

CompTIA® Cybersecurity Analyst (CSA+) Cert Guide

Troy McMillan

PEARSON

800 East 96th Street
Indianapolis, Indiana 46240 USA

CompTIA Cybersecurity Analyst (CSA+) Cert Guide

Copyright © 2017 by Pearson Education, Inc.

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

ISBN-13: 978-0-7897-5695-4

ISBN-10: 0-7897-5695-1

Library of Congress Control Number: 2017938509

Printed in the United States of America

First Printing: June 2017

Trademarks

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

Warning and Disclaimer

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

Special Sales

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

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

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

Editor-in-Chief

Mark Taub

Product Line Manager

Brett Bartow

Acquisitions Editor

Michelle Newcomb

Development Editor

Ellie Bru

Managing Editor

Sandra Schroeder

Senior Project Editor

Tonya Simpson

Copy Editor

Kitty Wilson

Indexer

Publishing Works, Inc.

Proofreader

Chuck Hutchinson

Technical Editors

Chris Crayton

Robin Abernathy

Publishing Coordinator

Vanessa Evans

Cover Designer

Chuti Prasertsith

Composer

Bronkella Publishing

Contents at a Glance

	Introduction	xxvii
CHAPTER 1	Applying Environmental Reconnaissance Techniques	3
CHAPTER 2	Analyzing the Results of Network Reconnaissance	37
CHAPTER 3	Recommending and Implementing the Appropriate Response and Countermeasure	69
CHAPTER 4	Practices Used to Secure a Corporate Environment	95
CHAPTER 5	Implementing an Information Security Vulnerability Management Process	113
CHAPTER 6	Analyzing Scan Output and Identifying Common Vulnerabilities	141
CHAPTER 7	Identifying Incident Impact and Assembling a Forensic Toolkit	187
CHAPTER 8	The Incident Response Process	213
CHAPTER 9	Incident Recovery and Post-Incident Response	237
CHAPTER 10	Frameworks, Policies, Controls, and Procedures	251
CHAPTER 11	Remediating Security Issues Related to Identity and Access Management	301
CHAPTER 12	Security Architecture and Implementing Compensating Controls	343
CHAPTER 13	Application Security Best Practices	385
CHAPTER 14	Using Cybersecurity Tools and Technologies	403
CHAPTER 15	Final Preparation	453
APPENDIX A	Answers to the “Do I Know This Already?” Quizzes and Review Questions	459
	Glossary	491
	Index	526

Table of Contents

Introduction	xxvii
Chapter 1 Applying Environmental Reconnaissance Techniques	3
“Do I Know This Already?” Quiz	3
Foundation Topics	5
Procedures/Common Tasks	5
Topology Discovery	5
OS Fingerprinting	5
Service Discovery	6
Packet Capture	6
Log Review	6
Router/Firewall ACLs Review	6
E-mail Harvesting	7
Social Media Profiling	7
Social Engineering	8
DNS Harvesting	8
Phishing	11
Variables	11
Wireless vs. Wired	12
Virtual vs. Physical	13
Internal vs. External	14
On-premises vs. Cloud	15
Tools	16
Nmap	16
Host Scanning	19
Network Mapping	20
Netstat	21
Packet Analyzer	23
IDS/IPS	25
HIDS/NIDS	27
Firewall Rule-Based and Logs	27
<i>Firewall Types</i>	27
<i>Firewall Architecture</i>	29
Syslog	30
Vulnerability Scanner	30

Exam Preparation Tasks	31
Review All Key Topics	31
Define Key Terms	32
Review Questions	32
Chapter 2 Analyzing the Results of Network Reconnaissance	37
“Do I Know This Already?” Quiz	37
Foundation Topics	40
Point-in-Time Data Analysis	40
Packet Analysis	40
Protocol Analysis	40
Traffic Analysis	40
NetFlow Analysis	41
Wireless Analysis	43
<i>CSMA/CA</i>	43
Data Correlation and Analytics	45
Anomaly Analysis	45
Trend Analysis	46
Availability Analysis	46
Heuristic Analysis	46
Behavioral Analysis	47
Data Output	47
Firewall Logs	47
Packet Captures	49
Nmap Scan Results	52
<i>Port Scans</i>	52
Event Logs	53
Syslog	55
IDS Report	56
Tools	57
SIEM	57
Packet Analyzer	59
IDS	60
Resource Monitoring Tool	61
NetFlow Analyzer	61
Exam Preparation Tasks	62

Review All Key Topics 62

Define Key Terms 63

Review Questions 63

Chapter 3 **Recommending and Implementing the Appropriate Response and Countermeasure 69**

“Do I Know This Already?” Quiz 69

Foundation Topics 72

Network Segmentation 72

LAN 72

Intranet 72

Extranet 72

DMZ 73

VLANs 73

System Isolation 75

Jump Box 76

Honeypot 77

Endpoint Security 77

Group Policies 78

ACLs 80

Sinkhole 81

Hardening 82

Mandatory Access Control (MAC) 82

Compensating Controls 83

Control Categories 83

Access Control Types 84

Administrative (Management) Controls 85

Logical (Technical) Controls 85

Physical Controls 85

Blocking Unused Ports/Services 86

Patching 86

Network Access Control 86

Quarantine/Remediation 88

Agent-Based vs. Agentless NAC 88

802.1x 88

Exam Preparation Tasks 90

	Review All Key Topics	90
	Define Key Terms	91
	Review Questions	91
Chapter 4	Practices Used to Secure a Corporate Environment	95
	“Do I Know This Already?” Quiz	95
	Foundation Topics	98
	Penetration Testing	98
	Rules of Engagement	100
	Reverse Engineering	101
	Isolation/Sandboxing	101
	Hardware	103
	Software/Malware	104
	Training and Exercises	105
	Risk Evaluation	106
	Technical Impact and Likelihood	106
	Technical Control Review	107
	Operational Control Review	107
	Exam Preparation Tasks	107
	Review All Key Topics	108
	Define Key Terms	108
	Review Questions	108
Chapter 5	Implementing an Information Security Vulnerability Management Process	113
	“Do I Know This Already?” Quiz	113
	Foundation Topics	117
	Identification of Requirements	117
	Regulatory Environments	117
	Corporate Policy	119
	Data Classification	119
	Asset Inventory	120
	Establish Scanning Frequency	120
	Risk Appetite	120
	Regulatory Requirements	121
	Technical Constraints	121
	Workflow	121

Configure Tools to Perform Scans According to Specification	122
Determine Scanning Criteria	122
<i>Sensitivity Levels</i>	122
<i>Vulnerability Feed</i>	123
<i>Scope</i>	123
<i>Credentialed vs. Non-credentialed</i>	125
<i>Types of Data</i>	126
<i>Server-Based vs. Agent-Based</i>	126
Tool Updates/Plug-ins	128
SCAP	128
Permissions and Access	131
Execute Scanning	131
Generate Reports	132
Automated vs. Manual Distribution	132
Remediation	133
Prioritizing	133
<i>Criticality</i>	134
<i>Difficulty of Implementation</i>	134
Communication/Change Control	134
Sandboxing/Testing	134
Inhibitors to Remediation	134
MOUs	134
SLAs	135
<i>Organizational Governance</i>	135
<i>Business Process Interruption</i>	135
<i>Degrading Functionality</i>	135
Ongoing Scanning and Continuous Monitoring	135
Exam Preparation Tasks	136
Review All Key Topics	136
Define Key Terms	136
Review Questions	137
Chapter 6 Analyzing Scan Output and Identifying Common Vulnerabilities	141
“Do I Know This Already?” Quiz	141
Foundation Topics	143

Analyzing Output Resulting from a Vulnerability Scan	143
Analyze Reports from a Vulnerability Scan	143
<i>Review and Interpret Scan Results</i>	145
Validate Results and Correlate Other Data Points	147
Common Vulnerabilities Found in Targets Within an Organization	148
Servers	148
<i>Web Servers</i>	149
<i>Database Servers</i>	160
Endpoints	161
Network Infrastructure	162
<i>Switches</i>	163
<i>MAC Overflow</i>	164
<i>ARP Poisoning</i>	164
<i>VLANs</i>	165
<i>Routers</i>	168
Network Appliances	169
Virtual Infrastructure	169
<i>Virtual Hosts</i>	169
<i>Virtual Networks</i>	170
<i>Management Interface</i>	171
Mobile Devices	173
Interconnected Networks	174
Virtual Private Networks	175
Industrial Control Systems/SCADA Devices	179
Exam Preparation Tasks	180
Review All Key Topics	181
Define Key Terms	182
Review Questions	182
Chapter 7 Identifying Incident Impact and Assembling a Forensic Toolkit	187
“Do I Know This Already?” Quiz	187
Foundation Topics	189
Threat Classification	189
Known Threats vs. Unknown Threats	190
Zero Day	190
Advanced Persistent Threat	191

Factors Contributing to Incident Severity and Prioritization	191
Scope of Impact	191
<i>Downtime and Recovery Time</i>	191
<i>Data Integrity</i>	193
<i>Economic</i>	193
<i>System Process Criticality</i>	193
Types of Data	194
<i>Personally Identifiable Information (PII)</i>	194
<i>Personal Health Information (PHI)</i>	195
<i>Payment Card Information</i>	195
<i>Intellectual Property</i>	197
<i>Corporate Confidential</i>	199
Forensics Kit	201
Digital Forensics Workstation	202
Forensic Investigation Suite	206
Exam Preparation Tasks	208
Review All Key Topics	208
Define Key Terms	208
Review Questions	209
Chapter 8 The Incident Response Process	213
“Do I Know This Already?” Quiz	213
Foundation Topics	216
Stakeholders	216
HR	216
Legal	217
Marketing	217
Management	217
Purpose of Communication Processes	217
Limit Communication to Trusted Parties	218
Disclosure Based on Regulatory/Legislative Requirements	218
Prevent Inadvertent Release of Information	218
Secure Method of Communication	218
Role-Based Responsibilities	218
Technical	219
Management	219

Law Enforcement	219
Retain Incident Response Provider	220
Using Common Symptoms to Select the Best Course of Action to Support Incident Response	220
Common Network-Related Symptoms	220
<i>Bandwidth Consumption</i>	221
<i>Beaconing</i>	221
<i>Irregular Peer-to-Peer Communication</i>	222
<i>Rogue Devices on the Network</i>	223
<i>Scan Sweeps</i>	224
<i>Unusual Traffic Spikes</i>	225
Common Host-Related Symptoms	225
<i>Processor Consumption</i>	226
<i>Memory Consumption</i>	227
<i>Drive Capacity Consumption</i>	227
<i>Unauthorized Software</i>	228
<i>Malicious Processes</i>	229
<i>Unauthorized Changes</i>	229
<i>Unauthorized Privileges</i>	229
<i>Data Exfiltration</i>	229
Common Application-Related Symptoms	230
<i>Anomalous Activity</i>	230
<i>Introduction of New Accounts</i>	231
<i>Unexpected Output</i>	231
<i>Unexpected Outbound Communication</i>	231
<i>Service Interruption</i>	231
<i>Memory Overflows</i>	231
Exam Preparation Tasks	232
Review All Key Topics	232
Define Key Terms	232
Review Questions	233
Chapter 9 Incident Recovery and Post-Incident Response	237
“Do I Know This Already?” Quiz	237
Foundation Topics	240

Containment Techniques	240
Segmentation	240
Isolation	240
Removal	241
Reverse Engineering	241
Eradication Techniques	242
Sanitization	242
Reconstruction/Reimage	242
Secure Disposal	242
Validation	243
Patching	243
Permissions	244
Scanning	244
Verify Logging/Communication to Security Monitoring	244
Corrective Actions	245
Lessons Learned Report	245
Change Control Process	245
Update Incident Response Plan	245
Incident Summary Report	246
Exam Preparation Tasks	246
Review All Key Topics	246
Define Key Terms	247
Review Questions	247
Chapter 10 Frameworks, Policies, Controls, and Procedures	251
“Do I Know This Already?” Quiz	251
Foundation Topics	254
Regulatory Compliance	254
Frameworks	258
National Institute of Standards and Technology (NIST)	258
Framework for Improving Critical Infrastructure Cybersecurity	259
ISO	260
Control Objectives for Information and Related Technology (COBIT)	263
Sherwood Applied Business Security Architecture (SABSA)	265
The Open Group Architecture Framework (TOGAF)	265
Information Technology Infrastructure Library (ITIL)	267

Policies	268
Password Policy	268
Acceptable Use Policy (AUP)	271
Data Ownership Policy	272
Data Retention Policy	272
Account Management Policy	273
Data Classification Policy	274
<i>Sensitivity and Criticality</i>	275
<i>Commercial Business Classifications</i>	276
<i>Military and Government Classifications</i>	276
Controls	277
Control Selection Based on Criteria	278
<i>Handling Risk</i>	278
Organizationally Defined Parameters	281
Access Control Types	282
Procedures	284
Continuous Monitoring	284
Evidence Production	285
Patching	285
Compensating Control Development	286
Control Testing Procedures	286
Manage Exceptions	287
Remediation Plans	287
Verifications and Quality Control	288
Audits	288
Evaluations	290
Assessments	290
Maturity Model	291
<i>CMMI</i>	291
Certification	291
<i>NIACAP</i>	292
<i>ISO/IEC 27001</i>	292
<i>ISO/IEC 27002</i>	294
Exam Preparation Tasks	294
Review All Key Topics	294

Define Key Terms 295

Review Questions 296

Chapter 11 Remediating Security Issues Related to Identity and Access Management 301

“Do I Know This Already?” Quiz 301

Foundation Topics 304

Security Issues Associated with Context-Based Authentication 304

Time 304

Location 304

Frequency 305

Behavioral 305

Security Issues Associated with Identities 305

Personnel 306

Employment Candidate Screening 306

Employment Agreement and Policies 308

Periodic Review 308

Proper Credential Management 308

Creating Accountability 309

Maintaining a Secure Provisioning Life Cycle 309

Endpoints 310

Social Engineering Threats 310

Malicious Software 311

Rogue Endpoints 311

Rogue Access Points 312

Servers 312

Services 313

Roles 315

Applications 316

IAM Software 316

Applications as Identities 317

OAuth 318

OpenSSL 319

Security Issues Associated with Identity Repositories 319

Directory Services 319

LDAP 319

Active Directory (AD) 320

<i>SESAME</i>	321
<i>DNS</i>	322
TACACS+ and RADIUS	323
Security Issues Associated with Federation and Single Sign-on	325
Identity Propagation	326
Federations	327
XACML	327
SPML	329
SAML	330
OpenID	331
Shibboleth	332
Manual vs. Automatic Provisioning/Deprovisioning	333
Self-Service Password Reset	334
Exploits	334
Impersonation	334
Man-in-the-Middle	334
Session Hijack	335
Cross-Site Scripting	335
Privilege Escalation	335
Rootkit	335
Exam Preparation Tasks	336
Review All Key Topics	336
Define Key Terms	337
Review Questions	338
Chapter 12 Security Architecture and Implementing Compensating Controls	343
“Do I Know This Already?” Quiz	343
Foundation Topics	346
Security Data Analytics	346
Data Aggregation and Correlation	346
Trend Analysis	346
Historical Analysis	347
Manual Review	348
Firewall Log	348
Syslogs	350

Authentication Logs	351
Event Logs	352
Defense in Depth	353
Personnel	354
<i>Training</i>	354
<i>Dual Control</i>	355
<i>Separation of Duties</i>	355
<i>Split Knowledge</i>	355
<i>Third Party/Consultants</i>	355
<i>Cross-Training/Mandatory Vacations</i>	356
<i>Succession Planning</i>	356
Processes	356
<i>Continual Improvement</i>	356
<i>Scheduled Reviews/Retirement of Processes</i>	357
Technologies	358
<i>Automated Reporting</i>	358
<i>Security Appliances</i>	358
<i>Security Suites</i>	359
<i>Outsourcing</i>	360
<i>Cryptography</i>	362
Other Security Concepts	373
<i>Network Design</i>	374
Exam Preparation Tasks	379
Review All Key Topics	379
Define Key Terms	380
Review Questions	380
Chapter 13 Application Security Best Practices	385
“Do I Know This Already?” Quiz	385
Foundation Topics	387
Best Practices During Software Development	387
Plan/Initiate Project	387
Gather Requirements (Security Requirements Definition)	388
Design	388
Develop	389

Test/Validate	389
Security Testing Phases	390
<i>Static Code Analysis</i>	390
<i>Web App Vulnerability Scanning</i>	391
<i>Fuzzing</i>	391
<i>Use Interception Proxy to Crawl Application</i>	392
Manual Peer Reviews	393
User Acceptance Testing	393
Stress Test Application	393
Security Regression Testing	394
Input Validation	394
Release/Maintain	395
Certify/Accredit	395
Change Management and Configuration Management/ Replacement	395
Secure Coding Best Practices	396
OWASP	396
SANS	396
Center for Internet Security	397
<i>System Design Recommendations</i>	397
<i>Benchmarks</i>	398
Exam Preparation Tasks	398
Review All Key Topics	398
Define Key Terms	399
Review Questions	399
Chapter 14 Using Cybersecurity Tools and Technologies	403
“Do I Know This Already?” Quiz	403
Foundation Topics	405
Preventative Tools	405
IPS	405
IDS	405
<i>Sourcefire</i>	405
<i>Snort</i>	406
<i>Bro</i>	407

HIPS	408
Firewall	408
<i>Firewall Architecture</i>	410
<i>Cisco</i>	415
<i>Palo Alto</i>	415
<i>Check Point</i>	415
Antivirus	415
Anti-malware	416
<i>Anti-spyware</i>	416
<i>Cloud Antivirus Services</i>	417
EMET	418
Web Proxy	418
<i>Web Application Firewall</i>	418
<i>ModSecurity</i>	420
<i>NAXSI</i>	420
<i>Imperva</i>	421
Collective Tools	421
SIEM	421
<i>ArcSight</i>	421
<i>QRadar</i>	422
<i>Splunk</i>	422
<i>AlienVault/OSSIM</i>	422
<i>Kiwi Syslog</i>	423
Network Scanning	423
<i>Nmap</i>	423
Vulnerability Scanning	423
<i>Qualys</i>	425
<i>Nessus</i>	425
<i>OpenVAS</i>	426
<i>Nexpose</i>	426
<i>Nikto</i>	427
<i>Microsoft Baseline Security Analyzer</i>	427
Packet Capture	428
<i>Wireshark</i>	428
<i>tcpdump</i>	429

