

# CompTIA Security+

Exam SY0-301

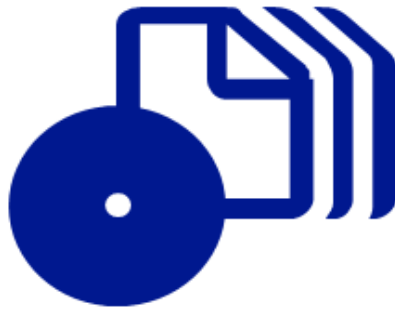


David Seidl  
Mike Chapple  
James Michael Stewart

# Training Kit



# How to access your CD files



The print edition of this book includes a CD. To access the CD files, go to <http://aka.ms/664265/files>, and look for the Downloads tab.

Note: Use a desktop web browser, as files may not be accessible from all ereader devices.

Questions? Please contact: [mspinput@microsoft.com](mailto:mspinput@microsoft.com)

Microsoft Press





# CompTIA Security+ (Exam SY0-301)

## Objective lesson map

	OBJECTIVE	CHAPTER
<b>1.0</b>	<b>NETWORK SECURITY (21 PERCENT)</b>	
1.1	Explain the security function and purpose of network devices and technologies: Firewalls; Routers; Switches; Load Balancers; Proxies; Web security gateways; VPN concentrators; NIDS and NIPS (Behavior based, signature based, anomaly based, heuristic); Protocol analyzers; Sniffers; Spam filter, all-in-one security appliances; Web application firewall vs. network firewall; URL filtering, content inspection, malware inspection	2
1.2	Apply and implement secure network administration principles: Rule-based management, Firewall rules, VLAN management, Secure router configuration, Access control lists, Port Security, 802.1x, Flood guards, Loop protection, Implicit deny, Prevent network bridging by network separation, Log analysis	2, 3
1.3	Distinguish and differentiate network design elements and compounds: DMZ, Subnetting, VLAN, NAT, Remote Access, Telephony, NAC, Virtualization, Cloud Computing (Platform as a Service, Software as a Service, Infrastructure as a Service)	3
1.4	Implement and use common protocols: IPSec, SNMP, SSH, DNS, TLS, SSL, TCP/IP, FTPS, HTTPS, SFTP, SCP, ICMP, IPv4 vs. IPv6	3
1.5	Identify commonly used default network ports: FTP, SFTP, FTPS, TFTP, TELNET, HTTP, HTTPS, SCP, SSH, NetBIOS	3
1.6	Implement wireless network in a secure manner: WPA, WPA2, WEP, EAP, PEAP, LEAP, MAC filter, SSID broadcast, TKIP, CCMP, Antenna Placement, Power level controls	3
<b>2.0</b>	<b>COMPLIANCE AND OPERATIONAL SECURITY (18 PERCENT)</b>	
2.1	Explain risk related concepts: Control types (Technical, Management, Operational); False positives; Importance of policies in reducing risk (Privacy policy, Acceptable use, Security policy, Mandatory vacations, Job rotation, Separation of duties, Least privilege); Risk calculation (Likelihood, ALE, Impact); Quantitative vs. qualitative; Risk-avoidance, transference, acceptance, mitigation, deterrence; Risks associated to Cloud Computing and Virtualization	1, 4
2.2	Carry out appropriate risk mitigation strategies: Implement security controls based on risk, Change management, Incident management, User rights and permissions reviews, Perform routine audits, Implement policies and procedures to prevent data loss or theft	1, 4
2.3	Execute appropriate incident response procedures: Basic forensic procedures (Order of volatility, Capture system image, Network traffic and logs, Capture video, Record time offset, Take hashes, Screenshots, Witnesses, Track man hours and expense), Damage and loss control, Chain of custody, Incident response: (first responder)	1
2.4	Explain the importance of security related awareness and training: Security policy training and procedures; Personally identifiable information; Information classification: Sensitivity of data (hard or soft); Data labeling, handling and disposal; Compliance with laws, best practices and standards; User habits (Password behaviors, Data handling, Clean desk policies, Prevent tailgating, Personally owned devices); Threat awareness, (New viruses, Phishing attacks, Zero-day exploits); Use of social networking and P2P	4
2.5	Compare and contrast aspects of business continuity: Business impact analysis, Removing single points of failure, Business continuity planning and testing, Continuity of operations, Disaster recovery, IT contingency planning, Succession planning	4

**Exam Objectives** The exam objectives listed here are current as of this book's publication date. Exam objectives are subject to change at any time without prior notice and at CompTIA's sole discretion. Please visit the CompTIA Certifications webpage for the most current listing of exam objectives: <http://certification.comptia.org/getCertified/certifications.aspx>.

<b>2.0</b>	<b>COMPLIANCE AND OPERATIONAL SECURITY (18 PERCENT)</b>	
2.6	Explain the impact and proper use of environmental controls: HVAC, Fire suppression, EMI shielding, Hot and cold aisles, Environmental monitoring, Temperature and humidity controls, Video monitoring	4
2.7	Execute disaster recovery plans and procedures: Backup / backout contingency plans or policies; Backups, execution and Frequency; Redundancy and fault tolerance (Hardware, RAID, Clustering, Load balancing, Servers); High availability; Cold site, hot site, warm site; Mean time to restore, mean time between failures, recovery time objectives and recovery point objectives	4
2.8	Exemplify the concepts of confidentiality, integrity and availability (CIA)	1
<b>3.0</b>	<b>THREATS AND VULNERABILITIES (21 PERCENT)</b>	
3.1	Analyze and differentiate among types of malware: Adware, Virus, Worms, Spyware, Trojan, Rootkits, Backdoors, Logic bomb, Botnets	5
3.2	Analyze and differentiate among types of attacks: Man-in-the-middle, DDoS, DoS, Replay, Smurf attack, Spoofing, Spam, Phishing, Spim, Vishing, Spear phishing, Xmas attack, Pharming, Privilege escalation, Malicious insider threat, DNS poisoning and ARP poisoning, Transitive access, Client-side attacks	5
3.3	Analyze and differentiate among types of social engineering attacks: Shoulder surfing, Dumpster diving, Tailgating, Impersonation, Hoaxes, Whaling, Vishing	5
3.4	Analyze and differentiate among types of wireless attacks: Rogue access points, Interference, Evil twin, War driving, Bluejacking, Bluesnarfing, War chalking, IV attack, Packet sniffing	5
3.5	Analyze and differentiate among types of application attacks: Cross-site scripting, SQL injection, LDAP injection, XML injection, Directory traversal/command injection, Buffer overflow, Zero day, Cookies and attachments, Malicious add-ons, Session hijacking, Header manipulation	5
3.6	Analyze and differentiate among types of mitigation and deterrent techniques: Manual bypassing of electronic controls (Failsafe/secure versus failopen), Monitoring system logs (Event logs, Audit logs, Security logs, Access logs), Physical security (Hardware locks, Mantraps, Video surveillance, Fencing, Proximity readers, Access list), Hardening (Disabling unnecessary services, Protecting management interfaces and applications, Password protection, Disabling unnecessary accounts), Port security (MAC limiting and filtering, 802.1x, Disabling unused ports), Security posture (Initial baseline configuration, Continuous security monitoring, remediation), Reporting (Alarms, Alerts, Trends), Detection Controls vs. prevention controls (IDS vs. IPS, Camera vs. guard)	6
3.7	Implement assessment tools and techniques to discover security threats and vulnerabilities: Vulnerability scanning and interpret results, Tools (Protocol analyzer, Sniffer, Vulnerability scanner, Honeypots, Honeynets, Port scanner), Risk calculations (Threat vs. likelihood), Assessment types (Risk, Threat, Vulnerability), Assessment technique (Baseline reporting, Code review, Determine attack surface, Architecture, Design reviews)	7
3.8	Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning: Penetration testing (Verify a threat exists, Bypass security controls, Actively test security controls, Exploiting vulnerabilities), Vulnerability scanning (Passively testing security controls, Identify vulnerability, Identify lack of security controls, Identify common misconfiguration), Black box, White box, Gray box	7
<b>4.0</b>	<b>APPLICATION, DATA AND HOST SECURITY (16 PERCENT)</b>	
4.1	Explain the importance of application security: Fuzzing, Secure coding Concepts (Error and exception handling, Input validation), Cross-site scripting prevention, Cross-site Request Forgery (XSRF) prevention, Application configuration baseline (proper settings), Application hardening, Application patch management	8
4.2	Carry out appropriate procedures to establish host security: Operating system security and settings, Anti-malware (Anti-virus, Anti-spam, Anti-spyware, Pop-up blockers, Host-based firewalls), Patch management, Hardware security (Cable locks, Safe, Locking cabinets), Host software baselining, Mobile devices (Screen lock, Strong password, Device encryption, Remote wipe/sanitization, Voice encryption, GPS tracking), Virtualization	9
4.3	Explain the importance of data security: Data Loss Prevention (DLP), Data encryption (Full disk, Database, Individual files, Removable media, Mobile devices), Hardware based encryption devices (TPM, HSM, USB encryption, Hard drive), Cloud Computing	10



<b>5.0</b>	<b>ACCESS CONTROL AND IDENTITY MANAGEMENT (13 PERCENT)</b>	
5.1	Explain the function and purpose of authentication services: RADIUS, TACACS, TACACS+, Kerberos, LDAP, XTACACS	11
5.2	Explain the fundamental concepts and best practices related to authentication, authorization and access control: Identification vs. authentication, Authentication (single factor) and authorization, Multifactor authentication, Biometrics, Tokens, Common access card, Personal identification verification card, Smart card, Least privilege, Separation of duties, Single sign on, ACLs, Access control, Mandatory access control, Discretionary access control, Role/rule-based access control, Implicit deny, Time of day restrictions, Trusted OS, Mandatory vacations, Job rotation	
5.3	Implement appropriate security controls when performing account management: Mitigates issues associated with users with multiple account/roles, Account policy enforcement (Password complexity, Expiration, Recovery, Length, Disablement, Lockout), Group based privileges, User assigned privileges	11
<b>6.0</b>	<b>CRYPTOGRAPHY (11 PERCENT)</b>	
6.1	Summarize general cryptography concepts: Symmetric vs. asymmetric, Fundamental differences and encryption methods (Block vs. stream), Transport encryption, Non-repudiation, Hashing, Key escrow, Steganography, Digital signatures, Use of proven technologies, Elliptic curve and quantum cryptography	12
6.2	Use and apply appropriate cryptographic tools and products: WEP vs. WPA/WPA2 and pre-shared key, MD5, SHA, RIPEMD, AES, DES, 3DES, HMAC, RSA, RC4, One-time-pads, CHAP, PAP, NTLM, NTLMv2, Blowfish, PGP/GPG, Whole disk encryption, TwoFish, Comparative strengths of algorithms, Use of algorithms with transport encryption (SSL, TLS, IPsec, SSH, HTTPS)	12
6.3	Explain the core concepts of public key infrastructure: Certificate authorities and digital certificates (CA, CRLs), PKI, Recovery agent, Public key, Private key, Registration, Key escrow, Trust models	12
6.4	Implement PKI, certificate management and associated components: Certificate authorities and digital certificates (CA, CRLs), PKI, Recovery agent, Public key, Private keys, Registration, Key escrow, Trust models	12



# CompTIA Security+ (Exam SYO-301)

Training Kit

David Seidl  
Mike Chapple  
James Michael Stewart



Copyright © 2013 by David Seidl, Mike Chapple, James Michael Stewart

All rights reserved. No part of the contents of this book may be reproduced or transmitted in any form or by any means without the written permission of the publisher.

ISBN: 978-0-7356-6426-5

1 2 3 4 5 6 7 8 9 QG 8 7 6 5 4 3

Printed and bound in the United States of America.

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at [mspinput@microsoft.com](mailto:mspinput@microsoft.com). Please tell us what you think of this book at <http://www.microsoft.com/learning/booksurvey>.

Microsoft and the trademarks listed at <http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx> are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation, nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

**Acquisitions and Developmental Editor:** Kenyon Brown

**Production Editor:** Melanie Yarbrough

**Editorial Production:** Online Training Solutions, Inc. (OTSI)

**Technical Reviewer:** Addam Schroll

**Copyeditor:** Online Training Solutions, Inc. (OTSI)

**Indexer:** BIM Publishing Services

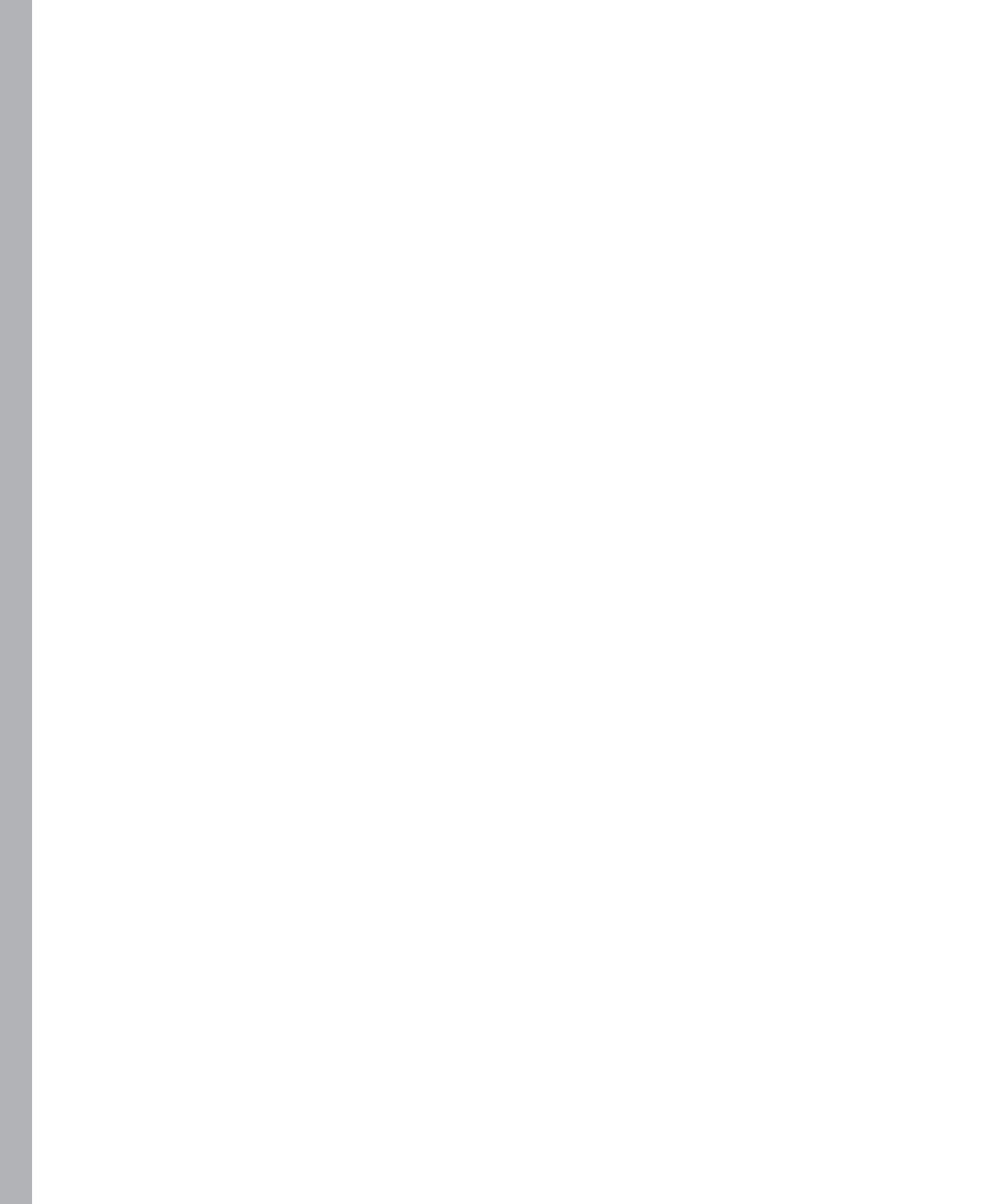
**Cover Design:** Twist Creative • Seattle

**Cover Composition:** Ellie Volkhausen

**Illustrator:** Online Training Solutions, Inc. (OTSI)

# Contents at a glance

	<i>Introduction</i>	<i>xix</i>
CHAPTER 1	Risk management and incident response	1
CHAPTER 2	Network security technologies	39
CHAPTER 3	Secure network design and management	67
CHAPTER 4	Operational and environmental security	109
CHAPTER 5	Threats and attacks	149
CHAPTER 6	Monitoring, detection, and defense	201
CHAPTER 7	Vulnerability assessment and management	253
CHAPTER 8	The importance of application security	287
CHAPTER 9	Establishing host security	317
CHAPTER 10	Understanding data security	371
CHAPTER 11	Identity and access control	411
CHAPTER 12	Cryptography	449
	<i>Glossary</i>	<i>489</i>
	<i>Index</i>	<i>503</i>





# Contents

<b>Introduction</b>	<b>xix</b>
<i>System requirements</i>	<i>xxii</i>
<i>Using the companion CD</i>	<i>xxiv</i>
<i>CompTIA professional certification program</i>	<i>xxvi</i>
<i>How certification helps your career</i>	<i>xxvi</i>
<i>It pays to get certified</i>	<i>xxvii</i>
<i>Four steps to getting certified and staying certified</i>	<i>xxvii</i>
<i>How to obtain more information</i>	<i>xxviii</i>
<i>Acknowledgments</i>	<i>xxviii</i>
<i>Support &amp; feedback</i>	<i>xxx</i>
<i>Preparing for the exam</i>	<i>xxxi</i>
<b>Chapter 1 Risk management and incident response</b>	<b>1</b>
CIA and DAD triads . . . . .	2
Confidentiality and disclosure	3
Integrity and alteration	3
Availability and denial	3
Risk assessment and mitigation . . . . .	4
Likelihood and impact	5
Managing risk	9
Security controls . . . . .	12
Technical controls	12
Operational controls	12
Management controls	13

---

**What do you think of this book? We want to hear from you!**

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

[www.microsoft.com/learning/booksurvey/](http://www.microsoft.com/learning/booksurvey/)

Incident response .....	14
Incident response team .....	14
Incident response life cycle .....	19
Incident communications .....	25
Collecting evidence .....	26
Computer forensics .....	28
Chapter summary .....	34
Chapter review .....	35
Answers .....	37
<b>Chapter 2 Network security technologies</b> .....	<b>39</b>
Network security .....	40
Humongous Insurance: a modern secure network .....	41
Firewalls .....	41
Routers .....	46
Switches .....	47
Load balancers .....	49
Proxies .....	51
VPN concentrators .....	52
Network intrusion detection systems (NIDS) and network intrusion prevention systems (NIPS) .....	54
Protocol analyzers .....	57
Inspection .....	58
All-in-one security appliances .....	62
Chapter summary .....	62
Chapter review .....	63
Answers .....	65
<b>Chapter 3 Secure network design and management</b> .....	<b>67</b>
Network design and implementation .....	69
IP: the Internet Protocol .....	69
Network and application protocols .....	77
Ports and protocols .....	83

Network design and segmentation . . . . .	84
Remote access	87
Telephony and VoIP	89
Virtualization	90
Network administration and management . . . . .	95
Access control lists (ACLs)	95
Firewall rules	96
Logging	96
Secure switch and router configuration . . . . .	98
VLAN management	98
Port security	98
802.1x authentication	99
Flood guards	99
Loop protection	100
Preventing network bridging	100
Wireless protocols: encryption and authentication . . . . .	101
Designing and implementing secure wireless networks	103
Chapter summary . . . . .	104
Chapter review. . . . .	105
Answers. . . . .	107

**Chapter 4 Operational and environmental security 109**

Security policies. . . . .	111
Security policy	113
Privacy policy	113
Acceptable use policy	115
Personnel security best practices	115
Security awareness and training. . . . .	118
Security policy training	118
Compliance training	119
User habits	119
Threat awareness	123

Information classification and labeling . . . . .	124
Personally identifying information (PII)	126
Environmental controls . . . . .	128
Heating, ventilation, and air conditioning (HVAC)	128
Fire suppression	129
EMI shielding	130
Environmental and video monitoring	130
Business continuity planning . . . . .	132
Business impact assessment (BIA)	132
Removing single points of failure	133
Designing and testing the business continuity plan	135
Succession planning	137
Disaster recovery planning . . . . .	138
Disaster recovery metrics	138
Backups	140
Building fault-tolerant environments	141
Disaster recovery sites	143
Chapter summary . . . . .	144
Chapter review . . . . .	145
Answers . . . . .	147

**Chapter 5 Threats and attacks 149**

Client-side attacks . . . . .	151
Malware	151
Application attacks	161
Application vulnerabilities	164
Web attacks . . . . .	166
Cookies	166
Header manipulation	168
Directory traversal	169
Cross-site scripting	170
Preventing XSS	171

Injection and modification attacks .....	171
SQL injection	172
LDAP and XML injection	173
Command injection	174
Network attacks .....	175
Spoofing	175
Packet sniffing	176
Man-in-the-middle	176
Replay attacks	177
DNS and ARP poisoning	178
Denial of service and distributed denial of service attacks	179
Smurf attacks	180
Xmas attacks	181
Wireless attacks.....	182
Rogue access points	183
Bluetooth attacks	185
War driving	185
Packet sniffing and wireless networks	186
Social engineering and phishing .....	188
Hoaxes	190
Phishing	190
Email attacks	193
Chapter summary .....	195
Chapter review.....	196
Answers.....	198

## **Chapter 6 Monitoring, detection, and defense 201**

Securing and defending systems.....	202
Hardening	203
Secure system configuration and management	209
Network device hardening	221

Monitoring and reporting . . . . .	223
Continuous security monitoring	223
System log monitoring	223
Reporting and monitoring	236
Physical security design and concepts . . . . .	241
Chapter summary . . . . .	248
Chapter review . . . . .	249
Answers . . . . .	251
<b>Chapter 7 Vulnerability assessment and management</b>	<b>253</b>
Vulnerabilities and vulnerability assessment . . . . .	255
Risk-based vulnerability assessments	256
Assessment techniques	258
Vulnerability scanning . . . . .	261
Vulnerability scanning tools	261
Port scanners	263
Vulnerability scanners	265
Honeypots and honeynets	269
Penetration testing . . . . .	272
Types of penetration tests	274
Conducting a penetration test	275
Chapter summary . . . . .	281
Chapter review . . . . .	282
Answers . . . . .	284
<b>Chapter 8 The importance of application security</b>	<b>287</b>
Fuzzing . . . . .	287
Secure coding concepts . . . . .	290
Error handling and exception handling	292
Input validation	293
Cross-site scripting prevention . . . . .	296
Cross-site request forgery (XSRF) prevention . . . . .	297
Application configuration baseline (proper settings) . . . . .	301

Application hardening . . . . .	303
Application patch management . . . . .	306
Chapter summary . . . . .	309
Chapter review . . . . .	311
Answers . . . . .	313

**Chapter 9 Establishing host security 317**

Operating system security and settings . . . . .	318
Anti-malware . . . . .	321
Anti-virus . . . . .	324
Anti-spam . . . . .	331
Anti-spyware . . . . .	333
Pop-up blockers . . . . .	336
Host-based firewalls . . . . .	337
Patch management . . . . .	339
Hardware security . . . . .	341
Cable locks . . . . .	343
Safe . . . . .	345
Locking cabinets . . . . .	347
Host software baselining . . . . .	349
Mobile devices . . . . .	351
Screen lock . . . . .	354
Strong password . . . . .	355
Device encryption . . . . .	356
Remote wipe/sanitization . . . . .	358
Voice encryption . . . . .	359
GPS tracking . . . . .	359
Chapter summary . . . . .	362
Chapter review . . . . .	364
Answers . . . . .	367

<b>Chapter 10 Understanding data security</b>	<b>371</b>
Data loss prevention (DLP) .....	371
Data encryption .....	373
Full-disk encryption	377
Database encryption	384
Individual file encryption	385
Removable media	388
Mobile devices	391
Hardware-based encryption devices .....	393
Trusted Platform Module	395
Hardware security module	396
USB encryption	398
Hard drive encryption	399
Cloud computing .....	401
Chapter summary .....	401
Chapter review .....	404
Answers .....	407
<b>Chapter 11 Identity and access control</b>	<b>411</b>
Identification and authentication .....	412
Authentication	413
Authentication and authorization .....	414
User accounts	414
Single-factor vs. multifactor authentication	414
Biometrics	416
Tokens	420
Authentication services .....	423
RADIUS	423
TACACS and TACACS+	424
The Kerberos protocol	425
LDAP	426
Active Directory Domain Services	428
Single sign-on	429



Access control concepts and models. . . . .	431
Trusted operating systems	432
Least privilege	432
Separation of duties	433
Job rotation	434
Time-of-day restrictions	434
Mandatory vacation	434
Access control models	435
Account management . . . . .	439
Passwords	439
Privileges	442
Centralized and decentralized privilege management	443
Chapter summary . . . . .	444
Chapter review. . . . .	445
Answers. . . . .	447

## **Chapter 12 Cryptography 449**

Goals of cryptography . . . . .	451
Cryptographic concepts. . . . .	452
Symmetric vs. asymmetric cryptography	454
One-time pads	459
Symmetric encryption algorithms . . . . .	460
Data Encryption Standard	460
Advanced Encryption Standard	465
Blowfish	465
Twofish	466
RC4	467
Asymmetric encryption algorithms . . . . .	467
Rivest, Shamir, and Adelman (RSA)	468
Pretty Good Privacy (PGP)	468
Elliptic curve cryptography (ECC)	470

Digital signatures . . . . .	471
Cryptographic hashes	471
Creating digital signatures	473
Public-key infrastructure . . . . .	476
Digital certificates	476
Key recovery and key escrow	478
Protecting data with encryption . . . . .	478
Encrypting data at rest	479
Encrypting data in motion	481
Authentication . . . . .	483
Chapter summary . . . . .	484
Chapter review . . . . .	485
Answers . . . . .	487
<i>Glossary</i>	489
<i>Index</i>	503

---

**What do you think of this book? We want to hear from you!**

Microsoft is interested in hearing your feedback so we can continually improve our books and learning resources for you. To participate in a brief online survey, please visit:

[www.microsoft.com/learning/booksurvey/](http://www.microsoft.com/learning/booksurvey/)

# Introduction

---

This training kit is designed for information technology (IT) professionals who want to earn the CompTIA Security+ certification. It is assumed that you have a basic understanding of computers and operating systems. However, the CompTIA Security+ certification is an entry-level certification, so you are not expected to have any in-depth knowledge to use this training kit.

To become a CompTIA Security+ certified technician, you must take and pass the SY0-301 exam. The primary goal of this training kit is to help you build a solid foundation of IT knowledge so that you can successfully pass the exam the first time you take it.

The materials covered in this training kit and on exam SY0-301 relate to the technologies a successful security professional is expected to understand. These include risk management, infrastructure security, application security, policy, and confidentiality/integrity/availability controls. You can download the objectives for the SY0-301 exam from the CompTIA website here:

*<http://certification.comptia.org/Training/testingcenters/examobjectives.aspx>*

By using this training kit, you will learn how to do the following:

- Conduct risk assessment and risk management activities.
- Respond to a security incident.
- Understand the risks associated with cloud computing and virtualization.
- Explain the various types of network security devices and technologies.
- Design a network with adequate security controls.
- Administer network security controls on an ongoing basis.
- Secure wireless networks with acceptable encryption.
- Provide adequate environmental and operational security controls.
- Understand the threats on the security landscape.
- Deploy defenses to prevent and mitigate attacks.
- Conduct vulnerability assessments and manage vulnerabilities.
- Secure applications against attack.
- Secure operating systems against common threats.
- Use encryption to protect information at rest and in motion.
- Deploy access controls to implement identification, authentication, and authorization.

Refer to the objective mapping page in the front of this book to see where in the book each exam objective is covered.

## About the exam

The SY0-301 exam is focused on skills required to secure systems, applications, and networks. It includes objectives in the following six areas:

- Network security (21 percent of exam)
- Compliance and operational security (18 percent of exam)
- Threats and vulnerabilities (21 percent of exam)
- Application, data, and host security (16 percent of exam)
- Access control and identity management (13 percent of exam)
- Cryptography (11 percent of exam)

The current version of the exam became available in 2011. Over the years, more than 45,000 people around the world have earned the CompTIA Security+ certification. Information security professionals often start with the CompTIA Security+ certification to lay a solid foundation of information security knowledge and later move on to higher-level certifications and better-paying jobs. Among those test takers are those who are working to meet the US Department of Defense's Directive 8570.01-M, which lists the CompTIA Security+ exam as one of the required certifications for employees and contractors who perform information security work.

The CompTIA Security+ exam has a maximum of 100 questions, including both multiple-choice and performance-based questions. You will have 90 minutes in which to take the test, and a score of 750 on a scale of 100-900 is considered a passing score. You can find more information about the exam at:

*<http://certification.comptia.org/getCertified/certifications/security.aspx>*

## Prerequisites

CompTIA recommends that test takers have the CompTIA Network+ certification as well as two years of technical networking experience with an emphasis on information security work.

Note that this is not a requirement to take the exams. Anyone can take the exams after paying for them, and if they pass, they earn the certification. However, you'll have the best chance of success if you have been studying and working with networks and information security professionally and are familiar with the material in the CompTIA Network+ exam.

## Performance-based testing

A significant difference in the SY0-301 exam over previous versions is the introduction of performance-based testing. Instead of just using multiple-choice questions, CompTIA is introducing questions that will require you to perform a task. You should expect to see somewhere around three of these questions on the exam, so don't stress over them.

Imagine that you wanted to know if a person could ride a bike. You could ask some multiple-choice questions but you'll find that these questions aren't always reliable. A person might answer questions correctly but not be able to actually ride the bike. Put the person in front of a bike, ask them to ride it, and you'll quickly know whether they can or not. Performance-based testing uses this philosophy to see if the candidate has a skill.

Consider this multiple-choice question:

1. What TCP port is used for SMTP traffic by default?
  - A. 21
  - B. 23
  - C. 25
  - D. 80

The correct answer is port 25.

In a performance-based question, you might instead be asked to complete a set of firewall rules by filling in the missing information. This might include selecting the ports corresponding to several services and specifying which rules should be set to allow or deny traffic.

When it's a multiple-choice question, you have a 25-percent chance of getting it correct. In a performance-based question, there are an infinite number of possibilities, and the test designers are able to test you on multiple concepts or facts simultaneously.

Throughout the book, we've included steps and instructions on how to do many tasks with performance-based testing in mind. If you do these tasks as you work through the book, you'll be better prepared to answer these performance-based tests.

## Study tips

There's no single study method that works for everyone, but there are some common techniques that many people use to successfully pass these exams. These include:

- **Setting a goal** Pick a date when you expect to take the exam, and set your goal to take it then. The date is dependent on how long it will take you to read the chapters and your current knowledge level. You might set a date two months from now, four months from now, or something else. However, pick a date and set a goal.

