community Clouds	232
Cloud Service Providers	233
Cloud Architecture Components	234
Fog and Edge Computing	234
Thin Clients	235
Containers	236
Microservices and APIs	240
Infrastructure as Code	241
Serverless Architecture	243
Services Integration	246
Resource Policies	246
Transit Gateway	246
Virtual Machine (VM) Sprawl Avoidance and VM Escape Protection	247
Understanding and Avoiding VM Sprawl	247
Protecting Against VM Escape Attacks	248
Chapter Review Activities	250
Review Key Topics	250
Define Key Terms	251
Review Questions	251
Chapter 11 Summarizing Secure Application Development, Deployment, and Automation Concepts	253
“Do I Know This Already?” Quiz	253
Foundation Topics	257
Software Development Environments and Methodologies	257
Application Provisioning and Deprovisioning	260
Software Integrity Measurement	261

Secure Coding Techniques	261
Core SDLC and DevOps Principles	263
Programming Testing Methods	266
<i>Compile-Time Errors vs. Runtime Errors</i>	266
<i>Input Validation</i>	267
<i>Static and Dynamic Code Analysis</i>	269
<i>Fuzz Testing</i>	269
Programming Vulnerabilities and Attacks	270
<i>Testing for Backdoors</i>	271
<i>Memory/Buffer Vulnerabilities</i>	271
<i>XSS and XSRF</i>	272
<i>More Code Injection Examples</i>	273
<i>Directory Traversal</i>	274
<i>Zero-Day Attack</i>	275
Open Web Application Security Project (OWASP)	276
Software Diversity	278
Automation/Scripting	278
Elasticity and Scalability	279
Chapter Review Activities	280
Review Key Topics	280
Define Key Terms	281
Review Questions	281
Chapter 12 Summarizing Authentication and Authorization Design Concepts	285
“Do I Know This Already?” Quiz	285
Foundation Topics	289
Authentication Methods	289
Directory Services	291
Federations	292
Attestation	294
Authentication Methods and Technologies	295
<i>Time-Based One-Time Password (TOTP)</i>	295
<i>HMAC-Based One-Time Password (HOTP)</i>	295

<i>Short Message Service (SMS)</i>	296
<i>Token Key</i>	297
<i>Static Codes</i>	298
<i>Authentication Applications</i>	298
<i>Push Notifications</i>	299
<i>Phone Call Authentication</i>	299
<i>Smart Card Authentication</i>	300
Biometrics	300
Fingerprints	300
Retina	301
Iris	301
Facial	301
Voice	302
Vein	302
Gait Analysis	302
Efficacy Rates	302
False Acceptance	303
False Rejection	303
Crossover Error Rate	304
Multifactor Authentication (MFA) Factors and Attributes	304
Authentication, Authorization, and Accounting (AAA)	306
Cloud vs. On-premises Requirements	306
Chapter Review Activities	308
Review Key Topics	308
Define Key Terms	308
Review Questions	308
Chapter 13 Implementing Cybersecurity Resilience	311
“Do I Know This Already?” Quiz	311
Foundation Topics	315
Redundancy	315
Geographic Dispersal	315
Disk Redundancy	315
<i>Redundant Array of Inexpensive Disks</i>	316

<i>Multipath</i>	319
Network Resilience	319
<i>Load Balancers</i>	319
<i>Network Interface Card (NIC) Teaming</i>	320
Power Resilience	320
<i>Uninterruptible Power Supply (UPS)</i>	320
<i>Generators</i>	321
<i>Dual Supply</i>	321
<i>Managed Power Distribution Units (PDUs)</i>	322
Replication	323
Storage Area Network	323
Virtual Machines	324
On-premises vs. Cloud	325
Backup Types	326
Full Backup	328
Differential Backup	328
Incremental Backup	328
Non-persistence	328
High Availability	329
Restoration Order	330
Diversity	331
Technologies	331
Vendors	331
Crypto	331
Controls	332
Chapter Review Activities	332
Review Key Topics	332
Define Key Terms	333
Review Questions	333
Chapter 14 Understanding the Security Implications of Embedded and Specialized Systems	335
“Do I Know This Already?” Quiz	335
Foundation Topics	339

Embedded Systems	339
Supervisory Control and Data Acquisition (SCADA)/Industrial Control Systems (ICS)	341
Internet of Things (IoT)	344
Specialized Systems	346
Medical Systems	347
Vehicles	347
Aircraft	348
Smart Meters	350
Voice over IP (VoIP)	351
Heating, Ventilation, and Air Conditioning (HVAC)	352
Drones	353
Multifunction Printers (MFP)	354
Real-Time Operating Systems (RTOS)	355
Surveillance Systems	355
System on a Chip (SoC)	356
Communication Considerations	357
5G	357
NarrowBand	358
Baseband Radio	359
Subscriber Identity Module (SIM) Cards	360
Zigbee	360
Embedded System Constraints	361
Power	361
Compute	361
Network	362
Crypto	362
Inability to Patch	362
Authentication	363
Range	363
Cost	363
Implied Trust	363

Chapter Review Activities	364
Review Key Topics	364
Define Key Terms	365
Review Questions	365
Chapter 15 Understanding the Importance of Physical Security Controls	367
“Do I Know This Already?” Quiz	367
Foundation Topics	370
Bollards/Barricades	370
Access Control Vestibules	372
Badges	373
Alarms	374
Signage	374
Cameras	375
Closed-Circuit Television (CCTV)	376
Industrial Camouflage	377
Personnel	377
Locks	378
USB Data Blockers	379
Lighting	380
Fencing	380
Fire Suppression	381
Sensors	381
Drones	382
Visitor Logs	383
Faraday Cages	383
Air Gap	384
Screened Subnet (Previously Known as Demilitarized Zone [DMZ])	384
Protected Cable Distribution	385
Secure Areas	385
Secure Data Destruction	386
Chapter Review Activities	387
Review Key Topics	387
Define Key Terms	388
Review Questions	389

Chapter 16 Summarizing the Basics of Cryptographic Concepts 391

“Do I Know This Already?” Quiz	391
Foundation Topics	395
Digital Signatures	395
Key Length	396
Key Stretching	397
Salting	397
Hashing	398
Key Exchange	399
Elliptic-Curve Cryptography	399
Perfect Forward Secrecy	400
Quantum	401
Communications	401
Computing	402
Post-Quantum	402
Ephemeral	403
Modes of Operation	403
Electronic Code Book Mode	404
Cipher Block Chaining Mode	405
Cipher Feedback Mode	406
Output Feedback Mode	407
Counter Mode	408
Blockchain	409
Cipher Suites	410
Symmetric vs. Asymmetric Encryption	411
Lightweight Cryptography	414
Steganography	415
Audio Steganography	415
Video Steganography	416
Image Steganography	416
Homomorphic Encryption	417
Common Use Cases	417
Limitations	418

Chapter Review Activities	420
Review Key Topics	420
Define Key Terms	421
Review Questions	421

Part III: Implementation

Chapter 17 Implementing Secure Protocols 423

“Do I Know This Already?” Quiz	423
Foundation Topics	426
Protocols	426
Domain Name System Security Extensions	426
SSH	427
Secure/Multipurpose Internet Mail Extensions	428
Secure Real-Time Transport Protocol	430
Lightweight Directory Access Protocol over SSL	432
File Transfer Protocol, Secure	432
Secure (or SSH) File Transfer Protocol	434
Simple Network Management Protocol Version 3	434
Hypertext Transfer Protocol over SSL/TLS	436
IPsec	437
<i>Authentication Header/Encapsulating Security Payloads</i>	437
<i>Tunnel/Transport</i>	438
Post Office Protocol/Internet Message Access Protocol	438
Use Cases	439
Voice and Video	440
Time Synchronization	440
Email and Web	441
File Transfer	441
Directory Services	442
Remote Access	442
Domain Name Resolution	442
Routing and Switching	443
Network Address Allocation	443
Subscription Services	444

Chapter Review Activities	444
Review Key Topics	444
Define Key Terms	445
Review Questions	445
Chapter 18 Implementing Host or Application Security Solutions	447
“Do I Know This Already?” Quiz	447
Foundation Topics	451
Endpoint Protection	451
Antivirus	451
Antimalware	452
Endpoint Detection and Response	452
Data Loss Prevention	453
Next-Generation Firewall	453
Host-based Intrusion Prevention System	454
Host-based Intrusion Detection System	456
Host-based Firewall	457
Boot Integrity	458
Boot Security/Unified Extensible Firmware Interface	459
Measured Boot	459
Boot Attestation	460
Database	461
Tokenization	461
Salting	462
Hashing	463
Application Security	463
Input Validations	464
Secure Cookies	465
Hypertext Transfer Protocol Headers	465
<i>End-to-End Headers</i>	466
<i>Hop-by-Hop Headers</i>	466
Code Signing	466
Allow List	467
Block List/Deny List	467

Secure Coding Practices	468
Static Code Analysis	468
Manual Code Review	470
Dynamic Code Analysis	470
Fuzzing	471
Hardening	471
Open Ports and Services	471
Registry	472
Disk Encryption	473
Operating System	473
Patch Management	474
Self-Encrypting Drive/Full-Disk Encryption	475
OPAL	476
Hardware Root of Trust	476
Trusted Platform Module	477
Sandboxing	478
Chapter Review Activities	479
Review Key Topics	479
Define Key Terms	481
Review Questions	481
Chapter 19 Implementing Secure Network Designs	483
“Do I Know This Already?” Quiz	483
Foundation Topics	488
Load Balancing	488
Active/Active	488
Active/Passive	488
Scheduling	488
Virtual IP	488
Persistence	489
Network Segmentation	489
Application-Based Segmentation and Microsegmentation	489
Virtual Local Area Network	490
Screened Subnet	491

East-West Traffic	492
Intranets and Extranets	492
Zero Trust	494
Virtual Private Network	494
Remote Access vs. Site-to-Site	496
IPsec	497
<i>IKEv1 Phase 1</i>	498
<i>IKEv1 Phase 2</i>	501
<i>IKEv2</i>	504
SSL/TLS	505
HTML5	508
Layer 2 Tunneling Protocol	508
DNS	509
Network Access Control	510
Out-of-Band Management	510
Port Security	511
Broadcast Storm Prevention	512
Bridge Protocol Data Unit Guard	512
Loop Prevention	512
Dynamic Host Configuration Protocol Snooping	512
Media Access Control Filtering	513
Network Appliances	513
Jump Servers	514
Proxy Servers	514
Network-Based Intrusion Detection System/Network-Based Intrusion Prevention System	516
<i>NIDS</i>	517
<i>NIPS</i>	518
Summary of NIDS vs. NIPS	519
<i>Signature-Based</i>	520
<i>Heuristic/Behavior</i>	521
<i>Anomaly</i>	521
<i>Inline vs. Passive</i>	523

HSM	524	
Sensors	524	
Collectors	525	
Aggregators	526	
Firewalls	526	
Hardware vs. Software	534	
Appliance vs. Host-based vs. Virtual	534	
Access Control List	535	
Route Security	535	
Quality of Service	536	
Implications of IPv6	536	
Port Spanning/Port Mirroring	537	
Monitoring Services	538	
<i>Performance Baselineing</i>	539	
File Integrity Monitors	542	
Chapter Review Activities	542	
Review Key Topics	542	
Define Key Terms	543	
Review Questions	544	
Chapter 20	Installing and Configuring Wireless Security Settings	547
“Do I Know This Already?” Quiz	547	
Foundation Topics	551	
Cryptographic Protocols	551	
Wi-Fi Protected Access 2 (WPA2)	551	
Wi-Fi Protected Access 3 (WPA3)	551	
Counter-mode/CBC-MAC Protocol (CCMP)	552	
Simultaneous Authentication of Equals	552	
Wireless Cryptographic Protocol Summary	552	
Authentication Protocols	553	
802.1X and EAP	553	
IEEE 802.1x	556	
Remote Authentication Dial-In User Service (RADIUS)		
Federation	556	

Methods	557
Wi-Fi Protected Setup	558
Captive Portals	559
Installation Considerations	559
Controller and Access Point Security	562
Wireless Access Point Vulnerabilities	563
Chapter Review Activities	564
Review Key Topics	564
Define Key Terms	564
Review Questions	565
Chapter 21 Implementing Secure Mobile Solutions	567
“Do I Know This Already?” Quiz	567
Foundation Topics	570
Connection Methods and Receivers	570
RFID and NFC	571
More Wireless Connection Methods and Receivers	572
Secure Implementation Best Practices	573
Mobile Device Management	574
MDM Security Feature Concerns: Application and Content Management	576
MDM Security Feature Concerns: Remote Wipe, Geofencing, Geolocation, Screen Locks, Passwords and PINs, Full Device Encryption	578
Mobile Device Management Enforcement and Monitoring	581
Mobile Devices	585
MDM/Unified Endpoint Management	587
SEAndroid	588
Deployment Models	588
Secure Implementation of BYOD, CYOD, and COPE	589
Chapter Review Activities	591
Review Key Topics	591
Define Key Terms	592
Review Questions	592

Chapter 22 Applying Cybersecurity Solutions to the Cloud 595

“Do I Know This Already?” Quiz	595
Foundation Topics	598
Cloud Security Controls	598
Security Assessment in the Cloud	598
Understanding the Different Cloud Security Threats	598
Cloud Computing Attacks	601
High Availability Across Zones	603
Resource Policies	603
Integration and Auditing	604
Secrets Management	604
Storage	605
<i>Permissions</i>	605
<i>Encryption</i>	605
<i>Replication</i>	605
<i>High Availability</i>	606
Network	606
<i>Virtual Networks</i>	606
<i>Public and Private Subnets</i>	606
<i>Segmentation</i>	607
<i>API Inspection and Integration</i>	607
Compute	607
<i>Security Groups</i>	607
<i>Dynamic Resource Allocation</i>	607
<i>Instance Awareness</i>	608
<i>Virtual Private Cloud Endpoint</i>	608
<i>Container Security</i>	608
Summary of Cloud Security Controls	609
Solutions	611
CASB	611
Application Security	612
Next-Generation Secure Web Gateway	613
Firewall Considerations in a Cloud Environment	613

<i>Cost</i>	613
<i>Need for Segmentation</i>	613
<i>Open Systems Interconnection Layers</i>	614
Summary of Cybersecurity Solutions to the Cloud	614
Cloud Native Controls vs. Third-Party Solutions	615
Chapter Review Activities	615
Review Key Topics	615
Define Key Terms	616
Review Questions	616
Chapter 23 Implementing Identity and Account Management Controls	619
“Do I Know This Already?” Quiz	619
Foundation Topics	623
Identity	623
Identity Provider (IdP)	623
Authentication	625
<i>Authentication by Knowledge</i>	625
<i>Authentication by Ownership</i>	625
<i>Authentication by Characteristic Attributes</i>	625
Certificates	626
Tokens	627
SSH Keys	628
Smart Cards	629
Account Types	629
Account Policies	633
Introduction to Identity and Access Management	633
<i>Phases of the Identity and Access Lifecycle</i>	633
<i>Registration and Identity Validation</i>	634
<i>Privileges Provisioning</i>	635
<i>Access Review</i>	635
<i>Access Revocation</i>	635
<i>Password Management</i>	636
<i>Password Creation</i>	636
Attribute-Based Access Control (ABAC)	638

	Rights, Permissions, and Policies	640
	<i>Users, Groups, and Account Permissions</i>	640
	Permission Inheritance and Propagation	645
	Chapter Review Activities	647
	Review Key Topics	647
	Define Key Terms	647
	Review Questions	648
Chapter 24	Implementing Authentication and Authorization Solutions	651
	“Do I Know This Already?” Quiz	651
	Foundation Topics	655
	Authentication Management	655
	Password Keys	655
	Password Vaults	655
	Trusted Platform Module	656
	Hardware Security Modules	656
	Knowledge-Based Authentication	656
	Authentication/Authorization	657
	Security Assertion Markup Language	659
	OAuth	661
	OpenID and OpenID Connect	663
	<i>802.1X and EAP</i>	664
	LDAP	667
	Kerberos and Mutual Authentication	668
	Remote Authentication Technologies	670
	Remote Access Service	670
	RADIUS versus TACACS+	672
	Access Control Schemes	674
	Discretionary Access Control	674
	Mandatory Access Control	676
	Role-Based Access Control	677
	Attribute-Based Access Control	678
	Rule-Based Access Control	678
	Conditional Access	678
	Privileged Access Management	678

Summary of Access Control Models	679
Access Control Wise Practices	680
Chapter Review Activities	681
Review Key Topics	681
Define Key Terms	682
Review Questions	682
Chapter 25 Implementing Public Key Infrastructure	685
“Do I Know This Already?” Quiz	685
Foundation Topics	688
Public Key Infrastructure	688
Key Management	688
Certificate Authorities	689
Certificate Attributes	691
Subject Alternative Name	693
Expiration	693
Types of Certificates	694
SSL Certificate Types	694
Certificate Chaining	696
Certificate Formats	697
PKI Concepts	698
Trust Model	698
Certificate Pinning	698
Stapling, Key Escrow, Certificate Chaining, Online vs. Offline CA	698
Chapter Review Activities	700
Review Key Topics	700
Define Key Terms	700
Review Questions	701
Part IV: Operations and Incident Response	
Chapter 26 Using the Appropriate Tool to Assess Organizational Security	703
“Do I Know This Already?” Quiz	703
Foundation Topics	707
Network Reconnaissance and Discovery	707
tracert/traceroute	707

nslookup/dig	709
ipconfig/ifconfig	710
nmap	711
ping/pathping	714
hping	717
netstat	718
netcat	720
IP Scanners	721
arp	721
route	723
curl	724
theHarvester	725
sn1per	726
scanless	727
dnsenum	728
Nessus	730
Cuckoo	731
File Manipulation	732
head	733
tail	734
cat	734
grep	735
chmod	736
Logger	737
Shell and Script Environments	738
SSH	739
PowerShell	740
Python	741
OpenSSL	741
Packet Capture and Replay	742
Tcpreplay	742
Tcpdump	742
Wireshark	743

- Forensics 744
 - dd** 744
 - Memdump 745
 - WinHex 746
 - FTK Imager 747
 - Autopsy 747
- Exploitation Frameworks 747
- Password Crackers 748
- Data Sanitization 750
- Chapter Review Activities 750
- Review Key Topics 750
- Define Key Terms 752
- Review Questions 752

Chapter 27 Summarizing the Importance of Policies, Processes, and Procedures for Incident Response 755

- “Do I Know This Already?” Quiz 755
- Foundation Topics 760
- Incident Response Plans 760
- Incident Response Process 761
 - Preparation 762
 - Identification 763
 - Containment 763
 - Eradication 764
 - Recovery 764
 - Lessons Learned 764
- Exercises 765
 - Tabletop 765
 - Walkthroughs 766
 - Simulations 766
- Attack Frameworks 767
 - MITRE ATT&CK 767
 - The Diamond Model of Intrusion Analysis 768
 - Cyber Kill Chain 770

Stakeholder Management	771
Communication Plan	771
Disaster Recovery Plan	772
Business Continuity Plan	773
Continuity of Operations Planning (COOP)	774
Incident Response Team	775
Retention Policies	776
Chapter Review Activities	776
Review Key Topics	776
Define Key Terms	777
Review Questions	778
Chapter 28 Using Appropriate Data Sources to Support an Investigation	781
“Do I Know This Already?” Quiz	781
Foundation Topics	785
Vulnerability Scan Output	785
SIEM Dashboards	786
Sensors	787
Sensitivity	788
Trends	788
Alerts	788
Correlation	788
Log Files	789
Network	790
System	791
Application	792
Security	793
Web	794
DNS	795
Authentication	796
Dump Files	797
VoIP and Call Managers	799
Session Initiation Protocol Traffic	800

- syslog/rsyslog/syslog-ng 800
- journalctl 802
- NXLog 803
- Bandwidth Monitors 804
- Metadata 805
 - Email 808
 - Mobile 808
 - Web 808
 - File 809
- NetFlow/sFlow 809
 - NetFlow 809
 - sFlow 810
 - IPFIX 811
- Protocol Analyzer Output 813
- Chapter Review Activities 814
- Review Key Topics 814
- Define Key Terms 816
- Review Questions 816
- Chapter 29 Applying Mitigation Techniques or Controls to Secure an Environment 819**
 - “Do I Know This Already?” Quiz 819
 - Foundation Topics 822
 - Reconfigure Endpoint Security Solutions 822
 - Application Approved Lists 822
 - Application Block List/Deny List 822
 - Quarantine 823
 - Configuration Changes 824
 - Firewall Rules 825
 - MDM 825
 - Data Loss Prevention 828
 - Content Filter/URL Filter 828
 - Update or Revoke Certificates 829
 - Isolation 830

Containment	830
Segmentation	831
SOAR	832
Runbooks	833
Playbooks	834
Chapter Review Activities	834
Review Key Topics	834
Define Key Terms	835
Review Questions	835
Chapter 30 Understanding the Key Aspects of Digital Forensics	837
“Do I Know This Already?” Quiz	837
Foundation Topics	842
Documentation/Evidence	842
Legal Hold	842
Video	842
Admissibility	843
Chain of Custody	844
Timelines of Sequence of Events	844
<i>Timestamps</i>	<i>844</i>
<i>Time Offset</i>	<i>845</i>
Tags	845
Reports	846
Event Logs	846
Interviews	846
Acquisition	847
Order of Volatility	848
Disk	848
Random-Access Memory	848
Swap/Pagefile	849
Operating System	850
Device	850
Firmware	851
Snapshot	851
Cache	852

Network	852
Artifacts	853
On-premises vs. Cloud	853
Right-to-Audit Clauses	854
Regulatory/Jurisdiction	855
Data Breach Notification Laws	855
Integrity	856
Hashing	856
Checksums	857
Provenance	857
Preservation	858
E-discovery	858
Data Recovery	859
Nonrepudiation	859
Strategic Intelligence/Counterintelligence	860
Chapter Review Activities	860
Review Key Topics	860
Define Key Terms	862
Review Questions	862

Part V: Governance, Risk, and Compliance

Chapter 31 Comparing and Contrasting the Various Types of Controls 865

“Do I Know This Already?” Quiz	865
Foundation Topics	868
Control Category	868
Managerial Controls	868
Operational Controls	868
Technical Controls	868
Summary of Control Categories	869
Control Types	869
Preventative Controls	869
Detective Controls	869
Corrective Controls	870
Deterrent Controls	870

	Compensating Controls	871
	Physical Controls	871
	Summary of Control Types	872
	Chapter Review Activities	873
	Review Key Topics	873
	Define Key Terms	873
	Review Questions	873
Chapter 32	Understanding the Importance of Applicable Regulations, Standards, or Frameworks That Impact Organizational Security Posture	875
	“Do I Know This Already?” Quiz	875
	Foundation Topics	878
	Regulations, Standards, and Legislation	878
	General Data Protection Regulation	879
	National, Territory, or State Laws	879
	Payment Card Industry Data Security Standard (PCI DSS)	881
	Key Frameworks	881
	Benchmarks and Secure Configuration Guides	885
	Security Content Automation Protocol	885
	Chapter Review Activities	889
	Review Key Topics	889
	Define Key Terms	889
	Review Questions	890
Chapter 33	Understanding the Importance of Policies to Organizational Security	893
	“Do I Know This Already?” Quiz	894
	Foundation Topics	897
	Personnel Policies	897
	Privacy Policies	897
	Acceptable Use	898
	Separation of Duties/Job Rotation	898
	Mandatory Vacations	898
	Onboarding and Offboarding	899
	Personnel Security Policies	900

	Diversity of Training Techniques	900
	User Education and Awareness Training	901
	Third-Party Risk Management	902
	Data Concepts	904
	Understanding Classification and Governance	904
	Data Retention	906
	Credential Policies	906
	Organizational Policies	908
	Change Management and Change Control	909
	Asset Management	909
	Chapter Review Activities	910
	Review Key Topics	910
	Define Key Terms	910
	Review Questions	911
Chapter 34	Summarizing Risk Management Processes and Concepts	913
	“Do I Know This Already?” Quiz	913
	Foundation Topics	917
	Risk Types	917
	Risk Management Strategies	918
	Risk Analysis	919
	Qualitative Risk Assessment	921
	Quantitative Risk Assessment	922
	Disaster Analysis	924
	Business Impact Analysis	926
	Disaster Recovery Planning	928
	Chapter Review Activities	930
	Review Key Topics	930
	Define Key Terms	931
	Review Questions	931
Chapter 35	Understanding Privacy and Sensitive Data Concepts in Relation to Security	935
	“Do I Know This Already?” Quiz	935
	Foundation Topics	940
	Organizational Consequences of Privacy and Data Breaches	940

Notifications of Breaches	941
Data Types and Asset Classification	941
Personally Identifiable Information and Protected Health Information	943
<i>PII</i>	943
<i>PHI</i>	944
Privacy Enhancing Technologies	944
Roles and Responsibilities	945
Information Lifecycle	947
Impact Assessment	948
Terms of Agreement	948
Privacy Notice	949
Chapter Review Activities	949
Review Key Topics	949
Define Key Terms	949
Review Questions	950

Part VI: Final Preparation

Chapter 36 Final Preparation 953

Hands-on Activities	953
Suggested Plan for Final Review and Study	953
Summary	954

Glossary of Key Terms 955

Appendix A Answers to the “Do I Know This Already?” Quizzes and Review Questions 1023

Appendix B *CompTIA Security+ (SY0-601) Cert Guide Exam Updates* 1087 **Index 1089**

Online Elements:

Appendix C	Study Planner
	Glossary of Key Terms

About the Authors

Omar Santos is an active member of the cybersecurity community, where he leads several industry-wide initiatives. He is a best-selling author and trainer. Omar is the author of more than 20 books and video courses, as well as numerous white papers, articles, and security configuration guidelines and best practices. Omar is a principal engineer of the Cisco Product Security Incident Response Team (PSIRT), Security Research and Operations, where he mentors and leads engineers and incident managers during the investigation and resolution of cybersecurity vulnerabilities.

Omar co-leads the DEF CON Red Team Village, is the chair of the Common Security Advisory Framework (CSAF) technical committee, is the co-chair of the Forum of Incident Response and Security Teams (FIRST) Open Source Security working group, and has been the chair of several initiatives in the Industry Consortium for Advancement of Security on the Internet (ICASI). 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. You can find additional information about Omar's current projects at h4cker.org and can follow Omar on Twitter @santosomar.

Ron Taylor has been in the information security field for more than 20 years working in various areas focusing on both offense and defense security roles. Ten of those years were spent in consulting. In 2008, he joined the Cisco Global Certification Team as an SME in information assurance. From there, he moved into a position with the Security Research and Operations group, 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, and provided consulting support to many product teams as an SME on product security testing. His next role was incident manager for the Cisco Product Security Incident Response Team (PSIRT). Currently, Ron is a security architect specializing in the Cisco security product line. He has held a number of industry certifications, including GPEN, GWEB, GCIA, GCIH, GWAPT, RHCE, CCSP, CCNA, CISSP, PenTest+, and MCSE. Ron has also authored books and video courses, teaches, and is involved in organizing a number of cybersecurity conferences, including the BSides Raleigh, Texas Cyber Summit, Grayhat, and the Red Team Village at DEFCON.

Twitter: @Gu5G0rman

Linkedin: www.linkedin.com/in/-RonTaylor

Joseph Mlodzianowski is an information security aficionado and adventurer; he started multiple villages at RSA Conference, DEFCON, and BLACK HAT, among others, including founding the Red Team Village with the help of great friends. He has been in the information technology security field for more than 25 years working in infrastructure, security, networks, systems, design, offense, and defense. Joseph is currently an enterprise security architect of Cisco Managed Services. He spent more than 10 years in the Department of Defense as an operator, principal security network engineer, and SME designing and deploying complex technologies and supporting missions around the world in multiple theaters. He has consulted, investigated, and provided support for multiple federal agencies over the past 15 years. Joseph continues to contribute to content, reviews, and editing in the certification testing and curriculum process. He spent almost 15 years in the energy sector supporting refineries, pipelines, and chemical plants; specializing in industrial control networks; and building data centers. Joseph holds a broad range of certifications, including the Cisco CCIE, CNE, CSNA, CNSS-4012, CISSP, ITILv4, NSA IAM, NSA IEM, OIAC1180, FEMA IS-00317, ACMA, First Responder, Hazmat Certified, Member of Bexar County Sheriff's Office CERT, MCSE, and Certified Hacking Investigator. He also is a founding contributor to the CyManII | Cybersecurity Manufacturing Innovation Institute, a member of Messaging Malware Mobile Anti-Abuse Working Group (M3aawg.org), and founder of the Texas Cyber Summit and Grayhat Conferences. He believes in giving back to the community and supporting nonprofits.

