PEARSON IT CERTIFICATION

Save 10% on Exam Voucher
See Inside

Practice Tests

Flash Cards

Review Exercises

Study Planner

Cert Guide

Advance your IT career with hands-on learning

CompTIA®

Advanced Security Practitioner (CASP+)

CAS-004

TROY McMILLAN

FREE SAMPLE CHAPTER

CompTIA® Advanced Security Practitioner (CASP+) CAS-004 Cert Guide

Troy McMillan

CompTIA® Advanced Security Practitioner (CASP+) CAS-004 Cert Guide

ISBN-13: 978-0-13-734895-4

ISBN-10: 0-13-734895-9

Library of Congress Control Number: 2022933627

ScoutAutomatedPrintCode

Editor-in-Chief
Mark Taub

Director, ITP Product Management
Brett Bartow

Executive Editor
Nancy Davis

Development Editor
Ellie Bru

Managing Editor
Sandra Schroeder

Senior Project Editor
Tonya Simpson

Copy Editor
Kitty Wilson

Indexer
Tim Wright

Proofreader
Barbara Mack

Technical Editor
Chris Crayton

Publishing Coordinator
Cindy Teeters

Cover Designer
Chuti Prasertsith

Compositor
codeMantra

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.

Pearson's Commitment to Diversity, Equity, and Inclusion

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

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

Our ambition is to purposefully contribute to a world where

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

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

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

Contents at a Glance

Introduction 1

Part I: Security Architecture

CHAPTER 1 Ensuring a Secure Network Architecture 3

CHAPTER 2 Determining the Proper Infrastructure Security Design 73

CHAPTER 3 Securely Integrating Software Applications 85

CHAPTER 4 Securing the Enterprise Architecture by Implementing Data Security Techniques 125

CHAPTER 5 Providing the Appropriate Authentication and Authorization Controls 149

CHAPTER 6 Implementing Secure Cloud and Virtualization Solutions 185

CHAPTER 7 Supporting Security Objectives and Requirements with Cryptography and Public Key Infrastructure (PKI) 203

CHAPTER 8 Managing the Impact of Emerging Technologies on Enterprise Security and Privacy 219

Part II: Security Operations

CHAPTER 9 Performing Threat Management Activities 231

CHAPTER 10 Analyzing Indicators of Compromise and Formulating an Appropriate Response 251

CHAPTER 11 Performing Vulnerability Management Activities 275

CHAPTER 12 Using the Appropriate Vulnerability Assessment and Penetration Testing Methods and Tools 293

CHAPTER 13 Analyzing Vulnerabilities and Recommending Risk Mitigations 315

CHAPTER 14 Using Processes to Reduce Risk 347

CHAPTER 15 Implementing the Appropriate Incident Response 367

CHAPTER 16 Forensic Concepts 385

CHAPTER 17 Forensic Analysis Tools 399

Part III: Security Engineering and Cryptography

CHAPTER 18 Applying Secure Configurations to Enterprise Mobility 419

CHAPTER 19 Configuring and Implementing Endpoint Security Controls 437

CHAPTER 20 Security Considerations Impacting Specific Sectors and Operational Technologies 459

CHAPTER 21 Cloud Technology's Impact on Organizational Security 477

CHAPTER 22 Implementing the Appropriate PKI Solution 499

CHAPTER 23 Implementing the Appropriate Cryptographic Protocols and Algorithms 519

CHAPTER 24 Troubleshooting Issues with Cryptographic Implementations 543

Part IV: Governance, Risk, and Compliance

CHAPTER 25 Applying Appropriate Risk Strategies 555

CHAPTER 26 Managing and Mitigating Vendor Risk 607

CHAPTER 27 The Organizational Impact of Compliance Frameworks and Legal Considerations 625

CHAPTER 28 Business Continuity and Disaster Recovery Concepts 657

CHAPTER 29 Final Preparation 673

APPENDIX A Answers to the Review Questions 679

Glossary 709

Index 761

Online Elements

APPENDIX B Memory Tables

APPENDIX C Memory Tables Answer Key

APPENDIX D Study Planner

Glossary

Table of Contents

Introduction 1

Part I: Security Architecture

Chapter 1 Ensuring a Secure Network Architecture 3

Services 3

Load Balancer 3

Intrusion Detection System (IDS)/Network Intrusion Detection System (NIDS)/Wireless Intrusion Detection System (WIDS) 3

Intrusion Prevention System (IPS)/Network Intrusion Prevention System (NIPS)/Wireless Intrusion Prevention System (WIPS) 6

Web Application Firewall (WAF) 6

Network Access Control (NAC) 8

Quarantine/Remediation 9

Persistent/Volatile or Non-persistent Agent 9

Agent vs. Agentless 9

Virtual Private Network (VPN) 10

Domain Name System Security Extensions (DNSSEC) 11

Firewall/Unified Threat Management (UTM)/Next-Generation Firewall (NGFW) 11

Types of Firewalls 12

Next-Generation Firewalls (NGFWs) 14

Firewall Placement 15

Deep Packet Inspection 19

Network Address Translation (NAT) Gateway 19

Stateful NAT 20

Static vs. Dynamic NAT 21

Internet Gateway 21

Forward/Transparent Proxy 21

Reverse Proxy 22

Distributed Denial-of-Service (DDoS) Protection 22

Routers 22

Routing Tables 23

Additional Route Protection 25
Mail Security 26
IMAP 26
POP 27
SMTP 27
Email Spoofing 27
Spear Phishing 28
Whaling 28
Spam 28
Captured Messages 29
Disclosure of Information 30
Malware 30
Application Programming Interface (API) Gateway/Extensible Markup Language (XML) Gateway 30
Traffic Mirroring 30
Switched Port Analyzer (SPAN) Ports 31
Port Mirroring 31
Virtual Private Cloud (VPC) 32
Network Tap 32
Sensors 32
Security Information and Event Management (SIEM) 33
File Integrity Monitoring (FIM) 35
Simple Network Management Protocol (SNMP) Traps 36
NetFlow 36
Data Loss Prevention (DLP) 37
Antivirus 39
Segmentation 39
Microsegmentation 40
Local Area Network (LAN)/Virtual Local Area Network (VLAN) 40
Jump Box 43
Screened Subnet 44
Data Zones 44
Staging Environments 45
Guest Environments 45
VPC/Virtual Network (VNET) 45

Availability Zone 46
NAC Lists 47
Policies/Security Groups 47
Regions 49
Access Control Lists (ACLs) 49
Peer-to-Peer 49
Air Gap 49
De-perimeterization/Zero Trust 49
Cloud 50
Remote Work 50
Mobile 50
Outsourcing and Contracting 52
Wireless/Radio Frequency (RF) Networks 53
WLAN-802.11 53
WLAN Standards 54
WLAN Security 56
Merging of Networks from Various Organizations 58
Peering 59
Cloud to on Premises 59
Data Sensitivity Levels 59
Mergers and Acquisitions 60
Cross-domain 61
Federation 61
Directory Services 61
Software-Defined Networking (SDN) 62
Open SDN 63
Hybrid SDN 64
SDN Overlay 64
Exam Preparation Tasks 66
Review All Key Topics 66
Define Key Terms 68
Complete Tables and Lists from Memory 69
Review Questions 69

Chapter 2 Determining the Proper Infrastructure Security Design 73

Scalability 73

Vertically 73

Horizontally 74

Resiliency 74

High Availability/Redundancy 74

Diversity/Heterogeneity 75

Course of Action Orchestration 75

Distributed Allocation 76

Replication 76

Clustering 76

Automation 76

Autoscaling 76

Security Orchestration, Automation, and Response (SOAR) 77

Bootstrapping 77

Performance 77

Containerization 78

Virtualization 79

Content Delivery Network 79

Caching 80

Exam Preparation Tasks 81

Review All Key Topics 81

Define Key Terms 81

Complete Tables and Lists from Memory 81

Review Questions 82

Chapter 3 Securely Integrating Software Applications 85

Baseline and Templates 85

Baselines 85

Create Benchmarks and Compare to Baselines 85

Templates 86

Secure Design Patterns/Types of Web Technologies 87

Storage Design Patterns 87

Container APIs 88

Secure Coding Standards 89
CVE 90
DISA STIG 90
PA-DSS 90
Application Vetting Processes 90
API Management 91
Middleware 91
Software Assurance 92
Sandboxing/Development Environment 92
Validating Third-Party Libraries 93
Defined DevOps Pipeline 93
Code Signing 94
Interactive Application Security Testing (IAST) vs. Dynamic Application Security Testing (DAST) vs. Static Application Security Testing (SAST) 95
Interactive Application Security Testing (IAST) 95
Static Application Security Testing (SAST) 95
Dynamic Application Security Testing (DAST) 95
Code Analyzers 95
Fuzzer 95
Static 98
Dynamic 98
Misuse Case Testing 99
Test Coverage Analysis 99
Interface Testing 100
Considerations of Integrating Enterprise Applications 100
Customer Relationship Management (CRM) 100
Enterprise Resource Planning (ERP) 100
Configuration Management Database (CMDB) 101
Content Management System (CMS) 101
Integration Enablers 101
Directory Services 101
Domain Name System (DNS) 101
Service-Oriented Architecture (SOA) 102
Enterprise Service Bus (ESB) 103

Integrating Security into Development Life Cycle 103
Formal Methods 103
Requirements 103
Fielding 104
Insertions and Upgrades 104
Disposal and Reuse 104
Testing 105
Validation and Acceptance Testing 107
Regression 107
Unit Testing 107
Development Approaches 109
SecDevOps 109
Agile 109
Spiral 111
Security Implications of Agile Software Development 112
Security Implications of the Waterfall Model 113
Security Implications of the Spiral Model 114
Versioning 114
Continuous Integration/Continuous Delivery (CI/CD) Pipelines 116
Best Practices 117
Open Web Application Security Project (OWASP) 117
Proper Hypertext Transfer Protocol (HTTP) Headers 117
Exam Preparation Tasks 119
Review All Key Topics 119
Define Key Terms 120
Complete Tables and Lists from Memory 121
Review Questions 121

Chapter 4 Securing the Enterprise Architecture by Implementing Data Security Techniques 125

Data Loss Prevention 125
Blocking Use of External Media 125
Print Blocking 126
Remote Desktop Protocol (RDP) Blocking 126

Clipboard Privacy Controls 127
Restricted Virtual Desktop Infrastructure (VDI) Implementation 128
Data Classification Blocking 128
Data Loss Detection 129
Watermarking 129
Digital Rights Management (DRM) 129
Network Traffic Decryption/Deep Packet Inspection 130
Network Traffic Analysis 130
Data Classification, Labeling, and Tagging 130
Metadata/Attributes 130
XACML 130
LDAP 131
Obfuscation 131
Tokenization 131
Scrubbing 131
Masking 132
Anonymization 132
Encrypted vs. Unencrypted 132
Data Life Cycle 132
Create 132
Use 133
Share 133
Store 133
Archive or Destroy 133
Data Inventory and Mapping 133
Data Integrity Management 134
Data Storage, Backup, and Recovery 134
Redundant Array of Inexpensive Disks (RAID) 138
Exam Preparation Tasks 143
Review All Key Topics 143
Define Key Terms 144
Complete Tables and Lists from Memory 144
Review Questions 144

Chapter 5 Providing the Appropriate Authentication and Authorization Controls 149

Credential Management 149

Password Repository Application 149

End-User Password Storage 149

On Premises vs. Cloud Repository 150

Hardware Key Manager 150

Privileged Access Management 151

Privilege Escalation 151

Password Policies 151

Complexity 153

Length 153

Character Classes 153

History 154

Maximum/Minimum Age 154

Auditing 155

Reversable Encryption 156

Federation 156

Transitive Trust 156

OpenID 156

Security Assertion Markup Language (SAML) 157

Shibboleth 158

Access Control 159

Mandatory Access Control (MAC) 160

Discretionary Access Control (DAC) 160

Role-Based Access Control 161

Rule-Based Access Control 161

Attribute-Based Access Control 161

Protocols 162

Remote Authentication Dial-in User Service (RADIUS) 162

Terminal Access Controller Access Control System (TACACS) 163

Diameter 164

Lightweight Directory Access Protocol (LDAP) 164

Kerberos 165
OAuth 166
802.1X 166
Extensible Authentication Protocol (EAP) 167
Multifactor Authentication (MFA) 168
Knowledge Factors 169
Ownership Factors 169
Characteristic Factors 170
Physiological Characteristics 170
Behavioral Characteristics 171
Biometric Considerations 172
2-Step Verification 173
In-Band 174
Out-of-Band 174
One-Time Password (OTP) 175
HMAC-Based One-Time Password (HOTP) 175
Time-Based One-Time Password (TOTP) 175
Hardware Root of Trust 176
Single Sign-On (SSO) 177
JavaScript Object Notation (JSON) Web Token (JWT) 178
Attestation and Identity Proofing 179
Exam Preparation Tasks 180
Review All Key Topics 180
Define Key Terms 181
Review Questions 181
Chapter 6 Implementing Secure Cloud and Virtualization Solutions 185
Virtualization Strategies 185
Type 1 vs. Type 2 Hypervisors 186
Type 1 Hypervisor 186
Type 2 Hypervisor 187
Containers 187
Emulation 188
Application Virtualization 189
VDI 189

Provisioning and Deprovisioning 189
Middleware 190
Metadata and Tags 190
Deployment Models and Considerations 190
Business Directives 191
Cost 191
Scalability 191
Resources 191
Location 191
Data Protection 192
Cloud Deployment Models 192
Private 193
Public 193
Hybrid 193
Community 193
Hosting Models 193
Multitenant 193
Single-Tenant 194
Service Models 194
Software as a Service (SaaS) 194
Platform as a Service (PaaS) 194
Infrastructure as a Service (IaaS) 195
Cloud Provider Limitations 196
Internet Protocol (IP) Address Scheme 196
VPC Peering 196
Extending Appropriate On-premises Controls 196
Storage Models 196
Object Storage/File-Based Storage 197
Database Storage 197
Block Storage 198
Blob Storage 198
Key-Value Pairs 198

Exam Preparation Tasks 199
Review All Key Topics 199
Define Key Terms 199
Complete Tables and Lists from Memory 200
Review Questions 200

Chapter 7 Supporting Security Objectives and Requirements with Cryptography and Public Key Infrastructure (PKI) 203

Privacy and Confidentiality Requirements 203
Integrity Requirements 204
Non-repudiation 204
Compliance and Policy Requirements 204
Common Cryptography Use Cases 205
Data at Rest 205
Data in Transit 205
Data in Process/Data in Use 205
Protection of Web Services 206
Embedded Systems 206
Key Escrow/Management 207
Mobile Security 209
Elliptic Curve Cryptography 209
P256 vs. P384 vs. P512 209
Secure Authentication 209
Smart Card 209
Common PKI Use Cases 210
Web Services 210
Email 210
GNU Privacy Guard (GPG) 211
Code Signing 211
Federation 211
Trust Models 212
VPN 212
SSL/TLS 212
Other Tunneling Protocols 213
Enterprise and Security Automation/Orchestration 213

Exam Preparation Tasks 214
Review All Key Topics 214
Define Key Terms 214
Complete Tables and Lists from Memory 214
Review Questions 215

Chapter 8 Managing the Impact of Emerging Technologies on Enterprise Security and Privacy 219

Artificial Intelligence 219
Machine Learning 220
Quantum Computing 220
Blockchain 220
Homomorphic Encryption **221**
Secure Multiparty Computation 221
- Private Information Retrieval 221
- Secure Function Evaluation 221
- Private Function Evaluation 221

Distributed Consensus 221
Big Data 222
Virtual/Augmented Reality 223
3-D Printing 224
Passwordless Authentication 224
Nano Technology 225
Deep Learning 225
- Natural Language Processing 225
- Deep Fakes 226

Biometric Impersonation 226
Exam Preparation Tasks 227
Review All Key Topics 227
Define Key Terms 227
Complete Tables and Lists from Memory 227
Review Questions 228

Part II: Security Operations

Chapter 9 Performing Threat Management Activities 231

Intelligence Types 231

Tactical 231

Commodity Malware 231

Strategic 232

Targeted Attacks 232

Operational 232

Threat Hunting 232

Threat Emulation 233

Actor Types 233

Advanced Persistent Threat (APT)/Nation-State 233

Insider Threat 234

Competitor 234

Hacktivist 234

Script Kiddie 235

Organized Crime 235

Threat Actor Properties 235

Resource 235

Time 235

Money 235

Supply Chain Access 235

Create Vulnerabilities 236

Capabilities/Sophistication 236

Identifying Techniques 237

Intelligence Collection Methods 237

Intelligence Feeds 237

Deep Web 237

Proprietary 238

Open-Source Intelligence (OSINT) 238

Social Media 238

Intelligence Collection Methods 239

Routing Tables 239

DNS Records 239

Search Engines 242

Human Intelligence (HUMINT) 243

Frameworks 243

MITRE Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK) 243

ATT&CK for Industrial Control System (ICS) 245

Diamond Model of Intrusion Analysis 245

Cyber Kill Chain 246

Exam Preparation Tasks 246

Review All Key Topics 246

Define Key Terms 247

Complete Tables and Lists from Memory 247

Review Questions 248

Chapter 10 Analyzing Indicators of Compromise and Formulating an Appropriate Response 251

Indicators of Compromise 251

Packet Capture (PCAP) 251

Protocol Analyzers 252

tshark 252

Logs 252

Network Logs 253

Vulnerability Logs 254

Operating System Logs 254

Access Logs 255

NetFlow Logs 256

Notifications 256

FIM Alerts 257

SIEM Alerts 257

DLP Alerts 257

IDS/IPS Alerts 258

Antivirus Alerts 259

Notification Severity/Priorities 260

Syslog 261

Unusual Process Activity 263

Response 265
Firewall Rules 265
IPS/IDS Rules 267
ACL Rules 267
Signature Rules 267
Behavior Rules 268
DLP Rules 268
Scripts/Regular Expressions 268
Exam Preparation Tasks 268
Review All Key Topics 269
Define Key Terms 269
Complete Tables and Lists from Memory 270
Review Questions 270
Chapter 11 Performing Vulnerability Management Activities 275
Vulnerability Scans 275
Credentialed vs. Non-credentialed 275
Agent-Based/Server-Based 276
Criticality Ranking 277
Active vs. Passive 278
Security Content Automation Protocol (SCAP) 278
Extensible Configuration Checklist Description Format (XCCDF) 278
Open Vulnerability and Assessment Language (OVAL) 279
Common Platform Enumeration (CPE) 279
Common Vulnerabilities and Exposures (CVE) 279
Common Vulnerability Scoring System (CVSS) 279
Common Configuration Enumeration (CCE) 282
Asset Reporting Format (ARF) 282
Self-assessment vs. Third-Party Vendor Assessment 283
Patch Management 283
Manual Patch Management 284
Automated Patch Management 284
Information Sources 284
Advisories 285

Bulletins 286
Vendor Websites 287
Information Sharing and Analysis Centers (ISACs) 287
News Reports 287
Exam Preparation Tasks 287
Review All Key Topics 287
Define Key Terms 288
Complete Tables and Lists from Memory 288
Review Questions 288

Chapter 12 Using the Appropriate Vulnerability Assessment and Penetration Testing Methods and Tools 293

Methods 293
Static Analysis/Dynamic Analysis 293
Side-Channel Analysis 293
Reverse Engineering 294
Software 294
Hardware 294
Wireless Vulnerability Scan 295
Rogue Access Points 295
Software Composition Analysis 296
Fuzz Testing 296
Pivoting 297
Post-exploitation 297
Persistence 298
Tools 298
SCAP Scanner 298
Network Traffic Analyzer 299
Vulnerability Scanner 300
Protocol Analyzer 302
Port Scanner 302
HTTP Interceptor 304
Exploit Framework 304
Password Cracker 306
Dependency Management 307
Requirements 308

Scope of Work 308
Rules of Engagement 308
Invasive vs. Non-invasive 308
Asset Inventory 308
Permissions and Access 309
Corporate Policy Considerations 310
Facility Considerations 310
Physical Security Considerations 310
Rescan for Corrections/Changes 310
Exam Preparation Tasks 310
Review All Key Topics 310
Define Key Terms 311
Complete Tables and Lists from Memory 312
Review Questions 312
Chapter 13 Analyzing Vulnerabilities and Recommending Risk Mitigations 315
Vulnerabilities 315
Race Conditions 315
Overflows 315
Buffer 316
Integer 318
Broken Authentication 318
Unsecure References 319
Poor Exception Handling 319
Security Misconfiguration 319
Improper Headers 320
Information Disclosure 321
Certificate Errors 321
Weak Cryptography Implementations 321
Weak Ciphers 322
Weak Cipher Suite Implementations 322
Software Composition Analysis 322
Use of Vulnerable Frameworks and Software Modules 323
Use of Unsafe Functions 323
Third-Party Libraries 323