- **Taking notes** If concepts aren't familiar to you, take the time to write them down. The process of transferring the words from the book, through your head, and down to your hand really helps to burn the knowledge into your brain.
- **Reading your notes** Go back over your notes periodically to see what has stuck, and what you need to review more. You can't bring notes with you into the testing area, but you can use them to review key material before the exam.
- **Using flash cards** Some people get a lot out of flash cards that provide a quick test of knowledge. These help you realize what you don't know and what you need to brush up on. Many practice test programs include flash cards, so you don't necessarily have to create them yourself.
- **Reviewing the objectives** This is what CompTIA says they'll test you on. Sometimes just understanding the objective will help you predict a test question and answer it correctly.
- **Recording your notes** Many people record their notes in an MP3 player and play them back regularly. You can listen while driving, while exercising, or just about any time. Some people have a partner read the notes, which can give an interesting twist to studying.
- **Taking the practice test questions on the CD** The practice test questions on the CD are designed to test the objectives for the exam but at a deeper level than you'll have on the live exam. Each question includes detailed explanations on why the correct answer is correct, and why the incorrect answers are incorrect. Ideally, you should be able to look at the answers to any question and not just know the correct answer, but also why the incorrect answers are incorrect.

## System requirements

---

The actual system requirements to use this book are minimal. The only requirement is a computer you can use to install the practice tests on the companion CD.

Many of the examples in the book use Windows 7 and Linux or Mac OS X. In most organizations, security staff work with a variety of operating systems, and we have attempted to reflect that in this book. You will find that most Windows commands remain the same whether you are using Windows XP, Windows Vista, Windows 7, or Windows 8, with most differences appearing in the menus used to get to settings. Thus, if you only have a Windows XP-based system to practice Windows commands with, you can still expect to successfully learn the critical practical techniques covered in the book.

Instead of having two or three separate computers to allow you to run Windows and Linux, you can use a single PC with virtualization software hosting these operating systems, or a Linux Live-CD or USB flash drive bootable system to work with. The next section provides suggested hardware requirements for running a virtualized workstation for practice. Booting into a LiveCD or portable Linux distribution can also be done on similar hardware.

## Hardware requirements for virtualization

If you plan to use virtualization, your computer should have the following:

- A processor that includes hardware-assisted virtualization (AMD-V or Intel VT) that is enabled in the BIOS. (Note that you can run Windows Virtual PC without Intel-VT or AMD-V.) Ideally, the processor will be a 64-bit processor so that you can have more RAM.
- At least 2.0 GB of RAM, but more is strongly recommended, and 4 GB is often a more practical minimum.
- 20 GB of available hard disk space for a single VM, and at least 80 GB of total hard disk space for a system running virtual machines.
- Internet connectivity.

## Software requirements

Most of the examples in this book use Windows 7, Linux, or Mac OS X. Virtualization allows you to use all three simultaneously, which can ease your learning experience. Fortunately, there are several free virtualization software packages available, including Windows Virtual PC, VirtualBox, and VMWare Player.

Oracle provides VirtualBox as a free download from <https://www.virtualbox.org/wiki/Downloads>, and you can download a free version of VMWare Player from <http://www.vmware.com/products/player/overview.html>. Both VirtualBox and VMWare Player support 64-bit host machines, but you can only run 32-bit hosts within Windows Virtual PC.

Linux virtual machines are commonly available, including BackTrack Linux, a security-focused distribution that combines an excellent collection of security tools into a downloadable virtual machine. You can download BackTrack Linux at <http://www.backtrack-linux.org/downloads/>. For the purposes of the examples in this book, most common Linux security distributions are also valid options.

## Using the companion CD

---

A companion CD is included with this training kit. The companion CD contains the following:

- **Practice tests** You can reinforce your understanding of the topics covered in this training kit by using electronic practice tests that you customize to meet your needs. You can practice for the SY0-301 certification exam by using tests created from a pool of 200 realistic exam questions, which give you many practice exams to ensure that you are prepared.
- **An ebook download** Instructions to download the electronic version (eBook) of this book is included for when you do not want to carry the printed book with you.

### **NOTE COMPANION CONTENT FOR DIGITAL BOOK READERS**

If you bought a digital-only edition of this book, you can enjoy select content from the print edition's companion CD. Visit <http://aka.ms/CompTIASecurityTK/files> to get your downloadable content.

## How to install the practice tests

To install the practice test software from the companion CD to your hard disk, perform the following steps:

1. Insert the companion CD into your CD drive and accept the license agreement. A CD menu appears.

### **NOTE IF THE CD MENU DOES NOT APPEAR**

If the CD menu or the license agreement does not appear, AutoRun might be disabled on your computer. Refer to the Readme.txt file on the CD for alternate installation instructions.

2. Click *Practice Tests* and follow the instructions on the screen.



## How to use the practice tests

To start the practice test software, follow these steps:

1. Click Start, All Programs, and then select Microsoft Press Training Kit Exam Prep.  
A window appears that shows all the Microsoft Press training kit exam prep suites installed on your computer.
2. Double-click the practice test you want to use.

When you start a practice test, you choose whether to take the test in Certification Mode, Study Mode, or Custom Mode:

- **Certification Mode** Closely resembles the experience of taking a certification exam. The test has a set number of questions. It is timed, and you cannot pause and restart the timer.
- **Study Mode** Creates an untimed test during which you can review the correct answers and the explanations after you answer each question.
- **Custom Mode** Gives you full control over the test options so that you can customize them as you like.

In all modes, the user interface when you are taking the test is basically the same but with different options enabled or disabled depending on the mode.

When you review your answer to an individual practice test question, a “References” section is provided that lists where in the training kit you can find the information that relates to that question and provides links to other sources of information. After you click Test Results to score your entire practice test, you can click the Learning Plan tab to see a list of references for every objective.

## How to uninstall the practice tests

To uninstall the practice test software for a training kit, use the Program And Features option in Windows Control Panel.

## CompTIA professional certification program

---



CompTIA professional certifications cover the technical skills and knowledge needed to succeed in a specific IT career. Certification is a vendor-neutral credential. An exam is an internationally recognized validation of skills and knowledge and is used by organizations and professionals around the globe. CompTIA certification is ISO 17024 Accredited (Personnel Certification Accreditation) and, as such, undergoes regular reviews and updates to the exam objectives. CompTIA exam objectives reflect the subject areas in an edition of an exam and result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of a professional with a number of years of experience.

### **MORE INFO** COMPTIA CERTIFICATIONS

For a full list of CompTIA certifications, go to <http://certification.comptia.org/getCertified/certifications.aspx>.



Training materials given the CAQC seal has gone through a rigorous approval process to confirm the content meets exam objectives, language standards, necessary hands-on exercises and labs and applicable Instructional Design standards.

## How certification helps your career

---



Certification can help your Security career in the following ways:

- **Security is one of the highest demand job categories** Growing in importance as the frequency and severity of security threats continues to be a major concern for organizations around the world.
- **Jobs for security administrators are expected to increase by 18%** The skill set required for these types of jobs maps to the CompTIA Security+ certification.
- **Network Security Administrators** Can earn as much as \$106,000 per year.
- **CompTIA Security+ is the first step** In starting your career as a Network Security Administrator or Systems Security Administrator.
- **More than ¼ million** Individuals worldwide are CompTIA Security+ certified.

- **CompTIA Security+ is regularly used in organizations** Such as Hitachi Systems, Fuji Xerox, HP, Dell, and a variety of major U.S. government contractors.
- **Approved by the U.S. Department of Defense (DoD)** As one of the required certification options in the DoD 8570.01-M directive, for Information Assurance Technical Level II and Management Level I job roles.

## It pays to get certified

In a digital world, digital literacy is an essential survival skill. Certification demonstrates that you have the knowledge and skill to solve technical or business problems in virtually any business environment. CompTIA certifications are highly-valued credentials that qualify you for jobs, increased compensation and promotion.



Some of the primary benefits individuals report from becoming Security+ certified are:

- More efficient troubleshooting
- Improved career advancement
- More insightful problem solving

## Four steps to getting certified and staying certified

If you want to get certified and stay certified, follow these steps:

1. **Review Exam Objectives** Review the Certification objectives to make sure you know what is covered in the exam. Visit <http://certification.comptia.org/examobjectives.aspx> for information.
2. **Practice for the Exam** After you have studied for the certification, review and answer the sample questions to get an idea what type of questions might be on the exam. Go to <http://certification.comptia.org/samplequestions.aspx> for additional information.

3. **Purchase an Exam Voucher** Purchase exam vouchers on the CompTIA Marketplace, which is located at: [www.comptiastore.com](http://www.comptiastore.com)
4. **Take the Test** Go to the Pearson VUE website and schedule a time to take your exam. Visit <http://www.pearsonvue.com/comptia/> for information.

## Stay certified! Take advantage of continuing education

Effective January 1, 2011, new CompTIA Security+ certifications are valid for three years from the date of certification. There are a number of ways the certification can be renewed. For more information, go to <http://certification.comptia.org/ce>.

## How to obtain more information

---

You can obtain more information about CompTIA in several ways:

- Visit CompTIA online: At <http://certification.comptia.org/home.aspx> to learn more about getting CompTIA certified.
- Contact CompTIA: Call 866-835-8020 and choose Option 2 or email [questions@comp-tia.org](mailto:questions@comp-tia.org).
- Connect with us:
  - **LinkedIn** <http://www.linkedin.com/groups?home=&gid=83900>
  - **Facebook** <http://www.facebook.com/CompTIA>
  - **Twitter** <https://twitter.com/comptia>
  - **Flickr** <http://www.flickr.com/photos/comptia>
  - **YouTube** <http://www.youtube.com/user/CompTIATV>

## Acknowledgments

---

I would like to thank Mike Chapple, who pulled me into the world of professional writing, and who is both a mentor and a friend. I'd also like to thank all of those involved in the creation of this book, including our co-author James Michael Stewart; our technical editor Addam Schroll, whose thoughtful analysis, useful comments, and deep knowledge helped make our content even better; my ever helpful agent Carole Jelen from Waterside Productions; Kenyon Brown, our awesome senior editor; and Melanie Yarbrough, Kathy Krause, and the other staff at O'Reilly, OTSI, and Microsoft Press for their great work in making this a polished work.

This book wouldn't have been possible without the information security team at the University of Notre Dame, and my students in MGTI 30640, who asked great questions and drove conversations that shaped how I wrote explanations and stories in this book. Thank you!

Finally, I'd like to thank Lauren for providing balance and care as I wrote, my many wonderful and supportive friends who cheered me on through this process, and my librarian parents, Jim and Kathleen Seidl, for raising me with a love of books and writing.

—DAVID SEIDL

I would like to thank the many people who contributed to this book. First, my co-authors, David Seidl and James Michael Stewart, without whom we never would have been able to complete this project. Ken Brown from O'Reilly Media was an invaluable resource who pitched the idea to us and then guided us through the editorial process. Addam Schroll provided valuable insight with detailed comments on each chapter, while Melanie Yarbrough, Kathy Krause, and Marlene Lambert kept us on track and ensured that we didn't mangle the English language too badly! Finally, Carole Jelen with Waterside Productions, my literary agent, has served as my advocate and coach for the past decade.

My deepest thanks go to my wife, Renee, and my boys, Richard, Matthew, and Christopher, for their patience over the past six months as Dad spent many evenings and weekends pecking away at the keyboard wrapping up this project.

—MIKE CHAPPLE

Thanks to Mike Chapple and David Seidl for inviting me to contribute to this book. Working with you guys is and always has been a pleasure. Thanks to the management and editors at O'Reilly for putting up with my bad grammar. Thanks to my wife, Cathy, and our wonderful kids, Slayde and Remi—you will never be able to comprehend my love for you. To my dad, you are missed. To my mom, thanks for your love and consistent support; we are always here for you. To my best friend Mark—now that I'm 42, I realize how important the answer is to the ultimate question. And as always, to Elvis—now I see the wisdom of deep-fried, battered bacon.

—JAMES MICHAEL STEWART

## Support & feedback

---

The following sections provide information on errata, book support, feedback, and contact information.

### Errata

We've made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed on our Microsoft Press site:

*<http://aka.ms/CompTIAsecurityTK/errata>*

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, email Microsoft Press Book Support at:

*[mspinput@microsoft.com](mailto:mspinput@microsoft.com)*.

Please note that product support for Microsoft software is not offered through the addresses above.

### We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback our most valuable asset. Please tell us what you think of this book at:

*<http://www.microsoft.com/learning/booksurvey>*

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

### Stay in touch

Let us keep the conversation going! We are on Twitter: *<http://twitter.com/MicrosoftPress>*.

## Preparing for the exam

---

The CompTIA Security+ exam is a great way to build your resume, and to show potential employers that you have the knowledge you need for a career in information security. This book covers the CompTIA Security+ body of knowledge, and includes both real-world knowledge and practical explanations that will help you apply what you learn in the real world.

As you prepare for the exam, we recommend that you use the self-check questions in the book to help test your knowledge as you read each chapter. When you're ready to test your knowledge, use the included self-tests to take the next step to prepare for the exam. If you want more hands-on classroom experience, you might also choose to take the CompTIA Security+ professional certification course.





# Risk management and incident response

Information security is the art and practice of managing the confidentiality, integrity, and availability risks associated with information. As you begin your exploration of the field, it is best to start with that in mind. In this chapter, we'll explore the process that security professionals use to identify, assess, and manage the risks facing their organizations. We will also review the incident response procedures used when a risk materializes.

**IMPORTANT**  
***Have you read page xxxi?***

It contains valuable information regarding the skills you need to pass the exam.

## Exam objectives in this chapter:

Objective 2.1: Explain risk related concepts

- Control types
  - Technical
  - Management
  - Operational
- Risk calculation
  - Likelihood
  - ALE
  - Impact
- Quantitative vs. qualitative
- Risk-avoidance, transference, acceptance, mitigation, deterrence
- Risks associated to Cloud Computing and Virtualization

Objective 2.2: Carry out appropriate risk mitigation strategies

- Implement security controls based on risk
- Change management

- Incident management
- User rights and permissions reviews
- Perform routine audits

Objective 2.3: Execute appropriate incident response procedures

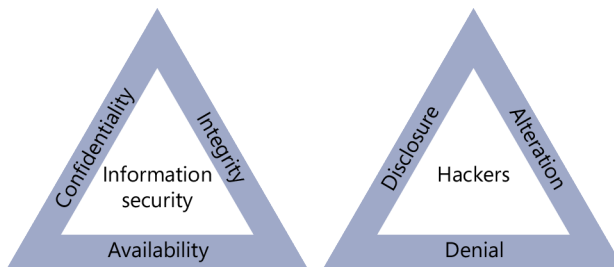
- Basic forensic procedures
  - Order of volatility
  - Capture system image
  - Network traffic and logs
  - Capture video
  - Record time offset
  - Take hashes
  - Screenshots
  - Witnesses
  - Track man hours and expense
- Damage and loss control
- Chain of custody
- Incident response: first responder

Objective 2.8: Exemplify the concepts of confidentiality, integrity and availability (CIA)

## CIA and DAD triads

---

Security professionals, tasked with protecting the information assets of an organization, typically think of their responsibilities in three realms: confidentiality, integrity, and availability (CIA). Adversaries, seeking to disrupt an organization's security, have three corresponding goals in mind: disclosure, alteration, and denial (DAD). These models, shown in Figure 1-1, are known as the CIA and DAD triads and are the classic models embraced by security professionals around the world.



**FIGURE 1-1** The CIA and DAD triads are the classic models of information security principles.

## Confidentiality and disclosure



The goal of *confidentiality* is to prevent unauthorized access to sensitive information. Quite simply, it is to keep secrets secret. Achieving confidentiality first requires that an organization classify its data—identifying which information assets are worthy of protection and the appropriate level of protection for each. For example, an organization might consider design documents for an unreleased product highly sensitive due to their competitive value. On the other hand, the internal phone book might be considerably less sensitive. Organizing confidential information into different data classifications allows security professionals to design appropriate controls, focusing scarce resources on the most sensitive data.

Adversaries, on the other hand, pursue the goal of *disclosure*, gaining access to sensitive information without permission. They may want to use this information for personal gain, to embarrass the organization publicly, or to simply make information freely available.

### Real world

#### WikiLeaks

The WikiLeaks website, made famous by disclosures of sensitive US government information by Bradley Manning in 2010 and Edward Snowden in 2013, is dedicated to the disclosure of information that governments and corporations may find embarrassing.

## Integrity and alteration



Security professionals also pursue the goal of *integrity*, ensuring that information is only modified or deleted by authorized means. Protecting the integrity of information requires controls against deliberate *alteration* by adversaries—such as an employee seeking to modify his payroll information without permission. It also requires protection against unintentional alteration, such as the corruption of data due to a software or hardware failure.

### **MORE INFO** INTEGRITY CONTROLS

Chapter 4, “Operational and environmental security,” covers integrity controls in more detail and includes a discussion of disaster recovery and business continuity procedures.

## Availability and denial



It's not sufficient for security professionals to provide confidentiality and integrity controls. These must be supplemented with *availability* protection that ensures that authorized individuals have access to information when needed. *Denial* attacks occur when an adversary is able to successfully interrupt the availability of information, such as through a denial of service (DoS) attack. Adversaries might also attempt to harness many systems around the world

to simultaneously perform a denial attack by using a technique known as distributed denial of service (DDoS).

#### **MORE INFO** DOS AND DDOS ATTACKS

Chapter 5, “Threats and attacks,” includes a discussion of denial of service and distributed denial of service attacks.

#### **Quick check**

1. What are the three goals of information security professionals?
2. What are the corresponding three goals of hackers?

#### **Quick check answers**

1. Confidentiality, integrity, and availability
2. Disclosure, alteration, and denial

## Risk assessment and mitigation

---

In order to meet the three goals of confidentiality, integrity, and availability, security professionals must have a solid understanding of the specific risks facing their organization. These will vary, depending upon the organization’s line of business, types of information handled, and even physical location. For example, an educational institution might consider the loss of student records, preventing grades from being issued, to be its greatest risk; whereas a military unit might believe that its greatest risk is the disclosure of secret plans that might lead to the death of personnel. Similarly, a business located in Florida might be very concerned about the risk posed by a hurricane, whereas a business in Nebraska would worry more about tornados.

To perform an assessment of risks, we first must have a common language. There are three important terms related to risk assessment:



- **Vulnerabilities** Weaknesses in an organization’s security controls that might allow a breach of confidentiality, integrity, or availability. Vulnerabilities are internal factors.
- **Threats** External forces that might undermine the security controls of an organization.
- **Risks** Situations that occur when there is an intersection of a vulnerability in an organization’s security controls and a threat that seeks to exploit that vulnerability (see Figure 1-2).



**FIGURE 1-2** This equation shows the relationship between threats, vulnerabilities, and risks.

Consider the example of a web server that contains sensitive, password-protected information that has limited distribution to the customers of an organization. An individual who seeks to gain access to this information without paying is a threat to the confidentiality of that data. A misconfiguration in the web server that allows unlimited attempts to guess the password is a vulnerability. The combination of this vulnerability with a corresponding threat seeking to exploit it presents the risk that the organization's information will be stolen.

A vulnerability without a corresponding threat does not pose a risk to the organization. For example, an organization's data center might be vulnerable to flooding. If the data center is in a desert environment where there is no threat of flooding, there is no risk to manage. Similarly, a threat without a corresponding vulnerability also does not pose a risk. If an intruder knows how to pick locks, he may pose a threat to your organization, but if you use locks that have keypads rather than keys, they are not vulnerable to this threat. (Of course, they remain vulnerable to an intruder who knows how to defeat the keypad!)

Organizations seeking to secure their information normally begin with a risk identification process that enumerates the threats facing the organization, the vulnerabilities in the organization's existing security controls, and the risks that result from intersections between these threats and vulnerabilities.

## Likelihood and impact

After an organization identifies those threats and vulnerabilities that pose a risk to their information assets, the next step in the risk assessment process is to evaluate the priority of those risks based upon two factors:

- The *likelihood* that a risk will materialize. Some risks are simply more likely than others, depending upon the nature of the vulnerability or threat. For example, the threat of a physical break-in is much more likely to occur in a high-crime urban environment than it is on a military base located in a desert.
- The *impact* that a risk will have on the organization if it does materialize. Some breaches of confidentiality, integrity, or availability will have more disruptive impacts on an organization than others. For example, a successful website denial of service attack might have low impact on a construction firm, but the same attack would be disastrous for an e-commerce retailer that depends upon the website to generate revenue.

Organizations might perform this risk assessment by using techniques that fall into two different categories: qualitative techniques and quantitative techniques.

## Qualitative risk assessment

Qualitative risk assessment uses the subjective judgment of experts to evaluate the likelihood and impact of risks facing the organization. The process used to create a qualitative risk assessment can range significantly, depending upon the sophistication of the organization. Some organizations with advanced risk assessment capabilities have standing executive committees that meet regularly to discuss and evaluate risks. In less formal approaches, several experts at lower levels in the organization might work together to develop a qualitative risk assessment.

Regardless of the approach, qualitative assessments rely upon the judgment and institutional knowledge of these individuals to rank risks based upon the likelihood that they will occur and the impact on the organization if they do. The most common approach is to assign each risk a rating of "high," "moderate," or "low" for both likelihood and impact. The results can then be visually portrayed in a matrix similar to the one shown in Figure 1-3.

Likelihood	High	Power outage	Disclosure of employee SSNs	Website DoS
	Moderate		Database corruption	
	Low	Theft of encrypted laptop		Tornado
		Low	Moderate	High
		Impact		

**FIGURE 1-3** A matrix such as this can be used for qualitative risk assessment.

Using this type of visual approach for a qualitative risk assessment allows decision-makers to easily grasp the priority of addressing each risk. In the matrix shown in Figure 1-3, it is apparent that the greatest risk facing the organization is a denial of service attack on the website (high likelihood, high impact). If the organization's chief information officer is trying to decide between investing in availability controls that will reduce the likelihood that the risk will materialize or purchasing anti-theft devices for encrypted laptops, she will be able to make the decision easily after reviewing the qualitative risk assessment. Improving the availability controls addresses a much more significant risk than protecting encrypted laptops against theft (low likelihood, low impact).

## Quantitative risk assessment

Quantitative risk assessments take a more rigorous approach, using numeric data to perform risk calculations in terms of financial value. This requires the use of several factors and formulas:



- Organizations must first identify the *asset value (AV)* for each asset covered by the risk assessment. AV is normally expressed in terms of dollar value. This can be done by using a variety of valuation techniques, such as purchase price, replacement cost, or depreciated value. It's a good idea to consult your organization's financial division to ensure that the asset valuation technique used in your risk assessment process is consistent with organizational standards.

### **NOTE DETERMINING ASSET VALUE**

Identifying the value of an asset can be quite difficult, especially for information assets. It's easy to put a value on a server by using either the purchase price or replacement cost. But what is the value of a list of employee Social Security numbers (SSNs)? One way of valuing such intangible assets is to estimate the costs you would incur if the information were disclosed or lost.

- For each risk facing an asset, the risk assessment process next identifies the *exposure factor (EF)*. The exposure factor is the amount of damage that would occur to an asset if the risk were to materialize; this is normally expressed as a percentage. For example, if the risk of fire is likely to destroy half of a data center, the EF is 50 percent.
- The last input into the quantitative risk assessment process is the *annualized rate of occurrence (ARO)*. This is the likelihood that the risk will materialize, expressed as the number of times the risk is expected to occur in a typical year. The value may be less than one if the risk is expected less than once per year. For example, a business located in a 100-year flood plain expects flooding once every 100 years. The ARO for this risk would be 1 in 100, or 0.01.
- Next, the risk assessment process calculates the *single loss expectancy (SLE)*. This is the impact of the risk, expressed as the financial loss that occurs each time the risk materializes; it is calculated by using this formula:

$$SLE = AV \times EF$$

- Finally, the risk is calculated as the product of likelihood (ARO) and impact (SLE) by using this formula:

$$ALE = SLE \times ARO$$

This formula provides the *annualized loss expectancy (ALE)*, or the expected financial loss that will occur due to the risk in a typical year.

## **NOTE** CLOUD COMPUTING RISKS

The rapid adoption of cloud computing services in many organizations poses new risks that must be brought into the risk assessment process. If you use cloud services in your organization, you should ensure that your process includes the identification and assessment of cloud-related risks, including:

- Information being stolen from the cloud provider.
- Another user of a shared cloud service gaining access to your data stored on a shared server.
- The cloud provider suddenly going out of business, leaving you unable to access your data.
- An outage at the cloud provider causing them to violate their service level agreement (SLA).
- The activity of another customer in the cloud service causing service degradation that disrupts your service.

Let's work through an example of quantitative risk assessment. Consider a data center located in the San Francisco Bay Area. Risk managers for the firm owning the data center would certainly be interested in assessing the risk associated with an earthquake damaging the data center. Here's the process they would go through to do this by using quantitative techniques:

1. Identify the asset value (AV). They might do this by consulting data center construction experts and determining that the replacement cost of the data center would be \$20 million. (AV = \$20 million)
2. Determine the exposure factor (EF). Consulting with those same experts might identify that the data center would be half destroyed by a significant earthquake. (EF = 50 percent)
3. Identify the annualized rate of occurrence (ARO). This is the likelihood of an earthquake occurring in a particular year. The US Geological Survey estimates that the Bay Area is likely to suffer an earthquake causing extensive damage once every 30 years. (ARO = 0.03)
4. Calculate the single loss expectancy (SLE). This is the impact of an earthquake, expressed as the financial loss that a single earthquake would create, and is calculated as the product of the asset value and exposure factor:

$$SLE = AV \times EF$$

$$SLE = \$20 \text{ million} \times 50 \text{ percent}$$

$$SLE = \$10 \text{ million}$$



5. Calculate the annualized loss expectancy (ALE). This is the risk, expressed as the financial loss from earthquakes expected in a typical year:

$$ALE = SLE \times ARO$$

$$ALE = \$10 \text{ million} \times 0.03$$

$$ALE = \$300,000$$

A risk manager can now use the annualized loss expectancy to make risk-based decisions. For example, an earthquake insurance policy with a \$50,000 annual premium would be a good investment!

## Managing risk

After an organization completes a risk assessment, it has a clear picture in quantitative and/or qualitative terms that allows it to prioritize the risks facing the organization. Security professionals must then take action to manage those risks. They have five options at their disposal: risk avoidance, risk transference, risk mitigation, risk deterrence, and risk acceptance. They can select one or more of these strategies for each risk identified in the risk assessment.

### Risk avoidance



In a *risk avoidance* strategy, the organization changes its business activities to avoid the risk entirely. For example, an organization considering the earthquake risk described in the quantitative risk assessment section of this chapter might decide that the risk is simply too high to justify and decide to relocate the data center to an area that is not threatened by earthquakes. In other cases, an organization might be able to stop performing a particular activity that creates risk. For example, an organization concerned about the theft of Social Security numbers might decide to stop collecting them and purge them from its databases.

Risk avoidance is often a dramatic step that involves significant time and expense to implement. In many cases, business requirements prevent the use of this strategy because of the disruption of necessary business activity. For example, a credit card processing company cannot decide to entirely avoid the risk of handling highly sensitive credit card information without going out of business!

### Risk transference



*Risk transference* moves the impact of a risk from one entity to another. The most common form of transferring risk is the purchase of an insurance policy where, in exchange for a periodic premium payment, an insurance company agrees to accept the financial risk associated with an asset or activity. Businesses often purchase insurance policies for fire, accident, theft, and other risks. It is also becoming more common to see organizations purchase insurance that protects against information security liabilities.

Another form of risk transference takes place when two entities sign a contract that contains an indemnification clause. When placed into a contract, an indemnification clause specifies the terms under which one entity will assume responsibility, especially financial responsibility, for a particular type of liability. For example, a company that provides you with cloud services might indemnify you against the risk that their software violates the intellectual property of a third party. In the event that a third party later attempted to sue you for damages, the indemnification clause of your contract would transfer liability for those damages to the cloud provider.

## Risk mitigation



The most common risk management strategy followed by information security professionals is *risk mitigation*. In this strategy, security professionals use controls designed to reduce the likelihood that a risk will affect an organization and/or the impact that a risk will have on the organization if it materializes.

When an organization decides to adopt a risk mitigation approach, it designs and implements one or more security controls that can be directly mapped to that risk. For example, an organization seeking to reduce the risk of network intrusion might decide to install a network firewall, a network intrusion prevention system, and monitoring software. Each of these three controls can then be directly mapped to the risk of network intrusion.

### **NOTE** VIRTUALIZATION RISKS

The increased use of virtualization to host multiple guest operating systems on a single hardware platform promises reduced costs and increased efficiencies, prompting many IT organizations to pursue virtualization strategies. Security professionals in organizations adopting virtualization have additional risks that they should consider mitigating. For example, they should take steps to ensure that it is not possible for someone working inside a guest operating system to gain access to the virtualization platform or other guest operating systems. This attack, known as a “VM escape,” runs the risk of exposing unrelated, and potentially sensitive, data to unauthorized individuals.

## Risk deterrence



In some cases, the organization might be able to adopt a strategy of *risk deterrence*. This approach uses measures designed to reduce the likelihood that a threat will surface. The most common example of deterrence is used to thwart criminal activity by counter-threatening with an aggressive reaction stance. For example, an organization might aggressively prosecute individuals who attempt to intrude into computer systems without permission. Similarly,

the owners of a physical facility might have vicious guard dogs on site that threaten intruders with bodily harm. This strategy, used judiciously, can be highly effective, because criminals looking for a target of opportunity will simply go elsewhere.



#### **EXAM TIP**

The CompTIA Security+ exam is just about the only place where you will see risk deterrence listed as a risk management strategy. Almost all security professionals, the authors included, consider risk deterrence a form of risk mitigation. However, when you are asked questions about risk management on the CompTIA Security+ exam, you should treat it as a separate category.

## Risk acceptance



In some cases, an organization might decide that *risk acceptance* is the most appropriate strategy for managing a particular risk. In this scenario, after careful evaluation, the organization decides that the most prudent course of action is to simply monitor the evolution of a risk. Cost or operational concerns dictate that the organization cannot or should not avoid, mitigate, transfer, or deter the risk, so no further action is taken.

#### **NOTE RISK ACCEPTANCE SHOULD BE ON AN EDUCATED BASIS**

It's far too easy to look at a complex risk and simply utter the words "we accept that risk as a cost of doing business." This is not an acceptable risk management strategy, because it is more akin to *ignoring* a risk rather than accepting it. Risks should only be accepted after careful study and analysis reveals that there simply is no other acceptable strategy for managing the risk.



#### **Quick check**

1. What are the five risk management strategies?
2. What risk management strategy is most commonly used by information security professionals?

#### **Quick check answers**

1. Risk avoidance, risk transference, risk mitigation, risk acceptance, and risk deterrence
2. Risk mitigation

# Security controls

---

As mentioned in the previous section, security professionals spend a large amount of their time developing ways to mitigate risks facing an organization's information assets. The methods they develop to reduce risk are known as security controls and are grouped into three categories: technical controls, operational controls, and management controls. A balanced approach to information security combines controls from each of these categories to mitigate a wide variety of risks.

## Technical controls



*Technical controls*, as the name implies, leverage technology to reduce the likelihood or impact of a risk on an organization. These controls are typically implemented with the advice and consultation of security professionals and are then maintained either by security professionals, system administrators, network engineers, database administrators, or other technical staff with the appropriate skillset.