Twitter: @Cedoxx

Linkedin: www.linkedin.com/in/mlodzianowski/

Dedication

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

—Omar

I would not be where I am today without the support of my family. Mom and Dad, you taught me the importance of work ethic and drive. Kathy, my wife of 20 years, you have supported me and encouraged me every step of the way. Kaitlyn, Alex, and Grace, you give me the strength and motivation to keep doing what I do.

—Ron

Without faith and spiritual guidance, none of us would be where we are. I would like to thank my Creator; Linda, my lovely wife of more than 20 years; and my daughter Lauren, for their unwavering support, patience, and encouragement while I work multiple initiatives and projects.

—Joseph

Acknowledgments

It takes a lot of amazing people to publish a book. Special thanks go to Chris Cleveland, Nancy Davis, Chris Crayton, and all the others at Pearson (and beyond) who helped make this book a reality. We appreciate everything you do!

About the Technical Reviewer

Chris Crayton is a technical consultant, trainer, author, and industry-leading technical editor. He has worked as a computer technology and networking instructor, information security director, network administrator, network engineer, and PC specialist. Chris has authored several print and online books on PC repair, CompTIA A+, CompTIA Security+, and Microsoft Windows. He has also served as technical editor and content contributor on numerous technical titles for several of the leading publishing companies. He holds numerous industry certifications, has been recognized with many professional and teaching awards, and has served as a state-level SkillsUSA final competition judge. Chris tech edited and contributed to this book to make it better for students and those wishing to better their lives.

We Want to Hear from You!

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

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

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

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

Email: community@informit.com

Introduction

Welcome to the *CompTIA Security+ SY0-601 Cert Guide*. The CompTIA Security+ certification is widely accepted as the first security certification you should attempt to attain in your information technology (IT) career. The CompTIA Security+ certification is designed to be a vendor-neutral exam that measures your knowledge of industry-standard technologies and methodologies. It acts as a great stepping stone to other vendor-specific certifications and careers. We developed this book to be something you can study from for the exam and keep on your bookshelf for later use as a security resource.

We would like to note that it's unfeasible to cover all security concepts in depth in a single book. However, the Security+ exam objectives are looking for a basic level of computer, networking, and organizational security knowledge. Keep this in mind while reading through this text, and remember that the main goal of this text is to help you pass the Security+ exam, not to be the master of all security. Not just yet, at least!

Good luck as you prepare to take the CompTIA Security+ exam. As you read through this book, you will be building an impenetrable castle of knowledge, culminating in hands-on familiarity and the know-how to pass the exam.

Goals and Methods

The number one goal of this book is to help you pass the SY0-601 version of the CompTIA Security+ certification exam. To that effect, we have filled this book and practice exams with hundreds of questions/answers and explanations, including two full practice exams. The exams are located in Pearson Test Prep practice test software in a custom test environment. These tests are geared to check your knowledge and ready you for the real exam.

The CompTIA Security+ certification exam involves familiarity with computer security theory and hands-on know-how. To aid you in mastering and understanding the Security+ certification objectives, this book uses the following methods:

- **Opening topics list:** This list defines the topics to be covered in the chapter.
- **Foundation Topics:** The heart of the chapter. The text explains the topics from a theory-based standpoint, as well as from a hands-on perspective. This includes in-depth descriptions, tables, and figures that are geared to build your knowledge so that you can pass the exam. Each chapter covers a full objective from the CompTIA Security+ exam blueprint.
- **Key Topics:** The Key Topic icons indicate important figures, tables, and lists of information that you should know for the exam. They are interspersed throughout the chapter and are listed in table format at the end of the chapter.

- **Key Terms:** Key terms without definitions are listed at the end of each chapter. See whether you can define them, and then check your work against the complete key term definitions in the glossary.
- **Review Questions:** These quizzes and answers with explanation are meant to gauge your knowledge of the subjects. If an answer to a question doesn't come readily to you, be sure to review that portion of the chapter.
- **Practice Exams:** The practice exams are included in the Pearson Test Prep practice test software. These exams test your knowledge and skills in a realistic testing environment. Take them after you have read through the entire book. Master one; then move on to the next.

Who Should Read This Book?

This book is for anyone who wants to start or advance a career in computer security. Readers of this book can range from persons taking a Security+ course to individuals already in the field who want to keep their skills sharp or perhaps retain their job due to a company policy mandating they take the Security+ exam. Some information assurance professionals who work for the Department of Defense or have privileged access to DoD systems are required to become Security+ certified as per DoD directive 8570.1.

This book is also designed for people who plan on taking additional security-related certifications after the CompTIA Security+ exam. The book is designed in such a way to offer an easy transition to future certification studies.

Although not a prerequisite, it is recommended that CompTIA Security+ candidates have at least two years of IT administration experience with an emphasis on security. The CompTIA Network+ certification is also recommended as a prerequisite. Before you begin your Security+ studies, it is expected that you understand computer topics such as how to install operating systems and applications, and networking topics such as how to configure IP, what a VLAN is, and so on. The focus of this book is to show how to secure these technologies and protect against possible exploits and attacks. Generally, for people looking to enter the IT field, the CompTIA Security+ certification is attained after the A+ and Network+ certifications.

CompTIA Security+ Exam Topics

If you haven't downloaded the Security+ certification exam objectives, do it now from CompTIA's website: <https://certification.comptia.org/>. Save the PDF file and print it out as well. It's a big document; review it carefully. Use the exam objectives list and acronyms list to aid in your studies while you use this book.

The following tables are excerpts from the exam objectives document. Table I-1 lists the CompTIA Security+ domains and each domain's percentage of the exam.

Table I-1 CompTIA Security+ Exam Domains

Domain	Exam Topic	% of Exam
1.0	Attacks, Threats, and Vulnerabilities	24%
2.0	Architecture and Design	21%
3.0	Implementation	25%
4.0	Operations and Incident Response	16%
5.0	Governance, Risk, and Compliance	14%

The Security+ domains are then further broken down into individual objectives. Table I-2 lists the CompTIA Security+ exam objectives and their related chapters in this book. It does not list the bullets and sub-bullets for each objective.

Table I-2 CompTIA Security+ Exam Objectives

Objective	Chapter(s)
1.1 Compare and contrast different types of social engineering techniques.	1
1.2 Given a scenario, analyze potential indicators to determine the type of attack.	2
1.3 Given a scenario, analyze potential indicators associated with application attacks.	3
1.4 Given a scenario, analyze potential indicators associated with network attacks.	4
1.5 Explain different threat actors, vectors, and intelligence sources.	5
1.6 Explain the security concerns associated with various types of vulnerabilities.	6
1.7 Summarize the techniques used in security assessments.	7
1.8 Explain the techniques used in penetration testing.	8
2.1 Explain the importance of security concepts in an enterprise environment.	9
2.2 Summarize virtualization and cloud computing concepts.	10
2.3 Summarize secure application development, deployment, and automation concepts.	11
2.4 Summarize authentication and authorization design concepts.	12
2.5 Given a scenario, implement cybersecurity resilience.	13
2.6 Explain the security implications of embedded and specialized systems.	14
2.7 Explain the importance of physical security controls.	15
2.8 Summarize the basics of cryptographic concepts.	16
3.1 Given a scenario, implement secure protocols.	17

Objective	Chapter(s)
3.2 Given a scenario, implement host or application security solutions.	18
3.3 Given a scenario, implement secure network designs.	19
3.4 Given a scenario, install and configure wireless security settings.	20
3.5 Given a scenario, implement secure mobile solutions.	21
3.6 Given a scenario, apply cybersecurity solutions to the cloud.	22
3.7 Given a scenario, implement identity and account management controls.	23
3.8 Given a scenario, implement authentication and authorization solutions.	24
3.9 Given a scenario, implement public key infrastructure.	25
4.1 Given a scenario, use the appropriate tool to assess organizational security.	26
4.2 Summarize the importance of policies, processes, and procedures for incident response.	27
4.3 Given an incident, utilize appropriate data sources to support an investigation.	28
4.4 Given an incident, apply mitigation techniques or controls to secure an environment.	29
4.5 Explain the key aspects of digital forensics.	30
5.1 Compare and contrast various types of controls.	31
5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.	32
5.3 Explain the importance of policies to organizational security.	33
5.4 Summarize risk management processes and concepts.	34
5.5 Explain privacy and sensitive data concepts in relation to security.	35

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. On your Account page, tap or click the **Registered Products** tab, and then tap or click the **Register Another Product** link.
3. Enter this book's ISBN (9780136770312).
4. Answer the challenge question as proof of book ownership.
5. Tap or click the **Access Bonus Content** link for this book to go 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 preceding steps, please visit <http://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.

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

Accessing the Pearson Test Prep Software Online

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

1. Go to www.PearsonTestPrep.com and select **Pearson IT Certification** as your product group.
2. Enter your email/password for your account. If you do not have an account on PearsonITCertification.com or InformIT.com, you will need to establish one by going to PearsonITCertification.com/join.

3. On the My Products tab, tap or click the **Activate New Product** button.
4. Enter this book's activation code and click **Activate**.
5. The product will now be listed on your My Products tab. Tap or 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 this 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 <http://www.pearsonitcertification.com/register> and entering the ISBN: 9780136770312.
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 click the **Activate Exam** button on the My Products tab.
9. Click the **Activate a Product** button in the Activate Product Wizard.
10. Enter the unique access code found on the card in the sleeve in the back of your book and click the **Activate** button.
11. Click **Next** and then 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 enables 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 specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

You can also select the exam banks on which to focus. Each exam bank comes complete with a full exam of questions that cover topics in every chapter. You can have the test engine serve up exams from all 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, or whether to serve up only specific types of questions. You can also create custom test banks by selecting only questions that you have marked or questions on which you have added notes.

Updating Your Exams

If you are using the online version of the Pearson Test Prep software, you should always have access to the latest version of the software as well as the exam data. If you are using the Windows desktop version, every time you launch the software, it will check to see if there are any updates to your exam data and automatically download

any changes 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 exams.

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

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

Premium Edition eBook and Practice Tests

This book also includes an exclusive offer for 80 percent off the Premium Edition eBook and Practice Tests edition of this title. Please see the coupon code included with the cardboard sleeve for information on how to purchase the Premium Edition.

Figure Credits

Cover image: TippaPatt/Shutterstock
Chapter opener image: Charlie Edwards/Photodisc/Getty Images
Figures 4-2 and 4-3 courtesy of Cisco Systems, Inc
Figure 5-1 © 2015-2021, The MITRE Corporation
Figure 7-5 courtesy of Cisco Systems, Inc
Figures 10-1, 10-7, 10-10 courtesy of Cisco Systems, Inc
Figure 10-8 © 2021, Amazon Web Services, Inc
Figure 12-3 courtesy of Secret Double Octopus
Figure 12-4 courtesy of Active-Directory-FAQ
Figure 12-5 courtesy of Robert Koczera/123RF
Figures 13-1 and 13-2 © AsusTek Computer Inc.
Figure 14-1 Raspberry Pi courtesy of handmadepictures/123RF
Figure 14-3 courtesy of CSS Electronics
Figure 14-4 courtesy of strajinsky/Shutterstock
Figure 14-5 courtesy of RingCentral
Figures 14-6 and 15-4 from rewelda/Shutterstock
Figure 15-1 courtesy of Kyril Gorlov/123RF
Figure 15-2 courtesy of Aliaksandr Karankevich/123RF
Figures 16-9 and 16-10 courtesy of ssl2buy.com
Figure 17-1 courtesy of hostinger.com
Figure 17-3 courtesy of wiki.innovaphone.com
Figure 17-4 courtesy of Adaptive Digital Technologies
Figure 18-4 © Microsoft 2021
Figure 18-5 courtesy of Microsoft Corporation
Figure 18-7 courtesy of Checkmarx Ltd
Figure 19-1 courtesy of Cisco Systems, Inc
Figures 19-5, 19-8 through 19-11, 19-15, and 19-16 courtesy of Cisco Systems, Inc
Figure 19-21 © Microsoft 2021
Figures 20-2 and Figure 24-4 © Microsoft 2021
Figure 20-4 © D-Link Corporation
Figure 20-5 courtesy of Cisco Systems, Inc
Figures 21-1 and 21-2 © 1992-2020 Cisco
Figures 23-1 and 23-2 courtesy of Cisco Systems, Inc
Figures 23-5 through 23-9 © Microsoft 2021
Figures 24-2 and 24-5 courtesy of Cisco Systems, Inc
Figures 24-6 through 24-10 © Microsoft 2021
Figures 25-1 and 25-2 ©1998–2021 Mozilla Foundation
Figure 26-1 © OffSec Services Limited 2021
Figures 26-2, 26-5, 26-6, 26-10 through 26-15, 26-18, 26-19 © 2021 The Linux Foundation
Figures 26-3, 26-4, 26-7 through 26-9 © Microsoft 2021
Figure 26-16 © 2021 Tenable, Inc
Figure 26-17 © 2010-2020, Cuckoo Foundation
Figure 26-21 © Wireshark Foundation
Figure 26-22 © X-Ways Software Technology AG
Figure 27-3 courtesy of Cisco Systems, Inc
Figure 27-4 courtesy of Evolve IP, LLC
Figure 28-1 © 2021 Tenable, Inc

Figure 28-2 © 2021 LogRhythm, Inc

Figure 28-3 © MaxBelkov

Figure 28-4 © 1992-2020 Cisco

Figure 28-5, 28-6, 28-10, 28-11, and 28-18 © Microsoft 2021

Figures 28-7 through 28-9, 28-14, and 28-15 © 2021 The Linux Foundation

Figures 28-12 and 28-13 © 1992-2020 Cisco

Figure 28-16 © 2021 NXLog Ltd

Figure 28-20 © 2021 SolarWinds Worldwide, LLC

Figure 28-21 © 2003-2021 sFlow.org

Figure 28-22 © Plixer, LLC

Figure 28-23 © Microsoft 2021

Figures 29-1 and 29-2 © Microsoft 2021

Figure 33-1 © Microsoft 2021

Summarizing the Techniques Used in Security Assessments

This chapter starts by introducing threat hunting and how the threat-hunting process leverages threat intelligence. Then you learn about vulnerability management tasks, such as keeping up with security advisories and performing vulnerability scans. You also learn about the importance of collecting logs (such as system logs [syslogs]) and analyzing those logs in a Security Information and Event Management (SIEM) system. In addition, you learn how security tools and solutions have evolved to provide Security Orchestration, Automation, and Response (SOAR) capabilities to better defend your network, your users, and your organizations overall.

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz enables you to assess whether you should read this entire chapter thoroughly or jump to the “Chapter Review Activities” section. If you are in doubt about your answers to these questions or your own assessment of your knowledge of the topics, read the entire chapter. Table 7-1 lists the major headings in this chapter and their corresponding “Do I Know This Already?” quiz questions. You can find the answers in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.”

Table 7-1 “Do I Know This Already?” Section-to-Question Mapping

Foundation Topics Section	Questions
Threat Hunting	1–3
Vulnerability Scans	4–6
Syslog and Security Information and Event Management (SIEM)	7–8
Security Orchestration, Automation, and Response (SOAR)	9–10

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

1. What is the act of proactively and iteratively looking for threats in your organization that may have bypassed your security controls and monitoring capabilities?
 - a. Threat intelligence
 - b. Threat hunting
 - c. Threat binding
 - d. None of these answers are correct.

2. Which of the following provides a matrix of adversary tactics, techniques, and procedures that modern attackers use?
 - a. ATT&CK
 - b. CVSS
 - c. CVE
 - d. All of these answers are correct.

3. Which identifier is assigned to disclosed vulnerabilities?
 - a. CVE
 - b. CVSS
 - c. ATT&CK
 - d. TTP

4. Which broad term describes a situation in which a security device triggers an alarm, but no malicious activity or actual attack is taking place?
 - a. False negative
 - b. True negative
 - c. False positive
 - d. True positive

5. Which of the following is a successful identification of a security attack or a malicious event?
 - a. True positive
 - b. True negative
 - c. False positive
 - d. False negative

6. Which of the following occurs when a vulnerability scanner logs in to the targeted system to perform deep analysis of the operating system, running applications, and security misconfigurations?
 - a. Credentialed scan
 - b. Application scan
 - c. Noncredentialed scan
 - d. None of these answers are correct.

7. Which of the following are functions of a SIEM?
 - a. Log collection
 - b. Log normalization
 - c. Log correlation
 - d. All of these answers are correct.

8. Which solution allows security analysts to collect network traffic metadata?
 - a. NetFlow
 - b. SIEM
 - c. SOAR
 - d. None of these answers are correct.

9. Which solution provides capabilities that extend beyond traditional SIEMs?
 - a. SOAR
 - b. CVSS
 - c. CVE
 - d. IPFIX

10. Which of the following can be capabilities and benefits of a SOAR solution?
- a. Automated vulnerability assessment
 - b. SOC playbooks and runbook automation
 - c. Orchestration of multiple SOC tools
 - d. All of these answers are correct.

Foundation Topics

Threat Hunting

No security product or technology in the world can detect and block all security threats in the continuously evolving threat landscape (regardless of the vendor or how expensive it is). This is why many organizations are tasking senior analysts in their computer security incident response team (CSIRT) and their security operations center (SOC) to hunt for threats that may have bypassed any security controls that are in place. This is why threat hunting exists.

Key Topic

Threat hunting is the act of proactively and iteratively looking for threats in your organization. This chapter covers details about threat-hunting practices, the operational challenges of a threat-hunting program, and the benefits of a threat-hunting program.

The threat-hunting process requires deep knowledge of the network and often is performed by SOC analysts (otherwise known as investigators, threat hunters, tier 2 or tier 3 analysts, and so on). Figure 7-1 illustrates the traditional SOC tiers and where threat hunters typically reside. In some organizations (especially small organizations), threat hunting could be done by anyone in the SOC because the organization may not have a lot of resources (analysts). The success of threat hunting completely depends on the maturity of the organization and the resources available.

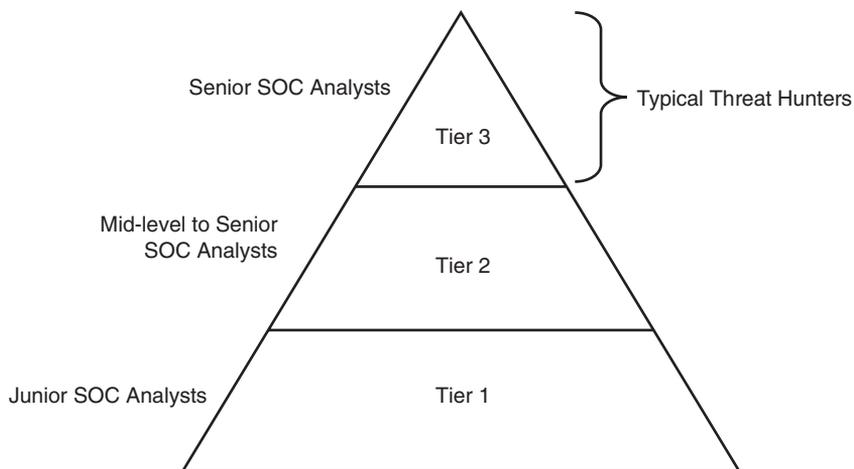


FIGURE 7-1 The SOC Tiers

Some organizations might have a dedicated team within or outside the SOC to perform threat hunting. However, one of the common practices is to have the hunters embedded within the SOC.

Threat hunters assume that an attacker has already compromised the network. Consequently, they need to come up with a hypothesis of what is compromised and how an adversary could have performed the attack. For the threat hunting to be successful, hunters need to be aware of the adversary tactics, techniques, and procedures (TTPs) that modern attackers use. This is why many organizations use MITRE's ATT&CK framework to be able to learn about the tactics and techniques of adversaries. Later in this chapter you learn more about how MITRE's ATT&CK can be used in threat hunting.

Threat hunting is not a new concept. Many organizations have performed threat hunting for a long time. However, in the last decade many organizations have adopted new ways to enhance the threat-hunting process with automation and orchestration.

Threat hunting is not the same as the traditional SOC incident response (reactive) activities. Threat hunting is also not the same as vulnerability management (the process of patching vulnerabilities across the systems and network of your organization, including cloud-based applications in some cases). However, some of the same tools and capabilities may be shared among threat hunters, SOC analysts, and vulnerability management teams. Tools and other capabilities such as data analytics, TTPs, vulnerability feeds, and *threat feeds* may be used across the different teams and analysts in an organization.

A high-level threat-hunting process includes the following steps:

- Step 1.** Threat hunting starts with a trigger based on an anomaly, threat intelligence, or a hypothesis (what could an attacker have done to the organization?). From that moment you should ask yourself: “Do we really need to perform this threat-hunting activity?” or “What is the scope?”
- Step 2.** Then you identify the necessary tools and methodologies to conduct the hunt.
- Step 3.** Once the tools and methodologies are identified, you reveal new attack patterns, TTPs, and so on.
- Step 4.** You refine your hunting tactics and enrich them using data analytics. Steps 2–3 can take one cycle or be iterative and involve multiple loops (depending on what you find and what additional data and research need to be done).

Step 5. A successful outcome could be that you identify and mitigate the threat. However, you need to recognize that in some cases this may not be the case. You may not have the necessary tools and capabilities, or there was no actual threat. This is why the success of your hunting program depends on the maturity of your capabilities and organization as a whole.

You can measure the maturity of your threat-hunting program within your organization in many ways. Figure 7-2 shows a matrix that can be used to evaluate the maturity level of your organization against different high-level threat-hunting elements.

These threat-hunting maturity levels can be categorized as easily as level 1, 2, and 3, or more complex measures can be used.

When it comes to threat intelligence and threat hunting, automation is key! Many organizations are trying to create threat *intelligence fusion* techniques to automatically extract threat intelligence data from heterogeneous sources to analyze such data. The goal is for the threat hunter and network defender to maneuver quickly—and faster than the attacker. This way, you can stay one step ahead of threat actors and be able to mitigate the attack.

Security Advisories and Bulletins

Key Topic

In Chapter 5, “Understanding Different Threat Actors, Vectors, and Intelligence Sources,” you learned how vendors, coordination centers, security researchers, and others publish *security advisories* and bulletins to disclose vulnerabilities. Most of the vulnerabilities disclosed to the public are assigned *Common Vulnerability and Exposure (CVE)* identifiers. CVE is a standard created by MITRE (www.mitre.org) that provides a mechanism to assign an identifier to vulnerabilities so that you can correlate the reports of those vulnerabilities among sites, tools, and feeds.

NOTE You can obtain additional information about CVE at <https://cve.mitre.org>.

One of the most comprehensive and widely used vulnerability databases is the National Vulnerability Database (NVD) maintained by the National Institute of Standards and Technology (NIST). NVD provides information about vulnerabilities disclosed worldwide.

NOTE You can access the NVD and the respective vulnerability feeds at <https://nvd.nist.gov>.

		Threat Hunting Maturity Level		
		Initial (Minimal) Level 1	Intermediate Level 2	Innovative and Leading Level 3
Threat Intelligence and Data Collection		Limited access of threat intelligence and collection of data	High collection of certain types of threat intelligence and data	High collection of many types of threat intelligence and data
Hypothesis Creation		Responds only to existing SIEM, IPS/IDS, firewall logs, etc.	Combines traditional logs with TTPs and threat intelligence	Combines traditional logs with TTPs and threat intelligence and develops automated threat risk scoring
Tools and Techniques for Hunting Hypothesis Testing		Reactive alerts and SIEM searches	Simple tools and analytics leveraging some visualizations, but mostly a manual effort	Advanced search capabilities, visualizations, creating new tools and not depending on traditional tools
TTP Detection		None, only traditional SIEM reactive detection	Identification of indicators of compromise (IoCs) and new attack trends	Able to detect adversary TTPs, IoCs, and create automation for the SOC to routinely detect them in the future
Analytics and Automation		None	Limited analytics and automation	Create automated tools for the SOC to routinely detect threats in the future

Threat Hunting High-level Elements

FIGURE 7-2 Threat-Hunting Maturity

Most mature vendors such as Microsoft, Intel, and Cisco publish security advisories and bulletins in their websites and are CVE Numbering Authorities (CNAs). CNAs can assign CVEs to disclosed vulnerabilities and submit the information to MITRE and subsequently to NVD.

NOTE You can find additional information about CNAs at <https://cve.mitre.org/cve/cna.html>.

The following links include examples of security advisories and bulletins published by different vendors:

- **Cisco:** <https://www.cisco.com/go/psirt>
- **Microsoft:** <https://www.microsoft.com/en-us/msrc>
- **Red Hat:** <https://access.redhat.com/security/security-updates>
- **Palo Alto:** <https://security.paloaltonetworks.com>

Vulnerability disclosures in security advisories are often coordinated among multiple vendors. Most of the products and applications developed nowadays use open-source software. Vulnerabilities in open-source software could affect hundreds or thousands of products and applications in the industry. In addition, vulnerabilities in protocols such as TLS, TCP, BGP, OSPF, and WPA could also affect numerous products and software. Patching open-source and protocol-related vulnerabilities among upstream and downstream vendors is not an easy task and requires good coordination. Figure 7-3 shows the high-level process of a coordinated vulnerability disclosure and underlying patching.

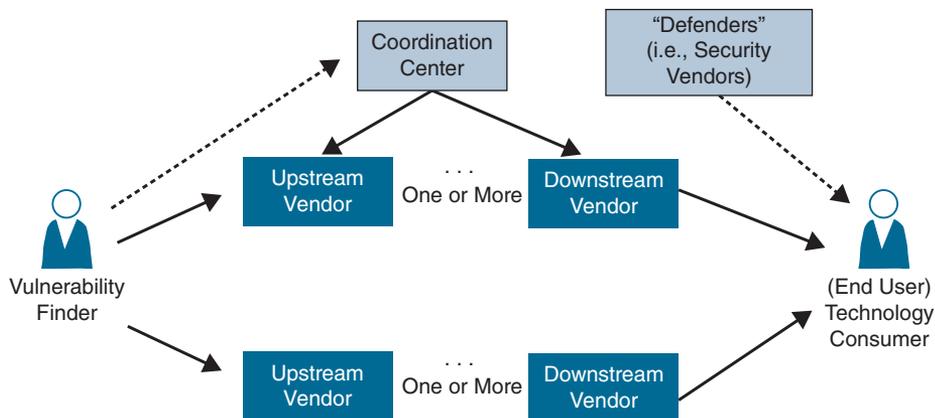


FIGURE 7-3 Coordinated Vulnerability Disclosures

The following steps are illustrated in Figure 7-3:

1. The finder (this can be anyone—a security researcher, customer, security company, an internal employee of a vendor) finds a security vulnerability and reports it to a vendor. The finder can also contact a vulnerability coordination center (such as www.cert.org) to help with the coordination and disclosure.
2. The upstream vendors triage and patch the vulnerability.
3. There could be one or more downstream vendors that also need to patch the vulnerability. In some cases, the coordination center may also interact with downstream vendors in the notification.
4. Security vendors (such as antivirus/antimalware, intrusion detection, and prevention technology providers) may obtain information about the vulnerability and create signatures or any other capabilities to help the end user detect and mitigate an attack caused by the vulnerability.
5. The end user is notified of the patch and the vulnerability.

TIP The preceding process can take days, weeks, months, or even years! Although this process looks very simple in an illustration like the one in Figure 7-3, it is very complicated in practice. For this reason, the Forum of Incident Response and Security Teams (FIRST) has created a Multi-Party Coordination and Disclosure special interest group (SIG) to help address these challenges. You can obtain details about guidelines and practices for multiparty vulnerability coordination and disclosure at <https://www.first.org/global/sigs/vulnerability-coordination/multiparty/>.

Vulnerability Scans

Vulnerability management teams often use other tools such as vulnerability scanners and software composition analysis (SCA) tools. Figure 7-4 illustrates how a typical automated vulnerability scanner works.

The following are the steps illustrated in Figure 7-4. Keep in mind that vulnerability scanners are all different, but most follow a process like this:

1. In the discovery phase, the scanner uses a tool such as Nmap to perform host and port enumeration. Using the results of the host and port enumeration, the scanner begins to probe open ports for more information.
2. When the scanner has enough information about the open port to determine what software and version are running on that port, it records that information in a database for further analysis. The scanner can use various methods to make this determination, including banner information.