Dependencies 324
Code Injections/Malicious Changes 324
End of Support/End of Life 324
Regression Issues 324
Inherently Vulnerable System/Application 325
Client-Side Processing vs. Server-Side Processing 325
JSON/Representational State Transfer (REST) 326
Browser Extensions 326
Flash 327
ActiveX 327
Hypertext Markup Language 5 (HTML5) 327
Asynchronous JavaScript and XML (AJAX) 327
Simple Object Access Protocol (SOAP) 329
Machine Code vs. Bytecode or Interpreted vs. Emulated 329
Attacks 329
Directory Traversal 330
Cross-site Scripting (XSS) 331
Cross-site Request Forgery (CSRF) 331
Injection 332
XML 332
LDAP 335
Structured Query Language (SQL) 335
Command 337
Process 337
Sandbox Escape 337
Virtual Machine (VM) Hopping 337
VM Escape 337
Border Gateway Protocol (BGP) Route Hijacking 338
Interception Attacks 339
Denial-of-Service (DoS)/DDoS 339
SYN Flood 339
Teardrop Attack 340
Authentication Bypass 340

Social Engineering 340
Phishing/Pharming 340
Shoulder Surfing 341
Identity Theft 341
Dumpster Diving 341
VLAN Hopping 341
Exam Preparation Tasks 341
Review All Key Topics 341
Define Key Terms 342
Complete Tables and Lists from Memory 343
Review Questions 343
Chapter 14 Using Processes to Reduce Risk 347
Proactive and Detection 347
Hunts 347
Developing Countermeasures 347
Deceptive Technologies 347
Honeynet/Honeypot 348
Decoy Files 348
Simulators 348
Dynamic Network Configurations 348
Security Data Analytics 348
Processing Pipelines 349
Data 349
Stream 349
Indexing and Search 350
Log Collection and Curation 350
Database Activity Monitoring 350
Preventive 351
Antivirus 352
Immutable Systems 352
Hardening 352
Sandbox Detonation 352
Application Control 353
License Technologies 353
Allow List vs. Block List 354

Time of Check vs. Time of Use 354
Atomic Execution 355
Security Automation 355
Cron/Scheduled Tasks 355
Bash 356
PowerShell 357
Python 357
Physical Security 358
Review of Lighting 358
Types of Lighting Systems 358
Types of Lighting 359
Review of Visitor Logs 359
Camera Reviews 359
Open Spaces vs. Confined Spaces 361
Natural Access Control 361
Natural Surveillance 361
Natural Territorial Reinforcement 361
Exam Preparation Tasks 362
Review All Key Topics 362
Define Key Terms 362
Complete Tables and Lists from Memory 363
Review Questions 363
Chapter 15 Implementing the Appropriate Incident Response 367
Event Classifications 367
False Positive 367
False Negative 367
True Positive 367
True Negative 367
Triage Event 367
Preescalation Tasks 368
Incident Response Process 368
Preparation 369
Training 369
Testing 370

Detection 370
Analysis 371
Containment 371
Minimize 371
Isolate 371
Recovery 371
Response 372
Lessons Learned 372
Specific Response Playbooks/Processes 373
Scenarios 373
Ransomware 373
Data Exfiltration 373
Social Engineering 374
Non-automated Response Methods 374
Automated Response Methods 374
Runbooks 374
SOAR 375
Communication Plan 375
Stakeholder Management 377
Legal 377
Human Resources 377
Public Relations 378
Internal and External 378
Law Enforcement 378
Senior Leadership 379
Regulatory Bodies 379
Exam Preparation Tasks 379
Review All Key Topics 379
Define Key Terms 380
Review Questions 380
Chapter 16 Forensic Concepts 385
Legal vs. Internal Corporate Purposes 385
Forensic Process 385
Identification 385
Evidence Collection 385

Chain of Custody 385
Order of Volatility 386
Memory Snapshots 387
Images 388
Cloning 388
Evidence Preservation 388
Secure Storage 389
Backups 389
Analysis 389
Media Analysis 389
Software Analysis 390
Network Analysis 390
Hardware/Embedded Device Analysis 391
Forensics Tools 391
Verification 391
Presentation 391
Integrity Preservation 392
Hashing 392
Cryptanalysis 394
Steganalysis 394
Exam Preparation Tasks 394
Review All Key Topics 394
Define Key Terms 395
Complete Tables and Lists from Memory 395
Review Questions 395
Chapter 17 Forensic Analysis Tools 399
File Carving Tools 399
Foremost 399
Strings 400
Binary Analysis Tools 401
Hex Dump 401
Binwalk 401
Ghidra 401
GNU Project Debugger (GDB) 401

OllyDbg 402
readelf 402
objdump 402
strace 402
ldd 402
file 403
Analysis Tools 403
ExifTool 403
Nmap 403
Aircrack-ng 403
Volatility 404
The Sleuth Kit 405
Dynamically vs. Statically Linked 405
Imaging Tools 405
Forensic Toolkit (FTK) Imager 405
dd 406
Hashing Utilities 407
sha256sum 407
ssdeep 407
Live Collection vs. Post-mortem Tools 407
netstat 407
ps 409
vmstat 409
ldd 410
lsof 410
netcat 410
tcpdump 411
conntrack 411
Wireshark 412
Exam Preparation Tasks 413
Review All Key Topics 413
Define Key Terms 414
Complete Tables and Lists from Memory 414
Review Questions 414

Part III: Security Engineering and Cryptography

Chapter 18 Applying Secure Configurations to Enterprise Mobility 419

Managed Configurations 419

Application Control 419

Password 419

MFA Requirements 420

Facial 421

Fingerprint 421

Iris Scan 421

Token-Based Access 421

Patch Repository 422

Firmware Over-the-Air 422

Remote Wipe 422

Wi-Fi 423

Wi-Fi Protected Access (WPA2/3) 423

Device Certificates 423

Profiles 424

Bluetooth 424

Near-Field Communication (NFC) 424

Peripherals 425

Geofencing 425

VPN Settings 425

Geotagging 426

Certificate Management 426

Full Device Encryption 427

Tethering 427

Airplane Mode 427

Location Services 427

DNS over HTTPS (DoH) 428

Custom DNS 428

Deployment Scenarios 429

Bring Your Own Device (BYOD) 429

Corporate-Owned 429

Corporate-Owned, Personally Enabled (COPE) 429

Choose Your Own Device (CYOD) 429

Implications of Wearable Devices 429
Unauthorized Remote Activation/Deactivation of Devices or Features 430
Encrypted and Unencrypted Communication Concerns 430
Physical Reconnaissance 430
Personal Data Theft 430
Health Privacy 430
Digital Forensics on Collected Data 430
Unauthorized Application Stores 431
Jailbreaking/Rooting 431
Side Loading 431
Containerization 432
Original Equipment Manufacturer (OEM) and Carrier Differences 432
Supply Chain Issues 432
eFuse 432
Exam Preparation Tasks 433
Review All Key Topics 433
Define Key Terms 433
Complete Tables and Lists from Memory 433
Review Questions 433
Chapter 19 Configuring and Implementing Endpoint Security Controls 437
Hardening Techniques 437
Removing Unneeded Services 437
Disabling Unused Accounts 438
Images/Templates 438
Removing End-of-Life Devices 438
Removing End-of-Support Device 438
Local Drive Encryption 439
Enabling No-Execute (NX)/Execute Never (XN) Bit 439
Disabling Central Processing Unit (CPU) Virtualization Support 439
Secure Encrypted Enclaves 440
Memory Encryption 440
Shell Restrictions 441
Address Space Layout Randomization (ASLR) 442
Processes 442
Patching 442

Firmware 442

Application 443

Logging 443

Monitoring 443

Mandatory Access Control 444

Security-Enhanced Linux (SELinux)/Security-Enhanced Android (SEAndroid) 444

SELinux 444

SEAndroid 444

Kernel vs. Middleware 445

Trustworthy Computing 445

Trusted Platform Module (TPM) 445

Secure Boot 446

Unified Extensible Firmware Interface (UEFI)/Basic Input/Output System (BIOS) Protection 447

Attestation Services 448

Hardware Security Module (HSM) 448

Measured Boot 449

Self-Encrypting Drives (SEDs) 450

Compensating Controls 450

Antivirus 450

Application Controls 451

Host-Based Intrusion Detection System (HIDS)/Host-Based Intrusion Prevention System (HIPS) 451

Host-Based Firewall 451

Endpoint Detection and Response (EDR) 451

Redundant Hardware 452

Self-Healing Hardware 452

User and Entity Behavior Analytics (UEBA) 452

Exam Preparation Tasks 452

Review All Key Topics 452

Define Key Terms 453

Complete Tables and Lists from Memory 454

Review Questions 454

Chapter 20 Security Considerations Impacting Specific Sectors and Operational Technologies 459

Embedded 459

Internet of Things (IoT) 459

IoT Examples 460

Methods of Securing IoT Devices 461

System on a Chip (SoC) 461

Application-Specific Integrated Circuit (ASIC) and Field-Programmable Gate Array (FPGA) 461

ICS/Supervisory Control and Data Acquisition (SCADA) 462

Programmable Logic Controller (PLC) 463

Historian 463

Ladder Logic 463

Safety Instrumented System 464

Heating, Ventilation, and Air Conditioning (HVAC) 464

Protocols 465

Controller Area Network (CAN) Bus 465

Modbus 466

Distributed Network Protocol 3 (DNP3) 466

Zigbee 467

Common Industrial Protocol (CIP) 467

Data Distribution Service 468

Sectors 468

Energy 469

Manufacturing 469

Healthcare 470

Public Utilities 470

Public Services 470

Facility Services 471

Exam Preparation Tasks 472

Review All Key Topics 472

Define Key Terms 472

Complete Tables and Lists from Memory 473

Review Questions 473

Chapter 21 Cloud Technology's Impact on Organizational Security 477

Automation and Orchestration 477
Encryption Configuration 477
Logs 478
Availability 479
Collection 479
Monitoring 479
Configuration 480
Alerting 480
Monitoring Configurations 480
Key Ownership and Location 481
Key Life-Cycle Management 483
Backup and Recovery Methods 485
Cloud as Business Continuity and Disaster Recovery (BCDR) 486
Primary Provider BCDR 486
Alternative Provider BCDR 486
Infrastructure vs. Serverless Computing 486
Application Virtualization 487
Software-Defined Networking 488
Misconfigurations 488
Collaboration Tools 488
Web Conferencing 488
Video Conferencing 489
Audio Conferencing 491
Storage and Document Collaboration Tools 491
Storage Configurations 492
Bit Splitting 493
Data Dispersion 493
Cloud Access Security Broker (CASB) 493
Exam Preparation Tasks 494
Review All Key Topics 494
Define Key Terms 495
Review Questions 495

Chapter 22 Implementing the Appropriate PKI Solution 499

PKI Hierarchy 499

Registration Authority (RA) 499

Certificate Authority (CA) 499

Subordinate/Intermediate CA 500

Certificate Types 501

Wildcard Certificate 501

Extended Validation 502

Multidomain 502

General Purpose 503

Certificate Usages/Profiles/Templates 504

Client Authentication 504

Server Authentication 504

Digital Signatures 504

Code Signing 505

Extensions 505

Common Name (CN) 505

Subject Alternate Name (SAN) 505

Trusted Providers 505

Trust Model 506

Cross-certification 506

Configure Profiles 507

Life-Cycle Management 507

Public and Private Keys 508

Digital Signature 512

Certificate Pinning 512

Certificate Stapling 512

Certificate Signing Requests (CSRs) 513

Online Certificate Status Protocol (OCSP) vs. Certificate Revocation List (CRL) 513

HTTP Strict Transport Security (HSTS) 514

Exam Preparation Tasks 514

Review All Key Topics 514

Define Key Terms 515

Review Questions 515

Chapter 23 Implementing the Appropriate Cryptographic Protocols and Algorithms 519

Hashing 519

Secure Hashing Algorithm (SHA) 519

Hash-Based Message Authentication Code (HMAC) 520

Message Digest (MD) 521

RACE Integrity Primitives Evaluation Message Digest (RIPEMD) 521

Poly1305 521

Symmetric Algorithms 522

Modes of Operation 523

Electronic Codebook (ECB) 523

Cipher Block Chaining (CBC) 524

Output Feedback (OFB) 524

Counter (CTR) 525

Galois/Counter Mode (GCM) 525

Stream and Block 526

Advanced Encryption Standard (AES) 527

Triple Digital Encryption Standard (3DES) 528

ChaCha/Salsa20 528

Asymmetric Algorithms 528

Key Agreement 529

Diffie-Hellman 529

Elliptic-Curve Diffie-Hellman (ECDH) 530

Signing 530

Digital Signature Algorithm (DSA) 530

Rivest, Shamir, and Adleman (RSA) 530

Elliptic-Curve Digital Signature Algorithm (ECDSA) 531

Known Flaws/Weaknesses 531

Protocols 532

Secure Sockets Layer (SSL)/Transport Layer Security (TLS) 532

Secure/Multipurpose Internet Mail Extensions (S/MIME) 533

Internet Protocol Security (IPsec) 534

Secure Shell (SSH) 534

EAP 535

Elliptic-Curve Cryptography 535
P256/P384 535
Forward Secrecy 536
Authenticated Encryption with Associated Data 536
Key Stretching 536
Password-Based Key Derivation Function 2 (PBKDF2) 537
Bcrypt 537
Exam Preparation Tasks 537
Review All Key Topics 537
Define Key Terms 538
Complete Tables and Lists from Memory 538
Implementation and Configuration Issues 542
Validity Dates 542
Chapter 24 Troubleshooting Issues with Cryptographic Implementations 543
Wrong Certificate Type 543
Revoked Certificates 543
Incorrect Name 543
Chain Issues 544
Invalid Root or Intermediate CAs 544
Self-signed 544
Weak Signing Algorithm 545
Weak Cipher Suite 545
Incorrect Permissions 546
Cipher Mismatches 546
Downgrade 546
Keys 546
Mismatched 547
Improper Key Handling 547
Embedded Keys 548
Rekeying 548
Exposed Private Keys 548
Crypto Shredding 548
Cryptographic Obfuscation 548

Key Rotation 549
Compromised Keys 549
Exam Preparation Tasks 549
Review All Key Topics 549
Define Key Terms 550
Complete Tables and Lists from Memory 550
Review Questions 550

Part IV: Governance, Risk, and Compliance

Chapter 25 Applying Appropriate Risk Strategies 555

Risk Assessment 555
Likelihood 556
Impact 556
Qualitative vs. Quantitative 557
Qualitative Risk Analysis 557
Quantitative Risk Analysis 558
Exposure Factor 558
Asset Value 558
Total Cost of Ownership (TCO) 559
Return on Investment (ROI) 560
Payback 561
Net Present Value (NPV) 562
Mean Time to Recovery (MTTR) 562
Mean Time Between Failure (MTBF) 562
Annualized Loss Expectancy (ALE)/Annualized Rate of Occurrence (ARO)/Single Loss Expectancy (SLE) 562
ALE 563
ARO 563
SLE 563
Gap Analysis 564
Risk Handling Techniques 565
Transfer 565
Accept 565
Avoid 566
Mitigate 566

Risk Types 566
Inherent 567
Residual 567
Exceptions 567
Risk Management Life Cycle 568
Identify 569
Assess 570
Control 570
People 572
Process 572
Technology 572
Control Types 572
Protect 572
Detect 572
Respond 572
Restore 573
Review 573
Frameworks 573
NIST 574
Open Source Security Testing Methodology Manual (OSSTMM) 588
COSO's Enterprise Risk Management (ERM) Integrated Framework 588
Risk Management Standard by the Federation of European Risk Management Associations (FERMA) 589
Risk Tracking 590
Risk Register 590
Key Performance Indicators/Key Risk Indicators 591
KPIs 592
KRIs 594
Risk Appetite vs. Risk Tolerance 594
Tradeoff Analysis 595
Usability vs. Security Requirements 595
Policies and Security Practices 595
Separation of Duties 595
Job Rotation 596

Mandatory Vacation 596
Least Privilege 597
Employment and Termination Procedures 598
Training and Awareness for Users 599
Auditing Requirements and Frequency 601
Exam Preparation Tasks 601
Review All Key Topics 601
Define Key Terms 603
Complete Tables and Lists from Memory 603
Review Questions 603

Chapter 26 Managing and Mitigating Vendor Risk 607

Shared Responsibility Model (Roles/Responsibilities) 607
Cloud Service Provider (CSP) 607
Geographic Location 608
Infrastructure 608
Compute/Storage/Networking 608
Services 608
Client 609
Encryption 609
Operating Systems 609
Applications 609
Data 609
Vendor Lock-in and Vendor Lock-out 610
Vendor Viability 610
Financial Risk 610
Merger or Acquisition Risk 610
Meeting Client Requirements 610
Legal 610
Change Management 611
Staff Turnover 612
Device and Technical Configurations 612
ACLs 612
Creating Rule Sets 613

Change Monitoring 614
Configuration Lockdown 614
Support Availability 615
Geographical Consideration 615
Supply Chain Visibility 615
Incident Reporting Requirements 616
Source Code Escrows 616
Ongoing Vendor Assessment Tools 616
Third-Party Dependencies 616
Code 617
Hardware 617
Modules 618
Technical Considerations 618
Technical Testing 618
Network Segmentation 618
Transmission Control 618
Shared Credentials 619
Exam Preparation Tasks 620
Review All Key Topics 620
Define Key Terms 620
Complete Tables and Lists from Memory 621
Review Questions 621

Chapter 27 The Organizational Impact of Compliance Frameworks and Legal Considerations 625

Security Concerns of Integrating Diverse Industries 625
Rules 625
Policies 626
Regulations 626
Data Considerations 626
Data Sovereignty 626
Data Ownership 627
Data Classifications 627
Commercial Business Classifications 628
Military and Government Classifications 628

Data Retention 629
Data Types 629
Health/Financial 630
Intellectual Property 630
Personally Identifiable Information (PII) 633
Data Removal, Destruction, and Sanitization 634
Geographic Considerations 635
Location of Data 636
Location of Data Subject 636
Location of Cloud Provider 637
Third-Party Attestation of Compliance 637
Regulations, Accreditations, and Standards 637
Open Standards 638
Adherence to Standards 638
Competing Standards 639
Lack of Standards 639
De Facto Standards 639
Payment Card Industry Data Security Standard (PCI DSS) 639
General Data Protection Regulation (GDPR) 640
International Organization for Standardization (ISO) 641
Capability Maturity Model Integration (CMMI) 643
National Institute of Standards and Technology (NIST) 644
Children's Online Privacy Protection Act (COPPA) 644
Common Criteria 644
Cloud Security Alliance (CSA) Security Trust Assurance and Risk (STAR) 646
Legal Considerations 646
Due Diligence/Due Care 646
Export Controls 647
Legal Holds 648
E-Discovery 648
Contract and Agreement Types 648
Service-Level Agreement (SLA) 649
Master Service Agreement (MSA) 649

Non-disclosure Agreement (NDA) 650
Memorandum of Understanding (MOU) 650
Interconnection Security Agreement (ISA) 650
Operational-Level Agreement 651
Privacy-Level Agreement 651
Exam Preparation Tasks 651
Review All Key Topics 651
Define Key Terms 652
Complete Tables and Lists from Memory 653
Business Impact Analysis 656
Chapter 28 Business Continuity and Disaster Recovery Concepts 657
Develop Contingency Planning Policy 658
Conduct the BIA 658
Identify Critical Processes and Resources 659
Recovery Time Objective 659
Recovery Point Objective 659
Recovery Service Level 659
Mission Essential Functions 659
Privacy Impact Assessment 660
Disaster Recovery Plan (DRP)/Business Continuity Plan (BCP) 660
Personnel Components 661
Project Scope 661
Business Continuity Steps 662
Recovery and Multiple Site Strategies 662
Cold Site 663
Warm Site 663
Hot Site 663
Mobile Site 664
Incident Response Plan 664
Roles/Responsibilities 665
After-Action Reports 666
Testing Plans 666

Checklist 666
Walk-through 666
Tabletop Exercises 666
Full Interruption Test 667
Parallel Test/Simulation Test 667
Exam Preparation Tasks 667
Review All Key Topics 667
Define Key Terms 668
Complete Tables and Lists from Memory 668
Tools for Final Preparation 672
Pearson Test Prep Practice Test Software and Questions on the Website 672

Chapter 29 Final Preparation 673

Accessing the Pearson Test Prep Software Online 673
Accessing the Pearson Test Prep Practice Test Software Offline 673
Customizing Your Exams 674
Updating Your Exams 675
Premium Edition 676
Chapter-Ending Review Tools 676
Suggested Plan for Final Review/Study 676
Summary 677

Appendix A Answers to the Review Questions 679

Glossary 709

Index 761

Online Elements

Appendix B Memory Tables
Appendix C Memory Tables Answer Key
Appendix D Study Planner
Glossary

About the Author

Troy McMillan, CASP, is a product developer and technical editor for CyberVista as well as a full-time trainer. He became a professional trainer more than 20 years ago, teaching Cisco, Microsoft, CompTIA, and wireless classes. His recent work includes

- Author of *CompTIA CySA+ CS0-002 Cert Guide* (Pearson IT Certification)
- Author of *CompTIA A+ Complete Review Guide* (Sybex)
- Author of *CompTIA Server + Study Guide* (Sybex)
- Contributing subject matter expert for *CCNA Cisco Certified Network Associate Certification Exam Preparation Guide* (Kaplan)
- Prep test question writer for *Network+ Study Guide* (Sybex)
- Technical editor for *Windows 7 Study Guide* (Sybex)
- Contributing author for *CCNA-Wireless Study Guide* (Sybex)
- Technical editor for *CCNA Study Guide*, *Revision 7* (Sybex)
- Author of *VCP VMware Certified Professional on vSphere 4 Review Guide: Exam VCP-410* and associated instructional materials (Sybex)
- Author of *Cisco Essentials* (Sybex)
- Co-author of *CISSP Cert Guide* (Pearson IT Certification)
- Prep test question writer for *CCNA Wireless 640-722* (Cisco Press)

He also has appeared in the following training videos for OnCourse Learning: Security+; Network+; Microsoft 70-410, 411, and 412 exam prep; ICND 1; ICND 2; and Cloud+.

