EXAM CRAM

CompTIA® Security+ SY0-601

Save 10% on Exam Voucher
See Inside

PEARSON IT
CERTIFICATION

MARTY M. WEISS

FREE SAMPLE CHAPTER
SHARE WITH OTHERS

EXAM CRAM

CompTIA® Security+ SY0-601 Exam Cram

Marty M. Weiss

Pearson
221 River Street
Hoboken, NJ 07030 USA

CompTIA® Security+ SY0-601 Exam Cram

Copyright © 2021 by Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions.

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: 978-0-13-679867-5

ISBN-10: 0-13-679867-5

Library of Congress Control Number: 2020914528

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 author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

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

Director, ITP Product Management
Brett Bartow

Executive Editor
Nancy Davis

Development Editor
Ellie C. Bru

Managing Editor
Sandra Schroeder

Project Editor
Mandie Frank

Copy Editor
Kitty Wilson

Indexer
Ken Johnson

Proofreader
Donna Mulder

Technical Editor
Christopher Crayton

Publishing Coordinator
Cindy Teeters

Designer
Chuti Prasertsith

Compositor
codeMantra

Credits

Figure Number	Attribution/Credit
Figure 2-1	Screenshot of an example of what user's see when they were infected with ransomware © WannaCry
Figure 5-1	Screenshot of an example of an interactive threat map © 2018 AO Kaspersky Lab
Figure 10-4	Screenshot of The AWS Management Console © 2020, Amazon Web Services, Inc.
Figure 12-1	Courtesy of Apple, Inc.
Figure 23-1	Screenshot of Windows local security policy settings for the account lockout policy © Microsoft 2020
Figure 23-2	Screenshot of Windows local security policy settings for the password policy © Microsoft 2020
Figure 24-1	Screenshot of Standard Microsoft Windows file permissions © Microsoft 2020
Figure 25-1	Screenshot of details of a digital certificate © 2020 Apple Inc.
Figure 26-1	Screenshot of using a command-line interface to access a remote computer by using SSH © 2020 Apple, Inc.
Figure 26-2	Screenshot of using the cURL command to return the source code of a web page © 2020 Apple, Inc.
Figure 26-3	Screenshot of using the ping command-line utility © 2020 Apple, Inc.
Figure 28-1	Screenshot of an example of a SIEM system security dashboard © security information and event management
Figure 28-2	Screenshot of Microsoft Windows Event Viewer Security log © Microsoft 2020
Figure 28-3	Screenshot of Activity Monitor for macOS © 2020 Apple, Inc.

Contents at a Glance

Introduction xxvii

Part I: Attacks, Threats, and Vulnerabilities 1

CHAPTER 1 Social Engineering Techniques 3
CHAPTER 2 Attack Basics 15
CHAPTER 3 Application Attacks 35
CHAPTER 4 Network Attacks 53
CHAPTER 5 Threat Actors, Vectors, and Intelligence Sources 73
CHAPTER 6 Vulnerabilities 89
CHAPTER 7 Security Assessment Techniques 99
CHAPTER 8 Penetration Testing Techniques 111

Part II: Architecture and Design 121

CHAPTER 9 Enterprise Security Concepts 123
CHAPTER 10 Virtualization and Cloud Computing 145
CHAPTER 11 Secure Application Development, Deployment, and Automation 165
CHAPTER 12 Authentication and Authorization Design 189
CHAPTER 13 Cybersecurity Resilience 205
CHAPTER 14 Embedded and Specialized Systems 225
CHAPTER 15 Physical Security Controls 239
CHAPTER 16 Cryptographic Concepts 261

Part III: Implementation 279

CHAPTER 17 Secure Protocols 281
CHAPTER 18 Host and Application Security Solutions 307
CHAPTER 19 Secure Network Design 339
CHAPTER 20 Wireless Security Settings 371
CHAPTER 21 Secure Mobile Solutions 389
CHAPTER 22 Cloud Cybersecurity Solutions 421
CHAPTER 23 Identity and Account Management Controls 433

CHAPTER 24 Authentication and Authorization Solutions 449
CHAPTER 25 Public Key Infrastructure 473

Part IV: Operations and Incident Response 491
CHAPTER 26 Organizational Security 493
CHAPTER 27 Incident Response 509
CHAPTER 28 Incident Investigation 529
CHAPTER 29 Incident Mitigation 541
CHAPTER 30 Digital Forensics 551

Part V: Governance, Risk, and Compliance 567
CHAPTER 31 Control Types 569
CHAPTER 32 Regulations, Standards, and Frameworks 575
CHAPTER 33 Organizational Security Policies 583
CHAPTER 34 Risk Management 597
CHAPTER 35 Sensitive Data and Privacy 613
Glossary of Essential Terms and Components 625
Index 655

Table of Contents

Introduction . . . . **xxvii**

Part I: Attacks, Threats, and Vulnerabilities **1**

CHAPTER 1:
Social Engineering Techniques **3**

The Social Engineer 4

Tailgating 5

Dumpster Diving 5

Shoulder Surfing 6

Phishing and Related Attacks 6

Watering Hole Attacks 9

Typo Squatting 9

Hoaxes and Influence Campaigns 10

Principles of Influence (Reasons for Effectiveness) 10

What Next? 14

CHAPTER 2:
Attack Basics **15**

Malware 16

Viruses 17

Worms 19

Trojan. 19

Rootkits 20

Logic Bombs 22

Bots 22

Crypto-Malware. 23

Potentially Unwanted Programs (PUPs) 25

Spyware 25

Adware 25

Cryptomining Software 26

Physical Attacks 26

Adversarial Artificial Intelligence (AI) 27

Password Attacks 28

Birthday Attacks. 30

Downgrade Attacks. 31

What Next? 34

CHAPTER 3:

Application Attacks 35
Race Conditions 36
Improper Software Handling 37
Resource Exhaustion 37
Overflows 38
Code Injections 39
Driver Manipulation 40
Request Forgeries 41
Directory Traversal 44
Replay Attack 45
Secure Sockets Layer (SSL) Stripping 45
Application Programming Interface (API) Attacks 47
Pass-the-Hash Attack 49
What Next? 52

CHAPTER 4:

Network Attacks 53
Wireless 54
Short-Range Wireless Communications 56
Bluetooth 56
Near-Field Communication 57
RFID 57
On-Path Attack 58
Layer 2 Attacks 59
MAC Spoofing 60
ARP Poisoning 60
MAC Flooding 61
Port Stealing 61
Domain Name System (DNS) Attacks 62
Domain Hijacking 62
Universal Resource Locator (URL) Redirection 62
DNS Poisoning 63
Denial of Service 64
Distributed DoS 66
Malicious Code and Script Execution 68
What Next? 71

CHAPTER 5:
Threat Actors, Vectors, and Intelligence Sources **73**

Threat Actor Attributes 74
Threat Actor Types 75
Script Kiddies 76
Insiders 77
Hacktivists 78
Criminal Syndicates 78
Competitors 78
State Actors 79
Vectors 80
Threat Intelligence and Research Sources 81
Sharing Centers 81
Open-Source Intelligence 82
What Next? 87

CHAPTER 6:
Vulnerabilities **89**

Cloud-Based vs. On-Premises 90
Zero-Day 90
Weak Configurations 91
Improper or Weak Patch Management 94
Third-Party Risks 95
Impacts 96
What Next? 98

CHAPTER 7:
Security Assessment Techniques **99**

Vulnerability Scans 100
Intrusive vs. Non-Intrusive 102
Credentialed vs. Non-Credentialed 103
Threat Assessment 103
Security Information and Event Management (SIEM) 104
Threat Hunting 107
Security Orchestration, Automation, and Response (SOAR) 108
What Next? 110

CHAPTER 8:
Penetration Testing Techniques 111
Testing Methodology 112
Planning 115
Discovery 115
Attack 117
Reporting 118
Team Exercises 118
What Next? 120

Part II: Architecture and Design 121

CHAPTER 9:
Enterprise Security Concepts 123
Configuration Management 124
Data Confidentiality 126
Data Loss Prevention 127
Cloud Access Security Brokers 128
Encryption and Data Obfuscation 129
Rights Management 132
Hardware Security Module (HSM) 133
Encrypted Traffic Management 134
Data Integrity 135
Data Availability 136
Site Resiliency 137
Geographic Considerations 138
Deception and Disruption 139
What Next? 143

CHAPTER 10:
Virtualization and Cloud Computing 145
Virtualization 145
Hypervisors 146
Type I Hypervisors 146
Type II Hypervisors 147
Type I vs. Type II Hypervisors 147
Containers and Microservices 148
Virtual Desktop Infrastructure (VDI) 150
Virtual Machine (VM) Sprawl Avoidance 151
VM Escape Protection 151

Software-Defined Networking (SDN) 152
Infrastructure as Code (IaC) 153
On-Premises vs. Off-Premises 154
Cloud Models 155
Service Models 156
IaaS 158
PaaS 159
SaaS 159
Deployment Models 161
Private 161
Public 161
Hybrid 162
Community 162
What Next? 164

CHAPTER 11:
Secure Application Development, Deployment, and Automation 165

Application Environment 166
Development and Testing 166
Staging and Production 167
Provisioning and Deprovisioning 168
Integrity Measurement 168
Change Management and Version Control 169
Secure Coding Techniques 170
Normalization 172
Stored Procedures 173
Encryption, Obfuscation, and Camouflage 173
Code Reuse and Dead Code 174
Use of Third-Party Libraries and SDKs 175
Server-Side vs. Client-Side Execution and Validation 175
Data Exposure 176
Proper Error Handling 176
Proper Input Validation 177
Code Signing 178
Memory Management 179
Automation and Scripting 180
Secure DevOps 181
Scalability and Elasticity 184
What Next? 187

CHAPTER 12:
Authentication and Authorization Design 189

Identification and Authentication, Authorization, and Accounting (AAA) 189
Multifactor Authentication 190
Single Sign-on 192
Federation 193
Transitive Trust 194
Authentication Technologies 195
Tokens 195
Biometrics 198
Card Authentication 200
Certificate-Based Authentication 201
What Next? 204

CHAPTER 13:
Cybersecurity Resilience 205

Redundancy 205
High Availability 208
Load Balancers 209
NIC Teaming 211
RAID 211
Backups 214
Full Backups 217
Differential Backups 217
Incremental Backups 218
Copies and Snapshots 218
Non-persistence 219
Revert to Known State or Good Configuration 220
Live Boot Media 221
Defense in Depth 221
What Next? 224

CHAPTER 14:
Embedded and Specialized Systems 225

Embedded Systems 225
SoC and RTOS 226
SCADA and ICS 227
Smart Devices and IoT 229
Heating, Ventilation, Air Conditioning (HVAC) 231

Multifunction Devices. 232
Surveillance Systems 233
Special-Purpose Devices 233
Medical Devices. 233
Vehicles 234
Aircraft and UAV 235
Resource Constraints 236
What Next? 238

CHAPTER 15:
Physical Security Controls **239**

Perimeter Security 239
Signs, Fencing, and Gates 240
Lighting 241
Barricades and Bollards 241
Cameras 242
Security Guards 242
Internal Security. 243
Alarms 244
Motion and Infrared Detection 244
Access Control Vestibules 245
Locks and Lock Types. 245
Equipment Security 246
Cable Locks 246
Cages and Safes 246
Locking Cabinets and Enclosures 247
Screen Filters. 248
Air Gaps 248
Environmental Controls 249
Protected Cabling, Protected Distribution, and Faraday Cages . . . 249
HVAC 251
Fire Suppression 252
Hot and Cold Aisles 254
Secure Data Destruction 255
What Next? 259

CHAPTER 16:
Cryptographic Concepts **261**

Cryptosystems 262

Keys 262
Key Exchange 263
Symmetric Algorithms 264
Asymmetric Algorithms 266
Elliptic Curve and Emerging Cryptography 268
Session Keys 268
Nonrepudiation and Digital Signatures 269
Hashing 271
Use of Proven Technologies and Implementation 272
Steganography 273
Cryptography Use Cases 274
Cryptography Constraints 276
What Next? 277

Part III: Implementation 279

CHAPTER 17:
Secure Protocols 281

Secure Web Protocols 282
Internet Protocol Security (IPsec) 284
Secure File Transfer Protocols 286
Secure Email Protocols 287
Secure Internet Protocols 288
Lightweight Directory Access Protocol (LDAP) 289
Secure Real-Time Transport Protocol (SRTP) 290
Simple Network Management Protocol (SNMP) 290
Secure Protocol Use Cases 293
Secure Web Communication 293
Using HTTPS for Web Communications 293
Using SSL/TLS for Remote Access 294
Using DNSSEC for Domain Name Resolution 294
Secure File Transfer Communication 295
Using FTPS and SFTP for File Transfer 295
Secure Email Communications 296
Using S/MIME, POP3S, and IMAPS for Email 296
Securing Internal Communications 297
Using SRTP for Voice and Video 297
Using LDAPS for Directory Services 298
Using SNMPv3 with Routing and Switching 298

Using Network Address Allocation . . . 299
Using Time Synchronization . . . 302
Using Subscription Services . . . 303
What Next? . . . 305

CHAPTER 18:
Host and Application Security Solutions . . . 307

Endpoint Protection . . . 308
Firewalls and HIPS/HIDS Solutions . . . 308
Anti-Malware and Other Host Protections . . . 310
Endpoint Detection and Response (EDR) . . . 314
Data Execution Prevention (DEP) . . . 314
Data Loss Prevention (DLP) . . . 315
Removable Media Control . . . 316
Application Allow/Block Lists . . . 317
Web Application Firewall . . . 317
Application Security . . . 318
Code Analyzers . . . 319
Static Code Analyzers . . . 319
Dynamic Analysis . . . 319
Stress Testing . . . 321
Application Sandboxing . . . 321
Hardware and Firmware Security . . . 322
FDE and SED . . . 322
TPM and HSM . . . 324
Boot Integrity . . . 326
Boot Attestation . . . 328
Hardware Root of Trust . . . 329
Operating System Security . . . 330
Patch Management . . . 331
Disabling Unnecessary Ports and Services . . . 332
Least Functionality . . . 335
Secure Configurations . . . 335
Trusted Operating System . . . 336
What Next? . . . 338

CHAPTER 19:
Secure Network Design . . . 339

Network Devices and Segmentation . . . 340

Routers . . . 340
Network Address Translation (NAT) . . . 341
Switches . . . 342
Port Security . . . 343
Virtual Local Area Network (VLAN) . . . 344
Bridges . . . 345
Security Devices and Boundaries . . . 347
Screened Subnet . . . 350
Web Application Firewalls . . . 353
Proxies . . . 354
Unified Threat Management (UTM) . . . 357
VPN Concentrators . . . 358
NIDS and NIPS . . . 360
Detection Methods . . . 362
Analytics . . . 364
Network Access Control (NAC) . . . 365
What Next? . . . 369

CHAPTER 20:
Wireless Security Settings . . . 371
Access Methods . . . 372
Wireless Cryptographic Protocols . . . 373
Wired Equivalent Privacy (WEP) . . . 374
Wi-Fi Protected Access (WPA) . . . 375
Temporal Key Integrity Protocol . . . 376
Counter Mode with Cipher Block Chaining Message Authentication Code Protocol . . . 376
Wi-Fi Protected Access Version 2 (WPA2) . . . 376
Wi-Fi Protected Access Version 3 (WPA3) . . . 377
Authentication Protocols . . . 377
Wireless Access Installations . . . 379
Antenna Types, Placement, and Power . . . 380
MAC Filter . . . 383
Disabling SSID Broadcast . . . 384
What Next? . . . 387

CHAPTER 21:
Secure Mobile Solutions . . . 389
Communication Methods . . . 389

Mobile Device Management Concepts 393
Device, Application, and Content Management 393
Mobile Device Management 394
Mobile Content Management 394
Mobile Application Management 395
Protections 398
Screen Locks, Passwords, and PINs 398
Biometrics and Context-Aware Authentication 398
Remote Wiping 399
Geolocation, Geofencing, and Push Notifications 400
Storage Segmentation and Containerization 402
Full Device Encryption (FDE) 403
Enforcement and Monitoring 405
Jailbreaking and Rooting 405
Custom Firmware, Carrier Unlocking, and OTA Updates . . 406
Third-Party App Stores and Sideloading 407
Storage and USB OTG 408
Enforcement for Normal Device Functions 409
Wi-Fi Methods, Tethering, and Payments 410
Deployment Models 412
BYOD, CYOD, COPE, and Corporate-Owned Devices 412
Virtual Desktop Infrastructure 413
Deployment Strategies 414
Architecture/Infrastructure Considerations 414
Adherence to Corporate Policies and Acceptable Use 415
Legal Concerns 416
Privacy 416
Data Ownership and Support 417
Patch and Antivirus Management 417
Forensics 418
What Next? 420

CHAPTER 22:
Cloud Cybersecurity Solutions 421

Cloud Workloads 422
Regions and Availability Zones 423
Virtual Private Cloud (VPC) 423
Security Groups 423
Policies 424

Managing Secrets 426
Central Logging. 427
Third-Party Cloud Security Solutions 428
What Next? 431

CHAPTER 23:
Identity and Account Management Controls 433

Account Types 433
Account Management 435
Onboarding and Offboarding. 435
Least Privilege 436
Access Auditing and Reviews 436
Time of Day and Location Restrictions. 438
Logical Access Controls 439
Account Policy Enforcement 441
Password Complexity 442
Account Expiration. 442
Forgotten Passwords. 443
Account Lockout 443
Password Age and History 444
Password Length and Rotation. 445
What Next? 448

CHAPTER 24:
Authentication and Authorization Solutions. 449

Authentication 450
Unencrypted Plaintext Credentials 451
Filesystem Permissions 452
Access Violations 456
Authentication Issues 457
Authentication Protocols. 457
802.1X 459
AAA Protocols and Services. 459
Federated Services 461
Kerberos 464
Access Control 466
Privileged Access Management. 469
What Next? 472

CHAPTER 25:

Public Key Infrastructure 473
- PKI Components 474
  - Certificate Authority (CA) 475
    - Certification Practice Statement 476
    - Trust Models 476
    - Key Escrow 477
  - Digital Certificate 478
    - Public and Private Key Usage 480
    - Certificate Signing Request 481
    - Certificate Policy 482
    - Certificate Types 482
    - Certificate Formats 484
  - Certificate Revocation 486
  - OCSP Stapling 487
  - Pinning 488
- What Next? 489

Part IV: Operations and Incident Response 491

CHAPTER 26:

Organizational Security 493
- Shell and Script Environments 494
- Network Reconnaissance and Discovery 496
  - Exploitation Frameworks 502
- Packet Capture and Replay 502
- Password Crackers 504
- Forensics and Data Sanitization 505
- What Next? 508

CHAPTER 27:

Incident Response 509
- Attack Frameworks 509
  - Cyber Kill Chain 510
  - MITRE ATT&CK 510
  - Diamond Model of Intrusion Analysis 511
- Incident Response Plan 512
  - Documented Incident Type/Category Definitions 513
  - Roles and Responsibilities 513
  - Reporting Requirements and Escalation 514

Cyber-Incident Response Teams . . . 515
Training, Tests, and Exercises . . . 516
Incident Response Process . . . 517
Preparation . . . 517
Incident Identification and Analysis . . . 518
Containment, Eradication, and Recovery . . . 519
Post-Incident Activities . . . 521
Continuity and Recovery Plans . . . 522
Disaster Recovery . . . 522
Continuity of Operations Planning . . . 524
What Next? . . . 528

CHAPTER 28:
Incident Investigation . . . 529

SIEM Dashboards . . . 530
Logging . . . 531
Network Activity . . . 536
Protocol Analyzers . . . 537
Network Flow . . . 538
What Next? . . . 539

CHAPTER 29:
Incident Mitigation . . . 541

Containment and Eradication . . . 541
Quarantining . . . 542
Configuration Changes . . . 543
Firewalls . . . 544
Application Control . . . 545
Secure Orchestration, Automation, and Response (SOAR) . . . 546
What Next? . . . 549

CHAPTER 30:
Digital Forensics . . . 551

Data Breach Notifications . . . 552
Strategic Intelligence/Counterintelligence Gathering . . . 554
Track Person-hours . . . 555
Order of Volatility . . . 555
Chain of Custody . . . 556
Data Acquisition . . . 559

Capture System Images 560
Capture Network Traffic and Logs 560
Capture Video and Photographs 561
Record Time Offset 562
Take Hashes 562
Capture Screenshots 563
Collect Witness Interviews 563
What Next? 565

Part V: Governance, Risk, and Compliance 567

CHAPTER 31:
Control Types 569

Nature of Controls 570
Functional Use of Controls 570
Deterrent Controls 571
Preventive Controls 571
Detective Controls 571
Corrective Controls 572
Compensating Controls 572
What Next? 574

CHAPTER 32:
Regulations, Standards, and Frameworks 575

Industry-Standard Frameworks and Reference Architectures 575
Regulatory and Non-regulatory Requirements 576
Industry-Specific Frameworks 577
Benchmarks and Secure Configuration Guides 579
Platform- and Vendor-Specific Guides 579
General-Purpose Guides 580
What Next? 581

CHAPTER 33:
Organizational Security Policies 583

Policy Framework 583
Human Resource Management Policies 584
Background Checks 584
Onboarding and Offboarding 584
Mandatory Vacations 585
Separation of Duties 585

Job Rotation 586
Clean Desk Policies 586
Role-Based Awareness and Training 586
Continuing Education 588
Acceptable Use Policy/Rules of Behavior 589
Internet Usage 590
Nondisclosure Agreements 591
Disciplinary and Adverse Actions 591
Exit Interviews 592
Third-Party Risk Management 592
Interoperability Agreements 593
What Next? 596

CHAPTER 34:
Risk Management 597

Risk Analysis 598
Risk Register 598
Risk Response Techniques 599
Threat Assessment 601
Risk Assessment 602
Qualitative vs. Quantitative Measures 604
Single Loss Expectancy 605
Annual Rate of Occurrence 606
Annual Loss Expectancy 606
Business Impact Analysis 606
Critical Functions 607
Identification of Critical Systems 607
Single Points of Failure 607
Recovery Objectives 608
MTTF, MTBF, and MTTR 609
Impact 610
What Next? 612

CHAPTER 35:
Sensitive Data and Privacy 613

Sensitive Data Protection 613
Data Sensitivity Labeling and Handling 614
Privacy Laws and Regulatory Compliance 616
Data Roles and Responsibilities 618

Data Retention and Disposal 620
Privacy Impact Assessment. 621
What Next? 623

Glossary of Essential Terms and Components **625**

Index **655**

About the Author

Marty M. Weiss has spent most of his career in information security and risk management, helping large organizations. Marty holds a bachelor of science degree in computer studies from the University of Maryland University College and an MBA from the Isenberg School of Management at the University of Massachusetts Amherst. He holds several certifications, including CISSP, CISA, and Security+. Marty has authored and coauthored more than a half-dozen books on information technology, many that have been described as riveting and Dostoevsky-esque in reviews by his mother. A Florida native, he now lives in New England.