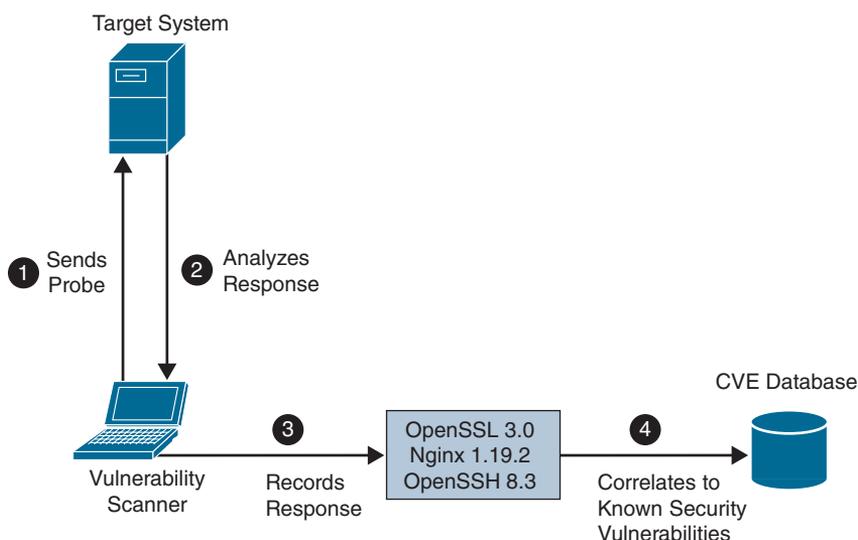


FIGURE 7-4 Coordinated Vulnerability Disclosures

3. The scanner tries to determine if the software that is listening on the target system is susceptible to any known vulnerabilities. It does this by correlating a database of known vulnerabilities against the information recorded in the database about the target services.
4. The scanner produces a report on what it suspects could be vulnerable. Keep in mind that these results are often false positives and need to be validated.

Key Topic

One of the main challenges with automated vulnerability scanners is the number of false positives and false negatives. **False positive** is a broad term that describes a situation in which a security device triggers an alarm, but no malicious activity or actual attack is taking place. In other words, false positives are false alarms, and they are also called benign triggers. False positives are problematic because by triggering unjustified alerts, they diminish the value and urgency of real alerts. Having too many false positives to investigate becomes an operational nightmare, and you most definitely will overlook real security events.

There are also **false negatives**, which is the term used to describe a network intrusion device's inability to detect true security events under certain circumstances—in other words, a malicious activity that is not detected by the security device.

A **true positive** is a successful identification of a security attack or a malicious event. A **true negative** occurs when the intrusion detection device identifies an activity as acceptable behavior and the activity is actually acceptable.

There are also different types of vulnerability scanners:

- **Application scanners:** Used to assess application-specific vulnerabilities and operate at the upper layers of the OSI model
- **Web application scanners:** Used to assess web applications and web services (such as APIs)
- **Network and port scanners:** Used to determine what TCP or UDP ports are open on the target system

Key Topic

Credentialed vs. Noncredentialed

To reduce the number of false positives, some vulnerability scanners have the capability to log in to a system to perform additional tests and see what programs, applications, and open-source software may be running on a targeted system. These scanners can also **review logs** on the target system. They can also perform **configuration reviews** to determine if a system may be configured in an unsecure way.

Key Topic

Intrusive vs. Nonintrusive

Vulnerability scanners sometimes can send numerous IP packets at a very fast pace (**intrusive**) to the target system. These IP packets can potentially cause negative effects and even crash the application or system. Some scanners can be configured in such a way that you can throttle the probes and IP packets that it sends to the target system in order to be **nonintrusive** and to not cause any negative effects in the system.

Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (or **CVSS**) is an industry standard used to convey information about the severity of vulnerabilities. In CVSS, a vulnerability is evaluated under three aspects, and a score is assigned to each of them. These three aspects (or groups) are the base, temporal, and environmental groups.

- The **base group** represents the intrinsic characteristics of a vulnerability that are constant over time and do not depend on a user-specific environment. This is the most important information and the only mandatory information to obtain for a vulnerability score.
- The **temporal group** assesses the vulnerability as it changes over time.
- The **environmental group** represents the characteristic of a vulnerability taking into account the organization's environment.

The CVSS score is obtained by taking into account the base, temporal, and environmental group information. The score for the base group is between 0 and 10, where 0 is the least severe and 10 is assigned to highly critical vulnerabilities (for example, for vulnerabilities that could allow an attacker to remotely compromise a system and get full control). Additionally, the score comes in the form of a vector string that identifies each of the components used to make up the score. The formula used to obtain the score takes into account various characteristics of the vulnerability and how the attacker is able to leverage these characteristics. CVSS defines several characteristics for the base, temporal, and environmental groups.

TIP You can read and refer to the latest CVSS specification documentation, examples of scored vulnerabilities, and a calculator at www.first.org/cvss.

The base group defines exploitability metrics that measure how the vulnerability can be exploited, and impact metrics that measure the impact on confidentiality, integrity, and availability. In addition to these two, a metric called scope change (S) is used to convey the impact on systems that are affected by the vulnerability but do not contain vulnerable code.

Exploitability metrics include the following:

- **Attack Vector (AV):** Represents the level of access an attacker needs to have to exploit a vulnerability. It can assume four values:
 - Network (N)
 - Adjacent (A)
 - Local (L)
 - Physical (P)
- **Attack Complexity (AC):** Represents the conditions beyond the attacker's control that must exist in order to exploit the vulnerability. The values can be one of the following:
 - Low (L)
 - High (H)
- **Privileges Required (PR):** Represents the level of privileges an attacker must have to exploit the vulnerability. The values are as follows:
 - None (N)
 - Low (L)
 - High (H)

- **User Interaction (UI):** Captures whether user interaction is needed to perform an attack. The values are as follows:
 - None (N)
 - Required (R)
- **Scope (S):** Captures the impact on systems other than the system being scored. The values are as follows:
 - Unchanged (U)
 - Changed (C)

The Impact metrics include the following:

- **Confidentiality Impact (C):** Measures the degree of impact to the confidentiality of the system. It can assume the following values:
 - Low (L)
 - Medium (M)
 - High (H)
- **Integrity Impact (I):** Measures the degree of impact to the integrity of the system. It can assume the following values:
 - Low (L)
 - Medium (M)
 - High (H)
- **Availability Impact (A):** Measures the degree of impact to the availability of the system. It can assume the following values:
 - Low (L)
 - Medium (M)
 - High (H)

The temporal group includes three metrics:

- **Exploit code maturity (E):** Measures whether or not public exploits are available

- **Remediation Level (RL):** Indicates whether a fix or workaround is available
- **Report Confidence (RC):** Indicates the degree of confidence in the existence of the vulnerability

The environmental group includes two main metrics:

- **Security Requirements (CR, IR, AR):** Indicate the importance of confidentiality, integrity, and availability requirements for the system
- **Modified Base Metrics (MAV, MAC, MAPR, MUI, MS, MC, MI, MA):** Allow the organization to tweak the base metrics based on specific characteristics of the environment

For example, a vulnerability that could allow a remote attacker to crash the system by sending crafted IP packets would have the following values for the base metrics:

- **Access Vector (AV)** would be Network because the attacker can be anywhere and can send packets remotely.
- **Attack Complexity (AC)** would be Low because it is trivial to generate malformed IP packets.
- **Privilege Required (PR)** would be None because no privileges are required by the attacker on the target system.
- **User Interaction (UI)** would also be None because the attacker does not need to interact with any user of the system in order to carry out the attack.
- **Scope (S)** would be Unchanged if the attack does not cause other systems to fail.
- **Confidentiality Impact (C)** would be None because the primary impact is on the availability of the system.
- **Integrity Impact (I)** would be None because the primary impact is on the availability of the system.
- **Availability Impact (A)** would be High because the device becomes completely unavailable while crashing and reloading.

CVSS also defines a mapping between a CVSS Base Score quantitative value and a qualitative score. Table 7-2 provides the qualitative-to-quantitative score mapping.

Table 7-2 Qualitative-to-Quantitative Score Mapping

Rating	CVSS Base Score
None	0.0
Low	0.1–3.9
Medium	4.0–6.9
High	7.0–8.9
Critical	9.0–10.0

TIP Organizations can use the CVSS score as input to their own risk management processes to evaluate the risk related to a vulnerability and then prioritize the vulnerability remediation.

Logs and Security Information and Event Management (SIEM)

Key Topic

Security Information and Event Management (SIEM) is a specialized device or software used for *security monitoring*; it collects, correlates, and helps security analysts analyze logs from multiple systems. SIEM typically allows for the following functions:

- **Log collection:** This includes receiving information from devices with multiple protocols and formats, storing the logs, and providing historical reporting and log filtering. A *log collector* is software that is able to receive logs from multiple sources (*data input*) and in some cases offers storage capabilities and log analysis functionality.
- **Log normalization:** This function extracts relevant attributes from logs received in different formats and stores them in a common data model or template. This allows for faster event classification and operations. Non-normalized logs are usually kept for archive, historical, and forensic purposes.
- **Log aggregation:** This function aggregates information based on common information and reduces duplicates.
- **Log correlation:** This is probably one of the most important SIEM functions. It refers to the capability of the system to associate events gathered by various systems, in different formats and at different times, and create a single actionable event for the security analyst or investigator. Often the quality of SIEM is related to the quality of its correlation engine.

- **Reporting:** Event visibility is also a key functionality of SIEM. Reporting capabilities usually include real-time monitoring and historical base reports.

Most modern SIEMs also integrate with other information systems to gather additional contextual information to feed the correlation engine. For example, they can integrate with an identity management system to get contextual information about users or with NetFlow collectors to get additional flow-based information.

NOTE NetFlow is a technology created by Cisco to collect network metadata about all the different “flows” of traffic on your network. There’s also the Internet Protocol Flow Information Export (*IPFIX*), which is a network flow standard led by the Internet Engineering Task Force (IETF). IPFIX was designed to create a common, universal standard of export for flow information from routers, switches, firewalls, and other infrastructure devices. IPFIX defines how flow information should be formatted and transferred from an exporter to a collector. IPFIX is documented in RFC 7011 through RFC 7015 and RFC 5103. Cisco NetFlow Version 9 is the basis and main point of reference for IPFIX. IPFIX changes some of the terminologies of NetFlow, but in essence they are the same principles of NetFlow Version 9.

Several commercial SIEM systems are available. Here’s a list of some commercial SIEM solutions:

- Micro Focus ArcSight
- LogRhythm
- IBM QRadar
- Splunk

Figure 7-5 shows how SIEM can collect and process logs from routers, network switches, firewalls, intrusion detection, and other security products that may be in your infrastructure. It can also collect and process logs from applications, antivirus, antimalware, and other host-based security solutions.

Security operation center analysts and security engineers often collect *packet captures* during the investigation of a security incident. Packet captures provide the greatest detail about each transaction happening in the network. Full packet capture has been used for digital forensics for many years. However, most malware and attackers use encryption to be able to bypass and obfuscate their transactions. IP packet metadata can still be used to potentially detect an attack and determine the attacker’s tactics and techniques.

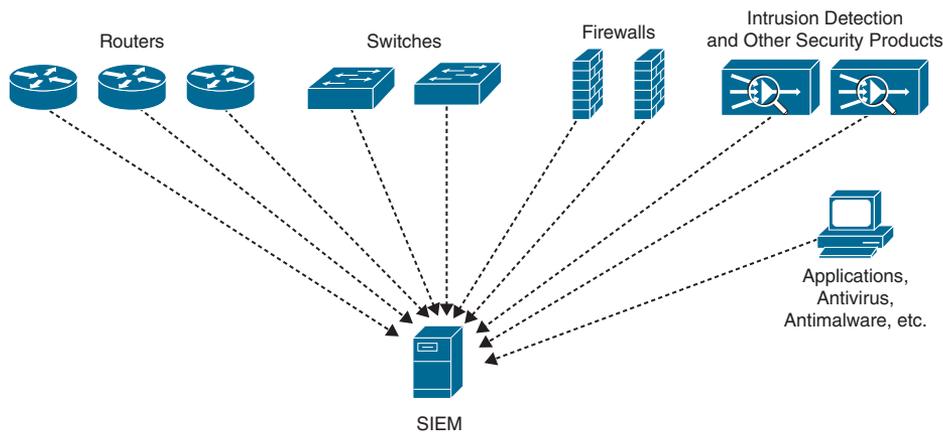


FIGURE 7-5 SIEM Collecting and Processing Logs from Disparate Systems

One of the drawbacks of collecting full packet captures in every corner of your network is the requirement for storage because packet captures in busy networks can take a significant amount of disk space. This is why numerous organizations often collect network metadata with NetFlow or IPFIX and store such data longer than when collecting packet captures.

Several sophisticated security tools also provide *user behavior analysis* mechanisms in order to potentially find insiders (internal attackers). Similarly, they provide insights of user behavior even if they do not present a security threat.

Organizations can also deploy *sentiment analysis* tools and solutions to help monitor customer sentiment and brand reputation. Often these tools can also reveal the intent and tone behind social media posts, as well as keep track of positive or negative opinions. Threat actors can also try to damage a company's reputation by creating fake accounts and bots in social media platforms like Twitter, Facebook, or Instagram. Attackers can use these fake accounts and bots to provide negative public comments against the targeted organization.

Security Orchestration, Automation, and Response (SOAR)

Key Topic

CSIRT analysts typically work in an SOC utilizing many tools to monitor events from numerous systems (firewalls, applications, IPS, DLP, endpoint security solutions, and so on). Typically, these logs are aggregated in a SIEM. Modern SOCs also use *Security Orchestration, Automation, and Response (SOAR)* systems that extend beyond traditional SIEMs.

The tools in the SOC are evolving and so are the methodologies. For example, now security analysts not only respond to basic cyber events but also perform threat hunting in their organizations. SOAR is a set of solutions and integrations designed to allow organizations to collect security threat data and alerts from multiple sources. SOAR platforms take the response capabilities of SIEM to the next level. SOAR solutions supplement, rather than replace, the SIEM. They allow the cybersecurity team to extend its reach by automating the routine work of cybersecurity operations.

TIP Unlike traditional SIEM platforms, SOAR solutions can also be used for threat and vulnerability management, security incident response, and security operations automation.

Deploying SOAR and SIEM together in solutions makes the life of SOC analysts easier. SOAR platforms accelerate incident response detection and eradication times because they can automatically communicate information collected by SIEM with other security tools. Several traditional SIEM vendors are changing their products to offer hybrid SOAR/SIEM functionality.

Another term adopted in the cybersecurity industry is Extended Detection and Response (XDR). XDR is a series of systems working together that collects and correlates data across hosts, mobile devices, servers, cloud workloads, email messages, web content, and networks, enabling visibility and context into advanced threats. The goal of an XDR system is to allow security analysts to analyze, prioritize, hunt, and remediate cybersecurity threats to prevent data loss and security breaches.

Chapter Review Activities

Use the features in this section to study and review the topics in this chapter.

Review Key Topics

Review the most important topics in the chapter, noted with the Key Topic icon in the outer margin of the page. Table 7-3 lists a reference of these key topics and the page number on which each is found.

**Key
Topic****Table 7-3** Key Topics for Chapter 7

Key Topic Element	Description	Page Number
Paragraph	Defining threat hunting	175
Paragraph	Understanding security advisories, bulletins, and what a CVE is	177
Paragraph	Understanding false positives and false negatives	181
Section	Credentialed vs. Noncredentialed	182
Section	Intrusive vs. Nonintrusive	182
Paragraph	Defining what SIEM is	186
Paragraph	Understanding the SOAR concept	188

Define Key Terms

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

threat hunting, threat feeds, intelligence fusion, security advisories, Common Vulnerability and Exposures (CVE), false positives, false negatives, true positive, true negative, application scanners, web application scanners, network and port scanners, review logs, configuration reviews, intrusive, nonintrusive, CVSS, base group, temporal group, environmental group, Security Information and Event Management (SIEM), security monitoring, log collector, data input, Log aggregation, IPFIX, packet captures, user behavior analysis, sentiment analysis, Security Orchestration, Automation, and Response (SOAR)

Review Questions

Answer the following review questions. Check your answers with the answer key in Appendix A.

1. What type of vulnerability scanner can be used to assess vulnerable web services?
2. What documents do vendors, vulnerability coordination centers, and security researchers publish to disclose security vulnerabilities?
3. What term is used to describe an organization that can assign CVEs to vulnerabilities?

4. What public database can anyone use to obtain information about security vulnerabilities affecting software and hardware products?
5. How many score “groups” are supported in CVSS?
6. A vulnerability with a CVSS score of 4.9 is considered a _____ severity vulnerability.
7. What is the process of iteratively looking for threats that may have bypassed your security controls?

Index

Symbols

../ (dot-dot-slash) attack 76, 274–275
; (semicolon) 73
' (single quotation mark) 73
_ (underscore) 740
0phtCrack 44
2FA (two-factor authentication) 298
5G communications 357–358
802.1X standard 510, 553–556, 562,
664–667, 673

A

A record (Address mapping record) 796
AAA (authentication, authorization, and
accounting) framework 306
AAR (after action report) 928–929
ABAC (attribute-based access control)
638–645, 678, 679
acceptable use policies (AUPs) 898, 900
acceptance of risk 919
access control. *See also* 802.1X standard;
identity; passwords
access control entries (ACEs) 643
access control lists (ACLs) 490, 528,
535, 643, 831
attribute-based 638–645, 678, 679
best practices 680–681
centralized versus decentralized 679
centralized/decentralized 640
conditional access 678, 679
delegation of access 662
discretionary 674–676, 679

identity and access management
(IAM) 605, 633
implicit deny 680
least privilege 264, 630, 681, 908
mandatory 676, 679
network 510–511
permissions 640–645
cloud computing 605, 610
inheritance 644–646
open 150
types of 646
privileged access management (PAM)
678, 679
role-based 677, 679
rule-based 677, 678, 679
summary of 679
user access recertification 645
vestibules 372–373
access control entries (ACEs) 643
access control lists (ACLs) 490, 528,
535, 643, 831
access points (APs)
rogue 99
security 562–563
accounting, AAA framework for 306
accounts 629–633. *See also* access
control; passwords
administrator 908
auditing 635, 639
harvesting 18
permissions 640–645
cloud computing 605, 610
inheritance 644–646

- open 150
 - types of 646
- policies 633
- root 908
- service 908
- ACEs (access control entries) 643
- ACI (Application Centric Infrastructure) 243
- acknowledgement (ACK) packets 84
- ACLs (access control lists) 490, 528, 535, 643, 831
- acquisition, forensic
 - artifacts 853
 - cache 852
 - checksums 857
 - data breach notification laws 855–856
 - definition of 847
 - device 850–851
 - disk 848
 - firmware 851
 - hashing 856–857
 - integrity 856
 - network 852–853
 - operating system 850
 - order of volatility 848
 - on-premises versus cloud 853–854
 - random-access memory (RAM) 848–849
 - regulatory and jurisdictional 855
 - right-to-audit clauses 854
 - snapshot 851–852
 - swap/pagefile 849–850
- Active Directory (AD) 291–292
 - Active Directory Certificate Services (AD CS) utility 691
 - Active Directory Users and Computers (ADUC) 640
- active reconnaissance 18, 204–205
- active/active load balancing 488
- active/passive load balancing 488
- Activity Monitor 542
- actors, threat
 - attack vectors 122–123
 - attributes of 122
 - types of 120–121
- AD. *See* Active Directory (AD)
- additional or associated data (AEAD) 404
- Address mapping record (A record) 796
- Address Resolution Protocol. *See* ARP (Address Resolution Protocol)
- address space layout randomization (ASLR) 76, 265, 272
- addresses
 - IPv4 443–444
 - IPv6 536–537
 - MAC (media access control) 101, 511
 - network address allocation 443–444
 - network address translation 501, 529, 562
 - virtual IP 488
- administrator accounts 908
- admissibility, evidence 843
- ADSP (Author Domain Signing Practices) 110
- ADUC (Active Directory Users and Computers) 640
- Advanced Encryption Standard (AES). *See* AES (Advanced Encryption Standard)
- Advanced IP scanner 721
- advanced persistent threats (APTs) 35, 120–121, 451, 770
- AE (authenticated encryption) 404
- AEAD (additional or associated data) 404
- aerospace application-embedded systems 348–350
- AES (Advanced Encryption Standard) 412, 430, 475, 552
 - AES-GCM 498
 - AES-GMAC 498
- AFL (American Fuzzy Lop) 269
- after action report (AAR) 928–929
- aggregation, log 186
- aggregators 526

- Agile development methodology 258–259
- agreement, terms of 948
- AH (Authentication Header) 437, 520
- AI (artificial intelligence) 50–51
- AI (Asset Identification) 885, 941–942
- AICPA (American Institute of Certified Public Accountants) 883
- AI/ML (artificial intelligence and machine learning) 50–51
- AIR (As-if Infinitely Ranged) integer model 77
- air gaps 384, 385
- air traffic control (ATC) 349–350
- aircraft systems 348–350
- AirMagnet 99
- AIS (automated indicator sharing) 125
- aisles, hot/cold 386
- alarms 374, 870
- ALE (annualized loss expectancy) 922
- alerts, SIEM 788
- ALG (application-level gateway) 529
- algorithms 50–51
 - Grover's 402
 - hashing 218–219, 856–857
 - Digital Signature Algorithm (DSA) 396, 412
 - Elliptic Curve Digital Signature Algorithm (ECDSA) 551–552
 - Message Digest Algorithm 5 (MD5) 55, 219
 - Secure Hash Algorithm (SHA) 55, 551–552
 - key generation 395
 - message authentication code (MAC) 410
 - online resources 498
 - public key 411
 - scheduling 488
 - Shor's 402
 - signature verifying 395
 - signing 395
- allocation, network address 443–444
- allow lists 467, 578, 583, 822
- ALTER DATABASE statement 71
- ALTER TABLE statement 71
- Alureon rootkit 35–36
- always-on VPN functionality 495
- Amazon Web Services (AWS) 232–233, 244, 603, 853, 870
- American Fuzzy Lop (AFL) 269
- American Institute of Certified Public Accountants (AICPA) 883
- amplification attacks 112
- analytics logs 383
- Android Auto 347
- Angry IP scanner 721
- annualized loss expectancy (ALE) 922
- annualized rate of occurrence (ARO) 922
- anomaly-based analysis 521–523
- anonymization 945
- anti-forensics 770
- antimalware 452
- antivirus software 451
- anycast addresses 537
- anything as a service (XaaS) 139, 232
- AP isolation 562
- Apache
 - HTTP Server 146
 - Mesos 240
 - web servers 794
- APIs (application programming interfaces) 86
 - API-based keyloggers 42
 - attacks 55, 85–86, 602
 - definition of 240–241
 - infrastructure as code 241–243
 - inspection and integration 607, 610
 - micro-segmentation 240–241
 - security considerations 216
 - Shodan 203–204
- APP (Australia Privacy Principles) 220
- Apple
 - Apple Pay 462, 584
 - CarPlay 347
 - macOS Activity Monitor 542

- appliances, network 513–514. *See also*
 - firewalls
 - aggregators 526
 - hardware security modules (HSMs) 524
 - jump servers 514
 - network intrusion detection systems (NIDSs) 517–518
 - advantages/disadvantages 519–520
 - anomaly-based analysis 521–523
 - definition of 519–520
 - heuristic-based analysis 521
 - inline versus passive 523–524
 - promiscuous mode 517
 - signature-based 520–521
 - stateful pattern-matching recognition 521
 - network intrusion prevention systems (NIPSs)
 - advantages/disadvantages 519–520
 - anomaly-based analysis 521–523
 - definition of 518–520
 - false positives/false negatives 519
 - heuristic-based analysis 521
 - inline versus passive 523–524
 - signature-based 520–521
 - proxy servers 514–516
 - sensors 524–525
- application allow lists. *See* allow lists
- application block/deny lists. *See* block/deny lists
- Application Centric Infrastructure (ACI) 243
- application development. *See also*
 - application security
 - application provisioning and deprovisioning 260
 - automation and scripting 278–279
 - diversity 278
 - elasticity 279–280
 - integrity measurement 261
 - Open Web Application Security Project (OWASP) 204, 276–277
 - programming testing methods
 - compile-time errors 266–267
 - fuzz testing 269–270
 - input validation 80, 267–268
 - penetration testing 266
 - runtime errors 266–267
 - static and dynamic code analysis 269
 - stress testing 80, 266
 - scalability 279–280
 - secure coding 261–263
 - software development environments 257–260
 - software development lifecycle (SDLC) 78, 261–262, 263–265, 468, 868
 - vulnerabilities and attacks 74–75
 - API attacks 55, 85–86, 602
 - backdoors 149, 271, 275
 - buffer overflows 75–76, 77, 149, 271–272, 275
 - code injection 149, 273–274, 276
 - cross-site request forgery (XSRF) 149, 272, 275
 - cross-site scripting (XSS) 54, 68–70, 110, 149, 272, 275, 601
 - directory traversal 75–76, 149, 274–275, 276
 - DLL injection 74
 - driver manipulation 89
 - error handling 79–82
 - LDAP injection 74
 - memory/buffer 77–78, 88, 149, 271–272, 275
 - pass the hash 89–90
 - pointer dereferencing 75–76
 - privilege escalation 67–68, 201, 770
 - race conditions 79
 - remote code execution (RCE) 78, 146, 149, 275
 - replay 82–85
 - request forgeries 85–86
 - resource exhaustion 87–88

- SQL injection (SQLi) 54, 70–74, 273–274
- SSL stripping 88–89
- summary of 275–276
- XML injection 74–75
- zero-day attack 149, 275, 276
- application logs 792–793
- application management, mobile 576–578
- application programming interfaces. *See* APIs (application programming interfaces)
- application scanners 182
- application security 463–464, 475–476, 612. *See also* application development
 - allow lists 467, 578, 583, 822
 - application shielding 471
 - authentication 298
 - block/deny lists 467–468, 822–823
 - code signing 466–467
 - disk encryption 473
 - dynamic code analysis 470–471
 - fuzzing 471
 - hardening 471
 - hardware root of trust 476–477
 - Hypertext Transfer Protocol (HTTP) 436–437, 465–466, 577
 - input validation 464
 - manual code review 470
 - mobile devices 581
 - open ports/services 471–472
 - operating system 473–474
 - patch management 474–475
 - registry 472
 - sandboxing 452, 478–479
 - secure coding practices 468
 - secure cookies 465
 - self-encrypting drives (SEDs) 475–476
 - static code analysis 468–469
 - Trusted Platform Module (TPM) 477–478
 - whitelisting 578, 583
- application service providers (ASPs) 139, 231
- application-aware devices 518
- application-based segmentation 489–490
- application-level gateways (ALGs) 529
- approved lists 822
- AppScan 204
- APs (access points)
 - rogue 99
 - security 562–563
- APT29 (Cozy Bear) 346
- apt-get install snmp snmpwalk command 436
- APTs (advanced persistent threats) 120–121, 451, 770
- archive.org 147
- Arduino 340
- ARF (Asset Reporting Format) 885
- ARO (annualized rate of occurrence) 922
- ARP (Address Resolution Protocol)
 - poisoning 105, 722
 - spoofing 513
- arp command 721–722
- artifacts, forensic 853
- artificial intelligence and machine learning (AI/ML) 50–51, 788
- As-if Infinitely Ranged (AIR) integer model 77
- ASLR (address space layout randomization) 76, 265, 272
- ASPs (application service providers) 139, 231
- assertion parties (SAML) 659
- assertions 623
- assessments, security. *See* security assessments
- Asset Identification (AI) 885, 941–942
- asset management 909–910
- Asset Reporting Format (ARF) 885
- asset values 921, 922
- asymmetric encryption 411–413
- ATC (air traffic control) 349–350

- ATT&CK framework (MITRE) 18, 128–129, 176, 205, 223, 767–768
- Attack Complexity (AC) metric 183
- Attack Vector (AV) metric 183
- attestation 294, 460–461
- attribute-based access control (ABAC) 638–645, 678, 679
- audio steganography 415–416
- auditing 635, 639
 - audit logs 869–870
 - audit trails 870
 - cloud computing 604, 609
- auditors 947
- AUPs (acceptable use policies) 898, 900
- Australia Privacy Principles (APP) 220
- 802.1X standard 510, 553–556, 562, 664–667, 673
- AAA framework 304–306
- attestation 294
- authenticated encryption (AE) 404
- authenticated modes 404
- authentication applications 298
- biometric systems 300, 378, 625–626, 869
 - crossover error rate (CER) 304
 - efficacy of 302
 - errors with 626
 - false acceptance rate (FAR) 303, 626
 - false rejection rate (FRR) 303, 626
 - fingerprints 300–301
 - gait analysis 302
 - iris recognition 301
 - retina scanning 301
 - vein authentication 302
 - voice/speech recognition 302
- captive portals 559
- Challenge-Handshake Authentication Protocol 673
- challenge-response authentication (CRA) 571–572
 - by characteristic attributes 625–626
- CIA (confidentiality, integrity, availability) 289
- cloud versus on-premises requirements 306–307
- context-aware authentication 658
- definition of 289–291, 625
- directory services 291–292
- embedded systems 363
- Extensible Authentication Protocol (EAP) 553–556, 664–667
 - EAP-FAST 556, 666
 - EAP-MD5 556, 666
 - EAP-TLS 556, 666
 - EAP-TTLS 556, 666
 - LEAP 666
 - PEAP 556, 666
- federation 292–293, 556–557, 658
- hardware security modules (HSMs) 656
- HMAC-based one-time password (HOTP) 295–296
- Kerberos 82–83, 89, 292, 553, 668–670, 673
 - by knowledge 625, 656–657
- Lightweight Directory Access Protocol (LDAP) 291, 442, 667–670
 - injection attacks 74, 144
 - Lightweight Directory Access Protocol over SSL (LDAPS) 432
- logs 789–796
- multifactor 304–306, 657
- mutual 668–670
- OAuth 661–662
- OpenID and OpenID Connect 663–664
 - by ownership 625
 - phone call 299–300
 - push notifications 299
- remote
 - Challenge-Handshake Authentication Protocol (CHAP) 670–672, 673

