

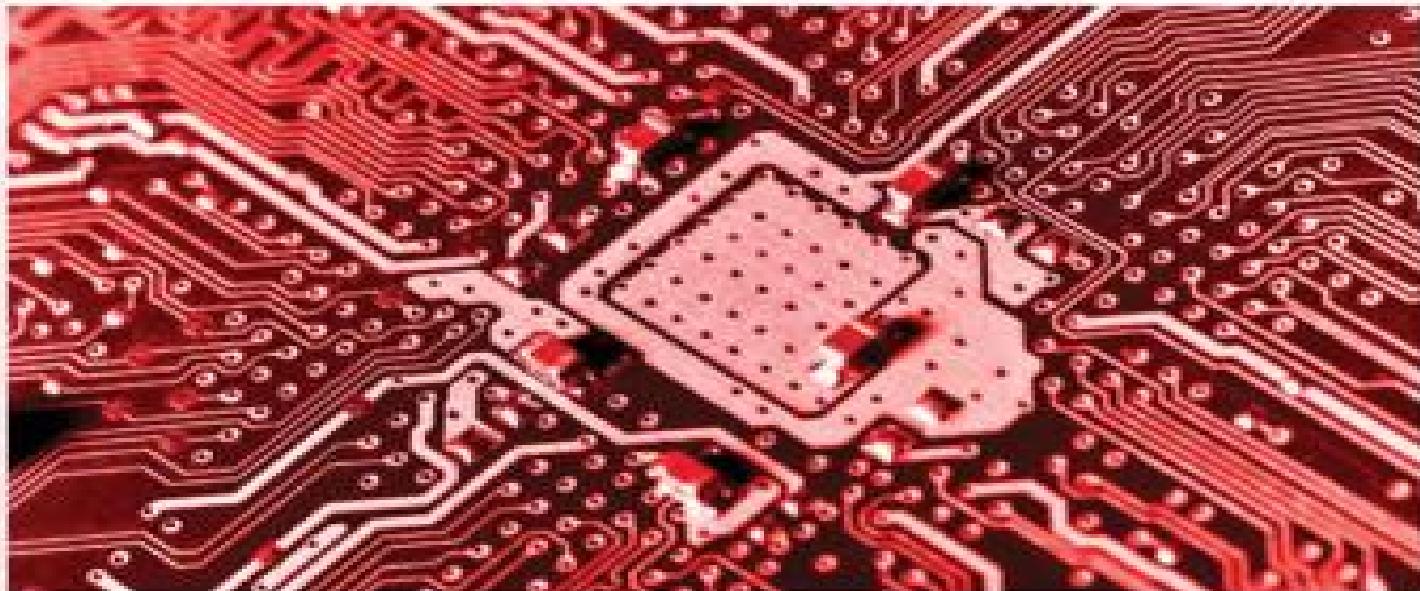
ComptIA

SECURITY+

Get Certified Get Ahead

SY0-601 Study Guide

- Real-world examples of security principles in action
- Over 300 realistic practice test questions with in-depth explanations
- Free access to online labs and additional practice test questions
- 100 percent coverage of all ComptIA Security+ SY0-601 exam objectives
- Save 10 percent on your exam voucher
Access to coupon inside



Darril Gibson

ComptIA A+, Network+, Security+,
CASP, (ISC)2 SSCP, CISSP

CompTIA Security+
Get Certified Get Ahead
SY0-601 Study Guide

Darril Gibson

CompTIA Security+: Get Certified Get Ahead SY0-601 Study Guide 2nd Edition
Copyright © 2020 by Darril Gibson

All rights reserved.

Printed in the United States of America.

No part of this book may be used or reproduced in any manner whatsoever without written permission except in the case of brief quotations embodied in critical articles and review. For information, contact YCDA, LLC

1124 Knights Bridge Lane,
Virginia Beach, VA, 23455

PDF versions of this book are not authorized.

YCDA, LLC books may be purchased for educational, business, or sales promotional use. For information, please contact Darril Gibson at darril@gcgpremium.com.

Copy editor: Karen Annett

Technical editors: Neil Castrence, Steve Johnson

Proofreader: Karen Annett

Project Manager: Jaena Nerona

Dedication

To my wife, who, even after 30 years of marriage, continues to remind me how wonderful life can be if you're in a loving relationship. Thanks for sharing your life with me.

Acknowledgments

A single person can't do books of this size and depth, and I'm grateful for the many people who helped me put this book together. First, thanks to my wife. She has provided me immeasurable support throughout this project.

Jaena Nerona, the project manager, did an outstanding job tracking the project from beginning to end. She helped with quality control along with keeping everything on track.

The technical editors, Steve Johnson and Neil Castrence, provided some great feedback throughout this book's creation.

Last, I'm incredibly grateful for all the effort Karen Annett put into this project. She's an excellent copy editor and proofer, and the book is tremendously better due to all of her work.

While I certainly appreciate everyone's feedback, I want to stress that any errors that may have snuck into this book are entirely my fault and not a reflection on anyone who helped. I always strive to identify and remove every error, but they still seem to sneak in.

Special thanks to:

- Chief Wiggum for bollards installation
- Nelson Muntz for personal physical security services
- Martin Prince for educating us about downgrade attacks
- Comp-Global-Hyper-Mega-Net for intermittent HTTP services
- Edna Krabapple for her thoughtful continuing education lessons
- Apu Nahasapeemapetilon for technical advice on secure coding concepts
- Moe Szyslak for refreshments and uplifting our spirits with his talks about RATs

About the Author

Darril Gibson is the CEO of YCDA, LLC (short for You Can Do Anything). He has contributed to more than 40 books as the author, co-author, or technical editor. Darril regularly writes, consults, and teaches on a wide variety of technical and security topics and holds several certifications, including CompTIA A+, Network+, Security+, CASP, (ISC)2 SSCP, and CISSP.

In response to repeated requests, Darril created the <https://gcp premiumpass.com/> site to provide study materials for certification exams, including the CompTIA Security+ exam. Darril regularly posts blog articles at <https://blogs.getcertifiedgetahead.com/>, and uses the site to help people stay abreast of certification exam changes. You can contact him through the contact us page on [gcp premiumpass.com \(https://gcp premiumpass.com/contact-us/\)](https://gcp premiumpass.com/contact-us/).

Additionally, Darril publishes the Get Certified Get Ahead newsletter. This weekly newsletter typically lets readers know about new blog posts, updates related to some certification exams, and current cybersecurity issues. You can sign up at <https://eepurl.com/g44Of>.

Darril lives in Virginia Beach with his wife. Whenever possible, they escape to a small cabin in the country on over twenty acres of land that continue to provide them with peace, tranquility, and balance.

Table of Contents

[**Dedication**](#)

[**Acknowledgments**](#)

[**About the Author**](#)

[**Table of Contents**](#)

[**Introduction**](#)

[Who This Book Is For](#)

[About This Book](#)

[Appendices](#)

[How to Use This Book](#)

[Conventions](#)

[Remember This](#)

[Vendor Neutral](#)

[Free Online Resources](#)

[Additional Web Resources](#)

[Assumptions](#)

[Set a Goal](#)

[**About the Exam**](#)

[Passing Score](#)

[Exam Prerequisites](#)

[Beta Questions](#)

[Exam Format](#)

[Question Types](#)

[Multiple Choice](#)

[Performance-Based Questions](#)

[Question Complexity](#)

[Practice Test Questions Strategy](#)

[Exam Test Provider](#)

Voucher Code for 10 Percent Off

Exam Domains

Objective to Chapter Map

1.0 Threats, Attacks and Vulnerabilities

2.0 Architecture and Design

3.0 Implementation

4.0 Operations and Incident Response

5.0 Governance, Risk, and Compliance

Recertification Requirements

601 Pre-Assessment Exam

Pre-Assessment Exam Answers

Chapter 1 Mastering Security Basics

Understanding Core Security Goals

What Is a Use Case?

Ensure Confidentiality

Encryption

Access Controls

Provide Integrity

Increase Availability

Redundancy and Fault Tolerance

Scalability and Elasticity

Patching

Understanding Resiliency

Resource Versus Security Constraints

Introducing Basic Risk Concepts

Understanding Security Controls

Managerial Controls

Operational Controls

Technical Controls

[Control Types](#)

[Preventive Controls](#)

[Detective Controls](#)

[Corrective and Recovery Controls](#)

[Physical Controls](#)

[Deterrent Controls](#)

[Compensating Controls](#)

[Response Controls](#)

[Combining Control Categories and Types](#)

[Using Command-Line Tools](#)

[Network Reconnaissance and Discovery](#)

[Ping](#)

[Using Ping to Check Name Resolution](#)

[Beware of Firewalls](#)

[Using Ping to Assess Organizational Security](#)

[hping](#)

[Ipconfig and ifconfig](#)

[Netstat](#)

[Tracert and traceroute](#)

[Pathping](#)

[Arp](#)

[Linux and LAMP](#)

[cat Command](#)

[grep Command](#)

[head Command](#)

[tail Command](#)

[logger Command](#)

[journalctl Command](#)

[chmod Command](#)

[Understanding Logs](#)

[Windows Logs](#)

Network Logs

Centralized Logging Methods

SIEM Systems

Syslog

Linux Logs

Chapter 1 Exam Topic Review

Chapter 1 Practice Questions

Chapter 1 Practice Question Answers

Chapter 2 Understanding Identity and Access Management

Exploring Authentication Management

Comparing Identification and AAA

Comparing Authentication Factors

Something You Know

Something You Have

Something You Are

Two-Factor and Multifactor Authentication

Authentication Attributes

Authentication Log Files

Managing Accounts

Credential Policies and Account Types

Privileged Access Management

Require Administrators to Use Two Accounts

Prohibiting Shared and Generic Accounts

Disablement Policies

Time-Based Logins

Account Audits

Comparing Authentication Services

Single Sign-On

[Kerberos](#)

[SSO and a Federation](#)

[SAML](#)

[SAML and Authorization](#)

[OAuth](#)

[OpenID and OpenID Connection](#)

[Comparing Access Control Schemes](#)

[Role-Based Access Control](#)

[Using Roles Based on Jobs and Functions](#)

[Documenting Roles with a Matrix](#)

[Establishing Access with Group-Based Privileges](#)

[Rule-Based Access Control](#)

[Discretionary Access Control](#)

[Filesystem Permissions](#)

[SIDs and DACLs](#)

[The Owner Establishes Access](#)

[Mandatory Access Control](#)

[Labels and Lattice](#)

[Establishing Access](#)

[Attribute-Based Access Control](#)

[Conditional Access](#)

[Chapter 2 Exam Topic Review](#)

[Chapter 2 Practice Questions](#)

[Chapter 2 Practice Question Answers](#)

[Chapter 3 Exploring Network Technologies and Tools](#)

[Reviewing Basic Networking Concepts](#)

[Basic Networking Protocols](#)

[Implementing Protocols for Use Cases](#)

[Voice and Video Use Case](#)

[File Transfer Use Case](#)

[Email and Web Use Cases](#)

[Directory Services and LDAPS](#)

[Remote Access Use Case](#)

[OpenSSH](#)

[Time Synchronization Use Case](#)

[Network Address Allocation Use Case](#)

[Domain Name Resolution Use Case](#)

[Subscription Services Use Case](#)

[Quality of Service](#)

Understanding Basic Network Devices

[Switches](#)

[Security Benefit of a Switch](#)

[Port Security](#)

[Broadcast Storm and Loop Prevention](#)

[Bridge Protocol Data Unit Guard](#)

[Routers](#)

[Routers and ACLs](#)

[Deny Implicit Deny](#)

[The Route Command and Route Security](#)

[Firewalls](#)

[Host-Based Firewalls](#)

[Software Versus Hardware Firewalls](#)

[Stateless Firewall Rules](#)

[Stateful Versus Stateless](#)

[Web Application Firewall](#)

[Next-Generation Firewall](#)

Implementing Network Designs

[Intranet Versus Extranet](#)

[Screened Subnet](#)

Network Address Translation Gateway

Physical Isolation and Air Gaps

Logical Separation and Segmentation

Isolating Traffic with a VLAN

East-West Traffic

Zero Trust

Network Appliances

Proxy Servers

Caching Content for Performance

Transparent Proxy Versus Non-transparent Proxy

Reverse Proxy

Unified Threat Management

Jump Server

Security Implications of IPv6

Summarizing Routing and Switching Use Cases

Chapter 3 Exam Topic Review

Chapter 3 Practice Questions

Chapter 3 Practice Question Answers

Chapter 4 Securing Your Network

Exploring Advanced Security Devices

Understanding IDSs and IPSs

HIDS

NIDS

Sensor and Collector Placement

Detection Methods

Data Sources and Trends

Reporting Based on Rules

False Positives Versus False Negatives

IPS Versus IDS—Inline Versus Passive

Honeypots

[Honeynets](#)

[Honeyfile](#)

[Fake Telemetry](#)

[Securing Wireless Networks](#)

[Reviewing Wireless Basics](#)

[Band Selection and Channel Overlaps](#)

[Access Point SSID](#)

[Enable MAC Filtering](#)

[Site Surveys and Footprinting](#)

[Wireless Access Point Placement](#)

[Wireless Cryptographic Protocols](#)

[WPA2 and CCMP](#)

[Open, PSK, and Enterprise Modes](#)

[WPA3 and Simultaneous Authentication of Equals](#)

[Authentication Protocols](#)

[IEEE 802.1X Security](#)

[Controller and Access Point Security](#)

[Captive Portals](#)

[Understanding Wireless Attacks](#)

[Disassociation Attacks](#)

[Wi-Fi Protected Setup](#)

[Rogue Access Point](#)

[Evil Twin](#)

[Jamming Attacks](#)

[IV Attacks](#)

[Near Field Communication Attacks](#)

[RFID Attacks](#)

[Bluetooth Attacks](#)

[Wireless Replay Attacks](#)

[War Driving and War Flying](#)

[Using VPNs for Remote Access](#)

[VPNs and VPN Appliances](#)

[Remote Access VPN](#)

[IPsec as a Tunneling Protocol](#)

[SSL/TLS as a Tunneling Protocol](#)

[Split Tunnel Versus Full Tunnel](#)

[Site-to-Site VPNs](#)

[Always-On VPN](#)

[L2TP as a Tunneling Protocol](#)

[HTML5 VPN Portal](#)

[Network Access Control](#)

[Host Health Checks](#)

[Agent Versus Agentless NAC](#)

[Authentication and Authorization Methods](#)

[PAP](#)

[CHAP](#)

[RADIUS](#)

[TACACS+](#)

[AAA Protocols](#)

[**Chapter 4 Exam Topic Review**](#)

[**Chapter 4 Practice Questions**](#)

[**Chapter 4 Practice Question Answers**](#)

[**Chapter 5 Securing Hosts and Data**](#)

[**Summarize Virtualization Concepts**](#)

[Thin Clients and Virtual Desktop Infrastructure](#)

[Containers](#)

[VM Escape Protection](#)

[VM Sprawl Avoidance](#)

[Replication](#)

[Snapshots](#)

[Non-Persistence](#)

Implementing Secure Systems

Endpoint Security

Hardening Systems

Configuration Management

Secure Baseline and Integrity Measurements

Using Master Images for Baseline Configurations

Patch Management

Change Management Policy

Application Approved Lists and Block Lists

Application Programming Interfaces

Microservices and APIs

FDE and SED

Boot Integrity

Boot Security and UEFI

Trusted Platform Module

Hardware Security Module

Protecting Data

Data Loss Prevention

Rights Management

Removable Media

Data Exfiltration

Protecting Confidentiality with Encryption

Database Security

Summarizing Cloud Concepts

Software as a Service

Platform as a Service

Infrastructure as a Service

Anything as a Service

Cloud Deployment Models

Managed Security Service Provider

Cloud Service Provider Responsibilities

Cloud Security Controls

On-Premises Versus Off-Premises

On-Premises

Off-Premises

Cloud Access Security Broker

Cloud-Based DLP

Next-Generation Secure Web Gateway

Firewall Considerations

Infrastructure as Code

Edge and Fog Computing

Cloud Security Alliance

Deploying Mobile Devices Securely

Deployment Models

Connection Methods and Receivers

Mobile Device Management

Mobile Device Enforcement and Monitoring

Unauthorized Software

Messaging Services

Hardware Control

Unauthorized Connections

SEAndroid

Exploring Embedded Systems

Understanding Internet of Things

ICS and SCADA Systems

IoT and Embedded Systems

Security Implications of Embedded Systems

Embedded System Constraints

Communication Considerations

Chapter 5 Exam Topic Review

Chapter 5 Practice Questions

Chapter 5 Practice Question Answers

Chapter 6 Comparing Threats, Vulnerabilities, and Common Attacks

Understanding Threat Actors

Attack Vectors

Shadow IT

Determining Malware Types

Viruses

Worms

Logic Bombs

Backdoors

Trojans

Remote Access Trojan

Keyloggers

Spyware

Rootkit

Bots and Botnets

Command and Control

Ransomware and Cryptomalware

Potentially Unwanted Programs

Fileless Virus

Potential Indicators of a Malware Attack

Recognizing Common Attacks

Social Engineering

Impersonation

Shoulder Surfing

Tricking Users with Hoaxes

Tailgating and Access Control Vestibules

Dumpster Diving

Zero-Day Vulnerabilities

Watering Hole Attacks
Typo Squatting
Eliciting Information
Pretexting and Prepending
Identity Theft and Identity Fraud
Invoice Scams
Credential Harvesting
Reconnaissance
Influence Campaigns
Attacks via Email and Phone
Spam
Spam over Internet Messaging
Phishing
Spear Phishing
Whaling
Vishing
Smishing
One Click Lets Them In

Blocking Malware and Other Attacks

Spam Filters
Antivirus and Anti-Malware Software

Signature-Based Detection

Heuristic-Based Detection

File Integrity Monitors

Cuckoo Sandbox

Why Social Engineering Works

Authority

Intimidation

Consensus

Scarcity

Urgency

Familiarity

Trust

Threat Intelligence Sources

Research Sources

Chapter 6 Exam Topic Review

Chapter 6 Practice Questions

Chapter 6 Practice Question Answers

Chapter 7 Protecting Against Advanced Attacks

Understanding Attack Frameworks

Cyber Kill Chain

Diamond Model of Intrusion Analysis

MITRE ATT&CK

Identifying Network Attacks

DoS Versus DDoS

SYN Flood Attacks

Spoofing

On-Path Attacks

Secure Sockets Layer Stripping

Layer 2 Attacks

ARP Poisoning Attacks

MAC Flooding

MAC Cloning

DNS Attacks

DNS Poisoning Attacks

Pharming Attack

URL Redirection

Domain Hijacking

Domain Reputation

DNS Sinkhole

DNS Log Files

Replay Attacks and Session Replays

Summarizing Secure Coding Concepts

OWASP

Code Reuse and Dead Code

Third-Party Libraries and SDKs

Input Validation

Client-Side and Server-Side Input Validation

Other Input Validation Techniques

Avoiding Race Conditions

Proper Error Handling

Code Obfuscation and Camouflage

Software Diversity

Outsourced Code Development

Data Exposure

HTTP Headers

Secure Cookie

Code Signing

Analyzing and Reviewing Code

Software Version Control

Secure Development Environment

Database Concepts

Normalization

SQL Queries

Provisioning and Deprovisioning

Integrity Measurement

Web Server Logs

Using Scripting for Automation

Identifying Malicious Code and Scripts

PowerShell

Bash

Python

Macros

Visual Basic for Applications (VBA)

OpenSSL

SSH

Identifying Application Attacks

Zero-Day Attacks

Memory Vulnerabilities

Memory Leak

Buffer Overflows and Buffer Overflow Attacks

Integer Overflow

Pointer/Object Dereference

Other Injection Attacks

Dynamic Link Library Injection

Lightweight Directory Access Protocol Injection

Extensible Markup Language Injection

Directory Traversal

Cross-Site Scripting

Cross-Site Request Forgery

Server-Side Request Forgeries

Client-Side Request Forgeries

Driver Manipulation

Artificial Intelligence and Machine Learning

AI and ML in Cybersecurity

Adversarial Artificial Intelligence

Tainted Data for Machine Learning

Security of Machine Learning Algorithms

Chapter 7 Exam Topic Review

Chapter 7 Practice Questions

Chapter 7 Practice Question Answers

Chapter 8 Using Risk Management Tools

Understanding Risk Management

Threats

Risk Types

Vulnerabilities

Risk Management Strategies

Risk Assessment Types

Risk Analysis

Supply Chain Risks

Threat Hunting

Comparing Scanning and Testing Tools

Checking for Vulnerabilities

Password Crackers

Network Scanners

Vulnerability Scanning

Credentialed Versus Non-Credentialed

Configuration Review

Penetration Testing

Rules of Engagement

Reconnaissance

Footprinting Versus Fingerprinting

Initial Exploitation

Persistence

Lateral Movement

Privilege Escalation

Pivoting

Known, Unknown, and Partially Known Testing Environments

Cleanup

Bug Bounty Programs

Intrusive Versus Non-Intrusive Testing

Exercise Types

Capturing Network Traffic

[Packet Capture and Replay](#)

[TcpREPLAY and Tcpdump](#)

[NetFlow, sFlow, and IPFIX](#)

Understanding Frameworks and Standards

[Key Frameworks](#)

[Risk Management Framework](#)

[Reference Architecture](#)

[Exploitation Frameworks](#)

[Benchmarks and Configuration Guides](#)

Chapter 8 Exam Topic Review

[Chapter 8 Practice Questions](#)

[Chapter 8 Practice Question Answers](#)

Chapter 9 Implementing Controls to Protect Assets

Comparing Physical Security Controls

[Securing Door Access with Cards](#)

[Comparing Locks](#)

[Physical Locks](#)

[Physical Cipher Locks](#)

[Biometric Locks](#)

[Cable Locks](#)

[Increasing Security with Personnel](#)

[Monitoring Areas with Cameras](#)

[Sensors](#)

[Fencing, Lighting, and Alarms](#)

[Securing Access with Barricades](#)

[Using Signage](#)

[Drones](#)

[Asset Management](#)

[Implementing Diversity](#)

Creating Secure Areas

Air Gap

Vaults

Faraday Cage

Safes

Hot and Cold Aisles

Physical Attacks

Malicious Universal Serial Bus (USB) Cable

Malicious Flash Drive

Card Skimming and Card Cloning

Fire Suppression

Protected Cable Distribution

Adding Redundancy and Fault Tolerance

Single Point of Failure

Disk Redundancies

RAID-0

RAID-1

RAID-5 and RAID-6

RAID-10

Disk Multipath

Server Redundancy and High Availability

Active/Active Load Balancers

Active/Passive Load Balancers

NIC Teaming

Power Redundancies

Protecting Data with Backups

Backup Media

Online Versus Offline Backups

Comparing Backup Types

Full Backups

Restoring a Full Backup

Differential Backups

Order of Restoration for a Full/Differential Backup Set

Incremental Backups

Order of Restoration for a Full/Incremental Backup Set

Choosing Full/Incremental or Full/Differential

Snapshot and Image Backups

Copy Backup

Testing Backups

Backups and Geographic Considerations

Comparing Business Continuity Elements

Business Impact Analysis Concepts

Site Risk Assessment

Impact

Recovery Time Objective

Recovery Point Objective

Comparing MTBF and MTTR

Continuity of Operations Planning

Site Resiliency

Restoration Order

Disaster Recovery

Testing Plans with Exercises

Chapter 9 Exam Topic Review

Chapter 9 Practice Questions

Chapter 9 Practice Question Answers

Chapter 10 Understanding Cryptography and PKI

Introducing Cryptography Concepts

Providing Integrity with Hashing

Hash Versus Checksum

[MD5](#)

[Secure Hash Algorithms](#)

[HMAC](#)

[Hashing Files](#)

[Hashing Messages](#)

[Using HMAC](#)

[Hashing Passwords](#)

[Understanding Hash Collisions](#)

[Understanding Password Attacks](#)

[Dictionary Attacks](#)

[Brute Force Attacks](#)

[Spraying Attacks](#)

[Pass the Hash Attacks](#)

[Birthday Attacks](#)

[Rainbow Table Attacks](#)

[Salting Passwords](#)

[Key Stretching](#)

[Providing Confidentiality with Encryption](#)

[Symmetric Encryption](#)

[Block Versus Stream Ciphers](#)

[Common Symmetric Algorithms](#)

[AES](#)

[3DES](#)

[Blowfish and Twofish](#)

[Asymmetric Encryption](#)

[Key Exchange](#)

[The Rayburn Box](#)

[Certificates](#)

[Ephemeral Keys](#)

[Elliptic Curve Cryptography](#)

[Quantum Computing](#)

Quantum Cryptography
Post-Quantum Cryptography
Lightweight Cryptography
Homomorphic Encryption
Key Length
Modes of Operation
Steganography
Audio Steganography
Image Steganography
Video Steganography

Using Cryptographic Protocols

Protecting Email
Signing Email with Digital Signatures
Encrypting Email
S/MIME
HTTPS Transport Encryption
TLS Versus SSL
Encrypting HTTPS Traffic with TLS
Downgrade Attacks on Weak Implementations
Blockchain
Crypto Diversity
Identifying Limitations
Resource Versus Security Constraints
Speed and Time
Size and Computational Overhead
Entropy
Predictability
Weak Keys
Longevity
Reuse
Plaintext Attack

Common Use Cases

Exploring PKI Components

Certificate Authority

Certificate Trust Models

Registration Authority and CSRs

Online Versus Offline CAs

Updating and Revoking Certificates

Certificate Revocation List

Validating a Certificate

Public Key Pinning

Key Escrow

Key Management

Comparing Certificate Types

Comparing Certificate Formats

Chapter 10 Exam Topic Review

Chapter 10 Practice Questions

Chapter 10 Practice Question Answers

Chapter 11 Implementing Policies to Mitigate Risks

Exploring Security Policies

Personnel Policies

Acceptable Use Policy

Mandatory Vacations

Separation of Duties

Least Privilege

Job Rotation

Clean Desk Space

Background Check

Onboarding

Offboarding
Non-Disclosure Agreement
Social Media Analysis
Third-Party Risk Management
Terms of Agreement
Measurement Systems Analysis

Incident Response Policies

Incident Response Plan
Communication Plan
Data Breach Responses
Stakeholder Management
Incident Response Process
Understanding SOAR
Playbooks
Runbooks

Understanding Digital Forensics

Key Aspects of Digital Forensics
Admissibility of Documentation and Evidence
On-Premises Versus Cloud Concerns
Acquisition and Preservation
Order of Volatility
Data Acquisition
Forensic Tools
Electronic Discovery
Data Recovery
Strategic Intelligence and Counterintelligence

Protecting Data

Classifying Data Types
PII and Health Information
Impact Assessment
Data Governance

[Privacy Enhancing Technologies](#)

[Data Masking](#)

[Anonymization](#)

[Pseudo-Anonymization](#)

[Tokenization](#)

[Data Retention Policies](#)

[Data Sanitization](#)

[Training Users](#)

[Computer-Based Training](#)

[Phishing Campaigns](#)

[Phishing Simulations](#)

[Gamification](#)

[Capture the Flag](#)

[Role-Based Awareness Training](#)

[Chapter 11 Exam Topic Review](#)

[Chapter 11 Practice Questions](#)

[Chapter 11 Practice Question Answers](#)

[Post-Assessment Questions](#)

[Post-Assessment Answers](#)

Introduction

Congratulations on your purchase of the *CompTIA Security+: Get Certified Get Ahead Study Guide*. You are one step closer to becoming CompTIA Security+ certified. This certification has helped many individuals get ahead in their jobs and careers, and it can help you get ahead as well.

It is a popular certification within the IT field. One IT hiring manager told me that if a résumé doesn't include the Security+ certification or higher-level security certification, he simply sets it aside. He won't even talk to applicants. That's not the same with all IT hiring managers, but it does help illustrate how important security is within the IT field.

Who This Book Is For

If you’re studying for the CompTIA Security+ exam and want to pass it on your first attempt, this book is for you. It covers 100 percent of the objectives identified by CompTIA for the Security+ exam.

The first target audience for this book is students in CompTIA Security+ classes. My goal is to give students a book they can use to study the relevant and important details of CompTIA Security+ in enough depth for the challenging topics, but without the minutiae in topics that are clear for most IT professionals. I regularly hear from instructors who use versions of the book to help students master the topics and pass the Security+ exam the first time they take it.

Second, this book is for those people who like to study on their own. If you’re one of the people who can read a book and learn the material without sitting in a class, this book has what you need to take and pass the exam.

Additionally, you can keep this book on your shelf (or in your Kindle) to remind yourself of important, relevant concepts. These concepts are important for security professionals and IT professionals in the real world.

Based on many conversations with students and readers of the previous versions of this book, I know that many people use the Security+ certification as the first step in achieving other security certifications. For example, you may follow Security+ with one of these cybersecurity certifications:

- (ISC)2 Systems Security Certified Practitioner (SSCP)
- (ISC)2 Certified Information Systems Security Professional (CISSP)
- CompTIA Advanced Security Practitioner (CASP)
- CompTIA Cybersecurity Analyst (CySA+)

If you plan to pursue any of these advanced security certifications, you’ll find this book will help you lay a solid foundation of security knowledge. Learn this material, and you’ll be a step ahead on the other exams.

About This Book

Over the past several years, I've taught hundreds of students literally, helping them become CompTIA Security+ certified. During that time, I've learned what concepts are easy to grasp and what concepts need more explanation. I've developed handouts and analogies that help students grasp the elusive concepts.

Feedback from students was overwhelmingly positive—both in their comments to me and their successful pass rates after taking the certification exam. When the objectives changed in 2008, I rewrote my handouts as the first edition of this book. When the objectives changed again in 2011, 2014, and 2017, I rewrote the book to reflect the new objectives. This book reflects the objective changes released in 2020.

Gratefully, this book has allowed me to reach a much larger audience and share security and IT-related information. Even if you aren't in one of the classes I teach, this book can help you learn the relevant material to pass the exam the first time you take it.

PDF versions of this book are not authorized. Criminals have created unauthorized versions of this book and sold them, indicating that they had permission to do so. However, they did not have permission, and no one has permission to sell or distribute PDF versions of this book

Appendices

In past versions of this book, some people have asked for more information on certain topics. This information is often trivial to others who meet the prerequisites of the exam. If I include this information in the book, many people look at it as needless fluff. However, if the people who need this prerequisite information don't have it, they often feel unprepared.

To resolve this, I've created some downloadable appendixes to fill in the gaps for anyone who needs them. As an example, the following list identifies some free appendixes I've created in PDF form for readers to download:

- **Appendix A—Command Line Basics.** If you're unfamiliar with how to launch the Windows Command line or the Linux terminal, this appendix will help you. It also includes some basics related to switches and the use of upper- and lowercase letters.
- **Appendix B—Log Basics.** Administrators often look at logs almost daily, so they dissect log entries from multiple sources regularly. Even when looking at a new source's log entry (such as from a new firewall), they can identify common elements and determine the log entry's meaning. This appendix outlines some basics about logs and how to look for common elements.
- **Appendix C—Well-Known Ports.** This describes how logical ports are mapped to protocols and how computers use these ports. You sometimes need to know well-known ports when setting up firewalls, and this appendix includes a couple of tables of ports mapped to protocols.
- **Appendix D—The OSI Model.** The CompTIA SY0-601 Security+ objectives mention the Open Systems Interconnection (OSI) layers a few times. Most people have heard about this and maybe even learned in depth while studying for another certification. However, you don't need to know the OSI model in depth. This appendix will remind you about the OSI model and what you need to know for the Security+ exam.

- **Appendix E—Glossary.** The glossary provides you with an alphabetized list of key terms related to the exam.

You can access them via the free online resources page. The URL is listed in the Online References section in each chapter's Exam Topic Review section.

How to Use This Book

Over the years, I've taught the Security+ course many times. During this process, I learned the best way to present the material so that students understand and retain the most knowledge. The book is laid out the same way.

For most people, the easiest way to use the book is by starting with the pre-assessment exam (after the intro) to gauge your initial understanding of the topics. Then, go through each chapter sequentially, including the end-of-chapter practice test questions. By doing so, you'll build a solid foundation of knowledge. This helps make the more advanced topics in later chapters easier to understand.

If you have a high level of IT security knowledge and only want to study the topics that are unclear to you on this exam, you can review the objective map listed at the end of this Introduction. The objective map lists all the objectives and identifies the chapter where they are covered. Additionally, you can look at the index to locate the exact page for these topics. If you have the Kindle version, it includes an excellent search feature to find specific topics. When practicing for any certification exam, the following steps are a good recipe for success:

- **Review the objectives.** The objectives for the SY0-601 exam are listed in the “Objective to Chapter Map” section in this Introduction.
- **Learn the material related to the objectives.** This book covers all the objectives, and the Introduction includes a map showing which chapter (or chapters) covers each objective. Along those lines, my goal when writing the book was to cover the objectives in enough depth to help you pass the exam. However, these topics all have a lot more depth. When I study for a certification exam, I typically dig in much deeper than necessary, often because the topics interest me. You can, too, if you want, but don't lose sight of the exam objectives.
- **Take practice questions.** When preparing for any certification exam, a key step is to make sure you can answer the exam questions. Yes, you need the knowledge, but you also must be

able to read a question and select the correct answer. This simply takes practice. When using practice test questions, ensure they have explanations. Questions without explanations often encourage rote memorization without understanding the content. Worse, they sometimes even give you the wrong answers.

- **Achieve high scores on practice exams.** I typically tell people that they should get scores of at least 90 percent on practice tests for the CompTIA Security+ exam. However, don't focus on only your scores. Make sure you understand the content, too.
- **Read and understand the explanations.** Ideally, you should be able to look at any practice test question and know why the correct answers are correct and why the incorrect answers are incorrect. Within this book, you'll find this information in the text and the explanations for the questions. When you understand the explanations, you have the best chance of accurately interpreting the questions on the live exam and answering them correctly no matter how CompTIA words or presents them.

This book has over 300 practice test questions that you can use to test your knowledge and your ability to answer them correctly. Every question has a detailed explanation to help you understand why the correct answers are correct and why the incorrect answers are incorrect.

You can find the practice questions in the following areas:

- **Pre-assessment exam.** Use these questions at the beginning of the book to get a feel for what you know and what you need to study more.
- **End-of-chapter practice questions.** Each chapter has practice questions to help you test your comprehension of the material in the chapter.
- **Post-assessment exam.** Use this as a practice exam to test your comprehension of the subject matter and readiness to take the actual exam.
- **Online.** We've also provided some additional questions online. They are free and listed with other free online resources available with this book.

It's OK if you do the practice questions in a different order. You may decide to tackle all the chapters in the book and then do the pre-assessment and post-assessment questions. That's fine. However, I strongly suggest you review all the questions in the book. Also, make sure you check out the additional free online resources at: [*https://greatadministrator.com/sy0-601-extras/*](https://greatadministrator.com/sy0-601-extras/).

Conventions

While creating this book, I've followed specific conventions to give you insight into the content. The following list shows how these conventions are used:

- **Glossary terms.** Important glossary items are presented in ***bold italic*** the first time they are mentioned or when they are defined.
- **Commands.** Some chapters include specific commands, and they are shown in ***bold***. I encourage you to enter these commands so that you can see how they work.
- **File names.** File names such as *md5sum.exe* are shown in *italic*.
- **Website URLs.** URLs such as *https://gcgapremium.com* are shown in *italic*.

Remember This

You'll see text boxes throughout the book that highlight important testable information. The surrounding content provides additional information needed to understand these key points fully, and the text boxes summarize the important points.

These text boxes look like this:

Remember this

I strongly encourage you to repeat the information in the text boxes to yourself as often as possible. The more you repeat the information, the more likely you are to remember it when you take the

A tried-and-true method of repeating key information is to take notes when you're first studying the material and then rewrite the notes later. This will expose you to the material a minimum of three times.

Another method that students have told me has been successful for them is to use an MP3 player. Many MP3 players can record. Start your MP3 recorder and read the information in each text box for a chapter and the Exam Topic Review section of each chapter. Save the MP3 file and regularly listen to it. This allows you to reaffirm the important information in your own voice.

You can play it while exercising, walking, or just about any time when it's not dangerous to listen to any MP3 file. If the MP3 method is successful for you, you can also record and listen to exam questions. Read the question, the possible answers, the correct answer, and the explanation in each practice question.

If you don't have time to create your own MP3 recordings, check out the companion website (<http://gcpagpremiumpass.com>) for this book. You can purchase MP3 recordings there that you can download and use.

Vendor Neutral

CompTIA certifications are vendor-neutral. In other words, certifications are not centered on any single vendor, such as Microsoft, Apple, or Linux distributions. However, you can expect to see questions that are focused on specific vendors or operating systems.

For example, many of the commands listed in the “Network Reconnaissance and Discovery” section of this version of the CompTIA Security+ exam are specific to Microsoft Windows and Linux operating systems.

Free Online Resources

There are many additional free resources available to you at <https://greatadministrator.com/sy0-601-extras/>, including:

- Free online labs
- Appendices for this book
- Sample performance-based questions
- Additional free multiple-choice practice test questions
- Other free resources such as links to additional content

I created this online content with a couple of goals. First, this version of the objectives was significantly longer than the last version. There was a lot I wanted to include in the book, but there just wasn't room. For example, if I included all the labs in the book, it would have inflated the book's page count to an unmanageable level. Second, I wanted to give myself a way to update the book's content. If it is helpful to readers, I can easily add additional labs and/or additional resources.

These materials are valuable free supplements, so you'll need to register to access this content and prove that you have the book by answering a question. As an example, you may have to answer a question such as this:

Locate the “Vendor Neutral” section in the Introduction of the book. What is the last word in that section?

The “Vendor Neutral” section is right before this section (“Free Online Resources”), and the last word in that section is systems. You will then need to enter the word systems. People guessing (or who don’t have the book) won’t be able to answer the question. You will.

Be careful, though. If you don’t answer the question correctly the first time, you won’t get another chance for several days. It’s essential that you take the time to enter the correct word the first time.

Additional Web Resources

Check out <https://getcertifiedgetahead.com/> for up-to-date details on the CompTIA Security+ exam. This site includes additional information related to the CompTIA Security+ exam and this book.

Although many people have spent a lot of time and energy trying to ensure that there are no errors in this book, errors occasionally slip through. This site includes an errata page listing any errors we've discovered.

If you discover any errors, please let me know through the Contact Us page on the website. I'd also love to hear about your success when you pass the exam. I'm constantly getting good news from readers and students who are successfully earning their certifications.

In response to all the requests I've received for additional materials, such as online practice test questions, flash cards, and audio files, I also created this site: <https://gcpapremium.com/>. It includes access to various study materials at an additional cost. Packages include all the materials in the book and in the free online resources area, plus additional materials such as more practice test questions, flash cards, audio, and additional performance-based questions.

Last, I've found that many people find cryptography topics challenging, so I've posted some videos on YouTube (<https://www.youtube.com/>). As time allows, I'll post additional videos, and you can get a listing of all of them by searching YouTube with "Darril Gibson."

Assumptions

The CompTIA Security+ exam assumes you have the equivalent of two years experience working in a security or systems administrator job role. However, I'm aware that two years of experience in a network could mean many different things. Your two years of experience may expose you to different technologies than someone else's two years of experience.

When it's critical that you understand an underlying concept to master the relevant exam material, I often include some background information to make it easier to understand.

Set a Goal

Look at a calendar right now and determine the date 45 days from today. This will be your target date to take this exam. Set this as your goal to complete studying the materials and to take the exam.

This target allows you to master about one and a half chapters per week. It may be that some of the chapters take you less time, and some of the chapters take you more time. No problem. If you want to modify your target date later, do so. However, a recipe for success in almost any endeavor includes setting a goal.

When I teach CompTIA Security+ at a local university, I often help the students register for the exam on the first night. They pick a date close to the end of the course and register. I've found that when we do this, about 90 percent of the students take and pass the exam within one week after completing the course. On the other hand, when I didn't help the students register on the first night, more than half of them did not complete the exam in the same time frame. Setting a goal helps.

About the Exam

CompTIA first released the Security+ exam in 2002, and it has quickly grown in popularity. They revised the exam objectives in 2008, 2011, 2014, 2017, and again in 2020. The 2020 exam is labeled SY0-601. The English version of the SY0-501 exam is scheduled to retire in July 2021.

Here's a summary of the exam details:

- **Number of questions:** Maximum of 90 questions
- **Length of test:** 90 minutes
- **Passing score:** 750
- **Grading criteria:** Scale of 100 to 900 (about 83 percent)
- **Question types:** Multiple choice and performance-based
- **Exam format:** Traditional—can move back and forth to view previous questions
- **Exam test provider:** Pearson VUE
(<https://home.pearsonvue.com/>)
- **Exam prerequisites:** None required but CompTIA lists the following recommendations:
 - At least 2 years of work experience in IT systems administration with a focus on security
 - Hands-on technical information security experience
 - Broad knowledge of security concepts

When it was first released, the exam was touted as an introductory level exam. However, it has morphed over the years. Some people now compare Security+ to the (ISC)2 Certified Information Systems Security Professional (CISSP), which has long been described as “a mile wide and an inch deep.” The implication is that both exams cover a wide breadth of knowledge but often don’t go too far in-depth with any of the topics.

Passing Score

A score of 750 is required to pass. This is on a scale of 100 to 900. If you take the exam but don't get a single question correct, you get a score of 100. If you get every question correct, you get a score of 900. A passing score of 750 divided by 900 equals .8333 or 83.33 percent.

Also, a score of 83 percent is higher than many other certification exams, so you shouldn't underestimate the difficulty of this exam. However, many people regularly pass it, and you can pass it, too. With this book and the free online resources, you will be well prepared.

Exam Prerequisites

All that is required for you to take the exam is money. Other than that, there are no enforced prerequisites. However, to successfully pass the exam, you're expected to have "at least 2 years of work experience in IT systems administration with a focus on security." If you have more than that, the exam materials will likely come easier to you. If you have less, the exam may be more difficult.

Beta Questions

Your exam may have some beta questions. They aren't graded but instead are used to test the validity of the questions. If everyone gets a beta question correct, it's probably too easy. If everyone gets it incorrect, there's probably something wrong with the question. After enough people have tested a beta question, CompTIA personnel analyze it and decide if they want to add it to the test bank. They may also rewrite it and test it again as a new beta question.

The good news is that CompTIA doesn't grade the beta questions. However, you don't know which questions are ungraded beta questions and which questions are live questions. You need to treat every question as if it was graded.

Exam Format

The exam uses a traditional format. You start at question 1 and go to the last question. You can skip questions and mark any questions you want to review as you're going through the exam. When you finish, you can go back to all your marked questions. Additionally, you can view previous questions if desired. For example, if you get to question 10 and then remember something that helps you answer question 5, you can go back and redo question 5.

Question Types

You will see two primary question types on the exam: multiple-choice and performance-based. Each type is described in the following sections.

Multiple Choice

Most questions are multiple-choice types where you select one answer or multiple answers. When you need to select multiple answers, the question will include a phrase such as “Select TWO” or “Select THREE.”

You may also see questions that use phrases such as “BEST choice,” “BEST description,” or “MOST secure.” In these examples, don’t be surprised if you see two answers that could answer the question, while only one is the best choice. As an example, consider this simple question:

Which one of the following numbers is between 1 and 10 and is the HIGHEST?

- A. 2
- B. 8
- C. 14
- D. 23

Clearly, 2 and 8 are between 1 and 10, but 14 and 23 are not. However, only 8 is both between 1 and 10 and the highest.

Performance-Based Questions

You can expect as many as 10 performance-based questions. These include matching, drag and drop, and data entry questions. CompTIA refers to these as performance-based questions, and instead of picking from a multiple-choice answer, you’re often required to perform a task. CompTIA’s goal is to provide more accurate testing to verify people have a full understanding of a topic.

People often ask if they get partial credit. CompTIA has said that you may get partial credit on some questions, but other questions may not give you partial credit. However, you’ll never know which questions give you partial credit and which questions don’t give you partial credit. It’s best to do the best you can with each question.

The following sections cover the different types of performance-based questions you can expect. You can also check out some of the blogs on performance-based questions that I've written here:

<https://blogs.getcertifiedgetahead.com/security-blog-links/>.

Matching

In a matching performance-based question, you will see two lists, and you need to match them. As an example, one list might include control types such as technical, managerial, and physical. The second list might include specific controls such as risk assessments, security guards, and encryption. You would match technical with encryption, managerial with risk assessments, and physical with security guards. If you understand the common security control types, this becomes trivial. Then again, if you don't understand the control types, this can be quite difficult.

Drag and Drop

You might need to drag items from one location on the screen to another location to answer some questions. You can think of these as multiple-choice questions with multiple answers that are correct. However, instead of selecting the checkboxes to indicate a correct answer, you drag it to somewhere else on the screen.

As an example, consider this question:

Q. Arrange the following list in order from most volatile to least volatile:

- Paging file
- File on local drive
- Archive media
- RAM
- Cache

You would drag and drop the items until they were in the following order:

- Cache
- RAM
- Paging file
- Files on local drive
- Archive media

Data Entry

Some performance-based questions might ask you to analyze a scenario and then enter appropriate data. For example, Chapter 3, “Exploring Network Technologies and Tools,” discusses the use of OpenSSH tools to create a key pair. A question may ask you to enter the command to create this key pair. The command is:

ssh-keygen -t rsa

Chapter 3 describes the use of ssh-keygen in more detail. Administrators often use it to create a passwordless login to systems with Secure Shell (SSH).

Performance-Based Questions Strategy

You’ll see the performance-based questions first, and they take much longer than typical multiple-choice questions. If the answer is clear to you, then take the time to answer it. However, if the question isn’t clear, mark the question and skip it. You can come back to it later. The question may be a poorly worded beta question that doesn’t even count. However, if you spend 45 minutes on it, you might run out of time before finishing the multiple-choice questions.

Performance-based questions have occasionally caused problems for the test systems. A common problem is that instead of displaying the question, the screen is mostly blank. If this happens, you can often just use the reset button for the question. This allows you to move past the problem and continue with the test. However, resetting the question erases any answer you’ve entered, so you’ll have to come back to it after you finish other questions.

Some readers reported that they skipped all of the performance-based questions and still passed. This was usually because the performance-based questions weren’t working correctly, or they simply weren’t clear. After finishing the multiple-choice questions, they ran out of time but still passed.

It’s common for people to be nervous when thinking about these performance-based test questions. However, most people who take the test say that they usually aren’t that difficult. If you understand the concepts from the exam objectives, you won’t have any problems. I do recommend

you check out the posts on performance-based questions that I've posted here: <https://blogs.getcertifiedgetahead.com/security-blog-links/>.

Question Complexity

In the past, the Security+ test questions were relatively straightforward. For example, a question may have been like this “What is 5×5 ?” Either you know the answer is 25, or you don’t. In other words, the exam simply required you to remember and recall facts and basic concepts.

However, the questions have been getting progressively more complex. Instead of just remembering facts, you’re expected to understand concepts and apply your knowledge in different situations. Some advanced questions require you to analyze a scenario, evaluate various indicators, and select the best possible answer.

Many of the objectives start with the phrase “given a scenario,” indicating you can expect advanced questions related to these objectives. Performance-based questions are often used to test these types of objectives. However, it’s also possible to use complex multiple-choice questions to test the same objectives.

Consider this example:

Q. You are driving a bus from Springfield to Shelbyville at 55 mph with 22 passengers. The bus is painted blue. At the same time, a train is traveling from Shelbyville to Springfield at 40 mph. The train has a yellow caboose. What color are the bus driver’s eyes?

Notice that the question adds a lot of superfluous information. The actual question is in the last sentence, and only one comment is directly related to this question. The question starts by saying, “You are driving a bus...” and then ends by asking, “What color are the bus driver’s eyes?” You’re required to put the two together and weed through the irrelevant information to come to the correct answer.

Some people memorize practice test questions and answers. However, this is not a successful path to success because CompTIA often modifies the questions. Ideally, you should know why the correct answers are correct and why the incorrect answers are incorrect. This will give you a much better chance of interpreting the questions and answering them correctly. Consider this question:

Q. Your organization hires temporary help and contractor personnel on a seasonal basis. These personnel need access to network resources, but only during working hours. Management has stressed that it is critically important to safeguard trade secrets and other confidential information. Which of the following account management concepts would be MOST important to meet these goals?

- A. Account expiration
- B. Account lockout
- C. Password history
- D. Password recovery
- E. Time-of-day restrictions

The key phrase here is “only during working hours.” Time-of-day restrictions can be applied to ensure these seasonal personnel cannot access network resources during off-hours or the weekend.

If someone memorizes a few keywords to the previous question along with the answer, they will likely have problems if CompTIA modifies the question. Compare it to this question:

Q. Your organization hires temporary help and contractor personnel on a seasonal basis. These personnel need access to network resources, but only during their employment period. Management has stressed that it is critically important to safeguard trade secrets and other confidential information. Which of the following account management concepts would be MOST important to meet these goals?

- A. Account expiration
- B. Account lockout
- C. Password history
- D. Password recovery
- E. Time-of-day restrictions

The key phrase here is “only during their employment period.” Setting account expiration will ensure the accounts are disabled when the employment period ends.

Notice that only a few words in the questions are different. The first question emphasizes working hours, while the second one emphasizes the employment period. However, if someone memorized questions and answers, they might jump on time-of-day restrictions for the second question without reading the full question.

Practice Test Questions Strategy

Some people want more and more practice test questions, but the quantity of practice test questions you use isn't as important as their quality. And how you use them. At the core, you want to ensure you understand the underlying concept.

Imagine you're being tested on addition. You could have 10,000 questions asking you to add 1+1, 1+2, 1+3, and so on up to 1+100, along with 2+1, 3+1, and so on, up to 100+100. That kind of repetition just isn't needed. However, if you can add 28+17 correctly, you probably understand the concept.

When going through practice test questions, it's important to remind yourself why the incorrect answers are incorrect. This effectively gives you four questions for every single question you take. Imagine this question:

Q. What two numbers added together will give you a sum of 45?

- A. 19 + 24
- B. 21 + 26
- C. 28 + 17
- D. 14 + 33

By reminding yourself why each of the incorrect answers is incorrect ($19+24=43$, $21+26=47$, $28+17=45$, $14+33=47$), it essentially gives you four questions from just one. Additionally, many people report that this strategy allows them to eliminate obvious incorrect answers and arrive at the correct answer, which wasn't obvious at first.

Exam Test Provider

You can take the exam at a Pearson VUE testing site. Some testing sites provide testing and nothing else. However, most testing sites are part of another organization, such as a training company, college, or university. You can take an exam at the training company's testing site even if you haven't taken a course with them.

The Pearson VUE website includes search tools you can use to find a testing site close to you. Check them out at <https://home.pearsonvue.com/>.

Voucher Code for 10 Percent Off

The cost of the CompTIA Security+ exam voucher is \$370 in the United States if you purchase it at full price, though CompTIA may raise the price in the future. However, you can get a 10 percent discount using a discount code. This code sometimes changes, so you'll need to go to this page to access the current code: <https://gcgapremium.com/discounted-comptia-vouchers/>. That page also includes instructions on how to use the voucher.

When you purchase a voucher, you'll get a voucher number that you can use to register at a testing site. A word of caution: some criminals sell bogus vouchers on Internet sites such as eBay. You won't know you've been ripped off until you try to use it, and by that time, the criminal will probably have disappeared. In contrast, if you use the discount code, you buy the voucher directly from CompTIA.

Exam Domains

The exam objectives are divided into the following domains, or general topic areas. Additionally, CompTIA publishes the percentage of questions you can anticipate in any of the domains:

- **1.0 Attacks, Threats, and Vulnerabilities.** 24 percent of examination content
- **2.0 Architecture and Design.** 21 percent of examination content
- **3.0 Implementation.** 25 percent of examination content
- **4.0 Operations and Incident Response.** 16 percent of examination content
- **5.0 Governance, Risk, and Compliance.** 14 percent of examination content

CompTIA publishes a listing of the objectives on its website. They also include these comments:

"The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on testing exam objectives. Please know that all related exam preparation materials will still be valid."

This indicates that you may see something that isn't on the objective list. As an example, the objectives clearly show an increased emphasis on commands. However, you won't see OpenSSH mentioned or the OpenSSH command **ssh-keygen**. However, you may see OpenSSH mentioned or questions that expect you to understand the purpose and use of **ssh-gen**.

I've done my best to predict how test item writers will interpret these objectives when writing test questions. However, there may be some surprises. Make sure you look at the free online materials at <https://greatadministrator.com/sy0-601-extras/>.

Additionally, you can check this book's companion site at <https://GetCertifiedGetAhead.com> for up-to-date information on the exam,

and read blogs about various topics, including the CompTIA Security+ exam, at <https://blogs.GetCertifiedGetAhead.com>. Also, online practice test questions, flash cards, and other study materials are available for purchase at <https://gcpagpremium.com/>.

Last, CompTIA added about 345 line items in the SY0-601 objectives for a total of 1,223 line items. As a comparison, the SY0-501 objectives had only 878 line items. With a 75 question exam, don't expect to see all of these 1,223 objective line items on your exam.

Objective to Chapter Map

The following list shows the SY0-601 objectives published by CompTIA. The chapter or chapters where the objective is covered is listed next to each objective.

1.0 Threats, Attacks and Vulnerabilities

1.1 Compare and contrast different types of social engineering techniques.

Chapters 6, 7

- Phishing Chapter 6
- Smishing Chapter 6
- Vishing Chapter 6
- Spam Chapter 6
- Spam over Internet messaging (SPIM) Chapter 6
- Spear phishing Chapter 6
- Dumpster diving Chapter 6
- Shoulder surfing Chapter 6
- Pharming Chapter 7
- Tailgating Chapter 6
- Eliciting information Chapter 6
- Whaling Chapter 6
- Prepending Chapter 6
- Identity fraud Chapter 6
- Invoice scams Chapter 6
- Credential harvesting Chapter 6
- Reconnaissance Chapter 6
- Hoax Chapter 6
- Impersonation Chapter 6
- Watering hole attack Chapter 6
- Typo squatting Chapter 6
- Pretexting Chapter 6
- Influence campaigns Chapter 6
 - Hybrid warfare Chapter 6
 - Social media Chapter 6
- Principles (reasons for effectiveness) Chapter 6

- Authority Chapter 6
- Intimidation Chapter 6
- Consensus Chapter 6
- Scarcity Chapter 6
- Familiarity Chapter 6
- Trust Chapter 6
- Urgency Chapter 6

1.2 Given a scenario, analyze potential indicators to determine the type of attack.

Chapters 5, 6, 7, 8, 9, 10

- Malware Chapter 6
 - Ransomware Chapter 6
 - Trojans Chapter 6
 - Worms Chapter 6
 - Potentially unwanted programs (PUPs) Chapter 6
 - Fileless virus Chapter 6
 - Command and control Chapter 6
 - Bots Chapter 6
 - Cryptomalware Chapter 6
 - Logic bombs Chapter 6
 - Spyware Chapter 6
 - Keyloggers Chapter 6
 - Remote access Trojan (RAT) Chapter 6
 - Rootkit Chapter 6
 - Backdoor Chapter 6
- Password attacks Chapter 10
 - Spraying Chapter 10
 - Dictionary Chapter 10
 - Brute force Chapter 10
 - Offline Chapter 10
 - Online Chapter 10
 - Rainbow table Chapter 10
 - Plaintext/unencrypted Chapter 10
- Physical attacks Chapter 9
 - Malicious universal serial bus (USB) cable Chapter 9
 - Malicious flash drive Chapter 9
 - Card cloning Chapter 9

- Skimming Chapter 9
- Adversarial artificial intelligence (AI) Chapter 7
 - Tainted training data for machine learning (ML) Chapter 7
 - Security of machine learning algorithms Chapter 7
- Supply-chain attacks Chapter 8
- Cloud-based vs. on-premises attacks Chapter 5
- Cryptographic attacks Chapter 10
 - Birthday Chapter 10
 - Collision Chapter 10
 - Downgrade Chapter 10

1.3 Given a scenario, analyze potential indicators associated with application attacks. Chapters 5, 7, 8, 10

- Privilege escalation Chapter 8
- Cross-site scripting Chapter 7
- Injections Chapter 7
 - Structured query language (SQL) Chapter 7
 - Dynamic link library (DLL) Chapter 7
 - Lightweight directory access protocol (LDAP) Chapter 7
 - Extensible markup language (XML) Chapter 7
- Pointer/object dereference Chapter 7
- Directory traversal Chapter 7
- Buffer overflows Chapter 7
- Race conditions Chapter 7
 - Time of check/time of use Chapter 7
- Error handling Chapter 7
- Improper input handling Chapter 7
- Replay attack Chapter 7
 - Session replays Chapter 7
- Integer overflow Chapter 7
- Request forgeries Chapter 7
 - Server-side Chapter 7
 - Client-side Chapter 7
- Application programming interface (API) attacks Chapter 5
- Resource exhaustion Chapter 7
- Memory leak Chapter 7
- Secure sockets layer (SSL) stripping Chapter 7

- Driver manipulation Chapter 7
 - Shimming Chapter 7
 - Refactoring Chapter 7
- Pass the hash Chapter 10

1.4 Given a scenario, analyze potential indicators associated with network attacks.

Chapters 4, 6, 7

- Wireless Chapter 4
 - Evil twin Chapter 4
 - Rogue access point Chapter 4
 - Bluesnarfing Chapter 4
 - Bluejacking Chapter 4
 - Disassociation Chapter 4
 - Jamming Chapter 4
 - Radio frequency identifier (RFID) Chapter 4
 - Near field communication (NFC) Chapter 4
 - Initialization vector (IV) Chapter 4
- On-path attack (previously known as man in the middle attack/man in the browser attack) Chapter 7
- Layer 2 attacks Chapter 7
 - Address resolution protocol (ARP) poisoning Chapter 7
 - Media access control (MAC) flooding Chapter 7
 - MAC cloning Chapter 7
- Domain name system (DNS) Chapter 7
 - Domain hijacking Chapter 7
 - DNS poisoning Chapter 7
 - Universal resource locator (URL) redirection Chapter 7
 - Domain reputation Chapter 7
- Distributed denial of service (DDoS) Chapter 6, 7
 - Network Chapter 7
 - Application Chapter 7
 - Operational technology (OT) Chapter 7
- Malicious code or script execution Chapter 7
 - PowerShell Chapter 7
 - Python Chapter 7
 - Bash Chapter 7
 - Macros Chapter 7

- Visual Basic for Applications (VBA) Chapter 7

1.5 Explain different threat actors, vectors, and intelligence sources. Chapters 4, 5, 6, 8, 11

- Actors and threats Chapter 6
 - Advanced persistent threat (APT) Chapter 6
 - Insider threats Chapter 6
 - State actors Chapter 6
 - Hacktivists Chapter 6
 - Script kiddies Chapter 6
 - Criminal syndicates Chapter 6
 - Hackers Chapter 6
 - Authorized Chapter 6
 - Unauthorized Chapter 6
 - Semi-authorized Chapter 6
 - Shadow IT Chapter 6
 - Competitors Chapter 6
- Attributes of actors Chapter 6
 - Internal/external Chapter 6
 - Level of sophistication/capability Chapter 6
 - Resources/funding Chapter 6
 - Intent/motivation Chapter 6
- Vectors Chapters 4, 5, 6, 8, 11
 - Direct access Chapter 4
 - Wireless Chapter 4
 - Email Chapter 6
 - Supply chain Chapter 8, 11
 - Social media Chapter 6
 - Removable media Chapter 5
 - Cloud Chapter 5
- Threat intelligence sources Chapter 6
 - Open source intelligence (OSINT) Chapter 6, 8
 - Closed/proprietary Chapter 6
 - Vulnerability databases Chapter 6
 - Public/private information sharing centers Chapter 6
 - Dark web Chapter 6
 - Indicators of compromise Chapter 6

- Automated indicator sharing (AIS) Chapter 6
 - Structured Threat Information eXchange (STIX)/Trusted Automated eXchange of Intelligence Information (TAXII) Chapter 6
- Predictive analysis Chapter 6
- Threat maps Chapter 6
- File/code repositories Chapter 6
- Research sources Chapter 6
 - Vendor websites Chapter 6
 - Vulnerability feeds Chapter 8
 - Conferences Chapter 6
 - Academic journals Chapter 6
 - Request for comments (RFC) Chapter 6
 - Local industry groups Chapter 6
 - Social media Chapter 6
 - Threat feeds Chapter 8
 - Adversary tactics, techniques, and procedures (TTP) Chapter 8

1.6 Explain the security concerns associated with various types of vulnerabilities.

Chapters 5, 6, 7, 8, 11

- Cloud-based vs. on-premises vulnerabilities Chapter 5
- Zero-day Chapter 6, 7
- Weak configurations Chapter 8
 - Open permissions Chapter 8
 - Unsecured root accounts Chapter 8
 - Errors Chapter 8
 - Weak encryption Chapter 8
 - Unsecure protocols Chapter 8
 - Default settings Chapter 8
 - Open ports and services Chapter 8
- Third-party risks Chapter 5, 7, 11
 - Vendor management Chapter 11
 - System integration Chapter 11
 - Lack of vendor support Chapter 11
 - Supply chain Chapter 11
 - Outsourced code development Chapter 7

- Data storage Chapter 5
- Improper or weak patch management Chapter 8
 - Firmware Chapter 8
 - Operating system (OS) Chapter 8
 - Applications Chapter 8
- Legacy platforms Chapter 8
- Impacts Chapters 5, 6, 11
 - Data loss Chapter 5
 - Data breaches Chapter 11
 - Data exfiltration Chapter 5, 6
 - Identity theft Chapter 6
 - Financial Chapter 5
 - Reputation Chapter 5
 - Availability loss Chapter 5

1.7 Summarize the techniques used in security assessments. Chapters 1, 8, 11

- Threat hunting Chapter 8
 - Intelligence fusion Chapter 8
 - Threat feeds Chapter 8
 - Advisories and bulletins Chapter 8
 - Maneuver Chapter 8
- Vulnerability scans Chapter 8
 - False positives Chapter 8
 - False negatives Chapter 8
 - Log reviews Chapter 8
 - Credentialled vs. non-credentialled Chapter 8
 - Intrusive vs. non-intrusive Chapter 8
 - Application Chapter 8
 - Web application Chapter 8
 - Network Chapter 8
 - Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS) Chapter 8
 - Configuration review Chapter 8
- Syslog/Security information and event management (SIEM) Chapter 1
 - Review reports Chapter 1
 - Packet capture Chapter 1

- Data inputs Chapter 1
- User behavior analysis Ch1
- Sentiment analysis Chapter 1
- Security monitoring Chapter 1
- Log aggregation Chapter 1
- Log collectors Chapter 1
- Security orchestration, automation, response (SOAR) Chapter 11

1.8 Explain the techniques used in penetration testing. Chapters 4, 6, 8

- Penetration testing Chapter 8
 - Known environment Chapter 8
 - Unknown environment Chapter 8
 - Partially known environment Chapter 8
 - Rules of engagement Chapter 8
 - Lateral movement Chapter 8
 - Privilege escalation Chapter 8
 - Persistence Chapter 8
 - Cleanup Chapter 8
 - Bug bounty Chapter 8
 - Pivoting Chapter 8
- Passive and active reconnaissance Chapters 4, 6, 8
 - Drones Chapter 4
 - War flying Chapter 4?
 - War driving Chapter 4?
 - Footprinting Chapter 8
 - OSINT Chapter 6, 8
- Exercise types Chapter 8
 - Red team Chapter 8
 - Blue team Chapter 8
 - White team Chapter 8
 - Purple team Chapter 8

2.0 Architecture and Design

**2.1 Explain the importance of security concepts in an enterprise environment.
Chapters 1, 4, 5, 7, 9, 10, 11**

- Configuration management Chapter 5
 - Diagrams Chapter 5

- Baseline configuration Chapter 5
- Standard naming conventions Chapter 5
- Internet protocol (IP) schema Chapter 5
- Data sovereignty Chapter 9
- Data protection Chapter 5, 10, 11
 - Data loss prevention (DLP) Chapter 5
 - Masking Chapter 11
 - Encryption Chapter 10
 - At rest Chapter 10
 - In transit/motion Chapter 10
 - In processing Chapter 10
 - Tokenization Chapter 11
 - Rights management Chapter 5
- Geographical considerations Chapter 9
- Response and recovery controls Chapter 1
- Secure Sockets Layer (SSL)/Transport Layer Security (TLS) inspection Chapter 4
- Hashing Chapter 10
- API considerations Chapter 5
- Site resiliency Chapter 9
 - Hot site Chapter 9
 - Cold site Chapter 9
 - Warm site Chapter 9
- Deception and disruption Chapter 4
 - Honeypots Chapter 4
 - Honeyfiles Chapter 4
 - Honeynets Chapter 4
 - Fake telemetry Chapter 4
 - DNS sinkhole Chapter 7

2.2 Summarize virtualization and cloud computing concepts. Chapter 5

- Cloud models Chapter 5
 - Infrastructure as a service (IaaS) Chapter 5
 - Platform as a service (PaaS) Chapter 5
 - Software as a service (SaaS) Chapter 5
 - Anything as a service (XaaS) Chapter 5
 - Public Chapter 5

- Community Chapter 5
- Private Chapter 5
- Hybrid Chapter 5
- Cloud service providers Chapter 5
- Managed service provider (MSP)/ Managed security service provider (MSSP) Chapter 5
- On-premises vs. off-premises Chapter 5
- Fog computing Chapter 5
- Edge computing Chapter 5
- Thin client Chapter 5
- Containers Chapter 5
- Micro-services/API Chapter 5
- Infrastructure as code Chapter 5
 - Software-defined networking (SDN) Chapter 5
 - Software-defined visibility (SDV) Chapter 5
- Serverless architecture Chapter 5
- Services integration Chapter 5
- Resource policies Chapter 5
- Transit gateway Chapter 5
- Virtualization Chapter 5
 - Virtual machine (VM) sprawl avoidance Chapter 5
 - VM escape protection Chapter 5

2.3 Summarize secure application development, deployment, and automation concepts. Chapters 1, 7

- Environment Chapter 7
 - Development Chapter 7
 - Test Chapter 7
 - Staging Chapter 7
 - Production Chapter 7
 - Quality assurance (QA) Chapter 7
- Provisioning and deprovisioning Chapter 7
- Integrity measurement Chapter 7
- Secure coding techniques Chapter 7
 - Normalization Chapter 7
 - Stored procedures Chapter 7
 - Obfuscation/camouflage Chapter 7

- Code reuse/dead code Chapter 7
- Server-side vs. client-side execution and validation Chapter 7
- Memory management Chapter 7
- Use of third-party libraries and software development kits (SDKs) Chapter 7
- Data exposure Chapter 7
- Open Web Application Security Project (OWASP) Chapter 7
- Software diversity Chapter 7
 - Compiler Chapter 7
 - Binary Chapter 7
- Automation/scripting Chapter 7
 - Automated courses of action Chapter 7
 - Continuous monitoring Chapter 7
 - Continuous validation Chapter 7
 - Continuous integration Chapter 7
 - Continuous delivery Chapter 7
 - Continuous deployment Chapter 7
- Elasticity Chapter 1
- Scalability Chapter 1
- Version control Chapter 7

2.4 Summarize authentication and authorization design concepts. Chapters 2, 3, 5

- Authentication methods Chapter 2, 3
 - Directory services Chapter 3
 - Federation Chapter 2
 - Attestation Chapter 5
 - Technologies Chapter 2
 - Time-based one-time password (TOTP) Chapter 2
 - HMAC-based one-time password (HOTP) Chapter 2
 - Short message service (SMS) Chapter 2
 - Token key Chapter 2
 - Static codes Chapter 2
 - Authentication applications Chapter 2
 - Push notifications Chapter 2

- Phone call Chapter 2
 - Smart card authentication Chapter 2
- Biometrics Chapter 2
 - Fingerprint Chapter 2
 - Retina Chapter 2
 - Iris Chapter 2
 - Facial Chapter 2
 - Voice Chapter 2
 - Vein Chapter 2
 - Gait analysis Chapter 2
 - Efficacy rates Chapter 2
 - False acceptance Chapter 2
 - False rejection Chapter 2
 - Crossover error rate Chapter 2
- Multifactor authentication (MFA) factors and attributes Chapter 2
 - Factors Chapter 2
 - Something you know Chapter 2
 - Something you have Chapter 2
 - Something you are Chapter 2
 - Attributes Chapter 2
 - Somewhere you are Chapter 2
 - Something you can do Chapter 2
 - Something you exhibit Chapter 2
 - Someone you know Chapter 2
- Authentication, authorization, and accounting (AAA) Chapter 2
- Cloud vs. on-premises requirements Chapter 5

2.5 Given a scenario, implement cybersecurity resilience. Chapters 1, 5, 9, 10, 11

- Redundancy Chapter 9
 - Geographic dispersal Chapter 9
 - Disk Chapter 9
 - Redundant array of inexpensive disks (RAID) levels Chapter 9
 - Multipath Chapter 9
 - Network Chapter 9
 - Load balancers Chapter 9
 - Network interface card (NIC) teaming Chapter 9

- Power Chapter 9
 - Uninterruptible power supply (UPS) Chapter 9
 - Generator Chapter 9
 - Dual supply Chapter 9
 - Managed power distribution units (PDUs) Chapter 9
- Replication Chapter 9
 - Storage area network (SAN) Chapter 9
 - VM Chapter 5
- On-premises vs. cloud Chapter 5
- Backup types Chapter 9
 - Full Chapter 9
 - Incremental Chapter 9
 - Snapshot Chapter 9
 - Differential Chapter 9
 - Tape Chapter 9
 - Disk Chapter 9
 - Copy Chapter 9
 - Network attached storage (NAS) Chapter 9
 - Storage area network Chapter 9
 - Cloud Chapter 9
 - Image Chapter 9
 - Online vs. offline Chapter 9
 - Offsite storage Chapter 9
 - Distance considerations Chapter 9
- Non-persistence Chapter 5
 - Revert to known state Chapter 5
 - Last known good configuration Chapter 5
 - Live boot media Chapter 5
- High availability Chapter 1, 9
 - Scalability Chapter 1
- Restoration order Chapter 9
- Diversity Chapters 9, 10, 11
 - Technologies Chapter 9
 - Vendors Chapter 9, 11
 - Crypto Chapter 10

- Controls Chapter 9

2.6 Explain the security implications of embedded and specialized systems.

Chapter 3, 4, 5

- Embedded systems Chapter 5
 - Raspberry Pi Chapter 5
 - Field programmable gate array (FPGA) Chapter 5
 - Arduino Chapter 5
- System control and data acquisition (SCADA)/industrial control system (ICS) Chapter 5
 - Facilities Chapter 5
 - Industrial Chapter 5
 - Manufacturing Chapter 5
 - Energy Chapter 5
 - Logistics Chapter 5
- Internet of Things (IoT) Chapter 5
 - Sensors Chapter 5
 - Smart devices Chapter 5
 - Wearables Chapter 5
 - Facility automation Chapter 5
 - Weak defaults Chapter 5
- Specialized Chapter 5
 - Medical systems Chapter 5
 - Vehicles Chapter 5
 - Aircraft Chapter 5
 - Smart meters Chapter 5
- Voice over IP (VoIP) Ch3
- Heating, ventilation, air conditioning (HVAC) Chapter 5
- Drones Chapter 4
- Multifunction printer (MFP) Chapter 5
- Real-time operating system (RTOS) Chapter 5
- Surveillance systems Chapter 5
- System on chip (SoC) Chapter 5
- Communication considerations Chapter 5
 - 5G Chapter 5
 - Narrow-band Chapter 5
 - Baseband radio Chapter 5

- Subscriber identity module (SIM) cards Chapter 5
- Zigbee Chapter 5
- Constraints Chapter 5
 - Power Chapter 5
 - Compute Chapter 5
 - Network Chapter 5
 - Crypto Chapter 5
 - Inability to patch Chapter 5
 - Authentication Chapter 5
 - Range Chapter 5
 - Cost Chapter 5
 - Implied trust Chapter 5

2.7 Explain the importance of physical security controls. Chapter 3, 6, 9, 11

- Bollards/barricades Chapter 9
- Access control vestibules Chapter 6
- Badges Chapter 9
- Alarms Chapter 9
- Signage Chapter 9
- Cameras Chapter 9
 - Motion recognition Chapter 9
 - Object detection Chapter 9
- Closed-circuit television (CCTV) Chapter 9
- Industrial camouflage Chapter 9
- Personnel Chapter 9
 - Guards Chapter 9
 - Robot sentries Chapter 9
 - Reception Chapter 9
 - Two-person integrity/control Chapter 9
- Locks Chapter 9
 - Biometrics Chapter 9
 - Electronic Chapter 9
 - Physical Chapter 9
 - Cable locks Chapter 9
- USB data blocker Chapter 5
- Lighting Chapter 9
- Fencing Chapter 9

- Fire suppression Chapter 9
- Sensors Chapter 9
 - Motion detection Chapter 9
 - Noise detection Chapter 9
 - Proximity reader Chapter 9
 - Moisture detection Chapter 9
 - Cards Chapter 9
 - Temperature Chapter 9
- Drones Chapter 9
- Visitor logs Chapter 9
- Faraday cages Chapter 9
- Air gap Chapter 9
- Screened subnet (previously known as demilitarized zone) Chapter 3
- Protected cable distribution Chapter 9
- Secure areas Chapter 9
 - Air gap Chapter 9
 - Vault Chapter 9
 - Safe Chapter 9
 - Hot aisle Chapter 9
 - Cold aisle Chapter 9
- Secure data destruction Chapter 11
 - Burning Chapter 11
 - Shredding Chapter 11
 - Pulping Chapter 11
 - Pulverizing Chapter 11
 - Degaussing Chapter 11
 - Third-party solutions Chapter 11

2.8 Summarize the basics of cryptographic concepts. Chapters 1, 2, 3, 10

- Digital signatures Chapter 10
- Key length Chapter 10
- Key stretching Chapter 10
- Salting Chapter 10
- Hashing Chapter 10
- Key exchange Chapter 10
- Elliptical curve cryptography Chapter 10

- Perfect forward secrecy Chapter 10
- Quantum Chapter 10
 - Communications Chapter 10
 - Computing Chapter 10
- Post-quantum Chapter 10
- Ephemeral Chapter 10
- Modes of operation Chapter 10
 - Authenticated Chapter 10
 - Unauthenticated Chapter 10
 - Counter Chapter 10
- Blockchain Chapter 10
 - Public ledgers Chapter 10
- Cipher suites Chapter 10
 - Stream Chapter 10
 - Block Chapter 10
- Symmetric vs. asymmetric Chapter 10
- Lightweight cryptography Chapter 10
- Steganography Chapter 10
 - Audio Chapter 10
 - Video Chapter 10
 - Image Chapter 10
- Homomorphic encryption Chapter 10
- Common use cases Chapters 1, 2, 3, 10
 - Low power devices Chapter 10
 - Low latency Chapter 10
 - High resiliency Chapter 10
 - Supporting confidentiality Chapters 1, 10
 - Supporting integrity Chapters 1, 10
 - Supporting obfuscation Chapter 10
 - Supporting authentication Chapter 2, 3
 - Supporting non-repudiation Chapter 10
- Limitations Chapter 10
 - Speed Chapter 10
 - Size Chapter 10
 - Weak keys Chapter 10
 - Time Chapter 10

- Longevity Chapter 10
- Predictability Chapter 10
- Reuse Chapter 10
- Entropy Chapter 10
- Computational overheads Chapter 10
- Resource vs. security constraints Chapter 10

3.0 Implementation

3.1 Given a scenario, implement secure protocols. Chapters 2, 3, 4, 10

- Protocols Chapter 3
 - Domain Name System Security Extension (DNSSEC) Chapter 3
 - SSH Chapter 3
 - Secure/Multipurpose Internet Mail Extensions (S/MIME) Chapter 10
 - Secure Real-time Transport Protocol (SRTP) Chapter 3
 - Lightweight Directory Access Protocol Over SSL (LDAPS) Chapter 3
 - File Transfer Protocol, Secure (FTPS) Chapter 3
 - SSH File Transfer Protocol (SFTP) Chapter 3
 - Simple Network Management Protocol, version 3 (SNMPv3) Chapter 3
 - Hypertext transfer protocol over SSL/TLS (HTTPS) Chapter 3
 - IPSec Chapter 3, 4
 - Authentication header (AH)/ Encapsulated security payload (ESP) Chapter 3, 4
 - Tunnel/transport Chapter 4
 - Post Office Protocol (POP)/Internet Message Access Protocol (IMAP) Chapter 3
- Use cases Chapters 2, 3
 - Voice and video Chapter 3
 - Time synchronization Chapter 3
 - Email and web Chapter 3
 - File transfer Chapter 3
 - Directory services Chapters 2, 3

- Remote access Chapter 3
- Domain name resolution Chapter 3
- Routing and switching Chapter 3
- Network address allocation Chapter 3
- Subscription services Chapter 3

3.2 Given a scenario, implement host or application security solutions. Chapters 3, 4, 5, 6, 7, 10, 11

- Endpoint protection Chapters 6,
 - Antivirus Chapter 6
 - Anti-malware Chapter 6
 - Endpoint detection and response (EDR) Chapter 5
 - DLP Chapter 5
 - Next-generation firewall (NGFW) Chapter 3
 - Host-based intrusion prevention system (HIPS) Chapter 4
 - Host-based intrusion detection system (HIDS) Chapter 4
 - Host-based firewall Chapter 3
- Boot integrity Chapter 5
 - Boot security/Unified Extensible Firmware Interface (UEFI) Chapter 5
 - Measured boot Chapter 5
 - Boot attestation Chapter 5
- Database Chapter 5
 - Tokenization Chapter 5, 11
 - Salting Chapter 5, 10
 - Hashing Chapter 5, 10
- Application security Chapter 5, 7
 - Input validations Chapter 7
 - Secure cookies Chapter 7
 - Hypertext Transfer Protocol (HTTP) headers Chapter 7
 - Code signing Chapter 7
 - Allow list Chapter 5
 - Block list/deny list Chapter 5
 - Secure coding practices Chapter 7
 - Static code analysis Chapter 7
 - Manual code review Chapter 7
 - Dynamic code analysis Chapter 7

- Fuzzing Chapter 7
- Hardening Chapter 5
 - Open ports and services Chapter 5
 - Registry Chapter 5
 - Disk encryption Chapter 5
 - OS Chapter 5
 - Patch management Chapter 5
 - Third-party updates Chapter 5
 - Auto-update Chapter 5
- Self-encrypting drive (SED)/ full disk encryption (FDE) Chapter 5
 - Opal Chapter 5
- Hardware root of trust Chapter 5
- Trusted Platform Module (TPM) Chapter 5
- Sandboxing Chapter 7

3.3 Given a scenario, implement secure network designs. Chapters 1, 3, 4, 5, 6, 9

- Load balancing Chapter 9
 - Active/active Chapter 9
 - Active/passive Chapter 9
 - Scheduling Chapter 9
 - Virtual IP Chapter 9
 - Persistence Chapter 9
- Network segmentation Chapter 3
 - Virtual local area network (VLAN) Chapter 3
 - Screened subnet (previously known as demilitarized zone) Chapter 3
 - East-west traffic Chapter 3
 - Extranet Chapter 3
 - Intranet Chapter 3
 - Zero trust Chapter 3
- Virtual private network (VPN) Chapter 4
 - Always on Chapter 4
 - Split tunnel vs. full tunnel Chapter 4
 - Remote access vs. site-to-site Chapter 4
 - IPSec Chapter 4
 - SSL/TLS Chapter 4
 - HTML5 Chapter 4

- Layer 2 tunneling protocol (L2TP) Chapter 4
- DNS Chapter 3
- Network access control (NAC) Chapter 4
 - Agent and agentless Chapter 4
- Out-of-band management Chapter 4
- Port security Chapter 3, 4
 - Broadcast storm prevention Chapter 3
 - Bridge Protocol Data Unit (BPDUs) guard Chapter 3
 - Loop prevention Chapter 3
 - Dynamic Host Configuration Protocol (DHCP) snooping Chapter 3
 - Media access control (MAC) filtering Chapter 4
- Network appliances Chapter 3
 - Jump servers Chapter 3
 - Proxy servers Chapter 3
 - Forward Chapter 3
 - Reverse Chapter 3
 - Network-based intrusion detection system (NIDS)/network-based intrusion prevention system (NIPS) Chapter 4
 - Signature based Chapter 4
 - Heuristic/behavior Chapter 4
 - Anomaly Chapter 4
 - Inline vs. passive Chapter 4
 - HSM Chapter 5
 - Sensors Chapter 4
 - Collectors Chapter 4
 - Aggregators Chapter 4
 - Firewalls Chapter 3
 - Web application firewall (WAF) Chapter 3
 - NGFW Chapter 3
 - Stateful Chapter 3
 - Stateless Chapter 3
 - Unified threat management (UTM) Chapter 3
 - Network address translation (NAT) gateway Chapter 3

- Content/URL filter Chapter 3
- Open-source vs. proprietary Chapter 3
- Hardware vs. software Chapter 3
- Appliance vs. host-based vs. virtual Chapter 3
- Access control list (ACL) Chapter 3
- Route security Chapter 3
- Quality of service (QoS) Chapter 3
- Implications of IPv6 Chapter 3
- Port spanning/port mirroring Chapter 4
 - Port taps Chapter 4
- Monitoring services Chapter 1
- File integrity monitors Chapter 6

3.4 Given a scenario, install and configure wireless security settings. Chapter 4

- Cryptographic protocols Chapter 4
 - WiFi protected access 2 (WPA2) Chapter 4
 - WiFi protected access 3 (WPA3) Chapter 4
 - Counter-mode/CBC-MAC protocol (CCMP) Chapter 4
 - Simultaneous Authentication of Equals (SAE) Chapter 4
- Authentication protocols Chapter 4
 - Extensible Authentication Protocol (EAP) Chapter 4
 - Protected Extensible Application Protocol (PEAP) Chapter 4
 - EAP-FAST Chapter 4
 - EAP-TLS Chapter 4
 - EAP-TTLS Chapter 4
 - IEEE 802.1X Chapter 4
 - Remote Authentication Dial-in User Server (RADIUS) Federation Chapter 4
- Methods Chapter 4
 - Pre-shared key (PSK) vs. Enterprise vs. Open Chapter 4
 - WiFi Protected Setup (WPS) Chapter 4
 - Captive portals Chapter 4
- Installation considerations Chapter 4
 - Site surveys Chapter 4
 - Heat maps Chapter 4
 - WiFi analyzers Chapter 4

- Channel overlaps Chapter 4
- Wireless access point (WAP) placement Chapter 4
- Controller and access point security Chapter 4

3.5 Given a scenario, implement secure mobile solutions. Chapter 5

- Connection methods and receivers Chapter 5
 - Cellular Chapter 5
 - WiFi Chapter 5
 - Bluetooth Chapter 5
 - NFC Chapter 5
 - Infrared Chapter 5
 - USB Chapter 5
 - Point-to-point Chapter 5
 - Point-to-multipoint Chapter 5
 - Global Positioning System (GPS) Chapter 5
 - RFID Chapter 5
- Mobile device management (MDM) Chapter 5
 - Application management Chapter 5
 - Content management Chapter 5
 - Remote wipe Chapter 5
 - Geofencing Chapter 5
 - Geolocation Chapter 5
 - Screen locks Chapter 5
 - Push notifications Chapter 5
 - Passwords and pins Chapter 5
 - Biometrics Chapter 5
 - Context-aware authentication Chapter 5
 - Containerization Chapter 5
 - Storage segmentation Chapter 5
 - Full device encryption Chapter 5
- Mobile devices Chapter 5
 - MicroSD hardware security module (HSM) Chapter 5
 - MDM/Unified Endpoint Management (UEM) Chapter 5
 - Mobile application management (MAM) Chapter 5
 - SEAndroid Chapter 5
- Enforcement and monitoring of: Chapter 5
 - Third-party app stores Chapter 5

- Rooting/jailbreaking Chapter 5
- Sideload Chapter 5
- Custom firmware Chapter 5
- Carrier unlocking Chapter 5
- Firmware over-the-air (OTA) updates Chapter 5
- Camera use Chapter 5
- SMS/Multimedia Message Service (MMS)/Rich Communication Services (RCS) Chapter 5
- External media Chapter 5
- USB On-The-Go (OTG) Chapter 5
- Recording microphone Chapter 5
- GPS tagging Chapter 5
- WiFi direct/ad hoc Chapter 5
- Tethering Chapter 5
- Hotspot Chapter 5
- Payment methods Chapter 5
- Deployment models Chapter 5
 - Bring your own device (BYOD) Chapter 5
 - Corporate-owned personally enabled (COPE) Chapter 5
 - Choose your own device (CYOD) Chapter 5
 - Corporate-owned Chapter 5
 - Virtual desktop infrastructure (VDI) Chapter 5

3.6 Given a scenario, apply cybersecurity solutions to the cloud. Chapter 5

- Cloud security controls Chapter 5
 - High availability across zones Chapter 5
 - Resource policies Chapter 5
 - Secrets management Chapter 5
 - Integration and auditing Chapter 5
 - Storage Chapter 5
 - Permissions Chapter 5
 - Encryption Chapter 5
 - Replication Chapter 5
 - High availability Chapter 5
 - Network Chapter 5
 - Virtual networks Chapter 5
 - Public and private subnets Chapter 5

- Segmentation Chapter 5
 - API inspection and integration Chapter 5
- Compute Chapter 5
 - Security groups Chapter 5
 - Dynamic resource allocation Chapter 5
 - Instance awareness Chapter 5
 - Virtual private cloud (VPC) endpoint Chapter 5
 - Container security Chapter 5
- Solutions Chapter 5
 - CASB Chapter 5
 - Application security Chapter 5
 - Next-generation secure web gateway (SWG) Chapter 5
 - Firewall considerations in a cloud environment Chapter 5
 - Cost Chapter 5
 - Need for segmentation Chapter 5
 - Open Systems Interconnection (OSI) layers Chapter 5
- Cloud native controls vs. third-party solutions Chapter 5

3.7 Given a scenario, implement identity and account management controls.

Chapters 2, 5, 10

- Identity Chapter 2
 - Identity provider (IdP) Chapter 2
 - Attributes Chapter 2
 - Certificates Chapter 2, Chapter 10
 - Tokens Chapter 2
 - SSH keys Chapter 2
 - Smart cards Chapter 2
- Account types Chapter 2
 - User account Chapter 2
 - Shared and generic accounts/credentials Chapter 2
 - Guest accounts Chapter 2
 - Service accounts Chapter 2
- Account policies Chapter 2
 - Password complexity Chapter 2
 - Password history Chapter 2
 - Password reuse Chapter 2

- Network location Chapter 2
- Geofencing Chapter 5
- Geotagging Chapter 5
- Geolocation Chapter 2
- Time-based logins Chapter 2
- Access policies Chapter 2
- Account permissions Chapter 2
- Account audits Chapter 2
- Impossible travel time/risky login Chapter 2
- Lockout Chapter 2
- Disablement Chapter 2

3.8 Given a scenario, implement authentication and authorization solutions.

Chapters 2, 4, 5

- Authentication management Chapter 2
 - Password keys Chapter 2
 - Password vaults Chapter 2
 - TPM Chapter 5
 - HSM Chapter 5
 - Knowledge-based authentication Chapter 2
- Authentication/authorization Chapter 2, 4
 - EAP Chapter 4
 - Challenge Handshake Authentication Protocol (CHAP) Chapter 4
 - Password Authentication Protocol (PAP) Chapter 4
 - 802.1X Chapter 4
 - RADIUS Chapter 4
 - Single sign-on (SSO) Chapter 2
 - Security Assertion Markup Language (SAML) Chapter 2
 - Terminal Access Controller Access Control System Plus (TACACS+) Chapter 4
 - OAuth Chapter 2
 - OpenID Chapter 2
 - Kerberos Chapter 2
- Access control schemes Chapter 2
 - Attribute-based access control (ABAC) Chapter 2
 - Role-based access control Chapter 2

- Rule-based access control Chapter 2
- MAC Chapter 2
- Discretionary access control (DAC) Chapter 2
- Conditional access Chapter 2
- Privileged access management Chapter 2
- Filesystem permissions Chapter 2

3.9 Given a scenario, implement public key infrastructure. Chapter 10

- Public key infrastructure (PKI) Chapter 10
 - Key management Chapter 10
 - Certificate authority (CA) Chapter 10
 - Intermediate CA Chapter 10
 - Registration authority (RA) Chapter 10
 - Certificate revocation list (CRL) Chapter 10
 - Certificate attributes Chapter 10
 - Online Certificate Status Protocol (OCSP) Chapter 10
 - Certificate signing request (CSR) Chapter 10
 - CN Chapter 10
 - Subject alternative name Chapter 10
 - Expiration Chapter 10
- Types of certificates Chapter 10
 - Wildcard Chapter 10
 - Subject alternative name Chapter 10
 - Code signing Chapter 10
 - Self-signed Chapter 10
 - Machine/computer Chapter 10
 - Email Chapter 10
 - User Chapter 10
 - Root Chapter 10
 - Domain validation Chapter 10
 - Extended validation Chapter 10
- Certificate formats Chapter 10
 - Distinguished encoding rules (DER) Chapter 10
 - Privacy enhanced mail (PEM) Chapter 10
 - Personal information exchange (PFX) Chapter 10
 - .cer Chapter 10
 - P12 Chapter 10

- P7B Chapter 10
- Concepts Chapter 10
 - Online vs. offline CA Chapter 10
 - Stapling Chapter 10
 - Pinning Chapter 10
 - Trust model Chapter 10
 - Key escrow Chapter 10
 - Certificate chaining Chapter 10

4.0 Operations and Incident Response

4.1 Given a scenario, use the appropriate tool to assess organizational security.
Chapters 1, 3, 6, 7, 8, 11

- Network reconnaissance and discovery Chapter 1, 3, 6, 8
 - tracert/traceroute Chapter 1
 - nslookup/dig Chapter 3
 - ipconfig/ifconfig Chapter 1
 - nmap Chapter 8
 - ping/pathping Chapter 1
 - hping Chapter 1,
 - netstat Chapter 1
 - netcat Chapter 8
 - IP scanners Chapter 8
 - arp Chapter 1
 - route Chapter 3
 - curl Chapter 8
 - theHarvester Chapter 8
 - sn1per Chapter 8
 - scanless Chapter 8
 - dnsenum Chapter 8
 - Nessus Chapter 8
 - Cuckoo Chapter 6
- File manipulation Chapter 1
 - head Chapter 1
 - tail Chapter 1
 - cat Chapter 1
 - grep Chapter 1

- chmod Chapter 1
- logger Chapter 1
- Shell and script environments Chapter 7
 - SSH Chapter 7
 - PowerShell Chapter 7
 - Python Chapter 7
 - OpenSSL Chapter 7
- Packet capture and replay Chapter 8
 - Tcpreplay Chapter 8
 - Tcpdump Chapter 8
 - Wireshark Chapter 8
- Forensics Chapter 11
 - dd Chapter 11
 - Memdump Chapter 11
 - WinHex Chapter 11
 - FTK imager Chapter 11
 - Autopsy Chapter 11
- Exploitation frameworks Chapter 8
- Password crackers Chapter 8
- Data sanitization Chapter 11

4.2 Summarize the importance of policies, processes, and procedures for incident response. Chapters 7, 9, 11

- Incident response plans Chapter 11
- Incident response process Chapter 11
 - Preparation Chapter 11
 - Identification Chapter 11
 - Containment Chapter 11
 - Eradication Chapter 11
 - Recovery Chapter 11
 - Lessons learned Chapter 11
- Exercises Chapter 9
 - Tabletop Chapter 9
 - Walkthroughs Chapter 9
 - Simulations Chapter 9
- Attack frameworks Chapter 7
 - MITRE ATT&CK Chapter 7

- The Diamond Model of Intrusion Analysis Chapter 7
- Cyber Kill Chain Chapter 7
- Stakeholder management Chapter 11
- Communication plan Chapter 11
- Disaster recovery plan Chapter 9
- Business continuity plan Chapter 9
- Continuity of operation planning (COOP) Chapter 9
- Incident response team Chapter 11
- Retention policies Chapter 11

4.3 Given an incident, utilize appropriate data sources to support an investigation.

Chapter 1, 2, 3, 7, 8, 11

- Vulnerability scan output Chapter 8
- SIEM dashboards Chapter 1
 - Sensor Chapter 1
 - Sensitivity Chapter 1
 - Trends Chapter 1
 - Alerts Chapter 1
 - Correlation Chapter 1
- Log files Chapter 1, 3
 - Network Chapter 1
 - System Chapter 1
 - Application Chapter 1
 - Security Chapter 1
 - Web Chapter 7
 - DNS Chapter 7
 - Authentication Chapter 2
 - Dump files Chapter 11
 - VoIP and call managers Chapter 3
 - Session Initiation Protocol (SIP) traffic Chapter 3
- syslog/rsyslog/syslog-ng Chapter 1
- journalctl Chapter 1
- NXlog Chapter 1
- Bandwidth monitors Chapter 11
- Metadata Chapter 11
 - Email Chapter 11
 - Mobile Chapter 11

- Web Chapter 11
- File Chapter 11
- Netflow/sFlow Chapter 8
 - Netflow Chapter 8
 - SFlow Chapter 8
 - IPfix Chapter 8
- Protocol analyzer output Chapter 8

4.4 Given an incident, apply mitigation techniques or controls to secure an environment. Chapters 3, 5, 10, 11

- Reconfigure endpoint security solutions Chapter 5
 - Application approved list Chapter 5
 - Application blocklist/deny list Chapter 5
 - Quarantine Chapter 5
- Configuration changes Chapters 5, 10
 - Firewall rules Chapter 5
 - MDM Chapter 5
 - DLP Chapter 5
 - Content filter/URL filter Chapter 5
 - Update or revoke certificates Chapter 10
- Isolation Chapter 3, Chapter 11
- Containment Chapter 11
- Segmentation Chapter 3
- SOAR Chapter 11
 - Runbooks Chapter 11
 - Playbooks Chapter 11

4.5 Explain the key aspects of digital forensics. Chapter 11

- Documentation/evidence Chapter 11
 - Legal hold Chapter 11
 - Video Chapter 11
 - Admissibility Chapter 11
 - Chain of custody Chapter 11
 - Timelines of sequence of events Chapter 11
 - Time stamps Chapter 11
 - Time offset Chapter 11
 - Tags Chapter 11
 - Reports Chapter 11

- Event logs Chapter 11
- Interviews Chapter 11
- Acquisition Chapter 11
 - Order of volatility Chapter 11
 - Disk Chapter 11
 - Random-access memory (RAM) Chapter 11
 - Swap/pagefile Chapter 11
 - OS Chapter 11
 - Device Chapter 11
 - Firmware Chapter 11
 - Snapshot Chapter 11
 - Cache Chapter 11
 - Network Chapter 11
 - Artifacts Chapter 11
- On-premises vs. cloud Chapter 11
 - Right to audit clauses Chapter 11
 - Regulatory/jurisdiction Chapter 11
 - Data breach notification laws Chapter 11
- Integrity Chapter 11
 - Hashing Chapter 11
 - Checksums Chapter 11
 - Provenance Chapter 11
- Preservation Chapter 11
- E-discovery Chapter 11
- Data recovery Chapter 11
- Non-repudiation Chapter 11
- Strategic intelligence/ counterintelligence Chapter 11

5.0 Governance, Risk, and Compliance

5.1 Compare and contrast various types of controls. Chapters 1, 9

- Category Chapter 1
 - Managerial Chapter 1
 - Operational Chapter 1
 - Technical Chapter 1
- Control type Chapter 1
 - Preventive Chapter 1

- Detective Chapter 1
- Corrective Chapter 1
- Deterrent Chapter 1
- Compensating Chapter 1
- Physical Chapter 1, 9

5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture. Chapters 5, 8, 11

- Regulations, standards, and legislation Chapter 11
 - General Data Protection Regulation (GDPR) Chapter 11
 - National, territory, or state laws Chapter 11
 - Payment Card Industry Data Security Standard (PCI DSS) Chapter 8
- Key frameworks Chapter 5, 8, 11
 - Center for Internet Security (CIS) Chapter 8
 - National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)/Cybersecurity Framework (CSF) Chapter 8
 - International Organization for Standardization (ISO) 27001/27002/27701/31000 Chapter 8
 - SSAE SOC 2 Type I/II Chapter 8
 - Cloud security alliance Chapter 5
 - Cloud control matrix Chapter 5
 - Reference architecture Chapter 8
- Benchmarks /secure configuration guides Chapter 8
 - Platform/vendor-specific guides Chapter 8
 - Web server Chapter 8
 - OS Chapter 8
 - Application server Chapter 8
 - Network infrastructure devices Chapter 8

5.3 Explain the importance of policies to organizational security. Chapters 2, 5, 7, 9, 11

- Personnel Chapter 11
 - Acceptable use policy Chapter 11
 - Job rotation Chapter 11
 - Mandatory vacation Chapter 11
 - Separation of duties Chapter 11

- Least privilege Chapter 11
- Clean desk space Chapter 11
- Background checks Chapter 11
- Non-disclosure agreement (NDA) Chapter 11
- Social media analysis Chapter 11
- Onboarding Chapter 11
- Offboarding Chapter 11
- User training Chapter 11
 - Gamification Chapter 11
 - Capture the flag Chapter 11
 - Phishing campaigns Chapter 11
 - Phishing simulations Chapter 11
 - Computer-based training (CBT) Chapter 11
 - Role-based training Chapter 11
- Diversity of training techniques Chapter 11
- Third-party risk management Chapter 11
 - Vendors Chapter 11
 - Supply chain Chapter 11
 - Business partners Chapter 11
 - Service level agreement (SLA) Chapter 11
 - Memorandum of understanding (MOU) Chapter 11
 - Measurement systems analysis (MSA) Chapter 11
 - Business partnership agreement (BPA) Chapter 11
 - End of life (EOL) Chapter 11
 - End of service life (EOS) Chapter 11
 - NDA Chapter 11
- Data Chapter 11
 - Classification Chapter 11
 - Governance Chapter 11
 - Retention Chapter 11
- Credential policies Chapter 2
 - Personnel Chapter 2
 - Third party Chapter 2
 - Devices Chapter 2
 - Service accounts Chapter 2
 - Administrator/root accounts Chapter 2

- Organizational policies Chapters 5, 7, 9
 - Change management Chapter 5
 - Change control Chapter 7
 - Asset management Chapter 9

5.4 Summarize risk management processes and concepts. Chapters 8, 9, 11

- Risk types Chapter 8
 - External Chapter 8
 - Internal Chapter 8
 - Legacy systems Chapter 8
 - Multiparty Chapter 8
 - IP theft Chapter 8
 - Software compliance/licensing Chapter 8
- Risk management strategies Chapter 8
 - Acceptance Chapter 8
 - Avoidance Chapter 8
 - Transference Chapter 8
 - Cybersecurity insurance Chapter 8
 - Mitigation Chapter 8
- Risk analysis Chapter 8, 11
 - Risk register Chapter 8
 - Risk matrix/heat map Chapter 8
 - Risk control assessment Chapter 8
 - Risk control self-assessment Chapter 8
 - Risk awareness Chapter 8
 - Inherent risk Chapter 8
 - Residual risk Chapter 8
 - Control risk Chapter 8
 - Risk appetite Chapter 8
 - Regulations that affect risk posture Chapter 11
 - Risk assessment types Chapter 8
 - Qualitative Chapter 8
 - Quantitative Chapter 8
 - Likelihood of occurrence Chapter 8
 - Impact Chapter 8
 - Asset value Chapter 8

- Single loss expectancy (SLE) Chapter 8
- Annualized loss expectancy (ALE) Chapter 8
- Annualized rate of occurrence (ARO) Chapter 8
- Disasters Chapter 9
 - Environmental Chapter 9
 - Person-made Chapter 9
 - Internal vs. external Chapter 9
- Business impact analysis Chapter 9
 - Recovery time objective (RTO) Chapter 9
 - Recovery point objective (RPO) Chapter 9
 - Mean time to repair (MTTR) Chapter 9
 - Mean time between failures (MTBF) Chapter 9
 - Functional recovery plans Chapter 9
 - Single point of failure Chapter 9
 - Disaster recovery plan (DRP) Chapter 9
 - Mission essential functions Chapter 9
 - Identification of critical systems Chapter 9
 - Site risk assessment Chapter 9

5.5 Explain privacy and sensitive data concepts in relation to security.

Chapter 11

- Organizational consequences of privacy and data breaches Chapter 11
 - Reputation damage Chapter 11
 - Identity theft Chapter 11
 - Fines Chapter 11
 - IP theft Chapter 11
- Notifications of breaches Chapter 11
 - Escalation Chapter 11
 - Public notifications and disclosures Chapter 11
- Data types Chapter 11
 - Classifications Chapter 11
 - Public Chapter 11
 - Private Chapter 11
 - Sensitive Chapter 11
 - Confidential Chapter 11
 - Critical Chapter 11

- Proprietary Chapter 11
- Personally identifiable information (PII) Chapter 11
- Health information Chapter 11
- Financial information Chapter 11
- Government data Chapter 11
- Customer data Chapter 11
- Privacy enhancing technologies Chapter 11
 - Data minimization Chapter 11
 - Data masking Chapter 11
 - Tokenization Chapter 11
 - Anonymization Chapter 11
 - Pseudo-anonymization Chapter 11
- Roles and responsibilities Chapter 11
 - Data owners Chapter 11
 - Data controller Chapter 11
 - Data processor Chapter 11
 - Data custodian/steward Chapter 11
 - Data protection officer (DPO) Chapter 11
- Information life cycle Chapter 11
- Impact assessment Chapter 11
- Terms of agreement Chapter 11
- Privacy notice Chapter 11

Recertification Requirements

The CompTIA Security+ certification was previously a lifetime certification. You passed the exam once, and you were certified for life. However, if you take it now, the certification expires after three years unless you renew it.

You can renew the certification by either taking the next version of the exam or by enrolling in CompTIA's Continuing Education (CE) program. You will be required to pay an annual fee and complete Continuing Education Units (CEUs). You can earn CEUs through a variety of activities. Some examples include presenting or teaching topics to others, attending training sessions, participating in industry events or seminars, or writing relevant articles, white papers, blogs, or books.

For full details, check out the CompTIA website:
<https://certification.comptia.org/>. Unfortunately, CompTIA frequently changes its URLs, so I didn't list the specific URL for CEU policies. However, you can usually find it by searching on their site or using their Contact Us page.

601 Pre-Assessment Exam

Use this assessment exam to test your knowledge of the topics before you start reading the book, and again before you take the live exam. An answer key with explanations is available at the end of the assessment exam.

1. Your organization is planning to expand the data center to support more systems. Management wants the plan to focus on resiliency and uptime. Which of the following methods would best support these goals? (Select TWO.)
 - A. UPS
 - B. Cold site
 - C. NIC teaming
 - D. Off-site backups

2. You are tasked with improving the overall security of several servers in your data center. Which of the following are preventive controls that will assist with this goal? (Choose TWO.)
 - A. Disabling unnecessary services
 - B. Adding cable locks
 - C. Monitoring logs on SIEM systems
 - D. Implementing a backup plan
 - E. Closing unneeded ports

3. Your organization houses a server room, and management wants to increase the server room security. You are tasked with identifying some deterrent controls that can be implemented to protect it. Which of the following choices would BEST meet this objective?
 - A. Hardware locks
 - B. Data encryption
 - C. A vulnerability assessment
 - D. Backups

4. You suspect that a Linux computer is establishing connections with a remote server on the Internet without any user interaction. You want to verify this by viewing a summary of protocol statistics on a Linux system. Which of the following commands would you use?

- A. dig
- B. nslookup
- C. ifconfig
- D. netstat

5. You are using a Linux computer to monitor network traffic. After connecting your computer to the mirror port of a switch, you started logging software on the computer. However, you discover that the only traffic being collected is traffic to or from the Linux computer. You want to collect all traffic going through the switch. Which of the following actions should you take?

- A. Run the command ifconfig eth0 promisc.
- B. Run the command ipconfig eth0 promisc.
- C. Connect the computer to a router.
- D. Reconfigure the switch.

6. You suspect that attackers have been performing a password spraying attack against a Linux server. Which of the following would be the BEST method of confirming your suspicions?

- A. Use the cat command to view the *auth.log* file.
- B. Implement an account lockout policy.
- C. Salt passwords to prevent the success of the spraying attack.
- D. Use the logger command to view unsuccessful logins.

7. Your network includes dozens of servers. Administrators in your organization are having problems aggregating and correlating the logs from these servers. Which of the following provides the BEST solution for these problems?

- A. SIEM
- B. Syslog
- C. NetFlow
- D. sFlow

8. You are comparing different types of authentication. Of the following choices, which one uses multifactor authentication?
- A. A system that requires users to enter a username and password
 - B. A system that checks an employee's fingerprint and does a vein scan
 - C. A cipher door lock that requires employees to enter a code to open the door
 - D. A system that requires users to have a smart card and a PIN
9. The chief information officer (CIO) at your organization suspects someone is entering the data center after normal working hours and stealing sensitive data. Which of the following actions can prevent this?
- A. Upgrade the CCTV system.
 - B. Require smart cards to enter the data center.
 - C. Implement time-based logins.
 - D. Enable advanced auditing.
10. A SQL database server was recently attacked. Cybersecurity investigators discovered the attack was self-propagating through the network. When it found the database server, it used well-known credentials to access the database. Which of the following would be the BEST action to prevent this from occurring again?
- A. Change the default application password.
 - B. This describes a worm.
 - C. Implement 2FA.
 - D. Conduct a code review.
11. You are reviewing security controls and their usefulness. You notice that account lockout policies are in place. Which of the following attacks will these policies thwart? (Select TWO.)
- A. Brute force
 - B. DNS poisoning
 - C. Dictionary
 - D. Replay
 - E. Buffer overflow

12. IT administrators created a VPN for employees to use while working from home. The VPN is configured to provide AAA services. Which of the following would be presented to the AAA system for identification?

- A. Password
- B. Permissions
- C. Username identification
- D. Tunneling certificate
- E. Hardware token

13. After a recent attack, security investigators discovered that attackers logged on with an administrator account. They recommend implementing a solution that will thwart this type of attack in the future. The solution must support the following requirements:

- Allow authorized users to access the administrator account without knowing the password.
- Allow authorized users to check out the credentials when needed.
- Log each time the credentials are used.
- Automatically change the password.

Which of the following answers would meet these requirements?

- A. Privileged access management
- B. OpenID Connect
- C. MAC scheme
- D. MFA

14. Lisa wants to implement a secure authentication system on a website. However, instead of collecting and storing user passwords, she wants to use a third-party system. Which of the following is the BEST choice to meet this goal?

- A. SAML
- B. Kerberos
- C. SSH
- D. OAuth

15. Your organization is implementing an SDN. Management wants to use an access control scheme that controls access based on attributes. Which of the following is the BEST solution?

- A. DAC
- B. MAC
- C. Role-BAC
- D. ABAC

16. Lisa uses a Linux system to regularly connect to a remote server named gcga with a secure ssh connection. However, the ssh account has a complex password, and she wants to avoid using it without sacrificing security. Which of the following commands would she use as a FIRST step when creating a passwordless login with the remote system?