He now creates certification practice tests and study guides and online courses for Cybervista. Troy lives in Asheville, North Carolina, with his wife, Heike.

Dedication

I dedicate this book to my wife. I love you, honey!

—Troy

Acknowledgments

I'd like to thank Robin Abernathy, my coauthor on the previous edition of the book. I must also thank my coworkers at CyberVista, who have helped me to grow over the past 15 years. Thank you, Ann, George, John, Josh, and Shahara. I also must as always thank my beautiful wife, who has supported me through the lean years and continues to do so. Finally, I have to acknowledge all the help and guidance from the Pearson team.

—Troy McMillan

About the Technical Reviewer

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

We Want to Hear from You!

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

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

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

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

Email: community@informit.com

Introduction

The CompTIA Advanced Security Practitioner (CASP+) certification is a popular certification for those in the security field. Although many vendor-specific networking certifications are popular in the industry, the CompTIA CASP+ certification is unique in that it is vendor neutral. The CompTIA CASP+ certification often acts as a stepping-stone to more specialized and vendor-specific certifications, such as those offered by ISC^2.

In the CompTIA CASP+ exam, the topics are structured so that they can apply to many security devices and technologies, regardless of vendor. Although the CompTIA CASP+ is vendor neutral, devices and technologies are implemented by multiple independent vendors. In that light, several of the examples associated with this book use particular vendors' configurations and technologies. More detailed training regarding a specific vendor's software and hardware can be found in books and training specific to that vendor.

Goals and Methods

The goal of this book is to assist you in learning and understanding the technologies covered in the CASP+ CAS-004 blueprint from CompTIA and help prepare you to pass the CAS-004 version of the CompTIA CASP+ exam.

To aid you in mastering and understanding the CASP + certification objectives, this book provides the following tools:

- **Opening topics list:** This list defines the topics that are covered in the chapter.
- **Key Topics icons:** These icons indicate important figures, tables, and lists of information that you need to know for the exam. They are sprinkled throughout each chapter and are summarized in table format at the end of each chapter.
- **Memory tables:** These can be found on the companion website and in Appendix B, "Memory Tables," and Appendix C, "Memory Tables Answer Key." Use them to help memorize important information.
- **Key terms:** Key terms without definitions are listed at the end of each chapter. Write down the definition of each term and check your work against the Glossary.

For current information about the CompTIA CASP+ certification exam, visit https://www.comptia.org/certifications/comptia-advanced-security-practitioner

Who Should Read This Book?

This book is for readers who want to acquire additional certifications beyond the CASP+ certification (for example, the CISSP certification and beyond). The book is designed in such a way to offer easy transition to future certification studies.

Strategies for Exam Preparation

Read the chapters in this book, jotting down notes with key concepts or configurations on a separate notepad.

Download the current list of exam objectives by submitting a form at https://www.comptia.org/training/resources/exam-objectives

Use the practice exams, available through Pearson Test Prep. As you work through the practice exams, note the areas where you lack confidence and review those concepts. After you review these areas, work through the practice exam a second time and rate your skills.

After you work through a practice exam a second time and feel confident with your skills, schedule the real CompTIA CASP+ exam (CAS-004). The following website provides information about registering for the exam: www.pearsonvue.com/comptia/.

CompTIA CASP+ Exam Topics

Table 1 lists general exam topics (*objectives*) and specific topics under each general topic (*subobjectives*) for the CompTIA CASP+ CAS-004 exam. This table lists the primary chapter in which each exam topic is covered. Note that many objectives and subobjectives are interrelated and are addressed in multiple chapters.

Table 1 CompTIA CASP+ Exam Topics

Chapter	CAS-004 Exam Objective	CAS-004 Exam Subobjective
1 Ensuring a Secure Network Architecture	1.1 Given a scenario, analyze the security requirements and objectives to ensure an appropriate, secure network architecture for a new or existing network.	■ Services ■ Segmentation ■ De-perimeterization/zero trust ■ Merging of networks from various organizations ■ Software-defined networking (SDN)

Chapter	CAS-004 Exam Objective	CAS-004 Exam Subobjective
2 Determining the Proper Infrastructure Security Design	1.2 Given a scenario, analyze the organizational requirements to determine the proper infrastructure security design.	■ Scalability ■ Resiliency ■ Automation ■ Performance ■ Containerization ■ Virtualization ■ Content delivery network ■ Caching
3 Securely Integrating Software Applications	1.3 Given a scenario, integrate software applications securely into an enterprise architecture.	■ Baseline and templates ■ Software assurance ■ Considerations of integrating enterprise applications ■ Integrating security into development life cycle
4 Securing the Enterprise Architecture by Implementing Data Security Techniques	1.4 Given a scenario, implement data security techniques for securing enterprise architecture.	■ Data loss prevention ■ Data loss detection ■ Data classification, labeling, and tagging ■ Obfuscation ■ Anonymization ■ Encrypted vs. unencrypted ■ Data life cycle ■ Data inventory and mapping ■ Data integrity management ■ Data storage, backup, and recovery
5 Providing the Appropriate Authentication and Authorization Controls	1.5 Given a scenario, analyze the security requirements and objectives to provide the appropriate authentication and authorization controls.	■ Credential management ■ Password policies ■ Federation ■ Access control ■ Protocols ■ Multifactor authentication (MFA) ■ One-time password (OTP) ■ Hardware root of trust ■ Single sign-on (SSO) ■ JavaScript Object Notation (JSON) web token (JWT) ■ Attestation and identity proofing

Chapter	CAS-004 Exam Objective	CAS-004 Exam Subobjective
6 Implementing Secure Cloud and Virtualization Solutions	1.6 Given a set of requirements, implement secure cloud and virtualization solutions.	■ Virtualization strategies ■ Provisioning and deprovisioning ■ Middleware ■ Metadata and tags ■ Deployment models and considerations ■ Hosting models ■ Service models ■ Cloud provider limitations ■ Extending appropriate on-premises controls ■ Storage models
7 Supporting Security Objectives and Requirements with Cryptography and Public Key Infrastructure (PKI)	1.7 Explain how cryptography and public key infrastructure (PKI) support security objectives and requirements.	■ Privacy and confidentiality requirements ■ Integrity requirements ■ Non-repudiation ■ Compliance and policy requirements ■ Common cryptography use cases ■ Common PKI use cases
8 Managing the Impact of Emerging Technologies on Enterprise Security and Privacy	1.8 Explain the impact of emerging technologies on enterprise security and privacy.	■ Artificial intelligence ■ Machine learning ■ Quantum computing ■ Blockchain ■ Homomorphic encryption ■ Secure multiparty computation ■ Distributed consensus ■ Big data ■ Virtual/augmented reality ■ 3-D printing ■ Passwordless authentication ■ Nano technology ■ Deep learning ■ Biometric impersonation
9 Performing Threat Management Activities	2.1 Given a scenario, perform threat management activities.	■ Intelligence types ■ Actor types ■ Threat actor properties ■ Frameworks

Chapter	CAS-004 Exam Objective	CAS-004 Exam Subobjective
10 Analyzing Indicators of Compromise and Formulating an Appropriate Response	2.2 Given a scenario, analyze indicators of compromise and formulate an appropriate response.	■ Indicators of compromise ■ Response
11 Performing Vulnerability Management Activities	2.3 Given a scenario, perform vulnerability management activities.	■ Vulnerability scans ■ Security Content Automation Protocol (SCAP) ■ Self-assessment vs. third-party vendor assessment ■ Patch management ■ Information sources
12 Using the Appropriate Vulnerability Assessment and Penetration Testing Methods and Tools	2.4 Given a scenario, use the appropriate vulnerability assessment and penetration testing methods and tools	■ Methods ■ Tools ■ Dependency management ■ Requirements
13 Analyzing Vulnerabilities and Recommending Risk Mitigations	2.5 Given a scenario, analyze vulnerabilities and recommend risk mitigations.	■ Vulnerabilities ■ Inherently vulnerable system/application ■ Attacks
14 Using Processes to Reduce Risk	2.6 Given a scenario, use processes to reduce risk.	■ Proactive and detection ■ Security data analytics ■ Preventive ■ Application control ■ Security automation ■ Physical security
15 Implementing the Appropriate Incident Response	2.7 Given an incident, implement the appropriate response.	■ Event classifications ■ Triage event ■ Preescalation tasks ■ Incident response process ■ Specific response playbooks/processes ■ Communications plan ■ Stakeholder management

Chapter	CAS-004 Exam Objective	CAS-004 Exam Subobjective
16 Forensics Concepts	2.8 Explain the importance of forensic concepts.	■ Legal vs. internal corporate purposes ■ Forensic process ■ Integrity preservation ■ Cryptanalysis ■ Steganalysis
17 Forensics Analysis Tools	2.9 Given a scenario, use forensic analysis tools.	■ File carving tools ■ Binary analysis tools ■ Analysis tools ■ Imaging tools ■ Hashing utilities ■ Live collection vs. post-mortem tools
18 Applying Secure Configurations to Enterprise Mobility	3.1 Given a scenario, apply secure configurations to enterprise mobility.	■ Managed configurations ■ Deployment scenarios ■ Security considerations
19 Configuring and Implementing Endpoint Security Controls	3.2 Given a scenario, configure and implement endpoint security controls.	■ Hardening techniques ■ Processes ■ Mandatory access control ■ Trustworthy computing ■ Compensating controls
20 Security Considerations Impacting Specific Sectors and Operational Technologies	3.3 Explain security considerations impacting specific sectors and operational technologies.	■ Embedded ■ ICS/supervisory control and data acquisition (SCADA) ■ Protocols ■ Sectors

Chapter	CAS-004 Exam Objective	CAS-004 Exam Subobjective
21 Cloud Technology's Impact on Organizational Security	3.4 Explain how cloud technology adoption impacts organizational security.	■ Automation and orchestration ■ Encryption configuration ■ Logs ■ Monitoring configurations ■ Key ownership and location ■ Key life-cycle management ■ Backup and recovery methods ■ Infrastructure vs. serverless computing ■ Application virtualization ■ Software-defined networking ■ Misconfigurations ■ Collaboration tools ■ Storage configurations ■ Cloud access security broker (CASB)
22 Implementing the Appropriate PKI Solution	3.5 Given a business requirement, implement the appropriate PKI solution.	■ PKI hierarchy ■ Certificate types ■ Certificate sages/profiles/templates ■ Extensions ■ Trusted providers ■ Trust model ■ Cross-certification ■ Configure profiles ■ Life-cycle management ■ Public and private keys ■ Digital signature ■ Certificate pinning ■ Certificate stapling ■ Certificate signing requests (CSRs) ■ Online Certificate Status Protocol (OCSP) vs. certificate revocation list (CRL) ■ HTTP Strict Transport Security (HSTS)

Chapter	CAS-004 Exam Objective	CAS-004 Exam Subobjective
23 Implementing the Appropriate Cryptographic Protocols and Algorithms	3.6 Given a business requirement, implement the appropriate cryptographic protocols and algorithms	■ Hashing ■ Symmetric algorithms ■ Asymmetric algorithms ■ Protocols ■ Elliptic-curve cryptography ■ Forward secrecy ■ Authenticated encryption with associated data ■ Key stretching
24 Troubleshooting Issues with Cryptographic Implementations	3.7 Given a scenario, troubleshoot issues with cryptographic implementations.	■ Implementation and configuration issues ■ Keys
25 Applying Appropriate Risk Strategies	4.1 Given a set of requirements, apply the appropriate risk strategies.	■ Risk assessment ■ Risk handling techniques ■ Risk types ■ Risk management life cycle ■ Risk tracking ■ Risk appetite vs. risk tolerance ■ Policies and security practices
26 Managing and Mitigating Vendor Risk	4.2 Explain the importance of managing and mitigating vendor risk.	■ Shared responsibility model (roles/responsibilities) ■ Vendor lock-in and vendor lockout ■ Vendor viability ■ Meeting client requirements ■ Support availability ■ Geographical considerations ■ Supply chain visibility ■ Incident reporting requirements ■ Source code escrows ■ Ongoing vendor assessment tools ■ Third-party dependencies ■ Technical considerations

Chapter	CAS-004 Exam Objective	CAS-004 Exam Subobjective
27 The Organizational Impact of Compliance Frameworks and Legal Considerations	4.3 Explain compliance frameworks and legal considerations, and their organizational impact	■ Security concerns of integrating diverse industries ■ Data considerations ■ Geographic considerations ■ Third-party attestation of compliance ■ Regulations, accreditations, and standards ■ Legal considerations ■ Contract and agreement types
28 Business Continuity and Disaster Recovery Concepts	4.4 Explain the importance of business continuity and disaster recovery concepts.	■ Business impact analysis ■ Privacy impact assessment ■ Disaster recovery plan (DRP)/business continuity plan (BCP) ■ Incident response plan ■ Testing plans

How This Book Is Organized

Although this book could be read cover-to-cover, it is designed to be flexible and allow you to easily move between chapters and sections of chapters to cover just the material that you need more work with. However, if you do intend to read all the chapters, the order in the book is an excellent sequence to use.

In addition to the 28 main chapters, this book includes tools to help you verify that you are prepared to take the exam. The companion website also includes flash cards and memory tables that you can work through to verify your knowledge of the subject matter.

Companion Website

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

To access this companion website, follow these steps:

1. Go to www.pearsonITcertification.com/register and log in or create a new account.
2. Enter the ISBN: **9780137348954**.
3. Answer the challenge question as proof of purchase.
4. Click the **Access Bonus Content** link in the Registered Products section of your account page, to be taken to the page where your downloadable content is available.

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

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

Pearson Test Prep Practice Test Software

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

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

Accessing the Pearson Test Prep Software Online

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

1. Go to http://www.PearsonTestPrep.com.
2. Select **Pearson IT Certification** as your product group.

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

Accessing the Pearson Test Prep Software Offline

If you wish to study offline, you can download and install the Windows version of the Pearson Test Prep software. There is a download link for this software on the book's companion website, or you can just enter this link in your browser: http://www.pearsonitcertification.com/content/downloads/pcpt/engine.zip.

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

1. Register your book by going to PearsonITCertification.com/register and entering the ISBN: **9780137348954**.
2. Respond to the challenge questions.
3. Go to your account page and select the **Registered Products** tab.
4. Click the **Access Bonus Content** link under the product listing.
5. Click the **Install Pearson Test Prep Desktop Version** link under the Practice Exams section of the page to download the software.
6. When the software finishes downloading, unzip all the files on your computer.
7. Double-click the application file to start the installation and follow the onscreen instructions to complete the registration.
8. When the installation is complete, launch the application and click **Activate Exam** button on the My Products tab.
9. Click the **Activate a Product** button in the Activate Product Wizard.
10. Enter the unique access code found on the card in the sleeve in the back of your book and click the **Activate** button.

11. Click **Next** and then the **Finish** button to download the exam data to your application.
12. You can now start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

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

Customizing Your Exams

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

- Study Mode
- Practice Exam Mode
- Flash Card Mode

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

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

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

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

Updating Your Exams

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

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

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

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

Premium Edition eBook and Practice Tests

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

Credits

Chapter Opener: Charlie Edwards/Getty Images

Figures 1-1–1-8, 1-11, 1-18–1-20, 2-4, 4-2, 4-3, 5-3(a)–5-5, 6-3, 12-3, 12-4, 13-2, 13-3, 13-8, 13-9, 13-11, 13-14, 14-2, 14-4(a), 14-7, 20-2: Cisco Systems, Inc

Figure 1-15: Micro Focus

Figure 3-4: Apple Inc

Figure 3-8: Mozilla Foundation

Figures 3-9, 4-1, 5-2, 9-1, 9-2, 10-1, 10-2, 10-4, 10-5, 10-9–10-11, 14-4(b), 14-5, 15-1, 17-5, 17-6, 19-1, 24-1–24-3: Microsoft

Figure 5-3(b): MyFreeTemplates.com

Figure 8-3: luchschen/123RF

Figure 10-3: Wazuh Inc

Figure 10-6: Comodo Group, Inc

Figure 10-7, 11-1–11-3: Tenable, Inc

Figure 10-8: SolarWinds Worldwide, LLC

Figure 11-6: National Security Agency

Figure 11-7: Philippine National Police

Figures 12-2, 12-7: Progress Software Corporation

Figures 12-5, 12-6: Nmap.Org

Figure 12-8: Rapid7

Figure 12-9: Massimiliano Montoro

Figure 13-4: Adaptive path

Figures 17-1, 17-2: Canonical Ltd

Figure 17-3: Aircrack-ng

Figure 17-4: The Open Group

Figure 17-7: Linus Torvalds

Figures 17-8, 17-9: The Wireshark Foundation

Figure 19-5: Puget Systems

Figures 25-1, 25-2: National Institute of Standards and Technology

Figure 25-8: ISO

Figure 25-9: COSO

Figure 25-10: Federation of European risk management associations

Securing the Enterprise Architecture by Implementing Data Security Techniques

Securing the enterprise architecture entails the use of many techniques and processes. In this chapter you'll learn about data security techniques and how they can be used to support securing of the overall architecture.

Data Loss Prevention

As you learned in Chapter 1, preventing the loss of critical and sensitive data requires the use of both policies and procedures that reflect best practices and software tools such as data loss prevention (DLP) software to prevent malicious as well as inadvertent data leaks. In this opening section of the chapter you'll learn about other techniques to prevent data loss.

Blocking Use of External Media

One of the many ways malware and other problems can be introduced to a network (right around all your fancy firewalls and security devices) is through the peripheral devices that users bring in and connect to their computers. Moreover, sensitive data can also leave your network this way. To address this, you should implement controls over the types of peripherals users can bring and connect (if any). The following sections look at the biggest culprits.

The use of any types of USB devices (thumb drives, external hard drives, network interfaces, and so on) should be strictly controlled—and in some cases prohibited altogether. Granular control of this issue is possible thanks to Windows Group Policy.

Some organizations choose to allow certain types of USB storage devices but require that the devices be encrypted before they can be used. It is also possible to allow some but not all users to use these devices, and it is even possible to combine digital rights management features with the policy to prohibit certain types of information from being copied to these devices.