- RADIUS 556–557, 672–673
 - Remote Access Service (RAS) 670–672
 - TACACS+ 672–673
 - Security Assertion Markup Language (SAML) 659–661
 - Short Message Service (SMS) 296–297
 - single sign-on (SSO) 292, 373, 624, 658–659
 - smart card 299–300, 629
 - static codes 298
 - summary of 673
 - time-based one-time password (TOTP) 295
 - token key 297
 - Trusted Platform Module (TPM) 294, 655
 - two-factor 298
 - Wi-Fi Protected Setup (WPS) 558–559
 - authentication attacks 55, 602
 - Authentication Header (AH) 437, 520
 - authentication servers 555, 665
 - authenticators 555, 665
 - Author Domain Signing Practices (ADSP) 110
 - authorization 290, 306
 - authorized hackers 121
 - Auto (Android) 347
 - automated indicator sharing (AIS) 125
 - automation
 - application development 278–279
 - auto-updates 474–475
 - facility 345
 - autonomous underwater vehicles (AUVs) 353–354
 - Autopsy 747, 850
 - AUVs (autonomous underwater vehicles) 353–354
 - availability 289
 - resource exhaustion 87–88
 - restoration order 330–331
 - site resiliency and 221–222
 - Availability Impact (I) metric 184
 - avalanche effect 463
 - avoidance, risk 918
 - awareness, risk 921
 - AWS (Amazon Web Services) 244, 603, 853
 - Azure 232–233, 603, 853
- B**
- backdoors 42–43, 149, 271, 275
 - background checks 899
 - backups 158
 - cloud 326
 - comparison of 326–327
 - copy 326
 - differential 326, 328
 - disk 326
 - full 326, 328–331
 - image 326
 - incremental 326, 328
 - NAS (network-attached storage) 326
 - offsite 327
 - online versus offline 326
 - snapshot 326
 - tape 326
 - badges 373, 382
 - baiting 19
 - balancers, load 319–320
 - bandwidth monitors 804
 - barricades 370–371
 - base groups 182
 - baseband radio 359
 - baselining 213, 539–542
 - Bash 113
 - Basic Encoding Rules (BER) 697
 - basic input/output system (BIOS) 851
 - BCDR (business continuity and disaster recovery) 139, 232
 - BCPs (business continuity plans) 773–774, 929
 - beamforming 560
 - Bell-LaPadula 677

- benchmarks 885–888
- BER (Basic Encoding Rules) 697
- BGP (Border Gateway Protocol)
 - hijacking 535–536
- BIA (business impact analysis) 773, 926–927
- Biba 677
- binaries 278
- binary planting 74
- biometric systems 300, 378, 625–626, 869
 - crossover error rate (CER) 304
 - efficacy of 302
 - errors with 626
 - false acceptance rate (FAR) 303, 626
 - false rejection rate (FRR) 303, 626
 - fingerprints 300–301
 - gait analysis 302
 - iris recognition 301
 - retina scanning 301
 - vein authentication 302
 - voice/speech recognition 302
- BIOS (basic input/output system) 851
- birthday attacks 56
- BiSL (Business Information Services Library) 882
- Bitcoin-related SMS scams 12
- BitTorrent 529
- black hat hackers 121
- black-box testing 80
- blackhole DNS servers 223
- Blackhole exploit kit 44, 111–112
- blacklisting 578, 583
- blanket purchase agreements (BPAs) 903
- blind hijacking 84
- blind SQL injection 73
- block all. *See* implicit deny
- block ciphers 411
- blockchain 409–410
- block/deny lists 467–468, 578, 583, 822–823
- blocking 417
- Blowfish 412
- blue teams 205, 902
- Bluetooth 570–571
 - bluejacking 100, 570–571
 - bluesnarfing 99–100, 570–571
- bollards 370–371
- Boolean technique 74
- boot integrity
 - boot attestation 460–461
 - definition of 458–459
 - measured boot 459–460
 - Unified Extensible Firmware Interface (UEFI) 459
- Border Gateway Protocol (BGP)
 - hijacking 535–536
- bots and botnets 37–38, 111–112, 580
- BPAs. *See* blanket purchase agreements (BPAs); business partnership agreements (BPAs)
- BPDU (Bridge Protocol Data Unit)
 - guard 512
- bring-your-own-device (BYOD) 215, 572, 574–576, 581, 588–590, 826, 898
- broadcast storm prevention 512
 - BPDU guard 512
 - DHCP snooping 512–513
 - loop protection 512
 - MAC filtering 513
- brute-force attacks 45, 749
- buckets 605
- buffer overflows 75–76, 77, 149, 271–272, 275, 522
- bug bounties 202–203
- BugCrowd 203
- building loss 925
- burning 386
- Burp Suite Professional 204
- buses, controller area network (CAN) 347–348
- business continuity and disaster recovery (BCDR) 139, 232
- business continuity plans (BCPs) 773–774, 929

- business impact analysis (BIA) 773, 926–927
 - business partnership agreements (BPAs) 903
 - BYOD. *See* bring-your-own-device (BYOD)
- C**
- cables
 - locks 379
 - malicious USB 48
 - CAC (Common Access Card) 629
 - cache
 - ARP cache poisoning 105
 - caching proxy 514
 - DNS cache poisoning 108–110
 - forensic acquisition 852
 - Cain and Abel 44
 - California Consumer Privacy Act (CCPA) 214, 220, 880
 - call management systems (CMSs) 351
 - Call Manager log files 799–800
 - CAM (content addressable memory) 106
 - cameras
 - centralized versus decentralized 375
 - closed-circuit television (CCTV) 376–377, 870
 - motion recognition 376
 - object detection 376
 - camouflage 265, 377
 - CAN (controller area network) bus 347–348
 - Canada, Personal Information Protection and Electronic Data Act (PIPEDA) 220
 - Canonical Encoding Rules (CER) 697
 - capital expenditure (CapEx) 598
 - captive portals 559
 - capture, packet. *See* packet capture and replay
 - capture the flag 902
 - card cloning attacks 48–49
 - CarPlay, Apple 347
 - carrier unlocking 584
 - CAs (certificate authorities) 466, 556, 689–691, 829
 - CASBs (cloud access security brokers) 142–143, 611–612, 614
 - cat command 734–735
 - CBC (Cipher Block Chaining) mode 405
 - CBT (computer-based training) 901
 - CBWFQ (class-based weighted fair queuing) 536
 - CCE (Common Configuration Enumeration) 886
 - CCleaner 51
 - CCPA (California Consumer Privacy Act) 214, 220, 880
 - CCSS (Common Configuration Scoring System) 886
 - CCTV (closed-circuit television) 376–377, 870
 - CD (continuous delivery) 279
 - CDP (clean desk policy) 23, 899, 900
 - Cellebrite 850–851
 - cellular connection methods and receivers 572–573
 - Center for Internet Security (CIS) 164, 881, 883
 - centralized access control 640, 679
 - centralized cameras 375
 - centralized controllers 242
 - CER (Canonical Encoding Rules) 697
 - CER (crossover error rate) 304, 626
 - .cer file extension 697
 - CERT (Community Emergency Response Team) 77
 - certificate authorities (CAs) 466, 556, 689–691, 829
 - certificate revocation lists (CRLs) 533, 689–690, 691, 829
 - certificate signing requests (CSRs) 689

- certificates 625, 626–627
 - attributes 691–692
 - chaining 696
 - expiration 693
 - formats 697
 - pinning 698
 - Subject Alternative Name 693
 - types of 694–696
 - updating/revoking 829–830
- CFB (Cipher Feedback) mode 406
- chain of custody 789, 844
- chain of trust 699
- Challenge-Handshake Authentication Protocol (CHAP) 673
- challenge-response authentication (CRA) 49–50, 102, 571–572
- change management 909
- CHAP (Challenge-Handshake Authentication Protocol) 82–83, 670–672, 673
- characteristic attributes, authentication by 625–626
- Check Point 518
- checksums 857, 870
- chief information officers (CIOs) 903
- chief security officers (CSOs) 930
- chkdsk command 157
- chmod command 644–645, 736–737
- choose-your-own-device (CYOD) 588–590
- CI (continuous integration) 279
- CIA (confidentiality, integrity, availability) 221, 263, 289
- CIDR (classless interdomain routing) netblock 203–204
- CIOs (chief information officers) 903
- Cipher Block Chaining (CBC) mode 405
- Cipher Feedback (CFB) mode 406
- cipher suites 409–411
- CIRT. *See* incident response (IR) teams
- CIS (Center for Internet Security) 164, 881, 883
- CISA (Cybersecurity and Infrastructure Security Agency) 353–354
- Cisco
 - Application Centric Infrastructure (ACI) 243
 - Application Policy Infrastructure Controller (APIC) 243
 - Cisco Discovery Protocol (CDP) 107
 - Email Security Appliance (ESA) 111
 - Identity Services Engine (ISE) 590
 - Mutiny Fuzzing Framework 269
 - NetFlow 187, 525, 809–810
 - OpenDNS 509–510
 - security advisories and bulletins 179
 - Talos 347
 - Umbrella 509
- Clark-Wilson 677
- class-based weighted fair queuing (CBWFQ) 536
- classification
 - asset 941–942
 - data 904–905
- classless interdomain routing (CIDR) netblock 203–204
- clean desk policy (CDP) 23, 899, 900
- clean pipe 112
- clickjacking 84
- client-based VPNs (virtual private networks) 497
- clientless VPNs (virtual private networks) 497, 507–508
- clientless web access 507
- clients, thin 235–236, 508
- client-side execution 267
- client-side validation 268
- clock, secure 477
- cloning
 - MAC (media access control) 106
 - SIM (subscriber identity module) cards 580, 584
- closed-circuit television (CCTV) 376–377, 870

- cloud access security brokers (CASBs)
 - 142–143, 611–612, 614
- cloud computing
 - advantages of 138
 - attacks and vulnerabilities 52–55, 123, 137–143, 601–603
 - authentication 306–307
 - backups 326
 - cloud access security brokers (CASBs)
 - 142–143, 611–612, 614
 - cloud service providers (CSPs) 139, 233, 598, 853–854
 - community cloud 140, 233
 - definition of 138
 - fog and edge computing 234–235
 - forensic acquisition 853–854
 - hybrid cloud 140, 233
 - managed detection and response (MDR) 234
 - managed service providers (MSPs) 233–234
 - models 231–232
 - off-premises versus on-premises services 234
 - private cloud 140, 232–233
 - public cloud 140, 232
 - resilience 325
 - security assessments 598
 - attacks 601–603
 - threats 598–600
 - security controls 595, 598
 - API inspection and integration 607, 610
 - compute 607, 611
 - container security 608–609
 - dynamic resource allocation 607–608, 611
 - high availability across zones 603, 609
 - instance awareness 608, 611
 - integration and auditing 604, 609
 - native versus third-party 615
 - network 606–607, 610
 - resource policies 603, 609
 - secrets management 604, 609
 - security groups 607, 611
 - storage 605, 610
 - summary of 608–609
 - virtual private cloud endpoint 608, 611
 - security solutions
 - application security 612
 - cloud access security brokers (CASBs) 611–612, 614
 - firewalls 613–614, 615
 - Secure Web Gateway (SWG) 613, 614
 - summary of 614–615
 - storage
 - encryption 605
 - high availability 606
 - permissions 605
 - replication 605
 - thin clients 235–236
 - VPCs (virtual private clouds) 607, 608, 611
- Cloud Controls Matrix 884
- Cloud Security Alliance (CSA) 139, 603, 884
- Cloud Service (Google) 603
- cloud service providers (CSPs) 139, 233, 598, 853–854
- Cloudflare 440
- cloudlets 235
- Cluster Server 488
- CMSs (call management systems) 351
- CMSS (Common Misuse Scoring System) 887
- COBIT framework 882
- code, infrastructure as 241–243
- code security 261–263
 - code camouflage 265
 - code checking 79, 265
 - code injection 149, 273–274, 276

- code reuse 179, 270
- code signing 466–467, 695, 696
- dynamic code analysis 470–471
- manual code review 470
- static code analysis 468–469
- cold aisles 386
- cold sites 222
- collection, log 186
- collisions 55–56, 463
- command-and-control (C2) servers
 - 37–38, 107
- commands. *See individual commands*
- comment delimiters 73
- Common Access Card (CAC) 629
- Common Configuration Enumeration (CCE) 886
- Common Configuration Scoring System (CCSS) 886
- Common Misuse Scoring System (CMSS) 887
- common names (CNs) 692
- Common Object Request Broker Architecture (CORBA) 86
- Common Platform Enumeration (CPE) 886
- Common Remediation Enumeration (CRE) 886
- Common Security Advisory Framework (CSAF) 164
- Common Vulnerabilities and Exposures (CVEs), Wi-Fi 78, 125, 146, 177, 571, 886
- Common Vulnerability Reporting Framework (CVRF) 164
- Common Vulnerability Scoring System (CVSS) 182–186, 886
- Common Weakness Enumeration (CWE) 75, 886
- Common Weakness Scoring System (CWSS) 887
- communications
 - communication plans 771–772
 - embedded systems
 - 5G 357–358
 - baseband radio 359
 - NarrowBand 358
 - subscriber identity module (SIM)
 - cards 360
 - Zigbee 360–361
 - community cloud 140, 233
 - Community Emergency Response Team (CERT) 77
 - community ports 491
 - company policies 878–879
 - compensating controls 871, 872
 - compilers 278
 - compile-time errors 81–82, 266–267
 - compliance, software 918
 - computer certificates 696
 - computer incident response teams. *See incident response (IR) teams*
 - computer-based training (CBT) 901
 - Concealment 415
 - concentrators, VPN 495
 - conditional access 678, 679
 - confidence tricks 19
 - Confidential information 905, 941–942
 - Confidentiality Impact (C) metric 184
 - configuration management 164, 213
 - configuration reviews 182
 - mitigation techniques 824
 - certificates, updating/revoking 829–830
 - content filter/URL filter 828–829
 - data loss prevention (DLP) 825–826
 - firewall rules 825
 - mobile device management (MDM) 825–826
 - secure configuration guides 885–888
 - weak configurations 150–155

- connection methods and receivers
 - Bluetooth 570–571
 - cellular 572–573
 - Global Positioning System (GPS) 572, 584
 - near-field communication (NFC) 570–571
 - Radio frequency identification (RFID) 571–572
 - satellite communications (SATCOM) 573
 - secure implementation best practices 573–574
- containers 236–240, 608–609
- containment, incident response (IR) 763–764, 830–831
- content addressable memory (CAM) 106
- content filters 533, 828–829
- content management 576–578
- context-aware authentication 658
- continuity of operations plans (COOPs) 774–775, 929
- continuous delivery (CD) 279
- continuous deployment 279
- continuous integration (CI) 279
- continuous monitoring 139, 278
- continuous validation 278
- Control Objectives for Information and Related Technology (COBIT) 882
- control systems, diversity in 332
- controller area network (CAN) bus 347–348
- controller-pilot data link communications (CPDLC) 349–350
- controllers 562–563, 946
- controls. *See also* physical security
 - compensating 871, 872
 - corrective 870, 872
 - detective 869–870, 872
 - deterrent 870–871, 872
 - managerial 868
 - operational 868, 869
 - physical 871–872
 - preventative 869, 872
 - technical 868, 869
- convert command 156
- cookie hijacking 465
- cookies 465
- cookies, secure 465
- COOPs (continuity of operations plans) 774–775, 929
- Coordinated Universal Time (UTC) 440, 845
- COPE (corporate-owned, personally enabled) environments 572, 588
- copy backups 326
- CORBA (Common Object Request Broker Architecture) 86
- corporate incidents 775
- corporate-owned, personally enabled (COPE) environments 572, 588–590
- corrective controls 870, 872
- correlation, log 186
- correlation, Security Information and Event Management (SIEM) 788–789
- Counter (CTR) mode 404, 408–409
- counterintelligence 860
- Counter-mode/CBC-MAC protocol (CCMP) 552
- counters, secure 477
- county names, certificate 692
- cover-files 416
- Cozy Bear 346
- CPE (Common Platform Enumeration) 886
- CRA (challenge-response authentication) 49–50, 102, 571–572
- cracking passwords 46

- CRE (Common Remediation Enumeration) 886
- CREATE DATABASE statement 70
- CREATE INDEX statement 71
- CREATE TABLE statement 71
- credentials
 - credentialed vulnerability scans 182, 349–350
 - harvesting 18
 - policies 906–908
- crimeware 44
- criminal syndicates 120
- Critical information 942
- critical systems, identification of 929
- CRLs (certificate revocation lists) 533, 689–690, 691, 829
- crossover error rate (CER) 304, 626
- cross-site request forgery (XSRF) 85–86, 149, 272, 275, 602
- cross-site scripting (XSS) 54, 68–70, 110, 149, 272, 275, 464, 601
- .crt file extension 697
- cryptography 396. *See also* encryption; hashing; secure protocols
 - algorithms 498
 - blockchain 409–410
 - cipher suites 409–411
 - common use cases 417–418
 - cryptographic attacks
 - birthday 56
 - collision 55–56
 - cryptographic protocols 551
 - Advanced Encryption Standard (AES) 552
 - Counter-mode/CBC-MAC protocol (CCMP) 552
 - Simultaneous Authentication of Equals (SAE) 551, 552
 - summary of 552
 - Wi-Fi Protected Access 2 (WPA2) 551
 - Wi-Fi Protected Access 3 (WPA3) 551–552
 - definition of 391
 - digital signatures 395–396, 520
 - diversity in 331
 - elliptic-curve cryptography (ECC) 399–400
 - encryption 159, 362
 - cloud computing 605, 610
 - data at rest 218
 - data in transit/motion 218
 - data in use/processing 218
 - disk 473
 - entropy 419
 - homomorphic 417
 - international mobile subscriber identity (IMSI) 49, 358, 584
 - mobile device management (MDM) 578–580
 - symmetric/asymmetric 411–413
 - vulnerabilities 150–151
 - entropy 419
 - keys
 - ephemeral 403
 - key exchanges 399
 - key signing keys (KSKs) 427
 - length of 396
 - password 655
 - personal unblocking keys (PUKs) 360
 - public/private 436–437
 - Secure Shell (SSH) 625, 628
 - stretching 397
 - zone signing keys (ZSKs) 427
 - lightweight 414–415
 - limitations of 418–420
 - modes of operation 403–409
 - authenticated 404
 - Cipher Block Chaining (CBC) 405
 - Cipher Feedback (CFB) 406
 - counter 404
 - Counter (CTR) 408–409
 - Electronic Code Book (ECB) 404
 - Output Feedback (OFB) 407
 - unauthenticated 404

- perfect forward secrecy 400–401
 - post-quantum 402
 - Public Key Cryptography Standards (PKCS) 412
 - quantum 401–402
 - communications 401–402
 - computing 402
 - definition of 401
 - salting 397–398, 462–463
 - steganography 415
 - audio 415–416
 - homomorphic 417
 - image 416–417
 - video 416
 - cryptomalware 33–34
 - CSA (Cloud Security Alliance) 139, 603, 884
 - CSAF (Common Security Advisory Framework) 164
 - CSF (Cybersecurity Framework) 882, 884
 - CSIRT. *See* incident response (IR) teams
 - CSOs (chief security officers) 930
 - CSPs (cloud service providers) 139, 233, 598, 853–854
 - CSRF (cross-site request forgery) 602
 - CSRs (certificate signing requests) 689
 - CTR (Counter) mode 404, 408–409
 - Cuckoo 731–732
 - curl command 724–725
 - custodians, data 946
 - custody, chain of 789, 844
 - CVE (Common Vulnerability and Exposure) 78, 125, 146, 177, 886
 - CVE Numbering Authorities (CNAs) 179
 - CVERF (Common Vulnerability Reporting Framework) 164
 - CVSS (Common Vulnerability Scoring System) 182–186, 886
 - CWE (Common Weakness Enumeration) 75, 886
 - CWSS (Common Weakness Scoring System) 887
 - cyber kill chain 770–771
 - Cybersecurity and Infrastructure Security Agency (CISA) 353–354
 - Cybersecurity Framework (CSF) 882, 884
 - cybersecurity insurance 918
 - cybersecurity resilience. *See* resilience
 - CYOD (choose-your-own-device) 588
- D**
- DAC (discretionary access control) 674–676, 679
 - DAEAD (deterministic authenticated encryption with associated data) 404
 - DAI (Dynamic ARP Inspection) 105
 - dark web 124–125, 143
 - Darkleech 146–147
 - dashboards, SIEM 786–789
 - DAST (dynamic application security testing) 470–471
 - data at rest 156, 218
 - data blockers, USB 379–380
 - data breaches
 - data types and asset classification 941–942
 - fines 940
 - identity theft 940
 - impact assessment 948
 - information lifecycle 947–948
 - intellectual property theft 940
 - notifications of 855–856, 941
 - personally identifiable information (PII) 943
 - privacy enhancing technologies 944–945
 - privacy notices 949
 - protected health information (PHI) 944
 - reputation damage from 940
 - response and recovery controls 220–221

- security roles and responsibilities 945–947
- terms of agreement 948
- data classification 904–905
- data controllers 946
- data custodians/stewards 946
- data destruction, secure 386–387
- Data Encryption Standard (DES) 412
- data exfiltration 907–908
- data exposure 267
- data governance 904–905
- data in transit/motion 156, 218
- data in use/processing 156, 218
- data input 186
- data labeling 676
- data loss prevention (DLP) 139, 214–215, 453, 582, 586, 699, 825–826, 871
- data masking 216–218, 945
- data minimization 944–945
- data owners 946
- data privacy. *See* privacy breaches
- data privacy officers (DPOs) 905
- data processors 946
- data protection 214–215
- data protection officers (DPOs) 947
- data recovery 859
- data retention policies 775–776, 906
- data sanitization 748–749
- data sources
 - bandwidth monitors 804
 - Internet Protocol Flow Information Export (IPFIX) 811–813
 - log files 789
 - application 792–793
 - authentication 789–796
 - Call Manager 799–800
 - Domain Name System (DNS) 795–796
 - dump files 797
 - journalctl 802
 - network 790
 - NXLog 803–804
 - security 793
 - Session Initiation Protocol (SIP) 800
 - syslog/rsyslog/syslog-ng 800–801
 - system 791–792
 - Voice over Internet Protocol (VoIP) 799–800
 - web server 794
 - metadata 805–806
 - in email 808
 - in files 809
 - on mobile devices 808
 - on web pages 808–809
 - NetFlow 809–810
 - protocol analyzers 813
 - Security Information and Event Management (SIEM)
 - alerts 788
 - correlation 788–789
 - dashboards 786–789
 - sensitivity 788
 - sensors 787
 - trends 788
 - sFlow 810–811
 - vulnerability scan output 785–786
- data sovereignty 214–215
- data types 941–942
- databases 461–462
- DC (direct current) 380
- DCOM (Distributed Component Object Model) 86
- DCS (distributed control systems) 343
- DCT (Discrete Cosine Transforms) 417
- dd utility 744–745
- DDoS (distributed denial-of-service) attacks 37–38, 54, 111–113, 601
- dead box forensic collection 858
- dead code 270
- Dead Peer Detection (DPD) 501
- deauthentication attacks 101
- decentralized access control 640, 679
- decentralized cameras 375

- decentralized trust models 698
- deception and disruption techniques
 - fake telemetry 223
 - honeypots 221–223
- DeepSound 415
- defense in depth 264
- defrag command 158
- defragmentation 158
- degaussing 387
- delegation of access 662
- DELETE statement 70
- delivery
 - continuous 279
 - malware 43–45
- demilitarized zones (DMZs) 384, 491
- denial-of-service (DoS) attacks 88, 122, 267, 601, 770
- deny lists 467–468, 578, 583, 822–823
- Department of Defense (DoD) security standards 674
- deployment, continuous 279
- deprovisioning, application 260
- DER (Distinguished Encoding Rules) 697
- dereferencing, pointer 75–76
- DES (Data Encryption Standard) 412
- design constraints, embedded systems 361
 - authentication 363
 - compute 361–362
 - cost 363
 - crypto 362
 - implied trust 363
 - inability to patch 362
 - network 362
 - power 361
 - range 363
- destruction and disposal services 387
- detective controls 869–870, 872
- deterministic authenticated encryption
 - with associated data (DAEAD) 404
- deterrent controls 869, 870–871, 872
- development environments 257–260
- development lifecycle. *See* software development lifecycle (SDLC)
- devices, forensic acquisition 850–851
- devices, mobile. *See* mobile solutions
- DevOps 259, 263–265, 278–279
- DevSecOps 259, 278–279
- DFIR (Digital Forensics and Incident Response) 744
- DHCP (Dynamic Host Configuration Protocol) 443
 - snooping 512–513
 - starvation attack 513
- diagrams, configuration 213
- Diamond Model of Intrusion Analysis 768–770
- dictionary attacks 45, 749
- differential backups 326, 328
- Diffie-Hellman 500–501
- dig command 709–710
- DigiCert 691
- digital forensics. *See* forensics, digital
- Digital Millennium Copyright Act 220
- digital rights management (DRM) 67, 219–220
- digital signal processors (DSPs) 359
- Digital Signature Algorithm (DSA) 396, 412
- digital signatures 395–396, 520
- digital video recorders (DVRs) 376–377
- direct current (DC) 380
- directory services 291–292, 442
- directory traversal 75–76, 149, 274–275, 276
- disablement 635, 639
- disassociation attacks 101
- disaster analysis 924–925
- disaster recovery plans (DRPs) 330–331, 772–773, 926, 928–930
- disclosures, public 940
- discovery of identity 623–624

- discovery tools
 - definition of 707
 - dig 709–710
 - hping 717
 - ifconfig 710–711
 - ipconfig 710
 - netcat 720–721
 - netstat 718–720
 - nmap 711–714
 - nslookup 709–710
 - pathping 716–717
 - ping 714–716
 - ping6 716
 - tracert/traceroute 707–709
- Discrete Cosine Transforms (DCT) 417
- discretionary access control (DAC)
 - 674–676, 679
- Disk Cleanup 157
- Disk Defragmenter 158
- disks
 - backups 326
 - encryption 473
 - forensic acquisition of 848
 - hardening 157–159
 - redundancy
 - definition of 315–316
 - multipath 319
 - Redundant Array of Inexpensive Disks (RAID) 315–316
 - Redundant Array of Inexpensive Disks (RAID) 869
 - self-encrypting 475–476
- Distinguished Encoding Rules (DER)
 - 697
- Distributed Component Object Model (DCOM) 86
- distributed control systems (DCS) 343
- distributed denial-of-service (DDoS)
 - attacks 37–38, 54, 111–113, 601
- Distributed Ledger Technology (DLT)
 - 409
- diversity 278, 331–332
- DKIM (Domain Keys Identified Mail)
 - 110, 426
- DLL (dynamic link library) injection 74, 274
- DLP (data loss prevention) 139, 214–215, 453, 582, 586, 699, 825–826, 871
- DLT (Distributed Ledger Technology)
 - 409
- DMARC (Domain-based Message Authentication, Reporting & Conformance) 111
- DMSSEC (Domain Name System Security Extensions) 796
- DMZs (demilitarized zones) 384, 491
- DNS (Domain Name System) 442–443
 - attacks 54
 - cloud-based 601
 - DDoS (distributed denial-of-service) 37–38, 54, 111–113, 601
 - DNS amplification attack 112
 - DNS poisoning 108–110, 223
 - domain hijacking 108
 - domain name kiting 109–110
 - domain reputation 110–111
 - prevalence of 107
 - URL redirection attacks 110
- DNS Security Extensions (DNSSEC)
 - 108, 426–427
- DNS sinkholes 223
- logs 795–796
- OpenDNS 509–510
- dnsenum 728–729, 796
- DNSSEC (Domain Name System Security Extensions) 108, 426–427, 442–443
- Docker 237–240
 - docker images command 237
 - docker ps command 238
 - docker search command 239
- Document Object Model (DOM)
 - 68–69