- A. ssh-copy-id -i ~.ssh/id_rsa.pub lisa@gcga
- B. chmod 644 ~/.ssh/id_rsa
- C. ssh-keygen -t rsa
- D. ssh root@gcga

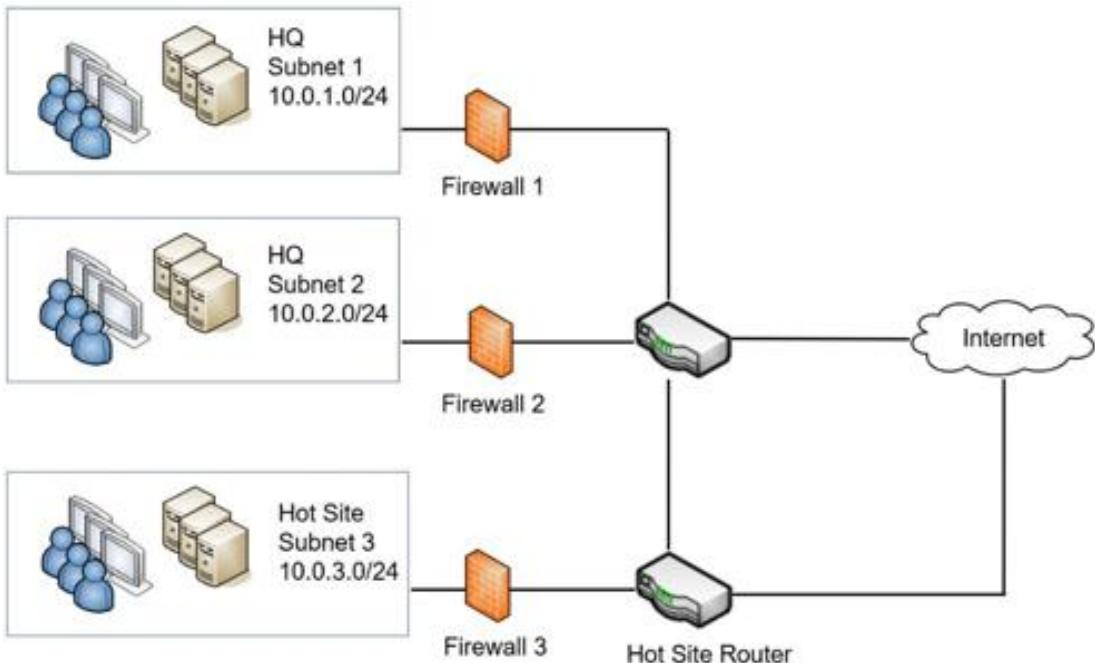
17. Your organization plans to deploy a server in the screened subnet that will perform the following functions:

- Identify mail servers
- Provide data integrity
- Prevent poisoning attacks
- Respond to requests for A and AAAA records

Which of the following will BEST meet these requirements?

- A. DNS
- B. DNSSEC
- C. TLS
- D. ESP

18. Your organization has added a hot site as shown in the following graphic.



All firewalls should enforce the following requirements:

- Use only secure protocols for remote management
- Block cleartext web traffic

Users in the hot site are unable to access websites in the Internet. The following graphic shows the current rules configured in Firewall 3.

Rule	Destination	Source	Protocol	Action
HTTPS Outbound	Any	10.0.3.0/24	HTTPS	Allow
HTTP Outbound	Any	10.0.3.0/24	HTTP	Block
DNS	Any	10.0.1.0/24	DNS	Allow
HTTPS Inbound	10.0.3.0/24	Any	HTTPS	Allow
HTTP Inbound	10.0.3.0/24	Any	HTTP	Block
Telnet	10.0.3.0/24	Any	Telnet	Block
SSH	10.0.3.0/24	Any	SSH	Allow

You're asked to verify the rules are configured correctly. Which rule, if any, should be changed in Firewall 3?

- HTTPS Outbound
- HTTP Outbound
- DNS
- Telnet
- SSH
- None. All rules are correct.

19. Bart incorrectly wired a switch in your organization's network. It effectively disabled the switch as though it was a victim of a denial-of-service attack. Which of the following should be done to prevent this situation in the future?

- A. Install an IDS.
- B. Only use Layer 2 switches.
- C. Install SNMPv3 on the switches.
- D. Implement STP or RSTP.

20. Maggie is a sales representative for a software company. While in a coffee shop, she uses her laptop to connect to the public Wi-Fi, check her work emails, and upload details of a recent sale. Which of the following would she use to prevent other devices on the public network from accessing her laptop? (Choose the BEST two choices.)

- A. TPM
- B. HSM
- C. Firewall
- D. DLP
- E. VPN

21. Your organization wants to combine some of the security controls used to control incoming and outgoing network traffic. At a minimum, the solution should include stateless inspection, malware inspection, and a content filter. Which of the following BEST meets this goal?

- A. VLAN
- B. NAT
- C. UTM
- D. DNSSEC
- E. WAF

22. Administrators are deploying a new Linux server in the screened subnet. After it is installed, they want to manage it from their desktop computers located within the organization's private network. Which of the following would be the BEST choice to meet this need?

- A. Forward proxy server

- B. Reverse proxy server
- C. Web application firewall
- D. Jump server

23. Attackers have recently launched several attacks against servers in your organization's DMZ. You are tasked with identifying a solution that will have the best chance at preventing these attacks in the future. Which of the following is the BEST choice?

- A. An anomaly-based IDS
- B. An inline IPS
- C. A passive IDS
- D. A signature-based IDS

24. A coffee shop recently stopped broadcasting the SSID (coffeewifi) for its wireless network. Instead, paying customers can view it on their receipt and use it to connect to the coffee shop's wireless network. Today, Lisa turned on her laptop computer, saw the SSID coffewifi, and connected to it. Which of the following attacks is MOST likely occurring?

- A. Rogue AP
- B. Evil twin
- C. Jamming
- D. Bluejacking

25. Before personnel can enter a secure area, they must first place their smartphones in one of several conductive metal lockboxes. The company implemented this policy because management is concerned about risks related to intellectual property. Which of the following represents the GREATEST risk to intellectual property that this policy will mitigate?

- A. Bluesnarfing
- B. Theft of the smartphones
- C. Data exfiltration over a mobile hotspot
- D. To enable geofencing

26. Administrators are designing a site-to-site VPN between offices in two different cities. Management mandated the use of certificates for mutual

authentication. Additionally, they want to ensure that internal IP addresses are not revealed. Which of the following is the BEST choice to meet these requirements?

- A. IPsec VPN using Tunnel mode
 - B. IPsec VPN using Transport mode
 - C. L2TP VPN
 - D. VLAN VPN
27. Network administrators are considering adding an HSM to a server in your network. What functions will this add to the server?
- A. Provide full drive encryption
 - B. Reduce the risk of employees emailing confidential information outside the organization
 - C. Provide webmail to clients
 - D. Generate and store keys used with servers
28. Bart needs to send an email to his supervisor with an attachment that includes sensitive information. He wants to maintain the confidentiality of this information. Which of the following choices is the BEST choice to meet his needs?
- A. Digital signature
 - B. Encryption
 - C. Data masking
 - D. Hashing
29. The Springfield school system stores some data in the cloud using its own resources. The Shelbyville Nuclear Power Plant also stores some data in the cloud using its own resources. Later, the two organizations decide to share some data in both clouds for educational purposes. Which of the following BEST describes the cloud created by these two organizations?
- A. Community
 - B. Private
 - C. Public
 - D. XaaS

30. Your organization is planning to implement a CYOD deployment model. You're asked to provide input for the new policy. Which of the following concepts are appropriate for this policy?

- A. SCADA access
- B. Storage segmentation
- C. Database security
- D. Embedded RTOS

31. Your organization plans to implement desktops via the cloud. Each desktop will include an operating system and a core group of applications needed by employees, and the cloud provider will manage the desktops. Employees with Internet access will be able to access these desktops from anywhere and almost any device. Which of the following BEST identifies this service?

- A. IaaS
- B. CASB
- C. SaaS
- D. XaaS

32. A small business owner has asked you for advice. She wants to improve the company's security posture, but she doesn't have any security staff. Which of the following is the BEST solution to meet her needs?

- A. SOAR
- B. MSSP
- C. SaaS
- D. XaaS

33. Management at the Goody New Shoes retail chain decided to allow employees to connect to the internal network using their personal mobile devices. However, the organization is having problems with these devices, including the following:

- Employees do not keep their devices updated.
- There is no standardization among the devices.
- The organization doesn't have adequate control over the devices.

Management wants to implement a mobile device deployment model to overcome these problems while still allowing employees to use their own devices. Which of the following is the BEST choice?

- A. BYOD
- B. COPE
- C. CYOD
- D. IaaS

34. During a vulnerability scan, you discover some new systems in the network. After investigating this, you verify that these systems aren't authorized because someone installed them without going through a standard approval process. What does this describe?

- A. Hacktivist
- B. Script kiddie
- C. Shadow IT
- D. Authorized hacker

35. Homer recently received a phishing email with a malicious attachment. He was curious so he opened it to see what it was. It installed malware on his system, and quickly spread to other systems in the network. Security investigators discovered that the malware exploited a vulnerability that wasn't previously known by any trusted sources. Which of the following BEST describes this attack?

- A. Open source intelligence
- B. Zero-day
- C. Hoax
- D. DDoS

36. Lisa completed an antivirus scan on a server and detected a Trojan. She removed the Trojan but was concerned that unauthorized personnel might still be able to access data on the server and decided to check the server further. Of the following choices, what is she MOST likely looking for on this server?

- A. Backdoor
- B. Logic bomb
- C. Rootkit

D. Botnet

37. Some network appliances monitoring incoming data have recently started sending alerts on potentially malicious files. You discover that these are PE32 files with the *tar.gz* extension, and they are being downloaded to several user systems. After investigating further, you discover these users previously opened an email with an infected MHT file. Which of the following answers BEST describes this scenario?

- A. The systems have joined a botnet.
- B. Users installed ransomware.
- C. Users installed a RAT, and it is downloading additional tools.
- D. Shadow IT is running in the network.

38. Employees at the Marvin Monroe Memorial Hospital are unable to access any computer data. Instead, they occasionally see a message indicating that attackers encrypted all the data and it would remain encrypted until the attackers received a hefty sum as payment. Which of the following BEST describes this attack?

- A. Criminal syndicate
- B. Ransomware
- C. Fileless virus
- D. Rootkit

39. A SIEM system is sending several alerts indicating malware has infected several employee computers. After examining the border firewall and NIDS logs, IT personnel cannot identify malicious traffic entering the network from the Internet. Additionally, they discover that all of these employees attended a trade show during the past two days. Which of the following is the MOST likely source of this malware?

- A. A fileless virus embedded in a vCard
- B. Malware on USB drives
- C. A Trojan delivered from a botnet
- D. Worms included in presentation media

40. Homer received an email letting him know he won the lottery. To claim the prize, he needs to confirm his identity by providing his name, phone

number, address, and birth date. The email states he'll receive the prize after providing this information. What does this describe?

- A. Spear phishing
- B. Phishing
- C. Smishing
- D. Whaling

41. Some protocols include sequence numbers and timestamps. Which of the following attacks are thwarted by using these components?

- A. MAC flooding
- B. Replay
- C. SYN flood
- D. Salting

42. You're reviewing the logs for a web server and see several suspicious entries. You suspect that an attacker is attempting to write more data into a web application's memory than it can handle. What does this describe?

- A. Pointer/object dereference
- B. Race condition exploit
- C. DLL injection attack
- D. Buffer overflow attack

43. Your organization hosts a web application selling digital products. Customers can also post comments related to their purchases. Management suspects that attackers are looking for vulnerabilities that they can exploit. Which of the following will BEST test the cybersecurity resilience of this application?

- A. Fuzzing
- B. Input validation
- C. Error handling
- D. Anti-malware

44. An attacker has launched several successful XSS attacks on a web application hosted by your organization. Which of the following are the BEST choices to protect the web application and prevent this attack? (Select TWO.)

- A. Dynamic code analysis
- B. Input validation
- C. Code obfuscation
- D. WAF
- E. Normalization

45. Hacker Harry has an account on a website that he uses when posting comments. When he visits, he enters his username and password to log on, and the site displays his username with any comments he makes. Today, he noticed that he could enter JavaScript code as part of his username. After entering the code, other users experienced unexpected results when hovering over his username. What does this describe?

- A. Cross-site scripting
- B. Input validation
- C. Privilege escalation
- D. Directory traversal

46. Which of the following BEST describes the purpose of a risk register?

- A. It shows risks on a plot or graph.
- B. It provides a listing of risks, the risk owner, and the mitigation measures.
- C. It shows risks on a color-coded graph.
- D. It evaluates the supply chain.

47. Maggie is performing a risk assessment for an organization. She identifies the loss for the previous year due to a specific risk as \$5,000. What does this represent?

- A. SLE
- B. ARO
- C. MTBF
- D. ALE

48. Ziffcorp is developing a new technology that they expect to become a huge success when it's released. The CIO is concerned about someone stealing their company secrets related to this technology. Which of the

following will help the CIO identify potential dangers related to the loss of this technology?

- A. Threat hunting
- B. Vulnerability scan
- C. SOAR
- D. SIEM

49. Your organization hired a cybersecurity expert to perform a security assessment. After running a vulnerability scan, she sees the following error on a web server:

- Host IP 192.168.1.10 OS Apache httpd 2.433 Vulnerable to mod_auth exploit

However, she verified that the mod_auth module has not been installed or enabled on the server. Which of the following BEST explains this scenario?

- A. A false negative
- B. A false positive
- C. The result of a credentialed scan
- D. The result of a non-credentialed scan

50. You are reviewing a report created after a recent vulnerability scan. However, it isn't clear if the scan was run as a credentialed scan or a non-credentialed scan. Which of the following would give you the BEST indication that the scan was a credentialed scan?

- A. The report shows software versions of installed applications.
- B. The report shows a large number of false positives.
- C. The report shows a listing of IP addresses it discovered.
- D. The report shows a listing of open ports.

51. Your IT department includes a subgroup of employees dedicated to cybersecurity testing. Each member of this group has knowledge of known TTPs and how to use them. Additionally, each member of this group has knowledge of security controls that would be implemented to protect network resources. Which of the following BEST describes members of this team?

- A. Members of the red team
- B. Members of the blue team

- C. Members of the purple team
- D. Members of the white team

52. You suspect servers in your screened subnet are being attacked by an Internet-based attacker. You want to view IPv4 packet data reaching these servers from the Internet. Which of the following would be the BEST choice to meet this need?

- A. Protocol analyzer
- B. IP scanner
- C. Vulnerability scanner
- D. Proxy server
- E. Heuristic-based IDS

53. Your organization has decided to move some data to a cloud provider, and management has narrowed their search down to three possible choices. Management wants to ensure that the cloud provider they choose has strong cybersecurity controls in place. Which of the following reports would they MOST likely want the cloud provider to give to them?

- A. SOC 2 Type I
- B. SOC 2 Type II
- C. SOC 3
- D. SOC 1

54. You need to identify and mitigate potential single points of failure in your organization's security operations. Which of the following policies would help you?

- A. A disaster recovery plan
- B. A business impact analysis
- C. Annualized loss expectancy
- D. Separation of duties

55. Administrators at your organization want to increase cybersecurity resilience of key servers by adding fault tolerance capabilities. However, they have a limited budget. Which of the following is the BEST choice to meet these needs?

- A. Alternate processing site

- B. RAID-10
- C. Backups
- D. Faraday cage

56. Your organization's backup policy for a file server dictates that the amount of time needed to restore backups should be minimized. Which of the following backup plans would BEST meet this need?

- A. Full backups on Sunday and incremental backups on the other six days of the week
- B. Full backups on Sunday and differential backups on the other six days of the week
- C. Incremental backups on Sunday and differential backups on the other six days of the week
- D. Differential backups on Sunday and incremental backups on the other six days of the week

57. A security analyst recently completed a BIA and defined the maximum acceptable outage time for a critical system. What does this identify?

- A. RTO
- B. RPO
- C. MTTR
- D. MTBF

58. The new chief technology officer (CTO) at your organization wants to ensure that critical business systems are protected from isolated outages. Which of the following would let her know how often these systems will experience outages?

- A. MTTR
- B. MTBF
- C. RTO
- D. RPO

59. The Ninth National Bank of Springfield is considering an alternate location as part of its continuity of operations plan. It wants to identify a site resiliency solution that provides the shortest recovery time. Which of the following is the BEST choice?

- A. Cold site
- B. Warm site
- C. Hot site
- D. Snapshot

60. Cybersecurity experts in your organization are creating a detailed plan identifying how to recover critical systems if these systems suffer a complete loss. What type of plan are they MOST likely creating?

- A. Backup plan
- B. Incident response plan
- C. Communications plan
- D. Disaster recovery plan

61. Your organization is planning to expand its cloud-based services offered to the public. In preparation, they expanded the data center. It currently has one row of racks for servers, but they plan to add at least one more row of racks for servers. Engineers calculated the power and HVAC requirements and said the best way to reduce utility costs is by ensuring the two server rows are facing in the opposite direction. What is the primary reason for this configuration?

- A. To provide fire suppression
- B. To reduce power consumption from the servers
- C. To create hot and cold aisles
- D. To create an air gap

62. As a security administrator, you receive an antivirus alert from a server in your network indicating one of the files has a hash of known malware. The file was pushed to the server from the organization's patch management system and is scheduled to be applied to the server early the next morning. The antivirus software indicates that the file and hash of the malware are:

- File: gcga_upgrade.exe
- Hash: 518b571e26035d95e5e9232b4affbd84

Checking the logs of the patch management system, you see the following information:

Status	Update Name	Hash
-----------------	--------------------	---------------

Pushed gcga_upgrade.exe
518b571e26035d95e5e9232b4affbd84

Which of the following indicates what MOST likely occurred?

- A. The file was infected after it was pushed out to the server.
- B. The file was embedded with crypto-malware before it was pushed to the server.
- C. The file was listed in the patch management system's blacklist.
- D. The file was infected when the patch management system downloaded it.

63. An organization requested bids for a contract and asked companies to submit their bids via email. After winning the bid, Bizzfad realized it couldn't meet the requirements of the contract. Bizzfad instead stated that it never submitted the bid. Which of the following would provide proof to the organization that Bizzfad did submit the bid, if it was used?

- A. Digital signature
- B. Integrity
- C. Repudiation
- D. Encryption

64. An application requires users to log on with passwords. The application developers want to store the passwords in such a way that it will thwart rainbow table attacks. Which of the following is the BEST solution?

- A. Implement salting.
- B. Implement hashing.
- C. Implement homomorphic encryption.
- D. Implement perfect forward secrecy.

65. Your SIEM system sent an alert related to multiple failed logins. Reviewing the logs, you notice login failures for about 100 different accounts. The logs then show the same accounts indicate login failures starting about three hours after the first login failure. Which of the following BEST describes this activity?

- A. A brute force attack
- B. A dictionary attack
- C. A spraying attack

D. An account lockout attack

66. Your organization maintains a data center to store data. Management has decided to move a large amount of financial data into cloud storage to reduce costs with the data center. This data is regularly accessed and sometimes manipulated by employees, customers, and vendors around the world. Management has mandated that the data always needs to be encrypted while in the cloud. Which of the following is the BEST choice to meet these requirements?

- A. Symmetric encryption
- B. Asymmetric encryption
- C. Homomorphic encryption
- D. Steganography encryption

67. Lisa and Bart need to exchange emails over the Internet using an unsecured channel. These emails need to provide non-repudiation. They decide to use certificates on each of their computers. What would they use to sign their certificates?

- A. CRL
- B. OCSP
- C. CSR
- D. CA
- E. DSA

68. An administrator is installing a certificate with a private key on a server. Which of the following certificate types is he MOST likely installing?

- A. DER
- B. P12
- C. CER
- D. P7B

69. Your organization is negotiating with an outside vendor to host cloud-based resources. Management wants to ensure the vendor commits to returning the systems to full operation after an outage within a certain time frame. Which of the following is the organization MOST likely negotiating?

- A. MTTR
- B. NDA
- C. SLA
- D. DLP

70. Your organization has hired outside consultants to evaluate forensic processes used by internal security specialists. The consultants are evaluating the tools and processes used for digital forensics to identify any variations that may exist. Which of the following BEST describes what these consultants are performing?

- A. AUP
- B. NDA
- C. SLA
- D. MSA

71. Your organization recently developed an incident response policy and is beginning to implement an incident response plan. Which of the following items is the FIRST step in an incident response process?

- A. Preparation
- B. Identification
- C. Containment
- D. Eradication

72. Security administrators have been responding to an increasing number of incident alerts, making it harder for them to respond to each promptly. Management wants to implement a solution that will automate the response of some of these incidents without requiring real-time involvement by security administrators. Which of the following will BEST meet this need?

- A. SOAR
- B. DLP
- C. STIX
- D. TAXII

73. Security administrators have isolated a Linux server after a successful attack. A forensic analyst is tasked with creating an image of the hard drive

of this system for analysis. Which of the following will the analyst MOST likely use to create the image?

- A. tcpreplay
- B. chmod
- C. dd
- D. Cuckoo

74. A forensic expert is preparing to analyze a hard drive. Which of the following should the expert do FIRST?

- A. Capture an image of the disk with dd.
- B. Identify the order of volatility.
- C. Copy the contents of memory with memdump.
- D. Create a chain of custody document.

75. Your company hosts an e-commerce site that sells renewable subscriptions for services. Customers can choose to renew their subscription monthly or annually automatically. However, management doesn't want to store customer credit card information on any database or system managed by the company. Which of the following can be used instead?

- A. Pseudo-anonymization
- B. Tokenization
- C. Data minimization
- D. Anonymization

Pre-Assessment Exam Answers

When checking your answers, take the time to read the explanations. Understanding the explanations will help ensure you're prepared for the live exam. The explanation also shows the chapter or chapters where you can get more detailed information on the topic.

1. **A** and **C** are correct. An uninterruptible power supply (UPS) and network interface card (NIC) teaming support resiliency and uptime goals. The UPS ensures the system stays up if power is lost. NIC teaming automatically recovers if one of the NICs or NIC inputs fail. Resiliency methods help systems heal themselves and recover from faults automatically. A cold site cannot take over automatically and is not quick. Off-site backups would need to be retrieved and applied by a person, so they aren't automatic. See Chapter 1.
2. **A** and **E** are correct. Disabling unnecessary services and closing unneeded ports are steps you can take to harden a server. They are preventive controls because they help prevent an incident. Cable locks are a type of physical control and are typically used on laptops, not on servers. Monitoring logs on security information and event management (SIEM) systems is a detective control. A backup plan is a corrective control. See Chapter 1.
3. **A** is correct. Hardware locks are deterrent controls because they would deter someone from entering or accessing the servers in bays if bay door locks are used. They are also examples of physical controls. None of the other answers increase the security of the server room. Data encryption is a technical control designed to protect data on the servers. A vulnerability assessment is a managerial control designed to discover vulnerabilities. Backups are corrective controls designed to reverse the impact of data loss or corruption. See Chapter 1.
4. **D** is correct. The **netstat -s** command will display a summary of protocol statistics on a Linux system. You can use the **dig** (short for domain

information proper) command on Linux systems to query Domain Name System (DNS) servers and verify if you can resolve names to IP addresses. The **nslookup** (short for name server lookup) command can also be used to query DNS servers. The **ifconfig** command is used to display information and configure network interfaces on Linux systems. See Chapter 1.

5. A is correct. You should run the command **ifconfig eth0 promisc** to enable promiscuous mode on eth0, the network interface card (NIC). Promiscuous mode allows a NIC to process all traffic it receives, instead of only traffic addressed to it. The **ipconfig** command is used on Windows systems and doesn't support this feature. The scenario indicates she wants to collect traffic going through the switch, so connecting to a router isn't necessary. Port mirroring on a switch sends a copy of all traffic received by the switch to the mirror port. The scenario indicates this is configured, so the switch doesn't need to be reconfigured. See Chapter 1.

6. A is correct. The **cat** command (short for concatenate) displays the entire contents of a file and the *auth.log* file shows all unsuccessful (and successful) logins, and this is the only choice of the available answers that confirms past activity. An account lockout policy locks an account after too many incorrect passwords within a certain time frame, but a spraying attack uses a time lapse between each password attempt to bypass an account lockout policy. Salting passwords is often used to prevent rainbow table-based attacks, but salts aren't effective against spraying attacks. The **logger** command is used to add log entries into the syslog file but doesn't examine log entries. See Chapter 1.

7. A is correct. A security information and event management (SIEM) system collects, aggregates, and correlates logs from multiple sources. Syslog is a protocol that specifies log entry formats that many SIEMs use. It is also the name of a log on Linux systems. NetFlow is a network protocol (developed by Cisco) used to collect and monitor network traffic. The sFlow (short for sampled flow) protocol is used to collect a sampling of network traffic for monitoring. See Chapter 1.

8. **D** is correct. A system that requires users to have a smart card and a personal identification number (PIN) uses multifactor authentication or two-factor authentication. The card is in the something you have factor, and the PIN is in the something you know factor. A username provides identification, and a password is in the something you know factor, providing single-factor authentication. Fingerprints and vein scans are both in the something you are factor, providing single-factor authentication. A code for a cipher door lock is in the something you know factor, providing single-factor authentication. See Chapter 2.

9. **C** is correct. Time-based logins (sometimes called time-of-day restrictions) would prevent this. They would prevent anyone from logging in after normal working hours and accessing sensitive data. All of the other answers can detect suspicious behavior, but they wouldn't prevent the users from logging in after normal working hours and stealing the data. See Chapter 2.

10. **A** is correct. The default application password for the SQL server should be changed. Some SQL Server software implementations can have a default blank password for the SA account (the System Administrator account), and these default credentials are well-known. While the scenario describes a worm because it is self-propagating, the question is asking for the best preventive action to take. Using two-factor authentication (2FA) is a good practice for users, but it isn't always feasible for application passwords. A code review can detect flaws and vulnerabilities in internally developed applications, but SQL Server is Microsoft software. See Chapter 2.

11. **A** and **C** are correct. Brute force and dictionary attacks attempt to guess passwords, but an account lockout control locks an account after the wrong password is guessed too many times. The other attacks are not password attacks, so they aren't mitigated using account lockout controls. Domain Name System (DNS) poisoning attempts to redirect web browsers to malicious URLs. Replay attacks attempt to capture packets to impersonate one of the parties in an online session. Buffer overflow attacks attempt to

overwhelm online applications with unexpected code or data. See Chapters 2 and 10.

12. **C** is correct. Users would typically enter a username as identification for an authentication, authorization, and accounting (AAA) system. Users would provide a password as proof that the claimed identity (the username) is theirs. The password provides authentication. Users are assigned permissions based on their proven identity, but the permissions do not provide authentication. The virtual private network (VPN) would encrypt traffic sent via the VPN tunnel, and this traffic may be encrypted with the use of a certificate. However, this is not called a tunneling certificate, and the certificate used for encryption does not provide identification. A hardware token is often used as an additional method of authentication, but it does not provide identification. See Chapter 2.

13. **A** is correct. A privileged access management system protects and limits access to privileged accounts such as administrator accounts. OpenID Connect is used for authentication and authorization on the Internet, not internal networks. A mandatory access control (MAC) scheme uses labels to control access, but it isn't used to control access to administrator accounts. Multifactor authentication (MFA) uses more than one factor of authentication, but it doesn't meet any of the requirements of this scenario. See Chapter 2.

14. **A** is correct. Security Assertion Markup Language (SAML) is a single sign-on SSO solution that can use third-party websites, and it provides authentication. Kerberos is an SSO solution used on internal networks such as in Microsoft Active Directory domains. Secure Shell (SSH) is used for remote administration. OAuth (think of this as Open Authorization) is used for authorization, but the scenario wants a solution for authentication. See Chapter 2.

15. **D** is correct. A software-defined network (SDN) typically uses an attribute-based access control (ABAC) scheme. The ABAC scheme is based on attributes that identify subjects and objects within a policy. A

discretionary access control (DAC) scheme has an owner, and the owner establishes access for the objects. A mandatory access control (MAC) scheme uses labels assigned to subjects and objects. A role-based access control scheme uses roles or groups to assign rights and permissions. See Chapter 2.

16. **C** is correct. The first step would be to enter **ssh-keygen -t rsa** at the terminal. This creates an RSA-based key pair (a private key and a public key). The public key's location and the name is `~/.ssh/id_rsa.pub`, and the private key's location and the name is `~/.ssh/id_rsa`. The second step is to copy the public key to the remote server using the command **ssh-copy-id -i ~.ssh/id_rsa.pub lisa@gcga**. The private key should always stay private, but the **chmod 644** command makes it readable by everyone, so it shouldn't be used. The **ssh** command connects to the remote server using Secure Shell (SSH). If the key pair is in place, it would use the key pair for authentication and not require the complex password. The **ssh-keygen** command is a utility within the OpenSSH suite of tools. See Chapter 3.

17. **B** is correct. Domain Name System Security Extensions (DNSSEC) add security to DNS systems and can prevent DNS poisoning attacks by adding data integrity to DNS records. The functions in the list indicate that the server in the screened subnet (sometimes called a demilitarized zone or DMZ) is a DNS server but for the DNS server to provide data integrity and prevent DNS poisoning, it needs DNSSEC. DNSSEC uses a Resource Record Signature (RRSIG), commonly referred to as a digital signature, to provide data integrity and authentication for DNS replies. RRSIG can use Transport Layer Security (TLS) to create the signature, but TLS by itself doesn't provide the required protection. Internet Protocol security (IPsec) uses Encapsulating Security Payload (ESP) to encrypt data. See Chapter 3.

18. **C** is correct. The Domain Name System (DNS) rule should be changed because the source IP address is incorrect. It should be 10.0.3.0/24 instead of 10.0.1.0/24. All other rules are configured correctly. See Chapter 3.

19. **D** is correct. Spanning Tree Protocol (STP) and Rapid STP (RSTP) both prevent switching loop problems. It's rare for a wiring error to take down a

switch. However, if two ports on a switch are connected to each other, it creates a switching loop and effectively disables the switch. An intrusion detection system (IDS) will not prevent a switching loop. Layer 2 switches are susceptible to this problem. Administrators use Simple Network Management Protocol version 3 (SNMPv3) to manage and monitor devices, but it doesn't prevent switching loops. See Chapter 3.

20. **C** and **E** are correct. A firewall and a virtual private network (VPN) would prevent other devices from accessing her laptop. A host-based firewall provides primary protection. The VPN encrypts all of her Internet-based traffic going over the public Wi-Fi. A Trusted Platform Module (TPM) provides full drive encryption and would protect the data if someone accessed the laptop, but it doesn't prevent access. A hardware security module (HSM) is a removable device that can generate and store RSA keys used with servers. A data loss prevention (DLP) device helps prevent unauthorized data from leaving a network, but it doesn't prevent access. See Chapter 3.

21. **C** is correct. A unified threat management (UTM) device is an advanced firewall and combines multiple security controls into a single device such as stateless inspection, malware inspection, and a content filter. None of the other answers include these components. You can configure a virtual local area network (VLAN) on a switch to provide network segmentation. Network Address Translation (NAT) translates public IP addresses to private IP addresses and private addresses back to public IP addresses. Domain Name System Security Extensions (DNSSEC) is a suite of extensions for DNS that provides validation for DNS responses. A web application firewall (WAF) protects a web server from Internet-based attacks. See Chapter 3.

22. **D** is correct. A jump server is a server placed between different security zones, such as an internal network and a screened subnet (sometimes called a demilitarized zone or DMZ) and is used to manage devices in the other security zone. In this scenario, administrators could connect to the jump server with Secure Shell (SSH) and then connect to the Linux server using SSH forwarding on the jump server. A forward proxy server (often called a

proxy server) is used by internal clients to access Internet resources, not resources in the screened subnet. Reverse proxy servers accept traffic from the Internet, not the internal network, and forward the traffic to one or more internal web servers. A web application firewall (WAF) protects a web server from Internet-based attacks but isn't used to control traffic between an internal network and the screened subnet. See Chapter 3.

23. **B** is correct. The best solution of the given choices is an in-band intrusion prevention system (IPS). Traffic goes through the IPS, and the IPS can prevent attacks from reaching internal systems. An intrusion detection system (IDS) is passive and not inline, so it can only detect and react to the attacks, not block them. A signature-based IDS can detect known attacks based on the attack's signature, but there isn't any indication that the past attacks were known. See Chapter 4.

24. **B** is correct. An evil twin is a rogue access point (AP) with the same or similar service set identifier (SSID) as a legitimate access point. The actual SSID coffeewifi has broadcasting turned off, but the evil twin SSID of coffewifi is broadcasting, allowing users to see it. While it is also a rogue AP, evil twin is a more accurate answer since it is similar to the actual SSID. Jamming typically prevents anyone from connecting to a wireless network. Bluejacking is related to Bluetooth, not wireless networks. See Chapter 4.

25. **A** is correct. This policy will prevent bluesnarfing, which is the unauthorized access of information from a wireless device through a Bluetooth connection. The conductive metal lockboxes act as a small Faraday cage and will block Bluetooth signals. While the lockboxes will help prevent theft, there's no need to pay extra for conductive lockboxes if theft is the greatest risk. Hotspots are typically in public locations. A company would set up a network providing Wi-Fi access, not a hotspot. Geofencing creates a virtual fence using GPS, but devices within a Faraday cage wouldn't be able to reach GPS. See Chapter 4.

26. **A** is correct. Internet Protocol security (IPsec) using Tunnel mode is the best choice of the available answers. IPsec provides mutual authentication,

and Tunnel mode will encrypt both the payload and the packet headers, hiding the internal IP addresses. Transport mode will encrypt the payload only, leaving the internal IP addresses exposed. A VPN using Layer 2 Tunneling Protocol (L2TP) only doesn't provide any encryption. Virtual local area networks (VLANs) provide network segmentation but can't be used as a VPN. See Chapter 4.

27. **D** is correct. A hardware security module (HSM) is a removable device that can generate and store RSA keys used with servers. The keys can be used to encrypt data sent to and from the server, but they wouldn't be used for full drive encryption. A Trusted Platform Module (TPM) provides full drive encryption and is included in many laptops. A data loss prevention (DLP) device is a device that can reduce the risk of employees emailing confidential information outside the organization. Software as a Service (SaaS) provides software or applications, such as webmail, via the cloud. See Chapter 5.

28. **B** is correct. Encryption is the best choice to provide confidentiality of any type of information, including sensitive information. A digital signature provides integrity, non-repudiation, and authentication. Data masking modifies the original data, producing data that looks valid but is not authentic. Hashing provides integrity. See Chapter 5.

29. **A** is correct. They created a community cloud. In the scenario, the two organizations have a common goal of sharing educational materials. The individual clouds created by each organization are private clouds, but the shared community cloud resources are not private. A public cloud would be available to anyone, but the scenario wants to restrict access to just two organizations. Anything as a Service (XaaS) refers to cloud services beyond IaaS, PaaS, and SaaS. See Chapter 5.

30. **B** is correct. Storage segmentation creates separate storage areas in mobile devices and can be used with a choose your own device (CYOD) mobile device deployment model where users own their devices. None of the other answers are directly related to mobile devices. A supervisory control and data acquisition (SCADA) system controls industrial control

systems (ICSs), such as those used in nuclear power plants or water treatment facilities, and SCADA systems should be isolated. Database security includes the use of permissions and encryption to protect data in a database but is unrelated to mobile device deployment. Some embedded systems use a real-time operating system (RTOS) when the system must react within a specific time. See Chapter 5.

31. **D** is correct. Anything as a Service (XaaS) refers to cloud services beyond IaaS, PaaS, and SaaS. It would include desktops as a service. Infrastructure as a Service (IaaS) is a cloud computing option where the vendor provides access to a computer. Still, customers must install the operating system and maintain the system. A cloud access security broker (CASB) is a software tool used to provide additional security for cloud resources, but it provides the underlying cloud services. Software as a Service (SaaS) provides access to specific applications such as an email application, but not entire desktops. See Chapter 5.

32. **B** is correct. A managed security service provider (MSSP) is a third-party vendor that provides security services for an organization, and it is the best solution for this scenario. A Security Orchestration, Automation, and Response (SOAR) solution automates incident response for some events, but it will augment services already provided by security staff within an organization. SOAR would not work here because the small business doesn't have any security staff. Software as a Service (SaaS) includes any software or application provided to users over a network such as the Internet. Anything as a Service (XaaS) refers to cloud services beyond SaaS, IaaS, and PaaS. See Chapter 5.

33. **C** is correct. A choose your own device (CYOD) mobile device deployment model includes a list of acceptable devices that employees can purchase and connect to the network. IT management can then implement a mobile device management (MDM) system to provide standardized management for these devices. The current policy is a bring your own device (BYOD) policy, but because of the lack of standardization, it's difficult for IT departments to adequately manage the devices and ensure they don't introduce vulnerabilities to the network. A corporate-owned

personally enabled (COPE) policy indicates the organization owns the devices, not the employees. Infrastructure as a Service (IaaS) is a cloud computing option where the vendor provides access to a computer, but customers must install the operating system and maintain the system. See Chapter 5.

34. **C** is correct. Shadow IT refers to any systems or applications installed on a network without authorization or approval. Employees often add them to bypass security controls. A hacktivist launches attacks as part of an activist movement or to further a cause. A script kiddie is an attacker who uses existing computer scripts or code to launch attacks and typically has limited technical skills. An authorized hacker (sometimes referred to as a white hat attacker) is a security professional working within the law to protect an organization from attackers. See Chapter 6.

35. **B** is correct. A zero-day exploit is one that isn't known by trusted sources such as antivirus vendors or operating system vendors. Attackers use open source intelligence to identify a target. Some typical sources are social media sites and news outlets. A hoax is not a specific attack. It is a message, often circulated through email that tells of impending doom from a virus or other security threat that simply doesn't exist. A distributed denial-of-service (DDoS) attack comes from multiple sources, not as a single phishing email. See Chapter 6.

36. **A** is correct. She is most likely looking for a backdoor because Trojans commonly create backdoors, and a backdoor allows unauthorized personnel to access data on the system. Logic bombs and rootkits can create backdoor accounts, but Trojans don't create logic bombs and would rarely install a rootkit. The computer might be joined to a botnet, but a botnet is a group of computers. See Chapter 6.

37. **C** is correct. This indicates that users installed a remote access Trojan (RAT) when they opened the email containing the malicious MHT file. An MHT file (or MHTML) is a webpage archive, and it will store HTML, CSS, images, JavaScript, and anything else in the webpage. After installing the RAT, attackers later began downloading Portable Executable (PE32) files to

the compromised systems. While the systems may have joined a botnet, the scenario doesn't indicate that they are part of a botnet. Ransomware would indicate that it has controlled the user's computer or data, but this isn't indicated in this scenario. Shadow information technology (IT) refers to any unauthorized systems or applications within an organization. See Chapter 6.

38. **B** is correct. The scenario describes ransomware, where attackers typically encrypt data and demand payment to release the data. Although the attack might have been launched by a criminal syndicate because their motivation is primarily money, the question is asking about the attack, not the attacker. A fileless virus injects code into existing scripts and may install ransomware, but a fileless virus is not ransomware. A rootkit is a program or group of programs that provide root-level access to a system but hides itself to evade detection. See Chapter 6.

39. **A** is correct. The most likely source (of the given answers) is a fileless virus embedded in a vCard, also known as a Virtual Contact File (VCF). People regularly share contact information at trade shows with vCards, but they can sometimes include malicious code. The scenario doesn't mention USB drives. Malicious traffic from a botnet comes from the Internet, but administrators didn't detect any malicious traffic from the Internet. Speakers use presentation media (such as PowerPoint presentations) while speaking, but viewing presentation media won't infect systems. See Chapter 6.

40. **B** is correct. This describes a phishing email that is trying to trick the user into revealing personal information. Spear phishing targets a group of people with a common connection, such as employees of a company. Smishing is a form of phishing that uses text messages. Whaling is a form of spear phishing that targets high-level executives in an organization. See Chapter 6.

41. **B** is correct. Timestamps and sequence numbers act as countermeasures against replay attacks. None of the other choices are attacks that timestamps and sequence numbers can thwart. A media access control (MAC) flood attack attempts to overload a switch with different MAC addresses. SYN

(synchronize) flood attacks disrupt the TCP three-way handshake. Salting isn't an attack, but it does protect against brute force attacks on passwords. See Chapter 7.

42. **D** is correct. A buffer overflow attack attempts to write more data into an application's memory than it can handle. A pointer or object dereference is a programming error that can corrupt memory, but programmers, not attackers, cause it. A race condition is a programming conflict when two or more applications or application models attempt to access or modify a resource at the same time. A Dynamic Link Library (DLL) injection attack injects a DLL into memory and causes it to run. See Chapter 7.

43. **A** is correct. Fuzzing is a type of dynamic code analysis, and it can test the application's cybersecurity resilience. Fuzzing sends random data to an application to verify the random data doesn't crash the application or expose the system to a data breach. Input validation and error-handling techniques protect applications but do not test them. Anti-malware protects systems from malware attacks, but it doesn't test a system. See Chapter 7.

44. **B** and **D** are correct. Input validation and a web application firewall (WAF) are the best choices of the available answers. Both protect against cross-site scripting (XSS) attacks. Input validation validates data before using it to help prevent XSS attacks. A WAF acts as an additional firewall that monitors, filters, and/or blocks HTTP traffic to a web server. None of the other answers will directly prevent XSS attacks. Dynamic code analysis (such as fuzzing) can test code. Code obfuscation makes the code more difficult to read. Normalization refers to organizing tables and columns in a database to reduce redundant data and improve overall database performance. See Chapters 2 and 7.

45. **A** is correct. This is an example of a cross-site scripting (XSS) attack. It can be prevented by using proper input validation techniques to prevent users from entering malicious code into a site's text box. Privilege escalation techniques attempt to give an attacker more rights and permissions. In a directory traversal attack, the attacker can navigate a system's directory structure and read files. See Chapter 7.

46. **B** is correct. A risk register lists risks and often includes the name of the risk, the risk owner, mitigation measures, and a risk score. A risk matrix plots risks onto a graph or chart, and a heat map plots risks onto a color-coded graph or chart. While a risk register may evaluate supply chain risks, it does much more. See Chapter 8.

47. **D** is correct. The annual loss expectancy (ALE) identifies the expected loss for a given year based on a specific risk and existing security controls. The single loss expectancy (SLE) identifies the cost of any single loss. The annual rate of occurrence (ARO) identifies how many times a loss is expected to occur in a year. Multiplying SLE \times ARO identifies the ALE. Note that the scenario refers to a specific risk, but it doesn't indicate how many times the loss occurred. This could have been five incidents (ARO of 5) incurring losses of \$1,000 for each incident (SLE), resulting in an ALE of \$5,000. The mean time between failures (MTBF) provides a measure of a system's reliability and is usually represented in hours. See Chapter 8.

48. **A** is correct. Threat hunting is the process of actively looking for threats within a network before an automated tool detects and reports on the threat. It typically includes several elements. A vulnerability scan evaluates vulnerabilities (or weaknesses) with a network or a specific system, but it doesn't look for threats. A Secure Orchestration, Automation, and Response (SOAR) platform can be configured to automatically respond to low-level incidents, but this scenario indicates that they need to look for more than just low-level threats. A security information and event management (SIEM) is used to collect and aggregate logs and can assist with threat hunting, but threat hunting is much broader. See Chapter 8.

49. **B** is correct. This is an example of a false positive. The vulnerability scanner is indicating a vulnerability exists with the mod_auth module. However, the mod_auth module is not installed or enabled on the server, so it cannot represent a vulnerability on the server. A false negative occurs when a vulnerability exists, but the scanner doesn't report it. The scenario doesn't give enough information to determine if this is a credentialed or a non-credentialed scan. However, a credentialed scan would allow a

vulnerability scanner to have more visibility over the systems it scans, allowing it to get a more accurate view of the systems. See Chapter 8.

50. **A** is correct. A credentialed scan will show software versions of installed applications. A credentialed scan will show fewer false positives, not more. Any scan should list IP addresses it discovered along with open ports on these hosts. See Chapter 8.

51. **C** is correct. A purple team is composed of personnel who can perform as either red team members or blue team members. A red team attacks and they often use tactics, techniques, and procedures (TTPs) that attackers have used in actual attacks. A blue team defends, and they would know about various security controls used to protect network resources. The white team wasn't mentioned in the scenario, but they don't perform any testing but instead set the rules and oversee the testing. See Chapter 8.

52. **A** is correct. A protocol analyzer can capture and analyze packets on a network. An IP scanner (sometimes called a network scanner) identifies hosts within a network by identifying active IP addresses and additional information about each active host. Vulnerability scanners scan hosts within a network looking for vulnerabilities. Proxy servers (also known as forward proxy servers) forward requests for services from a client. Heuristic-based (sometimes called behavior-based) intrusion detection systems (IDSs) detect intrusions by identifying anomalies. See Chapter 8.

53. **B** is correct. A System and Organization Controls (SOC) 2 report is a report on organizational controls that cover cybersecurity. A SOC 2 Type II report identifies the controls in place during a date range of at least six months. A SOC 2 Type I report identifies the controls in place during a specific date. A SOC 3 report is a generalized report sometimes available to the public. A SOC 1 report is a detailed report covering financial and auditable controls for an organization and is sometimes provided by organizations that process financial data. See Chapter 8.

54. **D** is correct. A separation of duties policy is the best answer. In this context, if only one person can perform tasks within the organization's

security operations, that person becomes a single point of failure. None of the other answers address a single point of failure. A disaster recovery plan (DRP) identifies how to recover critical systems and data after a disaster. A business impact analysis (BIA) helps an organization identify critical systems and components. An annualized loss expectancy (ALE) identifies the expected annual loss from a known risk. See Chapter 9.

55. **B** is correct. A redundant array of inexpensive disks 10 (RAID-10) subsystem provides fault tolerance for disks and increases cybersecurity resilience. In this context, cybersecurity resilience refers to a system's ability to continue to operate even after an adverse event. An alternate processing site can provide cybersecurity resilience for an entire site, but it is expensive and does much more than provide fault tolerance for some servers. Backups contribute to cybersecurity resilience, but they do not help with fault tolerance. A Faraday cage is a room or enclosure that prevents signals from emanating beyond the room. See Chapter 9.

56. **B** is correct. A full/differential backup strategy is best with one full backup on one day and differential backups on the other days. A restore would require only two backups, making it quicker than the other options. A full/incremental backup would typically require you to restore more than two backups. For example, data loss on Friday would require you to restore the full backup, plus four incremental backups. Backups must start with a full backup, so neither an incremental/differential nor a differential/incremental backup strategy is possible. See Chapter 9.

57. **A** is correct. A recovery time objective (RTO) identifies the maximum amount of time it can take to restore a system after an outage. It is directly related to the maximum acceptable outage time defined in a business impact analysis (BIA). None of the other answers are related to the maximum acceptable outage time. A recovery point objective (**RPO**) identifies a point in time where data loss is acceptable, and refers to databases. The mean time between failures (**MTBF**) provides a measure of a system's reliability and is usually represented in hours. The mean time to recover (**MTTR**) identifies the average (the arithmetic mean) time it takes to restore a failed system. See Chapter 9.

58. **B** is correct. The mean time between failures (MTBF) provides a measure of a system's reliability and would provide an estimate of how often the systems will experience outages. The mean time to recover (MTTR) refers to the time it takes to restore a system, not the time between failures. The recovery time objective (RTO) identifies the maximum amount of time it can take to restore a system after an outage. The recovery point objective (RPO) identifies a point in time where data loss is acceptable. See Chapter 9.

59. **C** is correct. A hot site has the shortest recovery time, but it is also the most expensive. Cold sites have the longest recovery time and are the least expensive. Warm sites have a shorter recovery time than cold sites but a longer recovery time than hot sites. A snapshot backup provides a backup of a disk at a moment in time and is sometimes used in digital forensics. See Chapter 9.

60. **D** is correct. A disaster recovery plan (DRP) identifies how to recover critical systems after a disaster. Backup plans are typically focused on backing up and restoring data, not systems. An incident response plan is implemented after a security incident, but all security incidents do not result in a complete loss of systems. A communications plan is part of an incident response plan and provides direction on how to communicate issues related to an incident. See Chapter 9.

61. **C** is correct. Hot and cold aisles have server rows facing the opposite direction and provide more efficient cooling systems within a data center. This results in reduced costs for the heating, ventilation, and air conditioning (HVAC) system and subsequently reduces power consumption to keep the data center cool. This does not reduce the power consumption of the servers. Hot and cold aisles do not provide fire suppression. An air gap ensures systems are not connected to the same network, but the scenario indicates the servers will be connected for the cloud-based servers. See Chapter 9.

62. **D** is correct. Of the given choices, the file was most likely infected when the patch management system downloaded it. This is because the name and hash of the file is the same on the server as it is on the patch management system. If it were infected after it was pushed out to the server, it would have a different hash. The scenario doesn't indicate what type of infection the malware has, so it isn't possible to tell if it is crypto-malware or another type of malware. A blacklist blocks files so if the file were listed in the patch management system's blacklist, the patch management system wouldn't push it out to systems. See Chapter 10.

63. **A** is correct. If BizzFad submitted the bid via email using a digital signature, it would provide proof that BizzFad submitted the bid. Digital signatures provide verification of who sent a message, non-repudiation preventing them from denying it, and integrity verifying the message wasn't modified. Integrity verifies the message wasn't modified. Repudiation isn't a valid security concept. Encryption protects the confidentiality of data, but it doesn't verify who sent it or provide non-repudiation. See Chapter 10.

64. **A** is correct. Salting passwords is a common method of preventing rainbow table attacks. Salting adds additional data to the password before hashing it. Rainbow table attacks use precomputed hashes to discover passwords so hashing the passwords won't thwart rainbow table attacks. Homomorphic encryption is used to protect data stored in cloud environments and it allows data to remain encrypted while it is being processed. Perfect forward secrecy is related to encryption and indicates that a cryptographic system generates random keys for each session. See Chapter 10.

65. **C** is correct. This describes a spraying attack. The security information and event management (SIEM) logs would show that the attack loops through a long list of accounts, guessing one password for one account at a time. A brute force attack attempts to guess all possible character combinations for a password, and a dictionary attack uses a dictionary of words trying to discover the correct password. However, neither a brute force attack nor a dictionary attack loops through a list of user accounts. A

spraying attack attempts to bypass an account lockout policy. An account lockout attack isn't relevant in this scenario. See Chapter 10.

66. **C** is correct. Homomorphic encryption allows data to be accessed and manipulated while it is encrypted. Symmetric and asymmetric encryption methods require the data to be decrypted before it is manipulated. Steganography isn't truly encryption, but instead it simply hides data within data. See Chapter 10.

67. **D** is correct. A certificate authority (CA) manages certificates and would sign certificates issued to users. Note that non-repudiation would be provided with digital signatures and each user would need a certificate assigned to them that they would use to create the digital signatures. A certificate revocation list (CRL) is a list of revoked certificates. Online Certificate Status Protocol (OCSP) is an alternative to a CRL and provides a real-time response indicating the validity of a certificate. The certificate signing request (CSR) is used to request a certificate. A Digital Signature Algorithm (DSA) is used to create a digital signature. They would use digital signatures to sign their emails, and they need a certificate to create a digital signature, but they can't sign their certificates with a digital signature. See Chapter 10.

68. **B** is correct. P12 (PKCS #12) certificates commonly include a private key and they are used to install a private key on a server. A Distinguished Encoding Rules (DER)-based certificate is a binary encoded file and a Canonical Encoding Rules (CER)-based certificate is an ASCII encoded file. However, DER and CER are used to define the format, not the content (such as a private key). While a P12 certificate does use a DER format, not all DER certificates include private keys. A P7B (PKCS #7) certificate is used to share the public key and never includes the private key. See Chapter 10.

69. **C** is correct. A service level agreement (SLA) is an agreement between a company and a vendor that stipulates performance expectations, including returning a system to full operation within a specific timeframe. The mean time to repair (MTTR) identifies the average (the arithmetic mean) time it

takes to restore a failed system, but it does not provide a guarantee that the vendor will restore the system within the MTTR every time. A non-disclosure agreement (NDA) ensures that individuals do not share proprietary data with others. A data loss prevention (DLP) device typically monitors outgoing traffic to prevent confidential information from getting outside the organization. See Chapter 11.

70. **D** is correct. A measurement systems analysis (MSA) evaluates the processes and tools used to make measurements. An acceptable use policy (AUP) informs users of company expectations when they use computer systems and networks, and it defines acceptable rules of behavior. A non-disclosure agreement (NDA) ensures that individuals do not share proprietary data with others. A service level agreement (SLA) is an agreement between a company and a vendor that stipulates performance expectations, such as minimum uptime and maximum downtime levels. See Chapter 11.

71. **A** is correct. The first step in an incident response process is preparation. When a potential incident occurs, the next step is identification. If the event is a security incident, the next step is containment to isolate the incident and limit the damage. Next, personnel take steps to eradicate all elements that caused the incident, such as malware or compromised accounts. The last two steps in the incident response process are recovery and lessons learned. See Chapter 11.

72. **A** is correct. A Secure Orchestration, Automation, and Response (SOAR) tool can be configured with SOAR runbooks to automate the response of these incidents and is the best choice of the available answers. A data loss prevention (DLP) device typically monitors outgoing traffic to prevent confidential information from getting outside the organization. While a SOAR runbook may include DLP action, a SOAR runbook can do much more. Structured Threat Information eXpression (STIX) defines standardized language used to share cyber threat information. TAXII (Trusted Automated eXchange of Indicator Information) defines a set of services and message exchanges that can be used to share information.

STIX identifies what to share and TAXII identifies how to share it. See Chapter 11.

73. **C** is correct. The **dd** command is available on Linux systems, and it is used to copy disks and files for analysis. As an example, the **dd if=/dev/sda2 of=sd2disk.img** command creates an image of a disk without modifying the original disk. None of the other choices creates an image of a drive. Tcpreplay is a suite of utilities used to edit packet captures and resend them, and it includes the **tcpreplay** command. The **chmod** (short for change mode) command is used to change permissions on Linux systems. Cuckoo is an open source malware analysis system. It analyzes malware within a sandbox environment. See Chapter 11.

74. **A** is correct. Before analyzing a hard drive, a forensic expert should capture an image of the hard drive and then analyze the image. The **dd** (short for data duplicator) command-line tool can be used to create an image of a disk without modifying it. This protects the original disk from accidental modifications and preserves it as usable evidence. While not available as a possible answer, a hash of the original drive should be created before capturing an image. The order of volatility identifies which data is most volatile (such as cache) and which is least volatile (such as hard drives). Although the **memdump** command is used to copy the contents of memory, this scenario is focused on a hard drive. A chain of custody document should be created when evidence is first collected. See Chapter 11.

75. **B** is correct. Tokenization is the best choice. It stores a token created by the credit card processor instead of the credit card number, and this token can be used to make charges. Pseudo-anonymization replaces data with artificial identities, but the process can be reversed. Data anonymization modifies data to protect the privacy of individuals by either removing all Personally Identifiable Information or encrypting it. Data minimization is a principle requiring organizations to limit the data they collect and use. See Chapter 11.

Chapter 1

Mastering Security Basics

CompTIA Security+ objectives covered in this chapter:

1.7 Summarize the techniques used in security assessments.

- Syslog/Security information and event management (SIEM)
(Review reports, Packet capture, Data inputs, User behavior analysis, Sentiment analysis, Security monitoring, Log aggregation, Log collectors)

2.1 Explain the importance of security concepts in an enterprise environment.

- Response and recovery controls

2.3 Summarize secure application development, deployment, and automation concepts.

- Elasticity, Scalability

2.5 Given a scenario, implement cybersecurity resilience.

- High availability (Scalability)

2.8 Summarize the basics of cryptographic concepts.

- Common use cases (Supporting confidentiality, Supporting integrity)

4.1 Given a scenario, use the appropriate tool to assess organizational security.

- Network reconnaissance and discovery (tracert/traceroute, ipconfig/ifconfig, ping/pathping, hping, netstat, arp)
- File manipulation (head, tail, cat, grep, chmod, logger)

4.3 Given an incident, utilize appropriate data sources to support an investigation.

- SIEM dashboards (Sensor, Sensitivity, Trends, Alerts, Correlation)
- Log files (Network, System, Application, Security, Web)

- syslog/rsyslog/syslog-ng, journalctl, NXLog

5.1 Compare and contrast various types of controls.

- Category (Managerial, Operational, Technical)
- Control type (Preventive, Detective, Corrective, Deterrent, Compensating, Physical)

**

Before you dig into some of the details related to IT security, you should have a solid understanding of core security goals. This chapter introduces many of these core goals to provide you with a big picture, and it presents basic risk concepts. Security controls reduce risks, and you'll learn about different security control categories in this chapter. You'll be expected to know about many Windows and Linux command-line tools, and this chapter introduces some. Last, this chapter provides details on some relevant logs and logging tools.

Understanding Core Security Goals

Security starts with several principles that organizations include as core security goals. These principles drive many security-related decisions at multiple levels. Understanding these basic concepts will help you create a solid foundation in security. Confidentiality, integrity, and availability form the CIA security triad, which is a model used to guide an organization's security principles. Each element is essential to address in any security program.

What Is a Use Case?

CompTIA includes the term ***use case*** in multiple objectives. A use case describes a goal that an organization wants to achieve. Engineers use it in systems analysis and software development to identify and clarify requirements to achieve the goal. A common naming strategy for a use case is in the verb-noun format. As an example, consider a use case named “Place Order.” Different departments within an organization might use it differently, but the use case can still retain the same name.

Developers can use the steps in the use case to create software to support the goal. The use case can help marketing personnel understand where they need to focus their efforts to motivate the buyer to place an order. Billing and Shipping departments use it to understand their responsibilities after the customer places the order.

Imagine that Lisa wants to place an order via an online e-commerce system. The “Place Order” use case for this might include the following elements:

- **Actors.** Lisa is one of the actors. She might have an account and be a registered user with her shipping and billing information in an existing database. Or, she might be a brand-new customer, and her information needs to be collected. Other actors include the billing system that bills her for the order and a fulfillment system that processes and ships the order.
- **Precondition.** A precondition must occur before the process can start. For example, Lisa needs to select an item to purchase before she can place the order.
- **Trigger.** A trigger starts the use case. In this case, it could be when Lisa clicks on the shopping cart to begin the purchase process.
- **Postcondition.** Postconditions occur after the actor triggers the process. In this case, Lisa’s order is placed into the system after she completes the purchase. She’ll receive an acknowledgment for her order, the Billing department may take additional steps to bill her (if she wasn’t billed during the purchase process), and the Shipping department will take steps to ship the product.

- **Normal flow.** A use case typically lists each of the steps in a specific order. In this example, you might see a dozen steps that start when Lisa picks an item to order and end when she completes the order and exits the purchase system.
- **Alternate flow.** All purchases won't be the same. For example, instead of using existing billing and shipping information, Lisa might want to use a different credit card or a different shipping address. It's also possible for Lisa to change her mind and abandon the process before completing the purchase or even cancel the purchase after completing the process.

Note that these are not the only possible elements in a use case. There are many more. However, you don't need to be an expert in project management to understand a use case's overall concept. Project management experts typically have thousands of hours developing, working with, and analyzing use cases. However, the CompTIA Security+ exam doesn't require you to be a project management expert or to know all the elements of use cases. It does require you to understand the basic concepts of a use case.

The following sections discuss some common use cases related to supporting confidentiality and integrity.

Ensure Confidentiality

Confidentiality prevents the unauthorized disclosure of data. In other words, authorized personnel can access the data, but unauthorized personnel cannot access it. You can ensure confidentiality using several different methods discussed in the following sections.

Encryption

Encryption scrambles data to make it unreadable by unauthorized personnel. Authorized personnel can decrypt the data to access it, but encryption techniques make it extremely difficult for unauthorized personnel to access encrypted data. Chapter 10, “Understanding Cryptography and PKI,” covers encryption in much more depth, including commonly used encryption algorithms like Advanced Encryption Standard (AES).

As an example, imagine you need to transmit Personally Identifiable Information (PII), such as medical information or credit card data via email. You wouldn’t want any unauthorized personnel to access this data, but once you click Send, you’re no longer in control of the data. However, if you encrypt the email before you send it, you protect the data’s confidentiality as it travels over the network.

Access Controls

Identification, authentication, and authorization provide access controls and help ensure that only authorized personnel can access data. Imagine that you want to grant Maggie access to some data, but you don’t want Homer to access the same data. You use access controls to grant and restrict access. The following list introduces key elements of access controls:

- **Identification.** Users claim an identity with a unique username. For example, both Maggie and Homer have separate user accounts identified with unique usernames. When Maggie uses her account, she is claiming the identity of her account.
- **Authentication.** Users prove their identity with authentication, such as with a password. For example, Maggie knows her password, but no one else should know it. When she logs on to

her account with her username and password, she claims her account's identity and proves her identity with the password.

- **Authorization.** Next, you can grant or restrict access to resources using an authorization method, such as permissions. For example, you can grant Maggie's account full access to some files and folders. Similarly, you can ensure that Homer doesn't have any permissions to access the data.

Chapter 2, "Understanding Identity and Access Management," covers these topics in more depth.

Remember this

Confidentiality ensures that data is only viewable by authorized users. The best way to protect the confidentiality of data is by encrypting it. This includes any type of data, such as PII, data in databases, and data on mobile devices. Access controls help protect confidentiality by restricting access.

Provide Integrity

Integrity provides assurances that data has not changed. This includes ensuring that no one has modified, tampered with, or corrupted the data. Ideally, only authorized users can modify data. However, there are times when unauthorized or unintended changes occur. This can be from unauthorized users, from malicious software (malware), and through system and human errors. When this happens, the data has lost integrity.

You can use hashing techniques to enforce integrity. Chapter 10 discusses the relevant hashing algorithms, such as the various versions of the Secure Hash Algorithm (SHA). Briefly, a hash is simply a number created by executing a hashing algorithm against data, such as a file or message. A hashing algorithm creates a fixed-length, irreversible output. If the data never changes, the resulting hash will always be the same. By comparing hashes created at two different times, you can determine if the original data is still the same. If the hashes are the same, the data is the same. If the hashes are different, the data has changed.

For example, imagine Homer is sending a message to Marge and they both want assurances that the message retains integrity. Homer's message is, "The price is \$19.99." He creates a hash of this message. For simplicity's sake, imagine the hash is 123. He then sends both the message and the hash to Marge.

Marge receives both the message and the hash. She (or software on her computer) can calculate the hash on the received message and compare her hash with the hash that Homer sent. If the hash of the received message is 123 (the same as the hash of the sent message), she knows the message hasn't lost data integrity. However, if the hash of the received message is something different, such as 456, she knows that the message she received is not the same as Homer's message. Data integrity is lost.

A variation in the hashes doesn't tell you what modified the message. It only tells you that the message has been modified. This lets you know that you shouldn't trust the integrity of the message.

You can use hashes with messages, such as emails, and any other type of data files. However, when you look at a fixed-length hash, you can't tell if it was created from a message, a file, or another data source.

Hashing techniques can also verify that integrity is maintained when files are downloaded or transferred. Some programs can automatically check hashes and determine if a file loses even a single bit during the download process. The program performing the download will detect it by comparing the source hash with the destination hash. If a program detects that the hashes are different, it knows that integrity has been lost and reports the problem to the user.

As another example, a web site administrator can calculate and post the hash of a file on a web site. Users can manually calculate the hash of the file after downloading it and compare the hash with the posted hash. If a virus infects a file on the web server, the hash of the infected file would be different from the hash of the original file (and the hash posted on the web site). You can use freeware such as *md5sum.exe* to calculate MD5 hashes. If you want to see this in action, check out the Creating and Comparing Hashes Lab in the online exercises for this book at <https://greatadministrator.com/sy0-601-labs/>.

Remember this

Integrity verifies that data has not been modified. Loss of integrity can occur through unauthorized or unintended changes. Hashing algorithms, such as SHA, calculate hashes to verify integrity. A hash is simply a number created by applying the algorithm to a file or message at different times. By comparing the hashes, you can verify integrity has been maintained.

Increase Availability

Availability indicates that data and services are available when needed. For some organizations, this simply means that the data and services must be available between 8:00 a.m. and 5:00 p.m., Monday through Friday. For other organizations, this means they must be available 24 hours a day, 7 days a week, 365 days a year.

Organizations commonly implement redundancy and fault-tolerant methods to ensure high levels of availability for key systems. Additionally, organizations ensure systems stay up to date with current patches to ensure that software bugs don't affect their availability.

Redundancy and Fault Tolerance

Redundancy adds duplication to critical systems and provides ***fault tolerance***. If a critical component has a fault, the redundancy's duplication allows the service to continue without interruption. In other words, a system with fault tolerance can suffer a fault, but it can tolerate it and continue to operate.

A common goal of fault tolerance and redundancy techniques is to remove each single point of failure (SPOF). If an SPOF fails, the entire system can fail. For example, if a server has a single drive, the drive is an SPOF because its failure takes down the server.

Chapter 9, “Implementing Controls to Protect Assets,” covers many fault tolerance and redundancy techniques in more depth. As an introduction, here are some common examples:

- **Disk redundancies.** Fault-tolerant disks, such as RAID-1 (mirroring), RAID-5 (striping with parity), and RAID-10 (striping with a mirror), allow a system to continue to operate even if a disk fails.
- **Server redundancies.** Failover clusters include redundant servers and ensure a service will continue to operate, even if a server fails. In a failover cluster, the service switches from the failed server in a cluster to an operational server in the same cluster. Virtualization can also increase the availability of servers by reducing unplanned downtime.

- **Network redundancies.** Load balancing uses multiple servers to support a single service, such as a high-volume web site. Network interface card (NIC) teaming can provide both redundancy support and increased bandwidth.
- **Power redundancies.** Uninterruptible power supplies (UPSS) and power generators can provide power to key systems even if commercial power fails.

Remember this

Availability ensures that systems are up and operational when needed and often addresses single points of failure. You can increase availability by adding fault tolerance and redundancies, such as RAID, failover clusters, backups, and generators.

Scalability and Elasticity

Both scalability and elasticity contribute to high availability. They allow systems to scale up by adding additional hardware resources such as memory, processing power, bandwidth capability, and/or drive space. They also allow systems to scale out by adding additional nodes or servers. Just as systems can scale up and out, they can also scale down or in by removing the additional resources or nodes. The primary difference is that static systems are scaled up or out manually, while dynamic systems use elasticity to scale up or out.

Scalability is a system's ability to handle increased workload either by scaling up or by scaling out. As an example, a server may have 16 GB of random access memory (RAM) installed. Administrators can scale the system up by manually adding an additional 16 GB of RAM, giving it 32 GB. However, there is typically a limit to scalability based on the system. For example, a server may only support 32 GB of RAM. Once it has 32 GB of RAM, you can no longer scale up the RAM. A key here is that the additional resources are added manually.

Elasticity is the ability of a system to handle an increased workload by dynamically scaling up or scaling out as the need arises. For example, a system may add more memory or more processors when it suddenly experiences high demand. When the workload decreases, the elasticity allows the system to dynamically remove the additional resources. Think of

a rubber band. Pull it, and it automatically stretches, but let it go, and it returns to its original size.

Cloud resources typically have elasticity capabilities allowing them to adapt to this increased and decreased demand on the fly. To consumers, the elasticity of cloud resources often appears to be unlimited.

Patching

Another method of ensuring systems stay available is by keeping them up to date with patches. Software bugs cause a wide range of problems, including security issues and even random crashes. When software vendors discover the bugs, they develop and release code that patches or resolves these problems. Organizations commonly implement patch management programs to ensure that systems stay up to date with current patches. Chapter 5, “Securing Hosts and Data,” covers patching and patch management in greater depth.

Remember this

Redundancy and fault tolerance methods increase the availability of systems and data. Scalability refers to manually adding or removing resources to a system to scale it up or out. Elasticity refers to dynamically adding or removing resources to a system to scale it.

Understanding Resiliency

A current trend is to increase the resiliency of systems rather than seek the highest possible availability. This ensures that systems are reliable but without the high cost associated with highly available systems. As an example, it’s possible to achieve 99.999 percent uptime (five nines) with systems. However, this requires eliminating every possible SPOF and adding multiple redundancies. These steps raise the total cost of ownership (TCO) significantly.

Resiliency methods help systems heal themselves or recover from faults with minimal downtime. They often use similar techniques that a highly available system uses. As an example, a system using resiliency methods may regularly perform and test full backups, have backup power sources (such as an uninterruptible power supply or generators), network interface card (NIC) teaming, or redundant disk subsystems. If power fails,

or one of the NICs stops receiving traffic, or one of the disk drives fails, the system can quickly recover.

Also, resiliency methods expect components to retry failed processes. If it fails at first, it tries again. For example, imagine a web server is slower than expected for some reason or returns error messages. You may not know why it slowed down or replied with the error message. However, the system will take steps to recover, and if the web browser requests the page again, it will succeed. Some web browsers do this automatically. For example, if you lose Internet access and visit *google.com* with the Chrome browser, it fails. However, when you restore your Internet access, Chrome automatically recovers and shows the Google home page.

Network protocols have implemented this concept for a long time. When using Transmission Control Protocol (TCP), packets may fail to reach the destination. If that happens, TCP processes simply ask the source to resend it.

Resource Versus Security Constraints

Organizations frequently need to balance resource availability with security constraints. Consider using encryption to maintain the confidentiality of data. If this is possible, why not just encrypt all the data? The reason is that encryption consumes resources.

As an example, the above paragraph is about 260 characters. Encrypted, it is about 360 characters. That's an increase of about 40 percent, which is typical with many encryption methods. If a company decides to encrypt all data, it will need approximately 40 percent more disk space to store it. Additionally, when processing the data, it consumes more memory and processing power to encrypt and decrypt the data, effectively slowing down applications.

Security experts might say the cost for additional resources is worth it, but executives looking to increase the company's value don't. Instead, executives have a responsibility to minimize costs without sacrificing security. They do this by looking for the best balance between resource costs and security needs.

Introducing Basic Risk Concepts

One of the basic goals of implementing IT security is to reduce risk. Because risk is so important and so many chapters refer to elements of risk, it's worth providing a short introduction here.

Risk is the possibility or likelihood of a threat exploiting a vulnerability resulting in a loss. A **threat** is any circumstance or event that has the potential to compromise confidentiality, integrity, or availability. A **vulnerability** is a weakness. It can be a weakness in the hardware, the software, the configuration, or even the users operating the system.

If a threat (such as an attacker) exploits a vulnerability, it can result in a security incident. A **security incident** is an adverse event or series of events that can negatively affect the confidentiality, integrity, or availability of an organization's information technology (IT) systems and data. This includes intentional attacks, malicious software (malware) infections, accidental data loss, and much more.

Threats can come from inside an organization, such as from a disgruntled employee (also known as a malicious insider). They can come from outside the organization, such as from an attacker anywhere in the world with access to the Internet. Threats can be natural, such as hurricanes, tsunamis, or tornadoes, or human-made, such as malware written by a criminal. Threats can be intentional, such as from attackers, or accidental, such as from employee mistakes or system errors.

Reducing risk is also known as risk mitigation. **Risk mitigation** reduces the chances that a threat will exploit a vulnerability. You reduce risks by implementing controls (also called countermeasures and safeguards), and many of the actions described throughout this book are different types of controls. You can't prevent most threats. For example, you can't stop a tornado or prevent a criminal from writing malware. However, you can reduce risk by reducing vulnerabilities to the threat or reducing the threat's impact.

For example, access controls (starting with authentication) ensure that only authorized personnel can access specific areas, systems, or data. If employees become disgruntled and want to cause harm, access controls reduce the amount of potential damage by reducing what they can access. If

a natural disaster hits, business continuity and disaster recovery plans help reduce the impact. Similarly, antivirus software prevents the impact of any malware by intercepting it before it causes any harm.

Remember this

Risk is the likelihood that a threat will exploit a vulnerability. Risk mitigation reduces the chances that a threat will exploit a vulnerability or reduces the risk's impact by implementing security controls.

Understanding Security Controls

There are hundreds, perhaps thousands, of security controls that organizations can implement to reduce risk. The good news is that you don't need to be an expert on all the possible security controls to pass the CompTIA Security+ exam. However, you do need to have a basic understanding of control categories and control types.

CompTIA lists the following control categories in the objectives:

- **Managerial controls** are primarily administrative in function. They are typically documented in an organization's security policy and focus on managing risk.
- **Operational controls** help ensure that the day-to-day operations of an organization comply with the security policy. People implement them.
- **Technical controls** use technology such as hardware, software, and firmware to reduce vulnerabilities.

Remember this

Security controls are categorized as managerial (documented in written policies), operational (performed in day-to-day operations), or technical (implemented with technology).

CompTIA also lists the following control types in the objectives:

- **Preventive controls** attempt to prevent an incident from occurring.
- **Detective controls** attempt to detect incidents after they have occurred.
- **Corrective controls** attempt to reverse the impact of an incident.
- **Deterrent controls** attempt to discourage individuals from causing an incident.
- **Compensating controls** are alternative controls used when a primary control is not feasible.
- **Physical controls** refer to controls you can physically touch.

NIST and SP 800 Documents

The National Institute of Standards and Technology (NIST) is a part of the U.S. Department of Commerce, and it includes a Computer Security Division hosting the Information Technology Laboratory (ITL). The ITL publishes Special Publications (SPs) in the 800 series that are of general interest to the computer security community.

Many IT security professionals use these documents as references to design secure IT systems and networks. Additionally, many security-related certifications (beyond the CompTIA Security+ certification) also reference the SP 800 documents both directly and indirectly.

SP 800-53 Revision 5, “Security and Privacy Controls for Information Systems and Organizations,” includes a wealth of information on security controls. It includes three chapters that discuss security controls followed by three appendixes. Appendix C is a security control catalog that provides details on hundreds (maybe thousands) of individual security controls, divided into 20 different families.

Each of these families includes multiple groups. As an example, the Access Control family (AC) includes 25 different groups (AC-1 through AC-25). Many of these groups list individual controls and provide details on how to implement them. As an example, AC-2 (Account Management) identifies multiple controls (as a. through l.) followed by a discussion on these controls.

It’s worth noting that earlier versions of SP 800-53 attempted to identify every control as managerial, operational, or technical. However, many controls included characteristics from more than just one of these classifications. NIST removed these references.

If you’re interested in pursuing other security-related certifications or making IT security a career, the SP 800 documents are well worth your time. You can download SP 800-53 Revision 4 and other SP 800 documents at <https://csrc.nist.gov/publications/PubsSPs.html>.

Managerial Controls

Managerial controls are primarily administrative in function and are typically documented in an organization's written security policy. They use planning and assessment methods to provide an ongoing review of the organization's ability to reduce and manage risk. Chapter 8, "Using Risk Management Tools," covers vulnerability assessments and penetration tests, which fall into this category.

For example, two common managerial controls are:

- **Risk assessments.** These help organizations quantify and qualify risks within an organization so that they can focus on the serious risks. For example, a quantitative risk assessment uses cost and asset values to quantify risks based on monetary values. A qualitative risk assessment uses judgments to categorize risks based on probability and impact.
- **Vulnerability assessments.** A vulnerability assessment attempts to discover current vulnerabilities. When necessary, additional controls are implemented to reduce the risk from these vulnerabilities.

Operational Controls

Operational controls help ensure that the day-to-day operations of an organization comply with their overall security plan. These are controls that are primarily implemented and executed by people instead of systems.

Operational controls include the following families:

- **Awareness and training.** The importance of training to reduce risks cannot be overstated. Training helps users maintain password security, follow a clean desk policy, understand threats such as phishing and malware, and much more.
- **Configuration management.** Configuration management often uses baselines to ensure that systems start in a secure, hardened state. Change management helps ensure that changes don't result in unintended configuration errors. Chapter 5 covers change and configuration management in more detail.
- **Media protection.** Media includes physical media such as USB flash drives, external and internal drives, and backup tapes.
- **Physical and environmental protection.** This includes physical controls such as cameras, door locks, and environmental controls such as heating and ventilation systems.

Remember this

Managerial controls are administrative in function and documented in security policies. Operational controls are implemented by people who perform the day-to-day operations to comply with an organization's overall security plan.

Technical Controls

Technical controls use technology such as hardware, software, and firmware to reduce vulnerabilities. An administrator installs and configures a technical control, and the technical control then provides the protection automatically. Throughout this book, you'll come across several examples of technical controls. The following list provides a few examples:

- **Encryption.** Encryption is a strong technical control used to protect the confidentiality of data. This includes data transferred over a network and data stored on devices, such as servers, desktop computers, and mobile devices.
- **Antivirus software.** Once installed, the antivirus software provides protection against malware infection. Chapter 6, “Comparing Threats, Vulnerabilities, and Common Attacks,” covers malware and antivirus software in more depth.
- **Intrusion detection systems (IDSs) and intrusion prevention systems (IPSSs).** IDSs and IPSSs can monitor a network or host for intrusions and provide ongoing protection against various threats. Chapter 4, “Securing Your Network,” covers different types of IDSs and IPSSs.
- **Firewalls.** Network firewalls restrict network traffic going in and out of a network. Chapter 3, “Exploring Network Technologies and Tools,” covers firewalls in more depth.
- **Least privilege.** The least privilege principle specifies that individuals or processes are granted only the privileges they need to perform their assigned tasks or functions, but no more. Privileges are a combination of rights and permissions.

Remember this

Technical controls use technology to reduce vulnerabilities. Some examples include encryption, antivirus software, IDSs, IPSSs, firewalls, and the least privilege principle. Physical security and environmental controls include motion detectors and fire suppression systems.

Control Types

Control types are controls designed to perform specific functions in relation to security incidents. Some common classifications are preventive, detective, corrective, deterrent, compensating, and physical. You'll see some crossover between the control categories and control types as you read through them. For example, training is in the operational category and is also included in the preventive type of controls.

Preventive Controls

Ideally, an organization won't have any security incidents, which is the primary goal of preventive controls—to prevent security incidents. You may see preventive controls referred to as preventative controls, but both terms mean the same thing. Some examples include:

- **Hardening.** Hardening is the practice of making a system or application more secure than its default configuration. This uses a defense-in-depth strategy with layered security. It includes disabling unnecessary ports and services, implementing secure protocols, keeping a system patched, using strong passwords along with a robust password policy, and disabling default and unnecessary accounts. Chapter 5 covers these topics in more depth.
- **Training.** Ensuring that users are aware of security vulnerabilities and threats helps prevent incidents. When users understand how social engineers operate, they are less likely to be tricked. For example, uneducated users might be tricked into giving a social engineer their passwords, but educated users will see through the tactics and keep their passwords secure.
- **Security guards.** Guards prevent and deter many attacks. For example, guards can prevent unauthorized access into secure areas of a building by first verifying user identities. Although a social engineer might attempt to fool a receptionist into letting him into a secure area, the presence of a guard will deter many social engineers from even trying these tactics.
- **Change management.** Change management ensures that changes don't result in unintended outages. In other words,

instead of administrators making changes on the fly, they submit the change to a change management process. Notice that change management is an operational control, which attempts to prevent incidents. In other words, it's both an operational control and a preventive control.

- **Account disablement policy.** An account disablement policy ensures that user accounts are disabled when an employee leaves the organization. This prevents anyone, including ex-employees, from continuing to use these accounts. Chapter 2 covers account disablement policies in more depth.
- **Intrusion prevention system (IPS).** An IPS can block malicious traffic before it reaches a network. This prevents security incidents. Chapter 4 covers IPSS in more depth.

Remember this

Preventive controls attempt to prevent security incidents. Hardening systems modifies the basic configuration to increase security. Security guards can prevent unauthorized personnel from entering a secure area. Change management processes help prevent outages from configuration changes. An account disablement policy ensures that accounts are disabled when a user leaves the organization.

Detective Controls

Although preventive controls attempt to prevent security incidents, some will still occur. Detective controls attempt to detect when vulnerabilities have been exploited, resulting in a security incident. The important point is that detective controls discover the event after it has occurred. Some examples of detective controls are:

- **Log monitoring.** Several different logs record details of activity on systems and networks. For example, firewall logs record details of all traffic that the firewall blocked. By monitoring these logs, it's possible to detect incidents. Some automated methods of log monitoring automatically detect potential incidents and report them right after they've occurred.
- **Security information and event management (SIEM) systems.** In addition to monitoring logs to detect any single incident, you can also use SIEMs to detect trends and raise

alerts in real time. By analyzing past alerts, you can identify trends, such as an increase of attacks on a specific system.

- **Security audit.** Security audits can examine the security posture of an organization. For example, an account audit can determine if personnel and technical policies are implementing account policies correctly.
- **Video surveillance.** A closed-circuit television (CCTV) system can record the activity and detect events that have occurred. It's worth noting that video surveillance can also be used as a deterrent control.
- **Motion detection.** Many alarm systems can detect motion from potential intruders and raise alarms.
- **Intrusion detection system (IDS).** An IDS can detect malicious traffic after it enters a network. It typically raises an alarm to notify IT personnel of a potential attack.

Remember this

Detective controls attempt to detect when vulnerabilities have been exploited. Some examples include log monitoring, trend analysis, security audits, and CCTV systems.

Corrective and Recovery Controls

Corrective and recovery controls attempt to reverse the impact of an incident or problem after it has occurred. Some examples of corrective and recovery controls are:

- **Backups and system recovery.** Backups ensure that personnel can recover data if it is lost or corrupted. Similarly, system recovery procedures ensure administrators can recover a system after a failure. Chapter 9 covers backups and disaster recovery plans in more depth.
- **Incident handling processes.** Incident handling processes define steps to take in response to security incidents. This typically starts with an incident response policy and an incident response plan. Chapter 11, “Implementing Policies to Mitigate Risks,” covers incident handling in more depth.

Physical Controls

Physical controls are any controls that you can physically touch. Some examples include bollards and other barricades, access control vestibules (sometimes called mantraps), lighting, signs, fences, sensors, and more. It's important to realize that you can identify physical controls as other control types. As an example, physical controls such as locks are also preventive and deterrent controls. A locked door prevents personnel from entering a secure area and deters individuals from even trying if they know the door is locked.

CompTIA has placed a lot more emphasis on physical security controls devoting an entire objective (2.7) to them. You'll see these covered in more depth in Chapter 9.

Deterrent Controls

Deterrent controls attempt to discourage a threat. Some deterrent controls attempt to discourage potential attackers from attacking, and others attempt to discourage employees from violating a security policy.

You can often describe many deterrent controls as preventive controls. For example, imagine an organization hires a security guard to control access to a building's restricted area. This guard will deter most people from trying to sneak in simply by discouraging them from even trying. This deterrence prevents security incidents related to unauthorized access.

The following list identifies some physical security controls used to deter threats:

- **Cable locks.** Securing laptops to furniture with a cable lock deters thieves from stealing the laptops. Thieves can't easily steal a laptop secured this way. If they try to remove the lock, they will destroy it. Admittedly, a thief could cut the cable with a large cable cutter. However, someone walking around with a four-foot cable cutter looks suspicious.
- **Physical locks.** Other locks such as locked doors, securing a wiring closet or a server room, also deter attacks. Many server bay cabinets also include locking cabinet doors.

Compensating Controls

Compensating controls are alternative controls used instead of a primary control. As an example, an organization might require employees

to use smart cards when authenticating on a system. However, it might take time for new employees to receive their smart card. To allow new employees to access the network and still maintain a high level of security, the organization might choose to implement a Time-based One-Time Password (TOTP) as a compensating control. The compensating control still provides a strong authentication solution.

Response Controls

Response controls, commonly referred to as incident response controls, are controls designed to prepare for security incidents and respond to them once they occur. These typically start with creating security policies (including incident response policies), followed by training personnel on how to respond to incidents. Chapter 11 covers incident response controls in more depth.

Combining Control Categories and Types

It's important to realize that the control categories (managerial, operational, and technical) and control types (such as preventive, detective, corrective, and so on) are not mutually exclusive. In other words, you can describe most controls using more than one category and more than one type.

As an example, encryption is a preventive technical control. It helps prevent the loss of data confidentiality, so it is a preventive control. You implement it with technology, so it is a technical control. If you understand control categories, you shouldn't have any problems picking out the correct answers on the exam even if CompTIA combines them in a question, such as a preventive technical control.

Similarly, a fire suppression system is a physical technical control. It is a physical security control because you can touch it. However, it's also a technical control because it uses technologies to detect, suppress, or extinguish fires.

Using Command-Line Tools

The CompTIA Security+ objectives list several command-line tools. Sometimes they list them in the question, and other times they want you to pick the best tool in the answers. If you’re familiar with the tools, these questions will often be trivial. However, if you’ve never entered the commands, these questions can be challenging.

Appendix A, “Command-Line Basics,” discusses the basics of the Windows Command Prompt and the Linux terminal. Many experienced administrators work with command-line tools daily, so they won’t need to read the appendix first. However, some people may find some of the following topics confusing without reading the appendix.

If you don’t have a Linux system, I strongly encourage you to check out the online labs. A lab for this chapter leads you through the steps to create a bootable USB. This allows you to boot any system into Kali Linux (mentioned throughout this book). Turn the system off and remove the USB, and you’ll boot back into your regular operating system.

Network Reconnaissance and Discovery

Network discovery allows devices on a network to discover other devices on the same network. Network reconnaissance attempts to learn additional details about the network and those devices. Administrators (and attackers) use many commands for network reconnaissance and discovery. Administrators use them for legitimate purposes, such as when troubleshooting. Attackers use them to gain more information about a network and individual hosts as they try to extend their foothold in an attack. The following sections discuss some of these commands, but you'll find others mentioned in other chapters.

The CompTIA Security+ objectives list several command-line tools that you should know to help you assess organizational security. Some are specific to Windows systems and run through the Windows Command Prompt window. Others are specific to Linux systems and run through the Linux ***terminal*** (sometimes called the shell). On test day, you can expect to see some commands within the question. Test takers who never saw the command may not even understand the question. Other times, you'll be expected to pick the best command to perform a specific task. As you read through this section and learn about these tools, I strongly encourage you to run the commands. You will find labs you can follow at <https://greatadministrator.com/sy0-601-labs/>.

Ping

Ping is a basic command used to test connectivity for remote systems. You can also use it to verify a system can resolve valid hostnames to IP addresses, test the NIC, and assess organizational security.

The ping command checks connectivity by sending Internet Control Message Protocol (ICMP) echo request packets. Remote systems answer with ICMP echo reply packets, and if you receive echo replies, you know that the remote system is operational. As a simple example, the following command verifies that your computer can connect with another computer on your network, assuming the other computer has the IP address of 192.168.1.1:

ping 192.168.1.1

On Windows systems, ping sends out four ICMP echo requests. Systems that receive the ICMP echo requests respond with ICMP echo replies. On Linux-based systems, ping continues until you press the Ctrl + C keys to stop it. You can mimic this behavior on Windows systems by using the -t switch like this:

ping -t 192.168.1.1

Similarly, you can mimic the behavior of a Windows ping on a Linux system using the -c switch (for count) like this:

ping -c 4 192.168.1.1

This example tested connectivity with an IP address in a local network, but you can just as easily test connectivity with any system. For example, if you knew the IP address of a system hosting a web site on the Internet, you could ping its IP address.

Using Ping to Check Name Resolution

The name resolution process resolves a hostname (such as *gcfgapremium.com*) to an IP address. There are several elements of name resolution. Typically, a computer queries a Domain Name System (DNS) with the hostname, and DNS responds with an IP address.

Some malware attempts to break the name resolution process for specific hosts. For example, Windows systems get updates from a Windows Update server. In some cases, malware changes the name resolution process

to prevent systems from reaching the Windows Update server and getting updates.

You can ping the hostname of a remote system and verify that name resolution is working. As an example, the following command resolves the hostname (*gcpapremium.com*) to an IP address:

ping gcpapremium.com

Here's the result when executing the command on a Windows 10 system.

```
Pinging gcpapremium.com [72.52.230.233] with 32 bytes of data:
```

```
Reply from 72.52.230.233: bytes=32 time=45ms TTL=116
```

```
Reply from 72.52.230.233: bytes=32 time=45ms TTL=116
```

```
Reply from 72.52.230.233: bytes=32 time=48ms TTL=116
```

```
Reply from 72.52.230.233: bytes=32 time=45ms TTL=116
```

```
Ping statistics for 72.52.230.233:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss), Approximate round  
trip times in milli-seconds:
```

```
Minimum = 45ms, Maximum = 48ms, Average = 45ms
```

Notice that the first line shows that ping resolved the hostname (*gcpapremium.com*) to its IP address (72.52.230.233). The four replies are responses from the server, indicating that it is up and operational.

Beware of Firewalls

If you receive replies from a system, it verifies the other system is operational and reachable. However, if the ping command fails, it doesn't necessarily mean that the remote system is not operational or not reachable. Ping might show a "Reply Timed Out" error even if the remote system is functioning properly.

Many denial-of-service (DoS) attacks use ICMP to disrupt services on Internet-based systems. A ping flood attack attempts to disrupt systems by sending ping requests repeatedly. Administrators often configure firewalls to block ICMP traffic or block ICMP echo requests, which prevents these attacks from succeeding. In other words, a remote system might be operational, but ping will fail because the firewall is blocking ICMP traffic.

As an example, you might be able to connect to the <https://blogs.getcertifiedgetahead.com> web site using a web browser, but ping might fail. This indicates that the web site is operational with Hypertext Transfer Protocol Secure (HTTPS), but a firewall is blocking ICMP ping traffic.

Using Ping to Assess Organizational Security

You can also use ping to assess organizational security. For example, if you've configured firewalls and routers to block ping traffic, you can verify that the firewalls and routers block the traffic by using ping to check it.

Chapter 4 covers intrusion prevention systems (IPSs) in more depth, but as an introduction, they can often detect attacks and block them automatically. For example, a distributed denial-of-service (DDoS) attack can send thousands of pings to a server and overload it. An IPS can detect the attack and automatically block ICMP ping traffic, effectively thwarting the attack.

You can use ping to verify the IPS is working as expected. You would start by sending endless pings from a couple of computers to simulate an attack. If the IPS is working, it will block these attacks, and the pings will stop receiving replies.

Remember this

Administrators use ping to check the connectivity of remote systems and verify name resolution is working. They also use ping to check systems and networks' security posture by verifying that routers, firewalls, and IPSs block ICMP traffic when configured to do so.

hping

The ***hping*** command is similar to the ping command, but it can send the pings using TCP, UDP, and ICMP. It is useful if you're trying to identify if a firewall is blocking ICMP traffic, but it is only available on Linux-like systems. The hping tool also has many other capabilities, such as scanning systems for open ports, and will be discussed further in Chapter 8.

Ipconfig and ifconfig

The ***ipconfig*** command (short for Internet Protocol configuration) shows the Transmission Control Protocol/Internet Protocol (TCP/IP) configuration information for a Windows system. This includes items such as the computer's IP address, subnet mask, default gateway, MAC address, and the address of a Domain Name System (DNS) server. The command shows the configuration information for all network interface cards (NICs) on a system, including wired and wireless NICs. Technicians often use ipconfig as a first step when troubleshooting network problems.

Linux-based systems use ***ifconfig*** (short for interface configuration) instead of ipconfig. The ifconfig command has more capabilities than ipconfig, allowing you to use it to configure the NIC in addition to listing the properties of the NIC.

The following list shows some common command usage:

- **ipconfig.** Entered by itself, this command provides basic information about the NIC, such as the IP address, subnet mask, and default gateway.
- **ipconfig /all and ifconfig -a.** This command shows a comprehensive listing of TCP/IP configuration information for each NIC. It includes the media access control (MAC) address, the address of assigned DNS servers, and the address of a Dynamic Host Configuration Protocol (DHCP) server if the system is a DHCP client. You can use ifconfig -a on Linux systems.
- **ipconfig /displaydns.** Each time a system queries DNS to resolve a hostname to an IP address, it stores the result in the DNS cache, and this command shows the contents of the DNS cache. It also shows any hostname to IP address mappings included in the hosts file.
- **ipconfig /flushdns.** You can erase the contents of the DNS cache with this command. Use this when the cache has incorrect information, and you want to ensure that the system queries DNS for up-to-date information.

The following commands are unique to Linux systems. Note that you need to run these with administrative permissions on some distributions.

You can often do so by preceding the command with the **sudo** command. For example, instead of entering just **ifconfig eth0**, you would enter **sudo ifconfig eth0**.

- **ifconfig eth0.** This command shows the configuration of the first Ethernet interface (NIC) on a Linux system. If the system has multiple NICs, you can use eth1, eth2, and so on. You can also use wlan0 to view information on the first wireless interface.
- **ifconfig eth0 promisc.** This command enables promiscuous mode on the first Ethernet interface. Promiscuous mode allows a NIC to process all traffic it receives. Normally, a NIC is in non-promiscuous mode, and it ignores all packets not addressed to it. You can disable promiscuous mode with this command: **ifconfig eth0 -promisc**.
- **ifconfig eth0 allmulti.** This command enables multicast mode on the NIC. This allows the NIC to process all multicast traffic received by the NIC. Normally, a NIC only processes multicast traffic for multicast groups that it has joined. You can disable multicast mode with this command:
ifconfig eth0 -allmulti.

Normally, a NIC uses non-promiscuous mode, and only processes packets addressed directly to its IP address. However, there are many times when you want the system to process all packets that reach the NIC. As an example, if you're using a protocol analyzer application on a system, you would typically want to see all the traffic. Putting the NIC in promiscuous mode shows all the packets in the protocol analyzer application.

Many Linux distributions deprecated the use of the ifconfig command. Deprecated means that its use is discouraged but tolerated. The ifconfig command is part of the net-tools package, and Linux Debian developers are no longer maintaining that package. However, you'll still see ifconfig and other tools in the net-tools package on most Linux systems, including Kali Linux.

Instead of using ifconfig, Linux developers recommend you use ip instead. Although the ip command can display information and configure network interfaces, it doesn't use the same commands or have the same abilities. For example, it doesn't have a command you can use to enable

promiscuous mode on a NIC. Here are a few commands that you can use with ip:

- **ip link show.** Shows the interfaces along with some details on them
- **ip link set eth0 up.** Enables a network interface
- **ip -s link.** Shows statistics on the network interfaces

Remember this

Windows systems use ipconfig to view network interfaces. Linux systems use ifconfig, and ifconfig can also manipulate the settings on the network interfaces. You can enable promiscuous mode on a NIC with ifconfig. The ip command is recommended in place of ifconfig in many situations, such as viewing and manipulating NIC settings.

Netstat

The **netstat** command (short for network statistics) allows you to view statistics for TCP/IP protocols on a system. It also gives you the ability to view active TCP/IP network connections. Many attacks establish connections from an infected computer to a remote computer. If you suspect this, you can often identify these connections with netstat.

Some of the common commands you can use with netstat are:

- **Netstat.** Displays a listing of all open TCP connections.
- **Netstat -a.** Displays a listing of all TCP and User Datagram Protocol (UDP) ports that a system is listening on, in addition to all open connections. This listing displays sockets (the IP address followed by a colon and the port number). You can use the port number to identify protocols. As an example, if you see an IP address followed by :80, it indicates the system is listening on the default port of 80 for HTTP. This indicates this system is likely a web server.
- **Netstat -r.** Displays the routing table.
- **Netstat -e.** Displays details on network statistics, including how many bytes the system sent and received.
- **Netstat -s.** Displays statistics of packets sent or received for specific protocols, such as IP, ICMP, TCP, and UDP.
- **Netstat -n.** Displays addresses and port numbers in numerical order. This can be useful if you're looking for information related to a specific IP address or a specific port.
- **Netstat -p protocol.** Shows statistics on a specific protocol, such as TCP or UDP. For example, you could use **netstat -p tcp** to show only TCP statistics.

You can combine many of the netstat switches to show different types of information. For example, if you want to show a listing of ports that the system is listening on (-a), listed in numerical order (-n), for only the TCP protocol (-p tcp), you could use this command:

netstat -anp tcp

Netstat displays the state of a connection, such as ESTABLISHED, to indicate an active connection. RFC 793 (<https://tools.ietf.org/rfc/rfc793.txt>) formally defines these states. Some of the common states are:

- **ESTABLISHED.** This is the normal state for the data transfer phase of a connection. It indicates an active open connection.
- **LISTEN.** This indicates the system is waiting for a connection request. The well-known port a system is listening on indicates the protocol.
- **CLOSE_WAIT.** This indicates the system is waiting for a connection termination request.
- **TIME_WAIT.** This indicates the system is waiting for enough time to pass to be sure the remote system received a TCP-based acknowledgment of the connection.
- **SYN_SENT.** This indicates the system sent a TCP SYN (synchronize) packet as the first part of the SYN, SYN-ACK (synchronize-acknowledge), ACK (acknowledge) handshake process and it is waiting for the SYN-ACK response.
- **SYN_RECEIVED.** This indicates the system sent a TCP SYN-ACK packet after receiving a SYN packet as the first part of the SYN, SYN-ACK, ACK handshake process. It is waiting for the ACK response to establish the connection. An excessive number of SYN_RECEIVED states indicate a SYN attack where an attacker is flooding a system with SYN packets but never finalizes the connection with ACK packets.

Tracert and traceroute

The **tracert** command lists all the routers between two systems. In this context, each router is referred to as a hop. Tracert identifies the IP address and sometimes the hostname of each hop in addition to the round-trip times (RTTs) for each hop. Windows-based systems use tracert and Linux-based systems use **traceroute**, but they both function similarly. I'm using the command name tracert in this section for simplicity, but this section applies to both equally.

Network administrators typically use tracert to identify faulty routers on the network. Ping tells them if they can reach a distant server. If the ping fails, they can use tracert to identify where the traffic stops. Some of the hops will succeed, but at some point, tracert will identify where packets are lost, giving them insight into where the problem has occurred. Other times, they will see where the RTTs increase as traffic is routed around a faulty router.

From a security perspective, you can use tracert to identify modified paths. As an example, consider Figure 1.1. Users within the internal network normally access the Internet directly through Router 1. However, what if an attacker installed an unauthorized router between Router 1 and the Internet?

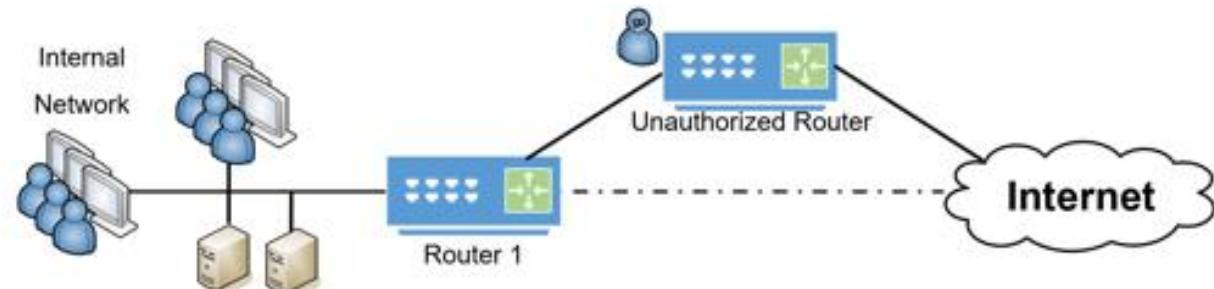


Figure 1.1: Tracing a path with tracert

Traffic will still go back and forth to the users. However, the attacker could capture the traffic with a protocol analyzer and view any data sent in cleartext. The attacker may also launch other attacks, such as some of the attacks discussed in Chapter 7, “Protecting Against Advanced Attacks.”

From another perspective, you can identify if Internet paths have been modified. Imagine that you often connect to a server in New York from a New York location. Today, the connection seems abnormally slow. You

could use tracert to verify the path. If you notice that traffic is now going through IP addresses in foreign countries, it indicates a problem.

Give it a try. Launch a command prompt and use the following commands to see some common uses and outputs from the tracert command:

- Type in **tracert blogs.getcertifiedgetahead.com** and press Enter. Identify how many hops are between your system and this web server. Identify if any RTTs are significantly longer than others.
- Type in **tracert -d blogs.getcertifiedgetahead.com** and press Enter. Notice that the -d switch forces tracert to not resolve IP addresses to hostnames, allowing the command to finish quicker.

Note that some of the switches are different between tracert and traceroute. As an example, to force traceroute to not resolve IP addresses to hostnames, you use the -n switch as in **traceroute -n blogs.getcertifiedgetahead.com**.

Pathping

The ***pathping*** command combines the functions of the ping and the tracert command. The tracert function identifies all the hops (routers) on the path. The ping function then sends pings to each router and computes statistics based on the number of responses. After identifying the hops, it pings each hop and computes statistics based on how many pings were sent and how many were received in response.

Administrators commonly use it to locate potential problems in the path between two systems. It's often an effective method of locating intermittent problems on any hops or problems on any of the segments between two hops. It's common to use the -n switch, which eliminates the hostnames in the output, making it easier to read.

Pathping first displays the hops the same way tracert does, numbering each hop. The following is a partial output from the **pathping -n 172.16.17.11** command. In this context, fileserver1 is a server in your network with the IP address of 172.16.17.11.

```
C:\>pathping 172.16.17.11
Tracing route to 172.16.17.11
over a maximum of 30 hops:
0 192.168.7.34
1 192.168.7.1
2 192.168.5.1
3 10.5.48.1
4 10.80.73.150
5 172.16.17.11
Computing statistics for 125 seconds...
```

By default, it tests each hop for 25 seconds, so the amount of time it takes to finish varies depending on how many routers are in the path. After it finishes sending the pings and calculating the statistics, it displays results like the following.

Source to Here This Node/Link	Hop	RTT	Lost/Sent=Pct	Lost/Sent=Pct	Address
	0	192.168.7.34	0/100 = 0%		
	1	45 ms	0 / 100 = 0%	0/100 = 0%	192.168.7.1
			10/100 = 10%		
	2	25 ms	15 / 100 = 15%	0/100 = 0%	192.168.5.1
			0/100 = 0%		
	3	22 ms	16 / 100 = 16%	0/100 = 0%	10.5.48.1

```
        0/100 = 0%    |
4 --- 100 / 100 = 100% 100/100 = 100% 10.80.73.150
        0/100 = 0%    |
5 23 ms 16 / 100 = 16%  0/100 = 0%   172.16.17.11
```

The Source to Here column shows statistics from where you ran the command (source) to the IP address listed in the Address column. For example, hop 2 shows that 15 packets were lost between the source (192.168.7.34) and the router at 192.168.5.1.

You can also see statistics for network segments between each of the routers in the This Node/Link column. For example, the link between 192.168.7.1 and 192.168.5.1 is dropping 10 percent of the packets. This could indicate excessive traffic on this network, causing collisions and the loss of packets. Because hops 2, 3, 4, and 5 all travel through this network, it makes sense that you see packet loss in those hops, too.

Notice that hop 4 shows 100 percent packet loss at 10.80.73.150, but the pathping still reaches hop 5. You might think that this is a problem, but it isn't. It indicates that the hop 4 router isn't responding to ICMP traffic. If it was blocking ICMP traffic, you would also see 100 percent packet loss on hop 5. Similarly, if the 10.80.73.150 router was down, you wouldn't see any traffic to hop 5.

The pathping command is only available on Windows systems. You can use mtr on Linux systems, but mtr is not listed in the CompTIA objectives.

Arp

Arp is a command-line tool that is related to the Address Resolution Protocol (ARP); however, arp (the command) and ARP (the protocol) are not the same thing. Chapter 3 discusses ARP (the protocol), but as a short introduction, ARP resolves IP addresses to MAC addresses and stores the result in the ARP cache.

You can use the arp command to view and manipulate the ARP cache. Here are some sample commands:

- **arp.** Without a switch, shows help on Windows
- **arp.** Without a switch, shows the ARP cache on Linux
- **arp -a.** Shows the ARP cache on Windows
- **arp -a 192.168.1.1.** Displays the ARP cache entry for the specified IP address

You can also use arp to identify the MAC address of other systems on your local network. As an example, imagine you want to identify the MAC address of server1. You can ping server1, and ARP will identify server1's IP address. You can then use arp -a to show the ARP cache, which includes the MAC address for server1.

Chapter 7 covers several attacks, including ARP cache poisoning, where attackers manipulate the ARP cache. If you suspect an ARP cache poisoning attack, you can use arp to check the cache.

Linux and LAMP

More and more networks are hosting Linux systems, so it's becoming increasingly important for IT administrators to be familiar with them. Many organizations host web servers using an open source LAMP stack. **LAMP** is an acronym for Linux, Apache, MySQL, and PHP or Perl or Python. Linux is the operating system, Apache is the web server application, and MySQL is the database management system. Developers create dynamic web pages with a scripting language such as PHP (short for PHP: Hypertext Preprocessor), Perl, or Python.

The following sections describe several file manipulation commands and log-related commands. They are all run from the Linux terminal. You'll also see some Linux commands mentioned elsewhere throughout the book. Make sure you do the labs associated with this chapter to practice them, and feel free to check out the appendix for a review of command basics. You may notice that headings for Linux commands (such as hping, ifconfig, and cat) are shown with the first letter in lower case. This is the way Linux commands must be entered.

cat Command

The **cat** command (short for concatenate) is used to display the contents of files. It has other uses, such as making copies of a file or merging multiple files into one, but it's one of the easiest ways to view a file's contents. As an example, imagine you want to view a listing of all authentication-related events on a Linux system. These events are logged in the */var/log/auth.log* file. You can use the following command to display the entire log file:

```
sudo cat /var/log/auth.log
```

The **sudo** command (short for super user do) allows you to run the command with root, or elevated privileges, assuming you have permission to do so. In many cases, the command displays “Permission denied” if you don't use sudo. Running the command as shown shows the entire contents of the *auth.log* file, scrolling it so fast, you can't see the beginning of the file. The following command shows one page at a time:

```
sudo cat /var/log/auth.log | more
```

The pipe operator (|) allows you to send the results of the first command (**sudo cat /var/log/auth.log**) to the second command (**more**). It displays the log one page at a time. Pressing the space bar shows the next page.

grep Command

The grep command (short for globally search a regular expression and print) is used to search for a specific string or pattern of text within a file. This can simplify the search. As an example, imagine that you are looking for any indications of someone trying to guess a password on your system. Every failed try is logged in the *auth.log* file as an “authentication failure.” You could use grep to search the *auth.log* file for that text with the following command:

```
sudo grep "authentication failure"/var/log/auth.log
```

This shows only the entries with the text “authentication failure” (without the quotes).

Note that it’s also possible to use the cat command and the grep command together like this:

```
sudo cat /var/log/auth.log | grep "authentication failure"
```

This reads the file with cat and then pipes the result to the grep command.

head Command

Sometimes you only want to see the beginning of a log file. The **head** command allows you to do so easily. By default, it shows the first 10 lines of a file. Imagine that you wanted to verify that the *var/log/syslog* file was being rotated successfully. The *logrotate.service* normally copies the *syslog* file to the *syslog.1* file. It then erases the *syslog* file, and new events are written there. One of the first entries (with a timestamp close to 00:00) indicates the *logrotate.service* succeeded. To see this, you can use the following command:

```
sudo head /var/log/syslog
```

tail Command

The **tail** command displays the last 10 lines of a log file by default. As an example, imagine you are troubleshooting issues related to application

errors on your system. You could issue the following command to view the last 15 messages in the /var/log/messages file.

sudo tail -n 15 /var/log/messages

Notice that the -n 15 switch specifies how many lines to display if you want to see something other than the default of 10 lines. You can use the same switch with the head command.

logger Command

You can use the **logger** command to add entries in the /var/log/syslog file from the terminal or from scripts and applications. Administrators sometimes use this command before performing an operation, such as when starting a backup operation. Here's an example:

logger Backup started

This gives you a timestamped entry with the text of "Backup started."

journalctl Command

The **journalctl** command queries the Linux system logging utility (journald) and displays log entries from several sources. You can't query journald directly because it stores log data in a binary format, but journalctl displays the data as text.

If you enter the command by itself, it displays all journal entries, which can be fairly extensive. However, there are multiple ways you can limit the output. For example, you can limit the logs displayed to only the last hour using this command:

journalctl -- since "1 hour ago"

You can also use it to view entries from previous boots. Imagine your system is currently showing errors when booting, but it didn't have any problems previously. The following commands show the available boot logs and retrieve the boot log identified with the number -1:

journalctl --list-boots

journalctl -1

As with any other command that sends output to the display, you can redirect the output to a text file using the redirect operator. The following command sends the output to the text file named myjournal.txt:

journalctl -- since "1 hour ago">> myjournal.txt

chmod Command

The **chmod** (short for change mode) command is used to modify permissions on Linux system files and folders. Any file can have read, write, and execute permissions. Appendix A goes into more depth on Linux permissions:

- Read (R) indicates someone can open the file and view its contents.
- Write (W) indicates a user can modify the contents. It is generally combined with read.
- Executes (X) indicates a user can launch the file and is used with executable files.