<i>Network General</i>	429
<i>Aircrack-ng</i>	429
Command Line/IP Utilities	430
<i>Netstat</i>	430
<i>ping</i>	431
<i>tracert/traceroute</i>	432
<i>ipconfig/ifconfig</i>	433
<i>nslookup/dig</i>	434
<i>Sysinternals</i>	435
<i>OpenSSL</i>	436
IDS/HIDS	436
Analytical Tools	436
Vulnerability Scanning	437
Monitoring Tools	437
<i>MRTG</i>	437
<i>Nagios</i>	438
<i>SolarWinds</i>	438
<i>Cacti</i>	439
<i>NetFlow Analyzer</i>	439
Interception Proxy	439
<i>Burp Suite</i>	440
<i>Zap</i>	440
<i>Vega</i>	440
Exploit Tools	440
Interception Proxy	440
Exploit Framework	441
<i>Metasploit</i>	441
<i>Nexpose</i>	442
Fuzzers	442
<i>Untidy/Peach Fuzzer</i>	442
<i>Microsoft SDL File/Regex Fuzzer</i>	442
Forensics Tools	443
Forensic Suites	443
<i>EnCase</i>	444
<i>FTK</i>	444

	<i>Helix</i>	444
	<i>Sysinternals</i>	444
	<i>Cellebrite</i>	445
	Hashing	445
	<i>MD5sum</i>	445
	<i>SHAsum</i>	445
	Password Cracking	445
	<i>John the Ripper</i>	445
	<i>Cain & Abel</i>	446
	Imaging	447
	<i>DD</i>	447
	Exam Preparation Tasks	447
	Review All Key Topics	447
	Define Key Terms	448
	Review Questions	448
Chapter 15	Final Preparation	453
	Tools for Final Preparation	453
	Pearson Test Prep Practice Test Software and Questions on the Website	453
	<i>Accessing the Pearson Test Prep Software Online</i>	454
	<i>Accessing the Pearson Test Prep Practice Test Software Offline</i>	454
	Customizing Your Exams	455
	Updating Your Exams	456
	<i>Premium Edition</i>	456
	Chapter-Ending Review Tools	457
	Suggested Plan for Final Review/Study	457
	Summary	457
Appendix A	Answers to the “Do I Know This Already?” Quizzes and Review Questions	459
	Glossary	491
	Index	526

About the Author

Troy McMillan is a product developer and technical editor for Kaplan IT as well as a full-time trainer. He became a professional trainer 16 years ago, teaching Cisco, Microsoft, CompTIA, and wireless classes. He has written or contributed to more than a dozen projects, including the following recent ones:

- Contributing subject matter expert for *CCNA Cisco Certified Network Associate Certification Exam Preparation Guide* (Kaplan)
- Author of *CISSP Cert Guide* (Pearson)
- Prep test question writer for *CCNA Wireless 640-722* (Cisco Press)
- Author of *CASP Cert Guide* (Pearson)

Troy has also appeared in the following training videos for OnCourse Learning: Security+; Network+; Microsoft 70-410, 411, and 412 exam prep; ICND1; and ICND2.

He delivers CISSP training classes for CyberVista, authorized online training provider for (ISC)².

Troy now creates certification practice tests and study guides for the Transcender and Self-Test brands. He lives in Pfafftown, North Carolina, with his wife, Heike.

Dedication

I dedicate this book to my wife, Heike, who has supported me every time I've reinvented myself.

Acknowledgments

I must thank everyone on the Pearson team for all of their help in making this book better than it would have been without their help. That includes Michelle Newcomb, Eleanor Bru, Chris Crayton, and Robin Abernathy.

About the Technical Reviewers

Chris Crayton, MCSE, is an author, a technical consultant, and a trainer. 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 leading publishing companies. He holds numerous industry certifications, has been recognized with many professional teaching awards, and has served as a state-level SkillsUSA competition judge.

Robin M. Abernathy has been working in the IT certification preparation industry at Kaplan IT Certification Preparation, the owners of the Transcender and Self Test brands, for more than a decade. Robin has written and edited certification preparation materials for many (ISC)², Microsoft, CompTIA, PMI, Cisco, and ITIL certifications and holds multiple IT certifications from these vendors.

Robin provides training on computer hardware and software, networking, security, and project management. Over the past couple years, she has ventured into the traditional publishing industry, technical editing several publications and coauthoring Pearson's *CISSP Cert Guide* and *CASP Cert Guide*. She presents at technical conferences and hosts webinars on IT certification topics.

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 e-mail or write to let us know what you did or didn't like about this book—as well as what we can do to make our books better.

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

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

E-mail: feedback@pearsonitcertification.com

Mail: Pearson IT Certification
ATTN: Reader Feedback
800 East 96th Street
Indianapolis, IN 46240 USA

Reader Services

Register your copy of *CompTIA Cybersecurity Analyst (CSA+) Cert Guide* at www.pearsonitcertification.com for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.pearsonitcertification.com/register and log in or create an account*. Enter the product ISBN 9780789756954 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

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

Becoming a CompTIA Certified IT Professional is Easy

It's also the best way to reach greater professional opportunities and rewards.

Why Get CompTIA Certified?

Growing Demand

Labor estimates predict some technology fields will experience growth of over 20% by the year 2020.* CompTIA certification qualifies the skills required to join this workforce.

Higher Salaries

IT professionals with certifications on their resume command better jobs, earn higher salaries and have more doors open to new multi-industry opportunities.

Verified Strengths

91% of hiring managers indicate CompTIA certifications are valuable in validating IT expertise, making certification the best way to demonstrate your competency and knowledge to employers.**

Universal Skills

CompTIA certifications are vendor neutral—which means that certified professionals can proficiently work with an extensive variety of hardware and software found in most organizations.



Learn

Learn more about what the exam covers by reviewing the following:

- Exam objectives for key study points.
- Sample questions for a general overview of what to expect on the exam and examples of question format.
- Visit online forums, like LinkedIn, to see what other IT professionals say about CompTIA exams.



Certify

Purchase a voucher at a Pearson VUE testing center or at CompTIAstore.com.

- Register for your exam at a Pearson VUE testing center.
- Visit pearsonvue.com/CompTIA to find the closest testing center to you.
- Schedule the exam online. You will be required to enter your voucher number or provide payment information at registration.
- Take your certification exam.



Work

Congratulations on your CompTIA certification!

- Make sure to add your certification to your resume.
- Check out the CompTIA Certification Roadmap to plan your next career move.

Learn more: Certification.CompTIA.org/networkplus

* Source: CompTIA 9th Annual Information Security Trends study: 500 U.S. IT and Business Executives Responsible for Security

** Source: CompTIA Employer Perceptions of IT Training and Certification

*** Source: 2013 IT Skills and Salary Report by CompTIA Authorized Partner

Introduction

CompTIA CSA+ bridges the skills gap between CompTIA Security+ and CompTIA Advanced Security Practitioner (CASP). Building on CSA+, IT professionals can pursue CASP to prove their mastery of the hands-on cybersecurity skills required at the 5- to 10-year experience level. Earn the CSA+ certification to grow your career within the CompTIA recommended cybersecurity career pathway.

CompTIA CSA+ certification is designed to be a “vendor-neutral” exam that measures your knowledge of industry-standard technology.

Goals and Methods

The number-one goal of this book is a simple one: to help you pass the 2017 version of the CompTIA CSA+ certification exam CS0-001.

Because the CompTIA CSA+ certification exam stresses problem-solving abilities and reasoning more than memorization of terms and facts, our goal is to help you master and understand the required objectives for each exam.

To aid you in mastering and understanding the CSA+ certification objectives, this book uses the following methods:

- The beginning of each chapter defines the topics to be covered in the chapter; it also lists the corresponding CompTIA CSA+ objectives.
- The body of the chapter explains the topics from a hands-on and theory-based standpoint. This includes in-depth descriptions, tables, and figures that are geared toward building your knowledge so that you can pass the exam. The chapters are broken down into several topics each.
- The key topics indicate important figures, tables, and lists of information that you should know for the exam. They are interspersed throughout the chapter and are listed in a table at the end of the chapter.
- 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 complete key terms in the glossary.

Who Should Read This Book?

The CompTIA CSA+ examination is designed for IT security analysts, vulnerability analysts, and threat intelligence analysts. The exam certifies that a successful candidate has the knowledge and skills required to configure and use threat detection tools, perform data analysis, and interpret the results to identify vulnerabilities,

threats, and risks to an organization, with the end goal of securing and protecting applications and systems in an organization.

The recommended experience for taking the CompTIA CSA+ exam includes Network+, Security+, or equivalent knowledge as well as a minimum of three or four years of hands-on information security or related experience. While there is no required prerequisite, CSA+ is intended to follow CompTIA Security+ or equivalent experience and has a technical, hands-on focus.

This book is for you if you are attempting to attain a position in the cybersecurity field. It is also for you if you want to keep your skills sharp or perhaps retain your job due to a company policy that mandates that you update security skills.

This book is also for you if you want to acquire additional certifications beyond Security+. The book is designed to offer easy transition to future certification studies.

Strategies for Exam Preparation

Strategies for exam preparation vary depending on your existing skills, knowledge, and equipment available. Of course, the ideal exam preparation would consist of three or four years of hands-on security or related experience followed by rigorous study of the exam objectives.

After you have read through the book, have a look at the current exam objectives for the CompTIA CSA+ Certification Exams, listed at <https://certification.comptia.org/certifications/cybersecurity-analyst#tab4>. If there are any areas shown in the certification exam outline that you would still like to study, find those sections in the book and review them.

When you feel confident in your skills, attempt the practice exams found on the website that accompanies this book. As you work through the practice exam, note the areas where you lack confidence and review those concepts or configurations in the book. After you have reviewed those areas, work through the practice exam a second time and rate your skills. Keep in mind that the more you work through the practice exam, the more familiar the questions will become.

After you have worked through the practice exam a second time and feel confident in your skills, schedule the CompTIA CSA+ CS0-001 exam through Pearson Vue (www.vue.com). To prevent the information from evaporating out of your mind, you should typically take the exam within a week of when you consider yourself ready to take it.

The CompTIA CSA+ certification credential for those passing the certification exams is now valid for three years. To renew your certification without retaking the

exam, you need to participate in continuing education (CE) activities and pay an annual maintenance fee of \$50 (that is, \$150 for three years). See <https://certification.comptia.org/continuing-education/how-to-renew/ce-program-fees> for fee details. To learn more about the certification renewal policy, see <https://certification.comptia.org/continuing-education>.

Table I-1 CSA+ Exam Topics

Chapter	Exam Topics	CompTIA CSA+ Exam Objectives Covered
1	1.1 Given a scenario, apply environmental reconnaissance techniques using appropriate tools and processes.	CS0-001 objective 1.1
2	1.2 Given a scenario, analyze the results of a network reconnaissance.	CS0-001 objective 1.2
3	1.3 Given a network-based threat, implement or recommend the appropriate response and countermeasure.	CS0-001 objective 1.3
4	1.4 Explain the purpose of practices used to secure a corporate environment.	CS0-001 objective 1.4
5	2.1 Given a scenario, implement an information security vulnerability management process.	CS0-001 objective 2.1
6	2.2 Given a scenario, analyze the output resulting from a vulnerability scan.	CS0-001 objective 2.2
	2.3 Compare and contrast common vulnerabilities found in the following targets within an organization.	CS0-001 objective 2.3
7	3.1 Given a scenario, distinguish threat data or behavior to determine the impact of an incident.	CS0-001 objective 3.1
	3.2 Given a scenario, prepare a toolkit and use appropriate forensics tools during an investigation.	CS0-001 objective 3.2
8	3.3 Explain the importance of communication during the incident response process.	CS0-001 objective 3.3
	3.4 Given a scenario, analyze common symptoms to select the best course of action to support incident response.	CS0-001 objective 3.4
9	3.5 Summarize the incident recovery and post-incident response process.	CS0-001 objective 3.5
10	4.1 Explain the relationship between frameworks, common policies, controls, and procedures.	CS0-001 objective 4.1
11	4.2 Given a scenario, use data to recommend remediation of security issues related to identity and access management.	CS0-001 objective 4.2

Chapter	Exam Topics	CompTIA CSA+ Exam Objectives Covered
12	4.3 Given a scenario, review security architecture and make recommendations to implement compensating controls.	CS0-001 objective 4.3
13	4.4 Given a scenario, use application security best practices while participating in the Software Development Life Cycle (SDLC).	CS0-001 objective 4.4
14	4.5 Compare and contrast the general purpose and reasons for using various cybersecurity tools and technologies.	CS0-001 objective 4.5

Book Features and Exam Preparation Methods

This book uses several key methodologies to help you discover the exam topics on which you need more review, to help you fully understand and remember those details, and to help you prove to yourself that you have retained your knowledge of those topics. Therefore, this book does not try to help you pass the exams only by memorization but by truly learning and understanding the topics.

The book includes many features that provide different ways to study so you can be ready for the exam. If you understand a topic when you read it but do not study it any further, you probably will not be ready to pass the exam with confidence. The features included in this book give you tools that help you determine what you know, review what you know, better learn what you don't know, and be well prepared for the exam. These tools include the following:

- **“Do I Know This Already?” Quizzes:** Each chapter begins with a quiz that helps you determine the amount of time you need to spend studying that chapter.
- **Foundation Topics:** These are the core sections of each chapter. They explain the protocols, concepts, and configuration for the topics in that chapter.
- **Exam Preparation Tasks:** The “Exam Preparation Tasks” section lists a series of study activities that should be done after reading the “Foundation Topics” section. Each chapter includes the activities that make the most sense for studying the topics in that chapter.
- **Key Topics Review:** The Key Topic icon appears next to the most important items in the “Foundation Topics” section of the chapter. The “Key Topics Review” section lists the key topics from the chapter and their page numbers. Although the contents of the entire chapter could be on the exam, you should

definitely know the information highlighted with Key Topic icons. Review these topics carefully.

- **Definition of Key Terms:** Although certification exams might be unlikely to ask a question such as “How do you define the term ____?” the CSA+ exam requires you to learn and know a lot of terminology. This section lists some of the most important terms from the chapter and asks you to write a short definition and compare your answer against the Glossary.
- **End-of-Chapter Review Questions:** The review questions help you confirm that you understand the content that you just covered.

Companion Website

Register this book to get access to the Pearson IT Certification test engine 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 most troublesome topics on the exam. Be sure to check the box indicating 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 9780789756954.
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 are very large, especially image and video files.

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

Accessing the Pearson Test Prep Software and Questions

This book comes complete with the Pearson Test Prep practice test software, which includes several exams. These practice tests are available to you either online or as

an offline Windows application. To access the practice exams that were developed to accompany this book, you need the unique access code printed on the card in the sleeve in the back of your book.

Note The cardboard case in the back of this book includes a paper that lists the activation code for the practice exam 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 that has a browser and connectivity to the Internet, including desktop machines, tablets, and smart phones. 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 e-mail and 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.

The online version of the Pearson Test Prep software is supported on the following browsers:

- Chrome (Windows and Mac), version 40 and above
- Firefox (Windows and Mac), version 35 and above
- Safari (Mac), version 7
- Internet Explorer 10 and 11
- Microsoft Edge
- Opera

The online version of the Pearson Test Prep software is supported on the following devices:

- Desktop and laptop computers
- Tablets running on Android and iOS
- Smartphones with a minimum screen size of 4.7 inches

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.

Previous users: If you have already installed the Pearson Test Prep software from another purchase, you do not need to install it again. Launch the Pearson Test Prep software from your Start menu. Click **Activate Exam** in the **My Products** or **Tools** tab and enter the activation key found in the sleeve in the back of your book to activate and download the free practice questions for this book.

New users: You need to install the Pearson Test Prep software on your Windows desktop. Follow the steps below to download, install, and activate your exams.

1. Click the **Install Pearson Test Prep Desktop Version** link under the **Practice Exams** section of the page to download the software.
2. Once the software finishes downloading, unzip all the files on your computer.
3. Double-click the application file to start the installation, and follow the on-screen instructions to complete the registration.
4. Once the installation is complete, launch the application and select **Activate Exam** button on the **My Products** tab.
5. Click the **Activate a Product** button in the **Activate Product Wizard**.
6. Enter the unique access code found on the card in the sleeve in the back of your book and click the **Activate** button.
7. Click **Next** and then the **Finish** button to download the exam data to your application.
8. You can now start using the practice exams by selecting the product and clicking the **Open Exam** button to open the exam settings screen.

Desktop version system requirements:

- Windows 10, Windows 8.1, Windows 7, or Windows Vista (SP2)
- Microsoft NET Framework 4.5 Client
- Pentium class 1 GHz processor (or equivalent)
- 512 MB RAM
- 650 MB hard disk space plus 50 MB for each downloaded practice exam
- Access to the Internet to register and download exam databases

Assessing Exam Readiness

Exam candidates never really know whether they are adequately prepared for the exam until they have completed about 30% of the questions. At that point, if you are not prepared, it is too late. The best way to determine your readiness is to work through the “Do I Know This Already?” quizzes at the beginning of each chapter and review the foundation and key topics presented in each chapter. It is best to work your way through the entire book unless you can complete each subject without having to do any research or look up any answers.

Premium Edition

In addition to the free practice exams provided with your purchase, you can purchase one additional exam with expanded functionality directly from Pearson IT Certification. The Premium Edition eBook and Practice Test for this title contains an additional full practice exam as well as an eBook (in both PDF and ePub format). In addition, the Premium Edition title provides remediation for each question, directing you to the specific part of the eBook that relates to that question.