For example, with Group Policy in Windows, you can use a number of policies to control the use of USB devices. Figure 4-1 shows a default domain policy to disallow the use of all removable storage. As you see, there are many other less drastic settings as well.

Key Topic

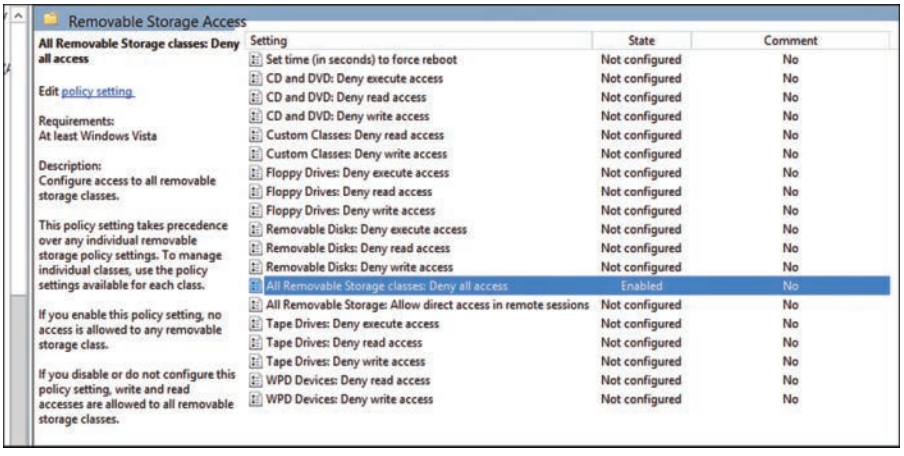

Figure 4-1 Controlling the Use of USB Devices

Print Blocking

As you learned in Chapter 1, blocking the printing of sensitive documents is entirely within the capabilities of DLP software. Print blocking can prevent someone from getting a copy of sensitive information off the printer and can prevent that information from being stored for any length of time in the memory of the print device, where it might be obtained by someone hacking into the printer.

Remote Desktop Protocol (RDP) Blocking

Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft that provides a graphical interface to connect to another computer over a network connection. Unlike Telnet and SSH, which allow only working from the command line, RDP enables you to work on a remote computer as if you were actually sitting at its console.

RDP sessions use native RDP encryption but do not authenticate the session host server. To mitigate this, you can use SSL/TLS for server authentication and to encrypt RDP session host server communications. This requires a certificate. You can use an existing certificate or the default self-signed certificate.

While RDP can be used for remote connections to a machine, it can also be used to connect users to a ***virtual desktop infrastructure (VDI)***. A VDI allows a user to connect from anywhere and work from a virtual desktop. Each user may have his or her own virtual machine (VM) image, or many users may use images based on the same VM.

The advantages and disadvantages of RDP are described in Table 4-1.

Key Topic

Table 4-1 Advantages and Disadvantages of RDP

Advantages	Disadvantages
Data is kept in the data center, so disaster recovery is easier.	Sever downtime can cause issues for many users.
Users can work from anywhere when using RDP in a VDI.	Network issues can cause problems for many users.
There is a potential reduction in the cost of business software when using an RDP model where all users are using the same base VM.	Insufficient processing power in the host system can cause bottlenecks.
	Implementing and supporting RDP requires solid knowledge.

RDP can be blocked at the firewall and at the system level by blocking port 3389.

Clipboard Privacy Controls

The clipboard function in desktops, laptops, and mobile devices is a convenient feature that stores information in memory until you paste it somewhere. But did you ever think of what happens after that? The information stays there until you copy over it! Moreover, in many systems, including Android, it has been found that any application can read that data without your permission.

While there is a fix to the Android issue, the point to be made is that organizations should be aware of this issue and take whatever steps are required to solve it as it may exist in your operating systems.

Restricted Virtual Desktop Infrastructure (VDI) Implementation

Virtual desktop infrastructures (VDIs) host desktop operating systems within a virtual environment in a centralized server. Users access the desktops and run them from the server. There are three models for implementing VDI:

Key Topic

- **Centralized model:** All desktop instances are stored in a single server, which requires significant processing power on the server.
- **Hosted model:** Desktops are maintained by a service provider. This model eliminates capital cost and is instead subject to operational cost.
- **Remote virtual desktops model:** An image is copied to the local machine, which means a constant network connection is unnecessary.

Figure 4-2 compares the remote virtual desktop models (also called streaming) with centralized VDI.

Key Topic

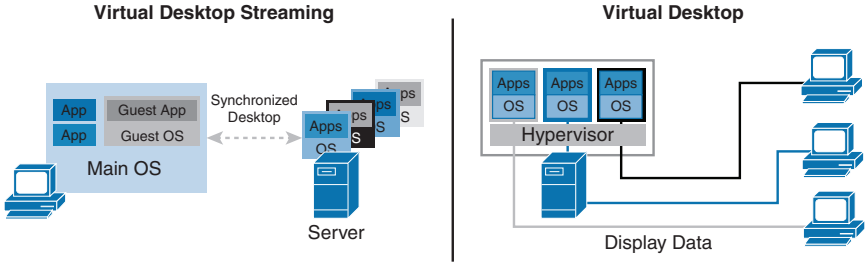

Figure 4-2 VDI Streaming and Centralized VDI

While a VDI environment can be beneficial, there are some steps that can be taken to restrict the infrastructure for security reasons:

- Consider disallowing copy and paste functions.
- Create an allow list (formerly known as a whitelist) or a block list (formerly known as a blacklist) to prevent users from accessing certain external sites or email providers.
- Evaluate the primary image for unnecessary services.
- Implement firewalls and antivirus software.
- Require multifactor authentication.

Data Classification Blocking

Data should be classified based on its value to the organization and its sensitivity to disclosure. Assigning a value to data allows an organization to determine the resources that should be used to protect the data. Resources that are used to protect data include human resources, monetary resources, and access control resources.

Classifying data as it relates to confidentiality, integrity, and availability (CIA) allows you to apply different protective measures.

After data is classified, the data can be segmented based on the level of protection it needs. Classification levels ensure that data is handled and protected in the most cost-effective manner possible. An organization should determine the classification levels it uses based on the needs of the organization. A number of commercial business and military and government information classifications are commonly used.

The information life cycle should also be based on the classification of the data. Organizations are required to retain certain information, particularly financial data, based on local, state, and federal laws and regulations.

Once data classification has occurred, you can then use the classifications to restrict access to data based on its classification. In Chapter 5, you'll will learn about an access control system called mandatory access control (MAC) that uses such classification labels to block access to data.

Data Loss Detection

It's bad enough when data leakages or data breaches occur, and it's even worse when you don't even know it's occurring! It is astounding how long it takes some companies to know they've been breached! In this section you'll learn about methods of detecting and preventing data loss.

Watermarking

Steganography occurs when a message is hidden inside another object, such as a picture or a document. In steganography, it is crucial that only those who are expecting the message know that the message exists.

Digital watermarking is a method used in steganography. It involves embedding a logo or trademark in documents, pictures, or other objects. The watermark deters people from using the materials in an unauthorized manner.

Digital Rights Management (DRM)

Hardware manufacturers, publishers, copyright holders, and individuals use ***digital rights management (DRM)*** to control the use of digital content. This often also involves device controls. First-generation DRM software controls copying. Second-generation DRM controls executing, viewing, copying, printing, and altering works or devices. The U.S. Digital Millennium Copyright Act (DMCA) of 1998 imposes criminal penalties on those who make available technologies whose primary purpose is to circumvent content protection technologies. DRM includes restrictive license agreements and encryption. DRM protects computer games and other software, documents, ebooks, films, music, and television.

In most enterprise implementations, the primary concern is the DRM control of documents by using open, edit, print, or copy access restrictions that are granted on a permanent or temporary basis. Solutions can be deployed that store the protected data in a central or decentralized model. Encryption is used in DRM to protect the data both at rest and in transit.

Network Traffic Decryption/Deep Packet Inspection

In Chapter 1 you learned about firewalls that can perform deep packet inspection. ***Deep packet inspection*** can be used to identify data types that should not be on the network as well as data types that should not be leaving the network.

When performing deep packet inspection on encrypted traffic, realize that the capturing system must be configured with the decryption key, and it will impact performance of the system doing the capture and subsequent decryption.

Network Traffic Analysis

When network traffic is captured for analysis, we typically are most concerned with which systems are communicating with which other systems and what they are sending to one another. One of the best tools for organizing traffic into conversations or flows is NetFlow (you learned about NetFlow in Chapter 1).

Data Classification, Labeling, and Tagging

Earlier in this chapter you learned about the value of classifying data into sensitivity levels. In this section you'll learn about how data is marked with its classification.

Metadata/Attributes

Data types are marked or labeled with their classification. This can be done physically with tags on storage devices containing data of various types and can also be done electronically so the DLP system can read this information and take the appropriate action, according to the DLP policy. Attributes (properties) of the data and its metadata (more details about the data) can also be used in this process.

XACML

Extensible Access Control Markup Language (XACML) is a standard for an access control policy language using Extensible Markup Language (XML). Its goal is to create an attribute-based access control system that decouples the access decision

from the application or the local machine. It provides for fine-grained control of activities based on criteria including:

Key Topic

- Attributes of the user requesting access (for example, all division managers in London)
- The protocol over which the request is made (for example, HTTPS)
- The authentication mechanism (for example, requester must be authenticated with a certificate)

LDAP

LDAP attributes are used in Active Directory. Examples include the Distinguished Name (DN) and Relative Distinguished Name (RDN), Common Name (CN), Domain Component (DC), and Organizational Unit (OU) attributes.

Obfuscation

Obfuscation is the act of making something obscure, unclear, or unintelligible. When we use that term with respect to sensitive or private information, it refers to changing the information in some way to make it unreadable to unauthorized individuals. It's not encryption, however. In this section you'll learn about methods of obfuscation.

Tokenization

Tokenization substitutes a sensitive value in data with another value that is not sensitive. It is an emerging standard for mobile transactions that uses numeric tokens to protect cardholders' sensitive credit and debit card information. Tokenization is a great security feature that substitutes the primary account number with a numeric token that can be processed by all participants in the payment ecosystem.

Scrubbing

Data ***scrubbing*** actually has two meanings:

- Scrubbing is used to maintain data quality. It involves checking main memory and storage for errors and making corrections using redundant data in the form of different checksums or copies of data. By detecting and correcting errors quickly, scrubbing reduces the likelihood that correctable errors will accumulate and lead to uncorrectable errors.
- Scrubbing also can refer to removing private data. This meaning relates to obfuscation.

Masking

Data masking means altering data from its original state to protect it. You already learned about two forms of masking: encryption and hashing. Encryption is storing the data in an encrypted form, and hashing is storing a hash value (generated from the data by a hashing algorithm) rather than the data itself. Many passwords are stored as hash values.

Other methods of data hiding are

- Using substitution tables and aliases for data
- Redacting or replacing sensitive data with random values
- Averaging or aggregating individual values

Anonymization

Data deidentification, or ***data anonymization***, is the process of deleting or masking personal identifiers, such as personal names, from a set of data. It is often done when the data is being used in the aggregate, such as when medical data is used for research. Anonymization is a technical control used as one of the main approaches to data privacy protection.

Encrypted vs. Unencrypted

While using obfuscation is appropriate for some data types, it is not sufficient for all types. When security is top of mind, data should be encrypted—both at rest and when it is in transit.

Data Life Cycle

You learned about the data life cycle earlier in this chapter. Review that section. You will learn more about it in Chapter 27. The information life cycle should also be based on the classification of the data. Organizations are required to retain certain information, particularly financial data, based on local, state, or government laws and regulations. This section looks at the steps in the data life cycle.

Create

The first step in the data life cycle is the creation or acquisition of the data. While most data is generated by an organization, in some cases, an organization might purchase data, such as purchasing a marketing report from an industry organization or demographic data that helps sell products. The important issue during this step is the proper classification of the data so it can receive the appropriate protection.

Use

Once the data is available to users, those who require access to it need to use the data in the manner intended. At this step, the important issue is proper access control and review of accounts given access to ensure that permissions are being used appropriately.

Share

The sharing of data with others is a step fraught with danger. Uncontrolled sharing can cancel out all of an organization's security safeguards. Granting the right to share the data should only be done when necessary, and this right should be held by as few individuals as possible.

Store

During the time that data is held by an organization, it must be stored somewhere. Security issues that are paramount at this step are ensuring that the prescribed encryption is in place, that the data is being successfully backed up, and that integrity is being ensured by frequently generating hash values of the data that can be used to identify data corruption if it occurs.

Archive or Destroy

All organizations need procedures in place for the retention and destruction of data. Data retention and destruction must follow all local, state, and federal regulations and laws. Documenting proper procedures ensures that information is maintained for the required time to prevent financial fines and possible incarceration of high-level organizational officers. These procedures must include both the retention period, including longer retention periods for legal holds, and the destruction process.

Data Inventory and Mapping

Data inventory and mapping is a process typically carried out using software tools to enumerate all the data, regardless of where it might be stored or which department uses it. It's also a stringent requirement of modern privacy legislation, like the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), because it also identifies privacy information. It also consolidates data from multiple databases.

Data Integrity Management

When data has been altered by an unauthorized process or individual, we say that it lacks integrity. To maintain integrity, access control is certainly important, but the best assurance that integrity has been maintained is to generate message digests of the relevant data by using hashing algorithms. The values can be used at a later time to verify that the data remains unchanged from the time the message digest was generated.

Data Storage, Backup, and Recovery

While protecting data on a device is always a good idea, in many cases an organization must comply with an external standard regarding the minimum protection provided to the data on the storage device. For example, the ***Payment Card Industry Data Security Standard (PCI DSS)*** enumerates requirements that payment card industry players should meet to secure and monitor their networks, protect cardholder data, manage vulnerabilities, implement strong access controls, and maintain security policies.

The operations team also must determine which data is backed up, how often the data is backed up, and the method of backup used. An organization must determine how data is stored, including data in use and data that is backed up. While data owners are responsible for determining data access rules, data life cycle, and data usage, they must also ensure that data is backed up and stored in alternate locations to ensure that it can be restored.

Let's look at an example. Suppose that an organization's security administrator has received a subpoena for the release of all the email received and sent by the company's chief executive officer (CEO) for the past three years. If the security administrator is only able to find one year's worth of email records on the server, he should check the organization's backup logs and archives before responding to the request. Failure to produce all the requested data could possibly have legal implications. The security administrator should restore the CEO's email from an email server backup and provide whatever is available for up to the past three years from the subpoena date. Keep in mind, however, that the organization should provide all the data that it has regarding the CEO's emails. If the security administrator is able to recover the past five years' worth of the CEO's email, the security administrator should notify the appropriate authorities and give them access to all five years' data.

As a rule of thumb, in a subpoena situation, you should always provide all the available data, regardless of whether it exceeds the requested amount or any internal data retention policies. For example, if users are not to exceed 500 MB of storage but you find that a user has more than 3 GB of data, you should provide all that data in

response to any legal requests. Otherwise, you and the organization could be held responsible for withholding evidence.

To design an appropriate data recovery solution, security professionals must understand the different types of data backups that can occur and how these backups are used together to restore the live environments.

Security professionals must understand the following data backup types and schemes:

- Full backup
- Differential backup
- Incremental backup
- Copy backup
- Daily backup
- Transaction log backup
- First-in, first-out rotation scheme
- Grandfather/father/son rotation scheme

Key Topic

The three main data backup types are full backups, differential backups, and incremental backups. To understand these three data backup types, you must understand the concept of archive bits. When a file is created or updated, the archive bit for the file is enabled. If the archive bit is cleared, the file will not be archived during the next backup. If the archive bit is enabled, the file will be archived during the next backup.

With a ***full backup***, all data is backed up. During the full backup process, the archive bit for each file is cleared. A full backup takes the longest time and the most space to complete. However, if an organization uses only full backups, then only the latest full backup needs to be restored. Any backup that uses a differential or incremental backup will first start with a full backup as its baseline. A full backup is the most appropriate for offsite archiving.

In a ***differential backup***, all files that have been changed since the last full backup will be backed up. During the differential backup process, the archive bit for each file is not cleared. A differential backup might vary from taking a short time and a small amount of space to growing in both the backup time and amount of space needed over time. Each differential backup will back up all the files in the previous differential backup if a full backup has not occurred since that time. In an organization that uses a full/differential scheme, the full backup and only the most recent differential backup must be restored, meaning only two backups are needed.

An ***incremental backup*** backs up all files that have been changed since the last full or incremental backup. During the incremental backup process, the archive bit for each file is cleared. An incremental backup usually takes the least amount of time and space to complete. In an organization that uses a full/incremental scheme, the full backup and each subsequent incremental backup must be restored. The incremental backups must be restored in order. If your organization completes a full backup on Sunday and an incremental backup daily Monday through Saturday, up to seven backups could be needed to restore the data. Table 4-2 provides a comparison of the three main backup types.

Key Topic

Table 4-2 Backup Types Comparison

Type	Data Backed Up	Backup Time	Restore Time	Storage Space
Full backup	All data	Slowest	Fast	High
Incremental backup	Only new/modified files/ folders since the last full or incremental backup	Fast	Moderate	Lowest
Differential backup	All data since the last full backup	Moderate	Fast	Moderate

Copy and daily backups are two special backup types that are not considered part of any regularly scheduled backup scheme because they do not require any other backup type for restoration. Copy backups are similar to normal backups but do not reset the file's archive bit. Daily backups use a file's timestamp to determine whether it needs to be archived. Daily backups are popular in mission-critical environments where multiple daily backups are required because files are updated constantly.

Transaction log backups are used only in environments where it is important to capture all transactions that have occurred since the last backup. Transaction log backups help organizations recover to a particular point in time and are most commonly used in database environments.

Although magnetic tape drives are still in use today to back up data, many organizations today back up their data to optical discs, including CD-ROMs, DVDs, and Blu-ray discs; high-capacity, high-speed magnetic drives; solid-state drives; or other media. No matter the media used, retaining backups both onsite and offsite is important. Store onsite backup copies in a waterproof, heat-resistant, fire-resistant safe or vault.

As part of any backup plan, an organization should also consider the backup rotation scheme that it will use. Cost considerations and storage considerations often dictate that backup media be reused after a period of time. If this reuse is not planned

in advance, media can become unreliable due to overuse. Two of the most popular backup rotation schemes are first-in, first-out and grandfather/father/son:

- ***First-in, first-out (FIFO)*:** In this scheme, the newest backup is saved to the oldest media. Although this is the simplest rotation scheme, it does not protect against data errors. If an error exists in the data, the organization might not have a version of the data that does not contain the error.
- ***Grandfather/father/son (GFS)*:** In this scheme, three sets of backups are defined. Most often these three definitions are daily, weekly, and monthly. The daily backups are the sons, the weekly backups are the fathers, and the monthly backups are the grandfathers. Each week, one son advances to the father set. Each month, one father advances to the grandfather set. Figure 4-3 displays a typical five-day GFS rotation using 21 tapes. The daily tapes are usually differential or incremental backups. The weekly and monthly tapes must be full backups.