Examples of technical controls abound in the security industry. Firewalls, intrusion detection systems, and wireless encryption are examples of technical controls used in network security. Antivirus software, full disk encryption, and user authentication are examples of technical controls for host security. Transport encryption, input validation, and role-based access are examples of application-oriented technical controls. Most organizations with a well-developed security program can likely list dozens of individual technical controls in place to mitigate various security risks.

## Operational controls



*Operational controls* are similar to technical controls in that they directly impact information systems, but the job of carrying out an operational control is primarily done by individuals, rather than technology. For example, although implementing access control systems is a technical control, performing periodic reviews of user rights and permissions is an operational control. Similarly, the process of business continuity planning, which is discussed in Chapter 4, is an operational control. Other operational controls include conducting routine information security audits, implementing change and configuration management procedures, ensuring physical security, and conducting background checks and other personnel security measures.



### **EXAM TIP**

This is another area where you might have to throw away what you've learned or read elsewhere and study the terminology that is specific to the CompTIA Security+ exam. Although the CompTIA Security+ exam classifies controls into technical, management, and operational categories, other references use different classification schemes. For example, the Certified Information Systems Security Professional (CISSP) curriculum classifies the categories as administrative, physical, and technical controls. Others might describe controls by their role: preventive, detective, and corrective. Just be sure to stick with technical, management, and operational when taking the CompTIA Security+ exam.

## Management controls



*Management controls* are those controls focused on the risk management process itself. They ensure that the risk management process is running effectively and, therefore, have an indirect impact on the security of an organization's information assets. Operational and technical controls, on the other hand, directly impact those assets.

Examples of management controls include conducting periodic risk assessments and security control assessments, following a security planning process, and protecting the security of the system and services acquisition life cycle.

### **MORE INFO CONTROLS**

A large portion of this book is dedicated to describing security controls in more detail. For example, Chapters 2 and 3 describe technical controls for network security, Chapter 4 covers operational controls, and Chapters 6 and 7 cover a variety of management controls.



### **Quick check**

1. What are the three categories of controls discussed on the CompTIA Security+ exam?
2. Firewalls are an example of what type of control?

### **Quick check answers**

1. Technical, operational, and management
2. Technical

# Incident response

---

Though security professionals strive to ensure that risk management and control processes prevent breaches of confidentiality, integrity, and availability, it is simply impossible to build a completely secure system. A determined (or lucky) attacker can often find a way to bypass even the most sophisticated control systems. Therefore, security professionals must also develop, train on, and implement sound incident response procedures to activate in the event of an information security incident. In this section, you'll learn the building blocks of a solid incident response program.

## Real world

### Advanced persistent threats

If you're wondering whether it is really possible to breach your well-designed security controls, consider the risk posed by the advanced persistent threat (APT). In this scenario, a determined attacker with tremendous resources focuses on breaching the security controls of your organization in particular. Although you certainly may have designed your defenses in such a way that they will easily foil the determined attacker, would you be able to defend against someone who carefully studies your organization, perhaps with insider knowledge, and then dedicates a team of highly skilled individuals with advanced tools to penetrating your defenses? Though this might sound far-fetched, it's exactly what happened to a nuclear enrichment plant in Iran that was the victim of the Stuxnet attack. In the Stuxnet case, a group of dedicated programmers spent several months developing a worm with one purpose—to work its way into the central control systems of the plant to destroy the centrifuges. Although no government has publicly taken credit for the attack, it is widely assumed that the United States and/or Israel was behind it.

## Incident response team

Appropriately responding to an information security incident requires the carefully coordinated actions of a team of highly skilled individuals who have been trained on the organization's consistent process for incident response. This is simply not something that you can pull together "on the fly." Success during a security incident requires careful advance planning, including the selection and training of an incident response team.

### First responder responsibilities

It's important to recognize that the first responders on the scene of an information security incident will most likely *not* be members of your trained incident response team. The first person to notice the sign of an information security incident is more likely going to be a

system administrator, computer operator, or even an end user. For this reason, you should consider every member of your staff to be a member of your “extended” incident response team and provide some level of training across the organization. There are three basic elements to this training:

- 1. Recognizing a security incident** Everyone in the organization should have an understanding of what constitutes a security incident in the eyes of your firm.
- 2. Activating the incident response process** Next, first responders should have a clear, easy way to activate your formal incident response process. It should be simple for them to, in a sense, dial your “information security 911” to have trained professionals jump into action to assume control of the incident.
- 3. Containing the incident** Finally, most technical staff in your organization should know how to perform the equivalent of “information security first aid.” Just as a bystander wouldn’t stand by and wait for an ambulance while an accident victim bled profusely, IT staff should feel confident enough to take immediate action to stem the effect of a security incident. Actions as simple as disconnecting the network cable from a system that appears to be transmitting unencrypted credit card data to an offsite location can mean the difference between a minor and major security incident. Seconds matter when it comes to the early stages of incident response.

**NOTE DON'T SHOOT THE MESSENGER**

When you train large portions of your staff on first responder tactics, understand that they will make mistakes. Staff members will jump the gun and activate the incident response process in cases where there simply is no security incident. The way your organization reacts to these mistakes is just as important as your response to a true security incident. If the person who activated the process feels belittled or punished in any way, he will hesitate to ever again activate the incident response process. Even worse, others in the organization will hear the story, and it will give them pause as well. No matter what, you should always thank first responders for bringing a potential incident to your attention and make sure they understand that they made the right decision calling in the incident response team.

Of course, the level of detail that you provide should vary depending upon the role of the individuals within your organization. Staff members with no technical responsibilities whatsoever might simply get an awareness message letting them know that they should report any suspicious computer activity to a centralized security operations center or network team. System and network administrators might receive a full day of training that helps them understand how to recognize the early warning signs of a security incident and the basic steps that should be followed during incident containment.

## Staffing the incident response team

Responding to an information security incident requires an interdisciplinary approach that will call upon the expertise of many different professionals from throughout your organization. Remember, responding to security incidents is not just an “infosec thing,” nor is it purely a technical matter. Although information security professionals and other technical staff play an important role in incident response, it is equally important to have a well-rounded team that can handle all aspects of incident response.

There are eight categories of staff that you should consider representing on your incident response team. This does not necessarily mean that you will only have eight slots on the team, for two reasons. First, you need to plan to have a redundant team. If the attorney on your team is vacationing in Barbados when an incident occurs, you need to know that there is someone else available who can represent the legal issues. Second, some areas are broad enough that no one person can represent the entire field. For example, a network engineer would not likely be able to address database administration issues, nor would a database administrator be able to cover network issues. The categories of staff you should consider when developing your team are:

- **Management** Quite simply, somebody needs to be in charge. Incident response without one officially designated leader can quickly devolve into many uncoordinated efforts, as everyone begins to pursue their own hunches and preferred courses of action. You need one strong leader to rein in these natural tendencies and direct the response. Additionally, difficult decisions will be made during the response to an information security incident, and you need to be sure that the team has a manager on hand with sufficient authority to make those calls without having to call in senior managers for consultation.
- **Information security** Information security staff will play an essential role in all stages of incident response. They bring subject matter expertise to the table that can be especially helpful when attempting to identify the root cause of an incident or to quickly develop *ad hoc* controls to contain the damage caused by a security incident. Security staff also have access to unique resources, such as firewalls, intrusion detection/prevention systems, and security incident and event management (SIEM) systems that might contain data relevant to the security incident.
- **Technical staff** In addition to information security professionals, you should have a representative from every major technical discipline in your organization on the incident response team. You certainly might not need all of these staff to respond to every incident, but you need to be prepared to react to a security incident that touches any part of your computing environment. System administrators, network engineers, database administrators, and application developers all might play critical roles in responding to an incident that either centers on or touches upon their operational domains.



- **Legal** Many security incidents turn into legal matters, either because criminal prosecution is involved or because the firm becomes engaged in civil litigation as a consequence of the security incident. In addition, there are specific legal provisions that might dictate elements of your incident response process. For example, most states now have data breach notification laws that require the timely notification of individuals if their data is known or reasonably believed to have been compromised during an information security incident.
- **Communications and public relations** You might need to issue some type of public statement, and you will need to react if the media gets wind of the fact that a security incident is unfolding at your organization. Communications staff should become involved early both to handle these situations and provide advice on the best time to inform outsiders that an incident is taking place.
- **Human resources** In any incident where insider involvement is suspected, you should include representatives from your human resources department. You should definitely consult HR before interviewing any suspects who are employees of the organization. HR should also lead any disciplinary process that might take place against employees who are believed to have been involved in the incident, because such investigations are personnel matters that are within their realm of expertise.
- **Risk management** Your organization's risk management staff will play an important role in security incidents of extended duration or impact. Individuals from this group will likely be the experts on your firm's business continuity and disaster recovery strategies and can help implement those contingency plans if it becomes necessary. Additionally, staff from the risk management area will be able to best inform the team on the provisions of any insurance policies that might cover portions of the incident response measures.

#### **MORE INFO BUSINESS CONTINUITY AND DISASTER RECOVERY**

Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP) are discussed in detail in Chapter 4. They are both important subjects on the CompTIA Security+ examination.

- **Facilities** If physical security is involved in a security incident, your facilities group can provide important expertise regarding your buildings and other physical infrastructure.

Developing a well-rounded incident response team is an important component of any strong incident response program. You should identify individuals to fill each of these roles and ensure that they understand the scope of their incident response functions.

#### **NOTE** OUTSOURCING INCIDENT RESPONSE

Many organizations are turning to outsourced providers to perform a variety of information technology functions, and incident response is no exception. Although it is possible to outsource your entire incident response program to an outside provider, this is uncommon, because some degree of institutional knowledge is critical to a successful response. However, it is certainly possible to outsource components of incident response, especially where very specialized technical skills are required. For example, you might not have use of a full-time computer forensics investigator on your staff if those skills are only required a few times a year. Instead, you might retain a forensics firm with a rapid response capability and have them perform this role on an as-needed basis. If you do choose to outsource components of incident response, remember that making these arrangements in advance should be a part of your incident response planning process. You don't want to wait until an incident is underway to try to identify and contract with a forensics firm. You should already have a contract signed so that you can simply activate the resource when you need it.

### **Training the incident response team**

The training you provide to your incident response team should cover a wide variety of topics that prepare the team members to handle different types of information security incidents. This training should include a core set of modules that all team members receive, covering the following topics:

- Overview of the organization's incident response process
- Roles and responsibilities of each team member
- Activation procedures in the event of an incident
- Detection and analysis of security incidents
- Containment procedures
- Eradication procedures
- Recovery procedures
- Post-incident procedures

In addition, each team member should receive specialized training on the incident response tools and techniques specific to her area of expertise. For example, database and system administrators should be familiar with their roles in a forensic analysis, including proper collection procedures and the chain of custody. Attorneys should have specialized continuing legal education on the laws and regulations that pertain to information security incidents.

All of these training modules should be conducted on both an initial and recurring basis. If you are developing a new incident response capability, you could have large group sessions to bring the entire team up to speed at once. If you are maintaining an existing program, you will need to conduct initial training sessions for those staff members who are new to the incident response team. Additionally, you will need to conduct periodic refresher training

for veteran team members to ensure both that they don't get "rusty" and that they become familiar with any changes in the incident response plan.

Finally, a critical component of any training program is giving responders hands-on experience. This is especially important in organizations that do not often activate their incident response teams. Conducting a series of drills can help familiarize staff with their roles in an actual incident. These drills can range from checklist reviews to tabletop exercises or even full-blown incident simulations.

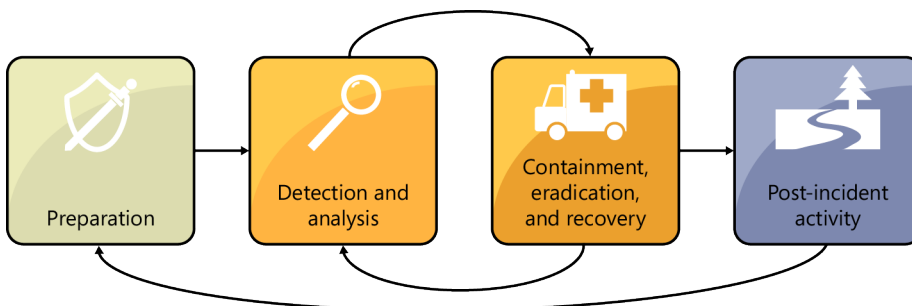
#### **MORE INFO CONDUCTING INCIDENT RESPONSE DRILLS**

Incident response drills are actually quite similar to the tests used for business continuity and disaster recovery plans that will be discussed in Chapter 4. You might want to integrate these two programs and conduct combined drills. For example, you might conduct a drill that simulates an attacker conducting a denial of service attack against your website. The drill might begin as an incident response scenario and then evolve into a disaster recovery effort when the website becomes completely inaccessible.

## Incident response life cycle

Every incident response process follows a life cycle approach, whether it is formally defined or not. The National Institute of Standards and Technology (NIST) defines one such life cycle approach, using the four-phase process shown in Figure 1-4. This includes four distinct phases:

1. Preparation
2. Detection and analysis
3. Containment, eradication, and recovery
4. Post-incident activity



**FIGURE 1-4** The incident response life cycle contains four steps (NIST).

Each of these stages has goals and objectives that will be discussed in the next several sections of this chapter. Also, be sure to take note of the multiple arrows and their directions

in Figure 1-4. The incident response life cycle is not a sequential march through four phases. Rather, it is an iterative process that might loop through some steps multiple times as an incident evolves. Most notably, the steps taken during the containment, eradication, and recovery phase might identify additional information that requires analysis, causing a loop back to the detection and analysis phase.

Additionally, the entire process should be viewed as a repeating cycle. At the conclusion of each incident, you engage in post-incident activity that includes a lessons-learned session assessing the functioning of the incident response process. This information then feeds back into the preparation phase, providing valuable input regarding potential improvements to your organization's incident response process.

## Preparation

The preparation phase of incident response includes establishing an incident response process, selecting a team, and training them on the plan. These steps were described earlier in this chapter.

In addition to those preparation steps, the incident response team members should ensure that they have the tools and resources needed to respond to any eventuality. Many teams choose to create a "go bag" that contains all of the tools needed to get an incident response underway quickly. At a minimum, the "go bag" should contain a forensic laptop, a variety of cables and connectors, several types of blank media for imaging systems, and other essential gear required by members of the response team. The "go bag" should be considered sacrosanct and should be inventoried periodically to ensure that nobody has "borrowed" equipment from the kit. You don't want to activate the team and get on site only to discover that essential equipment was purloined temporarily for a project and is not actually in the kit.

In addition to the incident response life cycle, NIST offers a suggested list of tools and resources that should be maintained by incident response teams. They suggest that every team have access to the following:

- **Communications and facilities resources**
  - Contact information for team members, other internal resources, law enforcement contacts, and contractors
  - On-call information for other teams within the organization that might play a role in incident response
  - Incident reporting mechanisms
  - Issue tracking system
  - Smartphones
  - Encryption software for intra-team communication and collaboration with outside parties

- A permanent or temporary war room to act as a central coordination point during incident response
- A secure storage facility for evidence gathered during an incident response effort
- **Incident analysis hardware and software**
  - Digital forensic workstations and/or backup devices to create disk images and preserve other types of digital evidence
  - Laptops for team member use that are separate from the forensic workstations
  - Spare equipment for use during the response, including workstations, servers, and network gear
  - Blank removable media (lots of it!)
  - Removable media loaded with forensic tools (potentially including bootable images)
  - A printer
  - Packet-sniffing and network protocol analysis hardware and software
  - Forensic software
  - Notebooks, cameras, recorders, and other equipment to gather evidence and notes
- **Incident analysis resources**
  - Network diagrams
  - Lists of critical information assets
  - Architectural diagrams, especially of critical/sensitive services
  - Baselines of “normal” system, network, and application activity
  - A detailed listing of firewall rules and ports

Many teams have a full-time incident response coordinator (often a member of the information security team) who is responsible for gathering resources and ensuring that everything is ready to go in the event of an actual incident. This coordinator might also facilitate the incident response planning, training, and simulation processes for the organization. Smaller organizations might choose to make this a part-time responsibility for a team member with other information security duties.

## Detection and analysis

The detection and analysis phase has two distinct components. First, during periods of normal activity, trained security analysts monitor systems for signs of a security incident. This may include monitoring:

- Intrusion detection and prevention systems.
- Security incident and event management (SIEM) systems.

- Firewalls.
- Centralized antivirus monitoring software.
- Logs from critical systems, applications, and devices.
- File/system integrity monitoring software.
- Vulnerability scanners.
- External reports of malicious activity (for example, attacks emanating from your network).
- Reports from staff and customers.

Analysts monitoring these sources for signs of an information security incident will activate the formal incident response process in the event that they detect an incident.

When an incident is detected, analysts are responsible for gathering enough information to guide the response effort. This can involve coordinating information from the same sources used to detect the incident as well as activating additional information collection mechanisms. For example, analysts might begin capturing network traffic in real-time by using packet sniffers to preserve evidence of a network-related incident.

Another important part of the analysis phase is assessing the impact of the incident. This can be done by classifying the event into one of three categories:

- **Low impact** Incidents that have minimal or no potential to affect the confidentiality, integrity, or availability of the organization's operations and/or information assets. It is unlikely that a low-impact event would warrant a major after-hours response or the activation of the full incident response team.
- **Moderate impact** Incidents that have the potential to have a significant impact on the confidentiality, integrity, or availability of the organization's operations and/or information assets. They might disrupt some business activities and might require the activation of the incident response team.
- **High impact** Incidents that have the potential to critically damage the confidentiality, integrity, or availability of the organization's operations and/or information assets. They might have a very serious, potentially permanent, impact on the organization and should entail immediate activation of the full incident response team.

Every organization will need to define its own criteria for triaging security incidents and determining the incident categorization scheme appropriate for its environment. Those criteria will vary depending upon the types of information handled by the organization and the criticality of various business processes supported by information technology.

## Containment, eradication, and recovery

The containment, eradication, and recovery phase of an incident response typically encompasses what most security professionals consider to be the "meat" of the process. It includes steps taken to minimize the damage caused by a security incident, remove the threat, and return to normal operations. Though incident response guides typically describe this as a single phase,

it is clearly divided into two different types of complementary activities: containment activities and eradication/recovery activities.

## CONTAINMENT ACTIVITIES

Containment activities are focused on damage control and preventing further loss to the organization. The steps followed will vary depending upon the type of incident taking place and the technical countermeasures available. Some examples of security incident containment strategies include:

- Provisioning additional bandwidth to cope with the impact of a network denial of service attack.
- Disconnecting a potentially compromised server from the network to prevent the exfiltration of sensitive information.
- Isolation of a network segment to prevent further spread of malware that has infected systems on that segment.
- Creating temporary firewall rules to block external access to a system that is acting suspiciously.

Security professionals must work closely with other technical staff during containment activities to design a containment strategy that appropriately balances the needs of the organization with security concerns. Your organization should maintain an incident containment plan for each of the major types of attack in your planning scheme to allow for advance planning in as many situations as possible.

NIST offers six criteria that incident response planners and teams can use when developing an appropriate containment strategy:

- Potential damage to and theft of resources
- Need for evidence preservation
- Service availability (for example, network connectivity or services provided to external parties)
- Time and resources needed to implement the strategy
- Effectiveness of the strategy (for example, partial containment or full containment)
- Duration of the solution (for example, an emergency workaround to be removed in four hours, a temporary workaround to be removed in two weeks, or a permanent solution to the problem).

Another important consideration is that containment strategies are likely to alert an attacker to the fact that security responders have detected his activity. This might cause an immediate termination of the attack. Although this is certainly good from the perspective of preventing further damage, it limits the ability of responders to gather evidence that can be used to track down and prosecute offenders. The incident response plan should contain guidelines to help teams make these determinations. Incident response team leaders should ensure that all staff participating in a response understand the incident's situation-specific rules of engagement regarding the relative priorities assigned to containment and evidence collection.

## ERADICATION AND RECOVERY ACTIVITIES

Eradication and recovery activities also take place during this phase and are focused on removing any aftereffects of the incident and returning the organization to normal technology operations as quickly as possible. The extent of the activities performed during this phase vary depending upon the type of incident. In some cases, there might be very little work to do. However, in cases where systems were compromised, eradication efforts might involve completely wiping affected systems to ensure that there are no lingering effects from the compromise.

Recovery includes not only restoring normal activity but also ensuring that any vulnerability that might have been exploited by attackers is remediated. If attackers found your vulnerability once, it is extremely likely that they will be able to do so a second time. You should not consider your operations fully recovered until they are functioning again and the vulnerabilities exploited by attackers are resolved so that they do not continue to pose a risk of compromise.

## Post-incident activity

The final phase of the incident response process, post-incident activity, consists primarily of a lessons-learned analysis that does a postmortem look at the incident response process. It provides an opportunity for everyone who participated to reflect upon the response and any changes that might benefit future responses. In Special Publication 800-61, NIST suggests a series of questions that can be addressed during a lessons-learned session:

- Exactly what happened and at what times?
- How well did staff and management perform in dealing with the incident? Were the documented procedures followed? Were they adequate?
- What information was needed sooner?
- Were any steps or actions taken that might have inhibited the recovery?
- What would the staff and management do differently the next time a similar incident occurs?
- How could information sharing with other organizations have been improved?
- What corrective actions can prevent similar incidents in the future?
- What additional tools or resources are needed to detect, analyze, and mitigate future incidents?

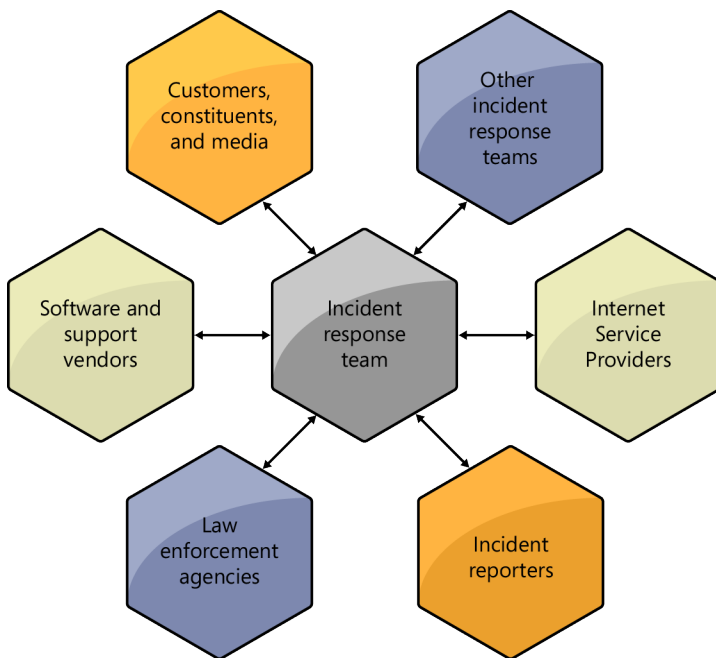
The session conducted to answer these questions should have a designated facilitator who moderates the conversation. This person should have enough incident response experience to ask the appropriate follow-up questions and guide the exploration, but should not have been involved in the actual response, to preserve a sense of objectivity. It can also be helpful to have a dedicated note-taker to ensure that everyone's input is accurately captured. At the conclusion of the meeting, the facilitator should prepare a lessons-learned report that highlights



the major findings of the session and key lessons learned that might benefit responders to future incidents. This document should be used to make revisions to the incident response process.

## Incident communications

During an incident response, the team might need to communicate with a wide range of external parties, as shown in Figure 1-5. These are individuals who either need to be informed of the incident or might provide information valuable to the response effort. All external communications should be coordinated through the communications lead on the incident response team to ensure that the team is presenting consistent information to the outside world.



**FIGURE 1-5** The incident response communications process suggested by NIST uses the incident response team as the core of all communications (NIST).

Some of the particular entities that the incident response team might communicate with include:

- **Customers, constituents, and the media** There are many stakeholders who will be interested in learning about the potential loss of sensitive information or who are otherwise affected by the incident. These communications *must* be coordinated through your public relations group.

- **Other incident response teams** If you are responding to an incident that affects multiple organizations, such as a widespread distributed denial of service (DDoS) attack, all responders will benefit from opening channels of communication between each organization's response team. This information sharing might help uncover important information more quickly and allows for a coordinated response.
- **Internet Service Providers (ISPs)** In a network-based incident, your ISP might be able to provide important information or implement strategies to help you contain the incident. For example, the ISP might be able to implement filtering that prevents traffic related to a DDoS attack from reaching your network in the first place.
- **Incident reporters** You might decide to report the incident to a state, national, or industry-specific incident response team. US federal government agencies are required to report security incidents to the United States Computer Emergency Readiness Team (US-CERT).
- **Law enforcement agencies** Depending upon the nature of the incident, you might be required to involve law enforcement or you might choose to voluntarily do so. For example, the Payment Card Industry Data Security Standard (PCI DSS) requires that merchants suspecting a security incident that involves credit card information must immediately alert both their merchant bank's fraud unit and the United States Secret Service.
- **Software and support vendors** You might need support from your vendors to diagnose and/or remediate the effects of a security incident.

Your incident response plan should include the procedures to be followed when involving each of the types of organizations listed here. It should describe who has the authority to initiate each contact during a security incident and should also contain contact information for each entity.

## Collecting evidence

Every incident response effort involves some form of evidence collection. In some cases, the evidence gathered is used solely by the incident response team. In other incidents, evidence might be turned over to the organization's legal team for use in civil litigation, or to law enforcement for use in a criminal prosecution. In cases where evidence is used outside of the incident response team, it is absolutely critical that it be collected by following established evidence handling procedures. Evidence that is mishandled might be inadmissible in court.

## Preserving the chain of custody



One of the most important aspects of evidence collection is preserving the evidence *chain of custody*. This means that you must create a paper trail that documents the history of the evidence from the time of collection until the moment it is used in court. This is done by using an evidence log that contains the following data elements:

- Identifying information that describes the nature of the evidence. This might include model numbers, serial numbers, IP/MAC addresses, user names, or other similar information.
- A description of the collection process used to gather the evidence, including contact information for the technician who collected it.
- Entries for every time the evidence was handled after collection. Each entry must include the name and contact information of the individual handling the information, the purpose for handling the evidence, and the location where it was stored after it was handled.

Quite simply, the chain of custody should tell a complete story of the life of the evidence. The evidence log should explain every single thing that happened to the evidence during and after collection, and it should document both the physical location of the evidence at all times and the names of any individuals who came into direct contact with it. The purpose of the chain of custody is to ensure that officials can provide definitive documentation of their evidence and ensure that it was not tampered with between the time of collection and the time of use.

## Interviewing witnesses

In many incidents, it might become necessary to interview witnesses to gather evidence. Interviews are conducted on a voluntary basis and should have a cooperative tone to them. Individuals conducting interviews should not be hostile toward witnesses or attempt to browbeat them into providing information. If either the interviewer or interviewee is uncomfortable with the proceedings, the interview should immediately be terminated. Don't let interviewers take lessons from police dramas!

Any interview that takes place should be thoroughly documented in a manner that is known to all participants. If the interview subject consents, you might use audio or video recording to document the interview. Otherwise, the interviewer might take paper notes to record the conversation.

Remember, an interview that turns hostile is no longer an interview, but an interrogation. At no time should anyone other than trained law enforcement personnel engage in the interrogation of a witness. In the best case, interrogation by untrained individuals might result in evidence that is not usable in court. In the worst case, the interrogator may find himself guilty of a crime.

## Tracking time and expense

Incident response teams should track the time and expenses associated with both evidence collection and other incident response efforts. Though these expenses might not be directly billable to any organization, they provide management with a method of identifying the resources that went into an incident response effort. At the very least, this information can be

used to plan for future incident responses. In some cases, management might be able to seek reimbursement through litigation or from an information security incident insurance policy purchased by the organization.

## Computer forensics

In many cases, investigators responding to an information security incident will need to collect information from computer systems believed to have played a role in the incident. This process, known as *computer forensics*, includes tools and techniques that ensure that evidence is collected in a manner that does not alter the evidence itself and preserves the chain of custody.

### **NOTE COMPUTER FORENSIC PROFESSIONALS**

Computer forensics is a complex subfield of information security. Conducting forensic examinations of computers requires specialized training and should not be attempted by individuals unfamiliar with proper evidence collection procedures. Most law enforcement agencies have officers dedicated to the proper collection of evidence who have undergone years of training in proper tools and techniques. The moral of this story? Don't try this at home! If you need to engage in the forensic investigation of a computer system, you should seek specialized assistance.

## Order of volatility

Unlike many kinds of physical evidence, computer-based evidence is often volatile. This means that it breaks down over time and, if not promptly and properly collected, it will disappear and be impossible to recover. Forensic investigators should consider the *order of volatility* when collecting evidence. Here's a summary of major computer evidence types, ordered from highest volatility (shortest life) to lowest volatility (longest life):

- RAM
- Network details
- Running process information
- System disk contents
- Removable flash media
- Removable magnetic media
- Removable optical media

Evidence from the first three elements on this list (memory contents, network details, and running process information) is only available as long as the system containing the evidence

has power. For this reason, most organizations have policies specifying that first responders should never unplug a computer believed to be involved in a security incident. Doing so could destroy critical evidence before it is forensically collected. Responders seeking to contain the damage caused by a security incident should instead disconnect the system from the network, leaving it powered on. Though this may destroy some network-based evidence, it leaves important memory and process information intact while containing damage.

As forensic analysts develop an evidence collection plan for a security incident, they should begin with the most volatile evidence from categories at the top of this list and work their way downward, collecting the least volatile evidence last. This approach maximizes the amount of data that can be collected before it expires.

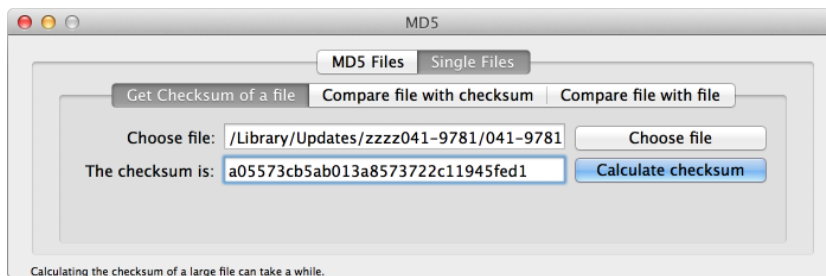
## Hashing



Investigators make use of cryptographic *hash* values to demonstrate that one file is a true copy of another file. Hashes are values generated by a mathematical function that provide a summary of the contents of one or more blocks of data. Hash functions must be designed in such a way that they are efficient to compute. Additionally, the hash value must be collision resistant, meaning that it should not be mathematically feasible to find two different files that generate the same hash value.

If a hash value is created by using a proper hash function, it can be used to quickly and reliably compare the contents of two files. If the files are identical, they will generate identical hash values. If the hash values generated by two files do not match, then the files themselves differ in some way. It is important to note that hashing does not give you a sense of “how close” the files might be. If a single character in the files is different, the hash values might be completely different. You simply can’t tell by comparing hash values whether a modification to a file was just a single letter or whether the files are completely different.