If you have purchased the print version of this title, you can purchase the Premium Edition at a deep discount. There is a coupon code in the cardboard sleeve that contains a one-time-use code as well as instructions for where to purchase the Premium Edition.



This chapter covers the following topics:

1.0 Threat Management

1.4 Explain the purpose of practices used to secure a corporate environment.

- **Penetration Testing:** Discusses the testing process and the rules of engagement.
- **Reverse Engineering:** Includes topics such as isolation and sandboxing, authenticity of hardware, and fingerprinting and decomposition of software and malware.
- **Training and Exercises:** Describes the functions of red, blue, and white teams.
- **Risk Evaluation:** Discusses the risk evaluation process both from technical and operational viewpoints.

Practices Used to Secure a Corporate Environment

Securing a corporate environment is not a one-time endeavor. It should entail a set of processes that are embedded into day-to-day operations. Some of these processes, such as penetration testing, are designed to locate weaknesses before attackers do, while other processes, such as fingerprinting and decomposition, are important to understand because they are techniques that attackers use to thwart your best efforts at preventing the delivery of malware. This chapter discusses the process of penetration testing, the value of understanding how attackers use fingerprinting and decomposition, the importance of training and exercises, and the steps in the risk management process.

“Do I Know This Already?” Quiz

The “Do I Know This Already?” quiz allows you to assess whether you should read the entire chapter. Table 4-1 lists the major headings in this chapter and the “Do I Know This Already?” quiz questions covering the material in those headings so you can assess your knowledge of these specific areas. The answers to the quiz appear in Appendix A, “Answers to the ‘Do I Know This Already?’ Quizzes and Review Questions.” If you miss no more than one of these self-assessment questions, you might want to move ahead to the “Exam Preparation Tasks.”

Table 4-1 “Do I Know This Already?” Foundation Topics Section-to-Question Mapping

Foundation Topics Section	Questions
Penetration Testing	1–3
Reverse Engineering	6
Training and Exercises	4, 5
Risk Evaluation	7

1. Which of the following is the first step in a pen test?
 - a. Gather information about attack methods against the target system or device.
 - b. Execute attacks against the target system or device to gain user and privileged access.
 - c. Document information about the target system or device.
 - d. Document the results of the penetration test.

2. In which type of tests is the testing team provided with limited knowledge of the network systems and device?
 - a. Blind test
 - b. Double-blind test
 - c. Target test
 - d. External test

3. Which of the following is also referred to as a closed, or black-box, test?
 - a. Zero-knowledge test
 - b. Partial-knowledge test
 - c. Full-knowledge test
 - d. Target test

4. Which of the following is not covered in the rules of engagement?
 - a. Timing
 - b. Scope
 - c. Compensation
 - d. Authorization

5. Which of the following acts as the network defense team?
 - a. Blue team
 - b. White team
 - c. Purple team
 - d. Red team

- 6.** With which of the following can malware executable files be executed without allowing the files to interact with the local system?
 - a.** Sandboxing
 - b.** DMZ
 - c.** Trusted Foundry
 - d.** Decomposition

- 7.** When performing qualitative risk evaluation, which of the following is considered in addition to the impact of the event?
 - a.** Attack vectors
 - b.** Likelihood
 - c.** Costs
 - d.** Frequency

Foundation Topics

Penetration Testing

A penetration test (often called a pen test) is designed to simulate an attack on a system, a network, or an application. Its value lies in its potential to discover security holes that may have gone unnoticed. It differs from a vulnerability test in that it attempts to exploit vulnerabilities rather than simply identify them. Nothing places the focus on a software bug like the exposure of critical data as a result of the bug.

In many cases, some of the valuable information that comes from these tests is the identification of single operations that, while benign on their own, create security problems when used in combination. These tests can be made more effective when utilized with a framework like Metasploit or CANVAS (discussed Chapter 14, “Using Cybersecurity Tools and Technologies”).

Penetration testing should be an operation that occurs at regular intervals, and its frequency should be determined by the sensitivity of the information on the network. An example of a pen test tool is Retina. Figure 4-1 shows Retina output from scanning a single device. In this output, you can see that the tool has identified eight serious problems (indicated by the upward-pointing arrows): weak encryption in Terminal Services, six weaknesses related to Oracle, and one weakness related to a virtualization product on the machine called Oracle VirtualBox.

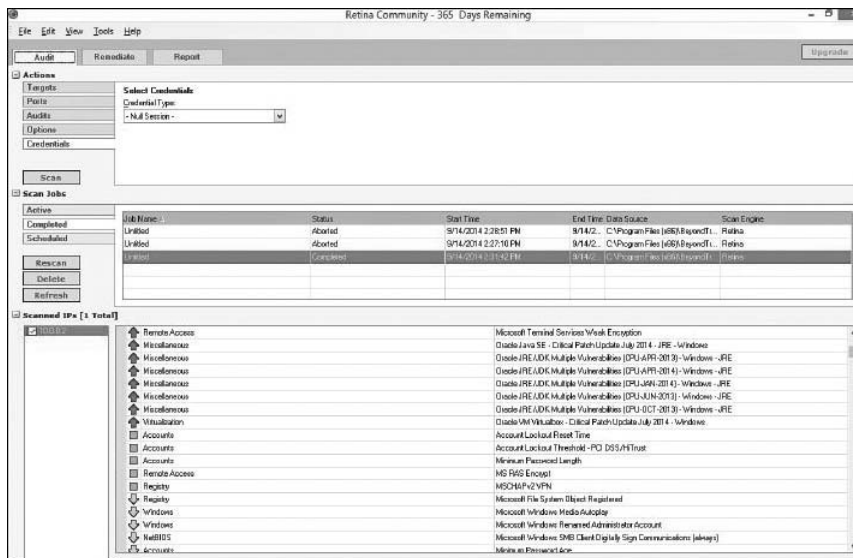


Figure 4-1 Retina Output

**Key
Topic**

The steps in performing a penetration test are as follows:

- Step 1.** Planning and preparation
- Step 2.** Information gathering and analysis
- Step 3.** Vulnerability detection
- Step 4.** Penetration attempt
- Step 5.** Analysis and reporting
- Step 6.** Cleaning up

Both internal and external tests should be performed. Internal tests occur from within the network, whereas external tests originate outside the network, targeting the servers and devices that are publicly visible.

Strategies for penetration testing are based on the testing objectives, as defined by the organization. The strategies that you should be familiar with include the following:

**Key
Topic**

- **Blind test:** The testing team is provided with limited knowledge of the network systems and devices, using publicly available information. The organization's security team knows that an attack is coming. This test requires more effort by the testing team, and the testing team must simulate an actual attack.
- **Double-blind test:** This test is like a blind test except the organization's security team does not know that an attack is coming. Only a few individuals at the organization know about the attack, and they do not share this information with the security team. This test usually requires equal effort for both the testing team and the organization's security team.
- **Target test:** Both the testing team and the organization's security team are given maximum information about the network and the type of test that will occur. This is the easiest test to complete but does not provide a full picture of the organization's security.

Penetration testing is also divided into categories based on the amount of information to be provided. The main categories that you should be familiar with include the following:

**Key
Topic**

- **Zero-knowledge test:** The testing team is provided with no knowledge regarding the organization's network. The testers can use any means at their disposal to obtain information about the organization's network. This is also referred to as closed, or black-box, testing.

- **Partial-knowledge test:** The testing team is provided with public knowledge regarding the organization's network. Boundaries might be set for this type of test.
- **Full-knowledge test:** The testing team is provided with all available knowledge regarding the organization's network. This test is focused more on what attacks can be carried out.

Other penetration testing applications include Metasploit, Wireshark, CORE Impact, Nessus, Back Track, Cain & Abel, and John the Ripper. When selecting a penetration testing tool, you should first determine which systems you want to test. Then research the different tools to discover which of them can perform the tests that you want to perform for those systems. When you have a tool in mind, research the tool's methodologies for testing. In addition, the correct individual needs to be selected to carry out the test. Remember that penetration tests should include manual methods as well as automated methods because relying on only one of these two does not result in a thorough result.

Rules of Engagement

The rules of engagement define how penetration testing should occur. These issues should be settled and agreed upon before any testing begins. The following are some of the key issues to be settled:

Key Topic

- **Timing:** The timeline for the test must be established. The start and end times will be included in the scope of the project, but creating the timeline does not mean it cannot change as reality dictates; rather, it means that you have a framework to work from. This also includes the times of day the testing will occur.
- **Scope:** The scope of the test includes the timeline and also includes a list of all devices that are included in the test, as well as a description of all testing methodologies to be used. The output of this process should be a set of documents that are provided to the tester that include the following:
 - A network diagram depicting all network segments in scope for the test
 - A data flow diagram
 - A list of services and ports exposed at the perimeter
 - Details of how authorized users access the network
 - A list of all network segments that have been isolated from the test to reduce scope

- **Authorization:** Formal authorization should be given to the tester to perform the test, with written approval by upper management. Without this, the tester could be liable for attempting to compromise the network.
- **Exploitation:** Before the test occurs, it should be determined whether exploits will be attempted if vulnerable systems are found. This is intentionally included in some cases so the incident response plan can be tested.
- **Communication:** Another of the issues in the rules of engagement is how communications are to occur between the tester and the stakeholders as the process unfolds. While regular meetings should be scheduled, there also must be a line of communication established for times when issues arise and changes may need to be made.
- **Reporting:** The type of reports to be generated is determined during the establishment of the rules of engagement. This includes the timing of reports, the format, and the specific information to be included. While postponing of reports should be allowed, it should not be allowed to become chronic, and the rules of engagement may include both incentives and penalties for the timelessness of reports.

Reverse Engineering

Reverse engineering is a term that has been around for some time. Generically, it means taking something apart to discover how it works and perhaps to replicate it. In cybersecurity, it is used to analyze both hardware and software and for various other reasons, such as to do the following:

- Discover how malware functions
- Determine whether malware is present in software
- Locate software bugs
- Locate security problems in hardware

The following sections look at the role of reverse engineering in cybersecurity analysis.

Isolation/Sandboxing

You may be wondering what the concepts of isolation and sandboxing are doing in a section on reverse engineering. How can you analyze malware without suffering the effects of the malware? The answer is to place the malware where it is safe to probe it and play with it. This is done by isolating, or sandboxing, the malware. You can

use a sandbox to run a possibly malicious program in a safe environment so that it doesn't infect the local system.

By using sandboxing tools, you can execute malware executable files without allowing the files to interact with the local system. Some sandboxing tools also allow you to analyze the characteristics of an executable. There are cases when this is not possible because malware can be specifically written to do different things if it detects that it's being executed in a sandbox.

In many cases, sandboxing tools operate by sending a file to a special server that analyzes the file and sends you a report on it. Sometimes this is a free service, but in many instances it is not. Some examples of these services include the following:

- Sandboxie
- Akana
- Binary Guard True Bare Metal
- BitBlaze Malware Analysis Service
- Comodo Automated Analysis System and Valkyrie
- Deepviz Malware Analyzer
- Detux Sandbox (Linux binaries)

Another option for studying malware is to set up a sheep dip computer. This is a system that has been isolated from the other systems and is used for analyzing suspect files and messages for malware. You can take measures such as the following on a sheep dip system:

- Install port monitors to discover ports used by the malware.
- Install file monitors to discover what changes may be made to files.
- Install network monitors to identify what communications the malware may attempt.
- Install one or more antivirus programs to perform malware analysis.

Often these sheep dip systems are combined with antivirus sensor systems to which malicious traffic is reflected for analysis.

The safest way to perform reverse engineering and malware analysis is to prepare a test bed. Doing so involves the following steps:

- Step 1.** Install virtualization software on the host.
- Step 2.** Create a VM and install a guest operating system on the VM.

- Step 3.** Isolate the system from the network by ensuring that the NIC is set to “host” only mode.
- Step 4.** Disable shared folders and enable guest isolation on the VM.
- Step 5.** Copy the malware to the guest operating system.

Also, you need isolated network services for the VM, such as DNS. It may also be beneficial to install multiple operating systems in both patched and non-patched configurations. Finally, you can make use of virtualization snapshots and re-imaging tools to wipe and rebuild machines quickly.

Once the test bed is set up, you also need to install a number of other tools to use on the isolated VM, including the following:

- **Imaging tools:** You need these tools to take images for forensics and prosecution procedures. Examples include Safe Back Version 2.0 and DD (which is covered in Chapter 14).
- **File/data analysis tools:** You need these tools to perform static analysis of potential malware files. Examples include PE Studio and PEframe.
- **Registry/configuration tools:** You need these tools to help identify infected settings in the registry and to identify the last saved settings. Examples include Microsoft’s Sysinternals Autoruns and Silent Runners.vbs.
- **Sandbox tools:** You need these tools for manual malware analysis (listed earlier in this chapter, the “Isolation/Sandboxing” section)
- **Log analyzers:** You need these tools to extract log files. Examples include AWStats and Apache Log Viewer.
- **Network capture tools:** You need these tools to understand how the malware uses the network. Examples include Wireshark and Omnipcap.

While the use of virtual machines to investigate the effects of malware is quite common, you should know that some well-written malware can break out of a VM relatively easily, making this approach problematic.

Hardware

You must be concerned with the safety and the integrity of the hardware that you purchase. The following are some of the methods used to provide this assurance:

- **Source authenticity of hardware:** When purchasing hardware to support any network or security solution, a security professional must ensure that the hardware’s authenticity can be verified. Just as expensive consumer items such as

purses and watches can be counterfeited, so can network equipment. While the dangers with counterfeit consumer items are typically confined to a lack of authenticity and potentially lower quality, the dangers presented by counterfeit network gear can extend to the presence of backdoors in the software or firmware. Always purchase equipment directly from the manufacturer when possible, and when purchasing from resellers, use caution and insist on a certificate of authenticity. In any case where the price seems too good to be true, keep in mind that it may be an indication the gear is not authentic.

- **Trusted Foundry:** The Trusted Foundry program can help you exercise care in ensuring the authenticity and integrity of the components of hardware purchased from a vendor. This DoD program identifies “trusted vendors” and ensures a “trusted supply chain.” A trusted supply chain begins with trusted design and continues with trusted mask, foundry, packaging/assembly, and test services. It ensures that systems have access to leading-edge integrated circuits from secure, domestic sources. At the time of this writing, 77 vendors have been certified as trusted.
- **OEM documentation:** One of the ways you can reduce the likelihood of purchasing counterfeit equipment is to insist on the inclusion of verifiable original equipment manufacturer (OEM) documentation. In many cases, this paperwork includes anti-counterfeiting features. Make sure to use the vendor website to verify all the various identifying numbers in the documentation.

Software/Malware

Software of any type can be checked for integrity to ensure that it has not been altered since its release. Checking for integrity is one of the ways you can tell when a file has been corrupted (or perhaps replaced entirely) with malware. Two main methods are used in this process:

- **Fingerprinting/hashing:** Fingerprinting, or hashing, is the process of using a hashing algorithm to reduce a large document or file to a character string that can be used to verify the integrity of the file (that is, whether the file has changed in any way). To be useful, a hash value must have been computed at a time when the software or file was known to have integrity (for example, at release time). Then at any time thereafter, the software file can be checked for integrity by calculating a new hash value and comparing it to the value from the initial calculation. If the character strings do not match, a change has been made to the software.

Fingerprinting/hashing has been used for some time to verify the integrity of software downloads from vendors. The vendor provides the hash value and specifies the hash algorithm, and the customer recalculates the hash value after

the download. If the result matches the value from the vendor, the customer knows the software has integrity and is safe.

Anti-malware products also use this process to identify malware. The problem is that malware creators know this, and so they are constantly making small changes to malicious code to enable the code to escape detection through the use of hashes or signatures. When they make a small change, anti-malware products can no longer identify the malware, and they won't be able to until a new hash or signature is created by the anti-malware vendor. For this reason, some vendors are beginning to use "fuzzy" hashing, which looks for hash values that are similar but not exact matches.

- **Decomposition:** Decomposition is the process of breaking something down to discover how it works. When applied to software, it is the process of discovering how the software works, perhaps who created it, and, in some cases, how to prevent the software from performing malicious activity.

When used to assess malware, decomposition can be done two ways: statically and dynamically. When static or manual analysis is used, it takes hours per file and uses tools called disassemblers. Advanced expertise is required. Time is often wasted on repetitive sample unpacking and indicator extraction tasks.

With dynamic analysis tools, an automated static analysis engine is used to identify, de-archive, de-obfuscate, and unpack the underlying object structure. Then proactive threat indicators (PTI) are extracted from the unpacked files. A rules engine classifies the results to calculate the threat level and to route the extracted files for further analysis. Finally, the extracted files are repaired to enable further extraction or analysis with a sandbox, decompiler, or debugger. While the end result may be the same, these tools are much faster and require less skill than manual or static analysis.

Training and Exercises

Security analysts must practice responding to security events in order to react to them in the most organized and efficient manner. There are some well-established ways to approach this. This section looks at how teams of analysts, both employees and third-party contractors, can be organized and some well-established names for these teams.

Security posture is typically assessed by war game exercises in which one group attacks the network while another attempts to defend the network. These games typically have some implementation of the following teams:

- **Red team:** The Red team acts as the attacking force. It typically carries out penetration tests by following a well-established process of gathering



information about the network, scanning the network for vulnerabilities, and then attempting to take advantage of the vulnerabilities. The actions they can take are established ahead of time in the *rules of engagement*. Often these individuals are third-party contractors with no prior knowledge of the network. This helps them simulate attacks that are not inside jobs.

- **Blue team:** The Blue team acts as the network defense team, and the attempted attack by the Red team tests the Blue team's ability to respond to the attack. It also serves as practice for a real attack. This includes accessing log data, using a SIEM, garnering intelligence information, and performing traffic and data flow analysis.
- **White team:** The White team is a group of technicians who referee the encounter between the Red team and the Blue team. Enforcing the rules of engagement might be one of the White team's roles, along with monitoring the responses to the attack by the Blue team and making note of specific approaches employed by the Red team.