Dedication

This book is dedicated to my parents.

Acknowledgments

Thank you, the reader of this book. It's a pleasure to help others achieve a goal, and I'm thankful for that opportunity. Thank you to the entire team that helped to bring this book together. I'd like to acknowledge, in particular, Carole Jelen, Nancy Davis, Ellie Bru, Chris Crayton, Mandie Frank, and Kitty Wilson. Also, thank you, Diane Barrett. While you weren't directly involved in this edition, many of your words and ideas exist from previous editions. Finally, thank you to my friends and family for their support and understanding through the entire process.

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.

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 send 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

Reader Services

Introduction

Welcome to *CompTIA® Security+ SY0-601 Exam Cram*, sixth edition. This book helps you get ready to take and pass the CompTIA Security+ SY0-601 exam.

This book is designed to remind you of everything you need to know to pass the SY0-601 certification exam. Each chapter includes a number of practice questions that should give you a reasonably accurate assessment of your knowledge, and, yes, we've provided the answers and their explanations for these questions. Read this book, understand the material, and you'll stand a very good chance of passing the real test.

Exam Cram books help you understand and appreciate the subjects and materials you need to know to pass CompTIA certification exams. *Exam Cram* books are aimed strictly at test preparation and review. They do not teach you everything you need to know about a subject. Instead, the authors streamline and highlight the pertinent information by presenting and dissecting the questions and problems they've discovered that you're likely to encounter on a CompTIA test.

We strongly recommend that you spend some time installing and working with security tools such as Wireshark and Metasploit and experimenting with the many network and security-related resources provided with many operating systems. The Security+ exam focuses on such activities and the knowledge and skills they can provide you. Nothing beats hands-on experience and familiarity when it comes to understanding the questions you're likely to encounter on a certification test. Book learning is essential, but without a doubt, hands-on experience is the best teacher of all!

Let's begin by looking at preparation for the exam.

How to Prepare for the Exam

This text follows the official exam objectives closely to help ensure your success. The CompTIA exam covers 5 domains and 35 objectives. This book is divided into 5 parts and 35 chapters, aligning with those domains and objectives. These official objectives from CompTIA can be found here: https://www.comptia.org/training/resources/exam-objectives.

As you examine the numerous exam topics now covered in Security+, resist the urge to panic! This book you are holding will provide you with the knowledge (and confidence) that you need to succeed. You just need to make sure you read it and follow the guidance it provides throughout your Security+ journey.

Practice Tests

This book is filled with practice exam questions to get you ready! Cram quizzes end each chapter, and each question also includes complete explanations.

In addition, the book includes two additional full practice tests in the Pearson Test Prep software, available to you either online or as an offline Windows application. To access the practice exams, 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.

In case you are interested in more practice exams than are provided with this book, Pearson IT Certification publishes a Premium Edition eBook and Practice Test product. In addition to providing you with three eBook files (EPUB, PDF, and Kindle) this product provides you with two additional exams' worth of questions. The Premium Edition version also offers you a link to the specific section in the book that presents an overview of the topic covered in the question, allowing you to easily refresh your knowledge. The insert card in the back of the book includes a special offer for an 80% discount off of this Premium Edition eBook and Practice Test product, which is an incredible deal.

Taking a Certification Exam

After you prepare for your exam, you need to register with a testing center. At the time of this writing, the cost to take the Security+ exam is US $349 for individuals. Students in the United States are eligible for a significant discount. In addition, check with your employer as many workplaces provide reimbursement programs for certification exams. For more information about these discounts, you can contact a local CompTIA sales representative, who can answer any questions you might have. If you don't pass, you can take the exam again for the same cost as the first attempt until you pass. The test is administered by Pearson VUE testing centers, with locations globally. In addition, the CompTIA Security+ certification is a requirement for many within the U.S. military, and testing centers are available on some military bases.

You will have 90 minutes to complete the exam. The exam consists of a maximum of 90 questions. If you have prepared, you should find that this is plenty of time to properly pace yourself and review the exam before submission.

Arriving at the Exam Location

As with any other examination, arrive at the testing center early (at least 15 minutes). Be prepared! You need to bring two forms of identification (one with a picture). The testing center staff requires proof that you are who you say you are and that someone else is not taking the test for you. Arrive early because if you are late, you will be barred from entry and will not receive a refund for the cost of the exam.

ExamAlert

You'll be spending a lot of time in the exam room. Plan on using the full 90 minutes allotted for your exam and surveys. Policies differ from location to location regarding bathroom breaks, so check with the testing center before beginning the exam.

In the Testing Center

You will not be allowed to take into the examination room study materials or anything else that could raise suspicion that you're cheating. This includes practice test material, books, exam prep guides, and other test aids. The testing center will provide you with scratch paper and a pen or pencil. These days, this often comes in the form of an erasable whiteboard.

Examination results are available immediately after you finish the exam. After submitting the exam, you will be notified if you have passed or failed. I trust that if you are reading this book, you will pass. The test administrator will also provide you with a printout of your results.

About This Book

The ideal reader for an *Exam Cram* book is someone seeking certification. However, it should be noted that an *Exam Cram* book is a very easily readable, rapid presentation of facts. Therefore, an *Exam Cram* book is also extremely useful as a quick reference manual.

The book is designed so that you can either read it cover to cover or jump across chapters, as needed. Because the book chapters align with the exam objectives, some chapters may have slight overlap on topics. Where required, references to the other chapters are provided for you. If you need to brush up on a topic or if you have to bone up for a second try at the exam, you can use the index, table of contents, or Table I.1 to go straight to the topics and questions that you need to study. Beyond helping you prepare for the test, we think you'll find this book useful as a tightly focused reference on some of the most important aspects of the Security+ certification.

This book includes other helpful elements in addition to the actual logical, step-by-step learning progression of the chapters. *Exam Cram* books use elements such as ExamAlerts, notes, and practice questions to make information easier to read and absorb. This text also includes a Glossary to assist you.

Note

Reading this book from start to finish is not necessary; this book is set up so that you can quickly jump back and forth to find sections you need to study.

Use the *Cram Sheet* to remember last-minute facts immediately before the exam. Use the practice questions to test your knowledge. You can always brush up on specific topics in detail by referring to the table of contents and the index. Even after you achieve certification, you can use this book as a rapid-access reference manual.

Exam Objectives

Table I.1 lists the skills the SY0-601 exam measures and the chapter in which each objective is discussed.

TABLE I.1 **SY0-601 Exam Domains and Objectives**

Exam Domain	Objective	Chapter in Book That Covers It
1.0 Attacks, Threats, and Vulnerabilities	1.1 Compare and contrast different types of social engineering techniques.	Chapter 1
1.0 Attacks, Threats, and Vulnerabilities	1.2 Given a scenario, analyze potential indicators to determine the type of attack.	Chapter 2
1.0 Attacks, Threats, and Vulnerabilities	1.3 Given a scenario, analyze potential indicators associated with application attacks.	Chapter 3
1.0 Attacks, Threats, and Vulnerabilities	1.4 Given a scenario, analyze potential indicators associated with network attacks.	Chapter 4

Exam Domain	Objective	Chapter in Book That Covers It
1.0 Attacks, Threats, and Vulnerabilities	1.5 Explain different threat actors, vectors, and intelligence sources.	Chapter 5
1.0 Attacks, Threats, and Vulnerabilities	1.6 Explain the security concerns associated with various types of vulnerabilities.	Chapter 6
1.0 Attacks, Threats, and Vulnerabilities	1.7 Summarize the techniques used in security assessments.	Chapter 7
1.0 Attacks, Threats, and Vulnerabilities	1.8 Explain the techniques used in penetration testing.	Chapter 8
2.0 Architecture and Design	2.1 Explain the importance of security concepts in an enterprise environment.	Chapter 9
2.0 Architecture and Design	2.2 Summarize virtualization and cloud computing concepts.	Chapter 10
2.0 Architecture and Design	2.3 Summarize secure application development, deployment, and automation concepts.	Chapter 11
2.0 Architecture and Design	2.4 Summarize authentication and authorization design concepts.	Chapter 12
2.0 Architecture and Design	2.5 Given a scenario, implement cybersecurity resilience.	Chapter 13
2.0 Architecture and Design	2.6 Explain the security implications of embedded and specialized systems.	Chapter 14
2.0 Architecture and Design	2.7 Explain the importance of physical security controls.	Chapter 15
2.0 Architecture and Design	2.8 Summarize the basics of cryptographic concepts.	Chapter 16
3.0 Implementation	3.1 Given a scenario, implement secure protocols.	Chapter 17
3.0 Implementation	3.2 Given a scenario, implement host or application security solutions.	Chapter 18
3.0 Implementation	3.3 Given a scenario, implement secure network designs.	Chapter 19
3.0 Implementation	3.4 Given a scenario, install and configure wireless security settings.	Chapter 20
3.0 Implementation	3.5 Given a scenario, implement secure mobile solutions.	Chapter 21
3.0 Implementation	3.6 Given a scenario, apply cybersecurity solutions to the cloud.	Chapter 22
3.0 Implementation	3.7 Given a scenario, implement identity and account management controls.	Chapter 23

Exam Domain	Objective	Chapter in Book That Covers It
3.0 Implementation	3.8 Given a scenario, implement authentication and authorization solutions.	Chapter 24
3.0 Implementation	3.9 Given a scenario, implement public key infrastructure.	Chapter 25
4.0 Operations and Incident Response	4.1 Given a scenario, use the appropriate tool to assess organizational security.	Chapter 26
4.0 Operations and Incident Response	4.2 Summarize the importance of policies, processes, and procedures for incident response.	Chapter 27
4.0 Operations and Incident Response	4.3 Given an incident, utilize appropriate data sources to support an investigation.	Chapter 28
4.0 Operations and Incident Response	4.4 Given an incident, apply mitigation techniques or controls to secure an environment.	Chapter 29
4.0 Operations and Incident Response	4.5 Explain the key aspects of digital forensics.	Chapter 30
5.0 Governance, Risk, and Compliance	5.1 Compare and contrast various types of controls.	Chapter 31
5.0 Governance, Risk, and Compliance	5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.	Chapter 32
5.0 Governance, Risk, and Compliance	5.3 Explain the importance of policies to organizational security.	Chapter 33
5.0 Governance, Risk, and Compliance	5.4 Summarize risk management processes and concepts.	Chapter 34
5.0 Governance, Risk, and Compliance	5.5 Explain privacy and sensitive data concepts in relation to security.	Chapter 35

The Chapter Elements

Each *Exam Cram* book has chapters that follow a predefined structure. This structure makes *Exam Cram* books easy to read and provides a familiar format for all *Exam Cram* books. The following elements typically are used:

- Chapter topics
- Essential Terms and Components

- Cram Quizzes
- ExamAlerts
- Notes
- Available exam preparation software practice questions and answers

Note

Bulleted lists, numbered lists, tables, and graphics are also used where appropriate. A picture can paint a thousand words sometimes, and tables can help to associate different elements with each other visually.

Now let's look at each of the elements in detail:

- **Chapter topics:** Each chapter contains details of all subject matter listed in the table of contents for that particular chapter. The objective of an *Exam Cram* book is to cover all the important facts without giving too much detail. When examples are required, they are included.
- **Essential Terms and Components:** The start of every chapter contains a list of terms and concepts you should understand. These are all defined in the book's accompanying Glossary.
- **Cram Quizzes:** Each chapter concludes with multiple-choice questions to help ensure that you have gained familiarity with the chapter content.
- **ExamAlerts:** ExamAlerts address exam-specific, exam-related information. An ExamAlert addresses content that is particularly important, tricky, or likely to appear on the exam. An ExamAlert looks like this:

ExamAlert

Make sure you remember the different ways in which you can access a router remotely. Know which methods are secure and which are not.

- **Notes:** Notes typically contain useful information that is not directly related to the topic currently under consideration. To avoid breaking up the flow of the text, they are set off from the regular text.

Note

This is a note. You have already seen several notes.

Other Book Elements

Most of this *Exam Cram* book on Security+ follows the consistent chapter structure already described. However, there are various important elements that are not part of the standard chapter format. These elements apply to the entire book as a whole.

- **Practice questions:** Exam-preparation questions conclude each chapter.
- **Answers and explanations for practice questions:** These follow each practice question, providing answers and explanations to the questions.
- **Glossary:** The Glossary defines important terms used in this book.
- **Cram Sheet:** The Cram Sheet is a quick-reference, tear-out cardboard sheet of important facts that is useful for last-minute preparation. The Cram Sheet provides a simple summary of the facts that may be most difficult to remember.
- **Companion website:** The companion website for your book allows you to access several digital assets that come with your book, including the following:
  - Pearson Test Prep software (both online and Windows desktop versions)
  - Key Terms Flash Cards application
  - A PDF version of the Cram Sheet

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

1. Register your book by going to **PearsonITCertification.com/register** and entering the ISBN 9780136798675.
2. Respond to the challenge questions.
3. Go to your account page and select the **Registered Products** tab.
4. Click on the **Access Bonus Content** link under the product listing.

Pearson Test Prep Practice Test Software

As noted previously, this book comes complete with the Pearson Test Prep practice test software. 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.

3. Go to your account page and select the **Registered Products** tab.
4. Click on the **Access Bonus Content** link under the product listing.
5. Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to download the software.
6. After the software finishes downloading, unzip all the files onto your computer.
7. Double-click the application file to start the installation and follow the onscreen instructions to complete the registration.
8. When the installation is complete, launch the application and click the **Activate Exam** button on the My Products tab.
9. Click the **Activate a Product** button in the Activate Product Wizard.
10. Enter the unique access code from the card in the sleeve in the back of your book and click the **Activate** button.
11. Click **Next** and then click the **Finish** button to download the exam data to your application.
12. To start using the practice exams, select the product and click the **Open Exam** button to open the exam settings screen.

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

Customizing Your Exams

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

- Study Mode
- Practice Exam Mode
- Flash Card Mode

Study Mode allows you to fully customize your exams and review answers as you are taking the exam. This is typically the mode you use first to assess your knowledge and identify information gaps. Practice Exam Mode locks certain customization options, as it presents 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 can select the source of your questions. You can choose to take exams that cover all of the chapters, or you can narrow your selection to just a single chapter or the chapters that make up specific parts in the book. All chapters are selected by default. If you want to narrow your focus to individual chapters, simply deselect all the chapters and then select only those on which you wish to focus in the Objectives area.

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

There are several other customizations you can make to your exam from the exam settings screen, such as the time you are allowed for taking 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. You must be 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 an 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.

Contacting the Author

Hopefully, this book provides you with the tools you need to pass the Security+ exam. Feedback is appreciated. You can follow and contact the author on Twitter @martyweiss.

Thank you for selecting my book; I have worked to apply the same concepts in this book that I have used in the hundreds of training classes I have taught. Spend your study time wisely and you, too, can achieve the Security+ designation. Good luck on the exam, although if you carefully work through this text, you will certainly minimize the amount of luck required!

CHAPTER 7

Security Assessment Techniques

This chapter covers the following official Security+ exam objective:

- 1.7 Summarize the techniques used in security assessments.

Essential Terms and Components

- threat hunting
- vulnerability scan
- CVE/CVSS
- security information and event management (SIEM)
- security orchestration, automation, and response (SOAR)

A number of tools and techniques are available to help organizations conduct security assessment. Identifying vulnerabilities and threats is key to maintaining organizational security. In addition to identifying vulnerabilities, organizations need an approach to assess threats against their systems. A myriad of solutions are available. In the past, an organization first needed to move beyond simple log management and find a method to efficiently store and analyze log data across all of its networks, devices, and applications. Security information management (SIM) was the solution. Then, in addition, the data needed to be analyzed in real time to provide correlation across events and enable alerts and reporting. Security event management (SEM) was the solution in this case. SIM and SEM were eventually combined into what's known today as security information and event management (SIEM). This chapter looks at security assessment techniques, including how they are combined and continue to evolve.

Vulnerability Scans

Many network scanners are designed to be passive and non-intrusive to the target systems. Passive scanning poses minimal risk to the assessed environment because it is designed to avoid interfering with normal activity or degrading performance. However, tests against the system can affect network and system performance. A comprehensive *vulnerability scan* helps an organization identify vulnerabilities, uncover common misconfigurations, and understand where further security controls are required. The following points briefly summarize these three goals:

- **Identify vulnerability:** Vulnerabilities include outdated software versions that contain flaws or are missing patches.
- **Identify common misconfigurations:** Vulnerability scanners can identify many common misconfigurations. Some scanners are even capable of remediation. Checking for misconfigurations is most beneficial when deployed configurations are compared against an organization's security policies and standards.
- **Identify lack of security controls:** Identifying vulnerabilities provides an opportunity to remediate weaknesses. In some cases, organizations may find that they need to implement more security controls to mitigate the risk.

Vulnerability scanners fall into three broad categories, based on the devices they evaluate:

- **Network scanners:** This type of scanner probes hosts for open ports, enumerates information about users and groups, and proactively looks for known vulnerabilities.
- **Application scanners:** This type of scanner requires access to application source code or binaries but does not need to actually execute the application. Thus, this type of scanner tests an application from the inside. Application scanning supports all types of applications and is also known as static application security testing (SAST).
- **Web application scanners:** This type of scanner applies specifically to web applications and identifies vulnerabilities such as cross-site scripting, SQL injection, and path traversal. This type of scan executes an application and tests from the outside in. This type of scanning is known as dynamic application security testing (DAST).

A network vulnerability scanner, for example, is a software utility that scans a range of IP addresses, testing for the presence of known vulnerabilities in software configuration and accessible services. A traditional vulnerability scanner relies on a database of known vulnerabilities. It is an automated tool that can be directed at a targeted system or systems. Unlike systems that test for open ports, which test only for the availability of services, vulnerability scanners can check for the version or patch level of a service to determine its level of vulnerability.