- documentation, forensic
 - admissibility of 843
 - chain of custody 844
 - event logs 845–846
 - interviews 846–847
 - legal hold 842
 - reports 846
 - tagging of 845–846
 - timelines and sequence of events
 - 844–845
 - time offset 844
 - timestamps 844
 - video 842–843
 - DOM (Document Object Model) 68–69
 - Domain Keys Identified Mail (DKIM)
 - 110, 426
 - domain name kiting 109–110
 - domain name resolution 442–443
 - Domain Name System. *See* DNS (Domain Name System)
 - domain reputation 110–111
 - domain validation (DV) certificates 694
 - Domain-based Message Authentication, Reporting & Conformance (DMARC) 111
 - DoS (denial-of-service) attacks 88, 601, 770
 - DPD (Dead Peer Detection) 501
 - DPOs (data privacy officers) 905
 - Dragonfly 101, 552
 - driver manipulation 89
 - drives. *See* disks
 - DRM (digital rights management) 67, 219–220
 - drones 205, 353–354, 382–383
 - DROP INDEX statement 71
 - DROP TABLE statement 71
 - DRPs (disaster recovery plans) 772–773, 926, 928–930
 - DSA (Digital Signature Algorithm) 396, 412
 - DSPs (digital signal processors) 359
 - DTP (Dynamic Trunking Protocol) 106
 - dual parity, striping with (RAID) 316, 318
 - dual power supplies 321
 - dual supply power 321–322
 - due care 900
 - due diligence 900
 - due process 900
 - dump files 797
 - dumpster diving 13
 - duties, separation of 898, 900
 - DV (domain validation) certificates 694
 - DVRs (digital video recorders) 376–377
 - dynamic application security testing (DAST) 470–471
 - Dynamic ARP Inspection (DAI) 105
 - dynamic code analysis 269, 470–471
 - Dynamic Host Configuration Protocol. *See* DHCP (Dynamic Host Configuration Protocol)
 - dynamic link library (DLL) injection 74, 274
 - dynamic resource allocation 607–608, 611
 - Dynamic Trunking Protocol (DTP) 106
- ## E
- EAP (Extensible Authentication Protocol)
 - 553–556, 664–667
 - EAP-FAST 556, 666
 - EAP-MD5 556, 666
 - EAP-TLS 556, 666
 - EAP-TTLS 556, 666
 - LEAP 666
 - PEAP 556, 666
 - Easter eggs 39–40
 - east-west traffic 492
 - ECB (Electronic Code Book) 404
 - ECC (elliptic-curve cryptography)
 - 399–400
 - ECDSA (Elliptic Curve Digital Signature Algorithm) 551–552
 - edge computing 234–235
 - e-discovery 858–859

- EDR (endpoint detection and response)
 - 452–453
- education, user 22–24, 899, 901–902
- EEA (European Economic Area) 214, 220
- EER (equal error rate). *See* crossover error rate (CER)
- eEye Digital Security, Retina Web Security Scanner 204
- EFS (Encrypting File System) 694
- EIGamal 412
- elasticity 279–280
- electrical metallic tubing (EMT) 385
- electromagnetic (EM) frequency band 102
- Electronic Code Book (ECB) 404
- electronic locks 379
- electronic serial numbers (ESNs) 49, 584
- eliciting information 15–16
- Elliptic Curve Digital Signature Algorithm (ECDSA) 551–552
- elliptic-curve cryptography (ECC) 399–400
- elliptic-curve techniques 412
- EM (electromagnetic) frequency band 102
- email
 - attack vectors 122
 - certificates 696
 - email protocol port numbers 441
 - email servers 145
 - metadata in 808
 - Spam 13
 - SPIM (Spam over Internet Messaging) 13
 - synchronization 440
- Email Security Appliance (ESA) 111
- embedded systems
 - aircraft 348–350
 - Arduino 340
 - communication considerations
 - 5G 357–358
 - baseband radio 359
 - NarrowBand 358
 - subscriber identity module (SIM) cards 360
 - Zigbee 360–361
- constraints 361
 - authentication 363
 - compute 361–362
 - cost 363
 - crypto 362
 - implied trust 363
 - inability to patch 362
 - network 362
 - power 361
 - range 363
- definition of 339
- drones 353–354
- Field-Programmable Gate Array (FPGA) 340
- heating, ventilation, and air conditioning (HVAC) 352–353
- industrial control systems (ICSs) 341–343
- Internet of Things (IoT) 38, 98, 113, 344–346, 358, 414
- medical systems 347
- multifunction printers (MFPs) 354
- Raspberry Pi 339
- real-time operating systems (RTOSs) 355
- smart meters 350
- supervisory control and data acquisition (SCADA) 341–343
- surveillance systems 355–356
- system on a chip (SoC) 356–357
- vehicles 347–348
- Voice over Internet Protocol (VoIP) 350, 799–800
- emergency preparedness logs 383
- EMT (electrical metallic tubing) 385
- Encapsulating Security Payload (ESP) 437, 503, 520
- EnCase 850–851

- Encrypting File System (EFS) 694
- encryption 159, 362
 - cloud computing 605, 610
 - data at rest 218
 - data in transit/motion 218
 - data in use/processing 218
 - disk 473
 - entropy 419
 - homomorphic 417
 - international mobile subscriber identity (IMSI) 49, 358, 584
 - mobile device management (MDM) 578–580
 - modes of operation 403–409
 - authenticated 404
 - Cipher Block Chaining (CBC) 405
 - Cipher Feedback (CFB) 406
 - Counter (CTR) 404, 408–409
 - Electronic Code Book (ECB) 404
 - Output Feedback (OFB) 407
 - unauthenticated 404
 - symmetric/asymmetric 411–413
 - vulnerabilities 150–151
 - end of life (EOL) 904
 - end of service life (EOSL) 904
 - end users 947
 - endpoint detection and response (EDR) 452–453
 - endpoint DLP systems 214
 - endpoint protection 451
 - endpoint security solutions 822
 - approved lists 822
 - block/deny lists 467–468, 578, 583, 822–823
 - quarantine 823–824
 - end-to-end headers (HTTP) 466
 - energy management, SCADA control systems 342–343
 - engagement, rules of 200
 - enterprise environments
 - API considerations 216
 - configuration management 213, 215–216
 - data masking 216–218
 - data protection 214–215
 - data sovereignty 214–215
 - deception and disruption techniques
 - fake telemetry 223
 - honeypots 223
 - honeypots 221–223
 - digital rights management (DRM) 219–220
 - DNS sinkholes 223
 - encryption 218
 - hashing 218–219
 - response and recovery controls 220–221
 - site resiliency 221–222
 - enterprise resource planning (ERP) 883
 - entropy 419
 - enumerations 886
 - env command 739
 - environmental disaster 924
 - environmental groups 182
 - environmental variables 740
 - environments, software development 257–260
 - known 198
 - partially known 199
 - unknown 198–199
 - EOL (end of life) 904
 - EOSL (end of service life) 904
 - ephemeral keys 403
 - equal error rate. *See* crossover error rate (CER)
 - eradication phase, incident response (IR) 764
 - ERP (enterprise resource planning) 883
 - error handling 79–82
 - compile-time errors 81–82, 266–267
 - error-based technique 74
 - input handling 80
 - runtime errors 81–82, 266–267

- escalation, privilege 67–68, 201, 941
- escape attacks, VM (virtual machine) 248–249
- escrow, key 699
- ESNs (electronic serial numbers) 49, 584
- ESP (Encapsulating Security Payload) 437, 503, 520
- ethical hacking. *See* penetration testing
- ETSI (European Telecommunications Standards Institute) 235
- EU (European Union)
 - European Economic Area (EEA) 214, 220
 - European Telecommunications Standards Institute (ETSI) 235
 - General Data Protection Regulation (GDPR) 42, 214, 220, 356, 434, 453, 760, 855, 878–879, 947
 - Information Society Directive 220
- EV (extended validation) certificates 694
- event logs 845–846
- Event Viewer 791–792
- events, sequence of 844–845
 - time offset 844
 - timestamps 844
- evidence, forensic
 - acquisition 847–854
 - artifacts 853
 - cache 852
 - checksums 857
 - data breach notification laws 855–856
 - definition of 847
 - device 850–851
 - disk 848
 - firmware 851
 - hashing 856–857
 - integrity 856
 - network 852–853
 - operating system 850
 - order of volatility 848
 - on-premises versus cloud 853–854
 - random-access memory (RAM) 848–849
 - regulatory and jurisdictional 855
 - right-to-audit clauses 854
 - snapshot 851–852
 - swap/pagefile 849–850
 - admissibility of 843
 - chain of custody 844
 - e-discovery 858–859
 - event logs 845–846
 - interviews 846–847
 - legal hold 842
 - preservation 858
 - provenance 857–858
 - reports 846
 - tagging of 845–846
 - timelines and sequence of events 844–845
 - time offset 844
 - timestamps 844
 - video 842–843
- evil twin attacks 98–99
- exam preparation
 - final review and study 953–954
 - hands-on activities 953
 - Pearson Test Prep practice test 954
 - test lab, building 953
- exam updates 02.0004–02.0026
- exchanges, key 399
- executives, security roles and responsibilities 945–947
- exercises
 - simulations 766–767
 - tabletop 765–766
 - walkthrough 766
- exFAT 850
- exfiltration 770, 907–908
- expiration, certificates 693
- explicit allow/deny 528
- Exploit code maturity (E) metric 184
- exploit kits 44
- Exploitability metrics 183–184

- exploitation frameworks 747–748, 770
 - Extended Detection and Response (XDR) 189
 - extended validation (EV) certificates 694
 - Extensible Authentication Protocol. *See* EAP (Extensible Authentication Protocol)
 - Extensible Configuration Checklist Description Format (XCCDF) 885
 - Extensible Markup Language (XML) injection 74–75, 273–274
 - external actors 122
 - external risk 917. *See also* risk management
 - extinguishers, fire 381
 - extranets 492–493, 899
- F**
- f8-mode (SRTP) 430
 - FAA (Federal Aviation Administration) 348–349, 353, 382–383
 - facility automation 345
 - facility codes 373
 - fail-closed 927
 - fail-open 927
 - failure, single point of 156, 926
 - failure in time (FIT) 926
 - fake telemetry 223
 - false acceptance rate (FAR) 303, 626
 - false negatives 181, 519, 520
 - false positives 181, 518, 520
 - false rejection rate (FRR) 303, 626
 - Faraday cages 383, 562–563
 - FAST (Flexible Authentication via Secure Tunneling) 556
 - Fast Identity Online (FIDO) 297
 - FAT 850
 - FDE (full-disk encryption) 473, 475–476
 - fdisk -l command 157
 - FEAT command 433
 - Federal Aviation Administration (FAA) 348–349, 353, 382–383
 - Federal Information Security Management Act (FISMA) 776
 - Federal Risk and Authorization Management Program (FedRAMP) 599
 - Federal Trade Commission (FTC) 17, 221
 - federated identity management (FIM) 658
 - federation 292–293, 623–624, 658, 672
 - FedRAMP (Federal Risk and Authorization Management Program) 599
 - fencing 380–381
 - FFmpeg 416
 - FIDO (Fast Identity Online) 297
 - Field-Programmable Gate Array (FPGA) 340
 - file and code repositories 127
 - file integrity monitors 542
 - file manipulation 732–733
 - cat command 734–735
 - chmod command 736–737
 - grep command 735–736
 - head command 733
 - logger command 737–738
 - tail command 734
 - file servers 144
 - file transfer 440
 - File Transfer Protocol. *See* FTP (File Transfer Protocol)
 - fileless viruses 37
 - files
 - log 789
 - application 792–793
 - authentication 789–796
 - Call Manager 799–800
 - Domain Name System (DNS) 795–796
 - dump files 797

- journalctl 802
- network 790
- NXLog 803–804
- security 793
- Session Initiation Protocol (SIP) 800
- syslog/rsyslog/syslog-ng 800–801
- system 791–792
- Voice over Internet Protocol (VoIP) 799–800
- web server 794
- metadata in 809
- filtering
 - content/URL 533, 828–829
 - MAC (media access control) 513
 - packet 528
- financial information. *See* personally identifiable information (PII)
- Financial Services Information Sharing and Analysis Center (FS-ISAC) 124
- files 940
- fingerprint authentication 300–301
- fire
 - disaster analysis for 924–925
 - suppression 381
- firewalls 146, 198
 - appliance 534
 - application-level gateway (ALG) 529
 - in cloud 613–614, 615
 - configuration 529–533
 - content URL/filtering 533
 - hardware versus software 534
 - host-based 457–458, 534
 - multihomed connections 532
 - NAT gateway 529
 - network-based application layer 530
 - next-generation firewall (NGFW) 453–454, 524
 - packet filtering 528
 - personal 534
 - purpose of 526–528
 - rules 528, 825
 - unified threat management (UTM) 524
 - virtual 534–535
 - web application 531
 - wireless security 562
- firmware
 - firmware over-the-air (OTA) updates 583
 - forensic acquisition of 851
- FIRST (Forum of Incident Response and Security Teams) 180
- FISMA (Federal Information Security Management Act) 776
- FIT (failure in time) 926
- flash drives, malicious 47–48
- Flexible Authentication via Secure Tunneling (FAST) 556
- flood, disaster analysis for 925
- flooding, MAC (media access control) 106
- FM200 381
- fog computing 234–235
- footprinting 205
- Forcepoint 533
- Forefront Identity Manager 658
- Foremost 415
- Forensic Toolkit (FTK) 747, 850–851
- forensics, digital
 - acquisition
 - artifacts 853
 - cache 852
 - checksums 857
 - data breach notification laws 855–856
 - definition of 847
 - device 850–851
 - disk 848
 - firmware 851
 - hashing 856–857
 - integrity 856
 - network 852–853
 - operating system 850
 - order of volatility 848

- on-premises versus cloud 853–854
 - random-access memory (RAM)
 - 848–849
 - regulatory and jurisdictional 855
 - right-to-audit clauses 854
 - snapshot 851–852
 - swap/pagefile 849–850
 - data recovery 859
 - definition of 744, 837
 - Digital Forensics and Incident Response (DFIR) 744
 - documentation/evidence
 - admissibility of 843
 - chain of custody 844
 - event logs 846
 - interviews 846–847
 - legal hold 842
 - reports 846
 - tagging of 845–846
 - timelines and sequence of events 844–845
 - video 842–843
 - e-discovery 858–859
 - nonrepudiation 859–860
 - preservation 858
 - provenance 857–858
 - strategic intelligence/
 - counterintelligence 860
 - tools
 - Autopsy 747
 - dd 744–745
 - FTK Imager 747
 - memdump 745
 - WinHex 746
 - forgeries, request 85–86
 - formats, certificate 697
 - Forum of Incident Response and Security Teams (FIRST) 180
 - forward proxy 516
 - forward secrecy 400–401
 - FPGA (Field-Programmable Gate Array) 340
 - frameworks
 - exploitation 747–748
 - IT security 881–884
 - FreeBSD 676
 - frequency distributions 159
 - FRR (false rejection rate) 303, 626
 - fsck command 158
 - FTC (Federal Trade Commission) 17, 221
 - FTK (Forensic Toolkit) 747, 850–851
 - FTP (File Transfer Protocol)
 - FTP servers 147–148
 - FTPS (File Transfer Protocol, Secure) 432–433
 - SFTP (Secure File Transfer Protocol) 434
 - full backups 326, 328–331
 - full tunnel mode, SSL/TLS VPN 508
 - full-disk encryption (FDE) 473, 475–476
 - functions, hash 218–219
 - fuzz testing 80, 269–270, 471
 - fuzzers 269–270
- ## G
- gait analysis 302
 - Galois Message Authentication Code (GMAC), AES in 498
 - Galois/Counter Mode (GCM) 498, 551–552
 - gamification 902
 - gapping 384
 - gateways
 - application-level 529
 - NAT 529
 - transit 246–247
 - GCM (Galois/Counter Mode) 498, 551–552
 - GDPR (General Data Protection Regulation) 42, 214, 220, 356, 434, 453, 760, 855, 878–879, 947
 - general-purpose I/O GPIO framework extension (GpioClx) 477

- generators 321
- generic accounts 629
- Generic Routing Encapsulation (GRE) 520
- geofencing 572–573, 578–580
- geographic dispersal 315
- geolocation 578–580, 639
- geotagging 572–573, 584, 586, 639
- GitHub repositories 8, 18, 127, 203, 258
- GitLab 127, 258
- Global Positioning System (GPS) 572, 584
- Global Regular Expression Print (grep) 735–736
- GMAC (Galois Message Authentication Code), AES in 498
- Gnutella 530
- Golden SAML attacks 293
- Google
 - Cloud 233, 603, 853
 - Google Pay 584
 - Kubernetes 239–240
 - OAuth 2.0 292
 - Secret Manager 604
- governance, risk, and compliance (GRC) 880, 904–905
- GpioGlx (general-purpose I/O GPIO framework extension) 477
- GPOs (group policy objects) 474
- GPS (Global Positioning System) 572, 584
- Gramm-Leach-Bliley (GLB) Act 880
- GraphQL 86
- gray hat hackers 121
- gray-box testing 80
- GRC (governance, risk, and compliance) 880, 904–905
- GRE (Generic Routing Encapsulation) 520
- grep command 735–736
- group policy objects (GPOs) 474

- groups
 - base 182
 - environmental 182
 - security 607, 611
 - temporal 182
- Grover's algorithm 402
- guards 377
- guest accounts 629
- Guidelines for Evidence Collection and Archiving 848

H

- HA (high availability) 329–330
 - across zones 603, 609
 - cloud computing 605, 610
- HackerOne 203
- hackers 121. *See also* penetration testing
- hacktivists 120, 122
- hands-on activities 953
- hard disks
 - backups 326
 - encryption 473
 - forensic acquisition of 848
 - hardening 157–159
 - redundancy
 - definition of 315–316
 - multipath 319
 - Redundant Array of Inexpensive Disks (RAID) 315–316
 - self-encrypting 475–476
- hardening
 - applications 471
 - hard disks 157–159
 - operating systems 473–474
- hardware root of trust 476–477
- hardware security modules (HSMs) 478, 524, 587, 656
- Hardware Shield 851
- hashcat 749
- HashCorp Nomad 240
- Hashed Message Authentication Mode (HMAC) 295–296, 551–552

- hashing 218–219, 463, 856–857
 - avalanche effect 463
 - collisions 463
 - definition of 398–399
 - Digital Signature Algorithm (DSA) 396
 - Elliptic Curve Digital Signature Algorithm (ECDSA) 551–552
 - Hashed Message Authentication Mode (HMAC) 295–296
 - Message Digest Algorithm 5 (MD5) 55, 219
 - padding 463
 - pass the hash 89–90
 - salting 47, 82
 - Secure Hash Algorithm (SHA) 55, 463, 551–552
 - SHA-256 463
- HAVA (Help America Vote Act) 880
- head command 733
- headers, HTTP (Hypertext Transfer Protocol) 465–466
- Health Insurance Portability and Accountability Act (HIPAA) 453, 880, 940, 944
- heat maps 559
- heating, ventilation, and air conditioning (HVAC) 352–353
- Help America Vote Act (HAVA) 880
- heuristic-based analysis 521
- heuristic-based intrusion detection 521
- HID Global 629
- HIDSs (host intrusion detection systems) 215, 456, 578, 586
- high availability (HA) 329–330
 - across zones 603, 609
 - cloud computing 605, 610
- hijacking
 - BGP 535–536
 - blind 84
 - cookie 465
 - session 54, 83, 465, 601
 - TCP/IP 84
 - URL 44
- hijacking, domain 108
- HIPAA (Health Insurance Portability and Accountability Act) 453, 880, 940, 944
- HIPSs (host intrusion prevention systems) 454–455, 523
- Hitachi 476
- HMAC (Hashed Message Authentication Mode) 295–296, 551–552
- HMAC-based one-time password (HOTP) 295–296
- HMI (human-machine interface) 341
- hoaxes 19
- holds, legal 842
- HOME environment variable 740
- homomorphic encryption 417
- homomorphic steganography 417
- honeyfiles 223
- honeypots 221–223
- hop-by-hop headers (HTTP) 466
- horizontal privilege escalation 67–68
- host command 716
- host intrusion detection systems (HIDS) 215, 456, 578, 586
- host intrusion prevention systems (HIPSs) 454–455, 523
- host security. *See also* application security
 - antimalware 452
 - antivirus software 451
 - boot integrity
 - boot attestation 460–461
 - definition of 458–459
 - measured boot 459–460
 - Unified Extensible Firmware Interface (UEFI) 459
 - data loss prevention (DLP) 453
 - databases 461–462
 - endpoint 451, 452–453
 - hashing 463

- host intrusion detection systems (HIDS) 215, 456, 578, 586
 - host intrusion prevention systems (HIPSs) 454–455, 523
 - host-based firewalls 457–458
 - next-generation firewall (NGFW) 453–454
 - salting 462–463
 - Host-based IPSs (HIPSs) 523
 - hot aisles 386
 - hot sites 221
 - hotfixes and patches 160–164, 179–180, 362, 474–475
 - HOTP (HMAC-based one-time password) 295–296
 - hotspots 585
 - hping command 717
 - Hping.org 717
 - HSMs (hardware security modules) 478, 524, 587, 656
 - HTTP (Hypertext Transfer Protocol) 465–466, 577
 - HTML5 505–508
 - HTTPS 82, 268, 436–437, 577
 - human resources (HR) personnel 901
 - human-machine interface (HMI) 341
 - HUMINT (human intelligence) 18
 - HVAC (heating, ventilation, and air conditioning) 352–353
 - hybrid attacks 749
 - hybrid cloud 140, 233
 - hyper-jacking 248
 - Hypertext Transfer Protocol. *See* HTTP (Hypertext Transfer Protocol)
 - hypervisors 325
 - attacks 601
 - hypervisor-based keyloggers 42
- I**
- IA (information assurance). *See* risk management
 - IaaS (infrastructure as a service) 139, 231, 603, 853
 - IaC (infrastructure as code) 241–243, 260
 - IACS 342
 - IACS (industrial automation and control systems) 342, 343
 - IAM (identity and access management) 633
 - identity and access lifecycle 633–635
 - account audits 635
 - disablement 635
 - privileges provisioning 635
 - registration and identity validation 633–635
 - policy 605
 - IBM
 - AppScan 204
 - Data Encryption Standard (DES) 412
 - QRadar 526
 - IC (integrated circuit) cards 373
 - ICCIDs (unique serial numbers) 360
 - ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) 362
 - ICs (industrial control systems) 353–354
 - identification phase, incident response (IR) 763
 - identity. *See also* authentication; certificates; passwords
 - discovery of 623–624
 - federation 623
 - identity and access management (IAM) 633–635
 - identity and access lifecycle 633–635
 - policy 605
 - identity fraud 17, 638
 - baiting 19
 - credential harvesting 18
 - hoaxes 19
 - identity theft 940
 - impersonation/pretexting 19
 - invoice scams 17
 - reconnaissance 18
 - typo squatting 20, 44
 - watering hole attacks 20, 85

- identity providers (IdPs) 292, 623–624, 661
- Secure Shell (SSH) keys 628
- smart cards 629
- tokens 627–628
- Identity Services Engine (ISE) 590
- IdPs (identity providers) 292, 623–624, 661
- IDSs (intrusion detection systems). *See* HIDSs (host intrusion detection systems); network intrusion detection systems (NIDSs)
- IEEE 802.1X standard 510, 553–556, 562, 664–667, 673
- IETF (Internet Engineering Task Force)
 - IPFIX (Internet Protocol Flow Information Export) 187
 - RFC (request for comments) 128
- ifconfig command 710–711
- IIS (Internet Information Services) 146, 697, 794
- IKE (Internet Key Exchange)
 - IKEv1 Phase 1 negotiation 498–501
 - IKEv1 Phase 2 negotiation 501–503
 - IKEv2 504–505
- image backups 326
- image steganography 416–417
- IMAP (Internet Message Access Protocol) 438–439
- IMEI (international mobile equipment identity) 49, 584
- immutability 263
- impact assessment 184, 920, 921, 948
- impersonation 19
- implicit deny 528, 680
- impossible travel time 639
- IMSI (international mobile subscriber identity) encryption 358, 584
- in-band SQL injection 73
- incident response (IR) plans
 - business continuity plans (BCPs) 773–774, 929
 - communication plans 771–772
 - continuity of operations plans (COOPs) 774–775, 929
 - cyber kill chain 770–771
 - data retention policies 775–776
 - definition of 760–761
 - Diamond Model of Intrusion Analysis 768–770
 - disaster recovery plans (DRPs) 772–773
 - exercises
 - simulations 766–767
 - tabletop 765–766
 - walkthrough 766
 - incident response teams 175, 760, 775–776
 - MITRE ATT&CK framework 18, 128–129, 176, 205, 223, 767–768
 - process and lifecycle
 - containment 763–764
 - eradication 764
 - identification 763
 - lessons learned 764–765
 - overview of 761–762
 - preparation 762–763
 - recovery 764
 - stakeholder management 771–772
- incident response (IR) teams 175, 760, 775–776
- incremental backups 326, 328
- indicators of compromise (IoCs) 123, 762, 832, 853
- industrial automation and control systems (IACS) 342, 343
- industrial camouflage 377
- Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) 362
- industrial control systems (ICSs) 341–343, 353–354
- Industry 4.0 342
- influence campaigns 21

- information assurance (IA). *See* risk management
- information lifecycle 947–948
- Information Sharing and Analysis Centers (ISACs) 123–125
- Information Society Directive 220
- information systems security officers (ISSOs) 930, 947
- Information Technology Infrastructure Library (ITIL) 882
- information technology operations 263
- InfraGard 128
- infrastructure as a service (IaaS) 139, 231, 603, 853
- infrastructure as code (IaC) 241–243, 260
- inherent risk 921
- inheritance, of permissions 644–646
- Initial Contact 501
- initialization vectors (IVs) 103, 403
- injection 70
 - code 149, 273–274, 276
 - DLL (dynamic link library) 74
 - LDAP (Lightweight Directory Access Protocol) 74, 144
 - SQL (Structured Query Language) 54, 70–74, 273–274, 464
 - XML (Extensible Markup Language) 74–75
- inline prevention detection systems (IPSS) 523–524
- input handling 79–82
- input validation 80, 81, 267–268, 464
- INSERT INTO statement 70
- inspection, API 607, 610
- instance awareness 608, 611
- insurance, cybersecurity 918
- integer overflows 77, 271
- integrated circuit (IC) cards 373
- integration
 - API 607, 610
 - cloud computing 604, 609
 - continuous 279
- integrity 289
 - boot
 - boot attestation 460–461
 - definition of 458–459
 - measured boot 459–460
 - Unified Extensible Firmware Interface (UEFI) 459
 - forensic acquisition 856
 - integrity control 378
 - measurement of 184, 261, 887
- Intel Hardware Shield 851
- intellectual property theft 917, 940
- intelligence
 - automated indicator sharing (AIS) 125
 - Information Sharing and Analysis Centers (ISACs) 123–125
 - intelligence fusion 177
 - MITRE ATT&CK framework 18, 128–129, 176, 205, 223, 767–768
 - research sources 127–128
 - strategic 860
 - Structured Threat Information eXpression (STIX) 125–127
 - Trusted Automated eXchange of Indicator Information (TAXII) 125–127
 - vulnerability databases 125
- interconnection security agreements (ISAs) 903
- intermediate certificate authorities 696
- internal actors 122
- internal information 905
- internal risk 917. *See also* risk management
- international mobile equipment identity (IMEI) 49, 584
- international mobile subscriber identity (IMSI) 49, 358, 584
- International Organization for Standardization (ISO) 881, 884, 893
- Internet Engineering Task Force (IETF)

- IPFIX (Internet Protocol Flow Information Export) 187
- RFC (request for comments) 128
- Internet Information Services (IIS) 146, 697, 794
- Internet Key Exchange. *See* IKE (Internet Key Exchange)
- Internet Message Access Protocol (IMAP) 438–439
- Internet of Things (IoT) 38, 98, 113, 344–346, 358, 414
- Internet Protocol. *See* IP (Internet Protocol)
- Internet Protocol Flow Information Export (IPFIX) 187, 524, 811–813
- Internet Security Association and Key Management Protocol (ISAKMP) 497
- Internet service providers (ISPs) 808
- interviews, forensic 846–847
- Intigriti 203
- intranets 492–493
- intrusion detection systems. *See* host intrusion detection systems (HIDS)
- intrusion detection systems (IDSs). *See* network intrusion detection systems (NIDSs)
- intrusion phase, cyber kill chain 770
- intrusion prevention systems. *See* host intrusion prevention systems (HIPSs)
- intrusive scans 182
- Investigate 509–510
- investigations, data sources for
 - bandwidth monitors 804
 - Internet Protocol Flow Information Export (IPFIX) 811–813
 - log files 789
 - application 792–793
 - authentication 789–796
 - Call Manager 799–800
 - Domain Name System (DNS) 795–796
 - dump files 797
 - journalctl 802
 - network 790
 - NXLog 803–804
 - security 793
 - Session Initiation Protocol (SIP) 800
 - syslog/rsyslog/syslog-ng 800–801
 - system 791–792
 - Voice over Internet Protocol (VoIP) 799–800
 - web server 794
- metadata
 - in email 808
 - in files 809
 - on mobile devices 808
 - types of 805–806
 - on web pages 808–809
- NetFlow 809–810
- protocol analyzers 813
- Security Information and Event Management (SIEM)
 - alerts 788
 - correlation 788–789
 - dashboards 786–789
 - sensitivity 788
 - sensors 787
 - trends 788
- sFlow 810–811
- vulnerability scan output 785–786
- invoice scams 17
- IoCs (indicators of compromise) 123, 762, 832, 853
- IoT (Internet of Things) 38, 98, 113, 344–346, 358, 414
- IP (Internet Protocol). *See also* IPsec
 - addresses
 - IPv4 443–444
 - IPv6 536–537
 - virtual 488