Risk Evaluation

Although penetration testing can identify vulnerabilities, it is not the recommended way to identify vulnerabilities. An organization should have a well-defined risk management process in place that includes the evaluation of risk that is present. When this process is carried out properly, *threat modeling* allows organizations to identify threats and potential attacks and implement the appropriate mitigations against these threats and attacks. These facets ensure that any security controls implemented are in balance with the operations of the organization. The three parts to this process are covered in the following sections.

Technical Impact and Likelihood

Once all assets have been identified and their value to the organization has been established, specific threats to each asset are identified. An attempt must be made to establish both the likelihood of the threat's realization and the impact to the organization if it occurs. While both quantitative and qualitative risk assessments may be performed, when a qualitative assessment is conducted, the risks are placed into the following categories:

- High
- Medium
- Low

Typically, a risk assessment matrix, such as the one in Figure 4-2, is created. Subject experts grade all risks based on their likelihood and impact. This helps prioritize the application of resources to the most critical vulnerabilities.

**Key
Topic**

		Impact				
		Trivial	Minor	Moderate	Major	Extreme
Probability	Rare	Low	Low	Low	Medium	Medium
	Unlikely	Low	Low	Medium	Medium	Medium
	Moderate	Low	Medium	Medium	Medium	High
	Likely	Medium	Medium	Medium	High	High
	Very Likely	Medium	Medium	High	High	High

Figure 4-2 Risk Assessment Matrix

Technical Control Review

Technical controls are implemented with technology and include items such as firewalls, access lists, permissions on files and folders, and devices that identify and prevent threats. After it understands the threats, an organization needs to establish likelihoods and impacts, and it needs to select controls that, while addressing a threat, do not cost more than the cost of the realized threat. The review of these controls should be an ongoing process.

Operational Control Review

Operational controls are the policies, procedures, and work practices that either help prevent a threat or make the threat more likely. The review of these controls should be an ongoing process.

Exam Preparation Tasks

As mentioned in the section “Strategies for Exam Preparation” in the Introduction, you have a couple choices for exam preparation: the exercises here, Chapter 15, “Final Preparation,” 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 Topics icon in the outer margin of the page. Table 4-2 lists these key topics and the page number on which each is found.

**Key
Topic**

Table 4-2 Key Topics in Chapter 4

Key Topic Element	Description	Page Number
Step List	Steps in a penetration test	99
List	Strategies for pen testing	99
List	Pen test categories	99
List	Rules of engagement	100
List	Security teams	105
Figure 4-2	Risk assessment matrix	107

Define Key Terms

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

penetration testing, blind test, double-blind test, target test, zero-knowledge test, partial-knowledge test, full-knowledge test, rules of engagement, reverse engineering, isolation, sandboxing, sheep dip computer, imaging tools, file/data analysis tools, registry/configuration tools, sandbox tools, log analyzers, network capture tools, Trusted Foundry, fingerprinting/hashing, decomposition, Red team, Blue team, White team, risk evaluation, risk assessment matrix, technical control review, operational control review

Review Questions

1. Which of following attempts to exploit vulnerabilities?
 - a. Vulnerability test
 - b. Pen test
 - c. Risk assessment
 - d. Port scan

2. Which of the following is the third step in a pen test?
 - a. Analysis and reporting
 - b. Vulnerability detection
 - c. Penetration attempt
 - d. Cleaning up

3. In which type of test are both the testing team and the organization's security team given maximum information about the network and the type of test that will occur?
 - a. Blind test
 - b. Double-blind test
 - c. Target test
 - d. External test

4. In which of the following is the testing team provided with public knowledge regarding the organization's network?
 - a. Zero-knowledge test
 - b. Partial-knowledge test
 - c. Full-knowledge test
 - d. Target test

5. Which of the following rules of engagement includes a list of all devices that are included in the test as well as a description of all testing methodologies to be used?
 - a. Timing
 - b. Scope
 - c. Authorization
 - d. Exploitation

6. Which of the following practices places malware where it is safe to probe it and play with it?
 - a. Sandboxing
 - b. Compartmentalizing
 - c. Boundary enforcement
 - d. File locks

7. Which of the following is a system that has been isolated from other systems and is used for analyzing suspect files and messages for malware?
 - a. Sheep dip computer
 - b. Virtual machine
 - c. Sandbox
 - d. Honeypot

8. Which of the following is a good example of exercising care in ensuring the authenticity and integrity of the components of hardware purchased from a vendor?
 - a. Trusted Foundry program
 - b. Fingerprinting
 - c. Hashing
 - d. Decomposition

9. Which of the following is the process of taking a large document or file and, with the use of a hashing algorithm, reducing the file to a character string that can be used to verify the integrity of the file?
 - a. Hashing
 - b. Decomposing
 - c. Sandboxing
 - d. Reverse engineering

10. Which of the following helps prioritize the application of resources to the most critical vulnerabilities?
 - a. Access control matrix
 - b. Risk assessment matrix
 - c. PERT chart
 - d. Gantt chart



Index

Symbols

802.1x, 88-90

/? argument (netstat command), 22

A

-a argument (netstat command), 21-23

-a parameter

ifconfig command, 434

netstat command, 431

ping command, 432

A records (DNS), 8

AAAA records (DNS), 8

AC (Access Complexity) vulnerabilities, 129

accepting risks, 278

access

complexity (AC) vulnerabilities, 129

context-based authentication, 304-305

control lists. *See* ACLs

controls, 84-86

NIST SP 800-53 control family, 259

provisioning life cycle, 274

types, 282-284

defense-in-depth strategy, 354

cryptography. *See* *cryptography*

dual control, 355

network design, 374-376

network segmentation, 377

outsourcing, 360-362

personnel, 354-356

processes, 356-357

security devices, 358-359

security suites, 359

technologies, 358

exploits, 334

impersonation, 334

man-in-the-middle, 334

privilege escalation, 335

rootkits, 335-336

session hijacking, 335

XSS, 335

identities. *See* identities

NAC, 86-90

points. *See* APs

SSO

identity propagation, 326-327

OpenID, 331-332

provisioning/deprovisioning, 333

SAML, 330-331

self-service password reset, 334

Shibboleth, 332

SPML, 329

XACML, 327-329

system, viewing, 436

users, viewing, 436

vector (AV) vulnerabilities, 129

vulnerability scanning, 131

AccessChk tool, 436

AccessEnum tool, 436

Acceptable Use Policy (AUP), 271-272

accountability (personnel), 309

accounting data, 200

accounting information systems (AIS), 200

accounts

lockout policies, 270

maintenance, 149

management policies, 273-274

new application, 231

provisioning/deprovisioning, 333

accreditation

certification, compared, 291

software development, 395

ACLs (access control lists), 80

misconfigurations, 14

packets, compared, 81

routers, configuring, 80

testing, 15

acquisitions, 200

action field (firewall logs), 349

actions

- response, 147

- Syslogs, 351

active vulnerability scanners (AVS), 31**AD (Active Directory), 78-79, 320****Adaptive Security Appliance (ASA), 415****addresses (e-mail), harvesting, 7****ADM (Architecture Development Method), 266****administrative controls, 84-85, 284****advanced persistent threats (APTs), 191****agentless log collection, 57****agents**

- log collection, 58

- NAC, 88

- vulnerability scanning tools, 126-127

aggregation, 161, 346**AHs (authentication headers), 177, 373****Aircrack-ng, 429-430****AIS (accounting information systems), 200****ALE (annual loss expectancy), 279****algorithms**

- asymmetric, 366-367

- hybrid, 367-368

- MD, 370

- symmetric, 364-366

AlienVault, 422**Amazon Web Services (AWS), 362****analysis**

- anomaly, 45

- availability, 46

- behavioral, 47

- cost-benefit, 280-281

- data flow, 390

- data output, 47

- event logs, 53-55*

- firewall logs, 47-49*

- IDS, 56-57, 60*

- NetFlow analyzer, 61*

- packet analyzer, 59-60*

- packet captures, 49-50*

- ping scanning, 52*

- port scanning, 52-53*

- resource monitoring, 61*

- SIEM, 57-58*

- Syslog, 55-56*

- heuristic, 46

- lexical, 390

- logs, 348

- authentication logs, 351*

- event logs, 352-353*

- firewall logs, 348-350*

- Syslogs, 350-351*

- malware, 101-103

- NetFlow data, 41-42

- packets, 40, 59-60

- point-in-time data, 40

- NetFlow, 41-42*

- packet analysis, 40*

- protocol analysis, 40*

- traffic analysis, 40-41*

- wireless, 43-45*

- protocols, 40

- reports, 143-147

- risk

- qualitative, 280*

- quantitative, 279*

- safeguards, selecting, 280-281*

- total risk vs. residual risk, 281*

- static code, 390

- taint, 390

- teams, 105-106

- tools, 436

- interception proxy, 439-440*

- monitoring, 437-439*

- vulnerability scanning, 437*

- traffic, 40-41

- trend, 46

- utilities (forensic investigation suites), 206

- vulnerability scan output, 143

- correlating with other data points, 147-148*

- reports, 143-147*

- reviewing, 145*

- wireless, 43-45

annual loss expectancy (ALE), 279**anomalous activity (applications), 230****anomaly analysis, 45****anomaly based IDS, 26****anti-malware software, 415-417****anti-spam software, 417****anti-spyware software, 416****AP (access point), 12, 312**

- rogue, 224, 312

- wireless analysis, 45*

- WLANs, 12*

Apple Pay, 196**applets, 162****applications**

- architecture domain (TOGAF), 266

- firewalls, 409

- IDS, 26

- incident indicators, 230

- anomalous activity, 230*

- memory overflows, 231*

- new accounts, 231*

- service interruptions, 231*
- unexpected outbound communication, 231*
- unexpected output, 231*
- logs, 53
- proxies, 28
- startup, viewing, 436
- APTs (advanced persistent threats), 191**
- architecture (firewalls), 29-30**
 - bastion hosts, 410
 - dual-homed, 411
 - multihomed, 412
 - screened host, 413
 - screened subnet, 414
- Architecture Development Method (ADM), 266**
- ArcSight, 421**
- ARP poisoning, 164-165**
- ASA (Adaptive Security Appliance), 415**
- assessments, 122, 290**
- assets**
 - criticality, 192
 - inventory, 120
- assisted password resets, 270**
- asymmetric algorithms, 366-367**
- AT (awareness and training) NIST SP 800-53 control family, 259**
- attacks. *See also threats***
 - database servers, 160-161
 - dumpster diving, 311
 - endpoints, 161-162
 - ICS, 179-180
 - identity theft, 311
 - interconnected networks, 174-175
 - man-in-the-middle, 178, 334
 - mobile devices, 173-174
 - network devices, 169
 - network infrastructure, 162
 - ARP poisoning, 164-165*
 - MAC overflow, 164*
 - routers, 168*
 - switches, 163*
 - VLANs, 165-168*
 - pharming, 310
 - phishing, 310
 - SCADA, 179-180
 - shoulder surfing, 310
 - Stuxnet virus, 180
 - SYN flood, 48
 - virtualization, 13, 169
 - hosts, 169-170*
 - management interfaces, 171-173*
 - networks, 170*
 - VM escape, 169
 - VPNs, 175-179
 - web servers
 - buffer overflows, 157-159*
 - click-jacking, 152-153*
 - CSRFs, 151-152*
 - errors/exceptions, handling, 156*
 - input validation, 154*
 - insecure direct object references, 150*
 - integer overflows, 159*
 - maintenance books, 149*
 - race conditions, 160*
 - sensitive data storage, 156*
 - session hijacking, 153*
 - SQL injections, 155*
 - time-of-check, 150*
 - time-of-use, 150*
 - XSS, 150-151*
 - wireless, 12
 - zero day, 46, 190
- AU (audit and accountability) NIST SP 800-53 control family, 259**
- audit logs (personnel accountability), 309**
- audits, 288-289**
- AUP (Acceptable Use Policy), 271-272**
- authentication**
 - context-based, 304-305
 - cryptosystems, 362
 - headers (Ahs), 177, 373
 - Kerberos, 321
 - logs, analyzing, 351
 - password period, 269
 - servers, 88, 323
 - step-up, 304
 - vulnerabilities, 129
 - WPA/WPA2, 12
- authenticators, 88, 323**
- authorization**
 - cryptosystems, 363
 - Open (OAuth), 318
 - penetration testing, 101
- automated distribution reports, 132**
- automated reporting, 358**
- Autoruns tool, 436**
- AV (Access Vector) vulnerabilities, 129**
- availability**
 - analysis, 46
 - vulnerabilities, 130
- avoiding risks, 278**
- AVS (active vulnerability scanners), 31**
- awareness and training (AT) NIST SP 800-53 control family, 259**
- AWS (Amazon Web Services), 362**

B

-b argument (netstat command), 23
backdoors, 313
bandwidth consumption, 221
base vulnerabilities, 129
Basel II, 256
bastion hosts, 29, 410
beaconing, 221
behavioral analysis, 47
benchmarks (CIS), 398
blacklisting, 154
blind penetration testing, 99
block ciphers, 365-366
Blue team (training), 106
Bluetooth hacking gear, 224
Bro, 407
buffer overflows, 157-159, 312
Burp suite, 440
business architecture domain (TOGAF), 266
business process interruption, 135
BYOD (bring your own device) policies, 173

C

CA (security assessment and authorization) NIST SP 800-53 control family, 259
cables, 203
Cain & Abel password cracker, 446
CALEA (Communications Assistance to Law Enforcement Act) of 1994, 256

call lists, 206
cameras (forensics kits), 204
Capability Maturity Model Integration (CMMI), 291
CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) passwords, 269
capturing packets, 428-430
 Aircrack-ng, 429-430
 environmental reconnaissance, 6
 Network General, 429
 output data, 49-50
 tcpdump, 429
 Wireshark, 428-429
carrier sense multiple access with collision avoidance (CSMA/CA), 43-45
categories
 controls, 277-278
 countermeasures, 83-84
 input validation tools, 394
 NIST SP 800-53 framework, 258-259
 penetration testing, 99
CCE (Common Configuration Enumeration), 128
Cellebrite, 445
Center for Internet Security (CIS), 397-398
certification, 291
 accreditation, compared, 291
 ISO/IEC 27001, 292-293
 ISO/IEC 27002, 294
 NIACAP, 292
 software development, 395
CFAA (Computer Fraud and Abuse Act), 255

chain of custody forms, 204
chain of custody tools (forensic investigation suites), 207
change control, 245
 passwords, 270
 reports, 132, 358
 software development, 395
 unauthorized changes as incident indicator, 229
 vulnerabilities, 134
Check Point firewalls, 415
checksum method (cryptography), 368
CIA (confidentiality, integrity, and availability), 362
ciphers, 365-366
circuit-level proxies, 28, 409
CIS (Center for Internet Security), 397-398
Cisco firewalls, 415
classifying
 data, 274-277
 threats, 189-190
clearing data, 243
click-jacking, 152-153
close-wait host connection, 22
closing host connection, 22
cloud
 antivirus software, 417
 environmental reconnaissance, 15-16
CM (configuration management) NIST SP 800-53 control family, 259
CMI (Copyright Management Information), 199
CMMI (Capability Maturity Model Integration), 291

- CN (common name)**, 320
- CNAME records (DNS)**, 8
- COBIT (Control Objectives for Information and Related Technology) framework**, 263-264
- cognitive passwords**, 269
- collective tools**, 421
 - command-line, 430-435
 - HIDS, 436
 - IDS, 436
 - network scanning, 423
 - packet capture, 428-430
 - SIEM, 421-423
 - vulnerability scanning, 423-427
- combination passwords**, 268
- command-line collective tools**, 430
 - Aircrack-ng, 429
 - ifconfig, 434
 - ipconfig, 433-434
 - netstat, 430-431
 - nslookup, 434-435
 - OpenSSL, 436
 - ping, 431-432
 - Sysinternals, 435-436
 - tracert, 432
- commands**
 - dd, 447
 - ifconfig, 434
 - ipconfig, 433-434
 - netstat, 21-23, 430-431
 - nslookup, 434-435
 - ping, 431-432
 - Sysinternals. *See* Sysinternals command
 - tcpdump, 429
 - tracert, 432
 - windump, 429
- commercial business data classifications**, 276
- Common Configuration Enumeration (CCE)**, 128
- common name (CN)**, 320
- Common Platform Enumeration (CPE)**, 128
- Common Vulnerabilities and Exposures (CVE)**, 128
- Common Vulnerability Scoring System (CVSS)**, 128-130
- Common Weakness Enumeration (CWE)**, 128
- communication**
 - irregular peer-to-peer, 222-223
 - penetration testing, 101
 - security monitoring, 244
 - stakeholders, 217-218
 - unexpected outbound, 231
 - vulnerability remediation, 134
- Communications Assistance to Law Enforcement Act (CALEA) of 1994**, 256
- community state (ports)**, 377
- compartmented security mode**, 82
- compensating countermeasures**, 83-84, 277
 - access controls, 84-86
 - control categories, 83-84
- complete regression testing**, 394
- Completely Automated Public Turing test to tell Computers and Humans (CAPTCHA) passwords**, 269
- compliance. *See* regulatory compliance**
- Computer Fraud and Abuse Act (CFAA)**, 255
- Computer Security Act of 1987**, 256
- confidentiality**
 - cryptosystems, 362
 - data, 119, 276
 - vulnerabilities, 130
- confidentiality, integrity, and availability (CIA)**, 362
- configuration management (CM) NIST SP 800-53 control family**, 259
- connections**
 - devices, 431
 - hosts, 21-23
 - SSL, 178
 - VPNs, 176
- containment techniques**, 240-241
- context-based authentication**, 304-305
- contingency planning (CP) NIST SP 800-53 control family**, 259
- continual improvement (processes)**, 356
- continuous monitoring procedures**, 284
- control flow graph**, 390
- Control Objectives for Information and Related Technology (COBIT) framework**, 263-264
- controlled security mode**, 83
- controls. *See also* countermeasures**
 - access, 282-284
 - categories, 277-278
 - CIS, 397
 - compensative, 277
 - corrective, 277