Keep in mind that a vulnerability does not necessarily indicate an issue that needs to be immediately remediated—or even remediated at all. Using an analogy, consider a home as a subject for a vulnerability assessment. A broken deadbolt lock certainly seems like a vulnerability. Ideally, the homeowner would replace it; however, in some parts of the world, residents do not lock their doors anyway. A smashed window is a vulnerability as well. In some cases, it might make sense to mitigate a broken window simply by covering it with plastic to protect against the elements. Even a perfectly functioning window is a vulnerability, however. The benefit a window offers typically outweighs the benefits gained by living without windows. What is counted as a vulnerability typically depends on what you are trying to protect.

Upon completion of a vulnerability scan, an organization can generally choose to take one of three approaches:

- **Remediation:** The organization can patch the vulnerability.
- **Mitigation:** The organization can introduce a control to reduce the likelihood of the vulnerability being exploited or the impact if it is exploited.
- **Acceptance:** The organization can take no action if the risk is low, especially compared with the cost or operational impact of addressing the vulnerability.

There isn't necessarily a quick method for determining risk based on the output of a vulnerability scanner. Relevancy to the business, trade-offs, and identified threats and likelihoods need to be considered to accurately interpret the results.

Vulnerability scanners rely heavily on catalogs of known vulnerabilities. Two standards are commonly used, both of which are open industry standards:

- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS)

CVE is a standard for identifying vulnerabilities. It is designed to allow vulnerability databases to be linked together and does not contain attributes such as risk, impact, remediation steps, or detailed technical information. It primarily includes a description and a unique identifier assigned by the vendor where a patch has been provided to fix the vulnerability. CVE also includes related references, such as vulnerability reports and advisories.

On the other hand, CVSS is a framework for communicating the characteristics and severity scores of vulnerabilities. A CVSS score is a rating from 0 to 10. Calculation of the score is complex and takes various components into consideration, such as how easy it would be to exploit the vulnerability. CVSS scoring seeks to address the following questions:

- What is the attack vector? Does it require physical access, or can it be exploited over the network?
- What is the attack complexity?
- Are elevated privileges required?
- Is user interaction required?

ExamAlert

CVE is a list of publicly known vulnerabilities containing an ID number, description, and reference. CVSS provides a score from 0 to 10 that indicates the severity of a vulnerability.

Note

In U.S. government agencies, vulnerability is discussed using the Open Vulnerability Assessment Language (OVAL), sponsored by the Department of Homeland Security's National Cyber Security Division (NCSD). OVAL is intended to be an international language for representing vulnerability information. It uses an Extensible Markup Language (XML) schema for expression, allowing tools to be developed to test for identified vulnerabilities in the OVAL repository. OVAL vulnerabilities are based on CVE data.

Intrusive vs. Non-Intrusive

Vulnerability tests seldom disrupt systems. However, an initial port scan can cause a system to fail, particularly if the implementation of a particular service does not follow proper standards. Intrusive scans aim to verify vulnerabilities by trying to exploit them. Organizations should take care before initiating such intrusive tests.

ExamAlert

Non-intrusive or non-invasive testing helps an organization minimize disruptions related to vulnerability assessment.

Credentialed vs. Non-Credentialed

Credentials such as usernames and passwords enable authorized access to a system. Scanners can be configured to run in either credentialed or non-credentialed mode. *Non-credentialed scans* are less invasive and provide an outsider's point of view. With *credentialed scans*, however, the system can ascertain more information, which results in a more complete vulnerability status with greater certainty. Both credentialed and non-credentialed scans can mistakenly identify a vulnerability when none exists; this is known as a *false positive*. Confirming a large number of false positives can be time-consuming and places a burden on IT resources. Credentialed scans tend to reduce false positives and can also reduce the opposite effect: *false negatives*. False negatives are more difficult to see than false positives. A false negative is a lack of result when there should be one. A false negative may occur, for example, when a vulnerability is new, and a check has not been developed yet to look for the vulnerability.

ExamAlert

With a false positive, a security scanner detects or flags a vulnerability when one does not exist. A false negative is the opposite: It is a lack of alert about a vulnerability when one actually exists.

Threat Assessment

Since evolving from SIM and SEM, SIEM has for years played a vital role in identifying threats and detecting security incidents. Now organizations are looking for ways to combine threat intelligence with SIEM as the intelligence gained can provide enriched data with greater context through correlation with external information. One trend that has emerged in recent years is that organizations now tend to assume that they have already been breached. Rather than be reactive, security teams look for ways to be proactive rather than simply respond to incidents. Targeted threat hunting assessments have gained popularity as a result, and the programs and tools continue to evolve.

Security Information and Event Management (SIEM)

A *security information and event management* (*SIEM*) system provides the technological means to accomplish a number of goals related to security monitoring, including the following:

- Identifying internal and external threats
- Monitoring activity and resource usage
- Conducting compliance reporting for internal and external audits
- Supporting incident response

SIEM tools collect and correlate and subsequently provide alerts and information dashboards based upon that data. SIEM output can be used proactively to detect emerging threats and improve overall security by defining events of interest (EOI) and resulting actions. SIEM systems are the main element in compliance regulations such as SOX, GLBA, PCI, FISMA, and HIPAA. SIEM systems provide a plethora of fine-grained details to support incident response programs. The purpose of SIEM is to store and turn a large amount of data into knowledge that can be acted upon. SIEM systems are generally part of the overall security operations center (SOC) and have three basic functions:

- Centrally managing security events
- Correlating and normalizing events for context and alerting
- Reporting on data gathered from various applications

ExamAlert

Individual log data sources can generate more than 100,000 events each day, so answering critical questions about how much data to log from critical systems is important when deciding to use a SIEM system.

Consider, for example, that just one intrusion detection sensor or log data source can generate more than 100,000 events each day. SIEM systems rely on *log collectors*, which are responsible for aggregating and ingesting the log data from the various sources such as security devices, network devices, servers, and applications. *Log aggregation* is the process by which SIEM systems combine similar events to reduce event volume. SIEM systems aggregate data from many network sources and consolidate the data so that crucial events are not missed. By default, events are usually aggregated based on the source IP address, destination IP address, and event ID. The purposes of aggregation are to reduce the event data load and improve efficiency. Conversely, if aggregation is incorrectly configured, important information could be lost. Confidence in this aggregated data is enhanced through techniques such as correlation, automated data filtering, and deduplication within the SIEM system.

Event aggregation alone is not enough to provide useful information in an expeditious manner. A common best practice is to use a correlation engine to automate threat detection and log analysis. The main goal of correlation is to build EOIs that can be flagged by other criteria or that allow for the creation of incident identification. To create EOIs, the correlation engine uses data aggregated by using the following techniques:

- Pattern matching
- Anomaly detection
- Boolean logic
- A combination of Boolean logic and context-relevant data

Finding the correct balance in correlation rules is often difficult. Correlation rules that try to catch all possible attacks generate too many alerts and can produce too many false-positive alerts.

A SIEM facilitates and automates alert triage to notify analysts about immediate issues. Alerts can be sent via email but are most often sent to a dashboard. To help with the large volume of alerts and notifications that SIEM systems generate, these systems typically provide data visualization tools. From a business perspective, reporting and alerting provide verification of continuous monitoring, auditing, and compliance. Event deduplication improves confidence in aggregated data, data throughput, and storage capacity. Event deduplication is also important because it provides the capability to audit and collect forensic data. The centralized log management and storage in SIEM systems provide validation for regulatory compliance storage or retention requirements. Regarding forensic data and regulatory compliance, WORM (write once read many) drives keep log data protected so that evidence cannot be altered. WORM drives permanently protect administrative data. This security measure should be implemented when an administrator with access to logs is under investigation or when an organization is discussing regulatory compliance.

Some SIEM systems are good at ingesting and querying flow data both in real time and retrospectively. However, significant issues are associated with time, including time synchronization, time stamping, and report time lag. For example, if a report takes 45 minutes to run, the analyst is already that far behind real time, and then time is also needed to read and analyze the results.

When designing a SIEM system, the volume of data generated for a single incident must be considered. SIEM systems must aggregate, correlate, and report output from devices such as firewalls, intrusion detection/prevention systems (IDSs/IPSs), access controls, and myriad network devices. How much data to log from critical systems is an important consideration when deciding to use a SIEM system.

SIEM systems have high acquisition and maintenance costs. If the daily events number in the millions per day and events are gathered from network devices, endpoints, servers, identity and access control systems, and application servers, a SIEM might be cost-effective. For smaller daily event occurrences, free or more cost-effective tools should be considered.

Note

SIEM systems can aggregate syslog data. Syslog is a decades-old standard for message logging. It is available on most network devices (such as routers, switches, and firewalls), as well as printers and Unix/Linux-based systems. Over a network, a syslog server listens for and then logs data messages coming from the syslog client.

SIEM systems continue to evolve to capture more and more use cases and to be combined with other solution sets. SIEM systems, for example, continue to help secure organizations against threats. Consider user behavior analysis, for example. A SIEM system can establish a baseline for user activity and identify anomalous behavior that deviates from that baseline. This often involves advanced techniques such as machine learning, and the SIEM system needs to be capable of comparing data across time horizons and across groups, such as the department the user works in. More recently, this data has been combined to perform *sentiment analysis*: Data can be tracked and analyzed to look for patterns that rely on human sentiment. In this way, systems are able to recognize threats before they become threats. This type of analysis should leverage external data sources, including those from the public domain. As discussed in the next section, SIEM systems are now being combined with other functions to perform security assessments.

ExamAlert

Know that sentiment analysis studies human emotions present within data—for example, negative, neutral, or positive opinions or attitudes. This data can be tracked and analyzed to look for patterns that rely on human sentiment.

Threat Hunting

Threat hunting is a proactive approach to finding an attacker before alerts are triggered. It is not reactive or detective. A reactive approach requires data such as the data a SIEM system provides; a detective approach relies on the use of various algorithms and rules. Threat hunting has the following key attributes:

- **Hypothesis:** Threat hunting starts with a hunch, often based on clues. Drivers may include analytics such as user behavior analytics, situational awareness (for example, based on internal risk assessment, trends, or high-value targets), and intelligence based on intelligence bulletins, intelligence feeds, or vulnerability scans.
- **People:** While many sources—such as those discussed in Chapter 5, "Threat Actors, Vectors, and Intelligence Sources," and earlier in this chapter—are used, threat hunting is centered around the security analyst, who has deep expertise and knowledge of the organization's environment.
- **Assumptive:** Threat hunting does not take a breach-preventive approach but rather assumes that the organization has already been breached.
- **Iterative:** Much like a penetration tester, a threat hunter must pivot frequently in order to continue lateral movement while seeking further evidence.

Throughout the process, a threat hunter is looking to disrupt the attacker during any phase of what's known as the *cyber kill chain*, which is a framework developed to track the steps or phases that an attacker goes through as part of an intrusion. (We examine the cyber kill chain more closely in Chapter 27, "Incident Response.") The threat hunting process combined with knowledge of the cyber kill chain allows a security analyst to quickly outmaneuver an attacker. The goal of the security team is to completely disrupt the attacker or quickly impede the attacker's ability to move across the attack chain.

A threat hunter relies on a number of intelligence sources, such as a SIEM system and external sources. Recall that in Chapter 5, we discussed various open and closed sources of threat intelligence and research. All the gathered data may be intelligently pulled together using commercially available software and services. This bringing together of internal and external threat feeds is known as *intelligence fusion*, and it enables an organization to establish a more accurate threat profile. Internal and external sources are defined as follows:

- **Internal threat data:** Internal threat data consists of alert and event data from the SIEM system and any other raw log sources. It includes previous knowledge about prior attacks, including vulnerabilities exploited, previous indicators of compromise, details about the attacker, and packet captures. Baseline data on network traffic also makes it possible to understand what's expected and aid in identifying anomalies.
- **External threat data:** External threat data consists of structured threat information such as STIX, as well as unstructured data from security advisories, bulletins, and other OSINT tools. External threat feeds from security organizations providing such data as a service can also be used as data sources. Attacks across organizations are often similar in their techniques. Chances are good that your organization isn't the first to see an attacker and his or her methods, and external threat data can give you a warning about what is happening elsewhere.

Fusion analysis can aid in processing data and yielding more meaningful insights to provide a comprehensive look at the threats to an organization. This analysis can even compare internal telemetry data with external data to provide prioritized insight. A threat hunter with good threat data can more quickly identify indicators of compromise and indicators of attacks. Some intelligence platforms integrate with and can also provide capabilities to automate and orchestrate the actions required by security.

Security Orchestration, Automation, and Response (SOAR)

Security orchestration, automation, and response (*SOAR*) tools can aggregate intelligence from internal and external sources to provide fusion analysis and other insights. SOAR combines data and also provides for case management and automated workflow. Gartner, a leading technology research company, came up with the idea of SOAR. According to Gartner, SOAR primarily does three things:

- Threat and vulnerability management
- Security incident response
- Security operations automation

You can see that, as a combined platform, a SOAR solution combines security orchestration and automation (SOA) with threat intelligence platforms (TIP) and incident response platforms (IRP). SOAR works with and augments SIEM. Gartner expects that in the future these capabilities will merge.

ExamAlert

SOAR integrates all the security tools available in an organization and then automates incident responses.

Cram Quiz

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

1. After conducting a vulnerability assessment, which of the following is the best action to perform?

❍ **A.** Disable all vulnerable systems until mitigating controls can be implemented.

❍ **B.** Contact the network team to shut down all identified open ports.

❍ **C.** Immediately conduct a penetration test against identified vulnerabilities.

❍ **D.** Organize and document the results based on severity.

2. Your team is tasked with conducting a vulnerability assessment and reports back with a high number of false positives. Which of the following might you recommend to reduce the number of false positives?

❍ **A.** Have the team run a vulnerability scan using non-credentialed access.

❍ **B.** Have the team run a vulnerability scan using credentialed access.

❍ **C.** Have the team run a port scan across all common ports.

❍ **D.** Have the team run a port scan across all ports.

3. SOAR combines functions from which of the following? (Select three.)

❍ **A.** Security orchestration and automation

❍ **B.** Incident response platforms

❍ **C.** Threat intelligence platforms

❍ **D.** Penetration tests

4. Which of the following studies human emotions in data to detect patterns such as negative, positive, or neutral opinions or attitudes?

○ **A.** False positive

○ **B.** False negative

○ **C.** Sentiment analysis

○ **D.** Log aggregation

Cram Quiz Answers

Answer 1: D. After an assessment, the results should be organized based on the severity of risk to the organization. Answer A is incorrect because it is generally an extreme response, except in rare situations. Answer B is incorrect because many open ports are required for a network to function. Answer C is incorrect because, although a penetration test often does follow a vulnerability scan, it is not an immediate necessity and certainly is not required for all identified vulnerabilities.

Answer 2: B. Non-credentialed vulnerability scans result in a greater number of false positives. This type of scan provides an outsider point of view, and although it might indicate what an outsider is more likely to see, it does not show as effectively the full extent of vulnerabilities. A credentialed vulnerability scan provides access to systems that might otherwise not be accessible, making it possible to further determine legitimate vulnerabilities. As a result, answer A is incorrect. Answers C and D are incorrect because vulnerability scans initially do scan specified ports as part of the process.

Answer 3: A, B, and C. Security orchestration, automation, and response (SOAR) combines functions from security orchestration and automation, incident response platforms, and threat intelligence platforms either as a complete solution or as an integrated solution. Penetration tests are not part of the SOAR platform, so answer D is incorrect.

Answer 4: C. Sentiment analysis studies human emotions present within data, such as negative, neutral, or positive opinions or attitudes. The data can be tracked and analyzed to look for patterns that rely on human sentiment. Answers A and B are incorrect because a false positive occurs when a security scanner detects or flags a vulnerability when one does not exist and a false negative says you don’t have a vulnerability when in fact you do. Answer D is incorrect. Log aggregation is the process by which SIEM systems combine similar events to reduce event volume. SIEM systems aggregate data from many network sources and consolidate the data so that crucial events are not missed.

What Next?

If you want more practice on this chapter’s exam objective before you move on, remember that you can access all of the Cram Quiz questions on the Pearson Test Prep software online. You can also create a custom exam by objective with the Online Practice Test. Note any objective you struggle with and go to that objective’s material in this chapter.

Index

Numbers

3DES (Triple Data Encryption Standard), 289

802.11, 375

802.1X standard, 201, 372, 459

A

AAA (Authentication, Authorization, and Accounting), 189–190
- RADIUS, 459–460
- TACACS+, 460–461

ABAC (Attribute-Based Access Control), 468–469

AC (Access Controllers), 379–380

acceptable use policies, mobile device deployments, 415–416

accepting risk, 600

access
- authentication, 456
- conditional access, 468
- control, 466–467
  - ABAC, 468–469
  - conditional access, 468
  - DAC, 467
  - MAC, 467
  - PAM, 469
  - RBAC, 467–468
- logs, 533–534
- TACACS+, 460–461
- user access
  - auditing/reviews, 436–437
  - logical access controls, 439–440
  - recertification, 436
- violations, 456
- wireless networks, 371–372
  - AC, 379–380
  - antenna placement, 381

  - AP, 379–380, 381
  - directional antennas, 380–381
  - intelligent antennas, 380
  - omnidirectional antennas, 380–381
  - WLAN controllers, 379–380

accidental threats, 601

accounting (AAA), 189–190

accounts

- lockouts, 30
- managing
  - access auditing/reviews, 436–437
  - access controls, 439–440
  - account expiration, 442
  - account policy enforcement, 441–442
  - administrative accounts, 434
  - IdP, 435
  - least privilege, 436
  - location restrictions, 438–439
  - lockouts, 443–444
  - logon hours, 438
  - offboarding, 435–436
  - onboarding, 435–436
  - time of date, 438
  - types, 433–435
  - UAC, 435
- passwords
  - age, 444–445
  - blank passwords, 434
  - complexity, 442
  - forgotten passwords, 443
  - history, 445
  - length, 445–446
  - rotating, 446

ACS (Audit Collection Services), 456

actors, threat, 73–74

- APT, 79
- attack vectors, 80–81
- attributes, 74–75
- competitors, 78–79
- criminal syndicates, 78
- hackers, 76
- hacktivists, 78
- inside threat actors, 77
- script kiddies, 76–77
- state actors, 79
- types (overview), 75–76

AD DS (Active Directory Domain Services), account policy enforcement, 442

adapters, malware, 27

adb (Android Debug Bridge), 408

addressing

- network address allocation, 299–302
- VIP addresses, 211

administrative accounts, 434

adminitrators, system, 587

adversarial AI, 27–28

adversarial threats, 601

adverse actions/disciplinary policies, 591–592

advertising, pop-up blockers, 313

adware, 25–26

after-action reports, 526

age of passwords, 444–445

agreement (privacy), terms of, 614

AH (Authentication Headers), IPsec, 285

AI (Artificial Intelligence)