- configuration management 213
 - IP proxy 514
 - IP scanners
 - arp command 721–722
 - Cuckoo 731–732
 - curl command 724–725
 - definition of 721
 - dnsenum 728–729
 - Nessus 730–731
 - route command 723–724
 - scanless 727–728
 - sn1per 726–727
 - theHarvester 725–726
 - IP-Box 850–851
 - ipconfig command 710
 - IPFIX (Internet Protocol Flow Information Export) 187, 524, 811–813
 - IPsec 247, 437–438, 497. *See also* IKE (Internet Key Exchange)
 - attributes 501–502
 - Authentication Header (AH) 437
 - Encapsulating Security Payload (ESP) 437, 503
 - IKEv1 Phase 1 negotiation 498–501
 - IKEv1 Phase 2 negotiation 501–503
 - IKEv2 504–505
 - modes 438, 503
 - passthrough 501
 - IPs (intrusion prevention systems). *See*
 - HIPSs (host intrusion prevention systems); network intrusion detection systems (NIDSs)
 - IR. *See* incident response (IR) plans
 - iris recognition 301
 - ISACA COBIT framework 882
 - ISACs (Information Sharing and Analysis Centers) 123–125
 - ISAKMP (Internet Security Association and Key Management Protocol) 497
 - ISAs (interconnection security agreements) 903
 - ISE (Identity Services Engine) 590
 - ISO (International Organization for Standardization) 881, 884, 893
 - isolation 491, 562, 830
 - ISPs (internet service providers) 808
 - ISSOs (information systems security officers) 930, 947
 - issuers, certificate 692
 - IT contingency planning (ITCP) 929
 - IT security frameworks 881–884
 - ITIL (Information Technology Infrastructure Library) 882
 - ITU-T X.690 encoding formats 697
 - IVs (initialization vectors) 103, 403
- J**
- jamming 102, 561–562
 - Japan’s Personal Information Protection Act (JPIPA) 220
 - JavaScript Object Notation (JSON) injection 273–274
 - JavaScript-based keyloggers 43
 - job rotation 898, 900
 - John the Ripper 44, 749
 - journalctl 802
 - jump servers 514
 - jurisdictional forensic intervention 855
- K**
- Kali forensics 850
 - Kali Linux 415, 953
 - Katacoda 239
 - KBA (knowledge-based authentication) 625, 656–657
 - KDC (key distribution center) 668
 - KE (Key Exchange) 500
 - Kerberoasting TGS 292
 - Kerberos 82–83, 89, 292, 553, 668–670, 673

- kernel-based keyloggers 42
 - Key Exchange (KE) 500
 - .key file extension 697
 - key recovery agents 699
 - key signing keys (KSKs) 427
 - keyloggers 42–43, 108, 113
 - keys 688
 - ephemeral 403
 - escrow 699
 - generation algorithms for 395
 - key distribution center (KDC) 668
 - key exchanges 399
 - key signing keys (KSKs) 427
 - length of 396
 - mobile device management (MDM) 577–578
 - password 655
 - personal unblocking keys (PUKs) 360
 - Public Key Cryptography Standards (PKCS) 412
 - public/private 436–437
 - Secure Shell (SSH) 625, 628
 - stretching 397
 - zone signing keys (ZSKs) 427
 - kiting, domain name 109–110
 - knowledge-based authentication (KBA) 625, 656–657
 - known environment/white box testing 198, 468–469
 - KSKs (key signing keys) 427
 - Kubernetes 239–240, 279–280
- L**
- L0phtCrack 47
 - L2F (Layer 2 Forwarding Protocol) 508
 - L2TP (Layer 2 Tunneling Protocol) 494, 505–508
 - LANG environment variable 740
 - last known good configuration (LKGC) 329
 - lateral movement 201, 770
 - lateral traffic 492
 - laws 879–880
 - Layer 2 attacks
 - ARP cache poisoning 105
 - MAC cloning attacks 106
 - MAC flooding attacks 106
 - security best practices 106–107
 - Layer 2 Forwarding Protocol (L2F) 508
 - Layer 2 security 512
 - Bridge Protocol Data Unit (BPDU) guard 512
 - DHCP snooping 512–513
 - loop protection 512
 - MAC filtering 513
 - Layer 2 Tunneling Protocol (L2TP) 494, 505–508
 - LCP (Link Control Protocol) 44
 - LDAP (Lightweight Directory Access Protocol)
 - injection attacks 144, 273–274, 291, 442, 667–670
 - Lightweight Directory Access Protocol over SSL (LDAPS) 432
 - LDAPS (Lightweight Directory Access Protocol over SSL) 432
 - leaks, memory 78, 88
 - LEAP (Lightweight EAP) 666
 - least functionality 152
 - least privilege 264, 630, 681, 908
 - least significant bit (LSB) steganography 416–417
 - least-trusted zones 825
 - ledgers, public 409–410
 - legacy platforms 165
 - legal hold 842
 - lessons learned phase, incident response (IR) 764–765
 - libraries, third-party 265
 - licensing 918
 - lifecycle
 - identity and access 633–635
 - account audits 635
 - disablement 635

- privileges provisioning 635
- registration and identity validation 633–635
- incident response (IR)
 - containment 763–764
 - eradication 764
 - identification 763
 - lessons learned 764–765
 - overview of 761–762
 - preparation 762–763
 - recovery 764
- information 947–948
- penetration testing 199–202
- lighting, security 380
- lightweight cryptography 414–415
- Lightweight Cryptography Project 415
- Lightweight Directory Access Protocol.
 - See* LDAP (Lightweight Directory Access Protocol)
- Lightweight Directory Access Protocol over SSL (LDAPS) 432
- Lightweight EAP (LEAP) 666
- Link Control Protocol (LCP) 44
- Linux
 - Kali Linux 415
 - Linux Kernel 236
 - System Monitor 542
- lists
 - allow 467, 578, 583, 822
 - block/deny 467–468, 822–823
 - certificate revocation 829
- live boot media 329
- live box forensics 858
- load balancers 319–320
- load balancing
 - active/active 488
 - active/passive 488
 - definition of 488
 - scheduling 488
 - Virtual IP address 488
- Local Security Authority Subsystem Service (LSASS) 47–48
- locality attribute (certificates) 692
- Lockheed Martin 770
- locks and lockout programs 378–379, 579, 639
- log collectors 186
- log files 789
 - aggregation 186
 - analytics 383
 - application 792–793
 - audit 869–870
 - authentication 789–796
 - Call Manager 799–800
 - collection of 186
 - correlation of 186
 - Domain Name System (DNS) 795–796
 - dump files 797
 - emergency preparedness 383
 - event 845–846
 - journalctl 802
 - network 790, 852–853
 - normalization of 186
 - NXLog 803–804
 - review 182
 - risk 920
 - security 383, 793
 - Session Initiation Protocol (SIP) 800
 - syslog/rsyslog/syslog-ng 800–801
 - system 791–792
 - visitor 383
 - Voice over Internet Protocol (VoIP) 799–800
 - web server 794
- logger command 737–738
- logic bombs 39–40
- logistics, SCADA control systems 343
- loop protection 512
- LS_COLORS environment variable 740
- LsaLogonUser 90
- LSASS (Local Security Authority Subsystem Service) 47–48
- LSB (least significant bit) steganography 416–417

M

- MaaS (monitoring as a service) 139, 232
- MAC (mandatory access control) 588, 676, 679, 905
- MAC (media access control) 511
 - addresses 511
 - cloning attacks 106
 - filtering 513
 - flooding attacks 106
 - spoofing 101
- MACB (Modified, Accessed, Changed, and Birth) times 844
- machine certificates 696
- machine learning. *See* AI/ML (artificial intelligence and machine learning)
- macOS Activity Monitor 542
- macros 113
- MACs (message authentication codes) 399, 410
- MAIL environment variable 740
- malicious software. *See* malware
- Maltego 203
- malware 113
 - antimalware 452
 - backdoors 42–43
 - bots and botnets 37–38, 111–112
 - cryptomalware 33–34
 - definition of 33
 - delivery mechanisms 43–45
 - fileless viruses 37
 - keyloggers 42–43
 - logic bombs 39–40
 - malvertising 40
 - mobile device security countermeasures 580
 - permanent damage from 45
 - potentially unwanted programs (PUPs) 40–42
 - ransomware 33–34, 111–112
 - spyware 40–42
 - time bombs 39
 - Trojans 35, 104, 113
 - worms 36–37
- MAM (mobile application management) 585–587
- managed detection and response (MDR) 234
- managed power distribution units (PDU)s 322–323
- managed security service providers (MSSPs) 233–234
- managed service providers (MSPs) 233–234
- management
 - managerial controls 868
 - roles and responsibilities 945–947
- Management Information Bases (MIBs) 436
- mandatory access control. *See* MAC (mandatory access control)
- mandatory vacation policies 900
- man-in-the-middle (MITM) attacks. *See* on-path (man-in-the-middle) attacks
- manipulating files. *See* file manipulation
- manual code review 470
- manufacturing, SCADA control systems 342
- mapping
 - many-to-one 690
 - one-to-one 690
- masking, data 945
- Mavituna Security Netsparker 204
- maximum transmission unit (MTU)
 - discovery 717
- MBR (master boot record) 35–36, 851
- MD5 algorithm 55, 219
- MDM (mobile device management) 152, 574–576, 825–826, 908
 - application and content management 576–578

- bring-your-own-device (BYOD) 215, 572, 574–576, 581, 588–590, 826, 898
- choose-your-own-device (CYOD) 588–590
- corporate-owned, personally enabled (COPE) 572, 588–590
- enforcement and monitoring 581–585
- metadata 808
- mobile application management (MAM) 585–587
- SEAndroid 588
- security concerns and countermeasures 578–581
- unified endpoint management (UEM) 587–588
- virtual desktop infrastructure (VDI) 589
- MDR (managed detection and response) 234
- mean time between failures (MTBF) 926
- mean time to failure (MTTF) 926
- mean time to repair (MTTR) 926
- measured boot 459–460
- Measurement System Analysis (MSA) 904
- MEC (multi-access edge computing) 235
- media access control. *See* MAC (media access control)
- medical systems 347
- MEIDs (mobile equipment identifiers) 49, 584
- memdump 745
- memorandum of understanding (MOU) 903
- memory management 265. *See also* buffer overflows
 - ARP cache poisoning 105
 - content addressable 106
 - leaks 78, 88, 271
 - random-access memory (RAM) 849–850
 - runtime 477
 - static random-access memory (SRAM) 340
 - virtual 850
 - vulnerabilities 77–78, 149, 271–272, 275
- memory-injection-based keyloggers 43
- Men & Mice Logeater 796
- Mentor Nucleus RTOS 347
- message authentication codes (MACs) 399, 410
- Message Digest Algorithm 5 (MD5) 55, 219
- metadata
 - in email 808
 - in files 809
 - on mobile devices 808
 - types of 805–806
 - on web pages 808–809
- Meterpreter scripts 90
- MFA (multifactor authentication) 304–306, 579, 656–657
- MFPs (multifunction printers) 354
- MicroSD hardware security modules (HSMs) 587
- microsegmentation 240–241, 489–490
- microservices 236–240
- Microsoft
 - Active Directory (AD) 291–292
 - Azure 232–233, 603, 853
 - Cluster Server 488
 - Defender Antivirus 823–824
 - Disk Defragmenter 158
 - Exchange 145
 - Forefront Identity Manager 658
 - Internet Information Services (IIS) 146
 - MS-CHAP 670–671
 - security advisories and bulletins 179
 - Security Bulletins 146
 - SQL Server 273
 - Visual Basic for Applications (VBA) 113
 - Web Application Proxy 516

- Windows Defender Firewall 457
- Windows Server 144
- Mimikatz 90
- minimal privilege 681
- minimization, data 944–945
- mirroring 316, 318, 537–538
- mission-essential functions 929
- mitigation 919, 921. *See also* segmentation
 - configuration changes 824
 - certificates, updating/revoking 829–830
 - content filter/URL filter 828–829
 - data loss prevention (DLP) 828
 - firewall rules 825
 - mobile device management (MDM) 825–826
 - containment 763–764, 830–831
 - endpoint security solutions 822
 - application approved lists 822
 - application block list/deny list 822–823
 - approved lists 822
 - block/deny lists 467–468, 578, 583, 822–823
 - quarantine 823–824
 - isolation 830
 - Security Orchestration, Automation, and Response (SOAR) 188–189, 832
 - playbooks 834
 - runbooks 833
- MITRE Corporation 18, 458
 - ATT&CK framework 18, 128–129, 176, 205, 223, 767–768
 - Common Vulnerabilities and Exposures (CVE) 125, 146, 177
 - Common Weakness Enumeration 75
 - PRE-ATT&CK framework 18
- MMS (Multimedia Messaging Service) 583, 585
- mobile equipment identifiers (MEIDs) 49, 584
- mobile solutions
 - Common Vulnerabilities and Exposures (CVEs) 571
 - connection methods and receivers 570
 - Bluetooth 570–571
 - cellular 572–573
 - Global Positioning System (GPS) 572, 584
 - near-field communication (NFC) 570–571
 - radio frequency identification (RFID) 571–572
 - satellite communications (SATCOM) 573
 - secure implementation best practices 573–574
 - mobile application management (MAM) 585–587
 - mobile device management (MDM) 215, 574–576
 - application and content management 576–578
 - bring-your-own-device (BYOD) 572, 574–576, 581, 588–590, 826, 898
 - choose-your-own-device (CYOD) 588–590
 - corporate-owned, personally enabled (COPE) 572, 588–590
 - enforcement and monitoring 581–585
 - mobile application management (MAM) 585–587
 - SEAndroid 588
 - security concerns and countermeasures 578–581
 - unified endpoint management (UEM) 587–588
 - virtual desktop infrastructure (VDI) 589
- Modified, Accessed, Changed, and Birth (MACB) times 844

Modified Base Metrics 185
 moisture detection systems 382
 monitoring 537–538
 bandwidth 804
 continuous 139, 278
 file integrity monitors 542
 mobile device management (MDM) 581–585
 monitoring as a service (MaaS) 139, 232
 performance baselining 539–542
 motion detection 382, 869–870
 motion recognition 376
 MOU (memorandum of understanding) 903
 moves, MAC 511
 MSA (Measurement System Analysis) 904
 MS-CHAP 670–671
 MSPs (managed service providers) 233–234
 MSSPs (managed security service providers) 233–234
 MTBF (mean time between failures) 926
 MTTF (mean time to failure) 926
 MTTR (mean time to repair) 926
 MTU (maximum transmission unit)
 discovery 717
 multi-access edge computing (MEC) 235
 multicast addresses 537
 multifactor authentication (MFA) 304–306, 579, 656–657
 multifunction printers (MFPs) 354
 multihomed connections 532
 Multimedia Messaging Service (MMS) 583, 585
 Multi-Party Coordination and Disclosure
 special interest group 180
 multiparty risks 918
 multipath I/O 319
 multitenancy 601
 Multi-User Multiple Input (MU-MIMO) 560–561

Mutiny Fuzzing Framework 269
 mutual authentication 668–670
 MySQL 273

N

NAC (network access control) 510–511, 871. *See also* 802.1X standard
 name resolution 442–443
 naming conventions 213
 NarrowBand 358
 NarrowBand-Internet of Things (NB-IoT) 358
 NAS (network-attached storage) 326, 375
 NAT (network address translation) 443–444, 501, 529, 562
 Nation State attacks 346
 National Cyber Awareness System (NCAS) 576
 National Institute of Standards and Technology (NIST) 884
 cloud computing defined by 139
 Cybersecurity Framework (CSF) 884
 Digital Signature Algorithm (DSA) 396
 firewall guidelines 825
 isolation guidelines 830
 mobile device security guidelines 826
 National Vulnerability Database (NVD) 125, 177, 199
 NIST Cybersecurity Framework (CSF) 882
 Protecting Controlled Unclassified Information 828
 Risk Management Framework (RMF) 884
 National Security Agency (NSA) 55, 498
 National Vulnerability Database (NVD) 125, 177, 199
 NAT-T (NAT Traversal) 501
 NB-IoT (NarrowBand-Internet of Things) 358
 NCAS (National Cyber Awareness System) 576

- nCircle WebApp360 204
- NDA (nondisclosure agreement) 901
- near-field communication (NFC) 50, 100, 102–103, 570–571
- negatives, false 181, 519, 520
- Nessus 204, 730–731
- net time command 669
- netcat command 720–721
- NetFlow 187, 525, 809–810
- netstat command 668, 718–720
- NetStumbler 99
- network access control (NAC) 510–511, 871. *See also* 802.1X standard
- network ACLs (access control lists) 535
- network address translation (NAT) 443–444, 501, 529, 562
- network and port scanners 182
- network attached storage (NAS) 375
- network attacks. *See also* network design, secure
 - DDoS (distributed denial-of-service) 113
 - DNS (Domain Name System)
 - DDoS (distributed denial-of-service) 37–38, 54, 111–113, 601
 - DNS amplification attack 112
 - DNS poisoning 108–110
 - domain hijacking 108
 - domain name kiting 109–110
 - domain reputation 110–111
 - prevalence of 107
 - URL redirection attacks 110
 - Layer 2
 - ARP cache poisoning 105
 - MAC cloning attacks 106
 - MAC flooding attacks 106
 - security best practices 106–107
 - malware 113
 - backdoors 42–43
 - bots and botnets 37–38, 111–112
 - cryptomalware 33–34
 - definition of 33
 - delivery mechanisms 43–45
 - fileless viruses 37
 - keyloggers 42–43
 - logic bombs 39–40
 - permanent damage from 45
 - potentially unwanted programs (PUPs) 40–42
 - ransomware 33–34, 111–112
 - spyware 40–42
 - time bombs 39
 - Trojans 35–36, 104, 113
 - worms 36–37
 - on-path attacks 54, 84–85, 103, 602
 - password attacks
 - brute-force 45
 - dictionary-based 45
 - password cracking 46
 - password spraying 45
 - plaintext/unencrypted 47–48
 - rainbow tables 47
 - replay attacks 82–85
 - script execution 113
 - wireless 98
 - bluejacking 100
 - bluesnarfing 99–100
 - disassociation and deauthentication 101
 - evil twin 98–99
 - initialization vector (IV) 103
 - jamming 102, 561–562
 - near-field communication (NFC) 102–103
 - radio frequency identification (RFID) 49, 102
 - rogue access points 99
- network controllers 144
- network design, secure. *See also* firewalls; network attacks; network reconnaissance; network resilience
 - access control lists (ACLs) 535, 643, 831
 - broadcast storm prevention 512

- Bridge Protocol Data Unit (BPDU)
 - guard 512
- DHCP snooping 512–513
- loop protection 512
- MAC filtering 513
- DLP (data loss prevention) systems 215
- Domain Name System (DNS) 509–510
- load balancing
 - active/active 488
 - active/passive 488
 - definition of 488
 - scheduling 488
 - Virtual IP address 488
- monitoring services 538–539
 - file integrity monitors 542
 - performance baselining 539–542
- network access control (NAC) 510–511
- network appliances 513–514
 - aggregators 526
 - hardware security modules (HSMs) 524
 - jump servers 514
 - network intrusion detection systems (NIDSs) 215, 223, 517–524, 870. *See also* network reconnaissance
 - network intrusion prevention systems (NIPSs) 99, 519, 869
 - network-based intrusion prevention system (NIPS) 518–524
 - proxy servers 514–516
 - sensors 524–525
- network segmentation
 - application-based 489–490
 - east-west traffic 492
 - example of 489
 - extranets 492–493
 - intranets 492–493
 - microsegmentation 489–490
 - screened subnets 491
 - virtual local-area networks (VLANs) 490–491
 - zero trust 494
- out-of-band management 510–511
- port security 511, 537–538
- route security 535–536
 - IPv6 536–537
- port spanning/port mirroring 537–538
- quality of service (QoS) 536
- virtual private networks (VPNs) 507, 606
 - always-on VPN functionality 495
 - clientless versus client-based 497
 - concentrators 495
 - definition of 494
 - description of 494–496
 - example of 494–495
 - HTML5 508
 - IKEv1 Phase 1 negotiation 498–501
 - IKEv1 Phase 2 negotiation 501–503
 - IKEv2 504–505
 - IPsec 497
 - Layer 2 Tunneling Protocol (L2TP) 508
 - remote-access 496–497
 - site-to-site 495, 496–497
 - split tunneling 495–496
 - SSL (Secure Sockets Layer) 505–508
- network forensic analysis tools (NFATs) 852–853
- network interface card (NIC) teaming 320
- network intrusion detection systems (NIDSs) 99, 215, 223, 517–518, 870. *See also* network reconnaissance
 - advantages/disadvantages 519–520
 - anomaly-based analysis 521–523
 - definition of 519–520
 - heuristic-based analysis 521
 - inline versus passive 523–524
 - promiscuous mode 517
 - signature-based 519–520

- stateful pattern-matching recognition 521
- network intrusion prevention systems (NIPSs) 99, 519, 869
- network logs 790
- Network Policy Server (NPS) 495
- network reconnaissance 18, 770
 - active 204–205
 - definition of 707
 - dig 709–710
 - hping 717
 - ifconfig 710–711
 - ipconfig 710
 - netcat 720–721
 - netstat 718–720
 - nmap 711–714
 - nslookup 709–710
 - passive 203–204
 - pathping 716–717
 - ping 714–716
 - ping6 716
 - tracert/traceroute 707–709
- network resilience
 - definition of 319
 - load balancers 319–320
 - network interface card (NIC) teaming 320
- network segmentation. *See* segmentation
- Network Time Protocol (NTP) 112, 440, 490, 790
- Network Time Security (NTS) 440
- network video recorders (NVRs) 375
- network-attached storage (NAS) 326
- network-based application layer firewalls 530
- New Technology File System (NTFS) 156, 646, 850. *See also* permissions
- Nexpose 204
- next-generation firewall (NGFW) 453–454, 524
- next-generation IPS systems (NGIPSs) 523
- NFATs (network forensic analysis tools) 852–853
- NFC (near-field communication) 50, 570–571
- NFC (near-field communication) attacks 102–103
- NGFW (next-generation firewall) 453–454, 524
- nginx 236, 794
- NGIPSs (next-generation IPS systems) 523
- NIC (network interface card) teaming 320
- NIDSs (network intrusion detection systems) 99, 215, 223, 517–518, 869, 870. *See also* network reconnaissance
 - advantages/disadvantages 519–520
 - anomaly-based analysis 521–523
 - definition of 519–520
 - heuristic-based analysis 521
 - inline versus passive 523–524
 - promiscuous mode 517
 - signature-based 519–520
 - stateful pattern-matching recognition 521
- Nikto 204
- Nimda 37
- NIPSs (network intrusion prevention systems) 99, 523, 869
 - advantages/disadvantages 519–520
 - anomaly-based analysis 521–523
 - definition of 518–520
 - false positives/false negatives 519
 - heuristic-based analysis 521
 - inline versus passive 523–524
 - signature-based 520–521
- NIST (National Institute of Standards and Technology) 396, 881
- Nmap 204, 527, 711–714
- noise detection 382
- Nomad 240

- nonces 82–83, 500
 - noncredentialed vulnerability scans 182
 - nondisclosure agreements (NDAs) 901
 - nonintrusive vulnerability scanners 182
 - non-persistence 328–329
 - nonrepudiation 859–860
 - normalization 186, 273–274
 - NoSQL databases 273–274
 - notifications
 - of privacy and data breaches 941
 - public 940
 - push 299
 - Novec 1230 381
 - NPS (Network Policy Server) 495
 - NSA (National Security Agency) 55, 498
 - nslookup command 709–710
 - NT LAN Manager (NTLM) 89
 - NTFS (New Technology File System)
 - 156, 646, 850. *See also* permissions
 - NTLM (NT LAN Manager) 89
 - NTP (Network Time Protocol) 112, 440, 490
 - NTS (Network Time Security) 440
 - Nucleus RTOS 347
 - null pointer dereferences 75, 271–272
 - NVD (National Vulnerability Database)
 - 125, 177, 199
 - NVRs (network video recorders) 375
 - NXLog 803–804
- O**
- Oakley 497
 - OAS (OpenAPI Specification) 87
 - OAuth 292, 578, 661–662
 - obfuscation 79, 265, 770
 - object detection 376
 - object identifiers (OIDs) 691
 - OCIL (Open Checklist Interactive Language) 885
 - OCSP (Online Certificate Status Protocol) 691, 698
 - OEM (original equipment manufacturer) 459
 - OFB (Output Feedback) mode 407
 - offboarding policies 575, 899, 900
 - Office of Personnel Management (OPM)
 - attack 300–301
 - offline backups 326
 - offline password cracking 46
 - off-premises services 234
 - offsite storage 327
 - Off-The-Record Messaging 400–401
 - OIDC (OpenID Connect) 663–664
 - OIDs (object identifiers) 691
 - OLDPWD environment variable 740
 - onboarding policies 575, 899, 900
 - one-time passwords (OTPs) 627
 - HMAC-based 295–296
 - time-based 295
 - one-to-one mapping 690
 - one-way functions 219
 - online backups 326
 - Online Certificate Status Protocol (OCSP) 691, 698
 - online password cracking 46
 - on-path (man-in-the-middle) attacks 54, 84–85, 103, 602
 - on-premises environments, vulnerabilities
 - in 137–143
 - on-premises services 234
 - Opal 476
 - Open Checklist Interactive Language (OCIL) 885
 - Open Network Environment 882
 - open permissions 150
 - open ports/services 471–472
 - Open Source Security Testing
 - Methodology Manual (OSSTMM) 199
 - Open Systems Interconnection (OSI)
 - model 103, 614, 615
 - Open vSwitch Database Management Protocol (OVSDB) 243

- Open vSwitch (OVS) 243
- Open Vulnerability and Assessment Language (OVAL) 164, 885
- Open Web Application Security Project. *See* OWASP (Open Web Application Security Project)
- OpenIX 554
- OpenAPI Specification (OAS) 87
- OpenCv 416
- OpenDNS 509–510
- OpenFlow 243, 882
- OpenID 663–664
- open-source intelligence (OSINT) 7–8, 18, 120–121, 124, 203
- OpenSSL 236, 741–742
- OPENSSL_CONF environment variable 740
- operating systems (OSs)
 - forensic acquisition 850
 - hardening 473–474
 - trusted operating systems (TOSs) 905
- operation, modes of (encryption)
 - authenticated 404
 - Cipher Block Chaining (CBC) 405
 - Cipher Feedback (CFB) 406
 - Counter (CTR) 404, 408–409
 - Electronic Code Book (ECB) 404
 - Output Feedback (OFB) 407
 - unauthenticated 404
- operational controls 868, 869
- operational expenditure (OpEx) 598
- operational technology (OT) 113
- The Orange Book 674
- order of volatility 848
- organization attribute (certificates) 692
- organizational incidents 775
- organizational security. *See also* forensics, digital; incident response (IR) plans
 - benchmarks and secure configuration guides 885–888
 - data sanitization 748–749
 - exploitation frameworks 747–748
 - file manipulation 732–733
 - cat command 734–735
 - chmod command 736–737
 - grep command 735–736
 - head command 733
 - logger command 737–738
 - tail command 734
 - IP scanners
 - arp command 721–722
 - Cuckoo 731–732
 - curl command 724–725
 - definition of 721
 - dnsenum 728–729
 - Nessus 730–731
 - route command 723–724
 - scanless 727–728
 - sn1per 726–727
 - theHarvester 725–726
 - IT security frameworks 881–884
 - network reconnaissance
 - definition of 707
 - dig 709–710
 - hping 717
 - ifconfig 710–711
 - ipconfig 710
 - netcat 720–721
 - netstat 718–720
 - nmap 711–714
 - nslookup 709–710
 - pathping 716–717
 - ping 714–716
 - ping6 716
 - tracert/traceroute 707–709
 - packet capture and replay
 - definition of 742
 - Tcpdump 742–743