There are many software products capable of generating hash values for use in forensic examinations. Figure 1-6 shows one of these programs creating a hash value for a system file by using the well-known Message Digest 5 (MD5) hash algorithm.



**FIGURE 1-6** This screen shot demonstrates the creation of an MD5 hash.

### **MORE INFO HASH FUNCTIONS**

Hash functions are complex mathematical functions used to create a unique digest for a file. Chapter 12, “Cryptography,” provides details on specific hash functions, including MD5, RIPEMD, SHA, and HMAC. It also discusses how hashes can be used in the creation of digital signatures to provide reliable cryptographic nonrepudiation.

## **Imaging systems**

One of the most important forms of evidence captured during forensic investigations is system images. These images, gathered by using specialized forensic imaging equipment, are bit-by-bit copies of hard drives from systems involved in a security incident. System images are collected in a manner that ensures that the act of creating the image does not alter the data stored on the hard drive. Forensic investigators typically ensure that this is the case by using specialized forensic devices known as write-blockers. These are hardware connectors that sit between the drive being imaged and the hardware performing the imaging and ensure that no data can be written onto the drive, while permitting data to be read from the drive during the imaging process.

One of the major benefits of capturing a bit-by-bit image, rather than copying individual files from the disk, is that you receive a copy of the unused space on the disk. This space might contain portions of deleted files or other information that can prove very significant during the investigation.

Investigators performing forensic analysis *never* work with original media. After creating the image, investigators seal the original media in an evidence bag and securely store it in an evidence locker, being careful to preserve the chain of custody. This is because the original drive is direct evidence that might be used in court. Furthermore, investigators usually don’t even work with the original image. They maintain it as a master image and make copies of that image for investigative purposes.

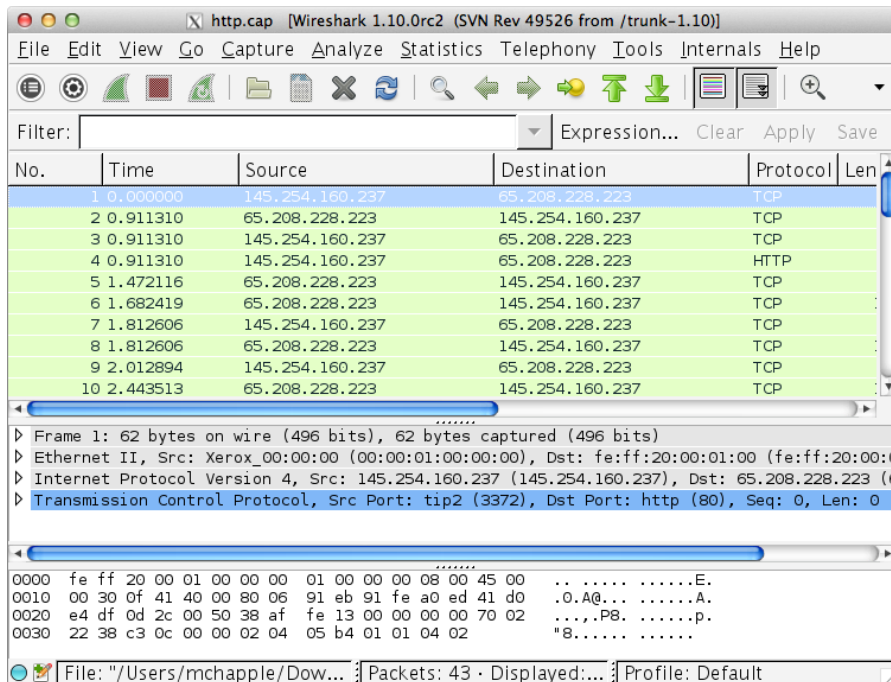
### **NOTE IMAGES AND HASHING**

With all these images and copies of images, how can a forensic team keep things straight and ensure that they are always working with a real copy of the original media? Through the use of cryptographic hashes! In the previous section, you learned how hashes can be used to verify the contents of a single file. Investigators also use hashes to verify the integrity of disk images. They record a hash of the original disk at the time it is collected and then they can perform a hash of an image at any time. If the hash value of the image matches that collected from the original disk, everyone can be certain that the image is a true copy of the disk that was collected as evidence. This hash verification technique is used in court to demonstrate the reliability of the imaging process and allow investigators to discuss information they gleaned from an image as if they had gleaned it from the original disk.

## Network traffic and logs

Network traffic is another important source of information for forensic investigators. In some cases, you might be able to capture the full contents of the data traveling on a network. This technique, known as packet sniffing, monitors a network segment, recording every bit that passes by on the wire, and then reassembles it to provide machine-readable and human-readable forms of the data transmitted on the network.

Analysts can use tools such as the free Wireshark tool shown in Figure 1-7 to capture the full contents of network traffic. It is important to note that capturing live network traffic can quickly consume massive amounts of storage. For this reason, it is extremely unusual to capture network traffic in real time unless there is a known incident taking place. It would simply be cost prohibitive to retain network traffic for any extended period of time.



**FIGURE 1-7** This screen shot demonstrates the use of Wireshark to capture network traffic.

Although analysts can't count on capturing network traffic 24 hours a day, seven days a week for use in a future investigation, there are sources of network data that might be retained for extended periods of time. First, many network devices create logs of activity that might contain information useful to a security investigation. For example, the logs on a router might show unsuccessful attempts to create administrative connections to the router that are indicative of an attack in progress. Firewalls might retain logs of permitted and blocked traffic that are useful to security investigators.

The second source of network information that is quite useful to forensic investigators is network flow data. These records, generated by network devices, track summary information about every connection that takes place on a network. They do not capture the full contents of the packet, to avoid the storage space dilemma discussed previously, but they do capture useful summary information, including:

- The source system IP address.
- The destination system IP address.
- The timestamp of the beginning of the connection.
- The timestamp of the end of the connection.
- The amount of data sent from the source system to the destination system.
- The source port for the communication.
- The destination port for the communication.
- The transport layer protocol used for the communication.

This information is enough to provide important details to those investigating a security incident. For example, if a system is known to have been compromised, flow data can be used to identify all of the remote systems that either connected to or were contacted by the compromised system. Flow data can also be used to disprove theories during a security investigation. For example, if a system contains a sensitive file that is 100 megabytes (MB) in size and flow data shows that no connections transmitted more than 25 MB, investigators can be confident that the entire file was not stolen.

## Time offsets

It is important to ensure that the system clocks on all computers and devices in an organization are synchronized. This facilitates the analysis phase of security investigations. If clocks are not synchronized, it becomes quite difficult to compare log entries generated by multiple systems. Many organizations handle this issue by using the Network Time Protocol (NTP) to ensure that all system clocks are synchronized to one of the atomic clocks maintained by the United States government, or another authoritative source. Access to these clocks is freely available, and the NTP protocol is able to adjust for the network latency between your site and the clock. For more information on the atomic clocks maintained by the US Department of Commerce and the US Naval Observatory, visit [www.time.gov](http://www.time.gov).

If an investigation must take place using information from systems without synchronized clocks, investigators must make use of time offsets. The investigators determine the difference between the clock on each system and the actual time, and then use this as an offset value to adjust the times retrieved from log entries and other timestamps generated by that system. For example, if a system clock is found to be running two minutes fast, analysts must then subtract two minutes from each time value generated by that system to adjust it back



to the correct time. This technique can also be used to compare data generated by systems located in different time zones.

## Screen shots

If an investigator encounters a computer that is currently involved in a security incident, that investigator can also use screen shots as a valuable source of evidence. Though it is possible to gather screen shots by using the built-in operating system functionality of the target computer, this is not an advisable technique for a forensic investigator, because the keyboard interaction might be viewed as tampering with the computer itself. One simple solution to this is to simply take a photo of the screen by using a digital camera dedicated to forensic investigations. Remember to timestamp your pictures and subject the clock on the camera to the same time offset procedure used for other systems. Finally, the memory card from the camera must then be treated in the same manner as any other form of digital evidence, with secure storage and a documented chain of custody.

## Video capture

Security investigators should also remember to turn to old-fashioned physical security tools when possible. For example, though it might not be possible to digitally determine who is logged onto a computer by using a stolen account, the room containing the computer might contain a surveillance camera that captures a picture of the perpetrator. If the room itself does not contain a camera, look for cameras in the hallway, at entrance points, or in other nearby areas that might have captured images of involved individuals.



### Quick check

1. What are the four phases of the incident response life cycle?
2. True or false: The incident response life cycle describes a sequential set of activities that should be followed when responding to an information security incident.

### Quick check answers

1. Preparation; detection and analysis; containment, eradication, and recovery; and post-incident activity
2. False. The incident response life cycle is an iterative, cyclical process that includes the potential to repeat steps. It is not a sequential, lockstep approach to incident response.

## Chapter summary

---

- The goals of information security professionals are to protect the confidentiality, integrity, and availability of an organization's information assets. Adversaries have the corresponding goals of disclosure, alteration, and denial.
- Vulnerabilities are weaknesses in an organization's security controls. Threats are external forces that seek to exploit vulnerabilities. Risks occur when there is an intersection between a vulnerability and a threat that can exploit that vulnerability.
- Qualitative risk assessment uses a subjective process to evaluate the likelihood and impact of a risk upon an organization. Qualitative assessments commonly use the categories of "low," "moderate," and "high" to express these attributes.
- Quantitative risk assessment calculates the financial risk that would occur if a risk materialized. It uses the concept of annualized rate of occurrence (ARO) to express likelihood and single loss expectancy (SLE) to express impact. Risks are calculated by using the annualized loss expectancy (ALE).
- Organizations have five strategy options at their disposal when determining how to manage a risk: risk acceptance, risk avoidance, risk mitigation, risk transference, and risk deterrence. They can use one or more of these strategies in response to each risk they face.
- Security professionals use controls to mitigate risk. These controls can reduce the likelihood and/or impact of a risk and are grouped into three categories: management controls, operational controls, and technical controls.
- Every organization should have a trained incident response team prepared to react in the event of an information security incident. This team should include technical, legal, communications, and management representatives that will join forces to coordinate a response.
- The incident response life cycle has four phases: preparation to get the team ready for future incidents, detection and analysis of an incident; containment, eradication, and recovery; and post-incident activity.

## Chapter review

---

Test your knowledge of the information in Chapter 1 by answering these questions. The answers to these questions, and the explanations of why each answer choice is correct or incorrect, are located in the "Answers" section at the end of this chapter.

- 1.** You are using encryption technology in an attempt to protect a file containing customer credit card numbers from unauthorized access. What information security goal are you pursuing?
  - A.** Confidentiality
  - B.** Integrity
  - C.** Disclosure
  - D.** Availability
  
- 2.** You are performing a risk assessment of an organization and decide that the likelihood of a particular risk materializing is "low." What type of risk assessment are you performing?
  - A.** Operational
  - B.** Quantitative
  - C.** Technical
  - D.** Qualitative
  
- 3.** You are conducting a quantitative risk assessment for an organization to identify the risk of a fire in a data center. The data center is valued at \$10 million and you expect a fire to occur once every 50 years that will damage three-quarters of the data center (including equipment). What is your exposure factor?
  - A.** 75 percent
  - B.** 10 percent
  - C.** 50 percent
  - D.** 25 percent

4. You are conducting a quantitative risk assessment for an organization to identify the risk of a fire in a data center. The data center is valued at \$10 million and you expect a fire to occur once every 50 years that will damage three-quarters of the data center (including equipment). What is your annualized loss expectancy?
  - A. 75 percent
  - B. \$7.5 million
  - C. 0.02
  - D. \$150,000
  
5. You are evaluating methods to manage the risk posed to your organization by hackers and decide that you will pursue a strategy of aggressively prosecuting anyone who attempts to break into your systems. What risk management strategy are you implementing?
  - A. Risk mitigation
  - B. Risk transference
  - C. Risk deterrence
  - D. Risk acceptance
  
6. You are conducting a lessons-learned session to identify gaps in your response to an information security incident. What phase in the incident response life cycle are you participating in?
  - A. Preparation
  - B. Detection and analysis
  - C. Containment, eradication, and recovery
  - D. Post-incident activity

# Answers

---

This section contains the answers to the questions for the “Chapter review” section in this chapter.

**1. Correct Answer: A**

- A. Correct:** Confidentiality controls protect information against unauthorized access. Preventing intruders from accessing the credit card file is an example of a confidentiality control.
- B. Incorrect:** Integrity controls protect information against unauthorized modification. This is not the goal stated in the scenario.
- C. Incorrect:** Disclosure is the goal of an attacker, rather than that of an information security professional.
- D. Incorrect:** Availability controls ensure that information is available to authorized users. This is not the goal stated in the scenario.

**2. Correct Answer: D**

- A. Incorrect:** The two types of risk assessment are quantitative and qualitative. Operational is not a type of risk assessment.
- B. Incorrect:** Quantitative risk assessments use objective numeric data rather than subjective categories such as “low.”
- C. Incorrect:** The two types of risk assessment are quantitative and qualitative. Technical is not a type of risk assessment.
- D. Correct:** Qualitative risk assessments use subjective categories, such as “low,” “moderate,” and “high,” to describe the likelihood and impact of risks.

**3. Correct Answer: A**

- A. Correct:** The exposure factor is the proportion of the asset that will be damaged in the event of a fire. In this case, that is 75 percent.
- B. Incorrect:** The exposure factor is the proportion of the asset that will be damaged in the event of a fire. 10 percent is not the correct value.
- C. Incorrect:** The exposure factor is the proportion of the asset that will be damaged in the event of a fire. 50 percent is not the correct value.
- D. Incorrect:** The exposure factor is the proportion of the asset that will be damaged in the event of a fire. 25 percent is not the correct value.

**4. Correct Answer: D**

- A. Incorrect:** 75 percent is the exposure factor.
- B. Incorrect:** \$7.5 million is the single loss expectancy.
- C. Incorrect:** 0.02 is the annualized rate of occurrence.
- D. Correct:** The annualized loss expectancy is calculated as the product of the single loss expectancy and the annualized rate of occurrence. The SLE is the asset value (\$10 million) multiplied by the exposure factor (75 percent), or \$7.5 million. The ARO is once every 50 years, or 0.02. The ALE is, therefore,  $\$7,500,000 \times 0.02$  or \$150,000.

**5. Correct Answer: C**

- A. Incorrect:** Risk mitigation reduces the likelihood that a risk will be successful or the impact that the risk will have on an organization. Prosecution reduces the likelihood that an attacker will attempt to exploit your vulnerabilities.
- B. Incorrect:** Risk transference moves the risk from one entity to another, such as through the purchase of an insurance policy.
- C. Correct:** Prosecuting attackers reduces the likelihood that others will try to attack you and is an example of risk deterrence.
- D. Incorrect:** Risk acceptance involves taking no other action to manage a risk. Prosecuting attackers is an active risk management approach and is a form of risk deterrence.

**6. Correct Answer: D**

- A. Incorrect:** The preparation phase includes activities designed to prepare the team for the next incident. Though this phase might include incorporating lessons from prior incidents, it does not include the actual lessons-learned session, which is part of the post-incident activity phase.
- B. Incorrect:** The detection and analysis phase includes activities designed to allow the team to notice that a security incident is underway and gather sufficient information to guide the response. It does not include a lessons-learned session.
- C. Incorrect:** The containment, eradication, and recovery phase involves protecting the organization against additional loss, removing the effects of a security incident, and restoring operations to normal order. This is usually followed by a lessons-learned session, which is part of the post-incident activity phase.
- D. Correct:** Conducting a lessons-learned session to identify potential improvements in the incident response process is an important part of the post-incident activity phase.

# Vulnerability assessment and management

The CompTIA Security+ exam covers common techniques used to identify risks and vulnerabilities. Organizations frequently assess their risks and vulnerabilities by using both formal and informal techniques, as well as technical tools.

In this chapter, we will explore how you can find exposed services and vulnerabilities on systems and devices by using port and vulnerability scanning tools. We will discuss vulnerability assessment methods, as well as ways to identify vulnerabilities by using both technical and nontechnical means. Finally, we will explore the art of penetration testing, including common techniques, types of penetration tests, and best practices for performing them.

## Exam objectives in this chapter:

Objective 3.7: Implement assessment tools and techniques to discover security threats and vulnerabilities

- Vulnerability scanning and interpret results
- Tools
  - Protocol analyzer
  - Sniffer
  - Vulnerability scanner
  - Honeypots
  - Honeynets
  - Port scanner
- Risk calculations
  - Threat vs. likelihood

- Assessment types
  - Risk
  - Threat
  - Vulnerability
- Assessment technique
  - Baseline reporting
  - Code review
  - Determine attack surface
  - Architecture
  - Design reviews

Objective 3.8: Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning

- Penetration testing
  - Verify a threat exist
  - Bypass security controls
  - Actively test security controls
  - Exploiting vulnerabilities
- Vulnerability scanning
  - Passively testing security controls
  - Identify vulnerability
  - Identify lack of security controls
  - Identify common misconfiguration
- Black box
- White box
- Gray box



# Vulnerabilities and vulnerability assessment

---

Vulnerabilities are weaknesses in systems, networks, applications, and other elements of an organization's security environment. Vulnerabilities can include a range of issues such as:

- Operating system issues that allow privilege escalation.
- Services that allow denial of service attacks.
- Poor coding that allows a web application to be susceptible to a SQL injection attack.
- Process issues that allow an intruder to enter a building without proper identification.

A typical server has the potential to have vulnerabilities in its operating system; in the third-party application software that it runs, including backup, remote administration, and other software; in its hardware components or the firmware that makes them work; or in the management and administration practices used by the support staff who work with it. Further vulnerabilities might exist in the network switches and routers the server uses to communicate to the outside world, as well as the power and cooling systems it relies on to function. With this broad range of potential vulnerabilities, it can be almost impossible to be sure that all known vulnerabilities are being appropriately handled via updates, workarounds, or other fixes at any point in time.

Attackers know that a software vulnerability is often the best way into a system, and they specifically target vulnerable applications and operating systems by using malware and other attack tools. Due to this, entire exploit testing packages such as the Metasploit Project have been created to provide an easy way for testers to use a variety of attacks against known vulnerabilities, providing both security staff members and attackers with a powerful tool. In other words, organizations focus on assessing vulnerabilities as part of their security program, and that is why vulnerability assessment is an important part of the CompTIA Security+ body of knowledge.

## **MORE INFO** WHAT IS METASPLOIT?

The Metasploit Project resulted in the Metasploit Framework and other related commercial tools. Metasploit includes exploits, payloads that are delivered via exploits, and a complete set of tools to manage attacks against systems. More detail on Metasploit can be found at [www.metasploit.com](http://www.metasploit.com). We will look at Metasploit's capabilities later in this chapter when we discuss penetration testing.

Organizations conduct vulnerability assessments by using many different methods and tools in an attempt to track and avoid the risks that they face. In this chapter, we will examine vulnerability assessment concepts and methodologies, including those used for system vulnerability and threat assessments. Using the risk assessment concepts explored earlier in this book, we will look at technical means to identify vulnerable systems and services. Finally, we will delve into penetration testing, the art of breaking into systems and networks to test their security.

## Risk-based vulnerability assessments



The first element of a vulnerability assessment program is a risk assessment. Of course, first you need to understand what a risk is. In this context, you can take the definition of *risk* from Chapter 1, “Risk management and incident response,” as “the intersection of a threat and a vulnerability,” and look at a risk as the potential that a threat will exploit vulnerabilities of a system, network, or other asset, resulting in harm. Here, threats are dangers that could result in an incident or breach.

### **MORE INFO** RISK ASSESSMENTS AND RISK MANAGEMENT

We discussed risk assessments and risk management as a discipline in Chapter 1.

A wide variety of threats have to be taken into account when you are performing risk assessments. In a full assessment, physical threats such as fires, floods, and tornados would be assessed at the same time as information security threats such as information exposure, system compromise, and outages. For the CompTIA Security+ exam, we will focus on threats that affect the confidentiality, availability, or integrity of systems, networks, and other assets.

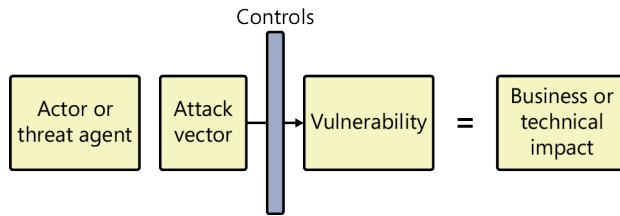
### **NOTE** DEFINING THREATS

The National Institute of Standards and Technology (NIST) defines a threat as “any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.” in the Federal Information Processing Standards (FIPS) 200 publication.

## Threat assessments



Threats are defined in several ways by various organizations, but in general, a *threat* can be defined as a possible danger that might exploit a vulnerability, resulting in harm to the organization. Threats are aimed at weaknesses, which are protected by controls, as shown in Figure 7-1.



**FIGURE 7-1** Threat agents attack vulnerabilities via attack vectors such as an exposed service, resulting in business or technical impact to the organization.

Threats require an actor, a vulnerability or weakness, and a motivation. This can be as simple as a tornado taking down power lines, or as complex as a group of criminals targeting vulnerable web applications in the banking industry to steal money from ATMs.

The threats an organization faces aren't always the result of attack, and most organizations assess threats that include physical threats such as fires, storms, and floods, as well as power outages, in addition to technical threats and human factors. Threat assessments build a list of the threats to an organization, allowing the organization to think coherently about what the threats it faces are.

Note that a threat may be included in a risk assessment, and in fact a threat assessment is often used as part of a risk assessment.

### **MORE INFO** OWASP'S GUIDE TO ASSESSING RISKS AND THREATS

OWASP, the Open Web Application Security Project, provides a useful example of assessing risk and threats to application security at [https://www.owasp.org/index.php/Top\\_10\\_2010-Main](https://www.owasp.org/index.php/Top_10_2010-Main).

## Vulnerability assessments



*Vulnerability* assessments specifically look at flaws and weaknesses in security systems, processes, controls, and designs. Thus, vulnerability assessments are targeted at the actual implementation of security, rather than considering who or what might attack, or what the

impact of the threat being realized is. Vulnerability assessments tend to follow risk and threat assessments, because they provide information about what the threats that an organization faces could result in. Performing a vulnerability assessment without performing some form of risk assessment is likely to lead to wasted effort, because low-risk areas can absorb significant amounts of time during their vulnerability assessment.

## Assessment techniques

There are a variety of ways to assess vulnerabilities, ranging from code reviews that consider the source code of applications to architecture and design reviews that validate the structure of systems and applications. The CompTIA Security+ exam covers a number of common vulnerability assessment techniques. Among them are:



- *Code reviews*, which use manual or automated review of source code for programs and applications to find vulnerabilities. Code review can expose flaws that cannot be found by a vulnerability scanner, including issues with internal logic. Many organizations perform code review before releasing application code into production, but code reviews are also performed as part of vulnerability assessments, penetration tests, and after attacks as part of a remediation process.
- Determining the *attack surface* of organizations and systems. The attack surface is the collection of services, applications, and other elements of a system or organization that are exposed to potential threats. Many organizations carefully design their network to minimize their attack surface, and vulnerability assessments will verify that the actual exposed elements match the design.
- *Architecture and design reviews*, which focus on the architecture of applications and services. These terms are often used interchangeably because the architecture of the application or service is typically part of its design. Design reviews consider how the service was designed to work internally, including how traffic flows, where data resides, and what servers, workstations, and other network and system elements work together to provide the service or to access it.
- *Baseline reporting*, a technique that relies on the baseline security standards discussed in Chapter 6, “Monitoring, detection, and defense.” Baseline reports check current settings against the baseline, then provide information about what differences, if any, exist. Baseline reporting is very useful for day-to-day monitoring of system configuration because it can easily point out issues with how security standards are applied. In some cases, changes from the baseline may mean that a system was compromised!

### **MORE INFO APPLICATION SECURITY AND BASELINING**

We will discuss application baselining in Chapter 8, “The importance of application security,” as part of our coverage of application security.



### EXAM TIP

The CompTIA Security+ exam includes all of these assessment techniques. Make sure you know the differences between them, and why you might choose to use each.

## Risk calculations: threat vs. likelihood

With these assessment methodologies in hand, you still need a way to decide which threats, risks, and vulnerabilities to pay attention to. Thus, in addition to the risk calculations explored in Chapter 1, you need one additional calculation, which is key to the CompTIA Security+ exam: the calculation of risk as the product of likelihood and impact. The equation is simple:



$$R = L \times I$$

Here, the likelihood is based on whether the threat appears and if it can exploit the vulnerability it is aimed at. The impact takes into account what harm the organization would experience if the threat succeeded, and should take into account the value of the assets involved.

### IMPORTANT PROBABILITY AND LIKELIHOOD

In many risk assessment methodologies likelihood is called probability, and it isn't uncommon to see this equation as  $R = P \times I$ , rather than  $R = L \times I$ .

In many risk calculations, these values are simply rated as high, medium, and low, although there are many variations in ratings and scales. Some organizations rate risks in more complex ways, with scales from 1 through 10 covering multiple impact factors to finances, business operations, and reputation, while others rate everything based on the detailed calculated value of each asset.

We can use the imaginary company, Humongous Insurance, to examine this process in more depth. For Humongous Insurance, a successful denial of service attack against their website is a significant threat because it could result in lost revenue for the company. If we assume that Humongous knows that they face a real threat from a group of attackers who want to disable their site, and assuming that they have some controls in place but think they might not work, Humongous might rate the likelihood of the threat appearing and succeeding as a medium.

If we assume that Humongous Insurance makes \$100,000 every 15 minutes through their website sales of insurance products, and that loss of that amount of money for hours or even a day is a significant loss to the company, we can easily calculate the impact of the risk they face. Here we will call the impact to the organization high, because they might lose customers and revenue, and suffer reputational damage.

The calculation would then be:

$$\text{Risk} = \text{Medium Likelihood} \times \text{High Impact}$$

Most organizations that use this calculation use a chart similar to the chart shown in Figure 7-2, where each level of impact has been given a number from 1 through 3, with low levels listed as 1, medium as 2, and high as 3, with the values multiplied by the likelihood to give a final score. Note that a risk with a high impact and a medium likelihood would be considered a high risk (6) and would receive prompt attention.

Impact	High	3	6	9
	Medium	2	4	6
	Low	1	2	3
		Low	Medium	High
		Likelihood		

**FIGURE 7-2** A Risk chart shows the intersection of likelihood with impact.

### Example: Humongous Insurance

We can also look at Humongous Insurance for a discussion of their assessment process. For this example, Humongous wants to assess the risks, threats, and vulnerabilities to their new web application environment, which allows customers to manage their insurance products online.

First, Humongous performs a risk assessment scoped to the new environment. They will consider what risks the organization would face if the new environment was compromised, if it was offline, or if it had another failure. Their assessment of the risks involved will likely require a threat assessment, which they will base on knowledge of what threats they have seen and what their competitors have dealt with. With that knowledge in hand, Humongous can more effectively choose where to spend their time assessing vulnerabilities.



#### Quick check

1. What type of assessment is intended to determine flaws that might be exploited by attackers?
2. What type of vulnerability assessment involves looking at the source code of the programs being assessed?

#### Quick check answers

1. A vulnerability assessment focuses on the flaws or weaknesses in systems, services, or applications that could be exploited by attackers.
2. Code review is an assessment technique that uses manual review or automated tools to find vulnerabilities in source code and its internal logic.

# Vulnerability scanning

---

Vulnerability scans serve several purposes for organizations. Not only do they help organizations identify vulnerabilities, they also help point out when security controls have not been properly put in place, or when an attacker or misconfiguration has disabled them. They also help organizations find common misconfigurations such as default usernames and passwords, default directories and scripts that can be dangerous, and a host of other, similar issues.

Organizations typically conduct vulnerability scanning one of two ways: by using internal tools to passively scan for vulnerabilities by checking version numbers and configurations, and by active scanning using a vulnerability scanning tool. We've already discussed security baselines, which can provide *passive identification*, so this chapter takes a look at active vulnerability scanning tools.

## Vulnerability scanning tools

A key part of assessing vulnerabilities is scanning for them. This is done by using a variety of tools, including packet sniffers, port scanners, vulnerability scanners, and specialized tools such as web application vulnerability scanners. Each of these tools has a role to play in a vulnerability assessment, and they are often used together or in sequence to help provide a faster, more accurate result.

We will examine each of these tools in the order in which they are frequently used to scan systems and networks. The process typically starts with a sniffer and a port scanner, which are used to look for hosts that provide services on the network. From there, vulnerability scanners are used to find vulnerable services and systems. Finally, if you discover web applications, you might want to use a web application vulnerability scanner's specialized abilities to test it.

## Protocol analyzers and sniffers

In Chapter 2, "Network security technologies," we looked at protocol analyzers and sniffers, tools that allow you to view and analyze network traffic on the wire. The capabilities that make these tools useful for detecting attacks and analyzing attack traffic also make them a useful part of vulnerability assessment.

**NOTE A SNIFFER BY ANOTHER NAME**

Remember that protocol analyzers, packet analyzers, packet sniffers, and sniffers are all names for the same tools used to read network traffic and display it.

There are a few ways in which sniffers are frequently used during vulnerability analyses and during penetration tests, which include:

- Capturing data during port scans and vulnerability scans to provide additional information about what data is being sent and received. This provides a log that penetration testers find useful to demonstrate what occurred and when. Capturing network activity can also provide more information about specific responses, allowing manual analysis if needed.
- Providing insight into the actual content of traffic sent by an attacker or attack tool, thus allowing security professionals to assess the significance of a threat. If the payload of the packets is an attack that your organization is vulnerable to, it is far more of a threat than a random attack that uses a tool you're not susceptible to.
- Analyzing the results of your own attack traffic when testing a system. This uses the same concepts as watching a third-party attack traffic but can be used inside of a network to monitor your own testing.
- Capturing traffic to determine whether network controls such as an IPS, firewall, or proxy work. A sniffer deployed at each point along the path between the sender and receiver can provide in-depth information about what traffic is permitted, and whether the network security devices are making changes to the traffic. This process is very similar to the process that many network and security professionals use when diagnosing network connectivity issues, but it changes the focus from making traffic flow to ensuring that controls work.

As you can see, sniffers are a critical part of your arsenal of tools when you are conducting vulnerability scans and penetration tests. The process for penetration testing, including the selection of tools from those discussed here, is covered in the "Penetration testing" section later in this chapter.

**IMPORTANT THE IMPORTANCE OF LOGGING**

Logging your scans by using a sniffer can be incredibly useful when your scanner is accused of causing problems such as a system crash or outage. Complete logs will allow you to provide details about which systems you were scanning at any given time and how they responded. Although it's rare, it is possible that your scan could take a system or network down!



## Port scanners



One of the first tools that a security professional uses from his toolbox when starting to assess a network is a *port scanner*. Port scanners provide a quick and easy way to assess the services that are exposed on a network and can help analysts quickly get an idea of whether an organization's systems are well maintained and secured or if there are problems throughout the network.

Port scanners attempt to connect to services hosted on systems and devices on a network, and then they monitor responses. In their simplest form, they check to see which ports respond, but they can provide a variety of capabilities beyond that if they analyze the responses from the systems they receive data from.