- adversarial AI, 27–28
- ML, 27–28

air gaps

- equipment security, 248
- network segmentation, 350

aircraft, embedded control systems, 235–236

AirDroid, 408

AIS (Automated Indicator Sharing), 83

aisles, hot/cold, 254–255

alarms, internal security, 244

ALE (Annual Loss Expectancy), 606

algorithms
asymmetric algorithms, 266–268
cryptography, 262
private key encryption, 267–268
public key encryption, 266–268
spanning tree algorithms, 346
symmetric algorithms, 264–266
analyzers
code analyzers, 318–319
dynamic code analysis, 319–320
fuzzing, 319–320
static code analyzers, 319
incidents, incident response, 518–519
protocol analyzers, 502–504
risk, 598
Wi-Fi analyzers, 381
anomaly-based detection, 363, 535
ANT+ communication, 392
antennas
directional antennas, 380–381
intelligent antennas, 380
omnidirectional antennas, 380–381
placement, 381
anti-malware, 311–312
antispam software, 312–313
antispyware programs, 313
antivirus software, 310–312, 417
AP (Access Points), 379–380
antenna placement, 381
fat AP, 380
fit AP, 380
intelligent access points, 380
rogue AP, 55
standalone AP, 380
thin AP, 380
API (Application Programming Interface)
attacks, 47–48
availability, 137
confidentiality, 137
integrity, 137
microservices, 148–149
appetite, risk, 599
application attacks, 36
API attacks, 47–48
buffer overflows, 38
code injection, 39
DLL injection, 39, 40
LDAP injection, 40
SQL injection, 39
XML injection, 40
XSS, 39
directory traversal, 44–45
driver manipulation, 40–41
refactoring, 41
shimming, 41
improper error handling, 37
improper input handling, 37
integer overflows, 38
memory leaks, 37
overflows, 38
pass-the-hash attacks, 49
privilege escalation, 36
race conditions, 36
replay attacks, 45
request forgeries, 41
CSRF, 41–43
SSRF, 42–43
resource exhaustion, 37
SSL stripping, 45–46
TOCTOU, 36
applications
API
availability, 137
confidentiality, 137
integrity, 137
microservices, 148–149
blacklists, 317, 396
incident mitigation, 546
camouflage, 174
change management, 169–170

coding
code reuse, 174–175
dead code, 174–175
containerization, 394
deploying, 167
automation, 180
CD, 182–184
CI, 182–184
production environments, 167
staging, 167
deprovisioning, 168
developing, 166–167
automation, 180–181
camouflage, 174
CD, 182–183
change management, 169–170
CI, 182–183
client-side validation, 175–176
code reuse, 174–175
code signing, 178–179
data exposure, 176–179
dead code, 174–175
DevOps, 170, 181–184
drivers, 178–179
elasticity, 184–185
encryption, 173
error handling, 176–177
fuzzing, 172
input validation, 177–178
integrity measurement, 168–169
memory management, 179
obfuscation, 173–174
provisioning, 168
QA, 167
resiliency, 180
scalability, 184
SDK, 175
secure coding, 170
server-side validation, 176
staging, 167
stored procedures, 173
third-party libraries, 175
version control, 170
elasticity, 184–185
encryption, 173
fuzzing, 319–320
integrity measurement, 168–169
logs, 531–532
MAM, 394, 395–397
normalization, 172–173
obfuscation, 173–174
production environments, 167
provisioning, 168
QA, 167
sandboxing, 321, 394
scalability, 184
secure coding, 170, 171–172
CSSLP, 171
OWASP, 170–171
SAFECode, 171
security
code analyzers, 318–320
code signing, 318
sandboxing, 321
secure cookies, 318
stress testing, 321
sideloading, 408
staging, 167
stored procedures, 173
testing, 166–167
third-party app stores, 407–408
validation
client-side validation, 175–176
server-side validation, 176
VBA, 69
version control, 170
vulnerability scanners, 100
web application firewalls, 317
whitelists, 317, 396, 545–546
APT (Advanced Persistent Threats), 79
AR (Access Requestors), NAC, 365

architectures, mobile device deployments, 414–415
armored viruses, 18, 19
ARO (Annual Rate of Occurrence), 606
ARP (Address Resolution Protocol), 497
  poisoning, 60–61
  RARP, 60–61
arrays, FPGA, 227
ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers), 254–255
assessments
  PIA, 621–622
  risk, 598, 602–604
  security
    cloud computing vulnerabilities, 429
    SIEM, 103–107
    SOAR, 108–109, 546–548
    threat hunting, 107–108
    vulnerability scanners, 100–103
  threats, 601–602
asymmetric cryptography, 266–268
ATT&CK (Adversary Tactics, Techniques, and Procedures), 82
attack phase, penetration testing, 117
attacks
  application attacks, 36
    API attacks, 47–48
    buffer overflows, 38
    code injection, 39–40
    directory traversal, 44–45
    driver manipulation, 40–41
    improper error handling, 37
    improper input handling, 37
    integer overflows, 38
    memory leaks, 37
    overflows, 38
    pass-the-hash attacks, 49
    race conditions, 36
    replay attacks, 45
    request forgeries, 41–43
    resource exhaustion, 37
    SSL stripping, 45–46
  cryptographic attacks
    birthday attacks, 30–31
    downgrade attacks, 31
    man-in-the-middle attacks, 31
  crypto-malware, 23
    CryptoLocker, 24
    WannaCry, 24, 141
  DoS attacks, 332
  frameworks, incident response, 509
    cyber kill chains, 510
    Diamond Model of Intrusion Analysis, 511
    documented incident types, 513
    incident response plans, 512–513
    MITRE ATT&CK, 510–511
  malware, 16
    adware, 25–26
    blended threats, 16
    botnets, 22–23
    bots, 22–23
    cryptojacking, 26
    crypto-malware, 23–24
    cryptomining, 26
    logic bombs, 22
    macros, 16, 17
    memory, 16
    PUP, 25–26
    ransomware, 23–24
    registries, 16
    rootkits, 20–21
    spyware, 25
    Trojans, 19–20
    viruses, 17–19
    worms, 19
    zombie armies, 22
  network attacks, 54
    ARP poisoning, 60–61
    bluejacking, 56
    bluesnarfing, 56

Bluetooth attacks, 56
confidentiality, 57
DDoS attacks, 66–68
deauthentication attacks, 55
dissociation attacks, 55
DNS poisoning, 63–64
domain hijacking, 62
DoS attacks, 57, 64–66
fraggle attacks, 65
IV attacks, 55–56
jamming attacks, 54–55
land attacks, 65
Layer 2 attacks, 59–60
MAC flooding, 61
MAC spoofing, 60
malicious code/script execution, 57, 68–69
MITB attacks, 59
MITM attacks, 57, 58–59
NFC attacks, 57
ping flooding, 65
port stealing, 61
RARP, 60–61
RFID attacks, 57–58
rogue AP, 55
smurfing attacks, 65
SYN flooding, 65
teardrop attacks, 65
URL redirection, 62–63
wireless networks, 54–56
password attacks, 28–29
brute-force attacks, 29
dictionary attacks, 29
hybrid attacks, 29–30
password spraying, 30
rainbow tables, 30
physical attacks
adapters, 27
adversarial AI, 27–28
cables, 27
card cloning, 27
peripheral devices, 26–27
skimming, 27
USB flash drives, 26–27
PUP, 25
adware, 25–26
cryptojacking, 26
cryptomining, 26
spyware, 25
slag code, 22
social engineering, 4–5
credential harvesting, 8
dumpster diving, 5–6
hoaxes, 10
hybrid warfare, 10
identity fraud, 4–5
influence campaigns, 10
invoice scams, 8
pharming, 8
phishing, 7–8
prepending notifications, email, 7
principles of influence, 10–12
reconnaissance, 4–5
shoulder surfing, 6
smishing, 8
spear phishing, 7
SPIM, 7
tailgating, 5
typo squatting, 9
vishing, 8
watering hole attacks, 9
whaling, 7
Trojans, 19–20
backdoor Trojans, 20
downloader Trojans, 20
infostealer Trojans, 20
keylogger Trojans, 20
RAT, 20
vectors, 80–81
viruses, 17, 19
armored viruses, 18, 19
boot sector viruses, 17

file-infecting viruses, 18
macro viruses, 17
multipartite viruses, 18
nonresident viruses, 17
polymorphic viruses, 18, 19
program-infecting viruses, 18
resident viruses, 17
stealth viruses, 18

attestation, 193
boot attestation, 328–329
TPM, 325, 328

auditing
ACS, 456
logs, 533
user access, 436–437
user permissions, 453

AUP (Accessible Use Policies), 589–590

authentication, 450
802.1X standard, 459
AAA, 189–190
access violations, 456
ACS, 456
attestation, 193
biometrics, 198–199
CER, 200
efficacy rates, 200
facial recognition, 199
FAR, 200
fingerprints, 199
FRR, 200
gaits, 199
hand geometry, 199
retinas, 199
signatures, 199
veins/blood vessels, 199
voiceprints, 199
CAC, 202
CCMP, 376
certificate-based authentication, 201–202
CHAP, 457–458
context-aware authentication, 399
deauthentication attacks, 55
EAP, 372–373, 377, 458
EAP-FAST, 378–379
EAPoL, 377–378
EAP-TLS, 377, 379
EAP-TTLS, 378, 379
federated identity systems, 193–194, 461–464
filesystem permissions, 452
auditing, 453
group policies, 453
Linux, 455–456
Manning, Chelsea, 452
Windows, 453–455
HOTP, 196, 198
HSM, 451
IEEE 802.1X authentication, 201
issues, 457
KBA, 450–451
Kerberos, 464–466
key fobs, 196
managing, 450–451
mobile devices, 395–396
MSCHAP, 458
multifactor authentication, 190–192
OTP, 196–198
PAP, 457–458
password vaults, 450–451
PEAP, 378, 379, 458–459
phone callbacks, 198
PIV cards, 201–202
private keys, 481
proximity cards, 195, 200–201
PSK, 372
RADIUS, 459–460
realms, 460
SAE, 377
SAML, 461–462
security tokens, 195–198

Shibboleth, 464
SMS OTP, 198
SSO, 192–193
static codes, 198
TACACS+, 460–461
token keys, 198
TOTP, 196, 198
TPM, 451
transitive trust, 194–195
unencrypted plaintext credentials, 451–452
user permissions, 452
auditing, 453
Manning, Chelsea, 452

authoritative servers, DNS, 284

authority, principles of influence, 10–11

authorization
AAA, 189–190
access control, 466–469
federated identity systems, 461–464
OAuth, 462–463
OpenID Connect, 463–464
RADIUS, 459–460
SAML, 461–462
TACACS+, 460–461

automation
application development, 180–181
home automation, IoT, 230

automobiles, embedded control systems, 234–235

Autopsy, 506

availability
API, 137
data
configuration management, 136–139
geographic considerations, 138–139
site resiliency, 137–138
sovereignty, 138–139
high availability, 208–209

availability zones, cloud computing, 423

avoiding risk, 599–600

awareness, risk, 599

AWS Management Console, 158

B

backdoor Trojans, 20

background checks, 584

backups, 214–215, 217
cloud computing, 430
differential backups, 217–218
full backups, 217
grandfather-father-son backups, 216
incremental backups, 218
recovery planning, 216
snapshots, 218–221
ten-tape rotation schemes, 216
Tower of Hanoi backups, 216

band direction/selection, wireless networks, 382–383

bandwidth monitoring tools, 536

barricades, perimeter security, 241–242

baseline configurations, 124–125

Bash, 68

BCP (Business Continuity Planning), 522

behaviors
intrusion detection, 362
rules of, 589–590

benchmarking, 579

best practices, cloud computing, 429

BIA (Business Impact Analysis), 606–607

biometric authentication, 198–199
CER, 200
efficacy rates, 200
facial recognition, 199
FAR, 200
fingerprints, 199

FRR, 200
gaits, 199
hand geometry, 199
mobile devices, 398–399
retinas, 199
signatures, 199
veins/blood vessels, 199
voiceprints, 199

birthday attacks, 30–31

bitcoin, 275

black box testing, 113

black hats, 76

blacklists, 317, 396, 546

blank passwords, 434

blended threats, 16

block ciphers, 265–266

blockchains, 275, 376

blood vessels/veins, biometric authentication, 199

blowfish, 288

Bluetooth
bluejacking, 56
bluesnarfing, 56
PAN, 391
piconets, 391

bollards, perimeter security, 241–242

Boot, Measured, 327

boot attestation, 328–329

boot integrity, 326–327

boot sector viruses, 17

botnets, 22–23

bots, 22–23

boundaries, network security, 347–350

BPA (Business Partner Agreements), 593

BPDU (Bridge Protocol Data Units), 346

BPDU Guard, 343

breach notifications, data, 552–554

bridge CA, 477

bridges, 345–346
BPDU, 346
loops, 346

browsers, MITB attacks, 59

brute-force attacks, 29

buffer overflows, 38

bug bounty programs, 112–113

BYOD, mobile device deployments, 412–413, 414–418

C

CA (Certificate Authorities), 475
bridge CA, 477
certificate chains, 475–476
CPS, 476
intermediate CA, 476–477
key escrow, 477–478
root CA, 476–477
trust hierarchies, 476–477
trust models, 476–477
web of trust, 477

cabinets, locking, 247–248

cable locks, 246

cabling
coaxial cables, 249–250
fiber-optic cables, 250
malware, 27
PDS, 250–251
plenums, 250
protected cabling, equipment security, 249–250
STP cables, 249–250
twisted-pair cables, 249–250
UTP cables, 249–250

CAC (Common Access Cards), 202

cache poisoning. *See* DNS poisoning

caching servers
DNS, 284
proxy servers, 354

cages
equipment security, 246–247
Faraday cages, 251

callbacks (phone), authentication, 198

cameras
- mobile device security, 409–410
- perimeter security, 242

camouflage
- applications, 174
- software, 174

captive portals, 372

capturing packets, 502–504

card cloning, 27

card emulation, NFC, 392

card skimming, 27

carrier unlocking, mobile devices, 406–407

CASB (Cloud Access Security Brokers), 128–129, 428–429

cat command, SSH, 496

CBT (Computer-Based Training), 588

CCMP (Counter Mode Cipher Block Chaining Message Authentication Code Protocol), 376

CCTV (Closed-Circuit Television)
- forensics, 561–562
- perimeter security, 242

CD (Continuous Delivery), 183

CDMA (Code-Division Multiple Access), 390

cellular communications, 389–390
- ANT+, 392
- Bluetooth, 391
- CDMA, 390
- GSM, 390
- IR, 392
- LTE, 390
- Mobile Wi-Fi, 391
- NFC, 391–392
- SATCOM, 390–391
- USB, 392–393

central logging, cloud computing, 427–428

CER (Crossover Error Rates), 200

certificate chains, 475–476

certificates
- authentication, 201–202
- CSR, 481–482
- digital certificates, 478–480
  - certificate policies, 482
  - code signing, 483
  - CRL, 486–487
  - CSR, 481–482
  - DER, 485
  - DV, 482–483
  - email, 484
  - EV, 483
  - formats, 484–485
  - machine/computer certificates, 484
  - OCSP, 486–487
  - OV, 483
  - P7B certificates, 485
  - PEM, 484–485
  - PFX, 485
  - pinning, 488
  - private keys, 480–481
  - public keys, 480–481
  - revoking, 486
  - root signing, 484
  - SAN, 483
  - self-signed digital certificates, 483
  - user (client certificates), 484
  - wildcards, 483
- policies, 482
- revocation, incident migration, 543
- X.509 certificates, 478–479

chain of custody, 556–559

chain of root, trust, 327

change management, applications, 169–170

CHAP (Challenge Handshake Authentication Protocol), 457–458

charging cables/devices, malware, 27

Cheney, U.S. Vice President Dick, 233–234

chmod command, SSH, 496

CI (Continuous Integration), 182–183
Cialdini, Robert, 10–12
CIDR (Classless Interdomain Routing), 300
cipher locks, 245
CIRT (Cyber Incident Response Teams), 515
CIS (Center for Internet Security), 579
clean desk policies, 586
cleanup, penetration testing, 117
client (user) certificates, 484
client-side validation, 175–176
clones/duplicate copies, forensics, 560
cloning cards, 27
cloud computing, 421–422
availability zones, 423
AWS Management Console, 158
backups, 430
best practices, 429
CASB, 128–129, 428–429
central logging, 427–428
community deployments, 162–163
compliance, 429
containers, 429
data encryption, 429
DevSecOps, 429
disaster recovery, 430
dynamic resource allocation, 422
edge computing, 160–161
endpoint detection/response, 430
FaaS, 159
firewalls, 430
fog computing, 160–161
hybrid deployments, 162
IaaS, 158, 427–428
IDS, 430
instances, 422, 429
models, 155–156
operational intelligence, 429
PaaS, 159
policies, 424–426
private deployments, 161
proxies, 430
public deployments, 161–162
regions, 423
restorations, 430
risk management, 429
SaaS, 159–160
secrets managers, 426
security groups, 423–424
security information/event management, 430
serverless architectures, 159
service models, 156–161
software composition analysis, 429
SWG, 428–429
third-party security solutions, 428–430
VPC, 422, 423
VPN, 429
vulnerabilities, 89–90, 429
workload isolation, 430
workloads, 422
XaaS, 160, 303
coaxial cables, 249
COBIT (Control Objectives for Information and Related Technology), 577, 578
code analyzers, 318–319
dynamic code analysis, 319–320
fuzzing, 319–320
static code analyzers, 319
code injection, 39
DLL injection, 39, 40
LDAP injection, 40
XML injection, 40
XSS, 39
coding
dead code, 174–175
IaC, 153
malicious code/script execution, 57, 68–69
outsourced code development, vulnerabilities, 95–96

repos (repositories), 83
reuse, 174–175
secure coding, 170, 171–172
CSSLP, 171
OWASP, 170–171
SAFECode, 171
signing, 318
application development, 178–179
digital certificates, 483
static codes, authentication, 198

cold sites, 138

cold/hot aisles, 254–255

communication

cellular, 389–390
ANT+, 392
Bluetooth, 391
CDMA, 390
GSM, 390
IR, 392
LTE, 390
Mobile Wi-Fi, 391
NFC, 391–392
SATCOM, 390–391
USB, 392–393
email communication, 296–297
FTP communication, 295–296
FTPS, 295–296
internal communications
LDAPS, 298
network address allocation, 299–302
NTP, 302
SNMP, 298–299
SRTP, 297–298
subscription services, 303
RCS, 409
SFTP, 295–296
web communication
DNSSEC, 294–295
HTTPS, 293–294
SSL, 294
TLS, 294
wireless communication
bluejacking, 56
bluesnarfing, 56
Bluetooth, 56
mobile devices, 391
Wi-Fi Alliance, 374

community cloud deployments, 162–163

compensating controls, 572–573

competitors as threat actors, 78–79

complexity of passwords, 442

compliance

cloud computing, 429
regulatory compliance, 616–618

Compromise (IOC), Indicators of, 83

computer/machine certificates, 484

concentrators, VPN, 358–360

conditional access, 468

confidentiality

API, 137
data, 126, 615
NFC attacks, 57

configuration management, 124

baseline configurations, 124–125
CASB, 128–129
contingency planning, 136
data availability, 136–137
data sovereignty, 138–139
geographic considerations, 138–139
site resiliency, 137–138
data confidentiality, 126
data encryption, 129–132
data integrity, 135–136
data obfuscation/encryption, 129–132
data protection, 126
deception, 139–141
diagrams, 125
disruption, 141
DLP, 127–129
HSM, 133–134
IP schemas, 125