Key Topic

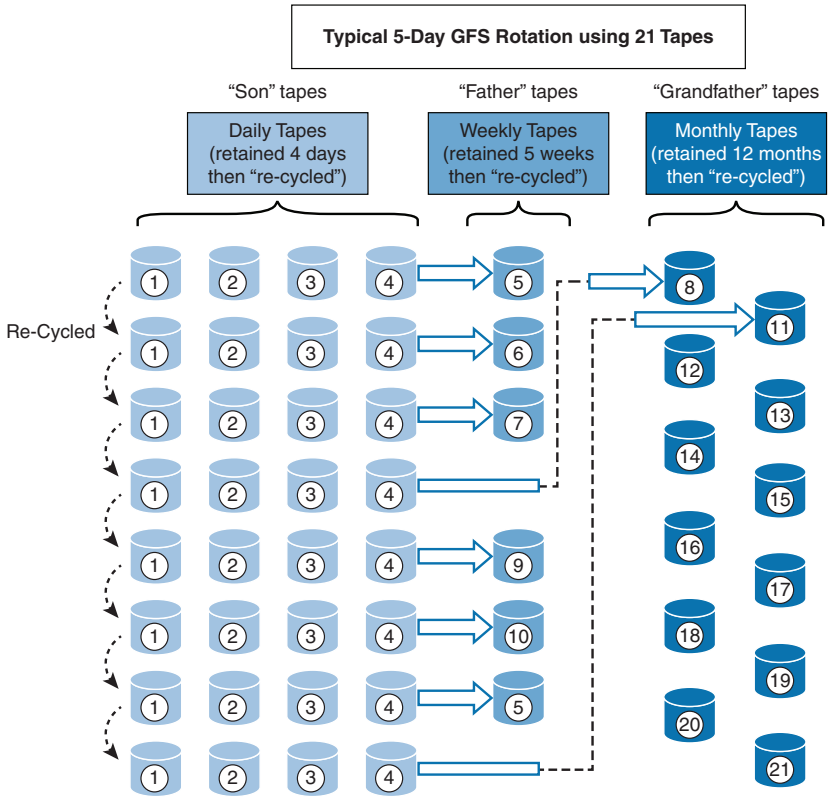

Figure 4-3 Grandfather/Father/Son Backup Rotation Scheme

Electronic backup solutions back up data more quickly and accurately than the normal data backups and are best implemented when information changes often. You should be familiar with the following electronic backup terms and solutions:

Key Topic

- ***Electronic vaulting*:** This method involves copying files as modifications occur in real time.
- ***Remote journaling*:** This method involves copying the journal or transaction log offsite on a regular schedule, in batches.
- ***Tape vaulting*:** This method involves creating backups over a direct communication line on a backup system at an offsite facility.
- ***Hierarchical storage management (HSM)*:** This method involves storing frequently accessed data on faster media and less frequently accessed data on slower media.
- ***Optical jukebox*:** This method involves storing data on optical discs and uses robotics to load and unload the optical discs as needed. This method is ideal when 24/7 availability is required.
- ***Replication*:** This method involves copying data from one storage location to another. Synchronous replication uses constant data updates to ensure that the locations are close to the same, whereas asynchronous replication delays updates to a predefined schedule.
- ***Cloud backup*:** Another method growing in popularity is to back up data to a cloud location.

Redundant Array of Inexpensive Disks (RAID)

RAID is a hard drive technology in which data is written across multiple disks in such a way that a disk can fail, and the data can be made available quickly by remaking disks in the array without resorting to a backup tape. The most common types of RAID are:

- ***RAID 0*:** Also called disk striping, this method writes the data across multiple drives. While it improves performance, it does not provide fault tolerance. RAID 0 is depicted in Figure 4-4.

Key Topic

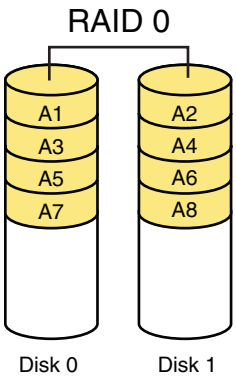

Figure 4-4 RAID 0

- ***RAID 1*:** Also called disk mirroring, RAID 1 uses two disks and writes a copy of the data to both disks, providing fault tolerance in the event of a single drive failure. RAID 1 is depicted in Figure 4-5.

Key Topic

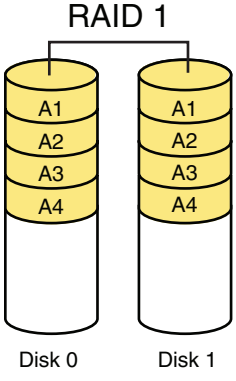

Figure 4-5 RAID 1

- ***RAID 3*:** This method, which requires at least three drives, writes the data across all drives, as with striping, and then writes parity information to a single dedicated drive. The parity information is used to regenerate the data in the event of a single drive failure. The downfall of this method is that the parity drive is a single point of failure. RAID 3 is depicted in Figure 4-6.

Key Topic

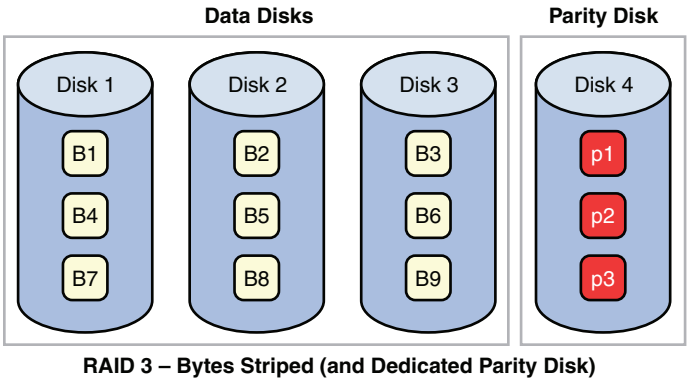

Figure 4-6 RAID 3

- ***RAID 5*:** This method, which requires at least three drives, writes the data across all drives, as with striping, and then writes parity information across all drives as well. The parity information is used in the same way as in RAID 3, but it is not stored on a single drive, so there is no single point of failure for the parity data. With hardware RAID 5, the spare drives that replace the failed drives are usually hot swappable, meaning they can be replaced on the server while it is running. RAID 5 is depicted in Figure 4-7.

Key Topic

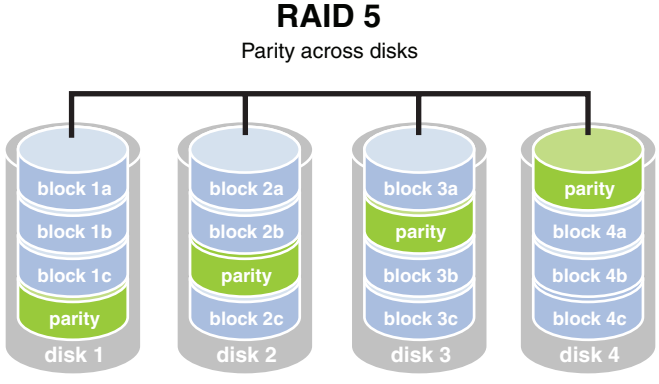

Figure 4-7 RAID 5

- ***RAID 7*:** While not a standard but a proprietary implementation, this system incorporates the same principles as RAID 5 but enables the drive array to continue to operate if any disk or any path to any disk fails. The multiple disks in the array operate as a single virtual disk.
- ***RAID 10*:** This method combines RAID 1 and RAID 0 and requires a minimum of four disks. However, most implementations of RAID 10 have four or

more drives. A RAID 10 deployment contains a striped disk that is mirrored on a separate striped disk. Figure 4-8 depicts RAID 10.

Key Topic

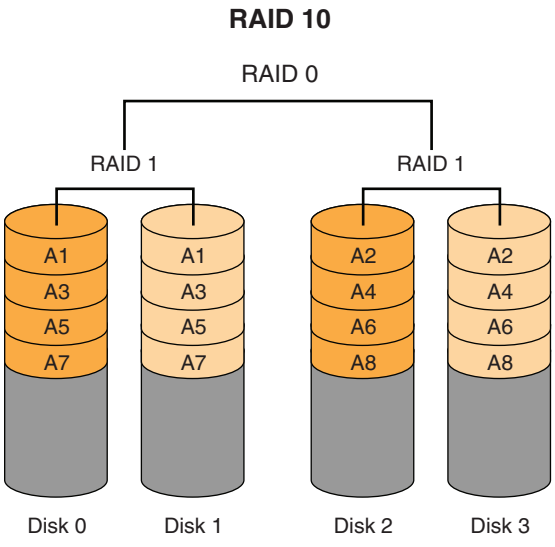

Figure 4-8 RAID 10

RAID can be implemented with software or with hardware, and certain types of RAID are faster when implemented with hardware. Both RAID 3 and 5 are examples of RAID types that are faster when implemented with hardware. Simple striping and mirroring (RAID 0 and 1), however, tend to perform well in software because they do not use the hardware-level parity drives. When software RAID is used, it is a function of the operating system. Table 4-3 summarizes the RAID types.

Key Topic

Table 4-3 RAID Types

RAID Level	Minimum Number of Drives	Description	Strengths	Weaknesses
RAID 0	2	Data striping without redundancy	Highest performance	No data protection; if one drive fails, all data is lost
RAID 1	2	Disk mirroring	Very high performance; very high data protection; very minimal penalty on write performance	High redundancy cost overhead; because all data is duplicated, twice the storage capacity is required

RAID Level	Minimum Number of Drives	Description	Strengths	Weaknesses
RAID 3	3	Byte-level data striping with a dedicated parity drive	Excellent performance for large, sequential data requests	Not well suited for transaction-oriented network applications; the single parity drive does not support multiple, simultaneous read and write requests
RAID 5	3	Block-level data striping with distributed parity	Best cost/performance for transaction-oriented networks; very high performance and very high data protection; supports multiple simultaneous reads and writes; can also be optimized for large, sequential requests	Write performance is slower than with RAID 0 or RAID 1
RAID 10	4	Disk striping with mirroring	High data protection, which increases each time you add a new striped/mirror set	High redundancy cost overhead; because all data is duplicated, twice the storage capacity is required

Exam Preparation Tasks

As mentioned in the Introduction, you have a couple choices for exam preparation: the exercises here and the practice exams in the Pearson IT Certification test engine.

Review All Key Topics

Review the most important topics in this chapter, noted with the Key Topic icon in the outer margin of the page. Table 4-4 lists these key topics and the page number on which each is found.

Key Topic

Table 4-4 Key Topics for Chapter 4

Key Topic Element	Description	Page Number
Figure 4-1	Controlling the Use of USB Devices	126
Table 4-1	Advantages and Disadvantages of RDP	127
List	VDI models	128
Figure 4-2	VDI Streaming and Centralized VDI	128
List	VDI attributes	131
List	Data masking methods	132
Section	Data Life Cycle	132
Paragraph	Backup types	135
Table 4-2	Backup Types Comparison	136
Figure 4-3	Grandfather/Father/Son Backup Rotation Scheme	137
List	Electronic backup terms and solutions	138
Figure 4-4	RAID 0	139
Figure 4-5	RAID 1	139
Figure 4-6	RAID 3	140
Figure 4-7	RAID 5	140
Figure 4-8	RAID 10	141
Table 4-3	RAID Types	141

Define Key Terms

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

Remote Desktop Protocol (RDP), virtual desktop infrastructure (VDI), digital watermarking, digital rights management (DRM), deep packet inspection, Extensible Access Control Markup Language (XACML), obfuscation, tokenization, scrubbing, data masking, data anonymization, data inventory and mapping, Payment Card Industry Data Security Standard (PCI DSS), full backup, differential backup, incremental backup, first-in, first-out (FIFO), grandfather/father/son (GFS), electronic vaulting, remote journaling, tape vaulting, hierarchical storage management (HSM), optical jukebox, replication, cloud backup, RAID, RAID 0, RAID 1, RAID 3, RAID 5, RAID 7, RAID 10

Complete Tables and Lists from Memory

There are no memory tables or lists in this chapter.

Review Questions

1. Which of the following forms of RAID places the parity information on a single drive?
   a. RAID 0
   b. RAID 1
   c. RAID 3
   d. RAID 5

2. Which of the following techniques or tools is used to deploy print blocking?
   a. DLP
   b. RAID
   c. RDP
   d. VDI

3. Which of the following is not a characteristic of RDP?
   a. Server downtime can cause issues for many users.
   b. Data is not kept in the data center, so disaster recovery is easier.
   c. Network issues can cause problems for many users.
   d. Insufficient processing power in the host system can cause bottlenecks.

4. In which of the following rotation schemes are three sets of backups defined?
   a. FIFO
   b. RAID
   c. GFS
   d. STP

5. In which VDI model are desktops maintained by a service provider?
   a. Centralized model
   b. Hosted model
   c. Remote virtual desktops model
   d. Streaming model

6. Which backup model is the fastest to back up but the slowest to restore?
   a. Full
   b. Copy
   c. Differential
   d. Incremental

7. Which backup type is used to capture all transactions that have occurred since the last backup?
   a. Transaction log backup
   b. Incremental backup
   c. Full backup
   d. Copy backup

8. Which backup method involves copying files as modifications occur in real time?
   a. Electronic vaulting
   b. Optical jukebox
   c. Remote journaling
   d. Tape vaulting

9. Which of the following enumerates requirements that payment card industry players should meet to secure and monitor their networks, protect cardholder data, manage vulnerabilities, implement strong access controls, and maintain security policies?
   a. GLBA
   b. PCI DSS
   c. COPPA
   d. SOX

10. Which RAID method can potentially survive two drive failures?
   a. RAID 1
   b. RAID 3
   c. RAID 5
   d. RAID 10

Index

Numbers

2-step verification, 173
3-D printing, 224
3DES (Triple Digital Encryption Standard), 528
128-bit AES encryption, 490
802.1X, 166–167

A

ABAC (attribute-based access control), 161–162
accept strategy, 565
acceptance testing, 107
access control, 159–160
  attribute-based, 161–162
  discretionary, 160, 598
  mandatory, 160, 444
    kernel, 445
    middleware, 445
    SEAndroid, 444–445
    SELinux (Security-Enhanced Linux), 444
  natural, 361
  role-based, 161
  rule-based, 161
access logs, 255–256
accountability, 208, 482–483
ACLs (access control lists), 49, 267, 612–613
active scanners, 278
ActiveX, 327
actors
  APTs (advanced persistent threats), 233–234
  black hat, 236
  competitors, 234
  crackers, 236
  gray hat, 236
  hackers, 236
  hacktivists, 234
  identifying techniques, 237
  insider threats, 234
  organized crime, 235
  properties
    create vulnerabilities, 236
    resources, 235
    supply chain access, 235–236
  script kiddies, 235
  white hat, 236
adb command, 445
ADCs (application delivery controllers), 3
advantages
  of firewalls, 14
  of NAC (network access control), 10
  of NGFWs (next-generation firewalls), 15
  of RDP (Remote Desktop Protocol), 127
  of SIEM, 35
  of virtualization, 185
AEG (automatic exploit generation), 219–220
AES (Advanced Encryption Standard), 527

agent-based vulnerability scanning, 276–277
Agile, 109–110, 111, 112–113
AHEAD (authenticated encryption with associated data), 536
AI (artificial intelligence), 219–220
air gap, 49
Aircrack-ng, 403–404
airplane mode, 427
AJAX (Asynchronous JavaScript and XML), 327–328
ALE (annualized loss expectancy), 561, 563
alert(s), 256
  antivirus, 259–260
  DLP (data loss prevention), 257
  fatigue, 259
  FIM (file integrity monitoring), 257
  IDS/IPS, 258
  SIEM (security information and event management), 257
alerts, 480
algorithms, 205. *See also* asymmetric algorithms; hashing; symmetric algorithms
  asymmetric, 528–529
    ECDSA (Elliptic-Curve Digital Signature Algorithm), 531
    RSA (Rivest, Shamir, and Adleman), 530–531
  digital signature, 530
  hashing, 519–520
  key agreement, 529
    Diffie-Hellman, 529
    ECDH (Elliptic-Curve Diffie-Hellman), 530
  known flaws and weaknesses, 531
  Lucifer, 528
  NFS (Number Field Sieve), 531
  Rijndael, 527
  symmetric, 522
alternative provider BCDR, 486
analysis tools
  Aircrack-ng, 403–404
  ExifTool, 403
  Nmap, 403
  Sleuth Kit, 405
  Volatility, 404
analytics, 348–349
Android
  fragmentation, 432
  remote wipe feature, 422–423
  rooting, 431
  side loading, 431–432
anomaly-based IDS (intrusion detection system), 4
anonymization, 132
anti-spam, 29
antivirus, 39, 259–260, 450, 618–619
APIs (application programming interfaces), 30
  classic model, 88–89
  container, 88, 89
  management, 91
  ROTs (roots of trust) and, 176–177
Apktool, 294
application control, 353, 419, 451
  allow lists, 354
  atomicity, 355
  block lists, 354
  license technologies, 353
  time of check vs. time of use, 354–355
application integration
  CMDB (configuration management database), 101
  CMS (content management system), 101
  CRM (customer relationship management), 100
  ERP (enterprise resource planning), 100–101
  integration enablers, 101
    directory services, 101

DNS (Domain Name System), 101–102
ESB (enterprise service bus), 103
SOA (service-oriented architecture), 102
application vetting process, 90–91
application virtualization, 189
application-level proxies, 13
apps, system, 431
APs (access points), 53, 295
APTs (advanced persistent threats), 233–234
AR (augmented reality), 223
ARF (Asset Reporting Format), 282
ARO (annualized rate of occurrence), 563
ASIC (application-specific integrated circuit), 462
ASLR (address space layout randomization), 442
asset value, 558–559
asymmetric encryption, 528–529
public/private keys, 508–511
RSA (Rivest, Shamir, and Adleman), 530–531
atomicity, 355
attacks
authentication bypass, 340
Bluetooth, 424
CSRF (Cross-Site Request Forgery), 331–332
DDoS (distributed DoS), 22
directory traversal, 330
DoS (denial-of-service), 22, 339–340
downgrade, 514, 546
injection, 332
command, 337
LDAP, 335
process, 337
SQL, 335–336
XML, 332–334
interception, 339
on-path, 477–478
persistence, 298
rainbow table, 393
side-channel, 293
social engineering, 340, 374
identity theft, 341
pharming, 340
phishing, 340
shoulder surfing, 341
spear phishing, 28
whaling, 28
targeted, 232
VLAN hopping, 42–43
VM escape, 337–338
XSS (cross-site scripting), 331
attestation, 179, 448
audio conferencing, 491
audit(ing), 155
cloud environments, 483
events, 256
requirements and frequency, 601
trails, 255–256
authentication. *See also* credential management
2-step verification, 173
802.1X, 166–167
biometric systems, 170–171, 172–173
behavioral, 171–172
physiological, 170–171
broken, 318–319
bypass, 340
characteristic factors, 170
client, 504
cross-domain, 61
Diameter, 164
EAP (Extensible Authentication Protocol), 167–168
gesture, 420
IPsec, 534
Kerberos, 165–166
knowledge factors, 169
LDAP (Lightweight Directory Access Protocol), 164–165

multifactor, 168
OAuth, 166
OpenID, 156–157
ownership factors, 169–170
passwordless, 224–225
RADIUS (Remote Authentication Dial-in User Service), 162–163
router, 24–26
server, 504
smart card, 209–210
TACACS (Terminal Access Controller Access Control System), 163–164
two-factor, 168
automated patch management, 284
automation, 76, 77, 213, 355
autoscaling, 76
availability, 479, 593–594
availability zone, 46–47
avoid strategy, 566
awareness training, 599–601

B

backups, 134–135. *See also* storage
of cloud environments, 485–486
copy, 136
daily, 136
differential, 135
electronic, 138
evidence preservation, 389
full, 135
incremental, 136
key management and, 207
rotation scheme, 136–137
storage, 136
transaction log, 136
types comparison, 136
verification, 391
BACnet (Building Automation and Control Network), 464–465
in-band interface, 174
baseband processor, 422
baselines, 85, 86, 438
Bash, 356
BCDR (business continuity and disaster recovery), 486
BCP (business continuity plan), 660–661. *See also* disaster recovery
after-action reports, 666
business continuity steps, 662
checklist, 666
full interruption test, 667
parallel/simulation test, 667
personnel components, 661
project scope, 661
tabletop exercises, 666
walkthrough test, 666
Bcrypt, 537
behavioral biometric systems, 171–172
benchmarks, 85–86
best practices
middleware, 91–92
stakeholder communication, 375–376
BGP route hijacking, 338
BIA (business impact analysis), 556, 656–658
identify critical processes and resources, 659
mission essential functions, 659
recovery service level, 659
RPO (recovery point objective), 659
RTO (recovery time objective), 659
big data, 222–223, 348
binary analysis tools, 401
binwalk, 401
file command, 403
GDB (GNU Project debugger), 401
Ghidra, 401
hexdump, 401
ldd, 402
objdump, 402
OllyDbg, 402
readelf, 402
strace, 402
binding, 446

binwalk, 401
biometric systems, 172–173, 420
  acceptability, 172
  accuracy, 172
  behavioral, 171–172
  CER (crossover error rate), 172
  enrollment time, 172
  facial scan, 421
  FAR (false acceptance rate), 172
  feature extraction, 172
  fingerprint scan, 421
  FRR (false rejection rate), 172
  impersonation, 226
  iris scan, 421
  physiological, 170–171
  throughput rate, 172
BIOS (Basic Input/Output System), 447–448
bit splitting, 493
BitLocker, 439
black hat, 236
blob storage, 198
block ciphers, 527
block storage, 198
blockchain, 220, 221–222
Bluesnarfing, 424
Bluetooth, 424
bootstrapping, 77
broken access control, 117
broken authentication, 318–319
browser extensions, 326
  ActiveX, 327
  Flash, 327
buffer overflow, 316–318
BYOD (bring your own device), 51, 429, 432
bytecode, 329