Additionally, permissions apply to three identities:

- The first set of permissions applies to the owner of the file.
- The second set of permissions applies to the owner group.
- The third set of permissions applies to everyone else.

It's common to set permissions using octal numbers (from 0 to 7). As an example, the following command gives read, write, and execute permissions to the owner, read and write permission to the owner group, and zero permissions to everyone else:

chmod 760 filename

It's also possible to assign permissions using the text method. The following letters are used:

- **u.** Indicates the file owner
- **g.** Indicates the owner group
- **o.** Indicates all others

You then assign permissions with these letters and the r, w, x permissions. As an example, if you want to add read permission to the group, you would use this command:

chmod g=r filename

You can remove permissions by using a dash. The following example removes execute permission from all others:

chmod o-x filename

Understanding Logs

The CompTIA Security+ exam expects test takers to look at log entries and interpret them. For administrators who work with logs every day, this becomes second nature. However, some test takers don't look at logs every day. For them, log entries can sometimes look like a foreign language. If you're the latter, please check out Appendix B, "Log Basics," to help you gain some insight into common elements in log entries and how to interpret them.

Log entries help administrators and security investigators determine what happened, when it happened, where it happened, and who or what did it. When examining entries from multiple logs, personnel create an audit trail that identifies all the events preceding a security incident. The following sections discuss many concepts related to logs that you should understand prior to test day.

Windows Logs

Operating systems have basic logs that record events. For example, Windows systems have several common logs that record what happened on a Windows computer system. These logs are viewable using the Windows Event Viewer. The primary Windows logs are:

- **Security log.** The *Security log* functions as a security log, an audit log, and an access log. It records auditable events such as successes or failures. Success indicates an audited event completed successfully, such as a user logging on or successfully deleting a file. Failure means that a user tried to perform an action but failed, such as failing to log on or attempting to delete a file but receiving a permission error instead. Windows enables some auditing by default, but administrators can add additional auditing.
- **System.** The operating system uses the *System log* to record events related to the functioning of the operating system. This can include when it starts, when it shuts down, information on services starting and stopping, drivers loading or failing, or any other system component event deemed important by the system developers.
- **Application log.** The *Application log* records events sent to it by applications or programs running on the system. Any application has the capability of writing events in the Application log. This includes warnings, errors, and routine messages.

If a system is attacked, you may be able to learn details of the attack by reviewing the operating system logs. Depending on the type of attack, any of the operating system logs may be useful.

Network Logs

Network logs record traffic on the network. These logs are on a variety of devices such as routers, firewalls, web servers, and network intrusion detection/prevention systems. You can typically manipulate these devices to log specific information, such as logging all traffic that the device passes, all traffic that the device blocks, or both. These logs are useful when troubleshooting connectivity issues and when identifying potential intrusions or attacks. They include information on where the packet came from (the source) and where it is going (the destination). This includes IP addresses, MAC addresses, and ports. Chapter 3 covers routers and firewalls, and Chapter 4 covers intrusion detection and prevention systems.

Web servers typically log requests to the web server for pages. These often follow the Common Log format standardized by the World Wide Web Consortium (W3C). A typical entry includes the following data:

- **host:** The IP address or hostname of the client requesting the page.
- **user-identifier:** The name of the user requesting the page (if known)
- **authuser:** The logon name of the user requested in the page, if the user logged on.
- **date:** The date and time of the request.
- **request:** The actual request line sent by the client.
- **status:** The HTTP status code returned to the client
- **bytes:** The byte length of the reply.

Centralized Logging Methods

It can be quite challenging to routinely check the logs on all the devices within a network. A standard solution is to use a centralized system to collect log entries. Two popular methods are with a SIEM system and with the syslog protocol.

SIEM Systems

A ***security information and event management (SIEM)*** system provides a centralized solution for collecting, analyzing, and managing data from multiple sources. It combines the services of security event management (SEM) and security information management (SIM) solutions. A SEM provides real-time monitoring, analysis, and notification of security events, such as suspected security incidents. A SIM provides long-term storage of data, along with methods of analyzing the data looking for trends or creating reports needed to verify compliance with laws or regulations.

SIEM systems are very useful in large enterprises that have massive amounts of data and activity to monitor. Consider an organization with over 1,000 servers. When an incident occurs on just one of those servers, administrators need to know about it as quickly as possible. A benefit is that SIEM systems use scripts to automate the monitoring and reporting.

Vendors sell SIEMs as applications that can be installed on centralized systems and as dedicated hardware appliances. However, no matter how a vendor bundles it, it will typically have common capabilities.

The following list outlines some additional capabilities shared by most SIEMs:

- **Log collectors.** The SIEM collects log data from devices throughout the network and stores these logs in a searchable database.
- **Data inputs.** Log entries come from various sources, such as firewalls, routers, network intrusion detection and prevention systems, and more. They can also come from any system that an organization wants to monitor, such as web servers, proxy servers, and database servers.
- **Log aggregation.** Aggregation refers to combining several dissimilar items into a single similar format. The SIEM system

collects data from multiple systems, and these systems typically format log entries differently. However, the SIEM system can aggregate the data and store it so that it is easy to analyze and search.

- **Correlation engine.** A correlation engine is a software component used to collect and analyze event log data from various systems within the network. It typically aggregates the data looking for common attributes. It then uses advanced analytic tools to detect patterns of potential security events and raises alerts. System administrators can then investigate the alert.
- **Reports.** Most SIEM systems include multiple built-in reports. These are typically grouped in different categories such as network traffic event monitoring, device events (such as events on border firewalls), threat events, logon/logoff events, compliance with specific laws, and more. Additionally, security professionals can create their own reports by specifying filters.
- **Packet capture.** Protocol analyzers (sometimes called sniffers) capture network traffic allowing administrators to view and analyze individual packets. Chapter 8 covers various packet capture tools in more depth. However, many SIEM systems include the same capabilities.
- **User behavior analysis.** User behavior analysis (UBA) focuses on what users are doing, such as what applications they are launching and their network activity. Some UBA processes watch critical files looking for who accessed them, what they did, and how frequently they access these files. UBA typically looks for abnormal patterns of activity that may indicate malicious intent. Some data loss prevention (DLP) systems include this ability.
- **Sentiment analysis.** Generically, sentiment analysis refers to analyzing text to detect an opinion or emotion. Within a SIEM system, it refers to using UBA technologies to observe user behaviors to detect unwanted behavior. This is no small feat and typically relies on artificial intelligence to analyze large data sets.

- **Security monitoring.** A SIEM typically comes with predefined alerts, which can provide continuous monitoring of systems and provide notifications of suspicious events. For example, if it detects a port scan on a server, it might send an email to an administrator group or display the alert on a heads-up display. SIEMs also include the ability to create new alerts.
- **Automated triggers.** Triggers cause an action in response to a predefined number of repeated events. As an example, imagine a trigger for failed logons is set at five. If an attacker repeatedly tries to log on to a server using Secure Shell (SSH), the server's log will show the failed logon attempts. When the SIEM detects more than five failed SSH logons, it can change the environment and stop the attack. It might modify a firewall to block these SSH logon attempts or send a script to the server to temporarily disable SSH. A SIEM includes the ability to modify predefined triggers and create new ones.
- **Time synchronization.** All servers sending data to the SIEM should be synchronized with the same time. This becomes especially important when investigating an incident so that security investigators know when events occurred. Additionally, large organizations can have locations in different time zones. Each of these locations might have servers sending data to a single centralized SIEM. If the server logs use their local time, the SIEM needs to ensure that it compensates for the time offset. One method is to convert all times to Greenwich Mean Time (GMT), which is the time at the Royal Observatory in Greenwich, London.
- **Event deduplication.** Deduplication is the process of removing duplicate entries. As an example, imagine 10 users receive the same email and choose to save it. An email server using deduplication processing keeps only one copy of this email, but makes it accessible to all 10 users. Imagine a network intrusion detection system (NIDS) collects data from a firewall and a SIEM collects data from the NIDS and the firewall. The SIEM stores only a single copy of any duplicate log entries, but also ensures that the entries are associated with both devices.

- **Logs/WORM.** A SIEM typically includes methods to prevent anyone from modifying log entries. This is sometimes referred to as write once read many (WORM). As logs are received, the SIEM aggregates and correlates the log entries. After processing the logs, it can archive the source logs with write protection.

The location of the SIEM (and the location of its correlation engine) varies based on how the SIEM is used. However, it's common to locate the SIEM within the private network, even if it collects data from a screened subnet. The internal network provides the best protection for the log data. In very large organizations, aggregation processes and the correlation engine can consume a lot of processing power, so organizations sometimes off-load these processes to another server. The primary SIEM appliance can then focus on alerts and triggers.

Dashboards in automobiles provide drivers with a view of what they need to know while driving. Similarly, a SIEM dashboard gives administrators views of meaningful activity. These views vary depending on the application developer and are usually customizable, but they provide continuous monitoring and real-time reporting. In a large network operations center (NOC), the SIEM might display alerts on a large heads-up display. In a smaller network, a single computer may show the dashboard. Some common elements of a SIEM dashboard are listed below:

- **Sensors.** Many SIEM systems use agents placed on systems throughout a network. These collect logs from devices and send these logs to the SIEM system. Dashboards can display data received from these agents.
- **Alerts.** After setting triggers in a SIEM system, it sends out alerts when the event fires. These alerts may trigger specific responses (such as sending an email to a group), but they are also displayed in the dashboard.
- **Sensitivity.** A challenge with triggers and alerts is setting the sensitivity levels to limit false positives while avoiding false negatives. As an example, imagine Homer enters an incorrect password when logging on. This isn't an attack, but an honest error. If the SIEM system raises an alert, it would be a false positive. Alternatively, imagine a system is under attack and

logs 100 failed login tries in about five minutes. If the SIEM system doesn't raise an alert, it is a false negative. When setting the sensitivity level for failed logins, administrators pick a number between 1 and 100.

- **Correlation.** As log entries arrive at the SIEM system, it correlates and analyzes the data. Administrators can configure the dashboard to display this data in multiple ways depending on their needs.
- **Trends.** As the SIEM system is analyzing the data, it can identify trends. For example, if there is suddenly a high rate of failed logins, it can identify the trend and raise an alert. Many SIEM systems display trends in graphs allowing users to digest a lot of information in a single picture.

Syslog

The *syslog* protocol specifies a general log entry format and the details on how to transport log entries. You can deploy a centralized syslog server to collect syslog entries from a variety of devices in the network, similar to how a SIEM server collects log entries.

Syslog was developed in the 1980s and became a standard on Unix-like systems. However, there wasn't a single publication that defined it. The IEEE documented it in an informational RFC (RFC 3164) in 2001. In 2009, they documented it as a standard in RFC 5424.

Any systems sending syslog messages are originators. They send syslog log entries to a collector (a syslog server). The collector can receive messages from external devices or services and applications on the same system.

It's important to note that the syslog protocol only defines how to format the syslog messages and send them to a collector. However, it doesn't define how the syslog server handles these log entries. Linux systems include the `syslogd` daemon, which is the service that handles the syslog messages. It collects the entries and processes them based on entries in the `/etc/syslog.conf` file. Many syslog messages are routed to the `/var/syslog` file.

It's also possible to use additional applications to collect and process syslog entries. Some sophisticated applications using syslog can perform

many of the same functions of a SIEM system.

Historically, systems sent syslog messages via UDP using port 514. UDP doesn't provide guaranteed delivery. Newer implementations can use TCP port 6514 with Transport Layer Security (TLS). TCP ensures the packets arrive, and TLS provides encryption.

Syslog-ng and Rsyslog

Two additional open source software utilities are used instead of syslogd on Linux-like systems. These are based on syslogd but provide additional extensions. They are:

- **Syslog-ng.** *Syslog-ng* extends syslogd, allowing a system to collect logs from any source. It also includes correlation and routing abilities to route log entries to any log analysis tool. It provides rich filtering capabilities, content-based filtering, and can be extended with tools and modules written in other languages. It supports TCP and TLS.
- **Rsyslog.** *Rsyslog* came out later as an improvement over syslog-ng. One significant change is the ability to send log entries directly into database engines. It also supports TCP and TLS.

NXLog

NXLog is another log management tool and is similar to rsyslog and syslog-ng. However, it supports log formats for Windows, such as event log entries. Additionally, it can be installed on both Windows and Linux-like systems. It functions as a log collector, and it can integrate with most SIEM systems. It comes in two versions:

- **NXLog Community Edition.** The Community Edition is a propriety log management tool available from <https://nxlog.co>. Installation packages are available for Microsoft Windows and GNU/Linux. While it's free, it includes a feature set comparable with some SIEM solutions.
- **NXLog Enterprise Edition.** The Enterprise Edition includes all the features of the Community Edition but adds additional capabilities. It provides real-time event correlation and remote administration.

Linux Logs

The CompTIA Security+ exam includes several Linux-based commands, as discussed previously in this chapter. With this in mind, it's valuable to know about some common Linux logs. These are located in the /var/log/directory. You can view logs using the System Log Viewer on Linux systems or by using the cat command from the terminal. As an example, you can view the authentication log (*auth.log*) with the following command:

```
cat /var/log/auth.log
```

Some common Linux logs are shown in the following list:

- **var/log/syslog.** The syslog file stores all system activity, including startup activity. Note that this is not the syslog protocol used to collect log entries from other systems.
- **var/log/messages.** This log contains a wide variety of general system messages. It includes some messages logged during startup, some messages related to mail, the kernel, and messages related to authentication.
- **var/log/boot.log.** This log includes entries created when the system boots.
- **var/log/auth.log.** The authentication log contains information related to successful and unsuccessful logins.
- **var/log/faillog.** This log contains information on failed login attempts. It can be viewed using the faillog command.
- **/var/log/kern.log.** The kernel log contains information logged by the system kernel, which is the central part of the Linux operating system.
- **/var/log/httpd/.** If the system is configured as an Apache web server, you can view access and error logs within this directory.

Chapter 1 Exam Topic Review

When preparing for the exam, make sure you understand these key concepts covered in this chapter.

Understanding Core Security Goals

- A use case helps professionals identify and clarify requirements to achieve a goal.
- Confidentiality ensures that data is only viewable by authorized users. Encryption is the best choice to provide confidentiality. Access controls also protect the confidentiality of data.
- Integrity provides assurances that data has not been modified, tampered with, or corrupted through unauthorized or unintended changes. Data can be a message, a file, or data within a database. Hashing is a common method of ensuring integrity.
- Availability ensures that data and services are available when needed. A common goal is to remove single points of failure. Fault tolerance methods and redundancies are commonly added to support high availability.
- Systems scale up by adding additional hardware resources such as memory, processing power, bandwidth capability, and/or drive space. Systems scale out by adding additional nodes or servers. They can scale down or scale in by removing these resources.
- Scalability is the ability of a system to handle increased workload either by scaling up or by scaling out. This is done manually by administrators.
- Elasticity is the ability of a system to handle the increased workload by dynamically scaling up or scaling out as the need arises. Cloud resources typically have elasticity capabilities allowing them to adapt to this increased and decreased demand on the fly.
- Resiliency methods help systems heal themselves or recover from faults with minimal downtime.

- Organizations balance resource availability with security constraints. Security professionals may want to apply security controls everywhere without considering the cost. However, executives have a responsibility to minimize costs without sacrificing security.

Introducing Basic Risk Concepts

- Risk is the possibility of a threat exploiting a vulnerability and resulting in a loss.
- A threat is any circumstance or event that has the potential to compromise confidentiality, integrity, or availability.
- A vulnerability is a weakness. It can be a weakness in the hardware, software, configuration, or users operating the system.
- Risk mitigation reduces risk by reducing the chances that a threat will exploit a vulnerability or reduce the risk's impact.
- Security controls reduce risks. For example, antivirus software is a security control that reduces the risk of virus infection.

Understanding Security Controls

- The three primary security control categories are managerial, operational, and technical.
- Managerial controls are primarily administrative and include items such as risk and vulnerability assessments.
- Operational controls are focused on the day-to-day operations of an organization. They help ensure an organization is complying with its overall security plan. Some examples include security awareness and training, configuration management, and change management.
- Technical controls use technology to reduce vulnerabilities. Encryption, antivirus software, IDSs, firewalls, and the principle of least privilege are technical controls.
- Preventive controls attempt to prevent security incidents. Examples include system hardening, user training, guards, change management, and account disablement policies.
- Detective controls attempt to detect when a vulnerability has been exploited. Examples include log monitoring, security

information and event management (SIEM) systems, trend analysis, video surveillance systems, and motion detection systems.

- Corrective and recovery controls attempt to reverse the impact of an incident or problem after it has occurred. Examples include backups, system recovery plans, and incident handling processes.
- Physical controls are any controls that you can physically touch. Some examples are bollards and other barricades, access control vestibules (sometimes called mantraps), lighting, fences, and signs.
- Deterrent controls attempt to prevent incidents by discouraging threats. Examples include locks and guards. Note that these can also be described as preventive controls. The primary difference is that they try to discourage people from trying to exploit a weakness.
- Compensating controls are alternative controls used when it isn't feasible or possible to use the primary control.
- Response controls, or incident response controls, help an organization prepare for security incidents and respond to them when they occur.

Using Command-Line Tools

- You run command-line tools in the Command Prompt window (in Windows) and the terminal (in Linux).
- The ping command can be used to check connectivity; check name resolution; and verify that routers, firewalls, and intrusion prevention systems block ping traffic.
- Linux systems support the hping command, which can be used instead of ping because it can use TCP or UDP instead of ICMP. It can also identify open ports on remote systems.
- The ipconfig command on Windows allows you to view the configuration of network interfaces.
- Linux uses ifconfig to view and manipulate the configuration of network interfaces. You can enable promiscuous mode on a NIC with ifconfig.

- Netstat allows you to view statistics for TCP/IP protocols and view all active network connections. This can be useful if you suspect malware is causing a computer to connect with a remote computer.
- Tracert (on Windows systems) lists the routers (also called hops) between two systems. It can verify a path has not changed. Linux systems use traceroute.
- The arp command allows you to view and manipulate the ARP cache. This can be useful if you suspect a system's ARP cache has been modified during an attack.
- The cat command (short for concatenate) displays the contents of files.
- The grep command (short for globally search a regular expression and print) searches for a specific string or pattern of text within a file.
- Linux supports several commands to view logs. The head command displays the beginning of a log file, and the tail command displays the end of a log file. The logger command adds entries to a log file.
- The journalctl command displays log entries from several different sources on Linux systems.
- You use the chmod (short for change mode) command to change permissions on files.

Understanding Logs

- Windows includes several logs that you can view with the Windows Event Viewer. The Security log functions as a security log, an audit log, and an access log. Windows records events related to the operating system in the System log. Applications record events in the Application log.
- Security information and event management (SIEM) systems provide a centralized solution for collecting, analyzing, and managing data from multiple sources.
- The syslog protocol specifies a log entry format and the details on how to transport log entries. You can deploy a centralized syslog server to collect syslog entries from a variety of devices in the network, similar to how a SIEM server collects log

entries. The syslog daemon (syslogd) on Linux systems collects and routes syslog entries.

- Syslog-ng extends syslogd, allowing a system to collect logs from any source.
- Rsyslog came out after syslog-ng and includes the ability to send log entries directly into database engines.
- NXLog is similar to rsyslog and syslog-ng, but it also supports Windows log formats.

Online References

- Remember, you can access online references such as labs and sample performance-based questions at <https://greatadministrator.com/sy0-601-extras/>.

Chapter 1 Practice Questions

1. Management within your organization has defined a use case to support the confidentiality of data stored in a database. Which of the following solutions will BEST meet this need?
 - A. Hashing
 - B. Disk redundancies
 - C. Encryption
 - D. Patching

2. Apu manages network devices in his store and maintains copies of the configuration files for all the managed routers and switches. On a weekly basis, he creates hashes for these files and compares them with hashes he created on the same files the previous week. Which of the following use cases is he MOST likely supporting?
 - A. Supporting confidentiality
 - B. Supporting integrity
 - C. Supporting encryption
 - D. Supporting availability

3. Which of the following is a cryptographic algorithm that will create a fixed-length output from a data file but cannot be used to re-create the original data file?
 - A. MD5
 - B. AES
 - C. IDS
 - D. SIEM

4. Your organization hosts an e-commerce web server selling digital products. The server randomly experiences a high volume of sales and usage, which causes spikes in resource usage. These spikes occasionally take the server down. Which of the following should be implemented to prevent these outages?
 - A. Elasticity
 - B. Scalability

- C. Normalization
- D. Stored procedures

5. An administrator recently installed an IDS to help reduce the impact of security incidents. Which of the following BEST identifies the control type of an IDS?

- A. Preventive
- B. Physical
- C. Deterrent
- D. Detective

6. Maggie works in the security section of the IT department. Her primary responsibilities are to monitor security logs, analyze trends reported by the SIEM, and validate alerts. Which of the following choices BEST identifies the primary security control she's implementing?

- A. Compensating
- B. Preventive control
- C. Detective control
- D. Corrective control

7. A server in your network's DMZ was recently attacked. The firewall logs show that the server was attacked from an external IP address with the following socket: 72.52.230.233:6789. You want to see if the connection is still active. Which of the following tools would be BEST to use?

- A. tracert
- B. arp
- C. netstat
- D. dig

8. You suspect that traffic in your network is being rerouted to an unauthorized router within your network. Which of the following command-line tools would help you narrow down the problem?

- A. ping
- B. tracert
- C. ipconfig
- D. netstat

9. Homer is complaining that he frequently has trouble accessing files on a server in the network. You determine the server's IP address is 172.16.17.11, but ping doesn't show any problem. You decide to use pathping and see the following results:

```
C:\>pathping 172.16.17.11
Tracing route to 172.16.17.11
over a maximum of 30 hops:
0 192.168.7.34
1 192.168.7.1
2 192.168.5.1
3 10.5.48.1
4 10.80.73.150
5 172.16.17.11
```

Computing statistics for 125 seconds...

Source to Here This Node/Link

Hop	RTT	Lost/Sent=Pct	Lost/Sent=Pct	Address
0				192.168.7.34
		0/100 = 0%		
1	45 ms	0 / 100 = 0%	0/100 = 0%	192.168.7.1
		14/100 = 14%		
2	25 ms	15 / 100 = 15%	0/100 = 0%	192.168.5.1
		0/100 = 0%		
3	22 ms	16 / 100 = 16%	0/100 = 0%	10.5.48.1
		0/100 = 0%		
4	---	100 / 100 = 100%	100/100 = 100%	10.80.73.150
		0/100 = 0%		
5	23 ms	16 / 100 = 16%	0/100 = 0%	172.16.17.11

Which of the following is the MOST likely problem?

- A. The router with the IP address of 10.80.73.150
- B. The router with the IP address of 192.168.5.1
- C. The segment between 192.168.7.1 and 192.168.5.1
- D. The router with the IP address of 192.168.7.1

10. You're troubleshooting a connectivity issue with a server that has an IP address of 192.168.1.10 from your Linux system. The server does not

respond to the ping command, but you suspect that a router is blocking the ping traffic. Which of the following choices would you use to verify the server is responding to traffic?

- A. hping
- B. ipconfig
- C. netstat
- D. arp

11. Lisa is manually searching through a large log file on a Linux system looking for brute force attack indicators. Which of the following commands will simplify this process for her?

- A. grep
- B. head
- C. tail
- D. cat

12. You want to verify that the syslog file is being rotated successfully on a Linux system. Which of the following commands is the BEST choice to use?

- A. logger
- B. cat
- C. tail
- D. head

13. You are writing a script that will perform backups on a Linux system and you plan to schedule the script to run after midnight daily. You want to ensure that the script records when the backup starts and when the backup ends. Which of the following is the BEST choice to meet this requirement?

- A. head
- B. tail
- C. grep
- D. logger

14. Maggie needs access to the *project.doc* file available on a Linux server. Lisa, a system administrator responsible for this server, sees the following permissions for the file:

rwx rw- ---

What should Lisa use to grant Maggie read access to the file?

- A. chmod
- B. journalctl
- C. cat
- D. LAMP

15. Which of the following describes the proper format of log entries for Linux systems?

- A. NXlog
- B. logger
- C. SIEM
- D. syslog

Chapter 1 Practice Question Answers

1. **C** is correct. Encryption is the best choice to provide confidentiality of any type of information, including data stored in a database. Hashing supports a use case of supporting integrity. Disk redundancies provide resilience and increase availability. Patching systems increases availability and reliability.
2. **B** is correct. He is most likely using a use case of supporting integrity. By verifying that the hashes are the same on the configuration files, he is verifying that the files have not changed. Confidentiality is enforced with encryption, access controls, and steganography. Encryption is a method of enforcing confidentiality, and it doesn't use hashes. Availability ensures systems are up and operational when needed.
3. **A** is correct. Message Digest 5 (MD5) is a hashing algorithm that creates a fixed-length, irreversible output. Hashing algorithms cannot re-create the original data file from just the hash. Advanced Encryption Standard (AES) is an encryption algorithm, and you can re-create the original data file by decrypting it. An intrusion detection system (IDS) is not a cryptographic algorithm but is a detective control. A security information and event management (SIEM) system provides centralized logging.
4. **A** is correct. Elasticity is the best choice because it allows the server to dynamically scale up or out as needed in response to high resource usage. Scalability isn't the best answer because it is done manually, however, the high resource usage is random and manually adding resources can't respond to the random spikes quick enough. Normalization refers to organizing tables and columns in a database to reduce redundant data and improve overall database performance. Stored procedures are a group of SQL statements that execute as a whole and help prevent SQL injection attacks.
5. **D** is correct. An intrusion detection system (IDS) is a detective control. It can detect malicious traffic after it enters a network. A preventive control, such as an intrusion prevention system (IPS), prevents malicious traffic

from entering the network. An IDS uses technology and is not a physical control. Deterrent controls attempt to discourage a threat, but attackers wouldn't know if a system had an IDS, so the IDS can't deter attacks.

6. **C** is correct. Monitoring security logs, analyzing trend reports from a security information and event management (SIEM), and validating alerts from a SIEM are detective controls. Detective controls try to detect security incidents after they happened. A compensating control is an alternative control used when a primary security control is not feasible or is not yet deployed. Preventive controls attempt to prevent incidents, but the scenario doesn't specifically describe any preventive controls. A corrective control attempts to reverse the impact of a security incident after it has happened.

7. **C** is correct. The **netstat** command can be used to display a list of open connections, including both the IP address and the port (or a socket). None of the other commands display active connections. The **tracert** command lists the routers between two systems. The **arp** command shows the contents of the Address Resolution Protocol (ARP) cache. The **dig** command can be used on Linux systems to query Domain Name System (DNS) servers.

8. **B** is correct. You can use **tracert** to track packet flow through a network, and if an extra router has been added to your network, tracert will identify it. You can use **ping** to check connectivity with a remote system, but it doesn't show the route. The **ipconfig** command shows the network settings on a Windows computer, but it doesn't identify failed routers. **Netstat** shows active connections and other network statistics on a local system, but it doesn't identify network paths.

9. **C** is correct. The segment between 192.168.7.1 and 192.168.5.1 is most likely the problem. The results show packet loss of 14 percent on this segment. The router at 10.80.73.150 (hop 4) is showing 100 percent packet loss but traffic is still getting to the server at 172.16.17.11 (hop 5). This indicates the router at 10.80.73.150 is not responding to ICMP traffic. The packet loss between the source and 192.168.5.1 is due to the packet loss on the previous network segment. There is no packet loss to 192.168.7.1.

10. A is correct. The **hping** command can be used in place of the **ping** command when network devices are blocking **ping** commands using Internet Control Message Protocol (ICMP) traffic. It can send packets using TCP and other protocols instead of ICMP. The **ipconfig** command is used to view TCP/IP configuration information. **Netstat** shows active connections and network statistics. The **arp** command shows the contents of the arp cache and does not use echo commands.

11. A is correct. The **grep** command (short for globally search a regular expression and print) is used to search for a specific string or pattern of text within a file and simplifies the search. None of the other answers listed search the entire file. The **head** command shows only a specific number of lines at the beginning of a file, and the **tail** command shows only a specific number of lines at the end of a file. The **cat** command (short for concatenate) is used to display the entire contents of a file but doesn't narrow the search for specific text strings found in a brute force attack.

12. D is correct. The **head** command shows the first 10 lines (by default) of a log file, and if the log is being rotated properly, one of the first log entries indicates the logrotate.service has succeeded. Rotating the log copies the current log, erases the log, and starts logging new entries at the beginning of every day.

The **logger** command is used to add entries into the syslog file. It doesn't read the file. The **cat** command (short for concatenate) displays the entire contents of a file but scrolls past the first entries very quickly making them difficult to catch. The **tail** command shows the last 10 lines (by default) of a log file, and is unlikely to include the first entries showing that the logrotate.service succeeded.

13. D is correct. The **logger** command is used to add entries into the syslog file and can be called from scripts, applications, or the terminal. The **head** command can be used to view the first lines in the syslog file and can view the logger entry, but it doesn't add any entries into the syslog file. The **tail** command shows the last 10 lines (by default) of a log file, but it doesn't

write into a log file. The **grep** command (short for globally search a regular expression and print) is used to search files but it doesn't write into files.

14. **A** is correct. The system administrator should modify permissions with the **chmod** (short for change mode) command. The **journalctl** command queries the Linux system logging utility (journald) and displays log entries from several sources. The **cat** command (short for concatenate) displays file contents. LAMP is an acronym for Linux, Apache, MySQL, and PHP (or Perl or Python).

15. **D** is correct. The syslog protocol (defined in RFC 5424) identifies the format of Linux log entries and describes how to transport these log entries. Note that syslog is also the name of a log on Linux systems. NXLog is a log management tool that can accept log entries from multiple sources, including Linux and Windows. The **logger** command is used to add entries into the syslog file but it doesn't describe the format. A security information and event management (SIEM) system collects, aggregates, and correlates logs from multiple sources.

Chapter 2

Understanding Identity and Access Management

CompTIA Security+ objectives covered in this chapter:

2.4 Summarize authentication and authorization design concepts.

- Authentication methods (Federation)
- Technologies (Time-based one-time password (TOTP), HMAC-based one-time password (HOTP), Short message service (SMS), Token key, Static codes, Authentication applications, Push notifications, Phone call), Smart card authentication
- Biometrics (Fingerprint, Retina, Iris, Facial, Voice, Vein, Gait analysis, Efficacy rates, False acceptance, False rejection, Crossover error rate)
- Multifactor authentication (MFA) factors and attributes
- Factors (Something you know, Something you have, Something you are), Attributes (Somewhere you are, Something you can do, Something you exhibit, Someone you know)
- Authentication, authorization, and accounting (AAA)

2.8 Summarize the basics of cryptographic concepts.

- Common use cases (Supporting authentication)

3.7 Given a scenario, implement identity and account management controls.

- Identity (Identity provider (IdP), Attributes, Certificates, Tokens, SSH keys, Smart cards)
- Account types (User account, Shared and generic accounts/credentials, Guest accounts, Service accounts)
- Account policies (Password complexity, Password history, Password reuse, Network location, Geolocation, Time-based logins, Access policies, Account permissions, Account audits, Impossible travel time/risky login, Lockout, Disablement)

3.8 Given a scenario, implement authentication and authorization solutions.

- Authentication management (Password keys, Password vaults, Knowledge-based authentication)
- Authentication/authorization (Single sign-on (SSO), Security Assertion Markup Language (SAML), OAuth, OpenID, Kerberos)
- Access control schemes (Attribute-based access control (ABAC), Role-based access control, Rule-based access control, MAC, Discretionary access control (DAC), Conditional access, Privileged access management, Filesystem permissions)

4.3 Given an incident, utilize appropriate data sources to support an investigation.

- Log files (Authentication)

5.3 Explain the importance of policies to organizational security.

- Credential policies (Personnel, Third party, Devices, Service accounts, Administrator/root accounts)

**

Identity and access management includes many important concepts that are tested on the CompTIA Security+ exam. Users claim an identity with a username and prove their identity by authenticating (such as with a password). They are then granted access to resources based on their proven identity. In this chapter, you'll learn about various authentication concepts and methods, along with some basic security principles used to manage accounts. This chapter closes with a comparison of some access control schemes.

Exploring Authentication Management

Authentication proves an identity with some type of credentials, such as a username and password. For example, **identification** occurs when users claim (or profess) their identity with identifiers such as usernames or email addresses. Users then prove their identity with authentication, such as with a password. In this context, a user's credentials refer to both a claimed identity and an authentication mechanism.

At least two entities know the credentials. One entity, such as a user, presents the credentials. The other entity is the authenticator that verifies the credentials. For example, Marge knows her username and password, and an authenticating server knows her username and password. Marge presents her credentials to the authenticating server, and the server authenticates her.

It's important to understand that you can't have any type of access control without authentication. Without authentication, you can't identify a user. In other words, if everyone is anonymous, then everyone has the same access to all resources.

Also, authentication is not limited to users. Services, processes, workstations, servers, and network devices all use authentication to prove their identities. Many computers use mutual authentication, where both parties authenticate to each other.

Comparing Identification and AAA

Authentication, authorization, and accounting (AAA) work together with identification to provide a comprehensive access management system. If you understand identification (claiming an identity, such as with a username) and authentication (proving the identity, such as with a password), it's easier to add in the other two elements of AAA—authorization and accounting.

If users can prove their identity, that doesn't mean that they are automatically granted access to all resources within a system. Instead, users are granted ***authorization*** to access resources based on their proven identity. This can be as simple as granting a user permission to read data in a shared folder. Access control systems include multiple security controls to ensure that users can access resources they're authorized to use, but no more.

Accounting methods track user activity and record the activity in logs. As an example, audit logs track activity, and administrators use these to create an ***audit trail***. An audit trail allows security professionals to re-create the events that preceded a security incident.

Effective access control starts with strong authentication mechanisms, such as robust passwords, smart cards, or biometrics. If users can bypass the authentication process, the authorization and accounting processes are ineffective.

Remember this

Identification occurs when a user claims an identity, such as with a username or email address. Authentication occurs when the user proves the claimed identity (such as with a password) and the credentials are verified (such as with a password). Access control systems provide authorization by granting access to resources based on permissions granted to the proven identity. Logging provides accounting.

Comparing Authentication Factors

Authentication is often simplified as types, or factors, of authentication. A common use case of supporting authentication may require administrators to implement one authentication factor for basic authentication, two factors for more secure authentication, or more factors for higher security. As an introduction, the factors are:

- Something you know, such as a password or personal identification number (PIN)
- Something you have, such as a smart card, a phone, or a USB token
- Something you are, such as a fingerprint or other biometric identification

Something You Know

The ***something you know*** authentication factor typically refers to a shared secret, such as a password, a static code, or a PIN. This factor is the least secure form of authentication. Because passwords stay the same for a long time, they are sometimes called static passwords or ***static codes***.

Best practice recommendations related to passwords have changed over the years. NIST SP 800-63b, “Digital Identity Guidelines,” refers to passwords as memorized secrets chosen by the user and recommends users create easy-to-remember and hard-to-guess passwords. Microsoft and the U.S. Department of Homeland Security (DHS) have adopted several of the same recommendations. As you read through the explanations in the following sections, consider some of NIST, Microsoft, and the U.S. DHS’s current password recommendations:

- Hash all passwords.
- Require multifactor authentication.
- Don’t require mandatory password resets.
- Require passwords to be at least eight characters.
- Check for common passwords and prevent their use.
- Tell users not to use the same work password anywhere else.
- Allow all special characters, including spaces, but don’t require them.

Chapter 10, “Understanding Cryptography and PKI,” covers hashing, salting, and key stretching to protect stored passwords. These techniques make it much harder for attackers to discover stored passwords.

Password Complexity

One method used to make passwords more secure is to require them to be complex and strong. A strong password is of sufficient length, doesn’t include words found in a dictionary or any part of a user’s name, and combines at least three of the four following character types:

- Uppercase characters (26 letters A–Z)
- Lowercase characters (26 letters a–z)
- Numbers (10 numbers 0–9)
- Special characters (such as !, \$, and *)

A complex password uses multiple character types, such as Ab0@. However, a complex password isn’t necessarily strong. It also needs to be sufficiently long. Many current recommendations suggest a length of at least 8 characters.

There are conflicting recommendations from other sources. As an example, the Payment Card Industry Data Security Standard (PCI DSS) version 3.2.1 recommends a password length of 7 characters. The HITRUST CSF (short for Common Security Framework) provides a way to comply with ISO/IEC 27000-series and HIPAA (Health Insurance Portability and Accountability Act) requirements. It recommends passwords be at least 15 characters long for administrators and changed at least every 90 days.

A key takeaway is that longer passwords using more character types are more secure than short passwords of 4 or 5 characters. It’s also worth pointing out that a longer password isn’t necessarily stronger if it isn’t complex. As an example, 1234567890 is a password that has shown up as a popular choice among users after data breaches. It’s 10 characters, but only uses numbers, and is trivial for an attacker to guess.

Password Expiration

A password expiration setting identifies when users must change their password. As an example, a password expiration of 60 indicates users must change their password every 60 days. If they don’t change their password,

they can no longer log on. This is often referred to as the maximum password age.

Remember this

Complex passwords use a mix of character types. Strong passwords use a mix of character types and have a minimum password length of at least eight characters. A password expiration identifies when a password must be changed.

Password History and Password Reuse

Many users would prefer to use the same password forever simply because it's easier to remember. Even when technical password policies force users to change their passwords, many users simply change them back to the original password. Unfortunately, this significantly weakens password security.

A password history system remembers past passwords and prevents users from reusing them. It's common for password policy settings to remember the last 24 passwords and prevent users from reusing them until they've used 24 new passwords.

When using password history, it's common to use the minimum password age setting. Imagine this is set to 1 day, and the password history is set to 24. After users change their password, they can't change it again until a day has passed. It'll take them 24 days of changing their password every day before they can reuse the original password.

Password Vaults

A password vault (or password manager) is a single source designed to keep most of your passwords. Instead of requiring you to memorize many different passwords, you only need to remember the password to open the vault. It keeps these passwords in an encrypted format, preventing unauthorized users from seeing them.

As an example, Google Chrome includes a password manager built into the browser. Once you log in to Google and enter a username and password at another site, Chrome will ask if you want to save it. Click Save and Chrome will store your credentials for you. The next time you go to the same site, Chrome will automatically fill in the credentials. Chrome allows

you to sync your passwords across multiple devices, too. When you enable this option, your passwords are stored with your Google account. After launching Chrome and logging onto Google, you'll have access to all of your passwords stored with your account.

Some password vaults are individual applications stored on a single computer. Once you open the vault with a password, you can store your credentials in it, and the app automatically fills in credentials when needed.

Password Keys

Password keys are used to reset passwords on systems. They are commonly a bootable optical disc or bootable USB flash drive. After rebooting the system to the device, they allow you to recover or reset all user and administrator passwords. These are useful to users who have forgotten their passwords. They are also helpful to forensic experts who need to access computers without knowing the passwords. Of course, they are also valuable for attackers who have stolen computers, such as laptops.

Many of these are available as free downloads on the Internet. You can download them and create your bootable optical disc or USB drive. Be careful, though. You may be downloading malware that installs itself on the computer as you're changing the password.

Knowledge-Based Authentication

Some organizations use ***knowledge-based authentication (KBA)*** to prove the identity of individuals. There are two types: static KBA and dynamic KBA.

Static KBA is typically used to verify your identity when you've forgotten your password. After creating your account (or when you create your account), you're prompted to answer questions about yourself, such as your first dog's name or your mother's maiden name. Later, when you try to retrieve a forgotten password, you're first prompted to answer the same questions.

Dynamic KBA identifies individuals without an account. Organizations use this for high-risk transactions, such as with a financial institution or a health care company. The site queries public and private data sources, such as credit reports or third-party organizations. It then crafts

multiple-choice questions that only the user would know and often includes an answer similar to “none of these apply.” Some examples are:

- Which of the following addresses indicate where you have lived?
- Which of the following is closest to your mortgage payment?
- How much is your car payment?
- When was your home built?

Users typically have a limited amount of time to answer these questions. This limits the amount of time an attacker can do searches on the Internet to identify accurate answers.

Implementing Account Lockout Policies

Accounts will typically have ***lockout policies*** preventing users from guessing the password. If a user enters the wrong password too many times (such as three or five times), the system locks the user’s account. Two key phrases associated with account lockout policies on Microsoft systems are:

- **Account lockout threshold.** This is the maximum number of times a user can enter the wrong password. When the user exceeds the threshold, the system locks the account.
- **Account lockout duration.** This indicates how long an account remains locked. It could be set to 30, indicating that the system will lock the account for 30 minutes. After 30 minutes, the system automatically unlocks the account. If the duration is set to 0, the account remains locked until an administrator unlocks it.

Account lockout policies thwart some password attacks, such as brute force attacks and dictionary attacks. Chapter 10 covers common password attacks.

Changing Default Passwords

Many systems and devices start with default passwords. A basic security practice is to change these defaults before putting a system into use. As an example, many wireless routers have default accounts named “admin” or “administrator” with a default password of “admin.” If you don’t change the password, anyone who knows the defaults can log on and

take control of the router. In that case, the attacker can even go as far as locking you out of your own network.

Changing defaults also includes changing the default name of the Administrator account, if possible. In many systems, the Administrator account can't be locked out through regular lockout policies, so an attacker can continue to try to guess the administrator's password without risking being locked out. Changing the name of the Administrator account to something else, such as Not4U2Know, reduces the chances of success for the attacker. The attacker needs to know the administrator account's new name before he can try to guess the password.

Some administrators go a step further and add a dummy user account named "administrator." This account has no permissions. If someone does try to guess this account's password, the system will lock it out after too many failures. This can alert administrators of possible illicit activity.

Remember this

Account lockout policies thwart some password attacks, such as brute force and dictionary attackers. Many applications and devices have default passwords. These should be changed before putting the application or device into service.

Training Users About Password Behaviors

Common user habits related to password behaviors have historically ignored security. Many users don't understand the value of their password or the potential damage if they give it out. Organizations need to provide adequate training to users on password security if they use passwords within the organization. This includes creating strong passwords, not using the same password with other systems, and never giving their password to someone else.

For example, the password "123456" frequently appears on lists as the most common password in use. The users who are creating this password probably don't know that it's almost like using no password at all. Also, they probably don't realize that they can significantly increase the password strength by using a simple passphrase such as "ICanCountTo6." A little training can go a long way.

Check out the online lab Using John the Ripper available at <https://greatadministrator.com/sy0-601-labs/>. It shows how easy it can be to crack weak passwords.

Something You Have

The *something you have* authentication factor refers to something you can physically hold. This section covers many of the common items in this factor, including smart cards, Common Access Cards, and hardware tokens. It also covers two open source protocols used with both hardware and software tokens.

Smart Card Authentication

Smart cards are credit card-sized cards that have an embedded microchip and a certificate. Users insert the *smart card* into a smart card reader, similar to how someone would insert a credit card into a credit card reader. The smart card reader reads the card's information, including the details from the certificate, which provides certificate-based authentication.

Chapter 10 covers certificates in more detail, but as an introduction, they are digital files that support cryptography for increased security. The embedded certificate allows the use of a complex encryption key and provides much more secure authentication than is possible with a simple password. Additionally, the certificate can be used with digital signatures and data encryption. The smart card provides confidentiality, integrity, authentication, and non-repudiation.

Requirements for a smart card are:

- **Embedded certificate.** The embedded certificate holds a user's private key (which is only accessible to the user) and is matched with a public key (that is publicly available to others). The private key is used each time the user logs on to a network.
- **Public Key Infrastructure (PKI).** Chapter 10 covers PKI in more depth, but in short, the PKI supports issuing and managing certificates.

Smart cards are often used with another factor of authentication. For example, a user may also enter a PIN or password and use the smart card. Because the smart card is in the something you have factor and the PIN is in

the something you know factor, this combination provides dual-factor authentication.

Remember this

Smart cards are often used with dual-factor authentication where users have something (the smart card) and know something (such as a password or PIN). Smart cards include embedded certificates used with digital signatures and encryption. They are used to gain access to secure locations and to log on to computer systems.

Token Key

A ***token key*** or (sometimes called a key fob or just a token) is an electronic device about the size of a remote key for a car. You can easily carry token keys in a pocket or purse or connect them to a key chain. They include a liquid crystal display (LCD) that displays a number, and this number changes periodically, such as every 60 seconds. They are sometimes called hardware tokens to differentiate them from logical or software tokens.

The token is synced with a server that knows what the number is at any moment. For example, at 9:01, the number displayed on the token may be 135792, and the server knows the number is 135792. At 9:02, the displayed number changes to something else, and the server also knows the new number.

This number is a one-time use, rolling password. Even if attackers do discover the password, it isn't useful to them for very long. For example, a shoulder surfing attacker might be able to look over someone's shoulder and read the number. However, the number expires within the next 60 seconds and is replaced by another one-time password.

Users often use tokens to authenticate via a website. They enter the number displayed in the token along with their username and password. This provides dual-factor authentication because the users must have something (the token) and know something (their password).

RSA sells RSA Secure ID, a popular token used for authentication. You can Google “Secure ID image” to view many pictures of these tokens. Although RSA tokens are popular, other brands are available.

HOTP and TOTP

Hash-based Message Authentication Code (HMAC) uses a hash function and cryptographic key for many different cryptographic functions. Chapter 1, “Mastering Security Basics,” introduced hashes. As a reminder, a hash is simply a number created with a hashing algorithm. **HMAC-based One-Time Password (HOTP)** is an open standard used for creating one-time passwords, similar to those used in tokens or key fobs. The algorithm combines a secret key and an incrementing counter, and uses HMAC to create a hash of the result. It then converts the result into an HOTP value of six to eight digits.

Imagine Bart needs to use HOTP for authentication. He requests a new HOTP number using a token or a software application. He can then use this number for authentication along with some other authentication method, such as a username and password. As soon as he uses it, the number expires. No one else is able to use it, and Bart cannot use it again either.

Here’s an interesting twist, though. A password created with HOTP remains valid until it’s used. Suppose Bart requested the HOTP number but then got distracted and never used it. What happens now? Theoretically, it remains usable forever. This presents a risk related to HOTP because other people can use the password if they discover it.

A **Time-based One-Time Password (TOTP)** is similar to HOTP, but it uses a timestamp instead of a counter. One-time passwords created with TOTP typically expire after 30 seconds, but the time is adjustable.

One significant benefit of HOTP and TOTP is the price. Hardware tokens that use these open source standards are significantly less expensive than tokens that use proprietary algorithms.

Authentication Applications

Many software applications use these algorithms to create software tokens used within the application. As an example, Figure 2.1 shows the free VIP Access app created by Symantec. It’s available for mobile devices and desktop systems. Once you configure it to work with a compatible authentication server, it creates a steady stream of one-time-use passwords. The six-digit security code is the password, and the counter lets you know how much more time you have before it changes again.

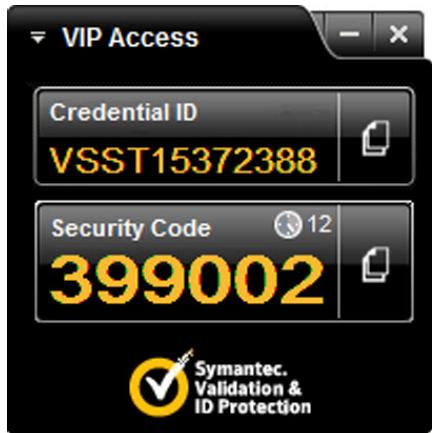


Figure 2.1: VIP Access app

Like a hardware token, the user enters a username and password as the something you know factor and then enters the app's security code as the something you have factor. This provides dual-factor authentication. Many public websites like eBay and PayPal support it, allowing many end users to implement dual-factor authentication as long as they have the app.

Some developers have created their own apps based on TOTP and HOTP but modified them with proprietary software. As an example, the Google Authenticator app (created by Google) originally used open source software but is currently using proprietary software. From the user's perspective, it still works like other authentication applications.

Remember this

HOTP and TOTP are open source standards used to create one-time-use passwords. HOTP creates a one-time-use password that does not expire until it is used, and TOTP creates a one-time password that expires after 30 seconds. Both can be used as software tokens for authentication.

Two-Step Verification

Two-step verification (also called two-factor authentication) adds an extra layer of security to accounts. Most methods rely on users having a smartphone or a regular phone. Users typically enter their username and password into a website using the something you know factor. Then, they receive a message or notification on their phone. By replying to this message, or with the message contents, it proves they have the phone (in the something you have factor).

Some authentication systems use ***Short Message Service (SMS)*** to send PINs. As an example, after you enter your credentials, it may challenge you by asking you to enter additional authentication information. If you registered your smartphone's number, it would send you a PIN to that phone. You enter the PIN, and the system authenticates you.

Careful though. NIST SP-800-63B (mentioned earlier) points out several vulnerabilities with SMS for two-step authentication and discourages its use. Normally, mobile devices display SMS text on the screen when it arrives. If someone stole the mobile device, he would see the PIN without logging on to the mobile device.

Systems that support SMS also give you an option to receive a phone call. After entering your credentials, you can choose to receive the PIN via a previously registered phone number. However, instead of coming as a text, it comes as a voice phone call. This is useful for anyone who doesn't have a phone that accepts texts.

Many users find entering additional data to be disruptive, and push notifications attempt to simplify the process. ***Push notifications*** send messages to users on another device. Imagine Lisa registered her smartphone with a website. Later, when she accesses the website and enters her username, the site sends a push notification to her phone. She can then approve the access, often by pressing a screen button on her smartphone. This eliminates the need to remember a password, making it very user-friendly. Unfortunately, it has vulnerabilities similar to SMS.

Remember this

Two-step verification methods typically use a PIN retrieved from a user's smartphone. They can be sent via SMS, a phone call, a push notification, or retrieved from an authentication application.

Something You Are

The ***something you are*** authentication factor uses biometrics for authentication. Biometric methods are the strongest form of authentication because they are the most difficult for an attacker to falsify. In comparison, passwords are the weakest form of authentication.

Biometric Methods

Biometrics uses a physical characteristic, such as a fingerprint, for authentication. Most biometric systems use a two-step process. In the first step, users register or enroll with the authentication system. For example, an authentication system first captures a user's fingerprint and then associates it with the user's identity. Later, when users want to access the system, they use their fingerprints to prove their identity.

Remember this

The third factor of authentication (something you are, defined with biometrics) is the strongest individual authentication factor. Biometric methods include fingerprints, palm veins, retina scans, iris scans, voice recognition, facial recognition, and gait analysis.

There are multiple types of biometrics, including:

- **Fingerprint.** Many laptop computers include *fingerprint scanners* or fingerprint readers, and they are also common on tablet devices and smartphones. Similarly, some USB flash drives include a fingerprint scanner. They can store multiple fingerprints to share access to the same USB device. Law enforcement agencies have used fingerprints for decades, but they use them for identification, not biometric authentication.
- **Vein.** *Vein matching* systems identify individuals using near-infrared light to view their veins. Most vein matching systems measure the veins in an individual's palm because there are more veins in the palm instead of a finger. Many hospitals and health care systems use palm scanners as a quick and easy way to identify patients and prevent patient misidentification.
- **Retina.** *Retina scanners* scan the retina of one or both eyes and use the pattern of blood vessels at the back of the eye for recognition. Some people object to the use of these scanners for authentication because they can identify medical issues, and because you typically need to have physical contact with the scanner.
- **Iris.** *Iris scanners* use camera technologies to capture the patterns of the iris around the pupil for recognition. They are used in many passport-free border crossings around the world.

They can take pictures from about 3 to 10 inches away, avoiding physical contact.

- **Facial.** *Facial recognition* systems identify people based on facial features. This includes the size of their face compared with the rest of their body, and the size, shape, and position of their eyes, nose, mouth, cheekbones, and jaw. As an example, newer iPhones include Face ID. After setting it up, you can unlock your phone simply by glancing at it.
- **Voice.** *Voice recognition* methods identify who is speaking using speech recognition methods to identify different acoustic features. One person's voice varies from another person's voice due to differences in their mouth and throat, and behavioral patterns that affect their speaking style. As an example, Apple's Siri supports voice recognition. After setting it up, Siri will only respond to the owner's voice.
- **Gait analysis.** *Gait analysis* identifies individuals based on the way they walk. It measures how someone's feet hit and leave the ground while walking. Some methods focus primarily on the feet, knees, and hips. Other methods have expanded this to examine silhouette sequences of individuals for identification. However, an individual can purposely change their gait, doing something as simple as adding a limp. In contrast, individuals can't change their fingerprints or the appearance of their iris at will.

It's worth noting that a formal enrollment process isn't always necessary, especially if the goal is identification instead of authentication. Many Las Vegas casinos have sophisticated systems that capture people's faces as they enter and roam around a casino. Casino personnel can match these faces to people recorded in massive databases.

Similarly, imagine Marge is crossing a border between two countries. As she presents her passport, a passive biometric system can capture her face. Gait analysis can also be passive by just observing and recording the gait of individuals. Combining facial recognition with gait analysis increases identification accuracy and can help prevent someone from using a fraudulent passport.

Remember this

Iris and retina scans are the strongest biometric methods mentioned in this section, though iris scans are used instead of retina scans because retina scans are intrusive and reveal private medical issues. Facial recognition and gait analysis can bypass the enrollment process when done for identification instead of authorization.

Biometric Efficacy Rates

The biometric ***efficacy rate*** refers to the performance of the system under ideal conditions. If the system is implemented correctly, it can be very exact. However, if it isn't implemented correctly, its real-world effectiveness may not match the efficacy rate.

The following bullets describe the four possibilities when a biometric system tries to authenticate a user. Refer to Figure 2.2 as you're reading them:

- **False acceptance.** This is when a biometric system incorrectly identifies an unknown user as a registered user. The ***false acceptance rate*** (FAR, also known as a false match rate) identifies the percentage of times false acceptance occurs.
- **False rejection.** This is when a biometric system incorrectly rejects a registered user. The ***false rejection rate*** (FRR, also known as a false nonmatch rate) identifies the percentage of times false rejections occur.
- **True acceptance.** This indicates that the biometric system correctly identified a registered user.
- **True rejection.** This indicates that the biometric system correctly rejected an unknown user.

		Biometric System Not Accurate	Biometric System Accurate
Registered User	False Acceptance	True Acceptance	
	False Rejection	True Rejection	

Figure 2.2: Acceptance and Rejection Matrix

Biometric systems allow you to adjust the sensitivity or threshold level where errors occur. Increasing sensitivity decreases the number of false matches and increases the number of false rejections. In contrast, reducing sensitivity increases false matches and decreases false rejections. By plotting the FAR and FRR rates using different sensitivities, you can determine a biometric system's efficacy.

Figure 2.3 shows the crossover error rate (CER) for two biometric systems (one using solid lines and the second using dotted lines). The CER is the point where the FAR crosses over with the FRR. A lower CER indicates that the biometric system is more accurate. The system represented with the solid lines is more accurate than the system represented by the dotted lines.

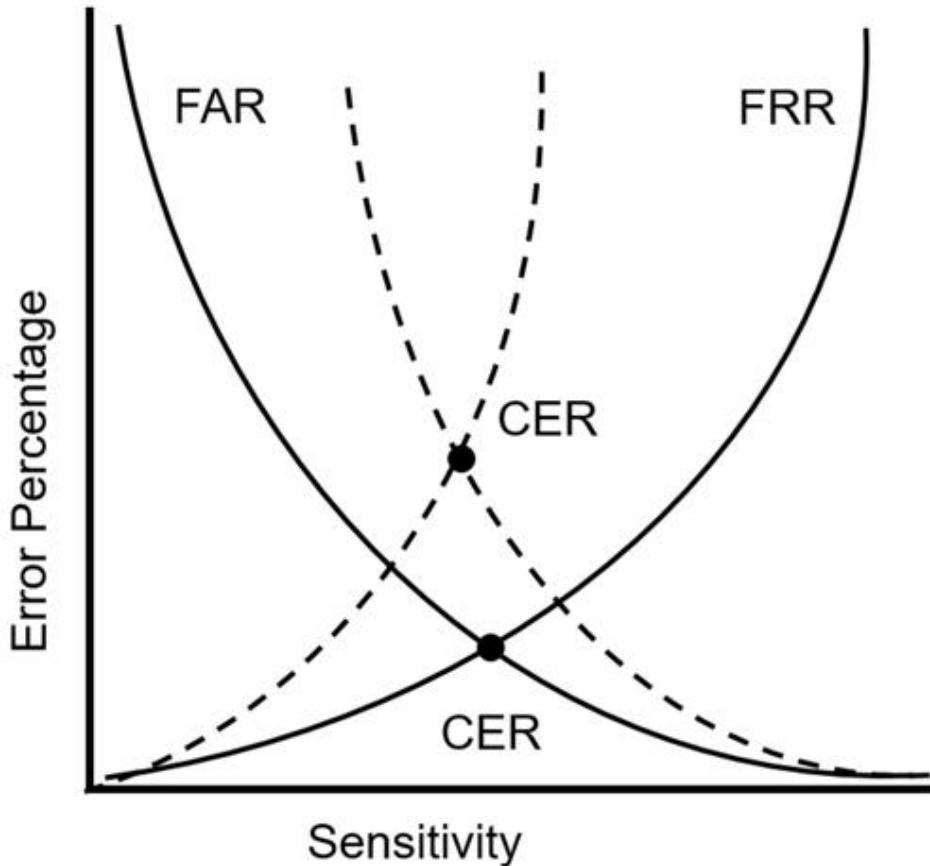


Figure 2.3: Crossover error rate

Two-Factor and Multifactor Authentication

Two-factor authentication (sometimes called dual-factor authentication) uses two different authentication factors such as something you have and something you know. Two-factor authentication often uses combinations of a smart card and a PIN, a USB token and a PIN, or a hardware token and a password.

The “Something You Have” section earlier in this chapter discussed token keys, HOTP, TOTP, authentication applications, SMS messages, and push notifications. These are common methods used to implement two-factor or multifactor authentication.

It’s worth noting that using two methods of authentication in the same factor is not two-factor authentication. For example, requiring users to enter a password and a reusable PIN (both in the something you know factor) is single-factor authentication, not dual-factor authentication. In this case, the reusable PIN isn’t sent to users via a smartphone. Instead, the user creates

the PIN, just as if it was a password. Similarly, using a thumbprint and a retina scan is not dual-factor authentication because both methods are in the something you are factor.

Remember this

Using two or more methods in the same factor of authentication (such as a PIN and a password) is single-factor authentication. Dual-factor (or two-factor) authentication uses two different authentication factors, such as using a hardware token and a PIN. Multifactor authentication uses two or more factors.

Authentication Attributes

Authentication attributes help identify a user or a device based on characteristics or traits. These are rarely used on their own but instead are used with one or more authentication factors. One way you may see them in action is with mobile devices, as discussed in Chapter 5, “Securing Hosts and Data.”

Somewhere You Are

The *somewhere you are* authentication attribute identifies a user’s location. Geolocation is a group of technologies used to identify a user’s location and is the most common method used in this factor. Many authentication systems use the Internet Protocol (IP) address for geolocation. The IP address provides information on the country, region, state, city, and sometimes even the zip code.

As an example, I once hired a virtual assistant in India to do some data entry for me. I created an account for the assistant in an online application called Hootsuite and sent him the logon information. However, Hootsuite recognized that his IP was in India when he attempted to log on. This looked suspicious, so Hootsuite blocked his access and then sent me an email saying that someone from India was trying to log on. They also provided me directions on how to grant him access if he was a legitimate user, but it was comforting to know they detected and blocked this access automatically.

The somewhere you are authentication attribute can also be used to identify impossible travel time or risky login situations. As an example,

imagine Lisa logs in to her account from her home in Springfield, and then a moment later, someone else logs in to her account from the country of Certaheadistan. Unless Lisa has a teleportation machine, she can't log in from both places simultaneously.

It's worth noting that using an IP address for geolocation isn't foolproof. There are many virtual private network (VPN) IP address changers available online. For example, a user in Russia can use one of these services in the United States to access a website. The website will recognize the VPN service's IP address but won't see the Russian IP address.

Within an organization, it's possible to use the computer name or the media access control (MAC) address of a system for the somewhere you are factor. For example, in a Microsoft Active Directory domain, you can configure accounts so that users can only log on to the network through one specific computer. If they aren't at that computer, the system blocks them from logging on at all.

Something You Can Do

The ***something you can do*** authentication factor refers to actions you can take such as gestures on a touch screen. As an example, Microsoft Windows 10 supports picture passwords. Users first select a picture, and then they can add three gestures as their picture password. Gestures include tapping in specific places on the picture, drawing lines between items with a finger, or drawing a circle around an item such as someone's head. After registering the picture and their gestures, users repeat these gestures to log on again later.

Something You Exhibit

Generically, exhibit refers to something that you show or display. Courts refer to exhibits as documents or evidence items submitted when attempting to prove or disprove something. Within the context of authentication attributes, a badge worn by an employee is something you can exhibit. Consider a secure area where everyone allowed access must wear a badge. Anyone without a badge sticks out.

Some military government organizations use Common Access Cards (CACs) or Personal Identity Verification (PIV) cards. They include a

picture of users along with personnel information, such as their name, and are worn as a badge when users are walking around the building. Additionally, they include smart card capabilities that users use to log on to computers.

Someone You Know

Someone you know indicates that someone is vouching for you. Imagine Lisa introduces you to Mary Bailey, the governor. This implies that Lisa is vouching for you. Because the governor trusts Lisa, the introduction extends a level of trust to you.

Many antivirus software applications extend this to websites. For example, if you do a search with Google and have the Norton extension, it'll show a green check mark next to the websites indicating that Norton considers the site safe.

A web of trust is another example where individuals create their own certificates using a decentralized trust model instead of a centralized certificate authority (as discussed in Chapter 10). Imagine Lisa creates a certificate and shares it with Mary. Mary trusts this certificate because she trusts Lisa. You create a certificate and share it with Lisa, and Lisa trusts this certificate because she trusts you. If you share your certificate with Mary, she trusts it because Lisa trusts it.

Authentication Log Files

Authentication log files can track both successful and unsuccessful login attempts. It's most important to monitor login activity for any privileged accounts, such as administrators. Chapter 1 discusses security information and event management (SIEM) systems. It's common to send entries from authentication logs to a SIEM system for analysis and notification of suspicious events.

As mentioned in Chapter 1, log entries help administrators determine what happened, when it happened, where it happened, and who or what did it. For authentication log entries:

- What happened is either a login success or failure
- When it happened is determined by the time and date stamps
- Where it happened is typically an IP address or computer name
- Who or what did it refers to the user account

For administrators looking at log entries daily, it's relatively easy to read logs. However, if you don't look at logs often, you might want to review Appendix B, "Log Basics."

Managing Accounts

Account management is concerned with the creation, management, disablement, and termination of accounts. When the account is active, access control methods are used to control what the user can do. Additionally, administrators use access controls to control when, where, and how users can log on. The following sections cover common account management practices, along with some basic principles used with account management.

An important concept to remember when creating accounts is to give users only the account permissions they need to perform their job, and no more. Chapter 11, “Implementing Policies to Mitigate Risks,” covers the principle of least privilege, emphasizing this in more depth.

Credential Policies and Account Types

Credential policies define login policies for different personnel, devices, and accounts. This includes items in the something you know factor (such as passwords) or any other factor or combination of factors. It's common for an organization to apply credential policies differently to different types of accounts. The following bullets identify different account types and credential policies associated with each:

- **Personnel or end-user accounts.** Most accounts are for regular users or the personnel working in the organizations. Administrators create these accounts and then assign appropriate privileges based on the user's job responsibilities. It's common to assign a basic credential policy that applies to all personnel. This could be a password policy defining things like the minimum password length, password history, and account lockout policies, as defined earlier in this chapter.
- **Administrator and root accounts.** Administrator and root accounts are privileged accounts that have additional rights and privileges beyond what a regular user has. As an example, someone with administrator privileges on a Windows computer has full control over the Windows computer. Linux systems have a root account, which grants additional privileges, similar to an administrator account on Windows systems. Credential policies require stronger authentication methods for these accounts, such as multifactor authentication. Additionally, privileged access management techniques (described in the next section) apply additional controls to protect these accounts.
- **Service accounts.** Some applications and services need to run under the context of an account, and a service account fills this need. As an example, SQL Server is a database application that runs on a server, and it needs access to resources on the server and the network. Administrators create a regular user account, name it something like sqlservice, assign it appropriate privileges, and configure SQL Server to use this account. Note

that this is like a regular end-user account. The only difference is that it's used by the service or application, not an end user. Credential policies may require long, complex passwords for these accounts, but they should not expire. If the password expires, the account can no longer log on, and the service or application will stop.

- **Device accounts.** Computers and other devices also have accounts though it isn't always apparent. As an example, Microsoft Active Directory only allows users to log on to computers joined to the domain. These computers have computer accounts and Active Directory manages their passwords.
- **Third-party accounts.** Third-party accounts are accounts from external entities that have access to a network. As an example, many organizations use security applications that have administrative access to a network. These should have strong credential policies in place with strong password policies enforced at a minimum.
- **Guest accounts.** Windows operating systems include a Guest account. These are useful if you want to grant someone limited access to a computer or network without creating a new account. For example, imagine an organization contracts with a temp agency to have someone do data entry. The agency may send a different person every day. Enabling the Guest account for this person would be simpler than creating a new account every day. Administrators commonly disable the Guest account and only enable it in special situations.
- **Shared and generic account/credentials.** An organization can create a regular user account that temporary workers will share. Shared accounts are discouraged for normal work. However, if a temp agency is sending someone different every day, a shared account may provide a better solution than a guest account because access can be tailored for the shared account. Basic credential policies apply to shared and generic accounts.

Privileged Access Management

Privileged access management (PAM, sometimes called privileged account management) allows an organization to apply more stringent security controls over accounts with elevated privileges, such as administrator or root-level accounts. PAM implements the concept of just-in-time administration. In other words, administrators don't have administrative privileges until they need them. When they need them, their account sends a request for the elevated privileges. The underlying PAM system grants the request, typically by adding the account to a group with elevated privileges. After a pre-set time (such as 15 minutes), their account is automatically removed from the group, revoking the privileges.

Some capabilities of PAM are:

- Allow users to access the privileged account without knowing the password
- Automatically change privileged account passwords periodically
- Limit the time users can use the privileged account
- Allow users to check out credentials
- Log all access of credentials

If an attacker can log on as an administrator, there's almost no limit to what he can do. Ideally, that isn't possible, but there are many different attack methods where an attacker can get an administrator password no matter how long or complex it is. PAM is the protection against these types of attacks. It reduces the opportunities for attackers to use administrative privileges. PAM systems use logging and monitoring to show when these accounts are used and what users did with them.

Remember this

Privileged access management (PAM) systems implement stringent security controls over accounts with elevated privileges such as administrator or root-level accounts. Some capabilities include allowing authorized users to access the administrator account without knowing the password, logging all elevated privileges usage, and automatically changing the administrator account password.

Require Administrators to Use Two Accounts

It's common to require administrators to have two accounts. They use one for regular day-to-day work. It has the same limited privileges as a regular end user. The other account has elevated privileges required to perform administrative work, and they use this only when performing administrative work. The benefit of this practice is that it reduces the exposure of the administrative account to an attack.

For example, when malware infects a system, it often attempts to gain additional rights and permissions using privilege escalation techniques. It may exploit a bug or flaw in an application or operating system. Or, it may simply assume the rights and permissions of the logged-on user. If an administrator logs on with an administrative account, the malware can assume these elevated privileges. In contrast, if the administrator is logged on with a regular standard user account, the malware must take additional steps to escalate its privileges.

This also reduces the risk to the administrative account for day-to-day work. Imagine Homer is an administrator, and he's called away to a crisis. He can walk away without locking his computer. If he was logged on with his administrator account, an attacker walking by can access the system and have administrative privileges. Although systems often have password-protected screen savers, these usually don't start until about 10 minutes or longer after a user walks away.

Prohibiting Shared and Generic Accounts

Account management policies often dictate that personnel should not use shared or generic accounts. Instead, each user has at least one account, which is only accessible to that user. If multiple users share a single account, you cannot implement basic authorization controls. As a reminder, four key concepts are:

- **Identification.** Users claim an identity with an identifier such as a username.
- **Authentication.** Users prove their identity using an authentication method such as a password.
- **Authorization.** Users are authorized access to resources, based on their proven identity.
- **Accounting.** Logs record activity using the users' claimed identity.

Imagine that Bart, Maggie, and Lisa all used the Guest account. If you want to give Lisa access to certain files, you would grant access to the Guest account, but Bart and Maggie would have the same access. If Bart deleted the files, logs would indicate the Guest account deleted the files, but you wouldn't know who actually deleted them. In contrast, if users have unique user accounts, you can give them access to resources individually. Additionally, logs would indicate who took an action.

Note that having a single, temporary user log on with the Guest account does support identification, authentication, authorization, and accounting. It is only when multiple users are sharing the same account that you lose these controls. Still, some organizations prohibit the use of the Guest account for any purposes.

Remember this

Requiring administrators to use two accounts, one with administrator privileges and another with regular user privileges, helps prevent privilege escalation attacks. Users should not use shared accounts.

Disablement Policies

Many organizations have a ***disablement policy*** that specifies how to manage accounts in different situations. For example, most organizations require administrators to disable user accounts as soon as possible when employees leave the organization. Additionally, it's common to disable default accounts (such as the Guest account mentioned previously) to prevent them from being used.

Disabling is preferred over deleting the account, at least initially. If administrators delete the account, they also delete any encryption and security keys associated with the account. However, these keys are retained when the account is disabled. As an example, imagine that an employee encrypted files with his account. The operating system uses cryptography keys to encrypt and decrypt these files. If administrators deleted this account, these files may remain encrypted forever unless the organization has a key escrow or recovery agent that can access the files.

Some contents of an account disablement policy include:

- **Terminated employee.** An account disablement policy specifies that accounts for ex-employees are disabled as soon as possible. This ensures a terminated employee doesn't become a disgruntled ex-employee who wreaks havoc on the network. Note that "terminated" refers to both employees who resign and employees who are fired.
- **Leave of absence.** If an employee will be absent for an extended period, the account should be disabled while the employee is away. Organizations define extended period differently, with some organizations defining it as only two weeks, whereas other organizations extend it out to as long as two months.
- **Delete account.** When the organization determines the account is no longer needed, administrators delete it. For example, the policy may direct administrators to delete accounts that have been inactive for 60 or 90 days.

Time-Based Logins

Time-based logins (sometimes referred to as time-of-day restrictions) ensure that users can only log on to computers during specific times. If a user tries to log on to a system outside the restricted time, the system denies access to the user.

As an example, imagine a company operates between 8:00 a.m. and 5:00 p.m. on a daily basis. Managers decide they don't want regular users logging on to the network except between 6:00 a.m. and 8:00 p.m., Monday through Friday. You could set time-of-day restrictions for user accounts to enforce this. If a user tries to log on outside the restricted time (such as during the weekend), the system prevents the user from logging on.

If users are working overtime on a project, the system doesn't log them off when the restricted time arrives. For example, if Maggie is working late on a Wednesday night, the system doesn't log her off at 8:00 p.m. However, the system will prevent her from creating any new network connections.

Remember this

An account disablement policy identifies what to do with accounts for employees who leave permanently or are on a leave of absence. Most policies require administrators to disable the account as soon as possible so that ex-employees cannot use the account. Disabling the account ensures that data associated with it remains available. Security keys associated with an account remain available when the account is disabled, but the security keys (and data they encrypted) are no longer accessible if it is deleted.

Time-based login restrictions prevent users from logging on or accessing network resources during specific hours.

Account Audits

An ***account audit*** looks at the rights and permissions assigned to users and helps enforce the least privilege principle. The audit identifies the privileges (rights and permissions) granted to users and compares them against what the users need. It can detect privilege creep, a common problem that violates the principle of least privilege.

Privilege creep (or permission bloat) occurs when a user is granted more and more privileges due to changing job requirements, but unneeded privileges are never removed. For example, imagine Lisa is working in the Human Resources (HR) department, so she has access to HR data. Later, she transfers to the Sales department, and administrators grant her access to sales data. However, no one removes her access to HR data even though she doesn't need it to perform her sales department job.

Organizations commonly use a role-based access control model with group-based privileges, as described later in this chapter. For example, while Lisa is working in the HR department, her account would be in one or more HR department security groups to grant her appropriate HR job privileges. When she transfers to the Sales department, administrators would add her to the appropriate Sales department groups, granting her new job privileges. An organization should also have account management controls in place to ensure that administrators remove her account from the HR department security groups. The permission auditing review verifies that these account management practices are followed.

Most organizations ensure that permission auditing reviews are performed at least once a year, and some organizations perform them more often. The goal is to do them often enough to catch potential problems and prevent security incidents. However, unless they can be automated, they become an unnecessary burden if security administrators are required to do them too often, such as daily or even once a week.

Remember this

Usage auditing records user activity in logs. A usage auditing review looks at the logs to see what users are doing and it can be used to re-create an audit trail. Permission auditing reviews help ensure that users have only the access they need and no more and can detect privilege creep issues.

Comparing Authentication Services

Several other authentication services are available that fall outside the scope of the previously described factors of authentication. A common goal they have is to ensure that unencrypted credentials are not sent across a network. In other words, they ensure that credentials are not sent in cleartext. If credentials are sent in cleartext, attackers can use tools such as a protocol analyzer to capture and view them. The following sections describe many of these services.

Single Sign-On

Single sign-on (SSO) refers to a user's ability to log on once and access multiple systems without logging on again. SSO increases security because the user only needs to remember one set of credentials and is less likely to write them down. It's also much more convenient for users to access network resources if they only have to log on one time.

As an example, consider a user who needs to access multiple servers within a network to perform normal work. Without SSO, the user needs to know one set of credentials to log on locally and an additional set of credentials for each of the servers. Many users would write these credentials down to remember them.

Alternatively, in a network with SSO capabilities, the user only needs to log on to the network once. The SSO system typically creates some type of SSO secure token used during the entire login session. Each time the user accesses a network resource, the SSO system uses this secure token for authentication. Kerberos includes SSO capabilities in networks. There are also several SSO alternatives used on the Internet.

SSO requires strong authentication to be effective. If users create weak passwords, attackers might guess them, giving them access to multiple systems. Some people debate that SSO adds in risks because if an attacker can gain the user's credentials, it provides the attacker access to multiple systems.

Kerberos

Kerberos is a network authentication mechanism used within Windows Active Directory domains and some Unix environments known as realms. It was originally developed at MIT (the Massachusetts Institute of Technology) for Unix systems and later released as a request for comments (RFC). Kerberos provides mutual authentication that can help prevent on-path attacks (also known as man-in-the-middle attacks) and uses tickets to help prevent replay attacks. Chapter 7, “Protecting Against Advanced Attacks,” covers these attacks in more depth.

Kerberos includes several requirements for it to work properly. They are:

- **A method of issuing tickets used for authentication.** The *Key Distribution Center (KDC)* uses a complex process of issuing ticket-granting tickets (TGTs) and other tickets. The KDC (or TGT server) packages user credentials within a ticket. Tickets provide authentication for users when they access resources such as files on a file server. These tickets are sometimes referred to as tokens, but they are logical tokens, not a key fob type of token discussed earlier in the “Something You Have” section.
- **Time synchronization.** Kerberos version 5 requires all systems to be synchronized and within five minutes of each other. The clock that provides the time synchronization is used to timestamp tickets, ensuring they expire correctly. This helps prevent replay attacks. In a replay attack, a third party attempts to impersonate a client after intercepting data captured in a session. However, if an attacker intercepts a ticket, the timestamp limits the amount of time an attacker can use the ticket.
- **A database of subjects or users.** In a Microsoft environment, this is Active Directory, but it could be any database of users.

When a user logs on with Kerberos, the KDC issues the user a ticket-granting ticket, which typically has a lifetime of 10 hours to be useful for a single workday. When users try to access a resource, they present the ticket-

granting ticket as authentication, and the user is issued a ticket to access the resource. However, the ticket expires if users stay logged on for an extended period, such as longer than 10 hours. This prevents them from accessing network resources. In this case, users may be prompted to provide a password to renew the ticket-granting ticket, or they might need to log off and back on to generate a new ticket-granting ticket.

Additionally, Kerberos uses symmetric-key cryptography to prevent unauthorized disclosure and to ensure confidentiality. Chapter 10 explains algorithms in more depth, but in short, symmetric-key cryptography uses a single key for both encryption and decryption of the same data.

Remember this

Kerberos is a network authentication protocol within a Microsoft Windows Active Directory domain or a Unix realm. It uses a database of objects such as Active Directory and a KDC (or TGT server) to issue timestamped tickets that expire after a certain time period.

SSO and a Federation

Some SSO systems can connect authentication mechanisms from different environments, such as different operating systems or different networks. One common method is with a federated identity management system, often integrated as a federated database. This federated database provides central authentication in a non-homogeneous environment.

As an example, imagine that the Springfield Nuclear Power Plant established a relationship with the Springfield school system, allowing the power plant employees to access school resources. It's not feasible or desirable to join these two networks into one. However, you can create a federation of the two networks. Once it's established, the power plant employees will log on using their power plant account and then access the shared school resources without logging on again.

A **federation** requires a federated identity management system that all members of the federation use. In the previous example, the members of the federation are the power plant and the school system. Members of the federation agree on a standard for federated identities and then exchange the information based on the standard. A federated identity links a user's credentials from different networks or operating systems, but the federation treats it as one identity.

SAML

Security Assertion Markup Language (SAML) is an ***Extensible Markup Language (XML)***–based data format used for SSO on web browsers. Imagine two websites hosted by two different organizations. Normally, a user would have to provide different credentials to access either website. However, if the organizations trust each other, they can use SAML as a federated identity management system. Users authenticate with one website and are not required to authenticate again when accessing the second website.

Many web-based portals use SAML for SSO. The user logs on to the portal once, and the portal then passes proof of the user's authentication to back-end systems. As long as one organization has authenticated users, they are not required to authenticate again to access other sites within the portal.

SAML defines three roles. While reading through these roles, think of Homer, who logs on at work (the nuclear power plant) and then accesses continuing education courses at the Springfield school system's website:

- **Principal.** This is typically a user, such as Homer. The user logs on once. If necessary, the principal requests an identity from the identity provider.
- **Identity provider.** An identity provider (IdP) creates, maintains, and manages identity information for principals. In the scenario, the IdP could be the nuclear power plant, the Springfield school system, or a third party.
- **Service provider.** A service provider is an entity that provides services to principals. In this example, the Springfield school system is the service provider for Homer. It hosts one or more websites accessible through a web-based portal. When Homer accesses a school system website, the service provider queries the IdP to verify that he has valid credentials before granting access.

This process sends several XML-based messages between the systems. However, it is usually transparent to the user.

SAML and Authorization

It's important to realize that the primary purpose of SSO is for the identification and authentication of users. Users claim an identity and prove that identity with credentials. SSO does not provide authorization. For example, suppose the power plant and the school system create a federation using SAML. This doesn't automatically grant everyone in the school system full access to the nuclear power plant resources. Authorization is completely separate.

However, many federation SSO systems, including SAML, include the ability to transfer authorization data between their systems. In other words, it's possible to use SAML for single sign-on authentication and for authorization.

Remember this

SAML is an XML-based standard used to exchange authentication and authorization information between different parties. SAML provides SSO for web-based applications.

OAuth

OAuth is an open standard for authorization many companies use to provide secure access to protected resources. Instead of creating a different account for each website you access, you can often use the same account you've created with Google, Facebook, PayPal, Microsoft, or Twitter. You can think of OAuth as open authorization.

As an example, imagine that the Try-N-Save Department Store decides to sell some of its products online, and management has decided to allow customers to make purchases through PayPal. Developers configure their website to exchange application programming interface (API) calls between it and PayPal servers. Now, when customers make a purchase, they log on with their PayPal account and make their purchase through PayPal. OAuth transfers data between PayPal and the Try-N-Save site so that the department store receives the money and knows what to ship to the customer. A benefit for the customers is that they don't have to create another account for Try-N-Save.

The key point is that OAuth focuses on authorization, not authentication. RFC 6749, “The OAuth 2.0 Authorization Framework,” describes it. OAuth 2.0 is not backward compatible with OAuth 1.0.

OpenID and OpenID Connection

OpenID is an authentication standard maintained by the OpenID Foundation. An OpenID provider holds the user's credentials, and websites that support OpenID prompt users to enter their OpenID. Imagine Homer created an OpenID identifier on the *myopenid.com* website as *homer.myopenid.com*. When prompted, he would enter his identifier and then click Sign in. He'll then be redirected to the provider's website (*myopenid.com* in this example). Homer enters his password to authenticate. In some cases, the OpenID provider prompts you to give the website other information, and Homer can allow or deny the release of this additional information. This page shows how the process works: <http://openidexplained.com/use>.

In my travels on the Internet, I don't see sites using OpenID these days. I'm sure some sites still use it but I don't see it. However, I often see OpenID Foundation's next iteration, ***OpenID Connection (OIDC)***. OIDC builds on OpenID for authorization and uses the OAuth 2.0 framework for authentication. Instead of an authorization token, OIDC uses a JavaScript Object Notation (JSON) Web Token (JWT), sometimes called an ID token.

As an example, imagine Homer has a Google account. He then downloads an app that requires him to log on, but the app gives him the choice of logging on with his Google account. If he selects it, the app will exchange data with Google and then indicate what Google will share with the app if Homer logs on. Once Homer logs on to Google, Google exchanges the JSON Web Token with the app, granting Homer access to the app and granting the app access to some data in Homer's account, such as his name and email address. The benefit for the app is that it doesn't have to manage the user's credentials and doesn't risk exposing them. The benefit for the user is that he doesn't have to memorize another set of credentials.

Comparing Access Control Schemes

Access control ensures that only authenticated and authorized entities can access resources. For example, it ensures that only authenticated users who have been granted appropriate permissions can access files on a server. This starts by ensuring that users are accurately identified and authenticated. Then, you grant access using one of several different schemes. The access control schemes (sometimes referred to as access control models) covered in this section are:

- Role-based access control
- Rule-based access control
- Discretionary access control (DAC)
- Mandatory access control (MAC)
- Attribute-based access control (ABAC)

Each of these access control schemes makes it easier to apply access policies to users within a network. By understanding a little more of the underlying design principles, you'll understand why some of the rules are important, and you'll be better prepared to ensure that security principles are followed.

Often, when using any of the schemes, you'll run across the following terms:

- **Subjects.** Subjects are typically users or groups that access an object. Occasionally, the subject may be a service that is using a service account to access an object.
- **Objects.** Objects are items such as files, folders, shares, and printers that subjects access. The access control helps determine how a system grants authorization to objects. Or, said another way, the access control scheme determines how a system grants users access to files and other resources.

Role-Based Access Control

Role-based access control (role-BAC) uses roles to manage rights and permissions for users. This is useful for users within a specific department who perform the same job functions. An administrator creates the roles and then assigns specific rights and permissions to the roles (instead of to the users). When an administrator adds a user to a role, the user has all the rights and permissions of that role.

Using Roles Based on Jobs and Functions

Imagine your organization has several departments, such as Accounting, Sales, and IT, and each department has a separate server hosting its files. You can create Accounting, Sales, and IT roles and assign these roles to users based on the department where they work. Next, you'd grant these roles access to the appropriate server. For example, you'd grant the Accounting role to the Accounting server, grant the Sales role to the Sales server, and so on.

Another example of the role-BAC scheme is Microsoft Project Server. The Project Server can host multiple projects managed by different project managers. It includes the following roles:

- **Administrators.** Administrators have complete access and control over everything on the server, including all of the projects managed on the server.
- **Executives.** Executives can access data from any project held on the server but do not have access to modify server settings.
- **Project Managers.** Project managers have full control over their own projects but do not control projects owned by other project managers.
- **Team Members.** Team members can typically report on work that project managers assign to them, but they have little access outside the scope of their assignments.

Microsoft Project Server includes more roles, but you can see the point with these four. Each of these roles has rights and permissions assigned to

it, and to give someone the associated privileges, you'd simply add the user's account to the role.

Documenting Roles with a Matrix

Think about the developers of Microsoft Project Server. They didn't just start creating roles. Instead, they did some planning and identified the roles they envisioned in the application. Next, they identified the privileges each of these roles required. It's common to document role-based permissions with a matrix listing all of the job titles and each role's privileges, as shown in Table 2.1.

Role	Server Privileges	Project Privileges
Administrators	All	All
Executives	None	All
Project Managers	None	All on assigned projects No access on unassigned projects
Team Members	None	Access for assigned tasks Limited views within scope of their assigned tasks No views outside the scope of their assigned tasks

Table 2.1: Role-BAC matrix for Project Server

Role-BAC is also called hierarchy-based or job-based:

- **Hierarchy-based.** In the Project Server example, you can see how top-level roles, such as the Administrators role, have significantly more permissions than lower-level roles, such as the Team Members role. Roles may mimic the hierarchy of an organization.
- **Job-, task-, or function-based.** The Project Server example also shows how the roles are centered on jobs or functions that users need to perform.

Remember this

A role-based access control scheme uses roles based on jobs and functions. A matrix is a planning document that matches the roles with the required privileges.

Establishing Access with Group-Based Privileges

Administrators commonly grant access in the role-BAC scheme using roles, and they often implement roles as groups. Windows systems refer to these as security groups. They assign rights and permissions (privileges) to groups and then add user accounts to the appropriate group. This type of group-based access control based on roles or groups simplifies user administration.

One implementation of the role-BAC scheme is the Microsoft built-in security groups and specially created security groups that administrators create on workstations, servers, and domains. The Administrators group is an example of a built-in security group. For example, the Administrators group on a local computer includes all of the rights and permissions on that computer. If you want to grant Marge full control to a computer, you could add Marge's user account to the Administrators group on that computer. Once Marge is a member of the Administrators group, she has all the group's rights and permissions.

Similarly, you can grant other users the ability to back up and restore data by adding their user accounts to the Backup Operators group. Although the built-in groups are very useful, they don't meet all the requirements in most organizations. For example, if your organization wants to separate backup and restore responsibilities, you can create one group that can only back up data and another group that can only restore data.

In Windows domains, administrators often create groups that correspond to the departments of an organization. For example, imagine that Homer, Marge, and Bart work in the Sales department and need to access data stored in a shared folder named Sales on a network server. An administrator would simplify administration with the following steps, as shown in Figure 2.4:

1. Create a Sales group and add each of the user accounts to the Sales group.
2. Add the Sales group to the Sales folder.
3. Assign appropriate permissions to the Sales group for the Sales folder.

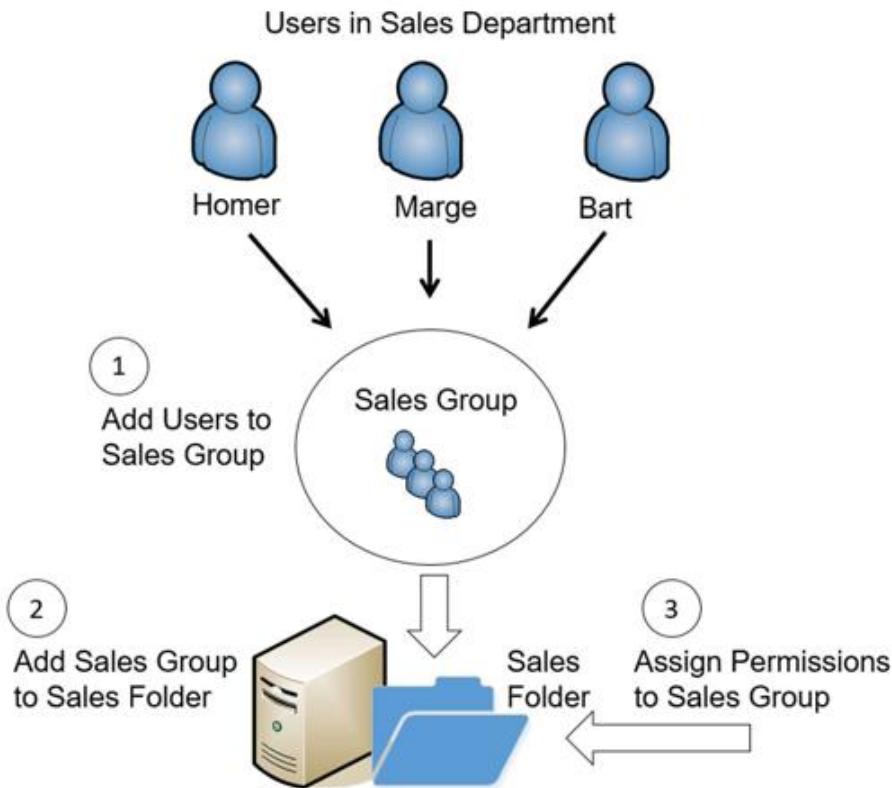


Figure 2.4: Establishing access with groups as roles

If the company adds new salespeople, the administrator creates accounts for them and places their accounts into the Sales group. These new salespeople now have access to everything assigned to this group. If any users change jobs within the company and leave the Sales department, the administrator removes them from the Sales group. This automatically prevents them from accessing any resources granted to the Sales group. This example shows how to use a group for the Sales department, but you can apply the same steps to any department or group of users.

Groups provide another security benefit. Imagine that a user is promoted out of the Sales department and now works in Marketing. If you have a Marketing group, you can place this user account into the Marketing group and remove the account from the Sales group. Removing the user from the Sales group removes all the user rights and permissions applied from that group. However, if you're not using groups and assign permissions to users directly, you probably won't remember which resources were assigned to the user as a Sales department employee.

Remember this

Group-based privileges reduce the administrative workload of access management. Administrators put user accounts into security groups and assign privileges to the groups. Users within a group automatically inherit the privileges assigned to the group.

Rule-Based Access Control

Rule-based access control (rule-BAC) uses rules. The most common example is with rules in routers or firewalls. However, more advanced implementations cause rules to trigger within applications, too.

Routers and firewalls use rules within access control lists (ACLs). These rules define the traffic that the devices allow into the network, such as allowing Hypertext Transfer Protocol (HTTP) traffic for web browsers. These rules are typically static. In other words, administrators create the rules, and the rules stay the same unless an administrator changes them again.

However, some rules are dynamic. For example, intrusion prevention systems can detect attacks and then modify rules to block traffic from attackers. In this case, the attack triggers a change in the rules.

As another example, it's possible to configure user applications with rules. For example, imagine you want to give Homer additional permissions to a database if Marge is absent. You can configure a database rule to trigger a change to these permissions when the system recognizes that Marge is absent.

Remember this

Rule-based access control is based on a set of approved instructions, such as an access control list. Some rule-BAC systems use rules that trigger in response to an event, such as modifying ACLs after detecting an attack or granting additional permissions to a user in certain situations.

Discretionary Access Control

In the ***discretionary access control (DAC)*** scheme, objects (such as files and folders) have an owner, and the owner establishes access for the objects. Many operating systems, such as Windows and most Unix-based systems, use the DAC scheme.

A common example of the DAC scheme is the New Technology File System (NTFS) used in Windows. NTFS provides security by allowing users and administrators to restrict access to files and folders with permissions. NTFS is based on the DAC scheme, and the following section explains how it uses the DAC scheme.

Filesystem Permissions

Chapter 1 covers filesystem permissions in Linux, using read, write, and execute permissions. Microsoft systems also use filesystem permissions with NTFS. The following bullets describe basic NTFS permissions:

- **Write.** Users can change the contents of a file, such as changing words in a text file. This doesn't give them the ability to delete a file, but they can delete the contents.
- **Read.** Read permission allows a user to open and view the contents of a file.
- **Read & execute.** This gives a user permission to run any executable files, including scripts.
- **Modify.** Modify allows users to view and change files, including deleting files or adding files to a folder.
- **Full control.** Users can do anything with a file and its permissions.

It's possible to assign either Allow or Deny access to any file. However, the filesystem uses a deny by default policy. If allow access is not granted, the system denies access by default. Firewalls often refer to this as implicit deny.

SIDs and DACLs

Microsoft systems identify users with security identifiers (SIDs), though you will rarely see a SID. A SID is a long string of characters that is

meaningless to most people and may look like this: S-1-5-21-3991871189-223218. Instead of the system displaying the SID, it looks up the name associated with the SID and displays the name. Similarly, Microsoft systems identify groups with a SID.

Every object (such as a file or folder) includes a discretionary access control list (DACL) that identifies who can access it in a system using the DAC scheme. The DACL is a list of Access Control Entries (ACEs). Each ACE is composed of a SID and the permission(s) granted to the SID. As an example, a folder named Study Notes might have the following permissions assigned:

- Lisa: Full Control
- Bart: Read
- Maggie: Modify

Each of these entries is an ACE, and combined, all of the entries are a DACL. You can view the DACL for a folder by using The Viewing a DACL Lab in the online exercises for this chapter.

The Owner Establishes Access

If users create a file, they are designated as the owner and have explicit control over the file. As the owner, users can modify the permissions on the object by adding user or group accounts to the DACL and assigning the desired permissions.

The DAC scheme is significantly more flexible than the MAC scheme described in the next section. MAC has predefined access privileges, and the administrator is required to make the changes. With DAC, if you want to grant another user access to a file you own, you simply make the change, and that user has access.

Remember this

The DAC scheme specifies that every object has an owner, and the owner has full, explicit control of the object. Microsoft NTFS uses the DAC scheme.

Mandatory Access Control

The ***mandatory access control (MAC)*** scheme uses labels (sometimes referred to as sensitivity labels or security labels) to determine access.

Security administrators assign labels to both subjects (users) and objects (files or folders). When the labels match, the system can grant a subject access to an object. When the labels don't match, the access scheme blocks access.

Military units make wide use of this scheme to protect data. You might have seen movies where they show a folder with a big red and black cover page labeled "Top Secret." The cover page identifies the sensitivity label for the data contained within the folder. Users with a Top Secret label (a Top Secret clearance) and a need to know can access the Top Secret folder's data.

Need to know is an important concept to understand. Just because individuals have a Top Secret clearance doesn't mean they should automatically have access to all Top Secret data. Instead, access is restricted based on a need to know.

Security-enhanced Linux (SELinux) is one of the few operating systems using the mandatory access control scheme. It was created to demonstrate how the MAC scheme can be added to an operating system. In contrast, Windows operating systems use the discretionary access control scheme.

An SELinux policy is a set of rules that override standard Linux permissions. However, even if an SELinux policy is in place, it isn't necessarily enforced. SELinux has three modes:

- Enforcing mode will enforce the SELinux policy and ignore permissions. In other words, even if the permissions allow access to a file or directory, users will be denied access unless they meet the relevant SELinux policy rules.
- Permissive mode does not enforce the SELinux policy but instead uses the permissions. However, the system logs any access that would normally be blocked. This is useful when testing a policy.
- Disabled mode does not enforce the SELinux policy and does not log anything related to the policy.

Acronyms

Don't you just love these acronyms? MD5, SHA, HMAC. There are actually three different meanings of MAC within the context of CompTIA Security+:

- Media access control (MAC) addresses are the physical addresses assigned to network interface cards (NICs).
- The mandatory access control (MAC) scheme is one of several access control schemes discussed later in this chapter.
- Message authentication code (MAC) provides integrity similar to how a hash is used.

If you're having trouble keeping them all straight, don't feel alone. The Glossary for this book spells out—and lists brief descriptions—for relevant acronyms. When taking practice test questions, I encourage you to think of the words instead of the acronyms. Knowing what it represents will make the question much easier when you see the acronym on the live test.

Labels and Lattice

The MAC scheme uses different levels of security to classify both the users and the data. These levels are defined in a lattice, which can be a complex relationship between different ordered sets of labels. These labels define the boundaries for the security levels.

Figure 2.5 shows how the MAC scheme uses a lattice to divide access into separate compartments based on a need to know. The lattice starts by defining different levels of Top Secret, Secret, Confidential, and For Official Use. Each of these labels defines specific security boundaries. Within these levels, the lattice defines specific compartments. For example, the Top Secret level includes compartments labeled Nuclear Power Plant, 007, and Happy Sumo.

Nuclear Power Plant	007	Happy Sumo	Top Secret Level
Research	Three-Eyed Fish	Legal Issues	Secret Level
Payroll	Budget	Safety Issues	Confidential Level
Training	Job Openings	Holidays	For Official Use Level

Figure 2.5: MAC scheme lattice

Imagine that Homer has a Top Secret clearance with a Nuclear Power Plant label. This gives him access to data within the Nuclear Power Plant compartment. However, he does not have access to data in the 007 or Happy Sumo compartment unless he also has those clearances (and associated labels).

Higher-level clearances include lower-level clearances. For example, because Homer has a Top Secret clearance, he can be granted access to Secret and lower-level data. Again, though, he will only be able to access data on these lower levels based on his need to know.

As another example, imagine that Lisa has a Secret level clearance. Administrators can grant her access to data on the Secret level and lower levels based on her need to know. For example, they might grant her access to the Research data by assigning the Research label to her, but not necessarily grant her access to Three-eyed Fish or Legal Issues data. However, they cannot grant her access to any data on the Top Secret level.

Remember this

The MAC scheme uses sensitivity labels for users and data. It is commonly used when access needs to be restricted based on a need to know. Sensitivity labels often reflect classification levels of data and clearances granted to individuals.

Establishing Access

An administrator is responsible for establishing access, but only someone at a higher authority can define the access for subjects and objects. Typically, a security professional identifies the specific access individuals are authorized to access. This person can also upgrade or downgrade the individuals' access when necessary. Note that the security professional does all this via paperwork and does not assign the rights and permissions on computer systems. Instead, the administrator assigns the rights and permissions based on the direction of the security professional.

Multiple approval levels are usually involved in the decision-making process to determine what a user can access. For example, in the military, an officer working in the security professional role would coordinate with higher-level government entities to upgrade or downgrade clearances. These higher-level entities approve or disapprove clearance requests.

Once an individual is formally granted access, a network administrator would be responsible for establishing access based on the clearances identified by the security professional. From the IT administrator's point of view, all the permissions and access privileges are predefined.

If someone needed different access, the administrator would forward the request to the security professional, who may approve or disapprove the request. On the other hand, the security professional may forward the request to higher entities based on established procedures. This process takes time and results in limited flexibility.

Attribute-Based Access Control

An ***attribute-based access control (ABAC)*** evaluates attributes and grants access based on the value of these attributes. Attributes can be almost any characteristic of a user, the environment, or the resource. ABAC uses policies to evaluate attributes and grant access when the system detects a match in the policy.

As a simple example, Homer is a Nuclear Safety Inspector at the Springfield Nuclear Power Plant. His user account may be defined with the following attributes: employee, inspector, and nuclear aware. A file server at the plant includes a share called Inspector, and it holds documents commonly used by nuclear safety inspectors. An ABAC policy for the share might grant access to the share for any subjects that have the attributes of employee, inspector, and nuclear aware.

Many software-defined networks (SDNs) use ABAC schemes. Instead of rules on physical routers, policies in the ABAC system control the traffic. These policies typically use plain language statements. For example, an ABAC policy rule for a company that employs researchers might be: “Allow logged-on researchers to access research sites via the main network.” Policy statements typically include four elements:

- **Subject.** This is typically a user. You can use any user property as an attribute such as employment status, group memberships, job roles, logged-on status, and more. In the example, the subject is identified as being logged on and a member of the researchers group.
- **Object.** This is the resource (such as a file, database, or application) that the user is trying to access. In the example, the object is research sites. The research sites object would include Internet access via a proxy server along with a specific list of URLs of research sites.
- **Action.** The action is what the user is attempting to do, such as reading or modifying a file, accessing specific websites, and accessing website applications. The example allows access to specific websites.

- **Environment.** The environment includes everything outside of the subject and object attributes. This is often referred to as the context of the access request. It can include the time, location, protocols, encryption, devices, and communication method. In the example, it specifies the main network as an environmental attribute.

An ABAC system has a lot of flexibility and can enforce both a DAC and a MAC scheme. There are also many similarities between the ABAC scheme and the DAC and MAC schemes. In the DAC scheme, owners have control over the access, and in an ABAC scheme, owners can create policies to grant access. The MAC scheme uses labels assigned to both subjects and objects and grants access when the labels match. The ABAC scheme uses attributes that identify both subjects and objects, and grants access when a policy identifies a match.

If you want to dig into the ABAC scheme a little more, check out NIST SP 800-162, “Guide to Attribute Based Access Control (ABAC) Definition and Considerations.”

Remember this

The ABAC scheme uses attributes defined in policies to grant access to resources. It’s commonly used in software-defined networks (SDNs).

Conditional Access

Microsoft has implemented **Conditional Access** within Azure Active Directory environments. It can be used with traditional access control schemes but adds additional capabilities to enforce organizational policies. Conditional Access uses policies, which are if-then statements.

As a simple example, imagine several shares on a server hold sensitive documents related to the nuclear power plant. In addition to protecting these shares with traditional permissions, administrators create a Conditional Access policy that requires users to log on with multifactor authentication (MFA) to access them. Homer has permission to access these shares, and when he tries to access one of them, the policy checks to see if he used MFA. If so, he's granted access, but if not, the policy blocks his access.

Conditional Access policies use signals, which are similar to attributes in an ABAC scheme. Some common signals are:

- **User or group membership.** For example, access may be allowed for users in a Nuclear Inspector group, but anyone else is blocked.
- **IP location.** Policies can block access from entire countries or regions based on their IP address. It's also possible to allow specific IP addresses or ranges.
- **Device.** Access can be allowed or blocked based on the device. For example, a policy can allow access from desktop PCs but deny access to any mobile device.

Chapter 2 Exam Topic Review

When preparing for the exam, make sure you understand these key concepts covered in this chapter.

Exploring Authentication Management

- Authentication allows entities to prove their identity by using credentials known to another entity.
- Identification occurs when a user claims or professes an identity, such as with a username, an email address, or biometrics.
- Authentication occurs when an entity provides proof of a claimed identity (such as with a password). A second entity is an authenticator, and it verifies the authentication.
- Authorization provides access to resources based on a proven identity.
- Accounting methods track user activity and record the activity in logs.
- Three factors of authentication are:
 - Something you know, such as a username and password
 - Something you have, such as a smart card or token
 - Something you are, using biometrics, such as fingerprints, vein scans, facial scans, and gait analysis
- Password vaults store and simplify the use of credentials for users. When users access websites needing credentials, the system automatically retrieves the stored credentials and submits them to the website.
- Push notifications are often used for 2FA. Users find them user-friendly and non-disruptive because they can verify their authentication by pressing a screen button.
- Account lockout policies lock out an account after a user enters an incorrect password too many times. This helps prevent brute force and dictionary attacks.

- Default passwords should be changed on any applications or devices before putting them into service.
- The false acceptance rate (FAR), or false match rate, identifies the percentage of times false acceptance occurs. The false rejection rate (FRR) identifies the percentage of times false rejections occur. The crossover error rate (CER) indicates the biometric system's quality or the system's efficacy rate. Lower CERs are better.
- HOTP and TOTP are open source standards used to create one-time-use passwords. HOTP creates a one-time-use password that does not expire until it is used, and TOTP creates a one-time password that expires after 30 seconds.
- Single-factor authentication includes one or more authentication methods in the same factor, such as a PIN and a password. Dual-factor (or two-factor) authentication uses two factors of authentication, such as a token key and a PIN. Multifactor authentication uses two or more factors and is stronger than any form of single-factor authentication.
- Authentication methods using two or more methods in the same factor are single-factor authentication. For example, a password and a PIN are both in the something you know factor, so they only provide single-factor authentication.
- Four attributes of authentication are:
 - Somewhere you are, using geolocation, a computer name, or a MAC address
 - Something you can do, such as gestures on a touch screen
 - Something you exhibit, such as an identification badge
 - Someone you know, such as someone trusting you because someone else trusts you

Managing Accounts

- Users should not share accounts, and most organizations ensure the Guest account is disabled. Shared accounts prevent

effective identification, authentication, authorization, and accounting.

- Privileged access management (PAM) implements stringent security controls over accounts with elevated privileges, such as administrator or root accounts. This includes allowing authorized users to access the administrator account without knowing the password, limiting the time users access the elevated privileges, and logging all related activity.
- Account policies often require administrators to have two accounts (an administrator account and a standard user account) to prevent privilege escalation and other attacks.
- An account disablement policy ensures that inactive accounts are disabled. Accounts for employees who either resign or are terminated should be disabled as soon as possible.
- Time-based logins (or time-based restrictions) prevent users from logging on or accessing network resources during specific hours. Location-based policies prevent users from logging on from certain locations.
- An account audit looks at the rights and permissions assigned to users and helps enforce the least privilege principle.

Comparing Authentication Services

- Single sign-on (SSO) allows users to authenticate with a single user account and access multiple resources on a network without authenticating again.
- Kerberos is a network authentication protocol using tickets issued by a KDC or TGT server. If a ticket-granting ticket expires, the user might not be able to access resources. Microsoft Active Directory domains and Unix realms use Kerberos for SSO authentication.
- SSO can be used to provide central authentication on the Internet with a federated database. A federated identity links a user's credentials from different networks or operating systems, but the federation treats it as one identity.
- SAML is an XML-based standard used to exchange authentication and authorization information between different

parties. SAML is used with web-based applications.

- OAuth is an open standard used for authentication. It allows users to log on with another account such as Google, Facebook, PayPal, Microsoft, or Twitter. It uses API calls to exchange information and a token to show that access is authorized.
- OpenID is an authentication standard maintained by the OpenID foundation.
- OpenID Connect (OIDC) builds on OpenID for authentication and uses the OAuth framework for authorization. Instead of an authorization token used by OAuth, it uses a JavaScript Object Notation (JSON) Web Token (JWT). Like OAuth, users can log on with other accounts such as one they have with Google, Facebook, PayPal, Microsoft, or Twitter.

Comparing Access Control Schemes

- The role-based access control (role-BAC) scheme uses roles to grant access by placing users into roles based on their assigned jobs, functions, or tasks. A matrix matching job titles with required privileges is useful as a planning document when using role-BAC.
- Group-based privileges are a form of role-BAC. Administrators create groups, add users to the groups, and then assign permissions to the groups. This simplifies administration because administrators do not have to assign permissions to users individually.
- The rule-based access control (rule-BAC) scheme is based on a set of approved instructions, such as ACL rules in a firewall. Some rule-BAC implementations use rules that trigger in response to an event, such as modifying ACLs after detecting an attack.
- In the discretionary access control (DAC) scheme, every object has an owner. The owner has explicit access and establishes access for any other user. Microsoft NTFS uses the DAC scheme, with every object having a discretionary access control list (DACL). The DACL identifies who has access and what access they are granted.

- Mandatory access control (MAC) uses security or sensitivity labels to identify objects (what you'll secure) and subjects (users). It is often used when access needs to be restricted based on a need to know. The administrator establishes access based on predefined security labels. These labels are often defined with a lattice to specify the upper and lower security boundaries.
- An attribute-based access control (ABAC) evaluates attributes and grants access based on these attributes' value. It is used in many software-defined networks (SDNs).

Online References

- Have you looked at the online content recently? You can view labs and additional sample questions at
[https://greatadministrator.com/sy0-601-extras.](https://greatadministrator.com/sy0-601-extras)

Chapter 2 Practice Questions

1. Your organization wants to identify biometric methods used for identification. The requirements are:

- Collect the data passively.
- Bypass a formal enrollment process.
- Avoid obvious methods that let the subject know data is being collected.

Which of the following biometric methods BEST meet these requirements? (Select TWO.)

- A. Fingerprint
- B. Retina
- C. Iris
- D. Facial
- E. Palm vein
- F. Gait analysis

2. Your organization recently updated an online application that employees use to log on when working from home. Employees enter their username and password into the application from their smartphone and the application logs their location using GPS. Which type of authentication is being used?

- A. One-factor
- B. Dual-factor
- C. Something you are
- D. Something you have

3. Management within your organization wants to add 2FA security for users working from home. Additionally, management wants to ensure that 2FA passwords expire after 30 seconds. Which of the following choices BEST meets this requirement?

- A. HOTP
- B. TOTP
- C. SMS
- D. Kerberos

4. Management within your organization has decided to implement a biometric solution for authentication into the data center. They have stated that the biometric system needs to be highly accurate. Which of the following provides the BEST indication of accuracy with a biometric system?