### **MORE INFO** NMAP SCANNING

Over the years, port scanners have added a range of capabilities intended to allow them to be more effective. A quick read through the Nmap guide to port scanning techniques can help you explore how many ways there are to scan a network. You can find the full list of techniques at <http://nmap.org/book/man-port-scanning-techniques.html>.

One of the major advantages of port scanners is that they can be quite fast. Unlike the vulnerability scanners we will discuss next, a port scanner is focused on a very limited set of information about systems, which helps it provide a quick list of ports and services, often with basic operating system identification thrown in. Most vulnerability scanners also limit themselves to a set of default ports, rather than scanning the full set of 65,535 ports that could be exposed to the world. Of course, scanning only part of the range of ports means that services that run on different ports might be missed!

### **Real world**

#### **Nmap**

The network mapper Nmap is an open-source security scanner that is one of the most popular port scanners in the world. Nmap provides the ability to discover hosts, identify which ports are accessible and what state they are in, perform service identification for the services running on those ports, and determine the likely operating system of the host (see Figure 7-3). Versions of Nmap have been created for most major operating systems, making it a common choice for most security professionals who need to conduct a port scan.

In the scan shown in Figure 7-3, Nmap also identified that the scan was run against a Linux system that appeared to be running a 2.6.x branch of Linux, and that the host itself appears to be a VMWare virtual machine. You now know much more about the system, but you don't know if these services are vulnerable.

```

Starting Nmap 5.59BETA1 ( http://nmap.org ) at 2013-05-08 23:03 EDT
Nmap scan report for 192.168.32.132
Host is up (0.00018s latency).
Not shown: 65504 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6200/tcp  open  unknown
6667/tcp  open  irc
6697/tcp  open  unknown
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  unknown
35013/tcp open  unknown
37742/tcp open  unknown
49753/tcp open  unknown
60310/tcp open  unknown
MAC Address: 00:0C:29:8D:24:33 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.9 - 2.6.31
Network Distance: 1 hop

```

**FIGURE 7-3** In this Nmap scan, a vulnerable Linux system provides a huge number of services, including FTP, SSH for remote access, SMTP email, DNS, a web server, and many other ports.

Of course, port scanning alone cannot provide a full understanding of the vulnerabilities that a system might have. When your scan completes, you will probably have useful information about potential targets, and you might even have some ideas about which systems might be vulnerable. With that data in hand, the next step for most security professionals is to scan the systems identified by a port scan with a vulnerability scanner.

## Vulnerability scanners



*Vulnerability scanners* are the next step up in the scanning process. There are two common types of vulnerability scanners: network vulnerability scanners and web application vulnerability scanners. We'll explore each in turn.

### Network vulnerability scanners

Network vulnerability scanners are designed to scan for vulnerable systems through a network. After they are provided with a target, which can be a single system, a network, or a whole range of addresses, they scan for and connect to services. This allows them to gather information about the version of the application or service running and to check it against a database of known vulnerable versions. More advanced vulnerability scanners also conduct tests to determine if specific vulnerabilities exist, either by testing for specific signs, or querying information on the system for details of what is installed. Some vulnerability scanning tools even allow you to embed administrative credentials that allow the scanner to log into systems they're scanning to verify software versions and other system settings directly.

In Figure 7-4, a scan was conducted against a sample vulnerable system by using Nessus, a popular vulnerability scanning package, resulting in a list of vulnerabilities. As you can see, the sample vulnerability selected from the scan is classified by its risk level based on the significance of the issue that would be created by exploitation of the vulnerability.

In this example, Nessus found 156 results, and the figure shows a high-security issue from that list that involves the SUDO command in Ubuntu Linux. Note that Nessus provides a description, a solution suggestion, links to details on the vulnerability itself, and information about when the vulnerability was discovered.

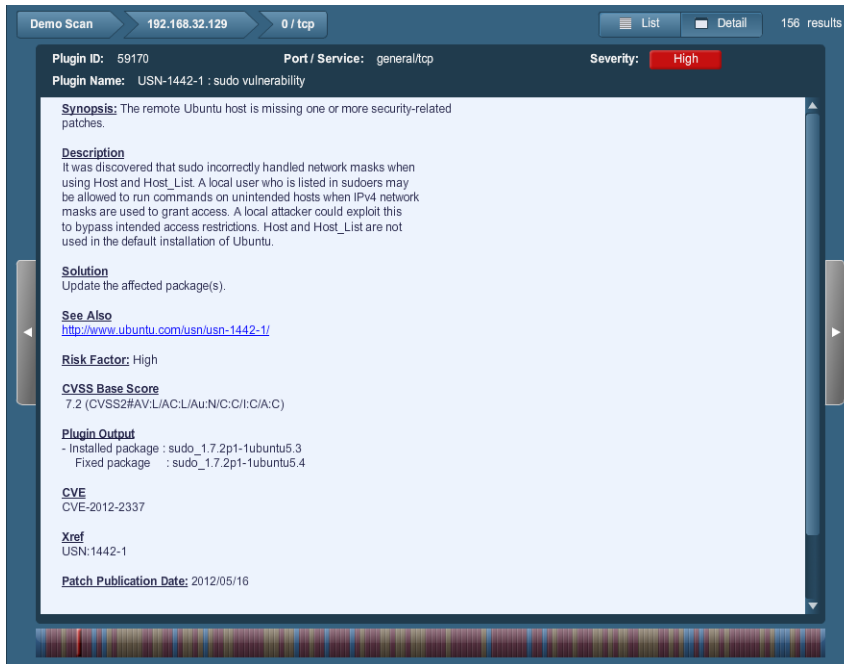


FIGURE 7-4 Nessus provides detailed vulnerability information for each vulnerability it discovers.

## Web application vulnerability scanners

Web applications are the face of most organizations, and those applications can have a wide range of vulnerabilities, such as to the cross-site scripting, SQL injection, and faulty logic issues we discussed in Chapter 5, “Threats and attacks.” Each application can respond differently to its users, and the way applications display data, accept input, and interact with back-end database servers can vary greatly. This means that web application assessment is a relatively specialized discipline. Until recently, most network vulnerability scanners did not have strong web application vulnerability assessment capabilities, leaving a niche for a variety of specialized *web application vulnerability scanners* (sometimes called *web application security scanners*). This is slowly changing, and major products are starting to add increasingly useful web application scanning tools to their existing vulnerability scanning products.

Web application vulnerability scanners act like an attacker might, and feed web applications bad input, change what forms send back to the application, and attempt to inject SQL statements, along with other specialized techniques. They also check for common misconfigurations, sample files and scripts, and vulnerable versions of the underlying software for websites such as their scripting engines and web servers.



## EXAM TIP

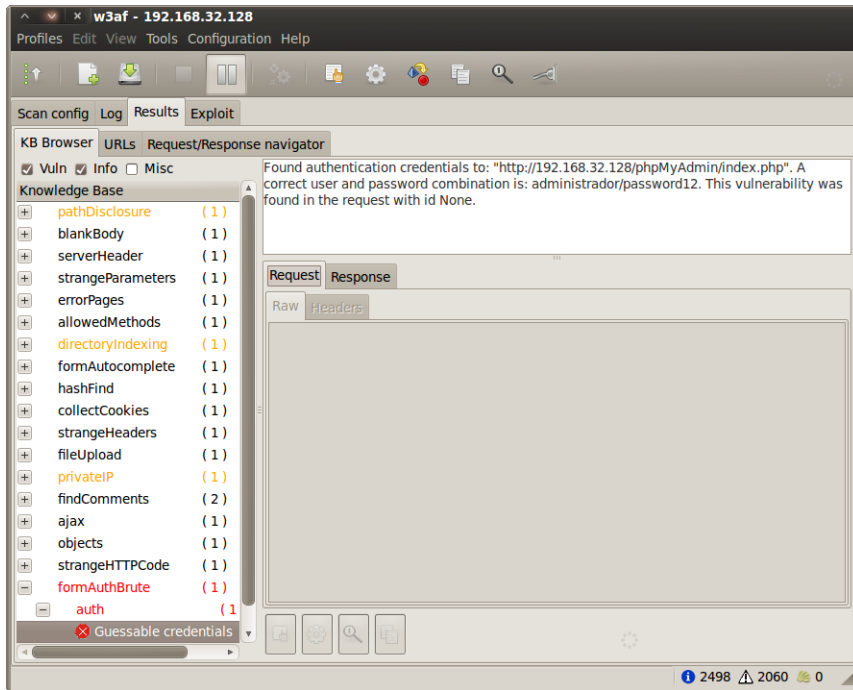
The CompTIA Security+ exam expects you to know the difference between vulnerability scanning and web application vulnerability scanning. Remember that web application vulnerability scanning focuses on application and logic vulnerabilities, and vulnerability scanners look at vulnerable versions and configurations of services.

In Figure 7-5, you can see a simple open-source web application and server vulnerability scanner called Nikto. Nikto's primary focus is on web servers and common vulnerabilities in known web applications, which means it is a useful tool to check for known vulnerabilities. Unlike more complex scanners, Nikto doesn't provide an in-depth scanning tool for custom applications.

```
- Nikto v2.1.4
-----
+ Target IP:      192.168.32.128
+ Target Hostname: 192.168.32.128
+ Target Port:    80
+ Start Time:     2013-05-12 14:44:30
-----
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.2.17). Apache 1.3.42 (final release) and 2.0.
+64 are also current.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8201xdh%28
+VS.80%29.aspx for details.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to XST
+ OSVDB-3233: /phpinfo.php: Contains PHP configuration information
+ OSVDB-3268: /doc/: Directory indexing found.
+ OSVDB-48: /doc/: The /doc/ directory is browsable. This may be /usr/doc.
+ OSVDB-12184: /index.php?PHPBB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive informatio
+ n via certain HTTP requests that contain specific QUERY strings.
+ OSVDB-3092: /phpMyAdmin/: phpMyAdmin is for managing MySQL databases, and should be protected or limited to au
+ thORIZED hosts.
+ OSVDB-3268: /test/: Directory indexing found.
+ OSVDB-3092: /test/: This might be interesting...
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ 6448 items checked: 1 error(s) and 13 item(s) reported on remote host
+ End Time:       2013-05-12 14:45:12 (42 seconds)
-----
+ 1 host(s) tested
```

**FIGURE 7-5** This Nikto scan identified the system as an Ubuntu Linux server running Apache 2.2.28 with PHP 5.2.4, which is outdated. In addition, Nikto identified multiple vulnerabilities listed in the Open Source Vulnerability Database (OSVDB) that could be issues or misconfigurations.

More complex scanners include internal logic that can analyze custom web applications and can identify vulnerabilities in how they handle input and user interaction. In Figure 7-6, the open-source Web Application Attack and Audit Framework (w3af) scanner has been run against a vulnerable application. Unlike Nikto, it explored the full application and attempted to feed it a variety of input.



**FIGURE 7-6** w3af provides far more information about vulnerabilities in the application than Nikto does.

In the example scan shown in the figure, you can see a list of issues with descriptions. Theselected vulnerability that is marked by red text provides more information, including the user name and password for a vulnerable phpMyAdmin installation on the target system.

#### **NOTE WHEN AUTOMATED TOOLS AREN'T ENOUGH**

Automated tools provide many features and don't get bored while scanning, but in many cases it takes a human to fully understand the internal logic of a web application. Thus, although web application scanning tools are a useful part of a vulnerability management program, you may still want to engage a talented web application assessment tester if it is absolutely critical that your web applications are secure.

No matter what type of vulnerability scanner you use, you should bear in mind that scanners are rarely 100 percent accurate. Vulnerability scanning is a useful tool as part of a strong vulnerability management program, and is a key part of a defense in depth strategy, but it isn't enough protection on its own.

### **MORE INFO** COMPARING WEB VULNERABILITY SCANNERS

Shay Chen's 2012 Web Application Vulnerability Scanner comparison tested a variety of the most popular vulnerability scanning tools available today and found that none of them identified all of the vulnerabilities he was testing for. You can find his full report at <http://sectooladdict.blogspot.com/2012/07/2012-web-application-scanner-benchmark.html>.


#### **Quick check**

1. What type of tool would you use to monitor the traffic sent by a vulnerability scanner?
2. How do web application vulnerability scanners differ from network vulnerability scanners?

#### **Quick check answers**

1. A sniffer or packet analyzer is typically used to monitor the packets sent by a vulnerability scanner or port scanner. This allows you to see what is sent and received by the scanning system, providing useful information about what systems were scanned and how they responded.
2. Web application vulnerability scanners focus on internal logic, vulnerabilities in how applications handle user input that allow attacks such as cross-site scripting, SQL injection, and similar problems. Vulnerability scanners typically look for vulnerable services and configuration issues and typically don't understand how the applications themselves work or handle user input.

## Honeypots and honeynets

 The CompTIA Security+ exam looks at two types of systems designed to lure attackers into targeting them: *honeypots* and *honeynets*. Honeypots are specially designed systems and applications that expose tempting interfaces and vulnerabilities to potential attackers. Often they will provide a complete copy of a legitimate vulnerable system, but will be designed in a way that prevents attackers from gathering actual data or performing further attacks. Instead, they gather information about what the attackers do and how they do it. Most honeypots log every action taken on the system, and many also keep copies of files and tools that attackers bring with them.

Honeypots are often classified into one of two types:

- Low-interaction honeypots, which provide a few commonly targeted services and are focused on studying the most heavily attacked applications and systems
- High-interaction honeypots, which emulate an entire operating system or application, allowing attackers to perform the actions they normally would on a compromised system

Honeynets work much like honeypots do, but on a much broader scale: they are entire networks of systems designed to lure attackers in. This means that some honeynets can detect attacks in a variety of locations or attacks aimed at a variety of systems on a network.

Network honeypots are often called *sinkholes*. Much like honeypots, sinkholes are designed to absorb attacks safely while providing researchers and security professionals with a chance to study malicious traffic.

#### **MORE INFO THE HONEYNET PROJECT**

Information security researchers around the world contribute to the Honeynet Project, a collaborative network of honeypots run through a nonprofit coordinating body. More information about the Honeynet Project can be found at [www.honeynet.org](http://www.honeynet.org).

Organizations might deploy honeypots or honeynets for research, allowing them to understand new threats, or for production use, to help detect attacks and new threats on their own internal networks. In addition to the honeynets and honeypots the CompTIA Security+ exam focuses on, two other common security tools exist, with related uses: darknets and tarpits.

## **Darknets**

*Darknets* are segments of unused network space that host no servers and provide no services. Thus, no traffic should be sent to them, because they don't advertise anything that should result in connections. This means that any network traffic sent to the darknet IP addresses is suspect and is likely to be of interest to security professionals.

Darknets typically host one or more systems that collect all network traffic sent to the network. When the traffic is captured, it can be analyzed to detect port scans such as those discussed earlier in this chapter. Darknets have been used to detect worm outbreaks, misconfigured systems, and a host of other abnormal network traffic.

#### **MORE INFO REAL-WORLD DARKNETS**

Team Cymru, a nonprofit security research organization, runs an extensive darknet to capture probes, malware, and other attacks that randomly attack IP addresses on the Internet. More details on the Darknet project can be found at [www.team-cymru.org/Services/darknets.html](http://www.team-cymru.org/Services/darknets.html), where you can access full instructions on how to set up your own darknet server.



## Tarpits

In addition to detecting scans, some organizations prefer to slow down scanners. Tarpits are the answer. A *tarpit* is a system specifically configured to delay network connections such as those made by a worm that is scanning for new systems to compromise, or a network vulnerability or port scanner that is searching for services.

Tarpit implementations can be as simple as an increased delay for connections to an email server, and as complex as a dedicated server that responds to every connection to a subnet with a variety of connection messages, resulting in scanners taking hours to scan, only to return a list of fake services and systems.

### **IMPORTANT** WHY TARPITS AND DARKNETS?

Though the CompTIA Security+ exam doesn't cover darknets, tarpits, or sinkholes, the concepts behind them are useful for security professionals to keep in mind when learning about how attackers can be monitored, stopped, and studied.



### **EXAM TIP**

The CompTIA Security+ exam covers honeypots and honeynets. Simply remember that a honeypot is a single system, and that a honeynet is more than one system, typically deployed in various network locations.



### **Quick check**

1. What type of network security tool is designed to allow attackers to break in and interact with the operating system so that security professionals can learn about their behavior?
2. Why might you deploy a honeynet?

### **Quick check answers**

1. A high-interaction honeypot is designed to provide a simulated, safe target for attackers that reacts like a real system would.
2. Honeynets are useful for detecting attacks that are distributed across a network or that occur in more than one location. Honeynets can help security professionals determine the scope and size of a scan or attack by capturing traffic in a variety of locations.

# Penetration testing

---



*Penetration testing* is the process of attacking an organization to test its technical security, practices, procedures, and other defenses. Penetration tests are conducted by, or for, organizations that want a real-world test of their security. Unlike actual attacks, penetration tests are conducted with the knowledge of the organization, although some types of penetration tests occur without the knowledge of the employees and departments being tested.

Penetration tests are typically used to verify threats or to test security controls. They do this by bypassing security controls and exploiting vulnerabilities, using a variety of tools and techniques, including the attack methods discussed earlier in this book. Social engineering, malware, and vulnerability exploit tools are all fair game when it comes to penetration testing.

## **IMPORTANT PENETRATION TESTING AND THE COMPTIA SECURITY+ EXAM**

The CompTIA Security+ exam focuses on the use of penetration testing for these purposes. Penetration tests actively test security controls by exploiting vulnerabilities and bypassing security controls, and this helps to verify that a threat exists.

Penetration tests are often classified as overt or covert and as internal-perspective or external-perspective tests. Overt penetration tests are intended to be visible to members of the organization being tested, and use techniques that are likely to be detected by security tools, system administrators, and security professionals. Covert tests better simulate more stealthy attacks and attempt to evade detection. Tests with an internal perspective or view are conducted from inside an organization's security perimeter, whereas external-perspective tests are conducted from outside that perimeter. Note that the designation of a test as an internal-perspective test does not imply that the testers were allowed past that perimeter. One common technique for penetration testers is to bypass external security perimeters physically by placing devices inside an organization.

## Real world

### My Little Pwnie Plug

Pwnie Express (pronounced “Pony Express”) is a company that specializes in penetration testing hardware. Among their products are penetration testing aids known as the Pwn Plug and the Power Pwn (see Figure 7-7), which are designed to help bypass security perimeters.



**FIGURE 7-7** The Pwn Plug looks like a common power adapter.

The Pwn Plug resembles a common “wall wart” power adapter but conceals a small Linux computer complete with flash memory, network adapters, and penetration testing software packages preloaded. The Pwn Plug shown in Figure 7-7 is an innocuous device that penetration testers can plug into any power outlet in buildings to which they can gain access. Once there, it can connect to wireless and wired networks, perform vulnerability testing with a variety of built-in open-source tools, and provide an encrypted tunnel in for penetration testers. The device even includes a set of stickers intended to make it look more like a common power adapter. Most of the staff in your organization would probably not think twice about a Pwn Plug.

Devices such as the Pwn Plug aren’t the only way in for penetration testers. Other recent techniques include seeding parking lots with USB flash drives that contain malware that phones home to the testing team after they’re plugged into a workstation, using social engineering techniques to persuade staff members into allowing the penetration testers themselves to access their PCs, and a host of other techniques.

## Types of penetration tests

The CompTIA Security+ exam divides penetration tests into three major types of testing, classified by how much information the testers have. The categories are black box, white box, and gray box testing. We'll take a look at each of them, and then we'll explore how they are performed.

### Black box penetration testing



*Black box penetration tests*, sometimes called *blind penetration tests*, are conducted with no knowledge of the environment. They are much more difficult to conduct than white box or gray box vulnerability tests, because they require the penetration testers to gather any information they need about an organization by themselves.

This makes black box penetration tests a far better test of what an actual attacker might manage to do. Because black box testing is as close to a real-world attack as possible, some organizations opt to use black box penetration tests to test their own defenses against attackers. As you might imagine, a black box penetration test is typically far more expensive in terms of both time and effort than tests that provide attackers with more knowledge. Worse, black box testing can leave entire sections of an IT infrastructure alone if the attacker misses them when scanning for targets.

### White box penetration testing



*White box penetration tests* provide the most information to the penetration testing team. Because white box testing provides a complete and unobstructed view of the environment to the attacker, it is sometimes called *crystal box penetration testing*.

White box penetration testing provides several advantages:

- More focus is placed on the test itself, rather than on gathering information.
- More in-depth testing can be accomplished, because everything that can be tested is exposed.
- Attacks against known systems and services are more likely to be the right attack and to demonstrate true issues with the systems and services.

White box testing can be very helpful in identifying vulnerabilities that might be missed by a black or gray box test, but they can add additional cost because of the broader scope that total visibility can create.



---

#### **EXAM TIP**

If you can't recall what information is available during a penetration test, remember that the color of the box tells you all you need to know. You can't see through a black box, but the white (crystal) box shows you everything.

---



## Gray box penetration testing

*Gray box penetration testing* is a middle ground between black box testing and white box testing. Gray box testers typically receive partial information about the subjects of their testing but don't have access to every detail of the target. Gray box testing can help avoid some of the problems with black box testing by ensuring that important parts of the target aren't missed. It can also prevent the common white box testing issue of not replicating an actual attack scenario.

### **NOTE GRAY BOXES: PARTIAL KNOWLEDGE TESTING**

Gray box testing is sometimes called "translucent box" testing, a halfway point between white box testing's "crystal box" and black box testing's "blind" testing.

### **Quick check**

1. A penetration that that is performed with full knowledge of the systems, network, and defenses of a target is known as what type of penetration test?
2. What are the advantages and disadvantages of a black box penetration test?

### **Quick check answers**

1. A white box, or crystal box penetration test provides full knowledge of the environment being tested to the attackers. This allows them to more fully test the environment, but it does not simulate a real-world attacker's view of the systems.
2. Black box penetration tests provide a real-world test by providing no internal knowledge of the organization or systems that are being tested. This can result in systems being missed due to lack of knowledge.

## Conducting a penetration test

After you have decided on the type of penetration test that will be conducted, a complex process still awaits. Thorough penetration testing can be very involved, and using a standard process can help keep the test from causing issues or breaking down midway through.

A typical penetration test will use most of the following steps:

1. Documentation of the request for the penetration test, including the authority under which it will be performed, its scope, and who the audience for the results will be
2. Planning and design
3. Identification of the targets of the test

4. Selection of methods and tools
5. Vulnerability testing and validation against the target and/or security assessment of the target
6. Reporting
7. Remediation of issues discovered during the penetration test

#### **IMPORTANT PENETRATION TESTING AND PERMISSION**

Penetration testing should only be done with appropriate authorization. Many penetration testers and security professionals refer to this as a “Get out of jail free card,” because having the right permission ensures that security testing won’t get the tester fired!

Next we will explore each of these steps, including what each requires, what it involves, and what you need to know to execute each step.

### **Authority, scope, and audience**

Three key elements to understand before you begin a penetration test are the authority under which you are conducting it, the scope of the penetration test, and who you are preparing the results for.

Penetration tests should be authorized by an appropriate member of the organization engaging the penetration tester. Often this means the CEO or CIO of an organization, or an equivalent member of management. Equally important is to have written authorization for the test.

The person or group that authorizes the test is typically the sponsor within the organization. The sponsor of a penetration test plays a key role, which usually includes coordination within the organization. In addition, the sponsor can help handle issues that arise during the penetration test, particularly if it is a black box test that staff members in the organization are not aware of.

The sponsor or sponsors of the penetration test will also help to set the scope of the test. Properly scoped tests will include appropriate systems and networks. If scope isn’t well defined, or if the scope includes the wrong systems, penetration tests can cause outages or other issues. Obviously, penetration tests bear some risk even at the best of times, but proper scoping can keep those risks within the risk appetite of the organization. Scoping also helps penetration testers estimate how much effort and time they will need to complete the test, which can ensure that appropriate resources are used.

During the scoping process, testers will also typically set the rules of engagement for the penetration test. These should clearly state what the testers are allowed to do, as well as what they are prohibited from doing. If testers are not allowed to use social engineering, or cannot seed the parking lot of the facility with flash drives filled with malware, they need to know this as part of the rules. This means that the penetration testers need to carefully explain what

they will be doing to the sponsors, because sponsors are unlikely to realize the full impact of what they may authorize if they are not told.

Finally, penetration testers need to know who their report will be provided to. Often, penetration tests include both a high-level executive summary suitable for senior management as well as a more technical, in-depth report. The executive summary must provide key information about the testing and what issues were found without venturing too far into esoteric technical data. The in-depth report typically includes far deeper detail on what actions were taken, what resulted from the actions, and how vulnerabilities were verified.

If these three initial elements aren't well understood, a penetration test can fail before it starts!

## Penetration test planning and design

In order to perform a thorough penetration test, you need a plan. Fortunately, several organizations provide documentation on penetration testing methodologies, including NIST's SP 800-115 Technical Guide to Information Security Testing, the OWASP (Open Web Application Security Project) guide to web application penetration testing, and the Institute for Security and Open Methodologies' (ISECOM's) Open Source Security Testing Methodology Manual, or OSSTMM.

### **MORE INFO** PENETRATION TESTING METHODOLOGIES

You can find these methodologies the following sites:

- NIST ([csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf](https://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf))
- OWASP ([www.owasp.org/index.php/Web\\_Application\\_Penetration\\_Testing](http://www.owasp.org/index.php/Web_Application_Penetration_Testing))
- ISECOM ([www.isecom.org/research/osstmm.html](http://www.isecom.org/research/osstmm.html))

Other methodologies exist, allowing you to choose the methodology or elements that best fit your organization's needs.

Whether you select a third-party methodology, use one to develop your own, or simply create one in house, a thorough penetration testing plan can help avoid problems. Plans help you identify tools and infrastructure, needed information and skills, and when and how the test will be conducted. A well-designed plan can reduce the potential negative impact that attacking an organization's infrastructure can have, while still allowing you to gather useful information.

## Target identification

The way targets are identified for a penetration test depends on the type of test being conducted. A white box test will usually be accompanied by a list of targets, including systems, applications, and security procedures that need to be tested. Black and gray box tests provide far less information, leaving identification of targets to the penetration testing team.

Target identification without full knowledge starts with gathering information about the organization. Public information includes public websites, information from web forums, and postings that employees have made about the company. With that information in hand, the penetration tester can gather more detail, including IP address ranges, domains, and other information that can help narrow the list of potential targets.

After the penetration testers have identified a list of potential targets, they will typically conduct information-gathering exercises such as DNS queries, port scans, and sometimes vulnerability scans. Each of these can provide more detail about the systems their target exposes to the world.

#### **MORE INFO EXPLOIT AND VULNERABILITY DATABASES**

Knowledge is also a key component of testing for vulnerabilities. Most vulnerability assessment tools provide links to known vulnerabilities, but knowing where to find more information is important. Fortunately, large-scale exploit databases exist that can provide information about vulnerabilities, often including working exploit code and details about which versions of software packages have the vulnerability.

Some of the most popular vulnerability resource and reference sites are:

- The Common Vulnerabilities and Exposures (CVE) dictionary run by MITRE ([cve.mitre.org/index.html](http://cve.mitre.org/index.html))
- The Exploit Database ([www.exploit-db.com/](http://www.exploit-db.com/))
- The Open Sourced Vulnerability Database ([www.osvdb.org/](http://www.osvdb.org/))
- The National Vulnerability Database ([nvd.nist.gov/](http://nvd.nist.gov/))

Simply entering an application's name into these reference sites can be a very informative exercise.

When they are done, penetration testers will have a list of targets with information about each. From there, they can build a list of penetration testing goals and tasks that will drive the rest of their assessment. In order to complete the assessment, they need to determine what methods and tools they will use to meet their penetration testing goals.

## **Methods and tools**

Penetration testing methods include many of the same attacks discussed in earlier chapters but are intended to determine if a vulnerability exists, rather than to disable the organization. Thus, attacks tend to focus on vulnerability verification, with exploits used to prove that the vulnerability exists or to gain further access to allow deeper testing. Most penetration tests avoid conducting denial of service attacks, although it is possible that an organization may include them in the scope.

Methods for testing are often selected in the planning phase of the penetration test to meet the scope of the assessment. After targets have been identified, those methods can be



refined based on information gathered about the targets. If the targets are web servers, then web application testing tools and techniques would be chosen, whereas a Windows domain would require the selection of tools that focus on Active Directory and common Windows vulnerabilities.

A broad variety of tools exist for penetration testers to choose from, ranging from commercial tools to open-source packages, and those that have both commercial and open-source versions, such as the Metasploit Framework. A key part of penetration testing is selecting appropriate tools for the targets of the test.

#### **MORE INFO LINUX PENETRATION TESTING DISTRIBUTIONS**

In addition to commercial tools, a variety of prepackaged open-source penetration testing tools are available. Some of the most popular include:

- BackTrack Linux ([www.backtrack-linux.org/](http://www.backtrack-linux.org/))
- Kali Linux, a recent replacement for BackTrack Linux: ([www.kali.org](http://www.kali.org))
- InGuardians Samurai Web Testing Framework ([samurai.inguardians.com/](http://samurai.inguardians.com/))
- Knoppix Security Tools Distribution (STD) ([s-t-d.org/](http://s-t-d.org/))
- BugTraq ([bugtraq-team.com/](http://bugtraq-team.com/))
- BackBox Linux ([www.backbox.org/](http://www.backbox.org/))

Penetration testing toolkits are constantly being created, and each has its strong points, so it is worth reviewing what toolkits are being actively updated at the time you need to conduct your test. If you prefer to test your skills, distributions such as Metasploitable, a product found at <http://sourceforge.net/projects/metasploitable/files/Metasploitable2/>, provide a playground for penetration testers to attack in a safe lab environment.

## **Vulnerability testing, validation, and assessment**

The full details of how to conduct a penetration test could fill a book on their own. For our purposes, it is important to know that a penetration test should be conducted in accordance with the rules of engagement that the sponsor helped set when the assessment was scoped, and that the tester or testers must be careful to not go beyond that scope without approval.

During a penetration test, the testers will use a variety of scan, attack, and analysis tools. All of the data that is collected should be carefully logged, including notes on when each attack is conducted, what target or targets it is aimed at, and what data was gathered from the attack.

Careful logging and analysis is important, and if a team is conducting the penetration test, a method to keep the team coordinated is very important. Penetration tests can be expensive and dangerous to an organization's business and infrastructure if they are not carefully conducted, so care and diligence are critical.

## Reporting

After a penetration test has been completed, a report needs to be prepared for the sponsor or sponsors. In many cases, additional technical reports will also be required for the areas in which issues were identified, because the report to the sponsor of the penetration test is typically a high-level report.

### **IMPORTANT TARGETING YOUR REPORTS**

High-level reports should prioritize issues. Penetration tests can provide massive amounts of information, and understanding what your sponsor is looking for and how to best provide that data to the sponsor is key!

Reports should include the scope, the targets, the tools and methods selected and used, and information about what vulnerabilities were found and successfully validated. Reports should also include details on any vulnerabilities that were identified but that testers were unable to exploit, particularly if they were not exploited due to constraints set by the scope or rules of engagement of the test.

Reports typically include technical information as an appendix or as an additional document. This allows the sponsors to provide detail to system administrators or security staff, which will allow them to put in place appropriate controls or fixes for the issues observed during the test.