C

CA (certificate authority), 499–500, 544
caching, 80
Cain and Abel, 306
CAN (Controller Area Network), 465
CANVAS, 305
captured email messages, 29
CASB (cloud access security broker), 196
CBC (cipher block chaining), 524
CCE (Common Configuration Enumeration), 282
CD (continuous delivery), 116
CDN (content delivery network), 79–80
CDP (continuous delivery pipeline), 116
Censys, 243
CER (crossover error rate), 172
certificate(s)
  chain issues, troubleshooting, 544–545
  classes, 543
  EV (extended validation), 502
  extensions, 505
  general purpose, 503
  life-cycle management, 507–508
  management, 426–427
  mismatched name, troubleshooting, 543–544
  multidomain, 502–503
  pinning, 512
  revocation list, 513–514
  revoked, 543
  signing requests, 513
  stapling, 512–513
  use cases
    client authentication, 504
    digital signatures, 504–505
    server authentication, 504
  validity dates, troubleshooting, 542
  wildcard, 501
  X.509, 503
    CN (Common Name), 505
    SAN (Subject Alternative Name), 505
ChaCha, 528
chain of custody, 385–386
change control process, 614
change management, 611

characteristic factors, 170
chroot, 186
CI (configuration item), 481
CI (continuous integration), 116
CIA triad, 128–129, 203, 204, 205–206, 570–571
ciphers
  block, 527
  stream-based, 526–527
circuit-level proxies, 13
classic API model, 88–89
click-jacking, 320
client-based application virtualization, 189
client-side processing, 325–326
clipboard privacy controls, 127
cloning, 388
cloud environments, 59. *See also* virtualization
  antivirus, 39
  availability, 479
  backup and recovery, 485–486
  BCDR (business continuity and disaster recovery), 486
  bit splitting, 493
  collaboration tools, 488
    audio conferencing, 491
    storage and document, 491–492
    video conferencing, 489–491
    web conferencing, 488–489
  deployment models
    community, 193
    cost and, 191
    data protection and, 192
    hybrid, 193
    location and, 191
    private, 193
    public, 193
    scalability and, 191
    single physical server hosting multiple organizations' VMs, 192
    single platform hosting multiple data types/owners on multiple virtual machines, 192
  erasure coding, 493
  extending appropriate on-premises controls, 196
  Faas (function as a service), 486
  hosting models
    multitenant, 193–194
    single-tenant, 194
  key management, 481–482
    accountability, 482–483
    audits, 483
    phases, 484–485
    survivability, 483
  live migration, 477
  load balancer, 3
  logs, 478–479
  provider limitations
    IP address scheme, 196
    VPC peering, 196
  segmentation, 50
  serverless, 486–487
  service models
    IaaS (infrastructure as a service), 195
    PaaS (platform as a service), 194
    SaaS (software as a service), 194
  SLAs (service-level agreements), 478
  storage configurations, 492
  virtualization, 79
clustering, 76
CMDB (configuration management database), 101
CMMI (Capability Maturity Model Integration), 643–644
CMS (content management system), 101
code, 617. *See also* testing
  byte, 329
  dependency management, 307–308, 323–324
  disposal and reuse, 104
  machine, 329

review, 98
signing, 94
cold site, 663
collaboration tools, 488
audio conferencing, 491
storage and document, 491–492
video conferencing, 489–491
web conferencing, 488–489
COM (Component Object Model), 327
command injection, 337
commands
adb, 445
encapsulation ppp, 24
Linux, 406
cron, 355–356, 357
dig, 242
file, 403
foremost, 399–400
ldd, 410
lsof, 410
readelf, 402
strace, 402
strings, 400–401
vmstat, 409–410
nc, 410
netstat, 407–409
nfdump, 37
nslookup, 242
objdump, 402
ps, 409
SFC, 35–36
tcpdump, 411
tshark, 252
commodity malware, 231
Common Criteria, 432, 644–645
communications analysis, 390
community cloud, 193
compensation controls, 450, 572–573
antivirus, 450
application control, 451
EDR (endpoint detection and response), 451
HIDS/HIPS, 451
host-based firewall, 451
redundant hardware, 452
self-healing hardware, 452
UEBA (user and entity behavior analytics), 452
compiler, 329
conditional access policy, 419
confidentiality, 205–206
configuration lockdown, 614–615
configuration management, 480–481
conntrack, 411
container APIs, 88, 89
containerization, 78–79, 187–188, 419, 432
containment, 371
isolate, 371
minimize, 371
content analysis, 390
contingency planning, 657–658
contracting, 52–53
controls, 570–572
compensative, 572–573
corrective, 573
detective, 572
deterrent, 573
protective, 572
recovery, 573
cookies, 618, 619
COPE (corporate owned, personally enabled), 429
COPPA (Children's Online Privacy Protection Act), 644
copy backups, 136
copyright, 632
corporate-owned device deployment, 429
corrective controls, 573
COSO ERM Integrated Framework, 588–589
cost/benefit analysis, 347
countermeasures, 347

CPE (Common Platform Enumeration), 279
CPTED (Crime Prevention Through Environmental Design), 361
CPU virtualization, disabling, 439–440
crackers, 236
credential management, 149. *See also* password(s)
  hardware key manager, 150
  password repository application, 149
    end-user password storage, 149
    on premises vs. cloud repository, 150
  shared credentials, 619
  SSO (single sign-on), 177–178
credentialed scans, 275–276
CRM (customer relationship management), 100
cron command, 355–356, 357
cross-certification, 506
cross-domain authentication, 61
cryptanalysis, 394
crypto shredding, 548
cryptocurrency, 220
cryptography, 203. *See also* certificate(s); encryption
  CIA triad, 203
  cipher mismatches, troubleshooting, 546
  cipher suites, troubleshooting, 545
  elliptic curve, 209, 535
  key management, 207–208
    accountability, 208
    audits, 208
    backups, 207
    survivability, 208
    troubleshooting, 546–549
  obfuscation, 548–549
  use cases
    data at rest, 205
    data in process/data in use, 205–206
    data in transit, 205
  weak, 321–322, 545
CSA (Cloud Security Alliance), STAR (Security Trust Assurance and Risk), 646
CSP (cloud service provider), 607–608
  compute resources, 608
  services, 608–609
  STAR (Security Trust Assurance and Risk), 646
CSP (cryptographic service provider), 506
CSRF (Cross-Site Request Forgery), 331–332
CTR (Counter), 525
custom DNS, 428
CVE (Common Vulnerabilities and Exposures) database, 279
CVSS (Common Vulnerability Scoring System), 279–282
Cyber Kill Chain, 246
CYOD (choose your own device), 429

D

DAC (discretionary access control), 160, 598
daily backups, 136
DAM (database activity monitoring), 350
  architectures, 350
  limitations, 350
  placement, 351
DAST (dynamic application security testing), 95
data
  classifications, 627–628
    commercial business, 628
    military and government, 628–629
  dispersion, 493
  exfiltration, 373
  geographic considerations, 635–637
  health/financial, 630
  integrity management, 134
  intellectual property, 630–631

copyright, 632
patent, 631
securing, 632–633
trade secret, 631–632
trademark, 632
inventory and mapping, 133
labeling and tagging
attributes, 130
blocking, 128–129
LDAP attributes, 131
metadata, 130
XACML (Extensible Access Control Markup Language), 130–131
life cycle, 132
archive or destroy, 133
create, 132
share, 133
store, 133
use, 133
loss detection, 129
deep packet inspection, 130
DRM (digital rights management), 129–130
network traffic analysis, 130
network traffic decryption, 130
watermarking, 129
ownership, 627
PII (personally identifiable information), 633–634
processing pipeline, 349
remnants, 478, 634
removal and destruction, 634–635
retention, 629
sovereignty, 626–627
third-party attestation of compliance, 637
types, 629
zones, 44–45
Data Distribution Service, 468
database storage, 197–198
dd command, 406
DDoS (distributed DoS) attack, 22
de facto standards, 639
decoy files, 348
deep fakes, 226
deep learning, 225
deep packet inspection, 19, 130
deep web, 237–238
Delphi technique, 557
dependency management, 307–308, 323–324
deperimeterization, 49–50
deployment scenarios, mobile device
BYOD (bring your own device), 429
COPE (corporate owned, personally enabled), 429
corporate-owned, 429
CYOD (choose your own device), 429
DES (Data Encryption Standard)
CBC (cipher block chaining), 524
CTR (Counter), 525
ECB (electronic codebook), 523
GCM (Galois/Counter Mode), 525–526
OFB (output feedback), 524–525
detective controls, 572, 596
deterrent controls, 573
development environment. *See also* software development
DevOps, 93–94
DevSecOps, 109
dex2jar, 294
Diameter, 164
Diamond Model of Intrusion Analysis, 245
differential backup, 135
Diffie-Hellman, 529
dig command, 242
digital
forensics, 430–431
signatures, 504–505
watermarking, 129

directory
  services, 61–62, 101
  traversal, 330
DISA STIGs, 90
disaster recovery, 660–661
  after-action reports, 666
  cold site, 663
  full interruption test, 667
  hot site, 663
  mobile site, 664
  parallel/simulation test, 667
  recovery and multiple site strategies, 662–663
  recovery service level, 659
  RTO (recovery time objective), 659
  warm site, 663
disclosure of information, email and, 30
disk imaging, 389
diStorm3, 294
distributed
  allocation, 76
  consensus, 221–222
diversity, 75
DLP (data loss prevention), 37–38, 125
  alerts, 257
  blocking of external media, 125–126
  clipboard privacy controls, 127
  data classification blocking, 128–129
  print blocking, 126
  RDP (Remote Desktop Protocol) blocking, 126–127
  rules, 268
  VDI (virtual desktop infrastructure) and, 128
DNP3 (Distributed Network Protocol 3), 466–467
DNS (Domain Name System), 101–102
  custom, 428
  harvesting, 240
  record types, 240
  threat intelligence information and, 239–242
DNSSEC (Domain Name System Security Extensions), 11, 101–102
documentation
  data life cycle, 132–133
  test plans, 105
DoH (DNS over HTTPS), 428
DoS (denial-of-service) attacks, 22, 339–340
downgrade attack, 514, 546
DRM (digital rights management), 129–130
DTP (Dynamic Trunking Protocol), 41
due diligence team, 61
dumpster diving, 341
dynamic analysis, 293
dynamic linking, 405
dynamic NAT (network address translation), 21
dynamic packet filtering, 13
dynamic testing, 98–99

E

EAM (enterprise access management), 178
EAP (Extensible Authentication Protocol), 167–168
ECB (electronic codebook), 523
ECC (elliptic curve cryptography), 209, 535
ECDH (Elliptic-Curve Diffie-Hellman), 530
ECDSA (Elliptic-Curve Digital Signature Algorithm), 531
edb-debugger, 294
e-discovery, 391–392, 648
EDR (endpoint detection and response), 451
EF (exposure factor), 558
eFuse, 432
electronic backups, 138
email. *See also* social engineering attacks
  captured messages, 29

disclosure of information and, 30
malware, 30
messaging protocols
IMAP (Internet Message Access Protocol), 26
POP (Post Office Protocol), 27
SMTP (Simple Mail Transfer Protocol), 27
MIME (Multipurpose Internet Mail Extensions), 210
S/MIME (Secure MIME), 533
spam, 28–29
spear phishing, 28
spoofing, 27
whaling, 28
embedded systems, 206–207, 459
analysis, 391
ASIC (application-specific integrated circuit), 462
FPGA (field-programmable gate array), 462
IoT (Internet of Things), 459–460
examples, 460
methods of securing devices, 461
PLD (programmable logic device), 461–462
SoC (system on a chip), 461
employment and termination procedures, 598–599
emulation, 188, 329
encapsulation ppp command, 24
encryption, 132, 203–204. *See also* algorithms; homomorphic encryption
128-bit AES, 490
algorithm, 205
asymmetric, public and private keys, 508–511
bit splitting, 493
block ciphers, 527
CBC (cipher block chaining), 524
configuration, 477–478
cryptanalysis, 394
CTR (Counter), 525
ECB (electronic codebook), 523
ECC (elliptic curve cryptography), 209
full device, 427
GCM (Galois/Counter Mode), 525–526
homomorphic, 221
incorrect permissions, troubleshooting, 546
keys, 205
local drive, 439
memory, 440–441
military-grade, 489–490
OFB (output feedback), 524–525
SEDs (self-encrypted drives), 450
shared responsibility model and, 609
stream-based ciphers, 526–527
end-of-support, 438
end-user password storage, 149
energy sector, 469
erasure coding, 493
ERP (enterprise resource planning), 100–101
ESB (enterprise service bus), 103
EV (extended validation) certificates, 502
event classifications
false negative, 367
false positive, 367
true negative, 367
true positive, 367
evidence
chain of custody, 385–386
cloning, 388
integrity preservation, 392
memory snapshots, 387
order of volatility, 386–387
presentation, 391–392
preservation, 388–389
backups, 389

secure storage, 389
relevance, 388
reliability, 388
system image, 388
ExifTool, 403
exploit frameworks, 304–305
export controls, 647–648
extensions, certificate, 505

F

FaaS (function as a service), 486
facial scan, 421
false negative, 367
false positive, 367
FAR (false acceptance rate), 172
fault tolerance, 74–75
feature extraction, 172
federation, 61, 156, 211–212
OpenID, 156–157
SAML (Security Assertion Markup Language), 157–158
Shibboleth, 158
transitive trust, 156
FERMA (Federation of European Risk Management Associations) Risk Management Standard, 589–590
field kit, 388
fielding, 104
FIFO (first-in, first-out) rotation, 137
file carving, 399
foremost command, 399–400
strings command, 400–401
file command, 403
file-based storage, 197
FIM (file integrity monitoring), 35–36, 257
final preparation, 672
Pearson Test Prep practice test software, 672
accessing offline, 673–674
accessing online, 673
customizing your exams, 674–675
updating your exams, 675
suggested plan for final review/study, 676–677
Financial Services Information Sharing and Analysis Center, 104, 617
fingerprint scan, 421
FIPS 199 (Standards for Security Categorization of Federal Information and Information Systems), 570–571
firewalls, 12
advantages of, 14
deep packet inspection, 19
host-based, 451
next-generation, 14–15
packet-filtering, 12
placement, 15–19
proxy, 13
application-level, 13
circuit-level, 13
kernel, 14
rules, 265–266
stateful, 12
firmware, patching, 442–443
Flash, 327
foremost command, 399–400
forensics, 385
analysis, 389
Aircrack-ng, 403–404
content, 390
ExifTool, 403
hardware/embedded device, 391
media, 389–390
network, 390
Nmap, 403
Sleuth Kit, 405
software, 390
Volatility, 404
backup verification, 391
binary analysis tools, 401
binwalk, 401
file command, 403

GDB (GNU Project debugger), 401
Ghidra, 401
hexdump, 401
ldd, 402
objdump, 402
OllyDbg, 402
readelf, 402
strace, 402
collection of evidence
chain of custody, 385–386
cloning, 388
memory snapshots, 387
order of volatility, 386–387
system image, 388
digital, 430–431
field kit, 388
file carving tools, 399
foremost command, 399–400
strings command, 400–401
hashing utilities, 407
sha256sum, 407
ssdeep, 407
identification, 385
imaging tools, 405
dd, 406
FTK (Forensic Toolkit), 405–406
live collection tools
conntrack, 411
ldd command, 410
lsof command, 410
netcat, 410
netstat, 407–409
ps command, 409
tcpdump command, 411
vmstat command, 409–410
Wireshark, 412–413
presentation of evidence, 391–392
preservation of evidence, 388–389
backups, 389
integrity preservation, 392
secure storage, 389
formal methods of software engineering, 103
forward proxy, 22
forward secrecy, 536
FPGA (field-programmable gate array), 462
fragmentation, 432
frameworks, 243. *See also* NIST (National Institute of Standards and Technology)
Cyber Kill Chain, 246
Diamond Model of Intrusion Analysis, 245
exploit, 304–305
MITRE ATT&CK (Adversarial Tactics, Techniques, & Common Knowledge), 243–245
risk, 573
COSO ERM Integrated Framework, 588–589
FERMA (Federation of European Risk Management Associations), 589–590
ISO/IEC 27005:2008, 587–588
NIST, 574–587
OSSTMM (Open Source Security Testing Methodology Manual), 588
vulnerable, 323
FRR (false rejection rate), 172
FTK (Forensic Toolkit), 405–406
full backup, 135
full device encryption, 427
fuzz testing, 95–97, 296–297
fuzzy hashing, 407

G

gap analysis, 564
GCM (Galois/Counter Mode), 525–526
GDB (GNU Project debugger), 401

GDPR (General Data Protection Regulation), 640
general purpose certificates, 503
generation-based fuzzing, 96, 297
geofencing, 425
geotagging, 426
gestures, 420
GFS (grandfather/father/son) rotation, 137
Ghidra, 401
GPG (GNU Privacy Guard), 211
gray hat, 236
Group Policy, 47–48, 125, 255, 438
guest environments, 45
GUI testing, 100

H

H.323, 490
HA (high availability), 75
hackers, 236
hacktivists, 234
Hadoop, 222–223
hardening techniques, 437
  ASLR (address space layout randomization), 442
  CPU virtualization support, disabling, 439–440
  disabling unused services, 438
  enabling No Execute (NX)/Execute Never (XN) bit, 439
  end-of-life devices, removing, 438
  end-of-support device, removing, 438
  images/templates, 438
  local drive encryption, 439
  memory encryption, 440–441
  removing unneeded services, 437
  secure encrypted enclaves, 440
  shell restrictions, 441
hardware
  analysis, 391
  key manager, 150
hashing, 392, 407
  Bcrypt, 537
  collisions, 393
  fuzzy, 407
  HMAC (hash-based message authentication code), 520
  limitations, 392
  MAC (message authentication code), Poly1305, 521
  MD5, 393
  message digest, 393, 521
  one-way, 392
  passwords, 393–394
  RIPEMD (RACE Integrity Primitives Evaluation Message Digest), 521
  SHA (Secure Hashing Algorithm), 519–520
  tools
    sha256sum, 407
    ssdeep, 407
HDFS (Hadoop Distributed File System), 222–223
healthcare, 470
heterogeneity, 75
hexdump utility, 401
H-ISAC (Health Information Sharing and Analysis Center), 470
historian server, 463
HMAC (hash-based message authentication code), 520
homomorphic encryption, 221
  distributed consensus, 221–222
  PFE (private function evaluation), 221
  PIR (private information retrieval), 221
  SFE (secure function evaluation), 221
honeypots, 348
horizontal scaling, 74
host-based IDS (intrusion detection system), 5
hosting models
  multitenant, 193–194

single-tenant, 194
hot site, 663
HOTP (HMAC-based one-time password), 175
hotspots, 427
HSM (hardware security module), 448–449
HSTS (HTTP Strict Transport Security), 514
HTML5 (Hypertext Markup Language 5), 327
HTTP (Hypertext Transfer Protocol)
  headers, 117–118
  interceptors, 304
human intelligence, 243
human interface, 462
hunt teaming, 232–233
hybrid cloud, 193
hybrid SDN (software-defined networking), 64
hypervisor, 185
  Type 1, 186
  Type 2, 187