- A. The lowest possible FRR
- B. The highest possible FAR
- C. The lowest possible CER
- D. The highest possible CER

5. The Marvin Monroe Memorial Hospital was recently sued after removing a kidney from the wrong patient. Hospital executives want to implement a method that will reduce medical errors related to misidentifying patients. They want to ensure medical personnel can identify a patient even if the patient is unconscious. Which of the following would be the BEST solution?

- A. Gait analysis
- B. Vein scans
- C. Retina scan
- D. Voice recognition

6. Users regularly log on with a username and password. However, management wants to add a second authentication factor for any users who launch the gcga application. The method needs to be user-friendly and non-disruptive. Which of the following will BEST meet these requirements?

- A. An authentication application
- B. TPM
- C. HSM
- D. Push notifications

7. Your organization hires students during the summer for temporary help. They need access to network resources, but only during working hours. Management has stressed that it is critically important to safeguard trade secrets and other confidential information. Which of the following account management concepts would be MOST important to meet these goals?

- A. Account expiration

- B. Account lockout
- C. Time-of-day restrictions
- D. Password recovery
- E. Password history

8. You need to provide a junior administrator with appropriate credentials to rebuild a domain controller after it suffers a catastrophic failure. Of the following choices, what type of account would BEST meet this need?

- A. User account
- B. Generic account
- C. Guest account
- D. Service account

9. Lisa is reviewing an organization's account management processes. She wants to ensure that security log entries accurately report the identity of personnel taking specific actions. Which of the following steps would BEST meet this requirement?

- A. Implement generic accounts.
- B. Implement role-based privileges.
- C. Use an SSO solution.
- D. Remove all shared accounts.

10. A recent security audit discovered several apparently dormant user accounts. Although users could log on to the accounts, no one had logged on to them for more than 60 days. You later discovered that these accounts are for contractors who work approximately one week every quarter. Which of the following is the BEST response to this situation?

- A. Remove the account expiration from the accounts.
- B. Delete the accounts.
- C. Reset the accounts.
- D. Disable the accounts.

11. An administrator is implementing a network from scratch for a medical office. The owners want to have strong authentication and authorization to protect the privacy of data on all internal systems. They also want regular

employees to use only a single username and password for all network access. Which of the following is the BEST choice to meet these needs?

- A. OpenID
- B. SAML
- C. Kerberos
- D. RADIUS

12. Web developers in your organization are creating a web application that will interact with other applications running on the Internet. They want their application to receive user credentials from an app running on a trusted partner's web domain. Which of the following is the BEST choice to meet this need?

- A. SSO 2
- B. SAML 2
- C. Kerberos 2
- D. RADIUS 4

13. Artie has been working at Ziffcorp as an accountant. However, after a disagreement with his boss, he decides to leave the company and gives a two-week notice. He has a user account allowing him to access network resources. Which of the following is the MOST appropriate step to take?

- A. Ensure his account is disabled when he announces that he will be leaving the company.
- B. Immediately terminate his employment.
- C. Force him to take a mandatory vacation.
- D. Ensure his account is disabled during his exit interview.

14. You administer access control for users in your organization. Some departments have a high employee turnover, so you want to simplify account administration. Which of the following is the BEST choice?

- A. User-assigned privileges
- B. Group-based privileges
- C. Domain-assigned privileges
- D. Network-assigned privileges

15. An administrator needs to grant users access to different shares on file servers based on their job functions. Which of the following access control schemes would BEST meet this need?

- A. Discretionary access control
- B. Mandatory access control
- C. Role-based access control
- D. Rule-based access control

Chapter 2 Practice Question Answers

1. **D** and **F** are correct. It's possible to collect facial scan data and perform gait analysis without an enrollment process. You would use cameras to observe subjects from a distance and collect data passively. You need a formal enrollment process for fingerprints, retinas, irises, and palm vein methods. Retina and iris scans need to be very close to the eye and are very obvious. Palm vein methods require users to place their palm on a scanner. While it's possible to collect fingerprints passively, you still need an enrollment process.
2. **A** is correct. This is using one-factor authentication—something you know. The application uses the username for identification and the password for authentication. Note that even though the application is logging the location using Global Positioning System (GPS), there isn't any indication that it is using this information for authentication. Dual-factor authentication requires another factor of authentication such as something you are or something you have. Something you are authentication factor refers to biometric authentication methods. The something you have authentication factor refers to something you can hold, such as a smart card.
3. **B** is correct. A Time-based One-Time Password (TOTP) meets the requirement of two-factor authentication (2FA). A user logs on with regular credentials (such as a username and password), and then must enter an additional one-time password. Some smartphone apps use HOTP and display a new password every 30 seconds. An HMAC-based One-Time Password (HOTP) creates passwords that do not expire until they are used. Short message service (SMS) is sometimes used to send users a one-time use password via email or a messaging app, but these passwords typically don't expire until at least 15 minutes later. Kerberos uses tickets instead of passwords.
4. **C** is correct. A lower crossover error rate (CER) indicates a more accurate biometric system. The false acceptance rate (FAR) and the false rejection rate (FRR) vary based on the sensitivity of the biometric system

and don't indicate accuracy by themselves. A higher CER indicates a less accurate biometric system.

5. **B** is correct. A vein scan implemented with a palm scanner would be the best solution of the available choices. The patient would place their palm on the scanner for biometric identification, or if the patient is unconscious, medical personnel can place the patient's palm on the scanner. None of the other biometric methods can be easily performed on an unconscious patient. Gait analysis attempts to identify someone based on the way they walk. A retina scan scans the retina of an eye, but this will be difficult if someone is unconscious. Voice recognition identifies a person using speech recognition.

6. **D** is correct. Push notifications are user-friendly and non-disruptive. Users receive a notification on a smartphone and can often acknowledge it by simply pressing a button. An authentication application isn't as user-friendly as a push notification. It requires users to log on to the smartphone, find the app, and enter the code. A Trusted Platform Module (TPM) provides full drive encryption and would protect the data if someone accessed the laptop, but it doesn't prevent access. A hardware security module (HSM) is a removable device that can generate and store RSA keys used with servers. Neither a TPM nor an HSM is relevant in this question.

7. **C** is correct. Time-of-day restrictions should be implemented to ensure that temporary workers can only access network resources during work hours. The other answers represent good practices, but don't address the need stated in the question that "personnel need access to network resources, but only during working hours." Account expiration should be implemented if the organization knows the last workday of these workers. Account lockout will lock out an account if the wrong password is entered too many times.

Password recovery allows users to recover a forgotten password or change their password if they forgot their password. Password history remembers previously used passwords and helps prevent users from using the same password.

8. **A** is correct. A user account is the best choice of the available answers. More specifically, it would be a user account with administrative privileges (also known as a privileged account) so that the administrator can add the domain controller. A generic account (also known as a shared account) is shared between two or more users and is not recommended. A guest account is disabled by default and it is not appropriate to grant the guest account administrative privileges. A service account is an account created to be used by a service or application, not a person.

9. **D** is correct. Removing all shared accounts is the best answer of the available choices. If two employees are using the same account, and one employee maliciously deletes data in a database, it isn't possible to identify which employee deleted the data. Generic accounts are the same as shared accounts and shouldn't be used. Role-based (or group-based) privileges assign the same permissions to all members of a group, which simplifies administration. A single sign-on (SSO) solution allows a user to log on once and access multiple resources.

10. **D** is correct. The best response is to disable the accounts and then enable them when needed by the contractors. Ideally, the accounts would include an expiration date so that they would automatically expire when no longer needed, but the scenario doesn't indicate the accounts have an expiration date. Because the contractors need to access the accounts periodically, it's better to disable them rather than delete them. Reset the accounts implies you are changing the password, but this isn't needed.

11. **C** is correct. Kerberos is the best choice of the available answers. Users claim an identity with a username for identification and prove their identity with a password for authentication. Kerberos uses a ticket-granting ticket (TGT) server for authentication and incorporates the user credentials in tickets. Users only have to sign in once with Kerberos, providing single sign-on (SSO). OpenID is an open source standard used for authentication on the Internet, not internal networks. Security Assertion Markup Language (SAML) is an XML-based standard that provides SSO for web-based applications. Remote Authentication Dial-In User Service (RADIUS) is an

authentication service that provides central authentication for remote access clients.

12. **B** is correct. Security Assertion Markup Language (SAML) is a single sign-on SSO solution used for web-based applications and would meet this requirement. All SSO solutions are not used on the Internet, so SSO isn't the best answer. Kerberos is an SSO solution used on internal networks such as in Microsoft Active Directory domains and Unix realms. Remote Authentication Dial-In User Service (RADIUS) provides authentication, authorization, and accounting (AAA) services for some remote access and wireless network solutions.

13. **D** is correct. His account should be disabled (or deleted if that is the company policy) during the exit interview. It's appropriate to conduct an exit interview immediately before an employee departs. Employees often give a two-week or longer notice. If their access is revoked immediately, they won't be able to do any more work. While some companies do terminate employment when someone gives notice, from a security perspective, that doesn't address the needed action related to the user account. The purpose of a mandatory vacation is to detect fraud, but if the employee is leaving, any potential fraud will be detected when that employee leaves.

14. **B** is correct. Group-based privileges are a form of role-based access control and they simplify administration. Instead of assigning permissions to new employees individually, you can just add new employee user accounts into the appropriate groups to grant them the rights and permissions they need for the job. User-assigned privileges require you to manage privileges for each user separately, and they increase the account administration burden. Domain-assigned and network-assigned privileges are not valid administration practices.

15. **C** is correct. The role-based access control (role-BAC) scheme is the best choice for assigning access based on job functions. A discretionary access control (DAC) scheme specifies that every object has an owner and owners have full control over objects, but it isn't related to job functions. A

mandatory access control (MAC) scheme uses labels and a lattice to grant access rather than job functions. A rule-based access control (rule-BAC) scheme uses rules that trigger in response to events.

Chapter 3

Exploring Network Technologies and Tools

CompTIA Security+ objectives covered in this chapter:

2.4 Summarize authentication and authorization design concepts.

- Authentication methods (Directory services)

2.7 Explain the importance of physical security controls.

- Screened subnet (previously known as demilitarized zone)

2.8 Summarize the basics of cryptographic concepts.

- Common use cases (Supporting authentication)

3.1 Given a scenario, implement secure protocols.

- Protocols (Domain Name System Security Extension (DNSSEC), SSH, Secure Real-time Transport Protocol (SRTP), Lightweight Directory Access Protocol Over SSL (LDAPS), File Transfer Protocol, Secure (FTPS), SSH File Transfer Protocol (SFTP), Simple Network Management Protocol, version 3 (SNMPv3), Hypertext transfer protocol over SSL/TLS (HTTPS), IPsec (Authentication header (AH) / Encapsulated security payload (ESP), Tunnel/transport), Post Office Protocol (POP) / Internet Message Access Protocol (IMAP))
- Use cases (Voice and video, Time synchronization, Email and web, File transfer, Directory services, Remote access, Domain name resolution, Routing and switching, Network address allocation, Subscription services)

3.2 Given a scenario, implement host or application security solutions.

- Next-generation firewall (NGFW), Host-based firewall

3.3 Given a scenario, implement secure network designs.

- Network segmentation (Virtual local area network (VLAN), Screened subnet (previously known as demilitarized zone), East-west traffic, Extranet, Intranet, Zero trust)
- DNS, Port security (Broadcast storm prevention), Bridge Protocol Data Unit (BPDU) guard, Loop prevention, Dynamic Host Configuration Protocol (DHCP) snooping)
- Network appliances (Jump servers, Proxy servers, Forward, Reverse)
- Firewalls (Web application firewall (WAF), NGFW, Stateful, Stateless, Unified threat management (UTM), Network address translation (NAT) gateway, Content/URL filter, Open-source vs. proprietary, Hardware vs. software, Appliance vs. host-based vs. virtual)
- Access control list (ACL), Route security, Quality of service (QoS), Implications of IPv6

4.1 Given a scenario, use the appropriate tool to assess organizational security.

- Network reconnaissance and discovery (nslookup/dig, route)

4.3 Given an incident, utilize appropriate data sources to support an investigation.

- VoIP and call managers, Log files (Session Initiation Protocol (SIP) traffic)

4.4 Given an incident, apply mitigation techniques or controls to secure an environment.

- Isolation, Segmentation

**

CompTIA expects prospective CompTIA Security+ exam takers to have at least two years of networking experience. However, even with that amount of experience, there are often gaps in information technology (IT) professionals' or security professionals' knowledge. For example, you may have spent a lot of time troubleshooting connectivity but rarely manipulated access control lists (ACLs) on a router or modified firewall rules. This chapter reviews some basic networking concepts, devices, and network

topologies used within secure networks. When appropriate, it digs into these topics a little deeper with a focus on security.

Reviewing Basic Networking Concepts

Before you can tackle any of the relevant security issues on a network, you'll need a basic understanding of networking. As a reminder, CompTIA expects you to have the equivalent of two years' experience working in a security/systems administrator job role. Further, CompTIA recommends obtaining the Network+ certification before taking the Security+ exam. Although the Network+ certification isn't required, the knowledge goes a long way in helping you pass the networking portion of the CompTIA Security+ exam.

This section includes a very brief review of many of the different protocols and networking concepts that are relevant to security. If any of these concepts are completely unfamiliar to you, you might need to pick up a networking book to review them.

This section also mentions some of the common attacks used against the protocols or the protocols help protect against. The following bullets introduce some of these attacks, and Chapter 7, "Protecting Against Advanced Attacks," covers these attacks in more depth:

- **Sniffing attack.** Attackers often use a protocol analyzer to capture data sent over a network. After capturing the data, attackers can easily read it within the protocol analyzer if it was sent in cleartext. Chapter 8, "Using Risk Management Tools," covers protocol analyzers in more depth.
- **DoS and DDoS.** A denial-of-service (DoS) attack is a service attack from a single source that attempts to disrupt the services provided by another system. A distributed DoS (DDoS) attack includes multiple computers attacking a single target.
- **Poisoning attack.** Many protocols store data in cache for temporary access. Poisoning attacks attempt to corrupt the cache with different data.

Several CompTIA Security+ objectives refer to Layer 2. While they don't mention it directly, they are referring to Layer 2 of the ***Open Systems Interconnection (OSI) model***, the Data Link layer.

The Data Link layer is responsible for ensuring that data is transmitted to specific devices on the network. It formats the data into frames and adds

a header that includes media access control (MAC) addresses for the source and destination devices. The Address Resolution Protocol (ARP) resolves IP addresses to MAC addresses. Layer 2 attacks attempt to exploit vulnerabilities in MAC addressing and ARP. Appendix D, “The OSI Model,” provides a short review of the OSI model for readers that need it.

Basic Networking Protocols

Networking protocols provide the rules needed for computers to communicate with each other on a network. Some Transmission Control Protocol/Internet Protocol (TCP/IP) protocols, such as TCP and IP, provide basic connectivity. Other protocols, such as Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP), support specific traffic types. This section includes information on common protocols that you'll need to understand for the CompTIA Security+ exam.

TCP/IP isn't a single protocol but instead, it's a full suite of protocols. Obviously, there isn't room in this book to teach the details of all the TCP/IP protocols. Instead, the purpose of this section is to remind you of some of the commonly used protocols. Additionally, many of these protocols meet specific use cases, and this section describes these protocols within the context of use cases.

CompTIA has historically placed a lot of emphasis on well-known ports used by protocols. For example, the default port for HTTP is 80, and CompTIA Security+ test-takers needed to know that. The current objectives have deemphasized the importance of ports. However, you may still need to know them when implementing access control lists (ACLs) in routers and stateless firewalls and disabling unnecessary ports and services. With that in mind, I've included the well-known ports for many of the protocols in this chapter and in Appendix C, "Well-Known Ports."

The following list describes some basic networking protocols:

- **TCP. *Transmission Control Protocol (TCP)*** provides connection-oriented traffic (guaranteed delivery). TCP uses a three-way handshake, and Figure 3.1 shows the TCP handshake process. To start a TCP session, the client sends a SYN (synchronize) packet. The server responds with a SYN/ACK (synchronize/acknowledge) packet, and the client completes the third part of the handshake with an ACK packet to establish the connection.

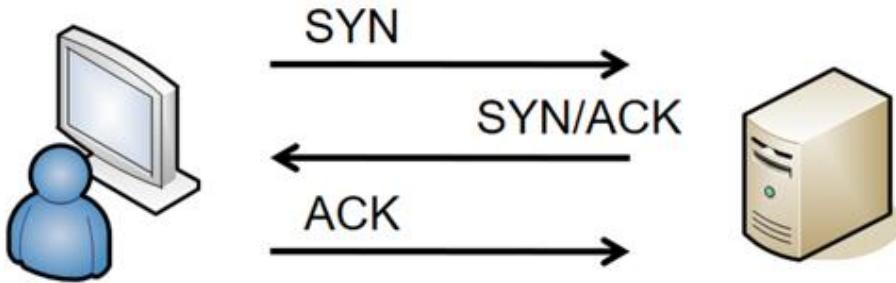


Figure 3.1: TCP handshake process

- **UDP.** *User Datagram Protocol (UDP)* provides connectionless sessions (without a three-way handshake). While TCP traffic provides guaranteed delivery, UDP makes a best effort to deliver traffic without using extra traffic to ensure delivery. ICMP traffic such as the ping command and audio/video streaming use UDP, and many network-based denial-of-service (DoS) attacks use UDP. TCP/IP traffic is either connection-oriented TCP traffic or connectionless UDP.
- **IP.** The Internet Protocol (IP) identifies hosts in a TCP/IP network and delivers traffic from one host to another using IP addresses. IPv4 uses 32-bit addresses represented in dotted decimal format, such as 192.168.1.100. IPv6 uses 128-bit addresses using hexadecimal code, such as FE80:0000:0000:0000:20D4:3FF7:003F:DE62.
- **ICMP.** *Internet Control Message Protocol (ICMP)* is used for testing basic connectivity and includes tools such as ping, pathping, and tracert. As an example, ping can check for basic connectivity between two systems, as discussed in Chapter 1, “Mastering Security Basics.” Many DoS attacks use ICMP. Because of how often ICMP is used in attacks, it has become common to block ICMP at firewalls and routers, which disables a ping response. Blocking ICMP prevents attackers from discovering devices in a network. For example, a scan can send a ping to every IP address in a subnet. The devices that reply verify that they are on and have an IP address.
- **ARP.** *Address Resolution Protocol (ARP)* resolves IPv4 addresses to media access control (MAC) addresses. MACs are also called physical addresses or hardware addresses. TCP/IP uses the IP

address to get a packet to a destination network. It then uses the MAC address to get it to the correct host. In other words, ARP is required once the packet reaches the destination subnet. ARP poisoning attacks (discussed in Chapter 7) use ARP packets to give clients false hardware address updates, and attackers use them to redirect or interrupt network traffic.

Implementing Protocols for Use Cases

Networks don't automatically support all the available protocols. Instead, IT professionals identify a need based on an organizational goal and enable the best protocol to meet that need. Chapter 1 discusses use cases. As a reminder, a use case typically describes an organizational goal. Many protocols mentioned in the CompTIA Security+ objectives support specific use cases and are discussed in this section.

Voice and Video Use Case

It's common for an organization to transport voice and video over a network, and some protocols work better with voice and video than others. As mentioned previously, UDP is commonly used instead of TCP as the underlying protocol with voice and video streaming.

The ***Real-time Transport Protocol (RTP)*** delivers audio and video over IP networks. This includes Voice over Internet Protocol (VoIP) communications, streaming media, video teleconferencing applications, and devices using web-based push-to-talk features. However, organizations often want to secure these transmissions. The ***Secure Real-time Transport Protocol (SRTP)*** provides encryption, message authentication, and integrity for RTP.

SRTP helps protect the confidentiality of data from these attacks while also ensuring the data transmissions' integrity. This protects against replay attacks. In a replay attack, an attacker captures data sent between two entities, modifies it, and then attempts to impersonate one of the parties by replaying the data. SRTP can be used for both unicast transmissions (such as one person calling another) and multicast transmissions where one person sends traffic to multiple recipients.

The ***Session Initiation Protocol (SIP)*** is used to initiate, maintain, and terminate voice, video, and messaging sessions. SIP uses request and response messages when establishing a session. These messages are text, so it's easy to read them if they are captured. After SIP establishes the session, RTP or SRTP transports the audio or video.

SIP messages don't contain any data, but they do contain metadata about sessions. This includes information on the equipment used, the

software used on the equipment, and the private IP. Many VoIP systems support SIP logging and can record these SIP messages. These logs may be useful in detecting SIP-based attacks. They can also be used in forensic investigations when trying to determine who is making certain calls and who they are calling.

Chapter 11, “Implementing Policies to Mitigate Risks,” covers incident response and forensics topics. In some cases, both VoIP log files and SIP log files are useful in an investigation. VoIP logs show timestamps, caller phone numbers, recipient phone numbers, extensions (if used), and missed calls. Many third-party VoIP call manager applications support call recording. SIP log files show timestamps, sender IP addresses, and recipient IP addresses, and some third-party applications can also capture SIP messages.

File Transfer Use Case

Data-in-transit is any traffic sent over a network. When data is sent in cleartext, attackers can use a protocol analyzer to capture and read it. You can protect the confidentiality of Personally Identifiable Information (PII) and any other sensitive data-in-transit by encrypting it. Note that you can also encrypt data-at-rest, which is data stored on any type of medium. Chapter 10, “Understanding Cryptography and PKI,” covers several specific encryption algorithms in more depth.

Some common use cases related to transferring files are *transmit data over the network, ensure confidentiality when transmitting data over a network, and ensure administrators connect to servers using secure connections*. The following list identifies several protocols used to transfer data over a network:

- **FTP. File Transfer Protocol (FTP)** uploads and downloads large files to and from an FTP server. By default, FTP transmits data in cleartext, making it easy for an attacker to capture and read FTP data with a protocol analyzer. FTP active mode uses TCP port 21 for control signals and TCP port 20 for data. FTP passive mode (also known as PASV) uses TCP port 21 for control signals, but it uses a random TCP port for data. If FTP traffic is going through a firewall, this random port is often blocked, so it is best to disable PASV in FTP clients.

- **TFTP.** *Trivial File Transfer Protocol (TFTP)* uses UDP port 69 and is used to transfer smaller amounts of data, such as when communicating with network devices. Many attacks have used TFTP, but it is not an essential protocol on most networks. Because of this, administrators commonly disable it.

The following list identifies several encryption protocols used to encrypt data-in-transit. They can be used for various use cases related to secure file transfer:

- **SSH.** *Secure Shell (SSH)* encrypts traffic in transit and can be used to encrypt other protocols such as FTP. Secure Copy (SCP) is based on SSH and is used to copy encrypted files over a network. SSH can also encrypt TCP Wrappers, a type of access control list used on Linux systems to filter traffic. When SSH encrypts traffic, it uses TCP port 22.
- **SSL.** The *Secure Sockets Layer (SSL)* protocol was the primary method used to secure HTTP traffic as Hypertext Transfer Protocol Secure (HTTPS). SSL can also encrypt other types of traffic, such as SMTP and Lightweight Directory Access Protocol (LDAP). However, it has been compromised and is not recommended for use.
- **TLS.** The *Transport Layer Security (TLS)* protocol is the designated replacement for SSL and should be used instead of SSL for browsers using HTTPS. Additionally, many protocols that support TLS use STARTTLS. STARTTLS looks like an acronym, but it isn't. Instead, it is a command used to upgrade an unencrypted connection to an encrypted connection on the same port.
- **IPsec.** *Internet Protocol security (IPsec)* is used to encrypt IP traffic. It is native to IPv6 but also works with IPv4. IPsec encapsulates and encrypts IP packet payloads and uses Tunnel mode to protect virtual private network (VPN) traffic. IPsec includes two main components: Authentication Header (AH) identified by protocol ID number 51 and Encapsulating Security Payload (ESP) identified by protocol ID number 50. It uses the Internet Key Exchange (IKE) over UDP port 500 to create a security association for the VPN. Chapter 4, “Securing Your Network,” covers IPsec in more depth.

- **SFTP.** *Secure File Transfer Protocol (SFTP)* is a secure implementation of FTP. It is an extension of Secure Shell (SSH) using SSH to transmit the files in an encrypted format. SFTP transmits data using TCP port 22.
- **FTPS.** *File Transfer Protocol Secure (FTPS)* is an extension of FTP and uses TLS to encrypt FTP traffic. Some implementations of FTPS use TCP ports 989 and 990. However, TLS can also encrypt the traffic over the ports used by FTP (20 and 21). Notice that the difference between SFTP and FTPS is that SFTP uses SSH and FTPS uses TLS.

Remember this

Secure Shell (SSH) encrypts traffic over TCP port 22 and is used to transfer encrypted files over a network. Transport Layer Security (TLS) is a replacement for SSL and is used to encrypt many different protocols, including browser-based connections using HTTPS. Secure FTP (SFTP) uses SSH to encrypt traffic. FTP Secure (FTPS) uses TLS to encrypt traffic.

SSL Versus TLS

SSL has been compromised and is not recommended for use. In September 2014, a team at Google discovered a serious vulnerability with SSL that they nicknamed the POODLE attack. POODLE is short for Padding Oracle on Downgraded Legacy Encryption. The SSL protocol is not maintained or patched, so this vulnerability remains.

This is one of the reasons that the U.S. government and many other organizations prohibit the use of SSL to protect any sensitive data. For example, the *National Institute of Standards and Technology (NIST)* Special Publication (SP) 800-52 rev 2 “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations” specifically states that federal agencies should not use SSL.

TLS is the recommended replacement. While TLS can be used in almost any implementation that previously used SSL, the two aren’t the same protocol. Still, you will often see both SSL and TLS mentioned as if they are the same. Even the CompTIA objectives for the Security+ exam sometimes use “SSL/TLS” as if they are the same protocol.

The reason seems to be that people understand SSL. By lumping the topics together as SSL/TLS, many people understand the general purpose. From a generic perspective, using the term SSL/TLS helps people understand the similarities. However, it's important to realize that SSL is compromised, and TLS should be used instead.

Email and Web Use Cases

Some common use cases related to email are *send and receive email*, *send and receive secure email*, and *manage email folders*. For the web, common use cases for internal employees are to *provide access to the Internet* and *provide secure access to the Internet*. Many organizations host web servers, and common use cases for these web servers are to provide access to web servers by external clients.

Many of these protocols support the use of STARTTLS. Instead of using one port to transmit data in cleartext and a second port to transmit data in ciphertext, the STARTTLS command allows the protocol to use the same port for both. Some common protocols used for email and the web include:

- **SMTP.** *Simple Mail Transfer Protocol (SMTP)* transfers email between clients and SMTP servers. SMTP uses TCP port 25 for unencrypted email and port 587 for email encrypted with TLS. SMTP can also use STARTTLS to initialize a secure connection. SMTP previously used port 465 for emails encrypted with SSL, but SSL is deprecated, and the Internet Assigned Numbers Authority (IANA) reassigned port 465.
- **POP3 and Secure POP.** *Post Office Protocol v3 (POP3)* transfers emails from servers down to clients. POP3 uses TCP port 110 for unencrypted connections and TCP port 995 for encrypted connections.
- **IMAP4 and Secure IMAP.** *Internet Message Access Protocol version 4 (IMAP4)* is used to store email on an email server, and it allows users to organize and manage email in folders on the server. As an example, Google Mail uses IMAP4. IMAP4 uses TCP port 143 for unencrypted connections and TCP port 993 for encrypted connections.

- **HTTP.** *Hypertext Transfer Protocol (HTTP)* transmits web traffic on the Internet and in intranets. Web servers use HTTP to transmit webpages to clients' web browsers, and Hypertext Markup Language (HTML) is the common language used to display webpages. HTTP uses TCP port 80.
- **HTTPS.** HTTP over SSL/TLS (HTTPS) encrypts web traffic to ensure it is secure while in transit. While CompTIA lists this as HTTP over SSL/TLS, SSL is no longer used to encrypt web sessions. The majority of Internet websites now use HTTPS instead of HTTP. Additionally, when a website isn't using HTTPS, many web browsers display "Not secure" next to the Uniform Resource Locator (URL). HTTPS uses TCP port 443.

Remember this

SMTP, POP3, and IMAP4 are primary email protocols. Well-known ports for encrypted and unencrypted traffic (respectively) are: SMTP uses ports 25 and 587, POP3 uses 110 and 995, IMAP4 uses 143 and 993. HTTP and HTTPS use ports 80 and 443, respectively.

Directory Services and LDAPS

Network operating systems commonly use a directory service to streamline management and implement secure authentication. A common directory service use case is to *provide secure access to the network*. As an example, many organizations use Microsoft Active Directory Domain Services (AD DS). AD DS is a database of objects that provides a central access point to manage users, computers, and other directory objects.

Chapter 2, "Understanding Identity and Access Management," covers Kerberos, which helps support this use case. Kerberos is the authentication protocol used in Windows domains and some Unix environments. It uses a Key Distribution Center (KDC) to issue timestamped tickets and uses UDP port 88.

Lightweight Directory Access Protocol (LDAP) specifies the formats and methods used to query directories, such as Microsoft AD DS. LDAP is an extension of the X.500 standard that Novell and early Microsoft Exchange Server versions used extensively. LDAP uses TCP port 389. **LDAP Secure (LDAPS)** encrypts data with TLS using TCP port 636.

Windows domains use Active Directory, which is based on LDAP. Queries to Active Directory use the LDAP format. Similarly, Unix realms use LDAP to identify objects. LDAP Secure (LDAPS) uses encryption to protect LDAP transmissions. When a client connects with a server using LDAPS, the two systems establish a Transport Layer Security (TLS) session, and TLS encrypts all data sent between the two systems.

Remember this

Directory services, such as Microsoft Active Directory Domain Services (AD DS), provide authentication services for a network. AD DS uses LDAP, encrypted with TLS when querying the directory.

Remote Access Use Case

There are many situations where personnel need to access systems from remote locations. Some common use cases are *remotely administer systems* and *remotely access desktops*. For example, imagine a server room hosts hundreds of servers, including domain controllers for a Microsoft domain. If administrators need to create a user account or implement a change in a Group Policy Object (GPO), they would rarely go to the server room. Instead, they access the server remotely and make the change from their desk computer.

Years ago, administrators often used Telnet when remotely administering systems. However, Telnet sends traffic over the network in cleartext, and it isn't recommended for use. Today, administrators commonly use SSH (discussed in the "File Transfer Use Case" section) instead of Telnet.

Administrators and clients often use ***Remote Desktop Protocol (RDP)*** to connect to other systems from remote locations. Microsoft uses RDP in different solutions such as Remote Desktop Services and Remote Assistance. RDP uses either port TCP 3389 or UDP 3389, though TCP port 3389 is more common. A common reason users cannot connect to systems with RDP is that port 3389 is blocked on a host-based or network firewall. Another method of supporting remote access use cases is with a virtual private network (VPN). Chapter 4 discusses VPNs in more depth.

Remember this

Administrators connect to servers remotely using protocols such as Secure Shell (SSH) and the Remote Desktop Protocol (RDP). In some cases, administrators use virtual private networks to connect to remote systems.

OpenSSH

OpenSSH is a suite of tools that simplify the use of SSH to connect to remote servers securely. It also supports the use of SCP and SFTP to transfer files securely. While OpenSSH is open source, many commercial products have integrated it into their applications. It was originally developed for Linux-based systems, but Windows systems have supported OpenSSH since 2015.

Imagine Maggie wants to connect to a server in the network named gcga from a Linux system. She could use the following command:

ssh gcga

This initiates an SSH connection to the remote server using the default SSH port of 22 and Maggie's username on the client. It's also possible to initiate the connection with an account on the remote system. For example, the following command initiates an SSH connection using the root account of the remote system.

ssh root@gcga

The remote server will prompt her to enter a password at this time. However, using a strong, complex password is essential, and it can get old entering these passwords each time. Instead, OpenSSH supports a use case of *supporting authentication* using a passwordless SSH login. You can use OpenSSH to create a public and private key pair. Maggie keeps the private key on her system and copies the public key to the remote server. Later, when she connects to the remote server, it prompts her system to authenticate with the private key.

The following OpenSSH command (ssh-keygen), entered at the client (Maggie's computer), will create the key pair:

ssh-keygen -t rsa

This creates a matched pair of a public and a private key similar to private/public key pairs used with certificates (described in Chapter 10). The keys are in two separate files. The file holding the public key is shared, but the private key file needs to stay private. The names of the two files are:

- **id_rsa.pub**. This is the public key. It is copied to the remote server.
- **id_rsa**. This is the private key. It is stored on the client and must stay private.

The last step is to copy the public key to the remote server with the OpenSSH command `ssh-copy-id`.

ssh-copy-id gega

The command knows the public key file's default location and where to copy it to on the remote server. Now, when Maggie connects (using `ssh root@gcga`), ssh will automatically use the key pair to provide strong authentication without requiring her to enter the password.

Remember this

OpenSSH is a suite of tools that simplify the use of SSH to connect to remote servers securely. The `ssh-keygen` command creates a public/private key pair, and the `ssh-copy-id` command copies the public key to a remote server. The private key should always stay private.

Time Synchronization Use Case

There are many instances when systems need to be using the same time (or at least a reasonably close time). A common use case is to *ensure systems have the accurate time*. As an example, Kerberos requires all systems to be synchronized and be within five minutes of each other.

Within a Microsoft domain, one domain controller periodically uses the Windows Time service to locate a reliable Internet server running the **Network Time Protocol (NTP)**. NTP is the most commonly used protocol for time synchronization, allowing systems to synchronize their time to within tens of milliseconds. Other domain controllers within the network periodically synchronize their time with the first domain controller. Last, all computers in the domain synchronize their time with one of these domain controllers. This process ensures all the computers have the accurate time.

The Simple NTP (SNTP) protocol can also be used for time synchronization. However, NTP uses complex algorithms and queries multiple time servers to identify the most accurate time. SNTP does not use these algorithms, so it might not be as accurate as NTP.

Network Address Allocation Use Case

Network address allocation refers to allocating IP addresses to hosts within your network. You can do so manually, but most networks use ***Dynamic Host Configuration Protocol (DHCP)*** to dynamically assign IP addresses to hosts. DHCP also assigns other TCP/IP information, such as subnet masks, default gateways, DNS server addresses, and much more. The following sections provide a review of some basic networking concepts.

IPv4

IPv4 uses 32-bit IP addresses expressed in dotted decimal format. For example, the IPv4 IP address of 192.168.1.5 is four decimals separated by periods or dots. You can also express the address in binary form with 32 bits.

All Internet IP addresses are public IP addresses, and internal networks use private IP addresses. Public IP addresses are tightly controlled. You can't just use any public IP address.

Instead, you must either purchase or rent it. Internet Service Providers (ISPs) purchase entire ranges of IP addresses and issue them to customers. If you access the Internet from home, you are very likely receiving a public IP address from an ISP.

Routers on the Internet include rules to drop any traffic that is coming from or going to a private IP address, so you cannot allocate private IP addresses on the Internet. RFC 1918 specifies the following private address ranges:

- **10.x.y.z.** 10.0.0.0 through 10.255.255.255
- **172.16.y.z–172.31.y.z.** 172.16.0.0 through 172.31.255.255
- **192.168.y.z.** 192.168.0.0 through 192.168.255.255

These are the only three IPv4 address ranges that you should allocate within a private network.

IPv6

Although the number of IP addresses at first seemed inexhaustible, the Internet Assigned Numbers Authority (IANA) assigned the last block of IPv4 addresses in February 2011. The Internet Engineering Task Force

(IETF) has since created IPv6, which provides a significantly larger address space than IPv4.

IPv6 uses 128-bit IP addresses expressed in hexadecimal format. For example, the IPv6 IP address of fe80:0000:0000:0000:02d4:3ff7:003f:de62 includes eight groups of four hexadecimal characters, separated by colons. Each hexadecimal character is composed of 4 bits.

Instead of private IP addresses, IPv6 uses unique local addresses. They are only allocated within private networks and not assigned to systems on the Internet. Unique local addresses start with the prefix of fc00.

DHCP Snooping

DHCP snooping sounds malicious, but it's actually a preventive measure. The primary purpose is to prevent unauthorized DHCP servers (often called rogue DHCP servers) from operating on a network. You enable it on Layer 2 switch ports.

DHCP clients and servers normally send four packets back and forth:

- **DHCP Discover.** A DHCP client broadcasts a message asking a DHCP server for a lease.
- **DHCP Offer.** A DHCP server answers, offering a lease. This includes an IP address, a subnet mask, a default gateway, and more, depending on the DHCP server configuration.
- **DHCP Request.** The DHCP client responds by requesting the offered lease.
- **DHCP Acknowledge.** The DHCP allocates the offered IP address to the DHCP client, and sends back an acknowledge packet. The DHCP server will not offer the same IP address to other clients after sending the acknowledge packet.

Normally, a switch will send all broadcast traffic it receives to all ports. However, when DHCP snooping is enabled, the switch will only send DHCP broadcast traffic (the DHCP discover message) to trusted ports.

Imagine an authorized DHCP server is connected to port 1 of a switch. Administrators configure the switch by first enabling DHCP snooping on the switch and then identifying the port connected to an authorized DHCP server, port 1 in this example. Later, Bart connects a wireless router he brought from home into a wall connection that connects into port 9 of a switch. His wireless router includes DHCP, so it will respond to all DHCP

Discover messages. However, the switch will not allow DHCP server messages coming from any port other than port 1.

Domain Name Resolution Use Case

The primary purpose of **Domain Name System (DNS)** is for domain name resolution. DNS resolves hostnames to IP addresses. Systems are constantly querying DNS, though it is usually transparent to users. Imagine that you want to visit <https://greatadministrator.com/>. You enter the URL into your web browser or click a link on a page, and your system queries a DNS server for the site's IP address. Figure 3.2 shows what is occurring between your system and DNS.

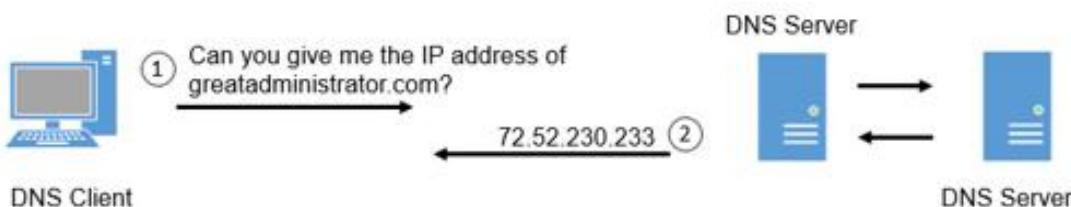


Figure 3.2: A basic DNS query

Sometimes, the DNS server you query knows the answer and just gives the response. Other times, it queries one or more other DNS servers to get the answer. When the DNS server queries other DNS servers, it puts the answer in its cache so that it doesn't have to do the same query again. Similarly, when clients receive answers from DNS servers, they store the answer in their cache so that they don't have to repeat the query.

DNS servers host data in zones, which you can think of as databases. Zones include multiple records, such as the following:

- **A.** Also called a host record. This record holds the hostname and IPv4 address and is the most commonly used record in a DNS server. A DNS client queries DNS with the name using a forward lookup request, and DNS responds with the IPv4 address from this record.
- **AAAA.** This record holds the hostname and IPv6 address. It's similar to an A record except that it is for IPv6.
- **PTR.** Also called a pointer record. It is the opposite of an A record. Instead of a DNS client querying DNS with the name, the DNS client queries DNS with the IP address. When configured to do so,

the DNS server responds with the name. PTR records are optional, so these reverse lookups do not always work.

- **MX.** Also called mail exchange or mail exchanger. An MX record identifies a mail server used for email. The MX record is linked to the A record or AAAA record of a mail server. When there is more than one mail server, the one with the lowest preference number in the MX record is the primary mail server.
- **CNAME.** A canonical name, or alias, allows a single system to have multiple names associated with a single IP address. For example, a server named Server1 in the domain *getcertifiedgetahead.com* might have an alias of FileServer1 in the same domain.
- **SOA.** The start of authority (SOA) record includes information about the DNS zone and some of its settings. For example, it includes the TTL (Time to Live) settings for DNS records. DNS clients use the TTL setting to determine how long to cache DNS results. TTL times are in seconds, and lower times cause clients to renew the records more often.

Most DNS servers on the Internet run Berkeley Internet Name Domain (BIND) software and run on Unix or Linux servers. Internal networks can use BIND, but in Microsoft networks, DNS servers commonly use the Microsoft DNS software.

Occasionally, DNS servers share information with each other in a process known as a zone transfer. In most cases, a zone transfer only includes a small number of updated records. However, some transfers include all the records in the zone. DNS servers use TCP port 53 for zone transfers. In contrast, name resolution queries use UDP port 53.

DNSSEC

One risk with DNS is **DNS poisoning**, also known as DNS cache poisoning. When successful, attackers modify the DNS cache with a bogus IP address. For example, imagine an attacker wants to send users to a malicious website each time they want to go to *msn.com*. One way is to modify the A or AAAA record in the DNS cache for *msn.com*. Instead of sending users to the IP address used by *msn.com*, it will send users to the malicious website's IP address.

One of the primary methods of preventing DNS cache poisoning is with ***Domain Name System Security Extensions (DNSSEC)***. DNSSEC is a suite of extensions to DNS that provides validation for DNS responses. It adds a Resource Record Signature (RRSIG), commonly referred to as a digital signature, to each record. The RRSIG provides data integrity and authentication for DNS replies. If a DNS server receives a DNSSEC-enabled response with digitally signed records, the DNS server knows that the response is valid.

Remember this

DNS zones include records such as A records for IPv4 addresses and AAAA records for IPv6 addresses. MX records identify mail servers and the MX record with the lowest preference is the primary mail server. DNS uses TCP port 53 for zone transfers and UDP port 53 for DNS client queries. DNSSEC adds a Resource Record Signature (RRSIG), which provides data integrity and authentication and helps prevent DNS poisoning attacks.

Nslookup and dig

Technicians use the ***nslookup*** command (short for name server lookup) to troubleshoot problems related to DNS. For example, you can use nslookup to verify that a DNS server can resolve specific hostnames or fully qualified domain names (FQDNs) to IP addresses. A fully qualified domain name includes the hostname and the domain name.

The ***dig*** command-line tool has replaced nslookup on Linux systems. It is sometimes referred to as domain information groper. You can use dig to query DNS servers to verify that the DNS server is reachable and verify that a DNS server can resolve hostnames to IP addresses. For example, these tools can verify that a DNS server has a host record that maps a hostname to an IP address for a web server (or any host). Just like nslookup, dig verifies DNS functionality by querying DNS, verifying a record exists, and verifying that the DNS server responds.

You can also use these tools to query specific records. As an example, you can query the domain for MX records to identify mail servers for a domain. The following nslookup query will identify mail servers for the *gcpagpremium.com* domain.

nslookup -querytype=mx gcgapremium.com

The following lines show a partial output:

gcgapremium.com MX preference = 10, mail exchanger =
mx1.emailsrvr.com

gcgapremium.com MX preference = 50, mail exchanger =
mx2.emailsrvr.com

The lowest preference number (10 in the example for mx1) identifies the primary server. The backup server is mx2, and it has a higher preference number (50 in the example).

Some versions of both commands support the @ symbol to identify a specific DNS server you want to query. This is useful if you want to pull all the records from a DNS zone. When doing this, you would use the *any* switch (indicating all records) or the *axfr* switch (short for all transfer). However, most DNS servers will block these queries.

Remember this

Nslookup and dig are two command-line tools used to test DNS. Microsoft systems include nslookup and Linux systems include dig. They can be used to query specific records such as mail servers. When a system has multiple mail servers, the lowest number preference identifies the primary mail server.

Subscription Services Use Case

Subscription services refer to a subscription-based business model. For example, instead of selling software applications to users, many vendors have moved to a subscription model where users pay over time.

For example, years ago, it was common for people to purchase Microsoft Office to access applications such as Microsoft Word, Microsoft Excel, Microsoft Outlook, and others. Today, organizations often pay monthly or annually for access to Office 365. This gives them the most current version of Microsoft Office products, along with additional features such as cloud storage.

The protocols used for subscription services use cases vary widely depending on the actual service. However, it's common for these to use HTTPS connections for security. Database servers maintain databases of customers, along with the products they're renting. The connections

between web servers and database servers should be secure and might use HTTPS or TLS. When the subscription is nearing an end, systems send automated emails to customers using SMTP.

Quality of Service

Quality of Service (QoS) refers to the technologies running on a network that measure and control different traffic types. It allows administrators to prioritize certain types of traffic over other types of traffic.

As an example, imagine a network isn't using QoS technologies, and some employees are streaming a high volume of video over the network. Unfortunately, these video streams are consuming so much bandwidth that other traffic suffers. Some employees using Voice over IP (VoIP) phones may find that their phones are unusable because they are experiencing a high volume of packet loss. By implementing QoS solutions, administrators can prioritize VoIP traffic and lower the priority of streaming video.

This is just one example. The key is that QoS technologies allow administrators to set the priority of any traffic.

Understanding Basic Network Devices

Networks connect computing devices together so that users can share resources, such as data, printers, and other devices. Any device with an IP address is a host, but you'll often see them referred to as clients or nodes.

A common use case for a switch is to *connect hosts together within a network*. A common use case for a router is to *connect multiple networks together* to create larger and larger networks.

When discussing the different network devices, it's important to remember the primary methods IPv4 uses when addressing TCP/IP traffic:

- **Unicast.** One-to-one traffic. One host sends traffic to another host using a destination IP address. The host with the destination IP address will process the packet. Other hosts on the same network may see the packet, but they will not process it because it isn't addressed to them.
- **Broadcast.** One-to-all traffic. One host sends traffic to all other hosts on the subnet, using a broadcast address such as 255.255.255.255. Every host that receives broadcast traffic will process it. Switches pass broadcast traffic between their ports, but routers do not pass broadcast traffic.

Switches

A **switch** can learn which computers are attached to each of its physical ports. It then uses this knowledge to create internal switched connections when two computers communicate with each other.

Consider Figure 3.3. When the switch turns on, it starts out without any knowledge other than knowing it has four physical ports. Imagine that the first traffic is the beginning of a TCP/IP conversation between Lisa's computer and Homer's computer.

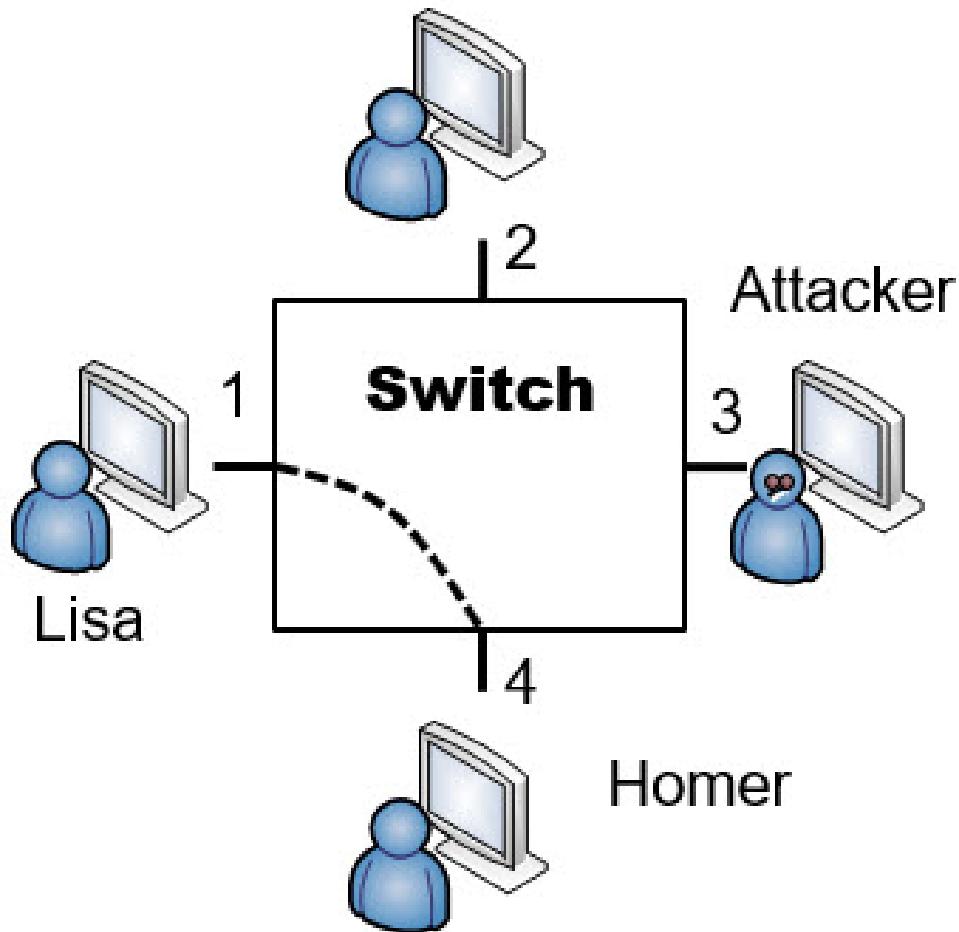


Figure 3.3: Switch

When Lisa's computer sends the first packet, it includes the MAC address of the destination computer. However, because the switch doesn't know which port Homer's computer is connected to, it forwards this first packet to all the ports on the switch.

Included in that first packet is the MAC address of Lisa's computer. The switch logs this information into an internal table. It then directs any future traffic addressed to Lisa's MAC address to port 1, and port 1 only.

When Homer's computer receives the packet, it responds. Embedded in this return packet is the MAC address of Homer's computer. The switch captures Homer's MAC address and logs it with port 4 in the internal table. From here on, any unicast traffic between Lisa's and Homer's computers is internally switched between only ports 1 and 4. Switches will internally switch unicast traffic. However, they pass broadcast traffic to all ports.

Security Benefit of a Switch

Most of the previous discussion is basic networking, but what you really need to know is why it's relevant in security. If an attacker installed a protocol analyzer on a computer attached to another port (such as port 3 in Figure 3.3), the protocol analyzer would not capture unicast traffic going through the switch to other ports. If Lisa and Homer are exchanging data on ports 1 and 4, none of the traffic reaches port 3. The protocol analyzer can't capture traffic that doesn't reach the port.

In contrast, if the computers were connected with a simple hub, the attacker could capture it because unicast traffic goes to all ports on a hub. This is the main security reason why organizations replace hubs with switches. The switch reduces the risk of an attacker capturing data with a protocol analyzer. Of course, switches also increase the efficiency of a network.

Port Security

Port security limits the computers that can connect to physical ports on a switch. At the most basic level, administrators disable unused ports. For example, individual RJ-45 wall jacks in an office lead to specific physical ports on a switch. If the wall jack is not in use, administrators can disable the switch port. This prevents someone from plugging in a laptop or other computer into the wall jack and connecting to the network.

MAC filtering is another example of port security. In a simple implementation, the switch remembers the first one or two MAC addresses that connect to a port. It then blocks access to systems using any other MAC addresses. You can also manually configure each port to accept traffic

only from a specific MAC address. This limits each port's connectivity to a specific device using this MAC address. This can be very labor-intensive, but it provides a higher level of security.

Remember this

Port security includes disabling unused ports and limiting the number of MAC addresses per port. A more advanced implementation is to restrict each physical port to only a single specific MAC address.

Broadcast Storm and Loop Prevention

In some situations, a network can develop a switching loop or bridge loop problem. This floods a network with traffic and can effectively disable a switch. For example, if a user connects two ports of a switch together with a cable, it creates a switching loop where the switch continuously sends and resends unicast transmissions through the switch. In addition to disabling the switch, it also degrades the performance of the overall network.

This is trivial for many network administrators because most current switches have ***Spanning Tree Protocol (STP)*** or the newer ***Rapid STP (RSTP)*** installed and enabled. They provide both ***broadcast storm prevention*** and ***loop prevention*** for switches. However, if these protocols are disabled, the switch is susceptible to loop problems. The simple solution is to ensure that switches include loop protection such as STP or RSTP.

Spanning Tree Protocol also protects the network against potential attackers. For example, imagine an attacker visits a conference room and has access to RJ-45 wall jacks. If loop protection isn't enabled, he can connect two jacks together with a cable, slowing network performance down to a crawl.

Remember this

Broadcast storm and loop prevention such as STP or RSTP is necessary to protect against switching loop problems, such as those caused when two ports of a switch are connected together.

Bridge Protocol Data Unit Guard

STP sends ***Bridge Protocol Data Unit (BPDU)*** messages in a network to detect loops. When the loops are detected, STP shuts down or blocks

traffic from switch ports sending redundant traffic. Switches exchange BPDU messages with each other using their non-edge ports.

An edge port is a switch port connected to a device, such as a computer, server, or printer. These devices should not generate BPDU messages. If they do, it indicates a problem, such as a malicious actor sending false BPDU messages.

Many switches support a BPDU Guard feature that is enabled on edge ports. It monitors the ports for any BPDU messages. If it receives any, it disables the port, effectively blocking the BPDU attack.

Comparing Ports and Ports

A physical port used by a network device, such as a switch or a router, is entirely different from the logical ports discussed previously. You plug a cable into a physical port. A logical port is a number embedded in a packet and identifies services and protocols.

This is like minute (60 seconds) and minute (tiny), or like the old joke about the meaning of secure. The Secretary of Defense directed members of different services to “secure that building.” Navy personnel turned off the lights and locked the doors. The Army occupied the building and ensured no one could enter. The Marines attacked it, captured it, and set up defenses to hold it. The Air Force secured a two-year lease with an option to buy.

Routers

A *router* connects multiple network segments into a single network and routes traffic between the segments. Because routers don't pass broadcasts, they effectively reduce traffic on any single segment. Segments separated by routers are sometimes referred to as broadcast domains. If a network has too many computers on a single segment, broadcasts can result in excessive collisions and reduce network performance. Moving computers to a different segment separated by a router can significantly improve overall performance. Similarly, subnetting networks creates separate broadcast domains.

Cisco routers are popular, but many other brands exist. Most routers are physical devices, and physical routers are the most efficient. However, it's also possible to add routing software to computers with more than one NIC. For example, Windows Server products can function as routers by adding additional services to the server.

Routers and ACLs

Access control lists (ACLs) are rules implemented on a router (and on firewalls) to identify what traffic is allowed and what traffic is denied. Rules within an ACL provide rule-based management for the router and control inbound and outbound traffic.

Router ACLs provide basic packet filtering. They filter packets based on IP addresses, ports, and some protocols, such as ICMP or IPsec, based on the protocol identifiers:

- **IP addresses and networks.** You can add a rule in the ACL to block access from any single computer based on the IP address. If you want to block traffic from one subnet to another, you can use a rule to block traffic using the subnet IDs. For example, the Sales department may be in the 192.168.1.0/24 network, and the Accounting department may be in the 192.168.5.0/24 network. You can ensure traffic from these two departments stays separate with an ACL on a router.
- **Ports.** You can filter traffic based on logical ports. For example, if you want to block HTTPS traffic, you can create a rule to block

traffic on port 443. Note that you can choose to block incoming traffic, outgoing traffic, or both. In other words, it's possible to allow outgoing HTTPS traffic while blocking incoming HTTPS traffic.

- **Protocol numbers.** Many protocols are identified by their protocol numbers. For example, ICMP uses a protocol number of 1, and many DoS attacks use ICMP. You can block all ICMP traffic (and the attacks that use it) by blocking traffic using this protocol number. Many automated intrusion prevention systems (IPSs) dynamically block ICMP traffic in response to attacks. Similarly, you can restrict traffic to only packets encrypted with IPsec ESP using a rule that allows traffic using protocol number 50 but blocks all other traffic. PPTP uses protocol number 47 and can be allowed by allowing traffic using protocol ID 47.

Deny Implicit Deny

Implicit deny is an important concept to understand, especially in the context of ACLs. It indicates that all traffic that isn't explicitly allowed is implicitly denied. For example, imagine you configure a router to allow Hypertext Transfer Protocol (HTTP) to a web server. The router now has an explicit rule defined to allow this traffic to the server. If you don't define any other rules, the implicit deny rule blocks all other traffic. Firewalls (discussed later in this chapter) also use an implicit deny rule.

The implicit deny rule is the last rule in an ACL. Some devices automatically apply the implicit deny rule as the last rule. Other devices require an administrator to place the rule at the end of the ACL manually. Syntax of an implicit deny rule varies on different systems, but it might be something like DENY ANY ANY, or DENY ALL ALL, where both ANY and ALL refer to any type of traffic.

While *implicit deny* is a common phrase used with routers and firewalls, it isn't common in everyday language. Simplified, you can think of it as *default deny* or *block by default*. In other words, the initial rules in an ACL identify traffic that is allowed. The last rule (*implicit deny*) denies, or blocks, all other traffic by default.

Remember this

Routers and stateless firewalls (or packet-filtering firewalls) perform basic filtering with an access control list (ACL). ACLs identify what traffic is allowed and what traffic is blocked. An ACL can control traffic based on networks, subnets, IP addresses, ports, and some protocols. Implicit deny blocks all access that has not been explicitly granted. Routers and firewalls use implicit deny as the last rule in the access control list.

The Route Command and Route Security

The **route** command is used to display or modify a system's routing table on both Windows and Linux systems. Using **route print**, you can see all the paths known by the computer to other networks. If the routing table doesn't include an entry to a specific network, the system uses the default gateway. The default gateway is the IP address of a router on a network and typically provides a path to the Internet. If you need to add a path to a different network, you can use the **route add** command.

You can also use the route command to verify route security. For example, the route table should point to a known default gateway. If malicious actors modify routing tables for systems, they can reroute traffic to a different router and use it to capture traffic in a man-in-the-middle (MITM) attack. MITM attacks are discussed in more depth in Chapter 7.

Firewalls

A *firewall* filters incoming and outgoing traffic for a single host or between networks. In other words, a firewall can ensure only specific types of traffic are allowed into a network or host, and only specific types of traffic are allowed out of a network or host.

The purpose of a firewall in a network is similar to a firewall in a car. The firewall in a car is located between the engine and passenger compartment. If a fire starts in the engine compartment, the firewall provides a layer of protection for passengers in the passenger compartment. Similarly, a firewall in a network will try to keep the bad traffic (often in the form of attackers) out of the network.

Of course, an engine has a lot of moving parts that can do damage to people if they accidentally reach into it while it's running. The firewall in a car protects passengers from touching any of those moving parts. Similarly, a network can also block users from going to places that an administrator deems dangerous. For example, uneducated users could inadvertently download damaging files, but many firewalls can block potentially malicious downloads.

Firewalls start with a basic routing capability for packet filtering as described in the “Routers and ACLs” section, including the use of an implicit deny rule. More advanced firewalls go beyond simple packet filtering and include advanced content filtering.

Host-Based Firewalls

A *host-based firewall* monitors traffic going in and out of a single host, such as a server or a workstation. It monitors traffic passing through the NIC and can prevent intrusions into the computer via the NIC. Many operating systems include software-based firewalls used as host-based firewalls. For example, Microsoft has included a host-based firewall on operating systems since Windows XP. Additionally, many third-party host-based firewalls are available. Host-based firewalls allow you to configure rules to allow or restrict inbound and outbound traffic.

Personal firewalls provide valuable protection for systems against unwanted intrusions. Many organizations use personal firewalls on each

system, along with network firewalls, as part of an overall defense-in-depth strategy.

It's especially important to use personal firewalls when accessing the Internet in a public place. Free Wi-Fi Internet access is often available in public places, such as airports, hotels, and many fast-food establishments, such as Starbucks and McDonald's. However, connecting to a public Wi-Fi hot spot without the personal firewall enabled is risky and never recommended.

Software Versus Hardware Firewalls

Firewalls come in many different forms. They can be hardware or software, open source or proprietary, host-based, appliances, or virtual.

A software firewall is an application running on a system. For example, host-based firewalls are additional software running on the host system. A network-based firewall is usually a dedicated hardware system with additional software installed to monitor, filter, and log traffic. For example, Cisco makes a variety of different network-based firewalls. Many of them are dedicated servers with proprietary firewall software installed.

A network-based firewall would have two or more network interface cards (NICs), and all traffic passes through the firewall. The firewall controls traffic going in and out of a network. It does this by filtering traffic based on firewall rules and allows only authorized traffic to pass through it. Most organizations include at least one network-based firewall at the network border between their intranet (or internal network) and the Internet.

You can also use open source Linux systems as firewalls. Linux systems support iptables and many additions to iptables, such as ipv6tables, arptables, and so on. Generically, administrators commonly refer to these as xtables. You can configure firewall rules within the different tables, and they function just like an ACL. It's also possible to configure a virtual system as a firewall.

Remember this

Host-based firewalls provide protection for individual hosts, such as servers or workstations. A host-based firewall provides intrusion protection for the host. Linux systems support xtables for firewall capabilities. Network-based

firewalls are often dedicated servers and provide protection for the network.

Stateless Firewall Rules

Stateless firewalls use rules implemented in ACLs to identify allowed and blocked traffic. This is similar to how a router uses rules within ACLs. Firewalls use an implicit deny strategy to block all traffic that is not explicitly allowed. Although rules within ACLs look a little different depending on what hardware you're using, they generally include the following elements:

- **Permission.** You'll typically see this as PERMIT or ALLOW allowing the traffic. Most systems use DENY to block the traffic.
- **Protocol.** Typically, you'll see TCP or UDP here, especially when blocking specific TCP or UDP ports. If you want to block both TCP and UDP traffic using the same port, you can use IP instead. Using ICMP here blocks ICMP traffic, effectively blocking ping and some other diagnostics that use ICMP.
- **Source.** Traffic comes from a source IP address. You identify an IP address to allow or block traffic from a single IP address or from a range of IP addresses, such as from a single subnet. Wildcards such as any or all include all IP addresses.
- **Destination.** Traffic is addressed to a destination IP address. You identify an IP address to allow or block traffic to a single IP address or to a range of IP addresses, such as to an entire subnet. Wildcards such as any or all include all IP addresses.
- **Port or protocol.** Typically, you'll often see a well-known port such as port 443 for HTTPS in a rule. However, some devices support codes such as HTTPS for HTTPS traffic. Some systems support the use of keywords such as eq for equal, lt for less than, and gt for greater than. For example, instead of just using port 443, it might indicate eq 443.

Some firewalls require you to include a subnet mask in the rule. For example, if you want to block all SMTP traffic to the 192.168.1.0/24 network, you would use an IP address of 192.168.1.0 and a subnet mask of 255.255.255.0. However, if you only want to allow SMTP traffic to a single computer with the IP address of 192.168.1.20 in the /24 network, you

would use an IP address of 192.168.1.20 and a subnet mask of 255.255.255.255 (or /32). Using Classless Inter-Domain Routing (CIDR) notation, the rule for the network is 192.168.1.0/24, and the rule for the computer is 192.168.1.20/32, respectively.

Remember this

Firewalls use a *deny any any*, *deny any*, or a *drop all* statement at the end of the ACL to enforce an implicit deny strategy. The statement forces the firewall to block any traffic that wasn't previously allowed in the ACL. The implicit deny strategy provides a secure starting point for a firewall.

Stateful Versus Stateless

A *stateful firewall* inspects traffic and makes decisions based on the traffic context or state. It keeps track of established sessions, inspects traffic based on its state within a session, and it blocks traffic that isn't part of an established session. As an example, a TCP session starts with a three-way handshake. If a stateful firewall detects TCP traffic without a corresponding three-way handshake, it recognizes this as suspicious traffic and can block it.

A common security issue with stateless firewalls is misconfigured ACLs. For example, if the ACL doesn't include an implicit deny rule, it can allow almost all traffic into the network.

Web Application Firewall

A web application firewall (WAF) is a firewall specifically designed to protect a web application. A web server hosts the web application, and the WAF is placed between the web server and web server clients. The WAF can be a stand-alone appliance or software added to another device, and it protects the web server from a wide variety of attacks, such as cross-site scripting (XSS) attacks. Chapter 7, “Protecting Against Advanced Attacks,” discusses XSS attacks in more depth.

Imagine an organization hosts an e-commerce website to generate revenue. The web server is placed within a screened subnet (discussed later in this chapter), but due to the data that the web server handles, it needs more protection. All traffic destined for the web server goes through the WAF first, and the WAF blocks malicious traffic.

Note that you wouldn't use a WAF in place of a network-based firewall. Instead, it provides an added layer of protection for the web application in addition to a network-based firewall.

Remember this

A stateless firewall blocks traffic using an ACL, and a stateful firewall blocks traffic based on the state of the packet within a session. Web application firewalls provide strong protection for web servers. They protect against several different types of attacks, focusing on web application attacks.

Next-Generation Firewall

A ***next-generation firewall (NGFW)*** is an advanced firewall that adds capabilities that aren't available in first-generation or second-generation firewalls. The first generation of firewalls were packet-filtering firewalls, using stateless firewall rules, and could only allow or block traffic after evaluating individual packets. The second generation of firewalls added in stateful firewall rules. This allows firewalls to evaluate traffic based on its session state.

Firewalls have steadily improved over the years, and if each improvement was labeled as another generation, we might be on the ninety-ninth generation. Thankfully, we're just using NGFW to indicate that a firewall adds additional capabilities to first- and second-generation firewalls.

An NGFW performs deep-packet inspection, adding application-level inspection as a core feature. The NGFW is aware of common application protocols used on the Internet, such as FTP and HTTP. By using deep-packet inspection, the NGFW can identify application commands and detect potentially malicious traffic. This allows it to apply content filtering and URL filtering.

Implementing Network Designs

There are several elements involved in creating a secure network. This includes the use of various topologies and different network appliances. Segmenting network devices and traffic can improve performance and increase security. This section covers physical security and logical security methods used for both segmentation and isolation. It also covers several different network appliances used for segmentation and isolation.

Intranet Versus Extranet

Most networks have Internet connectivity, but it's rare to connect a network directly to the Internet. Instead, it's common to divide the network into different zones, using different topologies. Two terms that are relevant here are:

- **Intranet.** An *intranet* is an internal network. People use the intranet to communicate and share content with each other. While it's common for an intranet to include web servers, this isn't a requirement.
- **Extranet.** An *extranet* is part of a network that can be accessed by authorized entities from outside of the network. For example, it's common for organizations to allow limited access to authorized business partners, customers, vendors, or others.

The network perimeter provides a boundary between the intranet and the Internet. Boundary protection includes multiple methods to protect the network perimeter.

Screened Subnet

A ***screened subnet*** (also known as a demilitarized zone or DMZ) is a buffered zone between a private network and the Internet. Attackers seek out servers on the Internet, so any server placed directly on the Internet has the highest amount of risk. However, the screened subnet provides a layer of protection for these Internet-facing servers while also allowing clients to connect to them.

As an example, Figure 3.4 shows a common network configuration with a screened subnet. The screened subnet is the area between the two firewalls (FW1 and FW2) and hosts several Internet-facing servers. Many screened subnets have two firewalls, creating a buffer zone between the Internet and the internal network, as shown in Figure 3.4, though other screened subnet configurations are possible.

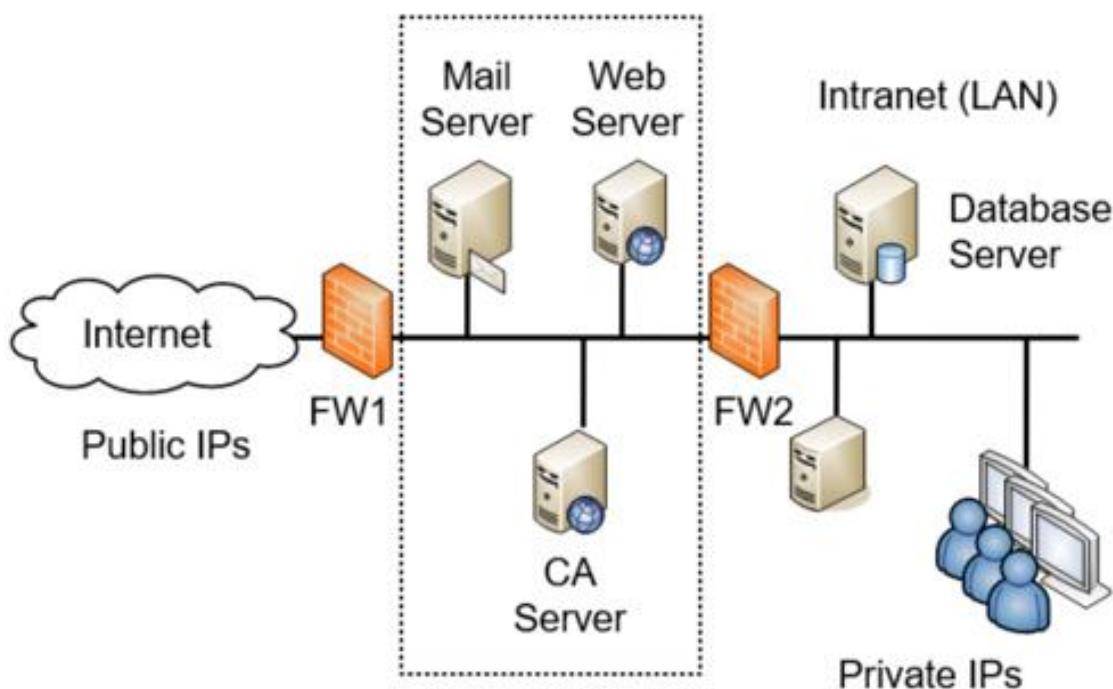


Figure 3.4: Network with screened subnet

In this configuration, one firewall separates the screened subnet from the Internet. The second firewall separates the screened subnet from the internal network. Each firewall includes detailed rules designed to filter traffic and protect both the internal network and public-facing servers. One way of saying this is that the screened subnet provides access to the services

hosted in the screened subnet while segmenting access to the internal network.

For example, FW1 can have rules to allow traffic to the servers in the screened subnet but block unsolicited traffic to FW2. The mail server would send and receive email to and from other email servers on the Internet through port 25 or port 465 of FW1 and send and receive email to internal clients through port 25 or port 465 on FW2. The web server hosts webpages to any Internet users through ports 80 and 443 on FW1, but FW2 blocks incoming traffic using these ports. The certificate authority (CA) server validates certificates for Internet clients by answering through FW1.

Notice in Figure 3.4 that the intranet includes a database server. The web server may use this to create webpages for an e-commerce site. The database server could hold product data, customer data, and much more. FW2 allows traffic between the web server (and only the web server) and the database server on port 1433. FW2 would block all other Internet traffic to the database server.

It's also possible for the web server and the database server to be part of an extranet. For example, imagine that the web server hosts a site that business partners can use to place orders. The web server would first authenticate them before granting them full access. After users log on, the website connects to the back-end database server, allowing them to browse the inventory and place orders. Because this site is only for authorized business partners, it is an extranet.

The screened subnet can host any Internet-facing server, not just those shown in the figure. Other examples include FTP servers used to upload and download files and virtual private network (VPN) servers used for providing remote access.

Remember this

A screened subnet (sometimes called a DMZ) is a buffer zone between the Internet and an internal network. It allows access to services while segmenting access to the internal network. In other words, Internet clients can access the services hosted on servers in the screened subnet, but the screened subnet provides a layer of protection for the intranet (internal network).

Network Address Translation Gateway

Network Address Translation (NAT) is a protocol that translates public IP addresses to private IP addresses and private addresses back to public. A **network address translation gateway** hosts NAT and provides internal clients with private IP addresses a path to the internet. Instead of using a NAT gateway, it's also possible to enable NAT on an Internet-facing firewall. A commonly used form of NAT is network address and port translation, commonly called Port Address Translation (PAT).

If you run a network at your home (such as a wireless network), the wireless router that connects to the Internet is very likely running NAT.

Some of the benefits of NAT include:

- **Public IP addresses don't need to be purchased for all clients.** A home or company network can include multiple computers that can access the Internet through one router running NAT. Larger companies requiring more bandwidth may use more than one public IP address.
- **NAT hides internal computers from the Internet.** Computers with private IP addresses are isolated and hidden from the Internet. NAT provides a layer of protection to these private computers because they aren't as easy to attack and exploit from the Internet.

One of the drawbacks to NAT is that it is not compatible with IPsec. You can use L2TP to create VPN tunnels and use it with IPsec to encrypt VPN traffic. Although there are ways of getting around NAT's incompatibility with IPsec, if your design includes IPsec going through NAT, you'll need to closely examine it.

NAT can be either static NAT or dynamic NAT:

- **Static NAT.** Static NAT uses a single public IP address in a one-to-one mapping. It maps a private IP address with a single public IP address.
- **Dynamic NAT.** Dynamic NAT uses multiple public IP addresses in a one-to-many mapping. Dynamic NAT decides which public IP address to use based on load. For example, if several users are connected to the Internet on one public IP address, NAT maps the next request to a less-used public IP address.

Remember this

NAT translates public IP addresses to private IP addresses and private IP addresses back to public. A common form of NAT is Port Address Translation. Dynamic NAT uses multiple public IP addresses, while static NAT uses a single public IP address.

Physical Isolation and Air Gaps

Physical isolation ensures that one network isn't connected to another network. As an example, consider ***supervisory control and data acquisition (SCADA)*** systems. These are typically industrial control systems within large facilities such as power plants or water treatment facilities. While SCADA systems operate within their own network, it's common to ensure that they are isolated from any other network.

This physical isolation significantly reduces risks to the SCADA system. If an attacker can't reach it from the Internet, it is much more difficult to attack it. However, if the system is connected to the internal network, an attacker can access internal computers and then access any internal network resource.

An ***air gap*** provides physical isolation, with a gap of air between an isolated system and other systems. When considered literally, an air-gapped system is not connected to any other systems. As an example, many organizations use both classified (red) and unclassified (black) networks. Strict rules ensure that these two systems are not connected to each other. Some rules require physical separation between red network cables and black network cables.

Remember this

An air gap isolates one network from another by ensuring there is physical space (literally a gap of air) between all systems and cables.

Logical Separation and Segmentation

As mentioned previously in this chapter, routers and firewalls provide a basic level of separation and ***segmentation***. Routers segment traffic between networks using rules within ACLs. Administrators use subnetting to divide larger IP address ranges into smaller ranges. They then implement rules within ACLs to allow or block traffic. Firewalls separate network

traffic using basic packet-filtering rules and can also use more sophisticated methods to block undesirable traffic.

It's also possible to segment traffic between logical groups of users or computers with a virtual local area network (VLAN). VLANs provide logical separation.

Isolating Traffic with a VLAN

A *virtual local area network (VLAN)* uses a switch to group several different computers into a virtual network. You can group the computers based on departments, job functions, or any other administrative need. This provides security because you're able to isolate the traffic between the computers in the different VLANs.

Normally, a router would group different computers onto different subnets, based on physical locations. As an example, computers in a routed segment are typically on the same office or same floor.

However, a single Layer 3 switch can create multiple VLANs to separate the computers based on logical needs rather than a physical location. Additionally, administrators can easily reconfigure the switch to add or subtract computers from any VLAN if needed.

For example, a group of users who normally work in separate departments may begin work on a project that requires them to be on the same subnet. You can configure a Layer 3 switch to logically group these workers together, even if the computers are physically located in different offices or different floors of a building. When the project is over, you can simply reconfigure the switch to return the network to its original configuration.

As another example, VoIP streaming traffic can consume quite a bit of bandwidth. One way to increase the availability and reliability of systems using this voice traffic is to put them on a dedicated VLAN. Other systems transferring traditional data traffic can be placed on a separate VLAN. This separates the voice and data traffic into their own VLANs.

Similarly, you can use a single switch with multiple VLANs to separate user traffic. For example, if you want to separate the traffic between the HR department and the IT department, you can use a single switch with two VLANs. The VLANs logically separate the computers between the two different departments, even if they are close to each other.

Remember this

Virtual local area networks (VLANs) separate or segment traffic on physical networks, and you can create multiple VLANs with a single Layer 3 switch. A VLAN can logically group several different computers together or logically separate computers without regard to their physical location. VLANs are also used to separate traffic types, such as voice traffic on one VLAN and data traffic on a separate VLAN.

East-West Traffic

Within a network, ***east-west*** traffic refers to traffic between servers. Imagine looking at a network diagram of servers within a network. These usually show servers configured horizontally (or side-by-side), so traffic between servers travels east and west. In contrast, network diagrams typically show clients above or below the servers, and traffic between clients and servers is north-south.

Zero Trust

A ***zero trust network*** is a network that doesn't trust any devices by default, even if it was previously verified. This helps reduce attacks from compromised internal clients. Zero trust isn't a technology, but instead, it's a security model based on the principle of zero trust. One way to implement it is by requiring multifactor authentication (described in Chapter 2).

As an example, imagine Homer regularly accesses files on servers in the network. Today, he clicked on a link in a malicious email and inadvertently installed malware on his system. The malware then uses Homer's system and credentials to access server files that Homer regularly accesses. However, the server prompts Homer to provide a second authentication factor, which is unknown to the malware. This effectively blocks the attack.

Network Appliances

Network ***appliances*** are dedicated systems designed to fulfill a specific need. The intent of the word *appliance* is to evoke a sense of simplicity. For example, you don't have to know the details of how a toaster works to make toast. Similarly, you don't have to know the details of how a computer appliance operates to use it. Vendors handle all of the details under the hood, making it easier for administrators.

Previous sections discussed different types of firewalls, and the following sections discuss proxy servers and jump servers. All of these can be dedicated appliances or services added to another server.

Proxy Servers

Many networks use *proxy servers* (or *forward proxy servers*) to forward requests for services (such as HTTP or HTTPS) from clients. They can improve performance by caching content, and some proxy servers can restrict users' access to inappropriate websites by filtering content. A proxy server is located on the edge of the network bordering the Internet and the intranet, as shown in Figure 3.5.

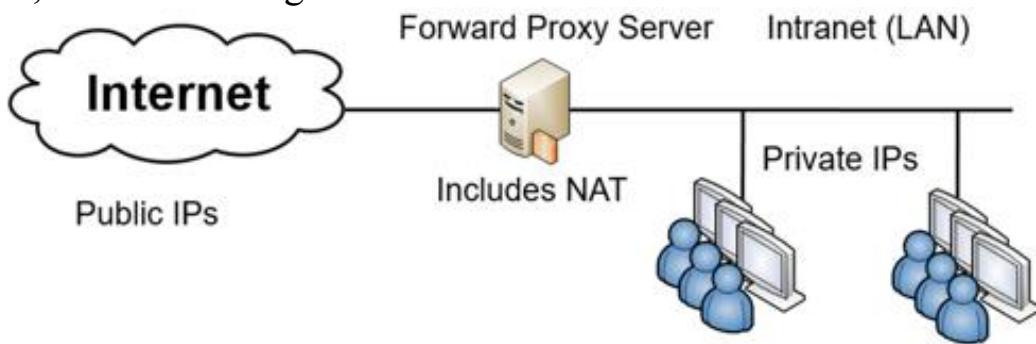


Figure 3.5: Proxy server

Administrators configure internal clients to use the proxy server for specific protocols. The proxy accepts their requests, retrieves the content from the Internet, and then returns the data to the client. Most proxy servers only act as a proxy for HTTP and HTTPS. However, proxy servers can also proxy other Internet protocols, such as FTP.

Caching Content for Performance

The proxy server increases the performance of Internet requests by caching each result received from the Internet. Any data that is in the proxy server's cache doesn't need to be retrieved from the Internet again to fulfill another client's request. In this context, cache simply means "temporary storage." Cache could be a dedicated area of RAM, or, in some situations, it could also be an area on a high-performance disk subsystem.

As an example, if Lisa retrieves a webpage from *GetCertifiedGetAhead.com*, the proxy server would store the result in cache. If Homer later requests the same page, the proxy server retrieves the page from cache and sends it to Homer. This reduces the amount of Internet bandwidth used for web browsing because the page doesn't need to be retrieved again.

Transparent Proxy Versus Non-transparent Proxy

A *transparent proxy* will accept and forward requests without modifying them. It is the simplest to set up and use and it provides caching. In contrast, a *non-transparent proxy* server can modify or filter requests. Organizations often use nontransparent proxy servers to restrict what users can access with the use of URL filters. A URL filter examines the requested URL and chooses to allow the request or deny the request.

Many third-party companies sell subscription lists for URL filtering. These sites scour the Internet for websites and categorize the sites based on what companies typically want to block. Categories may include anonymizers, pornography, gambling, web-based email, and piracy sites. Anonymizers are sites that give the illusion of privacy on the Internet. Employees sometimes try to use anonymizers to bypass proxy servers, but a proxy server usually detects, blocks, and logs these attempts. Web-based email bypasses the security controls on internal email servers, so many organizations block them.

The subscription list can be loaded into the proxy server, and whenever a user attempts to access a site on the URL filter block list, the proxy blocks the request. Often, the proxy server presents users with a warning page when they try to access a restricted page. Many organizations use this page to remind users of a corporate acceptable usage policy, and some provide reminders that the proxy server is monitoring their online activity.

Proxy servers include logs that record each site visited by users. These logs can be helpful to identify frequently visited sites and to monitor user web browsing activities.

Remember this

A proxy server forwards requests for services from a client. It provides caching to improve performance and reduce Internet bandwidth usage. Transparent proxy servers accept and forward requests without modifying them. Non-transparent proxy servers use URL filters to restrict access to certain sites. Both types can log user activity.

Reverse Proxy

A *reverse proxy* accepts requests from the Internet, typically for a single web server. It appears to clients as a web server but is forwarding the

requests to the web server and serving the pages returned by the web server. Figure 3.6 shows how a reverse proxy server is configured to protect a web server. Note that this configuration allows the web server to be located in the private network behind a second firewall.

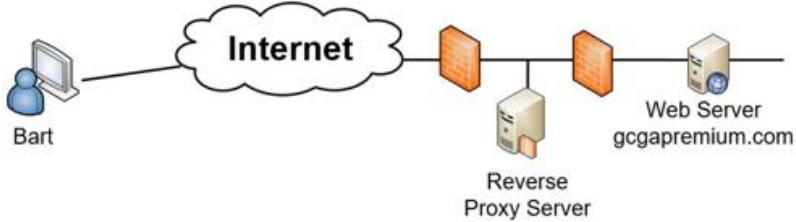


Figure 3.6: Reverse proxy server

Imagine that Bart wants to access <https://gcpapremium.com>. He types the URL into his browser and it connects to the reverse proxy server. The reverse proxy server connects to the web server and retrieves the webpage. It then sends the webpage to Bart. A reverse proxy server caches the webpages just as a forward proxy server does, so it can improve the overall website performance.

The reverse proxy server can be used for a single web server or a web farm of multiple servers. When used with a web farm, it can act as a ***load balancer***. You would place the load balancer in the screened subnet to accept the requests, and it then forwards the requests to different servers in the web farm using a load-balancing algorithm. Chapter 9, “Implementing Controls to Protect Assets,” covers load balancing in more depth.

Unified Threat Management

Unified threat management (UTM) is a single solution that combines multiple security controls. The overall goal of UTMs is to provide better security while also simplifying management requirements. In many cases, a UTM device will reduce the workload of administrators without sacrificing security.

As IT-based threats first began appearing, security experts created various solutions to deal with each of them. When attackers began releasing malware to infect computers, vendors created antivirus software. Attackers started attacking networks, and in response, security experts developed and steadily improved firewalls. Organizations implemented proxies with URL filters when they recognized a need to control what sites users can visit.

Although these solutions are effective, they are also complex. Administrators often find it challenging to manage each of these solutions separately. Because of this, UTM security appliances have become quite popular. They combine the features of multiple security solutions into a single appliance. For example, a UTM security appliance might include multiple capabilities such as those listed in the following bullets:

- **URL filtering.** URL filters within a UTM security appliance perform the same job as a proxy server. They block access to sites based on the URL. It's common to subscribe to a service and select categories to block access to groups of sites. Administrators can also configure URL filters manually to allow or block access to specific websites.
- **Malware inspection.** Malware often comes into a network via spam or malicious webpages. The malware inspection component of a UTM appliance screens incoming data for known malware and blocks it. Organizations often scan for malware at email servers and individual systems as part of a layered security or defense-in-depth solution.
- **Content inspection.** Content inspection includes a combination of different content filters. It monitors incoming data streams and attempts to block any malicious content. It can include a spam filter to inspect incoming email and reject spam. It can also block specific

types of transmissions, such as streaming audio and video, and specific types of files such as Zip files.

- **DDoS mitigator.** A DDoS mitigator attempts to detect DDoS attacks and block them. This is similar to how intrusion prevention systems (IPSs) block attacks. Chapter 4 covers IPSs in more depth.

The output of the UTM varies depending on the device and what it sees. For example, if it detects malware, it will typically raise an alert and send it to administrators.

A common security issue with UTMs is a misconfigured content filter. For example, if the spam filter is misconfigured, it can block valid mail or allow too much spam into the network. Administrators adjust the sensitivity of the spam filter to meet the needs of the organization. For example, one organization might find it unacceptable to block emails from customers or potential customers. Administrators would adjust the sensitivity, allowing more spam into the network to meet this need.

It's common to place UTM appliances at the network border, between the Internet and the intranet (or the private network). This allows it to intercept and analyze all traffic to and from the Internet. However, the placement is dependent on how the UTM appliance is being used. As an example, if it is being used as a proxy server, it can be placed within the screened subnet. Administrators would configure the clients to use the UTM appliance for proxy servers, ensuring that all relevant traffic goes through it.

Remember this

A unified threat management (UTM) appliance combines multiple security controls into a single appliance. They can inspect data streams and often include URL filtering, malware inspection, and content inspection components. Many UTMs include a DDoS mitigator to block DDoS attacks.

Jump Server

A ***jump server*** (sometimes called a jump box) is a hardened server used to access and manage devices in another network with a different security zone. As an example, if administrators want to administer servers in the screened subnet from the internal network, they could use a jump server. They could connect to the jump server and then access servers in the screened subnet through the jump server.

It's common to connect to a jump server using a passwordless SSH login, described earlier in the “OpenSSH” section, and then connect to the remote server via the jump server. Imagine Maggie has elevated privileges on a jump server (named jump) and on a certificate authority (CA) server in the screened subnet (named ca1). She could use the following command:

```
ssh -J maggie@jump maggie@ca1
```

The -J switch tells ssh to connect to the jump server and then use TCP forwarding to connect to the CA server.

While the preceding example used the jump server to connect to a server in the screened subnet, it's also possible to use a jump server to connect to an internal network, such as a SCADA system network isolated with a VLAN.

It's essential to ensure that the jump server is hardened. Ideally, it isn't used for anything else so it won't have any other services running. Any additional services on the server give attackers another target. Additionally, the target system should restrict connections from systems other than the jump server.

Remember this

A jump server is placed between different security zones and provides secure access from devices in one zone to devices in the other zone. It can provide secure access to devices in a screened subnet from an internal network.

Security Implications of IPv6

RFC 7123, “Security Implications of IPv6 on IPv4 Networks,” discusses some of the risks of using IPv6 on internal networks. One of the biggest challenges is when all devices on an internal network don’t support IPv6 natively. While IPv6 may still work, there are many vulnerabilities that attackers may be able to exploit.

As an example, an IPv4 firewall might be able to enforce rules for IPv4 but be unable to enforce similar rules for IPv6 traffic. Similarly, other network appliances might not recognize IPv6 traffic, allowing unwanted traffic into the network. Because of these security implications, many internal networks continue to use IPv4 and there’s nothing wrong with that.

Summarizing Routing and Switching Use Cases

This chapter discussed several use cases, but it was important to understand routers and switches before connecting them with routing and switching use cases. This section summarizes some of the routing and switching topics.

The following bullets identify some use cases that switches support:

- *Prevent switching loops.* You do this by implementing STP or RSTP on switches.
- *Prevent BPDU attacks.* A BPDU Guard enabled on edge ports of a switch will prevent BPDU attacks.
- *Prevent unauthorized users from connecting to unused ports.* Port security methods, such as disabling unused ports, and using MAC address filtering, prevent these unauthorized connections.
- *Provide increased segmentation of user computers.* Layer 3 switches support VLANs, and VLANs provide increased segmentation.

Simple Network Management Protocol version 3 (SNMPv3) monitors and manages network devices, such as routers or switches. This includes using SNMPv3 to modify the devices' configuration or have network devices report status back to a central network management system. SNMPv3 agents installed on devices send information to an SNMP manager via notifications known as traps (sometimes called device traps).

SNMPv1 and v2 both have vulnerabilities, including sending passwords across the network in cleartext, but SNMPv3 encrypts credentials before sending them over the wire. A common use case supported by SNMPv3 is to *provide secure management of network devices*. SNMPv3 uses UDP ports 161 and 162.

Remember this

Administrators use SNMPv3 to manage and monitor network devices, and SNMP uses UDP ports 161 and 162. SNMPV3 encrypts credentials before sending them over the network and is more secure than earlier versions.

Chapter 3 Exam Topic Review

When preparing for the exam, make sure you understand these key concepts covered in this chapter.

Reviewing Basic Networking Concepts

- A use case typically describes an organizational goal, and administrators enable specific protocols to meet organizational goals.
- Protocols used for voice and video include Real-time Transport Protocol (RTP) and Secure Real-time Transport Protocol (SRTP). SRTP provides encryption, message authentication, and integrity for RTP.
- File Transfer Protocol (FTP) is commonly used to transfer files over networks, but FTP does not encrypt the transmission. SSH encrypts Secure Copy (SCP) and Secure FTP (SFTP). TLS encrypts FTPS.
- SMTP sends email using TCP port 25 and port 587 for email encrypted with TLS. POP3 receives email using TCP port 110 and TCP port 995 for encrypted connections. IMAP4 uses TCP port 143 and port 993 for encrypted connections.
- HTTPS encrypts browser-based traffic with TLS using TCP port 443.
- Directory services solutions implement Kerberos as the authentication protocol. They also use Lightweight Directory Access Protocol (LDAP) over TCP port 389 and LDAP Secure (LDAPS) over TCP port 636.
- Administrators commonly connect to remote systems using SSH instead of Telnet because SSH encrypts the connection. Administrators also use Remote Desktop Protocol (RDP) to connect to remote systems using TCP port 3389.
- The Network Time Protocol (NTP) provides time synchronization services.
- OpenSSH tools simplify the use of SSH to connect to remote servers. The ssh-keygen command creates a public/private key pair,

and the ssh-copy-id command copies the public key to a remote server. The private key permissions should not be changed.

- Domain Name System (DNS) provides domain name resolution. DNS zones include A records for IPv4 addresses and AAAA records for IPv6 addresses. MX records identify mail servers, and the MX record with the lowest preference is the primary mail server. DNS uses TCP port 53 for zone transfers and UDP port 53 for DNS client queries.
- Domain Name System Security Extensions (DNSSEC) provides validation for DNS responses by adding a Resource Record Signature (RRSIG). The RRSIG provides data integrity and authentication and helps prevent DNS poisoning attacks.
- Two command-line tools used to query DNS are nslookup and dig. They can query DNS servers for specific records, such as MX records for mail servers. When a mail server has multiple MX records, the one with the lowest preference is the primary mail server.

Understanding Basic Network Devices

- Switches are used for network connectivity, and they map media access control (MAC) addresses to physical ports.
- Port security limits access to switch ports. It includes limiting the number of MAC addresses per port and disabling unused ports.
- Routers connect networks and direct traffic based on the destination IP address. Routers (and firewalls) use rules within access control lists (ACLs) to allow or block traffic.
- The route command is used to view and manipulate the routing table.
- Implicit deny indicates that unless something is explicitly allowed, it is denied. It is the last rule in an ACL.
- Host-based firewalls filter traffic in and out of individual hosts. Some Linux systems use iptables or xtables for firewall capabilities. Users should enable host-based firewalls when accessing the Internet from public locations.
- Network-based firewalls filter traffic in and out of a network. They are placed on the border of a network, such as between the Internet

and an internal network.

- A stateless firewall controls traffic between networks using rules within an ACL. The ACL can block traffic based on ports, IP addresses, subnets, and some protocols. Stateful firewalls filter traffic based on the state of a packet within a session.
- A web application firewall (WAF) protects a web server against web application attacks. It is typically placed in the screened subnet and will alert administrators of suspicious events.

Implementing Network Designs

- A screened subnet provides a layer of protection for servers that are accessible from the Internet.
- An intranet is an internal network. People use the intranet to communicate and share content with each other. An extranet is part of a network that can be accessed by authorized entities from outside of the network.
- NAT translates public IP addresses to private IP addresses, private back to public, and hides IP addresses on the internal network from users on the Internet. A NAT gateway is a device that implements NAT.
- Networks use various methods to provide network segregation, segmentation, and isolation.
- An air gap provides physical isolation for systems or networks. Systems or networks are completely isolated from other systems or networks with a gap of air.
- Routers provide logical separation and segmentation using ACLs to control traffic.
- Forward proxy servers forward requests for services from a client. It can cache content and record users' Internet activity. A transparent proxy accepts and forwards requests without modifying them. A non-transparent proxy can modify or filter requests, such as filtering traffic based on destination URLs.
- Reverse proxy servers accept traffic from the Internet and forward it to one or more internal web servers. The reverse proxy server is placed in the screened subnet and the web servers can be in the internal network.

- A unified threat management (UTM) security appliance includes multiple layers of protection, such as URL filters, content inspection, malware inspection, and a distributed denial-of-service (DDoS) mitigator. UTMs typically raise alerts and send them to administrators to interpret.
- Jump servers are placed between different security zones and provide secure access from devices in one zone to devices in the other zone. They are often used to manage devices in the screened subnet from the internal network.

Summarizing Routing and Switching Use Cases

- Loop protection protects against switching loop problems, such as when a user connects two switch ports together with a cable. Spanning Tree Protocols protect against switching loops.
- A Bridge Protocol Data Unit (BPDU) Guard, enabled on edge ports of a switch, protects against BPDU attacks.
- VLANs can logically separate computers or logically group computers regardless of their physical location. You create them with Layer 3 switches.
- SNMPv3 is used to monitor and configure network devices and uses notification messages known as traps. It uses strong authentication mechanisms and is preferred over earlier versions. SNMP uses UDP ports 161 and 162.
- Port security methods, such as disabling unused ports, and using MAC address filtering, prevent unauthorized users from connecting to unused ports.
- Layer 3 switches support VLANs, and VLANs provide increased segmentation of user computers.

Online References

- Remember, the online content includes some extras, such as labs, performance-based question examples, and more. Check it out at <https://greatadministrator.com/601-extras>.

Chapter 3 Practice Questions

1. An outside consultant performed an audit of the Municipal House of Pancakes network. She identified a legacy protocol being used to access browser-based interfaces on switches and routers within the network. She recommended replacing the legacy protocol with a secure protocol to access these network devices using the same interface. Which of the following protocols should be implemented?
 - A. The newest fully supported version of SSL
 - B. The newest fully supported version of TLS
 - C. The newest fully supported version of LDAPS
 - D. The newest fully supported version of SNMP

2. Your organization's security policy requires that confidential data transferred over the internal network must be encrypted. Which of the following protocols would BEST meet this requirement?
 - A. FTP
 - B. SSH
 - C. SNMPv3
 - D. SRTP

3. Maggie needs to collect network device configuration information and network statistics from devices on the network. She wants to protect the confidentiality of credentials used to connect to these devices. Which of the following protocols would BEST meet this need?
 - A. SSH
 - B. FTPS
 - C. SNMPv3
 - D. TLS

4. You are trying to determine what information attackers can gain about your organization using network reconnaissance methods via the Internet. Using a public wireless hot spot, you issue the following command:
****nslookup -querytype=mx gcgapremium.com****
You then see these results:

Server: UnKnown

Address: 10.0.0.1

Non-authoritative answer:

gcapremium.com MX preference = 90, mail exchanger =
mx1.emailsrvr.com

gcapremium.com MX preference = 20, mail exchanger =
mx2.emailsrvr.com

What does this tell you?

- A. 10.0.0.1 is the IP address of the primary mail server.
- B. gcapremium.com is unknown to DNS.
- C. The mx1.emailsrvr.com is a backup mail server.
- D. The MX servers are showing too much information to the public.

5. Administrators are configuring a server within your organization's screened subnet. This server will have the following capabilities when it is fully configured:

- It will use RRSIG.
- It will perform authenticated requests for A records.
- It will perform authenticated requests for AAAA records.

What BEST identifies the capabilities of this server?

- A. SSH
- B. SNMPv3
- C. S/MIME
- D. DNSSEC

6. Maggie regularly connects to a remote server named gcga using Secure Shell (ssh) from her Linux system. However, she has trouble remembering the password, and she wants to avoid using it without sacrificing security. She creates a cryptographic key pair to use instead. Which of the following commands is the BEST choice to use after creating the key pair?

- A. ssh-copy-id -i ~.ssh/id_rsa.pub maggie@gcga
- B. chmod 644 ~/.ssh/id_rsa
- C. ssh-keygen -t rsa
- D. ssh root@gcga

7. You are tasked with enabling NTP on some servers within your organization's screened subnet. Which of the following use cases are you MOST likely supporting with this action?

- A. Encrypting voice and video transmissions
- B. Providing time synchronization
- C. Enabling email usage
- D. Encrypting data-in-transit

8. Your organization has several switches in use throughout the internal network. Management wants to implement a security control to prevent unauthorized access to these switches within the network. Which of the following choices would BEST meet this need?

- A. Disable unused ports.
- B. Disable STP.
- C. Enable SSH.
- D. Enable DHCP.

9. Network administrators manage network devices remotely. However, a recent security audit discovered they are using a protocol that allows them to send credentials over the network in cleartext. Which of the following methods should be adopted to eliminate this vulnerability?

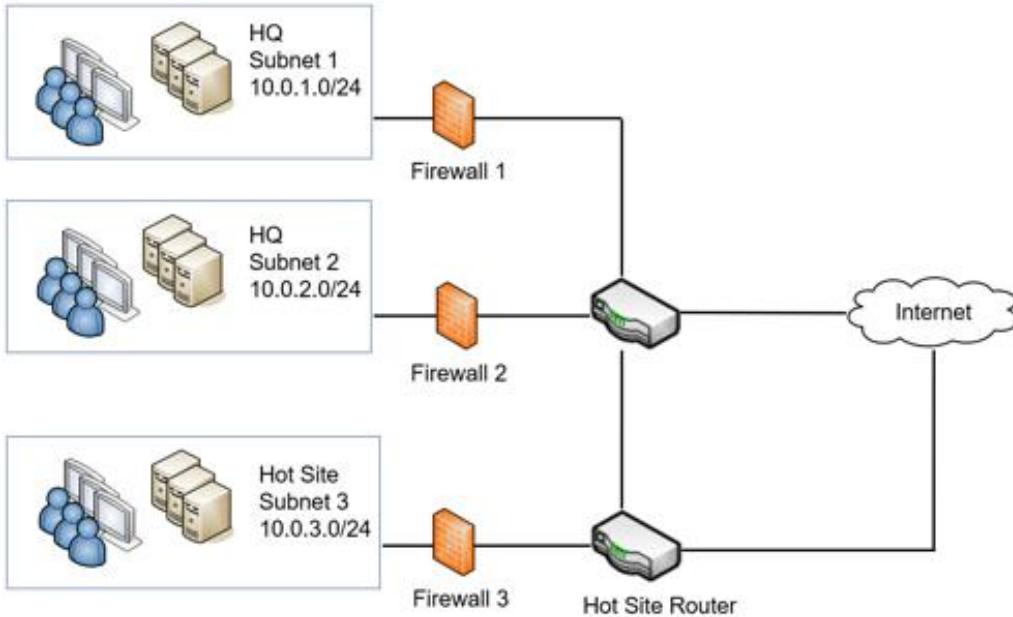
- A. Use SNMPv2c.
- B. Use SSH.
- C. Use SSL.
- D. Use SFTP.

10. Which of the following devices would MOST likely have the following entries used to define its operation?

permit IP any any eq 80
permit IP any any eq 443
deny IP any any

- A. Firewall
- B. Proxy server
- C. Web server
- D. Jump server

11. Your organization's network looks like the following graphic, and you've been asked to verify that Firewall 1 has the correct settings.



All firewalls should enforce the following requirements:

- Use only secure protocols for remote management.
- Block cleartext web traffic.

The following graphic shows the current rules configured in Firewall 1.

Rule	Destination	Source	Protocol	Action
HTTPS Outbound	Any	10.0.1.0/24	HTTPS	Allow
HTTP Outbound	Any	10.0.1.0/24	HTTP	Allow
DNS	Any	10.0.1.0/24	DNS	Allow
HTTPS Inbound	10.0.1.0/24	Any	HTTPS	Allow
HTTP Inbound	10.0.1.0/24	Any	HTTP	Block
Telnet	10.0.3.0/24	Any	Telnet	Allow
SSH	10.0.1.0/24	Any	SSH	Allow

You're asked to verify the rules are configured correctly. Which rule, if any, should be changed to ensure Firewall 1 meets the stated requirements?

- A. HTTPS Outbound
- B. HTTP Outbound
- C. DNS
- D. Telnet
- E. SSH
- F. None. All rules are correct.

12. The Springfield Nuclear Power Plant has several stand-alone computers used for monitoring. Employees log on to these computers using a local account to verify proper operation of various processes. The CIO of the organization has mandated that these computers cannot be connected to the organization's network or have access to the Internet. Which of the following would BEST meet this requirement?

- A. Air gap the computers.
- B. Place the computers in a screened subnet.
- C. Create a separate isolated network for these computers.
- D. Place the computers within a VLAN.

13. You have added another router in your network. This router provides a path to a limited access network that isn't advertised. However, a network administrator needs to access this network regularly. Which of the following could he do to configure his computer to access this limited network?

- A. Implement QoS technologies.
- B. Add a VLAN.
- C. Use the route command.
- D. Open additional ports on the router.

14. Several servers in your organization's screened subnet were recently attacked. After analyzing the logs, you discover that many of these attacks used TCP, but the packets were not part of an established TCP session. Which of the following devices would provide the BEST solution to prevent these attacks in the future?

- A. Stateless firewall
- B. Stateful firewall
- C. Network firewall
- D. Web application firewall

15. Your network currently has a dedicated firewall protecting access to a web server. It is currently configured with only the following two rules in the ACL:

```
PERMIT TCP ANY ANY 443  
PERMIT TCP ANY ANY 80
```

You have detected DNS requests and DNS zone transfer requests coming through the firewall and you need to block them. Which of the following would meet this goal? (Select TWO. Each answer is a full solution.)

- A. Add the following rule to the firewall: DENY TCP ALL ALL 53.
- B. Add the following rule to the firewall: DENY UDP ALL ALL 53.
- C. Add the following rule to the firewall: DENY TCP ALL ALL 25.
- D. Add the following rule to the firewall: DENY IP ALL ALL 53.
- E. Add an implicit deny rule at the end of the ACL.

Chapter 3 Practice Question Answers

1. **B** is correct. The newest version of Transport Layer Security (TLS) should be implemented to access the network devices. Because the scenario says the same interface is needed, the only possible choices are TLS or Secure Sockets Layer (SSL). However, SSL has been deprecated and should not be used. Lightweight Directory Access Protocol Secure (LDAPS) is used to communicate with directories such as Microsoft Active Directory. Simple Network Management Protocol version 3 (SNMPv3) adds security to SNMP and encrypts the credentials sent to and from the network devices, but it doesn't support access via a browser interface.
2. **B** is correct. You can use Secure Shell (SSH) to encrypt confidential data when transmitting it over the network. Secure File Transfer Protocol (SFTP) uses SSH to encrypt File Transfer Protocol (FTP) traffic, but FTP is unencrypted. Simple Network Management Protocol version 3 (SNMPv3) is used to monitor and manage network devices, not transmit data over a network. Secure Real-Time Transport Protocol (SRTP) provides encryption, message authentication, and integrity for voice and video, but not all data.
3. **C** is correct. Simple Network Management Protocol version 3 (SNMPv3) is a secure protocol that can monitor and collect information from network devices. It includes strong authentication mechanisms to protect the confidentiality of credentials. None of the other protocols listed are used to monitor network devices. Secure Shell (SSH) provides a secure method of connecting to devices but does not monitor them. File Transfer Protocol Secure (FTPS) is useful for encrypting large files in transit, using Transport Layer Security (TLS). TLS is commonly used to secure transmissions but doesn't include methods to monitor devices.
4. **C** is correct. This indicates that the mx1.emailsrvr.com is a backup mail server. The preference of mx1.emailsrvr.com is 90, which is higher than the preference of 20 for mx2.emailsrvr.com. In other words, mx2.emailsrvr.com is the primary email server and mx1.emailsrvr.com is the secondary email server. The "Address: 10.0.0.1" response indicates that the address of the

Domain Name System (DNS) server that gave the response is 10.0.0.1. The “Server: UnKnown” response indicates that the DNS server is not using PTR records, which resolve IP addresses to hostnames. Note that “UnKnown” looks like a typo but is the way that nslookup (short for name server lookup) displays it. The MX records are required so that other Internet-based mail servers can find the mail servers handling mail sent to a domain.

5. **D** is correct. This is a Domain Name System (DNS) server with the added capabilities of DNS Security Extensions (DNSSEC). DNSSEC is a suite of extensions to DNS. It uses a Resource Record Signature (RRSIG), commonly referred to as a digital signature, to provide data integrity and authentication for DNS replies. A DNS server resolves hostnames to IP addresses. Secure Shell (SSH) is commonly used to connect to remote systems and can be used to send files in an encrypted format over a network. Simple Network Management Protocol version 3 (SNMPv3) is used to manage and monitor network devices. Secure/Multipurpose Internet Mail Extensions(S/MIME) is a popular standard used to encrypt email, but email is not mentioned in the scenario.

6. **A** is correct. After creating the key pair, she should use the **ssh-copy-id** command to copy the public key to the server. The first step uses the **ssh-keygen -t rsa** command. This creates an RSA-based key pair (a private key and a public key). The public key’s location and the name is `~.ssh/id_rsa.pub`, and the private key’s location and the name is `~/.ssh/id_rsa`. The second step is to copy the public key to the remote server using the command **ssh-copy-id -i ~.ssh/id_rsa.pub maggie@gcga**. The private key should always stay private, but the **chmod 644** command makes it readable by everyone, so it shouldn’t be used. The **ssh** command connects to the remote server using Secure Shell (ssh). However, it’s not required to connect to the server before copying it. The **ssh-copy-id** command is a utility within the OpenSSH suite of tools.

7. **B** is correct. The Network Time Protocol (NTP) provides time synchronization services, so enabling NTP on servers in the screened subnet (sometimes called a demilitarized zone or DMZ) would meet this use case.

The Secure Real-time Transport Protocol (SRTP) provides encryption, message authentication, and integrity for audio and video over IP networks. Protocols such as Simple Mail Transfer Protocol (SMTP), Post Office Protocol v3 (POP3), and Internet Message Access Protocol version 4 (IMAP4) are used for email. Encrypting data isn't relevant to time synchronization services provided by NTP.

8. **A** is correct. You can prevent unauthorized access by disabling unused physical ports on the switches as an overall port security practice. This prevents the connection if someone plugs their computer into an unused disabled port. Spanning Tree Protocol (STP) prevents switching loop problems and should be enabled. Secure Shell (SSH) encrypts traffic and can be used to connect to network devices for management, but it doesn't directly protect a switch. Dynamic Host Configuration Protocol (DHCP) is used to dynamically issue IP addresses and is unrelated to this scenario.

9. **B** is correct. Secure Shell (SSH) can be used to connect to many network devices and is the best answer of the given choices. It encrypts the entire session, including the credentials. The scenario indicates that administrators are likely using Simple Network Management Protocol v1 (SNMPv1), SNMPv2, or SNMPv2c. These protocols all send a community string over the network in cleartext. SNMPv3 (which isn't available as a possible answer) encrypts the credentials before sending them over the network. Secure Sockets Layer (SSL) has been deprecated and shouldn't be used. Secure File Transfer Protocol (SFTP) is a secure implementation of FTP and is used to transfer files, not manage network devices.

10. **A** is correct. These are rules in an access control list (ACL) within a firewall. The first two rules indicate that traffic from any IP address, to any IP address, using ports 80 or 443 is permitted or allowed. The final rule is also known as an implicit deny rule and is placed last in the ACL. It ensures that all traffic that hasn't been previously allowed is denied. A proxy server would not use an ACL, although it would use ports 80 and 443 for Hypertext Transfer Protocol (HTTP) and HTTP Secure (HTTPS), respectively. A web server wouldn't use an ACL, although it would also use ports 80 and 443. A jump server is a server placed between different

security zones (such as an internal network and a screened subnet) and is used to manage devices in the other security zone.