- Tcpreplay 742
- Wireshark 743
- password crackers 748–749
- policies
 - acceptable use 898, 900
 - asset management 909–910
 - breadth and scope of 897
 - change management/change control 909
 - classification and governance 904–905
 - clean desk policy 23, 899, 900
 - credential 906–908
 - data retention 906
 - definition of 893
 - due care 900
 - due diligence 900
 - due process 900
 - job rotation 898, 900
 - mandatory vacations 898–899, 900
 - onboarding/offboarding 899, 900
 - privacy 897
 - procedures versus 893
 - separation of duties 898, 900
 - user education and awareness training 901–902
- privacy and data breach consequences
 - data types and asset classification 941–942
 - fines 940
 - identity theft 940
 - impact assessment 948
 - information lifecycle 947–948
 - intellectual property theft 940
 - notifications 941
 - personally identifiable information (PII) 943
 - privacy enhancing technologies 944–945
 - privacy notices 949
 - protected health information (PHI) 944
 - reputation damage 940
 - security roles and responsibilities 945–947
 - terms of agreement 948
- regulations and standards
 - company policies 878–879
 - General Data Protection Regulation (GDPR) 214, 220, 878–879, 947
 - laws 879–880
 - Payment Card Industry Data Security Standard (PCI DSS) 881
- shell and script environments
 - definition of 738–740
 - OpenSSL 741–742
 - PowerShell 740
 - Python 741
 - Secure Shell (SSH) 739–740
- organizational units (OUs) 692
- organizational validation (OV) certificates 694
- organized crime 120
- original equipment manufacturer (OEM) 459
- orthogonal frequency-division multiple access (OFDMA) 561
- OSI (Open Systems Interconnection)
 - model 103, 614, 615
- OSINT (open-source intelligence) 7–8, 18, 120–121, 124, 203
- OSSTMM (Open Source Security Testing Methodology Manual) 199
- OT (operational technology) 113
- OTA (over-the-air) technology 572–573, 583, 585
- OTPs. *See* one-time passwords (OTPs)
- out-of-band management 510–511
- out-of-band SQL injection 73
- Output Feedback (OFB) mode 407
- outsourced code development 155
- OV (organizational validation) certificates 694

- Password Authentication Protocol (PAP) 670–671
 - password keys 655
 - password vaults 655
 - policies 906–907
 - system-generated 638
 - time-based one-time password (TOTP) 295
 - user-generated 638
- Pastebin 18
- patches and hotfixes 160–164, 179–180, 362, 474–475
- PATH environment variable 740
- pathing command 716–717
- pattern-matching, stateful 521
- payment methods, mobile 584, 586
- PCI DSS (Payment Card Industry Data Security Standard) 453, 881
- PDS (protective distribution system) 385
- PDU's (power distribution units) 322–323
- Peach 270
- PEAP (Protected Extensible Authentication Protocol) 554, 556, 666
- Pearson Test Prep practice test 954
- peer to peer (P2P) networks 143
- PEM (Privacy-enhanced Electronic Mail) 697
- .pem file extension 697
- penetration testing 121, 266
 - active reconnaissance 204–205
 - advantages of 197–198
 - bug bounties versus 202–203
 - cleanup 202
 - definition of 193, 197
 - exercise types 205–206
 - known environment 198
 - lifecycle 199–202
 - methodologies 199
 - partially known environment 199
 - passive reconnaissance 203–204
 - post-exploitation techniques 201
 - unknown environment 198–199
- Penetration Testing Execution Standard (PTES) 199
- Perfect Forward Secrecy (PFS) 399–400, 502
- performance baselining 539–542
- Performance Monitor tool 540–542
- Performance tool 539
- permissions 640–645
 - cloud computing 605, 610
 - inheritance 644–646
 - open 150
 - privilege creep 645
 - types of 646
- persistence 201
- personal area networks (PANs) 570
- personal firewalls 534
- personal identification numbers (PINs) 360, 579
- Personal Identity Verification (PIV) cards 629
- Personal Information Protection and Electronic Documents Act (PIPEDA) 220, 880
- personal unblocking keys (PUKs) 360
- personally identifiable information (PII) 82, 216–218, 268, 577, 856, 897, 901, 943
- person-made disasters 924
- personnel policies 377–378
 - acceptable use 898, 900
 - breadth and scope of 897
 - clean desk policy 23, 899, 900
 - data retention 906
 - definition of 893
 - due care 900
 - due diligence 900
 - due process 900
 - job rotation 898, 900
 - mandatory vacations 898–899, 900
 - onboarding/offboarding 575, 899, 900
 - personnel credential policy 906–908

- privacy 897
- procedures versus 893
- separation of duties 898, 900
- summary of 900
- PFS (Perfect Forward Secrecy) 399–400, 502
- pharming 14–15, 109
- PHI (protected health information) 856, 944
- phishing 9–12, 902
- phone call authentication 299–300
- physical controls 871–872
- physical security 872
 - access control vestibules 372–373
 - air gap 384
 - alarms 374
 - attacks
 - card cloning 48–49
 - cloud-based attacks 52–55, 601–603
 - malicious flash drives 48
 - malicious USB cables 48
 - skimming 49–50
 - supply-chain attacks 51
 - badges 373, 382
 - bollards/barricades 370–371
 - cameras
 - centralized versus decentralized 375
 - closed-circuit television (CCTV) 376–377
 - motion recognition 376
 - object detection 376
 - drones 382–383
 - Faraday cages 383–384
 - fencing 380–381
 - fire suppression 381
 - industrial camouflage 377
 - lighting 380
 - locks 378–379
 - personnel 377–378
 - physical locks 379
 - protected cable distribution system 385
 - screened subnets 384
 - secure areas 385–386
 - secure data destruction 386–387
 - sensors 381–382
 - signage 374–375
 - USB data blockers 379–380
 - visitor logs 383
- PIA (Privacy Impact Assessments) 948
- piggybacking 15
- PII (personally identifiable information) 82, 216–218, 268, 577, 856, 897, 901, 943
- ping command 714–716
- Ping of Death 88
- ping6 command 716
- PINs (personal identification numbers) 360, 579
- PIPEDA (Personal Information Protection and Electronic Documents Act) 220, 880
- PIR (Post Incident Review) 764–765
- PIV (Personal Identity Verification) cards 629
- pivoting 201
- PKCS (Public Key Cryptography Standards) 412
- PKI (public key infrastructure) 84–85, 556
 - certificate authorities (CAs) 556, 689–691, 829
 - certificates
 - attributes 691–692
 - chaining 696
 - expiration 693
 - formats 697
 - pinning 698
 - Subject Alternative Name 693
 - types of 694–696
 - definition of 685
 - key escrow 699
 - key management 688

- key recovery agent 699
- stapling 698
- trust model 698
- PKIX (Public Key Infrastructure Exchange) 694
- plaintext 47–48
- plans
 - business continuity 773–774, 929
 - communication 771–772
 - disaster recovery 772–773, 926
 - incident response (IR)
 - business continuity plans (BCPs) 773–774, 929
 - communication plans 771–772
 - continuity of operations planning (COOP) 774–775
 - cyber kill chain 770–771
 - data retention policies 775–776
 - definition of 760–761
 - Diamond Model of Intrusion Analysis 768–770
 - disaster recovery plans (DRPs) 772–773, 926
 - exercises 765–767
 - incident response teams 760, 775–776
 - MITRE ATT&CK framework 128–129, 176, 205, 223, 767–768
 - process and lifecycle 761–765
 - stakeholder management 771–772
- platform as a service (PaaS) 139, 232, 853
- platform configuration registers (PCRs) 294
- playbooks 834
- PLCs (programmable logic controllers) 341, 343
- pluggable authentication modules (PAMs) 670
- PlugX RAT 35
- PMBOK (Project Management Body of Knowledge) 882
- PNAC. *See* 802.1X standard
- pointer dereferencing 75–76, 271–272
- point-of-sale (POS) systems 353
- Point-to-Point Tunneling Protocol (PPTP) 494, 558
- poisoning
 - ARP (Address Resolution Protocol) 105, 722
 - DNS (Domain Name System) 108–110
- policies 878–879
 - account 633
 - asset management 909–910
 - change management/change control 909
 - classification and governance 904–905
 - credential 906–908
 - data retention 775–776, 906
 - definition of 893
 - group policy objects (GPOs) 474
 - Identity and Access Management (IAM) 605
- personnel
 - acceptable use 898, 900
 - breadth and scope of 897
 - clean desk policy 23, 899, 900
 - due care 900
 - due diligence 900
 - due process 900
 - job rotation 898, 900
 - mandatory vacations 898–899, 900
 - onboarding/offboarding 575, 899, 900
 - personnel credential policy 906–908
 - privacy 897
 - separation of duties 898, 900
 - summary of 900
- procedures versus 893
- resource 246, 603, 609
- user education and awareness training 901–902
- POP (Post Office Protocol) 438–439

- port security 106, 511. *See also* 802.1X
 - standard
 - open ports 471–472
 - port numbers 441
 - port spanning/port mirroring 537–538
 - port taps 538
 - port-based network access control (PNAC) 553–554
 - protocols associated with 152–154
 - Switched Port Analyzer (SPAN) 537–538
 - vulnerabilities 151
- portals, captive 559
- PortSwigger Burp Suite Professional 204
- POS (point-of-sale) systems 353
- positives, true/false 181–182, 518, 520
- POST (power-on self-test) 851
- Post Incident Review (PIR) 764–765
- Post Office Protocol (POP) 438–439
- post-exploitation techniques 201
- post-quantum cryptography 402
- potentially unwanted programs (PUPs) 40–42
- power distribution units (PDUs) 322–323
- power loss 925
- power resilience
 - definition of 320
 - dual supply 321–322
 - generators 321
 - managed power distribution units (PDUs) 322–323
 - uninterruptible power source (UPS) 320–321
- power-on self-test (POST) 851
- PowerShell 113, 630, 740
- PPTP (Point-to-Point Tunneling Protocol) 494, 558
- PRE-ATT&CK 18
- predictive analysis 127
- preferred roaming list (PRL) 572
- PREMIS (Preservation Metadata Implementation Strategies) 805
- preparation phase, incident response (IR) 762–763
- prepending 17
- preservation, forensic 858
- Preservation Metadata Implementation Strategies (PREMIS) 805
- preshared key (PSK) 103, 551, 557–558
- pretexting 19
- preventative controls 869, 872
- principals 623
- printenv command 739
- Privacy Act of 1974 879, 897
- privacy breaches 220. *See also* identity
 - data types and asset classification 941–942
 - fines 940
 - identity theft 940
 - impact assessment 948
 - information lifecycle 947–948
 - intellectual property theft 940
 - notifications of 941
 - personally identifiable information (PII) 943
 - privacy enhancing technologies 944–945
 - privacy notices 949
 - privacy policies 897
 - protected health information (PHI) 944
 - reputation damage from 940
 - security roles and responsibilities 945–947
 - terms of agreement 948
- privacy enhancing technologies 944–945
- Privacy Impact Assessments (PIA) 948
- Privacy-enhanced Electronic Mail (PEM) 697
- private cloud 140, 232–233

- Private information 942
- private information sharing centers 124
- private keys 436
- private subnets 606, 610
- privilege
 - creep 645
 - escalation 67–68, 201, 770, 941
 - least 681
 - minimal 681
 - provisioning 635
- privileged access management (PAM) 678, 679
- Privileges Required (PR) metric 183
- PRNG (pseudorandom number generator) 49–50, 102, 571–572
- procedures, policies versus 879, 893
- production 260
- Programmable Attribute Maps (PAMs) 851
- programmable logic controllers (PLCs) 341, 343
- programming testing methods
 - compile-time errors 266–267
 - fuzz testing 269–270
 - input validation 80, 267–268
 - penetration testing 266
 - runtime errors 266–267
 - static and dynamic code analysis 269
 - stress testing 80, 266
- programming vulnerabilities. *See* vulnerabilities
- Project Management Body of Knowledge (PMBOK) 882
- promiscuous mode 517
- promiscuous ports 491
- Proprietary information 942
- protected cable distribution system 385
- Protected Extensible Authentication Protocol (PEAP) 554, 556, 666
- protected health information (PHI) 856, 944
- protective distribution system (PDS) 385
- protocol analyzers 813
- protocols. *See individual protocols*
- provenance, forensic 857–858
- provisioning, application 260
- proximity readers 373, 382
- proxy autoconfiguration (PAC) file 515
- proxy servers 514–516
 - forward proxy 516
 - reverse proxy 506–507, 516
 - transparent proxy 516
- PSEs (packet-switching exchanges) 137–138
- pseudo-anonymization 945
- pseudocodes 79
- pseudorandom number generator (PRNG) 49–50, 102, 571–572
- PSK (preshared key) 103, 551, 557–558
- PTES (Penetration Testing Execution Standard) 199
- public cloud 140, 232
- public incidents 775
- public information 905
- public information sharing centers 124
- public key algorithms 411
- Public Key Cryptography Standards (PKCS) 412
- public key infrastructure. *See* PKI (public key infrastructure)
- Public Key Infrastructure Exchange (PKIX) 694
- public keys 437
- public ledgers 409–410
- public notifications and disclosures 941
- public subnets 606, 610
- PUKs (personal unblocking keys) 360
- pulping 386
- pulverizing 387
- PUPs (potentially unwanted programs) 40–42
- purple team 205–206
- push notifications 299
- PWD environment variable 740
- Python 113, 741

Q

QKD (quantum key distribution)
401–402

QoS (quality of service) 536

QRadar 526

qualitative risk management 921–922,
923

qualitative-to-quantitative score mapping
186

quality assurance (QA) 260, 261

quality of service (QoS) 536

Qualys 204

quantitative risk management 922–923

quantum cryptography 401–402
communications 401–402
computing 402
definition of 401

quantum key distribution (QKD)
401–402

quarantine 823–824

quick mode, IKE 501

R

race conditions 79

Radamsa 269

radio, baseband 359

radio frequency identification (RFID)
attacks 49, 102, 571–572

radio frequency interference (RFI)
383–384

RADIUS (Remote Authentication
Dial-In User Service) 556–557,
672–673

RAID (Redundant Array of Inexpensive
Disks) 315–316, 869

Rainbow Series 674

rainbow tables 47

RainbowCrack 47

RAM (random-access memory), forensic
acquisition of 848–849

ransomware 33–34, 111–112

rapid application development (RAD) 262

Rapid STP 512

Rapid7 Nexpose 204

RAs (registration authorities) 690

RAS (Remote Access Service) 670–672

Raspberry Pi 339

RATs (remote access Trojans) 148

RBAC (role-based access control) 677,
679, 899

RC4 (Rivest Cipher 4) 412

RCE (remote code execution) 78, 146,
149, 275

RCS (Rich Communication Services) 585

RCSA (risk control self-assessment) 920

RDBMS (relational database management
system) 273

RDP (Remote Desktop Protocol) 472

readers, proximity 373, 382

Real-Time Monitoring Tool (RTMT)
799

real-time operating systems (RTOSs) 347,
355

Real-Time Transport Protocol (RTP)
152. *See also* Secure Real-Time
Transport Protocol (SRTP)

reception desks 378

recertification, user access 645

reconnaissance. *See* network
reconnaissance

Recon-ng 203

recovery 764, 859
disaster recovery planning 928–930
recovery point objective (RPO) 929
recovery time objective (RTO) 929
restoration order 330–331

Red Hat security advisories and bulletins
179

red teams 205, 902

redaction 945

redirection attacks, URL 110

reduced sign-on 656

redundancy 926–927
definition of 315

- disk
 - definition of 315–316
 - multipath 319
 - Redundant Array of Inexpensive Disks (RAID) 315–316
- diversity of 331–332
- geographic dispersal 315
- network
 - definition of 319
 - load balancers 319–320
 - network interface card (NIC)
 - teaming 320
- power
 - definition of 320
 - dual supply 321–322
 - generators 321
 - managed power distribution units (PDUs) 322–323
 - uninterruptible power source (UPS) 320–321
- Redundant Array of Inexpensive Disks (RAID) 315–316, 869
- refactoring, driver 89
- reference architecture 884
- Reflected XSS attacks 68
- reflection 112
- regedit command 472
- registers, risk 920
- registration, identity 633–635
- registration authorities (RAs) 690
- registry 472
- regulations and standards
 - company policies 878–879
 - General Data Protection Regulation (GDPR) 214, 220, 878–879, 947
 - laws 879–880
 - Payment Card Industry Data Security Standard (PCI DSS) 881
- regulatory forensic intervention 855
- relational database management system (RDBMS) 273
- Reliable Event Logging Protocol (RELP) 800
- relying parties (SAML) 659
- Remediation Level (RL) metric 185
- remote access 442
 - Remote Access Service (RAS) 670–672
- remote access Trojans (RATs) 148
- remote-access VPNs 496–497
- remote authentication
 - Challenge-Handshake Authentication Protocol (CHAP) 670–672, 673
 - RADIUS 556–557, 672–673
 - Remote Access Service (RAS) 670–672
 - TACACS+ 672–673
- Remote Authentication Dial-In User Service (RADIUS) 556–557, 672–673
- remote code execution (RCE) 78, 146, 149, 275
- Remote Desktop Connection 152
- Remote Desktop Protocol (RDP) 472
- remote terminal units (RTUs) 341
- remote wipe 579, 582
- remotely operated underwater vehicles (ROVs) 353–354
- removable media 123
- replay, packet
 - definition of 742
 - replay attacks 82–85
 - Tcpdump 742–743
 - Tcpreplay 742
 - Wireshark 743
- replication
 - cloud computing 605, 610
 - storage area networks (SANs) 323
 - virtual machines (VMs) 324–325
 - escape attacks 248–249
 - sprawl avoidance 247–248
- Report Confidence (RC) metric 185
- reports
 - after action report (AAR) 928–929
 - baseline 539–542

- forensic 846
- SIEM (Security Information and Event Management) 187
- repositories, file/code 127
- Representational State Transfer (REST) 86
- reputation 110–111, 940
- request for comments (RFC) 128
- request forgeries 85–86
- residual risk 919, 921
- resilience 221–222
 - backups
 - cloud 326
 - comparison of 326–327
 - copy 326
 - differential 326, 328
 - disk 326
 - full 326, 328–331
 - image 326
 - incremental 326, 328
 - NAS (network-attached storage) 326
 - offsite storage 327
 - online versus offline 326
 - snapshot 326
 - tape 326
 - definition of 311
 - high availability (HA) 329–330
 - network
 - definition of 319
 - load balancers 319–320
 - network interface card (NIC) teaming 320
 - non-persistence 328–329
 - power
 - definition of 320
 - dual supply 321–322
 - generators 321
 - managed power distribution units (PDUs) 322–323
 - uninterruptible power source (UPS) 320–321
 - on-premises versus cloud 325
- redundancy
 - definition of 315
 - disk 315–319
 - diversity of 331–332
 - geographic dispersal 315
 - network 319–320
 - power 320–323
 - Redundant Array of Inexpensive Disks (RAID) 315–316, 869
- replication
 - storage area networks (SANs) 323
 - virtual machines (VMs) 247–249, 324–325
 - restoration order 330–331
 - scalability 279–280, 328
- resolution, domain name 442–443
- resource allocation, dynamic 607–608, 611
- resource exhaustion 87–88
- resource policies 246, 603, 609
- resource records (RRs) 795
- response and recovery controls 220–221
- REST (Representational State Transfer) 86
- RESTful APIs 240
- restoration 158, 330–331
- retention, risk 919
- retention policies 775–776, 906
- retina scanning 301
- Retina Web Security Scanner 204
- reuse, code 270
- reverse proxy 506–507, 516
- revert to known state 329
- review, exam 953–954
- review logs 182
- reviews, configuration 182
- revoking certificates 829
- RFC (request for comments) 128
- RFI (radio frequency interference) 383–384

- RFID (radio frequency identification) attacks 49, 102, 571–572
- Rich Communication Services (RCS) 583, 585
- riding, session 602
- rights management 219–220, 640–645
- right-to-audit clauses 854
- Rijndael. *See* Advanced Encryption Standard (AES)
- risk management 155, 913
 - business impact analysis 926–927
 - disaster analysis 924–925
 - disaster recovery planning 928–930
 - external versus internal risk 917
 - residual risk 919
 - risk assessment 919–921
 - control risk 921
 - inherent risk 921
 - qualitative 921–922, 923
 - quantitative 922–923
 - residual risk 921
 - risk appetite 921
 - risk awareness 921
 - risk control assessment 920
 - risk control self-assessment (RCSA) 920
 - risk matrix/heat map 920
 - risk mitigation 921
 - steps of 919–920
 - risk avoidance 918
- Risk Management Framework (RMF) 884
- risk matrix/heat map 920
- risk mitigation 919
- risk registers 920
- risk transference 918
- risk types 917–918
- strategies for 918–919
- supply chain risk management (SCRM) 920
- third-party risks 155–160
- risky login 639
- RMF (Risk Management Framework) 884
- robot sentries 378
- rogue access points 99
- role-based access control (RBAC) 677, 679, 899
- role-based training 902
- roles and responsibilities, security 945–947
- rolling codes 102
- root accounts 150, 908
- root certificate authorities 696
- root certificates 696
- root of trust 476–477
- route command 723–724
- route security 443, 535–536
 - IPv6 536–537
 - port spanning/port mirroring 537–538
 - quality of service (QoS) 536
- Routing and Remote Access Service (RRAS) 495
- ROVs (remotely operated underwater vehicles) 353–354
- RPO (recover point objective) 929
- RRAS (Routing and Remote Access Service) 495
- RRs (resource records) 795
- RSA 412
- rsyslog 800–801
- RTMT (Real-Time Monitoring Tool) 799
- RTO (recovery time objective) 929
- RTOSs (real-time operating systems) 347, 355
- RTP (Real-Time Transport Protocol) 152. *See also* Secure Real-Time Transport Protocol (SRTP)
- RTUs (remote terminal units) 341, 343
- rule-based access control 677, 678, 679
- runbooks 833
- runtime errors 81–82, 266–267
- runtime memory 477

S

- SaaS (software as a service) 138, 231, 444, 853
- SAE (Simultaneous Authentication of Equals) 101, 551, 552
- safes 385
- salting 47, 82, 397–398, 462–463
- SAM (Security Accounts Manager) 89
- SAML (Security Assertion Markup Language) 659–661
- Samsung 476
- SAN (Subject Alternative Name) field 694–695
- sandboxing 266, 452, 478–479
- sanitization, data 748–749
- sanitizing mobile devices 579
- SANs (storage-area networks) 142, 323
- Santos, Omar 953
- Sarbanes–Oxley (SOX) 880, 882
- SASE (Secure Access Service Edge) 582
- SAST (static application security testing) 468–469
- SATCOM (satellite communications) 573
- SCADA (supervisory control and data acquisition) systems 341–343
- scalability 279–280, 328
- scanless 727–728
- scans
 - biometric. *See* biometric systems
 - IP scanners
 - arp command 721–722
 - Cuckoo 731–732
 - curl command 724–725
 - definition of 721
 - dnsenum 728–729
 - Nessus 730–731
 - route command 723–724
 - scanless 727–728
 - sn1per 726–727
 - theHarvester 725–726
 - vulnerability 785–786
- Common Vulnerability Scoring System (CVSS) 182–186
 - false negative 181
 - false positives 181
 - how it works 180–181
 - intrusive versus nonintrusive 182
 - noncredentialed 182
- SCAP (Security Content Automation Protocol) 883, 885–888
- scheduling algorithms 488
- SCP (secure copy) 456
- screen locks 579
- screened subnets 384, 491
- script environments 278–279
 - definition of 738–740
 - OpenSSL 741–742
 - PowerShell 740
 - Python 741
 - Secure Shell (SSH) 739–740
- script kiddies 120
- SCRM (supply chain risk management) 166, 920
- Scrum 258
- SDLC (software development lifecycle) 78, 261–262, 263–265, 468, 868
- SDN (software-defined networking) 241–243, 882
- SDV (software-defined visibility) 243
- SD-WAN (software-defined wide-area network) 246
- Seagate Technology 476
- SEAndroid 588
- search engine optimization (SEO) 808
- SEC (Securities and Exchange Commission) 941
- SECaaS (security as a service) 139
- secrecy, forward 400–401
- Secret information 905, 941–942
- Secret Manager 604
- secrets management 604, 609
- Secure Access Service Edge (SASE) 582
- secure areas 385–386

- secure copy (SCP) 456
- Secure File Transfer Protocol (SFTP) 434, 441
- Secure Hash Algorithm (SHA) 55, 463, 551–552
- Secure Key Exchange Mechanism (SKEME) 497
- secure protocols. *See also individual protocols*
 - definition of 426
 - use cases
 - directory services 442
 - domain name resolution 442–443
 - email and web 440
 - file transfer 441
 - network address allocation 443–444
 - remote access 442
 - routing and switching 443
 - subscription services 444
 - time synchronization 440
 - voice and video 440
- Secure Real-Time Transport Protocol (SRTP) 152, 430–431
- Secure Shell (SSH) 427–428, 625, 628, 739–740
- Secure Sockets Layer (SSL) 82–83, 436, 441
 - certificate types 694–696
 - SSL-based VPNs 505–508
 - Transport Layer Security Inspection (TLSI) 215–216
- Secure Web Gateway (SWG) 613, 614
- Secure/Multipurpose Internet Mail Extensions (S/MIME) 428–429
- Securities and Exchange Commission (SEC) 941
- Security Accounts Manager (SAM) 89
- security administrators 947
- security as a service (SECaaS) 139
- Security Assertion Markup Language (SAML) 292, 659–661
- security assessments. *See also* SIEM (Security Information and Event Management)
 - in cloud 598
 - attacks 601–603
 - threats 598–600
 - risk 919–921
 - control risk 921
 - inherent risk 921
 - qualitative 921–922, 923
 - quantitative 922–923
 - residual risk 921
 - risk appetite 921
 - risk awareness 921
 - risk control assessment 920
 - risk control self-assessment (RCSA) 920
 - risk matrix/heat map 920
 - risk mitigation 921
 - steps of 919–920
- security advisories and bulletins 177–180
- Security Orchestration, Automation, and Response (SOAR) 188–189, 832
- threat hunting 175–180
- vulnerability scans
 - credentialed versus noncredentialed 182
 - false negatives 181
 - false positives 181
 - how it works 180–181
 - intrusive versus nonintrusive 182
- Security Content Automation Protocol (SCAP) 883, 885–888
- security controls
 - cloud
 - API inspection and integration 607, 610
 - compute 611
 - high availability across zones 603, 609

- integration and auditing 604, 609
 - network 606–607, 610
 - resource policies 603, 609
 - secrets management 604, 609
 - storage 605, 610
- cloud computing
 - compute 607
 - container security 608–609
 - dynamic resource allocation 607–608, 611
 - instance awareness 608, 611
 - native versus third-party 615
 - security groups 607, 611
 - security solutions 611–614
 - summary of 608–609
 - virtual private cloud endpoint 608, 611
- security incident response simulations (SIRS) 766–767
- security incident response team (SIRT). *See* incident response (IR) teams
- Security Information and Event Management. *See* SIEM (Security Information and Event Management)
- security logs 383, 793
- security officers 947
- Security Onion 953
- security operations centers (SOCs) 123, 175–176, 223, 379, 760, 762, 776
- Security Orchestration, Automation, and Response (SOAR) 188–189, 832
 - playbooks 834
 - runbooks 833
- security posture assessments (SPAs) 539
- Security Requirements metrics 185
- Security-Enhanced Linux (SELinux) 588, 676
- SEDs (self-encrypting drives) 475–476
- segmentation 607, 610, 831–832
 - application-based 489–490
 - in cloud 613, 615
 - east-west traffic 492
 - example of 489
 - extranets 492–493
 - intranets 492–493
 - microsegmentation 489–490
 - screened subnets 491
 - virtual local-area networks (VLANs) 490–491
 - zero trust 494
- Segmented Integer Counter Mode (SRTP) 430
- SEH (structured exception handling) 81, 267
- SELECT statement 70
- self-encrypting drives (SEDs) 475–476
- self-signed certificates 695, 698
- SELinux (Security-Enhanced Linux) 588
- semi-authorized hackers 121
- semicolon (;) 73
- Sender Policy Framework (SPF) 110, 426
- sensitive data exposure 82
- Sensitive information 942
- sensors 345, 381–382, 524–525, 787
- sentiment analysis 188
- Sentinel 204
- SEO (search engine optimization) 808
- separation of duties 898, 900
- serial numbers, certificate 692
- serverless architecture 243–244
- servers 144
 - authentication 665
 - command-and-control [C2] 108
 - email 145
 - file 144
 - FTP 147–148
 - hardening 159–160
 - jump 514
 - Microsoft Cluster Server 488
 - network controllers 144
 - Network Time Protocol (NTP) 490
 - proxy 514–516
 - forward proxy 516