OS hardening, 125–126
review updates, 126
rights management, 132–133
secure configurations, 335–336
standard naming conventions, 125

configuring
baseline configurations, 124–125
incident mitigation
application control, 544–545
certificate revocation, 543
content filtering, 543
DLP, 543
firewalls, 544–545
URL filtering, 543
secure configurations guides, 579
weak configurations, 91–94

consensus/social proof, principles of influence, 11

containerization, 148–150, 394
mobile devices, 402–403
visibility, cloud computing, 429

containment, incident mitigation, 519–521, 541–542

content filtering
incident mitigation, 543
proxy servers, 355–357

context-aware authentication, mobile devices, 399

contingency planning, 136

continuing education policies, 588–589

continuity/recovery plans, 522
COOP, 522, 524–526
DRP, 522, 523

continuous monitoring, user access, 436–437

controls, 569
compensating controls, 572–573
corrective controls, 572
detective controls, 571
deterrent controls, 571
functional use of, 570–572
managerial controls, 570
nature of, 570
operational controls, 570
physical security, 570
preventive controls, 571
technical controls, 570

cookies, secure, 318

COOP (Continuity of Operations Planning), 522, 524–526

COPE, mobile device deployments, 413, 414–418

copies. *See* snapshots

corporate policies, mobile device deployments, 415–416

corrective controls, 572

COSO (Committee of Sponsoring Organizations), 578

counterintelligence, 554

CPS (Certification Practice Statements), 476

crackers, password, 504–505

C-RAN (Cloud-Radio Access Networks), 150

credential harvesting, 8

credentialed/noncredentialed vulnerability testing, 103

criminal syndicates (threat actors), 78

critical functions, risk management, 607–608

CRL (Certificate Revocation Lists), 486–487

Cross-Site Scripting (XSS), 39

CRTM (Core Root of Trust for Measurement), 169

cryptocurrencies, bitcoin, 275

cryptography
3DES, 289
algorithms, 262
asymmetric algorithms, 266–268
attacks
birthday attacks, 30–31
downgrade attacks, 31
man-in-the-middle attacks, 31

block ciphers, 265–266
blockchains, 275
blowfish, 288
constraints, 276
cryptocurrencies, bitcoin, 275
data encryption process, 262
DES, 288–289
digital signatures, 270–271
ECC, 268
FIPS 140–2, 273
hashing, 271–272
homomorphic encryption, 273–274
IDEA, 288
IV, 262–263
keys, 262–264, 286
nonces, 262–263
nonrepudiation, 269, 270
passwords, 262–263
PFS, 268–269
private key encryption, 267–268
pseudo-random numbers, 262–263
public key encryption, 266–268
quantum cryptography, 268
salting, 272
session keys, 268–269
steganography, 273–274
stream ciphers, 265–266
symmetric algorithms, 264–266
use cases, 274–275
use of proven technologies, 272–273
wireless cryptographic protocols, 373–377

cryptojacking, 26

CryptoLocker, 24

crypto-malware, 23
CryptoLocker, 24
WannaCry, 24, 141

cryptomining, 26

CSA (Cloud Security Alliance), 578

CSF (Cybersecurity Framework), 578

CSR (Certificate Signing Requests), 481–482

CSRF (Cross-Site Request Forgeries), 41–43

CSSLP (Certified Secure Software Lifecycle Professional), 171

Cuckoo command, 499

cURL command, 498, 499

custody, chain of, 556–559

custom firmware, mobile devices, 406

CVE (Common Vulnerabilities and Exposures) standard, 101–102

CVE Details, 82

CVSS (Common Vulnerabilities Scoring System), 102

cyber kill chains, 107, 510

CYOD (Choose Your Own Device), mobile device deployments, 413, 414–418

D

DAC (Discretionary Access Control), 467

dark web, 83

data acquistion, 559–560

data at rest, encryption, 129

data availability, configuration management, 136–137
data sovereignty, 138–139
geographic considerations, 138–139
site resiliency, 137–138

data breach notifications, 552–554

data confidentiality, configuration management, 126

data controllers, 620

data custodians/stewards, 619

data destruction, 255–256
declassification, 256
degaussing, 256
encryption, 256
paper records, 256–257
wiping, 256

data disposal, 620–621

data encryption

3DES, 289
blowfish, 288
cloud computing, 429
configuration management, 129–132
cryptography
  algorithms, 262
  asymmetric algorithms, 266–268
  blockchains, 275
  constraints, 276
  cryptocurrencies, bitcoin, 275
  data encryption process, 262
  digital signatures, 270–271
  ECC, 268
  FIPS 140–2, 273
  hashing, 271–272
  homomorphic encryption, 273–274
  IV, 262–263
  keys, 262–264
  nonces, 262–263
  nonrepudiation, 269, 270
  passwords, 262–263
  PFS, 268–269
  private key encryption, 267–268
  pseudo-random numbers, 262–263
  public key encryption, 266–268
  quantum cryptography, 268
  salting, 272
  session keys, 268–269
  steganography, 273–274
  symmetric algorithms, 264–266
  use cases, 274–275
  use of proven technologies, 272–273
data at rest, 129
data in motion, 129
data in processing, 129–130
data in transit, 129
data masking, 131
DES, 288–289
EFS, 322–323
embedded encryption, 404
enterprise-level encryption, 404
FDE, 322–323, 403–404
homomorphic encryption, 273–274
IDEA, 288
keys, 286
mobile devices, 397
process, 262
redaction, 131
secure data destruction, 256
SED, 323
tokenization, 130–131
traffic management, 134–135
voice encyption, 404
VoIP, 404

data exposure, application development, 176

data in motion, encryption, 129

data in processing, encryption, 129–130

data in transit, encryption, 129

data integrity, 135–136

Data Loss Prevention (DLP), 127–128

data masking, 131

data obfuscation/encryption, configuration management, 129–132

data owners, 587, 619

data ownership, mobile device deployments, 417

data processors, 620

data protection, configuration management, 126

data retention, 620–621

data sanitation, 505–506

data sensitivity, labeling/handling, 614–618

data sovereignty, 138–139

data storage, vulnerabilities, 95–96

database vulnerabilities, 82

dd command, 506

DDoS (Distributed Denial-of-Service) attacks, 66–68

dead code, 174–175

deauthentication attacks, 55

deception

- configuration management, 139–141
- honeyfiles, 139
- honeynets, 139
- honeypots, 139–141
- sandboxing, 141

declassification, secure data destruction, 256

defense in depth, 221–223

degaussing, secure data destruction, 256

Denial of Service (DoS) attacks, 57, 64, 91–94

- DDoS attacks, 66–68
- fraggle attacks, 65
- land attacks, 65
- ping flooding, 65
- smurfing attacks, 65
- SYN flooding, 65
- teardrop attacks, 65

DEP (Data Execution Prevention), 314

deploying

- applications, 167
    - automation, 180
    - CD, 182–184
    - CI, 182–184
    - production environments, 167
    - staging, 167
- mobile devices
    - deployment models, 412–413
    - deployment strategies, 414–418

deprovisioning applications, 168

DER (Distinguished Encoding Rules), 485

DES (Data Encryption Standard), 288–289

desktops

- VDE, 150
- VDI, 150

destroying data, 255–256

- declassification, 256
- degaussing, 256
- encryption, 256
- paper records, 256–257
- wiping, 256

detective controls, 571

detectors, internal security, 244

deterrence, risk, 600

deterrent controls, 571

developing applications, 166–167

- automation, 180–181
- camouflage, 174
- CD, 182–183
- change management, 169–170
- CI, 182–183
- client-side validation, 175–176
- code reuse, 174–175
- code signing, 178–179
- data exposure, 176–179
- dead code, 174–175
- DevOps, 170, 181–184
- drivers, 178–179
- elasticity, 184–185
- encryption, 173
- error handling, 176–177
- fuzzing, 172
- input validation, 177–178
- integrity measurement, 168–169
- memory management, 179
- obfuscation, 173–174
- provisioning, 168
- QA, 167
- resiliency, 180
- scalability, 184
- SDK, 175
- secure coding, 170
- server-side validation, 176
- staging, 167
- stored procedures, 173
- version control, 170

DevOps, 153
secure DevOps, 181–184
version control, 170
DevSecOps, cloud computing, 429
DHCP snooping, 344
DHS (U.S. Department of Homeland Security)
AIS, 83
NCSD, OVAL, 102
diagrams, configuration management, 125
Diamond Model of Intrusion Analysis, 511
dictionary attacks, 29
differential backups, 217–218
dig command, 498
digital certificates, 478–480
certificate policies, 482
code signing, 483
CRL, 486–487
CSR, 481–482
DER, 485
DV, 482–483
email, 484
EV, 483
formats, 484–485
machine/computer certificates, 484
OCSP, 486–487
OV, 483
P7B certificates, 485
PEM, 484–485
PFX, 485
pinning, 488
private keys, 480–481
public keys, 480–481
revoking, 486
root signing, 484
SAN, 483
self-signed digital certificates, 483
user (client certificates), 484
wildcards, 483
digital signatures, 270–271
directional antennas, 380–381
directory services, LDAPS, 298
directory traversal, 44–45
disaster recovery
after-action reports, 526
cloud computing, 430
COOP, 522, 526
DRP, 522, 523
incident response, 522–524
policies, 523
disciplinary/adverse actions policies, 591–592
discovery, networks, 496–502
discovery phase, penetration testing, 115–117
disposal of data, 620–621
disruption
configuration management, 141
DNS sinkholes, 141
dissociation attacks, 55
Distributed Denial-of-Service (DDoS) attacks, 66–68
distributions
PDS, 250–251
protected distributions, 250–251
diversity, software, 205–206
DLL injection, 39, 40
DLP (Data Loss Prevention), 127–128, 315–316, 543
DMZ (Demilitarized Zones), 350–353
DNS (Domain Name System), 62
domain hijacking, 62
domain reputation, 62
poisoning, 63–64
servers, 284
sinkholes, 141
dnsenum command, 498
DNSSEC (Domain Name System Security Extensions), 284, 294–295, 297
documented incident types, incident response, 513

domains
hijacking, 62
name resolution, DNSSEC, 294–295
reputation, 62
Domino's pizza, drones, 235
DoS attacks, 57, 64, 91–94, 332
DDoS attacks, 66–68
fraggle attacks, 65
land attacks, 65
ping flooding, 65
smurfing attacks, 65
SYN flooding, 65
teardrop attacks, 65
downgrade attacks, 31
downloader Trojans, 20
DPI firewalls, 317
DPO (Data Privacy Officers), 619
drivers, 40–41
code signing, 178–179
refactoring, 41
shimming, 41
DRM (Digital Rights Management), 132–133
drones
embedded control systems, 235–236
war flying, 116
DRP (Disaster Recovery Planning), 522, 523
dry-pipe fire suppression systems, 252–253
DSA (Directory System Agents), 289–290
dual power supplies, 207
dump files, 531–532
dumpster diving, 5–6
duplicate copies/clones, forensics, 560
Duronio, Roger, 22
duties, separation of, 585
DV (Domain Validation), digital certificates, 482–483
dynamic code analysis, 319–320
dynamic resource allocation, cloud computing, 422
dynamic/private ports, 333

E

EAP (Extensible Authentication Protocol), 372–373, 377
EAP-FAST, 378–379
EAPoL, 377–378
EAP-TLS, 377, 379
EAP-TTLS, 378, 379
PEAP, 378, 379, 458–459
east-west traffic, 350
ECC (Elliptic Curve Cryptography), 268
edge computing, 160–161
e-discovery, 552
EDR (Endpoint Detection and Response), 314
efficacy rates, biometric authentication, 200
EFS (Encrypting File Systems), 322–323
EK (Endorsement Keys), TPM, 325, 328
elasticity, applications, 184–185
email
digital certificates, 484
PEM, 484–485
prepending notifications, 7
secure communication, 296–297
secure protocols
IMAP, 287–288, 296–297
MIME, 287
POP3, 287–288, 296–297
S/MIME, 287, 296–297
embedded encryption, mobile devices, 404
embedded systems, 225–226
FPGA, 227
HVAC, 231

ICS, 228
MFD, 232
RTOS, 226–227
SCADA, 227–229
smart devices, IoT, 229–231
SoC, 226–227
special-purpose devices, 233
aircraft, 235–236
drones, 235–236
implied trust, 236
medical devices, 233–234
resource constraints, 236
UAV, 235–236
vehicles, 234–235
surveillance systems, 233

EMM (Enterprise Mobility Management), 405

encryption
3DES, 289
applications, 173
blowfish, 288
cloud computing, 429
configuration management, 129–132
cryptography
algorithms, 262
asymmetric algorithms, 266–268
blockchains, 275
constraints, 276
cryptocurrencies, bitcoin, 275
data encryption process, 262
digital signatures, 270–271
ECC, 268
FIPS 140–2, 273
hashing, 271–272
homomorphic encryption, 273–274
IV, 262–263
keys, 262–264
nonces, 262–263
nonrepudiation, 269, 270
passwords, 262–263
PFS, 268–269
private key encryption, 267–268
pseudo-random numbers, 262–263
public key encryption, 266–268
quantum cryptography, 268
salting, 272
session keys, 268–269
steganography, 273–274
symmetric algorithms, 264–266
use cases, 274–275
use of proven technologies, 272–273
data at rest, 129
data in motion, 129
data in processing, 129–130
data in transit, 129
data masking, 131
DES, 288–289
EFS, 322–323
embedded encryption, 404
enterprise-level encryption, 404
FDE, 322–323, 324, 403–404
homomorphic encryption, 273–274
IDEA, 288
keys, 286
mobile devices, 397
process, 262
redaction, 131
secure data destruction, 256
SED, 323
tokenization, 130–131
traffic management, 134–135
voice encryption, 404
VoIP, 404

endpoints
detection/response, cloud computing, 430
NAC, 366
protection. *See* host-based security

engagement (bug bounty programs), rules of, 112–113

engineering, social, 4–5
- credential harvesting, 8
- dumpster diving, 5–6
- hoaxes, 10
- hybrid warfare, 10
- identity fraud, 4–5
- influence campaigns, 10
- invoice scams, 8
- pharming, 8
- phishing, 7–8
- prepending notifications, email, 7
- principles of influence, 10–12
- reconnaissance, 4–5
- shoulder surfing, 6
- smishing, 8
- spear phishing, 7
- SPIM, 7
- tailgating, 5
- typo squatting, 9
- vishing, 8
- watering hole attacks, 9
- whaling, 7

enterprise security, configuration management, 124
- baseline configurations, 124–125
- CASB, 128–129
- contingency planning, 136
- data availability, 136–139
- data confidentiality, 126
- data encryption, 129–132
- data integrity, 135–136
- data obfuscation/encryption, 129–132
- data protection, 126
- deception, 139–141
- diagrams, 125
- disruption, 141
- DLP, 127–129
- HSM, 133–134
- IP schemas, 125
- OS hardening, 125–126
- review updates, 126
- rights management, 132–133
- standard naming conventions, 125

enterprise-level encryption, mobile devices, 404

entropy, keys, 262–263

environmental controls, 249
- fire suppression systems, 252–254
- hot/cold aisles, 254–255
- HVAC, 251–252

environmental threats, 602

ephemeral keys, 263

equipment security, 246
- air gaps, 248
- cable locks, 246
- cages, 246–247
- Faraday cages, 251
- fire suppression systems, 252–254
- HVAC, 251–252
- locking cabinets/enclosures, 247–248
- protected cabling, 249–250
- protected distributions, 250–251
- saves, 246–247
- screen filters, 248

eradication, incidents, 519–521

error handling
- application development, 176–177
- improper error handling, 37

escalation
- incident response, 514–515
- privilege escalation, 36, 117

escape protection, VM, 151–152

ESP (Encapsulating Secure Payloads), IPsec, 285

EV (Extended Validation), 483

event correlation, logging, 535

event logs, 531–533

exchanging keys, key exchanges, 263–264

executive users, 587

exhaustion, resource, 37

exit interviews, 592

expiration, accounts, 442

exploitation frameworks, 502

exposure of data, application development, 176

extranets, 351–352

F

FAA (Federal Aviation Administration, 235–236

FaaS (Function as a Service), 159

facial recognition, biometric authentication, 199

facilities planning
- environmental controls, 249
- fire suppression systems, 252–254
- hot/cold aisles, 254–255
- HVAC, 251–252

failures
- MTBF, 609–610
- MTTF, 609–610
- single points of failure, 607–608

false negatives/positives
- intrusion detection, 364–365
- vulnerability scanners, 103

familiarity/liking, principles of influence, 12

FAR (False Acceptance Rates), 200

Faraday cages, 251

fat AP, 380

FCC, jamming attacks, 54

FDA, medical devices, 234

FDE (Full Disk Encryption), 322–323, 324, 403–404

federated identity systems, 193–194, 461–464

federation, RADIUS, 377–378

fences, perimeter security, 240–241

fiber-optic cables, 250

file format fuzzing, 320

file integrity checkers, 310

file/code repositories (repos), 83

file-infecting viruses, 18

filesystem permissions, 452
- auditing, 453
- group policies, 453
- Linux, 455–456
- Manning, Chelsea, 452
- Windows, 453–455

filtering
- content, incident mitigation, 543
- MAC filtering, 343, 383–384
- URL filtering, 543

filters, screen, 248

fingerprints, biometric authentication, 199

FIPS 140–2, 273

fire suppression systems, 252
- class ratings, 253–254
- dry-pipe fire suppression systems, 252–253
- wet-pipe fire suppression systems, 252–253

firewalls, 347
- cloud computing, 430
- DMZ, 350–353
- DPI firewalls, 317
- host-based firewalls, 308
- incident mitigation, 544–545
- NGFW, 353–354
- rules, 348
- segmentation, 347–348, 544–545
- stateful firewalls, 348
- stateless firewalls, 347–348
- WAF, 353–354
- web application firewalls, 317

firmware
- custom firmware, mobile devices, 406
- security, 322
  - boot attestation, 328–329
  - boot integrity, 326–327

EFS, 322–323
FDE, 322–323, 324
HSM, 326
SED, 323
TPM, 324–326
UEFI, 326–327

fit AP, 380

flash drives
DLP, 316
malware, 26–27

flooding
MAC flooding, 61
ping flooding, 65
SYN flooding, 65

fobs, key, 196

fog computing, 160–161

footprinting, 115–116

forensics, 551–552
CCTV, 561–562
chain of custody, 556–559
counterintelligence, 554
data acquisition, 559–560
data breach notifications, 552–554
duplicate copies/clones, 560
e-discovery, 552
hashes, 562–563
images, 560
mobile device deployments, 418
network logs, 560–561
network traffic, 560–561
nonrepudiation, 556
order of volatility, 555–556
organizational security, 505–506
person-hours tracking, 555
photographs, 561–562
preservation, 552
record time offsets, 562
screenshots, 563
strategic intelligence, 554
video, 561–562
witness interviews, 563–564

forgeries, request, 41
CSRF, 41–43
SSRF, 42–43

forgotten passwords, 443

forward proxy servers, 354–355

forward secrecy (PFS), 268–269

FPGA (Field-Programmable Gate Arrays), 227

fraggle attacks, 65

frameworks, 575–576
attack frameworks, incident response, 509
cyber kill chains, 510
Diamond Model of Intrusion Analysis, 511
documented incident types, 513
incident response plans, 512–513
MITRE ATT&CK, 510–511
CSF, 578
exploitation frameworks, 502
industry-specific frameworks, 577–579
RMF, 578

FRCP, data breach notifications, 553

FRR (False Rejection Rates), 200

FTK Imager, 506

FTP (File Transfer Protocol), 286–287, 295–296

FTPS (File Transfer Protocol Secure), 286–287, 295–296

full backups, 217

full tunneling, VPN, 360

functionality, least, 335

fuzzing, 172, 319–320

G

gaits, biometric authentication, 199

gates, perimeter security, 241

GDPR (General Data Protection Regulation), 552–553, 576, 620

general users, 587

general-purpose guides, 580

General-Purpose Operating System Protection Profile (OSPP), 580

General-Purpose Operating System Security Requirements Guide (SRG), 580

generators, redundancy, 207

geofencing, 401–402, 438–439

geographic considerations, data availability, 138–139

geolocation, 400–401, 439

geotagging, 409, 439

GLBA (Gramm-Leach-Bliley Act), 576

GPO, account policy enforcement, 441

GPRS (General Packet Radio Service), 401

GPS (Global Positioning Systems), 400–401

grandfather-father-son backups, 216

gray box testing, 113

gray hats, 76

grep command, SSH, 496

group policies, filesystem permissions, 453

group-based access control model, 440

GSM (Global System for Mobile Communications), 390

guards, perimeter security, 242–243

guides, 575–576
- general-purpose guides, 580
- platform-specific guides, 579–580
- secure configurations guides, 579
- vendor-specific guides, 579–580

H

hackers, 76
- black hats, 76
- gray hats, 76
- white hats, 76

hacktivists, 78

hand geometry, biometric authentication, 199

Handshake protocol, TLS, 283

hard drives, imaging, 216, 218–221

hardening OS, 125–126, 332–334

hardware
- HSM, 133–134
- roots of trust, 329–330
- security, 322
  - boot attestation, 328–329
  - boot integrity, 326–327
  - EFS, 322–323
  - FDE, 322–323, 324
  - HSM, 326
  - SED, 323
  - TPM, 324–326

harvesting, credential, 8

hashing, 271–272, 562–563

head command, SSH, 495

health checks, host, 366

health monitoring, system, 533

heat maps
- risk, 603–604
- wireless network installations, 381–382

heuristic intrusion detection, 363–364

heuristic scanning, 311

HIDS (Host-based Intrusion Detection Systems), 308–310, 360–361

high availability, 208–209

hijacking, domain, 62

HIPAA (Health Insurance Portability and Accountability Act), 576

HIPS (Host-based Intrusion Prevention Systems), 309–310

history of passwords, 445

HITRUST CSF (Health Information Trust Alliance Common Security Framework), 578

HMAC, HOTP, 196, 198

hoaxes, 10

home automation, IoT, 230

homomorphic encryption, 275

honeyfiles, 139

honeynets, 139

honeypots, 139–141

host health checks, 366

host-based NAC, 366

host-based security, 308

- anti-malware, 311–312
- antispam software, 312–313
- antispyware programs, 313
- antivirus software, 310–312
- blacklists, 317
- DEP, 314
- DLP, 315–316
- DPI firewalls, 317
- EDR, 314
- file integrity checkers, 310
- firewalls, 308
- HIDS, 308–310, 360–361
- HIPS, 309–310
- NIDS, 309, 360–361
- NIPS, 309, 362
- pop-up blockers, 313
- removable media control, 316
- scanning, 311
- web application firewalls, 317
- whitelists, 317

hot sites, 137–138

hot/cold aisles, 254–255

hotfixes, 95

HOTP (HMAC-based One-Time Passwords), 196, 198

hping command, 498

HR management policies, 584

HSM (Hardware Security Modules), 133–134, 326

- authentication, 451
- mobile devices, 403–404

HTTP (HyperText Transfer Protocol), 282

HTTPS (HyperText Transfer Protocol over SSL), 45–46, 282, 293–294

hunting threats, 107

- cyber kill chains, 107, 510
- intelligence fusion, 107–108

HVAC (Heating, Ventilation, and Air Conditioning)