## Remediation

The final stage of a penetration test is remediation. After the sponsor and those who have a stake in the test have read the report, the issues that were reported must be prioritized and acted on. In most cases, penetration tests find a variety of issues, and not all of them will be remediated due to costs, time constraints, or other reasons.

When remediation is finished, long-term monitoring and maintenance is necessary. The network monitoring techniques we discussed in Chapter 6 are important to implement to ensure that ongoing monitoring occurs. Many organizations choose to perform penetration tests on a recurring basis, and some standards and laws require them.

### **MORE INFO PCI –DSS AND PENETRATION TESTING**

Requirement 11.3 of the Payment Card Industry Data Security Standard (PCI-DSS) credit card standard requires penetration tests at least annually, as well as any time a significant change is made to the credit card processing environment. In fact, the PCI Security Standards Council provides guidance that notes that all upgrades and modifications of the environment should be penetration tested! Their guidance document also suggests that the method and results should be documented to ensure that information about the testing is available. Details of this requirement can be found at [www.pcisecuritystandards.org/pdfs/infosupp\\_11\\_3\\_penetration\\_testing.pdf](http://www.pcisecuritystandards.org/pdfs/infosupp_11_3_penetration_testing.pdf).



### Quick check

1. Who authorizes a penetration test?
2. What information should a penetration test report contain?

### Quick check answers

1. A senior administrator such as a CEO or CIO should authorize a penetration test. Penetration tests should only be conducted with full authorization from a person who has the authority to permit them, and documentation of the authorization and scope should be retained as part of the test.
2. Penetration test reports should include the scope, methods used, and information about the issues discovered. Typically, reports should include both an executive overview and detailed information for technical staff who need to remediate vulnerabilities found during the test.

## Chapter summary

---

- Risk is used to determine organizational priorities. You can use the equation  $Risk = Likelihood \times Impact$ , to rate risks based on how often they occur and how much harm they would result in.
- Threats leverage vulnerabilities via attack vectors, resulting in business or technical impact. The relationship and differences between risks, threats, and vulnerabilities is important to remember: a risk is the potential that a threat will exploit vulnerabilities of a system, network, or other asset, resulting in harm. A threat is an actor that might exploit a vulnerability.
- A broad range of tools can be used for vulnerability assessment, including protocol analyzers, sniffers, port scanners, and vulnerability scanners. Protocol analyzers and sniffers are used to monitor traffic sent by other tools, and to look at responses. Port scanners and vulnerability scanners are used to actively scan systems and devices.
- The reasons for conducting vulnerability scans including identifying vulnerabilities, verifying security controls, checking for missing controls, and finding misconfigurations.
- Port scans identify accessible services, operating system versions, and other basic information about a system. Vulnerability scans check for service versions and other information about a system and compare that data to a list of known vulnerabilities. Penetration tests often take advantage of both by first scanning for open ports and then targeting specific services.
- Honeypots and honeynets are security tools that invite attackers to break in, and allow security professionals to learn their techniques and tools by capturing them.

- Organizations use assessment techniques such as baseline reporting, which checks current settings against those defined in a security baseline or template; and code review, which explores the source code of an application to ensure that it doesn't contain bugs, mistakes, or other flaws to monitor for new vulnerabilities and risks to their systems and software.
- Design and architecture review, which takes advantage of knowledge of how services, networks, and systems are put together to determine whether they are vulnerable. This also helps to assess the attack surface, which is the part of the design that is accessible to attackers.
- Penetration tests are a hands-on way to test actual vulnerabilities. Penetration tests typically follow a process that starts with authority to conduct a test, then moves through setting a scope, selecting tools, and then performing a penetration test. They typically conclude with a report, followed by application of controls or fixes to identified issues.
- Penetration test view, include black box penetration testing, which provides no data to the tester; gray box testing, which restricts available information; and white box testing, which provides full detail and visibility of the environment to those who are testing it.

## Chapter review

---

Test your knowledge of the information in Chapter 7 by answering these questions. The answers to these questions, and the explanations of why each answer choice is correct or incorrect, are located in the "Answers" section at the end of this chapter.

1. A security tool that is designed to allow attackers to attack a simulated system and that gathers information about the attackers' tools and techniques is known as what?
  - A. A vulnerability detection system
  - B. A port scanner
  - C. A darknet
  - D. A honeypot
2. What type of vulnerability review focuses on how systems are put together?
  - A. A penetration test
  - B. A vulnerability scan
  - C. A design or architecture review
  - D. A code review

3. The potential that a threat will exploit vulnerabilities is known as what?
- A. A risk
  - B. A vulnerability
  - C. A threat
  - D. An exploit
4. The equation to calculate risk is:
- A.  $Risk = Likelihood \times Vulnerability$
  - B.  $Risk = Impact \times Vulnerability$
  - C.  $Risk = Vulnerabilities \times Threats$
  - D.  $Risk = Likelihood \times Impact$
5. What type of penetration test provides partial visibility into the details of the environment to the testers?
- A. Red box
  - B. White box
  - C. Gray box
  - D. Black box
6. What type of testing would you perform to identify services and accessible ports via a network?
- A. A port scan
  - B. A penetration test
  - C. A vulnerability scan
  - D. A ping sweep

# Answers

---

This section contains the answers to the questions for the “Chapter review” section in this chapter.

**1. Correct Answer: D**

- A. Incorrect:** Vulnerability detection system is a made-up term.
- B. Incorrect:** Port scanners are tools used to scan for open services.
- C. Incorrect:** A darknet is an unused network set up and instrumented to detect attacks—any traffic sent to a darknet is suspect, because no valid systems should exist there.
- D. Correct:** A honeypot is designed to allow attackers to compromise a fake system, providing the opportunity to study their actions.

**2. Correct Answer: C**

- A. Incorrect:** A penetration test tests a broad variety of security controls by attacking systems and networks to attempt to gain access.
- B. Incorrect:** A vulnerability scan scans for vulnerabilities by using a scanning tool.
- C. Correct:** A design or architecture review investigates the design of a system, network, or application.
- D. Incorrect:** A code review targets the source code of an application or service to check it for vulnerabilities and bugs.

**3. Correct Answer: A**

- A. Correct:** A risk is the potential that a threat will exploit vulnerabilities.
- B. Incorrect:** A vulnerability is a weakness in a system or asset that can be exploited.
- C. Incorrect:** A threat is a possible danger that might exploit a vulnerability, resulting in harm to the organization.
- D. Incorrect:** An exploit is a successful attack against a vulnerability, or a known method of attacking a vulnerability successfully.

**4. Correct Answer: D**

- A. Incorrect:** Likelihood is important to risk, but vulnerability isn’t used in the calculation.
- B. Incorrect:** Impact is important to risk, but vulnerability isn’t used in the calculation.
- C. Incorrect:** Neither vulnerability nor threats are used in the calculation of risk.
- D. Correct:** Risk is calculated by multiplying likelihood and impact. This makes higher-impact or higher-probability risks more important.

**5. Correct Answer: C**

- A. Incorrect:** Red box is not a term associated with penetration testing.
- B. Incorrect:** White box or crystal box penetration testing allows full visibility and knowledge of the penetration test target.
- C. Correct:** Gray box penetration testing provides partial knowledge of the target.
- D. Incorrect:** Black box testing provides no knowledge of the testing target.

**6. Correct Answer: A**

- A. Correct:** A port scan provides information about open ports, helping to identify services on a network.
- B. Incorrect:** A port scan is often part of a penetration test, but you are unlikely to perform a complete penetration test to identify services.
- C. Incorrect:** Vulnerability scans search for vulnerable services but are not the best way to identify them.
- D. Incorrect:** A ping sweep tries to ping a series of machines to see if they are online and responding to pings—something that most modern operating systems don't do by default.

# Index

## Symbols & Numbers

- 3DES (Triple DES) algorithm
  - defined, 501
  - encrypting files, 479
  - overview, 464–465
- 802.1x authentication
  - defined, 489
  - hardening devices, 222
  - overview, 99
- 2012 Web Application Vulnerability Scanner
  - comparison, 269
- & (ampersand), 294
- \ (backslash), 294
- = (equals symbol), 294
- > (greater-than symbol), 294
- < (less-than symbol), 294
- (minus sign), 294
- + (plus symbol), 294
- " (quotation mark), 294
- ;(semicolon), 294
- ' (single quote), 294
- / (slash), 71

## A

- acceptable use policies (AUPs), 115
- acceptance of risk, 11
- Access component, Safe Harbor program, 114
- access control
  - audits, 117
  - authentication
    - AD DS, 428–429
    - defined, 413
    - Kerberos protocol, 425–426
    - LDAP, 426–428
    - OpenID, 429–430
    - RADIUS, 423–424
    - SAML, 430–431
    - services for, 423
    - single-factor vs. multifactor, 414–416
    - SSO, 429
    - TACACS, 424–425
  - authorization, 414
  - biometrics
    - deploying, 419–420
    - failure modes, 417–419
    - overview, 416–417
    - technologies, 417
  - concepts
    - job rotation, 434
    - least privilege, 432–433
    - mandatory vacation, 434
    - separation of duties, 433
    - time-of-day restrictions, 434
    - trusted operating systems, 432
  - identification, 412–413
  - models
    - discretionary access control, 436–437
    - mandatory access control, 435–436
    - role-based access control, 437–438
  - tokens
    - CAC cards, 421
    - overview, 420
    - PIV cards, 422
    - smart cards, 421
  - user accounts
    - centralized vs. decentralized privilege management, 443–448
    - group-based privilege management, 442
    - overview, 414
    - passwords, 439–441
    - role-based privilege management, 442



## access control lists (ACLs)

- user-assigned privilege management, 444–448
- user-based privilege management, 442
- access control lists (ACLs), 47, 95, 155, 206, 436, 489
- access logs, 234–236
- account lockout, 440
- account logons, 232
- account management events, 232
- accounts
  - renaming, 221
  - unnecessary, disabling, 220–221
- ACLs (access control lists), 47, 95, 155, 206, 436, 489
- Active Directory Group Policy, 217
- active-scan technology for anti-virus software, 326
- addresses, IP, 71
- address space layout randomization (ASLR), 166, 292, 489
- address variable, 165
- AD DS (Active Directory Domain Services)
  - authentication using, 428–429
  - defined, 489
- ad hoc controls, 16
- administrative controls, 13, 218
- Advanced Encryption Standard algorithm. *See* AES algorithm
- advanced persistent threat. *See* APTs
- advertisement interpretation, 300
- adware
  - defined, 489
  - vs. freeware, 334
  - overview, 152
- AES (Advanced Encryption Standard) algorithm
  - defined, 489
  - encrypting files, 479
  - full-disk encryption, 379
  - hardware encryption, 395
  - overview, 465
  - in standards, 112
  - WPA2, 102
- AfriNIC (African NIC), 71
- AHs (authentication Headers), 482
- ALE (annualized loss expectancy), 7, 132, 489
- alerts
  - defined, 489
  - monitoring logs, 239
- algorithm, 374
- all-in-one security appliances
  - defined, 489
  - overview, 62–66

- allowed character confirmation, 294
- allow rules, 41
- alteration vs. integrity, 3
- Alt+F4 keyboard shortcut, 336
- American Registry of Internet Numbers (ARIN), 71
- American Society of Heating, Refrigeration, and Air-Conditioning Engineers (ASHRAE), 128
- ampersand ( & ), 294
- analysis phase of incident response, 21–22
- Android
  - encryption of device, 357
  - finding missing device using GPS, 360
  - passwords, strong, 355
  - remote wipe, 358
  - screen lock settings, 354
- annualized loss expectancy (ALE), 7, 132, 489
- annualized rate of occurrence (ARO), 7, 489
- anomaly detection, 54, 322
- anti-malware
  - defined, 489
  - host-based firewalls, 337–339
  - overview, 321–323
  - pop-up blockers, 336–337
- anti-spam
  - defined, 489
  - overview, 330–333
- anti-spyware
  - defined, 489
  - overview, 333–335
- anti-virus
  - defined, 489
  - overview, 324–330
  - as technical control, 12
- APNIC (Asia-Pacific Network Information Centre), 71
- application attacks
  - insider threats, 163
  - privilege escalation, 162–163
- application configuration baseline, 301–303
- application events, event logs, 228
- application hardening, 303–306
- application-layer firewalls
  - defined, 42, 490
  - filtering in, 43
- application logs, 231–232
- application patch management, 306–315
- application security
  - application configuration baseline, 301–303
  - application hardening, 303–306

- application patch management, 306–315
- cross-site request forgery, 297–301
- cross-site scripting, 296–297
- fuzzing, 289–290
- overview, 287–289
- secure coding concepts
  - error handling, 292–293
  - exception handling, 292–293
  - input validation, 293–295
  - overview, 290–292
- vulnerabilities
  - buffer overflow, 165–166
  - zero-day attacks, 164–165
- APTs (Advanced Persistent Threats)
  - defined, 14, 489
  - overview, 160–161
- architecture reviews, 258, 490
- ARIN (American Registry of Internet Numbers), 71
- ARO (annualized rate of occurrence), 7, 489
- ARP poisoning, 178–179
- AS (authentication server), 425
- ASHRAE (American Society of Heating, Refrigeration, and Air-Conditioning Engineers), 128–129
- Asia-Pacific Network Information Centre (APNIC), 71
- ASLR (address space layout randomization), 166, 292, 489
- assessments. *See also* vulnerability
  - risk-based
    - likelihood and impact, 5
    - overview, 4–5, 256
    - qualitative risk assessment, 6
    - quantitative risk assessment, 7–9
    - threat assessments, 257
    - vulnerability assessments, 258
  - techniques for
    - overview, 258–259
    - threat vs. likelihood, 259–260
- asset value (AV), 7, 490
- asymmetric encryption algorithms
  - defined, 490
  - ECC, 470
  - PGP, 468–470
  - RSA, 468
  - vs. symmetric encryption algorithms, 454–457
- attachment handling, 193
- attacks and threats. *See also* defense againsts attacks
  - client-side attacks
    - adware, 152
    - APTs, 160–161
    - backdoors, 159
    - botnets, 156–157
    - buffer overflow, 165–166
    - insider threats, 163
    - logic bomb, 159–160
    - malicious add-ons, 157
    - overview, 151
    - privilege escalation, 162–163
    - rootkits, 157–158
    - spyware, 152
    - trojans, 156
    - viruses, 152–154
    - worms, 154–155
    - zero-day attacks, 164–165
  - injection attacks
    - command injection, 174
    - LDAP injection, 173
    - overview, 171–172
    - SQL injection, 172–173
    - XML injection, 174
  - network attacks
    - ARP poisoning, 178–179
    - DDoS, 179–180
    - DNS poisoning, 178–179
    - DoS, 179–180
    - man-in-middle, 176–177
    - packet sniffing, 176
    - replay attack, 177
    - smurf attacks, 180–181
    - spoofing, 175–176
    - Xmas attacks, 181–182
  - social engineering
    - email attachments, 193
    - hoaxes, 190
    - overview, 188–189
    - phishing, 190–192
    - spam, 193–194
  - web attacks
    - directory traversal, 169–170
    - header manipulation, 168
    - XSS, 170–171
  - wireless attacks
    - Bluetooth attacks, 185
    - packet sniffing, 186–188
    - rogue access points, 183–184
    - war driving, 185–186
- attack surface, 258, 490

## audience for penetration testing

- audience for penetration testing, 276–277
- audio questions, 300
- audits
  - for access control, 117
  - hardening process, 304
  - logs, 228, 229, 490
  - as operational control, 12
- AUPs (acceptable use policies), 115
- authentication
  - AD DS, 428–429
  - defined, 413, 490
  - and digital signatures, 473
  - handler log, 226
  - hardening process, 305
  - Kerberos protocol, 425–426
  - LDAP, 426–428
  - OpenID, 429–430
  - RADIUS, 423–424
  - SAML, 430–431
  - services for, 423
  - single-factor vs. multifactor, 414–416
  - SSO, 429
  - TACACS, 424–425
  - as technical control, 12
  - using cryptography, 483
- authentication header, IPsec, 78
- Authentication Headers (AHs), 482
- authentication server (AS), 425
- authority for penetration testing, 276–277
- authorization
  - defined, 414, 490
  - penetration testing and, 276
- automated responses, to events, 238
- availability
  - defined, 490
  - vs. denial, 3–4
- AV (asset value), 7, 490
- avoidance of risk, 9
- awareness programs, 118

## B

- BaaS (backend as a service), 94
- BackBox, 279
- backdoors
  - defined, 490
  - malware, 324
  - overview, 159

- backend as a service (BaaS), 94
- background checks, 12
- backout plans, 140
- backslash (\), 294
- BackTrack Linux, 279
- backups
  - for disaster recovery planning, 140–141
  - hardening process, 305
  - patch management, 340
  - and RAID disks, 143
  - storing in safes, 347
- baiting technique, social engineering, 189
- bandwidth
  - and DoS attacks, 23
  - in UTM devices, 62
- baselines
  - defined, 490
  - hardening process, 305
  - for host software, 349–350
  - reporting, 258
- Baseline Security Analyzer, 207–208
- batch total check, 294
- BCP (business continuity planning). *See* business continuity planning
- behavior
  - avoiding malware by modifying, 323
  - detection based on, 54
  - detection based upon, 322
- Bell-LaPadula, 436
- BIA (business impact assessment)
  - defined, 490
  - overview, 132
- binary numbers, 70
- biometrics
  - defined, 490
  - deploying, 419–420
  - failure modes, 417–419
  - locks, 242
  - overview, 416–417
  - technologies, 417
- BIOS, 490
- bit-by-bit copies, 30. *See also* imaging systems
- BitLocker encryption, 480
- black box penetration testing, 274, 490
- blacklists
  - DNS, 60
  - for web security gateways, 61
- blended threats, 322

blind penetration tests, 274  
 block ciphers  
     defined, 490  
     vs. stream ciphers, 458  
 Blowfish algorithm  
     defined, 490  
     overview, 465–466  
 bluejacking, 185  
 bluesnarfing, 185  
 bluesniping, 185  
 border router, 46  
 botnets  
     defined, 490  
     malware, 324  
     overview, 156–157  
 bots, 490  
 bottlenecks, 320, 490  
 bridging, network, 100–101  
 bring your own device (BYOD) policies, 122, 204, 351, 391, 490  
 browsers, pop-ups in, 337  
 brute-force attacks, 454  
 buffer overflow, 165–166, 292–294, 321, 490  
 BugTraq, 279  
 business continuity planning  
     business impact assessment, 132  
     defined, 132, 490  
     disaster recovery plan, 135  
     removing single points of failure, 133–134  
     succession planning, 137–138  
     testing, 135–137  
 business impact assessment. *See* BIA  
 button press-based tokens, 420  
 BYOD (bring your own device) policies, 122, 204, 351, 391, 490

## C

cable locks, 343–345, 491  
 CAC (Common Access Card), 421  
 Caesar Cipher, 451  
 Cain and Abel, 326  
 caller ID spoofing, 175  
 CAM (content-addressable memory) table  
     defined, 47  
     overflow, 48  
 cameras  
     physical security, 245–246  
     taking screen shots, 33  
 canonicalization, 491  
 CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart), 300  
 cardinality check, 295  
 careers, xxvi  
 CAS (Central Authentication Service), 430  
 CAs (certificate authorities), 82, 476  
 C&C (command and control) networks, 156  
 CC (Common Criteria), 432  
 CCMP (Counter Cipher Mode Protocol), 102  
 Center for Internet Security (CIS), 203  
 Central Authentication Service (CAS), 430  
 centralized privilege management, 443–448  
 certificate authorities (CAs), 82, 476  
 certificate revocation lists, 478  
 Certified Information Systems Security Professional (CISSP), 13  
 CGI scripting attacks, 293  
 chain of custody  
     defined, 491  
     preserving, 26–27  
 CHAP (Challenge Handshake Authentication Protocol), 483, 491  
 check digits validation, 295  
 checklist reviews, 136  
 Chen, Shay, 269  
 Chief Information Security Officer (CISO), 113  
 Children’s Online Privacy Protection Act (COPPA), 119  
 Choice component, Safe Harbor program, 114  
 Christmas tree packets. *See* Xmas attacks  
 CIA triad  
     availability, 3–4  
     confidentiality, 3  
     and cryptography, 451  
     integrity, 3  
     overview, 2  
 CIDR (Classless Inter-Domain Routing)  
     defined, 491  
     overview, 71–72  
 cipher locks, 242  
 ciphertext, 374  
 CIS (Center for Internet Security), 203  
 CISO (Chief Information Security Officer), 113  
 CISSP (Certified Information Systems Security Professional), 13

## Class A/B/C/D extinguishers

- Class A/B/C/D extinguishers, 129–130
- classifying information
  - overview, 124–126
  - personally identifying information, 126–127
- Class K extinguishers, 130
- Classless Inter-Domain Routing. *See* CIDR
- clean desk policy, 121
- cleartext, 373
- client-side attacks
  - application attacks
    - insider threats, 163
    - privilege escalation, 162–163
  - application vulnerabilities
    - buffer overflow, 165–166
    - zero-day attacks, 164–165
  - malware
    - adware, 152
    - APTs, 160–161
    - backdoors, 159
    - botnets, 156–157
    - logic bomb, 159–160
    - malicious add-ons, 157
    - rootkits, 157–158
    - spyware, 152
    - trojans, 156
    - viruses, 152–154
    - worms, 154–155
    - zombies, 156–157
  - overview, 151
- cloning, 352
- cloud computing, 8, 94–95, 361
- clustered servers, 142, 491
- code reviews, 258, 491
- coding, security concepts
  - error handling, 292–293
  - exception handling, 292–293
  - input validation, 293–295
  - overview, 290–292
- coffer, 345
- cold aisle, 128
- cold boot attack, 383, 491
- cold sites, 143
- command and control (C&C) networks, 156
- command injection
  - defined, 491
  - input validation, 293
  - overview, 174
- Common Access Card (CAC), 421
- Common Criteria (CC), 432
- Common Vulnerabilities and Exposures (CVE), 278
- communication
  - during incident response, 25–26
  - staff for, 17
- companion CD, xxiv
- Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA), 300
- compliance training, 119
- computational complexity of cryptography, 457
- computer forensics
  - hashing, 29–30
  - imaging systems, 30
  - logs, 31–32
  - network traffic, 31–32
  - order of volatility, 28–29
  - overview, 28
  - screen shots, 33
  - time offsets, 32–33
  - video capture, 33
- concentrators, 48
- Conficker virus, 326
- confidentiality
  - and cryptography, 451
  - defined, 491
  - information classification, 125
  - vs. disclosure, 3
- configuration baseline
  - for applications, 301–303
  - hardening, 205–206
- configuration profiles, 206
- configuring systems
  - disabling unnecessary accounts, 220–221
  - disabling unnecessary ports, 214–216
  - disabling unnecessary services, 214–216
  - host firewalls, 216–217
  - overview, 209–210
  - password protection, 219–220
  - patch management methodologies, 212–214
  - protecting administrative interfaces, 218
  - updates, 211–212
- congestion window reduced (CWR) flags set, 181
- consistency check, 295
- containment, eradication, and recovery phase of incident response, 22–24
- content-addressable memory. *See* CAM
- content inspection, 491

- continuous security monitoring
  - defined, 491
  - overview, 223
- cookies
  - defined, 491
  - web attacks using, 166–168
- Coordinated Universal Time, 224
- COPPA (Children’s Online Privacy Protection Act), 119
- CORE logging, 226
- corrective controls, 13
- Counter Cipher Mode Protocol (CCMP), 102
- covert perspective tests, 272
- credit card security incidents, 26
- CRL (certificate revocation list), 478
- cron, 226
- crossover error rate, 418, 491
- cross-site request forgery. *See* XSRF
- cross-site scripting. *See* XSS
- cryptography, 374, 491
  - asymmetric encryption algorithms
    - ECC, 470
    - PGP, 468–470
    - RSA, 468
    - vs. symmetric encryption algorithms, 454–457
  - authentication using, 483
  - computational complexity, 457
  - digital signatures
    - creating, 473–475
    - cryptographic hashes, 471–473
    - defined, 471
  - encrypting data
    - file encryption, 479–480
    - IPsec, 482
    - SSH, 482
    - SSL, 481
    - TLS, 481
    - transport encryption, 480
    - whole-disk encryption, 480
  - goals of, 451–452
  - one-time pads, 459
  - overview, 452–454
  - public-key infrastructure
    - certificate revocation lists, 478
    - digital certificates, 476–478
    - key escrow, 478
    - key recovery, 478
    - overview, 476
  - scalability, 457–458

- stream vs. block ciphers, 458
- symmetric encryption algorithms
  - 3DES, 464–465
  - AES, 465
  - Blowfish, 465–466
  - DES, 460–463
  - RC4, 467
  - Twofish, 466
  - vs. asymmetric encryption algorithms, 454–457
- crystal box penetration testing, 274
- CSRF (cross-site request forgery). *See* XSRF
- CVE (Common Vulnerabilities and Exposures), 278
- CWR (congestion window reduced) flags set, 181

## D

- DaaS (desktop as a service), 94
- DAC (discretionary access control), 435–437, 492
- DAD triad
  - alteration, 3
  - denial, 3–4
  - disclosure, 3
  - overview, 2
- darknets, 270
- database encryption, 384–385, 492
- database management system (DBMS), 436
- data breach notification law, California, 127
- data disposal, 120–121
- data encryption, 491
- data execution prevention (DEP), 166, 292, 491
- data exfiltration, 372, 492
- data handling, 120–121
- Data Integrity component, Safe Harbor program, 114
- data leak, 372
- data loss prevention. *See* DLP
- Data Protection Directive (DPD), 114
- data security
  - data loss prevention, 371–373
  - encryption
    - databases, 384–385
    - files, 385–387
    - full-disk, 377–383
    - mobile devices, 391–393
    - overview, 373–376
    - removable media, 388–390
  - hardware-based encryption devices
    - hard drive encryption, 399–401

## data theft

- HSM, 396–397
- overview, 393–395
- TPM, 395–396
- USB encryption, 398–399
- data theft, 112
- data type check, 295
- DBMS (database management system), 436
- dc (domain component), 427
- DDoS (distributed denial of service) attacks
  - defined, 4, 492
  - incident response teams, 26
  - overview, 179–180
- decentralized privilege management, 443–448
- decommissioning encrypted device, 380, 492
- decreasing traffic using firewalls, 40
- decryption
  - in 3DES, 464
  - defined, 453, 492
  - full-disk encryption, 380–382
- default passwords, 219
- defense against attacks. *See also* attacks and threats
  - hardening
    - 802.1x, 222
    - configuration baseline, 205–206
    - disabling ports, 222
    - MAC filtering, 222
    - overview, 203
    - standards for, 203–205
    - templates for, 206–209
  - monitoring and reporting
    - access logs, 234–236
    - alerts, 239
    - application logs, 231–232
    - audit logs, 229
    - continuous security monitoring, 223
    - event logs, 227–228
    - security logs, 232–234
    - SIEMs, 237–239
    - success vs. failure logs, 229–231
    - system logs, 224–225
    - time stamps in logs, 224–225
    - trends and thresholds, 240–241
    - Windows vs. Linux logs, 226–227
  - physical security
    - access lists, 244
    - fences, 244
    - guards, 245
    - hardware locks, 241–242
    - mantraps, 246–252
    - proximity readers, 242–244
    - video surveillance, 245–246
  - system configuration
    - disabling unnecessary accounts, 220–221
    - disabling unnecessary ports, 214–216
    - disabling unnecessary services, 214–216
    - host firewalls, 216–217
    - overview, 209–210
    - password protection, 219–220
    - patch management methodologies, 212–214
    - protecting administrative interfaces, 218
    - updates, 211–212
  - defense in depth, 40, 492
  - demilitarized zone (DMZ), 84, 492
  - denial of service attacks. *See* DoS attacks
  - denial vs. availability, 3–4
  - deny-by-default rule, 96
  - deny rules, 41
  - DEP (data execution prevention), 166, 292, 491
  - DES (Data Encryption Standard) algorithm
    - defined, 491
    - overview, 460–463
  - design reviews, 258, 492
  - desktop as a service (DaaS), 94
  - detection and analysis phase of incident response, 21–22
  - detection vs. prevention, 245
  - detective controls, 13
  - deterrence of risk, 10–11
  - device drivers, 305
  - differential backups, 140, 492
  - DigiNotar, 82
  - digital certificates, 476–478, 492
  - digital signatures
    - in certificates, 477
    - creating, 473–475
    - cryptographic hashes, 471–473
    - defined, 471, 492
  - direct memory access (DMA) attacks, 383
  - directory service events, 232
  - directory traversal, 169–170, 492
  - disabling scripts, 296, 298
  - disaster recovery planning
    - backups, 140–141
    - and business continuity plan, 135
    - defined, 492
    - disaster recovery sites

- cold sites, 143
- hot sites, 143
- warm sites, 143
- fault-tolerant environments
  - disk redundancy, 142–143
  - hardware redundancy, 141
  - server redundancy, 141–142
- metrics
  - mean time between failures, 139
  - mean time to restore, 138
  - recovery point objective, 138
  - recovery time objective, 138
- overview, 138
- disclosure vs. confidentiality, 3
- discretionary access control (DAC), 431, 435–437, 492
- disguised storage devices, 342
- disks
  - encrypting, 480
  - mirroring, 142
  - redundancy, 142–143
  - striping, 142
  - verifying integrity of, 30
- disposing of mobile devices, 352
- distinguished name (DN), 427
- distributed denial of service attacks. *See* DDoS attacks
- distribution router, 46
- DLP (data loss prevention)
  - defined, 492
  - overview, 371–373
  - security policies, 342
- DMA (direct memory access) attacks, 383
- DMZ (demilitarized zone), 52, 84, 492
- DN (distinguished name), 427
- DNS changers, 322, 492
- DNS (Domain Name System)
  - blacklisting, 60
  - overview, 79
- DNS poisoning, 168, 178–179
- DNSSEC (Domain Name System Security Extension), 178
- DNS spoofing attacks, 175
- documentation
  - of every security activity, 308
  - hardening process, 304
  - patch management process, 308
  - for witness interviews, 27
- domain component (dc), 427
- Domain Name System. *See* DNS

- Domain Name System Security Extensions (DNS-SEC), 178
- Doom virus, 325
- DoS (denial of service) attacks
  - defined, 492
  - overview, 179–180
  - routers, 47
- double submit cookies, 299
- downloading files, 323
- DPD (Data Protection Directive), 114
- drivers, device, 305
- DRP (Disaster Recovery Planning), 17
- dry pipe, 130
- dumb switches, 48
- dumpster diving, 189, 492
- dynamic learning, port security, 98

## E

- EALs (Evaluation Assurance Levels), 432
- EAP (Extensible Authentication Protocol), 102, 493
- eavesdropping, 352
- ECC (elliptic curve cryptography) algorithm
  - defined, 492
  - overview, 470
- Edge Transport Server, 59
- EF (exposure factor), 7, 493
- EFS (Encryption File System), 385
- EICAR, 326, 492
- electronic serial number (ESN), 352
- elliptic curve cryptography algorithm. *See* ECC algorithm
- email
  - attacks using attachments, 193–194
  - attacks using spam, 193–194
  - malware through attachments, 323
  - marking as spam, 58
- emergency power off (EPO) mechanism, 130
- EMI (electromagnetic interference)
  - defined, 492
  - overview, 130–131
- Encapsulating Security Payloads (ESPs), 78, 482
- encryption
  - databases, 384–385
  - and data handling, 120
  - defined, 452, 491, 493
  - file encryption, 479–480