11. **B** is correct. The Hypertext Transfer Protocol (HTTP) rule should be changed from Allow to Block to block cleartext web traffic. The Telnet rule has the incorrect Destination address and the incorrect action. It should be 10.0.1.0/24 and set to Block because it is not a secure protocol for remote management. However, because it has the incorrect address (10.0.3.0/24), it won't have any effect on traffic to Firewall 1.

12. **A** is correct. The best choice of the available answers is to air gap the computers. An air gap provides physical isolation, indicating that there is a gap of air between an isolated system and other systems. A screened subnet (sometimes called a demilitarized zone or DMZ) provides a buffer between the Internet and an internal network and would connect these computers to both the internal network and the Internet. The scenario doesn't indicate the computers need to be connected, so a separate isolated network is not needed. Placing the computers within a virtual local area network (VLAN) would connect the computers to a network.

13. **C** is correct. The **route** command can be used to display and manipulate the routing table on a Linux computer. Using this, you can provide another gateway path through this router to the limited access network. None of the other choices can add routing paths. Quality of Service (QoS) technologies allow administrators to give priority of some network traffic over other network traffic. A virtual local area network (VLAN) is used to segment or isolate a network, so configuring one won't grant access to a network. A router doesn't have ports that can be opened for individual users.

14. **B** is correct. A stateful firewall filters traffic based on the state of the packet within a session. It would filter a packet that isn't part of an established Transmission Control Protocol (TCP) session, which starts with a TCP three-way handshake. A stateless firewall filters traffic based on the IP address, port, or protocol ID. While it's appropriate to place a network firewall in a screened subnet (sometimes called a demilitarized zone or

DMZ), a network firewall could be either a stateless firewall or a stateful firewall. A web application firewall (WAF) is specifically designed to protect a web application, commonly hosted on a web server, but the attack was on several servers, not just a web server.

15. **D** and **E** are correct. The easiest way is to add an implicit deny rule at the end of the access control list (ACL) and all firewalls should have this to block all unwanted traffic. You can also deny all IP traffic using port 53 with DENY IP ALL ALL 53. Domain Name System (DNS) requests use UDP port 53, and DNS zone transfers use TCP port 53, so blocking only TCP 53 or UDP 53 does not block all DNS traffic. Port 25 is for Simple Mail Transfer Protocol (SMTP) and unrelated to this question.

Chapter 4

Securing Your Network

CompTIA Security+ objectives covered in this chapter:

1.4 Given a scenario, analyze potential indicators associated with network attacks.

- Wireless (Evil twin, Rogue access point, Bluesnarfing, Bluejacking, Disassociation, Jamming, Radio frequency identifier (RFID), Near field communication (NFC), Initialization vector (IV))

1.5 Explain different threat actors, vectors, and intelligence sources.

- Vectors (Direct access, Wireless)

1.8 Explain the techniques used in penetration testing.

- Passive and active reconnaissance (Drones, War flying, War driving, Footprinting)

2.1 Explain the importance of security concepts in an enterprise environment.

- Deception and disruption (Honeypots, Honeyfiles, Honeynets, Fake telemetry)

3.1 Given a scenario, implement secure protocols.

- Protocols (IPSec, Authentication header (AH)/Encapsulated security payload (ESP), Tunnel/transport)

3.2 Given a scenario, implement host or application security solutions.

- Host intrusion prevention system (HIPS), Host intrusion detection system (HIDS)

3.3 Given a scenario, implement secure network designs.

- Virtual private network (VPN) (Always on, Split tunnel vs. full tunnel, Remote access vs. site-to-site, IPSec, SSL/TLS, HTML5, Layer 2 tunneling protocol (L2TP), Network access control (NAC) (Agent and agentless))
- Out-of-band management, Port Security (Media access control (MAC) filtering)
- Network Appliances (Network-based intrusion detection system (NIDS)/network-based intrusion prevention system (NIPS), (Signature based, Heuristic/behavior, Anomaly, Inline vs. passive), Sensors, Collectors, Aggregators), Port spanning/port mirroring (Port taps)

3.4 Given a scenario, install and configure wireless security settings.

- Cryptographic protocols (WiFi protected access 2 (WPA2), WiFi protected access 3 (WPA3), Counter-mode/CBC-MAC Protocol (CCMP), Simultaneous Authentication of Equals (SAE))
- Authentication protocols (Extensible Authentication Protocol (EAP), Protected Extensible Application Protocol (PEAP), EAP-FAST, EAP-TLS, EAP-TTLS, IEEE 802.1X, Remote Authentication Dial-in User Server (RADIUS) Federation)
- Methods (Pre-shared key (PSK) vs. Enterprise vs. Open, WiFi Protected Setup (WPS), Captive portals)
- Installation considerations (Site surveys, Heat maps, WiFi analyzers, Channel overlaps, Wireless access point (WAP) placement, Controller and access point security)

3.8 Given a scenario, implement authentication and authorization solutions.

- Authentication/Authorization (EAP, Challenge Handshake Authentication Protocol (CHAP), Password Authentication Protocol (PAP), 802.1X, RADIUS, Terminal Access

Controller Access Control System Plus (TACACS+)

**

In this chapter, you'll learn about some of the more advanced network security concepts. Topics include intrusion detection systems (IDSs) and intrusion prevention systems (IPSs), methods used to secure wireless networks, common wireless attacks, and virtual private network (VPN) technologies.

Exploring Advanced Security Devices

Chapter 3, “Exploring Network Technologies and Tools,” discusses basic network technologies and protocols. This section explores many of the more advanced security devices used to secure networks.

Understanding IDSs and IPSs

Intrusion detection systems (IDSs) monitor a network and send alerts when they detect suspicious events on a system or network. Intrusion prevention systems (IPSs) react to attacks in progress and prevent them from reaching systems and networks.

Chapter 8, “Using Risk Management Tools,” discusses protocol analyzers, or sniffers, in more depth, but as an introduction, administrators use them to capture and analyze network traffic sent between hosts. IDSs and IPSs have the same capability. They capture the traffic and analyze it to detect potential attacks or anomalies.

Both IDSs and IPSs act as detective security controls using similar detection methods. The biggest difference is in their responses to an attack. This section presents IDSs first and then wraps up with some information on IPSs and compares the two. However, as you go through this section, it’s worth remembering that IDSs and IPSs can implement the same monitoring and detection methods.

HIDS

A ***host-based intrusion detection system (HIDS)*** is additional software installed on a system such as a workstation or a server. It protects the individual host, can detect potential attacks, and protects critical operating system files. The primary goal of any IDS is to monitor traffic. For a HIDS, this traffic passes through the network interface card (NIC).

Many host-based IDSs have expanded to monitor application activity on the system. As one example, you can install a HIDS on different Internet-facing servers, such as web servers, mail servers, and database servers. In addition to monitoring the network traffic reaching the servers, the HIDS can also monitor the server applications.

It’s worth stressing that a HIDS can help detect malicious software (malware) that traditional antivirus software might miss. Because of this, many organizations install a HIDS on every workstation as an extra layer of protection in addition to traditional antivirus software. Just as the HIDS on a server will monitor network traffic, a workstation HIDS will monitor network traffic reaching the workstation. However, a HIDS can also

monitor some applications and protect local resources such as operating system files.

In other organizations, administrators only install a HIDS when there's a perceived need. For example, suppose an administrator is concerned that a specific server with proprietary data is at increased risk of an attack. In that case, the administrator might choose to install a HIDS on this system as an extra layer of protection.

Remember this

A HIDS can monitor all traffic on a single host system such as a server or a workstation. In some cases, it can detect malicious activity missed by antivirus software.

NIDS

A ***network-based intrusion detection system (NIDS)*** monitors activity on the network. An administrator installs NIDS sensors or collectors on network devices such as switches, routers, or firewalls. These sensors gather information and report to a central monitoring network appliance hosting a NIDS console.

A NIDS cannot detect anomalies on individual systems or workstations unless the anomaly causes a significant difference in network traffic. Additionally, a NIDS is unable to decrypt encrypted traffic. In other words, it can only monitor and assess threats on the network from traffic sent in plaintext or non-encrypted traffic.

Figure 4.1 shows an example of a NIDS configuration. In the figure, sensors are located before the firewall, after the firewall, and on routers. These sensors collect and monitor network traffic on subnets within the network and report to the NIDS console. The NIDS provides overall monitoring and analysis and can detect attacks on the network.

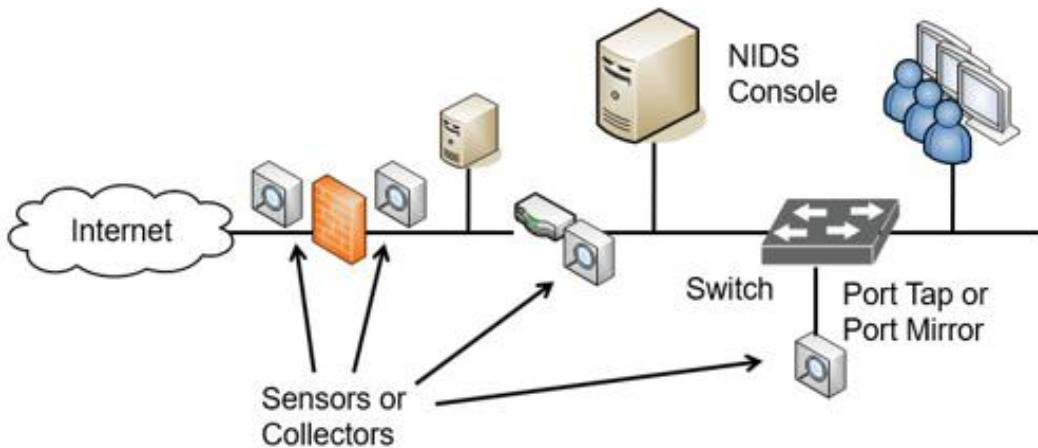


Figure 4.1: NIDS sensors

Figure 4.1 also shows a port tap or port mirror on the internal switch. Most switches support port mirroring (sometimes called port spanning), allowing administrators to configure the switch to send all traffic the switch receives to a single port. After configuring a port mirror, you can use it as a tap to send all switch data to a sensor or collector and forward this to a NIDS console. Similarly, it's possible to configure port taps on routers to capture all traffic sent through the router and send it to the IDS.

Sensor and Collector Placement

The decision on where you want to place the sensors depends on what you want to measure. For example, the sensor on the Internet side of the firewall will see all the traffic. However, the sensor on the firewall's internal side will only see traffic that passes through the firewall. In other words, the firewall will filter some attacks, and the internal sensor won't see them.

If you want to see all attacks on your network, put a sensor on the Internet side. If you only want to see what gets through, put your sensors on the internal network only. If you want to see both, put sensors in both places.

Remember this

A NIDS console is installed on a network appliance. Sensors are installed on network devices such as switches, routers, or firewalls to monitor network traffic and detect network-based attacks. It can also use taps or port

mirrors to capture traffic. A NIDS cannot monitor encrypted traffic and cannot monitor traffic on individual hosts.

Detection Methods

An IDS can only detect an attack. It cannot prevent attacks. In contrast, an IPS prevents attacks by detecting them and stopping them before they reach the target. In this context, an attack is an attempt to compromise confidentiality, integrity, or availability.

The two primary detection methods are signature-based and heuristic- or behavioral-based (also called anomaly-based). Any IDS can detect attacks based on signatures, anomalies, or both. The HIDS monitors the network traffic reaching its NIC, and the NIDS monitors the network's traffic.

Signature-Based Detection

Signature-based IDSS (sometimes called definition-based) use a database of known vulnerabilities or known attack patterns. For example, tools are available for an attacker to launch a SYN flood attack on a server by simply entering the IP address of the system to attack. The attack tool then floods the target system with synchronize (SYN) packets but never completes the three-way Transmission Control Protocol (TCP) handshake with the final acknowledge (ACK) packet. If the attack isn't blocked, it can consume resources on a system and ultimately cause it to crash.

However, this is a known attack with a specific pattern of successive SYN packets from one IP to another IP. The IDS can detect these patterns when the signature database includes the attack definitions. The process is very similar to what antivirus software uses to detect malware. You need to update both IDS signatures and antivirus definitions from the vendor regularly to protect against current threats.

Heuristic/Behavioral Detection

Heuristic/behavioral-based detection (sometimes called anomaly-based detection) starts by identifying the network's regular operation or normal behavior. It does this by creating a performance baseline under normal operating conditions.

The IDS continuously monitors network traffic and compares current network behavior against the baseline. When the IDS detects abnormal activity (outside normal boundaries as identified in the baseline), it gives an alert indicating a potential attack.

Heuristic-based detection is similar to how heuristic-based antivirus software works. Although the internal methods are different, both examine activity and detect abnormal activity that is beyond the capability of signature-based detection.

SYN Flood Attack

The SYN flood attack is a common denial-of-service (DoS) attack. Chapter 3 describes the three-way handshake to establish a session. As a reminder, one system sends a SYN packet, the second system responds with a SYN/ACK packet, and the first system then completes the handshake with an ACK packet. However, in a SYN flood attack, the attacker sends multiple SYN packets but never completes the third part of the TCP handshake with the last ACK packet.

This is like a friend extending his hand to shake hands with you, you extending your hand in response, and then, at the last instant, the friend pulls his hand away. Although you or I would probably stop extending our hand back to someone doing this, the server doesn't know any better and keeps answering every SYN packet with a SYN/ACK packet.

Each uncompleted session consumes resources on the server, and if the SYN flood attack continues, it can crash the server. Some servers reserve a certain number of resources for connections, and once the attack consumes these resources, the system blocks additional connections. Instead of crashing the server, the attack prevents legitimate users from connecting to the server.

IDSs and IPSs can detect a SYN flood attack, and IPSs can prevent the attack. Additionally, many firewalls include a SYN flood guard that can detect SYN flood attacks and take steps to close the open sessions. This is different than a flood guard on a switch designed to stop MAC flood attacks, as discussed in Chapter 3.

Heuristic detection can be effective at discovering zero-day exploits. A zero-day vulnerability is usually defined as one that is unknown to the

vendor, so the vendor has not released a patch. If the vulnerability isn't known and there's no patch for it, there won't be a signature for it either.

Any time administrators make any significant changes to a system or network that cause the normal behavior to change, they should re-create the baseline. Otherwise, the IDS will constantly alert on what is now normal behavior.

Remember this

Signature-based detection identifies issues based on known attacks or vulnerabilities. Signature-based detection systems can detect known anomalies. Heuristic or behavior-based IDSSs (also called anomaly-based) can detect unknown anomalies. They start with a performance baseline of normal behavior and then compare network traffic against this baseline. When traffic differs significantly from the baseline, the system sends an alert.

Data Sources and Trends

Any type of IDS will use various raw data sources to collect network activity information. This includes a wide variety of logs, such as firewall logs, system logs, and application logs.

Chapter 1, “Mastering Security Basics,” discusses security information and event management (SIEM) systems and how they collect and aggregate information. A SIEM collects data from multiple systems and aggregates the data, making it easier to analyze. Similarly, an IDS includes an **aggregator** to store log entries from dissimilar systems. The IDS can analyze these log entries to provide insight into trends. These trends can detect a pattern of attacks and provide insight into improving a network’s protection.

Many IDSSs can monitor logs in real time. Each time a system records a log entry, the IDS examines the log to determine if it is an item of interest or not. Other IDSSs will periodically poll relevant logs and scan new entries looking for items of interest.

Reporting Based on Rules

An IDS reports on events of interest based on rules configured within the IDS. All events aren't attacks or actual issues, but instead, they provide

a report indicating an event might be an alert or an alarm. Administrators investigate to determine if it is valid. Some systems consider an alarm and an alert as the same thing. Other systems use an alarm for a potentially serious issue and an alert as a relatively minor issue. The goal in these latter systems is to encourage administrators to give higher precedence to alarms than alerts.

The actual reporting mechanism varies from system to system and in different organizations. For example, one IDS might write the event into a log as an alarm or alert, and then send an email to an administrator account. In a large network operations center (NOC), the IDS might send an alert to a monitor easily viewable by all NOC personnel. The point is that administrators configure the rules within the IDS based on the needs of the organization.

False Positives Versus False Negatives

While IDSs use advanced analytics to examine traffic, they are susceptible to false positives and false negatives. A false positive is an alert or alarm on an event that is nonthreatening, benign, or harmless. A false negative is when an attacker is actively attacking the network, but the system does not detect it. Neither is desirable, but it's impossible to eliminate both. Most IDSs trigger an alert or alarm when an event exceeds a threshold.

The following list describes the four possible responses of an IDS to an attack or perceived attack. Refer to Figure 4.2 as you're reading them:

- **False positive.** A *false positive* occurs when an IDS or IPS sends an alarm or alert when there is no actual attack.
- **False negative.** A *false negative* occurs when an IDS or IPS fails to send an alarm or alert even though an attack is active.
- **True negative.** A true negative occurs when an IDS or IPS does not send an alarm or alert, and there is no actual attack.
- **True positive.** A true positive occurs when an IDS or IPS sends an alarm or alert after recognizing an attack.

	IDS/IPS Accurate	IDS/IPS Not Accurate
No Attack	True Negative (No alarm or alert)	False Positive (Alarm or alert sent)
Actual Attack	True Positive (Alarm or alert sent)	False Negative (No alarm or alert sent)

Figure 4.2: IDS/IPS False Positives and False Negatives

Consider the classic SYN flood attack, where the attacker withholds the third part of the TCP handshake. A host will send a SYN packet and a server will respond with a SYN/ACK packet. However, instead of completing the handshake with an ACK packet, the attacking host never sends the ACK, but continues to send more SYN packets. This leaves the server with open connections that can ultimately disrupt services.

If a system receives 1 SYN packet without the accompanying ACK packet, is it an attack? Probably not. This can happen during normal operations. If a system receives over 1,000 SYN packets from a single IP address in less than 60 seconds, without the accompanying ACK packet, is it an attack? Absolutely.

Administrators configure rules within the IDS and set the threshold to a number between 1 and 1,000 to indicate an attack. If administrators set it too low, they will have too many false positives and a high workload as they spend their time chasing ghosts. If they set the threshold too high, actual attacks will get through without administrators knowing about them. Similarly, they can configure many settings based on the analytics and capabilities of the IDS.

Most administrators want to know if their system is under attack. That's the primary purpose of the IDS. However, an IDS that constantly cries "Wolf!" will be ignored when the real wolf attacks. It's important to set the threshold high enough to reduce the number of false positives but low enough to alert on any actual attacks.

There is no perfect number for the threshold. Administrators adjust thresholds in different networks based on the network's activity level and their personal preferences.

Remember this

A false positive incorrectly indicates an attack is occurring when an attack is not active. A high incidence of false positives increases the administrator's workload. A false negative is when an attack is occurring, but the system doesn't detect and report it. Administrators often set the IDS threshold high enough that it minimizes false positives but low enough that it does not allow false negatives.

IPS Versus IDS—Inline Versus Passive

Intrusion prevention systems (IPSs) are an extension of IDSs. Just as you can have both a HIDS and a NIDS, you can also have a HIPS and a NIPS, but a network-based IPS (NIPS) is more common. There are some primary distinctions of an IPS when compared with an IDS:

- An IPS can detect, react to, and prevent attacks.
- In contrast, an IDS monitors and will respond after detecting an attack, but it doesn't prevent attacks.
- An IPS is inline with the traffic. In other words, all traffic passes through the IPS, and the IPS can block malicious traffic.
- In contrast, an IDS is out-of-band. It monitors the network traffic, but the traffic doesn't go through the IDS.
- Because an IPS is inline with the traffic, it is sometimes referred to as active. In contrast, an IDS is referred to as passive because it is not inline with the traffic. Instead, it is out-of-band with the network traffic.

Most IDSs will only respond by raising alerts. For example, an IDS will log the attack and send a notification. The notification can come in many forms, including an email to a group of administrators, a text message, a pop-up window, or a notification on a central monitor.

Some IDSs have additional capabilities allowing them to change the environment in addition to sending a notification. For example, an IDS might be able to modify access control lists (ACLs) on firewalls to block offending traffic, close processes on a system that were caused by the attack, or divert the attack to a safe environment, such as a honeypot or honeynet (discussed later in this chapter).

Remember this

An IPS is placed inline with the traffic and can detect, react to, and prevent attacks. An IDS monitors and responds to an attack. It is not inline but instead collects data passively (also known as out-of-band).

As a reminder from the introduction of this section, both IDSs and IPSs have protocol analyzer capabilities. This allows them to monitor data streams looking for malicious behavior. An IPS can inspect packets within

these data streams and block malicious packets before they enter the network.

In contrast, a NIDS has sensors or data collectors that monitor and report the traffic. An active NIDS can take steps to block an attack, but only after the attack has started. The inline configuration of the IPS allows an IPS to prevent attacks from reaching the internal network. As an example, Figure 4.3 shows the location of two network-based IPSs (NIPS 1 and NIPS 2). All Internet traffic flows through NIPS 1, giving it an opportunity to inspect incoming traffic. NIPS 1 protects the internal network by detecting malicious traffic and preventing attacks from reaching the internal network.

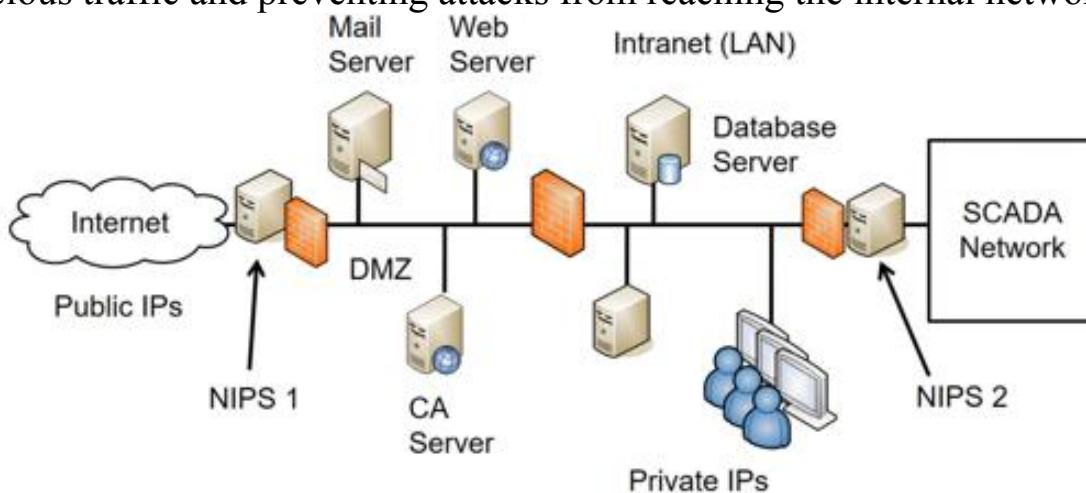


Figure 4.3: NIPS used to detect and prevent attacks

NIPS 2 is protecting an internal private network. As an example, imagine that Homer needs to manage some equipment within a supervisory control and data acquisition (SCADA) network in the nuclear power plant. The SCADA equipment is in the private network. The firewall next to NIPS 2 can have rules that allow traffic from Homer's computer into the network, but block all other traffic. NIPS 2 will then inspect all the incoming traffic and block malicious traffic.

This might seem like overkill, but many advanced persistent threats (APTs) have successfully installed remote access Trojans (RATs) onto internal systems through phishing or malware attacks. Once the RAT is installed, attackers can now attack from within. If an attacker began launching attacks on the private network from Homer's system, the firewall wouldn't block it. However, the NIPS will prevent this attack from reaching the private network.

Notice that each IPS is placed on the edge of the protected network. NIPS 1 is placed on the edge of the network between the Internet and the screened subnet. NIPS 2 is on the edge of the SCADA network between it and the intranet. This placement ensures that the NIPS can inspect all traffic going into the network.

Remember this

An intrusion prevention system (IPS) is a preventive control. It is placed inline with traffic. An IPS can actively monitor data streams, detect malicious content, and stop attacks in progress. It can also be used internally to protect private networks.

Honeypots

A **honeypot** is a sweet-looking server—at least it’s intended to look sweet to the attacker, similar to how honey looks sweet to a bear. It’s a server that is left open or appears to have been locked down sloppily, allowing an attacker relatively easy access. The intent is for the server to look like an easy target so that the attacker spends his time in the honeypot instead of in a live network. In short, the honeypot diverts the attacker away from the live network.

As an example, a honeypot could be a web server designed to look like a live web server. It would have bogus data such as files and folders containing fabricated credit card transaction data. If an organization suspects it has a problem with a malicious insider, it can create an internal honeypot with bogus information on proprietary projects.

Honeypots typically have some protection that an attacker can easily bypass. If administrators don’t use any security, the honeypot might look suspicious to experienced attackers, and they might avoid it.

Security personnel often use honeypots as a tool to gather intelligence on the attacker. Attackers are constantly modifying their methods to take advantage of different types of attacks. Some sophisticated attackers discover vulnerabilities before a patch is released (also known as a zero-day exploit or zero-day vulnerability). In some cases, security professionals observe attackers launching zero-day vulnerability attacks against a honeypot.

Honeypots never hold any data that is valuable to the organization. The data may appear to be valuable to an attacker, but its disclosure is harmless. Some goals of honeypots are:

- **Deceive the attackers and divert them from the live network.** If an attacker is spending time in the honeypot, he is not attacking live resources.
- **Allow observation of an attacker.** While an attacker is in the honeypot, security professionals can observe the attack and learn from the attacker’s methodologies. Honeypots can also help security professionals learn about zero-day exploits or previously unknown attacks.

Honeynets

A ***honeynet*** is a group of honeypots within a separate network or zone but accessible from an organization's primary network. Security professionals often create honeynets using multiple virtual servers contained within a single physical server. The servers within this network are honeypots, and the honeynet mimics the functionality of a live network.

As an example, you can use a single powerful server with a significant amount of RAM and processing power. This server could host multiple virtual servers, where each virtual server is running an operating system and applications. A physical server hosting six virtual servers will appear as seven systems on a subnet. An attacker looking in will not be able to easily determine if the servers are physical or virtual.

This virtual network aims to deceive the attacker and disrupt any attack on the actual network. If the attacker is in the honeynet, he isn't attacking the live network and administrators can observe the attacker's actions.

Sun Tzu famously wrote in *The Art of War*, "All warfare is based on deception," and "Know your enemies." Cyberwarfare is occurring daily, and security professionals on the front lines of network and system attacks recognize that these attacks mimic warfare in many ways. Honeypots and honeynets provide these professionals with some additional tools to use in this war.

Honeyfile

A honeyfile is a file designed to attract the attention of an attacker. The primary way a file can attract an attacker is by the name. As an example, a file named *password.txt* will probably contain passwords.

Experienced administrators won't be so careless with security and name a file with actual credentials *password.txt*. However, creating such a file as a honeyfile, and placing it somewhere that an attacker can find it, may deceive some attackers.

Remember this

Honeypots and honeynets attempt to deceive attackers and disrupt attackers. They divert attackers from live networks and allow security personnel to observe current methodologies attackers are using. A honeyfile is a file with a name (such as *password.txt*) that will attract the attacker's attention.

Fake Telemetry

In general, ***telemetry*** refers to collecting information such as statistical data and measurements and forwarding it to a centralized system for processing. Telemetry is used in various systems, such as water management systems, oil and gas drilling systems, natural gas delivery systems, and supervisory control and data acquisition (SCADA) systems.

Fake telemetry corrupts the data sent to monitoring systems and can disrupt a system.

As an example, many commercial and residential customers throughout the United States use natural gas to heat buildings, cook, and more. Natural gas systems use telemetry to identify the pressure of the natural gas lines. As usage rises, the pressure drops, and the delivery system automatically raises the pressure to ensure customers receive a steady stream of natural gas.

In September 2018, excessive pressure in natural gas lines caused explosions and fires in as many as 40 homes, killing one person and forcing 30,000 residents to evacuate. The National Transportation Safety Board (NTSB) reported the cause was an increase in the gas pressure (from .5 psi to 75 psi). The report indicated the problem was caused when workers replaced some low-pressure piping without including pressure sensor regulators.

The Massachusetts example shows that excessive pressure in natural gas lines can cause explosions and fires. Imagine that an attacker modifies data sent to the natural gas pressure monitoring system. If the system acts on this fake telemetry, it may turn up the pressure sent to homes and businesses and cause explosions and fires.

Securing Wireless Networks

Wireless local area networks (WLANs) have become quite popular in both home and business networks. A wireless network is easy to set up and can quickly connect several computers without running cables, which significantly reduces costs.

However, wireless networks have become a popular attack vector, and one of the challenges with wireless networks is security. Wireless security has improved over the years, but wireless networks are still susceptible to vulnerabilities, and many users don't understand how to lock down a wireless network adequately.

Reviewing Wireless Basics

Before digging into wireless security, you need to understand some basic concepts related to wireless devices and networks. If you've recently passed the CompTIA Network+ exam, these topics will likely be very familiar to you, but they are still worth looking at to ensure you understand them from the perspective of the CompTIA Security+ exam.

A wireless **access point (AP)** connects wireless clients to a wired network. However, many APs also have routing capabilities. Vendors commonly market APs with routing capabilities as wireless routers, so that's how you'll typically see them advertised. Two distinctions are:

- **All wireless routers are APs.** These are APs with an extra capability—routing.
- **Not all APs are wireless routers.** Many APs do not have any additional capabilities. They provide connectivity for wireless clients to a wired network but do not have routing capabilities.

Figure 4.4 shows a diagram of a wireless router providing connectivity to multiple systems. Notice that the wireless router has both a switch component and a router component, and the drawing at the bottom of Figure 4.4 shows the network's logical configuration. The devices connect to the switch component. The router component provides connectivity to the Internet through a broadband modem or similar device depending on the Internet Service Provider (ISP) requirements.

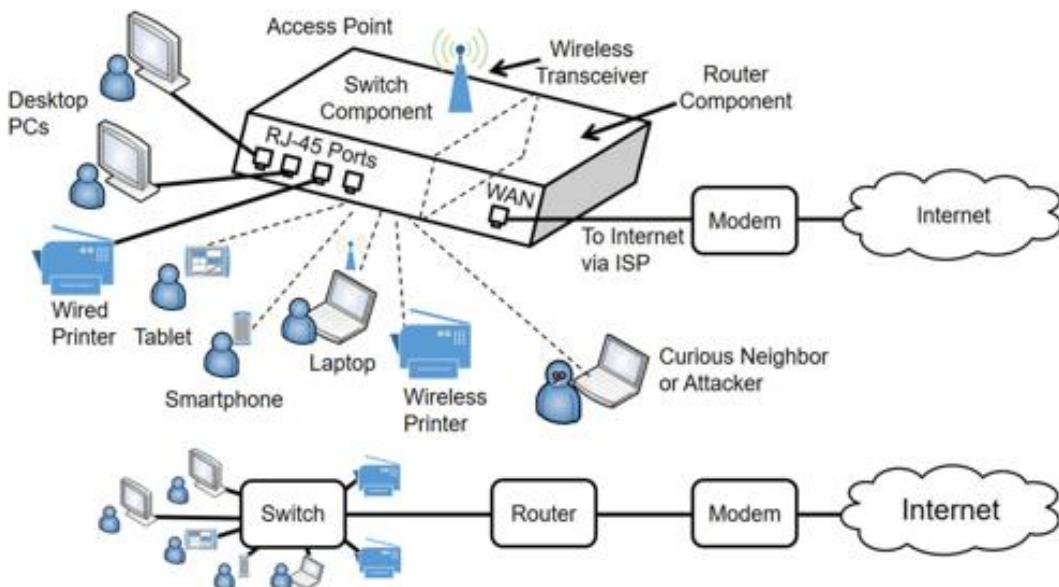


Figure 4.4: Wireless access point with routing capabilities (wireless router)

Most APs include physical ports for wired access (labeled as “RJ-45 Ports” in the diagram) and a wireless transceiver for wireless clients. In other words, some users can connect with regular twisted-pair cable, and other users can connect using wireless transmissions. The wired ports and wireless connections all connect through the switch component of the wireless router. Many vendors label the Internet connection WAN for wide area network, but some vendors label this port as “Internet.”

When used as shown in Figure 4.4, the AP also includes extra services and capabilities, such as routing, Network Address Translation (NAT), Dynamic Host Configuration Protocol (DHCP), and more. These extra services reduce the setup time required for the WLAN.

Because wireless networks broadcast on known frequency bands, other wireless users can often see them. This includes authorized users, curious neighbors, and attackers.

Band Selection and Channel Overlaps

Wireless networks use two primary radio bands: 2.4 GHz and 5 GHz. However, wireless devices don’t transmit exactly on 2.4 GHz or 5 GHz. Instead, the two bands have multiple channels starting at about 2.4 GHz and 5 GHz. In general, wireless signals travel the farthest with the 2.4-GHz frequency range, and you can get the widest bandwidth (transfer the most data) with the 5-GHz frequency. The following list shows some wireless standards along with the radio bands they use:

- 802.11b, 2.4 GHz
- 802.11g, 2.4 GHz
- 802.11n, 2.4 GHz, and 5 GHz
- 802.11ac, 5 GHz

There isn’t a single standard that applies to every country, so you’ll find that the number of channels within each band varies from country to country. Additionally, some of these channels overlap with others. As an example, Figure 4.5 shows channels in the 2.4 GHz range used by 802.11b, 802.11g, and 802.11n.

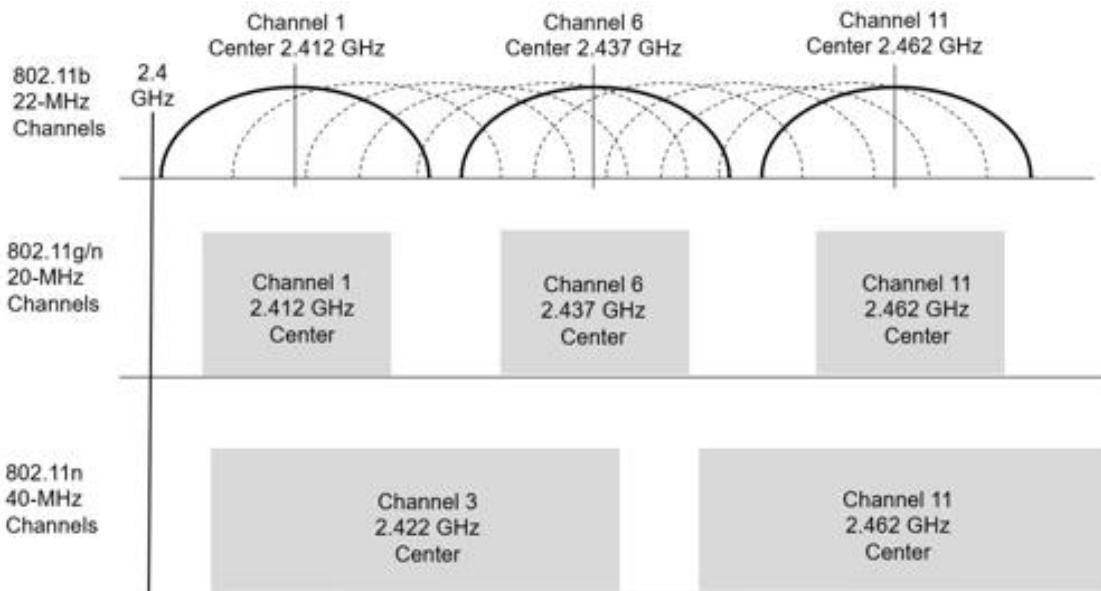


Figure 4.5: Channels and channel overlaps with 802.11 standards

It's easiest to see the channel overlaps in 802.11b. Channels 1, 6, and 11 are solid lines, while the other channels use dotted lines. Channel 1 overlaps with Channels 2 through 5, Channel 6 overlaps with Channels 2 through 10, and Channel 11 overlaps with Channels 7 through 10. Imagine a device is using Channel 6. If another wireless device is using an overlapping channel, it can impact the efficiency of the traffic on Channel 6. The other standards displayed in the figure only show some of the channels, but they also suffer from channel overlap problems.

The frequency band (2.4 GHz or 5 GHz) you select is dependent on the standard (802.11 b, g, n, or ac) you're using. Most wireless devices will automatically pick the best channel, but some devices allow you to change the channel to improve performance. As an example, if you have a wireless router in an apartment complex, you may find that Channel 6 is noisy because of other wireless routers nearby. By changing your router to Channel 1, you can improve the performance of your wireless network.

Access Point SSID

Wireless networks are identified by a service set identifier (SSID), which is simply the wireless network name. Some APs still come with default SSIDs, though most vendors have moved away from this practice. For example, the default SSID of some older Linksys APs is “Linksys.”

Some newer APs force you to enter a name for the SSID when you first install it and do not include a default. From a defense-in-depth perspective, it's a good idea to change the SSID name if it comes with a default. This practice gives attackers less information about the AP.

For example, if an attacker sees a wireless network with an SSID of Linksys, the attacker has a good idea that the network uses a Linksys AP. If the attacker knows about specific weaknesses with this AP, he can start exploiting these weaknesses. In contrast, if you gave your AP an SSID of "Success" attackers wouldn't have any clues about your AP.

Enable MAC Filtering

Chapter 3 discusses *media access control (MAC) filtering* in the context of port security for switches. You can also enable MAC filtering on many wireless routers.

The MAC address (also called a physical address or hardware address) is a 48-bit hexadecimal address used to identify network interface cards (NICs). You will usually see the MAC address displayed as six pairs of hexadecimal characters such as 00-16-EA-DD-A6-60. Every NIC, including wireless NICs, has a MAC address. Most wireless routers allow you to specify what MAC addresses to allow, and it will block all others, or you can specify what MAC addresses to block, and it will allow all others.

This might sound secure, but an attacker can easily bypass MAC filtering. Using a wireless sniffer, an attacker can identify MAC addresses allowed in a wireless network. Once he knows what MAC addresses are allowed, he can change his system's MAC address to impersonate one of the allowed MAC addresses.

Remember this

MAC filtering can restrict access to a wireless network to specific clients. However, an attacker can use a sniffer to discover allowed MAC addresses and circumvent this form of network access control. It's relatively simple for an attacker to spoof a MAC address.

MAC Cloning

MAC cloning refers to the process of changing the MAC address on a PC or other device, with the same MAC address as the wide area network

(WAN) port on an Internet-facing router. MAC cloning sometimes resolves connectivity issues on small home or office networks. In a ***MAC cloning attack*** (sometimes called a MAC spoofing attack), an attacker changes his computer's MAC address to the MAC address of an authorized system. This will bypass MAC filtering.

Site Surveys and Footprinting

Administrators often perform a site survey when planning and deploying a wireless network. The ***site survey*** examines the wireless environment to identify potential issues, such as areas with noise or other devices operating on the same frequency bands. Additionally, administrators and security personnel periodically repeat the site survey to verify that the environment hasn't changed and to detect potential security issues.

One method of performing a site survey is with a ***Wi-Fi analyzer***. Wi-Fi analyzers identify activity on channels within the wireless spectrum and analyze activity in the 2.4-GHz and 5-GHz frequency ranges. They typically allow you to analyze one frequency range at a time and see each channel's level of activity on a graph. Others will give power levels for each channel.

Other site survey tools will create a ***heat map***, which gives you a color-coded representation of wireless signals. For example, the color red may show where the wireless signals are the strongest, and the color blue may show where they are the weakest. By walking around an organization and recording wireless activity, the heat map will show where the wireless signals are the strongest and where you may have dead spots.

Figure 4.6 shows heat maps for two organizations. Organization 1 has a lot of uncovered areas, while Organization 2 has almost complete coverage of the organization.

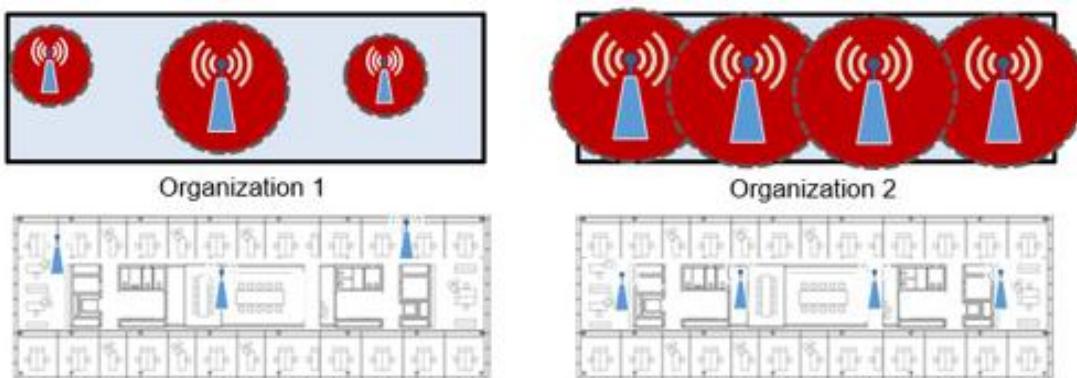


Figure 4.6: Heat map

Wireless ***footprinting*** creates a detailed diagram of APs and hotspots within an organization. By overlaying the heat map onto a basic

architectural drawing of an organization's spaces, it's possible to see the location of the APs along with dead spots and hotspots.

Remember this

A site survey examines the wireless environment to identify potential problem areas. A heat map shows wireless coverage and dead spots if they exist. Wireless footprinting gives you a detailed diagram of wireless access points, hotspots, and dead spots within an organization.

Wireless Access Point Placement

The most commonly used wireless antenna on both APs and wireless devices is an omnidirectional (or omni) antenna. Omnidirectional antennas transmit and receive signals in all directions at the same time. This allows wireless devices to connect to an AP from any direction. Another type of antenna is a directional antenna. A directional antenna transmits in a single direction and receives signals back from the same direction. Because the power of the antenna is focused in a single direction, the directional antenna has greater gain than an omni antenna, and it can transmit and receive signals over greater distances.

Data from the site survey can help administrators determine the best place to locate APs. After placing them, administrators commonly do the site survey again to verify they are getting the coverage they want.

Wireless Cryptographic Protocols

Because wireless networks broadcast over the air, anyone who has a wireless transceiver can intercept the transmissions. In the early days of wireless networks, security was an afterthought. As a result, early wireless cryptographic protocols such as Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) were weak, and attackers quickly found ways to exploit them. WEP and WPA are deprecated and should not be used. The following sections discuss current wireless cryptographic protocols.

WPA2 and CCMP

The Wi-Fi Alliance developed Wi-Fi Protected Access 2 (WPA2) to replace earlier cryptographic protocols. WPA2 (also known as IEEE 802.11i) uses strong cryptographic protocols such as Advanced Encryption Standard (AES) and Counter-mode/CBC-MAC Protocol (CCMP).

Although WPA2 provides significant security improvements over previous wireless encryption techniques, some enterprises need stronger security. Another step you can take is to enable authentication with Enterprise mode, described later in this chapter.

Open, PSK, and Enterprise Modes

WPA2 can operate in either open, *pre-shared key (PSK)*, or *Enterprise* modes. Open mode doesn't use any security. Instead, all data is transferred in cleartext, making it easy for anyone who captured it to read it.

When using **PSK** mode, users access the wireless network anonymously with a PSK or passphrase. This doesn't provide authentication. As a reminder, authentication proves a user's identity with the use of credentials such as a username and password. Users claim an identity with a username and prove their identity with a password. Just a passphrase without a username provides authorization without authentication.

Enterprise mode forces users to authenticate with unique credentials before granting them access to the wireless network. Enterprise mode uses an 802.1X server, often implemented as a RADIUS server, which accesses a database of accounts. If users don't have the proper credentials, Enterprise

mode (using an 802.1X server) blocks their access. Also, an 802.1X server can provide certificate-based authentication to increase the security of the authentication process. The authentication protocol (discussed later in this chapter) determines if the 802.1X server will use a certificate or not.

When you select Enterprise mode, you'll need to enter three pieces of information:

- **RADIUS server.** You enter the IP address assigned to the 802.1X server, which is often a RADIUS server.
- **RADIUS port.** You enter the port used by the RADIUS server. The official default port for RADIUS is 1812. However, some vendors have used other ports, such as 1645. The key is that you must enter the same port here that the server is using.
- **Shared secret.** The shared secret is similar to a password, and you must enter it here exactly as it is entered on the RADIUS server. This is different than the user's password.

After configuring WPA2 Enterprise on an AP, it redirects all attempts to connect to the RADIUS server to authenticate. After users authenticate, the RADIUS server tells the AP to grant them access.

Wireless authentication systems using an 802.1X server are more advanced than most home networks need, but many larger organizations use them. In other words, most home networks use PSK mode, but organizations that want to increase wireless security may use Enterprise mode. A combination of both a security protocol such as WPA2 and an 802.1X authentication server significantly reduces the chance of a successful access attack against a wireless system.

Remember this

WPA2-PSK uses a pre-shared key and does not provide individual authentication. Open mode doesn't use any security and allows all users to access the AP. Enterprise mode is more secure than Personal mode, and it provides strong authentication. Enterprise mode uses an 802.1X server (implemented as a RADIUS server) to add authentication.

WPA3 and Simultaneous Authentication of Equals

Wi-Fi Protected Access 3 (WPA3) is the newest wireless cryptographic protocol. It uses Simultaneous Authentication of Equals (SAE) instead of the PSK used with WPA2. SAE is a variant of the Dragonfly Key Exchange, which is based on the Diffie–Hellman key exchange (initially published in 1976). In other words, it is based on robust, time-tested cryptographic protocols.

The Wi-Fi Alliance announced in 2018 that WPA3 is a replacement for WPA2. Hardware that supports WPA2 should support WPA3, but it is up to vendors to write the firmware to perform upgrades. In addition to providing better security than WPA2 with a PSK, it also offers better security when setting up new devices with Wi-Fi Protected Setup (WPS), discussed later in this chapter.

WPA3 also supports Enterprise mode. While it improves security over WPA2 Enterprise mode, WPA3 Enterprise still uses a RADIUS server and requires users to authenticate.

Remember this

WPA2 supports CCMP (based on AES) and replaced earlier wireless cryptographic protocols. WPA3 uses Simultaneous Authentication of Equals (SAE) instead of a pre-shared key (PSK) used with WPA2.

Authentication Protocols

Wireless networks support several different authentication protocols. Many are built on the Extensible Authentication Protocol (EAP), an authentication framework that provides general guidance for authentication methods. IEEE 802.1X servers typically use one of these methods to increase the level of security during the authentication process.

Additionally, while they are often used in wireless networks, they can also be used anywhere an 802.1X server is implemented.

A key point to remember for each of these methods is if they support or require certificates. Some methods are:

- **EAP.** EAP provides a method for two systems to create a secure encryption key, also known as a Pairwise Master Key (PMK). Systems then use this key to encrypt all data transmitted between the devices. AES-based CCMP uses this key.
- **Protected EAP (PEAP).** PEAP provides an extra layer of protection for EAP. The EAP designers assumed that EAP would be used with adequate physical security to ensure the communication channel was secure. That wasn't always the case in practice, but PEAP protects the communication channel by encapsulating and encrypting the EAP conversation in a Transport Layer Security (TLS) tunnel. PEAP requires a certificate on the server but not on the clients. A common implementation is with Microsoft Challenge Handshake Authentication Protocol version 2 (MS-CHAPv2).
- **EAP-FAST.** Cisco designed EAP-Flexible Authentication via Secure Tunneling (EAP-FAST) as a secure replacement for Lightweight EAP (LEAP) that Cisco also designed. EAP-FAST supports certificates, but they are optional.
- **EAP-TLS.** EAP-Transport Layer Security (EAP-TLS) is one of the most secure EAP standards. The primary difference between PEAP and EAP-TLS is that EAP-TLS requires certificates on the 802.1X server and the clients.
- **EAP-TTLS.** EAP-Tunneled TLS (EAP-TTLS) is an extension of PEAP, allowing systems to use some older authentication methods

- such as Password Authentication Protocol (PAP) within a TLS tunnel. EAP-TTLS requires a certificate on the 802.1X server but not the clients.
- **RADIUS Federation.** Chapter 2, “Understanding Identity and Access Management,” covers federations used for single sign-on (SSO). As a reminder, a federation includes two or more entities (such as companies) that share the same identity management system. Users can log on once, and access shared resources with the other entity without logging on again. Similarly, it’s possible to create a federation using 802.1X and RADIUS servers.

Note that EAP-FAST supports digital certificates, but they are optional. PEAP and EAP-TTLS require a certificate on the server, but not the clients. EAP-TLS requires certificates on both the server and the clients. Chapter 10, “Understanding Cryptography and PKI,” digs into certificates much deeper, but as an introduction, certificates help provide strong authentication and encryption services. However, a certificate authority (CA) must issue certificates, so an organization must either purchase certificates from a public CA or implement a private CA within the network.

Remember this

Enterprise mode requires an 802.1X server. EAP-FAST supports certificates. PEAP and EAP-TTLS require a certificate on the 802.1X server. EAP-TLS also uses TLS, but it requires certificates on both the 802.1X server and each of the clients.

IEEE 802.1X Security

Chapter 3 discusses port security by disabling unused ports or using MAC address filtering. Another method of port security is to use ***IEEE 802.1X***, a port-based authentication protocol. It requires users or devices to authenticate when they connect to a specific wireless access point or a specific physical port. Administrators implement it in both wireless and wired networks, and can also use it with virtual private networks (VPNs) described later in this chapter.

It secures the authentication process prior to a client gaining access to a network and blocks network access if the client cannot authenticate. 802.1X can use simple usernames and passwords for authentication, or certificates for certificate-based authentication.

The 802.1X server prevents rogue devices from connecting to a network. Consider open RJ-45 wall jacks. Although disabling them is a good port security practice, you can also configure an 802.1X server to require authentication for these ports. If clients cannot authenticate, the 802.1X server blocks or restricts access to the network.

It's possible to combine an 802.1X server with other network elements such as a virtual local area network (VLAN). For example, imagine you want to provide visitors with Internet access but prevent them from accessing internal network resources. You can configure the 802.1X server to grant full access to authorized clients but redirect unauthorized clients to a guest area of the network via a VLAN.

You can implement 802.1X as a Remote Authentication Dial-In User Service (RADIUS) or Diameter server, as discussed later in this chapter. This helps authenticate virtual private network (VPN) clients before they connect. You can also implement 802.1X in wireless networks to force wireless clients to authenticate before they connect.

RFC 3580, “IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines,” describes IEEE 802.1X in much greater detail in case you want to dig deeper.

Remember this

An 802.1X server provides port-based authentication, ensuring that only authorized clients can connect to a device or a network. It prevents rogue devices from connecting.

Controller and Access Point Security

After doing a site survey and determining the best location for APs, it's also important to consider physical security. If attackers can access an AP, they can connect unauthorized devices to them to collect network traffic. It's also possible for attackers to reset the AP to factory settings, effectively removing access to the network for everyone using the AP. Additionally, it's important to use newer cryptographic protocols such as WPA2 and WPA3. Older deprecated wireless protocols such as WEP and WPA should not be used.

Captive Portals

A ***captive portal*** is a technical solution that forces clients using web browsers to complete a specific process before it allows them access to the network. Organizations commonly use it as a hotspot that requires users to log on or agree to specific terms before they can access the Internet. Here are three common examples:

- **Free Internet access.** Many hospitals and other medical facilities provide free Internet access to patients and visitors. The captive portal requires users to acknowledge and agree to abide by an acceptable use policy (AUP). Free captive portals rarely require users to log on but instead, just require them to check a box indicating they agree and then click a button to continue.
- **Paid Internet access.** Many hotels, resorts, cruise ships, and airlines provide Internet access to customers, but on a pay-as-you-go basis. When users attempt to access the Internet, they are redirected to the captive portal. They must successfully log on with a pre-created account or enter credit card information to pay for access.
- **Alternative to IEEE 802.1X.** Adding an 802.1X server can be expensive and is sometimes not a feasible option. Organizations can use captive portals as an alternative. It requires users to authenticate before granting them access.

Understanding Wireless Attacks

There are several known attacks against wireless networks. Most can be avoided by using strong security protocols such as WPA2 with CCMP. In contrast, WPA is vulnerable to many attacks, especially if it is using TKIP.

Disassociation Attacks

A ***disassociation attack*** effectively removes a wireless client from a wireless network. It's easier to understand this attack if you understand the normal operation of wireless devices and wireless APs.

After a wireless client authenticates with a wireless AP, the two devices exchange frames, causing the client to be associated with the AP. At any point, a wireless device can send a disassociation frame to the AP to terminate the connection. This frame includes the wireless client's MAC address. When the AP receives the disassociation frame, it deallocates all its memory for the connection.

In a disassociation attack, attackers send a disassociation frame to the AP with a spoofed MAC address of the victim. The AP receives the frame and shuts down the connection. The victim is now disconnected from the AP and must go through the authentication process again to reconnect.

Interestingly, some hotels used this attack to prevent guests from using their own personal wireless networks. For example, if you have an iPhone with cellular access to the Internet, you can enable the Personal Hotspot feature. This lets you share the connection with other devices, such as a laptop. Some hotels looked for these personal wireless networks and launched disassociation attacks against them. Customers were forced to pay for the hotel's wireless services if they needed reliable Internet access.

Wi-Fi Protected Setup

Wi-Fi Protected Setup (WPS) allows users to configure wireless devices without typing in the passphrase. Instead, users can configure devices by pressing buttons or by entering a short eight-digit personal identification number (PIN).

For example, a user can configure a new wireless device by pressing a button on the AP and on the wireless device. It will automatically configure the device within about 30 seconds with no other actions needed. These buttons can be physical buttons on the devices or virtual buttons that the user clicks via an application or webpage. When using the PIN method, users first identify the eight-digit PIN on the AP and then enter the PIN on the new wireless device.

Unfortunately, WPS is susceptible to brute force attacks. A WPS attack keeps trying different PINs until it succeeds. For example, Reaver is an open source tool that allows attackers to discover the PIN within about 10 hours and often much quicker. Once it discovers the PIN, it can then discover the passphrase in WPA2 wireless networks. However, WPS is safe if it is used with WPA3.

Security experts recommend disabling WPS on all devices. This is typically possible via the AP configuration page. Even if you choose to enable WPS to easily connect some devices, you should immediately turn it off once you're done.

Remember this

A disassociation attack effectively removes a wireless client from a wireless network, forcing it to reauthenticate. WPS allows users to easily configure a wireless device by entering an eight-digit PIN. A WPS attack guesses all possible PINs until it finds the correct one. It will typically discover the PIN within hours and use it to discover the passphrase.

Rogue Access Point

A *rogue access point* (rogue AP) is an AP placed within a network without official authorization. It might be an employee who is bypassing security or installed by an attacker. If an employee installs a rogue AP, the chances are higher that this AP will not be adequately managed, increasing vulnerabilities to the network. This is an example of shadow IT described in Chapter 6, “Comparing Threats, Vulnerabilities, and Common Attacks.”

Generically, you can think of a rogue as a scoundrel, a crook, or a villain. Clearly, if a rogue is a crook or villain, then rogue access points are not an administrator’s friend. You might also see them called counterfeit access points, which is also a clear indication they aren’t legitimate.

Attackers may connect a rogue access point to network devices in wireless closets that lack adequate physical security. This access point acts as a sniffer to capture traffic passing through the wired network device and then broadcasts the traffic using the AP’s wireless capability. The attacker can then capture the exfiltrated data files while sitting in the parking lot. Data exfiltration is the unauthorized transfer of data from an organization to a location controlled by an attacker.

Additionally, attackers may be able to use the rogue access point to connect to the wired network. This works the same way that regular users can connect to a wired network via a wireless network. The difference is that the attacker configures all the security for the counterfeit access point and can use it for malicious purposes.

If you discover an unauthorized AP, you should disconnect it as quickly as possible. A basic first step to take when you discover any attack is to contain or isolate the threat. By simply unplugging the Ethernet cable, you can stop the unauthorized AP from capturing network traffic.

Evil Twin

An ***evil twin*** is a rogue access point with the same SSID (or similar) as a legitimate access point. You can think of the SSID of the evil twin as a twin of the legitimate AP's SSID. For example, many public places such as coffee shops, hotels, and airports include free Wi-Fi as a service. An attacker can set up an AP using the same SSID as the public Wi-Fi network, and many unsuspecting users will connect to this evil twin.

Some people have trouble differentiating the difference between rogue access points and evil twins. If you compare them to two twins, it may be clearer. Imagine Sherri and Terri are identical twins. Which of the following MOST accurately describes them? Twins or sisters? The answer is twins because it is the most accurate description. Yes, they are sisters, but all sisters are not twins.

Once a user connects to an evil twin, wireless traffic goes through the evil twin instead of the legitimate AP. Often, the attacker presents bogus login pages to users to capture usernames and passwords. Other times, they simply capture traffic from the connection, such as email or text typed into webpage text boxes, and analyze it to detect sensitive information they can exploit.

Although it might sound complex to set up an evil twin, it's rather easy. Attackers can configure a laptop that has a wireless access card as an AP. With it running, the attackers look just like any other user in a coffee shop or airport waiting area. They'll have their laptop open and appear to be working (just like you perhaps), and you'll have no idea they are trying to steal your credentials or other personal data that you send over the Internet via the evil twin. Similarly, attackers can set one up in a parking lot or another location close to an organization and try to trick employees or visitors.

Often, administrators will use wireless scanners to perform site surveys. In addition to detecting noise on frequency bands, they can also detect rogue APs, including evil twins. The site survey can help them identify access points' physical locations because the signal will get stronger as the administrator gets closer.

Remember this

Rogue access points are often used to capture and exfiltrate data. An evil twin is a rogue access point using the same SSID (or a similar SSID) as a legitimate access point. A secure AP blocks unauthorized users, but a rogue access point provides access to unauthorized users.

Jamming Attacks

Attackers can transmit noise or another radio signal on the same frequency used by a wireless network. This interferes with the wireless transmissions and can seriously degrade performance. This type of denial-of-service attack is commonly called ***jamming***, and it usually prevents all users from connecting to a wireless network. In some cases, users have intermittent connectivity because the interference causes them to lose their association with the AP and forces them to reconnect.

In some cases, you can increase the power levels of the AP to overcome the attack. Another method of overcoming the attack is to use different wireless channels. Each wireless standard has several channels you can use, and if one channel is too noisy, you can use another one. Although this is useful to overcome interference in home networks, it won't effectively combat an interference attack. If you switch channels, the attacker can also switch channels.

IV Attacks

An initialization vector (IV) is a number used by encryption systems, and a wireless IV attack attempts to discover the pre-shared key after first discovering the IV. Some wireless protocols use an IV by combining it with the pre-shared key to encrypt data in transit. When an encryption system reuses the same IV, an ***IV attack*** can discover the IV easily. As an example, WEP, an early wireless security protocol, uses a relatively small 24-bit number for the IV. This small IV resulted in wireless networks reusing keys, making WEP easy to crack.

In many IV attacks, the attacker uses packet injection techniques to add additional packets into the data stream. The AP responds with more packets, increasing the probability that it will reuse a key. An IV attack using packet injection decreases the time it takes to crack a WEP key. It's worth repeating that WEP has been deprecated and should not be used.

Near Field Communication Attacks

Near field communication (NFC) is a group of standards used on mobile devices that allow them to communicate with other mobile devices when they are close to them. For example, you can share pictures, contacts, and other data with friends. One person shares the data, and after placing the smartphones close to each other, the other person selects it to download.

Many point-of-sale card readers support NFC technologies with credit cards. Instead of swiping your card or inserting it to read the chip data, you wave your card over the reader. It is often advertised as a contactless payment method. Some smartphone applications support payments with NFC-enabled smartphones. Users wave their smartphones over the reader to make a payment.

During a ***near field communication*** attack, an attacker uses an NFC reader to capture data from another NFC device. One method is an eavesdropping attack. The NFC reader uses an antenna to boost its range and intercepts the data transfer between two other devices. For example, imagine Marge is making a purchase at a store, and Bart is behind her with his own NFC reader. If Bart can boost the receiving range of his NFC reader, he can capture Marge's transaction. The primary indication of an NFC attack is unauthorized charges on a credit card statement.

RFID Attacks

Radio-frequency identification (RFID) systems include an RFID reader and RFID tags placed on objects. They are used to track and manage inventory, and any type of valuable assets, including objects and animals.

There's an almost endless assortment of tags available for multiple purposes. This includes tags implanted into animals, packaging for any type of product (such as computers), pharmaceuticals, transportation systems (such as shipping containers, railcars, and busses), and controlled substances (such as pharmaceutical containers). Some tags are only slightly larger than a grain of rice.

Tags do not have a power source. Instead, they include electronics that allow them to collect and use power to transmit data stored on the device. This is similar to how a proximity card (described in Chapter 9, “Implementing Controls to Protect Assets”) receives a charge from a proximity card reader and then transmits data to the reader. One difference is that RFID transmitters can send to and from tags from a much greater distance than proximity readers.

Some of the common RFID attacks are:

- **Sniffing or eavesdropping.** Because RFID transmits data over the air, an attacker can collect it by listening. A key requirement is to know the RFID system's frequency and have a receiver tuned to that frequency. The attacker also needs to know the protocols used by the RFID system to interpret the data.
- **Replay.** Successful eavesdropping attacks allow the attacker to perform a replay attack. For example, an attacker can configure a bogus tag to mimic the tag attached to a valuable object. The attacker can then steal the valuable object without the theft being easily detected.
- **DoS.** A denial-of-service (DoS) attack attempts to disrupt services. If an attacker knows the RFID system's frequency, it's possible to launch a jamming or interference attack, flooding the frequency with noise. This prevents the RFID system from operating normally.

Bluetooth Attacks

Bluetooth is a short-range wireless system used in personal area networks (PANs) and within networks. A PAN is a network of devices close to a single person. Bluetooth devices include smartphones, headsets, and computer devices.

The Bluetooth range was designed initially for about three meters (about 10 feet), but the range is often farther and ultimately extends beyond a person's personal space. Attackers have discovered methods of exploiting these networks. Some common attacks are bluejacking, bluesnarfing, and bluebugging:

- ***Bluejacking*** is the practice of sending unsolicited messages to nearby Bluetooth devices. Bluejacking messages are typically text but can also be images or sounds. Bluejacking is relatively harmless but does cause some confusion when users start receiving messages.
- ***Bluesnarfing*** refers to the unauthorized access to, or theft of information from, a Bluetooth device. A bluesnarfing attack can access information, such as email, contact lists, calendars, and text messages.
- ***Bluebugging*** is like bluesnarfing, but it goes a step further. In addition to gaining full access to the phone, the attacker installs a backdoor. The attacker can have the phone call the attacker at any time, allowing the attacker to listen in on conversations within a room. Attackers can also listen in on phone conversations, enable call forwarding, send messages, and more.

When Bluetooth devices are first configured, they are configured in Discovery mode. Bluetooth devices use MAC addresses, and in Discovery mode, the Bluetooth device broadcasts its MAC address, allowing other devices to see it and connect to it. This is required when pairing Bluetooth devices.

In earlier versions of Bluetooth, this pairing process could happen any time a device is in Discovery mode. However, most software vendors have rewritten their software to prevent this. Today, users typically manually pair the device. If a user doesn't acknowledge an attempted pairing, it fails. As a

result, Bluetooth attacks are rare today. However, if a device doesn't require a user to pair a device manually, it is still susceptible to these attacks. Also, by placing devices into conductive metal lockboxes that act as a Faraday cage, it blocks Bluetooth attacks.

Remember this

Bluejacking is the unauthorized sending of text messages to a nearby Bluetooth device. Bluesnarfing is the unauthorized access to, or theft of information from, a Bluetooth device. Ensuring devices cannot be paired without manual user intervention prevents these attacks, and placing them in Faraday cages will prevent pairing.

Wireless Replay Attacks

In a replay attack, an attacker captures data sent between two entities, modifies it, and then attempts to impersonate one of the parties by replaying the data. Chapter 7, “Protecting Against Advanced Attacks,” covers replay attacks in a wired network. A wireless replay attack is similar. However, WPA2 and WPA3 are resistant to replay attacks. The best protection is to eliminate the use of deprecated wireless cryptographic protocols.

War Driving and War Flying

War driving is the practice of looking for a wireless network. Although war driving is more common in cars, you can just as easily do it by walking around in a large city. Attackers use war driving to discover wireless networks that they can exploit and often use directional antennas to detect wireless networks with weak signals.

Administrators sometimes use war driving as part of a wireless audit. A wireless audit is a detective control and examines the signal footprint, antenna placement, and encryption of wireless traffic. These audits are useful at detecting weaknesses in wireless networks. For example, administrators can sometimes detect the existence of rogue access points and evil twins by war driving, and determine when their WAP's footprint extends too far.

War flying is similar to war driving. However, instead of walking or driving around, people fly around in private planes. In some cases, people have intercepted wireless transmissions at altitudes of 2,500 feet. Most of these transmissions are using 2.4 GHz, which can travel farther than 5-GHz signals. Additionally, there isn't much interference between the access points and the planes. However, planes quickly move out of range of access points because they are flying.

An alternative to a plane is a drone. An aircraft drone's technical definition is any aircraft that can fly on its own without a human in control. However, people commonly think of a drone as any aircraft controlled by remote control instead of an onboard pilot. By adding a little hardware, a drone can look for wireless networks.

It's also possible for attackers to use drones for reconnaissance. Chapter 8 discusses reconnaissance in the context of penetration testing. Pentesters use a variety of methods to collect information on targeted systems. They can also use drones to collect pictures of a target and scan for wireless networks.

Remember this

Administrators use war driving techniques as part of a wireless audit. A wireless audit checks a wireless signal footprint, power levels, antenna placement, and encryption of wireless traffic. Wireless audits using war

driving can detect rogue access points and identify unauthorized users. War flying is similar to war driving, but it uses planes or drones instead of cars.

Using VPNs for Remote Access

A *virtual private network (VPN)* is often used for remote access. Direct access VPNs allow users to access private networks via a public network. The public network is most commonly the Internet, but it can also be a semiprivate leased line from a telecommunications company. Because the telecommunications company will often lease access to one physical line to several companies, the leased line is not truly private.

Access over a public network is a core security concern with VPNs. With more people working from home and connecting to company networks via direct access VPNs, these VPNs have become a popular attack vector. Different tunneling protocols encapsulate and encrypt the traffic to protect the data from unauthorized disclosure. The tunnel prevents anyone from reading the data transferred through it.

VPNs and VPN Appliances

It's possible to create a VPN by enabling services on a server. For example, if you have a Windows server, you can enable the Direct Access VPN role and configure the Routing and Remote Access console. The only additional hardware requirement is that the server has two network interface cards (NICs). One NIC is accessible from the Internet, and the second NIC provides access to the private network. If you are only supporting a few VPN clients, this might be the perfect solution.

Larger organizations often use a VPN appliance, which is a dedicated device used for VPNs. A VPN appliance includes all the services needed to create a VPN, including strong encryption and authentication techniques, and it supports many clients.

When using a VPN appliance, you would typically place it in the screened subnet. The firewall between the Internet and the screened subnet would forward VPN traffic to the VPN appliance. The VPN appliance would route all private VPN traffic to the firewall between the screened subnet and the intranet.

Remember this

A virtual private network (VPN) provides remote access to a private network via a public network. VPN appliances are dedicated devices used for VPNs. They include all the services needed to create a secure VPN supporting many clients.

Remote Access VPN

Figure 4.7 shows an example of how users can connect to internal networks from remote locations. You may see this referenced as a remote access VPN or a direct access VPN. The VPN client first connects to the Internet using a broadband connection to an Internet Service Provider (ISP). After connecting to the Internet, the VPN client can then initiate the VPN connection.

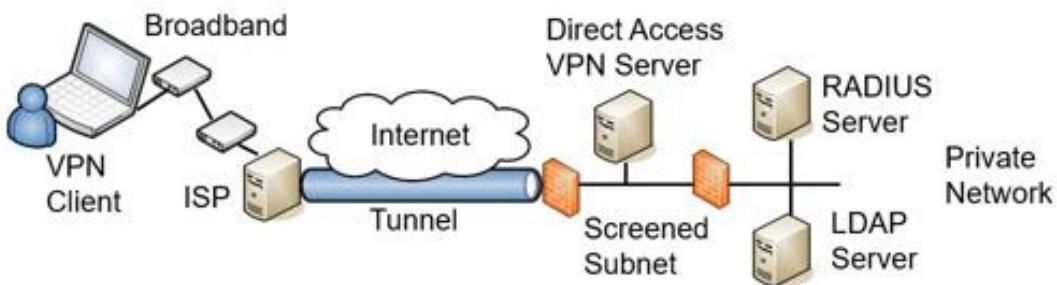


Figure 4.7: Connecting to a VPN server

The VPN server is in the screened subnet and reachable through a public IP address. This makes it accessible from any other host on the Internet. A VPN server needs to authenticate clients, and a common method is to use an internal Remote Authentication Dial-in User Service (RADIUS) server. When a user logs on, the VPN server sends the user's credentials to the RADIUS server.

While the RADIUS server might have a database of users and passwords, it's more common for it to pass the credentials on to another server to validate them. For example, the RADIUS server can pass the credentials on to a Lightweight Directory Access Protocol (LDAP) server during the authentication process. In a Microsoft domain, the LDAP server is a domain controller.

IPsec as a Tunneling Protocol

Chapter 3 introduces Internet Protocol security (IPsec) as a method of encrypting data in transit. IPsec supports both Tunnel mode and Transport mode.

Tunnel mode encrypts the entire IP packet, including both the payload and the packet headers, and VPNs commonly use Tunnel mode. Packet

headers include IP addresses and MAC addresses. A benefit of using Tunnel mode is that the IP addressing used within the internal network is encrypted and not visible to anyone who intercepts the traffic. If attackers do intercept the traffic, they can see the source IP address from the client and the destination address to the VPN server, but the internal IP address information remains hidden.

Transport mode only encrypts the payload and is commonly used in private networks, but not with VPNs. If traffic is transmitted and used only within a private network, there isn't any need to hide the IP addresses by encrypting them.

IPsec provides security in two ways:

- **Authentication.** IPsec includes an Authentication Header (AH) to allow each of the IPsec conversation hosts to authenticate with each other before exchanging data. AH provides authentication and integrity. AH uses protocol number 51.
- **Encryption.** IPsec includes Encapsulating Security Payload (ESP) to encrypt the data and provide confidentiality. ESP includes AH so it provides confidentiality, authentication, and integrity. ESP uses protocol number 50.

The term protocol number might look like a typo, but it isn't. AH and ESP are identified with protocol numbers, not port numbers. Chapter 3 discusses routers and firewalls. You may remember from Chapter 3 that a basic packet-filtering firewall can filter packets based on IP addresses, ports, and some protocols, such as Internet Control Message Protocol (ICMP) and IPsec. Packet filters use the protocol numbers to identify AH and ESP traffic.

IPsec uses Internet Key Exchange (IKE) over port 500 to authenticate clients in the IPsec conversation. IKE creates security associations (SAs) for the VPN and uses these to set up a secure channel between the client and the VPN server.

SSL/TLS as a Tunneling Protocol

Some tunneling protocols use Transport Layer Security (TLS) to secure the VPN channel. As an example, Secure Socket Tunneling Protocol (SSTP) encrypts VPN traffic using TLS over port 443. Using port 443 provides a lot of flexibility for many administrators and rarely requires

opening additional firewall ports. It is a useful alternative when the VPN tunnel must go through a device using NAT, and IPsec is not feasible. OpenVPN and OpenConnect are two open source applications that can use TLS to create a secure channel.

While this can also use Secure Sockets Layer (SSL), SSL has known weaknesses, and TLS is the designated replacement. Even though SSL is rarely, if ever, used today, you'll still see it referenced. For example, SSTP indicates it uses SSL, but it actually uses TLS.

Split Tunnel Versus Full Tunnel

Imagine that Lisa connects to a company VPN server using IPsec from her home computer. The VPN is using ESP, so all traffic in the tunnel is encrypted. Now, Lisa wants to do an Internet search on saxophones. Will her computer connect directly to the Internet for her search? Or will her computer make a connection through the VPN server first? It depends on the VPN's configuration.

In a *split tunnel*, a VPN administrator determines what traffic should use the encrypted tunnel. For example, it's possible to configure the tunnel to encrypt only the traffic going to private IP addresses used within the private network. If Lisa did an Internet search with the VPN server configured in a split tunnel configuration, her Internet search traffic would not go through the encrypted tunnel. Instead, her search would go directly to Internet sites via her ISP.

In a *full tunnel*, all traffic goes through the encrypted tunnel while the user is connected to the VPN. If Lisa was connected to the VPN and then tried to connect to a public website, the traffic would first go through the encrypted tunnel and then out to the public website from within the private network. If the private network routed Internet traffic through a unified threat management (UTM) device, Lisa's traffic would go through the organization's UTM device. The website would send webpages back to the UTM device, and the VPN server would encrypt it and send it back to Lisa via the encrypted tunnel.

Chapter 3 discusses UTM devices. A UTM device can perform URL filtering, malware inspection, and content inspection of all traffic sent through it. This is one reason why an organization may choose to use a full tunnel for users connected to a VPN server. A disadvantage is that it can be

slow. Not only is the Internet traffic taking an indirect route through the VPN server, but it's also being encrypted and decrypted a couple of times.

Remember this

IPsec is a secure encryption protocol used with VPNs. Encapsulating Security Payload (ESP) provides confidentiality, integrity, and authentication for VPN traffic. IPsec uses Tunnel mode for VPN traffic and can be identified with protocol ID 50 for ESP. It uses IKE over port 500. A full tunnel encrypts all traffic after a user has connected to a VPN. A split tunnel only encrypts traffic destined for the VPN's private network.

Site-to-Site VPNs

A site-to-site VPN includes two VPN servers that act as gateways for two networks separated geographically. For example, an organization can have two locations. One is its headquarters, and the other is a remote office. It can use two VPN servers to act as gateways to connect the two locations together, as shown in Figure 4.8.

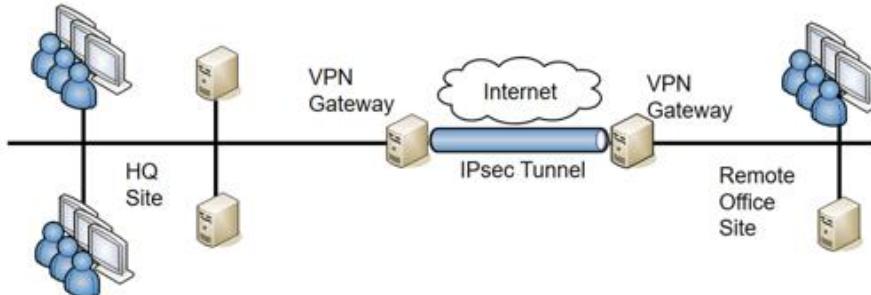


Figure 4.8: Site-to-site VPN

The site-to-site model's benefit is that it connects both networks without requiring additional steps on the part of the user. Users in the remote office can connect to servers in the headquarters location as easily as if the servers were in the remote office. Connecting to the remote server might be slower than connecting to a local server, but otherwise, it's transparent to end users.

In contrast, in a traditional remote access VPN (also called a host-to-gateway model), the end user makes the direct connection to the VPN server and is very much aware of the process.

Always-On VPN

Some VPNs are ***always-on VPNs***. They can be used with both site-to-site VPNs and direct access VPNs. When used with a site-to-site VPN, the two VPN gateways maintain the VPN connection. In contrast, some site-to-site VPNs use an on-demand connection. The VPN connection is established when it's needed, such as when a user connects to a remote system.

Several vendors have always-on VPNs for direct access VPNs. They attempt to create a VPN connection as soon as the user's device connects to the Internet. For a home user, this might be right after the user turns on a desktop PC or laptop computer.

When configured on mobile devices, such as cell phones, the device will connect to the always-on VPN anytime the device connects to an Internet connection. For example, if a user visits a coffee shop with free Internet access and the user connects to the network, the device will automatically connect to the always-on VPN.

L2TP as a Tunneling Protocol

Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol that is also used for VPNs. The most recent version is L2TPv3. However, none of the L2TP versions provide any encryption, so it is not used by itself for VPN traffic. Instead, data is encrypted with another protocol, such as IPsec, and then passed to L2TP for transport over the VPN.

HTML5 VPN Portal

Some network devices include the ability to configure an HTML5 VPN portal. An HTML5 VPN allows users to connect to the VPN using their web browser, making it rather simple for the users. It uses TLS to encrypt the session, but it can be very resource-intensive. In general, organizations use it to give one or two users access to limited resources. As an example, if a consultant managed a Voice over IP (VoIP) private branch exchange (PBX), an organization could use an HTML5 VPN to give this consultant access to the PBX. However, the other employees would use a traditional VPN for remote access.

Network Access Control

Allowing remote access to your private network can expose your network to many risks from the clients. If a user logs on to a VPN with a malware-infected computer, this computer can then infect other computers on the internal network. ***Network access control (NAC)*** methods provide continuous security monitoring by inspecting computers and preventing them from accessing the network if they don't pass the inspection.

Most administrators have complete control over computers in their network. For example, they can ensure desktop computers have up-to-date antivirus software installed, operating systems have current patches applied, and their firewalls are enabled. However, administrators don't have complete control of computers that employees use at home or on the road.

NAC provides a measure of control for these other computers. It ensures that clients meet predetermined characteristics before accessing a network. NAC systems often use health as a metaphor, indicating that a client meets these predetermined characteristics. Just as doctors can quarantine patients with certain illnesses, NAC can quarantine or isolate unhealthy clients that don't meet the predefined NAC conditions.

Host Health Checks

Administrators set predefined conditions for healthy clients, and those that meet these preset conditions can access the network. The NAC system isolates computers that don't meet the conditions. Common health conditions checked by a NAC are:

- The client's firewall is enabled.
- The client's operating system is up to date and has all current patches and fixes.
- The client's antivirus software is up to date and has all updated signature definitions.

NAC systems use authentication agents (sometimes called health agents) to inspect NAC clients. These ***agents*** are applications or services that check different computer conditions and document the status in a statement of health. When a client connects to a NAC-controlled network, the agent reports the NAC client's health status.

Consider Figure 4.9. When a VPN client accesses the network, the VPN server queries the NAC health server to determine required health conditions. The VPN server also queries the client for a statement of the client's health. If the client meets all health requirements, the NAC system allows the client to access the network.

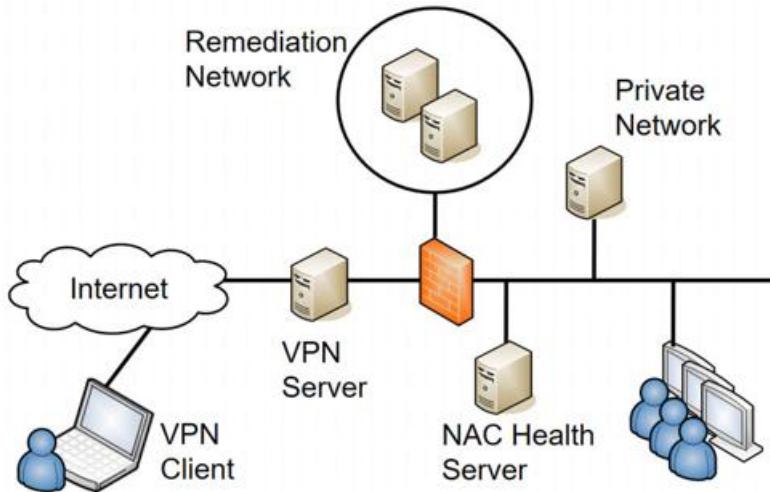


Figure 4.9: Using network access control

However, if a client doesn't meet the health conditions mandated by the NAC server, the VPN server redirects the client to a remediation network (also called a quarantine network). The remediation network includes resources the client can use to get healthy. For example, it would include currently approved patches, antivirus software, and updated virus signatures. The client can use these resources to improve its health and then try to access the network again.

While NAC can inspect the health of VPN clients, you can also use it to inspect the health of internal clients. For example, internal computers may occasionally miss patches and be vulnerable. NAC will detect the unpatched system and quarantine it. If you use this feature, it's important that the detection is accurate. A false positive by the NAC system can quarantine a healthy client and prevent it from accessing the network.

Similarly, your organization may allow visitors or employees to plug in their mobile computers to live wall jacks for connectivity or connect to a wireless network. NAC inspects the clients, and if they don't meet health conditions, they may be granted Internet access through the network but remain isolated from any other network activity.

Agent Versus Agentless NAC

Agents on clients can be either permanent or dissolvable. A permanent agent (sometimes called a persistent NAC agent) is installed on the client and stays on the client. NAC uses the agent when the client attempts to log on remotely.

A dissolvable agent is downloaded and runs on the client when the client logs on remotely. It collects the information it needs, identifies the client as healthy or not healthy, and reports the status back to the NAC system. Some dissolvable NAC agents remove themselves immediately after they report back to the NAC system. Others remove themselves after the remote session ends. Many NAC vendors refer to dissolvable agents as an agentless capability, though this is somewhat of a misnomer. The NAC is still using an agent to inspect the client, but it is not installing the agent on the client.

An agentless NAC system scans a client remotely without installing code on the client, either permanently or temporarily. This is similar to how vulnerability scanners scan network systems looking for vulnerabilities. Chapter 8 explores vulnerability scanners in more depth.

Remember this

Network access control (NAC) includes methods to inspect clients for health, such as having up-to-date antivirus software, and can restrict access of unhealthy clients to a remediation network. You can use NAC for VPN clients and internal clients.

Authentication and Authorization Methods

An important step when implementing a VPN is to ensure only authorized entities can access it. Authorization begins with authentication, and VPNs support multiple methods of authentication. The following sections describe several remote access authentication methods.

PAP

Password Authentication Protocol (PAP) is used with Point-to-Point Protocol (PPP) to authenticate clients. A significant weakness of PAP is that it sends passwords over a network in cleartext, representing a considerable security risk.

PPP was primarily used with dial-up connections. Believe it or not, there was a time when the thought of someone wiretapping a phone was rather remote. Because of this, security was an afterthought with PPP. Today, PPP is only used as a last resort due to passwords being passed in cleartext or used with another protocol that provides encryption.

CHAP

Challenge Handshake Authentication Protocol (CHAP) also uses PPP and authenticates remote users, but it is more secure than PAP. The goal of CHAP is to allow the client to pass credentials over a public network (such as a phone or the Internet) without allowing attackers to intercept the data and later use it in an attack.

The client and server both know a shared secret (similar to a password) used in the authentication process. However, the client doesn't send the shared secret over the network in plaintext as PAP does. Instead, the client hashes it after combining it with a nonce (number used once) provided by the server. This handshake process is used when the client initially tries to connect to the server and at different times during the connection.

Remember this

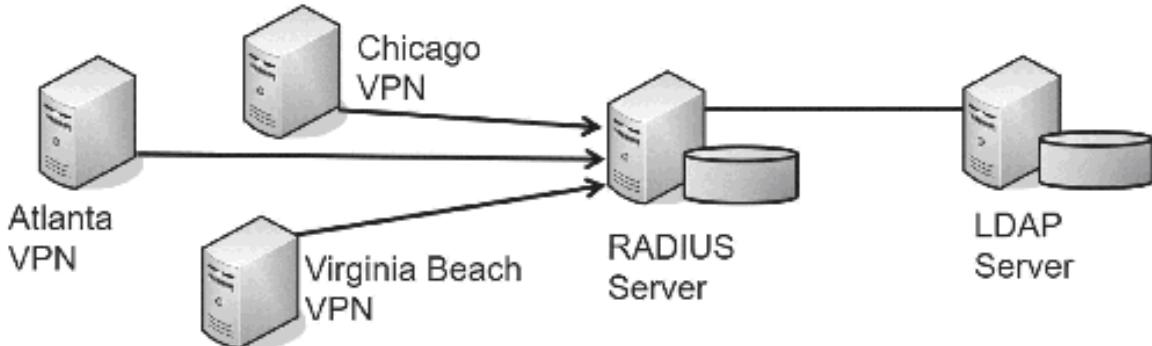
PAP authentication uses a password or a PIN. A significant weakness is that PAP sends the information across a network in cleartext, making it susceptible to sniffing attacks. CHAP is more secure than PAP because CHAP doesn't send passwords over the network in cleartext.

RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a centralized authentication service. Instead of each individual VPN server needing a separate database to identify who can authenticate, the VPN servers forward the authentication requests to a central RADIUS server. RADIUS can also be used as an 802.1X server with WPA2 Enterprise mode (described earlier in this chapter).

Imagine your company has locations in Virginia Beach, Atlanta, and Chicago. Each location has a VPN server that users can access. Bart is a traveling salesman, and he can connect to any of these VPN servers. When entering sales data, he connects to the Atlanta VPN. He connects to the Virginia Beach VPN server when using the company-sponsored always-on VPN for his mobile devices. Bart has one account for all company access, and today he was prompted to change his password.

If each VPN server has a separate database with Bart's username and password, each of these databases must be updated. This can be labor-intensive and result in needless errors.



However, the company could use a centralized RADIUS server, as shown in Figure 4.10, instead. Each VPN server is configured with a shared secret (similar to a password) and the RADIUS server is configured with a matching shared secret for each of the VPN servers.

Figure 4.10: RADIUS configuration

This centralized RADIUS server could hold a centralized database of user accounts. However, it is more common for the RADIUS server to access an LDAP server that holds the accounts. For example, in a Microsoft domain, the RADIUS server would pass the credentials to a domain controller. A significant benefit is that there is only one account for the user. If Bart changes his password, the domain controller knows the new password.

RADIUS uses the User Datagram Protocol (UDP), which provides a best-effort delivery mechanism. As a result, RADIUS includes logic to detect communication problems. In contrast, RADIUS alternatives use TCP, which provides guaranteed delivery. These alternatives allow TCP to detect and handle

communication issues. Also, RADIUS only encrypts the password by default, while alternatives encrypt the entire authentication process.

Even though RADIUS was created before Extensible Authentication Protocol (EAP) was developed, RADIUS does work with EAP. RFC 3579 “RADIUS Support for EAP” is an informational RFC and describes how to do so.

TACACS+

Terminal Access Controller Access-Control System Plus (TACACS+) is an alternative to RADIUS, and it provides two essential security benefits over RADIUS. First, it encrypts the entire authentication process, whereas RADIUS encrypts only the password by default. Second, TACACS+ uses multiple challenges and responses between the client and the server.

Although Cisco created TACACS+, it can interact with Kerberos. This allows a Cisco VPN concentrator to interact in a Microsoft Active Directory environment. As a reminder, Microsoft Active Directory uses Kerberos for authentication.

Organizations also use TACACS+ as an authentication service for network devices. In other words, you can use it to authenticate users before they are able to access a configuration page for a router or a switch. The network devices must be TACACS+ enabled, and a TACACS+ server provides the authentication services.

Remember this

RADIUS and TACACS+ provide centralized authentication. RADIUS only encrypts the password by default, but can be used with EAP to encrypt entire sessions. TACACS+ encrypts the entire session by default and can be used with Kerberos.

AAA Protocols

AAA protocols provide authentication, authorization, and accounting. Authentication verifies a user’s identification, and authorization determines if a user should have access. Accounting tracks user access with logs.

As an example, RADIUS, TACACS+, and Diameter are considered AAA protocols because they provide all three services. They authenticate users who attempt remote access, determine if the user is authorized for remote access by checking a database, and then record the user’s activity. TACACS+ uses multiple challenges and responses during a session. Kerberos is sometimes referred to as an AAA protocol, but it does not provide any accounting services.

Chapter 4 Exam Topic Review

When preparing for the exam, make sure you understand these key concepts covered in this chapter.

Exploring Advanced Security Devices

- Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) inspect traffic using the same functionality as a protocol analyzer.
- A host-based IDS (HIDS) can detect attacks on local systems such as workstations and servers. The HIDS protects local resources on the host and can detect some malware that isn't detected by traditional antivirus software. A network-based IDS (NIDS) detects attacks on networks.
- A signature-based IDS or IPS uses signatures to detect known attacks or vulnerabilities.
- Heuristic-based or behavioral-based IDSs (also called anomaly-based IDSs) require a baseline and detect attacks based on anomalies or when traffic is outside expected boundaries.
- A false positive incorrectly raises an alert indicating an attack when an attack is not active. False positives increase the workload of administrators. A false negative is when an attack is active, but not reported.
- An IPS is similar to an active IDS except that it's placed inline with the traffic (sometimes called in-band) and can stop attacks before they reach the internal network. An IPS can actively monitor data streams, detect malicious content, and prevent it from reaching a network. In contrast, an IDS is out-of-band.
- IDSs and IPSs can also protect internal private networks, such as private supervisory control and data acquisition (SCADA) networks.
- Honeypots and honeynets appear to have valuable data and attempt to divert attackers away from live networks. Security personnel use them to deceive attackers, disrupt attacks, and observe attackers' current attack methodologies. A honeyfile is a file designed to attract the attention of an attacker.

- Fake telemetry sends corrupted or modified data to a monitoring system.

Securing Wireless Networks

- Wireless access points (APs) connect wireless clients to a wired network.
- The service set identifier (SSID) is the name of the wireless network. Disabling the SSID broadcast hides a wireless network from casual users.
- You can restrict access to wireless networks with media access control (MAC) filtering. However, attackers can discover authorized MACs and spoof an authorized MAC address.
- A site survey examines the wireless environment to identify potential problem areas. Wireless footprinting uses a heat map to give you a detailed diagram of wireless access points, hotspots, and dead spots within an organization.
- Wi-Fi analyzers show signal levels on individual wireless frequency channels.
- WPA2 uses AES with CCMP and supports open, pre-shared key (PSK), and Enterprise modes.
- Enterprise mode is more secure than Personal mode because it adds authentication. It uses an 802.1X authentication server implemented as a RADIUS server.
- WPA3 uses Simultaneous Authentication of Equals (SAE) instead of the PSK. WPA3 supports Enterprise mode, similar to WPA2 Enterprise mode.
- Open mode doesn't use a PSK or an 802.1X server. Many hotspots use Open mode when providing free wireless access to customers.
- 802.1X servers use one of the Extensible Authentication Protocol (EAP) versions, such as Protected EAP (PEAP), EAP-Tunneled TLS (EAP-TTLS), EAP-TLS, or EAP-Flexible Authentication via Secure Tunneling (EAP-FAST).
- The most secure EAP method is EAP-TLS, and it requires a certificate on the server and on each of the wireless clients. PEAP and EAP-TTLS require a certificate on the server, but not the client.

- An 802.1X server provides strong port security using port-based authentication. It prevents rogue devices from connecting to a network by ensuring that only authorized clients can connect.
- A captive portal forces wireless clients to complete a process, such as acknowledging a policy or paying for access, before it grants them access to the network.

Understanding Wireless Attacks

- A disassociation attack effectively removes a wireless client from a wireless network, forcing the wireless client to reauthenticate.
- Wi-Fi Protected Setup (WPS) allows users to easily configure a wireless device by pressing a button or entering a short PIN. WPS is not secure with WPA2. A WPS attack can discover the PIN within hours. It then uses the PIN to discover the passphrase. However, WPA3 thwarts WPS attacks.
- A rogue access point (rogue AP) is an AP placed within a network without official authorization. An evil twin is a rogue access point with the same or similar SSID as a legitimate access point.
- A jamming attack floods a wireless frequency with noise, blocking wireless traffic.
- An initialization vector (IV) attack attempts to discover the IV and uses it to discover the passphrase.
- Near field communication (NFC) attacks use an NFC reader to read data from mobile devices.
- Radio-frequency identification (RFID) attacks include eavesdropping, replay, and DoS.
- Bluejacking is the practice of sending unsolicited messages to a phone. Bluesnarfing is the unauthorized access to or theft of information from a Bluetooth device. Placing devices into conductive metal lockboxes that act as a Faraday cage will block Bluetooth attacks.
- In a wireless replay attack, an attacker captures data sent between two entities, modifies it, and then impersonates one of the parties by replaying the data. WPA2 and WPA3 are resistant to wireless replay attacks.

Using VPNs for Remote Access

- A virtual private network (VPN) provides access to private networks via a public network, such as the Internet.
- IPsec is a common tunneling protocol used with VPNs, and it secures traffic within a tunnel. IPsec provides authentication with an Authentication Header (AH). Encapsulating Security Payload (ESP) encrypts VPN traffic and provides confidentiality, integrity, and authentication.
- IPsec Tunnel mode encrypts the entire IP packet used in the internal network. IPsec Transport mode only encrypts the payload and is commonly used in private networks, but not with VPNs.
- A full tunnel encrypts all traffic after a user has connected to a VPN. A split tunnel only encrypts traffic destined for the VPN's private network.
- Site-to-site VPNs provide secure access between two networks. These can be on-demand VPNs or always-on VPNs.
- Mobile devices can also use always-on VPNs to protect traffic when users connect to public hotspots.
- Other protocols used with VPNs include TLS, L2TP, and HTML5.
- Network access control (NAC) inspects clients for specific health conditions such as up-to-date antivirus software, and can redirect unhealthy clients to a remediation network.
- A permanent NAC agent (sometimes called a persistent NAC agent) is installed on the client and stays on the client. A dissolvable NAC agent is downloaded and run on the client when the client logs on and deletes it after the session ends.
- An agentless NAC system will scan systems remotely instead of installing an agent on the system.
- Remote access authentication is used when a user accesses a private network from a remote location, such as with a VPN connection.
- Password Authentication Protocol (PAP) uses a password or PIN for authentication. A significant weakness is that PAP sends passwords across a network in cleartext.
- Challenge Handshake Authentication Protocol (CHAP) is more secure than PAP and uses a handshake process when authenticating

clients.

- RADIUS provides central authentication for multiple remote access services. RADIUS relies on the use of shared secrets and only encrypts the password during the authentication process, by default. It can be used with EAP to encrypt the entire session.
- TACACS+ is used by some Cisco systems as an alternative to RADIUS. TACACS+ uses TCP, encrypts the entire authentication process, and supports multiple challenges and responses.
- RADIUS and TACACS+ are authentication, authorization, and accounting (AAA) protocols.

Online References

- Have you done any of the online labs at <https://greatadministrator.com/sy0-601-extras/>? Online resources also include sample practice test questions, including performance-based questions.

Chapter 4 Practice Questions

1. A HIDS reported a vulnerability on a system based on a known attack. After researching the alert from the HIDS, you identify the recommended solution and begin applying it. What type of HIDS is in use?
 - A. Network-based
 - B. Signature-based
 - C. Heuristic-based
 - D. Anomaly-based

2. You are preparing to deploy a heuristic-based detection system to monitor network activity. Which of the following would you create first?
 - A. BPDU guard
 - B. Signatures
 - C. Baseline
 - D. Honeypot

3. Lenny noticed a significant number of logon failures for administrator accounts on the organization's public website. After investigating it further, he notices that most of these attempts are from IP addresses assigned to foreign countries. He wants to implement a solution that will detect and prevent similar attacks. Which of the following is the BEST choice?
 - A. Implement a passive NIDS.
 - B. Block all traffic from foreign countries.
 - C. Implement an inline NIPS.
 - D. Disable the administrator accounts.

4. Lisa created a document called *password.txt* and put the usernames of two accounts with elevated privileges. She then placed the file on her administrator account desktop on several servers. Which of the following BEST explains her actions?
 - A. She can use this file to retrieve the passwords if she forgets them.
 - B. This file will divert attackers from the live network.
 - C. The document is a honeyfile.
 - D. The file is needed by an application to run when the system starts.

5. Your organization is planning to upgrade the wireless network used by employees. It will provide encrypted authentication of wireless users over TLS. Which of the following protocols are they MOST likely implementing?

- A. EAP
- B. PEAP
- C. WPA2
- D. WPA3

6. Lisa is creating a detailed diagram of wireless access points and hotspots within your organization. What is another name for this?

- A. Remote access VPN
- B. Wireless footprinting
- C. Channel overlap map
- D. Architectural diagram

7. You are assisting a small business owner in setting up a public wireless hotspot for her customers. She wants to allow customers to access the hotspot without entering a password. Which of the following is MOST appropriate for this hotspot?

- A. Use Open mode.
- B. Use a PSK.
- C. Use Enterprise mode.
- D. Disable SSID broadcast.

8. A network administrator routinely tests the network looking for vulnerabilities. He recently discovered a new access point set to open. After connecting to it, he found he was able to access network resources. What is the BEST explanation for this device?

- A. Evil twin
- B. A Raspberry Pi device
- C. Rogue AP
- D. APT

9. You are an administrator at a small organization. Homer contacted you today and reported the following:

- He logged on normally on Monday morning and accessed network shares.
- Later, when he tried to access the Internet, a pop-up window with the organization's wireless SSID prompted him to log on.
- After doing so, he could access the Internet but no longer had access to the network shares.
- Three days later, his bank notified him of suspicious activity on his account.

Which of the following indicates the MOST likely explanation for this activity?

- A. An evil twin
- B. A rogue access point
- C. A DDoS attack
- D. A captive portal

10. Mobile users in your network report that they frequently lose connectivity with the wireless network on some days, but they don't have any problems on other days. You suspect this is due to an attack. Which of the following attacks is MOST likely to cause these symptoms?

- A. Wireless jamming attack
- B. IV attack
- C. Replay attack
- D. Bluesnarfing attack

11. An attacker can access email contact lists on your smartphone. What type of attack is this?

- A. Bluesnarfing
- B. Bluejacking
- C. Captive portal
- D. WPS

12. Your organization plans to implement a connection between the main site and a remote office giving remote employees on-demand access to resources at headquarters. The chief information officer (CIO) wants to use

the Internet for this connection. Which of the following solutions will BEST support this requirement?

- A. Remote access VPN
- B. Site-to-site VPN
- C. Always-on VPN
- D. Full-tunnel VPN
- E. Split-tunnel VPN

13. Your organization is allowing more employees to work from home, and they want to upgrade their VPN. Management wants to ensure that after a VPN client connects to the VPN server, all traffic from the VPN client is encrypted. Which of the following would BEST meet this goal?

- A. Split tunnel
- B. Full tunnel
- C. IPsec using Tunnel mode
- D. IPsec using Transport mode

14. An organization is hosting a VPN that employees are using while working from home. Management wants to ensure that all VPN clients are using up-to-date operating systems and antivirus software. Which of the following would BEST meet this need?

- A. NAT
- B. NAC
- C. VLAN
- D. DMZ

15. Your organization recently implemented a BYOD policy. However, management wants to ensure that mobile devices meet minimum standards for security before they can access any network resources. Which of the following would the NAC MOST likely use?

- A. Permanent
- B. Health
- C. RADIUS
- D. Agentless

Chapter 4 Practice Question Answers

1. **B** is correct. If the host-based intrusion detection system (HIDS) identified a known issue, it is using signature-based detection (sometimes called definition-based detection). A HIDS is not network-based but a network-based IDS (NIDS) can also use signature-based detection. Heuristic-based or behavior-based (sometimes called anomaly-based) detection systems identify issues by comparing current activity against a baseline. They can identify issues that are not previously known.
2. **C** is correct. A heuristic-based (also called behavior-based or anomaly-based) detection system compares current activity with a previously created baseline to detect any anomalies or changes. Signature-based systems (also called definition-based) use signatures of known attack patterns to detect attacks. A honeypot is a server designed to look valuable to an attacker and can divert attacks. A Bridge Protocol Data Unit (BPDU) guard is used to protect against BPDU-related attacks and is unrelated to this question.
3. **C** is correct. An inline network-based intrusion prevention system (NIPS) can dynamically detect, react to, and prevent attacks. An inline system is placed inline with the traffic, and in this scenario, it can be configured to detect the logon attempts and block the traffic from the offending IP addresses before it reaches the internal network. A passive network-based intrusion detection system (NIDS) is not placed inline with the traffic and can only detect the traffic after it has reached the internal network, so it cannot prevent the attack. If you block all traffic from foreign countries, you will likely block legitimate traffic. You should disable administrator accounts if they're not needed. However, if you disable all administrator accounts, administrators won't be able to do required work.
4. **C** is correct. A honeyfile is a file with a deceptive name (such as *password.txt*) that will deceive an attacker and attract his attention. It is not appropriate to place a file holding credentials on a desktop for any reason. A honeypot or honeynet diverts attackers from the live network. A file on an administrator's desktop is on the live network. It is unlikely that any

application needs a file named *password.txt* to run. Even if an application needed such a file, the file would be inaccessible if it is placed on an administrator's desktop.

5. **B** is correct. Protected EAP (PEAP) can be used for wireless authentication and it uses Transport Layer Security (TLS) to encapsulate and encrypt the authentication conversation within a TLS tunnel. Extensible Authentication Protocol (EAP) is the basic framework for authentication. By itself, EAP doesn't provide encryption, but it can be combined with other encryption protocols. Neither Wi-Fi Protected Access 2 (WPA2) nor Wi-Fi Protected Access 3 (WPA3) use TLS.

6. **B** is correct. Wireless footprinting creates a detailed diagram of wireless access points and hotspots within an organization. It typically displays a heat map and dead spots if they exist. A remote access virtual private network (VPN) provides access to a private network and is unrelated to this question. Wi-Fi analyzers provide a graph showing channel overlaps but not a diagram of wireless access points. An architectural diagram is typically laid on top of a heat map to create the wireless footprint document, but by itself, it shows the building layout.

7. **A** is correct. Open mode is the best choice of those given for a public wireless hotspot that doesn't require a password. A pre-shared key (PSK) is the same as a password and the scenario says a password isn't desired. Enterprise mode requires each user to authenticate and is typically enabled with a RADIUS server. If you disable service set identifier (SSID) broadcast, it will make it harder for the customers to find the hotspot, but unless Open mode is used, it will still require a password.

8. **C** is correct. This describes a rogue access point (AP). A rogue AP is not authorized (also known as shadow IT) but provides access to an internal network because it has been plugged into the network. In this scenario, the access point has no security, so someone could connect to it from the parking lot and then access the internal network. An evil twin has the same or similar service set identifier (SSID) as a legitimate access point, but the SSID isn't mentioned. A Raspberry Pi device is an embedded system, and it

can be configured as a wireless AP, but there isn't any indication of the type of wireless AP in this scenario. An advanced persistent threat (APT) attacks from external locations and is unlikely to connect to a physical wireless AP inside a network.

9. **A** is correct. This describes an evil twin. Normally, a user shouldn't have to log on again to access the Internet. Because he lost access to network resources after logging on, it indicates he didn't log on to a corporate access point (AP) but instead logged on to an unauthorized AP. Because the service set identifier (SSID) is the same as the corporate SSID, it indicates the AP is an evil twin. An evil twin is a rogue access point with the same or similar SSID as a legitimate AP, so an evil twin is a more accurate description. A distributed denial-of-service (DDoS) attack is an attack against a single computer from multiple attackers and is unrelated to this question. A captive portal forces web browser users to complete a specific process, such as agreeing to an acceptable use policy, before it allows them access to a network.

10. **A** is correct. A wireless jamming attack is a type of denial-of-service (DoS) attack that can cause wireless devices to lose their association with access points and disconnect them from the network. It transmits noise or another radio signal on the same frequency used by the existing wireless network. An initialization vector (IV) attack attempts to discover the passphrase. A replay attack captures traffic intending to replay it later to impersonate one of the parties in the original transmission. Bluesnarfing is a Bluetooth attack that attempts to access information on Bluetooth devices.

11. **A** is correct. A successful bluesnarfing attack allows attackers to access data (including email contact lists) on a smartphone. Bluejacking is the practice of sending unsolicited messages to other Bluetooth devices. A captive portal is not an attack. Instead, it forces users to acknowledge a usage policy or pay for access. A Wi-Fi Protected Setup (WPS) attack attempts to discover an access point WPS PIN by guessing PIN numbers.

12. **B** is correct. A site-to-site virtual private network (VPN) includes two VPN servers that act as gateways for two networks separated

geographically, such as a main site network and a remote office network. A remote access VPN is used by individuals to connect to the main network, such as employees working from home. An always-on VPN would have the connection enabled all the time, but the scenario states that employees should have on-demand access. A full-tunnel VPN encrypts all traffic to and from the Internet after a user has connected to the VPN. A split-tunnel VPN only encrypts the VPN tunnel but not other Internet connections. The scenario didn't provide any directions related to a full-tunnel or a split-tunnel VPN.

13. **B** is correct. A full tunnel encrypts all traffic after a user has connected to a virtual private network (VPN) using a tunnel. A split tunnel only encrypts traffic destined for the VPN's private network. Traffic from the client directly to another Internet site is not encrypted. Internet Protocol security (IPsec) Tunnel mode encrypts the entire IP packet used in the internal network. It encrypts all traffic used within the VPN's private network, but not all traffic from the VPN client. IPsec Transport mode only encrypts the payload and is used within private networks, instead of for VPN traffic.

14. **B** is correct. Network access control (NAC) technologies can inspect virtual private network (VPN) clients for health status, including having up-to-date operating systems and antivirus software. None of the other answers will inspect VPN clients. Network Address Translation (NAT) allows multiple users with private IP addresses to share a single public IP address. A virtual local area network (VLAN) can segment clients, but not inspect them. A demilitarized zone (DMZ) provides a layer of protection for Internet-facing servers, putting them in a buffer zone between the Internet and an internal network.

15. **D** is correct. An agentless network access control (NAC) system is often used on employee-owned devices and would be appropriate if an organization implemented a bring your own device (BYOD) policy. A permanent network access control (NAC) agent is installed on the device permanently, but this might cause problems for employee-owned devices.

Any NAC agent is a health agent. Remote Authentication Dial-In User Service (RADIUS) is used for authentication, not to inspect clients.