- embedded systems, 231
- equipment security, 251–252

hybrid attacks, 29–30

hybrid cloud deployments, 162

hybrid warfare, 10

hypervisors, 146

- Type I hypervisors, 146, 147–148
- Type II hypervisors, 147–148

I

IaaS (Infrastructure as a Service), 158, 427–428

IaC (Infrastructure as Code), 153

ICMP (Internet Control Message Protocol), 500–501

ICS (Industrial Control Systems), 228

IDEA (International Data Encryption Algorithm), 288

identity

- cloud computing policies, identity-based, 424–426
- federated identity systems, 193–194, 461–464
- fraud, 4–5
- managing
  - access auditing/reviews, 436–437
  - access controls, 439–440
  - account expiration, 442
  - account policy enforcement, 441–442
  - administrative accounts, 434
  - IdP, 435
  - least privilege, 436
  - location restrictions, 438–439
  - lockouts, 443–444
  - logon hours, 438
  - offboarding, 435–436

onboarding, 435–436
passwords, 434, 442, 443, 444–446
time of date, 438
types of accounts, 433–435
UAC, 435
OAuth, 462–463
OpenID Connect, 463–464
SAML, 461–462
Shibboleth, 464

IdP (Identity Providers), 435

IDS (Intrusion Detection Systems)
cloud computing, 430
HIDS, 308–310, 360–361
NIDS, 309, 360–361

IEEE 802.11, 375

IEEE 802.1X authentication, 201, 372

ifconfig command, 497

IKE (Internet Key Exchange), 286

IM (Internet Messaging), SPIM, 7

IMA (Integrity Measurement Architectures), 169

imaging hard drives, 216, 218–221

IMAP (Internet Message Access Protocol), 287–288, 296–297

impact from vulnerabilities, 96–97

impact of incidents, 518–519

impersonation. *See* social engineering

implicity deny, 348–349

implied trust, 236

improper error handling, 37

improper input handling, 37

improper/weak patch management, 94–95

in-band devices, 362

incidents
identification/analysis, 518–519
investigation, 529
bandwidth monitoring tools, 536
logging, 531–535
macOS Activity Monitor, 536–537
NetFlow, 538
network activity monitors, 536–537
protocol analyzers, 536, 537–538
sFlow, 538
SIEM dashboards, 530–531
mitigation, 520, 541
application control, 545–546
blacklists, 546
certificate revocation, 543
containment, 541–542
content filtering, 543
DLP, 543
firewalls, 544–545
quarantining, 542–543
SOAR, 546–548
URL filtering, 543
whitelists, 545–546
response, 509
BCP, 522
CIRT, 515
containment, 519–521
continuity/recovery plans, 522
COOP, 522, 524–526
cyber kill chains, 510
Diamond Model of Intrusion Analysis, 511
disaster recovery, 522–524
documented incident types, 513
DRP, 522, 523
eradication, 519–521
escalation, 514–515
impact of incidents, 518–519
incident identification/analysis, 518–519
incident mitigation, 520
incident response plans, 512–513
IRT, 512, 515
MITRE ATT&CK, 510–511
post-incident activities, 521–522
preparation, 517–518
process, 517

recoverability from incidents, 519–521
recovery planning, 522
reporting requirements, 514–515
roles/responsibilities, 513–514
tabletop exercises, 516–517
testing, 516–517
training, 516–517

incremental backups, 218

indicators, threats
AIS, 83
TAXII, 83

industry-specific frameworks, 577–579

influence
campaigns, 10
principles of influence
authority, 10–11
consensus/social proof, 11
familiarity/liking, 12
scarcity, 11–12
trust, 12
urgency, 11–12

information life cycle management, 614–615

infostealer Trojans, 20

infrared detectors, internal security, 244

injection, code, 39
DLL injection, 39, 40
LDAP injection, 40
SQL injection, 39
XML injection, 40
XSS, 39

inline NAC, 366

input handling, improper, 37

input validation, application development, 177–178

inside threat actors, 77

instances, cloud computing, 422, 429

integer overflows, 38

integrity
API, 137
boot integrity, 326–327
CRTM, 169
data integrity, 135–136
file integrity checkers, 310
IMA, 169
measurement, 168–169
sealed storage, 168
TCG, 169
TKIP, 376
TPM, 168–169

intelligence fusion, 107–108

intelligence/resource sources, threat, 81
ISAC, 82
ISAO, 82
OSINT, 81, 82–85
sharing centers, 81–82

intelligence, strategic, 554

intelligent access points, 380

intelligent antennas, 380

interference, wireless networks, 382–383

intermediate CA, 476–477

internal communications, secure
LDAPS, 298
network address allocation, 299–302
NTP, 302
SNMP, 298–299
SRTP, 297–298
subscription services, 303

internal security, 243–244
alarms, 244
infrared detectors, 244
locks, 245
mantraps, 245
motion detectors, 244

Internet protocols, secure, 288–289

internet usage policies, 590–591

interoperability agreements, 593–594

interviews
- exit interviews, 592
- witness interviews, 563–564

inter-VLAN routing, 344, 345

intimidation, principles of influence, 11

intranets, 351

Intrusion Analysis, Diamond Model of, 511

intrusion detection, 364–365
- anomaly-based intrusion detection, 363
- behavior-based intrusion detection, 362
- false positives, 364–365
- heuristic intrusion detection, 363–364
- signature-based intrusion detection, 363

intrusive/nonintrusive vulnerability testing, 102–103

invoice scams, 8

IOC (Indicators of Compromise), 83

IoT (Internet of Things)
- home automation, 230
- scanners, 230–231
- security, 230–231
- smart devices, 229–231
- wearable technology, 229–230

ip command, 497

IP (Internet Protocol)
- load balancers, 210–211
- VIP addresses, 211
- VoIP encryption, mobile devices, 404

IP schemas, configuration management, 125

ipconfig command, 497

IPS (Intrusion Protection Systems), 309–310, 362

IPsec (Internet Protocol Security), 284–286

IPv4 (Internet Protocol version 4), network address allocation, 299–302

IPv6 (Internet Protocol version 6)
- NAT, 342
- network address allocation, 299–302

IR (Infra-Red) communication, 392

IRM (Information Rights Management), 132–133

IRT (Incident Response Teams), 512, 515

ISA (Interconnection Security Agreements), 594

ISAC (Information Sharing and Analysis Centers), 82

ISAKMP (Internet Security Association and Key Management Protocol), 286

ISAO (Information Sharing and Analysis Organizations), 82

ISO/IEC (International Organization for Standardization/International Electrotechnical Commission), 577
- ISO/IEC 27001, 577
- ISO/IEC 27002, 578
- ISO/IEC 27701, 577
- ISO/IEC 31000, 577

isolation/quarantining, incident mitigation, 542–543

ISP (Internet Service Providers), redundancy, 208

IV (Initialization Vectors)
- attacks, 55–56
- cryptography, 262–263

J

jailbreaking, 405–406

jamming attacks, 54–55

Jeep Cherokee, embedded control systems, 235

job rotation, 586

journalctl, 535

jump servers, 352

JVM (Java Virtual Machines), 149–150

K

KBA (Knowledge-Based Authentication), 450–451

Kerberos, 464–466

key fobs, 196

keylogger Trojans, 20

keys
- cryptography
  - entropy, 262–263
  - ephemeral keys, 263
  - IKE, 286
  - key exchanges, 263–264
  - key length, 262–263
  - key strength, 262–263
  - private key encryption, 267–268
  - public key encryption, 266–268
  - session keys, 268–269
  - static keys, 263
  - stretching, 263
- EK, TPM, 325, 328
- escrow, 477–478
- mobile devices, key management, 397
- PKI
  - CA, 475–478
  - components, 474–475
  - digital certificates, 478–480
  - RA, 475
- private keys, digital certificates, 480–481
- PSK, 372
- public keys, digital certificates, 480–481
- SRK, TPM, 325
- symmetric keys, Kerberos authentication, 464
- TKIP, 376

L

LAN, EAPoL, 377–378

land attacks, 65

lateral movement, penetration testing, 117

Layer 2 attacks, 59–60

LDAP (Lightweight Directory Access Protocol), 40, 289

LDAPS (Lightweight Directory Access Protocol over SSL), 289–290, 298

leaks, memory, 37

least functionality, 335

least privilege
- account management, 436
- organizational security, 585

length of passwords, 445–446

lighting, perimeter security, 241

liking/familiarity, principles of influence, 12

Linux, filesystem permissions, 455–456

load balancers, 209–211, 340, 355

location restrictions, account management, 438–439

Lockheed Martin, state actors, 79

locking cabinets/enclosures, equipment security, 247–248

lockouts, account, 30, 443–444

locks, 245
- cable locks, 246
- cipher locks, 245
- pattern locks, 398
- screen locks, 398
- swipe card locks, 245
- wireless locks, 245

logger command, SSH, 496

logging, 535
- access logs, 533–534
- anomaly detection, 535
- application logs, 531–532
- audit logs, 533
- central logging, cloud computing, 427–428
- dump files, 531–532
- event logs, 531–533

journalctl, 535
log files, 531–532
network logs, forensics, 560–561
security logs, 533
syslog, 535
system event logs, 533–534
system health monitoring, 533
system logs, 531–532
W3C logs, 531–532
web application logs, 531–532
web server logs, 531–532
Windows Event Viewer, 534

logic bombs, 22

logical access controls, 439–440

logon hours, account management, 438

looping
bridge loops, 346
detecting loops, 343–344
STP loops, 346

LTE (Long-Term Evolution), 390

M

MAC (Media Access Control), 467
filtering, 343, 383–384
flooding, 61
spoofing, 60

machine/computer certificates, 484

macOS Activity Monitor, 536–537

macros
macro viruses, 17
malware, 16, 17

malicious code/script execution, 57, 68–69

malware, 16
adapters, 27
adware, 25–26
anti-malware, 311–312
blended threats, 16
botnets, 22–23
bots, 22–23
cables, 27
cryptojacking, 26
crypto-malware, 23
CryptoLocker, 24
WannaCry, 24, 141
cryptomining, 26
logic bombs, 22
macros, 16, 17
memory, 16
peripheral devices, 26–27
PUP, 25
adware, 25–26
cryptojacking, 26
cryptomining, 26
spyware, 25
quarantining, 542–543
ransomware, 23–24
registries, 16
rootkits, 20–21
slag code, 22
spyware, 25
Trojans, 19–20
backdoor Trojans, 20
downloader Trojans, 20
infostealer Trojans, 20
keylogger Trojans, 20
RAT, 20
USB
cables, 27
flash drives, 26–27
viruses, 17, 19
armored viruses, 18, 19
boot sector viruses, 17
file-infecting viruses, 18
macro viruses, 17
multipartite viruses, 18
nonresident viruses, 17
polymorphic viruses, 18, 19
program-infecting viruses, 18

resident viruses, 17
stealth viruses, 18
worms, 19
zombie armies, 22
MAM (Mobile Application Management), 394, 395–397
managed PDU (Power Distribution Units), 207–208
managerial controls, 570
managing
accounts/identity
access auditing/reviews, 436–437
access controls, 439–440
account expiration, 442
account policy enforcement, 441–442
administrative accounts, 434
age of passwords, 444–445
blank passwords, 434
complexity of passwords, 442
forgotten passwords, 443
history of passwords, 445
IdP, 435
least privilege, 436
length of passwords, 445–446
location restrictions, 438–439
lockouts, 443–444
logon hours, 438
offboarding, 435–436
onboarding, 435–436
rotating passwords, 446
time of date, 438
types of accounts, 433–435
UAC, 435
applications, MAM, 394, 395–397
authentication, 450–451
change management, applications, 169–170
cloud computing vulnerabilities, 429
configurations, 124
baseline configurations, 124–125
CASB, 128–129
contingency planning, 136
data availability, 136–139
data confidentiality, 126
data encryption, 129–132
data integrity, 135–136
data obfuscation/encryption, 129–132
data protection, 126
deception, 139–141
diagrams, 125
disruption, 141
DLP, 127–129
HSM, 133–134
IP schemas, 125
OS hardening, 125–126
review updates, 126
rights management, 132–133
secure configurations, 335–336
standard naming conventions, 125
encrypted traffic management, 134–135
memory, application development, 179
mobile devices
EMM, 405
keys, 397
MAM, 394, 395–397
MCM, 394–395
MDM, 393–394
UEM, 394
PAM, 469
patches, 331–332
mobile device deployments, 417
weak/improper patch management, 94–95
rights management, 132–133
risk management
ALE, 606
ARO, 606
BIA, 606–607
cloud computing, 429

impact, 610–611
mission-essential functions, 607–608
MTBF, 609–610
MTTF, 609–610
MTTR, 609–610
qualitative risk management, 604
quantitative risk management, 604–605
risk acceptance, 600
risk analysis, 598
risk appetite, 599
risk assessments, 598, 602–604
risk avoidance, 599–600
risk awareness, 599
risk deterrence, 600
risk heat maps, 603–604
risk matrices, 603
risk mitigation, 600
risk response, 599–601
risk transference, 600
risks registers, 598–599
RPO, 608
RTO, 608
single points of failure, 607–608
SLE, 605
third-party risk management, 592–593
threat assessments, 601–602
secrets managers, cloud computing, 426
security information/event management, cloud computing, 430
threats, UTM, 357–358
mandatory vacations, 585
MANET (Mobile Ad hoc Networks), 410–411
man-in-the-browser (MITB) attacks, 59
man-in-the-middle (MITM) attacks, 31, 57, 58–59
manipulating drivers, 40–41
refactoring, 41
shimming, 41
Manning, Chelsea, 452
mantraps, internal security, 245
maps
risk heat maps, 603–604
threat maps, 83
masking data, 131
matrices, risk, 603
MCM (Mobile Content Management), 394–395
MDM (Mobile Device Management), 393–394
Measured Boot, 327
medical devices, embedded control systems, 233–234
Memdump command, 506
memory
application development, 179
leaks, 37
malware, 16
messaging, Internet, 7
metadata, 536
MFD (Multifunction Devices), 232
microservices, 148–149
Miller, Charlie, 235
MIME (Multipurpose Internet Mail Extensions), 287
mission-essential functions, 607–608
MITB attacks, 59
mitigating
incidents, 520
application control, 545–546
blacklists, 546
certificate revocation, 543
containment, 541–542
content filtering, 543
DLP, 543
firewalls, 544–545

quarantining, 542–543
SOAR, 546–548
URL filtering, 543
whitelists, 545–546
risk, 600
MITM attacks, C01.0192, 57, 58–59
MITRE, 82
MITRE ATT&CK, 82, 510–511
ML (Machine Learning), 27–28
MMS texting/pictures, 409
mobile devices
authentication, 395–396
biometrics, 398–399
blacklists, 396
cameras, 409–410
carrier unlocking, 406–407
cellular communications, 389–390
ANT+, 392
Bluetooth, 391
CDMA, 390
GSM, 390
IR, 392
LTE, 390
Mobile Wi-Fi, 391
NFC, 391–392
SATCOM, 390–391
USB, 392–393
containerization, 402–403
context-aware authentication, 399
custom firmware, 406
data encryption, 397
deploying
acceptable use policies, 415–416
antivirus software, 417
architectures/infrastructures, 414–415
BYOD, 412–413, 414–418
COPE, 413, 414–418
corporate policies, 415–416
CYOD, 413, 414–418
data ownership, 417
deployment models, 412–413
deployment strategies, 414–418
forensics, 418
legal concerns, 416
patches, 417
privacy, 416
support, 417
UWYT, 413
embedded encryption, 404
EMM, 405
enterprise-level encryption, 404
FDE, 403–404
geofencing, 401–402
geolocation, 400–401
geotagging, 409
GPRS, 401
GPS, 400–401
HSM, 403–404
jailbreaking, 405–406
key management, 397
MAM, 394, 395–397
MANET, 410–411
MCM, 394–395
MDM, 393–394
MMS, texting/pictures, 409
mobile payments, 411–412
OTA updates, 407
passwords, 395–396, 398
pattern locks, 398
PIN/passcodes, 398
push notifications, 402
RCS, 409
remote wiping, 399–400
RFID, 401
rooting, 405–406
screen locks, 398
SEAndroid, 393, 394
segmentation, 402–403
sideloading applications, 408
storage, 408–409
tethering, 411
third-party app stores, 407–408
transitive trust, 396–397

UEM, 394
USB OTG, 408
VDI, 413–414
video, 409–410
voice encryption, 404
VoIP, encryption, 404
whitelists, 396
Wi-Fi Direct, 410–411

Mobile Wi-Fi, 391

monitoring
system health, 533
user access, 436–437

motion, data in, 129

motion detectors, internal security, 244

MOU (Memorandum of Understanding), 593–594

MSCHAP (Microsoft CHAP), 457–458

MSP (Managed Service Providers), 154

MSSP (Managed Security Service Providers), 154

MTBF (Mean Time Between Failures), 609–610

MTTF (Mean Time to Failure), 609–610

MTTR (Mean Time to Repair), 609–610

multifactor authentication, 190–192

Multifunction Devices (MFD), 232

multipartite viruses, 18

multipath, RAID, 214

N

NAC (Network Access Control), 365–367

naming conventions, configuration management, 125

NAS (Network-Area Storage), 353

NAT (Network Address Translation), 341–342

nation-state actors, 79

nbtstat command, 498

NCSD (National Cyber Security Division), OVAL, 102

NDA (Nondisclosure Agreements), 591, 615

Nessus command, 499

Netcat command, 498

NetFlow, 538

netstat command, 498

networks
activity monitors, incident investigation, 536–537
address allocation, 299–302
attacks, 54
ARP poisoning, 60–61
bluejacking, 56
bluesnarfing, 56
Bluetooth attacks, 56
confidentiality, 57
DDoS attacks, 66–68
deauthentication attacks, 55
dissociation attacks, 55
DNS poisoning, 63–64
domain hijacking, 62
DoS attacks, 57, 64–66
fraggle attacks, 65
IV attacks, 55–56
jamming attacks, 54–55
land attacks, 65
Layer 2 attacks, 59–60
MAC flooding, 61
MAC spoofing, 60
malicious code/script execution, 57, 68–69
MITB attacks, 59
MITM attacks, 57, 58–59
NFC attacks, 57
ping flooding, 65
port stealing, 61
RARP, 60–61
RFID attacks, 57–58
rogue AP, 55
smurfing attacks, 65

SYN flooding, 65
teardrop attacks, 65
URL redirection, 62–63
wireless networks, 54–56
bridges, 345–346
C-RAN, 150
discovery, 496–502
DMZ, 350–353
east-west traffic, 350
extranets, 351–352
firewalls, 347–348, 350–354
IDS, 360–361
implicity deny, 348–349
intranets, 351
intrusion detection, 362–365
IPS, 362
jump servers, 352
LAN, EAPoL, 377–378
Layer 2 attacks, 59–60
load balancers, 209–211, 340, 355
logs, forensics, 560–561
MANET, 410–411
NAC, 365–367
NAS, 353
NAT, 341–342
NIDS, 360–361
NIPRNET, 250–251
NIPS, 362
north-south traffic, 350
PAN, 391
piconets, 391
policies, 350
proxy servers, 354–357
RADIUS servers, 352, 353
reconnaissance, 496–502
routers, 340–342
SAN, 205–206
SDN, 152–153
segmentation, 340, 349–350
air gaps, 350
bridges, 345–346
DMZ, 350–353
firewalls, 347–348, 544–545
implicity deny, 348–349
physical security, 350
routers, 340–342
switches, 342–343, 350
VLAN, 342–343, 344–345
short-range wireless communications, 56
bluejacking, 56
bluesnarfing, 56
Bluetooth, 56
DoS attacks, 57
malicious code/script execution, 57
MITB attacks, 59
MITM attacks, 57, 58–59
NFC, 57
RFID, 57–58
SIRPNET, 250–251
switches, 342–343, 350
traffic, forensics, 560–561
UTM, 357–358
VLAN, 342–343, 344–345
VPN
cloud computing, 429
concentrators, 358–360
site-to-site VPN, 359
tunneling, 360
vulnerability scanners, 100
wireless networks, 54
AC, 379–380
access methods, 371–372
antenna placement, 381
AP, 379–380, 381
authentication, 372–373
band direction/selection, 383
captive portals, 372
deauthentication attacks, 55
directional antennas, 380–381
dissociation attacks, 55
EAP, 372–373, 377–379
EAP-FAST, 378–379