## Encryption File System (EFS)

- files, 385–387
  - full-disk
    - decommissioning encrypted device, 380
    - decrypting, 380–382
    - implementing, 378–380
    - recovery options, 382
    - vulnerabilities, 382–383
  - IPsec, 482
  - for mobile devices
    - overview, 356–357
    - voice encryption, 359
  - mobile devices, 391–393
  - overview, 373–376
  - removable media, 388–390
  - SSH, 482
  - SSL, 481
  - as technical control, 12
  - TLS, 481
  - transport encryption, 480
  - VoIP communications, 359
  - whole-disk encryption, 480
- Encryption File System (EFS), 385
- Enforcement component, Safe Harbor program, 114
- environmental controls
  - electromagnetic interference, 130–131
  - fire suppression, 129–130
  - HVAC, 128
  - monitoring, 130–131
- EPO (emergency power off) mechanism, 130
- equals symbol ( = ), 294
- eradication phase of incident response, 22–24
- error handling, 292–293
- Error log entry, Windows Application log, 231
- escaping metacharacters, 294, 297, 493
- ESN (electronic serial number), 352
- ESPs (Encapsulating Security Payloads), 78, 482
- Ettercap, 326
- EU (European Union), 114
- EU Safe Harbor program, 113
- Evaluation Assurance Levels (EALs), 432
- event logs
  - defined, 493
  - overview, 227–228
- evidence for incident response
  - interviewing witnesses, 27
  - overview, 26
  - preserving chain of custody, 26–27
  - tracking time and expense, 27–28
- evil twins, 183, 493
- exception handling, 292–293
- Exclusive OR (XOR) operation, 461
- expandable storage in mobile devices, 351
- explicit proxies, 51
- Exploit Database, 278
- exploits, 321, 493
- exposure factor (EF), 7, 493
- ExpressCards, 396
- Extensible Authentication Protocol (EAP), 102, 493
- external-perspective tests, 272

## F

- Facebook security policies, 122
- facial recognition, 417
- facilities group, 17
- fail open, 210
- fail secure, 210
- Failure log entry, Windows Application log, 231
- failure modes for biometrics systems, 417–419
- failure-to-capture rate (FTC), 420
- failure-to-enroll rate (FTE), 420
- fake software
  - anti-spyware, 335
  - anti-virus, 329
- fallback plans, 140
- false acceptance mode, 417–418
- false acceptance rate (FAR), 418, 493
- false match rate (FMR), 418
- false positives, 55–56, 493
- false rejection mode, 417–418
- false rejection rate (FRR), 418, 493
- Family Educational Rights and Privacy Act (FERPA), 119, 238
- Faraday cage, 130
- FAR (false acceptance rate), 418, 493
- fault-tolerant environments
  - disk redundancy, 142–143
  - hardware redundancy, 141
  - server redundancy, 141–142
- Federal Information Processing Standard (FIPS), 256, 375, 422
- FedRAMP (Federal Risk and Authorization Management Program), 95
- Feistel function, 460–462, 465
- fences, 244

- FERPA (Family Educational Rights and Privacy Act), 119, 238
  - file-based scanner, 328
  - File Transfer Protocol (FTP), 80, 493
  - File Transfer Protocol Secure (FTPS), 493
  - FileVault encryption, 480
  - filtering URLs, 59–60
  - fingerprint systems, 417
  - FIPS (Federal Information Processing Standard), 256, 375, 422
  - Firesheep, 187
  - fire suppression
    - extinguisher classes, 130
    - overview, 129–130
  - firewalls
    - defined, 493
    - hardening process, 305
    - host-based, 337–339
    - host firewalls, 216–217
    - and IPv6, 74
    - as network shields, 40
    - networks without, 45
    - network traffic analysis, 31
    - overview, 41–43
    - rules for, 96
    - software, 338
    - as technical control, 12
    - in UTM devices, 62
    - web application firewalls (WAF), 44–46
  - firmware
    - defined, 493
    - patch management, 319
  - first responder, incident response team, 14–15
  - flood guards
    - defined, 493
    - overview, 99–100
    - tools for, 100
  - FMR (false match rate), 418
  - forensics
    - hashing, 29–30
    - imaging systems, 30
    - logs, 31–32
    - network traffic, 31–32
    - order of volatility, 28–29
    - overview, 28
    - screen shots, 33
    - time offsets, 32–33
    - video capture, 33
  - format check, 295
  - forwarded events, event logs, 228
  - forward proxies, 51
  - forward slash (/), 71
  - Frankenstein malware, 292
  - FreeBSD, 228
  - Free Open Wi-Fi, 184
  - FRR (false rejection rate), 418, 493
  - F-Secure, 322
  - FTC (failure-to-capture rate), 420
  - FTE (failure-to-enroll rate), 420
  - FTP (File Transfer Protocol), 80, 493
  - FTPS (File Transfer Protocol Secure), 493
  - full backups, 140, 493
  - full-disk encryption
    - decommissioning encrypted device, 380
    - decrypting, 380–382
    - defined, 493
    - implementing, 378–380
    - recovery options, 382
    - vulnerabilities, 382–383
  - full interruption tests, 137
  - fuzz testing
    - defined, 289–290, 493
    - hardening process, 305
- ## G
- gateway spoofing, 175
  - gateways proxies, 51
  - gestures for lock screen, 354
  - GLBA (Gramm-Leach-Bliley Act), 119, 238
  - GNU Privacy Guard (GPG) package, 470
  - GNU Public License, 470
  - go bag, 20
  - GPG (GNU Privacy Guard) package, 470
  - GPS tracking, 359–361, 493
  - Gramm-Leach-Bliley Act (GLBA), 119, 238
  - gray box penetration testing, 275, 493
  - greater-than symbol ( > ), 294
  - Greenwich Mean Time, 224
  - group-based privilege management, 442
  - guards, 245
  - guidelines
    - defined, 111, 493
    - vs. policies, 112

**H**

- Hacker Defender, 158
  - hand geometry systems, 417
  - hardening
    - 802.1x authentication, 222
    - applications, 303–306
    - configuration baseline, 205–206
    - defined, 493
    - disabling ports, 222
    - MAC filtering, 222
    - overview, 203
    - standards for, 203–205
    - templates for, 206–209
  - hardware
    - backdoors, 159
    - cable locks, 343–345
    - encryption devices based on
      - hard drive encryption, 399–401
      - HSM, 396–397
      - overview, 393–395
      - TPM, 395–396
      - USB encryption, 398–399
    - locking cabinets, 347–349
    - locks, 241–242, 493
    - overview, 341–343
    - redundancy, 141
    - requirements for virtualization, xxiii
    - safes, 345–347
  - hardware security module (HSM), 384, 396–397, 494
  - Hash-based message authentication code (HMAC), 473
  - hashes
    - cryptography, 374, 471–473
    - defined, 494
    - overview, 29–30
    - verifying disk integrity using, 30
  - header manipulation, 168, 494
  - Health Insurance Portability and Accountability Act (HIPAA), 119, 238, 373
  - heating, ventilation, and air conditioning (HVAC), 128
  - heuristic detection, 54
  - hidden field test, 300
  - HIDS (host-based intrusion detection), 54
  - high-interaction honeypots, 270
  - highly sensitive information (HSI), 125–126
  - HInet, 184
  - HIPAA (Health Insurance Portability and Accountability Act), 119, 238, 373
  - HIPS (host-based intrusion prevention), 54
  - HMAC (hash-based message authentication code), 473
  - hoaxes, 190, 329
  - honeynets
    - defined, 494
    - overview, 269–270
  - honeypots
    - defined, 494
    - overview, 269–270
  - host-based firewalls
    - defined, 494
    - overview, 216–217, 337–339
    - pairing with network firewalls, 43
  - host-based IDS, 54–55
  - host-based IPS, 54–55
  - host-based mode, sniffers, 57
  - host security
    - anti-malware
      - anti-spam, 330–333
      - anti-spyware, 333–335
      - anti-virus, 324–330
      - host-based firewalls, 337–339
      - overview, 321–323
      - pop-up blockers, 336–337
    - hardware security
      - cable locks, 343–345
      - locking cabinets, 347–349
      - overview, 341–343
      - safes, 345–347
  - host software baselining, 349–350
  - mobile devices
    - encrypting, 356–357
    - GPS tracking, 359–361
    - overview, 351–353
    - passwords, 355–356
    - remote wipe/sanitization, 358–359
    - screen lock, 354
    - voice encryption, 359
  - operating system security, 318–320
  - patch management, 339–341
- host software baselining, 349–350
- hot aisle, 128
- hot sites, 143
- HR (human resources), 17, 115
- HSI (highly sensitive information), 125, 126
- HSM (hardware security module), 384, 396–397, 494
- HTTP (Hypertext Transfer Protocol), 44, 81, 494
- HttpOnly cookies, 167

HTTP response splitting, 168  
 HTTPS (Hypertext Transfer Protocol Secure), 44, 481, 494  
 hubs  
   defined, 48  
   monitoring network using, 49  
 human resources (HR), 17, 115  
 HVAC (heating, ventilation, and air conditioning), 128  
 Hypertext Transfer Protocol (HTTP), 44, 81, 494  
 Hypertext Transfer Protocol Secure (HTTPS), 44, 481, 494  
 hypervisors, 91

## I

laaS (infrastructure as a service), 94, 494  
 IANA (Internet Assigned Numbers Authority), 71  
 ICMP (Internet Control Message Protocol), 76, 494  
 identification, 412–413, 494  
 IDS (intrusion detection systems)  
   defined, 494  
   false positives, 55–56  
   host-based, 54–55  
   overview, 54  
   in UTM devices, 62  
 IETF (Internet Engineering Task Force), 103  
 ifconfig command, 73  
 ignoring risks, 11  
 image map, 336  
 IMAP (Internet Message Access Protocol), 82  
 IMEI (International Mobile Station Equipment Identity), 352  
 impact of risk, 5  
 impersonation, 189, 247, 494  
 implicit deny, 41, 432, 494  
 incident response  
   collecting evidence  
     interviewing witnesses, 27  
     overview, 26  
     preserving chain of custody, 26–27  
     tracking time and expense, 27–28  
   communication during, 25–26  
   computer forensics  
     hashing, 29–30  
     imaging systems, 30  
     logs, 31–32  
     network traffic, 31–32  
   order of volatility, 28–29  
   overview, 28  
   screen shots, 33  
   time offsets, 32–33  
   video capture, 33  
 drills, 19  
 life cycle  
   containment, eradication, and recovery phase, 22–24  
   detection and analysis phase, 21–22  
   overview, 19–20  
   post-incident phase, 24–25  
   preparation phase, 20–21  
 outsourcing, 18  
 overview, 14  
 team  
   categories needed, 16–18  
   first responder, 14–15  
   overview, 14  
   training, 18–19  
 incremental backups, 140, 494  
 indemnification clauses, 10  
 information classification  
   overview, 124–126  
   personally identifying information, 126–127  
 Information log entry, Windows Application log, 231  
 information security staff, 16  
 infrastructure as a service (IaaS), 94, 494  
 InGuardians Samurai Web Testing Framework, 279  
 initialization vector (IV), 101, 374  
 injection attacks  
   command injection, 174  
   input validation, 293  
   LDAP injection, 173  
   overview, 171–172  
   SQL injection, 172–173  
   XML injection, 174  
 Inline mode, deploying sniffers, 57  
 in-motion events, 372  
 in-place events, 372  
 input limit check, 494  
 input validation  
   defined, 494  
   overview, 293–295  
   sanitizing, 297  
   as technical control, 12  
 insider threats, 163

## inspecting traffic

- inspecting traffic
  - malware inspection, 59
  - protocols, 43
  - spam filters, 58–59
  - URL filtering, 59–60
  - web security gateways, 60–61
- installing practice tests, xxiv
- Institute for Security and Open Methodologies (ISECOM), 277
- integrity
  - and cryptography, 451
  - defined, 494
  - and digital signatures, 473
  - vs. alteration, 3
- interference, 183, 494
- internal information, 125
- internal-perspective tests, 272
- International Mobile Station Equipment Identity (IMEI), 352
- International Telecommunication Union (ITU), 476
- Internet Assigned Numbers Authority (IANA), 71
- Internet Control Message Protocol (ICMP), 76, 494
- Internet Engineering Task Force (IETF), 103
- internet-facing proxies, 51
- Internet Message Access Protocol (IMAP), 82
- Internet Protocol Security (IPsec), 52, 73, 77, 494
- Internet Relay Chat (IRC), 156
- Internet Security Association and Key Management Protocol (ISAKMP), 78
- Internet Service Providers (ISPs), 26
- Internet Worm, 154
- interviewing witnesses, 27
- intrinsic information, 343
- intrusion detection
  - incident response life cycle, 21
  - as technical control, 12
- intrusion detection systems. *See* IDS
- intrusion prevention systems. *See* IPS
- in-use events, 372
- IP (Internet Protocol)
  - addresses, 71
  - CIDR, 71–72
  - defined, 69, 494
  - IPv4, 70
  - IPv6, 72–74
  - subnets, 71–72
  - suite, 74–77
- IPsec (Internet Protocol Security), 52, 73, 77, 482, 494

- IPsec VPNs, 52, 89
- IPS (intrusion prevention systems)
  - defined, 494
  - false positives, 55–56
  - host-based, 54–55
  - overview, 54
  - pairing firewalls with, 217
  - signatures, 55
  - in UTM devices, 62
- IPv4, 70, 495
- IPv6, 72–74, 495
- IRC (Internet Relay Chat), 156
- iris recognition, 417
- ISAKMP (Internet Security Association and Key Management Protocol), 78
- ISECOM (Institute for Security and Open Methodologies), 277
- isolation of network components, 23
- ISPs (Internet Service Providers), 26
- IT contingency planning, 138
- ITU (International Telecommunication Union), 476
- IV (initialization vector), 101, 374

## J

- jailbreaking, 162
- job rotation, 115–116, 434
- John the Ripper, 326

## K

- Kali Linux, 279
- KDC (key distribution center), 425
- Kensington Security Slot (K-slot), 344
- Kerberos protocol
  - authentication using, 425–426
  - defined, 495
- key distribution center (KDC), 425
- keylogger, 321, 495
- key recovery agent (KRA), 386
- keys
  - defined, 495
  - escrow, 478
  - exchanging, 374
  - length of, 453
  - recovery, 478

keystroke loggers, 324  
 Klez virus, 325  
 Knoppix Security Tools Distribution, 279  
 KRA (key recovery agent), 386  
 K-slot (Kensington Security Slot), 344

## L

L2TP (Layer 2 Tunneling Protocol), 88  
 labeling information  
   overview, 124–126  
   personally identifying information, 126–127  
 language check, 295  
 LastPass, 355  
 Layer 2 Tunneling Protocol (L2TP), 88  
 layering  
   defense, 40  
   malware protection, 152  
 LDAP (Lightweight Directory Access Protocol)  
   authentication using, 426–428  
   defined, 495  
   injection attacks, 173, 293, 495  
   queries, 173  
 LEAP (Lightweight Extensible Authentication Protocol), 102, 495  
 least privilege principle  
   defined, 116–117, 495  
   hardening process, 305  
   overview, 432–433  
   and worms, 154  
 legal staff, 17  
 less-than symbol ( < ), 294  
 life cycle, incident response  
   containment, eradication, and recovery phase, 22–24  
   detection and analysis phase, 21–22  
   overview, 19–20  
   post-incident phase, 24–25  
   preparation phase, 20–21  
 Lightweight Directory Access Protocol. *See* LDAP  
 Lightweight Extensible Authentication Protocol (LEAP), 102, 495  
 likelihood of risk, 5, 259–260  
 LinkedIn security policies, 122  
 Linux  
   logs in, 226–227  
   modify/access/change logs, 236

  running services, 215  
   viruses for, 324  
 load balancing, 49–50, 142, 495  
 location tracking of mobile devices, 359  
 locking cabinets, 347–349  
 log analysis, 97  
 logging  
   network administration, 96–97  
   sniffer scans, 262  
   in UTM devices, 62  
 logic bomb  
   defined, 495  
   malware, 324  
   overview, 159–160  
 logic check, 295  
 logon credentials, not saving, 298  
 logs  
   access logs, 234–236  
   application logs, 231–232  
   audit logs, 229  
   computer forensics activities, 31–32  
   event logs, 227–228  
   hardening process, 304  
   parsing, 227  
   rotating, 224–225, 495  
   security logs, 232–234  
   sizes for, 225  
   success vs. failure, 229–231  
   time stamps in, 224–225  
   Windows vs. Linux, 226–227  
 Lookout Mobile Security app, 358, 360  
 loop protection  
   defined, 495  
   overview, 100  
 lossy mathematical operation, 375, 495  
 Love virus, 326  
 low-interaction honeypots, 270

## M

MAC (mandatory access control), 206, 431, 435–436, 496  
 MAC (media access control) addresses  
   defined, 47  
   filtering, 104, 495  
   hardening devices, 222  
   port security, 98  
   spoofing, 175

## Mac OS logging

- Mac OS logging, 234
- MailRoute, 332
- malicious add-ons
  - defined, 495
  - overview, 157
- malicious insider threats, 163
- malicious pop-ups, 336
- malware
  - adware, 152
  - APTs, 160–161
  - backdoors, 159
  - botnets, 156–157
  - defined, 495
  - inspection for, 59, 62
  - layering protection against, 152
  - logic bomb, 159–160
  - malicious add-ons, 157
  - rootkits, 157–158
  - scanning for, 305
  - spyware, 152
  - trojans, 156
  - viruses, 152–154
  - worms, 154–155
  - zombies, 156–157
- managed switches, 48
- management controls, 13, 218
- management procedures, 12
- management staff, 16
- mandatory access control (MAC), 206, 431, 435–436, 496
- mandatory vacation, 115–116, 434
- man-in-the-middle attacks
  - defined, 496
  - overview, 176–177
- mantraps
  - defined, 496
  - physical security, 246–252
- MAPI (Messaging Application Programming Interface), 82
- math operations, 300
- maximum tolerable outage (MTO), 139
- McAfee, 322
- MD5 (Message Digest 5) hash algorithm, 29, 379, 471
- mean time between failures (MTBF), 139, 496
- mean time to recovery (MTTR), 496
- mean time to restore (MTTR), 138
- media access control addresses. *See* MAC addresses
- Message Digest 5 (MD5) hash algorithm, 29, 379, 471
- Messaging Application Programming Interface (MAPI), 82
- metacharacters
  - defined, 294, 496
  - escaping, 297
- Metasploitable, 279
- Metasploit Project, 255
- metrics for disaster recovery planning
  - mean time between failures, 139
  - mean time to restore, 138
  - recovery point objective, 138
  - recovery time objective, 138
- Microsoft Baseline Security Analyzer, 207–208
- Microsoft Challenge Handshake Authentication Protocol (MS-CHAP), 483
- Microsoft Security Compliance Manager tool, 207
- Microsoft Windows. *See* Windows
- MIN (mobile identification number), 352
- minus sign ( - ), 294
- Missing Device GPS location feature, 360
- mitigation of risk, 10
- mobile devices
  - encrypting, 356–357, 391–393
  - GPS tracking, 359–361
  - overview, 351–353
  - passwords, 355–356
  - remote wipe/sanitization, 358–359
  - screen lock, 354
  - voice encryption, 359
- mobile identification number (MIN), 352
- models, access control
  - discretionary access control, 436–437
  - mandatory access control, 435–436
  - role-based access control, 437–438
- monitoring
  - alerts, 239
  - continuous security monitoring, 223
  - environmental controls, 130–131
  - performance levels, 320
  - SIEMs, 237–239
  - system logs
    - access logs, 234–236
    - application logs, 231–232
    - audit logs, 229
    - event logs, 227–228
    - log rotation, 224–225
    - security logs, 232–234
    - success vs. failure, 229–231

- time stamps in, 224–225
- Windows vs. Linux, 226–227
- trends and thresholds, 240–241
- Morris Worm, 154
- MS-CHAP (Microsoft Challenge Handshake Authentication Protocol), 483
- MTBF (mean time between failures), 139, 496
- MTO (maximum tolerable outage), 139
- MTTR (mean time to recovery), 496
- MTTR (mean time to restore), 138
- multi-criteria locks, 242
- multifactor authentication
  - defined, 496
  - vs. single-factor authentication, 414–416

## N

- NAC (network access control), 99, 307
- National Institute of Standards and Technology (NIST), 19, 126, 203, 256, 422, 465
- National Security Agency (NSA), 203
- National Vulnerability Database, 278
- NAT (Network Address Translation), 71, 86, 496
- Nessus, 265
- NetBIOS, 82–83, 496
- Netcat, 326
- Netsky virus, 326
- NetStumbler, 186
- network access control (NAC), 99, 307
- Network Address Translation (NAT), 71, 86, 496
- network attacks
  - ARP poisoning, 178–179
  - DDoS, 179–180
  - DNS poisoning, 178–179
  - DoS, 179–180
  - man-in-middle, 176–177
  - packet sniffing, 176
  - replay attack, 177
  - smurf attacks, 180–181
  - spoofing, 175–176
  - Xmas attacks, 181–182
- network design
  - administration
    - ACLs, 95
    - firewall rules, 96
    - logging, 96–97
    - rule-based management, 95
  - Internet Protocol
    - addresses, 71
    - CIDR, 71–72
    - defined, 69
    - IPv4, 70
    - IPv6, 72–74
    - subnets, 71–72
    - suite, 74–77
  - ports, 83–84
  - protocols
    - overview, 77–83
    - ports, 83–84
  - remote access
    - Remote Access Services, 89
    - VPNs, 87–89
  - routers and switches
    - 802.1x authentication, 99
    - flood guards, 99–100
    - loop protection, 100
    - port security, 98
    - preventing network bridging, 100–101
    - VLANs, 98
  - segmentation
    - overview, 84–87
    - and remote access, 87–89
    - telephony, 89–90
    - and virtualization, 90–95
    - VoIP, 89–90
  - virtualization
    - cloud computing, 94–95
    - overview, 90–92
    - secure virtual data centers, 93–94
  - wireless protocols
    - common settings, 103–104
    - overview, 101–103
- network security
  - all-in-one security appliances, 62–66
  - firewalls
    - absence of, 45
    - overview, 41–43
    - web application firewalls, 44–46
  - IDS
    - false positives, 55–56
    - host-based, 54–55
    - overview, 54
  - IPS
    - false positives, 55–56
    - host-based, 54–55



## network stumbling

- overview, 54
- load balancers, 49–50
- overview, 40
- protocol analyzers, 57–58
- proxy servers, 51
- routers, 46–47
- switches, 47–49
- topology example, 41
- traffic inspection
  - malware inspection, 59
  - spam filters, 58–59
  - URL filtering, 59–60
  - web security gateways, 60–61
- VPN concentrators, 52–53
- network stumbling, 186
- Network Time Protocol (NTP), 32, 224
- network vulnerability scanners, 265–266
- next-generation firewalls, 43
- NIDS (network intrusion detection systems). *See* IDS
- Nikto, 267
- NIPS (network intrusion prevention systems). *See* IPS
- NIST (National Institute of Standards and Technology), 19, 126, 203, 223, 256, 277, 422, 465
- Nmap, 263–264, 326
- nonrepudiation, 451, 473, 496
- nonsecure management interfaces, 218
- NoScript plugin, 298
- Notice component, Safe Harbor program, 114
- NSA (National Security Agency), 203
- NT LAN Manager (NTLM), 483, 496
- NTP (Network Time Protocol), 32, 224

## O

- offline scanning, 327, 496
- onboard encryption, 399
- on-demand scanning, 327
- on-device storage encryption, 357
- one-time pads, 459
- one-to-many NAT, 86
- online virus scanners, 328
- Onward Transfer component, Safe Harbor program, 114
- OpenBSD, 228
- OpenID, 429–430
- Open Source Security Testing Methodology Manual (OSSTMM), 277
- open-source software, 288
- Open Source Vulnerability Database (OSVDB), 267, 278
- Open Systems Interconnection (OSI) model, 52
- Open Web Application Security Project (OWASP), 257, 277
- operating systems
  - security for, 318–320
  - trusted, 432
- operational controls
  - business continuity planning
    - business impact assessment (BIA), 132
    - defined, 132
    - removing single points of failure, 133–134
    - succession planning, 137–138
    - testing, 135–137
  - disaster recovery planning
    - backups, 140–141
    - disaster recovery sites, 143
    - fault-tolerant environments, 141–143
    - metrics, 139
    - overview, 138
- environmental controls
  - electromagnetic interference, 130–131
  - fire suppression, 129–130
  - HVAC, 128
  - monitoring, 130–131
- information classification and labeling
  - overview, 124–126
  - personally identifying information (PII), 126–127
- overview, 12–13
- policies
  - acceptable use policies, 115
  - job rotation, 115–116
  - least privilege, 116–117
  - mandatory vacations, 115–116
  - overview, 111–112
  - privacy policy, 113–114
  - security policy, 113
  - separation of duties, 116
- training
  - clean desk policy, 121
  - compliance training, 119
  - data handling and disposal, 120–121
  - P2P computing, 123
  - passwords, 120
  - personally owned devices, 122
  - security policy training, 118
  - social networking, 122

- tailgating prevention, 121–122
- threat awareness, 123–124
- order of volatility, 28–29
- OSI (Open Systems Interconnection) model, 52
- OSSTMM (Open Source Security Testing Methodology Manual), 277
- OSVDB (Open Source Vulnerability Database), 267, 278
- out-of-bounds input, 289, 293
- outsourcing, 18, 53, 95
- overt penetration tests, 272
- OWASP (Open Web Application Security Project), 257, 277

## P

- P2P (peer-to-peer) computing
  - avoiding malware, 323
  - training effective use of, 123
- PaaS (platform as a service), 94, 497
- packet analyzers. *See also* protocol analyzers
  - defined, 262
  - overview, 57
- packet capture, 168
- packet filter firewalls, 42, 496
- packet sniffing. *See also* sniffers
  - defined, 31, 57
  - overview, 176
  - software, 21
  - vulnerability scanning, 261
  - wireless attacks, 186–188
- PAP (Password Authentication Protocol), 483, 496
- parallel tests, 136
- passive identification, 261
- passphrases, 440, 496
- Password Authentication Protocol (PAP), 483, 496
- passwords
  - default, 219
  - expiration, 439–440
  - guidelines for strong, 355
  - for lock screen, 354
  - for mobile devices, 355–356
  - recovery, 439
  - remembering, 356
  - resetting, 439
  - system configuration for, 219–220
  - training effective use of, 120
  - unchangeable, 220
  - for user accounts, 439–441
- patches
  - analysis of, 289
  - application patch management, 306–315
  - defined, 496
  - hardening process, 304
  - host security, 339–341
  - management methodologies, 212–214
  - system configuration for, 211–212
- Payment Card Industry Data Security Standard (PCI DSS), 26, 119, 131, 184, 238, 373
- Payment Card Industry Data Security Standard (PCI-DSS), 280
- PBX (private branch exchange), 89
- PC cards, 396
- PCI DSS (Payment Card Industry Data Security Standard), 26, 119, 131, 184, 238, 373
- PCI-DSS (Payment Card Industry Data Security Standard), 280
- PCMCIA (Personal Computer Memory Card International Association), 396
- PEAP (Protected Extensible Authentication Protocol), 102, 497
- peer-to-peer computing. *See* P2P computing
- penetration testing
  - assessment, 279
  - audience, 276–277
  - authority, 276–277
  - black box penetration testing, 274
  - defined, 497
  - gray box penetration testing, 275
  - methods for, 278–279
  - overview, 275–276
  - planning for, 277
  - remediation, 280–285
  - reporting, 280
  - scope, 276–277
  - target identification, 277–278
  - white box penetration testing, 274
- performance-based testing, xxi
- performance, monitoring, 320
- peripherals, 342, 351
- permissions, and penetration testing, 276
- persistent cookies, 167
- persistent XSS, 170
- Personal Computer Memory Card International Association (PCMCIA), 396
- personally identifying information. *See* PII
- personally owned devices, 122

## PGP (Pretty Good Privacy)

- PGP (Pretty Good Privacy), 468–470, 497
- pharming, 191, 497
- phishing attacks
  - defined, 497
  - example of, 124
  - overview, 190–192
  - threat awareness, 123
- phone hacker, 352
- phreaker, 352
- physical controls, 13
- physical security
  - access lists, 244
  - fences, 244
  - guards, 245
  - hardware locks, 241–242
  - importance of, 341
  - mantraps, 246–252
  - proximity readers, 242–244
  - video surveillance, 245–246
- PII (personally identifying information)
  - defined, 497
  - overview, 126–127
  - privacy policy, 113
- PIN for lock screen, 354
- ping utility, 163
- Pinterest security policies, 122
- PIV (Personal Identification Verification) cards, 422
- plain old telephone service (POTS) lines, 89
- plaintext, 373
- platform as a service (PaaS), 94, 497
- plus symbol ( + ), 294
- Point-to-Point Protocol (PPP), 87
- Point-to-Point Tunneling Protocol (PPTP), 88
- policies
  - acceptable use policies, 115
  - defined, 497
  - job rotation, 115–116
  - least privilege, 116–117
  - mandatory vacations, 115–116
  - mobile device-specific, 353
  - overview, 111–112
  - privacy policy, 113–114
  - security policy, 113
  - separation of duties, 116
- Pony Express. *See* Pwnie Express
- POP (Post Office Protocol), 82
- pop-up blockers, 336–337, 497
- portable storage devices
  - avoiding malware, 323
  - physical threats, 342
- ports
  - blocking unneeded, 305
  - disabling in hardening process, 222
  - disabling unnecessary, 214–216
  - firewalls and, 42
  - overview, 83–84
  - scanners, 324
  - scanning, 497
    - overview, 261
    - for vulnerabilities, 263–265
  - securing in routers and switches, 98
- post-incident phase of incident response, 24–25
- Post Office Protocol (POP), 82
- POTs (plain old telephone service) lines, 89
- power level controls, 103, 497
- Power Pwn, 273
- PPP (Point-to-Point Protocol), 87
- PPTP (Point-to-Point Tunneling Protocol), 88
- preparation phase of incident response, 20–21
- prerequisites for exam, xx
- presence check, 295
- preset locks, 242
- pretexting technique, social engineering, 189
- Pretty Good Privacy (PGP), 468–470, 497
- prevention vs. detection, 245
- preventive controls, 13
- privacy policy, 113–114
- privacy screen film, 342
- private branch exchange (PBX), 89
- private key, 456
- privilege creep, 117, 443, 497
- privilege escalation, 162–163
- privileges, user account
  - centralized vs. decentralized management of, 443–448
  - group-based privilege management, 442
  - role-based privilege management, 442
  - user-assigned privilege management, 444–448
  - user-based privilege management, 442
- procedures, 111, 497
- Protected Extensible Authentication Protocol (PEAP), 102, 497
- protocol analyzers
  - defined, 262, 497
  - overview, 57–58
  - scanning for vulnerabilities, 261–262

protocols  
 firewalls and, 42–43  
 overview, 77–83  
 ports, 83–84

proximity cards/readers, 242–244, 497

proxy, 497

proxy servers, 51

pseudorandom session IDs, 299

public information, 125

public-key infrastructure  
 asymmetric cryptography, 456  
 certificate revocation lists, 478  
 digital certificates, 476–478  
 key escrow, 478  
 key recovery, 478  
 overview, 476  
 SSL encryption, 481

public relations group  
 and incident response communications, 25  
 staffing, 17