- detective, 277
- deterrent, 277
- developing, 286
- directive, 277
- handling risk, 278
- operational, 107
- preventive, 278
- recovery, 278
- selecting
 - access controls*, 282-284
 - handling risk*, 278
 - organizationally defined parameters*, 281
 - qualitative risk analysis*, 280
 - quantitative risk analysis*, 279
 - safeguards, selecting*, 280-281
 - total risk vs. residual risk*, 281
- technical, 107
- testing procedures, 286
- copyright, 198**
- Copyright Management Information (CMI), 199**
- corporate confidential data, 199-201**
- corporate policy requirements, 119**
- corrective actions, 245**
- corrective controls, 277**
- corrective countermeasures, 83**
- cost-benefit analysis, 280-281**
- countermeasures**
 - access, 84-86
 - ACLs, 80-81
 - ARP poisoning, 165
 - buffer overflow attacks, 157
 - categories, 83-84
 - click-jacking, 153
 - cloud viruses, 417
 - control selection
 - access controls*, 282-284
 - handling risk*, 280-281
 - organizationally defined parameters*, 281
 - qualitative risk analysis*, 280
 - quantitative risk analysis*, 279
 - total risk vs. residual risk*, 281
 - controls
 - categories*, 277-278
 - development*, 286
 - handling risk*, 278
 - testing procedures*, 286
 - CSRFs, 152
 - data remnants, 243
 - defined, 69
 - endpoint
 - security*, 77-78
 - vulnerabilities*, 162
 - group policies, 78-79
 - hardening, 82
 - compensating countermeasures*, 83-86
 - MAC*, 82-83
 - patching*, 86
 - unused ports/services, blocking*, 86
 - honeypots, 77
 - integer overflow attacks, 160
 - MAC overflow attacks, 164
 - maintenance hooks, 149
 - malware. *See* anti-malware software
 - NAC, 86
 - 802.1x*, 88-90
 - access decisions*, 87
 - agents/agentless*, 88
 - limitations*, 87
 - quarantine/remediation*, 88
 - network segmentation, 72
 - DMZs*, 73
 - extranet*, 72
 - intranet*, 72
 - jump boxes*, 76-77
 - LANs*, 72
 - system isolation*, 75-76
 - VLANs*, 73-74
 - race conditions, 160
 - safeguard selection, 280-281
 - sensitive data storage attacks, 157
 - session hijacking, 153
 - sinkholes, 81-82
 - social engineering threats, 310
 - spam, 417
 - spyware, 416
 - SQL injection attacks, 156
 - time-of-check/time-of-use attacks, 150
 - viruses, 415
 - VLAN
 - hopping*, 166
 - vulnerabilities*, 167
 - VM escape attacks, 170
 - XSS, 151
- CP (contingency planning) NIST SP 800-53 control family, 259**
- CPE (Common Platform Enumeration), 128**
- cracking passwords, 445-446**
- credentials**
 - management (personnel), 308-309
 - vulnerability scanning tools, 125
- credit card data, 195-197**

- credit history, 307
 - CredSSP (Credential Security Support Provider), 326
 - crime tape (forensics kits), 204
 - criminal history checks, 306
 - criticality
 - assets, 120, 192
 - data, 275
 - levels, 192
 - resources, 192
 - system process, 193
 - cross-certification model (federations), 327
 - cross-site request forgeries (CSRFs), 151-152
 - cross-site scripting (XSS), 150-151, 335
 - cross-training personnel, 356
 - cryptography, 362
 - applying, 371
 - authentication, 362
 - authorization, 363
 - CIA, 362
 - confidentiality, 362
 - defense-in-depth strategy, 363-364
 - hashing functions, 369-371
 - integrity, 363
 - keys, 363-364
 - non-repudiation, 363
 - tools (forensic investigation suites), 207
 - transport encryption, 372-373
 - types, 364-368
 - asymmetric algorithms*, 366-367
 - hybrid ciphers*, 367-368
 - symmetric algorithms*, 364-365
 - CSMA/CA (carrier sense multiple access with collision avoidance), 43-45
 - CSRFs (cross-site request forgeries), 151-152
 - customizing practice tests, 455-456
 - CVE (Common Vulnerabilities and Exposures), 128
 - CVSS (Common Vulnerability Scoring System), 128-130
 - CWE (Common Weakness Enumeration), 128
 - Cybersecurity framework, 259
- ## D
-
- DAI (dynamic ARP inspection), 165
 - DAP (Directory Access Protocol), 319
 - data
 - analysis. *See* data analysis
 - accounting, 200
 - aggregation, 346
 - architecture domain (TOGAF), 266
 - classification
 - policies*, 274-277
 - requirements*, 119-120
 - exfiltration, 229-230
 - flow analysis, 390
 - haven, 258
 - integrity, 193
 - loss prevention (DLP), 230
 - mining warehouses, 161
 - ownership policies, 272
 - remnants, 170, 243
 - retention policies, 272-273
 - sensitive, 156
 - transport encryption, 372-373
 - types, 194
 - corporate confidential*, 199-201
 - intellectual property*, 197-199
 - payment card information*, 195-197
 - PHI*, 195
 - PII*, 194
 - vulnerability scanning tools, 126
 - data analysis, 346
 - anomaly, 45
 - availability, 46
 - behavioral, 47
 - heuristic, 46
 - historical, 347
 - output, 47
 - event logs*, 53-55
 - firewall logs*, 47-49
 - IDS*, 56-60
 - NetFlow analyzer*, 61
 - packet analyzer*, 59-60
 - packet captures*, 49-50
 - ping scanning*, 52
 - port scanning*, 52-53
 - resource monitoring*, 61
 - Syslog*, 55-56
 - point-in-time, 40
 - NetFlow*, 41-42
 - packet analysis*, 40
 - protocol analysis*, 40
 - traffic analysis*, 40-41
 - wireless*, 43-45
 - tools, 103
 - trends, 46, 346-347
 - Data Protection Directive (EU), 257**
 - database server vulnerabilities, 160-161**

- DC (domain component), 320**
- dd command, 447**
- DDoS (distributed denial-of-service) attacks, 312**
- debugging malware, 241**
- decompiling malware, 241**
- dedicated security mode, 82**
- defense-in-depth strategy, 354**
 - network design, 374-377
 - network segmentation, 377
 - personnel, 354-356
 - processes, 356-357
 - technologies, 358
 - automated reporting, 358*
 - cryptography*. *See cryptography*
 - outsourcing, 360-362*
 - security devices, 358-359*
 - security suites, 359*
- degrading functionality, 135**
- delegation, 317**
- delete program tool, 436**
- demilitarized zones (DMZs), 29, 73**
- Deming cycle, 357**
- denial-of-service (DoS) attacks, 14, 312**
- deprovisioning federated identity systems, 333**
- designing**
 - networks, 374-377
 - software, 388, 397-398
- destination field (firewall logs), 349**
- destination (Syslogs), 351**
- destruction (data), 243**
- detective countermeasures, 83, 277**
- deterrent countermeasures, 84, 277**
- develop phase (SDLC), 389**
- developing software. *See* SDLC**
- devices**
 - availability analysis, 46
 - connectivity, 431
 - defense-in-depth strategy, 358-359
 - disposing, 242
 - IP configurations, viewing, 433
 - mobile
 - forensic tools, 445*
 - vulnerabilities, 173-174*
 - network
 - design, 374-377*
 - infrastructure, 162-168*
 - vulnerabilities, 169*
 - physical, 13
 - reconstructing, 242
 - removing, 241
 - rogue, 223-224
 - sanitization, 242
 - virtual. *See* virtualization
 - virtual infrastructure, 169-173
- DHCP snooping, 165**
- digital forensics kits, 201-204**
- direct object references, 150**
- directive countermeasures, 84, 277**
- Directory Access Protocol (DAP), 319**
- directory services, 319-322**
 - AD, 320
 - DNS, 322
 - LDAP, 319
 - SESAME, 321
- disassembling malware, 241**
- discovery**
 - scans, 122
 - services, 6
 - topology, 5
- distributed denial-of-service (DDoS) attacks, 312**
- distribution (reports), 132**
- DLP (data loss prevention), 230**
- DMZs (demilitarized zones), 29, 73**
- DNS (Domain Name System), 322**
 - records, 8-10
 - servers, testing, 434
- DNSSEC (Domain Name System Security Extensions), 322**
- documentation**
 - forensics kits, 204
 - OEM, 104
- documents (security policies)**
 - account management, 273-274
 - AUP, 271-272
 - data
 - classification, 274-277*
 - ownership, 272*
 - retention, 272-273*
 - passwords, 268-271
- domain component (DC), 320**
- Domain Name System. *See* DNS**
- Domain Name System Security Extensions (DNSSEC), 322**
- domains**
 - COBIT, 263
 - TOGAF, 266

DoS (denial-of-service)
 attacks, 14, 312
 double blind penetration
 testing, 99
 double tagging VLANs, 167
 downstream liability, 360
 downtime, 191-192
 drive adapters, 204
 drive capacity consumption,
 227
 driving records, 307
 DTP (Dynamic Trunking
 Protocol), 166
 dual control (personnel),
 355
 dual-homed firewalls, 29,
 411
 due care, 360
 due diligence, 360
 dumpster diving, 311
 dynamic ARP inspection
 (DAI), 165
 Dynamic Trunking
 Protocol (DTP), 166

E

-e argument (netstat
 command), 23
 -e parameter (netstat
 command), 431
 eavesdropping, 428
 Economic Espionage Act of
 1996, 257
 economic impact
 (incidents), 193
 ECPA (Electronic Commu-
 nications Privacy Act of
 1986), 255
 education verification (per-
 sonnel), 307
 EEOC (Equal Employment
 Opportunity Com-
 mission), 307
 Electronic Security
 Directive (EU), 258
 e-mail
 harvesting, 7
 pass-around reviews, 393
 emanations, 313
 EMET (Enhanced Miti-
 gation Experience
 Toolkit), 418
 Employee Privacy Issues
 and Expectation of
 Privacy, 257
 employment agreements/
 policies, 308
 employment candidate
 screenings, 306-308
 Encapsulating Security
 Payload (ESP), 177, 373
 EnCase Forensic, 444
 encryption, 24
 endpoints, 77-78
 DLP, 230
 SAs, 178
 threats, 310-312
malware, 311
rogue access points, 312
rogue endpoints, 311
social engineering,
 310-311
 vulnerabilities, 161-162
 Enhanced Mitigation Expe-
 rience Toolkit (EMET),
 418
 environmental recon-
 naissance
 defined, 3
 DNS harvesting, 8-10
 e-mail harvesting, 7
 logs, reviewing, 6
 OS fingerprinting, 5
 packet capture, 6
 phishing, 11
 routers, reviewing, 6
 service discovery, 6
 social engineering, 8
 social media profiling, 7
 tools, 16
firewalls, 27-30
HIDS, 27
host scanning, 19
IDS, 25-26
IPS, 26
netstat command, 21-23
network mapping, 20
NIDS, 27
packet analyzer, 23-24
port scanning, 16-19
syslog, 30
vulnerability scanners,
 30-31
 topology discovery, 5
 variables, 11
cloud resources, 15-16
*internal vs. external
 resources*, 14-15
on-premises resources, 15
physical devices, 13
virtualization, 13-14
wired networks, 12
wireless networks, 12
 environmental vulner-
 abilities, 129
 Equal Employment Oppor-
 tunity Commission
 (EEOC), 307
 eradication techniques,
 242-243
 escalation
 lists, 206
 privileges, 335
 ESP (Encapsulating
 Security Payload), 177,
 373
 essential data, 275
 established host con-
 nection, 22

Ethernet II (packets), 50

EU (European Union)

regulatory legislation, 257

evaluations, 290

event logs

analyzing, 352-353

output analysis, 53-55

evidence production procedures, 285

exceptions

management procedures, 287

vulnerability scans, identifying, 146

web servers handling, 156

executive reports, 132, 358

exploits, 441-442

identity and access management, 334

impersonation, 334

man-in-the-middle, 334

privilege escalation, 335

rootkits, 335-336

session hijacking, 335

XSS, 335

penetration testing, 101

tools, 440

exploit framework, 441-442

fuzzers, 442

interception proxy, 440

Extensible Access Control Markup Language (XACML), 327-329

external penetration testing, 99

external resources, 14-15

extranet, 72

F

-f argument (netstat command), 23

facility (Syslogs), 350

Fair Credit Reporting Act (FCRA), 306

false positives, 145

FCRA (Fair Credit Reporting Act), 306

Federal Information Security Management Act (FISMA), 256

Federal Intelligence Surveillance Act of 1978 (FISA), 255

Federal Privacy Act of 1974, 255

federations, 327

OpenID, 331-332

provisioning/deprovisioning, 333

SAML, 330-331

self-service password resets, 334

Shibboleth, 332

SPML, 329

XACML, 327-329

file analysis tools, 103

File Fuzzer, 442

file shares, viewing, 436

FIN scans, 17

fin-wait-1 host connection, 22

fin-wait-2 host connection, 22

final review plan, 457

fingerprinting

networks, 20

software, 104

firewall field (firewall logs), 349

firewalls, 408

architecture, 29-30

bastion hosts, 410

dual-homed, 411

multihomed, 412

screened host, 413

screened subnet, 414

Check Point, 415

Cisco, 415

DMZs, 29

dual-homed, 29

environmental reconnaissance, 27

kernel proxy, 29

logs

analyzing, 348-350

data, 47-49

multihomed, 29

next-generation, 375-377

packet-filtering, 27

Palo Alto, 415

placement, 409

proxy, 28

reviewing, 6

screened host, 30

screened subnet, 30

SOCKS, 28

stateful, 28

three-legged, 29

types, 27-29, 408

web application (WAF), 418-419

FISA (Federal Intelligence Surveillance Act of 1978), 255

FISMA (Federal Information Security Management Act), 256

Flash Card mode (practice test), 455

“Forensic Examination of Digital Evidence: A Guide for Law Enforcement,” 204

Forensic Toolkit (FTK), 444

forensics

kits, 201

cables, 203*cameras*, 204*crime tape*, 204*documentation/forms*, 204*drive adapters*, 204*tamper-proof seals*, 204*wiped removable media*,
204*workstations*, 202-203*write blockers*, 203

suites, 206-207, 443-445

analysis utilities, 206*Cellebrite*, 445*chain of custody*, 207*cryptography utilities*, 207*EnCase*, 444*FTK*, 444*hashing utilities*, 207*Helix*, 444*imaging utilities*, 206*log viewer utilities*, 207*mobile devices utilities*, 207*OS/process analysis
utilities*, 207*password crackers*, 207*Sysinternals*, 444

tools

hashing, 445*imaging*, 447*password cracking*,
445-446**Framework for Improving
Critical Infrastructure
Cybersecurity**, 259**frameworks**, 258

COBIT, 263-264

exploit, 441-442

ISO/IEC 27000 Series,
260-263

ITIL, 267

NIST, 258-259

profiles (Cybersecurity
framework), 260

SABSA, 265

TOGAF, 265-266

frequencycontext-based authenti-
cation, 305

vulnerability scans, 120-121

FTK (Forensic Toolkit),
444**full-knowledge penetration
tests**, 100**functions**

criticality levels, 192

hashing, 368-371

fuzzers, 442**fuzzing**, 391-392**G****-g argument (netstat
command)**, 23**gathering requirements
phase (SDLC)**, 388**generation-based fuzzing**,
392**GLBA (Gramm-Leach-
Bliley Act of 1999)**, 118,
255**Google Wallet**, 196**government data classifi-
cations**, 119, 276-277**GPOs (group policy
objects)**, 78**GPRS (General Packet
Radio Service)**, 178**graphical passwords**, 269**graphing traffic flows**, 437**group policies**, 78-79**guest vulnerabilities (virtu-
alization)**, 13**H****-h argument (netstat
command)**, 22**handling risk**, 278

qualitative risk analysis, 280

quantitative risk analysis,
279safeguards, selecting,
280-281total risk vs. residual risk,
281**hardening systems**, 82compensating counter-
measures, 83-84*access controls*, 84-86*control categories*, 83-84