- reverse proxy 506–507, 516
- transparent proxy 516
- virtual network computing (VNC) 632
- web
 - log files 794
 - vulnerabilities 146–147
- server-side execution 267
- server-side request forgery (SSRF) 85–86
- server-side validation 268
- service accounts 629, 908
- service nxlog start command 803
- service providers (SPs) 292, 623, 661
- service set identifiers (SSIDs) 98, 205, 532
- service-level agreements (SLAs) 53, 273–274, 600, 902–903
- services, open 471–472
- services integration 246
- session hijacking 54, 83, 465, 601
- Session Initiation Protocol (SIP) 351, 431, 800
- session replay 83
- session riding 54, 602
- session theft 83
- SET (Social Engineering Toolkit) 10
- SFC (System File Checker) command 158
- sFlow 810–811
- SFTP (Secure File Transfer Protocol) 434, 441
- SHA (Secure Hash Algorithm) 55, 551–552
- shadow IT 121
- share permissions 646. *See also* permissions
- shared accounts 629
- shell and script environments
 - definition of 738–740
 - OpenSSL 741–742
 - PowerShell 740
 - Python 741
 - Secure Shell (SSH) 739–740
 - SHELL environment variable 740
- shielding, application 471
- shimming, driver 89
- Shodan 203–204
- Shor's algorithm 402
- Short Message Service (SMS) 12, 296–297, 583, 585
- shoulder surfing 14
- shredding 386
- side-channel attacks 54, 602
- sideloading 581
- SIEM (Security Information and Event Management) 186–188, 526, 869–870
 - alerts 788
 - correlation 788–789
 - dashboards 786–789
 - sensitivity 788
 - sensors 787
 - trends 788
- SIFT workstation 850
- signage 374–375
- signatures, digital 395–396, 466–467, 520
 - signature verifying algorithms 395
 - signature-based intrusion detection 519–520
 - signing algorithms 395
- SIM (subscriber identity module) cards 49, 360, 580, 584
- Simple Network Management Protocol version 3 (SNMPv3) 434–436, 443
- Simple Object Access Protocol (SOAP) 86
- simulations 766–767
- Simultaneous Authentication of Equals (SAE) 101, 551, 552
- single loss expectancy (SLE) 922
- single point of failure 156, 926
- single quotation mark (') 73
- single sign-on (SSO) 292, 373, 624, 658–659
- sinkholes, DNS 223

- SIP (Session Initiation Protocol) 351, 431, 800
- SIRS (security incident response simulations) 766–767
- SIRT. *See* incident response (IR) teams
- site resiliency 221–222
- site surveys 559, 561–562
- sites, physical 385
- site-to-site configuration 495
- site-to-site VPNs 496–497
- SKEME (Secure Key Exchange Mechanism) 497
- SKEYID 500
- skimming 49–50
- SLAs (service-level agreements) 53, 273–274, 600, 902–903
- SLE (single loss expectancy) 922
- Sleuth Kit 850
- smart cards 299–300, 625, 629
- smart devices 345
- smart factories 342
- smart meters 350
- S/MIME (Secure/Multipurpose Internet Mail Extensions) 428–429
- smishing 12
- SMS (Short Message Service) 12, 296–297, 583, 585
- sn1per 726–727
- snapshots 326, 851–852
- SNMPv3 (Simple Network Management Protocol version 3) 434–436, 443
- snmpwalk v3 command 436
- snooping, DHCP 512–513
- SOAP (Simple Object Access Protocol) 86
- SOAR. *See* Security Orchestration, Automation, and Response (SOAR)
- SOC (System and Organization Controls) 884
- SoC (system on a chip) 356–357, 477, 571
- social engineering attacks
 - description of 7–9
 - dumpster diving 13
 - eliciting information 15–16
 - hybrid warfare 22
 - identity fraud 17
 - baiting 19
 - credential harvesting 18
 - hoaxes 19
 - impersonation/pretexting 19
 - invoice scams 17
 - reconnaissance 18
 - typo squatting 20, 44
 - watering hole attacks 20, 85
 - influence campaigns 21
 - pharming 14–15
 - phishing and spear phishing 9–12
 - piggybacking 15
 - prepending 17
 - principles of 21
 - reasons for effectiveness 21
 - shoulder surfing 14
 - smishing 12
 - Spam 13
 - Spam over Internet Messaging (SPIM) 13
 - tailgating 15
 - user security awareness education 22–24
 - vishing 12–13
 - war-dialing 13
 - whaling 9, 16–17
- Social Engineering Toolkit (SET) 10
- social media
 - attacks and vulnerabilities 22, 123, 143
 - as research source 128
- social media analysis 899
- SOCs (security operations centers) 123, 175–176, 223, 379, 760, 762, 776
- software application development. *See* application development
- software as a service (SaaS) 138, 231, 444, 853

- software compliance/licensing 918
- software development environments
 - 257–260
- software development lifecycle (SDLC)
 - 78, 261–262, 263–265, 468, 868
- software diversity 278
- software integrity measurement 261
- Software of Unknown Providence (SOUP) 347
- software-defined networking (SDN)
 - 241–243, 882
- software-defined visibility (SDV) 243
- software-defined wide-area network (SD-WAN) 246
- SolarWinds 721, 789
- solid-state drives (SSDs), forensic
 - acquisition of 848
- SOUP (Software of Unknown Providence) 347
- sovereignty, data 214–215
- SOX (Sarbanes–Oxley) 880, 882
- Spam 13
- Spam over Internet Messaging (SPIM) 13
- SpamCop 13
- SPAN (Switched Port Analyzer) ports
 - 537–538
- spanning, port 537–538
- Spanning Tree Protocol (STP) 105, 512
- spanning-tree portfast bpduguard
 - command 512
- SPAs (security posture assessments) 539
- specialized embedded systems 346–347
 - aircraft 348–350
 - communication considerations
 - 5G 357–358
 - baseband radio 359
 - NarrowBand 358
 - subscriber identity module (SIM)
 - cards 360
 - Zigbee 360–361
 - constraints 361
 - authentication 363
 - compute 361–362
 - cost 363
 - crypto 362
 - implied trust 363
 - inability to patch 362
 - network 362
 - power 361
 - range 363
 - drones 353–354
 - heating, ventilation, and air
 - conditioning (HVAC) 352–353
 - medical systems 347
 - multifunction printers (MFPs) 354
 - real-time operating systems (RTOSs)
 - 355
 - smart meters 350
 - surveillance systems 355–356
 - system on a chip (SoC) 356–357
 - vehicles 347–348
- Voice over Internet Protocol (VoIP)
 - 350, 799–800
- speech recognition 302
- SPF (Sender Policy Framework) 110, 426
- SPI (stateful packet inspection) 528, 562
- SpiderFoot 203
- SPIM (Spam over Internet Messaging) 13
- split tunneling 495–496
- Splunk 526
- spoofing
 - ARP (Address Resolution Protocol)
 - 105, 513
 - MAC (media access control) 101, 106
- sprawl avoidance 247–248
- spraying, password 45
- SPs (service providers) 292, 623, 661
- spyware 40–42
- SQL (Structured Query Language) 273
 - SQL injection (SQLi) 54, 70–74, 273–274, 464, 602
 - SQL Server 273
- SquidProxies 514

- SRAM (static random-access memory) 340
- SRTP (Secure Real-Time Transport Protocol) 152, 430–431
- SSAE (Statement on Standards for Attestation Engagements) 881, 883, 884
- SSDs (solid-state drives), forensic acquisition of 848
- SSH (Secure Shell) 427–428, 625, 628, 739–740
- ssh command 427
- SSIDs (service set identifiers) 98, 205, 532
- SSL (Secure Sockets Layer) 82–83, 436, 441
 - certificate types 694–696
 - SSL-based VPNs 505–508
 - stripping 88–89
 - Transport Layer Security Inspection (TLSI) 215–216
- SSL Inspection (SSSI) 215
- SSO (single sign-on) 292, 373, 624, 658–659
- SSRF (server-side request forgery) 85–86
- SSSI (SSL Inspection) 215
- staging 259
- stakeholder management 771–772
- standard load 540
- standards. *See* regulations and standards
- stapling 698
- starvation attack, DHCP 513
- state actors 120–121
- state laws 879–880
- stateful packet inspection (SPI) 528, 562
- stateful pattern-matching recognition 521
- stateless packet inspection 528
- Statement on Standards for Attestation Engagements (SSAE) 881, 883, 884
- statements, SQL (Structured Query Language) 70
- static application security testing (SAST) 468–469
- static code analysis 269, 468–469
- static codes 298
- static random-access memory (SRAM) 340
- Stegais 415
- steganography 415
 - audio 415–416
 - homomorphic 417
 - image 416–417
 - video 416
- Steghide 415
- stego-files 416
- stewards, data 946
- sticky sessions 489
- STIX (Structured Threat Information eXpression) 125–127
- storage
 - cloud 610
 - encryption 605
 - high availability 605
 - permissions 605
 - replication 605
 - secure 477
 - storage DLP systems 215
 - vulnerabilities 156
- storage-area networks (SANs) 142, 323
- Stored (persistent) XSS attacks 68
- stored procedures 273
- STP (Spanning Tree Protocol) 105, 512
- strategic intelligence 860
- stream ciphers 410
- stress testing 80, 266
- stretching, key 397
- striping (RAID) 316, 317–318
 - with dual parity 316, 318
 - with parity 316, 318
 - stripe and mirror 316, 319
- stripping, SSL 88–89
- structured exception handling (SEH) 81, 267

Structured Query Language. *See* SQL (Structured Query Language)

Structured Threat Information eXpression (STIX) 125–127

Stuxnet 363

Subject Alternative Name (SAN) 693, 694–695

subnets

- public/private 606, 610
- screened 384, 491

subscriber identity module (SIM) cards 49, 360, 580, 584

substitution 216, 416–417

supervisory control and data acquisition (SCADA) systems 341–343

supplicants 555, 665

supply chains

- attacks 51, 123, 156
- business partnership agreements (BPAs) 903
- supply chain risk management (SCRM) 166, 920

surge protectors 159

surveillance systems 355–356

surveys, site 559, 561–562

svStrike 850–851

Swagger (OpenAPI) 87

swap files, forensic acquisition of 849–850

SWG (Secure Web Gateway) 613, 614

Switched Port Analyzer (SPAN) ports 537–538

switching 443

symmetric encryption 411–413

synchronization 82–83

- email and web 440
- time 440

synchronization (SYN) packets 84

syslog 800–801

syslog-ng 800–801

System and Organization Controls (SOC) 884

System Information 161

system integration 155

system logs 791–792

System Monitor 542

system on a chip (SoC) 356–357, 477, 571

system owners 946–947

System Restore 158

systemd 802

system-generated passwords 638

systeminfo command 161

T

tables, rainbow 47

tabletop exercises 765–766

TACACS+ (Terminal Access Controller Access Control System Plus) 672–673

tactics, techniques, and procedures (TTPs) 128, 176, 767, 809

tags, evidence 845–846

tail command 734, 795

tailgating 15

Talos 347

tamper resistance 477

tape backups 326

taps, port 538

TAXII (Trusted Automated eXchange of Indicator Information) 125–127

TCB (trusted computing base) 676

TCG (Trusted Computing Group), Opal 476

Tcl 241

TCP (Transmission Control Protocol) 503

Tcpdump 742–743

TCP/IP hijacking 84

Tcpreplay 742

TCSEC (Trusted Computer System Evaluation Criteria) 674

teaming, network interface card (NIC) 320

teams, incident response (IR) 760, 775–776

- Teardrop 88
- technical controls 868, 869
- Technical Guide to Information Security Testing and Assessment (NIST) 199
- TEE (trusted execution environment) 476
- telemetry, fake 223
- temperature sensors 382
- temporal groups 182
- Temporal Key Integrity Protocol (TKIP) 552
- temporary files 157
- Tenable Network Security Nessus 204
- TERM environment variable 740
- Terminal Access Controller Access Control System Plus (TACACS+) 672–673
- terms of agreement 948
- testing 259
 - black-box 80
 - compile-time errors 266–267
 - fuzz 80, 269–270
 - gray-box 80
 - input validation 80, 267–268
 - known environment/white box 468–469
 - penetration 121, 266
 - active reconnaissance 204–205
 - advantages of 197–198
 - bug bounties versus 202–203
 - cleanup 202
 - definition of 193, 197
 - exercise types 205–206
 - known environment 198
 - lifecycle 199–202
 - methodologies 199
 - partially known environment 199
 - passive reconnaissance 203–204
 - post-exploitation techniques 201
 - rules of engagement 200
 - unknown environment 198–199
 - runtime errors 266–267
 - static and dynamic code analysis 269
 - stress 80, 266
 - white-box 80
- tethering 584
- TGTs (ticket-granting tickets) 668
- THC Hydra 749
- theft
 - disaster analysis 925
 - identity 940
 - intellectual property 917
 - mobile device 580
 - session 83
- theHarvester 203, 725–726
- thin clients 235–236, 508
- “third countries” 220
- third-party destruction and disposal services 387
- third-party libraries 265
- third-party risks 155–160
- threat actors
 - attack vectors 122–123
 - attributes of 122
 - types of 120–121
- threat feeds 176
- threat hunting 175–180
- threat intelligence
 - automated indicator sharing (AIS) 125
 - Information Sharing and Analysis Centers (ISACs) 123–125
 - MITRE ATT&CK framework 128–129
 - research sources 127–128
 - Structured Threat Information eXpression (STIX) 125–127
 - Trusted Automated eXchange of Indicator Information (TAXII) 125–127
 - vulnerability databases 125
- threat maps 127
- threat modeling 264
- thumbprint algorithm 692

- ticket-granting tickets (TGTs) 668
- tickets, Kerberos 668
- time 844–845
 - delay 74
 - offset 844
 - synchronization 440
 - time bombs 39
 - time of check (TOC) attacks 79
 - time of use (TOU) attacks 79
 - time-based logins 639
 - time-based one-time password (TOTP) 295
 - timestamps 82–83, 844
- Time Machine 158
- time-to-live (TTL) 795
- TKIP (Temporal Key Integrity Protocol) 552
- TLS (Transport Layer Security) 82–83, 88, 108, 351, 410, 436, 441, 556, 577, 656, 698
- TLSI (Transport Layer Security Inspection) 215–216
- TMSAD (Trust Model for Security Automation Data) 887
- TOC (time of check) attacks 79
- token key 297
- token-based authentication 297
- tokenization 218, 461–462, 945
- tokens 461, 625, 627–628
- Top 10 Web Application Security Risks 277
- Top Secret information 905, 941–942
- TOS (trusted operating system) 160, 905
- ToS (type of service) bits 536
- Toshiba 476
- TOTP (time-based one-time password) 295
- TOU (time of use) attacks 79
- TPM (Trusted Platform Module) 294, 459–460, 477–478, 524, 655
- traceroute command 707–709
- tracert command 707–709
- traffic
 - east-west 492
 - lateral 492
- training, user 22–24, 899, 901–902
- Transaction Signature (TSIG) 108
- transference of risk 918
- transit gateways 246–247
- transitive trust 577–578
- Transmission Control Protocol (TCP) 503
- transparent proxy 516
- Transport Layer Security Inspection (TLSI) 215–216
- Transport Layer Security (TLS) 82–83, 88, 108, 351, 410, 436, 441, 556, 577, 656, 698
- transport mode, IPsec 438, 503
- traversal, directory 75–76, 149, 274–275, 276
- Triple DES 412
- TRNG (true random number generators) 477
- Trojans 35, 104, 108, 113
- true random number generators (TRNGs) 477
- trust
 - models 698
 - root of 476–477
 - transitive 577–578
 - Trusted Computer System Evaluation Criteria (TCSEC) 674
 - zero 494
- Trust Model for Security Automation Data (TMSAD) 887
- Trusted Automated eXchange of Indicator Information (TAXII) 125–127
- trusted computing base (TCB) 676
- Trusted Computing Group (TCG) 476
- trusted execution environment (TEE) 476
- trusted operating system (TOS) 160, 905

- Trusted Platform Module (TPM) 294, 459–460, 477–478, 524, 655
 - trusted zones 825
 - trustworthy computing 39–40
 - Try-SQL Editor 71
 - TSIG (Transaction Signature) 108
 - TTLS (Tunneled Transport Layer Security) 556
 - TTPs (tactics, techniques, and procedures) 128, 176, 767, 809
 - tunnel mode, IPsec 438, 503
 - Tunneled Transport Layer Security (TTLS) 556
 - tunneling 495–496, 505–508, 556
 - two-factor authentication (2FA) 298
 - Twofish 412
 - two-person integrity control 378
 - Type I errors 626
 - Type II errors 626
 - type of service (ToS) bits 536
 - typo squatting 20, 44
- U**
- UAC (User Account Control) 67
 - UAs (user agents) 800
 - UAVs (unmanned aerial vehicles) 353–354
 - ubuntu keyword 239
 - UDP (User Datagram Protocol) 503
 - UEFI (Unified Extensible Firmware Interface) 459, 851
 - UEM (unified endpoint management) 587–588, 825
 - Umbrella 509
 - unauthenticated modes 404
 - unauthorized hackers 121
 - Unclassified information 941–942
 - underscore (_) 740
 - unicast addresses 537
 - unified endpoint management (UEM) 587–588, 825
 - Unified Extensible Firmware Interface (UEFI) 459, 851
 - unified threat management (UTM) 495, 524
 - uniform resource locators (URLs)
 - redirection attacks 110
 - URL hijacking 44
 - uninterruptible power source (UPS) 320–321
 - union operator 73
 - unique serial numbers (ICCID) 360
 - Universal Serial Bus. *See* USB (Universal Serial Bus)
 - UNIX 144
 - unknown environment 198–199
 - unmanned aerial vehicles (UAVs) 353–354
 - UPDATE statement 70
 - updates, exam 02.0004–02.0026
 - UPN (User Principal Name) 696
 - UPS (uninterruptible power source) 320–321
 - URLs (uniform resource locators)
 - filtering 828–829
 - redirection attacks 110
 - URL hijacking 44
 - US Computer Emergency Readiness Team (US-CERT) 576
 - US Office of Personnel Management (OPM) attack 300–301
 - USB (Universal Serial Bus)
 - condoms 379
 - data blockers 379–380
 - malicious flash drives 47–48
 - malicious USB cables 48
 - USB OTG (USB On-The-Go) 583
 - USB sticks 123
 - US-DMCA (Digital Millennium Copyright Act) 220
 - use case analysis 882
 - user access recertification 645

User Account Control (UAC) 67
 user accounts. *See* accounts
 user agents (UAs) 800
 user behavior analysis 188
 user certificates 696
 User Datagram Protocol (UDP) 503
 user education 899, 901–902
 USER environment variable 740
 User Interaction (UI) metric 184
 User Principal Name (UPN) 696
 user security awareness education 22–24
 user-controlled input 464
 user-generated passwords 638
 users command 631–632
 UTC (Coordinated Universal Time) 845
 UTM (unified threat management) 495,
 524

V

vacations, mandatory 898–899, 900
 validation
 continuous 278
 identity 633–635
 input 267–268, 464
 validity dates, certificate 692
 variables, environmental 740
 /var/log directory 791
 vaults 385, 655
 VBA (Visual Basic for Applications) 113
 VDEs (virtual desktop environments)
 139, 232
 VDIs (virtual desktop infrastructures)
 139, 232
 vectors, attack 122–123
 vehicle systems 347–348
 vein authentication 302
 vendor management 155, 156, 331,
 902–903
 ver command 161
 Veracode Web Application Security 204
 Verisign 112, 577
 version control 258, 279
 vertical privilege escalation 67
 vestibules, access control 372–373
 video
 forensic video analysis 842–843
 secure 440
 steganography 416
 virtualization 606, 610. *See also* VPNs
 (virtual private networks)
 APIs (application programming
 interfaces)
 definition of 240–241
 infrastructure as code 241–243
 micro-segmentation 240–241
 cloud computing
 cloud models 231–232
 cloud service providers (CSPs) 233
 community cloud 233
 fog and edge computing 234–235
 hybrid cloud 233
 managed detection and response
 (MDR) 234
 managed service providers (MSPs)
 233–234
 off-premises versus on-premises
 services 234
 private cloud 232–233
 public cloud 232
 thin clients 235–236
 VPCs (virtual private clouds) 607,
 608, 611
 containers 236–240
 definition of 247
 firewalls 534–535
 IP addresses 488
 memory 850
 microservices 236–240
 resource policies 246
 serverless architecture 243–244
 services integration 246
 transit gateways 246–247
 VDEs (virtual desktop environments)
 139, 232

- VDIs (virtual desktop infrastructures)
 - 139, 232, 589
- VLANs (virtual local-area networks)
 - 490–491, 831
- VMs (virtual machines) 324–325
 - attacks 248–249, 601
 - sprawl avoidance 247–248
- VNC (virtual network computing)
 - servers 632
- VPCs (virtual private clouds) 607, 608, 611
- viruses
 - antivirus software 451
 - fileless 37
- vishing 12–13
- visitor logs 383
- Visual Basic for Applications (VBA) 113
- VLANs (virtual local-area networks)
 - 490–491, 831
- VMs (virtual machines) 324–325
 - attacks 248–249, 601
 - sprawl avoidance 247–248
- VNC (virtual network computing) servers
 - 632
- voice, secure 440
- voice recognition 302
- VoIP (Voice over Internet Protocol) 350, 799–800
- volatility, order of 848
- VPCs (virtual private clouds) 607, 608, 611
- VPNs (virtual private networks) 99
 - always-on functionality 495
 - clientless versus client-based 497, 507
 - definition of 494
 - description of 494–496
 - example of 494–495
 - HTML5 508
 - IKEv1 Phase 1 negotiation 498–501
 - IKEv1 Phase 2 negotiation 501–503
 - IKEv2 504–505
 - IPsec 497, 501–502
 - Layer 2 Tunneling Protocol (L2TP)
 - 508
 - remote-access 496–497
 - SCADA systems 341–342
 - site-to-site configuration 495, 496–497
 - split tunneling 495–496
 - SSL-based 505–508
 - VPN concentrators 495
- vulnerabilities
 - backdoors 149, 271, 275
 - cloud-based versus on-premises
 - 137–143
 - code injection 149, 273–274, 276
 - cross-site request forgery (XSRF) 149, 272, 275
 - cross-site scripting (XSS) 54, 68–70, 110, 149, 272, 275, 601
 - dark web 143
 - directory traversal 149, 274–275, 276
 - error handling 79–82
 - compile-time errors 81–82
 - input handling 79–82
 - runtime errors 81–82
 - impact of cybersecurity breaches and attacks 165–166
 - legacy platforms 165
 - memory/buffer 77–78, 149, 271–272, 275
 - peer to peer (P2P) networks 143
 - remote code execution (RCE) 78, 146, 149, 275
 - server defense 144
 - email servers 145
 - file servers 144
 - FTP servers 147–148
 - network controllers 144
 - web servers 146–147
 - social media 143
 - summary of 149–150, 275–276
 - third-party risks 155–160
 - vulnerability databases 125
 - weak configurations 150–155

- weak patch management 160–164
- zero-day 149, 275, 276, 522
- vulnerability scans 180–181, 559
 - Common Vulnerability Scoring System (CVSS) 182–186
 - false negative 181
 - false positives 181
 - intrusive versus nonintrusive 182
 - noncredentialed 182
 - output 785–786
- VUPEN Web Application Security Scanner 204

W

- w command 631
- WADL (Web Application Description Language) documents 87
- WAF (web application firewall) 198, 531
- walkthrough exercises 766
- WannaCry 34, 37
- WAP (Wireless Application Protocol) 558, 585
- WAPs (wireless access points) 98, 101, 513, 559
- war driving 205
- war flying 205
- war-dialing 13
- warm sites 221
- waterfall development methodology 257–258
- watering hole attacks 20, 85
- weak configurations 150–155
- weak defaults 346
- weak patch management 160–164
- wearables 345
- Web Application Description Language (WADL) documents 87
- web application firewall (WAF) 198, 531
- Web Application Proxy 516
- web application scanners 182
- Web form-grabbing keyloggers 43

- web of trust 698
- web pages, metadata from 808–809
- web protocol port numbers 441
- web servers
 - logs 794
 - vulnerabilities 146–147
- Web Services Description Language (WSDL) documents 87
- web synchronization 440
- WebApp360 204
- webification 507
- Websense 533
- WebSploit 72, 238, 953
- weighted random early detection (WRED) 536
- WEP (Wired Equivalent Privacy) 102
- WER (Windows Error Reporting) 853
- Western Digital 476
- whaling 9, 16–17
- white box testing 468–469
- white hat hackers 121
- white teams 206
- white-box testing 80
- WhiteHat Sentinel 204
- whitelisting 578, 583
- who command 631–632
- whoami command 632
- whois 108, 203
- Wi-Fi
 - vulnerabilities and exposures 571
 - Wi-Fi ad hoc 584
 - Wi-Fi Analyzers 559, 561
 - Wi-Fi direct 584
 - Wi-Fi disassociation attack 101
 - WPA2 (Wi-Fi Protected Access 2) 551
 - WPA3 (Wi-Fi Protected Access 3) 551
 - WPS (Wi-Fi Protected Setup) 558–559
- Wigle 205
- wildcard certificates 694–695

- Windows Defender Firewall 457
- Windows Error Reporting (WER) 853
- Windows Event Viewer 791–792, 846
- Windows Performance Monitor 540–542
- Windows Performance tool 539
- Windows PowerShell 630
- WinGate 514
- WinHex 746
- Wired Equivalent Privacy (WEP) 102
- wireless access points (WAPs) 98, 101, 513, 559
- Wireless Application Protocol (WAP) 558, 585
- wireless LAN (WLAN) controllers 558
- wireless networks 547, 557–558
 - attacks 98, 122
 - bluejacking 100
 - bluesnarfing 99–100
 - disassociation and deauthentication 101
 - evil twin 98–99
 - initialization vector (IV) 103
 - jamming 102, 561–562
 - mobile device security
 - countermeasures 580
 - near-field communication (NFC) 102–103
 - radio frequency identification (RFID) 49, 102
 - rogue access points 98–99
 - authentication protocols 556–557
 - cryptographic protocols 551
 - Advanced Encryption Standard (AES) 552
 - Counter-mode/CBC-MAC protocol (CCMP) 552
 - Simultaneous Authentication of Equals (SAE) 551, 552
 - summary of 552
 - Wi-Fi Protected Access 2 (WPA2) 551
 - Wi-Fi Protected Access 3 (WPA3) 551–552
 - installation considerations
 - AP isolation 562
 - captive portals 559
 - controller and access point security 562–563
 - firewalls 562
 - heat maps 559
 - IEEE 802.1X standard 562
 - Multi-User Multiple Input (MU-MIMO) 560–561
 - orthogonal frequency-division multiple access (OFDMA) 561
 - site surveys 559, 561–562
 - Wi-Fi Analyzer tools 559
 - Wi-Fi Protected Setup (WPS) 558–559
 - wireless access point (WAP) placement 559
- Wireless Transport Layer Security (WTLS) 558
- Wireshark 539, 559, 743
- WLAN (wireless LAN) controllers 558
- workstations, hardening 159–160
- WORM (write once read many) device 789
- worms 36–37
- WPA2 (Wi-Fi Protected Access 2) 551
- WPA3 (Wi-Fi Protected Access 3) 551
- WPS (Wi-Fi Protected Setup) 558–559
- wrap 77
- write once read many (WORM) devices 789
- WSDL (Web Services Description Language) documents 87
- WTLS (Wireless Transport Layer Security) 558
- wuapp.exe 161

X

- X.509 standard 694
- X.690 encoding formats 697
- XaaS (anything as a service) 139, 232
- XCCDF (Extensible Configuration Checklist Description Format) 885
- XDR (Extended Detection and Response) 189
- Xiao 415
- XML (Extensible Markup Language)
 - XML injection 74–75, 273–274
 - XSD (XML Schema Definition) 86
 - XXE (XML External Entity) 74
- XSRF (cross-site request forgery) 85–86, 149, 272, 275
- XSS (cross-site scripting) 54, 68–70, 110, 149, 272, 275, 464, 601
- Xways 850–851
- X-Ways Software Technology AG 746
- XXE (XML External Entity) 75

Y

- YOLO (You Only Look Once) 376
- YubiKey 297

Z

- Zed Attack Proxy 204
- zero trust 494
- zero-day vulnerabilities 149, 275, 276, 522
- Zigbee 360–361
- Zimbra 145
- zombies 111–112
- zones
 - high availability across 603, 609
 - zone signing keys (ZSKs) 427
 - zone transfers 109
- ZSKs (zone signing keys) 427
- Zune 850–851