Pwnie Express, 273

Pwn Plug, 273

## Q

QKD (Quantum Key Distribution), 470

QoS (quality of service), 47

qualitative risk assessment, 6

quantitative risk assessment, 7–9

Quantum Key Distribution (QKD), 470

quid pro quo technique, social engineering, 189

quotation mark ( " ), 294

## R

RACE Integrity Primitives Evaluation Message Digest (RIPEMD), 472

radio frequency ID (RFID), 421

RADIUS (Remote Authentication Dial-In User Service)  
 authentication using, 423–424  
 defined, 497

RAID (redundant array of independent disks)  
 and backups, 143  
 defined, 498  
 overview, 142

ransomware, 153, 288, 321, 497

RA (registration authority), 477

rating risks, 6

RAT (remote administration tool), 156, 498

RBAC (role-based access control), 117, 435, 437–438, 498

RBLs (Real-time Blackhole Lists), 59

RC4 algorithm  
 defined, 497  
 overview, 467

RDN (relative distinguished name), 427

reading logs, 227

Real-time Blackhole Lists (RBLs), 59

real-time scanning, 327–328

reauthentication, 301

recovery  
 full-disk encryption, 382  
 phase of incident response, 22–24  
 of public key, 478

recovery point objective (RPO), 138, 498

recovery sites, disaster  
 cold sites, 143  
 hot sites, 143  
 warm sites, 143

recovery time objective (RTO), 138, 498

Red Hat Linux, 234

redundancy  
 and single points of failure, 133–134  
 for disks, 142–143  
 hardware, 141  
 for incident response team, 16  
 routers and, 46  
 for servers, 141

redundant array of independent disks. *See* RAID

reflected XSS, 170, 498

refresher training, 118

regional Internet registries (RIRs), 71

registration authority (RA), 477

relative distinguished name (RDN), 427

relative operating characteristic (ROC), 418

relying parties, 429

remediation, 209, 280–285

remote access  
 malware, 324  
 and network segmentation, 87–89  
 Remote Access Services, 89  
 VPNs, 87–89

Remote Access Services, 89

remote administration tool (RAT), 156, 498

- Remote Authentication Dial-In User Service. *See* RADIUS
- remote wipe, 358–359, 498
- removable media
  - defined, 498
  - encrypting, 388–390
- renaming accounts, 221
- repeaters, 48
- replay attack
  - defined, 498
  - overview, 177
- reporting. *See also* monitoring
  - for penetration testing, 280
  - in UTM devices, 62
- Requests for Comment (RFCs), 103
- restoring systems, 209
- reverse proxies, 51
- RFCs (Requests for Comment), 103
- RFID (radio frequency ID), 421
- RIPEDM (RACE Integrity Primitives Evaluation Message Digest), 472
- RIRs (regional Internet registries), 71
- risk, 4, 498
- risk acceptance, 11, 498
- risk avoidance, 9, 498
- risk-based assessments
  - overview, 256
  - threat assessments, 257
  - vulnerability assessments, 258
- Risk chart, 260
- risk deterrence, 10–11, 498
- risk equation, 498
- risk management. *See also* incident response
  - assessing
    - likelihood and impact, 5
    - overview, 4–5
    - qualitative risk assessment, 6
    - quantitative risk assessment, 7–9
  - CIA triad
    - availability, 3–4
    - confidentiality, 3
    - integrity, 3
    - overview, 2
  - cloud computing services, 8
  - DAD triad
    - alteration, 3
    - denial, 3–4
    - disclosure, 3
    - overview, 2
  - managing
    - risk acceptance, 11
    - risk avoidance, 9
    - risk deterrence, 10–11
    - risk mitigation, 10
    - risk transference, 9–10
  - security controls
    - management controls, 13
    - operational controls, 12–13
    - overview, 12
    - technical controls, 12
  - staffing, 17
  - virtualization, 10
- risk mitigation, 10, 498
- risk transference, 9–10, 498
- Rivest, Shamir, and Adelman algorithm. *See* RSA algorithm
- ROC (relative operating characteristic), 418
- rogue access point, 498
- role-based access control (RBAC), 117, 414, 431, 435
- role-based privilege management, 442
- rootkits
  - anti-virus software, 324
  - defined, 498
  - overview, 157–158
- round-robin distribution, 49–50
- routers
  - 802.1x authentication, 99
  - defined, 498
  - flood guards, 99–100
  - loop protection, 100
  - naming, 46
  - overview, 46–47
  - port security, 98
  - preventing network bridging, 100–101
  - routing switches, 48
  - in UTM devices, 62
  - VLANs, 98
- RPO (recovery point objective), 138, 498
- RSA (Rivest, Shamir, and Adelman) algorithm
  - defined, 498
  - overview, 468
- RTO (recovery time objective), 138, 498
- rule-based management, 95
- ruleset, 498
- rules, firewall
  - effectivity of firewalls, 45
  - overview, 41

## S

- SaaS (software as a service), 94, 499
- Safe Harbor program, 114
- safes, 345–347
- Salinity virus, 325
- SAML (Security Assertion Markup Language)
  - authentication using, 430–431
  - for SSO, 429
- sanitization
  - of mobile devices, 358
  - of user input, 297
- Sarbanes-Oxley Act (SOX), 119
- SAs (Security Associations), 482
- scalability of cryptography, 457–458
- scanning
  - logging results, 262
  - tools for
    - darknets, 270
    - honeynets, 269–270
    - honeypots, 269–270
    - network vulnerability scanners, 265–266
    - port scanners, 263–265
    - protocol analyzers, 261–262
    - sniffers, 261
    - tar pits, 271
    - web application vulnerability scanners, 266–268
- SCCM (System Center Configuration Manager), 209
- scheduling
  - patch updates, 308
  - virus scans, 327
- scope for penetration testing, 276–277
- SCP (Secure Copy Protocol), 78
- screen lock, 354, 498
- screen shots, 33
- ScriptNo plugin, 298
- scripts, disabling, 296, 298
- SDLC (software development life cycle), 291, 499
- secondary confirmation page, 300
- secret information, 125
- secure coding concepts
  - error handling, 292–293
  - exception handling, 292–293
  - input validation, 293–295
  - overview, 290–292
- secure cookies, 167
- Secure Copy Protocol (SCP), 78
- Secure Hash Algorithm (SHA), 379, 472–473
- Secure Shell (SSH), 78, 162, 470, 498
- Secure Sockets Layer. *See* SSL
- Security Assertion Markup Language. *See* SAML
- security association, IPsec, 78
- Security Associations (SAs), 482
- Security Compliance Manager, 207
- Security component, Safe Harbor program, 114
- security controls
  - management controls, 13
  - operational controls, 12–13
  - overview, 12
  - technical controls, 12
- security events, event logs, 228
- security information and event management systems. *See* SIEMs
- security logs
  - defined, 499
  - overview, 232–234
- security, network
  - all-in-one security appliances, 62–66
  - firewalls
    - overview, 41–43
    - web application firewalls (WAF), 44–46
  - IDS
    - false positives, 55–56
    - host-based, 54–55
    - overview, 54
  - IPS
    - false positives, 55–56
    - host-based, 54–55
    - overview, 54
  - load balancers, 49–50
  - overview, 40
  - protocol analyzers, 57–58
  - proxy servers, 51
  - routers, 46–47
  - switches, 47–49
  - topology example, 41
  - traffic inspection
    - malware inspection, 59
    - spam filters, 58–59
    - URL filtering, 59–60
    - web security gateways, 60–61
  - VPN concentrators, 52–53
- security policy
  - overview, 113
  - patch management in, 308
  - and training, 353
  - training, 118

## security through obscurity

- security through obscurity, 453
- segmentation, network
  - overview, 84–87
  - and remote access, 87–89
  - telephony, 89–90
  - and virtualization, 90–95
  - VoIP, 89–90
- self-updating tokens, 420
- semicolon (;), 294
- SEMs (security event management systems). *See* SIEMs
- sensitive information, 125
- separation of duties
  - defined, 499
  - hardening process, 305
  - overview, 116, 433
- servers
  - clusters of, 142
  - redundancy, 141–142
  - XSS attacks, 296
- service level agreement (SLA), 8
- services, disabling unnecessary, 214–216
- service server (SS), 425
- service set identifier (SSID), 103, 183, 499
- service -status-all command, 215
- session cookies, 167
- session key, 481
- settings, application, 301–303
- setup events, event logs, 228
- SFTP (SSH File Transfer Protocol), 78
- shared secret key, 454, 457
- SHA (Secure Hash Algorithm), 379, 472–473
- sheep dip, 390, 499
- shelfware, 135
- Short Message Service (SMS), 239
- shoulder surfing, 188, 342, 499
- SIEMs (security information and event management systems)
  - defined, 499
  - overview, 237–239
- signatures
  - algorithm used by CA, 477
  - biometric systems, 417
  - defined, 54, 499
  - detection for IDS and IPS, 54
- Simple Mail Transfer Protocol (SMTP), 82, 499
- Simple Security Property, Bell-LaPadula, 436
- SIMs (security information management systems). *See* SIEMs
- SIM (subscriber identity module) cards, 352
- single-factor authentication, 414–416
- single loss expectancy (SLE), 7, 499
- single point of failure, 133–134, 499
- single quote ( ' ), 294
- single sign-on. *See* SSO
- sinkholes, 270
- SLA (service level agreement), 8
- slash (/), 71
- SLE (single loss expectancy), 7, 499
- small office/home office (SOHO) networks, 321
- smart cards
  - defined, 499
  - overview, 421
  - tokens based on, 420
- SMS (Short Message Service), 239
- SMTP (Simple Mail Transfer Protocol), 82, 499
- smurf attacks
  - defined, 499
  - overview, 180–181
- sniffers
  - anti-virus software, 324
  - deploying, 57
  - determining packet flow, 58
  - using with hubs, 49
  - scanning for vulnerabilities, 261
  - VoIP and, 58
- social engineering
  - defined, 499
  - email attachments, 193
  - hoaxes, 190
  - overview, 188–189
  - phishing, 190–192
  - spam, 193–194
- social networking
  - avoiding malware, 323
  - training effective use of, 122
- Social Security numbers (SSNs), 7, 118, 127
- software as a service (SaaS), 94, 499
- software-based firewalls, 43
- software development life cycle (SDLC), 291, 499
- software firewall, 338
- software requirements for this book, xxiii
- SOHO (small office/home office) networks, 321
- Solaris system, 163
- solid-state drives (SSDs), 395, 400
- source code review, 288, 499
- SOX (Sarbanes-Oxley Act), 119

- spam
  - filtering, 58–59, 62, 331, 499
  - social engineering attacks, 193–194
- spambot, 331, 499
- span mode, sniffers, 57
- spanning tree protocol (STP), 100
- span ports, 49
- spear phishing, 191, 499
- Special Publication 800-12, 127
- Special Publication 800-61, 24
- spelling and grammar check, 295
- SPIM (spam via instant message), 191, 500
- spoofing
  - defined, 500
  - overview, 175–176
- spyware
  - anti-virus software, 324
  - defined, 500
  - overview, 152
- SQL injection, 172–173, 266, 293, 500
- SQL Slammer, 155, 326
- SQL (Structured Query Language), 172
- SSDs (solid-state drives), 395, 400
- SSH File Transfer Protocol (SFTP), 78
- SSH scanners, 216
- SSH (Secure Shell), 78, 162, 470, 482, 498
- SSID (service set identifier), 103, 183, 499
- SSL Portal VPNs, 89
- SSL (Secure Sockets Layer)
  - acceleration of traffic, 44
  - defined, 498
  - history of, 80
  - load balancers and, 50
  - overview, 481
  - scalability, 458
- SSL Tunnel VPNs, 89
- SSNs (Social Security numbers), 7, 118, 127
- SSO (single sign-on)
  - authentication using, 429
  - defined, 499
- SS (service server), 425
- standards
  - defined, 111, 500
  - for hardening, 203–205
  - vs. policies, 112
- standby servers, 141
- Star Property, Bell-LaPadula, 436
- stateful filtering, 43
- stateful packet inspection, 42, 500
- stateful protocols, 74
- static learning mode, port security, 98
- static NAT, 86
- steganography, 480
- sticky learning mode, port security, 98
- storage devices
  - mobile devices as, 351
  - peripherals as threat to host, 342
- storage-level scan, 329
- stored XSS, 170, 500
- storm control, 100
- Storm virus, 326
- STP (spanning tree protocol), 100
- stream ciphers, 458, 500
- strongbox, 345
- strong passwords, 439
- Structured Query Language (SQL), 172
- studying for exam, xxi–xxii
- Stuxnet attack, 14
- subnets
  - defined, 500
  - overview, 71–72
- subscriber identity module (SIM) cards, 352
- succession planning, 137–138
- Success log entry, Windows Application log, 231
- SUDO command, 265
- supercookie, 168
- supernet, 500
- SuperScan, 326
- surveillance cameras, 33
- SWATing technique, 175
- switch-based flood protection, 100
- switches
  - authentication, 99
  - 802.1x authentication, 99
  - defined, 500
  - flood guards, 99–100
  - loop protection, 100
  - overview, 47–49
  - port security, 98
  - preventing network bridging, 100–101
  - in UTM devices, 62
  - VLANs, 98
- Symantec, 322
- symmetric encryption algorithms
  - 3DES, 464–465
  - AES, 465



## SYN (synchronize)

- vs. asymmetric encryption algorithms, 454–457
- Blowfish, 465–466
- defined, 500
- DES, 460–463
- RC4, 467
- Twofish, 466
- SYN (synchronize), 74
- syslog format, 226
- System Center Configuration Manager (SCCM), 209
- system configuration
  - disabling unnecessary accounts, 220–221
  - disabling unnecessary ports, 214–216
  - disabling unnecessary services, 214–216
  - host firewalls, 216–217
  - overview, 209–210
  - password protection, 219–220
  - patch management methodologies, 212–214
  - protecting administrative interfaces, 218
  - updates, 211–212
- system logs
  - access logs, 234–236
  - application logs, 231–232
  - audit logs, 229
  - event logs, 227–228
  - log rotation, 224–225
  - security logs, 232–234
  - success vs. failure, 229–231
  - time stamps in, 224–225
  - Windows vs. Linux, 226–227
- system requirements for this book, xxii
- system-wide scanning, 328–329

## T

- tabletop simulations, 136
- TACACS (Terminal Access Controller Access-Control System)
  - authentication using, 424–425
  - defined, 500
- tailgating, 121–122, 188, 500
- tampering with evidence, 27
- tap mode, sniffers, 57
- taps, 49
- tar pits, 271
- task activities, 300
- TCPDump, 326
- TCP (Transmission Control Protocol)
  - defined, 500
  - ports, 78
  - stateful protocol, 74
- TCSEC (Trusted Computer System Evaluation Criteria), 435
- Team Cymru, 270
- team, incident response
  - categories needed, 16–18
  - first responder, 14–15
  - overview, 14
  - training, 18–19
- technical controls, 12–13
- technical staff, 16
- telephony, and network segmentation, 89–90
- Telnet, 78, 500
- templates
  - for baseline configuration, 302
  - for hardening, 206–209
- Temporal Key Integrity Protocol (TKIP), 500
- Terminal Access Controller Access-Control System. *See* TACACS
- testing
  - business continuity plan, 135–137
  - new software and configurations, 325
  - patches, 307
  - penetration vulnerability
    - assessment, 279
    - audience, 276–277
    - authority, 276–277
    - black box penetration testing, 274
    - gray box penetration testing, 275
    - methods for, 278–279
    - overview, 275–276
    - planning for, 277
    - remediation, 280–285
    - reporting, 280
    - scope, 276–277
    - target identification, 277–278
    - white box penetration testing, 274
- tethering, 352
- text message alerting, 239
- TGS (ticket granting service), 425
- TGT (ticket granting ticket), 425
- theft, 345
- threats. *See also* attacks and threats
  - defined, 4, 257, 500
  - training awareness, 123–124
  - vs. likelihood, 259–260
  - and vulnerability, 5

- thresholds, monitoring logs for, 240–241
  - ticket granting service (TGS), 425
  - ticket granting ticket (TGT), 425
  - time and expense, tracking, 27–28
  - time-of-day restrictions, 434, 500
  - time stamps
    - in logs, 224–225
    - replay attacks, 177
  - time zones, 224
  - timing detection, 300
  - TKIP (Temporal Key Integrity Protocol), 500
  - TLS (Transport Layer Security), 80, 467, 481, 501
  - Toal virus, 325
  - tokens
    - CAC cards, 421
    - defined, 500
    - overview, 420
    - PIV cards, 422
    - smart cards, 421
  - tools, scanning
    - darknets, 270
    - honeynets, 269–270
    - honeypots, 269–270
    - network vulnerability scanners, 265–266
    - port scanners, 263–265
    - protocol analyzers, 261–262
    - sniffers, 261
    - tarpits, 271
    - web application vulnerability scanners, 266–268
  - top-down approach, 308
  - topologies, network, 41
  - top secret information, 125
  - tower triangulation, 360
  - TPM only option, 381
  - TPM (Trusted Platform Module), 380, 395–396, 501
  - tracking cookies, 167
  - traffic
    - decreasing using firewalls, 40
    - inspecting
      - malware inspection, 59
      - spam filters, 58–59
      - URL filtering, 59–60
      - web security gateways, 60–61
  - training
    - clean desk policy, 121
    - compliance training, 119
    - data handling and disposal, 120–121
    - incident response team, 18–19
    - P2P computing, 123
    - passwords, 120
    - personally owned devices, 122
    - and security policy, 353
    - security policy training, 118
    - social networking, 122
    - tailgating prevention, 121–122
    - threat awareness, 123–124
  - transference of risk, 9–10
  - translucent box testing, 275
  - Transmission Control Protocol. *See* TCP
  - transparent proxies, 51
  - transport encryption, 480
  - Transport Layer Security (TLS), 80, 467, 501
  - trends
    - defined, 501
    - monitoring logs, 240–241
  - Triple DES algorithm. *See* 3DES algorithm
  - trivia questions, 300
  - trojans
    - defined, 501
    - malware, 324
    - overview, 156
  - Trusted Computer System Evaluation Criteria (TCSEC), 435
  - trusted operating system, 501
  - Trusted Platform Module (TPM), 380, 501
  - tunneling proxies, 51
  - Twitter security policies, 122
  - two-factor authentication, 415
  - Twofish algorithm
    - defined, 501
    - overview, 466
  - Type I/II error, 501
- ## U
- UBE (unsolicited bulk email), 331
  - UCE (unsolicited commercial email), 331
  - UDP (User Datagram Protocol), 75, 501
  - unbreakable cipher, 459
  - unchangeable passwords, 220
  - unclassified information, 125
  - Unified threat management (UTM) devices, 62
  - uniqueness check, 295
  - United States Computer Emergency Readiness Team (US-CERT), 26, 94

- United States Secret Service, 26
- Unix, 324
- unmanaged switches, 48
- unnecessary features, 305
- unpatched systems, 213
- unsolicited bulk email, 193
- unsolicited bulk email (UBE), 331
- unsolicited commercial email (UCE), 331
- updates
  - anti-virus, 328
  - defined, 501
  - system configuration for, 211–212
- URLs (uniform resource locators)
  - filtering, 59–60, 501
  - filtering, in UTM devices, 62
  - injection attacks, 321–322, 501
- USB devices
  - encryption on, 398–399
  - tokens based on, 420
- USB only option, 381
- USB with TPM option, 381–382
- US-CERT (United States Computer Emergency Readiness Team), 26, 94
- US Department of Commerce clocks, 32
- user accounts
  - overview, 414
  - passwords, 439–441
  - privileges
    - centralized vs. decentralized management, 443–448
    - group-based privilege management, 442
    - role-based privilege management, 442
    - user-assigned privilege management, 444–448
    - user-based privilege management, 442
- user-assigned privilege management, 444–448
- user authentication as technical control, 12
- user-based privilege management, 442
- user behavior modification, 501
- User Datagram Protocol (UDP), 75, 501
- userID variable, 165
- user password with TPM option, 381
- user password with USB and TPM option, 382
- US Naval Observatory clocks, 32
- UTM (Unified threat management) devices, 62

## V

- vacations, mandatory, 115–116, 434
- validity period, 477
- VeriSign, 477
- Verizon, 53
- video capture, 33
- video surveillance
  - defined, 501
  - physical security, 245–246
- VirtualBox, 325
- virtual cluster, 91
- virtualization
  - attacks, 92, 94
  - cloud computing, 94–95
  - defined, 501
  - hardware requirements for, xxiii
  - overview, 90–92
  - secure virtual data centers, 93–94
- virtual LANs (VLANs), 85, 98, 501
- virtual machines. *See* VM
- virtual patching, 44
- virtual private networks. *See* VPNs
- virus
  - defined, 501
  - hoax, 501
  - overview, 152–154
- Virut virus, 325
- vishing, 191, 502
- VLANs (virtual LANs), 85, 98, 501
- VM escape attack, 10
- VM (virtual machines)
  - hypervisor, 91
  - risks associated with, 10
  - testing anti-virus software, 325
- VMWare, 325
- voice encryption, 359
- voice print systems, 417
- voice/video calls, 352
- VoIP (voice over Internet Protocol)
  - Caller ID spoofing, 175
  - defined, 502
  - mobile apps for, 359
  - and network segmentation, 89–90
  - using QoS prioritization, 47
  - unencrypted traffic for, 58
- volatility. *See* order of volatility
- VPN concentrator, 52–53, 502

- VPNs (virtual private networks)
  - connections for, 482
  - defined, 501
  - overview, 87–89
- vulnerability
  - assessment techniques
    - overview, 258–259
    - threat vs. likelihood, 259–260
  - defined, 4, 502
  - of full-disk encryption, 382–383
  - hardening process, 305
  - penetration testing
    - assessment, 279
    - audience, 276–277
    - authority, 276–277
    - black box penetration testing, 274
    - gray box penetration testing, 275
    - overview, 275–276
    - planning for, 277
    - remediation, 280–285
    - reporting, 280
    - scope, 276–277
    - target identification, 277–278
    - white box penetration testing, 274
  - risk-based assessments
    - overview, 256
    - threat assessments, 257
    - vulnerability assessments, 258
  - scanning for, 502
  - scanning tools
    - darknets, 270
    - honeynets, 269–270
    - honeypots, 269–270
    - network vulnerability scanners, 265–266
    - port scanners, 263–265
    - protocol analyzers, 261–262
    - sniffers, 261
    - tarpits, 271
    - web application vulnerability scanners, 266–268
- war driving, 185–186
- warm sites, 143
- Warning log entry, Windows Application log, 231
- war walking, 186
- Web Application Attack and Audit Framework (w3af), 267
- web application firewalls (WAF), 44–46, 502
- web application security scanners, 266
- web application vulnerability scanners
  - defined, 261, 502
  - using, 266–268
- web attacks
  - cookies, 166–168
  - directory traversal, 169–170
  - header manipulation, 168
  - XSS
    - overview, 170
    - preventing, 171
- web security gateways
  - defined, 502
  - overview, 60–61
- weighted round robin, 50
- well-known ports, 83
- WEP (Wired Equivalent Privacy), 101, 187, 467, 502
- whaling, 191, 502
- white box penetration testing, 274, 502
- whitelisting, 61, 323, 330, 502
- Wi-Fi Protected Access II (WPA2), 502
- Wi-Fi Protected Access (WPA), 102, 467, 502
- WikiLeaks website, 3
- Windows
  - Application log, 231
  - Event Viewer, 228
  - logs in, 226–227
- Windows Defender Offline, 327
- WinDump, 326
- WinZIP, 479
- Wired Equivalent Privacy (WEP), 101, 187, 467, 502
- wireless attacks
  - packet sniffing, 186–188
  - war driving, 185–186
- wireless protocols
  - common settings, 103–104
  - overview, 101–103
- Wireshark tool, 31
- witnesses, interviewing, 27
- workarounds, 211

## W

- w3af (Web Application Attack and Audit Framework), 267
- WAF (web application firewalls), 44–46, 502
- war biking, 186
- war chalking, 186

## worms

### worms

- defined, 502
  - malware, 324
  - overview, 154–155
- WPA2 (Wi-Fi Protected Access II), 356, 502
- WPA (Wi-Fi Protected Access), 102, 467, 502

## X

- Xmas attacks, 181–182, 502
- XML injection, 174, 293, 502
- XOR operation, 461
- XSRF (cross-site request forgery)
- and cookies, 168
  - defined, 491
  - input validation, 293
  - online resources, 299
  - overview, 297–301
- XSS (cross-site scripting)
- and cookies, 168
  - defined, 491
  - input validation, 293
  - online resources, 297
  - overview, 170, 296–297
  - preventing, 171
  - web application firewalls, 44
- XTACACS, 502

## Z

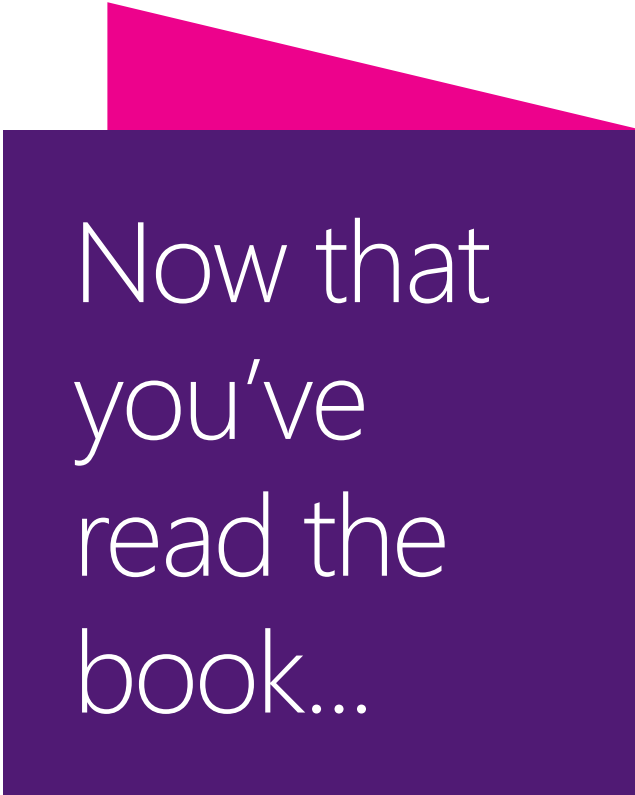
- zero-day attacks
- defined, 123, 288, 502
  - and deny by default concept, 323
  - overview, 164–165
- Zeus banking trojan, 299
- zombies
- cookies, 167
  - defined, 502
  - overview, 156–157

# About the authors

**DAVID SEIDL** is the Director of Information Security at the University of Notre Dame, where he leads the university's dedicated information security team. He also serves as a concurrent instructor for the Mendoza College of Business, where he teaches a popular networking and security course. David has been recognized as a leader in the security industry, receiving Network Computing's Security Seven award in 2013 for his contributions to higher education information security. David holds the CISSP, GCIH, and GPEN certifications, as well as a master's degree in Information Security.

**MIKE CHAPPLE**, Ph.D., is Senior Director for Enterprise Support Services at the University of Notre Dame. In this role, he oversees the information security, IT architecture, project management, strategic planning, and communications functions for the Office of Information Technologies. Mike also serves as a concurrent assistant professor in the university's Computer Applications Department, where he teaches an undergraduate course on information security. He is a technical editor for *Information Security* magazine and has written several books, including *Information Security Illuminated* (Jones and Bartlett, 2004), *SQL Server 2008 for Dummies* (Wiley, 2008), and the *CISSP Study Guide 6th Edition* (Sybex, 2012). Mike earned both his bachelor's and doctoral degrees from Notre Dame in computer science and engineering. He also holds an MS in computer science from the University of Idaho and an MBA from Auburn University. You can reach Mike by email at [mike@chapple.org](mailto:mike@chapple.org).

**JAMES MICHAEL STEWART** has been working with computers and technology for nearly 30 years. His work focuses on security, certification, and various operating systems. Recently, Michael has been teaching job skill and certification courses, such as CISSP, ethical hacking/penetration testing, computer forensics, and CompTIA Security+. He is the primary author of the *CISSP Study Guide 6th Edition* (Sybex, 2012), the *Security+ Review Guide 2nd Edition (SY0-301)* (Sybex, 2011), and *Network Security, Firewalls, and VPNs* (Jones & Bartlett Learning, 2010). Michael has also contributed to many other security-focused materials, including exam preparation guides, practice exams, DVD video instruction, and courseware. In addition, Michael has co-authored numerous books on other security, certification, and administration topics. He has developed certification courseware and training materials as well as presented these materials in the classroom. Michael holds a variety of certifications, including CISSP, CEH, CHFI, and CompTIA Security+. Michael graduated in 1992 from the University of Texas at Austin with a bachelor's degree in philosophy. Despite his degree, his computer knowledge is self-acquired, based on seat-of-the-pants, hands-on, "street smarts" experience. You can reach Michael by email at [michael@impactonline.com](mailto:michael@impactonline.com).



Now that  
you've  
read the  
book...

Tell us what you think!

Was it useful?

Did it teach you what you wanted to learn?

Was there room for improvement?

**Let us know at <http://aka.ms/tellpress>**

Your feedback goes directly to the staff at Microsoft Press,  
and we read every one of your responses. Thanks in advance!



# Practice. Practice. Practice. **Pass.**

## Get more practice with MeasureUp® & ace the exam!

You've practiced — but have you practiced enough? The disk included with this book has dozens of quality questions from the publisher to get you started. MeasureUp offers additional practice tests with more than 100 new and different questions at MeasureUp.com. And when you use our practice test you'll pass — guaranteed.

- Performance-based simulation questions – similar to the ones found on Microsoft exams – are available online and via download.
- Study Mode helps you review the material with detailed answers and references to help identify areas where you need more study.
- Certification Mode simulates the timed test environment.

Get certified today! Purchase your complete practice test at [www.measureup.com](http://www.measureup.com).

For tips on installing the CD software located in this Training Kit, visit the FAQ section at MeasureUp.com. For questions about the content, or the physical condition of the CD, visit [microsoft.com/learning/en/us/training/format-books-support.aspx](http://microsoft.com/learning/en/us/training/format-books-support.aspx).

## Save 20% on MeasureUp Practice Tests!

Prepare for your **IT Pro**, **Developer** or **Office** certification exams with MeasureUp Practice Tests and you'll be ready to pass, we guarantee it. Save 20% on MeasureUp Practice Tests when you use this coupon code at checkout:

Coupon Code: **MSP020112**

[www.measureup.com](http://www.measureup.com)

\*excludes VMware



**MEASUREUP**<sup>®</sup>  
Powered by Certiport