MAC, 82-83

patching, 86

unused ports/services,
blocking, 86**hardware**

authenticity, 103

OEM documentation, 104

safety/integrity, checking,
103-104Trusted Foundry program,
104**harvesting**

DNS records, 8-10

e-mail addresses, 7

hashing, 369-371

forensics, 445

integrity, 368

one-way, 369

process, 369

SHA, 371

tools, 207

**Health Care and Education
Reconciliation Act of
2010**, 257

- Health Insurance Portability and Accountability Act of 1996 (HIPAA)**, 118, 195, 254
- Helix**, 444
- heuristic analysis**, 46
- heuristic based IDS**, 26
- HIDS (host intrusion detection system)**, 27, 436
- HIPAA (Health Insurance Portability and Accountability Act)**, 118, 195, 254
- HIPS (host-based IPS)**, 408
- historical data analysis**, 347
- honeypots**, 77
- horizontal privilege escalation**, 335
- host-based IPS (HIPS)**, 408
- hosts**
- application indicators, 230-231
 - bastion, 29, 410
 - connections
 - improper active, identifying*, 22-23
 - states, identifying*, 21-22
 - incident indicators, 225
 - data exfiltration*, 229-230
 - drive capacity consumption*, 227
 - malicious processes*, 229
 - memory consumption*, 227
 - processor consumption*, 226
 - unauthorized changes*, 229
 - unauthorized privileges*, 229
 - unauthorized software*, 228
 - scanning, 19
 - screened host firewalls, 413
 - Summary report, 143
 - virtual, 169-170
 - vulnerabilities, 13
- HR departments**, 216
- HTTP (Hypertext Transfer Protocol)**, 372
- HTTPS (Hypertext Transfer Protocol Secure)**, 372
- human interfaces**, 180
- hybrid ciphers**, 367-368
- hypervisor attacks**, 13, 171-173
-
- I**
- i argument (netstat command)**, 23
- IA (identification and authentication) NIST SP 800-53 control family**, 259
- IAM (identity and access management)**, 316
- ICMP sweeps**, 225
- ICS (industrial control system)**, 179-180
- IDaaS (Identity as a Service)**, 316
- identification and authentication (IA) NIST SP 800-53 control family**, 259
- identities**, 305
- applicants, 316-319
 - endpoints, 310-312
 - exploits, 334-336
 - federations. *See* federations
 - management policies, 274
 - personnel, 306-309
 - propagation, 326-327
 - providers (IPs), 332
 - RBAC, 315-316
 - repositories, 319
 - directory services*, 319-322
 - RADIUS*, 323-324
 - TACACS+*, 323-325
 - servers, 312-313
 - services, 313-315
- identity and access management (IAM) software**, 316
- Identity as a Service (IDaaS)**, 316
- identity theft**, 311
- Identity Theft Enforcement and Restitution Act**, 255
- ID-FF (Liberty Identity Federation Framework)**, 330
- IDS (Intrusion Detection Systems)**, 25, 405-407
- anomaly based, 26
 - as collective tool, 436
 - Bro, 407
 - environmental reconnaissance, 25-26
 - host-based, 27, 436
 - network-based. *See* NIDS
 - output analysis, 56-57, 60
 - signature based, 25
 - Snort, 406
 - Sourcefire, 405
- IEC (International Electrotechnical Commission)**, 260
- ifconfig command**, 434
- IKE (Internet Key Exchange)**, 177
- imaging tools**, 103, 206, 447
- impersonation**, 334
- Imperva**, 421
- implementation tiers (Cybersecurity framework)**, 260
- important resources**, 192
- imprecise methods (DLP)**, 230
- inadequate VM isolation attacks**, 14

incident responses

- forms, 206
- NIST SP 800-53 control family, 259
- provider responsibilities, 220
- role-based responsibilities, 218-220
- stakeholders, 216
 - communication*, 217-218
 - HR departments*, 216
 - legal departments*, 217
 - management*, 217
 - marketing departments*, 217
- teams, 216-217

incidents

- application-related indicators, 230-231
- classifications, 189-190
- data types, 194
 - corporate confidential*, 199-201
 - intellectual property*, 197-199
 - payment card information*, 195-197
 - PHI*, 195
 - PII*, 194
- forensics
 - kits*, 201-204
 - suites*, 206-207
- host-related indicators, 225
 - data exfiltration*, 229-230
 - drive capacity consumption*, 227
 - malicious processes*, 229
 - memory consumption*, 227
 - processor consumption*, 226
 - unauthorized changes*, 229
 - unauthorized privileges*, 229
 - unauthorized software*, 228

- network-related indicators, 220
 - bandwidth consumption*, 221
 - beaconing*, 221
 - irregular peer-to-peer communication*, 222-223
 - rogue devices*, 223-224
 - scan sweeps*, 224
 - unusual traffic spikes*, 225
- response and recovery
 - containment techniques*, 240-241
 - corrective actions*, 245
 - eradication techniques*, 242-243
 - plans*, 205, 245
 - summary report*, 246
 - validation techniques*, 243-244
- scope, 191
 - data integrity*, 193
 - downtime/recovery time*, 191-192
 - economic impact*, 193
 - system process criticality*, 193
- severity/prioritization, 191
- industrial control system (ICS), 179**
- inference, 160**
- Information Technology Infrastructure Library (ITIL), 267**
- Infrastructure Mode wireless networks, 43**
- infrastructure vulnerabilities, 162**
 - ARP poisoning, 164-165
 - MAC overflow, 164
 - routers, 168
 - switches, 163

- virtualization, 169
 - hosts*, 169-170
 - management interfaces*, 171-173
 - networks*, 170
- VLANs, 165-168
- inhibitors, 134-135**
- initialization vectors (IVs), 366**
- input validation, 154, 394-395**
- insecure direct object references, 150**
- integer overflow attacks, 159**
- integrity**
 - cryptography, 368
 - cryptosystems, 363
 - data, 193
 - hardware, 103-104
 - software, 104-105
 - vulnerabilities, 130
- intellectual property, 197-199**
- interactive mode (nslookup), 435**
- interception proxies**
 - exploit capabilities, 440
 - monitoring capabilities, 439-440
 - software development testing, 392
- interconnected networks vulnerabilities, 174-175**
- interface field (firewall logs), 349**
- internal penetration testing, 99**
- internal resources, 14-15**
- International Electrotechnical Commission (IEC), 260**

- International Organization for Standardization (ISO), 260**
- Internet Key Exchange (IKE), 177**
- Internet Protocol version 4 (packets), 50**
- Internet Security Association and Key Management Protocol (ISAKMP), 177**
- interval argument (netstat command), 22**
- intranet, 72**
- Intrusion Detection Systems. *See* IDS**
- Intrusion Prevention Systems. *See* IPS**
- inventory assets, 120**
- IP (identity provider), 332**
- IP (Intellectual Property), 199, 433**
- ipconfig command, 433-434**
- IPS (Intrusion Prevention Systems), 25, 405**
- environmental reconnaissance, 26
 - host-based (HIPS), 408
- IPsec, 177, 373**
- irregular peer-to-peer communication, 222-223**
- ISAKMP (Internet Security Association and Key Management Protocol), 177**
- ISO (International Organization for Standardization), 260**
- ISO/IEC 27000 Series, 260-263**
- ISO/IEC 27001 certification standard, 292-293**
- ISO/IEC 27002 certification standard, 294**
- isolated state (ports), 377**
- isolation**
- incident containment, 240
 - reverse engineering
 - malware analysis, 103
 - systems, 75-76
- ITIL (Information Technology Infrastructure Library), 267**
- IVs (initialization vectors), 366**
-
- J**
-
- job rotation (personnel), 356**
- John the Ripper password cracker, 445**
- jump boxes, 76-77**
-
- K**
-
- KDC (key distribution center), 317**
- Kennedy-Kassebaum Act, 118, 195, 254**
- Kerberos**
- advantages/disadvantages, 321
 - delegation, 317
 - KDC, 317
- kernel**
- debugger, 241
 - proxy firewalls, 29, 409
- keys**
- cryptosystems, 363-364
 - PKI, 178
 - wireless key loggers, 224
- Kiwi Syslog, 423**
- known threats, 190**
-
- L**
-
- L2TP (Layer 2 Tunneling Protocol), 176**
- LAN (local area network), 72**
- LAN Manager (LM), 271**
- last-ack host connection, 22**
- law enforcement responsibilities (incident responses), 219**
- LDAP (Lightweight Directory Access Protocol), 319**
- legal departments, 217**
- legislation**
- Basel II, 256
 - CALEA, 256
 - CFAA, 255
 - Computer Security Act of 1987, 256
 - Economic Espionage Act of 1996, 257
 - ECPA, 255
 - Employee Privacy Issues and Expectation of Privacy, 257
 - EU, 257
 - Federal Privacy Act of 1974, 255
 - FISA, 255
 - FISMA, 256
 - GLBA, 255
 - Health Care and Education Reconciliation Act of 2010, 257
 - HIPAA, 254
 - PIPEDA, 256
 - security requirements, 117
 - SOX, 254
 - United States Federal Sentencing Guidelines of 1991, 256
 - USA PATRIOT Act, 257
- lessons learned reports, 245**
- lexical analysis, 390**
- Liberty Alliance, 330**
- Liberty Identity Federation Framework (ID-FF), 330**

licensure verification (personnel), 307

life cycles

- access control provisioning, 274
- patching, 286

Lightweight Directory Access Protocol (LDAP), 319

Linux

- Bro, 407
- ifconfig command, 434
- Nikto, 427
- passwords, 270
- tcpdump, 429

listen host connections, 21

listening ports, viewing, 430

live VM migration attacks, 171

LM (LAN Manager), 271

local area networks (LANs), 72

Local Security Authority Subsystem Service (LSASS), 318

location

- access decisions, 88
- context-based authentication, 304
- firewalls, 409

log viewers (forensic investigation suites), 207

logged on users, viewing, 436

logical controls, 84-85, 283

logon sessions, listing, 436

LogonSessions tool, 436

logs

- analyzers, 103
- application, 53
- audit, 309
- authentication, 351

collecting from log generators, 57-58

event

- analyzing, 352-353*
- output analysis, 53-55*

firewalls

- analyzing, 348-350*
- data, 47-49*

manual reviews, 348

- authentication logs, 351*
- event logs, 352-353*
- firewall logs, 348-350*
- Syslogs, 350-351*

reviewing, 6

security, 53, 244

syslog

- analyzing, 350-351*
- environmental reconnaissance, 30*
- output analysis, 55-56*

system, 53

LSASS (Local Security Authority Subsystem Service), 318

M

-m argument (netstat command), 23

MAC (mandatory access control), 82-83, 164

maintenance

- accounts, 149
- hooks, 149
- NIST SP 800-53 control family, 259
- software development, 395

malicious processes, 229

malware

- analysis, 102-103
- anti-malware software, 416-417
- endpoints, 311

reverse engineering, 241
types, 311

MAM (mobile application management), 173

man-in-the-middle attacks, 178, 334

managed security service providers (MSSPs), 362

management interface vulnerabilities, 171-173

management responsibilities (incident responses), 219

mandatory access control (MAC), 82-83, 164

mandatory vacations, 356

manual distribution reports, 132

manual log reviews, 348

- authentication logs, 351
- event logs, 352-353
- firewall logs, 348-350
- Syslogs, 350-351

manual peer reviews (software), 393

marketing departments, 217

maturity model, 291

maximum period time of disruption (MPTD), 192

maximum tolerable downtime (MTD), 192

MBSA (Microsoft Baseline Security Analyzer), 427

MD algorithms, 370

MD5 hashing algorithm, 445

MDM (mobile device management), 173

mean time between failures (MTBF), 192

mean time to repair (MTTR), 192

- media protection (MP)**
NIST SP 800-53 control family, 259
- memorandum of understanding (MOU), 134**
- memory**
consumption, 227
overflows, 231
- mergers, 200**
- message digests, 369**
- Metasploit framework, 441**
- Microsoft Baseline Security Analyzer (MBSA), 427**
- Microsoft SDL File/Regex Fuzzer, 442**
- Microsoft Security Compliance Manager (SCM), 285**
- Microsoft System Center Configuration Manager (MSCCM), 285**
- military data classifications, 276-277**
- mitigating risks, 278**
- mobile application management (MAM), 173**
- mobile code, 312**
- mobile devices**
forensic tools, 207, 445
management (MDM), 173
vulnerabilities, 173-174
- mobile hacking gear, 224**
- ModSecurity, 420**
- monitoring (personnel accountability), 309**
- monitoring tools, 437-439**
Cacti, 439
MRTG, 437
Nagios, 438
NetFlow Analyzer, 439
SolarWinds, 438
- MOU (memorandum of understanding), 134**
- MP (media protection)**
NIST SP 800-53 control family, 259
- MPTD (maximum period time of disruption), 192**
- MRTG (Multi Router Traffic Grapher), 437**
- MSCCM (Microsoft System Center Configuration Manager), 285**
- MSSPs (managed security service providers), 362**
- MTBF (mean time between failures), 192**
- MTD (maximum tolerable downtime), 192**
- MTTR (mean time to repair), 192**
- multihomed firewalls, 29, 412**
- multilevel security mode, 83**
- Multi Router Traffic Grapher, 437**
- mutation fuzzing, 392**
- MX records (DNS), 8**
- N**
-
- n argument (netstat command), 23**
- n parameter (netstat command), 431**
- NAC (network access control), 86**
802.1x, 88-90
access decisions, 87
agents/agentless, 88
limitations, 87
quarantine/remediation, 88
- Nagios, 438**
- National Information Assurance Certification and Accreditation Process (NIACAP), 292**
- National Institute of Standards and Technology. See NIST**
- NAXSI (Nginx Anti XSS & SQL Injection), 420**
- NDAs (nondisclosure agreements), 198**
- near field communication (NFC), 196**
- Nessus, 425**
- NetFlow Analyzer, 61, 439**
- netstat command, 21-23, 430-431**
- Network General, 429**
- networks**
access control. *See* NAC
capture tools, 103
design, 374-377
device vulnerabilities, 169
DLP, 230
incident indicators, 220
bandwidth consumption, 221
beaconing, 221
irregular peer-to-peer communication, 222-223
rogue devices, 223-224
scan sweeps, 224
unusual traffic spikes, 225
- infrastructure vulnerabilities, 162
ARP poisoning, 164-165
MAC overflow, 164
routers, 168
switches, 163
VLANs, 165-168
- interconnected, 174-175
intrusion detection system. *See* NIDS
intrusion prevention system (NIPS), 375
mapping, 20
scanning tools, 423

- segmentation, 72, 377
 - DMZs*, 73
 - extranet*, 72
 - intranet*, 72
 - jump boxes*, 76-77
 - LANs*, 72
 - system isolation*, 75-76
 - VLANs*, 73-74
 - VPNs
 - ICS*, 179-180
 - SCADA*, 179-180
 - vulnerabilities*, 175-179
 - vulnerability tests (NVT), 426
 - New Technology LAN Manager (NTLM)**, 271
 - Nexpose**, 426, 442
 - NFC (near field communication)**, 196
 - NGFWs (next-generation firewalls)**, 375-377
 - Nginx Anti XSS & SQL Injection (NAXSI)**, 420
 - NIACAP (National Information Assurance Certification and Accreditation Process)**, 292
 - NIDS (network intrusion detection system)**, 374
 - environmental reconnaissance, 27
 - Bro, 407
 - Snort, 406
 - Nikto**, 427
 - NIPS (network intrusion prevention system)**, 375
 - NIST (National Institute of Standards and Technology)**, 180, 258
 - Cybersecurity framework, 259
 - SP 800-53 framework, 258-259
 - Nmap tool**, 423
 - host scanning, 19
 - ping scanning output analysis, 52
 - port scanning, 16-19, 52-53
 - non-credentialed vulnerability scans**, 125
 - non-critical assets**, 120
 - nondisclosure agreements (NDAs)**, 198
 - non-essential data**, 275
 - nonessential resources**, 192
 - noninteractive mode (nslookup)**, 434
 - non-repudiation**, 363
 - normal resources**, 192
 - NS records (DNS)**, 8
 - nslookup command**, 434-435
 - NTLM (New Technology LAN Manager)**, 271
 - Null scans**, 17
 - numeric passwords**, 269
 - NVT (network vulnerability tests)**, 426
-
- O**
- o argument (netstat command)**, 23
 - OAuth (Open Authorization)**, 318
 - OEM (original equipment manufacturer) documentation**, 104
 - on-premises resources**, 15
 - one-time passwords (OTP)**, 269
 - one-way hash functions**, 369
 - Open Authorization (OAuth)**, 318
 - OpenID**, 331-332
 - Open Source Security Information Management (OSSIM)**, 422
 - Open Web Application Security Project (OWASP)**, 396, 440
 - OpenSSL**, 319, 436
 - OpenVAS tool**, 426
 - operating system fingerprinting**, 5
 - operational controls**, 107
 - organizational unit (OU)**, 320
 - organizations**
 - governance, 135
 - requirements, 117
 - asset inventory*, 120
 - corporate policies*, 119
 - data classification*, 119-120
 - regulatory*, 117-118
 - original equipment manufacturer (OEM)**, 104
 - OS analysis tools (forensic investigation suites)**, 207
 - OS fingerprinting**, 5
 - OSSIM (Open Source Security Information Management)**, 422
 - OTP (one-time passwords)**, 269
 - OUs (organizational units)**, 320
 - outbound communication**, 231
 - output**
 - analysis, 47
 - event logs*, 53-55
 - firewall logs*, 47-49
 - IDS*, 56-57
 - packet captures*, 49-50
 - ping scanning*, 52
 - port scanning*, 52-53

- Syslog*, 55-56
 - tools*, 58-61
 - reconciling, 147
 - unexpected application, 231
 - vulnerability scans, analyzing, 143
 - correlating with other data points*, 147-148
 - reports*, 143-147
 - reviewing*, 145
 - outsourcing**
 - defense-in-depth strategy, 355, 360-362
 - third-party, 174
 - over-the-shoulder reviews**, 393
 - overflows**
 - buffers, 157-159, 312
 - integer, 159
 - MAC, 164
 - memory, 231
 - OWASP (Open Web Application Security Project)**, 396, 440
 - ownership (data)**, 272
- P**
-
- p argument (netstat command)**, 22-23
 - p parameter (netstat command)**, 431
 - P protocol argument (netstat command)**, 23
 - PAC (Privileged Attribute Certificate)**, 321
 - packet-filtering firewalls**, 27, 409
 - packets**
 - ACLs, compared, 81
 - analyzing, 40
 - environmental reconnaissance*, 23-24
 - output analysis*, 59-60
 - capture tools, 428-430
 - Aircrack-ng*, 429-430
 - Network General*, 429
 - tcpdump*, 429
 - Wireshark*, 428-429
 - capturing
 - environmental reconnaissance*, 6
 - output data*, 49-50
 - paths, tracing, 432
 - pair programming reviews**, 393
 - Palo Alto firewalls**, 415
 - parity bits**, 368
 - partial-knowledge penetration tests**, 100
 - partial regression testing**, 394
 - passive vulnerability scanner (PVS)**, 30
 - passphrase passwords**, 268
 - password crackers (forensic investigation suites)**, 207
 - passwords**, 268, 271
 - account lockout policies, 270
 - authentication period, 269
 - complexity, 270
 - cracking tools, 445-446
 - history, 269
 - length, 270
 - life, 269
 - Linux, 270
 - resetting, 270
 - types, 268-269
 - Windows, 271
 - patching**, 86, 243, 285-286
 - patents**, 197
 - pattern matching (IDS)**, 25
 - payment card information data**, 195-197
 - PCI-DSS (Payment Card Industry Data Security Standard)**, 118, 195
 - PDCA (Plan-Do-Check-Act)**, 357
 - PDP (policy decision point)**, 328
 - PE (physical and environmental protection) NIST SP 800-53 control family**, 259
 - Peach fuzzer**, 442
 - Pearson IT Certification test engine**, 453
 - Pearson Test Prep practice test**, 453
 - accessing, 454
 - customizing, 455-456
 - modes, 455
 - purchasing additional, 456
 - updating, 456
 - peer reviews (software)**, 393
 - peer-to-peer botnets**, 222
 - peer-to-peer communication**, 222-223
 - penetration testing**, 98
 - categories, 99
 - frequency, 98
 - internal vs external, 99
 - rules of engagement, 100-101
 - strategies, 99
 - tools, 100
 - PEP (policy enforcement point)**, 328
 - periodic reviews (personnel)**, 308
 - permissions**
 - incident validation, 244
 - vulnerability scanning, 131
 - personal health information (PHI)**, 195