EAPoL, 377–378
EAP-TLS, 377, 379
EAP-TTLS, 378, 379
heat maps, 381–382
intelligent antennas, 380
interference, 382–383
IV attacks, 55–56
jamming attacks, 54–55
MAC filtering, 383–384
omnidirectional antennas, 380–381
PEAP, 378, 379
PSK, 372
rogue AP, 55
site surveys, 381–382
SSID broadcasts, 384–385
WEP, 373–375
Wi-Fi Alliance, 374
Wi-Fi analyzers, 381
Wi-Fi Direct, 410–411
wireless cryptographic protocols, 373–377
WLAN controllers, 379–380
WPA, 374, 375–376
WPA2, 374, 376
WPA3, 374, 376, 377
WPA-Enterprise, 375
WPA-Personal, 375
WPS, 373–374
Zero Trust, 352

NFC (Near Field Communication), 57, 391–392
confidentiality, 57
DoS attacks, 57
malicious code/script execution, 57
MITB attacks, 59
MITM attacks, 57, 58–59

NGFW (Next-Generation Firewalls), 353–354

NIC (Network Interface Cards), teaming, 211

NIDS (Network-based Intrusion Detection Systems), 309, 360–361

NIPRNET (Non-Classified but Sensitive Internet Protocol Router Network), 250–251

NIPS (Network-based Intrusion Prevention Systems), 309, 362

NIST (National Institute of Standards and Technology), 576, 577, 578
CSF, 578
FIPS 140–2, 273
incident response plans, 512–513
RMF, 578

Nmap command, 498

NMI (Neural-Machine Interfaces), 233

nonces, 262–263

noncredentialed/credentialed vulnerability testing, 103

nondisclosure agreements (NDA), 591, 615

nonintrusive/intrusive vulnerability testing, 102–103

nonpersistence, snapshots, 219–220

nonregulatory requirements, 576–577

nonrepudiation, 269, 270, 556

nonresident viruses, 17

normalization, applications, 172–173

north-south traffic, 350

notifications
data breaches, 552–554
prepending notifications, email, 7
push notifications, 402

NSA (National Security Agency), inside threat actors, 77

nslookup command, 498

NTP (Network Time Protocol), 302

nxlog, 535

O

OAuth (Open Authorization), 462–463

obfuscation
applications, 173–174
data, 129–132

obscurity, security through, 272

OCSP (Online Certificate Status Protocol), 486–487

OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), 578–579

offboarding

- account management, 435–436
- organizational security, 584–585

omnidirectional antennas, 380–381

onboarding

- account management, 435–436, 442
- organizational security, 584–585

on-premises systems, vulnerabilities, 90

on-premises vs off-premises virtualization solutions, 154–155

OpenID Connect, 463–464

OpenSSH, 494

OpenSSL, 494

operational controls, 570

operational intelligence, cloud computing, 429

Operational Technology (OT), DDoS attacks, 67

order of volatility, 555–556

organizational security

- AUP, 589–590
- background checks, 584
- BPA, 593
- CBT, 588
- clean desk policies, 586
- continuing education policies, 588–589
- data sanitation, 505–506
- disciplinary/adverse actions policies, 591–592
- exit interviews, 592
- exploitation frameworks, 502
- forensics, 505–506
- HR management policies, 584
- internet usage policies, 590–591
- interoperability agreements, 593–594
- ISA, 594
- job rotation, 586
- least privilege, 585
- mandatory vacations, 585
- MOU, 593–594
- NDA, 591, 615
- network reconnaissance/discovery, 496–502
- offboarding, 584–585
- onboarding, 584–585
- packet capture, 502–504
- password crackers, 504–505
- policy framework, 583–584
- protocol analyzers, 502–504
- replay, 502–504
- role-based awareness, 586–588
- rules of behavior, 589–590
- separation of duties, 585
- shell environments, 494–496
- SLA, 593
- sniffers, 503–504
- SOP, 584
- third-party risk management, 592–593
- training, 588

OS (Operating Systems)

- hardening, 125–126, 332–334
- RTOS, 226–227
- security, 330–331
  - configurations, 335–336
  - disabling unnecessary ports, 332–334
  - least functionality, 335
  - OS hardening, 332–334
  - patch management, 331–332
  - trusted OS, 336
- trusted OS, 336
- unnecessary ports, disabling, 332–334

OSINT (Open-Source Intelligence), 81, 82–85

OSPP (Operating System Protection Profile), 580

OT (Operational Technology), DDoS attacks, 67

OTA updates, mobile devices, 407

OTP (One-Time Passwords), 196–198, 396

out-of-band devices, 361

out-of-band NAC, 366

outsourced code development, vulnerabilities, 95–96

OV (Organizational Validation), digital certificates, 483

OVAL (Open Vulnerability Assessment Language), 102

overflows, 38
- buffer overflows, 38
- integer overflows, 38

OWASP (Open Web Application Security Project), 47–48, 170–171

ownership of data, mobile device deployments, 417

P

P7B certificates, 485

PaaS (Platform as a Service), 159

packet capture, 502–504

PAM (Privileged Access Management), 469

PAN (Personal Area Networks), 391

PAP (Password Authentication Protocol), 457–458

paper records, secure data destruction, 256–257

passcodes/PIN, mobile devices, 398

pass-the-hash attacks, 49

passwords
- account lockouts, 30
- age, 444–445
- attacks, 28–29
  - brute-force attacks, 29
  - dictionary attacks, 29
  - hybrid attacks, 29–30
  - password spraying, 30
  - rainbow tables, 30
- blank passwords, 434
- complexity, 442
- crackers, 504–505
- FDE, 324
- forgotten passwords, 443
- history, 445
- HOTP, 196, 198
- keys, 262–263
- length, 445–446
- mobile devices, 398
- OTP, 196–198, 396
- PAP, 457–458
- rotating, 446
- spraying, 30
- static passwords, 396
- TOTP, 196, 198
- vaults, 450–451

patches
- managing, 331–332
- mobile device deployments, 417
- weak/improper patch management, 94–95

pattern locks, mobile devices, 398

payments, mobile, 411–412

PCI DSS (Payment Card Industry Data Security Standard), 576

PCR (Platform Configuration Registers), 169

PDP, NAC, 365

PDS (Protected Distribution Systems), 250–251

PDU (Power Distribution Units), 207–208

PEAP (Protected EAP), 378, 379, 458–459

peer-to-peer mode, NFC, 392

PEM (Privacy Enhanced Mail), 484–485

penetration testing, 111–112
- attack phase, 117
- black box testing, 113
- bug bounty programs, 112–113
- cleanup, 117

discovery phase, 115–117
footprinting, 115–116
gray box testing, 113
lateral movement, 117
methodology, 112–118
persistence, 117
pivoting, 117
planning phase, 115
reconnaissance, 115–117
reporting phase, 118
security controls, 114
team exercises, 118–119
threat verification, 114
vulnerabilities, 114
war driving, 116
war flying, 116
white box testing, 113, 319

PEP (Policy Enforcement Points), NAC, 365

perimeter security, 239–240
barricades, 241–242
bollards, 241–242
cameras, 242
CCTV, 242
fences, 240–241
gates, 241
guards, 242–243
lighting, 241
signs, 240

peripheral devices, malware, 26–27

permissions, filesystem, 452
auditing, 453
group policies, 453
Linux, 455–456
Manning, Chelsea, 452
Windows, 453–455

persistence, penetration testing, 117

person-hours tracking, 555

PFS (Perfect Forward Secrecy), 268–269

PFX (Personal Information Exchange), 485

pharming, 8

PHI (Personal Health Information), 617

phishing, 7, 8
pharming, 8
smishing, 8
spear phishing, 7
vishing, 8
whaling, 7

phone callbacks, authentication, 198

photographs. *See* pictures

physical attacks
adapters, 27
adversarial AI, 27–28
cables, 27
card cloning, 27
peripheral devices, 26–27
skimming, 27
USB flash drives, 26–27

physical controls, 570

physical security
data destruction, 255–257
environmental controls, 249
fire suppression systems, 252–254
hot/cold aisles, 254–255
HVAC, 251–252
equipment security, 246
air gaps, 248
cable locks, 246
cages, 246–247
Faraday cages, 251
fire suppression systems, 252–254
HVAC, 251–252
locking cabinets/enclosures, 247–248
protected cabling, 249–250
protected distributions, 250–251
saves, 246–247
screen filters, 248
internal security, 243–244
alarms, 244
infrared detectors, 244
locks, 245

mantraps, 245
motion detectors, 244
network segmentation, 350
perimeter security, 239–240
barricades, 241–242
bollards, 241–242
cameras, 242
CCTV, 242
fences, 240–241
gates, 241
guards, 242–243
lighting, 241
signs, 240

PIA (Privacy Impact Assessments), 621–622

piconets, 391

pictures
forensics, 561–562
sending/receiving, mobile device security, 409

PII (Personally Identifiable Information), 616–617

ping command, 497, 500–501

ping flooding, 65

pinning certificates, 488

PIN/passcodes, mobile devices, 398

PIPEDA (Personal Information Protection and Electronic Documents Act), 618

PIV cards, 201–202

pivoting, penetration testing, 117

PKI (Public Key Infrastructure)
CA, 475
bridge CA, 477
certificate chains, 475–476
CPS, 476
intermediate CA, 476–477
key escrow, 477–478
root CA, 476–477
trust hierarchies, 476–477
trust models, 476–477
web of trust, 477
components, 474–475
digital certificates, 478–480
certificate policies, 482
code signing, 483
CRL, 486–487
CSR, 481–482
DER, 485
DV, 482–483
email, 484
EV, 483
formats, 484–485
machine/computer certificates, 484
OCSP, 486–487
OV, 483
P7B certificates, 485
PEM, 484–485
PFX, 485
pinning, 488
private keys, 480–481
public keys, 480–481
revoking, 486
root signing, 484
SAN, 483
self-signed digital certificates, 483
user (client certificates), 484
wildcards, 483
RA, 475

plaintext credentials, unencrypted, 451–452

planning
BCP, 522
contingency planning, 136
COOP, 522, 524–526
DRP, 522, 523
facilities planning
environmental controls, 249
fire suppression systems, 252–254
hot/cold aisles, 254–255
HVAC, 251–252
incident response plans, 512–513
recovery planning, 216, 522

planning phase, penetration testing, 115

platform-specific guides, 579–580

playbooks (SOAR), incident mitigation, 547

plenums, cabling, 250

poisoning

- ARP, 60–61
- DNS, 63–64

policies

- acceptable use policies, mobile device deployments, 415–416
- certificate policies, 482
- corporate policies, mobile device deployments, 415–416
- disaster recovery, 523
- group policies, filesystem permissions, 453
- internet usage policies, 590–591
- organizational security, 583–584
  - AUP, 589–590
  - background checks, 584
  - BPA, 593
  - CBT, 588
  - clean desk policies, 586
  - continuing education policies, 588–589
  - disciplinary/adverse actions policies, 591–592
  - exit interviews, 592
  - HR management policies, 584
  - interoperability agreements, 593–594
  - ISA, 594
  - job rotation, 586
  - least privilege, 585
  - mandatory vacations, 585
  - MOU, 593–594
  - NDA, 591, 615
  - offboarding, 584–585
  - onboarding, 584–585
  - role-based awareness, 586–588
  - rules of behavior, 589–590
  - separation of duties, 585
  - SLA, 593
  - third-party risk management, 592–593
  - training, 588

polymorphic viruses, 18, 19

POP3 (Post Office Protocol 3), 287–288, 296–297

pop-up blockers, 313

portals, captive, 372

ports

- BPDU Guard, 343
- commonly used ports, 333–334
- DHCP snooping, 344
- dynamic/private ports, 333
- loop detection, 343–344
- MAC filtering, 343
- registered ports, 333
- security, 343–344
- stealing, 61
- unnecessary ports, disabling, 332–334
- well-known ports, 333

post-incident activities, incident response, 521–522

power

- adapters, malware, 27
- dual power supplies, 207
- generators, 207
- managed PDU, 207–208
- redundancy, 207–208
- UPS, 207

PowerShell, 68, 495

prepending notifications, email, 7

preservation, forensics, 552

preventive controls, 571

principles of influence

- authority, 10–11
- consensus/social proof, 11
- familiarity/liking, 12
- intimidation, 11
- scarcity, 11–12
- trust, 12

urgency, 11–12

privacy, 613–614

confidential data, 615

data custodians/stewards, 619

data disposal, 620–621

data owners, 619

data retention, 620–621

data roles/responsibilities, 618–620

DPO, 619

GDPR, 620

information life cycle management, 614–615

labeling/handling data, 614–618

mobile device deployments, 416

NDA, 615

PEM, 484–485

PHI, 617

PIA, 621–622

PII, 616–617

PIPEDA, 618

privacy laws, 616–618

privacy notices, 614

private data, 615

proprietary data, 615

public data, 614–615

regulatory compliance, 616–618

screen filters, 248

sensitive data, 615

terms of agreement, 614

private cloud deployments, 161

private keys

digital certificates, 480–481

encryption, 267–268

private/dynamic ports, 333

privileges

escalation, 36, 117

least privilege, account management, 436

user privileges, 587

processing, data in, 129–130

production environments, applications, 167

program-infecting viruses, 18

programmable infrastructures, IaC, 153

proof, social, 11

proprietary data, 615

protected cabling, equipment security, 249–250

protected distributions, 250–251

protecting data, configuration management, 126

protocols, 281

analyzers, 502–504, 536, 537–538

email protocols

IMAP, 287–288, 296–297

MIME, 287

POP3, 287–288, 296–297

S/MIME, 287, 296–297

FTP communication, 295–296

FTPS, 286–287, 295–296

fuzzing, 320

Internet protocols, secure, SSH, 288–289

IPsec, 284–286

LDAPS, 289–290, 298

SFTP, 286–287, 295–296

SNMP, 290–292, 298–299

SRTP, 290, 297–298

web communication

DNSSEC, 294–295

HTTPS, 293–294

SSL, 294

TLS, 294

web protocols

DNS, 284

DNSSEC, 284, 294–295, 297

HTTPS, 282, 293–294

S-HTTP, 282

SSL, 282–283, 294

TLS, 283, 294

provisioning applications, 168

proximity cards, 195, 200–201

proxy servers, 354, 357
caching proxy servers, 354
cloud computing, 430
content filtering proxy servers, 355–357
forward proxy servers, 354–355
reverse proxy servers, 355
transparent proxy servers, 354
pseudo-random numbers, cryptography, 262–263
PSK (Pre-Shared Keys), 372
public cloud deployments, 161–162
public data, 614–615
public keys
digital certificates, 480–481
encryption, 266–268
PUP (Potentially Unwanted Programs), 25
adware, 25–26
cryptojacking, 26
cryptomining, 26
spyware, 25
purple teaming, penetration testing, 118–119
push notifications, 402
Python, 68, 495

Q

QA (Quality Assurance), applications, 167
qualitative risk management, 604
quantitative risk management, 604–605
quantum cryptography, 268
quarantining/isolation, incident mitigation, 542–543

R

RA (Registration Authorities), 475
race conditions, 36
privilege escalation, 36
TOCTOU, 36
RADIUS (Remote Authentication Dial-In User Service), 459–460
EAPoL, 377–378
federation, 377–378
servers, 352, 353, 375
RAID (Redundant Array of Inexpensive Disks), 205–206, 211–214
rainbow tables, 30
ransomware, 23–24
RARP (Reverse ARP), 60–61
RAT (Remote Access Trojans), 20
RBAC (Role-Based Access Control), 467–468
RCS (Rich Communication Service), 409
read/write mode, NFC, 392
realms, authentication, 460
recertification, user access, 436
reconnaissance
networks, 496–502
penetration testing, 115–117
social engineering, 4–5
Record protocol, TLS, 283
records, time offset, 562
recovery
disaster recovery, cloud computing, 430
planning, 216, 522
COOP, 522, 526
DRP, 522, 523
recoverability from incidents, 519–521
recursive (caching) servers, DNS, 284
red teaming, penetration testing, 118–119
redaction, data encryption, 131
redirection, URL, 62–63
redundancy
ISP, 208
power, 207–208
RAID, 205–206, 211–214

- SAN, 205–206
- software, 205–206

refactoring, 41

regions, cloud computing, 423

registered ports, 333

registers, risk, 598–599

registries, malware, 16

regulatory compliance, 616–618

regulatory requirements, 576

remote access, SSL/TLS, 294

remote wiping, mobile devices, 399–400

removable media control, 26–27, 316

replay
- attacks, 45
- organizational security, 502–504

reporting
- after-action reports, 526
- incident response requirements, 514–515
- penetration testing, 118

repos (repositories), 83

reputation, domains, 62

request forgeries, 41
- CSRF, 41–43
- SSRF, 42–43

resident viruses, 17

resiliency, 519–521
- application development, 180
- backups, 214–219
- defense in depth, 221–223
- high availability, 208–209
- load balancers, 209–211
- nonpersistence, snapshots, 219–220
- RAID, 205–206, 211–214
- redundancy, 205–208
- site resiliency, 137, 138
  - cold sites, 138
  - hot sites, 137–138
  - warm sites, 137–138
- snapshots, 218–221

resources
- cloud computing policies, 424–426
- constraints, special-purpose embedded devices, 236
- dynamic resource allocation, 422
- exhaustion, 37

rest, data at, 129

restorations, cloud computing, 430

retention, data, 620–621

retinas, biometric authentication, 199

reusing code, 174–175

reverse proxy servers, 355

review updates, configuration management, 126

reviewing user access, 436–437

revoking
- certificates, incident mitigation, 543
- digital certificates, 486

RFID (Radio Frequency Identification), 57–58, 401

rights management, 132–133

risk management
- ALE, 606
- ARO, 606
- BIA, 606–607
- cloud computing, 429
- critical functions, 607–608
- impact, 610–611
- mission-essential functions, 607–608
- MTBF, 609–610
- MTTF, 609–610
- MTTR, 609–610
- qualitative risk management, 604
- quantitative risk management, 604–605
- risk acceptance, 600
- risk analysis, 598
- risk appetite, 599
- risk assessments, 598, 602–604
- risk avoidance, 599–600
- risk awareness, 599
- risk deterrence, 600

risk heat maps, 603–604
risk matrices, 603
risk mitigation, 600
risk response, 599–601
risk transference, 600
risks registers, 598–599
RPO, 608
RTO, 608
single points of failure, 607–608
SLE, 605
third-party risk management, 592–593
threat assessments, 601–602

RMF (Risk Management Framework), 578

rogue AP, 55

role-based access control model, 440

role-based awareness, 586–588

ROM bootloader, 327

root, chain of, 327

root CA, 476–477

root signing, digital certificates, 484

rooting, 405–406

rootkits, 20–21

roots of trust, hardware, 329–330

rotating
jobs, 586
passwords, 446

route command, 498

routers
CIDR, 300
inter-VLAN routing, 344, 345
network segmentation, 340–342
NIPRNET, 250–251
SIRPNET, 250–251
SNMP, 298–299

RPO (Recovery Point Objectives), 608

RSA Security, state actors, 79

RTO (Recovery Time Objectives), 608

RTOS (Real-Time Operating Systems), 226–227

RTP (Real-time Transfer Protocol), 290

rules of behavior, 589–590

rules of engagement, bug bounty programs, 112–113

runbooks (SOAR), incident mitigation, 547

S

SaaS (Software as a Service), 159–160

SAE (Simultaneous Authentication of Equals), 377

SAFECode (Software Assurance Forum for Excellence in Code), 171

safes, equipment security, 246–247

salting, 272

SAML (Security Assertion Markup Language), 461–462

SAN (Storage Area Networks), 205–206

SAN (Subject Alternate Name), digital certificates, 483

sandboxing, 141, 321, 394

sanitation, data, 505–506

SATCOM (Satellite Communication), 390–391

SCADA (Supervisory Control and Data Acquisition), 227–229, 578

scalability, applications, 184

scanless command, 499

scanners
heuristic scanning, 311
host-based security, 311
IoT scanners, 230–231
vulnerability scanners, 89, 100
application scanners, 100
CVE standard, 101–102
CVSS, 102
false negatives/positives, 103
network scanners, 100
web application scanners, 100

scarcity, principles of influence, 11–12

schemas, IP, 125

Schneier, Bruce, 600

screen filters, equipment security, 248

screen locks, 398

screenshots, forensics, 563

scripting
- Bash, 68
- malicious code/script execution, 57, 68–69
- PowerShell, 68
- Python, 68
- script kiddies, 76–77
- VBA, 69