I

IaaS (infrastructure as a service), 195
IAST (interactive application security testing), 95
ICS (industrial control system), 462. *See also* protocol(s); SCADA (supervisory control and data acquisition)
  BACnet (Building Automation and Control Network), 464–465
  MITRE ATT&CK for, 245
  PLC (programmable logic controller), 463
    historian server, 463
    ladder logic, 463–464
  safety instrumented system, 464
identity management, 155
  federated, 156
  OpenID, 156–157
  SAML (Security Assertion Markup Language), 157–158
  transitive trust, 156
IDS (intrusion detection system), 3
  alerts, 258
  anomaly-based, 4
  host-based, 5, 451
  network, 5
  rule- or heuristic-based, 4
  rules, 267
  signature-based, 3–4
  wireless, 5
IKE (Internet Key Exchange), 534
images, 438
imaging tools, 405
  dd, 406
  FTK (Forensic Toolkit), 405–406
IMAP (Internet Message Access Protocol), 26
immutable systems, 352
IMPACT, 305
incident response, 368–369, 372
  analysis, 371
  automated, 374
    runbooks, 374–375
    SOAR, 375
  containment, 371
    isolate, 371
    minimize, 371
  detection, 370–371
  forensic process, 385
    evidence collection, 385–388
    identification, 385
  law enforcement and, 378–379
  legal vs. internal corporate purposes, 385
  lessons learned, 372
  non-automated response methods, 374
  plans, 664–665

preparation and, 369
recovery, 371–372
regulatory bodies and, 379
reporting requirements, 616
roles, 665–666
human resources, 377
internal and external stakeholders, 378
legal department, 377
public relations, 378
selecting team members, 377
senior leadership and, 379
testing, 370
training, 369–370
incremental backup, 136
indexing, 350
inherent risk, 567
injection attacks, 332
command, 337
LDAP, 335
process, 337
SQL, 335–336
XML, 332–334
input validation, 324
insider threats, 234
integer overflow, 318
integrating diverse industries
data considerations, 626–635
policies, 626
regulations, 626
rules and, 625–626
integration enablers, 101
directory services, 101
DNS (Domain Name System), 101–102
ESB (enterprise service bus), 103
SOA (service-oriented architecture), 102
integration testing, 108
integrity, 204, 205–206
Intel TXT (Trusted Execution Technology), 449
intellectual property, 630–631
copyright, 632
patent, 631
securing, 632–633
trade secret, 631–632
trademark, 632
interception attacks, 339
interface testing, 100
Internet gateway, 21
interpretation, 329
IoC (indicator of compromise), 251
alerts, 256
antivirus, 259–260
DLP, 257
FIM, 257
IDS/IPS, 258
SIEM, 257
logs, 252–253
access, 255–256
NetFlow, 256
network, 253–254
operating system, 254–255
vulnerability, 254
responses
ACL rules, 267
behavior rules, 268
DLP rules, 268
firewall rules, 265–266
IPS/IDS rules, 267
signature rules, 267
unusual process activity, 263–264
iOS, 432
jailbreaking, 431
remote wipe feature, 422
side loading, 431–432
Xcode 7, 432
IoT (Internet of Things), 206, 459–460
examples, 460
methods of securing devices, 461

IP video systems, 359–360
iPhone. *See* iOS
IPS (intrusion prevention system), 3–5, 6
  alerts, 258
  host-based, 451
  network, 6
  rules, 267
  wireless, 6
IPsec, 534
iptables, 265–266
iris scan, 421
ISA (interconnection security agreement), 650–651
ISACs (information sharing and analysis centers), 287
ISO (International Organization for Standardization), 283, 641–643
ISO/IEC 27005:2008, 587–588
IVRE, 243

J

Jad Debugger, 294
jailbreaking, 431
JavaSnoop, 294
job rotation, 596
John the Ripper, 306–307
JSON, 326
jump box, 43–44
jurisdictions, 615
JWT (JSON Web Token), 178–179

K

Kerberos, 165–166
kernel, 445
kernel proxy firewalls, 14
key agreement algorithms, 529
  Diffie-Hellman, 529
  ECDH (Elliptic-Curve Diffie-Hellman), 530
key management, 207–208, 481–482. *See also* PKI (public key infrastructure)
  accountability, 208, 482–483
  audits, 208, 483
  backups, 207
  phases, 484–485
  public and private keys, 508–511
  states, 483–484
  survivability, 208, 483
  troubleshooting, 546–549
key stretching, 536–537
keychain, router authentication, 25–26
knowledge factors, 169
KPIs (key performance indicators), 591–593
  availability, 593–594
  reliability, 593
  scalability, 593
KRIs (key risk indicators), 594

L

L2TP (Layer 2 Tunneling Protocol), 213
ladder logic, 463–464
LAN (local area network), 40
law enforcement, incident response and, 378–379
LDAP (Lightweight Directory Access Protocol), 164–165, 335
ldd command, 402, 410
least privilege, 597–598
legal compliance, 204
legal holds, 648
lessons-learned/after-action review, 297–298
libraries
  dependencies, 323–324
  standard software, 323
license technologies, 353
lighting, 358–359
likelihood, 556

limitations
of hashing, 392
of IDS (intrusion detection systems), 4–5
of NAC (network access control), 9
linking, 405
Linux
Bash, 356
cron command, 355–356, 357
dd command, 406
dig command, 242
file command, 403
foremost command, 399–400
hexdump utility, 401
iptables, 265–266
ldd command, 410
lsof command, 410
readelf command, 402
strace command, 402
strings command, 400–401
traceroute tool, 240
virtualization and, 186
vmstat command, 409–410
live collection tools
conntrack, 411
ldd command, 410
lsof command, 410
netcat, 410
netstat, 407–409
ps command, 409
tcpdump command, 411
vmstat command, 409–410
Wireshark, 412–413
live migration, 477
load balancers, 3
local drive encryption, 439
location services, 427
logs, 252–253, 350, 478–479
access, 255–256
alerts, 480
analysis, 390
configuration settings, 480
NetFlow, 256
network, 253–254
notifications, 260–261
operating system, 254–255
patch management and, 443
Syslog, 261–263
visitor, 359
vulnerability, 254
lsof command, 410

M

M2M (machine-to-machine) communication, 206
MAC (mandatory access control), 160
MAC (message authentication code), 392, 520, 521
MAC filters, 58
malware, 30
commodity, 231
ransomware, 373
managed configurations
airplane mode, 427
application control, 419
Bluetooth, 424
certificate management, 426–427
custom DNS, 428
DoH (DNS over HTTPS), 428
full device encryption, 427
geofencing, 425
geotagging, 426
location services, 427
MFA requirements, 420
facial scan, 421
fingerprint scan, 421
iris scan, 421
NFC (near-field communication), 424–425
over-the-air update, 422
passwords, 419–420
patch repository, 422
peripherals, 425
profiles, 424

remote wipe, 422–423
tethering, 427
token-based access, 421
VPN settings, 425–426
WiFi, 423
SCEP (Simple Certificate Enrollment Protocol), 423
WPA2/3, 423
management interfaces
in-band, 174
out-of-band, 174–175
mandatory access control, 444
kernel, 445
middleware, 445
SEAndroid, 444–445
SELinux (Security-Enhanced Linux), 444
mandatory vacation, 596–597
manual patch management, 284
manufacturing, 469–470. *See also* ICS (industrial control system)
masking, 132
MD5 (message-digest 5), 393, 520
MDM (mobile device management), 51, 424
measured boot, 449–450
media analysis, 389–390
memory
card, 169–170
encryption, 440–441
snapshots, 387
mergers and acquisitions, 60
cross-domain authentication, 61
data considerations, 626–635
data sensitivity levels, 59–60
due diligence team, 61
policies, 626
regulations, 626
message digest, 392, 393, 521
messages, Syslog, 261–263
messaging protocols
IMAP (Internet Message Access Protocol), 26
POP (Post Office Protocol), 27
SMTP (Simple Mail Transfer Protocol), 27
metadata, 130, 190
Metasploit, 305
MFA (multifactor authentication), 168
biometrics, 420
facial scan, 421
fingerprint scan, 421
iris scan, 421
microsegmentation, 40
Microsoft NAP (network access protection), 8
agent vs. agentless, 9
persistent and non-persistent agents, 9
quarantine/remediation, 9
middleware, 91–92, 190, 445, 468
military-grade encryption, 489–490
misuse case testing, 99
mitigate strategy, 566
MITRE
ATT&CK (Adversarial Tactics, Techniques, & Common Knowledge), 243–245
CVE (Common Vulnerabilities and Exposures) database, 90
ML (machine learning, 219, 220
mobile devices, 50–52
containerization, 432
deployment scenarios
BYOD (bring your own device), 429
COPE (corporate owned, personally enabled), 429
corporate-owned, 429
CYOD (choose your own device), 429
digital forensics, 430–431
ECC (elliptic curve cryptography), 209
jailbreaking, 431
managed configurations

airplane mode, 427
application control, 419
Bluetooth, 424
certificate management, 426–427
custom DNS, 428
DoH (DNS over HTTPS), 428
full device encryption, 427
geofencing, 425
geotagging, 426
location services, 427
MFA requirements, 420–421
NFC (near-field communication), 424–425
over-the-air update, 422
passwords, 419–420
patch repository, 422
peripherals, 425
profiles, 424
tethering, 427
token-based access, 421
VPN settings, 425–426
WiFi, 423
OEM (original equipment manufacturer), 432
remote wipe feature, 309, 422–423
ROTs (roots of trust), 176–177
side loading, 431–432
supply chain issues, 432
unauthorized application stores, 431
Modbus, 466
monitoring, 443–444
MOU (memorandum of understanding), 650
MSA (master service agreement), 649–650
MSSPs (managed security service providers), 505–506
MTBF (mean time between failure), 562
MTTR (mean time to recovery), 562
multidomain certificate, 502–503
multitenancy, 193–194
mutation fuzzing, 96, 297

N

NAC (network access control), 8. *See also* Microsoft NAP (network access protection)
advantages of, 10
lists, 47
nano technology, 225
NAT (network address translation), 19–20
dynamic, 21
static, 21
natural access control, 361
natural territorial reinforcement, 361
NDA (non-disclosure agreement), 650
need-to-know principle, 597
netcat, 410
netflow, 36–37, 256
netstat command, 407–409
network analysis, 390
network tap, 32
network traffic analysis, 130
NFC (near-field communication), 424–425
nfdump command, 37
NFS (Number Field Sieve), 531
NGFWs (next-generation firewalls), 14–15
NIDS (network intrusion detection system), 5
NIPS (network intrusion prevention system), 6
NIST (National Institute of Standards and Technology), 644
Framework for Improving Critical Infrastructure Cybersecurity, 585–587
Interagency Report 7924, "Reference Certificate Policy", 507–508
SP 800–24 Rev. 1, 657–658
SP 800–30, 568
SP 800–34 Rev. 1, 662

SP 800–37 Rev. 1, 581–583
SP 800–39, 583–585
SP 800–53 Rev. 4, 576–578
SP 800–57 Revision 5, 508–511
SP 800–60 Vol. 1 Rev. 1, 575–576
SP 800–82, 463
SP 800–160, 578–580
system life-cycle processes, 580–581
NLP (natural language processing), 225–226
Nmap, 302–303, 403
non-credentialed scans, 275–276
non-persistent agents, 9
non-repudiation, 204
NPV (net present value), 562
nslookup command, 242
NX (no-execute) bit, 439

O

OAuth, 166
obfuscation, 131, 548–549
anonymization, 132
data scrubbing, 131
masking, 132
tokenization, 131
objdump, 402
object-based storage, 197
OCSP (Online Certificate Status Protocol), 512–514
OEM (original equipment manufacturer), 432
OFB (output feedback), 524–525
OLA (operation-level agreement), 651
OllyDbg, 402
one-way hash, 392
open SDN (software-defined networking), 63
open standards, 638
OpenID, 156–157
operating systems. *See also* Linux
logs, 254–255
secure enclaves, 440
shared responsibility model and, 609
operational threat information, 232
threat emulation, 233
threat hunting, 232–233
orchestration, 75–76, 213
order of volatility, 386–387
organized crime, 235
OSA (Open System Authentication), 58
OSINT (open-source intelligence), 238–239
OSSTMM (Open Source Security Testing Methodology Manual), 588
OTP (one-time password), 175
HMAC-based, 175
time-based, 175–176
out-of-band interface, 174–175
outsourcing, 52–53
OVAL (Open Vulnerability and Assessment Language), 279
overflows, 315
buffer, 316–318
integer, 318
over-the-air update, 422
OWASP, ZAP (Zed Attack Proxy), 319
ownership factors, 169–170

P

P256/P384, 535
PaaS (platform as a service), 194
packet-filtering
dynamic, 13
firewalls, 12
PA-DSS (Payment Application Data Security Standard), 90
PAP (Password Authentication Protocol), 24–25
passive scanners, 278
passwordless authentication, 224–225
password(s). *See also* identity management
crackers, 306
Cain and Abel, 306

John the Ripper, 306–307
hash values, 393–394
mobile device, 419–420
one-time, 175
policies, 151–156
repository application, 149
end-user password storage, 149
on premises vs. cloud repository, 150
patch management, 283, 442
automated, 284
firmware, 442–443
logging and, 443
manual, 284
patch repository, 422
patents, 631
on-path attacks, 477–478
path tracing, 390
pattern matching, 4
payback, 561
PBKDF2 (Password-Based Key Derivation Function 2), 537
PCAP (packet capture), 251
protocol analyzers, 252
tshark command, 252
PCI DSS (Payment Card Industry Data Security Standard), 639–640
Peach, 97
Pearson Test Prep practice test software
accessing offline, 673–674
accessing online, 673
customizing your exams, 674–675
updating your exams, 675
peer review, 109
peering, 59
peer-to-peer networks, 49
PEnE (Policy Enforcement Engine), 176, 177
penetration testing
asset inventory, 308–309
corporate policy considerations, 310
facility considerations, 310
invasive vs. non-invasive, 308
permissions and access, 309–310
physical security considerations, 310
rescanning, 310
rules of engagement, 308
scope of work, 308
performance, 77–78
peripherals, 425
persistence attacks, 298
persistent agents, 9
PFE (private function evaluation), 221
PFS (perfect forward secrecy), 536
PGP (Pretty Good Privacy), 29, 211
pharming, 340
PHI (protected health information), 470
phishing, 340
physical security, 358
CPTED (Crime Prevention Through Environmental Design), 361
IP video systems, 359–360
lighting, 358–359
natural access control, 361
natural surveillance, 361
natural territorial reinforcement, 361
visitor logs, 359
physiological biometric systems, 170–171
PII (personally identifiable information), 633–634
PIN code, 420
PIR (private information retrieval), 221
pivoting, 297
PKI (public key infrastructure), 202, 210, 499
CA (certificate authority), 499–500
profiles, 507
RA (registration authority), 499
subordinate/intermediate CA, 500
use cases
email, 210
federation, 211–212
GPG (GNU Privacy Guard), 211

trust models, 212
web services, 210
PLA (privacy-level agreement), 651
placement
DAM (database activity monitoring), 351
firewall, 15–19
WAF (web application firewall), 7
PLCs (programmable logic controllers), 462, 463
historian server, 463
ladder logic, 463–464
PLD (programmable logic device), 461–462
policies, 38, 48, 595
change control, 614
conditional access, 419
contingency planning, 658
corporate, 310
employment and termination procedures, 598–599
job rotation, 596
mandatory vacation, 596–597
mergers and acquisitions, 626
password, 151–156
separation of duties, 595–596
social media, 239
Poly1305, 521
POP (Post Office Protocol), 27
port mirroring, 31
port scanners, 302–303
PowerShell, 357
PPP (Point-to-Point Protocol) encapsulation, 24
PPTP (Point-to-Point Tunneling Protocol), 213
preescalation tasks, 368
preventive controls, 351–352
hardening, 352
immutable systems, 352
sandbox detonation, 352–353
separation of duties, 595–596
PRI (product release information), 422
primary provider BCDR, 486
principle of least privilege, 597–598
print blocking, 126
privacy
anonymization, 132
impact assessment, 660
personal health information, 430
private cloud, 193
private keys, 508–511
privilege
escalation, 151
management, 151
PRL (preferred roaming list), 422
proactive and detection techniques, 347
developing countermeasures, 347
dynamic network configurations, 348
honeypots, 348
simulators, 348
process injection, 337
processing pipeline, 349
data, 349
stream, 349
profiles
MDM configuration, 424
PKI (public key infrastructure), 507
protective controls, 572
protocol(s)
analyzers, 252, 302
anomaly-based IDS (intrusion detection system), 4
authentication
802.1X, 166–167
Diameter, 164
EAP (Extensible Authentication Protocol), 167–168
Kerberos, 165–166
LDAP (Lightweight Directory Access Protocol), 164–165

MFA (multifactor authentication), 168
OAuth, 166
RADIUS (Remote Authentication Dial-in User Service), 162
TACACS (Terminal Access Controller Access Control System), 163–164
CAN (Controller Area Network), 465
CIP (Common Industrial Protocol), 467–468
Data Distribution Service, 468
decoy files, 348
DNP3 (Distributed Network Protocol 3), 466–467
IPsec, 534
messaging
IMAP (Internet Message Access Protocol), 26
POP (Post Office Protocol), 27
SMTP (Simple Mail Transfer Protocol), 27
Modbus, 466
OSCP (Online Certificate Status Protocol), 513–514
S/MIME (Secure MIME), 533
SSH (Secure Shell), 534–535
SSL (Secure Sockets Layer), 532–533
Syslog, 261–263
TLS (Transport Layer Security), 533
tunneling, 213
VPNs (virtual private networks) and, 10
Zigbee, 467
provisioning/deprovisioning, 189
proxy firewalls, 13
application-level, 13
circuit-level, 13
kernel, 14
ps command, 409
public cloud, 193
public keys, 508–511
public services, 470–471
Python, 357–358

Q

qualitative risk analysis, 557
quantitative risk analysis, 558
ALE (annualized loss expectancy), 563
ARO (annualized rate of occurrence), 563
asset value, 558–559
EF (exposure factor), 558
MTBF (mean time between failure), 562
MTTR (mean time to recovery), 562
NPV (net present value), 562
payback, 561
ROI (return on investment), 560–561
SLE (single loss of expectancy), 563–564
TCO (total cost of ownership), 559–560
quantum computing, 220
quarantine/remediation, Microsoft NAP (network access protection), 9

R

RA (registration authority), 499
race conditions, 315, 355
RADIUS (Remote Authentication Dial-in User Service), 162–163
RAID (redundant array of inexpensive disks), 138–142
rainbow table attack, 393
ransomware, 373
RBAC (role-based access control), 161
RDP (Remote Desktop Protocol), 126–127
readelf command, 402
recovery controls, 573
redundant hardware, 452

Regex Fuzzer, 97
regions, 49
regression, 107, 108–109, 324
regular expressions, 268
regulations, 637
  due diligence/due care, 646–647
  export controls, 647–648
  GDPR (General Data Protection Regulation), 640
  legal holds, 648
relevance, 388
reliability, 593
remote wipe, 422–423
remote work, 50
remote-access VPN (virtual private network), 11
Replicant, 461
replication, 76
reports, lessons-learned/after-action, 297–298
repositories, 93
residual risk, 567
resiliency, 74
  automation, 76
  autoscaling, 76
  bootstrapping, 77
  caching, 80
  CDN (content delivery network), 79–80
  clustering, 76
  distributed allocation, 76
  diversity, 75
  fault tolerance, 74–75
  HA (high availability), 75
  orchestration, 75–76
  replication, 76
REST (representational state transfer), 326
reverse engineering, 294
  Ghidra, 401
  hardware, 294–295
  software, 294
  tools, 294
reverse proxy, 22
revoked certificates, 543
Rijndael algorithm, 527
RIPEMD (RACE Integrity Primitives Evaluation Message Digest), 521
risk
  analysis. *See also* qualitative risk analysis; quantitative risk analysis
    qualitative, 557
    quantitative, 558
  appetite, 594
  assessment, 555–556
    impact, 556–557
    likelihood, 556
  exceptions, 567–568
  frameworks, 573. *See also* NIST (National Institute of Standards and Technology)
    COSO ERM Integrated Framework, 588–589
    FERMA (Federation of European Risk Management Associations), 589–590
    ISO/IEC 27005:2008, 587–588
    NIST, 574–587
    OSSTMM (Open Source Security Testing Methodology Manual), 588
  handling techniques, 565
    accept, 565
    avoid, 566
    mitigate, 566
    transfer, 565
  inherent, 567
  management lifecycle, 568–569
    assess, 570
    control, 570–573
    identify, 569–570
    review, 573

register, 590–591
  residual, 567
  tolerance, 594
  tracking, 590
rogue access points, 295
ROI (return on investment), 560–561
rooting, 431
rotation schemes, 136–137
ROTs (roots of trust), 176–177
routers, 22–23
  authentication, 24–26
  PPP (Point-to-Point Protocol) encapsulation, 24
routing table, 23–24, 239
RPO (recovery point objective), 659
RSA (Rivest, Shamir, and Adleman), 530–531
RTO (recovery time objective), 659
RTUs (remote terminal units), 462
rule- or heuristic-based IDS (intrusion detection system), 4
rule sets, 613
rule-based access control, 161
rules
  ACL, 267, 612–613
  behavior, 268
  DLP (data loss prevention), 268
  of engagement, 308
  firewall, 265–266
  IPS/IDS, 267
  signature, 267
  Snort, 258
RUM (real user monitoring), 99
runbooks, 374–375