- Personal Information Protection and Electronic Documents Act (PIPEDA), 256**
- personally identifiable information (PII), 194**
- personnel, 306-309**
 - accountability, 309
 - credential management, 308-309
 - defense-in-depth strategy, 354
 - cross-training, 356*
 - dual control, 355*
 - mandatory vacations, 356*
 - separation of duties, 355*
 - split knowledge, 355*
 - succession planning, 356*
 - third-party outsourcing, 355*
 - training, 354-355*
 - employment agreements policies, 308
 - employment candidate screenings, 306-308
 - periodic reviews, 308
 - provisioning life cycle, 309
 - security (PS) NIST SP 800-53 control family, 259
- pharming, 310**
- PHI (personal health information), 195**
- phishing, 11, 310**
- physical and environmental protection (PE) NIST SP 800-53 control family, 259**
- physical controls, 84-85, 282**
- physical devices, 13**
- PII (personally identifiable information), 194**
- ping command, 431-432**
- ping scanning, 19, 52**
- ping sweeps, 225**
- PIPEDA (Personal Information Protection and Electronic Documents Act), 256**
- PIX (Private Internet Exchange), 415**
- PKI (Public Key Infrastructure), 178**
- PL (planning) NIST SP 800-53 control family, 259**
- Plan-Do-Check-Act (PDCA), 357**
- planning (PL) NIST SP 800-53 control family, 259**
- PLCs (programmable logic controllers), 180**
- plug-ins, 128-130**
- PM (program management) NIST SP 800-53 control family, 259**
- point-in-time data analysis, 40**
 - NetFlow, 41-42
 - packets, 40
 - protocols, 40
 - traffic, 40-41
 - wireless, 43-45
- Point-to-Point Tunneling Protocol (PPTP), 176**
- policies, 268**
 - account management, 273-274
 - AUP, 271-272
 - BYOD (bring your own device), 173
 - data classification, 274
 - commercial business, 276*
 - criticality, 275*
 - essential/non-essential, 275*
 - military/government, 276-277*
 - sensitivity, 275*
- data ownership, 272
- data retention, 272-273
- decision point (PDP), 328
- employment, 308
- enforcement point, 328
- group, 78-79
- password, 268-271
- ports**
 - listening, viewing, 430
 - PVLANS, 377
 - scanning, 16, 52-53, 225
 - switch, 166
 - unused, blocking, 86
- power cables, 203**
- PPTP (Point-to-Point Tunneling Protocol), 176**
- Practice Exam mode (practice test), 455**
- practice test, 453**
 - accessing, 454
 - customizing, 455-456
 - modes, 455
 - purchasing additional exams, 456
 - updating, 456
- precise methods (DLP), 230**
- Premium Edition, 456**
- preventative tools, 405**
 - anti-malware software, 416
 - anti-spam software, 417
 - anti-spyware software, 416
 - antivirus software, 415
 - cloud antivirus software, 417
 - EMET, 418
 - firewalls, 408
 - bastion hosts, 410*
 - Check Point, 415*
 - Cisco, 415*
 - dual-homed, 411*
 - multihomed, 412*

- Palo Alto*, 415
- placement*, 409
- screened host*, 413
- screened subnet*, 414
- types*, 408
- HIPS, 408
- IDS, 405-407
 - Bro*, 407
 - Snort*, 406
 - Sourcefire*, 405
- IPS, 405
- web proxy servers, 418-421
 - Imperva*, 421
 - ModSecurity*, 420
 - NAXSI*, 420
 - WAF*, 418-419
- preventive counter-measures**, 84, 278
- Principles on Privacy (EU)**, 257
- prioritization (incidents)**, 191
 - data types, 194
 - corporate confidential*, 199-201
 - intellectual property*, 197-199
 - payment card information*, 195-197
 - PHI*, 195
 - PII*, 194
 - response actions, 147
 - scope, 191
 - data integrity*, 193
 - downtime/recovery time*, 191-192
 - economic impact*, 193
 - system process criticality*, 193
 - vulnerabilities, 133-134
- private data**, 119, 276
- Private Internet Exchange (PIX)**, 415
- private VLANs (PVLANS)**, 377
- Privileged Attribute Certificates (PACs)**, 321
- privileges**
 - elevation attacks, 171
 - escalation, 335
 - unauthorized, 229
- proactive threat indicators (PTI)**, 105
- procedures**, 284
 - continuous monitoring, 284
 - control development/testing, 286
 - evidence production, 285
 - exceptions, managing, 287
 - patching, 285-286
 - remediation plans, 287-288
- Process Explorer**, 226
- processes**
 - analysis tools (forensic investigation suites), 207
 - defense-in-depth strategy, 356-357
 - malicious, 229
- processor consumption**, 226
- product field (firewall logs)**, 349
- profiling social media**, 7
- program management (PM)**
 - NIST SP 800-53 control family, 259
- programmable logic controllers (PLCs)**, 180
- promiscuous state (ports)**, 377
- proprietary data**, 119
- protocol field (firewall logs)**, 349
- protocols**
 - analyzing. *See* packets, analyzing
 - anomaly based IDS, 26
 - DAP, 319
 - DTP, 166
 - HTTP, 372
 - HTTPS, 372
 - IPsec, 177, 373
 - L2TP, 176
 - LDAP, 319
 - PPTP, 176
 - SCP, 179
 - SHTTP, 372
 - SSH, 373
 - SSL, 372
 - Syslog, 55-56
 - TCP, 50
 - TLS, 372
- provisioning**
 - federated identity systems, 333
 - life cycle (personnel), 309
 - service providers (PSPs), 329
 - service targets (PSTs), 329
- proxies**
 - application-level, 28, 409
 - circuit-level, 28, 409
 - firewalls, 28
 - interception
 - exploit capabilities*, 440
 - monitoring capabilities*, 439
 - software development testing*, 392
 - kernel proxy firewalls, 409
 - monitoring tools, 440
 - web proxy servers, 418, 421
 - Imperva*, 421
 - ModSecurity*, 420

NAXSI, 420

WAF, 418-419

PS (personnel security)
 NIST SP 800-53 control family, 259

PsLoggedOn tool, 436

PSPs (provisioning service providers), 329

PSTs (provisioning service targets), 329

PTI (proactive threat indicators), 105

Public Company Accounting Reform and Investor Protection Act of 2002 (SOX), 117, 254

public data, 119, 276

Public Key Infrastructure (PKI), 178

purging data, 243

PVLANS (private VLANs), 377

PVS (passive vulnerability scanner), 30

Q

QRadar, 422

qualitative risk analysis, 280

quality control
 assessments, 290
 audits, 288-289
 certification, 291
ISO/IEC 27001, 292-293
ISO/IEC 27002, 294
NIACAP, 292
 evaluations, 290
 maturity model, 291

quality improvement, 357

Qualys, 425

quantitative risk analysis, 279

quarantine (counter-measures), 88

R

-r argument (netstat command), 22

-r parameter (netstat command), 431

RA (request authority), 329

RA (risk assessment) NIST SP 800-53 control family, 259

race conditions, 150, 160

RADIUS (Remote Authentication Dial-in User Service), 89, 323-324

Rapid7 Exploit Database, 441

RBAC (role-based access control), 88, 315-316

RDBMS (relational database management system), 326

real user monitoring (RUM), 391

reconciling output, 147

reconstructing devices, 242

recovery
 countermeasures, 84, 278
 point objective (RPO), 192
 time, 191-192

Red team (training), 105

reference checks (personnel), 307

Regex Fuzzer, 442

registry tools, 103

regression testing, 394

regulatory compliance, 254
 Basel II, 256
 CALEA, 256
 CFAA, 255
 Computer Security Act of 1987, 256
 Economic Espionage Act of 1996, 257

ECPA, 255

Employee Privacy Issues and Expectation of Privacy, 257

EU, 257

Federal Privacy Act of 1974, 255

FISA, 255

FISMA, 256

GLBA, 255

Health Care and Education Reconciliation Act of 2010, 257

HIPAA, 254

PIPEDA, 256

requirements, 117-118

SOX, 254

United States Federal Sentencing Guidelines of 1991, 256

USA PATRIOT Act, 257

relational database management system (RDBMS), 326

release/maintenance phase (software development), 395

relying parties (RPs), 331

remediation, 88, 133
 change control, 134
 communication, 134
 inhibitors, 134-135
 plan procedures, 287-288
 prioritizing, 133-134
 sandboxing, 134

Remote Authentication Dial-in User Service (RADIUS), 89, 323-324

remote terminal units (RTUs), 180

removable media, 204

removing devices, 241

reports

- automated, 358
- change, 132, 358
- distribution, 132
- executive, 132, 358
- formats, 143
- Hosts Summary, 143
- IDS, 56-57
- lessons learned, 245
- penetration testing, 101
- senior executive, 358
- SOC, 289-290
- technical, 132, 358
- trend, 132
- Vulnerabilities by Host, 144
- Vulnerabilities by Plug-in, 145
- vulnerability scanning, 132
- vulnerability scans, analyzing, 143-147
- repositories (identity), 319**
 - directory services, 319-322
 - AD*, 320
 - DNS*, 322
 - LDAP*, 319
 - SESAME*, 321
 - RADIUS, 323-324
 - TACACS+, 323-325
- request authorities (RAs), 329**
- resetting passwords, 270**
- residual risk, 281**
- resources**
 - cloud, 15-16
 - criticality levels, 192
 - internal vs. external, 14-15
 - monitoring, 61
 - on-premises, 15
- response actions, prioritizing, 147**
- response and recovery process (incidents)**

- containment techniques, 240-241
- corrective actions, 245
- eradication techniques, 242-243
- plans, 205, 245
- summary report, 246
- validation techniques, 243-244
- responsibilities (incident response role-based), 218-220**
- retention (data), 272-273**
- reverse engineering, 101**
 - hardware, 103-104
 - incident containment, 241
 - isolation, 103
 - sandboxing, 101-102
 - sheep dip computers, 102
 - software, 104-105
 - test beds, 102
- reviewing**
 - firewalls, 6
 - logs, 6
 - processes, 357
 - routers, 6
 - user accounts, 274
 - vulnerability scan results, 145
- risks**
 - appetite (vulnerability scans), 120
 - assessment (RA) NIST SP 800-53 control family, 259
 - handling, 278
 - acceptance*, 278
 - avoidance*, 278
 - mitigation*, 278
 - qualitative risk analysis*, 280
 - quantitative risk analysis*, 279

- safeguards, selecting*, 280-281
- total risk vs. residual risk*, 281
- transferring*, 278
- management, 106-107
- rogue access points, 12, 45, 224, 312**
- rogue devices, 223-224**
- rogue endpoints, 311**
- rogue switches, 224**
- role-based access control (RBAC), 88, 315-316**
- role-based responsibilities, 218-220**
- rootkits, 335-336**
- routers**
 - ACLs, 80
 - reviewing, 6
 - sinkholes, 81-82
 - vulnerabilities, 168
- RP (relying party), 331**
- RPO (recovery point objective), 192**
- RTO (recovery time objective), 192**
- RTUs (remote terminal units), 180**
- rule based access decisions, 87**
- rule based IDS, 26**
- rule field (firewall logs), 349**
- rules of engagement, 100-101**
- RUM (real user monitoring), 391**

S

- s argument (netstat command), 22**
- s parameter (netstat command), 431**

- SA (security association), 177-178
- SA (system and services acquisition) NIST SP 800-53 control family, 259
- SaaS (Software as a Service), 316, 362
- SABSA (Sherwood Applied Business Security Architecture) framework, 265
- safe harbor, 258
- Safe Harbor Privacy Principles (EU), 257
- safeguards. *See* countermeasures
- SAM (Security Account Manager), 271
- SAML (Security Assertion Markup Language), 330-331
- sandboxing
 - malware analysis, 101-102
 - tools, 103
 - vulnerability remediation, 134
- sanitization, 242
- SANS (SysAdmin, Audit, Network, and Security Institute), 396
- Sarbanes-Oxley Act (SOX), 117, 254
- SAS (Statement on Auditing Standards), 289
- SC (system and communications protection) NIST SP 800-53 control family, 259
- SCADA (supervisory control and data acquisition), 179-180
- scanning
 - assessment, 122
 - data output, 47
 - firewall logs*, 47-49
 - packet captures*, 49-50
 - ping scanning*, 52
 - port scanning*, 52-53
 - discovery, 122
 - hosts, 19
 - incident validation, 244
 - network tools, 423
 - ping, 52, 225
 - ports, 225
 - Nmap*, 16
 - output analysis*, 52-53
 - sweeps, 224
 - vulnerabilities. *See* vulnerabilities, scanning
 - web applications, 391
- SCAP (Security Content Automation Protocol), 128-130, 287
- SCM (Microsoft Security Compliance Manager), 285
- scope
 - incidents, 191
 - data integrity*, 193
 - downtime/recovery time*, 191-192
 - economic impact*, 193
 - system process criticality*, 193
 - penetration testing, 100
 - vulnerability scanning tools, 123
- SCP (Secure Copy Protocol), 179
- screened host firewalls, 30, 413
- screened subnet firewalls, 30, 414
- SDelete tool, 436
- SDLC (Software Development Life Cycle), 387
 - accreditation, 395
 - best practices
 - CIS*, 397-398
 - OWASP*, 396
 - SANS*, 396
 - certification, 395
 - change management, 395
 - design, 388
 - developing, 389
 - gathering requirements, 388
 - input validation, 394-395
 - planning/initiating projects, 387
 - release/maintenance phase, 395
 - testing, 390
 - fuzzing*, 391-392
 - interception proxies*, 392
 - manual peer reviews*, 393
 - regression*, 394
 - static code analysis*, 390
 - stress*, 393-394
 - unit testing*, 390
 - user acceptance*, 393
 - web application vulnerabilities*, 391
 - testing/validating, 389
- secret data, 119, 276
- Secure Copy Protocol (SCP), 179
- secure disposal, 242
- Secure European System for Applications in a Multi-vendor Environment (SESAME), 321
- Secure Hash Algorithm (SHA), 371, 445
- Secure Hypertext Transfer Protocol (SHTTP), 372
- Secure Sockets Layer (SSL), 178

security

assessment and authorization (CA) NIST SP 800-53 control family, 259
 associations (SAs), 177
 awareness training, 354
 data analytics, 346-347
 logs, 53
 modes, 82
 parameter index (SPI), 178
 regression testing, 394
 suites, 359

Security Account Manager (SAM), 271**Security Assertion Markup Language (SAML), 330-331****Security Content Automation Protocol (SCAP), 128-130, 287****Security Information and Event Management. *See* SIEM**

segmentation, 240

segmenting networks, 72, 377

DMZs, 73

extranet, 72

intranet, 72

jump boxes, 76-77

LANs, 72

system isolation, 75-76

VLANs, 73-74

self-service password resets, 270, 334**senior executive reports, 358****sensitive but unclassified data, 120, 277****sensitive data, 156, 275-276****sensitivity levels, 122****sensors, 179****separation of duties (personnel), 355****servers**

authentication, 88, 323

database, 160-161

DNS, 434

isolating, 75

jump, 76-77

Syslog, 55

threats, 312-313

vulnerability scanning tools, 126-127

web

proxy, 418-421

vulnerabilities, 149-160

service field (firewall logs), 349**service interruptions (applications), 231****service level agreements (SLAs), 135****Service Organization Control (SOC), 289****service providers (SPs), 332****Service Provisioning Markup Language (SPML), 329****services**

discovery, 6

threats, 313-315

unused, blocking, 86

SESAME (Secure European System for Applications in a Multi-vendor Environment), 321**session hijacking, 153, 335****setup logs, 53****severity (incidents), 191, 350**

data types, 194

corporate confidential, 199-201

intellectual property, 197-199

payment card information, 195-197

PHI, 195

PII, 194

scope, 191

data integrity, 193

downtime/recovery time, 191-192

economic impact, 193

system process criticality, 193

SHA (Secure Hash Algorithm), 371, 445**ShareEnum tool, 436****sheep dip computers, 102****Sherwood Applied Business Security Architecture (SABSA) framework, 265****Shibboleth, 332****shoulder surfing, 310****SHTTP (Secure Hypertext Transfer Protocol), 372****SI (system and information integrity) NIST SP 800-53 control family, 259****SIEM (Security Information and Event Management), 57-58, 244, 421**

AlienVault, 422

ArcSight, 421

incident recovery validation, 244

Kiwi Syslog, 423

log collection, 57-58

network design, 375

OSSIM, 422

QRadar, 422

Splunk, 422

signal cables, 203**signature-based IDS, 25****Simple Object Access Protocol (SOAP), 329**