SDK (Software Development Kits), application development, 175

SDN (Software-Defined Networking), 152–153

SDV (Software-Defined Visibility), 152–153

sealed storage, 168, 325

sealing/unsealing TPM, 325

SEAndroid, 393, 394

secrets managers, cloud computing, 426

secure configurations, 335–336, 579

secure cookies, 318

secure data destruction, 255–256
- declassification, 256
- degaussing, 256
- encryption, 256
- paper records, 256–257
- wiping, 256

security groups, cloud computing, 423–424

security guards, perimeter security, 242–243

security logs, 533

SED (Self-Encrypting Drives), 323

segmentation
- mobile devices, 402–403
- networks, 340, 349–350
  - air gaps, 350
  - bridges, 345–346
  - DMZ, 350–353
  - firewalls, 347–348, 544–545
  - implicity deny, 348–349
  - physical security, 350
  - routers, 340–342
  - switches, 342–343, 350
  - VLAN, 342–343, 344–345

self-signed digital certificates, 483

sensitive data protection/privacy, 613–614
- confidential data, 615
- data custodians/stewards, 619
- data disposal, 620–621
- data owners, 619
- data retention, 620–621
- data roles/responsibilities, 618–620
- DPO, 619
- GDPR, 620
- information life cycle management, 614–615
- labeling/handling data, 614–618
- NDA, 615
- PHI, 617
- PIA, 621–622
- PII, 616–617
- PIPEDA, 618
- privacy laws, 616–618
- privacy notices, 614
- private data, 615
- proprietary data, 615
- public data, 614–615
- regulatory compliance, 616–618
- sensitive data, 615
- terms of agreement, 614

sensors, NIDS, 361

separation of duties, 585

serverless architectures, 159

servers
- authoritative servers, DNS, 284
- DNS servers, 284
- server-side validation, 176

service packs, 95

session affinity, 210

session keys, 268–269

sFlow, 538

SFTP (SSH File Transfer Protocol), 286–287, 295–296

sharing centers, threat intelligence/ resource sources, 81–82

shell environments

- OpenSSH, 494
- OpenSSL, 494
- PowerShell, 495
- Python, 495
- SSH, 288–289, 494
  - command-line interface, 495
  - file-manipulation commands, 495–496

Shibboleth, 464

shimming, 41

short-range wireless communications, 56

- Bluetooth, 56
- NFC, 57
  - confidentiality, 57
  - DoS attacks, 57
  - malicious code/script execution, 57
  - MITB attacks, 59
  - MITM attacks, 57, 58–59
- RFID, 57–58

shoulder surfing, 6

S-HTTP (Secure HyperText Transfer Protocol), 282

sideloading applications, 408

SIEM (Security Information and Event Management), 103–107, 530–531

signatures

- biometric authentication, 199
- digital signatures, 270–271
- intrusion detection, 363

signing, code, 318

signs, perimeter security, 240

single points of failure, 607–608

sinkholes, DNS, 141

SIRPNET (Secure Internet Protocol Router Network), 250–251

site resiliency, 137, 138

- cold sites, 138
- hot sites, 137–138
- warm sites, 137–138

site surveys, wireless network installations, 381–382

site-to-site VPN, 359

skimming, 27

SLA (Service-Level Agreements), 593

slag code, 22

SLE (Single Loss Expectancy), 605

smart cards, FDE, 324

smart devices, IoT, 229–231

smart meters, 234–235

S/MIME (Secure Multipurpose Internet Mail Extensions), 287, 296–297

smishing, 8

SMS (Short Message Service), OTP, 198

smurfing attacks, 65

snapshots, 218–221

sniffers, 503–504

snlper command, 499

SNMP (Simple Network Management Protocol), 290–292, 298–299

snooping, DHCP, 344

Snopes.com, 10

Snowden, Edward, 77

SOAR (Security Orchestration, Automation, and Response), 108–109, 546–548

SOC (Service Organizational Control), 577, 578

SoC (System on a Chip), 226–227

social engineering, 4–5

- credential harvesting, 8
- dumpster diving, 5–6
- hoaxes, 10

hybrid warfare, 10
identity fraud, 4–5
influence campaigns, 10
invoice scams, 8
pharming, 8
phishing, 7–8
prepending notifications, email, 7
principles of influence, 10–12
reconnaissance, 4–5
shoulder surfing, 6
smishing, 8
spear phishing, 7
SPIM, 7
tailgating, 5
typo squatting, 9
vishing, 8
watering hole attacks, 9
whaling, 7

social proof/consensus, principles of influence, 11

software
antispam software, 312–313
antispyware programs, 313
antivirus software, 310–312, 417
camouflage, 174
composition analysis, 429
diversity, 205–206
fuzzing, 172
improper error handling, 37
improper input handling, 37
race conditions, 36
SaaS, 159–160
SDN, 152–153
SDV, 152–153
white box testing, 113, 319

SOP (Standard Operational Procedures), 584

source routing bridges, 346

sovereignty, data, 138–139

SOX (Sarbanes-Oxley Act), 576

spam
antispam software, 312–313
SPIM, 7

spanning tree algorithms, 346

spear phishing, 7

special-purpose embedded devices, 233
aircraft, 235–236
drones, 235–236
implied trust, 236
medical devices, 233–234
resource constraints, 236
UAV, 235–236
vehicles, 234–235

SPIM (Spam over Internet Messaging), 7

split tunneling, VPN, 360

spoofing, MAC, 60

sprawl, VM, 151

spraying, password, 30

spyware, 25

SQL (Structured Query Language)
SQL injection, 39
stored procedures, 173

SRG (System security Requirements Guide), 580

SRK (Storage Root Keys), TPM, 325

SRTP (Secure Real-time Transfer Protocol), 290, 297–298

SSH (Secure Shell), 288–289, 494
command-line interface, 495
file-manipulation commands, 495–496

SSID (Service Set Identifiers), 384–385

SSL (Secure Socket Layer), 282–283, 294
encrypted traffic management, 134–135
HTTPS, 134–135, 282, 293–294
LDAPS, 289–290, 298
SFTP, 286–287, 295–296
stripping, 45–46

SSO (Single-Sign On), 192–193, 450–451, 460, 464

SSRF (Server-Side Request Forgeries), 42–43

staging applications, 167

standalone AP, 380

standard naming conventions, configuration management, 125

standards, 575–576

state actors, 79

stateful firewalls, 348

stateless firewalls, 347–348

static code analyzers, 319

static codes, authentication, 198

static keys, 263

static passwords, 396

stealing, port, 61

stealth viruses, 18

steganography, 273–274

sticky sessions, 210

STIX (Structured Threat Information eXpression), 83

storage

- data storage, vulnerabilities, 95–96
- mobile devices, 408–409
- NAS, 353
- removable media control, 316
- sealed storage, 168, 325
- SRK, TPM, 325
- USB flash drives
  - DLP, 316
  - malware, 26–27

storage segmentation. *See* segmentation

stored procedures, 173

STP (Spanning Tree Protocol)

- cables, 249–250
- loops, 346

strategic intelligence, 554

stream ciphers, 265–266

stress testing, 321

stretching, key, 263

stripping, SSL, 45–46

structural threats, 602

Stuxnet, state actors, 79

subscription services, 303

supply chains, vulnerabilities, 95–96

surveillance systems, 233

SWG (Secure Web Gateways), 428–429

swipe card locks, 245

switches

- NAC, 366
- network segmentation, 342–343, 350
- port security, 343–344
- SNMP, 298–299

symmetric cryptography, 264–265

- block ciphers, 265–266
- stream ciphers, 265–266

symmetric keys, Kerberos authentication, 464

SYN flooding, 65

synchronization, time, NTP, 302

syndicates (threat actors), criminal, 78

syslog, 106, 535

system administrators, 587

system event logs, 533–534

system hardening, 332–334

system health monitoring, 533

system images, data acquisition, 559–560

system logs, 531–532

system owners, 587

T

tabletop exercises, incident response, 516–517

TACACS+ (Terminal Access Controller Access Control System Plus), 460–461

tail command, SSH, 495

tailgating, 5

Target, HVAC intrusion case, 231

TAXII (Trusted Automated eXchange of Indicator Information), 83

TCG (Trusted Computing Groups), 169

tcpdump, 503

tcpreplay, 503

team exercises, penetration testing, 118–119

teaming, NIC, 211

teardrop attacks, 65

technical controls, 570

ten-tape rotation backup schemes, 216

terms of agreement, privacy, 614

testing

- applications, 166–167
- fuzzing, 172
- incident response, 516–517
- penetration testing, 111–112
    - attack phase, 117
    - black box testing, 113
    - bug bounty programs, 112–113
    - cleanup, 117
    - discovery phase, 115–117
    - footprinting, 115–116
    - gray box testing, 113
    - lateral movement, 117
    - methodology, 112–118
    - persistence, 117
    - pivoting, 117
    - planning phase, 115
    - reconnaissance, 115–117
    - reporting phase, 118
    - security controls, 114
    - team exercises, 118–119
    - threat verification, 114
    - vulnerabilities, 114
    - war driving, 116
    - war flying, 116
    - white box testing, 113, 319
- stress testing, 321
- white box testing, 113, 319

tethering, mobile devices, 411

texting (MMS), mobile device security, 409

theharvester command, 499

thin AP, 380

third-party app stores, 407–408

third-party cloud security solutions, 428–430

third-party libraries, application development, 175

third-party risk management, 592–593

third-party risks, 95–96

third-party updates, hardware roots of trust, 329

threats

- accidental threats, 601
- adversarial threats, 601
- assessments, 601–602
- environmental threats, 602
- hunting, 107
    - cyber kill chains, 107, 510
    - intelligence fusion, 107–108
- intelligence/resource sources, 81
    - ISAC, 82
    - ISAO, 82
    - OSINT, 81, 82–85
    - sharing centers, 81–82
- management, UTM, 357–358
- maps, 83
- structural threats, 602
- threat actors, 73–74
    - APT, 79
    - attack vectors, 80–81
    - attributes, 74–75
    - competitors, 78–79
    - criminal syndicates, 78
    - hackers, 76
    - hacktivists, 78
    - inside threat actors, 77
    - script kiddies, 76–77
    - state actors, 79
    - types (overview), 75–76
- verification, penetration testing, 114

time of date, account management, 438
time offset, records, 562
time synchronization, NTP, 302
TKIP (Temporal Key Integrity Protocol), 376
TLS (Transport Layer Security), 134–135, 283, 294
  EAP-TLS, 377, 379
  EAP-TTLS, 378, 379
TOCTOU (Time-of-Check to Time-to-Use), 36
token keys, 198
tokenization, 130–131
tokens, security, 195–198
TOTP (Time-based One-Time Passwords), 196, 198
Tower of Hanoi backups, 216
TPM (Trusted Platform Modules), 168–169, 324–326, 328, 451
traceroute command, 498, 500–501
tracert comand, 498
tracking person-hours, 555
traffic management, encryption, 134–135
training
  computer-based training, 588
  incident response, 516–517
transferring risk, 600
transit, data in, data encryption, 129
transitive trust, 194–195, 396–397
transparent basic bridges, 345
transparent learning bridges, 346
transparent proxy servers, 354
transparent spanning bridges, 346
transport mode, IPsec, 284–285
traversal, directory, 44–45
Trojans, 19–20
  backdoor Trojans, 20
  downloader Trojans, 20
  infostealer Trojans, 20
  keylogger Trojans, 20
  RAT, 20
trust
  chain of root, 327
  hierarchies, 476–477
  implied trust, 236
  models, 476–477
  OS, 336
  principles of influence, 12
  roots of trust, hardware, 329–330
  transitive trust, 194–195, 396–397
  web of trust, 477
  Zero Trust, 352
tunnel mode, IPsec, 285
tunneling
  EAP-FAST, 378–379
  EAP-TTLS, 378, 379
  VPN, 360
twisted-pair cables, 249–250
Type I hypervisors, 146, 147–148
Type II hypervisors, 147–148
typo squatting, 9

U

UAC (User Account Control), 435
UAV (Unmanned Aerial Vehicles)
  embedded control systems, 235–236
  war flying, 116
UEFI (Unified Extended Firmware Interface), 326–327
UEM (Unified Endpoint Management), 394
unencrypted plaintext credentials, 451–452
unlocking carriers, mobile devices, 406–407
unnecessary ports, disabling, 332–334
unsealing/sealing TPM, 325
updates, 95
  antivirus software, 311
  hotfixes, 95

- OTA updates, mobile devices, 407
- reviews, configuration management, 126
- service packs, 95
- third-party updates, hardware roots of trust, 329

UPS (Uninterruptible Power Supplies), 207

urgency, principles of influence, 11–12

URL (Uniform Resource Locators)
- filtering, incident mitigation, 543
- redirection, 62–63

U.S. Department of Homeland Security (DHS), AIS, 83

U.S. Organized Crime Control Act of 1970, 78

USB (Universal Serial Bus)
- cables, malware, 27
- communication, 392–393
- flash drives
  - DLP, 316
  - malware, 26–27
- smart card-enabled USB tokens, FDE, 324
- USB OTG, 408

users
- access, auditing/reviews, 436–437
- access control model, 439–440
- client certificates, 484
- data owners, 587, 619
- executive users, 587
- general users, 587
- permissions, 452
  - auditing, 453
  - Manning, Chelsea, 452
- privileged users, 587
- system administrators, 587
- system owners, 587
- usernames, FDE, 324

UTM (Unified Threat Management), 357–358

UTP cables, 249–250

UWYT, mobile device deployments, 413

V

vacations, mandatory, 585

Valasek, Chris, 235

validation
- client-side validation, 175–176
- digital certificates
  - DV, 482–483
  - EV, 483
  - OV, 483
- input validation, application development, 177–178
- server-side validation, 176

vaults, password, 450–451

VBA (Virtual Basic for Applications), 69

VDE (Virtual Desktop Environments), 150

VDI (Virtual Desktop Infrastructure), 150
- mobile devices, 413–414

vectors, attack, 80–81

vehicles, embedded control systems, 234–235

veins/blood vessels, biometric authentication, 199

vendors
- vendor-specific guides, 579–580
- vulnerabilities, 95–96

verifying threats, penetration testing, 114

version control
- applications, 170
- DevOps, 170

video
- forensics, 561–562
- mobile devices, 409–410
- SRTP, 297–298

VIP addresses, 211

virtualization, 145–146

- containers, 148–150
- C-RAN, 150
- hypervisors, 146
  - Type I hypervisors, 146, 147–148
  - Type II hypervisors, 147–148
- IaC, 153
- JVM, 149–150
- microservices, 148–149
- MSP, 154
- MSSP, 154
- on-premises vs off-premises solutions, 154–155
- SDN, 152–153
- SDV, 152–153
- VDE, 150
- VDI, 150
- VM, 149
  - escape protection, 151–152
  - JVM, 149–150
  - sprawl, 151
  - staging environments, 167
- VMM, 147

viruses, 17, 19

- antivirus software, 310–312
- armored viruses, 18, 19
- boot sector viruses, 17
- file-infecting viruses, 18
- macro viruses, 17
- multipartite viruses, 18
- nonresident viruses, 17
- polymorphic viruses, 18, 19
- program-infecting viruses, 18
- resident viruses, 17
- stealth viruses, 18

vishing, 8

VLAN (Virtual Local Area Networks), 342–343, 344–345

VM (Virtual Machines), 149

- escape protection, 151–152
- JVM, 149–150
- sprawl, 151
- staging environments, 167

VMM (Virtual Machine Monitors), 147

voice

- encryption, mobile devices, 404
- SRTP, 297–298
- voiceprints, biometric authentication, 199

VoIP (Voice over Internet Protocol), encryption, mobile devices, 404

volatility, order of, 555–556

VPC (Virtual Private Clouds), 422, 423

VPN (Virtual Private Networks)

- cloud computing, 429
- concentrators, 358–360
- site-to-site VPN, 359
- tunneling, 360

VulnDB, 82

vulnerabilities

- cloud computing, 90, 429
- credentialed/noncredentialed vulnerability testing, 103
- CVE standard, 101–102
- CVSS, 102
- data storage, 95–96
- impact, 96–97
- intrusive/nonintrusive vulnerability testing, 102–103
- medical devices, 234
- on-premises systems, 90
- outsourced code development, 95–96
- OVAL, 102
- penetration testing, 114
- scanners, 89, 100
  - application scanners, 100
  - CVE standard, 101–102
  - CVSS, 102
  - false negatives/positives, 103
  - network scanners, 100
  - web application scanners, 100
- supply chains, 95–96
- vendors, 95–96

weak configurations, 91–94
weak/improper patch management, 94–95
zero-day vulnerabilities, 89–91
vulnerability databases, 82

W

W3C logs, 531–532
WAF (Web Application Firewalls), 353–354
wall adapters, malware, 27
WannaCry, 24, 141
war driving, 116
war flying, 116
warm sites, 137–138
watering hole attacks, 9
weak configurations, 91–94
weak/improper patch management, 94–95
wearable technology, IoT, 229–230
web applications
firewalls, 317
logs, 531–532
scanners, 100
web browsers, MITB attacks, 59
web communication, secure
DNSSEC, 294–295
HTTPS, 293–294
SSL, 294
TLS, 294
web of trust, 477
web protocols, secure
DNS, 284
DNSSEC, 284, 294–295, 297
HTTPS, 282, 293–294
S-HTTP, 282
SSL, 282–283, 294
TLS, 283, 294
web server logs, 531–532
websites, resiliency, 137, 138
cold sites, 138
hot sites, 137–138
warm sites, 137–138
well-known ports, 333
WEP (Wired Equivalent Privacy), 373–375
wet-pipe fire suppression systems, 252–253
whaling, 7
white box testing, 113, 319
white hats, 76
white teaming, penetration testing, 118–119
whitelists, 43, 317, 396, 545–546
Wi-Fi Alliance, 374
Wi-Fi analyzers, 381
Wi-Fi Direct, mobile devices, 410–411
wildcards, digital certificates, 483
Windows
Event Viewer, 534
filesystem permissions, 453–455
WinHex, 506
wiping
remote wiping, 399–400
secure data destruction, 256
wireless communication
Bluetooth, 56
Mobile Wi-Fi, mobile devices, 391
NFC, 57
confidentiality, 57
DoS attacks, 57
malicious code/script execution, 57
MITB attacks, 59
MITM attacks, 57, 58–59
RFID, 57–58
Wi-Fi Alliance, 374
wireless locks, 245
wireless networks, 54
AC, 379–380
access methods, 371–372
antennas
directional antennas, 380–381

- intelligent antennas, 380
- omnidirectional antennas, 380–381
- placement, 381
- AP, 379–380, 381
- authentication, PSK, 372
- band direction/selection, 383
- captive portals, 372
- deauthentication attacks, 55
- dissociation attacks, 55
- EAP, 372–373, 377
  - EAP-FAST, 378–379
  - EAPoL, 377–378
  - EAP-TLS, 377, 379
  - EAP-TTLS, 378, 379
  - PEAP, 378, 379
- heat maps, 381–382
- interference, 382–383
- IV attacks, 55–56
- jamming attacks, 54–55
- MAC filtering, 383–384
- PSK, 372
- rogue AP, 55
- site surveys, 381–382
- SSID broadcasts, 384–385
- WEP, 373–375
- Wi-Fi Alliance, 374
- Wi-Fi analyzers, 381
- Wi-Fi Direct, 410–411
- wireless cryptographic protocols, 373–377
- WLAN controllers, 379–380
- WPA, 374, 375–376
  - TKIP, 376
  - WPA2, 374, 376
  - WPA3, 374, 376, 377
  - WPA-Enterprise, 375
  - WPA-Personal, 375
- WPS, 373–374

Wireshark, 503

witness interviews, forensics, 563–564

WLAN controllers, 379–380

workloads, cloud computing, 422, 430

worms, 19

WPA (Wi-Fi Protected Access), 374, 375–376
- TKIP, 376
- WPA2, 374, 376
- WPA3, 374, 376, 377
- WPA-Enterprise, 375
- WPA-Personal, 375

WPS (Wi-Fi Protected Security), 373–374

wrapping, TPM, 325

X

X.509 certificates, 478–479

XaaS (Anything as a Service), 160, 303

XML injection, 40

XSS (Cross-Site Scripting), 39

Y - Z

Zero Trust, 352

zero-day vulnerabilities, 89–91

Zigbee, 230–231

zombie armies, 22

EXAM CRAM

CompTIA® Security+ SY0-601

Save 10% on Exam Voucher

See Inside

PEARSON IT CERTIFICATION

MARTY M. WEISS