Chapter 5

Securing Hosts and Data

CompTIA Security+ objectives covered in this chapter:

- 1.2 Given a scenario, analyze potential indicators to determine the type of attack.**
 - Cloud-based vs. on-premises attacks
- 1.3 Given a scenario, analyze potential indicators associated with application attacks.**
 - Application programming interface (API) attacks
- 1.5 Explain different threat actors, vectors, and intelligence sources.**
 - Vectors (Removable media, Cloud)
- 1.6 Explain the security concerns associated with various types of vulnerabilities.**
 - Cloud-based vs. on-premises vulnerabilities, Third-party risks (Data storage)
 - Improper or weak patch management (Firmware, Operating system (OS), Applications)
 - Impacts (Data loss, Financial, Reputation, Availability loss)
- 2.1 Explain the importance of security concepts in an enterprise environment.**
 - Configuration management (Diagrams, Baseline configuration, Standard naming conventions, Internet protocol (IP) schema)
 - Data protection (Data loss prevention (DLP), Rights management)
 - API considerations
- 2.2 Summarize virtualization and cloud computing concepts.**
 - Cloud models (Infrastructure as a service (IaaS), Platform as a service (PaaS), Software as a service (SaaS), Anything as a service (XaaS), Public, Community, Private, Hybrid)
 - Cloud service providers, Managed service provider (MSP)/managed security service provider (MSSP), On-premises vs. off-premises
 - Fog computing, Edge computing, Microservices/API
 - Infrastructure as code (Software-defined networking (SDN), Software-defined visibility (SDV))
 - Serverless architecture, Services integration, Resource policies, Transit gateway
- 2.3 Summarize secure application development, deployment, and automation concepts**
 - Secure coding techniques (Data exposure)
- 2.4 Summarize authentication and authorization design concepts.**
 - Authentication methods (Attestation)
 - Cloud vs. on-premises requirements
- 2.5 Given a scenario, implement cybersecurity resilience.**
 - Replication (VM), On-premises vs. cloud, Non-persistence(Revert to known state, Last known good configuration, Live boot media)
- 2.6 Explain the security implications of embedded and specialized systems.**
 - Embedded systems (Raspberry Pi, Field programmable gate array (FPGA), Arduino)
 - Supervisory control and data acquisition (SCADA)/industrial control system (ICS) (Facilities, Industrial, Manufacturing, Energy, Logistics)

- Internet of Things (IoT) (Sensors, Smart devices, Wearables, Facility automation, Weak defaults), Specialized (Medical systems, Vehicles, Aircraft, Smart meters)
- Voice over IP (VoIP), Heating, ventilation, air conditioning (HVAC)
- Multifunction printer (MFP), Real-time operating system (RTOS), Surveillance systems, System on chip (SoC), Communication considerations (5G, Narrow-band, Baseband radio, Subscriber identity module (SIM) cards, Zigbee)
- Constraints (Power, Compute, Network, Crypto, Inability to patch, Authentication, Range, Cost, Implied trust)

2.7 Explain the importance of physical security controls.

- USB data blocker

3.2 Given a scenario, implement host or application security solutions.

- Endpoint protection (Endpoint detection and response (EDR), DLP)
- Boot integrity (Boot security/Unified Extensible Firmware Interface (UEFI), Measured boot, Boot attestation)
- Database (Tokenization, Salting, Hashing)
- Application security (Allow list, Block list/deny list)
- Hardening (Open ports and services, Registry, Disk encryption, OS, Patch management (Third-party updates, Auto-update))
- Self-encrypting drive (SED)/full disk encryption (FDE) (Opal)
- Hardware root of trust, Trusted Platform Module (TPM)

3.3 Given a scenario, implement secure network designs.

- Network appliances (HSM)

3.5 Given a scenario, implement secure mobile solutions.

- Connection methods and receivers (Cellular, WiFi, Bluetooth, NFC, Infrared, USB, Point to point, Point to multipoint, Global Positioning System (GPS), RFID)
- Mobile device management (MDM) (Application management, Content management, Remote wipe, Geofencing, Geolocation, Screen locks, Push notifications, Passwords and PINs, Biometrics, Context-aware authentication, Containerization, Storage segmentation, Full device encryption)
- Mobile devices (MicroSD hardware security module (HSM), MDM/Unified Endpoint Management (UEM), Mobile application management (MAM), SEAndroid)
- Enforcement and monitoring of: (Third-party application stores, Rooting/jailbreaking, Sideload, Custom firmware, Carrier unlocking, Firmware over-the-air (OTA) updates, Camera use, SMS/Multimedia Messaging Service (MMS)/Rich Communication Services (RCS), External media, USB On-the-Go (USB OTG), Recording microphone, GPS tagging, WiFi direct/ad hoc, Tethering, Hotspot, Payment methods)
- Deployment models (Bring your own device (BYOD), Corporate-owned personally enabled (COPE), Choose your own device (CYOD), Corporate-owned, Virtual desktop infrastructure (VDI))

3.6 Given a scenario, apply cybersecurity solutions to the cloud.

- Compute (Security groups, Dynamic resource allocation, Instance awareness, Virtual private cloud (VPC) endpoint, Container security)
- Solutions (CASB, Application security, Next-generation secure web gateway (SWG))
- Firewall considerations in a cloud environment (Cost, Need for segmentation, Open Systems Interconnection (OSI) layers)

- Cloud native controls vs. third-party solutions

3.7 Given a scenario, implement identity and account management controls.

- Account policies (Geofencing, Geotagging)

3.8 Given a scenario, implement authentication and authorization solutions.

- Authentication management (TPM, HSM)

4.4 Given an incident, apply mitigation techniques or controls to secure an environment.

- Reconfigure endpoint security solutions (Application approved list, Application blocklist/deny list, Quarantine)
- Configuration changes (Firewall rules, MDM, DLP, Content filter/URL filter)

5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.

- Key frameworks (Cloud security alliance, Cloud control matrix)

5.3 Explain the importance of policies to organizational security.

- Organizational policies (Change management)

**

In this chapter, you'll learn about different methods used to implement systems securely. This includes hardening endpoints when deploying them and using change management policies to keep them secure.

More and more organizations are using cloud resources, and this chapter summarizes the important cloud concepts. Additionally, the use of mobile devices has exploded in the last few years, with more and more organizations allowing employees to connect mobile devices to the network. This results in many challenges for an organization, but mobile device management tools help administrators handle these challenges. This chapter also covers the security implications of embedded systems and Internet of Things (IoT) devices.

Summarize Virtualization Concepts

Virtualization is a popular technology used within data centers. It allows you to host one or more virtual systems, or virtual machines (VMs), on a single physical system. With today's technologies, you can host an entire virtual network within a single physical system, and organizations are increasingly using virtualization to reduce costs.

When discussing VMs, you should understand the following terms:

- **Hypervisor.** The software that creates, runs, and manages the VMs is the hypervisor. Several virtualization technologies currently exist, including VMware products, Microsoft Hyper-V products, and Oracle VM VirtualBox. These applications have their own hypervisor software.
- **Host.** The physical system hosting the VMs is the host. It requires more resources than a typical system, such as multiple processors, massive amounts of RAM, fast and abundant hard drive space, and one or more fast network cards. Although these additional resources increase the cost of the host, it is still less expensive than paying for multiple physical systems. It also requires less electricity, less cooling, and less physical space.
- **Guest.** Operating systems running on the host system are guests or guest machines. Most hypervisors support several different operating systems, including various Microsoft operating systems and various Linux distributions. Additionally, most hypervisors support both 32-bit and 64-bit operating systems.
- **Host scalability.** Scalability refers to the ability to resize the computing capacity of the VM. You do this by assigning it more memory, processors, disk space, or network bandwidth. Scalability is a manual process, and it often requires a reboot. In other words, an administrator would manually change the resources assigned to the VM.
- **Host elasticity.** Elasticity refers to the ability to dynamically change resources assigned to the VM based on the load. As an example, imagine a VM has increased traffic. Monitoring software

senses this increased load and automatically increases the VM resources to handle it. This does not require a reboot.

Virtualization typically provides the best return on investment (ROI) when an organization has many underutilized servers. Imagine an organization has nine physical servers, with each using less than 20 percent processing power, memory, and disk space. You could convert three physical servers to virtual hosts and run three guest servers on each physical server. Assuming all the servers are similar, this wouldn't cost any more money for the physical servers. Additionally, three physical servers consume less electricity and require less heating and ventilation to maintain.

In contrast, imagine the organization has nine servers, with each using about 80 percent of its processing power, memory, and disk space. It is possible to convert them all to virtual servers, with each virtual server hosting one VM. However, this doesn't reduce the number of physical servers. Still, the organization could choose to purchase two or three powerful servers and host the nine servers as VMs on these new servers. This reduces the cost of electricity, heating, and ventilation but may not reduce the total cost of ownership (TCO).

Thin Clients and Virtual Desktop Infrastructure

A ***thin client*** is a computer with enough resources to boot and connect to a server to run specific applications or desktops. When the thin client is a traditional computer, it typically has a keyboard, mouse, and screen and may support other peripherals such as speakers and USB ports. The server is a powerful server located on-site or in the cloud, supporting multiple thin clients.

A ***virtual desktop infrastructure (VDI)*** hosts a user's desktop operating system on a server. While traditional computers typically access VDIs within a network, it's also possible to deploy a VDI that users can access with their mobile device. This allows users to access any applications installed on their desktop. When the organization hosts a remote access solution such as a virtual private network (VPN), users can access the mobile VDI from anywhere if they have Internet access.

Containers

Container virtualization runs services or applications within isolated containers or application cells. Figure 5.1 shows an example of container virtualization. Notice that the containers don't host an entire operating system. Instead, the host's operating system and kernel run the service or app within each of the containers. However, because they are running in separate containers, none of the services or apps can interfere with services and apps in other containers.

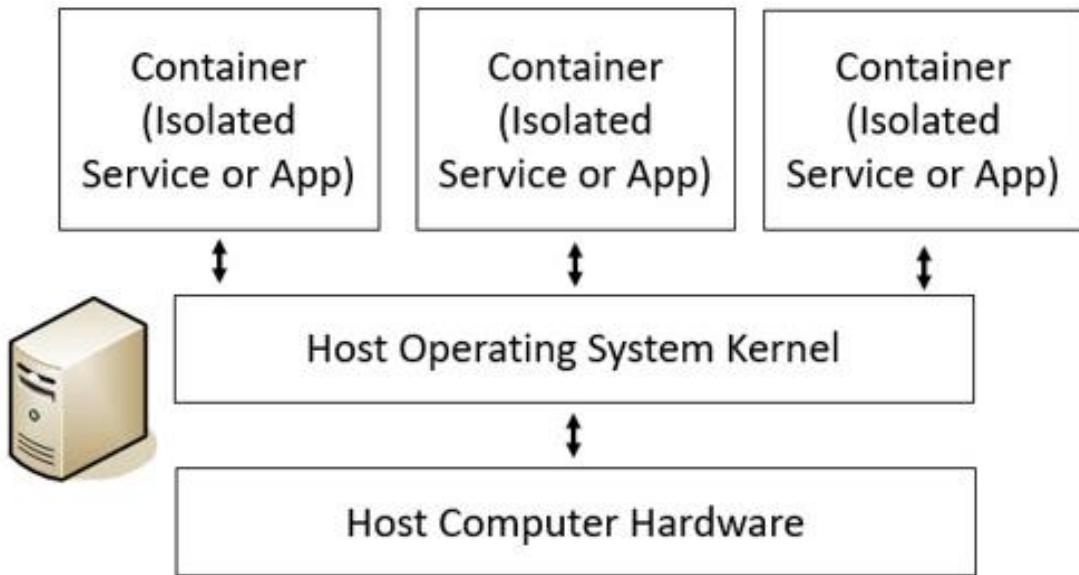


Figure 5.1: Container-based virtualization

A benefit of container virtualization is that it uses fewer resources and can be more efficient than a system using a traditional Type II hypervisor virtualization. Internet Service Providers (ISPs) often use it for customers who need specific applications. One drawback is that containers must use the operating system of the host. As an example, if the host is running Linux, all the containers must run Linux.

VM Escape Protection

VM escape is an attack that allows an attacker to access the host system from within the virtual system. As previously mentioned, the host system runs an application or process called a hypervisor to manage the virtual systems. In some situations, the attacker can run code on the virtual system and interact with the hypervisor.

Most virtual systems run on a physical server with elevated privileges, similar to administrator privileges. A successful VM escape attack often gives the attacker unlimited control over the host system and each virtual system within the host.

When vendors discover VM escape vulnerabilities, they write and release patches. Just as with any patches, it is important to test and install these patches as soon as possible. This includes keeping both the physical and the virtual servers patched.

VM Sprawl Avoidance

VM sprawl occurs when an organization has many VMs that aren't appropriately managed. Most organizations have specific policies in place to ensure physical servers are kept up to date, and personnel only make changes to these servers after going through a change management process. These same policies should also apply to virtual servers.

Consider this scenario. Bart creates a VM running a Microsoft Windows Server version to test a software application. After testing the application, he leaves the VM running. Later, Microsoft releases security patches for the server. The IT department tests these patches and applies them to all of the known servers that need them. However, because Bart didn't tell anyone he was creating the VM, it remains unpatched and vulnerable to attack.

Another challenge with VM sprawl is that each VM adds additional load onto a server. If personnel add unauthorized VMs to physical servers, they can consume system resources. The servers might become slower and potentially crash.

Replication

It's worth pointing out that virtual machines are simply files. These files certainly have some complexity, but still, they are just files. Because the VM is just a group of files, it becomes relatively easy to replicate a VM by copying the files from one physical server to another. If the original VM is damaged, the replicated VM can be used as a backup.

Replication makes it easy to restore a failed virtual server. If you create a backup of the virtual server files and the original server fails, you simply restore the files. You can measure the amount of time it takes to restore a replicated virtual server in minutes. In contrast, rebuilding a physical server can take hours.

Snapshots

A ***snapshot*** provides you with a copy of a VM at a moment in time, which you can use as a backup. You are still able to use the VM just as you normally would. However, after taking a snapshot, the hypervisor keeps a record of all changes to the VM. If the VM develops a problem, you can revert the VM to the state it was in when you took the snapshot.

Administrators commonly take snapshots of systems prior to performing any risky operation. Risky operations include applying patches or updates, testing security controls, and installing new applications. Ideally, these operations do not cause any problems, but occasionally they do. By creating snapshots before these operations, administrators can easily revert or roll back the system to a known good state with a known good configuration.

Remember this

Virtualization allows multiple virtual servers to operate on a single physical server providing increased cybersecurity resilience with lower operating costs. Keeping systems up to date with current patches is the best protection from VM escape attacks.

Non-Persistence

A primary consideration when running virtual desktops is whether they will support persistence or non-persistence. In a persistent virtual desktop, each user has a custom desktop image. Users can customize them and save their data within the desktop. A drawback is that it increases the amount of disk space required on the server to support unique desktop images for all users.

Virtual desktops that support non-persistence serve the same desktop for all users. When a user accesses the remote server, it provides a desktop operating system from a preconfigured snapshot. Although users can make changes to the desktop as they're using it, it reverts to a known state (the original snapshot) when they log off. Another way of viewing this is that it rolls back to a known configuration or a last known good configuration.

Many systems support booting to an operating system from the USB drive. Some bootable USB drives are live media, meaning that they save any changes to the operating system on the USB drive. If you install software packages or change system settings, they will be persistent on a live media USB drive.

Implementing Secure Systems

Secure systems design concepts help ensure that computing systems are deployed and maintained in a secure state. In this context, a system is any host such as a server, workstation, laptop, network device, or mobile device. In an ideal world, systems start in a secure state. Unfortunately, it's not an ideal world, and administrators need to be proactive in securing systems before deployment and keeping them secure after deployment. This section outlines several steps used to secure hosts.

Endpoint Security

Endpoints are computing devices such as servers, desktops, laptops, mobile devices, or Internet of Things (IoT) devices. Endpoint detection and response (EDR), sometimes called endpoint threat detection and response (ETDR), provides continuous monitoring of endpoints.

EDR tools are part of a defense-in-depth strategy. Other tools such as intrusion detection and prevention systems monitor traffic on the network and attempt to detect and block all malicious traffic. Unfortunately, attackers still get through. EDR tools perform a deep investigation of all activity on endpoints.

There isn't a standard set of capabilities that all EDR platforms include. However, they commonly include anti-malware solutions, host-based intrusion detection systems (HIDSs), and application allow and blocklists (described later in this chapter).

Chapter 4, “Securing Your Network,” covers HIDS, and Chapter 6, “Comparing Threats, Vulnerabilities, and Common Attacks,” covers anti-malware.

Hardening Systems

Hardening is the practice of making an operating system (OS) or application more secure from its default installation. It helps eliminate vulnerabilities from default configurations, misconfigurations, and weak configurations.

When deploying systems, they should only have the applications, services, and protocols they need to meet their purpose. If a service or protocol is not running on a system, attackers cannot attack it. As a simple example, a system is not vulnerable to any File Transfer Protocol (FTP) attacks if FTP is not running and available on the system. When you disable or close a port on a system, you disable the related protocol or service.

In addition to disabling unnecessary services to reduce vulnerabilities, it's essential to uninstall unneeded software. Software frequently has bugs and vulnerabilities. Although patching software closes these vulnerabilities, you can eliminate these vulnerabilities by simply removing unnecessary applications.

Recently, it's become necessary for administrators to modify the Registry to harden systems. As an example, attackers frequently use PowerShell in attacks. However, the PowerShell scripts that attackers run aren't logged by default. Many administrators modify the Registry as part of the hardening process to ensure that all PowerShell activity is logged.

It has also become more common for organizations to implement disk encryption as part of the hardening process. This chapter covers multiple ways to encrypt disks.

Chapter 8, "Using Risk Management Tools," discusses the use of vulnerability scanners to discover vulnerabilities in systems. It also includes a list of common vulnerabilities related to weak configurations. By eliminating weak configuration items, it helps administrators harden systems.

Configuration Management

Configuration management practices help organizations deploy systems with secure configurations. Administrators often use baselines and imaging (discussed in the next sections) with configuration management. Change management practices (discussed later in this chapter) complement configuration management practices and help ensure that systems remain secure, even as the configurations change over the lifetime of systems.

Some organizations use diagrams to show configuration management processes. These sometimes use flowcharts to document the decision-making process involved in modifying a configuration.

Large organizations often use standard naming conventions to identify standard configurations. The standard an organization uses isn't as important as identifying a standard and following it consistently. A possible choice is an endpoint device (such as a laptop, desktop, or server), the department or location, and the version. For example, the third major version of an image for a desktop used by employees in the Sales department could be Desktop_Sales_3.0.

RFC 3139 “Requirements for Configuration Management of IP-based Networks” discusses the use of configuration management in different IP networks. This is only useful in large networks with multiple subnets and would only be done after the primary configuration. As an example, administrators could create separate scripts for different networks. These scripts could configure network-based settings for devices in the different networks. However, Dynamic Host Configuration Protocol (DHCP), discussed in Chapter 3, “Exploring Network Technologies and Tools,” could probably meet most needs.

Secure Baseline and Integrity Measurements

A baseline is a known starting point, and organizations commonly use secure baselines to provide known starting points for systems. One of the primary benefits of secure baselines is that they improve the overall security posture of systems. Weak security configurations are a common security issue, but secure baselines help eliminate this.

The use of baselines works in three steps:

1. **Initial baseline configuration.** Administrators use various tools to deploy systems consistently in a secure state.
2. **Integrity measurements for baseline deviation.** Automated tools monitor the systems for any baseline changes, which is a common security issue. Some tools such as vulnerability scanners monitor the systems and report any changes they detect. Other tools such as Group Policy automatically reconfigure the systems to the baseline settings when they detect changes.
3. **Remediation.** Chapter 4 covers network access control (NAC). NAC methods can detect some changes to baseline settings and automatically isolate or quarantine systems in a remediation network. Typically, administrators need to correct the problems in these systems manually.

Using Master Images for Baseline Configurations

One of the most common methods of deploying systems is with images starting with a master image. An image is a snapshot of a single system that administrators deploy to multiple other systems. Imaging has become an important practice for many organizations because it streamlines deployments while ensuring they are deployed securely. Figure 5.2 and the following text identify the overall process of capturing and deploying an image:

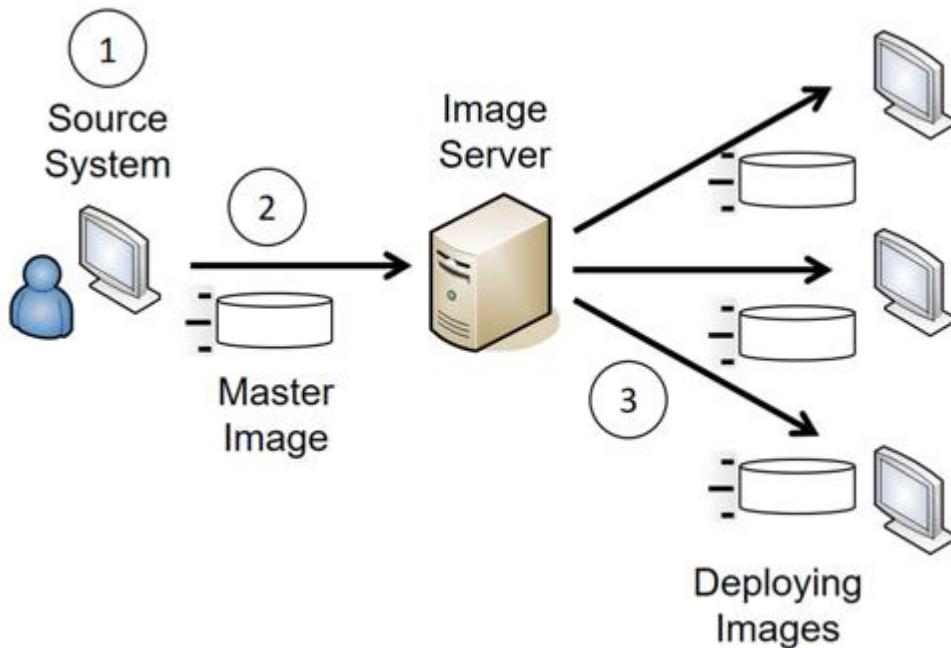


Figure 5.2: Capturing and deploying images

1. Administrators start with a blank source system. They install and configure the operating system, install and configure any desired applications, and modify security settings. Administrators perform extensive testing to ensure the system works as desired and that it is secure before going to the next step.
2. Next, administrators capture the image, which becomes their master image. Symantec Ghost is a popular imaging application, and Windows Server versions include free tools many organizations use to capture and deploy images. The

captured image is simply a file stored on a server or copied to external media, such as a DVD or external USB drive.

3. In step 3, administrators deploy the image to multiple systems. When used within a network, administrators can deploy the same image to dozens of systems during initial deployment or to just a single system to rebuild it. The image installs the same configuration on the target systems as the original source system created in step 1.

Administrators will often take a significant amount of time to configure and test the source system. They follow the same hardening practices discussed earlier and often use security and configuration baselines. If they're deploying the image to just a few systems, such as in a classroom setting, they may create the image in just a few hours. However, if they're deploying it to thousands of systems within an organization, they may take weeks or months to create and test the image. Once they've created the image, they can deploy it relatively quickly with minimal administrative effort.

Imaging provides two important benefits:

- **Secure starting point.** The image includes mandated security configurations for the system. Personnel who deploy the system don't need to remember or follow extensive checklists to ensure that new systems are set up with all the detailed configuration and security settings. The deployed image retains all the settings of the original image. Administrators will still configure some settings, such as the computer name, after deploying the image.
- **Reduced costs.** Deploying imaged systems reduces the overall maintenance costs and improves reliability. Support personnel don't need to learn several different end-user system environments to assist end users. Instead, they learn just one. When troubleshooting, support personnel spend their time helping the end user rather than learning the system configuration. Managers understand this as reducing the total cost of ownership (TCO) for systems.

Imaging isn't limited to only desktop computers. You can image any system, including servers. For example, consider an organization that maintains 50 database servers in a large data center. The organization can

use imaging to deploy new servers or as part of its disaster recovery plan to restore failed servers. It is much quicker to deploy an image to rebuild a failed server than rebuild a server from scratch. If administrators keep the images up to date, this also helps ensure the recovered server starts in a secure state.

Remember this

A master image provides a secure starting point for systems. Administrators sometimes create them with templates or with other tools to create a secure baseline. They then use integrity measurements to discover when a system deviates from the baseline.

Patch Management

Software is not secure. There. I said it. As someone who has written a few programs over the years, that's not easy to say. In a perfect world, extensive testing would discover all the bugs, exploits, and vulnerabilities that cause so many problems.

However, because operating systems, applications, and firmware include millions of lines of code, testing simply doesn't find all the problems. Instead, most companies attempt to create secure and bug-free software as they're developing it and then make a best effort to test the software before releasing it. Later, as problems crop up, companies write and release patches or updates. Administrators must apply these patches to keep their systems up to date and protected against known vulnerabilities.

Some smaller organizations enable auto-updates. Systems regularly check for updates, download them when they're available, and automatically apply them.

Patch management ensures that systems and applications stay up to date with current patches. This is one of the most efficient ways to reduce operating system and application vulnerabilities because it protects systems from known vulnerabilities. Patch management includes a group of methodologies and consists of identifying, downloading, testing, deploying, and verifying patches.

Administrators often test updates in a sandbox environment such as a virtual machine. A sandbox environment provides an isolated environment. After testing the patches, administrators deploy them. They don't typically deploy the patches manually. Instead, they use third-party tools to deploy the patches in a controlled manner. For example, Microsoft Endpoint Configuration is a systems management tool used for many purposes, including patch management. It examines endpoints to determine if patches are installed.

In addition to deploying patches, systems management tools also include a verification component that verifies patch deployment. They periodically query the systems and retrieve a list of installed patches and updates. They then compare the retrieved list with the list of deployed patches and updates, providing reports for discrepancies. In some networks,

administrators combine this with network access control (NAC) technologies and isolate unpatched systems in quarantined networks until they are patched.

Improper or weak patch management results in preventable vulnerabilities that attackers can exploit. This includes vulnerabilities in operating systems, applications, and firmware.

Change Management Policy

The worst enemies of many networks have been unrestrained administrators. A well-meaning administrator can make what appears to be a minor change to fix one problem, only to cause a major problem somewhere else. A misconfiguration can take down a server, disable a network, stop email communications, and even stop all network traffic for an entire enterprise.

For example, I once saw a major outage occur when an administrator was troubleshooting a printer problem. After modifying the printer's Internet Protocol (IP) address, the printer began to work. Sounds like a success, doesn't it? Unfortunately, the new IP address was the same IP address assigned to a Domain Name System (DNS) server, and it created an IP address conflict. The conflict prevented the DNS server from resolving names to IP addresses. This resulted in a major network outage until another administrator discovered and corrected the problem.

These self-inflicted disasters were relatively common in the early days of IT. They still occur today, but organizations with mature change management processes in place have fewer of these problems. ***Change management*** defines the process for any type of system modifications or upgrades, including changes to applications. It provides two key goals:

- To ensure changes to IT systems do not result in unintended outages
- To provide an accounting structure or method to document all changes

When a change management program is in place, administrators are discouraged from making configuration changes without submitting the change for review and approval. In other words, they don't immediately make a change as soon as they identify a potential need for the change. This includes making any type of configuration changes to systems, applications, patches, or any other change. Instead, they follow the change management process before making a change.

Experts from different areas of an organization examine change requests and can either approve or postpone them. The process usually approves simple changes quickly. A formal change review board regularly

reviews postponed requests and can approve, modify, or reject the change. This entire process provides documentation for approved changes. For example, some automated change management systems create accounting logs for all change requests. The system tracks the request from its beginning until implementation. Administrators use this documentation for configuration management and disaster recovery. If a modified system fails, change and configuration management documentation identifies how to return the system to its pre-failure state.

Change management isn't only for computing devices. It's important to use these processes for any devices on the network, including firewalls, proxy servers, data loss prevention systems, mobile device management systems, routers, and switches.

Remember this

Patch management procedures ensure that operating systems, applications, and firmware are up to date with current patches. This protects systems against known vulnerabilities. Change management defines the process and accounting structure for handling modifications and upgrades. The goals are to reduce risks related to unintended outages and provide documentation for all changes.

Application Approved Lists and Block Lists

Application ***approved lists*** (sometimes called whitelists) and ***block lists*** (sometimes called application deny lists or black lists) are two additional methods used as endpoint security solutions. They can help protect hosts, including workstations, servers, and mobile devices.

An application ***allow list*** is a list of applications authorized to run on a system. After you identify the allowed list of applications, the system will block all other applications. This is the most restrictive of the two types of lists.

In contrast, an application ***block list*** is a list of applications the system blocks. As an example, if you found that users were installing a game called *ycda.exe*, you could create an application block list and add *ycda.exe*. However, all other applications would still be allowed.

Many mobile device management (MDM) applications use application allow lists and block lists to allow or block applications on mobile devices. MDM applications are discussed later in this chapter.

Messages that users see when they can't install an application due to an allow list or block list are sometimes cryptic. When users try to install an application that isn't allowed, the system will often report a permission issue or sometimes just fail with a vague error. However, application logs will typically include details on why the installation failed.

Some systems support quarantining applications that don't comply with allow or block lists. For example, if a user tries to install an application that isn't on an allow list, the system will quarantine the application, placing it in a protected area. A quarantined application won't run on the system but is retained so that administrators can examine it.

Remember this

An application approved list is a list of authorized software, and it prevents users from installing or running software that isn't on the list. An application block list is a list of unauthorized software and prevents users from installing or running software on the list.

Application Programming Interfaces

An ***application programming interface (API)*** is a software component that gives developers access to features or data within another application, a service, or an operating system. It's common for developers to use APIs with web applications, Internet of Things (IoT) devices, and cloud-based services.

As an example, Amazon provides tracking data by using web service-based APIs provided by different shippers. The input is the tracking ID, and the output is all the tracking data provided by the shipper. Similarly, APIs interact with IoT devices such as wireless thermostats to set and adjust temperatures.

APIs are susceptible to attacks, so developers need to address several API considerations to ensure that APIs aren't vulnerable to common exploits. These include:

- **Authentication.** Strong authentication methods will prevent unauthorized entities from using the APIs. The authentication method used can vary. For example, an API may use passwords with a second authentication factor, such as an authenticator app.
- **Authorization.** Authorization methods secure access to the API. For example, developers may have one level of access, and web applications may have another level of access. APIs could use cloud-based authorization services, such as OAuth. Chapter 2, “Understanding Identity and Access Management,” covers various authentication and authorization methods in more depth.
- **Transport level security.** The API should use strong security, such as TLS when transferring any traffic over the Internet. Early implementations of some wireless thermostats sent data over the Internet leaking information about thermostat owners. TLS encrypts the traffic preventing unauthorized entities from seeing the traffic.

Failure to address these issues increases the chance of successful API attacks. APIs are commonly used to access data. Any data breach is an

indicator of a potential attack using an API.

Indicators of potential API attacks vary depending on the API's purpose. If the API is accessing or transmitting data, a primary indicator is data leaked onto the Internet. If the API is interacting with websites, a potential indicator of an attack is hacked websites. API inspection and integration refers to testing the API for security and usability. Effective test processes can discover vulnerabilities before attackers exploit them.

Microservices and APIs

Microservices are code modules designed to do one thing well. They are typically small code modules that receive a value and respond with a value. Think of the Amazon example where the value is the tracking ID, and the output is the tracking data. Amazon must use a different web services-based API for each shipper.

In contrast, a single microservices code module could be used for any shipper. Customers would enter a tracking ID, and the microservices API would determine the shipper. It would then send the tracking ID to the appropriate shipper, receive the tracking data, and send the tracking data to the customer. A web services-based API is tied to a specific business, such as the individual shippers in this example. In contrast, a microservices module isn't tied to any specific business. This allows developers to use it in different applications without modifying it.

FDE and SED

Full disk encryption (FDE) encrypts an entire disk. Several applications are available to do this. For example, VeraCrypt is an open source utility that can encrypt partitions or an entire storage device.

Many hardware vendors now manufacture ***self-encrypting drives (SEDs)***, also known as hardware-based FDE drives. SEDs include encryption circuitry built into the drive. These typically allow users to enter credentials when they set up the drive. When users power up the system, they enter their credentials to decrypt the drive and boot the system.

The Opal Storage Specification is a set of specifications for SEDs. It defines what hardware vendors must do to ensure SEDs are configured to prevent unauthorized access. As an example, an Opal-compliant SED requires authentication by a user entering a username and password to unlock the drive upon bootup.

By default, SEDs don't need authentication. If an attacker removed one of these non-Opal-compliant drives from one system and installed it in another one, the attacker could access all the data. In contrast, when the SED is Opal-compliant, the attacker couldn't access the data without the user's credentials.

Remember this

A self-encrypting drive (SED) automatically encrypts and decrypts data on a drive without user intervention. An Opal-compliant drive requires users to enter credentials to unlock the drive when booting the system.

Boot Integrity

Many organizations implement boot integrity processes. These processes verify the integrity of the operating system and boot loading systems. For example, it can verify that key operating system files haven't been changed.

A ***measured boot*** goes through enough of the boot process to perform these checks without allowing a user to interact with the system. If it detects that the system has lost integrity and can no longer be trusted, the system won't boot.

Boot Security and UEFI

The Basic Input/Output System (BIOS) includes software that provides a computer with basic instructions on starting. It runs some basic checks, locates the operating system, and boots. The BIOS is a hardware chip that you can physically see and touch, and it includes software that executes code on the computer. The combination of hardware and software is firmware.

Newer systems use ***Unified Extensible Firmware Interface (UEFI)*** instead of BIOS. UEFI performs many of the same functions as BIOS but provides some enhancements. As an example, it can boot from larger disks, and it is designed to be CPU-independent.

Both BIOS and UEFI can be upgraded using a process called flashing. Flashing overwrites the software within the chip with newer software.

Trusted Platform Module

A ***Trusted Platform Module (TPM)*** is a hardware chip on the computer's motherboard that stores cryptographic keys used for encryption. Many laptop computers include a TPM, and you may see them on some mobile devices, too. However, if the system doesn't include a TPM, it is not feasible to add one. Once enabled, the TPM provides full disk encryption capabilities. It keeps hard drives locked or sealed until the system completes a system verification and authentication process.

A TPM supports secure ***boot attestation*** processes. When the TPM is configured, it captures signatures of key files used to boot the computer and

stores a report of the signatures securely within the TPM. When the system boots, the ***secure boot*** process checks the files against the stored signatures to ensure they haven't changed. If it detects that the files have been modified, such as from malware, it blocks the boot process to protect the data on the drive.

A ***remote attestation*** process works like the secure boot process. However, instead of checking the boot files against the report stored in the TPM, it uses a separate system. Again, when the TPM is configured, it captures the signatures of key files, but sends this report to a remote system. When the system boots, it checks the files and sends a current report to the remote system. The remote system verifies the files are the same and attests, or confirms, that the system is safe.

The TPM ships with a unique Rivest, Shamir, Adleman (RSA) private key burned into it, which is used for asymmetric encryption and can be used to support authentication. This private key is matched with a public key and provides a ***hardware root of trust*** or a known secure starting point. The private key remains private and is matched with a public key. Additionally, the TPM can generate, store, and protect other keys used for encrypting and decrypting disks. Chapter 10, “Understanding Cryptography and PKI,” discusses asymmetric encryption and public and private keys in more depth.

If the system includes a TPM, you use an application within the operating system to enable it. For example, many Microsoft systems include BitLocker, which you can enable for systems that include the TPM.

BitLocker uses the TPM to detect tampering of any critical operating system files or processes as part of a platform verification process. Additionally, users provide authentication, such as with a smart card, a password, or a personal identification number (PIN). The drive remains locked until the platform verification, and user authentication processes are complete.

If a thief steals the system, the drive remains locked and protected. An attacker wouldn't have authentication credentials, so he can't access the drive using a normal boot process. If the attacker tries to modify the operating system to bypass security controls, the TPM detects the tampering and keeps the drive locked. If a thief moves the drive to another system, the drive remains locked because the TPM isn't available.

Remember this

A Trusted Platform Module (TPM) is a hardware chip included on many laptops and mobile devices. It provides full disk encryption and supports a secure boot process and remote attestation. A TPM includes a unique RSA asymmetric key burned into the chip that provides a hardware root of trust.

Hardware Security Module

A hardware security module (**HSM**) is a security device you can add to a system to manage, generate, and securely store cryptographic keys. High-performance HSMs are external network appliances using TCP/IP. Smaller HSMs come as expansion cards you install within a server or as devices you plug into computer ports.

A **microSD HSM** is a microSD card that includes an HSM. A microSD card is small at 15 mm long x 11 mm wide x 1 mm thick, or .59 inches x .43 inches x .03 inches. You can install a microSD HSM into any device that has a microSD slot. With an adapter, you can install any microSD card into an SD card slot.

HSMs support the security methods of a TPM. They provide a hardware root of trust, secure boot, and can be configured for remote attestation. The cryptographic keys stored within the HSM also support authentication solutions.

One of the noteworthy differences between an HSM and a TPM is that HSMs are removable or external devices. In comparison, a TPM is a chip embedded into the motherboard. You can easily add an HSM to a system or a network, but if a system didn't ship with a TPM, it's not feasible to add one later. Both HSMs and TPMs provide secure encryption capabilities by storing and using RSA keys. Many high-performance servers use HSMs to store and protect keys.

Remember this

A hardware security module (HSM) is a removable or external device that can generate, store, and manage RSA keys used in asymmetric encryption. Many server-based applications use an HSM to protect keys. A microSD HSM is an HSM device installed on a microSD chip and can be installed on any device with a microSD or SD slot.

Protecting Data

Data is one of the most valuable resources any organization manages, second only to its people. If you ever tune into the news, you've likely heard about data breaches at organizations around the world. Unfortunately, data breaches are frequent, and they affect millions of people. In the worst-case scenarios, thieves use the stolen data to empty bank accounts, rack up fraudulent charges on credit cards, and steal individuals' identities.

Losing control of data affects the reputation, and often the financial bottom line, of an organization. One of the goals of attackers is often theft of data. If attackers can infiltrate a network, they often try to collect proprietary data and send it out of the network. In other situations, attackers take actions resulting in the loss of availability. For example, ransomware encrypts data so that users can no longer access it unless they pay a ransom.

Chapter 11, “Implementing Policies to Mitigate Risks,” covers security policies that an organization can implement to protect data. The security policy helps an organization classify and label its data. This section presents many of the security controls an organization can use to protect data based on the requirements set within a data security policy.

It's also important to use secure coding techniques to prevent data exposure or the loss of confidentiality. Confidentiality is primarily protected through encryption and strong access controls. This chapter discusses software-based and hardware-based encryption methods, and Chapter 10 covers specific encryption algorithms used to protect data. Chapter 6 discusses ransomware in more depth.

Data Loss Prevention

Organizations often use ***data loss prevention (DLP)*** techniques and technologies to prevent data loss. They can block the use of USB flash drives and control the use of removable media. They can also examine outgoing data and detect many types of unauthorized data transfers.

All traffic leaving the network is directed through an appliance that can examine the traffic. Administrators configure the DLP to look for specific words, phrases, or character strings. As an example, imagine an organization is working on a secret project with a code word of “DOH.” All documents associated with this project have the keyword within them. The DLP includes this keyword in its searches, and when it detects the keyword within an email, an attachment, or any other outgoing data, it blocks it. Administrators have the choice of configuring the DLP to notify security personnel, the user who sent it, or both.

Rights Management

Rights management (often called digital rights management) refers to the technologies used to provide copyright protection for copyrighted works. Copyright laws protect original creative works such as books, music, art, and other intellectual property. Unfortunately, criminals ignore laws.

Imagine you spent every moment of your free time for over a year writing a book. You decide to include a PDF version of the book to make it easier for some people to read it. After a short while, the book makes it onto a bestseller list on Amazon, and sales take off. Unfortunately, criminals post the PDF on the dark web and start selling it. Other criminals buy copies of the PDF and sell them on other websites claiming they are authorized to do so. After a short time, your sales drop off while the criminals continue to collect money from selling pirated copies.

Rights protection methods often prevent people from copying or printing files. Some encrypt the file and require a password to open them. While these sometimes work, criminals continue to find ways to bypass rights protection methods.

Removable Media

Removable media refers to any storage system that you can attach to a computer and easily copy data. It primarily refers to USB hard drives and USB flash drives, but many personal music devices, such as MP3 players, use the same type of flash drive memory as a USB flash drive. Users can plug them into a system and easily copy data to and from a system. Additionally, many of today's smartphones include storage capabilities using the same type of memory.

A USB data blocker can prevent someone from writing any data to a USB drive. Some USB data blockers will also prevent systems from reading data from a USB or other removable device.

Organizations recognize that removable media can be an attack vector, so it's common for an organization to include security policy statements to prohibit the use of USB flash drives and other removable media. Some technical policies block the use of USB drives completely. A USB data blocker prevents users from writing any data to a USB drive. Some USB data blockers will also prevent systems from reading data from a USB or other removable device. This prevents malware from being delivered via removable media, as discussed in Chapter 9, "Implementing Controls to Protect Assets."

A DLP solution is more selective and can prevent a user from copying or printing files with specific content. For example, it's possible to configure a DLP solution to prevent users from copying or printing any classified documents marked with a label of Confidential. The DLP software scans all documents sent to the printer, and if it contains the label, the DLP software blocks it from reaching the printer.

In addition to blocking the transfer, a DLP solution will typically log these events. Some DLP solutions will also alert security administrators of the event. Depending on the organization's policy, personnel may be disciplined for unauthorized attempts to copy or print files.

Data Exfiltration

Data exfiltration is the unauthorized transfer of data outside an organization and is a significant concern. In some cases, attackers take control of systems and transfer data outside an organization using malware. It's also possible for malicious insiders to transfer data.

Chapter 3 discusses different types of content filters used in unified threat management (UTM) devices. These devices monitor incoming data streams looking for malicious code. In contrast, a network-based DLP monitors outgoing data looking for sensitive data, specified by an administrator.

DLP systems can scan the text of all emails and the content of any attached files, including documents, spreadsheets, presentations, and databases. Even if a user compresses a file as a zipped file before sending it, the DLP examines the contents by simply unzipping it.

As an example, I know of one organization that routinely scans all outgoing emails looking for Personally Identifiable Information (PII), such as Social Security numbers. The network-based DLP includes a mask to identify Social Security numbers as a string of numbers in the following format: ####-##-####. If an email or an attachment includes this string of numbers, the DLP detects it, blocks the email, and sends an alert to a security administrator.

Many organizations classify and label data using terms such as Confidential, Private, and Proprietary. It is easy to include these search terms in the DLP application, or any other terms considered important by the organization.

Network-based DLP systems are not limited to scanning only email. Many can scan the content of other traffic, such as FTP and HTTP traffic. Sophisticated data exfiltration attacks often encrypt data before sending it out, making it more difficult for a DLP system to inspect the data. However, a DLP system can typically be configured to look for outgoing encrypted data and alert security administrators when it is detected.

Remember this

Data exfiltration is the unauthorized transfer of data out of a network. Data loss prevention (DLP) techniques and technologies can block the use of USB devices to prevent data loss and monitor outgoing email traffic for unauthorized data transfers.

Protecting Confidentiality with Encryption

As mentioned in Chapter 1, “Mastering Security Basics,” one of the primary ways you can prevent the loss of confidentiality is by encrypting

data. This includes encrypting data at rest no matter what type of device it is stored on and encrypting data in transit no matter what type of transmission media is used. It is much more difficult for an attacker to view encrypted data than it is to view unencrypted data.

You can use other tools to restrict access to data, but this isn't always effective. For example, consider the Microsoft New Technology File System (NTFS), which allows you to configure permissions within access control lists (ACLs). You can use NTFS to set permissions on files and folders to restrict access. However, if a thief steals a laptop with NTFS-protected files, it's a simple matter to access them. The thief simply moves the drive to another system as an extra drive, logs on as the administrator, and takes ownership of the files. Encryption isn't as easy to bypass.

Database Security

Another form of software-based encryption is with databases. For example, many database applications such as Oracle Database or Microsoft SQL Server can encrypt data held within a database. Although it's possible to encrypt the entire database, it's more common to encrypt specific data elements.

As an example, imagine a database that includes a table named Customers. Each record within the table has multiple columns, including customer number, last name, first name, credit card number, and security code. Instead of encrypting the entire table, administrators can choose to encrypt only the credit card number and security code columns within each record. Database column encryption protects the sensitive data but doesn't waste valuable processing power encrypting data that isn't sensitive.

Some customer databases store passwords as hashes or salted hashes. Chapter 10 discusses hashing and salting techniques in more depth, and Chapter 11 discusses tokenization, another database security technique. Tokenization replaces sensitive data elements with substitute values.

Remember this

The primary methods of protecting the confidentiality of data are with encryption and strong access controls. Database column encryption protects individual fields within a database.

Summarizing Cloud Concepts

Cloud computing refers to accessing computing resources via a different location than your local computer. In most scenarios, you're accessing these resources through the Internet or off-premises.

As an example, if you use web-based email such as Gmail, you're using cloud computing. More specifically, web-based email is a Software as a Service cloud computing service. You know that you're accessing your email via the Internet, but you don't know the location of the physical server hosting your account. It could be in a data center in the middle of Virginia, tucked away in Utah, or just about anywhere else in the world.

Cloud storage has become very popular for both individuals and organizations. For example, Apple offers iCloud storage, Microsoft offers OneDrive, and Google offers Google Drive. You can typically get some storage for free or pay nominal fees for more storage.

Heavily utilized systems and networks often depend on cloud computing resources to handle increased loads. As an example, consider the biggest shopping day in the United States—Black Friday, the day after Thanksgiving, when retailers hope to go into the black. Several years ago, Amazon.com had so much traffic during the Thanksgiving weekend that its servers could barely handle it. The company learned its lesson, though. The next year, it used cloud computing to rent access to servers specifically for the Thanksgiving weekend, and, despite increased sales, it didn't have any problems.

As many great innovators do, Amazon didn't look at this situation as a problem but as an opportunity. If it needed cloud computing for its heavily utilized system, other companies probably had the same need. Amazon now hosts cloud services to other organizations via its Amazon Elastic Compute Cloud (Amazon EC2) service. Amazon EC2 combines virtualization with cloud computing, and they currently provide a wide variety of services via Amazon EC2.

Software as a Service

Software as a Service (SaaS) includes any software or application provided to users over a network such as the Internet. Internet users access the SaaS applications with a web browser. It usually doesn't matter which web browser or operating system a SaaS customer uses. They could be using Microsoft Edge, Chrome, Firefox, or just about any web browser.

As mentioned previously, web-based email is an example of SaaS. This includes Gmail, Yahoo! Mail, and others. The service provides all the components of email to users via a simple web browser.

If you have a Gmail account, you can also use Google Docs, another example of SaaS. Google Docs provides access to several SaaS applications, allowing users to open text documents, spreadsheets, presentations, drawings, and PDF files through a web browser.

A talented developer and I teamed up to work on a project a while ago. He's an Apple guy running a macOS while I'm a Microsoft guy running Windows, and we live in different states. However, we post and share documents through Google Docs, and despite different locations and different applications running on our individual systems, we're able to collaborate easily. One risk is that our data is hosted on Google Docs, and if attackers hack into Google Docs, our data may be compromised.

Platform as a Service

Platform as a Service (PaaS) provides customers with a preconfigured computing platform they can use as needed. It provides the customer with an easy-to-configure operating system, combined with appropriate applications and on-demand computing.

Many cloud providers refer to this as a managed hardware solution. As an example, I host <https://gcfgacert.com/> on a virtual server through a hosting provider using one of their offerings.

The hosting provider provides several features, including an installed operating system, a core software package used for web servers, Apache as a web server, antivirus software, spam protection, and more. Additionally, they keep the operating system up to date with relevant updates and patches. I manage the software used for the website, including software changes and updates. However, I don't need to worry about managing the server itself. Often, when the server has developed a problem, the hosting provider fixed it before I was even aware of the problem.

Remember this

Applications such as web-based email provided over the Internet are Software as a Service (SaaS) cloud-based technologies. Platform as a Service (PaaS) provides customers with a fully managed platform, including hardware, operating systems, and limited applications. The vendor keeps systems up to date with current patches.

Infrastructure as a Service

Infrastructure as a Service (IaaS) allows an organization to outsource its equipment requirements, including the hardware and all support operations. The IaaS service provider owns the equipment, houses it in its data center, and performs all the required hardware maintenance. The customer essentially rents access to the equipment and often pays on a per-use basis.

Many cloud providers refer to this as a self-managed solution. They provide access to a server and may include a default operating system installation, but customers must configure it and install additional software based on their needs. Additionally, customers are responsible for all operating system updates and patches.

IaaS can also be useful if an organization is finding it difficult to manage and maintain servers in its own data center. By outsourcing its requirements, the company limits its hardware footprint. It can do this instead of, or in addition to, virtualizing some of its servers. With IaaS, it needs fewer servers in its data center and fewer resources, such as power and personnel, to manage the servers.

IaaS is often used as a serverless architecture. A serverless architecture allows an organization to build and run applications without managing the infrastructure. The applications are still running on servers, but the organization doesn't have to worry about maintaining them.

Anything as a Service

Anything as a Service (XaaS) refers to cloud services beyond SaaS, PaaS, and IaaS. XaaS includes a wide assortment of services that can be delivered via the cloud, such as communications, databases, desktops, storage, security, and more. The cloud provider typically manages all the resources keeping everything operational and up to date.

Information technology (IT) as a service is another way of thinking of XaaS. In other words, any IT services delivered over the cloud can simply be labeled as XaaS. A great benefit to all of us is that we don't need to memorize an endless number of additional acronyms.

Remember this

Infrastructure as a Service (IaaS) provides customers with access to hardware in a self-managed platform. Anything as a Service (XaaS) refers to cloud-based services other than SaaS, PaaS, or IaaS. XaaS includes services such as communications, databases, desktops, storage, security, and more.

Cloud Deployment Models

There are four categories of cloud deployment models: public, private, community, and hybrid. These identify who has access to the cloud infrastructure.

Public cloud services are available from third-party companies, such as Amazon, Google, Microsoft, and Apple. They provide similar services to anyone willing to pay for them.

A ***private cloud*** is set up for specific organizations. For example, the Shelbyville Nuclear Power Plant might decide it wants to store data in the cloud, but does not want to use a third-party vendor. Instead, the plant chooses to host its own servers and make these servers available to internal employees through the Internet.

Communities with shared concerns (such as shared goals, security requirements, or compliance considerations) can share cloud resources within a ***community cloud***. As an example, imagine that the Shelbyville Nuclear Power Plant and several schools within Springfield decided to share educational resources within a cloud. They could each provide resources for the cloud, and only organizations within the community would have access to the resources.

Not all cloud implementations fit exactly into these definitions, though. A ***hybrid cloud*** is a combination of two or more clouds. They can be private, public, community, or a combination of these. These retain separate identities to help protect resources in private clouds. However, they are bridged together, often in such a way that it is transparent to the users.

Remember this

Private clouds are only available for one organization. Third-party companies provide public cloud services, and public cloud services are available to anyone. Two or more organizations with shared concerns can share a community cloud. A hybrid cloud is a combination of two or more clouds.

Managed Security Service Provider

A managed security service provider (MSSP) is a third-party vendor that provides security services for smaller companies. Many small companies use them to improve the companies' overall security posture without adding an army of security professionals to their staff.

In the early days of the Internet, an Internet Service Provider (ISP) provided basic services to customers. They sometimes sold firewalls to these customers and administered the firewalls remotely. MSSPs have expanded basic firewall service to just about anything a larger organization would have. The following list shows some of the services an MSSP may provide:

- Patch management
- Vulnerability scanning
- Spam and virus filtering
- Data loss prevention (DLP)
- Virtual private network connections
- Proxy services for web content filtering
- Intrusion detection and prevention systems
- Unified threat management (UTM) appliances
- Advanced firewalls such as next-generation firewalls (NGFWs)

An MSSP may sell appliances, such as NGFWs and UTMs hosted on the organization's premises, and administer them remotely. However, it's also possible to host such devices within the cloud and redirect all organizational traffic through the cloud connection.

A managed service provider (MSP) is similar to an MSSP. However, instead of focusing only on security services, an MSP provides any information technology (IT) services that an organization needs.

Remember this

A managed security service provider (MSSP) is a third-party vendor that provides security services for an organization. A managed service provider (MSP) provides any IT services needed by an organization, including security services provided by an MSSP.

Cloud Service Provider Responsibilities

One important consideration with cloud service models is the difference in responsibilities assigned to a ***cloud service provider (CSP)*** and the customer. A CSP is an entity that offers one or more cloud services via one or more cloud deployment models. Figure 5.3 (derived partly from Figure 2 in the US Department of Defense (DoD) “Cloud Computing Security Requirements Guide”) shows how responsibilities are divided between the customer and the CSP in the IaaS, PaaS, and SaaS models. This includes both maintenance responsibilities and security responsibilities.

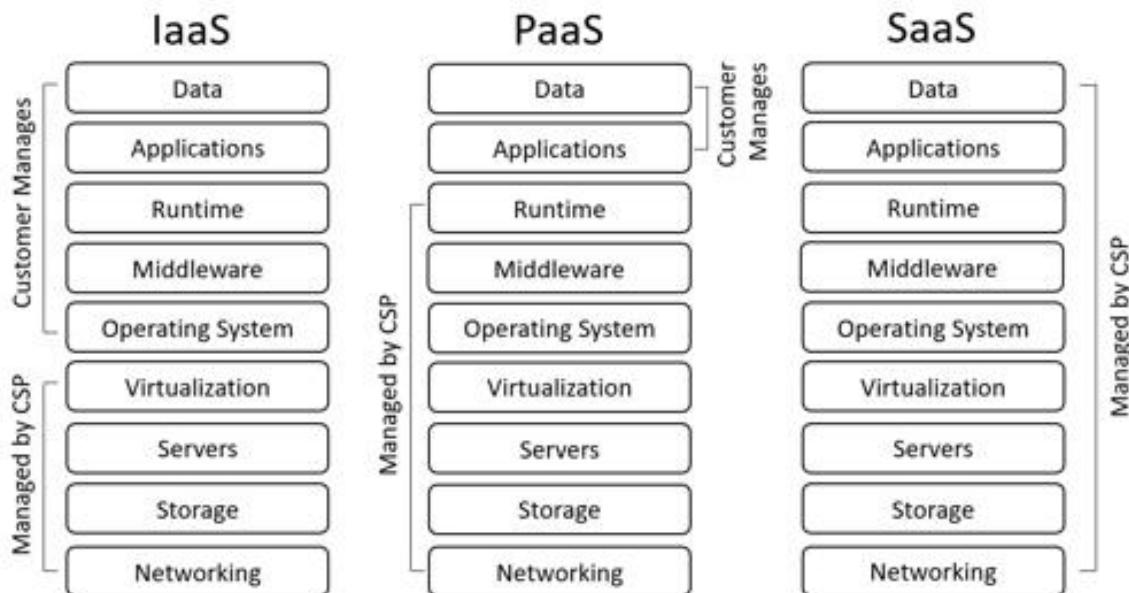


Figure 5.3: Security responsibilities with cloud models

As an example, consider Gmail for SaaS. Google is responsible for maintaining everything to ensure Gmail is available. Additionally, Google has the primary responsibility of ensuring security for Gmail. If you use it, you still have some responsibility, such as ensuring you use a strong password that is different from other online accounts to protect your data. The SaaS model typically provides application security because the cloud provider manages everything.

In the PaaS model, the CSP is responsible for providing a platform and ensuring it remains available. This includes everything except applications

and data, which the customer provides. Middleware and runtime components may not be familiar to you.

Middleware is software that is added to an operating system to extend its basic capabilities. As an example, Apache can be added to a Linux operating system to allow the system to function as a web server. Runtime is a hosting environment, such as a container on a server. The CSP typically rents access to any server to multiple users. Each customer has access to core elements of the operating system, but runs within a container. The runtime environment isolates each customer's container from other containers on the server.

The customer assumes more responsibility in the IaaS model, taking responsibility for installing and maintaining the operating system and any runtime and middleware components. A CSP will typically rent an entire server to a customer in the IaaS model. This can be either a physical server or a virtual server.

CSPs are also responsible for services integration. This ensures that all elements of a cloud solution work together.

Cloud Security Controls

When picking a CSP, an organization needs to consider various cloud security controls. CompTIA listed the security controls covered in this section, and many of them match terminology listed in Google Cloud and Amazon Web Services (AWS) documentation:

- **High availability and high availability across zones.** High availability indicates a system or service remains operational with almost zero downtime. It's typically achieved by using multiple load-balancing nodes, as discussed in Chapter 9. High availability across zones indicates that the nodes are located in different cloud locations, such as separate geographic locations. If one node fails, other nodes can take on its load.
- **Resource policies.** In this context, resources refer to cloud-based resources such as folders, projects, and virtual machine instances. Customers rent access to resources, and the CSP resource policies ensure customers don't create more resources than their plan allows.
- **Secrets management.** Secrets refer to passwords and encryption keys that users create. A secrets management system stores and manages secrets, including keeping them secure.
- **Integration and auditing.** The CSP integrates security controls into the cloud-based resources, and auditing methods help customers identify the effectiveness of security controls at protecting the confidentiality, integrity, and availability of cloud-based resources.

Cloud-based storage allows customers to store data in the cloud. AWS stores data in buckets. Google uses Google Drive and allows users to store files in a hierarchical format similar to folders in Windows. However, both support the following characteristics:

- **Permissions.** Permissions identify who can access the data. While the processes differ with different CSPs, the concepts are similar to file system permissions covered in Chapter 2.
- **Encryption.** Encryption protects the confidentiality of data, and CSPs commonly provide encryption services. This prevents unauthorized personnel from accessing data.

- **Replication.** Data replication is the process of creating a copy of data and storing it in a different location. For example, you can replicate data on a desktop computer to a removable drive. Cloud data replication creates a copy of data in the cloud.

CSPs provide entire networks to organizations that need them. The following list describes some common characteristics of cloud-based networks:

- **Virtual networks.** A CSP creates virtual networks for customers that need them. These typically use software-defined network technologies (described later in this chapter) instead of physical routers and switches. A single server can host an entire virtual network.
- **Public and private subnets.** Public subnets have public IP addresses and are accessible via the Internet. Private subnets have private IP addresses and aren't directly accessible via the Internet. Organizations typically use screened subnets for any public subnets that need to be accessible via the Internet. Virtual networks can mimic this design with both public and private subnets.
- **Segmentation.** Just as local networks support segmentation with virtual local area networks (VLANs) and screened subnets, cloud-based networks can segment computers or networks.

The CSPs compute engine lets customers create and run a variety of solutions from single websites to full virtual networks:

- **Security groups.** Security groups are similar to groups used in Windows and described in the role-based access control model discussed in Chapter 1. Administrators assign permissions to a group and add users to the account.
- **Dynamic resource allocation.** Cloud-based resources typically support elasticity (also discussed in Chapter 1). Elasticity indicates the CSP can dynamically allocate additional resources, such as more processors, more memory, or more disk space to a cloud-based resource when it's needed. When the additional resources are no longer needed, the CSP can dynamically remove them.
- **Instance awareness.** Instance awareness refers to the ability of the CSP to know and report how many instances of cloud-based

resources an organization is renting. This can help an organization avoid VM sprawl.

- **Virtual private cloud (VPC) endpoint.** A VPC endpoint is a virtual device within a virtual network. Users or services can connect to the VPC endpoint and then access other resources via the virtual network instead of accessing the resources directly via the Internet. This can significantly reduce the bandwidth required to access resources directly.
- **Transit gateway.** A transit gateway is used to connect VPCs to an on-premises network.
- **Container security.** Container virtualization (described earlier) runs services or applications within containers. CSPs commonly use containers with cloud resources, and container security protects these containers.

On-Premises Versus Off-Premises

Organizations can access cloud-based resources on-premises or off-premises. On-premises indicates that all resources are owned, operated, and maintained within the organization's properties. Employees may still access the resources via the cloud while working from home, while traveling, or from remote offices.

It's more common for an organization to rent access to cloud-based resources from a cloud service provider (CSP) located off-premises. The CSP maintains the hardware used to host the resources. Depending on the cloud model (discussed later in this chapter), the CSP may maintain more than just the hardware.

On-Premises

In an on-premises solution, the organization retains complete control over all the cloud-based resources, including any data stored in the on-premises cloud. This allows the organization to implement multiple security controls to protect the on-premises cloud resources and provide cybersecurity resilience.

The organization can also implement its own authentication and authorization controls. This makes it easier to use single sign-on (SSO) without requiring employees to have separate accounts for cloud-based resources.

However, the organization is responsible for all maintenance of the on-premises resources. Unless the organization already has a large IT department, maintenance of on-premises cloud-based resources may be overwhelming.

Off-Premises

One of the primary benefits of an off-premises solution is that the CSP performs the maintenance. As discussed previously, the CSP has the most responsibility for maintaining the cloud-based resources in the SaaS model. Even in the IaaS model, the CSP still ensures the hardware is operational.

A drawback with cloud-based resources kept off-premises is that an organization doesn't know where data is stored. If data is stored in another

country, it could result in legal implications requiring the organization to comply with different laws in different countries. However, organizations can require CSPs to store data in a single country only.

Digital forensics (discussed in Chapter 11) can be challenging enough when all the evidence is on-premises. When an organization uses cloud resources, it can add additional risks. Anytime an organization contracts with a cloud provider, the cloud provider becomes a third-party source providing the service. This includes when the cloud provider holds data or provides any type of service.

Cloud Access Security Broker

CSPs employ native controls to protect cloud-based resources. This may be enough for some customers, but other customers want more security features and seek third-party solutions, such as a cloud access security broker (CASB).

A CASB is a software tool or service deployed between an organization's network and the cloud provider. It provides security by monitoring traffic and enforcing security policies. Anything accessible via the Internet is an attack vector, and that includes cloud-based resources. However, a CASB can help organizations mitigate risks.

The CASB software can be on-premises or in the cloud. If it is on-premises, every device needs to have the CASB software installed. Installing software on all devices can be a challenge if employees are connecting to the corporate network with their own devices. In contrast, if the CASB software is in the cloud, endpoint devices do not need additional software. However, the organization needs to redirect all Internet traffic to the cloud-based CASB solution.

Cloud-Based DLP

It's common for personnel within organizations to store data in the cloud. This makes it easier to access the data from any location and from almost any device. Cloud-based DLP solutions allow an organization to implement policies for data stored in the cloud.

As an example, an organization can implement policies to detect Personally Identifiable Information (PII) or Protected Health Information (PHI) stored in the cloud. After detecting the data, a DLP policy can be configured to take one or more actions such as sending an alert to a security administrator, blocking any attempts to save the data in the cloud, and quarantining the data.

Remember this

A cloud-based DLP can enforce security policies for data stored in the cloud, such as ensuring that Personally Identifiable Information (PII) is encrypted.

Next-Generation Secure Web Gateway

A next-generation secure web gateway (SWG) is a combination of a proxy server and a stateless firewall. The SWG is typically a cloud-based service, but it can be an on-site appliance. Clients are configured to access all Internet resources via the SWG, and it filters traffic to prevent threats from infiltrating the network. Some of the services provided by the SWG include:

- URL filtering to prevent users from visiting unauthorized sites
- Stateless packet filtering to detect and block malicious traffic
- Malware detection and filtering to block malware
- Network-based data loss protection (DLP)
- Sandboxing to check for threats

Remember this

A cloud access security broker (CASB) is a software tool or service deployed between an organization's network and the cloud provider. It provides security by monitoring traffic and enforcing security policies. A next-generation secure web gateway (SWG) provides proxy services for traffic from clients to Internet sites, such as filtering URLs and scanning for malware.

Firewall Considerations

When creating virtual networks in the cloud, there are some additional items to consider. Just as physical networks need firewalls to prevent unauthorized access, virtual networks also need firewalls. It's common to use two firewalls to create a screened subnet, as discussed in Chapter 3. This provides segmentation and helps reduce an attacker's success when attacking the virtual network.

Cloud-based firewalls typically operate on all seven layers of the Open Systems Interconnection (OSI) model, allowing them to filter traffic on the application layer. Appendix D, "The OSI Model," provides a refresher on the OSI model if you need it.

The cost of cloud-based firewalls varies depending on how they're used. Smaller organizations can rent access to a firewall for employees on a per-user basis. This relieves the organization from managing the firewall. Larger organizations might use a virtual server instance for a firewall, and they're charged based on bandwidth.

Infrastructure as Code

Infrastructure as code refers to managing and provisioning data centers with code to define VMs and virtual networks. It reduces the complexity of creating virtual objects by allowing administrators to run a script to create them.

Software-Defined Networking

A ***software-defined network (SDN)*** uses virtualization technologies to route traffic instead of using hardware routers and switches. More and more cloud service providers are implanting SDNs as part of an overall IaaS solution.

An SDN separates the data planes and control planes within a network. Another way of thinking of this is that an SDN separates the logic used to forward or block traffic (the data plane) and the logic used to identify the path to take (the control plane).

Hardware routers use rules within an ACL to identify whether a router will forward or block traffic on the data plane. This is always proprietary because it's implemented on specific hardware routers. However, an SDN implements the data plane with software and virtualization technologies, allowing an organization to move away from proprietary hardware.

Routing protocols such as Open Shortest Path First (OSPF) and Border Gateway Protocol (BGP) help routers determine the best path to route traffic on the control plane. Routers use these protocols to share information, creating a map of the known network. An SDN can still use these routing protocols but without the hardware routers.

Chapter 2 discusses attribute-based access control (ABAC), commonly used in SDNs. Instead of rules within ACLs, ABAC models allow administrators to create data plane policies to route traffic. A huge benefit of these policies is that they typically use plain language statements instead of complex rules within an ACL.

Software-Defined Visibility (SDV)

Software-defined visibility (SDV) refers to the technologies used to view all network traffic. As an organization uses more cloud-based

resources, some network traffic may bypass security devices. By adding SDV capabilities, it ensures that all traffic is viewable and can be analyzed.

Edge and Fog Computing

Edge computing is the practice of storing and processing data close to the devices that generate and use the data. Many non-edge solutions store all the data in the cloud, requiring round trips to retrieve and process the data. However, this takes too much time for many situations.

As an example, think of autonomous technologies in automobiles. Imagine the speed limit is 60 miles per hour (MPH), and you set the adaptive cruise control to 60 MPH. If the highway becomes congested, cars ahead of you will start slowing down. However, the adaptive cruise control senses the change and automatically slows down, keeping a specified distance between you and the car in front of you. In some cases, the congestion might appear quickly, requiring quick responses from the adaptive cruise control and a crash avoidance system. If your car is sending sensor data to the cloud for processing, your car may crash before it gets any responses.

However, onboard processors monitor the sensors with edge computing, process the data, and slow your car down almost immediately. This eliminates issues with latency.

Fog computing is almost the same thing as edge computing. The primary difference is that fog computing uses a network close to the device and may have multiple nodes sensing and processing data within the fog network. In contrast, edge computing stores and processes the data on single nodes or appliances.

Cloud Security Alliance

The Cloud Security Alliance (CSA) is a not-for-profit organization that promotes best practices related to the cloud. It's a member-based organization and has several thousand volunteers working on research and other projects. They created the Certificate of Cloud Security Knowledge (CCSK) certification, which focuses on cloud security.

They also created the CSA Cloud Controls Matrix (CCM), a cybersecurity control framework. Version 4.0 of the CCM organizes over 200 security control objectives in 17 domains. Many of the security controls in the CCM are similar to the security controls in SP-800-53 Revision 5, "Security and Privacy Controls for Information Systems and Organizations." The big difference is that the CCM is focused on security controls related to cloud-based resources. However, SP 800-53 Revision 5 is for all computing systems.

Deploying Mobile Devices Securely

Mobile devices represent significant challenges for organizations today. Organizations need to determine if employees can connect mobile devices to the network. If so, organizations need to identify methods to manage the security related to the devices, monitor the devices, and enforce security policies.

What is a mobile device? Within the context of the CompTIA Security+ exam, you can think of a mobile device as a smartphone or tablet. Further, NIST SP 800-124, “Guidelines for Managing the Security of Mobile Devices in the Enterprise,” mentions that mobile devices have additional characteristics, such as at least one wireless network interface, local data storage, an operating system, and the ability to install additional applications.

Mobile devices typically have other optional features. This includes other networking options such as Bluetooth, near field communication, cellular access for voice communications, and Global Positioning System (GPS) services. They typically include a digital camera, a video recorder, a microphone, and the ability to transfer data to another system such as a traditional computer or to other mobile devices.

NIST SP 800-124 excludes laptop and desktop computers because they don’t contain features in many mobile devices, such as a GPS and sensors that monitor the device’s movement, such as accelerometers and a gyroscope. A GPS can pinpoint the location of a device, even if it moves. NIST also excludes basic cell phones, digital cameras, and Internet of Things (IoT) devices. These don’t have an operating system or a limited functioning operating system.

Deployment Models

Any device connected to an organization's network represents a potential risk. As a simple example, if someone connects an infected device to a network, it might be able to infect other devices on the network. To limit this risk, organizations take steps to monitor and manage mobile devices.

If the organization owns all the devices connected to the network, it's a simple matter to monitor and manage them. However, if employees own these devices (such as their own smartphone), monitoring and managing the devices becomes more challenging. As an example, employees want to access the network resources with their own device, but they are sometimes resistant to allowing the organization to monitor and manage their personal devices.

The following list identifies some common deployment models for mobile devices. Notice that in some models, the organization owns the device, but in other models, employees own the device:

- **Corporate-owned.** In this traditional deployment model, the organization purchases devices and issues them to employees.
- **COPE (corporate-owned, personally enabled).** *COPE* is similar to the traditional corporate-owned model, but the primary difference is that the employees are free to use the device as if it was their personally owned device. This allows employees to use the devices for personal activities in addition to connecting them to the organization's network. Because the organization owns the devices, it makes it easier to manage them.
- **BYOD (bring your own device).** Some organizations allow employees to bring their own mobile devices to work and attach them to the network. Employees are responsible for selecting and supporting the device, and they typically must comply with a ***BYOD*** policy when connecting their device to the network. While this is simple for the employees, it is sometimes referred to as *bring your own disaster* among IT professionals. Because employees can have any possible device, the IT department is now responsible for

supporting, monitoring, and managing any possible device owned by employees.

- **CYOD (choose your own device).** To avoid some of the challenges related to supporting any possible mobile devices, some organizations create a list of acceptable devices and publish the list in a BYOD policy. Employees can purchase devices on the list and bring them to work. This gives the IT department a specific list of devices to support, monitor, and manage. Some people confuse CYOD with COPE. In the COPE model, the organization purchases the device and may give the employees a choice of different devices. In the CYOD model, the employee purchases the device.

Remember this

Corporate-owned, personally enabled (COPE) devices are owned by the organization, but employees can use them for personal reasons. A bring your own device (BYOD) policy allows employees to connect their own personal devices to the corporate network. A choose your own device (CYOD) policy includes a list of approved devices that employees can purchase and connect to the network.

Connection Methods and Receivers

There are several methods that mobile devices can use to connect to networks and other devices. They include:

- **Cellular.** Smartphones (and many tablets) include the ability to connect to a cellular network, such as a third-generation (3G), long-term-evolution (LTE), fourth-generation (4G), 4G LTE, or 5G network. The type of network you connect with is dependent on your cellular provider and your device. Newer generations typically provide increased speed for digital transfers and improved voice communications.
- **Wi-Fi.** Mobile devices almost always have a wireless network interface that you can configure to connect to a wireless network. Chapter 4 discusses common wireless security methods and wireless protocols.
- **Bluetooth.** Most mobile devices include Bluetooth support. Bluetooth is a wireless protocol commonly used with personal area networks. For example, most smartphones support the use of a Bluetooth headset for hands-free use of the phone. Additionally, some technologies use Bluetooth to connect two smartphones. Chapter 4 discusses some Bluetooth attacks.
- **NFC (near field communication).** NFC is commonly used as a payment gateway allowing you to make payments simply by waving your phone in front of an NFC reader at a retailer. You can also create a peer-to-peer network between two devices with NFC.
- **RFID (Radio Frequency Identification).** RFID systems transmit data over the air using RF signals and some NFC systems use RFID technologies. Chapter 4 discusses NFC and RFID attacks.
- **Infrared.** Infrared is a line-of-sight wireless technology used by some mobile devices. This is the same technology used by most remote controls for TVs and other audiovisual equipment. Some people add apps to their smartphones and use them as a universal remote for their equipment. It's also possible to transfer files between smartphones using infrared, as long as both smartphones support infrared.

- **USB (Universal Serial Bus).** Mobile devices can typically connect to a desktop PC or laptop via a USB cable. Most Apple devices have a Lightning port and can connect to PCs via a Lightning to USB cable. Many Android devices have a mini-USB cable and can connect to PCs via a mini-USB to standard USB cable.
- **Point-to-point.** A point-to-point connection is between two wireless devices, such as between two smartphones. Point-to-point connections can use technologies such as Bluetooth, NFC, and RFID.
- **Point-to-multipoint.** A point-to-multipoint connection creates an ad hoc network. In ad hoc mode, wireless devices connect to each other without an AP. For example, if you and another user have wireless laptops, you can create an ad hoc wireless network to connect your two computers. Ad hoc is Latin for “as needed,” which is a good way to think about an ad hoc wireless network. You create it as needed. In contrast, when you connect to a wireless network via an AP, you are using infrastructure mode.
- **Payment methods.** Some organizations restrict the use of payment methods on COPE devices. This can reduce risks for the devices owned by the organization. However, an organization is unlikely to restrict payment methods on devices owned by employees.

Mobile Device Management

Mobile device management (MDM) includes the technologies to manage mobile devices. The goal is to ensure these devices have security controls in place to keep them secure. Some vendors sell **unified endpoint management (UEM)** solutions to manage mobile devices.

UEM tools ensure systems are kept up to date with current patches, have antivirus software installed with up-to-date definitions, and are secured using standard security practices. While some of these tools initially focused on desktop PCs and laptops, they have expanded to include many mobile devices. As an example, Microsoft Endpoint Configuration Manager includes support for mobile devices such as Apple iOS-based devices and Android-based devices.

MDM applications help administrators manage mobile devices. The following bullets describe many of the MDM concepts that apply to mobile devices:

- **Application management.** MDM tools can restrict what applications can run on mobile devices. They often use application allow lists to control the applications and prevent unapproved applications from being installed. Mobile application management (MAM) tools are typically built into MDM tools, but some MAM tools focus only on controlling applications.
- **Full device encryption.** Encryption protects against loss of confidentiality on multiple platforms, including workstations, servers, mobile devices, and data transmissions. Encryption methods such as full device encryption provide device security, application security, and data security. While an organization can ensure corporate-owned devices use full device encryption, this isn't always possible when employees use their own devices.
- **Storage segmentation.** In some mobile devices, it's possible to use storage segmentation to isolate data. For example, users might be required to use external storage for any corporate data to reduce the risk of data loss if the device is lost or stolen. It's also possible to create separate segments within the device. Users would store

corporate data within an encrypted segment and personal data elsewhere on the device.

- **Content management.** After creating segmented storage spaces, it's important to ensure that appropriate content is stored there. An MDM system can ensure that all content retrieved from an organization source (such as a server) is stored in an encrypted segment. Also, content management can force the user to authenticate again when accessing data within this encrypted segment.
- **Containerization.** The virtualization section earlier in this chapter discusses the use of container virtualization. Organizations can also implement containerization in mobile devices and encrypt the container to protect it without encrypting the entire device. Running an organization's application in a container isolates and protects the application, including any of its data. This is very useful when an organization allows employees to use their own devices.
- **Passwords and PINs.** Mobile devices commonly support the use of passwords or personal identification numbers (PINs). MDM systems typically support password policies, similar to the password policies used in desktop systems. The only limitation is that some mobile devices only support PINs, while others support either passwords or PINs.
- **Biometrics.** Chapter 2 discusses biometrics as one of the authentication factors (something you are). Many mobile devices now support biometrics for authentication. For example, you can teach the device your fingerprint and then use your fingerprint to authenticate instead of entering a password or PIN.
- **Screen locks.** Most devices support the use of a passcode or password to lock the device. This is like a password-protected screen saver on desktop systems that automatically locks the device after a specified number of minutes. It prevents someone from easily accessing the device and the data it contains. This is often combined with an erase function. For example, if someone steals the phone and enters the incorrect passcode 10 times, the smartphone will automatically erase all data on the phone.

- **Remote wipe.** *Remote wipe* capabilities are useful if the phone is lost. It sends a remote signal to the device to wipe or erase all the data. The owner can send a remote wipe signal to the phone to delete all the data on the phone. This also deletes any cached data, such as cached online banking passwords, and provides a complete sanitization of the device by removing all valuable data.

Remember this

Mobile device management (MDM) tools help enforce security policies on mobile devices. This includes the use of storage segmentation, containerization, and full device encryption to protect data.

Containerization is useful when using the BYOD model. They also include enforcing strong authentication methods to prevent unauthorized access.

- **Geolocation.** Mobile devices commonly include GPS capabilities that are used for geolocation. Applications commonly use GPS to identify the location of the device and device movement. GPS can also be used to locate a lost device.
- **Geofencing.** Organizations sometimes use GPS to create a virtual fence or geographic boundary using geofencing technologies. Apps can respond when the device is within the virtual fence. As an example, an organization can configure mobile apps so that they will only run when the device is within the virtual fence. Similarly, an organization can configure a wireless network to only operate for mobile devices within the defined boundary.
- **GPS tagging.** *GPS tagging* (also called geotagging) adds geographical information to files such as pictures when posting them to social media websites. For example, when you take a picture with a smartphone with GPS features enabled, the picture application adds latitude and longitude coordinates to the picture. Thinking of friends and family, this is a neat feature. However, thinking of thieves and criminals, they can exploit this data. For example, if Lisa frequently posts pictures of friends and family at her house, these pictures identify her address. If she later starts posting pictures from a vacation location, thieves can realize she's gone and burglarize her home.

- **Context-aware authentication.** *Context-aware authentication* uses multiple elements to authenticate a user and a mobile device. It can include the user's identity, geolocation, verification that the device is within a geofence, time of day, and type of device. These elements help prevent unauthorized users from accessing apps or data.
- **Push notifications.** *Push notification* services send messages to mobile devices from apps. As an example, if Lisa installs the Facebook app on her smartphone and enables notifications, the Facebook app will send her notifications. Software developers can configure the notifications to appear even if the device is in screen lock mode and even if the app is not running. MDM apps can send notifications to remind users of security settings or let them know if their device complies with security policy requirements.

Remember this

Remote wipe sends a signal to a lost or stolen device to erase all data. Geolocation uses Global Positioning System (GPS) and can help locate a lost or stolen device. Geofencing creates a virtual fence or geographic boundary and can be used to detect when a device is within an organization's property. GPS tagging adds geographical data to files such as pictures. Context-aware authentication uses multiple elements to authenticate a user and a mobile device.

Mobile Device Enforcement and Monitoring

MDM tools often manage devices differently depending on who owns them. If the organization owns the device, the MDM tool will typically download and install all required applications and ensure they are kept up to date.

If the device is employee-owned, MDM tools will monitor them for compliance and block access to the network if the device doesn't meet minimum requirements. For example, suppose the device isn't patched or doesn't have up-to-date antivirus software. In that case, the MDM software works with network access control (NAC) technologies to prevent the device from connecting to the network. The following paragraphs identify many common issues that an MDM can monitor and enforce.

Unauthorized Software

Organizations typically want users to only install apps obtained from approved sources. For example, all iPhone and iPad devices would only obtain apps from Apple's App Store. Apple is aggressive in testing these apps for malware, and any developer who attempts to distribute malware through the Apple store is often banned. Similarly, Google maintains the Google Play site for Android devices.

A third-party app store is something other than Apple's App Store or Google Play. Apps obtained from these ***third-party app stores*** don't undergo the same level of scrutiny as apps on the App Store or Google Play and represent a higher risk. Apple makes it very difficult to obtain apps from a third-party app store, but it is relatively easy to obtain apps from third-party stores for Android devices.

Jailbreaking refers to removing all software restrictions from an Apple device. After jailbreaking a device, users can install software from any third-party source. ***Rooting*** is the process of modifying an Android device to give the user root-level (or full administrator) access to the device. Rooting and jailbreaking introduce risks and vulnerabilities to the device, so it's common for an MDM to block all access to a network if it detects a device has either been rooted or jailbroken.

Mobile devices typically have the operating system stored in onboard memory, such as flash memory, which retains data even without power. Because the operating system is the software and the memory is hardware, this is commonly called firmware. Updates to the operating system overwrite the firmware using ***over-the-air (OTA) updates*** techniques. Firmware OTA updates keep the device up to date.

It's also possible to overwrite the firmware with ***custom firmware***. Some people do this as another method of rooting Android devices. The process is typically complex and fraught with risks. However, some people find downloadable images and copy them onto their devices to overwrite the firmware.

It's also possible to install applications on Android devices by ***sideload***ing them. Sideload is the process of copying an application package in the Application Packet Kit (APK) format to the device and then activating it. The device must be set to allow apps from Unknown Sources, which can significantly weaken security. Sideload is useful for developers testing apps, but considered risky when installing apps from third parties.

Remember this

Jailbreaking removes all software restrictions from an Apple device. Rooting modifies an Android device, giving users root-level access to the device. Overwriting the firmware on an Android device with custom firmware is another way to root an Android device. Sideload is the process of installing software on an Android device from a source other than an authorized store.

Messaging Services

Many people use text messaging services such as ***Short Message Service (SMS)*** and ***Multimedia Message Service (MMS)***. SMS is a basic text messaging service supported on many telephone and mobile devices. MMS is an extension of SMS that allows users to include multimedia content such as a picture, a short video, audio, or even a slideshow of multiple images.

There are two primary risks with text messaging. First, both send text in plaintext, allowing the information to be intercepted and read by others.

However, some apps offer encryption capabilities.

The second risk only applies to MMS because it can send media. Attackers have discovered ways to send an MMS message to a phone number and gain remote code execution privileges on the user's phone.

Most smartphones can store credit card data and be used for payments. For example, NFC (described earlier in this chapter) is often used as a payment gateway with some mobile devices. When issuing phones to users, organizations need to consider if they want to put their own payment methods on the phone for some payments. If so, this typically needs to be monitored closely.

Rich communication services (RCS) is a newer communication protocol designed to replace SMS for text messaging. Similar to MMS, RCS can transmit multimedia, but it has additional features. If a user sends an RCS message, but the network doesn't support RCS, it will default to MMS or SMS.

Hardware Control

An organization might want to control some of the hardware on mobile devices, and MDM tools can help. Mobile devices commonly include a camera and a recording microphone. These are useful for regular users but can present significant risks for employees within an organization.

As an example, attackers have successfully inserted malicious code into some apps available on some third-party sites. When users install the apps, it allows an attacker to remotely connect to the phone, snap pictures, record audio, and much more.

An organization can configure the MDM software to disable the camera and recording microphone to eliminate the risk. Ideally, the MDM tool will only disable the camera and microphone when it detects the device is within a previously configured geofence. Unfortunately, all MDM tools don't support disabling hardware based on geolocation. If the MDM tool doesn't support this feature, the organization may prohibit the possession of smartphones in certain areas.

MDM tools can also prevent the use of external media and ***Universal Serial Bus On-The-Go (USB OTG)*** cables. Mobile devices commonly have one or more ports where you can plug in a cable. Apple devices have a Lightning port, and Android devices typically have a micro-USB or mini-

USB. In some cases, it's possible to connect external media (such as an external drive) to the device. Organizations might want to prevent this because the media presents additional risks. It could contain malware. It might also allow a malicious insider to copy a massive amount of data. USB OTG cables allow you to connect just about any device to your mobile device, including another mobile device. This includes a mouse, keyboard, Musical Instrument Digital Interface (MIDI) keyboard, and external media. Many people find this useful to transfer photos from cameras to their mobile devices. Again, though, because this allows connections to external media, an organization might choose to disable the feature using MDM tools.

Unauthorized Connections

Management within an organization might want to limit a mobile device's connection abilities. For example, if the mobile device can connect to the primary network, management might want to ensure that the mobile device cannot access the Internet using another connection. This section identifies other connections that can be modified and blocked with an MDM tool.

Most smartphones support **tethering**, which allows you to share one device's Internet connection with other devices. For example, you can connect your smartphone to the Internet and then share this Internet connection with a laptop, a tablet, or any device with a wireless connection. If employees use tethering within the organization, they can bypass security such as firewalls and proxy servers. Imagine Bart wants to visit a not safe for work (NSFW) site with his work laptop. The proxy server blocks his access. However, he can tether his laptop to his smartphone and visit the site. This direct connection will also bypass any content filters in the network and possibly allow malware onto his laptop.

Similarly, many carrier companies sell mobile hotspots. These connect to the Internet and allow multiple systems to access the Internet via the **hotspot**. If employees bring these to work, they can bypass network controls just as if they were using tethering.

Many mobile devices also support **Wi-Fi Direct**, a standard that allows devices to connect without a wireless access point or wireless router. This is similar to a wireless ad hoc network, allowing devices to connect together

without a wireless access point or wireless router. The difference is that Wi-Fi Direct uses single radio hop communication. In other words, none of the devices in a Wi-Fi Direct network can share an Internet connection. In contrast, systems in a wireless ad hoc network use multihop wireless communications and can share an Internet connection.

Smartphones are typically locked into a specific carrier such as Verizon or AT&T. A subscriber identification module (SIM) card identifies what countries and/or networks the phone will use. In other words, if Lisa has a smartphone and a Verizon plan, the SIM card in her phone will connect her to a Verizon network instead of an AT&T network.

If Lisa purchased her phone under a two-year contract and fulfilled all the terms of her plan, she can unlock her phone (also called *carrier unlocking*) and use it with another carrier. An organization might want to block this capability for all COPE devices.

Remember this

Tethering and mobile hotspots allow devices to access the Internet and bypass network controls. Wi-Fi Direct is a standard that allows devices to connect without a wireless access point or wireless router. MDM tools can block access to devices using tethering, mobile hotspot, or Wi-Fi Direct to access the Internet.

SEAndroid

The security-enhanced Android (SEAndroid) security model uses Security-Enhanced Linux (SELinux) to enforce access security.

It operates using a default denial principle. In other words, anything not allowed by the SELinux policy is denied.

When enabled, SELinux supports two modes:

- **Enforcing mode.** This mode enforces the SELinux policy. Any activity that is denied by the policy is blocked and logged.
- **Permissive mode.** This mode does not enforce the SELinux policy, but it does log all activity that the policy would block if it was in enforcing mode. Permissive mode is useful when testing an SELinux policy. Administrators use it to verify that the policy works as intended before changing it to Enforcing mode.

SEAndroid is only used on Android devices. However, more than 70 percent of mobile devices use an Android operating system

Exploring Embedded Systems

An *embedded system* is any device that has a dedicated function and uses a computer system to perform that function. Desktop PCs, laptops, and servers all use central processing units (CPUs), operating systems, and applications to perform various functions. Similarly, embedded systems use CPUs, operating systems, and one or more applications to perform multiple functions.

As a simple example, a wireless multifunction printer (MFP) typically includes an embedded system. It runs a website that you can access wirelessly to configure the printer. Of course, you can also send print jobs to it, scan documents, and copy documents with the printer. Many include faxing capabilities and can send documents via email.

The CompTIA Security+ objectives mention three embedded systems described in the following paragraphs.

A *field programmable gate array (FPGA)* is a programmable integrated circuit (IC) installed on a circuit board. It starts off without any configuration or program. When turned on, it transfers a configuration program from a configuration memory chip or an external processor.

The memory chip is non-volatile flash memory, allowing it to retain the programming, even without power. Additionally, it's possible to rewrite the configuration stored on the memory chip, effectively changing the function of the FPGA the next time the device is turned on. Similarly, the external processor can send a different configuration to the FPGA each time it's turned on.

Arduino is a microcontroller board, and the circuit board contains the CPU, random access memory (RAM), and read-only memory (ROM). Arduino doesn't need an operating system to run but instead uses firmware, and it is often used for simple repetitive tasks. For example, it can monitor the temperature and show the results in a liquid crystal display (LCD).

Raspberry Pi is a microprocessor-based mini-computer, and it uses the Raspberry Pi OS to run. It has more extensive capabilities than Arduino. For example, instead of just monitoring and displaying the temperature, a Raspberry Pi system can send signals to a heating, ventilation, and air conditioning (HVAC) system to control the temperature.

Understanding Internet of Things

The Internet of Things (IoT) refers to a wide assortment of technologies that interact with the physical world. They commonly have embedded systems and typically connect to a central device or app and communicate via the Internet, Bluetooth, or other wireless technologies.

The National Institute of Standards and Technology Internal Report (NISTIR) 8228 “Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy Risks” states that the full scope of IoT is not precisely defined. This is because the technologies are in a wide assortment of sectors such as health care, transportation, and home security.

Many have sensors used to monitor an environment, such as temperature and humidity. However, they can do much more than control thermostats. Many organizations use IoT devices for facility automation, such as motion-controlled lighting, security cameras and recorders, fire detection and suppression systems, and more.

IoT technologies are also used in many other technologies such as medical systems, vehicles, aircraft, and smart meters. IoT devices can provide remote temperature monitoring for vaccines and capture vital signs for patients. More and more automobiles use both embedded systems and IoT devices to control all facets of the operation of an automobile. As an example, cars regularly update themselves with over-the-air updates. Manufacturers could decide to integrate all the embedded systems in an automobile, making them all accessible via the Internet and accessible by attackers.

Aircraft use IoT technologies to track the maintenance and performance of almost every moving part on the plane. Aircraft and unmanned aerial vehicles (UAVs) include embedded systems. Hobbyists use small UAVs to take pictures remotely. Other organizations such as the military include sophisticated embedded systems for reconnaissance and to deliver weapons.

Smart meters are commonly used on the electrical grid. They remotely monitor and record energy consumption, sending data analytics to centralized servers.

ICS and SCADA Systems

An ***industrial control system (ICS)*** typically refers to systems within large facilities such as power plants or water treatment facilities. A ***supervisory control and data acquisition (SCADA) system*** typically controls an ICS by monitoring it and sending it commands. Ideally, these systems are protected within isolated networks that can't access the Internet. From another perspective, attackers on the Internet can't access SCADA systems or an ICS.

Common uses of ICS and SCADA systems include:

- **Manufacturing and industrial.** Manufacturing and industrial uses include any plants used to manufacture products. The systems can monitor every processing stage and report anomalies in real time. Many systems can also send signals to adjust processes based on changes in the environment.
- **Facilities.** Facilities uses include monitoring the temperature and humidity and keeping the environment relatively stable. In water treatment facilities, these systems can monitor each phase of the process, report problems, and adjust to changes.
- **Energy.** Energy uses include oil and gas processing, power generation, and more.
- **Logistics.** Logistics uses include monitoring processes within shipping facilities.

Some SCADA systems and ICSs are connected to the corporate network. However, they are typically placed within an isolated virtual local area network (VLAN), and the VLAN is protected by a network intrusion prevention system (NIPS) to block unwanted traffic. Chapter 3 discusses VLANs and Chapter 4 discusses NIPS.

Remember this

A supervisory control and data acquisition (SCADA) system has embedded systems that control an industrial control system (ICS), such as one used in a power plant or water treatment facility. Embedded systems are also used for many special purposes, such as medical devices, automotive vehicles, aircraft, and unmanned aerial vehicles (UAVs).

Understanding ICS

Industrial Control Systems (ICS) is a broad term encompassing supervisory control and data acquisition (SCADA) systems, distributed control systems, and programmable logic control (PLC) systems. These systems are widely used in power generation, chemical processing, and telecommunications industries. As an example, ICS systems maintain the proper pressure in natural gas lines delivering gas to homes and businesses. If this pressure is too high, it can cause natural gas to build up, causing explosions and fires.

That's exactly what happened in Merrimack Valley, Massachusetts in September 2018. Excessive pressure built up in the natural gas lines feeding homes and businesses causing explosions and fires in three towns. One person died, more than 25 people were injured, and about 50,000 people were evacuated. The total cost was estimated at more than \$1 billion.

When it happened, I thought about Stuxnet, a malicious computer worm that infected SCADA and PLC systems used to control Iranian nuclear centrifuges. The worm is widely believed to have destroyed as many as 1,000 centrifuges, by changing the rotor speed. If a worm could infect Iran's SCADA and PLC systems, could a worm infect systems controlling natural gas pipelines?

The National Transportation Safety Board (NTSB) investigated the Merrimack Valley incident and attributed the problem to overpressurized gas mains. However, they reported in September 2019, that the problem was due to deficiencies in management and oversight within Columbia Gas of Massachusetts. Specifically, they reported that Columbia Gas contract workers were replacing some piping, using a faulty procedure created by Columbia Gas.

IoT and Embedded Systems

The CompTIA Security+ objectives include a lengthy list of embedded systems and specialized systems. Some of these might be familiar to you, but others may be new. The following section describes many embedded systems that haven't been covered in this chapter previously.

A smart television (TV) is one of many smart devices that you might have in your home. You can easily connect it to your home's wired or wireless network and use it to access the Internet. Many people use it to stream TV shows and movies to their TV. This is possible because these smart TVs have embedded systems giving them additional capabilities.

Wearables refers to any device you can wear or have implanted. These devices can then be used to interact with other devices, such as a smartphone. As an example, Fitbit has manufactured a range of products that you can wear to monitor your health and fitness. Combined with an app on their smartphone, people can gain insight into how well they're doing on their goals.

Most veterinarians recommend implanting microchips in pets. Animal shelters routinely look for these, and if found, they can help return the pets to their owners. Some can even be used to open pet doors. The company Dangerous Things sells a similar device for people that can reportedly be injected into your hand at the tattoo parlor. Once injected, you can program it to open some smart locks or control your cell phone. Be careful, though. Dangerous Things warns, "Use of this device is strictly at your own risk."

Home automation includes Internet-connected devices, such as wireless thermostats, lighting, coffee makers, and more. These devices typically connect to the home's network, which gives them Internet access. This allows people to access or control these devices from the Internet, even when they aren't home.

Camera systems often include Internet-connected cameras. These cameras can be within a home automation system or used as a surveillance system for an organization. However, if they are connected to the Internet, they have IP addresses, and attackers can find them. If attackers learn of vulnerabilities with them, you can bet they'll try to exploit the vulnerabilities.

A **system on a chip (SoC)** is an integrated circuit that includes all the functionality of a computing system within the hardware. It typically includes an application contained within onboard memory, such as read-only memory (ROM), electrically erasable programmable ROM (EEPROM), or flash memory. Many mobile computing devices include an SoC.

A **real-time operating system (RTOS)** is an operating system that reacts to input within a specific time. If it can't respond within the specified time, it doesn't process the data and typically reports an error. As an example, imagine an automated assembly line used to create donuts. Each location on the line receives materials from the previous location, adds additional materials, or somehow processes the materials (such as mixing them), and passes the result to the next location. Each of these locations could include an embedded system with an RTOS to ensure it receives and processes the materials within a specified time. If it doesn't, it can raise an error or alert and stop the assembly line.

Admittedly, an RTOS is probably overkill for a donut assembly line. There are simpler ways. However, some assembly lines are much quicker and require response times for each location in the millisecond or nanosecond range. An RTOS can be used reliably in these systems.

Some companies are producing embedded system modules that enhance phones. For example, these modules can be plugged into some smartphones allowing them to interact with Voice over IP (VoIP) networks. This allows them to use either a cellular network or a local area network.

HVAC systems keep computing systems at the proper temperature and with the proper humidity. Most have embedded systems to control them. If attackers can access these systems, they may be able to remotely turn off the HVAC system or trick it into keeping the temperature at 95 degrees within a data center. The resulting damage to systems within this data center could be catastrophic.

Remember this

An embedded system is any device that has a dedicated function and uses a computer system to perform that function. It includes any devices in the Internet of Things (IoT) category, such as wearables and home automation systems. Some embedded systems use a system on a chip (SoC).

Security Implications of Embedded Systems

A challenge with embedded systems is keeping them up to date with security fixes. When vendors discover vulnerabilities in computers and applications, they write and release patches. When you apply the patch, the system is no longer vulnerable to the exploit. In contrast, embedded systems vendors are not as aggressive in identifying vulnerabilities and creating patches to fix them.

Also, patch management is a routine function for IT administrators in most organizations. They regularly review patches, test them, and apply them when necessary. In contrast, how often does a regular user think about checking or applying patches to his refrigerator?

Another significant security concern is when embedded systems are deployed with default configurations. For example, imagine Homer creates a home security system using Internet-accessible security cameras, deployed with default usernames and passwords. If attackers discover the cameras, they can access them over the Internet. Worse, if attackers discover a vulnerability within the cameras' embedded systems, they can exploit them.

Embedded System Constraints

Embedded systems have several constraints that can limit their use. The following list describes these constraints:

- **Compute.** The computing ability of embedded systems is typically limited compared with full computing systems. Because they are small, they don't have full CPUs.
- **Crypto.** With limited processing power, embedded systems can't use all cryptographic protocols. If designers sacrifice security by not encrypting data, they may inadvertently create vulnerabilities.
- **Power.** Embedded devices don't have their own power supplies but instead use power from the parent device. In some cases, devices must use batteries that occasionally need to be replaced. This results in a conflict with the computing capabilities. Stronger computing ability draws more power and requires batteries to be replaced more often.
- **Range.** Devices typically connect to other devices using a wireless protocol. However, with limited power, these devices can have a limited range.
- **Authentication.** It's common for designers to skip authentication when designing embedded systems due to the extra requirements. If so, attackers may be able to access and exploit the system.
- **Network.** When connecting to a network, you often need an interface to configure a device. Without an interface, the device must accept the defaults.
- **Cost.** The cost of the device can be minimized by sacrificing features such as security. By adding features, it increases the cost. It can sometimes be a challenge between management and designers when balancing the cost against the desired features.
- **Inability to patch.** Unlike most endpoint devices such as desktops and mobile devices, it often isn't possible to patch embedded systems. Vendors don't always include methods to patch devices, and even if they do, they don't always write and release patches in a timely manner.

- **Implied trust.** Most users trust that embedded systems are secure. Unfortunately, many devices have vulnerabilities that either aren't known by most people or aren't widely reported.
- **Weak defaults.** Because security is often an afterthought with embedded systems, designers often release embedded systems with weak defaults. This may be weak defaults used for authentication or defaulting to no encryption when sending traffic.

Communication Considerations

You have several choices when deciding which communication methods to use for embedded systems and IoT devices. The following list describes some choices:

- **5G.** 5G can reach peak speeds significantly higher than 4G, allowing it to transfer data much quicker. However, there's a lot of variabilities related to the actual speeds of both 5G and 4G. Unfortunately, 5G has a limited range. With nothing blocking 5G signals, they have a range of about 1,000 feet, which is significantly lower than the 4G range of about 10 miles. This means that 5G needs a huge increase in infrastructure to support 5G towers and antennas. Additionally, 5G signals can be blocked by physical barriers like trees, walls, and glass, further limiting the range.
- **Narrow-band.** As the name implies, narrow-band signals have a very narrow frequency range. It is commonly used in two-way radio systems, such as walkie-talkies. Think of a large construction site. Workers often need to communicate with other workers. They can select a common channel on their devices and easily talk to other workers on the job site.
- **Baseband radio.** Baseband radio signals include frequencies that are very near zero. They are typically used when transferring data over a cable rather than over the air.
- **Subscriber identity module (SIM) cards.** Mobile devices such as smartphones and tablets with Internet capabilities use SIM cards to connect with a cellular provider. A SIM card has a unique serial number. A user pays a subscription fee for access, and the cellular provider grants access as long as the SIM card's serial number matches a valid account. While SIM cards are used around the world, different countries have different standards. When using a SIM card, you need to ensure it is compatible with technologies used in the country where the embedded system or IoT device is used.
- **Zigbee.** Zigbee is a suite of communication protocols used for smaller networks, such as within a home for home automation. It's

designed to be simpler to use and cheaper than other wireless protocols, such as Bluetooth and traditional wireless networks. It has a relatively low data rate and low power consumption, with Zigbee devices having a battery life of two years or more. It supports strong security, including data encryption.

Chapter 5 Exam Topic Review

When preparing for the exam, make sure you understand these key concepts covered in this chapter.

Summarizing Virtualization Concepts

- Virtualization allows multiple servers to operate on a single physical host. It also supports virtual desktops.
- A virtual desktop infrastructure (VDI) hosts a user's desktop operating system on a server. Thin clients, including mobile devices, can connect to a server and access a VDI.
- Container virtualization runs services or applications within isolated containers or application cells. Containers use the kernel of the host.
- VM escape attacks allow an attacker to access the host system from the VM. The primary protection is to keep the host and guests up to date with current patches.
- VM sprawl occurs if personnel within the organization don't manage the VMs.
- Persistence indicates a VM saves changes made by users. Non-persistence indicates the VM doesn't save the changes.
- Live media (such as bootable USBs) supports persistence.

Implementing Secure Systems

- Endpoints are computing devices such as servers, desktops, laptops, mobile devices, or Internet of Things (IoT) devices. Endpoint detection and response (EDR) provides continuous monitoring of endpoints.
- Hardening is the practice of making an operating system or application more secure from its default installation.
- Configuration management practices help organizations deploy systems with secure configurations.
- A master image provides a secure starting point for systems. Master images are typically created with templates or other baselines to

provide a secure starting point for systems. Integrity measurement tools detect when a system deviates from the baseline.

- Patch management procedures ensure operating systems, applications, and firmware are kept up to date with current patches. This ensures they are protected against known vulnerabilities.
- Change management policies define the process for making changes and help reduce unintended outages from changes.
- An application allow list identifies authorized software but blocks all other software. An application block list identifies unauthorized software but allows other software to run.
- Full disk encryption (FDE) encrypts an entire disk. A self-encrypting drive (SED) has the encryption circuitry built into the drive. Opal-compliant SEDs require users to enter credentials to unlock the drive when booting the system.
- A Trusted Platform Module (TPM) is a chip included with many laptops and some mobile devices, and it provides full disk encryption, a secure boot process, and supports remote attestation. TPMs have an encryption key burned into them that provides a hardware root of trust.
- A hardware security module (HSM) is a removable or external device used for encryption. An HSM generates and stores RSA encryption keys and can be integrated with servers to provide hardware-based encryption. A microSD HSM is a microSD chip with an HSM device installed on it.
- The primary method of protecting the confidentiality of data is with encryption and strong access controls. File system security includes the use of encryption to encrypt files and folders.
- You can encrypt individual columns in a database (such as credit card numbers), entire databases, individual files, entire disks, and removable media.
- Data loss prevention (DLP) techniques and technologies help prevent data loss. They can block transfer of data to USB devices and analyze outgoing data via email to detect unauthorized transfers.
- Data exfiltration is the unauthorized transfer of data outside an organization.

Summarizing Cloud Concepts

- Cloud computing provides an organization with additional resources. Most cloud services are provided via the Internet or a hosting provider. On-premise clouds are owned and maintained by an organization.
- Software as a Service (SaaS) includes web-based applications such as web-based email.
- Platform as a Service (PaaS) provides an easy-to-configure operating system and on-demand computing for customers. The vendor keeps systems up to date with current patches.
- Infrastructure as a Service (IaaS) provides hardware resources via the cloud. It can help an organization limit the size of its hardware footprint and reduce personnel costs.
- Anything as a Service (XaaS) refers to any other services delivered via the cloud, such as communication, databases, desktops, storage, security, and more.
- A managed service provider (MSP) is a third-party vendor that provides any IT services needed by an organization, including security services. A managed security service provider (MSSP) focuses on providing security services for an organization.
- A cloud access security broker (CASB) is a software tool or service deployed between an organization's network and the cloud provider. It monitors all network traffic and can enforce security policies.
- Private clouds are only available to personnel within the organization.
- Third-party vendors sell access to public cloud services to anyone who wants them.
- Two or more organizations with shared concerns can share a community cloud.
- A hybrid cloud is a combination of two or more clouds.
- Cloud-based DLP systems can enforce security policies for any data stored in the cloud.
- A next-generation secure web gateway provides proxy services for traffic from clients to Internet sites. It can filter URLs and scan for malware.

- Edge and fog computing technologies move the storing and processing of data closer to the devices that generate and use the data.

Deploying Mobile Devices Securely

- Mobile devices include smartphones and tablets and run a mobile operating system.
- Corporate-owned, personally enabled (COPE) mobile devices are owned by the organization, but employees can use them for personal reasons.
- Bring your own device (BYOD) policies allow employees to connect their mobile devices to the organization's network. Choose your own device (CYOD) policies include a list of acceptable devices and allow employees who own one of these devices to connect them to the network.
- A virtual desktop infrastructure (VDI) is a virtual desktop, and these can be created so that users can access them from a mobile device.
- Mobile devices can connect to the Internet, networks, and other devices using cellular, wireless, Bluetooth, near field communication (NFC), infrared, and USB connections.
- Mobile device management (MDM) tools help ensure that devices meet minimum security requirements. They can monitor devices, enforce security policies, and block network access if devices do not meet these requirements.
- MDM tools can restrict applications on devices, segment and encrypt data, enforce strong authentication methods, and implement security methods such as screen locks and remote wipe.
Containerization is useful when using the BYOD model.
- A screen lock is like a password-protected screen saver on desktop systems that automatically locks the device after some time. A remote wipe signal removes all the data from a lost phone.
- Geolocation uses Global Positioning System (GPS) to identify a device's location. Geofencing uses GPS to create a virtual fence or geographic boundary. Organizations use geofencing to enable access

to services or devices within the boundary and block access outside the boundary.

- Geotagging uses GPS to add geographical information to files (such as pictures) when posting them on social media sites.
- A third-party app store is something other than the primary store for a mobile device. Apple's App Store is the primary store for Apple devices. Google Play is a primary store for Android devices.
- Jailbreaking removes all software restrictions on Apple devices, and rooting provides users with root-level access to an Android device. Custom firmware can also root an Android device. MDM tools block network access for jailbroken or rooted devices.
- Sideloaded is the process of copying an application to an Android device instead of installing it from an online store.
- A Universal Serial Bus On-The-Go (USB OTG) cable allows you to connect mobile devices.
- Tethering allows one mobile device to share its Internet connection with other devices. Wi-Fi Direct allows you to connect devices together without a wireless router.

Exploring Embedded Systems

- An embedded system is any device that has a dedicated function and uses a computer system to perform that function. A security challenge with embedded systems is keeping them up to date.
- Internet of Things (IoT) devices interact with the physical world. They commonly have embedded systems and typically communicate via the Internet, Bluetooth, or other wireless technologies.
- A supervisory control and data acquisition (SCADA) system controls an industrial control system (ICS). The ICS is used in large facilities such as power plants or water treatment facilities.
- SCADA and ICS systems are typically in isolated networks without access to the Internet and are often protected by network intrusion prevention systems.
- A system on a chip (SoC) is an integrated circuit that includes a full computing system.

- A real-time operating system (RTOS) is an operating system that reacts to input within a specific time.
- A major constraint with embedded systems and IoT devices is the lack of updates. They often don't include an ability to update them, and even when they do, vendors don't consistently update them.
- Embedded systems include smart devices sometimes called the Internet of Things (IoT), such as wearable technology and home automation devices.

ine References

- Are you ready for performance-based questions? Don't forget to check out the online content at <https://greatadministrator.com/sy0-601-extras/>.

Chapter 5 Practice Questions

1. Attackers recently exploited vulnerabilities in a web server hosted by your organization. Management has tasked administrators with checking the server and eliminating any weak configurations on it. Which of the following will meet this goal?
 - A. Installing a NIDS
 - B. Disabling unnecessary services
 - C. Enabling root accounts
 - D. Implementing SSL encryption

2. The BizzFad organization develops and sells software. Occasionally they update the software to fix security vulnerabilities and/or add additional features. However, before releasing these updates to customers, they test them in different environments. Which of the following solutions provides the BEST method to test the updates?
 - A. Baseline configuration
 - B. BYOD
 - C. Sandbox
 - D. Change management

3. Network administrators have identified what appears to be malicious traffic coming from an internal computer, but only when no one is logged on to the computer. You suspect the system is infected with malware. It periodically runs an application that attempts to run hping3 via remote websites. After comparing the computer with a list of applications from the master image, they verify this application is likely the problem. What allowed them to make this determination?
 - A. Version control
 - B. Sandbox
 - C. Blacklist
 - D. Integrity measurements

4. While investigating a recent data breach, investigators discovered a RAT on Bart's computer. Antivirus software didn't detect it. Logs show a user

with local administrator privileges installed it. Which of the following answers has the BEST chance of preventing this from happening again in the future?

- A. Enforce an application allow list.
 - B. Enforce an application block list.
 - C. Implement a BYOD policy.
 - D. Implement a DLP system.
5. Salespeople within a company regularly take company-owned laptops with them on the road. The company wants to implement a solution to protect laptop drives against data theft. The solution should operate without user interaction for ease of use. Which of the following is the BEST choice to meet these needs?
- A. DLP
 - B. HSM
 - C. MDM
 - D. SEDs
6. Managers within your organization want to implement a secure boot process for some key computers. During the boot process, each computer should send data to a remote system to check the computer's configuration. Which of the following will meet this goal?
- A. Trusted Platform Module
 - B. Hardware root of trust
 - C. Remote attestation
 - D. Tokenization
7. Your organization recently updated its security policy to prohibit the use of external storage devices. The goal is to reduce threats from insiders. Which of the following methods would have the BEST chance of reducing the risk of data exfiltration using external storage devices?
- A. Train employees about the policy.
 - B. Monitor firewall logs to detect data exfiltration.
 - C. Block write capabilities to removable media.
 - D. Implement a network-based DLP solution.

8. Maggie, the new CTO at your organization, wants to reduce costs by utilizing more cloud services. She has directed the use of a cloud service instead of purchasing all the hardware and software needed for an upcoming project. She also wants to ensure that the cloud provider maintains all the required hardware and software. Which of the following BEST describes the cloud computing service model that will meet these requirements?

- A. IaaS
- B. PaaS
- C. SaaS
- D. XaaS

9. You are asked to research prices for cloud-based services. The cloud service provider needs to supply servers, storage, and networks, but nothing else. Which of the following will BEST meet your needs?

- A. IaaS
- B. PaaS
- C. SaaS
- D. XaaS

10. Your organization has been using more cloud resources and Lisa, the CIO, is concerned about security. She wants to add a service that is logically placed between the organization's network and the cloud provider. This service will monitor all network traffic and ensure that data sent to the cloud for storage is encrypted. Which of the following will BEST meet these requirements?