S

SaaS (software as a service), 194
safety instrumented system, 464
Salsa20, 528
SAML (Security Assertion Markup Language), 157–158
sandbox(ing), 92–93
  detonation, 352–353
  escape, 337
SAST (static application security testing), 95
SCA (software composition analysis), 296
SCADA (supervisory control and data acquisition), 462–463
scalability, 73, 191, 593
  horizontal, 74
  vertical, 73–74
SCAP (Security Content Automation Protocol), 278, 298
  ARF (Asset Reporting Format), 282
  CCE (Common Configuration Enumeration), 282
  CPE (Common Platform Enumeration), 279
  CVE (Common Vulnerabilities and Exposures), 279
  CVSS (Common Vulnerability Scoring System), 279–282
  OVAL (Open Vulnerability and Assessment Language), 279
  XCCDF (Extensible Configuration Checklist Description Format), 278–279
SCEP (Simple Certificate Enrollment Protocol), 423
screened subnet, 44
script kiddie, 235
scrubbing, 131
SDN (software-defined networking), 62–63
  hybrid, 64
  open, 63
  overlay, 64–65
sealing, 446
SEAndroid, 444–445. *See also* Android
search engines, threat intelligence information and, 242–243

searching, 350
sectors
  energy, 469
  facility services, 471
  healthcare, 470
  manufacturing, 469–470
  public services, 470–471
  public utilities, 470
secure boot, 446–447
secure coding standards, 89–90
  application vetting process, 90–91
  CVE (Common Vulnerabilities and Exposures) database, 90
  DISA STIGs, 90
  PA-DSS (Payment Application Data Security Standard), 90
secure enclaves, 440
security
  accreditation, 638
  analytics, 348–349
  automation, 77, 355–356
  awareness training, 369–370, 599–601
  baselines, 438
  controls, 556–557, 570–572
  by default, 87
  by deployment, 87
  by design, 87
  frameworks, 243
    Cyber Kill Chain, 246
    Diamond Model of Intrusion Analysis, 245
    MITRE ATT&CK (Adversarial Tactics, Techniques, & Common Knowledge), 243–245
  legal compliance, 204
  misconfiguration, 319–320
  mobile, 209
  physical
    CPTED (Crime Prevention Through Environmental Design), 361
    IP video systems, 359–360
    lighting, 358–359
    natural access control, 361
    natural surveillance, 361
    natural territorial reinforcement, 361
  templates, 86–87
  wireless network, 56
    MAC filter, 58
    OSA (Open System Authentication), 58
    SKA (Shared Key Authentication), 58
    SSID broadcast, 57
    WPA (Wi-Fi Protected Access), 56, 57
    WPA3 (Wi-Fi Protected Access 3), 57
SEDs (self-encrypted drives), 450
segmentation, 39
  ACLs (access control lists), 49
  air gap, 49
  availability zone, 46–47
  cloud, 50
  data zones, 44–45
  deperimeterization, 49–50
  guest environments, 45
  jump box, 43–44
  LAN (local area network), 40
  micro, 40
  mobile, 50–52
  peer-to-peer networks, 49
  regions, 49
  remote work, 50
  screened subnet, 44
  staging environments, 45
  VLAN (virtual local area network), 40–41
    hopping, 42–43
    trunk links, 41–42
  VPC (virtual private cloud), 46
  VPN (virtual private network), 45–46
  wireless network, 53
    APs (access points), 53

infrastructure mode vs. ad hoc mode, 54
SSID (service set identifier), 53
zero trust, 49–50
self-assessment, 283
self-healing hardware, 452
self-signed certificates, 544–545
SELinux (Security-Enhanced Linux), 444
sensors, 32, 462
antivirus, 39
DLP (data loss prevention), 37–38
FIM (file integrity monitoring), 35–36
netflow, 36–37
SIEM (security information and event management), 33–34
advantages and disadvantages of, 35
agent-based collection, 33
agentless collection, 33
log sources, 34
when to use, 35
SNMP (Simple Network Management Protocol) traps, 36
separation of duties, 595–596
server-based
application virtualization, 189
vulnerability scanning, 276–277
serverless computing, 486–487
server-side processing, 325–326
services
DNSSEC (Domain Name System Security Extensions), 11
firewalls, 12
advantages of, 14
deep packet inspection, 19
NGFWs (next-generation firewalls), 14–15
packet-filtering, 12
placement, 15–19
proxy, 13–14
stateful, 12
IDS (intrusion detection system), 3
anomaly-based, 4
limitations of, 4–5
network, 5
rule- or heuristic-based, 4
signature-based, 3–4
wireless, 5
IPS (intrusion prevention system), 6
network, 6
wireless, 6
Microsoft NAP (network access protection)
agent vs. agentless, 9
persistent and non-persistent agents, 9
quarantine/remediation, 9
NAC (network access control), 8, 10
NAT (network address translation), 19–20
dynamic, 21
stateful, 20
static, 21
UTM (unified threat management), 11
VPN (virtual private network), 10–11
WAF (web application firewall), 6–7
wireless network
WEP (Wired Equivalent Privacy, 56
WPA2 (Wi-Fi Protected Access 2, 57
SFC command, 35–36
SFE (secure function evaluation), 221
SHA (Secure Hashing Algorithm), 519–520
sha256sum, 407
shared credentials, 619
shared responsibility model, 607
client, 609
application, 609
data, 609
encryption, 609
operating systems, 609

cloud service provider, 607
compute resources, 608
geographic location, 608
infrastructure, 608
services, 608–609
shell restrictions, 441
Shibboleth, 158
Shodan, 243
shoulder surfing, 341
side loading, 431–432
side-channel analysis, 293
SIEM (security information and event management), 33–34, 479
advantages and disadvantages of, 35
agent-based collection, 33
agentless collection, 33
log sources, 34
Snort, 258
when to use, 35
signature rules, 267
signature-based IDS (intrusion detection system), 3–4
simulators, 348
single-tenancy, 194
site-to-site VPN (virtual private network), 11
SKA (Shared Key Authentication), 58
slack space analysis, 390
SLAs (service-level agreements), 478, 607, 649
SLE (single loss of expectancy), 563–564
Sleuth Kit, 405
smart cards, 170, 209–210
S/MIME (Secure MIME), 210, 533
SMTP (Simple Mail Transfer Protocol), 27
sniffers, 302, 412–413. *See also* protocol analyzers
SNMP (Simple Network Management Protocol), 36
Snort, 258
SOA (service-oriented architecture), 102
SOAP (Simple Object Access Protocol), 206, 329
SOAR (security orchestration, automation, and response), 77, 375
SoC (system on a chip), 461
social engineering attacks, 340, 374
dumpster diving, 341
identity theft, 341
pharming, 340
phishing, 340
shoulder surfing, 341
spear phishing, 28
whaling, 28
social media, threat intelligence information and, 238–239
software, 91–92. *See also* testing
analysis, 390
assurance, 92
composition analysis, 322–323
fielding, 104
insertions, 104
libraries, 481, 612
modules, 323
patch management, 283
automated, 284
manual, 284
reverse engineering, 294
sandboxing, 92–93
upgrades, 104
validating third-party libraries, 93
Waterfall model, 113
software development
Agile, 109–110, 111, 112–113
DevSecOps, 109
spiral model, 111–112, 114
versioning, 114–116
Waterfall method, 110
software engineering
CD (continuous delivery), 116
CI (continuous integration), 116

formal methods, 103
source code escrows, 616
spam, 28–29
SPAN (switched port analyzer) ports, 31
spear phishing, 28
SPF (Sender Policy Framework), 27
spiral model, 111–112, 114
spoofing, email, 27
SQL (Structured Query Language) injection, 335–336
SRTM (security requirements traceability matrix), 103
ssdeep, 407
SSH (Secure Shell), 534–535
SSHDroid, 445
SSID (service set identifier), 53
SSL (Secure Sockets Layer), 212, 532–533
SSO (single sign-on), 157, 177–178
staging environments, 45
stakeholder management
best practices, 375–376
selecting the incident response team, 377
standard software library, 323
standards, 637–638
adherence to, 638
competing, 639
de facto, 639
ISO (International Organization for Standardization), 641–643
lack of, 639
open, 638
PCI DSS (Payment Card Industry Data Security Standard), 639–640
STAR (Security Trust Assurance and Risk), 646
stateful
firewalls, 12
matching, 4
NAT (network address translation), 20
static
analysis, 293
linking, 405
NAT (network address translation), 21
testing, 98
statistical anomaly-based IDS (intrusion detection system), 4
steganalysis, 390, 394
steganography, 129
storage
backup, 136
bit splitting, 493
blob, 198
block, 198
collaboration tools, 491–492
configurations, 492
database, 197–198
design patterns, 87–88
evidence, 389
file-based, 197
object-based, 197
password repository application
end-user password storage, 149
on premises vs. cloud repository, 150
RAID (redundant array of inexpensive disks), 138–142
replication, 76
smart cards, 209–210
USB, controlling the use of, 125–126
strace, 402
strategic threat information, 232
stream pipeline, 349
stream-based ciphers, 526–527
strings command, 400–401
Stuxnet virus, 462
subordinate/intermediate CA, 500
supply chain, 615–616
surveillance, natural, 361
survivability, key management, 483
swipe patterns, 420
switches, SFC command, 35–36

symmetric algorithms, 522
3DES (Triple Digital Encryption Standard), 528
AES (Advanced Encryption Standard), 527
DES
CBC (cipher block chaining), 524
CTR (Counter), 525
ECB (electronic codebook), 523
GCM (Galois/Counter Mode), 525–526
OFB (output feedback), 524–525
SYN flood, 339
synthetic transaction monitoring, 98–99
Sysinternals, 264
Syslog, 261–263
system apps, 431
system image, 388

T

TACACS (Terminal Access Controller Access Control System), 163–164
tactical threat information, 231
tags, 190
tampering, 309
targeted attacks, 232
Task Manager, 263–264
TCO (total cost of ownership), 50, 559–560
tcpdump command, 411
teardrop attack, 340
telecommuting, 50
telemetry system, 462
templates, 86–87, 105–107, 438
test coverage analysis, 99–100
testing
acceptance, 107
DAST (dynamic application security testing), 95
dynamic, 98–99
fuzz, 95–97, 296–297
IAST (interactive application security testing), 95
incident response and, 370
integration, 108
interface, 100
misuse case, 99
peer review, 109
plans, 105
regression, 107, 108–109
SAST (static application security testing), 95
software composition analysis, 322–323
static, 98
technical, 618
templates, 105–107
unit, 107–108
user acceptance, 108
validation, 107
tethering, 427
third-party
assessment, 283
dependencies, 616
code, 617
hardware, 617
mitigating risks, 618–619
modules, 618
libraries, validating, 93
threat intelligence information, 231. *See also* actors
collection methods
DNS records, 239–242
routing tables, 239
search engines, 242–243
operational, 232
threat emulation, 233
threat hunting, 232–233
sources, 237
advisories, 285
bulletins, 286
deep web, 237–238
intelligence feeds, 237
ISACs, 287

news reports, 287
OSINT (open-source intelligence), 238–239
proprietary, 238
vendor websites, 287
strategic, 232
tactical, 231
TLS (Transport Layer Security), 212, 533
token device, 169
token-based access, 421
tokenization, 131
tools
analysis
Aircrack-ng, 403–404
ExifTool, 403
Nmap, 403
Sleuth Kit, 405
Volatility, 404
binary analysis, 401
binwalk, 401
file command, 403
GDB (GNU Project debugger), 401
Ghidra, 401
hexdump, 401
ldd, 402
objdump, 402
OllyDbg, 402
readelf, 402
strace, 402
Censys, 243
collaboration, 488
audio conferencing, 491
storage and document, 491–492
video conferencing, 489–491
web conferencing, 488–489
dependency management, 308
eFuse, 432
exploit frameworks, 304–305
file carving, 399
foremost command, 399–400
strings command, 400–401
for final preparation, 672
chapter-ending review, 676
Pearson Test Prep practice test software, 672
fuzzers, 96–97
hashing, 407
sha256sum, 407
ssdeep, 407
HTTP interceptors, 304
imaging, 405
dd, 406
FTK (Forensic Toolkit), 405–406
live collection
conntrack, 411
ldd command, 410
lsof command, 410
netcat, 410
netstat, 407–409
ps command, 409
tcpdump command, 411
vmstat command, 409–410
Wireshark, 412–413
password crackers, 306
Cain and Abel, 306
John the Ripper, 306–307
port scanners, 302–303
PowerShell, 357
protocol analyzers, 302
reverse engineering, 294
SCA (software composition analysis), 296
SCAP (Security Content Automation Protocol) scanner, 298
SIEM (security information and event management), 479
Snort, 258
Task Manager, 263–264
traceroute/tracert, 240
traffic analyzers, 299
vendor assessment, 616
vulnerability scanners, 300–301
Windows Software Licensing Management, 353

WLAN vulnerability scanners, 295
TOTP (time-based one-time password), 175–176
TPM (Trusted Platform Module) chip, 179, 445–446
traceroute tool, 240
tracert, 240
trade secret, 631–632
trademark, 632
tradeoff analysis, 595
traffic analyzers, 299
traffic anomaly-based IDS (intrusion detection system), 4
traffic mirroring, 30
network tap, 32
port mirroring, 31
SPAN (switched port analyzer) ports, 31
VPC (virtual private cloud), 32
training, security awareness, 369–370, 599–601
transaction log backups, 136
Transaction Signature (TSIG), 11
transfer strategy, 565
transitive trust, 156
transmission control, 618–619
triage event, 367–368
troubleshooting
certificates
chain issues, 544–545
incorrect name, 543–544
revoked, 543
validity dates, 542
wrong type, 543
cryptography
cipher mismatches, 546
cipher suites, 545
incorrect permissions, 546
keys, 546–549
weak signing algorithm, 545
true negative, 367
true positive, 367
trunk links, 41–42
trust models, 212, 506
Trusted Foundry program, 616
trusted providers, 505–506
trustworthy computing
attestation, 448
HSM (hardware security module), 448–449
measured boot, 449–450
secure boot, 446–447
SEDs (self-encrypted drives), 450
TPM (Trusted Platform Module) chip, 445–446
UEFI (Unified Extensible Firmware Interface), 447–448
tshark command, 252
tunneling protocols, 213
two-factor authentication, 168
Type 1 hypervisor, 186
Type 2 hypervisor, 187

U

UEBA (user and entity behavior analytics), 452
UEFI (Unified Extensible Firmware Interface), 447–448
United States, COPPA (Children's Online Privacy Protection Act), 644
unsigned applications, 431
unstructured data, 222–223
updates
over-the-air, 422
PRI (product release information), 422
PRL (preferred roaming list), 422
US EPA (Environmental Protection Agency), 567–568
US NSA (National Security Agency), 489–490
usability, 595
USB devices, controlling the use of, 125–126

user acceptance testing, 108
utilities, 470
UTM (unified threat management), 11

V

validating third-party libraries, 93
validation testing, 107
VDI (virtual desktop infrastructure), 128, 189
vendor(s)
  assessment tools, 616
  geographical considerations, 615
  lock-in/lock-out, 610
  meeting client requirements, 610
    change management, 611
    configuration management, 611–612
    device and technical configurations, 612–615
    legal, 610–611
    staff turnover, 612
  source code escrows, 616
  supply chain, 615–616
  support availability, 615
  third-party dependencies, 616
    code, 617
    hardware, 617
    modules, 618
  viability, 610
verification, of backups, 391
versioning, 114–116
vertical scaling, 73–74
video conferencing, 489–491
virtualization, 79, 186
  advantages of, 185
  application, 189
  containers, 187–188
  CPU, 439–440
  emulation, 188
  hypervisor, 185
    Type 1, 186
    Type 2, 187
  on Linux machines, 186
  provisioning/deprovisioning, 189
  VM (virtual machine), 185
visitor logs, 359
VLAN (virtual local area network), 11, 40–41
  hopping, 42–43
  trunk links, 41–42
VM (virtual machine), 92–93, 185
  escape, 337–338
  hopping, 337
  live migration, 477
  sandbox escape, 337
vmstat command, 409–410
Volatility, 404
VPC (virtual private cloud), 32, 46, 196
VPN (virtual private network), 10–11, 45–46, 212
  IPsec, 534
  PFS (perfect forward secrecy), 536
  remote-access, 11
  settings, 425–426
  site-to-site, 11
  SSL (Secure Sockets Layer), 212
  TLS (Transport Layer Security), 212
  tunneling protocols, 213
VR (virtual reality), 223–224
vulnerability(ies), 315
  AJAX (Asynchronous JavaScript and XML), 327–328
  assessment
    corporate policy considerations, 310
    facility considerations, 310
    invasive vs. non-invasive, 308
    permissions and access, 309–310
    physical security considerations, 310
    rescanning, 310
    scope of work, 308
  broken authentication, 318–319
  browser extensions, 326
    ActiveX, 327
    Flash, 327
  certificate errors, 321

end of support/end of life, 324
frameworks, 323
HTML5 (Hypertext Markup Language 5), 327
improper headers, 320
information disclosure, 321
logs, 254
overflow, 315
  buffer, 316–318
  integer, 318
poor exception handling, 319
race conditions, 315
regression issues, 324
rules of engagement, 308
scans, 275, 300–301. *See also* event classifications
  active, 278
  agent-based, 276–277
  cloud-based, 300
  credentialed, 275–276
  criticality ranking, 277
  CVSS (Common Vulnerability Scoring System), 279–282
  non-credentialed, 275–276
  passive, 278
  premises-based, 300–301
  SCAP (Security Content Automation Protocol), 278
  server-based, 276–277
  wireless, 295
  XCCDF (Extensible Configuration Checklist Description Format), 278–279
security misconfiguration, 319–320
SOAP (Simple Object Access Protocol), 329
unsafe functions, 323
unsecure references, 319
weak ciphers, 322, , 322
weak cryptography implementations, 321–322

W

WAF (web application firewall), 6–7
warm site, 663
Waterfall model, 110, 113
watermarking, 129
wearable devices, security issues
  encrypted and unencrypted communication, 430
  health privacy, 430
  personal data theft, 430
  physical reconnaissance, 430
  unauthorized remote activation/deactivation of devices or features, 430
web conferencing, 488–489
web security, 206
  HTTP (Hypertext Transfer Protocol) headers, 117–118
  OWASP (Open Web Application Security Project), 117
websites, OWASP, 117
WEP (Wired Equivalent Privacy, 56
whaling, 28
WhatsUp Gold, 299
white hat, 236
WIDS (wireless intrusion detection system), 5
WiFi, 423
  SCEP (Simple Certificate Enrollment Protocol), 423
  WPA2/3, 423
wildcard certificate, 501
Windows
  Group Policy. *See* Group Policy
  Task Manager, 263–264
WIPS (wireless intrusion prevention system), 6
wireless networks
  802.11
    APs (access points), 53

infrastructure mode vs. ad hoc mode, 54
SSID (service set identifier), 53
security, 56
MAC filter, 58
OSA (Open System Authentication), 58
SKA (Shared Key Authentication), 58
SSID broadcast, 57
WEP (Wired Equivalent Privacy, 56
WPA (Wi-Fi Protected Access), 56, 57
WPA2 (Wi-Fi Protected Access 2, 57
WPA3 (Wi-Fi Protected Access 3), 57
standards
802.11a, 54
802.11ac, 55
802.11ax, 55
802.11b, 54
802.11f, 54
802.11g, 55
802.11n, 55
Wireshark, 412–413
WPA (Wi-Fi Protected Access), 56, 57
WPA2 (Wi-Fi Protected Access 2, 57, 423
WPA3 (Wi-Fi Protected Access 3), 57, 423
WSS (Web Services Security), 206

X-Y

X.500, 164
X.509 certificate, 503
CN (Common Name), 505
SAN (Subject Alternative Name), 505
XACML (Extensible Access Control Markup Language), 130–131
XCCDF (Extensible Configuration Checklist Description Format), 278–279
Xcode 7, 432
XML (Extensible Markup Language), 30, 332–334
XN (never execute) bit, 439
XSS (cross-site scripting) attacks, 331

Z

ZAP (Zed Attack Proxy), 319
Zenmap, 302–303
zero trust, 49–50
Zigbee, 467