- single loss expectancy (SLE), 279**
- single sign-on (SSO), 320**
- sinkholes, 81-82**
- site accreditation, 292**
- SLAs (service level agreements), 135**
- SLE (single loss expectancy), 279**
- sniffers, 428**
 - Aircrack-ng, 429-430
 - Network General, 429
 - tcpdump, 429
 - Wireshark, 428-429
 - WLANs, 45
- Snort, 406**
- SOA (Start of Authority), 8, 322**
- SOAP (Simple Object Access Protocol), 329**
- SOC (Service Organization Control), 289**
- social engineering threats, 8, 310-311**
- social media profiling, 7**
- Social Security verification (personnel), 307**
- SOCKS firewall, 28**
- software**
 - anti-malware, 416
 - anti-spam, 417
 - anti-spyware, 416
 - antivirus, 415
 - application-related incident indicators, 230-231
 - cloud antivirus, 417
 - development. *See* SDLC
 - DLP, 230
 - integrity, checking, 104-105
 - startup programs, viewing, 436
 - unauthorized, 228-230
 - vulnerability scanning updates/plugin-ins, 128-130
- Software as a Service (SaaS), 316, 362**
- Software Development Life Cycle. *See* SDLC**
- SolarWinds, 438**
- source field (firewall logs), 349**
- Sourcefire, 405**
- sources (Syslogs), 351**
- SOX (Sarbanes-Oxley Act), 117, 254**
- SP (service provider), 332**
- SPI (security parameter index), 178**
- SPL (Splunk Search Processing Language), 422**
- split knowledge (personnel), 355**
- Splunk, 422**
- Splunk Search Processing Language (SPL), 422**
- SPML (Service Provisioning Markup Language), 329**
- spoofing switches, 166**
- spyware, 311**
- SQL injection attacks, 155**
- SSAE (Statement on Standards for Attestation Engagements), 289**
- SSH, 373**
- SSL (Secure Sockets Layer), 178**
 - advantages/disadvantages, 179
 - implementing, 178
 - TLS, compared, 179
 - transport encryption, 372
- SSO (single sign-on), 320**
 - identity propagation, 326-327
 - OpenID, 331-332
 - provisioning/deprovisioning, 333
 - SAML, 330-331
 - self-service password reset, 334
 - Shibboleth, 332
 - SPML, 329
 - XACML, 327-329
- stakeholders (incident response), 216-217**
 - communication, 217-218
 - HR, 216
 - legal, 217
 - management, 217
 - marketing, 217
- standard word passwords, 268**
- Start of Authority (SOA), 322**
- startup programs, viewing, 436**
- stateful firewalls, 28**
- stateful matching (IDS), 25**
- Statement on Auditing Standards (SAS), 289**
- Statement on Standards for Attestation Engagements (SSAE), 289**
- states**
 - host connections, identifying, 21-22
 - PVLAN ports, 377
- static code analysis, 390**
- static passwords, 268**
- statistical anomaly based IDS, 26**
- step-up authentication, 304**
- stream-based ciphers, 365**
- stress testing software, 393-394**

strong identification (personnel accountability), 309

Study mode (practice test), 455

study plan, 457

Stuxnet virus, 180

subnets, 414

substance-abuse testing, 307

succession planning (personnel), 356

supervisory control and data acquisition (SCADA), 179

supplicants, 88, 323

switches

- rogue, 224
- spoofing, 166
- vulnerabilities, 163

symmetric algorithms, 364-365

- block ciphers, 365-366
- stream-based ciphers, 365

symptoms (incidents)

- application-related, 230-231
- host-related, 225-229
- network-related, 220-225

SYN flood attacks, 48

syn-received host connection, 21

syn-sent host connection, 21

synthetic transaction monitoring, 391

SysAdmin, Audit, Network, and Security Institute (SANS), 396

Sysinternals command, 435-436

- forensic tools, 444
- processor consumption, 226

Syslogs, 30

- analyzing, 350-351
- output analysis, 55-56

system and communications protection (SC) NIST SP 800-53 control family, 259

system and information integrity (SI) NIST SP 800-53 control family, 259

system and services acquisition (SA) NIST SP 800-53 control family, 259

systems

- access, viewing, 436
- accreditation, 292
- hardening, 82-86
- high security mode, 82
- isolating, 75-76
- logs, 53
- process criticality, 193

T

-t argument (netstat command), 22

TACACS+ (Terminal Access Controller Access Control System Plus), 89, 323-325

taint analysis, 390

tamper-proof seals (forensics kits), 204

target penetration testing, 99

Task Manager, 226

TCA (third-party connection agreement), 174

TCP (Transmission Control Protocol), 50

tcpdump command, 429

technical architecture domain (TOGAF), 266

technical controls, 107

technical reports, 132, 358

technical responsibilities (incident responses), 219

telemetry system, 180

TEMPEST program, 313

temporal vulnerabilities, 129

Terminal Access Controller Access Control System Plus (TACACS+), 89, 323-325

test beds, 102

test preparation

- Pearson IT Certification test engine, 453
- Pearson Test Prep practice test, 453
 - customizing*, 455-456
 - modes*, 455
 - offline access*, 454
 - online access*, 454
 - purchasing additional*, 456
 - updating*, 456

testing

- ACLs, 15
- controls, 286
- device connectivity, 431
- DNS servers, 434
- network vulnerabilities (NVT), 426
- penetration, 98
 - categories*, 99
 - frequency*, 98
 - internal vs external*, 99
 - rules of engagement*, 100-101
 - strategies*, 99
 - tools*, 100
- software, 389-390
 - fuzzing*, 391-392
 - interception proxies*, 392

- manual peer reviews, 393*
- regression, 394*
- static code analysis, 390*
- stress, 393-394*
- unit testing, 390*
- user acceptance, 393*
- web application vulnerabilities, 391*
- TGT (ticket-granting ticket), 321**
- The Open Group Architecture Framework (TOGAF), 265-266**
- third-party**
 - connection agreement (TCA), 174
 - IAM software, 316
 - incident response providers, 220
 - outsourcing, 174, 355, 360-362
- threats. *See also attacks***
 - applicants, 316-319
 - as identities, 317*
 - IAM software, 316*
 - OAuth, 318*
 - OpenSSL, 319*
 - classifications, 189-191
 - APTs, 191*
 - known threats, 190*
 - unknown threats, 190*
 - zero day, 190*
 - endpoints, 310-312
 - malware, 311*
 - rogue access points, 312*
 - rogue endpoints, 311*
 - social engineering threats, 310-311*
 - identity and access management
 - impersonation, 334*
 - man-in-the-middle, 334*
 - privilege escalation, 335*
 - rootkits, 335-336*
 - session hijacking, 335*
 - XSS, 335*
 - managing. *See counter-measures*
 - modeling, 106-107
 - RBAC, 315-316
 - servers, 312-313
 - services, 313-315
 - social engineering, 310-311
- three-legged firewalls, 29**
- ticket-granting ticket (TGT), 321**
- time**
 - access decisions, 87
 - context-based authentication, 304
 - penetration testing, 100
- time field (firewall logs), 349**
- time-of-check attacks, 150**
- time-of-use attacks, 150**
- Time to Live (TTL), 322**
- TLS (Transport Layer Security), 179, 372**
- TOGAF (The Open Group Architecture Framework), 265-266**
- tool-assisted code reviews, 393**
- tools**
 - analytical, 436
 - interception proxy, 439-440*
 - monitoring, 437-439*
 - vulnerability scanning, 437*
 - collective, 421
 - command-line, 430-436*
 - HIDS, 436*
 - IDS, 436*
 - network scanning, 423*
 - packet capture, 428-430*
 - SIEM, 421-423*
 - vulnerability scanning, 423-427*
- configuration, 103
- data analysis, 103
- environmental reconnaissance, 16
 - firewalls, 27-30*
 - HIDS, 27*
 - host scanning, 19*
 - IDS, 25-26*
 - IPS, 26*
 - netstat command, 21-23*
 - network mapping, 20*
 - NIDS, 27*
 - packet analyzer, 23-24*
 - port scanning, 16-19*
 - syslog, 30*
 - vulnerability scanners, 30-31*
- exploit, 440-442
- file analysis, 103
- forensic investigation suites
 - analysis utilities, 206*
 - chain of custody, 207*
 - cryptography utilities, 207*
 - hashing utilities, 207*
 - imaging utilities, 206*
 - log viewers utilities, 207*
 - mobile devices utilities, 207*
 - OS/process analysis utilities, 207*
 - password crackers, 207*
- forensics
 - hashing, 445*
 - imaging, 447*
 - password cracking, 445-446*
 - suites, 443-445*
- imaging, 103
- input validation, 394
- log analyzers, 103

- monitoring, 437
 - Cacti*, 439
 - MRTG*, 437
 - Nagios*, 438
 - NetFlow Analyzer*, 439
 - SolarWinds*, 438
- NetFlow, 61
- network captures, 103
- Nmap, 52-53
- output analysis
 - IDS*, 60
 - NetFlow analyzer*, 61
 - packet analyzer*, 59-60
 - resource monitoring*, 61
 - SIEM*, 57-58
- penetration testing, 100
- preventative, 405
 - anti-malware software*, 416
 - anti-spam software*, 417
 - anti-spyware software*, 416
 - antivirus software*, 415
 - cloud antivirus software*, 417
 - EMET*, 418
 - firewalls*, 408-415
 - HIPS*, 408
 - IDS*, 405-407
 - IPS*, 405
 - web proxy servers*, 418-421
- Process Explorer, 226
- registry, 103
- rootkits, 335-336
- sandboxing, 103
- Sysinternals
 - forensics*, 444
 - processor consumption*, 226
- Task Manager, 226
- tracert, 9
- vulnerability scanning, 122
 - credential vs. non-credentialed*, 125
 - data types*, 126
 - permissions/access*, 131
 - scope*, 123
 - sensitivity levels*, 122
 - server-based vs. agent-based*, 126-127
 - updates/plugin-ins*, 128-130
 - vulnerability feeds*, 123
- Whois, 9
- top secret data**, 119, 276
- topology discovery**, 5
- total risk**, 281
- tracert command**, 9, 432
- trade secrets**, 198
- trademarks**, 198
- traffic**
 - analyzing, 40-41
 - anomaly based IDS, 26
 - flows, 437
 - NetFlow analysis, 41-42
 - sinkholes, 81-82
 - trend analysis, 46
 - unencrypted, identifying, 24
 - unusual spikes, 225
- training**
 - personnel, 354-355
 - teams, 105-106
- Transaction Signature (TSIG)**, 322
- transferring risks**, 278
- translation field (firewall logs)**, 349
- Transmission Control Protocol (TCP)**, 50
- transparent bridging**, 163
- transport encryption**, 372-373
- Transport Layer Security (TLS)**, 179, 372
- trapdoors**, 313
- trends**
 - analysis, 46, 346-347
 - reports, 132
 - vulnerability, 148
- Trojan horses**, 311
- Trusted Foundry program**, 104
- trusted party communication**, 218
- trusted third-party model (federations)**, 327
- TSIG (Transaction Signature)**, 322
- TTL (Time to Live)**, 322
- type accreditation**, 292
- types**
 - access
 - countermeasures*, 84-86, 282-284
 - decisions*, 87
 - analysis, 45-47
 - cryptography, 364-368
 - data, 194
 - corporate confidential*, 199-201
 - intellectual property*, 197-199
 - payment card information*, 195-197
 - PHI*, 195
 - PII*, 194
 - DNS records, 8
 - firewalls, 27-29, 408
 - IDS, 25
 - malware, 311
 - Nmap scans, 17-18
 - passwords, 268-269
 - regression testing, 394
 - virtualization attacks, 13
 - WPA/WPA2, 12

U

- UEBA (user entity behavior analytics), 47
 - unauthorized changes, 229
 - unauthorized privileges, 229
 - unauthorized software, 228
 - unclassified data, 120, 277
 - unencrypted traffic, identifying, 24
 - Unified Security Management (USM), 422
 - unified threat management (UTM), 359
 - unit regression testing, 390, 394
 - United States Federal Sentencing Guidelines of 1991, 256
 - Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act), 255-257
 - Unix
 - Bro, 407
 - dd command, 447
 - ifconfig command, 434
 - tcpdump, 429
 - unknown threats, 190
 - unsecured VM migration attacks, 13
 - Untidy fuzzer, 442
 - unused ports/services, blocking, 86
 - updates
 - incident response plans, 245
 - practice tests, 456
 - vulnerability scanning tools, 128-130
 - urgent resources, 192
 - USA PATRIOT (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism) Act, 255-257
 - user entity behavior analytics (UEBA), 47
 - usermode debugger, 241
 - users
 - acceptance testing, 393
 - access, viewing, 436
 - logged on, viewing, 436
 - USM (Unified Security Management), 422
 - utilities. *See* tools
 - UTM (unified threat management), 359
- ## V
-
- v argument (netstat command), 22
 - validating
 - input, 154
 - software, 389
 - software input, 394-395
 - techniques, 243-244
 - testing, 389
 - vulnerability scan results, 147-148
 - Vega, 440
 - verification
 - assessments, 290
 - audits, 288-289
 - certification, 291
 - ISO/IEC 27001, 292-293
 - ISO/IEC 27002, 294
 - NIACAP, 292
 - evaluations, 290
 - maturity model, 291
 - testing, 389
 - vertical privilege escalation, 335
 - virtual private networks. *See* VPNs
 - virtualization
 - attacks, 13
 - environmental reconnaissance, 13-14
 - hosts, 169-170
 - private networks. *See* VPNs
 - vulnerabilities, 169
 - hosts, 169-170
 - management interfaces, 171-173
 - networks, 170
 - viruses, 311
 - VLANs (virtual local area networks), 73-74, 165
 - advantages/disadvantages, 166
 - hopping, 166
 - vulnerabilities, 165-168
 - VM escape attacks, 13, 169
 - VM sprawl attacks, 13
 - VPNs (virtual private networks), 175
 - connection protocols, 176
 - man-in-the-middle attacks, 178
 - vulnerabilities, 175-179
 - vulnerabilities
 - APTs, 191
 - countermeasures. *See* countermeasures
 - database servers, 160-161
 - endpoints, 161-162
 - exploit tools, 440-442
 - feeds, 123
 - ICS, 179-180
 - interconnected networks, 174-175
 - mobile devices, 173-174
 - network devices, 169

network infrastructure, 162
ARP poisoning, 164-165
MAC overflow, 164
routers, 168
switches, 163
VLANs, 165-168

network tests (NVT), 426

organizational requirements, 117

SCADA, 179-180

scanning, 30-31
Access Complexity, 129
Access Vector, 129
authentication, 129
availability, 130
benefits, 135
confidentiality, 130
executing, 131
frequency, 121
integrity, 130
organizational requirements, 117-120
output, analyzing, 143-148
remediation, 133-135
reports, 132
tools, 122-128

trends, 148

virtualization, 169
hosts, 169-170
management interfaces, 171-173
networks, 170

VPNs, 175-179

web applications, 391

web servers, 149
buffer overflows, 157-159
click-jacking, 152-153
CSRFs, 151-152
errors/exceptions, handling, 156
input validation, 154

insecure direct object references, 150
integer overflows, 159
maintenance books, 149
race conditions, 160
sensitive data storage, 156
session hijacking, 153
SQL injections, 155
time-of-check, 150
time-of-use, 150
XSS, 150-151

zero day, 190

Vulnerabilities by Host report, 144

Vulnerabilities by Plug-in report, 145

W

-W argument (netstat command), 22

WAF (web application firewall), 418-419

WAN (wide area network), 72

warchalking, 44

wardriving, 44

web application firewall (WAF), 418-419

web application vulnerability scanning, 391

web proxy servers, 418-421

Imperva, 421

ModSecurity, 420

NAXSI, 420

WAF, 418-419

web server vulnerabilities, 149

buffer overflows, 157-159

click-jacking, 152-153

CSRFs, 151-152

errors/exceptions, handling, 156

input validation, 154

insecure direct object references, 150

integer overflows, 159

maintenance hooks, 149

race conditions, 160

sensitive data storage, 156

session hijacking, 153

SQL injections, 155

time-of-check, 150

time-of-use, 150

XSS, 150-151

websites

ArcSight, 421

Cacti, 439

Cellebrite, 445

CIS Benchmarks, 398

CIS Controls, 398

EnCase Forensic, 444

FTK, 444

Helix, 444

Imperva, 421

ISO standards, 263

ISO/IEC 27001 certification, 293

MRTG, 437

NAXSI, 421

Pearson Test Prep download link, 454

Pearson Test Prep software, 454

Premium Edition, 457

QRadar, 422

SANS, 397

Sourcefire, 405

Sysinternals, 444

tcpdump command, 429

White team (training), 106

Whois tool, 9

wide area connections (WANs), 72

Wi-Fi hacking gear, 224

Windows

firewall log, 48

MBSA, 427

passwords, 271

Snort, 406

windump, 429

windump command, 429

**wiped removable media,
204**

**WIPO (World Intellectual
Property Organization),
199**

**WIPS (wireless intrusion
prevention system), 224**

wired networks, 12

wireless intrusion pre-
vention system (WIPS),
224

wireless key loggers, 224

Wireshark, 23-24, 428-429

**WLANs (wireless LANs),
12**

analysis, 43-45

environmental recon-
naissance, 12

Infrastructure Mode

wireless networks, 43

rogue APs, 12

sniffing, 45

WPA/WPA2, 12

**work history verification,
307**

**work recovery time (WRT),
192**

workflow, 121

workstations, 202-203

**World Intellectual Property
Organization (WIPO),
199**

worms, 311

WPA, 12

WPA2, 12

write blockers, 203

**WRT (work recovery time),
192**

X

**XACML (Extensible
Access Control Markup
Language), 327-329**

XMAS scans, 18

**XSS (cross-site scripting),
150-151, 335**

Z

Zap, 440

**ZAP (Zed Attack Proxy),
392**

zero day attacks, 46, 190

zero-knowledge pen-
etration tests, 99

zone transfers, 10