- A. CASB
- B. Storage permissions
- C. A storage encryption policy
- D. Firewall

11. Management at your organization wants to add a cloud-based service to filter all traffic going to or from the Internet from internal clients. At a minimum, the solution should include URL filtering, DLP protection, and malware detection and filtering. Which of the following will BEST meet these requirements?

- A. Next-generation SWG
- B. Container security
- C. Cloud-based segmentation
- D. API inspection and integration

12. Your organization is planning to implement a BYOD policy. However, management wants to implement a comprehensive solution to protect the organization's data when the BYOD policy is put into place. Which of the following is the BEST choice to meet these needs?

- A. FDE
- B. SED
- C. MDM
- D. MAM

13. Your organization recently implemented a security policy requiring that all endpoint computing devices have a unique identifier to simplify asset inventories. Administrators implemented this on servers, desktop PCs, and laptops with an RFID system. However, they haven't found a reliable method to tag corporate-owned smartphones and tablet devices. Which of the following choices would be the BEST alternative?

- A. VDI
- B. MDM application
- C. RFID tag
- D. GPS tagging

14. Your organization is switching from a COPE model to a BYOD model due to the cost of replacing lost or damaged mobile devices. Which of the following is the BEST choice to protect the organization's data when using the BYOD model?

- A. Full-disk encryption
- B. Containerization
- C. Remote wipe
- D. Geolocation

15. Bart is showing Wendell a new app that he downloaded from a third party onto his iPhone. Wendell has the same model of smartphone, but

when he searches for the app, he is unable to find it. Of the following choices, what is the MOST likely explanation for this?

- A. Jailbreaking
- B. Tethering
- C. Sidebreaking
- D. Rooting

Chapter 5 Practice Question Answers

1. **B** is correct. Unnecessary open ports and services are common elements that contribute to weak configurations so it's important to close ports that aren't needed and disable unnecessary services. A network-based intrusion detection system (NIDS) helps protect internal systems, but a NIDS would not be installed on the server and administrators are tasked with checking the server. Unsecured root accounts indicate a weak configuration. If root accounts are disabled, enabling them won't increase security on the server. Secure Sockets Layer (SSL) is a weak encryption protocol and should not be implemented on servers.
2. **C** is correct. A sandbox provides a simple method of testing updates. It provides an isolated environment and is often used for testing. A baseline configuration is a starting point of a computing environment. Bring your own device (BYOD) refers to allowing employee-owned mobile devices in a network and is not related to this question. Change management practices ensure changes are not applied until they are approved and documented.
3. **D** is correct. The master image is the baseline, and the administrators performed integrity measurements to identify baseline deviations. By comparing the list of applications in the baseline with the applications running on the suspect computer, it's possible to identify unauthorized applications. None of the other answers include the troubleshooting steps necessary to discover the problem. Version control tracks software versions as software is updated. A sandbox is an isolated area of a system, typically used to test applications. A blacklist is a list of prohibited applications.
4. **A** is correct. Enforcing an application allow list (sometimes called an application whitelist) would prevent this. An application allow list identifies the only applications that can be installed on a computer and would not include a malicious remote access tool (RAT). An application block list identifies applications to block, but malware changes so often, this wouldn't help. Code signing verifies code is valid and hasn't been modified. A bring your own device (BYOD) policy identifies mobile devices employees can

buy and connect to a network but is unrelated to this question. A data loss protection (DLP) system typically monitors outgoing traffic and wouldn't stop a user from installing a malicious application.

5. **D** is correct. Self-encrypting drives (SEDs) are the best solution. SEDs have encryption circuitry built into the drive. They encrypt and decrypt data without user interaction, though it's common to require personnel to use credentials to unlock the SED when booted. A data loss prevention (DLP) solution typically monitors outgoing traffic to prevent confidential information from getting outside the organization. A hardware security module (HSM) is used to manage, generate, and store cryptographic keys. It's generally used on a network instead of on laptops. Mobile device management (MDM) refers to technologies used to manage mobile devices.

6. **C** is correct. A remote attestation process checks a computer during the boot cycle and sends a report to a remote system. The remote system attests or confirms that the computer is secure. None of the other answers sends data to a remote system. A Trusted Platform Module (TPM) is a hardware chip on a motherboard and provides a local secure boot process. A TPM includes an encryption key burned into the CPU, which provides a hardware root of trust. Tokenization replaces sensitive data with a token or substitute value, and this token can be used in place of the original data.

7. **C** is correct. Blocking write capabilities to removable media is the best choice. This can be done with a data loss prevention (DLP) solution on all computers. Training employees might help, but it won't stop an insider threat. Monitoring firewall logs might detect data exfiltration out of the network, but it won't monitor the use of external storage devices. A network-based DLP solution might detect and stop data exfiltration out of the network, but it would stop users from copying data to removable media.

8. **B** is correct. Platform as a Service (PaaS) provides customers with a preconfigured computing platform including the hardware and software. The cloud provider maintains the hardware and specified software such as the operating system and key applications such as a web server application. Infrastructure as a Service (IaaS) is a cloud computing option where the

vendor provides access to a computer, but customers must install the operating system and maintain the system. Software as a Service (SaaS) provides access to specific applications such as an email application. Anything as a Service (XaaS) refers to cloud services beyond IaaS, PaaS, and SaaS.

9. **A** is correct. An Infrastructure as a Service (IaaS) cloud model provides clients with hardware but nothing else. A Platform as a Service (PaaS) model provides customers with a computing platform including operating systems and some applications. A Software as a Service (SaaS) model provides customers with one or more applications. Anything as a Service (XaaS) refers to cloud services beyond IaaS, PaaS, and SaaS, but this scenario clearly describes an IaaS model.

10. **A** is correct. A cloud access security broker (CASB) is placed between a network and a cloud provider and would meet the chief information officer (CIO) requirements. It can monitor traffic and enforce security policies, such as ensuring all data sent to the cloud is encrypted. Permissions should be set on cloud storage locations to ensure only authorized personnel can access them, but they don't encrypt the data. A storage encryption policy can be created to require encryption of data stored in the cloud, but the policy wouldn't monitor all traffic to and from the cloud. A firewall can filter traffic, but it doesn't include all the capabilities of a CASB, such as verifying data is encrypted.

11. **A** is correct. A next-generation secure web gateway (SWG) provides proxy services for traffic from clients to Internet sites, such as filtering Uniform Resource Locators (URLs) and scanning for malware. Permissions should be set on cloud storage locations to ensure only authorized personnel can access them, but they don't encrypt the data. Container security can be applied as a cloud security control to protect data by placing it in different containers with different permissions or encryption controls. Segmentation within a network isolates hosts or networks, and cloud-based segmentation does the same thing, except the isolation occurs within the cloud.

Application programming interface (API) inspection and integration refers

to testing an API for usability, but this scenario is much too complex for an API.

12. **C** is correct. A mobile device management (MDM) solution is the best choice because it can manage multiple risks related to mobile devices in a bring your own device (BYOD) scenario. Full disk encryption (FDE) typically isn't feasible in a BYOD scenario because it requires an organization to encrypt devices owned by employees. Some FDE drives use self-encrypting drive (SED) technology, and they aren't feasible for the same reason FDE drives aren't feasible. Mobile application management (MAM) only manages applications on mobile devices, and it isn't a comprehensive solution.

13. **B** is correct. Mobile Device Management (MDM) applications can assign unique digital identifiers to endpoint devices such as smartphones and tablets. It uses this to manage the device remotely, and the identifier can also be used to simplify asset inventories. A virtual desktop infrastructure (VDI) provides a virtual desktop to users (including users with mobile devices), allowing them to connect to a server hosting the desktop. Radio-frequency identification (RFID) tags are being used on other devices, but the scenario states it isn't a reliable method for smartphones and tablet devices. Global Positioning System (GPS) tagging adds geographical data to pictures to indicate where the photo was taken.

14. **B** is correct. Containerization is the best choice. Organizations can ensure that organizational data is encrypted in some containers without encrypting user data. In a bring your own device (BYOD) model, employees own the devices, and an organization typically can't encrypt user data with full-disk encryption. In a corporate-owned, personally enabled (COPE) model, the organization could use full-device encryption. Remote wipe sends a signal to a lost device to erase data, but it won't erase data if the device is damaged, and an attacker may be able to recover data from a damaged device. Geolocation technologies can help locate a lost device, but they won't protect data.

15. A is correct. Jailbreaking is the most likely reason for this. It's possible to jailbreak an iPhone to remove all software restrictions, including the ability to install applications from sources other than the Apple App Store. Tethering allows you to share an Internet connection with one mobile device to other mobile devices. Sideloaded is the process of installing application packages from an Application Packet Kit (APK) but sidebreaking isn't a relevant term in this context. Rooting is done to Android devices and provides users root-level access to the device.

Chapter 6

Comparing Threats, Vulnerabilities, and Common Attacks

CompTIA Security+ objectives covered in this chapter:

1.1 Compare and contrast different types of social engineering techniques.

- Phishing, Smishing, Vishing, Spam, Spam over Internet messaging (SPIM), Spear phishing, Dumpster diving, Shoulder surfing, Tailgating, Eliciting information, Whaling, Prepending, Identity fraud, Invoice scams, Credential harvesting, Reconnaissance, Hoax, Impersonation, Watering hole attack, Typo squatting, Pretexting, Influence campaigns (Hybrid warfare, Social media)
- Principles (reasons for effectiveness) (Authority, Intimidation, Consensus, Scarcity, Familiarity, Trust, Urgency)

1.2 Given a scenario, analyze potential indicators to determine the type of attack.

- Malware (Ransomware, Trojans, Worms, Potentially unwanted programs (PUPs), Fileless virus, Command and control, Bots, Cryptomalware, Logic bombs, Spyware, Keyloggers, Remote access Trojan (RAT), Rootkit, Backdoor)

1.5 Explain different threat actors, vectors, and intelligence sources.

- Actors and threats (Advanced persistent threat (APT), Insider threats, State actors, Hacktivists, Script kiddies, Criminal syndicates, Hackers, Authorized, Unauthorized, Semi-authorized, Shadow IT, Competitors)
- Attributes of actors (Internal/external, Level of sophistication/capability, Resources/funding, Intent/motivation), Vectors (Email, Social media)
- Threat intelligence sources (Open source intelligence (OSINT), Closed/proprietary, Vulnerability databases, Public/private information sharing centers, Dark web, Indicators of compromise, Automated indicator sharing (AIS), Structured Threat Information Exchange (STIX)/Trusted Automated eXchange of Intelligence Information (TAXII), Predictive analysis, Threat maps, File/code repositories)
- Research sources (Vendor websites, Conferences, Academic journals, Request for comments (RFC), Local industry groups, Social media)

1.6 Explain the security concerns associated with various types of vulnerabilities.

- Zero-day, Impacts (Data exfiltration, Identity theft)

1.8 Explain the techniques used in penetration testing.

- Passive and active reconnaissance (OSINT)

2.7 Explain the importance of physical security controls.

- Access control vestibules

3.2 Given a scenario, implement host or application security solutions.

- Endpoint protection (Antivirus, Anti-malware)

3.3 Given a scenario, implement secure network designs.

- File integrity monitors

4.1 Given a scenario, use the appropriate tool to assess organizational security.

- Network reconnaissance and discovery (Cuckoo)

**

Organizations need to understand many different types of threat actors, so it's valuable to know a little about them, their attributes, and the types of attacks they are likely to launch. Malicious software (malware) and social engineering are two common attack categories that any organization will face, but there are some complexities to each category. Attackers are becoming more and more sophisticated with these attacks, so it's important to know how to reduce attackers' success. This chapter covers these topics along with sources for additional threat intelligence.

Understanding Threat Actors

When considering attacks, it's important to realize that there are several different types of threat actors, and they each have different attributes. Don't let the phrase threat actors confuse you. It's just a fancier name given to attackers—anyone who launches a cyberattack on others. The attackers are the actors, and they represent a threat to an organization.

Some attackers are highly organized and dedicated. An ***advanced persistent threat (APT)*** is a group of organized threat actors that engage in targeted attacks against organizations. These APTs typically have both the capability and intent to launch sophisticated and targeted attacks over a long period of time.

While APTs can be any group of highly organized attackers, they are typically sponsored by nation-states or governments. In this context, APT members are ***state actors***. These state actors typically have specific targets, such as a certain company, organization, or government agency. Successful attacks often allow unauthorized access for long periods of time, giving the APTs the ability to exfiltrate a significant amount of data.

Being funded by nation-states, they often have a significant amount of resources and funding. Cybersecurity firms have written about APTs sponsored by several governments, including:

- **China.** Some reported names are PLA Unit 61398, Buckeye, and Double Dragon.
- **Iran.** Some reported names are Elfin Team, Helix Kitten, and Charming Kitten.
- **North Korea.** Some reported names are Ricochet Chollima and Lazarus Group.
- **Russia.** Some reported names are Fancy Bear, Cozy Bear, Voodoo Bear, and Venomous Bear.

These governments deny these reports. With so many governments reportedly sponsoring several APTs, it's clear that this is a threat that organizations need to take seriously.

Criminal syndicates are composed of a group of individuals working together in criminal activities. These groups are typically organized within a hierarchy composed of a leader and workers, like a normal business.

Depending on how large the criminal syndicate is, it can have several layers of management. However, unlike a legitimate business, the enterprise is focused on criminal activity. The primary motivation of criminal syndicates is money. Almost all their efforts can be traced back to greed with the goal of getting more money, regardless of how they get it.

For example, Crowdstrike, a cybersecurity technology company, documented a criminal syndicate known as WIZARD SPIDER. Crowdstrike reported this is a Russia-based criminal group. Further, they discovered evidence that this group operated Ryuk, a well-known ransomware that targeted enterprise environments. Ransomware is discussed further later in this chapter.

Remember this

An advanced persistent threat (APT) refers to an organized and sophisticated group of threat actors. Nation-states (governments) sponsor them and give them specific targets and goals. Criminal syndicates are groups of individuals involved in crime. Their primary motivation is money.

Years ago, a ***hacker*** was known as someone proficient with computers who wanted to share knowledge with others. However, the definition has morphed over the years. Today, the media commonly refers to hackers as malicious individuals who use their technical expertise to launch attacks and break into systems or networks for personal gain.

A ***script kiddie*** is an attacker who uses existing computer scripts or code to launch attacks. Script kiddies typically have very little expertise or sophistication and very little funding. Many people joke about the bored teenager as the script kiddie, attacking sites or organizations for the fun of it. However, there isn't any age limit for a script kiddie. More importantly, they can still obtain powerful scripts and launch dangerous attacks. Their motivations vary, but they are typically launching attacks out of boredom or just to see what they can do.

A ***hacktivist*** launches attacks as part of an activist movement or to further a cause. Hacktivists typically aren't launching these attacks for their benefit but instead to increase awareness about a cause. For example, the Yes Men, an activist group that tries to raise awareness of social and political issues, launches disinformation campaigns against organizations.

In January 2019, they created a fake website that looked like BlackRock, a large financial asset manager that owned the largest number of fossil fuel companies at the time. They then released a fake letter from BlackRock's CEO Larry Fink indicating that BlackRock required any company it invests in to align their business models with the Paris climate agreement to combat climate change. Many media outlets were fooled and reported the letter as legitimate. While the hoax was quickly revealed, it did raise awareness.

Many people are referred to as white hats, black hats, and gray hats within cybersecurity circles. They are reminiscent of the Wild West, where you could easily identify the good guys and the bad guys by their hat's color. **Black hat** (also known as an unauthorized hacker) identifies a malicious attacker performing criminal activities, similar to how the media refers to hackers. **White hat** (also known as an authorized hacker) identifies a security professional working within the law, such as a cybersecurity professional working to protect an organization from attackers. **Gray hat** (also known as a semi-authorized hacker) identifies individuals who may have good intentions, but their activities may cross ethical lines. For example, a hacktivist may use attack methods to further a cause, but not for personal gain.

An **insider threat** is anyone who has legitimate access to an organization's internal resources. Common security issues caused by insider threats include loss of confidentiality, integrity, and availability of the organization's assets. The extent of the threat depends on how much access the insider has. For example, an administrator would have access to many more IT systems than a regular user.

Malicious insiders have a diverse set of motivations. For example, some malicious insiders are driven by greed and simply want to enhance their finances, while others want to exact revenge on the organization. They may steal files that include valuable data, install or run malicious scripts, or redirect funds to their personal accounts. Chapter 5, "Securing Hosts and Data," covers data loss prevention (DLP) techniques and some DLP solutions can prevent users from writing data to external media devices.

All insider threats aren't malicious. An uneducated user could open a malicious attachment in an email and unwittingly release malware throughout the organization.

Remember this

A script kiddie is an attacker who uses existing computer scripts or code to launch attacks. Script kiddies typically have very little expertise, sophistication, and funding. A hacktivist launches attacks as part of an activist movement or to further a cause. An insider is anyone who has legitimate access to an organization's internal resources, such as an employee of a company. DLP solutions can prevent users from writing data to external media devices.

A **competitor** is any organization engaged in economic or commercial competition with another organization. Their motivation is typically to gain proprietary information about another company. Although it's legal to gather information using open source intelligence, greed sometimes causes competitors to cross the line into illegal activity. This can be as simple as rummaging through a competitor's trash bin, known as dumpster diving. In some cases, competitors hire employees from other companies and then get these new employees to provide proprietary information about their previous employer.

Attack Vectors

Attack vectors are the paths that attackers use to gain access to computers and networks. When successful, these vectors allow attackers to exploit vulnerabilities. Organizations often may think that they aren't a logical attack target. However, it's become increasingly clear that attackers often try to infiltrate lower-level targets in order to gain access to high-value targets.

As an example, Springfield Elementary School is very likely a low-level target. However, imagine they share cloud resources with the Springfield Nuclear Power Plant for educational purposes. The Nuclear Power Plant is a high-value target, though they also devote a lot of resources to security. In contrast, the school has limited resources to devote to security. If attackers can infiltrate the school, they may be able to infiltrate the Power Plant via the shared cloud resources.

Two attack vectors discussed in this chapter are:

- **Email.** Attackers frequently send out spam with malicious links or attachments. It's estimated that as much as 91 percent of all attacks start with an email. This includes phishing, spear phishing, and whaling attacks, presented later in this chapter.
- **Social media.** Attackers often use social media to gather information on targets via social media. This includes social media sites such as Facebook and Twitter.

Chapter 4, "Securing Your Network," discusses direct access virtual private networks (VPNs) as potential attack vectors. Chapter 5, "Securing Hosts and Data," discusses wireless, removable media, and cloud resources as potential attack vectors, and Chapter 8, "Using Risk Management Tools," discusses the supply chain as a potential attack vector.

Shadow IT

Shadow information technology (IT) refers to any unauthorized systems or applications within an organization. Most organizations have specific processes in place to approve new systems and applications. However, users sometimes install systems without approval, often to bypass security controls. Shadow IT increases risks because these systems aren't managed.

The IT department will normally manage all systems and applications under its control. This includes things like keeping them up to date and maintaining backups. However, if these systems and applications are hidden from the IT department, they won't be managed and will be susceptible to emerging vulnerabilities.

Remember this

Shadow IT refers to unauthorized systems or applications installed on a network without authorization or approval.

Determining Malware Types

Malware (malicious software) includes a wide range of software that has malicious intent. Malware is not software that you would knowingly purchase or download and install. Instead, it is installed onto your system through devious means. Infected systems give various symptoms, such as running slower, starting unknown processes, sending out email without user action, rebooting randomly, and more.

You might hear people use the term virus to describe all types of malware, but that isn't accurate. A virus is a specific type of malware, and malware includes many other types of malicious software, including worms, logic bombs, Trojans, ransomware, rootkits, spyware, and more.

Different types of malware have different indicators. By recognizing these indicators, you have a better chance of determining the type of attack.

Viruses

A **virus** is malicious code that attaches itself to a host application. The host application must be executed to run, and the malicious code executes when the host application is executed. The virus tries to replicate by finding other host applications to infect with the malicious code. At some point, the virus activates and delivers its payload.

Typically, the payload of a virus is damaging. It may delete files, cause random reboots, join the computer to a botnet, or enable backdoors that attackers can use to access systems remotely. Most viruses won't cause damage immediately. Instead, they give the virus time to replicate first. A user will often execute the virus (though unknowingly), but other times, an operating system will automatically execute it after user interaction. For example, when a user plugs in an infected USB drive, the system might automatically execute the virus, infecting the system.

Worms

A **worm** is self-replicating malware that travels throughout a network without the assistance of a host application or user interaction. A worm resides in memory and can use different transport protocols to travel over the network.

One of the significant problems caused by worms is that they consume network bandwidth. Worms can replicate themselves hundreds of times and spread to all the systems in the network. Each infected system tries to locate and infect other systems on the network, and network performance can slow to a crawl.

Remember this

Malware includes a wide variety of malicious code, including viruses, worms, Trojans, ransomware, and more. A virus is malicious code that attaches itself to an application and runs when the application is started. A worm is self-replicating and doesn't need user interaction to run.

Logic Bombs

A ***logic bomb*** is a string of code embedded into an application or script that will execute in response to an event. The event might be a specific date or time, or a user action such as when a user launches a specific program.

There's an often-repeated story about a company that decided it had to lay off an engineer due to an economic downturn. His bosses didn't see him doing much, so they thought they could do without him. Within a couple of weeks after he left, they started having all sorts of computer problems they just couldn't resolve. They called him back, and within a couple of weeks, everything was fine. A few months later, they determined they had to lay him off again. You guessed it. Within a couple of weeks, things went haywire again.

The engineer had programmed a logic bomb that was executed when the payroll program ran. It checked for his name on the payroll, and when it was there, things were fine, but when his name wasn't there, kaboom—the logic bomb exploded.

Remember this

A logic bomb executes in response to an event, such as when a specific application is executed, or a specific time arrives.

Backdoors

A ***backdoor*** provides another way of accessing a system, similar to how a backdoor in a house provides another method of entry. Malware often installs backdoors on systems to bypass normal authentication methods. Many types of malware create a backdoor quickly after infecting a system or network. This gives them discreet access to the system or network. Even if the malware is later discovered and removed, the backdoor remains.

While application developers often code backdoors into applications, this practice is not recommended. For example, an application developer might create a backdoor within an application intended for maintenance purposes. However, if attackers discover the backdoor, they can use it to access the application.

Effective account management policies help prevent ex-employees from creating backdoors after they are fired. For example, if an employee loses network access immediately after being fired, the employee cannot create a backdoor account. In contrast, if an administrator retains network access, he might create another administrative account. IT personnel might disable his account after they learn he has been fired, but he can still use this new backdoor account.

Remember this

A backdoor provides another way to access a system. Many types of malware create backdoors, allowing attackers to access systems from remote locations. Employees have also created backdoors in applications and systems.

Trojans

A ***Trojan***, also called a Trojan horse, typically looks like something beneficial, but it's actually something malicious. Trojan horses are named after the infamous horse from the Trojan War. In Greek mythology, the Achaeans tried to sack the city of Troy for several years, but they simply couldn't penetrate the city's defenses. At some point, someone got the idea of building a huge wooden horse and convincing the people of Troy that it was a gift from the gods. Warriors hid inside, and the horse was rolled up to the gates.

The people of Troy partied all day and all night celebrating their good fortune, but when the city slept, the warriors climbed down from inside the horse and opened the gates. The rest of the warriors flooded in. What the Greek warriors couldn't do for years, the Trojan horse helped them do in a single day.

In computers, a Trojan horse can come as pirated software, a useful utility, a game, or something else that users might be enticed to download and try. Attackers have often used drive-by downloads to deliver Trojans. In a drive-by download, web servers include malicious code that attempts to download and install itself on user computers after the user visits. Here are the typical steps involved in a drive-by download:

- Attackers compromise a website to gain control of it.
- Attackers install a Trojan embedded in the website's code.
- Attackers attempt to trick users into visiting the site.
Sometimes, they simply send the link to thousands of users via email, hoping that some of them click the link.
- When users visit, the website attempts to download the Trojan onto the users' systems.

Another Trojan method that attackers have used is rogueware, also known as scareware. Rogueware masquerades as a free antivirus program. When a user visits a site, they see a message on the webpage, or a pop-up appears indicating it detected malware on the user's system. The user is encouraged to download and install free antivirus software.

On the surface, this free antivirus software looks useful. However, it isn't. If a user installs and runs it on a system, it appears to do a system

scan. After the scan completes, it reports finding multiple issues, such as infections by dozens of viruses. The report isn't true. The application reports these issues even on a freshly installed operating system with zero infections.

It then encourages the user to resolve these issues immediately. If the user tries to resolve the issues, the program informs the user that this is only the trial version, and the trial version won't resolve these issues. However, for the small fee of \$79.95, users can unlock the full version to remove the threats. Some rogueware installs additional malicious components. For example, it might install a backdoor allowing the attacker to take remote control of the infected system.

Many web browser extensions have also included malicious Trojans. Duo Security (now a part of Cisco) released CRXcavator, an automated tool used to assess risks posed by Chrome extensions. Jamila Kaya, an independent security researcher, used this to identify numerous Chrome extensions that initially appeared legitimate but were exhibiting suspicious behavior. Google followed up, searching the entire Chrome Web Store, and eventually removed more than 500 Chrome extensions from the store in early 2020.

Further research showed that most of these extensions were created by a single threat actor during at least the previous two years. Much of the malicious code was very similar, and in some cases, identical. It's suspected that millions of computers have been infected.

Remember this

A Trojan appears to be something useful but includes a malicious component, such as installing a backdoor on a user's system. Many Trojans are delivered via drive-by downloads. They can also infect systems from fake antivirus software, pirated software, games, and browser extensions.

Remote Access Trojan

A remote access Trojan (RAT) is a type of malware that allows attackers to control systems from remote locations. It is often delivered via drive-by downloads or malicious attachments in email. Once installed on a system, attackers can then access the infected computer at any time and install additional malware if desired.

A growing trend is for attackers to deliver trojans as Portable Executable (PE) files in 32-bit (PE32) and 64-bit (PE64) formats. They often compress the PE files using compression tools, such as tar (sometimes called tarball). Tar files have the *.tar.gz* file extension.

Some RATs automatically collect and log keystrokes, usernames and passwords, incoming and outgoing email, chat sessions, and browser history as well as take screenshots. The RAT can then automatically send the data to the attackers at predetermined times.

Additionally, attackers can explore the network using the credentials of the user or the user's computer. Attackers often do this to discover, and exploit, additional vulnerabilities within the network. It's common for attackers to exploit this one infected system and quickly infect the entire network with additional malware, including installing RATs on other systems.

Keyloggers

Keyloggers attempt to capture a user’s keystrokes. The keystrokes are stored in a file and either sent to an attacker immediately, or saved until the attacker retrieves the file. While a keylogger is typically software, it can also be hardware. For example, you can purchase a USB keylogger, plug it into the computer, and plug the keyboard into the USB keylogger. This hardware keylogger will record all keystrokes and store them within memory on the USB device.

One of the ways keyloggers can be thwarted is by using two-factor authentication (2FA), such as a text message sent to a phone, as discussed in Chapter 2, “Understanding Identity and Access Management.” Even if the attackers capture a password via a keylogger, they won’t have access to the text message sent to the phone.

Spyware

Spyware is software installed on users' systems without their awareness or consent. Its purpose is often to monitor the user's computer and the user's activity. Spyware takes some level of control over the user's computer to learn information and sends this information to a third party. If spyware can access a user's private data, it results in a loss of confidentiality.

Some examples of spyware activity are changing a user's home page, redirecting web browsers, and installing additional software within the browser. In some situations, these changes can slow a system down, resulting in poor performance. These examples are rather harmless compared with what more malicious spyware (called privacy-invasive software) might do.

Privacy-invasive software tries to separate users from their money using data-harvesting techniques. It attempts to gather information to impersonate users, empty bank accounts, and steal identities. For example, some spyware includes keyloggers. The spyware periodically reads the data stored by the keylogger and sends it to the attacker. In some instances, the spyware allows the attacker to take control of the user's system remotely.

Spyware is often included with other software like a Trojan. The user installs one application but unknowingly gets some extras. Spyware can also infect a system in a drive-by download. The user simply visits a malicious website that includes code to automatically download and install the spyware onto the user's system.

Remember this

Keyloggers capture a user's keystrokes and store them in a file. This file can be automatically sent to an attacker or manually retrieved depending on the keylogger. Spyware monitors a user's computer and often includes a keylogger.

Rootkit

A *rootkit* is a group of programs (or, in rare instances, a single program) that hides the fact that the system has been infected or compromised by malicious code. A user might suspect something is wrong, but antivirus scans and other checks indicate everything is fine because the rootkit hides its running processes to avoid detection.

In addition to modifying the internal operating system processes, rootkits often modify system files such as the Registry. In some cases, the rootkit modifies system access, such as removing users' administrative access.

Rootkits have system-level access to systems. This is sometimes called root-level access, or kernel-level access, indicating that they have the same level of access as the operating system. Rootkits use hooked processes, or hooking techniques, to intercept calls to the operating system. In this context, hooking refers to intercepting system-level function calls, events, or messages. The rootkit installs the hooks into memory and uses them to control the system's behavior.

Antivirus software often calls the operating system to detect malware, but the rootkit prevents the antivirus software from making these calls. This is why antivirus software will sometimes report everything is OK, even if the system is infected with a rootkit. However, antivirus software can often detect the hooked processes by examining the contents of the system's random access memory (RAM).

Another method used to detect rootkits is to boot into safe mode or have the system scanned before it boots, but this isn't always successful. It's important to remember that rootkits are very difficult to detect because they can hide so much of their activity. A clean bill of health by a malware scanner may not be valid.

It's important to remember that behind any type of malware, you'll likely find an attacker involved in criminal activity. Attackers who have successfully installed a rootkit on a user's system might log on to the user's computer remotely, using a backdoor installed by the rootkit. Similarly, attackers might direct the computer to connect to computers on the Internet and send data. Data can include anything collected from a keylogger,

collected passwords, or specific files or file types stored on the user's computer.

Remember this

Rootkits have system-level or kernel access and can modify system files and system access. Rootkits hide their running processes to avoid detection with hooking techniques. Tools that can inspect RAM can discover these hidden hooked processes.

Bots and Botnets

Generically, ***bots*** are software robots. For example, Google uses bots as search engine spiders to crawl through the Internet looking for webpages. However, attackers also use bots for malicious purposes. A botnet combines the words robot and network. It includes multiple computers that act as software robots (bots) and function together in a network (such as the Internet), often for malicious purposes. The bots in a botnet are often called zombies, and they will do the bidding of whoever controls the botnet.

Bot herders are criminals who manage botnets. They attempt to infect as many computers as possible and control them through systems on the Internet running command and control software. The infected computers periodically check in with the command and control systems, receive commands, and then go to work. The user is typically unaware of the activity.

As an example, Emotet is a banking Trojan designed to steal sensitive and private information, such as credentials used to access bank accounts. It has morphed into a botnet to grow. Once Emotet infects one computer, it then uses worm-like capabilities to spread to other computers within a network. Each of these computers are added to a botnet and attackers use the infected computers to send more phishing emails, attempting to infect more computers. Emotet has been so effective that it was recognized as one of the top five threats globally in 2019. The Department of Homeland Security (DHS) reported that Emotet infections cost an average of about \$1 million per incident to remediate.

Command and Control

Attackers use ***command and control*** resources to control infected computers. After a computer is infected with malware, the malware then attempts to connect to a command and control resource for instructions. Command and control resources have commonly been used to control zombies within botnets. However, they are now being used by many types of malware including ransomware.

Internet Relay Chat (IRC) networks were often used in early botnets. Infected computers were given Internet locations (such as a server or website) that they would connect to periodically using an IRC channel. The bot herder would upload commands to the resource, which were then downloaded to the zombie when it connected. The benefit of IRC channels is that it made it easy for bot herders to upload commands and for the infected computers to receive them. However, legal professionals have become adept at locating and disabling these IRC networks, effectively taking down the botnets.

Some criminals have migrated to peer-to-peer (P2P) botnets to host command and control resources. In a P2P botnet, each infected system looks for other infected systems, progressively building a larger list of infected machines that can work together. Each of the infected systems can act as a command and control system issuing commands to other systems and as a botnet zombie receiving commands. Because there is no central command and control, legal professionals can't take down the entire botnet by taking down just a few central command and control servers. Bot herders often use cryptography methods to access the botnet and insert commands.

Some malware creates command and control resources on Internet of Things (IoT) devices. As an example, the banking Trojan Trickbot has created command and control resources on hacked wireless routers.

Remember this

Botnets are groups of computers controlled by attackers, and computers in a botnet check in with command and control servers periodically for instructions. Attackers frequently use botnets to launch DDoS attacks.

Ransomware and Cryptomalware

Specific types of Trojans are ***ransomware*** and cryptomalware. With ransomware, attackers take control of computers or networks, locking out users. With cryptomalware, attackers encrypt the data on computers within the network to prevent access. In both cases, attackers then demand that the user or organization pay a ransom to regain access to the data or computers.

Today, almost all ransomware attacks use cryptomalware techniques. If the ransom is paid, attackers promise to provide the decryption key. If the ransom isn't paid, attackers typically threaten to destroy the key removing access to the data forever.

Criminals often deliver ransomware via drive-by downloads or embedded in other software delivered via email. Attackers originally focused their attacks on individuals demanding payments of about \$300 each. However, they have increasingly been targeting organizations demanding larger and larger payoffs.

As an example, Travelex reportedly paid attackers about \$2.3 million in 2020. Travelex is a foreign exchange company widely known for its kiosks in airports around the world where people can obtain money in different currencies. Attackers infected the Travelex network with Sodinokibi ransomware. While Travelex reported the attack shortly after it occurred, they didn't publicly report paying the ransom.

Interestingly, Travelex was warned about vulnerabilities with Pulse Secure virtual private networking (VPN) software that they were using. Pulse Secure released patches in April 2019. Pulse Secure informed Travelex directly in September 2019 that it detected multiple unpatched Pulse Secure servers. Cybersecurity experts suspect that attackers infiltrated Travelex networks by exploiting Pulse Secure vulnerabilities.

Ryuk, another ransomware tool used by attackers, reportedly netted \$3.7 million in 52 transactions in 2018 alone. That equates to an average of \$71,000 per transaction. Two similar ransomware families are Phobos and Sodinokibi that have launched waves of attacks against hospitals, cities, and schools. The following examples show some of the destructive results of ransomware attacks:

- The Hackensack Meridian health network in New Jersey suffered an attack that took the network down for two days and impacted operations in 17 hospitals. This resulted in them canceling non-emergency medical procedures and resorting to pen and paper for other patient care. It's unclear how much money attackers wanted, but the Hackensack Meridian reportedly paid an undisclosed amount.
- In Pensacola, Florida, the Sanitation department suffered an attack that locked up telephone and email systems, Internet servers, and their online payment system. Attackers demanded \$1 million. It's unclear if the city paid anything.
- The Virtual Care Provider Inc. (VCPI) suffered a massive ransomware attack in 2019. VCPI is an IT vendor for more than 100 nursing homes in 45 states. They provide Internet access, cloud-based data storage, and vendor maintenance support for about 80,000 computers. The attack prevented some facilities from ordering drugs or submitting Medicaid bills on time. VCPI reportedly had trouble making payroll due to the loss of data. Attackers demanded a ransom of \$14 million but VCPI chief executive and owner Karen Christianson said they couldn't afford to pay that amount. It's unclear if they paid a ransom, but they did get their systems back up in a few weeks.

With the massive amounts of revenue these attacks are bringing to criminals, it's logical to think they will continue. The Federal Bureau of Investigation (FBI) and other legal entities discourage the paying of any ransoms. However, some organizations see paying a ransom as cheaper than suffering the outage while trying to re-create their data.

Unfortunately, some organizations haven't received a usable decryption key even after paying the ransom. Worse, the attackers have sometimes demanded additional money after receiving the first ransom. The attackers are criminals, after all.

Remember this

Ransomware is a type of malware that takes control of a user's system or data. Cryptomalware encrypts the user's data. Criminals then attempt to extort payment from the victim. Ransomware often includes threats of

damaging a user's system or data if the victim does not pay the ransom, and attackers increasingly target hospitals, cities, and other larger organizations.

Potentially Unwanted Programs

Potentially unwanted programs (PUPs) are programs that a user may not want, even if a user consented to download it. Some of these unwanted programs are legitimate, but some are malicious, such as Trojans. The extras have often been called spyware, adware, junkware, or crapware.

As an example, if you download and install 7-zip, a popular compression tool, from a site other than 7-zip.org, the installer may include PUPs. Many PUPs are browser hijackers. They change the user's browser settings without the user's clear consent. They may change the home page, the default search engine, add additional toolbars, open additional tabs when the browser is opened, and inject advertising. Some browser hijackers gather user data and behavior (such as search terms used in search queries) and use it to display unwanted advertisements and other paid links that generate revenue for the author of the browser hijacker.

Often the fine print in the Terms of Use page, presented in the installation program, will explain this. However, it's buried so deep and obfuscated with legalese that most people miss it. They simply click Agree and continue with the install. Worse, many PUPs present multiple Terms pages, requiring users to either read them all, or cancel the installation of everything, including the software they wanted.

The download.cnet.com site (previously download.com and download.com.com) was known to include PUPs in their downloads from at least 2011 to 2016. The site included malware and adware packaged within other downloads. At one time, they used an installation manager called CNET TechTracker to deliver and install software, including PUPs. Multiple security professionals documented what happened (terrible, horrible, no good, and very bad things) when users downloaded these packages. Eventually, CNET cleared out the PUPs from their downloads, as did several other download sites.

At this point, you may wonder which download sites are safe? The best bet is to assume that none of them are. If you want to download freeware, go to the source. If you want to download 7-zip, go to <https://7-zip.org>. If you want to download Adobe Reader, go to <https://adobe.com>.

The same goes for any freeware you want to download. Always go to the source.

Fileless Virus

A ***fileless virus*** (also called fileless malware) is a type of malicious software that runs in memory. In contrast, most malware is a file written to disk. It's relatively new in the malware family but is increasing in popularity among attackers due to its success at bypassing anti-malware programs. Symantec reported that fileless malware attacks increased more than 1,000 percent in 2018. Some techniques used by fileless malware are:

- **Memory code injection.** The malware injects code into legitimate applications using known and unpatched vulnerabilities in these applications. Java and Adobe Flash have been popular targets. In some cases, it embeds scripts into legitimate PowerShell scripts. When the PowerShell script runs, the malicious code runs, too. PowerShell is very powerful and allows administrators (and attackers) to query and infect other computers within the network.
- **Script-based techniques.** Two common examples are SamSam ransomware and Operation Cobalt Kitty. SamSam used encrypted code that is only decrypted when run, making it difficult to detect. Operation Cobalt Kitty used PowerShell to target an organization for almost six months, starting with a spear-phishing email.
- **Windows Registry manipulation.** The malware uses a Windows process to write and execute code into the Registry. Kovter and Poweliks are two malware examples that use this method.

Fileless viruses can also be embedded within other files. As an example, vCard is a file format used for electronic business cards. Instead of exchanging paper business cards, users can exchange their data electronically. Because these typically have a free-text area where users can add any data, they can contain malicious code. Imagine employees go to a trade show and exchange business cards with others to build their contact list, and some attendees have malicious vCards. These employees can bring malware back into their organization via these malicious vCards.

Remember this

Fileless viruses run in memory instead of from a file on a disk. They are often scripts that are injected into legitimate programs. They can also be hidden in vCards.

Potential Indicators of a Malware Attack

There are many indicators of malware attacks. Some generic indicators are:

- **Extra traffic.** Malware typically adds a lot of extra traffic to a network. Abnormal traffic can be identified by comparing it with a baseline of known regular traffic.
- **Data exfiltration.** Data exfiltration refers to the unauthorized transfer of data out of a network. Malware often attempts to download data, such as databases of credentials, to locations controlled by the attacker. Data loss prevention (DLP) techniques can often detect this data as it is being downloaded.
- **Encrypted traffic.** Some malware will encrypt the data before data exfiltration attempts. This can bypass typical DLP techniques because a DLP system can't read the encrypted data. However, a large amount of encrypted data can indicate data exfiltration, even if the data can't be identified.
- **Traffic to specific IPs.** Bot zombies will often attempt to connect to known command and control servers. However, firewalls can blacklist traffic going to the servers when the IPs are known. Monitoring firewall logs for traffic attempting to access these blacklisted IPs are a strong indicator of infection.
- **Outgoing spam.** Desktop computers don't normally send large amounts of email. When they do, it's often because they have been added to a botnet and are sending phishing emails as zombies.

Recognizing Common Attacks

In addition to malware, it's important to understand some other common attacks. Social engineering includes several techniques attackers use to trick users. Additionally, many attackers use email, instant messaging, and the phone to deliver attacks.

Social Engineering

Social engineering is the practice of using social tactics to gain information. It's often low-tech and encourages individuals to do something they wouldn't normally do or cause them to reveal some piece of information, such as user credentials. Some of the individual methods and techniques include:

- Using flattery and conning
- Assuming a position of authority
- Encouraging someone to perform a risky action
- Encouraging someone to reveal sensitive information
- Impersonating someone, such as an authorized technician
- Tailgating or closely following authorized personnel without providing credentials

In the movie *Catch Me If You Can*, Leonardo DiCaprio played Frank Abagnale Jr., an effective con artist. He learned some deep secrets about different professions by conning and flattering people into telling him. He then combined all he learned to impersonate pilots and doctors and perform some sophisticated forgery.

Social engineers con people in person, as Frank Abagnale Jr. did, and they use other methods as well. They may use the phone, send email with phishing tactics, and even use some trickery on websites, such as fooling someone into installing malware.

As an example of a social engineer using the phone, consider this scenario. Maggie is busy working and receives a call from Hacker Herman, who identifies himself as a member of the IT department.

Hacker Herman: “Hi, Maggie. I just wanted to remind you, we’ll be taking your computer down for the upgrade today, and it’ll be down for a few hours.”

Maggie: “Wait. I didn’t hear anything about this. I need my computer to finish a project today.”

Hacker Herman: “You should have gotten the email. I’m sorry, but I have to get the last few computers updated today.”

Maggie: “Isn’t there any other way? I really need my computer.”

Hacker Herman: "Well...it is possible to upgrade it over the network while you're still working. We don't normally do it that way because we need the user's password to do it."

Maggie: "If I can still work on my computer, please do it that way."

Hacker Herman: "OK, Maggie. Don't tell anyone I'm doing this for you, but if you give me your username and password, I'll do this over the network."

This is certainly a realistic scenario, and many end users will give out their passwords unless security-related awareness and training programs consistently repeat the mantra: "Never give out your password."

Attackers aren't always so blatant, though. Instead of asking you for your password outright, they often ask questions they can use in a password reset system to reset your password. A skilled con man can ask these questions as though he's generally interested in you. Before you know it, you've told him the name of your first dog, your childhood best friend, the name of your first boss, and more. When people post this information on social media, attackers don't even need to ask.

The following sections describe many common security issues related to social engineering.

Remember this

Social engineering uses social tactics to trick users into giving up information or performing actions they wouldn't normally take. Social engineering attacks can occur in person, over the phone, while surfing the Internet, and via email.

Impersonation

Some social engineers often attempt to impersonate others. The goal is to convince an authorized user to provide some information or help the attacker defeat a security control.

As an example, an attacker can impersonate a repair technician to gain access to a server room or telecommunications closet. After gaining access, the attacker can install hardware such as a rogue access point to capture data and send it wirelessly to an outside collection point. Similarly, attackers impersonate legitimate organizations over the phone and try to

gain information. Identity verification methods are useful to prevent the success of impersonation attacks.

Shoulder Surfing

Shoulder surfing is simply looking over the shoulder of someone to gain information. The goal is to gain unauthorized information by casual observation, and it's likely to occur within an office environment. This can be to learn credentials, such as a username and password, or a PIN used for a smart card or debit card. Attackers sometimes use cameras to monitor locations where users enter PINs, such as at automatic teller machines (ATMs).

A simple way to prevent shoulder surfing is to position monitors and other types of screens so that unauthorized personnel cannot see them. This includes ensuring people can't view them by looking through a window or from reception areas. Another method used to reduce shoulder surfing is to use a screen filter placed over the monitor. This restricts the visibility of the screen for anyone who isn't looking directly at the monitor.

Remember this

A social engineer can gain unauthorized information just by looking over someone's shoulder. This might be in person, such as when a user is at a computer or remotely using a camera. Screen filters help prevent shoulder surfing by obscuring people's view unless they are directly in front of the monitor.

Tricking Users with Hoaxes

A ***hoax*** is a message, often circulated through email, which tells of impending doom from a virus or other security threat that simply doesn't exist. Users may be encouraged to delete files or change their system configuration.

Serious virus hoaxes have the potential to be as damaging as a real virus. If users are convinced to delete important files, they may make their systems unusable. Additionally, they waste help-desk personnel's time due to needless calls about the hoax or support calls if users damaged their systems in response to the hoax.

I recently received several hoax messages telling me that an attacker had infected my system and taken compromising videos of me with my computer's webcam. The attacker then threatened to release them unless I paid a fee. The most compromising thing I've done in front of my computer is fall asleep. However, my webcam is either disconnected or covered on all my computers, so the attacker didn't have any videos of me catching 40 winks. Still, the emails continued and became increasingly threatening. Someone who hadn't covered their webcam might indeed believe the hoax and pay.

Tailgating and Access Control Vestibules

Tailgating is the practice of one person following closely behind another without showing credentials. For example, if Homer uses a badge to gain access to a secure building and Francesca follows closely behind Homer without using a badge, Francesca is tailgating.

Employees often do this as a matter of convenience and courtesy. Instead of shutting the door on the person following closely behind, they often hold the door open for the person. However, this bypasses the access control, and if employees tailgate, it's easy for a non-employee to slip in behind someone else. Often, all it takes is a friendly smile from someone like Francesca to encourage Homer to keep the door open for her.

An access control vestibule (sometimes called a mantrap) prevents tailgating. It is a room, or even a building, with two doors that creates a large buffer area between the secure and unsecured areas. Access through the entry door, and the exit door is tightly controlled, either with guards or with an access card such as a proximity card. Security guards can check each person's credentials, and they won't be fooled by a smile as easily as Francesca might fool Homer.

A simple turnstile, like those used in subways or bus stations, also prevents tailgating. Imagine two men trying to go through a turnstile like this together. It's just not likely.

Remember this

Tailgating is a social engineering tactic that occurs when one user follows closely behind another user without using credentials. Access control vestibules (sometimes call mantraps) allow only a single person to pass at a

time. Sophisticated mantraps can identify and authenticate individuals before allowing access.

Dumpster Diving

Dumpster diving is the practice of searching through trash or recycling containers to gain information from discarded documents. Many organizations either shred or burn paper instead of throwing it away.

For example, old copies of company directories can be valuable to attackers. They may identify the names, phone numbers, and titles of key people within the organization. Attackers may be able to use this information in a whaling attack against executives or social engineering attacks against anyone in the organization. An attacker can exploit any document containing detailed employee or customer information and often find value in seemingly useless printouts and notes.

On a personal basis, credit card companies' preapproved credit applications or blank checks can be quite valuable to someone attempting to gain money or steal identities. Documentation with any Personally Identifiable Information (PII) or Protected Health Information (PHI) should be shredded or burned.

Remember this

Dumpster divers search through trash looking for information. Shredding or burning papers instead of throwing them away mitigates this threat.

Zero-Day Vulnerabilities

A **zero-day vulnerability** is a vulnerability or bug that is unknown to trusted sources, such as operating system and antivirus vendors. Operating system vendors write and release patches once they know about them, but the vulnerability remains until the vendors know about them. As an example, the Heartbleed vulnerability existed for a couple of years before it was widely published. Up until the time that OpenSSL developers released a fix, everyone using it was vulnerable.

Users might adopt the idea that up-to-date antivirus software will protect them from all malware. This simply isn't true. No matter how great an antivirus company is at identifying new malware, there will always be a

lag between the time when criminals release the malware, and the antivirus company releases new signatures to discover it. This is especially true when attackers are releasing more than 200,000 new variants of malware daily. This includes malware designed to take advantage of zero-day vulnerabilities.

Remember this

Zero-day exploits take advantage of vulnerabilities that don't have available patches. It could be because vendors don't know about the vulnerability or haven't written patches to fix it yet. Zero-day exploits can evade up-to-date antivirus software.

Watering Hole Attacks

A **watering hole attack** attempts to discover which websites a group of people are likely to visit and then infects those websites with malware that can infect the visitors. The attacker's goal is to infect a website that users trust already, making them more likely to download infected files.

Think of a lion looking for prey. It is much easier to hide by a watering hole and wait for the prey to come, than for the lion to chase the prey. Similarly, attackers can use a variety of techniques to infiltrate a network or lay a trap and wait for the prey to come to them. In this analogy, the websites that users visit are the watering holes.

As an example, imagine that attackers want to infiltrate the Springfield Nuclear Power Plant. The Power Plant has strong cybersecurity and the attackers have been unsuccessful so far. However, the attackers learn that employees frequently visit the Capital City Capitals baseball team website, which has limited security. The attackers install malware on the baseball team's website, and when Power Plant employees visit it, the site attempts to download malware on the employee systems.

Watering hole attacks often infect websites with zero-day vulnerabilities giving them a better chance of infecting the ultimate target. Advanced persistent threats have used this as a method of infiltrating high-profile targets.

Typo Squatting

Typo squatting (also called **URL hijacking**) occurs when someone buys a domain name that is close to a legitimate domain name. People often do so for malicious purposes. As an example, CompTIA hosts the *comptia.org* website. If an attacker purchases the name *comptai.org* with a slight misspelling at the end of *comptia*, some users might inadvertently go to the attacker's website instead of the legitimate website. Attackers might buy a similar domain for a variety of reasons, including:

- **Hosting a malicious website.** The malicious website might try to install drive-by malware on users' systems when they visit.
- **Earning ad revenue.** The attacker can host pay-per-click ads. When visitors go to the site and click on the ads, advertisers pay revenue to the attacker.
- **Reselling the domain.** Attackers can buy domain names relatively cheap, but resell them to the original site owner for a hefty profit.

Eliciting Information

Elicitation is the act of getting information without asking for it directly. Social engineers often use casual conversation to gather information without giving targets any idea the attacker is trying to gather information. They often start by trying to gain trust and build rapport with a target through flattery or by encouraging the target to brag about their accomplishments.

Next, the social engineers use a variety of techniques to gather information, such as:

- **Active listening.** People are often busy and preoccupied with mobile devices, and they sometimes don't give their full attention when someone is speaking. However, when an attacker gives his full attention to a target, the target is encouraged to keep talking.
- **Reflective questioning.** Reflective questioning demonstrates active listening and encourages a target to talk more. It simply repeats a statement as a question. For example, a target may state that a security system blocked an outgoing email. The attacker may reply with, "You couldn't even send the email."

- **False statements.** The attacker gives a false statement hoping that the target corrects him. For example, the attacker might say, “I’ve heard that employees aren’t able to visit any non-government websites. They can’t go to Amazon or Facebook. They can even get disciplined for certain Google searches.”
- **Bracketing.** Attackers often try to get specific information by stating a specific number or a range of numbers. For example, the attacker may say, “I heard they have a dozen cameras in the lobby alone,” or “I hear they have between 10 and 20 motion detectors activated in the lobby after hours.” If the target knows the specific number, he may reveal it to brag about what he knows or correct the attacker.

It’s important to realize that this section provides a few techniques used to elicit information, but there are many more. Salespeople are often trained to use similar techniques to develop rapport and gain the information they can use to close the sale. Spy agencies and legal professionals go through in-depth training on how to elicit information. Penetration testers also use elicitation techniques along with other social engineering techniques.

Pretexting and Prepending

Pretexting and *prepend* are similar, and some people use the terms interchangeably. However, there is a subtle difference. They both start with *pre* indicating that something is being added to the beginning of something else. Contrast prepend with append, which adds something to the end.

A pretext is a fictitious scenario added to a conversation to make a request more believable. For example, a social engineer may state he works with a known vendor and claims that there’s a problem with some of the applications. He follows this with a request for information on the products used by the company. This prepended scenario may trick an employee into giving up information. In contrast, if someone called and just started asking for details about products used by a company, employees are much more likely to be suspicious.

Prepending simply means to add something to the beginning of something else. As an example, it’s possible to prepend the subject, headers, or body of emails with additional data.

Organizations can use this defensively to warn users of potentially malicious email by prepending the subject line with [EXTERNAL] to indicate it came from an Internet source and is not necessarily safe. Attackers can use this offensively by prepending the subject line with [SAFE] to indicate that the email has been checked and is not malicious. Untrained users may be more likely to click on a malicious link if the email is marked as [SAFE].

Identity Theft and Identity Fraud

Identity theft occurs when someone steals personal information about you. It could be things like your name, address, Social Security number, health insurance number, credit card data, or bank account information.

Criminals take this a step further and use the stolen identity information to commit *identity fraud*. Some common examples of identity fraud include applying for a loan, falsely filing tax returns to get the victim's refund, and using a health insurance number to send fake bills to an insurer.

Any criminal who steals personal information (identity theft) will almost always try to use that information in some type of fraud (identity fraud). Because of this, you'll often see identity theft defined as both the theft of information and the fraudulent use of that information.

Invoice Scams

Some criminals use invoice scams trying to trick people or organizations into paying for goods or services they didn't request and usually didn't receive. Invoices may be for advertising, to renew a domain name, or to ask for payment of an unpaid or late bill. These typically arrive via email, but some scammers send fake invoices via regular mail, or call demanding payment for an unpaid invoice.

Emailed invoices often warn about an unpaid bill and dire consequences if the organization doesn't pay. They include a malicious attachment and encourage the user to open it with a threat of legal action or a threat to turn the account over to a debt collection agency. If the user opens the attachment, it may install ransomware or some other type of malware.

Years ago, I received several bills from a so-called debt collection agency, trying to collect money for an unpaid telephone bill of over \$700. However, I knew the bill wasn't valid and noticed they misspelled my name. They later began calling, demanding payment, and threatening legal action. A lawyer friend drafted and sent a cease and desist letter, which stopped them. However, they started again a while ago. I ignored the first bill and returned the second bill unopened after I wrote "addressee unknown" on the front. I haven't heard from them since.

Credential Harvesting

Attackers use credential harvesting techniques to collect usernames and passwords (credentials) from users. Classic credential harvesting is based on a simple idea. If you want a user's credentials, just ask. Attackers send phishing emails out to users claiming a problem with an account and encouraging users to click a link and log on to their account to fix it. The link brings them to a malicious website that often looks like the real thing. If the user enters credentials, the site captures them and then redirects the user to the actual logon page. Users typically think they must have entered the password wrong and just enter it again.

Some malware attempts credential harvesting by waiting until a user visits a banking or financial site. It then uses keyboard logging or screenshots to capture the user's credentials. Sometime later, the malware will send the captured data to an Internet source that the attacker controls.

Reconnaissance

Within the context of social engineering, ***reconnaissance*** refers to gathering as much information as possible on a target. They typically use open source sources to gather information using the Internet and follow this up with phone calls and/or site visits. Penetration testers (discussed in Chapter 8) use technical methods for reconnaissance.

Influence Campaigns

Influence campaigns use a variety of sources to influence public perception such as hybrid warfare and social media. ***Hybrid warfare*** is a military strategy that blends conventional warfare with unconventional

methods to influence people. In other words, the battles of wars aren't fought on battlefields alone.

As an example, every state in the Union denied women the right to vote since about 1807. Women tried to change this for more than a century. However, they were largely ignored, at least until the early 1900s. Instead of taking their fight to the battlefield, they took their fight to golf fields. In the wee hours of the night, they replaced the hole flags with the purple, green, and white flags of the suffrage movement. They spelled out "Votes for Women" by carefully cutting into the putting greens. Some were less creative and simply destroyed the turf and threw acid on the putting greens. This wasn't the only method women used to get the right to vote. But it was an effective hybrid warfare method of getting the attention of men of power.

Today, a popular hybrid warfare method uses social media, often just to spread misinformation. For example, I remember reading a short blurb on Facebook saying the NFL permanently expelled Tom Brady because of deflategate (where he reportedly ordered the deflation of footballs). I clicked the link, but it took me down a rabbit hole of conspiracy theories, such as Tom Brady being in the early stages of Alzheimer's due to concussions.

I went back to Google and did a couple of searches. No. There weren't any other sources that confirmed these claims. Years later, Tom Brady was named the Most Valuable Player (MVP) after leading the Buccaneers to the 2021 Super Bowl win. However, Facebook's algorithms remembered I clicked that link and continued to show me ads with links to Tom Brady and other football articles. I stopped clicking.

As another example, Cambridge Analytica (CA) was a British political consulting firm that engaged in social media influence campaigns, according to several media outlets. Video footage showed CA executives saying they worked on over 200 elections around the world. The CA managing director of political operations said on video, "We've done it in Mexico, we've done it in Malaysia, we're now moving into Brazil, Australia, China." They closed after these reports surfaced in 2018.

They often used online surveys that looked benign but helped them categorize potential voters by personality style. These surveys also gathered information about political preferences and how respondents gathered

information to make decisions. CA personnel were then able to craft ads targeting these personality styles.

Gaslighting and Influence Campaigns

Gaslighting is a form of psychological manipulation to get individuals to question their sanity. The term comes from the 1938 play *Gas Light* where a husband attempts to convince his wife she is insane by changing things in the environment and then insisting they haven't changed when his wife notices them. As an example, he slowly dims the gas lights in their home. Each time she asks about the dimming lights, he denies it and suggests she is going insane.

Today, people use the term to describe how people use manipulation techniques to control others. The manipulators aren't necessarily trying to convince others that they are insane. Instead, they're trying to replace one idea or belief with another one.

One technique is simply to repeat a lie often enough until people believe it. Paul Goebbels, a Nazi politician and Reich Minister of Propaganda, is attributed with saying, "If you tell a lie big enough and keep repeating it, people will eventually come to believe it." Adolf Hitler used similar techniques to manipulate others. The U.S. Office of Strategic Services included the following in a report describing the psychological profile of Hitler:

"His primary rules were: never allow the public to cool off; never admit a fault or wrong; never concede that there may be some good in your enemy; never leave room for alternatives; never accept blame; concentrate on one enemy at a time and blame him for everything that goes wrong; people will believe a big lie sooner than a little one; and if you repeat it frequently enough people will sooner or later believe it."

One way this succeeds is by controlling information that supports the truth. Admittedly, this is easier to do within a totalitarian state such as Nazi Germany. Influence campaigns in countries with a free press use alternate methods to spread the lie, such as social media and websites that look legitimate. They also discount the legitimate information sources reporting the truth and encourage people not to believe them.

Attacks via Email and Phone

Attackers have been using email to launch attacks for years. One of the primary reasons is because they've been so successful. Many people don't understand how dangerous a simple email can be for the entire organization. Without understanding the danger, they often click a link within a malicious email, which gives attackers access to an entire network. Email attacks include spam, phishing, smishing, vishing, spear phishing, and whaling.

Spam

Spam is unwanted or unsolicited email. While a lot of technologies have reduced spam, it still exists. Some spam is harmless advertisements, while much more is malicious and can include malicious links, malicious code, or malicious attachments. Even when it's not malicious, when it's almost half of all the email you receive, it can waste a lot of your time.

In some cases, legitimate companies encourage users to opt in if they want to receive email about their products. When users opt in to a mailing list, they agree to the terms. On the surface, you'd think that this means that you agree to receive email from the company, and that's true. However, terms often include agreeing to allow their partners to send you email, which means the original company can share your email address with others.

Legitimate companies don't send you malicious spam, but they might send you more email than you want. Laws require them to include the ability to opt out, indicating you don't want to receive any more emails from them. Once you opt out, you shouldn't receive any more emails from that company.

Criminals use a variety of methods to collect email addresses. They buy lists from other criminals, harvest them from websites, and some malware scans address books of infected computers to collect email. Because they are criminals, they don't care about laws, but they might include opt-out instructions in spam they send. However, instead of using this to remove you from their email list, attackers use this as confirmation that your email address is valid. The result is more spam.

Spam over Internet Messaging

Spam over Internet messaging (SPIM) is unwanted messages sent over instant messaging (IM) channels. IM is a technology that allows people to communicate in real time or chat with each other by sending and receiving short text messages.

The original Short Message Service (SMS) was limited to only 160 text characters. However, advanced texting apps support attachments which can easily be malware. Some scammers have sent SPIM with malicious links.

Mobile devices such as phones and tablets have default texting apps installed. Other messaging apps include Facebook Messenger, WhatsApp, and Snapchat. While spam is sent to email addresses, SPIM can be sent to you via your username or your telephone number. A challenge is that SPIM bypasses typical antivirus and spam filters.

During the COVID-19 pandemic, two scam types were quite popular among criminals. In one, the text informs recipients that they have been in contact with someone who has tested positive for COVID-19 and encourages them to take further action. The text includes a malicious link. If clicked, it may allow attackers access to the user's mobile device.

In another scam, recipients receive a message related to the U.S. stimulus payments for U.S. citizens. Scammers claimed they could get the money for a fee, but fees were never required. Some scammers attempted to get personal information such as Social Security numbers and bank account numbers and then used the information for identity theft and identity fraud.

Phishing

Phishing is the practice of sending email to users with the purpose of tricking them into revealing personal information or clicking on a link. A phishing attack often sends the user to a malicious website that appears to the user as a legitimate site. Other times, it includes a malicious attachment and encourages the user to open it.

The classic example is where a user receives an email that looks like it came from eBay, PayPal, a bank, or some other well-known company. The "phisher" doesn't know if the recipient has an account at the company, just as a fisherman doesn't always know if any fish are in the water where he

casts his line. However, if the attacker sends out enough emails, the odds are good that someone who receives the email has an account and will be fooled. The email may look like this:

“We have noticed suspicious activity on your account. To protect your privacy, we will suspend your account unless you log in and validate your credentials. Click here to validate your account and prevent it from being locked out.”

The email often includes the same graphics that you would find on the vendor’s website or an actual email from the vendor. Although it might look genuine, it isn’t. Legitimate companies do not ask you to revalidate your credentials via email. If you go directly to the actual site, you might be asked to provide additional information to prove your identity beyond your credentials, but legitimate companies don’t send emails asking you to follow a link and input your credentials to validate them.

Remember this

Spam is unwanted email. Phishing is malicious spam. Attackers attempt to trick users into revealing sensitive or personal information or clicking on a link. Links within email can also lead unsuspecting users to install malware.

Beware of Email from Friends

Criminals have become adept at impersonating your friends. They scan social media sites and identify your friends and family. They then send emails to you that look like they are from your friends or family members, but they really aren’t. This has become a common security issue related to social media.

As an example, imagine you are friends with Lisa Simpson and her email address is lisa@simpsons.com. You might receive an email that includes “Lisa Simpson” in the From block. However, if you look closely at the actual email address, you’d find it is something different, such as homer@hacker.com. The underlying email address might belong to someone, but the forgery doesn’t mean that they sent the email. To identify the actual sender, you often need to look at the full header of the email address.

I see emails such as this quite often. They seem to be related to comments or Likes that I’ve made on social media. For example, after

“liking” a Facebook post on Lisa Simpson’s Facebook page, I later receive an email with Lisa Simpson in the From block and a forged email address. These emails typically include a single line such as “I thought you might like this” and a malicious link. Clicking the link often takes the user to a server that attempts a drive-by download. It might include a cat or a baby video, but this is just to distract you while the malicious code is being downloaded.

Another possible scenario is that an attacker has joined your friend’s computer to a botnet. A bot herder is now using your friend’s computer to send out phishing emails.

Phishing to Install Malware

One phishing email looked like it was from a news organization with headlines of recent news events. If the user clicked anywhere in the email, it showed a dialog box indicating that the user’s version of Adobe Flash was too old to view the story. It then asked, “Would you like to upgrade your version of Adobe Flash?” If the user clicked Yes, it downloaded and installed malware. The “upgrade” fake has been used successfully over the years and continues to be used today.

Another email had the subject line “We have hijacked your baby” and the following content:

“You must pay once to us \$50,000. The details we will send later.
We have attached photo of your family.”

The English seems off, and the receiver might not even have a baby, making this look bogus right away. However, the attackers are only trying to pique your curiosity. The attached file isn’t a photo. Instead, it’s malware. If a user clicks on the photo to look at it, it may show a photo, but it also installs malware on the user’s system.

Phishing to Validate Email Addresses

A simple method used to validate email addresses is the use of beacons. A beacon is a link included in the email that links to an image stored on an Internet server. The link includes a unique code that identifies the receiver’s email address.

For the email application to display the image, it must retrieve the image from the Internet server. When the server hosting the image receives the

request, it marks the user's email address indicating it's valid. This is one of the reasons that most email programs won't display images by default.

Phishing to Get Money

The classic Nigerian scam (also called a 419 scam) continues to thrive. You receive an email from someone claiming a relative or acquaintance has millions of dollars. Unfortunately, the sender can't get the money without your help. The email says that you'll get a substantial portion of the money for your troubles if you help retrieve the money.

This scam often requires the victim to pay a small sum of money with the promise of a large sum of money. However, the large sum never appears. Instead, the attackers come up with reasons why they need just a little more money. In many cases, the scammers request access to your bank account to deposit your share, but instead they use it to empty your bank account.

There are countless variations on this scam. Lottery scams inform email recipients they won. Victims sometimes pay small fees to release the funds or provide bank information to get the money deposited. They soon learn there is no prize, but instead they've lost all their savings.

Spear Phishing

Spear phishing is a targeted form of phishing. Instead of sending the email out to everyone indiscriminately, a spear phishing attack attempts to target specific groups of users, or even a single user. Spear phishing attacks may target employees within a company or customers of a company.

As an example, an attacker might try to impersonate the CEO of an organization in an email. It's relatively simple to change the header of an email so that the From field includes anything, including the CEO's name and title. Attackers can send an email to all employees requesting that they reply with their password. Because the email looks like it's coming from the CEO, these types of phishing emails fool uneducated users.

One solution that deters the success of these types of spear phishing attacks is to use digital signatures. The CEO and anyone else in the company can sign their emails with a digital signature. This provides a high level of certainty to personnel on who sent the email. Chapter 10,

“Understanding Cryptography and PKI,” covers digital signatures in great depth.

Whaling

Whaling is a form of spear phishing that attempts to target high-level executives. Las Vegas casinos refer to the big spenders as whales, and casino managers are willing to spend extra time and effort to bring them into their casinos. Similarly, attackers consider high-level executives the whales, and attackers are willing to put in some extra effort to catch a whale because the payoff can be so great. When successful, attackers gain confidential company information that they might not be able to get anywhere else.

Some whaling attacks target senior executives of organizations. Other whaling attacks impersonate these senior executives and send malicious emails to high-level employees. One attacker sent an email to the HR department of Seagate, making it look like the email came from the company’s CEO. The email asked for W-2 tax forms and other Personally Identifiable Information. The HR department released details of almost 10,000 employees.

A similar attack occurred within Snapchat. The payroll team received an email that looked like it was the Snapchat CEO and requested payroll data. The payroll team complied, and the information was soon leaked on the Internet.

Similar whaling attacks have masqueraded as complaints from the Better Business Bureau or the Justice Department. Executives are sensitive to issues that may affect the company’s profit and reputation, and these complaints get their attention. Although not as common, some whaling attacks attempt to reach the executive via phone to get the data. However, many executives have assistants who screen calls to prevent attackers from reaching the executive via phone.

Remember this

A spear phishing attack targets specific groups of users. It could target employees within a company or customers of a company. Digital signatures provide assurances to recipients about who sent an email and can reduce the

success of spear phishing. Whaling targets high-level executives or impersonates high-level executives.

Vishing

Vishing attacks use the phone system to trick users into giving up personal and financial information. Vishing often uses Voice over IP (VoIP) technology allowing the attacker to spoof caller ID, making it appear as though the call came from a real company.

In one form of the attack, a machine leaves a phone message saying that you need to return the call concerning one of your credit cards. In another form, you receive an email with the same information. If you call, you'll hear an automated recording giving some vague excuse about a policy and prompting you to verify your identity. One by one, the recording prompts you for more information, such as your name, birthday, Social Security number, credit card number, expiration date, and so on. Sometimes, the recording asks for usernames and passwords. If you give all the requested information, the recording indicates they have verified your account. In reality, you just gave up valuable information on yourself.

Another example of vishing is just a regular phone call from a criminal. A popular ploy is a call from a company claiming to be "Credit Services" and offering to give you lower credit card rates. They play around with caller ID and have it display anything they want. A common ploy is to display a number with the same area code as yours, making them appear local. They often announce, "This is your second and final notice," trying to evoke a sense of urgency.

If you answer, the automated system forwards you to a live person who begins asking a series of "qualifying" questions, such as how much credit card debt you have and what your interest rates are. They then promise that they can help you lower your debt and get you a better rate. Next, they start asking some personal questions. They might ask for the last four digits of your Social Security number so they can "verify your account is in good standing." They might ask you for the code on your credit card "to verify you still have it."

Eventually, they hope to get your credit card number, expiration date, and code so that they can use it to post fraudulent charges. Some people

have reported similar callers trying to get their bank information so that they can transfer money out of the accounts.

They hang up right away if you ask them to take you off their list or stop calling. Similarly, they hang up when they hear words such as criminal, thief, and other words I'll leave out of this book. Some even reply with insults. They've called me so often I've played along a few times. I love it when they ask for information on my credit card. I respond by saying, "Can you hold on so I can get it?" I then put the phone in a drawer and go back to work. Once, they stayed on the line for more than three hours waiting for me.

Smishing

Smishing (a mashup of SMS and phishing) is a form of phishing that uses text instead of email. Some smishing texts include malicious attachments, and some try to trick the user into giving up personal information.

As an example, one smishing attack sent users a text claiming to be from Google security. It reported suspicious activity on the user's Google account, and said that Google would be sending a verification code. It then encouraged the user to reply to the text with the verification code and threatened to permanently lock the user's account if the user didn't reply. This was not sent by Google but instead was sent by an attacker. Shortly after sending the text, the attacker went to the Google login page, entered the user's email address, and clicked the Forgot password link. He then clicked through to send a verification code to the user's phone. If the user sends this code to the attacker, it allows the attacker to change the password for the account and log in as the user.

The same method can be used with any organization where a user has implemented 2FA (two-factor authentication). If the user replies with the verification code, it allows the attacker to hijack the user's account. If it is a financial organization, the attacker can quickly empty the victim's account.

Remember this

Vishing is a form of phishing that uses the phone system or VoIP. Some vishing attempts are fully automated. Others start as automated calls, but an

attacker takes over at some point during the call. Smishing is a form of phishing using text messages.

One Click Lets Them In

It's worth stressing that it only takes one click by an uneducated user to give an attacker almost unlimited access to an organization's network. Consider Figure 6.1. It outlines the process APTs have used to launch attacks.

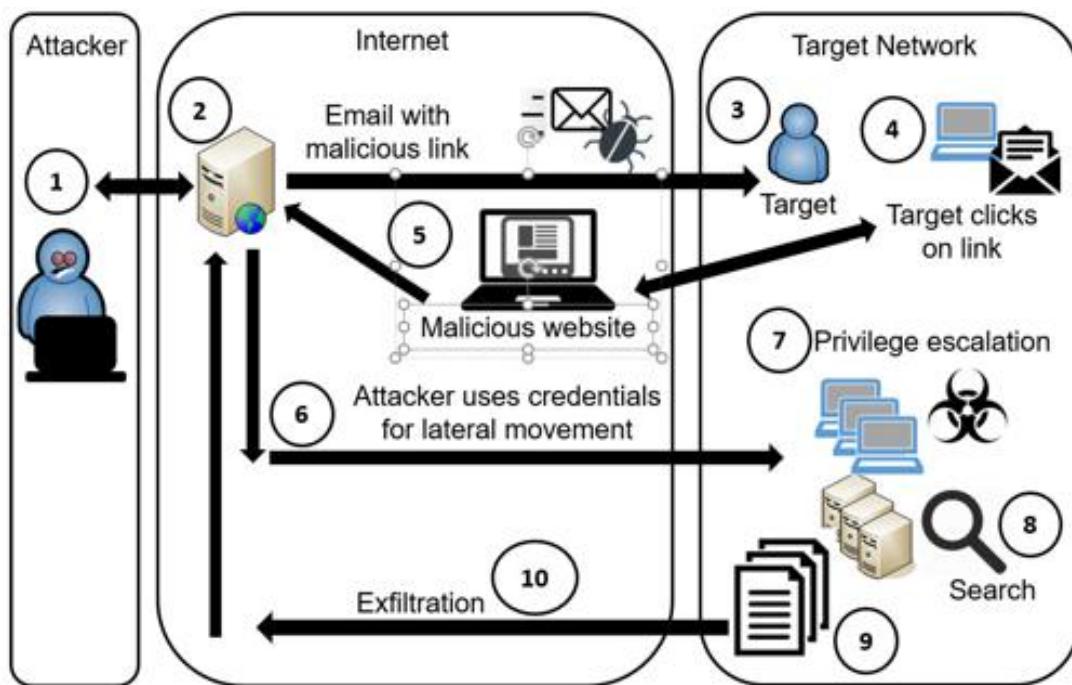


Figure 6.1: Steps in an attack

Note that the attacker can be located anywhere in the world and only needs access to the Internet. The attacker controls resources within the Internet, such as servers owned and operated by the attackers. They might be in the same country as the attacker, or they might be in another country. In some cases, attackers use servers owned by others but controlled by the attackers, such as servers in a botnet or compromised servers.

The target is within an internal network of a targeted organization. Refer to Figure 6.1 as you read the following steps in an attack:

- The attacker uses open source intelligence to identify a target. Some typical sources are social media sites and news outlets. Other times, attackers use social engineering tactics via phone calls and emails to get information on the organization or individuals employed by the organization.

- Next, the attacker crafts a spear phishing email with a malicious link. The email might include links to malware hosted on another site and encourage the user to click the link. In many cases, this link can activate a drive-by download that installs itself on the user's computer without the user's knowledge. This download can be any kind of malware, including ransomware. Other attacks use credential harvesting techniques encouraging users to click a link and enter their usernames and passwords on bogus sites that look real. While not shown in the figure, the attacker could include an attachment and encourage the recipient to open it instead of using a malicious link.
- The attacker sends the spear phishing email to the target from an Internet-based system. This email includes a malicious link and uses words designed to trick the user into clicking it.
- If the user clicks on the link, it takes the user to a website that looks legitimate. This website might attempt a drive-by download, or it might mimic a legitimate website and encourage the user to enter a username and password.
- If the malicious link tricked the user into entering credentials, the website sends the information back to the attacker. Suppose the malicious link installed malware on the user's system, such as a RAT. In that case, the attacker uses it to collect information on the user's computer (including the user's credentials, once discovered) and sends it back to the attacker.
- The attacker uses the credentials to access the targeted system. It then uses the targeted system for lateral movement. In other words, it uses the targeted system and the targeted user credentials to access other systems within the network. Windows Management Instrumentation (WMI) and PowerShell are frequently used to scan the network.
- The original target may have limited access within the network. However, attackers use privilege escalation techniques to gain more permissions within the network and access more resources, such as servers holding sensitive data. The attacker uses these elevated permissions to install malware on other

systems, along with creating new backdoor accounts within the network.

- Malware searches for data within the network such as emails and files on computers and servers.
- The malware gathers all data of interest and typically divides it into encrypted chunks.
- These encrypted chunks are exfiltrated out of the network and back to the attacker.

The time it takes for an attacker to begin lateral movement within a network after the initial infection is typically less than two hours. At that point, the attacker can begin data exfiltration. In a ransomware attack, the malware can begin encrypting data as soon as it locates it within the network. However, some ransomware attempts to locate important data, such as online backups, before it begins encryption.

Blocking Malware and Other Attacks

The previous sections described several different methods attackers and criminals use to launch new attacks. Malware is a significant threat for any organization. Administrators commonly implement layered security, or a defense-in-depth plan, to protect against malware. The following bullets list some common security controls used to protect against malware:

- **Spam filter on mail gateways.** Phishing attacks are delivered as malicious spam. Spam filters on email servers detect and filter spam before it ever gets to users. Some networks route email through another device first to filter out spam. If users never receive a malicious email, there isn't any chance of them clicking on a malicious link in that email.
- **Anti-malware software on mail gateways.** Malicious email often includes malware as attachments. Anti-malware software on the mail server can detect and block it. The software strips potentially malicious attachments off the email, and typically sends a notification to the user explaining what was removed and why.
- **All systems.** All workstations and servers have anti-malware software installed. Servers may have additional, specialized anti-malware software installed depending on the applications running on the servers.
- **Boundaries or firewalls.** Many networks include detection tools that monitor network traffic through the firewall. For example, unified threat management (UTM) inspects network traffic to reduce the risk of malware entering the network. Chapter 3, “Exploring Network Technologies and Tools,” covers UTM systems.

Spam Filters

Organizations often implement a multipronged approach to block spam. For example, many UTM systems include spam filters to detect and block spam. The output of the UTM goes to an email server. Email servers also have methods of detecting and blocking spam. The email server sends all email to the users, except for what it detects as spam. User systems also have anti-spam filters, or junk mail options, as a final check.

The challenge with any ***spam filter*** is to filter out spam only and never filter out legitimate email. For example, a company wouldn't want a spam filter to filter out an email from a customer trying to buy something. Because of this, most spam filters err on the side of caution, allowing spam through rather than potentially marking valid email as spam. Although the science behind spam filtering continues to improve, criminals have also continued to adapt.

Spam filters typically allow you to identify email addresses as safe or to be blocked. You can add these as individual addresses or entire domains. For example, if you want to ensure you get an email from Homer when he sends an email from springfield.com, you can identify homer@springfield.com as a safe email address. If you want to ensure you get all emails from springfield.com, you can designate springfield.com as a safe domain. Similarly, you can block either the single email address homer@springfield.com or the entire domain springfield.com.

Antivirus and Anti-Malware Software

Anti-malware software protects against many types of malware. You'll often hear the term ***antivirus*** software indicating it only protects against viruses. However, the lines have blurred. Viruses aren't the only threats. Attackers have changed their methodologies using different types of malware, and antivirus software vendors have adapted by including methods to detect and block these new threats. Most antivirus software detects, blocks, and removes several types of malware, such as viruses, Trojans, worms, rootkits, spyware, and adware. Antivirus software provides real-time protection and can perform both scheduled and manual scans. The real-time protection continuously monitors the system. For example, when a user visits a website, antivirus software scans the downloaded website files and attempts to block malicious code.

Similarly, when a user downloads or opens a file, antivirus software scans it before opening it. Scheduled scans occur regularly, such as once a week. If users or technicians detect suspicious activity, they can perform manual scans to check the system.

If the antivirus software detects malware, it will typically quarantine it and notify the user. However, the exact way antivirus software does so varies from one vendor to another. The key to analyzing and interpreting the antivirus software's output is to recognize the alert and read it. Some people just click OK without paying attention to alerts and can inadvertently override the antivirus software.

Antivirus software detects viruses using either signature-based detection or heuristic-based detection.

Signature-Based Detection

Viruses and other malware have known patterns. Signature files (also called data definition files) define the patterns, and the antivirus software scans files for matching patterns. When the software identifies a matching pattern, it reports it as an infection and takes action, such as deleting or quarantining the file.

A quarantined virus is not harmful to the system while it is in quarantine, but it's still available for analysis. As an example, a security

professional could release a quarantined virus into an unprotected but isolated virtual machine environment for research and study.

Malware developers regularly release new viruses, so it's essential to update signature definition files regularly. Most antivirus software includes the ability to automate the process of checking and downloading updated signature definition files. They typically check for updates several times a day.

It's also possible to download and install signature files manually. Administrators do this when updating systems that do not have Internet access. When doing so, administrators need to ensure the signature file has not lost data integrity by comparing the hash of the signature file posted on the antivirus vendor's website with the hash of the downloaded file.

Heuristic-Based Detection

Some antivirus software includes heuristic-based detection. Heuristic-based detection attempts to detect viruses that were previously unknown and do not have signatures. This includes zero-day exploits mentioned earlier in this chapter.

Heuristic-based analysis runs questionable code in a sandbox or virtualized environment specifically designed to protect the live environment while observing the code's behavior. Most viruses engage in malicious or suspicious activities that you won't see in legitimate programs. The heuristic-based analysis detects these activities.

As an example, polymorphic malware adds variations to files when it creates copies. It's highly unusual for any application to add variations in files like this, and heuristic methods are often successful at detecting polymorphic malware.

Remember this

Antivirus software detects and removes malware, such as viruses, Trojans, and worms. Signature-based antivirus software detects known malware based on signature definitions. Heuristic-based software detects previously unknown malware based on behavior.

File Integrity Monitors

Some antivirus scanners use ***file integrity monitors*** to detect modified system files. A file integrity checker calculates hashes on system files as a baseline. It then periodically recalculates the hashes on these files and compares them with the hashes in the baseline. If the hashes are ever different, it indicates the system files have been modified. When an antivirus scanner detects a modified file, it sends an alert. Many times, these alerts can detect rootkit infections.

Cuckoo Sandbox

Cuckoo Sandbox is an open-source automated software analysis system. Its primary purpose is to analyze suspicious files, such as suspected malware. Unlike malware that analyzes files in real-time, you need to submit files to Cuckoo Sandbox. Cuckoo then runs it in a virtual machine (VM) and creates a report on its activity.

You submit files to Cuckoo through a web interface or a console. Cuckoo determines the best VM image to use and the best analysis method. It then launches the VM, submits the file to the VM, and performs the analysis.

The primary reason IT professionals use Cuckoo Sandbox is to get quick and definitive feedback on suspicious files and URLs. For example, a user may receive a suspicious attachment via email, but anti-virus software doesn't recognize it as malware. By submitting it to Cuckoo Sandbox, IT professionals can identify what the file would do if unleashed in the live environment.

Why Social Engineering Works

Social engineers typically use one or more psychology-based principles to increase the effectiveness of their attacks. By teaching users about the different social engineering tactics and these underlying principles, it reduces the chances that they'll be tricked. The following sections introduce these topics.

Authority

Many people were raised to respect authority and are more likely to comply when a person of authority says to do so. As an example, volunteers participating in the Milgram experiment continued to send shocks to unseen subjects even though they could hear them scream in pain simply because a man in a lab coat told them to continue. They weren't actually sending shocks, and the screams were fake, but everything seemed real to the volunteers. Psychologists have repeated these experiments and have seen similar results. Using authority is most effective with impersonation, whaling, and vishing attacks:

- **Impersonation.** Some social engineers impersonate others to get people to do something. For example, many have called users on the phone claiming they work for Microsoft, the IRS, or some other government agency. Other times, social engineers attempt to impersonate a person of authority, such as an executive within a company or a technician.
- **Whaling.** Executives respect authorities such as legal entities. Many whaling attacks send malicious files as email attachments and identify them as lawsuits or subpoenas, and encourage the executives to open them.
- **Vishing.** Some attackers use the phone to impersonate authority figures.

Intimidation

In some cases, the attacker attempts to intimidate the victim into acting. Intimidation might be through bullying tactics, and it is often

combined with impersonating someone else. Using intimidation is most effective with impersonation and vishing attacks.

For example, a social engineer might call an executive's receptionist with this request: "Mr. Simpson is about to give a huge presentation to potential customers, but his files are corrupt. He told me to call you and get you to send the files to me immediately so that I can get him set up for his talk." If the receptionist declines, the social engineer can use intimidation tactics by saying something like: "Look, if you want to be responsible for this million-dollar sale falling through, that's fine. I'll tell him you don't want to help."

Note that this tactic can use multiple principles at the same time. In this example, the attacker is combining intimidation with urgency. The receptionist doesn't have much time to respond.

Consensus

People are often more willing to like something that other people like. Some attackers take advantage of this by creating websites with fake testimonials that promote a product. For example, criminals have set up multiple websites with dozens of testimonials listing all the benefits of their fake antivirus software. If users search the Internet before downloading the fake antivirus software, they will come across these websites and believe that other real people are vouching for the product.

Using consensus, sometimes called social proof, is most effective with Trojans and hoaxes. Victims are more likely to install a Trojan if everyone seems to indicate it's safe. Similarly, if a person suspects a virus notice is just a hoax, but everyone seems to be saying it's real, the victim is more likely to be tricked.

Scarcity

People are often encouraged to act when they think there is a limited quantity of an item. As an example of scarcity, think of Apple iPhones. When Apple first releases a new version, they typically sell out quickly. A phishing email can take advantage of this and encourage users to click a link for exclusive access to a new product. If the users click, they'll end up at a malicious website. Scarcity is often effective with phishing and Trojan attacks. People make quick decisions without thinking them through.

Urgency

Some attacks use urgency as a technique to encourage people to act. As an example, ransomware uses the scarcity principle with a countdown timer and the countdown timer provides a sense of urgency. Victims typically have 72 hours to pay up before they lose all their data. Each time they look at their computer, they'll see the timer counting down.

Using urgency is most effective with ransomware, phishing, vishing, and whaling. For example, phishing emails with malicious links might indicate that there are a limited number of products at a certain price, so the user should "Click Now." Similarly, executives might be tricked into thinking a subpoena requires immediate action.

Remember this

Many of the reasons that social engineers are effective are because they use psychology-based techniques to overcome users' objections. These techniques include representing themselves as authority figures, using intimidation, faking scarcity, creating a sense of urgency, establishing familiarity, and creating a sense of trust.

Familiarity

If you like someone, you are more likely to do what the person asks. This is why so many big companies hire well-liked celebrities. It's also why they fire them when the celebrity becomes embroiled in a scandal that affects their credibility.

Some social engineers attempt to build rapport with the victim to build a relationship before launching the attack. This principle is most effective with shoulder surfing and tailgating attacks:

- **Shoulder surfing.** People are more likely to accept someone looking over their shoulder when they are familiar with the other person, or they like them. In contrast, if you don't know or don't like someone, you are more likely to recognize a shoulder surfing attack and stop it immediately.
- **Tailgating.** People are much more likely to allow someone to tailgate behind them if they know the person or like the person. Some social engineers use a simple, disarming smile to get the other person to like them.

Trust

In addition to familiarity, some social engineers attempt to build a trusting relationship between them and the victim. This often takes a little time, but the reward for the criminal can be worth it. Vishing attacks often use this method.

As an example, someone identifying himself as a security expert once called me. He said he was working for some company with “Secure” in its name, and they noticed that my computer was sending out errors. He stressed a couple of times that they deploy and support Windows systems. The company name and their experience was an attempt to start building trust.

He then guided me through the process of opening Event Viewer and viewing some errors on my system. He asked me to describe what I saw and eventually said, “Oh my God!” with the voice of a well-seasoned actor. He explained that this indicated my computer was seriously infected. However, I knew that the errors were trivial.

After seriously explaining how much trouble I was in with my computer, he then added a smile to his voice and said, “But this is your lucky day. I’m going to help you.” He offered to guide me through the process of fixing my computer before the malware damaged it permanently.

All of this was to build trust. At this point, he went in for the kill. He had me open the Run window and type in a website address, and asked me to click OK. This is where I stopped. I didn’t click OK.

I tried to get him to answer some questions, but he was evasive. Eventually, I heard a click. My “lucky day” experience with this social engineering criminal was over.

The link probably would have taken me to a malicious website ready with a drive-by download. Possibly the attacker was going to guide me through the process of installing malware on my system. If my system objected with an error, I’m betting he would have been ready with a soothing voice saying “That’s normal. Just click OK. Trust me.” He spent a lot of time with me. I suspect that they’ve been quite successful with this ruse with many other people.

Threat Intelligence Sources

One common method that attackers often use before launching an attack is to gather information from ***open source intelligence (OSINT)***. Penetration testers (discussed in more detail in Chapter 8) also use OSINT methods to gather information on targets. This includes any information that is available to the general public, such as via websites and social media. For example, if attackers want to get the name of the chief executive officer (CEO) of a company, they can probably find it on the company's website. Similarly, many organizations post information on social media sites such as Facebook and Twitter.

In contrast, ***closed/proprietary intelligence*** refers to trade secrets such as intellectual property. An organization tries to keep these private, but attackers sometimes infiltrate an organization to steal these trade secrets.

Some common types of OSINT are:

- **Vulnerability databases.** Vulnerability databases document known vulnerabilities and many public databases help automate vulnerability management. Two examples are the National Vulnerability Database (NVD), maintained by the U.S. government, and the Common Vulnerabilities and Exposures (CVE) list maintained by the MITRE Corporation.
- **Trusted Automated eXchange of Indicator Information (TAXII).** TAXII is an open standard that defines a set of services and message exchanges used to share information. It provides a standard way for organizations to exchange cyber threat information, but it does not specify what information organizations should exchange.
- **Structured Threat Information eXpression (STIX).** STIX is an open standard that identifies what cyber threat information organizations should share. It provides a common language for addressing a wide range of cyber threat information. STIX data is shared via TAXII.
- **Automated indicator sharing (AIS).** The Cybersecurity and Infrastructure Security Agency (CISA) maintains the Automated Indicator Sharing site (<https://www.cisa.gov/ais>)

used for real-time exchange of threat indicators and defensive measures. AIS uses both TAXII and STIX.

- **Dark web.** The dark web is an area of the Internet that you won't find using a search engine. Criminals and attackers maintain sites on the dark web (sometimes called darknets), but users need specific software or authentication to access them. Criminals often store and sell hacking tools, access to botnets, pirated materials, and more on the dark web. Some dark web sites provide up-to-date information on known vulnerabilities. Vulnerabilities are sometimes posted on the dark web before it makes it to vulnerability databases such as the NVD or CVE.
- **Public/private information sharing centers.** Many public and private organizations are also involved in sharing information on cyber threats. For example, InfraGard is a non-profit organization that shares information between the Federal Bureau of Investigation (FBI) and members in specific sectors.
- **Indicators of compromise.** Indicators of compromise (IoC) are evidence that a cyberattack is happening or has happened. Obvious IoCs are confirmed alerts from antivirus software or other devices that have detected malware or other potential attacks. Often, an IoC isn't as obvious but alerts indicate what cybersecurity professionals should look for. As an example, CISA released a Malware Analysis Report (AR21-048A) on "AppleJeus: Celas Trade Pro." IoCs included in the report included the URL where users could download the malware, the name of specific files included in the malware, and more. Cybersecurity professionals can use this data to search proxy logs to see if users accessed the URL and then search systems for the specific files.
- **Predictive analysis.** Predictive analysis techniques attempt to predict what attackers will do next and how to thwart their attacks. While cybersecurity professionals are getting better every day at predicting and stopping attacks, it's worth noting that this requires them to predict the future. This may be easy if you have a DeLorean time machine allowing you to travel back

to the future at will. Without the DeLorean though, predictive analysis remains challenging.

- **Threat maps.** Threat maps provide a visual representation of active threats. They typically show a replay of recent attacks rather than real-time data. Additionally, the data is anonymized so you don't know who is being attacked, but you can see the location within countries. Redlegg (<https://www.redlegg.com/blog/cyber-threat-maps>) has a listing and description of many threat maps maintained by other organizations.
- **File/code repositories.** Many repositories include prewritten code that developers can use for a variety of purposes, including gathering intelligence. As an example, GitHub offers distributed version control and source code management for software projects. This allows multiple developers to work together on the same project collaboratively. Some GitHub projects are file repositories. For example, the Awesome Threat Intelligence repository (<https://github.com/hslatman/awesome-threat-intelligence>) provides a listing of resources.

Research Sources

There's an almost endless list of additional sources that cybersecurity personnel can reference when researching threats. Chapter 8 discusses some in the context of threat hunting. The following bullets introduce additional resources:

- **Vendor websites.** Vendor websites are a good source for reliable information on a vendor's products. This is especially true related to any vulnerabilities and patches used to fix them.
- **Conferences.** Many organizations host conferences dedicated to sharing cybersecurity information. These typically last three to five days, include several knowledgeable speakers, and include various training tracks allowing attendees to pick what workshops they want to attend.
- **Local industry groups.** A local industry group is any group of people or organizations that work in the same industry and

decide to collaborate to share information. This is similar to people joining a networking group to build their contacts.

- **Public/private information sharing centers.** Many public and private organizations are also involved in sharing information on cyber threats. For example, InfraGard is a non-profit organization that shares information between the Federal Bureau of Investigation (FBI) and members in specific sectors.
- **Academic journals.** Cybersecurity professionals often publish scholarly articles in academic journals. These are often used to document research on a technical topic, and it's common for peers to review the articles prior to publication. This gives them added credibility.
- **Request for comments (RFC).** The Internet Engineering Task Force (IETF) publishes documents called RFCs for a variety of purposes. Many are Internet standards, and they are the authoritative source of knowledge for technical specifications. As an example, Chapter 1, “Mastering Security Basics,” mentioned RFC 6749, “The OAuth 2.0 Authorization Framework.” RFC 6749 describes how authorization tokens are created and exchanged on the Internet. As long as websites follow the specifications in RFC 6749, they can exchange authorization tokens relatively easily.
- **Social media.** Some people exchange data via social media groups, which can be useful. This allows people to communicate with their peers about potential threats. However, it's important to realize that social media groups aren't authoritative, so it's a good idea to verify information shared in social media groups before acting on it.

Chapter 6 Exam Topic Review

When preparing for the exam, make sure you understand these key concepts covered in this chapter.

Understanding Threat Actors

- An advanced persistent threat (APT) is a group of individuals sponsored by a nation-state giving them a significant amount of resources and funding. APTs have both the capability and intent to launch sophisticated and targeted attacks.
- Script kiddies use existing computer scripts or code to launch attacks. They typically have very little expertise or sophistication and very little funding.
- A hacktivist launches attacks as part of an activist movement or to further a cause.
- Insiders (such as employees of a company) have legitimate access to an organization's internal resources. They sometimes become malicious insiders out of greed or revenge. DLP solutions can prevent users from writing data to external media devices.
- Competitors sometimes engage in attacks to gain proprietary information about another company.
- Organized crime is an enterprise that employs a group of individuals working together in criminal activities. Their primary motivation is money.
- Shadow IT refers to unauthorized systems or applications installed on a network without authorization or approval.
- Cybersecurity professionals and attackers use open source intelligence (OSINT) sources to learn about vulnerabilities, how attackers exploit them, and how organizations can protect against the threats.

Determining Malware Types

- Malware includes several different types of malicious code, including viruses, worms, logic bombs, backdoors, Trojans, ransomware, rootkits, and more.
- A virus is malicious code that attaches itself to a host application. The code runs when the application is launched.
- A worm is self-replicating malware that travels throughout a network without user intervention.
- A logic bomb executes in response to an event, such as a day, time, or condition. Malicious insiders have planted logic bombs into existing systems, and these logic bombs have delivered their payload after the employee left the company.
- Backdoors provide another way of accessing a system. Programmers can create backdoors in applications, and malware can insert backdoors into systems. Backdoors give attackers remote access to systems.
- A Trojan appears to be one thing, such as pirated software or free antivirus software, but is something malicious. A remote access Trojan (RAT) is a type of malware that allows attackers to take control of systems from remote locations.
- Ransomware is a type of malware that takes control of a user's system or data. Criminals demand a ransom payment before returning control of the computer. Cryptomalware is ransomware that encrypts the user's data. Attackers demand payment to decrypt the data.
- Spyware is software installed on user systems without the user's knowledge or consent and it monitors the user's activities. It sometimes includes a keylogger that records user keystrokes.
- A botnet is a group of computers called zombies controlled through a command and control server. Attackers use malware to join computers to botnets. Bot herders launch attacks, such as DDoS attacks, through botnets.
- Rootkits take root-level or kernel-level control of a system. They hide their processes to avoid detection, and they can remove user privileges and modify system files.

- A potentially unwanted program (PUP) is software installed when a user installs another program, often without the user's knowledge. Many PUPs change the default home page of a user's browser or change the default search engine.
- A fileless virus is a type of malicious software that runs in memory instead of a written file to disk. Fileless viruses often use PowerShell scripts, but can also travel in vCards.

Recognizing Common Attacks

- Social engineering uses social tactics to gain information or trick users into performing actions they wouldn't normally take. Social engineering attacks can occur in person, over the phone, while surfing the Internet, and via email. Many social engineers attempt to impersonate others.
- Shoulder surfing is an attempt to gain unauthorized information through casual observation, such as looking over someone's shoulder, or monitoring screens with a camera. Screen filters can thwart shoulder surfing attempts.
- A hoax is a message, often circulated through email, that tells of impending doom from a virus or other security threat that simply doesn't exist.
- Tailgating is the practice of one person following closely behind another without showing credentials. Access control vestibules (sometimes called mantraps) help prevent tailgating.
- Dumpster divers search through trash looking for information. Shredding or burning documents reduces the risks associated with dumpster diving.
- Zero-day exploits take advantage of previously unknown vulnerabilities. Either vendors don't know about the vulnerability or haven't written patches for it yet.
- Watering hole attacks discover sites that a targeted group visits and trusts. Attackers then modify these sites to download malware. When the targeted group visits the

modified site, they are more likely to download and install infected files.

- Social engineers use prepping by presenting a fake scenario before asking for information.
- Spam is unwanted or unsolicited email. Attackers often use spam in different types of attacks.
- Phishing is the practice of sending email to users to trick them into revealing sensitive information, installing malware, or clicking on a link.
- Spear phishing and whaling are types of phishing. Spear phishing targets specific groups of users, and whaling targets high-level executives.
- Vishing is a form of phishing that uses voice over the telephone and often uses Voice over IP (VoIP). Some vishing attacks start with a recorded voice and then switch over to a live person.

Blocking Malware and Other Attacks

- Anti-spam software attempts to block unsolicited email. You can configure a spam filter to block individual email addresses and email domains.
- Antivirus software can detect and block different malware types, such as worms, viruses, and Trojans. Antivirus software uses signatures to detect known malware and heuristics to detect potential malware based on behavior.
- When downloading signatures manually, hashes can verify the integrity of signature files. Antivirus software typically includes a file integrity checker to detect files modified by a rootkit.
- Social engineers and other criminals employ several psychology-based principles to help increase the effectiveness of their attacks. They are authority, intimidation, consensus, scarcity, urgency, familiarity, and trust.

in References

- Have you done the online labs? Check out the online content to view some extra materials at <https://greatadministrator.com/601-extras>. They might help you understand some key content.

Chapter 6 Practice Questions

1. A tech company recently discovered an attack on its organization, resulting in a significant data breach of customer data. After investigating the attack, they realized it was very sophisticated and likely originated from a foreign country. Which of the following identifies the MOST likely threat actor in this attack?
 - A. Hacktivist
 - B. APT
 - C. Competitors
 - D. Insiders

2. An attacker purchased an exploit on the Internet. He then used it to modify an item's price in an online shopping cart during checkout. Which of the following BEST describes this attacker?
 - A. Insider
 - B. Script kiddie
 - C. Competitor
 - D. Hacktivist
 - E. APT

3. Lisa is a database administrator. She received a phone call from someone identifying himself as a representative from a known hardware vendor. He said he's calling customers to inform them of a problem with database servers they've sold, but he said the problem only affects servers running a specific operating system version. He asks Lisa what operating system versions the company is running on their database servers. Which of the following BEST describes the tactic used by the caller in this scenario?
 - A. Pretexting
 - B. Tailgating
 - C. Pharming
 - D. Smishing

4. An attacker recently attacked a web server hosted by your company. After investigating the attack, security professionals determined that the

attacker used a previously unknown application exploit. Which of the following BEST identifies this attack?

- A. Buffer overflow
- B. Zero-day attack
- C. Man-in-the-browser
- D. Integer overflow

5. After Bart logged on to his computer, he was unable to access any data. Instead, his screen displayed a message indicating that unless he made a payment, his hard drive would be formatted, and he'd permanently lose access to his data. What does this indicate?

- A. Keylogger
- B. Ransomware
- C. Backdoor
- D. Trojan

6. Recently, malware on a computer at the Monty Burns Casino destroyed several important files after it detected that Homer was no longer employed at the casino. Which of the following BEST identifies this malware?

- A. Logic bomb
- B. Rootkit
- C. Backdoor
- D. Spyware

7. Maggie was on the programming team that developed an application used by your Human Resources department. Personnel use this application to store and manage employee data. Maggie programmed in the ability to access this application with a username and password that only she knows to perform remote maintenance on the application if necessary. Which of the following does this describe?

- A. Virus
- B. Worm
- C. Backdoor
- D. Trojan

8. Homer complained of abnormal activity on his workstation. After investigating, an administrator discovered his workstation connects to systems outside the organization's internal network using uncommon ports. The administrator discovered the workstation is also running several hidden processes. Which of the following choices BEST describes this activity?

- A. Rootkit
- B. Backdoor
- C. Spam
- D. Trojan

9. Bart downloaded and installed the nmap security scanner from <https://passsecurityplus.com>. After completing the install, he noticed that his browser's home page and default search engine was changed. What is the MOST likely cause of the activity?

- A. PUP
- B. Fileless virus
- C. Worm
- D. Rootkit

10. Your SIEM system alerted on potential malicious activity from a system in your network. After investigating the alert, you determine it was generated after it detected suspicious activity generated through a PowerShell script. Additionally, you verified that the system is sending traffic to and from an unknown IP address in the Internet. Which of the following is the BEST description of this threat?

- A. Ransomware
- B. Fileless virus
- C. Command and control
- D. Rootkit

11. A man in a maintenance uniform walked up to your organization's receptionist desk. He said he was called by the CIO and asked to fix an issue with the phones and needed access to the wiring closet. The receptionist asked the man to show his building access badge, and then she verified that he was on the list of approved personnel to access this secure

area. What type of attack will the checks performed by the receptionist prevent?

- A. Tailgating
- B. Phishing
- C. Impersonation
- D. Whaling
- E. Prepending

12. An organization's security policy requires employees to place all discarded paper documents in containers for temporary storage. These papers are later burned in an incinerator. Which of the following attacks are these actions MOST likely trying to prevent?

- A. Shoulder surfing
- B. Tailgating
- C. Smishing
- D. Dumpster diving

13. Lisa is a database administrator and received a phone call from someone identifying himself as a technician working with a known hardware vendor. He said he's calling customers to inform them of a problem with database servers they've sold, but he said the problem only affects servers running a specific operating system version. He asks Lisa what operating system versions the company is running on their database servers. Which of the following choices is the BEST response from Lisa?

- A. Let the caller know what operating system and versions are running on the database servers to determine if any further action is needed.
- B. Thank the caller and end the call, report the call to her supervisor, and independently check the vendor for issues.
- C. Ask the caller for his phone number so that she can call him back after checking the servers.
- D. Contact law enforcement personnel because this is a pretexting attack.

14. Homer, the chief financial officer (CFO) of a bank, received an email from Lisa, the company's chief executive officer (CEO). Lisa states she is on vacation and lost her purse, containing all her cash and credit cards. She

asks Homer to transfer \$5,000 to her account. Which of the following best identifies this attack?

- A. Phishing
- B. Vishing
- C. Smishing
- D. Whaling

15. Homer has been looking for the newest version of a popular smartphone. However, he can't find it in stock anywhere. Today, he received an email advertising the smartphone. After clicking the link, his system was infected with malware. Which of the following principles is the email sender employing?

- A. Authority
- B. Intimidation
- C. Scarcity
- D. Trust

Chapter 6 Practice Question Answers

1. **B** is correct. This was most likely an advanced persistent threat (APT) because it was a sophisticated attack and originated from a foreign country. A hacktivist launches attacks to further a cause, but the scenario didn't mention any cause. Competitors might launch attacks, but they would typically focus on proprietary data rather than customer data. An insider would not launch attacks from a foreign country.
2. **B** is correct. A script kiddie will typically obtain a ready-made exploit rather than code it himself. An insider would cause damage from within the network or use inside knowledge when attacking. A competitor is unlikely to purchase a single item at a lower price but would be more interested in gaining proprietary data. Hacktivists launch attacks as part of an activist movement, not to get a better price on an item. An advanced persistent threat (APT) is typically a state actor sponsored by a nation-state and will use advanced tools to launch sophisticated attacks, rather than just lowering a price for an item.
3. **A** is correct. The caller is using the social engineering tactic of pretexting by setting up a scenario that has a better chance of getting someone to give him information. If he just asked for the operating system versions on the servers without a prepended scenario, his chance of success would be diminished. Tailgating is the practice of one person following closely behind another without showing credentials. A pharming attack attempts to manipulate the DNS name resolution process. Smishing is a form of phishing using text messages.
4. **B** is correct. A zero-day attack takes advantage of an undocumented exploit or an exploit that is unknown to the public. A buffer overflow attack sends unexpected data to a system to access system memory or cause it to crash. Although some buffer overflow attacks are unknown, others are known. If the server isn't kept up to date with patches, it can be attacked with a known buffer overflow attack. A man-in-the-browser attack is a type of proxy Trojan horse that takes advantage of vulnerabilities in web

browsers, not web servers. An integer overflow attack attempts to use or create a numeric value that is too big for an application to handle.

5. **B** is correct. Ransomware attempts to take control of user's system or data and then demands payment (ransom) to return control. Keyloggers capture a user's keystrokes and store them in a file. This file can be automatically sent to an attacker or manually retrieved depending on the keylogger. It's possible that Bart's computer was infected with a Trojan, which created a backdoor. However, not all Trojans or backdoor accounts demand payment as ransom.

6. **A** is correct. A logic bomb executes in response to an event. In this scenario, the logic bomb is delivering its payload when it detects that Homer is no longer employed at the company. A rootkit doesn't respond to an event. A backdoor provides another method of accessing a system, but it does not delete files. Spyware is software installed on user systems without their awareness or consent.

7. **C** is correct. A backdoor provides someone an alternative way of accessing a system or application, which is what Maggie created in this scenario. It might seem as though she's doing so with good intentions, but if attackers discover a backdoor, they can exploit it. A virus is malicious code that attaches itself to an application and executes when the application runs, not code that is purposely written into the application. A worm is self-replicating malware that travels throughout a network without the assistance of a host application or user interaction. A Trojan is software that looks like it has a beneficial purpose but includes a malicious component.

8. **A** is correct. A rootkit typically runs hidden processes and it commonly attempts to connect to computers via the Internet. The scenario doesn't address the initial infection. Although an attacker might have used a backdoor to access the user's computer and install the rootkit, backdoors don't run hidden processes. A Trojan is malware that looks like it's beneficial, but it is malicious. Spam is unwanted email and is unrelated to this question.

9. **A** is correct. A potentially unwanted program (PUP) is installed along with a desired program, and many PUPs hijack browsers by changing the home page and/or changing the default search engine. Because the user downloaded nmap from a site other than *nmap.org*, it is conceivable that the alternative site added PUPs to the nmap program. A fileless virus is a type of malicious software that runs in memory, often within a PowerShell script, instead of being a file that is written to disk. A worm is self-replicating malware that travels throughout a network without the assistance of a host application or user interaction. A rootkit is a program or group of programs that provide root-level access to a system.

10. **B** is correct. This describes a fileless virus, which commonly injects PowerShell commands into existing scripts. Security information and event management (SIEM) systems can be configured to send alerts when PowerShell commands are detected. Ransomware typically encrypts data and the attacker then demands payment as ransom, but there isn't any indication that a ransom is requested in this scenario. The fileless virus may have joined the computer to a botnet and the traffic to and from the unknown IP address may be a connection to a command and control server. However, there isn't enough information to make this conclusion. A rootkit is a program or group of programs that provide root-level access to a system and hides itself to evade detection.

11. **C** is correct. These checks are security controls that will help prevent impersonation, a social engineering attack. Tailgating is the practice of one person following closely behind another without showing credentials. Phishing is the practice of sending email to users with the purpose of tricking them into revealing personal information or clicking on a link. Whaling is a form of spear phishing that attempts to target high-level executives. By first saying that he was called by the chief information officer (CIO), he was using prepadding to add the impression of validity to his request.

12. **D** is correct. Dumpster diving is the practice of looking for documents in the trash dumpsters, but shredding or incinerating documents ensures dumpster divers cannot retrieve any paper documents. Shoulder surfers

attempt to view something on a monitor or other screen, not papers. Tailgating refers to entering a secure area by following someone else. Smishing is a form of phishing using text messages.

13. **B** is correct. This sounds like a social engineering attack where the caller is attempting to get information on the servers, so it's appropriate to end the call, report the call to a supervisor, and independently check the vendor for potential issues. It is not appropriate to give external personnel information on internal systems from a single phone call. It isn't necessary to ask for a phone number because you wouldn't call back and give information on the servers. While the caller is pretexting the request with a somewhat believable scenario, the caller has not committed a crime by asking questions, so it is not appropriate to contact law enforcement personnel.

14. **D** is correct. This is most likely a whaling attack because an executive (the CFO of the bank) is being targeted. While whaling is a type of phishing, whaling is more specific and a better answer than phishing. Vishing is a form of phishing that uses the phone, but this scenario used email. Smishing is a form of phishing that uses text messages.

15. **C** is correct. The attacker is using scarcity to entice the user to click the link. A user might realize that clicking on links from unknown sources is risky, but the temptation of getting a new smartphone might cause the user to ignore the risk. There isn't any indication that the email is from any specific authority. It isn't trying to intimidate the recipient, and there isn't any indication it is trying to build trust.

Chapter 7

Protecting Against Advanced Attacks

CompTIA Security+ objectives covered in this chapter:

1.1 Compare and contrast different types of social engineering techniques.

- Pharming

1.2 Given a scenario, analyze potential indicators to determine the type of attack.

- Adversarial artificial intelligence (AI) (Tainted training data for machine learning (ML), Security of machine learning algorithms)

1.3 Given a scenario, analyze potential indicators associated with application attacks.

- Cross-site scripting, Injections (Structured query language (SQL), Dynamic link library (DLL), Lightweight directory access protocol (LDAP), Extensible markup language (XML))
- Pointer/object dereference, Directory traversal, Buffer overflows, Race conditions
- (Time of check/time of use), Error handling, Improper input handling, Replay attack (Session replays), Integer overflow, Request forgeries (Server-side, Client-side), Resource exhaustion, Memory leak, Secure sockets layer (SSL) stripping, Driver manipulation (Shimming, Refactoring)

1.4 Given a scenario, analyze potential indicators associated with network attacks.

- On-path attack (previously known as man in the middle attack/man in the browser attack)
- Layer 2 attacks (Address resolution protocol (ARP) poisoning, Media access control (MAC) flooding, MAC cloning)
- Domain name system (DNS) (Domain hijacking, DNS poisoning, Universal resource locator (URL) redirection, Domain reputation)
- Distributed denial of service (DDoS) (Network, Application, Operational technology (OT))
- Malicious code or script execution (PowerShell, Python, Bash, Macros, Visual Basic for Applications (VBA))

1.6 Explain the security concerns associated with various types of vulnerabilities.

- Zero-day, Third-party risks (Outsourced code development)

2.1 Explain the importance of security concepts in an enterprise environment.

- DNS sinkhole

2.3 Summarize secure application development, deployment, and automation concepts.

- Environment (Development, Test, Staging, Production, Quality assurance (QA))
- Provisioning and deprovisioning, Integrity measurement
- Secure coding techniques (Normalization, Stored procedures, Obfuscation/camouflage, Code reuse/dead code, Server-side vs. client-side execution and validation, Memory management, Use of third-party libraries and software development kits (SDKs))
- Open Web Application Security Project (OWASP), Software diversity (Compiler, Binary)

- Automation/scripting (Automated courses of action, Continuous monitoring, Continuous validation, Continuous integration, Continuous delivery, Continuous deployment)
- Version control

3.2 Given a scenario, implement host or application security solutions.

- Application security (Input validations, Secure cookies, Hypertext Transfer Protocol (HTTP) headers, Code signing, Secure coding practices)
- Static code analysis, Manual code review, Dynamic code analysis, Fuzzing
- Sandboxing

4.1 Given a scenario, use the appropriate tool to assess organizational security.

- Shell and script environments (SSH, PowerShell, Python, OpenSSL)

4.2 Summarize the importance of policies, processes, and procedures for incident response.

- Attack frameworks (MITRE ATT&CK, The Diamond Model of Intrusion Analysis, Cyber Kill Chain)

4.3 Given an incident, utilize appropriate data sources to support an investigation.

- Log files (Web, DNS)

**

If there's one thing that's abundant in the IT world, it is attacks and attackers. Attackers lurk almost everywhere. If you have computer systems, you can't escape them. However, you can be proactive in identifying the different types of attacks and take steps to prevent them or at least prevent their effectiveness. This chapter covers some popular attack frameworks, along with a wide assortment of attacks from different sources.

Understanding popular attacks and attack frameworks provides some insight into how many attacks can be prevented.

Understanding Attack Frameworks

Cybersecurity professionals use several attack frameworks to identify tactics, techniques, and procedures (TTPs) used by attackers. The goal is to understand how attackers operate to decrease the impact of future attacks. The following sections describe some of these frameworks.

Cyber Kill Chain

Historically, ***kill chain*** has been a military concept related to an attack. It starts with the identification of a target, dispatching resources to the target, someone deciding to attack and giving the order, and it ends with the destruction of the target. Military personnel attempt to break an opponent's kill chain, such as by disrupting communication methods.

The cyber kill chain is similar. Scientists at Lockheed-Martin identified an intrusion kill chain with the following elements performed in order from start to finish:

1. **Reconnaissance.** This includes researching, identifying, and selecting targets.
2. **Weaponization.** Malware, such as a remote access Trojan (RAT), is embedded within a deliverable payload, such as an infected Microsoft Office document.
3. **Delivery.** The payload is transmitted to the target. Malware is often delivered as an attachment within a phishing email.
4. **Exploitation.** After the weapon is delivered, it activates and triggers the exploit. Exploits often target an application or operating system vulnerability.
5. **Installation.** The exploit will often install a remote access Trojan or a backdoor on the attacked system. This allows the attacker to maintain persistence inside the exploited environment.
6. **Command and Control (C2).** Infected systems often send out a beacon to an Internet-based server. This establishes the C2 channel, giving attackers full access to the infected system.
7. **Actions on Objectives.** At this point, attackers can begin taking action to achieve their ultimate goals. It could be installing ransomware or collecting, encrypting, and extracting data from the infected environment.

By understanding the intrusion kill chain, it becomes a little easier to identify ways to disrupt it.

Diamond Model of Intrusion Analysis

The Diamond Model of Intrusion Analysis focuses on understanding the attacker by analyzing four key components of every intrusion event. These four components are:

- **Adversary.** Adversaries can be identified by email addresses, handles used in online forums, memberships in advanced persistent threat groups, and other identifiers.
- **Capabilities.** Capabilities refer to the malware, exploits, and other hacker tools used in the intrusion.
- **Infrastructure.** The infrastructure refers to the Internet domain names, email addresses, and IP addresses used by the adversary.
- **Victim.** Victims can be identified by their names, email addresses, or network identifiers.

It starts with the idea that every intrusion event has an adversary that uses a capability across an infrastructure against a victim. These core components can be mapped to different phases of a cyber kill chain. The same adversary performs reconnaissance, delivers a weapon, exploits a vulnerability, and so on through the cyber kill chain. The capabilities, infrastructure, and victim may change within the kill chain, but the adversary remains the same. For example, the capability at the delivery stage may be malware delivered via a phishing email. The capability at the installation stage may be a malicious script that creates a backdoor.

By analyzing these components in multiple attacks, it reveals similarities. For example, an attack against BizzFad might have the same components as an attack against Monstromart. This knowledge gives cybersecurity professionals insight into possible future attacks, and they can disrupt the kill chain.

MITRE ATT&CK

MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a knowledge base of tactics and techniques used in real-world attacks. The knowledge base is presented in a matrix or table format. Tactics represent the adversary's tactical objective for performing an action or why the adversary is doing what he's doing. The techniques document how an adversary achieves a tactical objective or what the adversary gains by performing an action.

As an example, an adversary may retrieve a list of credentials on a system. He can then analyze these credentials to find an account he can use to move throughout the network.

MITRE ATT&CK is complementary to Lockheed's cyber kill chain. However, it isn't an ordered set of steps like the kill chain. Instead, it's a matrix of tactics and techniques used by attackers at different stages of an attack. The tactics in the matrix are initial access, execution, persistence, privilege escalation, defense evasion, credential access, discovery, lateral movement, collection and exfiltration, and command and control.

The matrix lists these tactics along the top. In each tactic column, it lists techniques used to achieve the tactic. As an example, the initial access tactic includes several techniques such as a spear phishing attachment, a spear phishing link, and a drive-by compromise.

MITRE is a not-for-profit organization that receives federal funding to perform research and development in cybersecurity. In addition to MITRE ATT&CK, they also maintain the Common Vulnerabilities and Exposures (CVE) system and the Common Weakness Enumeration (CWE) project. The CVE has become the standard for naming vulnerabilities and exposures and is used by Security Content Automation Protocol (SCAP) when naming vulnerabilities. The CWE project identifies software weaknesses and vulnerabilities in over 600 categories, and cybersecurity professionals have been creating automated tools to identify, fix, and prevent each of the issues listed in the CWE.

Remember this

Attack frameworks help cybersecurity professionals understand the tactics, techniques, and procedures used by attackers. The cyber kill chain includes

seven elements tracking an attack from reconnaissance to performing actions to achieve the attacker's objectives. The Diamond Model of Intrusion Analysis identifies four key components of every intrusion event. MITRE ATT&CK is a matrix of ten tactics and techniques attackers use to achieve each.

CISA Uses Frameworks to ID Attackers

The Cybersecurity and Infrastructure Security Agency (CISA) has frequently used MITRE ATT&CK and Pre-ATT&CK frameworks to identify attackers. As an example, in September 2020, they released a cybersecurity advisory titled “Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity.” The advisory shows how several attacks used the same TTPs used by the Chinese Ministry of State Security (MSS) actors.

As an example, they observed the attackers deploying China Chopper in exploited networks. China Chopper is an open source web shell hosted on a web server. It gives the attackers a backdoor into a system and includes two components. A command and control component configures the web server as a client that occasionally contacts a command and control server controlled by the attackers. A web shell component allows attackers to enter commands on the exploited server.

CISA documented the use of many more TTPs that are commonly used by China MSS actors. Combined, they were able to provide specific mitigation steps to prevent successful attacks.

Interestingly, many of these attacks started by using open source intelligence to identify known vulnerabilities. Next, they looked for soft targets that didn't patch their systems or take other corrective action to prevent attackers from exploiting these vulnerabilities. In short, networks with aggressive security practices avoided these attacks. Networks without aggressive security practices were soft targets.

Identifying Network Attacks

This section summarizes many common attacks launched against systems and networks, along with the indicators of these attacks. It's important to realize that effective countermeasures exist for all attacks listed in this book. However, attackers are actively working on beating the countermeasures. As they do, security professionals create additional countermeasures, and the attackers try to beat them. The battle continues daily.

The goal in this section is to become aware of many of the well-known attacks. By understanding these, you'll be better prepared to comprehend the improved attacks as they emerge and the enhanced countermeasures.

DoS Versus DDoS

A ***denial-of-service*** (DoS) attack is an attack from one attacker against one target. A ***distributed denial-of-service*** (DDoS) attack is an attack from two or more computers against a single target. The goal of both is ***resource exhaustion***, which overloads the system's resources and prevents legitimate users from accessing services on the target computer.

As an example, a web server responds to Hypertext Transfer Protocol (HTTP) requests to serve webpages. A DDoS attack can overload the web server by sending thousands of HTTP requests a second. These requests overload the resources leading to resource exhaustion. At some point, the attacked system is no longer able to keep up with the requests. The attacked computer typically slows down significantly, preventing legitimate users from viewing webpages. In extreme cases of resource exhaustion, the attacked computer might crash.

An indicator of a network-based DDoS attack is a sustained, abnormally high amount of network traffic on the network interface card (NIC) of the attacked computer. As the computer is trying to respond to this traffic, it can't respond as quickly to legitimate traffic. Another indicator of a DDoS attack is abnormally high usage of other system resources such as the processor or memory.

Some DDoS attacks focus on a specific application. As an example, web servers run web applications, and a DDoS attack can overload the web applications. One way is to overload the server with login attempts. They can come from thousands of locations around the world, overloading the server as it tries to verify the credentials of each login attempt.

Operational technology (OT) refers to the methods used to monitor and manage industrial control systems and manufacturing equipment. When these systems are accessible via the Internet, they are also susceptible to DDoS attacks. Any indication that these systems are behaving erratically should be investigated as a possible DDoS attack.

Remember this

A distributed denial-of-service (DDoS) attack is an attack from multiple computers against a single target. DDoS attacks typically include sustained, abnormally high network traffic and usage of memory and processor time

resulting in resource exhaustion. In addition to network attacks, DDOS attacks can also impact applications and operational technology (OT) systems such as industrial control systems.

SYN Flood Attacks

The SYN flood attack is a common DDoS attack used against servers on the Internet. They are easy for attackers to launch and can cause significant problems. The SYN flood attack disrupts the Transmission Control Protocol (TCP) handshake process and can prevent legitimate clients from connecting.

TCP sessions use a three-way handshake when establishing a session. Two systems usually start a TCP session by exchanging three packets in a TCP handshake. For example, when a client establishes a session with a server, it takes the following steps:

1. The client sends a SYN (synchronize) packet to the server.
2. The server responds with a SYN/ACK (synchronize/acknowledge) packet.
3. The client completes the handshake by sending an ACK (acknowledge) packet. After establishing the session, the two systems exchange data.

However, in a SYN flood attack, the attacker never completes the handshake by sending the ACK packet. Additionally, the attacker sends a barrage of SYN packets, leaving the server with multiple half-open connections. Figure 7.1 compares a normal TCP handshake with the start of a SYN flood attack. Attackers that control botnets can launch SYN flood attacks from hundreds or thousands of different systems in a DDoS attack.



Figure 7.1: TCP handshake and SYN flood attack

In some cases, these half-open connections can consume a server's resources while it is waiting for the third packet, and it can crash. More often, though, the server limits the number of these half-open connections. Once the limit is reached, the server won't accept any new connections, blocking connections from legitimate users. For example, Linux systems support an iptables command that can set a threshold for SYN packets, blocking SYN

packets after reaching the threshold. Although this prevents the SYN flood attack from crashing the system, it also denies service to legitimate clients.

Spoofing

Spoofing occurs when one person or entity impersonates or masquerades as someone or something else. Some common spoofing methods are related to an email address, an Internet Protocol (IP) address, and a media access control (MAC) address.

In email address spoofing, an attacker changes the sender address so it appears the email is coming from someone else. Sometimes they will also change the Reply-to address. Spam and phishing emails commonly forge these email addresses.

With IP spoofing, the attacker changes the source address so that it looks like the IP packet originated from a different source. This can allow an attacker to launch an attack from a single system, while it appears that the attack is coming from different IP addresses.

Host systems on a network have media access control (MAC) addresses assigned to the NIC. These are hard coded into the NIC. However, it's possible to use software methods to associate a different MAC address to the NIC in a MAC spoofing attack.

On-Path Attacks

An **on-path attack** (sometimes referred to as a **man-in-the-middle** attack) is a form of active interception or active eavesdropping. It uses a separate computer that accepts traffic from each party in a conversation and forwards the traffic between the two. The two computers are unaware of the attacking computer, but the attacker can interrupt the traffic at will, insert malicious code, or simply eavesdrop.

For example, imagine that Maggie and Bart are exchanging information with their two computers over a network. If Hacker Harry can launch an on-path attack from a third computer, he can intercept all traffic. Maggie and Bart still receive all the information, so they are unaware of the attack. However, Hacker Harry also receives all the information. Because the on-path computer can control the entire conversation, it is easy to insert malicious code and send it to the computers.

A sophisticated on-path attack can create multiple secure connections. Instead of Maggie and Bart having one secure connection between their computers, Maggie would have one secure connection with Hacker Harry, and Hacker Harry would have another secure connection with Bart. Hacker Harry receives the data in an encrypted format. His computer decrypts and stores it, and then encrypts it again before sending it on.

Because traffic goes through the on-path computer, it may cause a delay, especially if it is decrypting and encrypting the data again. This delay can be a strong indicator of an on-path attack. Additionally, the computer certificates used to create the secure sessions may not be issued by a trusted certificate authority. Users will receive certificate warnings and can only continue if they ignore the warnings.

Secure Shell (SSH) sessions are also susceptible to on-path attacks if administrators ignore warnings. When administrators connect to remote systems using SSH, the two systems establish cryptographic keys, and they use these keys in subsequent connections. These keys encrypt the SSH session and provide authentication.

Imagine Lisa established an SSH session with a remote system. SSH creates the two keys (one on her system and one on the remote system) and creates fingerprints to identify them. These fingerprints are expressed in 16

hexadecimal pairs, such as

1A:2B:3C:4E:5F:6A:7B:8C:9D:1E:2F:3A:4B:5C:6D:7E.

When Lisa connects to the server with SSH, it expects to see the same fingerprint. If it is different, it indicates that the administrator is connecting to a different computer. SSH will issue a warning similar to the following:

```
@@@@@@@  
@@@  
@
```

**WARNING: REMOTE HOST IDENTIFICATION HAS
CHANGED!**

```
@@@@@@@  
@@@  
@
```

**IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING
NASTY!**

Someone could be eavesdropping on you (man-in-the-middle attack)!

The fingerprint for the RSA key sent by the remote host is

1E:2F:3A:4B:5C:6D:7E:1A:2B:3C:4E:5F:6A:7B:8C:9D:

An on-path attack can also be what is known as a man-in-the-browser attack. This is a type of proxy Trojan horse that infects vulnerable web browsers. Successful on-path browser attacks can capture browser session data. This includes keyloggers to capture keystrokes, along with all data sent to and from the web browser. Some of these have included keystroke logging and form grabbing. Once the attackers collect logon information for a user's bank, they use it to log on and transfer money to offshore accounts.

Remember this

An on-path attack (also known as a man-in-the-middle or man-in-the browser attack) is a form of active eavesdropping. It captures data from two other computers in a session. When secure channels are used, the on-path system may use certificates that aren't issued by a CA and will generate certificate warnings. SSH gives a warning if previously established keys have changed.

Secure Sockets Layer Stripping

A ***Secure Sockets Layer (SSL) stripping*** attack changes a Hypertext Transfer Protocol Secure (HTTPS) connection to a Hypertext Transfer Protocol (HTTP) connection. HTTPS uses Transport Layer Security (TLS) instead of SSL in almost all instances, so you can also think of this as TLS stripping.

HTTPS sessions are encrypted, so data sent within a session is unreadable. However, the session is not encrypted until TLS sets up the session. If an attacker can intercept the beginning of the TLS negotiation, the attacker can redirect the user to an HTTP page instead of an HTTPS page.

The primary indication of an SSL stripping (or TLS stripping) attack is in the web browser itself. If the area to the left of the URL indicates “Not secure” or the URL includes HTTP instead of HTTPS, a SSL stripping attack may be active. Most browsers indicate the session is secure by showing a lock icon in the browser URL or HTTPS instead of HTTP.

Layer 2 Attacks

Some attacks attempt to exploit vulnerabilities at the Data Link layer (Layer 2) of the Open Systems Interconnection (OSI) model. Appendix D, “The OSI Model,” provides a refresher on the OSI model, in case you want to review the basics. Layer 2 transfers data frames between systems, and one of the primary protocols on this layer is the Address Resolution Protocol (ARP).

ARP Poisoning Attacks

ARP poisoning is an attack that misleads computers or switches about the actual MAC address of a system. The MAC address is the physical address, or hardware address, assigned to the NIC. ARP resolves the IP addresses of systems to their hardware address and stores the result in an area of memory known as the ARP cache.

TCP/IP uses the IP address to get a packet to a destination network. Once the packet arrives on the destination network, it uses the MAC address to get it to the correct host. ARP uses two primary messages:

- **ARP request.** The ARP request broadcasts the IP address and essentially asks, “Who has this IP address?”
- **ARP reply.** The computer with the IP address in the ARP request responds with its MAC address. The computer that sent the ARP request caches the MAC address for the IP. In many operating systems, all computers that hear the ARP reply also cache the MAC address.

A vulnerability with ARP is that it is very trusting. It will believe any ARP reply packet. Attackers can easily create ARP reply packets with spoofed or bogus MAC addresses and poison the ARP cache on systems in the network. Two possible attacks from ARP poisoning are an on-path attack and a DoS attack.

ARP On-Path Attacks

In an ARP on-path attack, an attacker can eavesdrop, redirect network traffic, and, in some cases, insert malicious code. Consider Figure 7.2. Normally, traffic from the user to the Internet will go through the switch

directly to the router, as shown in the top of Figure 7.2. However, after poisoning the ARP cache of the victim, traffic is redirected to the attacker.

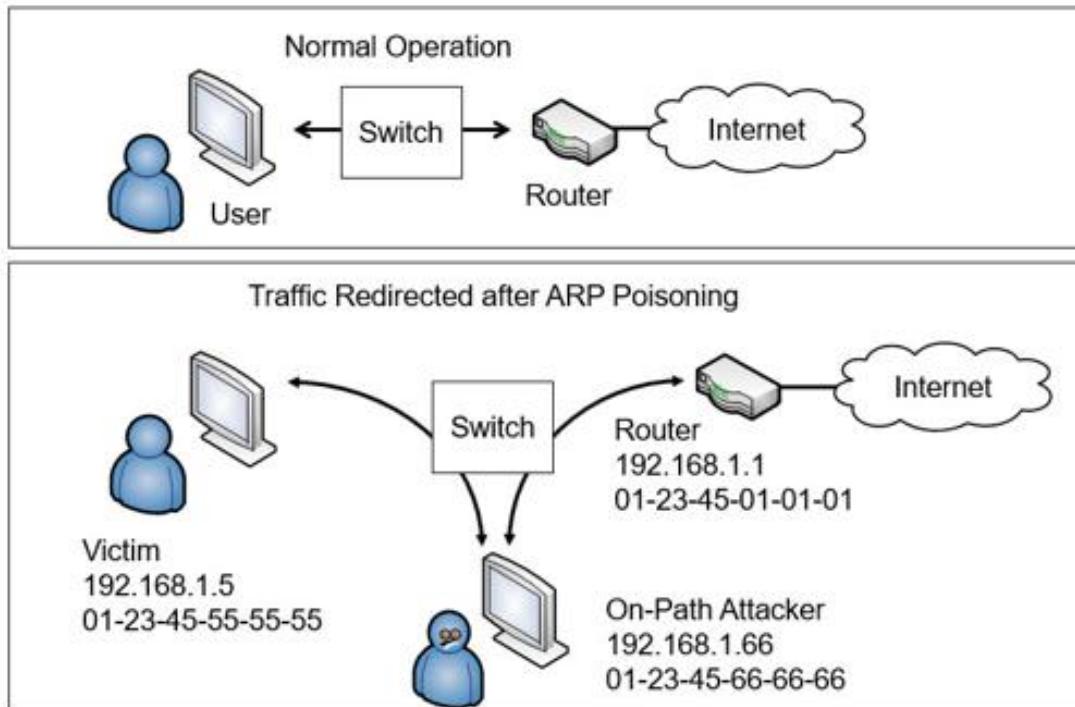


Figure 7.2: ARP poisoning used to redirect traffic

The victim's ARP cache should include this entry to send data to the router:

192.168.1.1, 01-23-45-01-01-01

However, after poisoning the ARP cache, it includes this entry:

192.168.1.1, 01-23-45-66-66-66

The victim now sends all traffic destined for the router to the attacker. The attacker captures the data for analysis later. It can also use another method, such as IP forwarding, to send the traffic to the router so that the victim is unaware of the attack.

Remember this

ARP poisoning attacks attempt to mislead systems about the actual MAC address of a system. ARP poisoning is sometimes used in on-path attacks.

ARP DoS Attacks

An attacker can also use ARP poisoning in a DoS attack. For example, an attacker can send an ARP reply with a bogus MAC address for the default gateway. The default gateway is the IP address of a router

connection that provides a path out of the network. If all the computers cache a bogus MAC address for the default gateway, none of them can reach it, and it stops all traffic out of the network.

MAC Flooding

MAC flooding is an attack against a switch that attempts to overload it with different MAC addresses associated with each physical port. You typically have only one device connected to any physical port. During normal operation, the switch's internal table stores the MAC address associated with this device and maps it to the port. An attacker sends a large amount of traffic with spoofed MAC addresses to the same port in a MAC flooding attack.

At some point in a MAC flooding attack, the switch runs out of memory to store all the MAC addresses and enters a fail-open state. Instead of working as a switch, it begins operating as a simple hub. Traffic sent to any port of the switch is now sent to all other switch ports. At this point, the attacker can connect a protocol analyzer to any port and collect all the traffic going through the switch.

Many switches include a flood guard to protect against MAC flood attacks. When enabled, the switch will limit the amount of memory used to store MAC addresses for each port. For example, switches can limit the number of entries for any port to 132 entries. This is much more than you need for normal operation. If the switch detects an attempt to store more than 132 entries, it raises an alert.

The flood guard typically sends a Simple Network Management Protocol (SNMP) trap or error message in response to the alert. Additionally, it can either disable the port or restrict updates for the port. By disabling the port, it effectively blocks all traffic through the port until an administrator intervenes. If it restricts updates, the switch will use currently logged entries for the port but ignore attempts to update it. All other ports will continue to operate normally.

MAC Cloning

MAC cloning is simply changing a system's MAC address to another MAC address. This is sometimes done to fool an Internet Service Provider (ISP) into thinking that a different networking device isn't different.

As an example, imagine you connect to the Internet through the WAN port of a router. The ISP knows the MAC address of this port on the router and associates it with your ISP account. If you replace this router, the ISP won't recognize it and won't give it an IP address, at least until you call and register the new MAC address to your account. However, if you use MAC cloning and set the new router's MAC address to be the same as the old router, the ISP will recognize it and give it an IP address.

DNS Attacks

Chapter 3, “Exploring Network Technologies and Tools,” covers Domain Name System (DNS) in much more depth, but as a reminder, DNS resolves hostnames to IP addresses. This eliminates the need for you and me to have to remember the IP addresses for websites. Instead, we simply type the name into the browser, and it connects. For example, if you type in *gcpagpremium.com* as the Uniform Resource Locator (URL) in your web browser, your system queries a DNS server for the IP address. DNS responds with the correct IP address and your system connects to the website using the IP address.

DNS also provides reverse lookups. In a reverse lookup, a client sends an IP address to a DNS server with a request to resolve it to a name. Some applications use this as a rudimentary security mechanism to detect spoofing. For example, an attacker may try to spoof the computer’s identity by using a different name during a session. However, the Transmission Control Protocol/Internet Protocol (TCP/IP) packets in the session include the masquerading system’s IP address, and a reverse lookup shows the system’s actual name. If the names are different, it shows suspicious activity. Reverse lookups are not 100 percent reliable because reverse lookup records are optional on DNS servers. However, they are useful when they’re available.

The following sections cover some common DNS attacks.

DNS Poisoning Attacks

A **DNS poisoning** attack attempts to modify or corrupt DNS data. For example, a successful DNS poisoning attack can modify the IP address associated with *google.com* and replace it with a malicious website’s IP address. If successful, and users attempt to go to Google, they will be sent to the malicious website instead. This is the primary indicator of a DNS poisoning attack—users enter the Uniform Resource Locator (URL) of one website but are taken to a different website.

There have been several successful DNS poisoning attacks over the years. Many current DNS servers use Domain Name System Security

Extensions (DNSSEC) to protect the DNS records and prevent DNS poisoning attacks. Chapter 3 covers DNSSEC in more depth.

Pharming Attack

A *pharming attack* is another type of attack that manipulates the DNS name resolution process. It either tries to corrupt the DNS server or the DNS client. Just as a DNS poisoning attack can redirect users to different websites, a successful pharming attack redirects a user to a different website.

Pharming attacks on the client computer have modified the hosts file used on Windows systems. This file is in the `C:\Windows\System32\drivers\etc\` folder and can include IP addresses along with hostname mappings. By default, it doesn't have anything other than comments on current Windows computers. However, a mapping might look like this:

```
127.0.0.1      localhost  
13.207.21.200 google.com
```

The first entry maps the name `localhost` to the loopback IP address of 127.0.0.1. The second entry maps the name `google.com` to the IP address of `bing.com` (13.207.21.200). If a user enters `google.com` into the browser's address bar, the browser will instead go to `bing.com`. Practical jokers might do this to a friend's computer, and it isn't malicious. However, if the IP address points to a malicious server, this might cause the system to download malware.

Remember this

A DNS poisoning attack attempts to modify or corrupt DNS data. Pharming is also an attack on DNS, and it manipulates the DNS name resolution process. A primary indicator of both attacks is that a user tries to go to one website but is taken to a different website.

URL Redirection

URL redirection is a common technique used to redirect traffic to a different page within a site, or even a different site completely. For example, I own the `darrilgibson.com` domain, and I sometimes use it to play

around with different web technologies such as Python. When I finish, I set up the site to redirect traffic to another one of my sites.

In some cases, attackers use URL redirection for malicious purposes. Imagine an attacker discovers a vulnerability with a website and gains access to the underlying files. He may be able to implement a URL redirection attack and send all traffic to an alternate malicious website. The indicator of a successful URL redirection attack is simple. You attempt to go to a website, and you're redirected to another website.

Domain Hijacking

In a ***domain hijacking*** attack, an attacker changes a domain name registration without permission from the owner. Attackers often do so with social engineering techniques to gain unauthorized access to the domain owner's email account.

As an example, imagine that Homer sets up a domain named *homersimpson.com*. He uses his Gmail account as the email address when he registers it, though he rarely checks his Gmail account anymore.

Attackers watch his Facebook page and notice that he often adds simple comments like "Doh!" Later, they try to log on to his Gmail account with a brute force attempt. They try the password of Doh!Doh! and get in. They then go to the domain name registrar and use the Forgot Password feature. It sends a link to Homer's Gmail account to reset the password. After resetting the password at the domain name registrar site, the attackers change the domain ownership. They also delete all the emails tracking what they did. Later, Homer notices his website is completely changed, and he no longer has access to it.

Remember this

In a domain hijacking attack, an attacker changes a domain name registration without permission from the owner.

Domain Reputation

Domain reputation helps ISPs determine the likelihood that an email is being sent by a legitimate organization or it is a malicious email. If a domain name has a low domain reputation, ISPs may decide to drop the emails instead of forwarding them.

If an organization finds that some ISPs are not forwarding their emails to internal recipients, the domain reputation should be checked. A search on domain reputation checker will give you multiple choices.

DNS Sinkhole

A **DNS sinkhole** is a DNS server that gives incorrect results for one or more domain names. If you enter a domain name into your web browser during normal operation, the web browser queries DNS for the website and takes you to the site. However, if the DNS server has a sinkhole for the domain name, you won't be able to reach the site.

Investigative authorities have used sinkholes to disrupt botnets and malware. Infected computers frequently check in with command and control servers, and the malware includes the domain names of these servers. Authorities reverse engineer the malware to discover these domain names, and then they coordinate with DNS owners to redirect traffic destined for these domain names. This effectively prevents infected computers from contacting the command and control servers for instructions.

DNS Log Files

DNS log files record DNS queries, such as each request to resolve a hostname to an IP address. These log entries would include the system that sent the request and the IP address returned for the hostname.

These log entries can be useful in identifying potentially malicious websites. As an example, imagine Bart spends a few hours browsing the Internet using his company computer. One of the websites downloaded malware onto his system, but he doesn't know which one and can't remember all of the sites he visited. By searching the DNS log files, administrators can identify all of the sites he visited based on his DNS queries.

Replay Attacks and Session Replays

A *replay attack* is one where an attacker replays data that was already part of a communication session. The attacker first captures data sent over a network between two systems. The attacker modifies the data and then tries to impersonate one of the clients in the original session and send the modified data in session replays. Replay attacks can occur on both wired and wireless networks.

As an example, Maggie and Bart may initiate a session with each other. During the communication, each client authenticates with the other using authentication credentials. Hacker Harry intercepts all the data, including the credentials, and later initiates a conversation with Maggie pretending to be Bart. When Maggie's system challenges Hacker Harry, his system sends Bart's credentials.

Many protocols use timestamps and sequence numbers to thwart replay attacks. For example, Kerberos, covered in Chapter 2, "Understanding Identity and Access Management," helps prevent replay attacks with timestamped tickets.

Remember this

Replay attacks capture data in a session to impersonate one of the parties in the session. Timestamps and sequence numbers are effective countermeasures against replay attacks.

Summarizing Secure Coding Concepts

Secure application development and deployment concepts are important for application developers to understand. Additionally, IT security managers who manage development projects should understand these concepts, too, even if they aren't writing the code.

Applications often provide an avenue for attackers to generate attacks unless developers create them using secure coding concepts. This section covers common application security techniques and concepts that developers use to create secure applications.

OWASP

The Open Web Application Security Project (OWASP) is a nonprofit foundation that is focused on improving the security of software. It includes hundreds of local chapters worldwide and tens of thousands of members. This online community has produced free documentation, tools, methodologies, and technologies used to improve web application security. Some of their publications and resources are mentioned within this secure coding section.

Code Reuse and Dead Code

Developers are encouraged to reuse code whenever possible instead of re-creating code that already exists. As an example, imagine a developer created code for a web application to create, modify, and authenticate users, and this code has been in use for a year. The code has gone through internal testing and has survived its usage within the application. Instead of creating brand-new code for a similar application, it's best to use this tested code.

Code reuse saves time and helps prevent the introduction of new bugs.

However, developers should ensure that they are using all the code that they copy into another application when reusing code. Imagine a developer created a module that has three purposes: create users, modify users, and authenticate users. While working on a new application, he realizes he needs a module that will authenticate users. If he simply copies the entire module into the new application, it creates dead code. ***Dead code*** is code that is never executed or used. In this example, the copied code to create and modify users isn't used in the new application, so it is dead code.

Logic errors can also create dead code. For example, imagine a function tests the value of a variable called `Donuts`. If `Donuts` has a value (such as 12), it squares it. If `Donuts` is null (a value of nothing), it returns an error and exits the function.

Next, the function checks to see if `Donuts` is null and if so, it prints a message in an error log. Do you see the problem? The code to print to an error log never executes. If `Donuts` is null, the previous check exited the function, so the second check never occurs. This logic error creates the dead code.

Third-Party Libraries and SDKs

Another popular method of code reuse is the use of ***third-party libraries*** and ***software development kits*** (SDKs). As an example, JavaScript is a rich, interpreted language used by many web applications. There are dozens of JavaScript libraries that include a wide assortment of prewritten and tested code that can be used for almost any purpose.

A JavaScript library is a file that includes functions and other code snippets. Developers add a line of code within a web application to reference a library available online. They can then call any of the library's functions from within their web application without needing to write the code from scratch.

Software development kits (SDKs) are like third-party libraries, but they are typically tied to a single vendor. For example, if you're creating an Android app, you can use the Android SDK. It includes software tools that will help you create apps for Android-based devices. An SDK includes a code library, but it has much more. It will include tools for debugging an app, application programming interfaces (APIs), documentation, and tutorials.

Input Validation

One of the most important security steps that developers should adopt is to include ***input validation***. Input validation is the practice of checking data for validity before using it. Input validation prevents an attacker from sending malicious code that an application will use by either sanitizing the input to remove malicious code or rejecting the input.

Improper input handling (or the lack of input validation) is one of the most common security issues with web-based applications. It allows many different types of attacks, such as buffer overflow attacks, Structured Query Language (SQL) injection, dynamic link library (DLL) injection, and cross-site scripting attacks. This chapter covers each of these attacks.

Consider a web form that includes a text box for a first name. You can logically expect a valid first name to have only letters and be no more than 25 letters. The developer uses input validation techniques to ensure that the user's name meets this validity check. If a user enters other data, such as numbers, semicolons, or HTML code, it fails the validity check. Instead of using the data, the application rejects it and provides an error to the user.

You've probably seen input validation checks and error-handling routines in use if you've ever filled out a form on a webpage. If you didn't fill out all the required text boxes, or if you entered invalid data into one or more of the boxes, the website didn't crash. Instead, it redisplayed the page and showed an error. Websites often use a red asterisk next to text boxes with missing or invalid data, along with a message about the error.

Some common checks performed by input validation include:

- **Verifying proper characters.** Some fields such as a zip code use only numbers, whereas other fields such as state names use only letters. Other fields are a hybrid. For example, a phone number uses only numbers and dashes. Developers can configure input validation code to check for specific character types and even verify that they are entered correctly. For example, a telephone number mask of `###-###-####` accepts only three numbers, a dash, three numbers, a dash, and four numbers.

- **Blocking HTML code.** Some malicious attacks embed HTML code within the input as part of an attack. Input validation code can detect HTML code, such as the < and > characters and not use it.
- **Preventing the use of certain characters.** Some attacks, such as SQL injection attacks, use specific characters such as the dash (-), apostrophe ('), and equal sign (=). Blocking these characters helps to prevent these attacks.
- **Implementing boundary or range checking.** These checks ensure that values are within expected boundaries or ranges. For example, if the maximum purchase for a product is three, a range check verifies the quantity is three or less. The validation check identifies data outside the range as invalid and the application does not use it.

Client-Side and Server-Side Input Validation

It's possible to perform input validation at the client and the server. Client-side execution indicates that the code runs on the client's system, such as a user's web browser. Server-side execution indicates that the code runs on the server, such as on a web server.

Client-side input validation is quicker but is vulnerable to attacks. Server-side input validation takes longer but is secure because it ensures the application doesn't receive invalid data. Many applications use both. Imagine Homer is using a web browser to purchase the newest version of Scrabbleships through the Duff website. Customers cannot purchase more than three at a time.

In client-side input validation, the validation code is included in the HTML page sent to Homer. If he enters a quantity of four or more, the HTML code gives him an error message and doesn't submit the page to the server until Homer enters the correct data.

Unfortunately, it's possible to bypass client-side validation techniques. Many web browsers allow users to disable JavaScript in the web browser, which bypasses client-side validation. It's also possible to use a web proxy to capture the client's data in the Hypertext Transfer Protocol (HTTP) POST command and modify it before forwarding to the server.

Server-side input validation checks the inputted values when it reaches the server. This ensures that the user hasn't bypassed the client-side checks.

Using both client-side and server-side validation provides speed and security. The client-side validation checks prevent roundtrips to the server until the user has entered the correct data. The server-side validation is a final check before the server uses the data.

Remember this

The lack of input validation is one of the most common security issues on web-based applications. Input validation verifies the validity of inputted data before using it, and server-side validation is more secure than client-side validation. Input validation protects against many attacks, such as buffer overflow, SQL injection, dynamic link library injection, and cross-site scripting attacks.

Other Input Validation Techniques

Other input validation techniques attempt to sanitize HTML code before sending it to a web browser. These methods are sometimes referred to as escaping the HTML code or encoding the HTML code. As a simple example, the greater than symbol (>) can be encoded with the ASCII replacement characters (>). Doing so and following specific guidelines related to not inserting untrusted data into webpages helps prevent many web application attacks.

Most languages include libraries that developers can use to sanitize the HTML code. For example, the OWASP Enterprise Security API (ESAPI) is a free, open source library for many programming languages. It includes a rich set of security-based tools, including many used for input validation.

Avoiding Race Conditions

When two or more modules of an application, or two or more applications, attempt to access a resource at the same time, it can cause a conflict known as a ***race condition***. Most application developers are aware of race conditions and include methods to avoid them when writing code. However, when new developers aren't aware of race conditions or ignore them, a race condition can cause significant problems.

As a simple example of a potential problem, imagine you are buying a plane ticket online and use a web application to pick your seat. You find a window seat and select it. However, at the same time you're selecting this window seat, someone else is, too. You both make the purchase simultaneously, and you both have tickets with the same seat number. You arrive after the other person, and he's unwilling to move, showing his ticket with the seat number. A flight attendant ultimately helps you find a seat. Unfortunately, it's between two burly gentlemen who have been on an all-cabbage diet for the last week. You probably wouldn't be too happy.

Online ticketing applications for planes, concerts, and other events avoid this type of race condition. In some cases, they lock the selection before offering it to a customer. In other cases, they double-check for a conflict later in the process. Most database applications have internal concurrency control processes to prevent two entities from modifying a value at the same time. However, inexperienced web application developers sometimes overlook race conditions.

Attackers can sometimes exploit a ***time of check to time of use*** (TOCTOU) race condition. This is sometimes called a state attack. The attacker tries to race the operating system to do something malicious with data after the operating system verifies access is allowed (time of check) but before the operating system performs a legitimate action at the time of use.

Think about the plane ticket analogy. Imagine the application first checked to see what seats are available and only offered available seats (time of check). The two people selected the same seats. A secure application would check again before reserving the seat (time of use). The

first person to complete the checkout process would reserve the seat, but the second person would learn the seat is no longer available.

As another example, imagine Homer tries to access a file. The operating system checks his permissions to verify he has access. If an attacker can act quickly enough, it is sometimes possible for the attacker to access the original file, modify it, or even replace it with a malicious file. This is sometimes possible when a symbolic link is used instead of a direct path.

Proper Error Handling

Error-handling and exception-handling routines ensure that an application can handle an error gracefully. They catch errors and provide user-friendly feedback to the user. When an application doesn't catch an error, it can cause the application to fail. In the worst-case scenario, improper error-handling techniques within an application can cause the operating system to crash. Using effective error- and exception-handling routines protects the integrity of the underlying operating system.

Improper error handling can often give attackers information about an application. When an application doesn't catch an error, it often provides debugging information that attackers can use against the application. In contrast, when an application catches the error, it can control what information it shows to the user. There are two important points about error reporting:

- **Errors to users should be general.** Detailed errors provide information that attackers can use against the system, so the errors should be general. Attackers can analyze the errors to determine details about the system. For example, if an application is unable to connect with a database, a detailed error can let the attacker know what type of database the system is using. This indirectly lets the attacker know what types of commands the system will accept. Also, detailed errors confuse most users.
- **Detailed information should be logged.** Detailed information on the errors typically includes debugging information. By logging this information, it makes it easier for developers to identify what caused the error and how to resolve it.

Remember this

Error and exception handling helps protect the operating system's integrity and controls the errors shown to users. Applications should show generic error messages to users but log detailed information.

Code Obfuscation and Camouflage

Developers often spend a lot of time developing code. If it is JavaScript, it is rather easy for other developers to just copy the code and use it. One way to slow this down is with an obfuscation or camouflage method.

Obfuscation attempts to make something unclear or difficult to understand, and code obfuscation (or code camouflage) attempts to make the code unreadable. It does things like rename variables, replace numbers with expressions, replace strings of characters with hexadecimal codes, and remove comments. For example, a meaningful variable of strFirstName might be renamed to 94mdiwl, and the number 11 might be changed to 0xF01B – 0x73 – 0xEF9D (which still results in the decimal number 11).

It's worth noting that most security experts reject security through obscurity as a reliable method of maintaining security. Similarly, code obfuscation might make the code difficult to understand by most people. However, it's still possible for someone with skills to dissect the code.

Software Diversity

Automated software diversity is sometimes used to mimic the use of multiple different core languages. Normally, a ***compiler*** converts code written in a programming language into a binary executable file. The compiler checks the program for errors and provides a report of items developers might like to check. Some commonly used compiled programming languages are C++, C#, and Java. Automated software diversity methods use a compiler that mimics the compilers of multiple languages.

In other words, a program written in C# and compiled with this multicompile would create a binary executable that includes all the functions and modules of the code as if it was written in C# and any number of other languages. Automated software diversity methods also add a level of randomness to the code allowing the same program to behave slightly differently on different systems but still achieving the same result.

The idea is that this automated diversity provides an added layer of protection. An attack that succeeds on one system would fail on another system using the same multicomplied program.

Outsourced Code Development

Not all organizations have developers in-house. They either need to hire developers or outsource code development. When outsourcing code development, organizations should address several specific security concerns. The following list identifies some vulnerabilities to consider:

- **Make sure the code works as expected.** At the top of the list is ensuring that the code works. While potential developers may claim they can write the code, an organization should thoroughly test it before accepting it.
- **Vulnerable code.** If the developers don't follow best practices for secure code, they could easily create code that is vulnerable to attack. Unfortunately, an organization might not discover poor coding practices until it is too late and the application has been exploited.

- **Malicious code.** Developers could insert malicious code such as backdoors or logic bombs. These may be difficult to detect using normal testing procedures.
- **Lack of updates.** Security vulnerabilities are common on code. However, developers are usually able to update the code to fix any vulnerabilities. If the contract for outsourced code development doesn't mention updates, it may be difficult to get updates.

Data Exposure

Most applications work with data, and it's essential to protect the data. Secure coding techniques take steps to protect data at rest, data in transit, and data in processing. If the data isn't protected, it can result in a data breach exposing the data to unauthorized entities. It's common to protect data at rest and in transit with encryption. If an application processes encrypted data, it typically decrypts it first. After processing it in memory, it encrypts it again and stores it. The application should also flush the memory buffers to ensure unauthorized entities can't access unencrypted remnants.

Chapter 10, "Understanding Cryptography and PKI," discusses data at rest, data in transit, and data in processing. It also discusses common encryption methods.

HTTP Headers

Systems send and receive HTTP messages between web servers and web clients. The client sends HTTP requests, and the server sends HTTP responses. These messages have multiple sections including the header. Even the header can have different groups. They are formatted as pairs separated by a colon (:). A general header group applies to the entire message. The request header group typically includes information about the browser, the language (such as English), and any encoding that the client browsers may accept. The entity header group gives information about the body of the message.

OWASP hosted the Secure Headers Project (<https://owasp.org/www-project-secure-headers/>), which includes detailed recommendations on what to include in response headers. Some headers that are commonly recommended as a best practice are:

- **HTTP Strict-Transport-Security.** This tells the browser to display the page only if it is sent as HTTP Secure (HTTPS). It includes the max-age=SECONDS and the includeSubDomains values.
- **Content-Security-Policy.** This defines multiple sources of acceptable content. It includes sources allowed for scripts, styles (CSS), images, plug-ins, and more.
- **X-Frame-Options.** This tells the browser if X-frames are allowed. X-Frames are rarely used anymore because they open up the page to vulnerabilities.

Secure Cookie

When a user visits a website, the website often creates a cookie and writes it to the user's system. This cookie is a small text file and can include anything that web developers choose to write. When the user returns to the website, the web application reads the cookie and uses it to enhance the user experience. Unfortunately, attackers can sometimes read the cookies and exploit various vulnerabilities.

A *secure cookie* is one that has a Secure attribute set. This ensures that the cookie is only transmitted over secure channels, such as HTTPS. This protects the confidentiality of the cookie's contents and prevents attackers from reading them. Many browsers (such as Chrome and Firefox) will not transfer cookies over HTTP even if the cookie has the Secure attribute set.

Code Signing

Chapter 10 describes certificates in-depth. They are used for various purposes, such as encryption and authenticating users and computers. They can also be used to authenticate and validate software code. As an example, developers can purchase a certificate and associate it with an application or code. This code signing process provides a digital signature for the code, and the certificate includes a hash of the code.

Code signing provides two benefits. First, the certificate identifies the author. Second, the hash verifies the code has not been modified. If malware changes the code, the hash no longer matches, alerting the user that the code has been modified.

Analyzing and Reviewing Code

Many organizations that create applications also employ testers to verify the quality of the code. Testers use a variety of different methods to put the code through its paces. Ideally, they will detect problems with the code before it goes live. Some common methods of testing code include:

- **Static code analysis.** *Static code analysis* examines the code without executing it. A developer performing a manual code review goes through the code line by line to discover vulnerabilities. It's also possible to use automated tools, which can analyze code and mark potential defects. Some tools work as the developer creates the code, like a spell checker in Microsoft Word, while other tools can examine the code once it is semifinalized.
- **Manual code review.** *Manual code review* is static code analysis where someone goes through the code line by line. It is done by someone other than the programmer who wrote the code, and the goal is to identify potential vulnerabilities.
- **Dynamic code analysis.** *Dynamic code analysis* checks the code as it is running. A common method is to use fuzzing. **Fuzzing** uses a computer program to send random data to an application. In some cases, the random data can crash the program or create unexpected results, indicating a vulnerability. The goal is to discover problems during a dynamic analysis so that they can be fixed before releasing the application.
- **Sandboxing.** *Sandboxing* is used to test applications within an isolated area specifically created for testing. The term comes from a sandbox in a playground. Children can play in the sandbox where they are relatively safe (and parents can easily keep their eyes on them). Similarly, application developers can test applications in a sandbox, knowing that any changes they make will not affect anything outside the sandbox. Virtual machines (VMs) are often used for sandboxing. For example, Java virtual machines include a sandbox to restrict untrusted applications.

Remember this

Static code analysis examines the code without running it. In a manual review, a developer goes through the code line by line, looking for vulnerabilities. Dynamic code analysis checks the code while it is running. Fuzzing techniques send random strings of data to applications looking for vulnerabilities.

Software Version Control

Software version control tracks the versions of software as it is updated, including who made the update and when. Many advanced software development tools include sophisticated version control systems. Developers check out the code to work on it and check it back into the system when they're done. The version control system can then document every single change made by the developer. Even better, this version control process typically allows developers to roll back changes to a previous version when necessary.

Effective version control processes also help eliminate unauthorized changes. If developers can make changes that aren't tracked, they can easily cause unintended problems.

Secure Development Environment

A secure development environment includes multiple stages and typically includes different systems used for each stage. As an example, imagine a software development team is creating an application that will be used to sell products via the Internet. The different stages used in this process are:

- **Development.** In the development stage, software developers use an isolated development environment to create the application. It's isolated from a production environment to ensure that any bugs don't impact other systems. This typically includes version and change controls to track the application development.
- **Test.** Testers put the application through its paces and attempt to discover any bugs or errors in the testing stage. The testing environment typically doesn't simulate a full production environment but instead includes enough hardware and software to test software modules.
- **Staging.** The staging environment simulates the production environment and is used for late-stage testing. It provides a complete but independent copy of the production environment. It attempts to discover any bugs that might adversely impact the live environment.
- **Production.** In the production stage, the application goes live as the final product. It includes everything needed to support the application and allow customers to use it. In this example, it would include the live web server, possibly a back-end database server, and Internet access.
- **Quality assurance (QA).** Quality assurance is an ongoing process used throughout the lifetime of the project from the development stage and after it is deployed. It helps ensure that an application maintains a high level of quality and meets the original requirements. Some organizations follow specific standards used for quality assurance, such as those published by

the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

Remember this

A secure development environment includes multiple stages. Stages are completed in separate nonproduction environments. Quality assurance methods are used in each of the stages.

Database Concepts

Several of the secure coding techniques and attacks apply directly to databases, so they’re organized in this section. SQL (pronounced as “sequel” or “es-que-el”) is a Structured Query Language used to communicate with databases. SQL statements read, insert, update, and delete data to and from a database. Many websites use SQL statements to interact with a database, providing users with dynamic content.

A database is a structured set of data. It typically includes multiple tables, and each table holds multiple columns and rows. As an example, consider Figure 7.3. It shows the database schema for a database intended to hold information about books and their authors. It includes two incorrect entries, which are described in the “Normalization” section.



Figure 7.3: Database schema

The Book table (on the left) identifies the column names for the table. Each of these columns has a name and identifies the data type or attribute type allowed in the column. For example, INT represents integer, VARCHAR represents a variable number of alphanumeric characters, TEXT is used for paragraphs, and DECIMAL can store monetary values.

The Author table holds information on authors, such as their names and addresses. The BookAuthor table creates a relationship between the Book table and the Author table. The Publisher column should not be there, but it helps describe normalization in the next section.

Figure 7.4 shows three rows of the Author table. It also shows the difference between columns and rows. Because the column identifies the data type, columns are sometimes referred to as attributes. Also, because each row represents a record, rows are sometimes called records or tuples.

Column
↓

AuthorID	FirstName	LastName	StreetAddress	City	State
1	Lisa	Simpson	742 Evergreen Terrace	Springfield	IDK
2	Moe	Szylak	1313 Walnut Street	Springfield	IDK
3	Ned	Flanders	744 Evergreen Terrace	Springfield	IDK

← Row
← Row
← Row

Figure 7.4: Database table

Individual elements within a database are called fields. For example, the field in the second row of the FirstName column is a field holding the value of Moe.

Normalization

Normalization of a database refers to organizing the tables and columns to reduce redundant data and improve overall database performance. Although there are several normal forms, the first three are the most important.

First Normal Form

A database is in first normal form (1NF) if it meets the following three criteria:

- **Each row within a table is unique and identified with a primary key.** For example, the Author table has a primary key of AuthorID, and each row within the table has a different and unique AuthorID, or a different primary key. Primary keys are shown in Figure 7.3 as small key icons. The primary key in the Book table is BookID. The BookAuthor table has a composite primary key using two values: Book_BookID and Author_AuthorID.
- **Related data is contained in a separate table.** The author information is contained in a different table. While it's possible to enter all of the author information into the Book table, this creates multiple problems. First, you'd have to create several extra columns such as FirstName, LastName, and you'd have to enter this data every time you added a book. Imagine Lisa Simpson writes five books. Each of her books in the book table would then need to include all of Lisa's information. However,

entering the same information multiple times increases the chance for errors. If she moves to a new address, you need to change the address five times.

- **None of the columns include repeating groups.** As an example, the Author table includes FirstName for the first name and LastName for the last name. If you combine these into a single column of name, it violates this rule. It also makes it more difficult to access only one part of the repeating group, such as the first name or the last name.

Second Normal Form

Second normal form (2NF) only applies to tables that have a composite primary key, where two or more columns make up the full primary key. The BookAuthor table has a composite key that includes the Book_BookID column and the Author_AuthorID column. A database is in 2NF if it meets the following criteria:

- It is in 1NF.
- Non-primary key attributes are completely dependent on the composite primary key. If any column is dependent on only one column of the composite key, it is not in 2NF.

The BookAuthor table shown in Figure 7.3 violates this with the Publisher column. A book has a unique publisher, so the publisher is related to the Book_BookID column. However, an author can publish books through multiple publishers, so the publisher value is not dependent on the Author_AuthorID column.

Notice that the Book table correctly has the Publisher column, so the easy fix to have this database in 2NF is to delete the Publisher column in the BookAuthor table.

Third Normal Form

Third normal form (3NF) helps eliminate unnecessary redundancies within a database. A database is in 3NF if it meets the following criteria:

- It is in 2NF. This implies it is also in 1NF.
- All columns that aren't primary keys are only dependent on the primary key. In other words, none of the columns in the table are dependent on non-primary key attributes.

The Book table violates the second rule of 3NF with the PublisherCity column. The city where the publisher is located is dependent on the publisher, not the book. Imagine this table had 100 book entries from the same publisher located in Virginia Beach. When entering the data, you'd need to repeatedly enter Virginia Beach for this publisher.

There are two ways to fix this. First, ask if the city is needed. If not, delete the column, and the database is now in 3NF. If the city is needed, you can create another table with publisher data. You would then relate the Publisher table with the Book table.

Remember this

Normalization is a process used to optimize databases. While several normal forms are available, a database is considered normalized when it conforms to the first three normal forms.

SQL Queries

One of the vulnerabilities related to databases is SQL injection attacks. The following sections identify how SQL queries work, how attackers launch a SQL injection attack, and how to protect against SQL injection attacks.

As a simple example of a website that uses SQL queries, think of *Amazon.com*. When you enter a search term and click Go (as shown in Figure 7.5), the web application creates a SQL query, sends it to a database server, and formats the results into a webpage that it sends back to you.



Figure 7.5: Webpage querying a database with SQL

In the example, I selected the Books category and entered Darril Gibson. The result shows a list of books authored by Darril Gibson available for sale on Amazon. The query sent to the database from the Amazon web application might look like this:

```
SELECT * FROM Books WHERE Author = 'Darril Gibson'
```

The * is a wildcard and returns all columns in a table. Notice that the query includes the search term entered into the webpage form (Darril Gibson) and encloses the search term in single quotes. If the website simply plugs the search term into the SELECT statement, surrounded by single

quotes, it will work, but it's also highly susceptible to SQL injection attacks.

SQL Injection Attacks

In a SQL injection attack, the attacker enters additional data into the webpage form to generate different SQL statements. SQL query languages use a semicolon (;) to indicate the SQL line's end and use two dashes (--) as an ignored comment. With this knowledge, the attacker could enter different information into the web form like this:

```
Darril Gibson'; SELECT * FROM Customers;--
```

If the web application plugged this string of data directly into the SELECT statement surrounded by the same single quotes, it would look like this:

```
SELECT * FROM Books WHERE Author = 'Darril Gibson';
SELECT * FROM Customers;
--'
```

The first line retrieves data from the database, just as before. However, the semicolon signals the end of the line, and the database will accept another command. The next line reads all the data in the Customers table, giving the attacker access to names, credit card data, and more. The last line comments out the second single quote to prevent a SQL error.

Suppose the application doesn't include error-handling routines. In that case, the errors provide details about the type of database the application is using, such as an Oracle, Microsoft SQL Server, or MySQL database. Different databases format SQL statements slightly differently, but once the attacker learns the database brand, it's a simple matter to format the SQL statements required by that brand. The attacker then follows with SQL statements to access the database. This may allow the attacker to read, modify, delete, and/or corrupt data.

This attack won't work against Amazon (please don't try it) because Amazon is using secure coding principles. I don't have access to its code, but I'd bet the developers are using input validation and SQL-based stored procedures (described in the next section).

Many SQL injection attacks use a phrase of **or '1' = '1'** to create a true condition. For example, if an online database allows you to search a

Customers table looking for a specific record, it might expect you to enter a name. If you entered **Homer Simpson**, it would create a query like this:

```
SELECT * FROM Customers WHERE name = 'Homer Simpson'
```

This query will retrieve a single record for Homer Simpson. However, if the attacker enters

' or '1'='1';-- instead of Homer Simpson, it will create a query like this:

```
SELECT * FROM Customers WHERE name = '' or '1'='1';--
```

Although this is a single SELECT statement, the or clause causes it to behave as two separate SELECT statements:

```
SELECT * FROM Customers WHERE name = ''
```

```
SELECT * FROM Customers WHERE '1'='1'
```

The first clause will likely not return any records because the table is unlikely to have any records with the name field empty. However, because the number 1 always equals the number 1, the WHERE clause in the second statement always equates to True. The SELECT statement will retrieve all records from the Customers table.

In many cases, a SQL injection attack starts by sending improperly formatted SQL statements to the system to generate errors. Proper error handling prevents the attacker from gaining information from these errors, though. Instead of showing the errors to the user, many websites simply present a generic error webpage that doesn't provide any details.

Protecting Against SQL Injection Attacks

As mentioned previously, input validation provides strong protection against SQL injection attacks. Before using the data entered into a web form, the web application verifies that the data is valid.

Additionally, database developers often use **stored procedures** with dynamic webpages. A stored procedure is a group of SQL statements that execute as a whole, similar to a mini-program. A parameterized stored procedure accepts data as an input called a parameter. Instead of copying the user's input directly into a SELECT statement, the input is passed to the stored procedure as a parameter. The stored procedure performs data validation, but it also handles the parameter (the inputted data) differently and prevents a SQL injection attack.

Consider the previous example searching for a book by an author where an attacker entered the following text: Darril Gibson'; SELECT *

From Customers;--. The web application passes this search string to a stored procedure. The stored procedure then uses the entire search string in a SELECT statement like this:

```
SELECT * From Books Where Author =“Darril Gibson”; SELECT * From Customers;-- ”
```

In this case, the user’s text is interpreted as harmless text rather than malicious SQL statements. It will look for books with an author name using all of this text: Darril Gibson’; SELECT * From Customers;--. Books don’t have author names with SELECT statements embedded in them, so the query comes back empty.

Depending on how well the database server is locked down (or not), SQL injection attacks may allow the attacker to access the structure of the database, all the data, and even modify data. In some cases, attackers have modified the price of products from several hundred dollars to just a few dollars, purchased several of them, and then returned the price to normal.

Remember this

Attackers use SQL injection attacks to pass queries to back-end databases through web servers. Many SQL injection attacks use the phrase ’ or ‘1’=‘1’ to trick the database server into providing information. Input validation techniques and stored procedures help prevent SQL injection attacks.

Provisioning and Deprovisioning

Provisioning and deprovisioning processes typically refer to user accounts. For example, when an employee starts working at an organization, administrators create the account and give it appropriate privileges. This way, the user can use the account to access various resources. Deprovisioning an account refers to removing access to these resources and can be as simple as disabling or deleting the account.

Within the context of secure application development and deployment concepts, these terms apply to an application. Provisioning an application refers to preparing and configuring the application to launch on different devices and to use different application services.

As an example, developers who create iOS apps (running on Apple devices) provision the apps based on the devices they'll run on. Apps can run on iPhones, iPads, and Macs. Additionally, these apps can use different services, such as an accelerometer and gyroscope to detect movement. The app needs to be properly provisioned with the appropriate code on the target device to use these services.

Deprovisioning an app refers to removing it from a device. For example, if a user decides to delete the app, the app should be able to remove itself and all data created by the app. Leaving remnants of the app consumes resources on the device.

Integrity Measurement

Within the context of software development, integrity measurement refers to the quality of the code. Code integrity measures the quality of code based on how extensively and effectively the code was tested throughout the development life cycle.

Without effective integrity measurements for the code, the initial release is often delayed. Testers will identify bugs and other issues in the staging environment forcing the development team to go back and fix issues that should have been identified and fixed early in the project.

Web Server Logs

Web server logs typically log activity on the server. These web server logs will show normal activity, such as HTTP requests from users and the server's responses. If your organization owns or controls the server, administrators will have access to the web server logs. However, administrators can't examine logs of servers owned by others. As an example, you can't access logs of Google servers.

These logs will also record abnormal traffic, such as any of the attacks described in this chapter on a web server. As an example, if you suspect that attackers are launching SQL injection attacks, you can search the logs for instances of the phrase '`' or '1'='1`'. Similarly, you can search the logs for indicators of other potential attacks.

Chapter 1, "Mastering Security Basics," introduces centralized logging methods such as security information and event management (SIEM) systems. Instead of analyzing logs manually, it's common to send log entries to a centralized logging system and configure it to send alerts after detecting suspicious traffic.

Using Scripting for Automation

It's common to use scripting techniques for automation. SIEM systems include a wide variety of scripts working behind the scenes to collect and analyze log entries. After detecting items of interest, they often trigger a script to respond to the entry based on preconfigured settings. For example, a script may send an email to a group of administrators in response to specific log entries.

Chapter 11, "Implementing Policies to Mitigate Risks," discusses Secure Orchestration, Automation, and Response (SOAR) tools. These respond to low-level security events using prewritten scripts. An effective SOAR platform can handle many simple administrative and cybersecurity tasks without taking up the administrator's time.

It's also possible to use automation to streamline application development. Some development operations models, such as DevOps, use several specific software development processes to automate code development. The following list summarizes the various processes. However, some implementations combine two processes into one. As an example, continuous integration frequently includes continuous validation.

- **Automated courses of action.** Automation is a core principle of the DevOps model. After developers do almost anything to the code, it will trigger an automated response. As an example, if a developer makes a change, the system will detect the change and verify it doesn't break any other part of the application.
- **Continuous monitoring.** The continuous monitoring process automatically monitors code changes to detect compliance issues and security threats. This detects issues at any stage of the project and allows developers to address them in real time.
- **Continuous validation.** The continuous validation stage revalidates code after every change. As a simple example, imagine code has a module that receives two numbers and returns the result. Code changes shouldn't break this module, but sometimes they do. By revalidating the code after every

change, it allows developers to see problems as soon as they occur.

- **Continuous integration.** Continuous integration occurs after continuous validation. It refers to the practice of merging code changes into a version control repository regularly. Team members may merge changes into the repository several times a day. It's common for continuous integration processes to include continuous validation, which validates all code changes as they are merged into the central repository.
- **Continuous delivery.** Continuous delivery refers to a process where code changes are released automatically to a testing or staging environment. After testing, someone (such as a lead developer) will decide when to release the code to the production environment.
- **Continuous deployment.** In a continuous deployment process, code changes are deployed automatically to the production environment. The code is still tested but without requiring manual approval. Note that the primary difference between continuous deployment and continuous delivery is that continuous deployment deploys the changes to a production environment. In contrast, continuous delivery only sends the changes to a testing or staging environment..

Identifying Malicious Code and Scripts

Software code and scripts are often useful to administrators, and they can simplify a lot of tasks. Unfortunately, criminals have learned how to write code and scripts, and they use these skills to launch sophisticated attacks. Potential indicators of most malicious code and scripts are similar to indicators of almost any type of malware. The following list shows some common indicators of malware infections:

- You can't update the system.
- Antivirus software is disabled.
- A system runs slower than normal.
- Internet traffic increases on its own.
- Programs appear to start on their own.
- A system randomly crashes or freezes.
- Pop-ups or security warnings begin to appear.
- Your browser home page or default search engine changes.
- A ransom demand appears along with the inability to access data or a system.

Unfortunately, a system may not show any malware infection indicators, at least not right away. As an example, ransomware typically doesn't launch as soon as it infects a system. Instead, it searches the computer and the network looking for data and other systems. After discovery, it will then encrypt the data and show the ransom demand message. Chapter 6, “Comparing Threats, Vulnerabilities, and Common Attacks,” covers malware in more depth.

The following items describe various code and scripting techniques. A primary indicator of attacks using a script is in logs. Centralized logging systems, such as a security information and event management (SIEM) system, can be configured to detect these scripts automatically. A SIEM system (described in Chapter 1) can then send alerts after detecting the scripts.

PowerShell

Windows PowerShell is a task-based command-line shell and scripting language that uses cmdlets. Just like the Microsoft command prompt, the PowerShell command prompt allows you to enter commands directly. Similarly, just as you can create and run batch files (.bat) composed of multiple commands, you can also create PowerShell script files (.ps1) composed of multiple PowerShell commands.

PowerShell has full access to the Microsoft Component Object Model (COM) and Windows Management Instrumentation (WMI), giving it quite a bit of power within Windows-based networks. New additions to PowerShell now allow administrators to query and manage Linux and macOS systems, too. As mentioned in Chapter 6, fileless malware often uses PowerShell because the attackers can run a script within memory instead of saving a malicious file to disk.

The best way to detect a PowerShell cmdlet is by viewing logs and looking for PowerShell cmdlets. PowerShell cmdlets use a verb and noun name pair as verb-noun. For example, the `Invoke-Command` cmdlet uses the verb *Invoke* to run a *Command* (the noun) on a computer.

Some common verbs used in PowerShell are: Get, Add, Test, Remove, New, Find, and Move. Some PowerShell common nouns are: Command, Service, Location, Process, Childitem, WmiObject, PSDrive. The **Get-Command** cmdlet will give you a list of all PowerShell commands.

Bash

Bash (short for Bourne-Again Shell) is the command language interpreter for Unix and Unix-like operating systems. Chapter 1 introduced the Linux terminal. When you run commands in the Linux terminal, you are using the bash interpreter. You can create a script file with several bash commands and invoke the script file, just as you can create a batch file and run all the commands within a batch file. However, when running a bash script file, you must prefix it with the **bash** or **sh** command or the full path as */bin/bash* or */bin/sh*.

As an example, if you have a script in the current directory named *mytest.sh*, you would run it with:

bash mytest.sh or **sh mytest.sh**

Users are sometimes required to enter the full path for bash or sh as follows:

bin/bash mytest.sh or **/bin/sh mytest.sh**

If logs show that **bash** or **sh** is being invoked to run scripts, it's worth investigating. It may be a potential indicator of an attack.

Remember this

PowerShell cmdlets use a verb-noun structure such as **Invoke-Command**. Bash scripts typically call either **/bin/bash** or **/bin/sh**. If logs show verb-noun cmdlets or calls to **bash** or **sh**, it may be a potential attack indicator.

Python

Python is an interpreted programming language that includes extensive libraries, which simplify many programming tasks. After installing Python on a computer, you can enter code in the Python shell and run it. You can also create Python files and launch them from the Python shell. Most Python script files end with .py. It's also possible to compile a Python script and compiled scripts end with .pyc. Some compiled scripts may end with .pyo or pyw, but these extensions are discouraged. A potential indicator of a system running Python scripts is any reference to .py* files.

Macros

A macro is a short instruction that will run a longer set of instructions. Macros are very useful at automating repetitive functions. As an example, I frequently type this paragraph when responding to queries:

When taking practice tests, it's important to understand why the correct answers are correct and why the incorrect answers are incorrect. This practice will help you answer the questions correctly on the live exam, no matter how CompTIA words them.

I've created a macro in Microsoft Word and assigned it to the key combination of CTRL+Q. Now when I press CTRL+Q, it types the paragraph for me.

If attackers can edit these macros, they can replace them with malicious steps. A potential indicator that an attacker has modified a macro is if the macro no longer works or works differently. Microsoft Office uses Visual Basic for Applications (VBA) when creating macros, but macros in other applications may use something different than VBA.

Visual Basic for Applications (VBA)

Microsoft created Visual Basic for Applications (VBA), which runs as an internal programming language within Microsoft applications, such as Microsoft Word. VBA is an event-driven tool, and functions created within VBA are started by initiating macros. The example used in the “Macros” section showed how the VBA macro was initiated by pressing CTRL+Q, and it then types the paragraph.

Macros (including VBA macros) are disabled by default in Microsoft Office applications because it is easy for attackers to create malicious macros and VBA code. It’s sometimes useful to enable VBA when using files created within a company. However, users can enable VBA and macros if prompted to do so after receiving a file. If a user complains of a system acting erratically after opening a file, it’s possible that the user inadvertently enabled VBA and macros on the system.

OpenSSL

OpenSSL is a software library used to implement SSL and TLS protocols. TLS has replaced SSL because of SSL vulnerabilities, so OpenSSL is primarily used with TLS, not SSL. It is accessible via the terminal in most Unix-like operating systems, such as Linux.

Chapter 10 mentions how administrators use OpenSSL to create key pairs before requesting a certificate. After creating the key pair, you can export the public key to a file and submit it to the certificate authority. You can also use OpenSSL to create certificate signing requests (CSRs).

SSH

Chapter 3 describes the use of the Secure Shell (SSH) protocol to connect with remote systems. You launch it from the Windows command prompt or the Linux terminal by entering the ssh command. Technically, it is a shell environment, which is probably why CompTIA lumped it together with PowerShell, Python, and OpenSSL. OpenSSH is a suite of tools that simplify the use of SSH. For example, Chapter 3 describes how to create a key pair with OpenSSH tools that administrators use for passwordless SSH logins.

Identifying Application Attacks

Many attacks target server applications such as those hosted on web servers. Web servers are highly susceptible to several types of attacks, such as buffer overflow attacks and SQL injection attacks, because they commonly accept data from users. Application attacks are successful because they exploit known vulnerabilities.

Zero-Day Attacks

A ***zero-day*** vulnerability is a weakness or bug that is unknown to trusted sources, such as antivirus and operating system vendors. A zero-day attack exploits an undocumented vulnerability. Many times, the vendor isn't aware of the issue. At some point, the vendor learns of the vulnerability and writes, tests, and releases a patch to eliminate it. However, until the vendor releases the patch, the vulnerability is still a zero-day vulnerability.

In most cases, a zero-day vulnerability is a new threat. However, there have been zero-day vulnerabilities that have existed for years. As an example, a bug existed in the virtual DOS machine (VDM) that shipped with every version of 32-bit Windows systems from 1993 to 2010. The bug allowed attackers to escalate their privileges to full system level, effectively allowing them to take over the system. Google researcher Tavis Ormandy stated that he reported the bug to Microsoft in mid-2009. At this point, Microsoft (the vendor) knew about the bug, but didn't release a work-around until January 2010 and a patch until February 2010. Because the bug wasn't known publicly until January 2010, it remained a zero-day vulnerability until then.

Both attackers and security experts are constantly looking for new threats, such as zero-day vulnerabilities. Attackers want to learn about them so that they can exploit them. Most security experts want to know about them to help ensure that vendors patch them before causing damage to users.

Because the vulnerability isn't known, the best indicator of a zero-day exploit is erratic, unexpected behavior on the attacked system.

Remember this

Zero-day exploits are undocumented and unknown to the public. The vendor might know about it but has not yet released a patch to address it. The best indicator of a zero-day attack is erratic or unexpected behavior on an attacked system.

Memory Vulnerabilities

Many application attacks take advantage of vulnerabilities in a system's memory or buffers. Because of this, developers need to use secure memory management techniques within their code. For example, poor memory management techniques can result in a memory leak or allow various overflow issues. The following sections describe some common memory issues related to applications.

Memory Leak

A ***memory leak*** is a bug in a computer application that causes the application to consume more and more memory the longer it runs. In extreme cases, the application can consume so much memory that the operating system crashes.

Memory leaks are typically caused by an application that reserves memory for short-term use but never releases it. For example, imagine a web application that collects user profile data to personalize users' browsing experiences. However, it collects this data every time a user accesses a webpage, and it never releases the memory used to store the data.

An initial indicator of a memory leak is a system running slower and slower until it is rebooted. It's possible to detect memory leaks by looking at the memory usage per application in operating system tools, such as the Windows Task Manager.

Buffer Overflows and Buffer Overflow Attacks

A ***buffer overflow*** occurs when an application receives more input, or different input, than it expects. The result is an error that exposes system memory that would otherwise be protected and inaccessible. Normally, an application will have access only to a specific area of memory, called a buffer. The buffer overflow allows access to memory locations beyond the application's buffer, enabling an attacker to write malicious code into this memory area.

For example, an application may expect to receive a string of 15 characters for a username. If it receives more than 15 characters and tries to store the data in a buffer, it can cause a buffer overflow and expose system

memory. The following HTTP GET command shows an example of sending a long string to the system to create a buffer overflow:

GET /index.php?

The buffer overflow exposes a vulnerability, but it doesn't necessarily cause damage by itself. However, once attackers discover the vulnerability, they exploit it and overwrite memory locations with their own code.

More often, the attacker's goal is to insert malicious code in a memory location that the system will execute. It's not easy for an attacker to know the exact memory location where the malicious code is stored, making it difficult to get the computer to execute it. However, an attacker can make educated guesses to get close.

A popular method that makes guessing easier is with no operation (NOP, pronounced as “no-op”) commands, written as a NOP slide or NOP sled. Many Intel processors use hexadecimal 90 (often written as x90) as a NOP command, so a string of x90 characters is a NOP sled. The attacker writes a long string of x90 instructions into memory, followed by malicious code. When a computer is executing code from memory and comes to a NOP, it just goes to the next memory location. With a long string of NOPs, the computer simply slides through all of them until it gets to the last one and then executes the code in the next instruction. If the attacker can get the computer to execute code from a memory location anywhere in the NOP slide, the system will execute the attacker’s malicious code. Log entries showing a string of NOPs or x90 characters are a strong indicator of an attempted buffer overflow.

The malicious code varies. In some instances, the attackers write code to spread a worm through the web server's network. In other cases, the code modifies the web application so that the web application tries to infect every user who visits the website with other malware. The attack possibilities are almost endless.

Although error-handling routines and input validation go a long way to prevent buffer overflows, they don't prevent them all. Attackers occasionally discover a bug allowing them to send a specific string of data to an application, causing a buffer overflow. When vendors discover buffer overflow vulnerabilities, they are usually quick to release a patch or hotfix.

From an administrator's perspective, the solution is easy: Keep the systems up to date with current patches.

Remember this

Buffer overflows occur when an application receives more data than it can handle or receives unexpected data that exposes system memory. Buffer overflow attacks often include NOP instructions (such as x90) followed by malicious code. When successful, the attack causes the system to execute the malicious code. Input validation helps prevent buffer overflow attacks.

Integer Overflow

An *integer overflow* occurs if an application receives a numeric value that is too big for the application to handle. The result is that the application gives inaccurate results. As an example, if an application reserves 8 bits to store a number, it can store any value between 0 and 255. If the application attempts to multiply two values, such as 95×59 , and store the result (5,605) in an 8-bit memory location, it causes an integer overflow.

It's a good practice to double-check the size of memory buffers to ensure they can handle any data generated by applications. It's also possible to use input validation techniques to prevent integer overflow issues. If the application doesn't have adequate error- and exception-handling routines, this might cause an integer overflow condition.

Pointer/Object Dereference

Programming languages commonly use pointers, which simply store a reference to a variable or object. Many programming languages refer to these pointers as references. In short, the pointer or reference is the memory address of the variable or object. Unfortunately, different programming languages use the term *dereference* differently.

As an example, Java refers to dereferencing a pointer or object as setting it to null. When set to null, it lets the garbage collection process free up the memory previously used by the pointer.

C++ and C# both support a dereference operator that allows the program to read and write to a pointer. In other words, if the variable has a value of 5, you can use dereferencing to retrieve the variable, perform an action to modify it (such as multiply it by 10), and then store the new value

(such as 50 in this example) in the original memory location. In these languages, a pointer or object dereference isn't a problem.

Almost any programming language allows you to set an object or variable to null. In general, a value of null indicates an unknown value. Null isn't nothing. It's not true or false, 1 or 0, or any other defined value. It is completely unknown. When setting an object to null in any language, it can cause problems if the program later tries to access the object.

In Java, the compiler will typically catch this and throw a `NullPointerException` error. This prevents the program from compiling. In other words, the `NullPointerException` error is an indicator of a pointer or object dereference error in Java.

In C++ and C#, setting an object to null and trying to use it at run time can cause a memory leak. It's relatively easy to identify the program causing a memory leak. However, it's not so easy to find the code within the application causing the memory leak.

The best way to avoid the problem within an application's code is by performing a simple check to verify a value is not null before using it. If an application is causing memory leaks, it's worthwhile to verify the application is performing null checks.

Other Injection Attacks

There are multiple types of injection attacks beyond SQL injection attacks discussed previously in this chapter. They include dynamic link library injection, Lightweight Directory Access Protocol injection, and Extensible Markup Language (XML) injection attacks.

Dynamic Link Library Injection

Applications commonly use a dynamic link library (DLL) or multiple DLLs. A DLL is a compiled set of code that an application can use without re-creating the code. As an example, most programming languages include math-based DLLs. Instead of writing the code to discover a number's square root, a developer can include the appropriate DLL and access the square root function within it.

DLL injection is an attack that injects a DLL into a system's memory and causes it to run. For example, imagine an attacker creates a DLL named *malware.dll* that includes several malicious functions. In a successful DLL injection attack, the attacker attaches this malicious DLL to a running process, allocates memory within the running process, connects the DLL within the allocated memory, and then executes functions within the DLL.

Lightweight Directory Access Protocol Injection

Lightweight Directory Access Protocol (LDAP) specifies the formats and methods used to query databases of objects such as users, computers, and other objects within a network. As an example, Microsoft Active Directory uses LDAP to access objects within a domain.

An LDAP injection attack is sometimes possible when a web application is used to query an LDAP-based database. As an example, imagine a help-desk technician needs to access Homer's account to modify it. The technician enters Homer's username into the application, and the application crafts an LDAP query to retrieve Homer's account information.

However, imagine the help-desk technician (or someone else) uses the application to enter more than just Homer's username. In that case, it may be possible to trick the application into crafting a longer LDAP query and accessing much more than just the user's information.

The best way to prevent this is by validating the input before using it, as discussed in the previous “Input Validation” section.

Extensible Markup Language Injection

Extensible Markup Language (XML) is a markup language commonly used to transfer data. It is extensible, meaning that it supports the use of any user-defined tags to describe data. Many online applications use XML to transfer data.

As an example, imagine an online web application is used to create and transfer user information. A user would be prompted to enter a username and an email address. The XML data may look like this:

```
<user>
    <username>Homer</username>
    <email>homer@simpson.com</email>
</user>
```

However, imagine the user entered the following data for the email address:

```
homer@simpson.com<user><username>Attacker</username>
<email>attacker@gcgacert.com</email></user>
```

If input validation is not used, this added data will create a second user account. In some instances, the XML application receiving the data will create the second account (Attacker in this example) but ignore the first account.

A primary indicator of XML injection is the creation of unwanted accounts, but it may take detailed logging and auditing to discover this. The best thing to do is to prevent XML injection with strong input validation.

Directory Traversal

Directory traversal is a specific type of injection attack that attempts to access a file by including the full directory path or traversing the directory structure on a computer.

For example, in Unix systems, the `passwd` file includes user logon information, and it is stored in the `/etc` directory with a full directory path of `/etc/passwd`. Attackers can use commands including the path to the file (such as `../../etc/passwd` or `/etc/passwd`) to read it. Similarly, they could use a remove directory command (such as **`rm -rf`**) to delete a directory, including all files and subdirectories. Input validation can prevent these types of attacks.

Cross-Site Scripting

Cross-site scripting (XSS) is a web application vulnerability that allows attackers to inject scripts into webpages. The CWE team has included XSS in their annual list of the top 25 Most Dangerous Software Weaknesses for several years. It is number 1 on their 2020 list. More specifically, they identify the weakness as “improper neutralization of input during webpage generation (cross-site scripting)” because this allows cross-site scripting.

The XSS attack starts by entering untrusted data into a web application. This generally occurs in one of two ways:

- **Reflected XSS or non-persistent.** This starts by an attacker crafting a malicious email and then encouraging a user to click it. The malicious URL is often placed within a phishing email, but it could also be placed on a public website, such as a link within a comment. When the user clicks the malicious URL, it sends an HTTP request to a server. This request includes malicious code, and the server sends it back to the user in the HTTP response.
- **Stored XSS or persistent.** Instead of the user sending the malicious code to the server, it is stored in a database or other location trusted by the web application. The web application can retrieve the malicious code later, such as when an administrator logs on to the website.

The primary protection against XSS attacks is at the web application with sophisticated input validation techniques. Developers should avoid any methods that allow the webpage to display untrusted data. Additionally, OWASP strongly recommends the use of a security encoding library. When implemented, an encoding library will sanitize HTML code and prevent XSS attacks. OWASP includes more than 10 rules that developers can follow to prevent XSS attacks.

Cross-Site Request Forgery

Cross-site request forgery (XSRF or CSRF) is an attack where an attacker tricks a user into performing an action on a website. The attacker creates a specially crafted HTML link, and the user performs the action without realizing it.

As an innocent example of how HTML links create action, consider this HTML link: <https://www.google.com/search?q=Success>. If users click this link, it works just as if the user browsed to Google and entered Success as a search term. The `?q=Success` part of the query causes the action.

Many websites use the same type of HTML queries to perform actions. For example, imagine a website that supports user profiles. If users wanted to change profile information, they could log on to the site, make the change, and click a button. The website may use a link like this to perform the action:

```
https://getcertifiedgetahead.com/edit?  
action=set&key=email&value=you%40home.com
```

Attackers use this knowledge to create a malicious link. For example, the following link could change the email address in the user profile, redirecting the user's email to the attacker:

```
https://getcertifiedgetahead.com/edit?  
action=set&key=email&value=hacker%40hackersrs.com
```

Although this shows one possibility, there are many more. If a website supports any action via an HTML link, an attack is possible. This includes making purchases, changing passwords, transferring money, and much more.

Websites typically won't allow these actions without users first logging on. However, if users have logged on before, authentication information is stored on their system either in a cookie or in the web browser's cache. Some websites automatically use this information to log users on as soon as they visit. In some cases, the XSRF attack allows the attacker to access the user's password.

Users should be educated on the risks related to links from sources they don't recognize. Phishing emails (covered in Chapter 6) often include

malicious links that look innocent enough to users but can cause significant harm. If users don't click the link, they don't launch the XSRF attack.

However, just as with cross-site scripting, the primary burden of protection from XSRF falls on the website developers. Developers need to be aware of XSRF attacks and the different methods used to protect against them. One method is to use a Completely Automated Public Turing Test to Tell Computers and Humans apart (CAPTCHA). This forces a user to interact with the site and prevents an automated action by a malicious link. Another method is to use dual authentication and force the user to manually enter credentials prior to performing actions.

Many programming languages support XSRF tokens. For example, Python and Django, two popular web development languages, require the use of an XSRF token in any page that includes a form, though these languages call them CSRF tokens. This token is a large random number generated each time the form is displayed. When a user submits the form, the webpage includes the token along with other form data. The web application then verifies that the token in the HTML request is the same as the token included in the web form.

The HTML request might look something like this:
getcertifiedgetahead.com/edit?
action=set&key=email&value=you@home.com&token=1357924

The token is typically much longer. If the website receives a query with an incorrect token, it typically raises a 403 Forbidden error. Attackers can't guess the token, so they can't craft malicious links that will work against the site.

Remember this

Cross-site scripting (XSS) attacks allow attackers to capture user information such as cookies. Input validation techniques at the server help prevent XSS attacks. Cross-site request forgery attacks often include a question mark to modify the URL.

Server-Side Request Forgeries

Server-Side Request Forgeries (SSRF) exploit how a server processes external information. As an example, some web applications read data from an external URL and use it when creating the webpage. If an attacker can modify the external URL, he can potentially inject malicious code into the webpage. Other external data sources include API data, databases, and files.

Successful SSRF attacks have allowed attackers to exfiltrate data. For example, the Capital One data breach in 2019 was reportedly a result of attackers exploiting an SSRF vulnerability. This attack exposed personal information of about 106 million people.

Client-Side Request Forgeries

Client-Side Request Forgeries occur if an attacker can inject code into the client-side webpage after the server has crafted it and sent it to the user. The most common way to do this is using cookies. If an attacker can modify existing cookies that the web application expects to read on the client, it's possible to inject malicious code in these cookies, which will then be placed in the webpage on the client-side.

Remember this

Cross-site request forgery (XSRF) scripting causes users to perform actions on websites, such as making purchases, without their knowledge. In some cases, it allows an attacker to steal cookies and harvest passwords.

Driver Manipulation

Operating systems use drivers to interact with hardware devices or software components. For example, when you print a page using Microsoft Word, Word accesses the appropriate print driver via the Windows operating system. Similarly, if you access encrypted data on your system, the operating system typically accesses a software driver to decrypt the data so that you can view it.

Occasionally, an application needs to support an older driver. For example, Windows 10 needed to be compatible with drivers used in Windows 8, but all the drivers weren't compatible at first. ***Shimming*** provides the solution that makes it appear that the older drivers are compatible.

A driver shim is additional code that can be run instead of the original driver. When an application attempts to call an older driver, the operating system intercepts the call and redirects it to run the shim code instead. ***Refactoring*** code is the process of rewriting the code's internal processing without changing its external behavior. It is usually done to correct problems related to software design.

Developers have a choice when a driver is no longer compatible. They can write a shim to provide compatibility or completely rewrite the driver to refactor the relevant code. If the code is clunky, it's appropriate to rewrite the driver.

Attackers with strong programming skills can use their knowledge to manipulate drivers by creating shims or rewriting the internal code. If the attackers can fool the operating system into using a manipulated driver, they can cause it to run malicious code contained within the manipulated driver.

However, when attackers manipulate a driver for malicious purposes, it often causes unforeseen results. These typically show up as intermittent problems with the device or software component that the driver services.

Artificial Intelligence and Machine Learning

Artificial intelligence (AI) is intelligence that machines can demonstrate. In contrast, humans and animals display natural intelligence.

Machine learning (ML) and AI aren't the same. Machine learning refers to technologies that help computer systems improve with experience. Machine learning is a part of AI, but AI is much broader. AI typically starts with basic machine learning techniques and expands itself by applying this knowledge to learn more and act on the new knowledge.

AI systems often start with algorithms that represent a set of knowledge and rules. They then repeat scenarios to learn information beyond the basics and apply that new knowledge. From a basic standpoint, they do the same things that many successful people do:

- Learn what works and keep doing it.
- Learn what doesn't work and stop.
- Try new things.

As an example, DeepMind Technologies developed AlphaGo, a computer program that plays the game of Go. Google bought it and later created newer versions called AlphaGo Master and AlphaGo Zero.

AlphaGo Zero was completely self-taught and learned many games. It started with a rule book that explained how the pieces move, which moves are legal for every piece, and what a win looks like (such as a checkmate in chess).

DeepMind also created MuZero, which can learn games without being taught the rules. MuZero's starting program doesn't know anything about the game, but an external program lets it know if it attempts an illegal move. By playing itself repeatedly, it creates game data learning the rules. It continues to play against itself and eventually moves into a training mode to learn strategies needed to win against other opponents.

AI and ML in Cybersecurity

Cybersecurity technologies can use ML and AI methods, too. By watching traffic, an AI program can identify patterns, detect abnormalities, and take actions to block malicious traffic. Chapter 4, “Securing Your Network,” discusses network-based intrusion detection systems (NIDSs)

and network-based intrusion prevention systems (NIPSSs). Some use heuristic or behavior-based methods to detect anomalies. An AI program can first watch network traffic to determine what is normal and document normal activity in a baseline. Later, it can compare network traffic to the baseline to identify anomalies.

Chapter 11 discusses Secure Orchestration, Automation, and Response (SOAR). SOAR starts with knowledge about well-known attacks, and when it detects a well-known attack, it takes steps to mitigate it. Administrators don't need to act on the alerts freeing them up to do other tasks. The following list gives some examples of AI and ML in action:

- Google uses machine learning to block as many as 100 million spam emails daily.
- IBM's Watson uses machine learning to detect cyber threats as they're happening.
- The Balbix platform uses AI-powered risk predictions to protect networks.

Adversarial Artificial Intelligence

Adversarial AI attempts to fool AI models by supplying it with deceptive input. When successful, it can cause an error or malfunction in the AI model. As a simple example, imagine MuZero playing a game of checkers. Normally, when a piece reaches the other end of the board, it becomes a king with the ability to move forward or backward. However, imagine MuZero is tricked into thinking that this piece is randomly promoted to a king or randomly captured and removed from the board. It wouldn't be able to determine a consistent rule and wouldn't be able to create winning strategies.

Some real-world examples show how manipulating images fool AI and ML systems:

- By placing some stickers on a Stop sign, some AI systems interpreted it as a Speed Limit 45 sign. This can cause some serious problems for self-driving cars.
- After overlaying a picture of a sloth with a picture of a race car that isn't visible to the human eye, AI systems identified it as a race car.

- After overlaying a picture of a panda with pixel noise of a gibbon, AI systems identified the panda as a gibbon.

These examples prove it's possible to feed AI and ML systems with adversarial data to fool them. If generic AI and ML systems can be fooled, you can bet that dedicated attackers will find ways to fool cybersecurity AI and ML systems. It's just a matter of time.

Tainted Data for Machine Learning

It's possible to use tainted data for machine learning to cause AI and ML systems to give inconsistent results. As an example, a simulated soccer game includes a goalie protecting the net and a kicker trying to score. After training for a while, both players become experts. An expert playing against a goalie with less training will have a high percentage of scores. However, the kicker trained against a goalie trying to protect the net. What if the goalie starts to behave unpredictably? Researchers at the University of California, Berkeley, programmed the goalie to lay down and wiggle its legs. This confused the kicker so much that it did a little sideways dance, waving an arm, and fell over.

These researchers tried unexpected behavior with other games and found that it fooled the other games, too. They added a pixel into the display, and the AI player became so confused, it consistently lost.

A potential indicator of tainted data being used to confuse an AI or ML system is sudden unexpected activity. If a behavior-based NIPS previously gave at least one false positive every day but hasn't raised any alerts for a few days, it could indicate an attack on the NIPS.

Security of Machine Learning Algorithms

Machine learning systems use algorithms to learn the environment. However, if an attacker knew these algorithms, it would be easier for him to create attacks that trick the ML system. Because of this, it's important to treat these algorithms as proprietary data to prevent unauthorized disclosure.

Chapter 7 Exam Topic Review

When preparing for the exam, make sure you understand the key concepts covered in this chapter.

Understanding Attack Frameworks

- Attack frameworks help cybersecurity professionals understand the tactics, techniques, and procedures (TTPs) used by attackers.
- Scientists at Lockheed-Martin identified seven elements in the cyber kill chain. It includes seven elements tracking an attack in order from start to finish.
- The Diamond Model of Intrusion Analysis identifies four key components of every intrusion event. These events can be mapped to some cyber kill chain elements to identify common TTPs used by attackers.
- MITRE ATT&CK is a matrix of tactics that attackers use. Each tactic has a column listing known techniques used to achieve the tactics.

Identifying Network Attacks

- DDoS attacks are DoS attacks from multiple computers. DDoS attacks typically include sustained, abnormally high network traffic, high processor usage, or high memory usage resulting in resource exhaustion.
- On-path attacks (also known as man-in-the-middle attacks) are a form of interception or active eavesdropping. Sophisticated on-path attacks establish secure channels and users may see certificate warnings indicating an on-path attack. SSH will give users a warning if it detects a man-in-the-middle attack.
- Secure Sockets Layer (SSL) stripping is a man-in-the-middle attack that attempts to convert encrypted HTTPS sessions into unencrypted HTTP sessions.
- ARP poisoning attacks attempt to mislead computers or switches about the actual MAC address of a system. They can

- be used to launch on-path attacks.
- A MAC flooding attack overloads a switch causing it to act as a hub.
- DNS poisoning attacks corrupt or modify DNS data and can redirect users to malicious sites.
- A pharming attack attempts to manipulate the DNS name resolution process.
- URL redirection causes a web browser to go to a different URL when a user visits a website.
- Domain hijacking attacks allow an attacker to change a domain name registration without permission from the owner. Owners learn of the hijack after they've lost access to the site.
- Replay attacks capture data in a session. After manipulating the capture, they send it back on the network as a session replay. Timestamps and sequence numbers thwart replay attacks.

Summarizing Secure Coding Concepts

- Code reuse refers to reusing code instead of re-creating code that already exists. It saves time and helps prevent the introduction of new bugs.
- Third-party libraries and software development kits include prewritten and tested code.
- A common coding error in web-based applications is the lack of input validation. Input validation checks the data before passing it to the application and prevents many types of attacks, including buffer overflow, SQL injection, command injection, and cross-site scripting attacks.
- Server-side input validation is the most secure. Attackers can bypass client-side input validation but not server-side input validation. It is common to use both.
- Race conditions allow two processes to access the same data at the same time, causing inconsistent results. Problems can be avoided by locking data before accessing it.
- Error-handling routines within applications can prevent application failures and protect the integrity of the operating

systems. Error messages shown to users should be generic, but the application should log detailed information on the error.

- Compiled code has been optimized by an application and converted into an executable file. Runtime code is code that is evaluated, interpreted, and executed when the code is run.
- Code signing uses a digital signature within a certificate to authenticate and validate software code.
- Code quality and testing techniques include static code analysis, dynamic analysis (such as fuzzing), stress testing, sandboxing, and model verification.
- SQL injection attacks provide information about a database and can allow an attacker to read and modify data within a database. They commonly use the phrase ' or '1'='1' to trick the database server into providing information. Input validation and stored procedures provide the best protection against SQL injection attacks.
- The DevOps model includes several processes to use when developing code. These include automated courses of action, continuous monitoring, continuous validation, continuous integration, continuous delivery, and continuous deployment.

Identifying Malicious Code and Scripts

- Attackers commonly use legitimate script languages to create malicious code. You should be able to recognize potential indicators of various scripts.
- PowerShell cmdlets use a verb-noun structure such as Invoke-Command or Get-Command. Seeing PowerShell cmdlets in logs may indicate potential attacks.
- Bash scripts call either **/bin/bash** or **/bin/sh**. If logs show calls to bash or sh, it may be a potential attack indicator.
- Python is an interpreted programming language, and Python files end in .py. Any log entry showing Python files running on a system may indicate a problem.
- A macro is typically a key combination that will run a set of instructions, and Visual Basic for Applications (VBA) runs macros within Microsoft Office applications. Macros and VBA

are disabled by default. If macros or VBA are enabled, it can be a potential indicator of a problem.

Identifying Application Attacks

- Attackers exploiting unknown or undocumented vulnerabilities are taking advantage of zero-day vulnerabilities. The vulnerability is no longer a zero-day vulnerability after the vendor releases a patch to fix it.
- Buffer overflows occur when an application receives more data, or unexpected data, than it can handle and exposes access to system memory. Integer overflow attacks attempt to use or create a numeric value bigger than the application can handle.
- Buffer overflow attacks exploit buffer overflow vulnerabilities. A common method uses NOP instructions or NOP sleds such as a string of x90 commands. Two primary protection methods against buffer overflow attacks are input validation and keeping a system up to date.
- Cross-site scripting (XSS) allows an attacker to redirect users to malicious websites and steal cookies. It uses HTML and JavaScript tags with < and > characters.
- Cross-site request forgery (XSRF) attacks cause users to perform actions on websites without their knowledge and allow attackers to steal cookies and harvest passwords. A giveaway of a potential XSRF attack is the inclusion of a question mark (?) in the URL.
- XSS and XSRF attacks are mitigated with input validation techniques.
- A driver shim is additional code that can be run instead of the original driver. Refactoring code is the process of rewriting the code's internal processing without changing its external behavior.
- Machine learning (ML) is a part of artificial intelligence (AI). Tainting training data for ML systems is one possible attack against ML and AI systems. Algorithms used for ML are proprietary and should be protected.

ine References

- Remember, you have additional resources available online. Check them out at <https://greatadministrator.com/sy0-601-extras/>.

Chapter 7 Practice Questions

1. An IDS has sent multiple alerts in response to increased traffic. Upon investigation, you realize it is due to a spike in network traffic from several sources. Assuming this is malicious, which of the following is the MOST likely explanation?
 - A. An ARP poisoning attack
 - B. A DNS poisoning attack
 - C. A domain hijacking attack
 - D. A DDoS attack

2. While investigating performance issues on a web server, you verified that the CPU usage was about 10 percent five minutes ago. However, it now shows that CPU usage has been averaging over 98 percent for the last two minutes. Which of the following BEST describes what this web server is experiencing?
 - A. Resource exhaustion
 - B. DDoS
 - C. A buffer overflow attack
 - D. A memory leak

3. An administrator regularly connects to a server using SSH without any problems. Today, he sees a message similar to the following graphic when he connects to the server.

```
@@@@@@@  
@   WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!      @  
@@@@@@@  
IT IS POSSIBLE THAT SOMEONE IS UP TO NO GOOD!  
Someone could be eavesdropping on you right now (man-in-the-middle attack)!  
It is also possible that a host key has just been changed.  
The fingerprint for the RSA key sent by the remote host is  
12:34:56:78:9a:bc:de:f1:23:45:67:89:ab:cd:ef:12.  
Please contact your system administrator.  
Add correct host key in /home/hostname/.ssh/known_hosts to get rid of this message.  
Offending RSA key in /var/lib/sss/pubconf/known_hosts:4  
RSA host key for ycda has changed and you have requested strict checking.  
Host key verification failed.
```

Which of the following is the MOST likely reason for this message?

- A. Rogue access point
- B. On-path attack
- C. MAC flooding

D. ARP poisoning

4. Homer complains that his system started acting erratically today. You discover that malware infected his system, but you discover he didn't open any email during the day. He mentions that he has been browsing the Internet all day. Which of the following could you check to see where the malware MOST likely originated?
 - A. Web server logs
 - B. Mail server logs
 - C. PowerShell logs
 - D. DNS server logs
5. While reviewing logs for a web application, a security analyst notices that it has crashed several times, reporting a memory error. Shortly after it crashes, the logs show malicious code that isn't part of a known application. Which of the following is MOST likely occurring?
 - A. Buffer overflow
 - B. ARP poisoning
 - C. Privilege escalation
 - D. Replay
6. Web developers are implementing error handling in a database application accessed by a web server. Which of the following would be the BEST way to implement this?
 - A. Display a detailed error message but log generic information on the error
 - B. Display a generic error message but log detailed information on the error
 - C. Display a generic error message and log generic information on the error
 - D. Display a detailed error message and log detailed information on the error
7. A web developer is adding input validation techniques to a website application. Which of the following should the developer implement during this process?

A. Validation on the server-side

B. Validation on the client-side

C. Normalization techniques

D. Memory management techniques

8. Developers in the YCDA organization have created an application that users can download and install on their computers. Management wants to provide users with a reliable method of verifying that the application has not been modified after YCDA released it. Which of the following methods provides the BEST solution?

A. Code signing

B. Input validation

C. Obfuscation

D. Stored procedures

9. Your organization is preparing to deploy a web-based application, which will accept user input. Which of the following will BEST test the reliability of this application to maintain availability and data integrity?

A. Static code analysis

B. Input validation

C. Error handling

D. Dynamic code analysis

10. Several developers in your organization are working on a software development project. Recently, Bart made an unauthorized change to the code that effectively broke several modules. Unfortunately, there isn't any record of who made the change or details of the change. Management wants to ensure it is easy to identify who makes any changes in the future. Which of the following provides the BEST solution for this need?

A. Dynamic code analysis

B. Version control

C. Static code analysis

D. Use of third-party SDKs

11. Database administrators have created a database used by a web application. However, testing shows that application queries against the

database take a significant amount of time. Which of the following actions is MOST likely to improve the overall performance of the database?

- A. Normalization
- B. Client-side input validation
- C. Server-side input validation
- D. Obfuscation

12. Looking at logs for an online web application, you see that someone has entered the following phrase into several queries: ' or '1'='1'; --

Which of the following provides the BEST protection against this attack?

- A. Normalization
- B. Proper error handling
- C. Removing dead code
- D. Stored procedures

13. You are examining logs generated by an online web application. You notice that the following phrase is appearing in several queries

' or '1'='1'; --

Which of the following is the MOST likely explanation for this?

- A. A buffer overflow attack
- B. A DLL injection attack
- C. A SQL injection attack
- D. A race condition

14. Your organization has created a web application that will go live after testing is complete. An application tester sees the following URL:

<https://gcapremium.com/info.php?sessionID=10123&acct=homer>.

The tester resends the following URL to the website:

<https://gcapremium.com/info.php?sessionID=32101&acct=homer>.

Which of the following attacks is the tester checking?

- A. Pass the hash
- B. Buffer overflow
- C. Cross-site request forgery
- D. Race condition

15. Your SIEM sent an alert after detecting the following script was run on a system within your network.

```
invoke-command {  
    $a = net localgroup administrators |  
        where {$_. -AND $_ -notmatch "command completed"} |  
        select -skip 4 }
```

What BEST describes this script?

- A. A Python script to list local administrators
- B. A script used to create a logic bomb
- C. A PowerShell script to list local administrators
- D. A script used to create a backdoor

Chapter 7 Practice Question Answers

1. **D** is correct. A distributed denial-of-service (DDoS) attack causes spikes in network traffic as multiple systems attempt to connect to a server and deplete the target's resources. An Address Resolution Protocol (ARP) poisoning attack attempts to mislead systems about the source media access control (MAC) address. A Domain Name System (DNS) poisoning attack attempts to redirect web browsers to malicious URLs. In a domain hijacking attack, an attacker changes a domain name registration without permission from the owner.
2. **A** is correct. CPU usage averaging 98 percent indicates resource exhaustion. The scenario doesn't indicate the cause of the increased usage, so resource exhaustion is the best answer. A distributed denial-of-service (DDoS) attack could cause this. However, a surge in traffic from an effective marketing campaign sent via email could also cause a surge in resource usage. A buffer overflow attack is a type of DDoS attack, but the scenario doesn't give enough information to indicate a buffer overflow attack has taken place. The scenario only mentions CPU usage, so there isn't any indication of a memory leak.
3. **B** is correct. The message indicates a potential man-in-the-middle (MITM) attack, which is also known as an on-path attack. Specifically, it indicates that the key on the host system has changed, which may be due to the administrator connecting to the MITM system instead of the target system. None of the other answers are related to incorrect cryptographic keys. A rogue access point is an unauthorized wireless access point. Media access control (MAC) flooding is an attack on a switch, attempting to overload it with different MAC addresses. An Address Resolution Protocol (ARP) poisoning attack misleads computers or switches about a system's actual MAC address.
4. **D** is correct. Domain Name System (DNS) logs will record DNS queries, such as what hostnames it resolved to IP addresses. The log entries would show all the domains that Homer visited during the day. One of these is

most likely the one that downloaded malware onto his system. A web server would show activity on the web server, but you wouldn't have access to web servers controlled by others. Homer didn't open any email, so the mail server logs wouldn't help. PowerShell logs may show activity, but only if the malware used PowerShell. However, the PowerShell logs are unlikely to show who ran PowerShell scripts.

5. **A** is correct. Buffer overflow attacks often cause an application to crash and expose system memory. Attackers then write malicious code into the exposed memory and use different techniques to get the system to run this code. None of the other attacks insert malicious code into memory. An Address Resolution Protocol (ARP) poisoning attack attempts to mislead systems about the source media access control (MAC) address. Privilege escalation techniques attempt to give an attacker more rights and permissions. In a replay attack, the attacker intercepts data and typically attempts to use the intercepted data to impersonate a user or system.

6. **B** is correct. You should display a generic error message but log detailed information on the error. Detailed error messages to the user are often confusing to them and give attackers information they can use against the system. Logging generic information makes it more difficult to troubleshoot the problem later.

7. **A** is correct. At a minimum, input validation should be performed on the server-side. Client-side validation can be combined with server-side validation, but attackers can bypass client-side input validation if it is used alone. Normalization techniques organize tables and columns in a database to reduce redundant data but have nothing to do with input validation. Memory management is a secure coding technique that helps prevent memory errors.

8. **A** is correct. Code signing provides a digital signature for the code, verifies the publisher of the code, and verifies that it hasn't been modified since the publisher released it. None of the other answers verify the application hasn't been modified. Input validation verifies data is valid before using it. Code obfuscation or code camouflage techniques make the

code more difficult to read. Stored procedures are used with SQL databases and can be used for input validation.

9. **D** is correct. Dynamic code analysis techniques test an application during its execution and is the best choice of the available answers to verify the application can maintain availability and data integrity. Static code analysis (such as a manual code review) is done without executing any code, but it won't test its reliability. Input validation is the practice of checking data for validity before using it, but this is done within the application, not as a method to test the application. Error-handling techniques are also done within the application.

10. **B** is correct. A version control system will track all changes to a software project, including who made the change and when. Dynamic code analysis techniques test an application during its execution. Static code analysis examines the code without executing it as a method of code testing. The use of third-party software development kits (SDKs) is a secure coding technique, but it won't detect unauthorized changes.

11. **A** is correct. Normalization techniques organize tables and columns in a database and improve overall database performance. None of the other answers improve the database performance. Input validation techniques help prevent many types of attacks, and server-side input validation techniques are preferred over client-side input validation techniques. Obfuscation techniques make code more difficult to read.

12. **D** is correct. Attackers commonly use the phrase '`' or='1'--`' in SQL injection attacks, and stored procedures are an effective method of preventing SQL injection attacks. Normalization techniques organize tables and columns in a database to reduce redundant data but don't block SQL injection attacks. This phrase won't cause an error, so proper error-handling techniques won't help. Dead code is code that is never executed, and it should be removed, but dead code is unrelated to a SQL injection attack.

13. **C** is correct. Attackers use the character string '`' or='1'='1';--`' in SQL injection attacks to query or modify databases. A buffer overflow attack

sends more data or unexpected data to an application with the goal of accessing system memory. A dynamic link library (DLL) injection attack attempts to inject DLLs into memory, causing DLL commands to run. A race condition is a programming conflict when two or more applications or application models attempt to access a resource at the same time.

14. **C** is correct. This indicates an attempt to launch a cross-site request forgery attack. The question mark (?) in the URL is the giveaway here. A pass the hash attack is a password attack. A buffer overflow attack sends unexpected data, but the URLs are primarily the same, so it isn't unexpected data. A race condition occurs when a system attempts to do two or more operations simultaneously instead of in a specific order.

15. **C** is correct. This is a PowerShell script using the invoke-command cmdlet and it lists members of the local Administrators group. This is not a Python script. This is not a logic bomb because it isn't taking any action other than creating a list. It is not creating a backdoor either.

Chapter 8

Using Risk Management Tools

CompTIA Security+ objectives covered in this chapter:

- 1.2 Given a scenario, analyze potential indicators to determine the type of attack.
 - Supply-chain attacks
- 1.3 Given a scenario, analyze potential indicators associated with application attacks.
 - Privilege escalation
- 1.5 Explain different threat actors, vectors, and intelligence sources.
 - Vectors (Supply chain)
 - Threat intelligence sources (Open source intelligence (OSINT))
 - Research sources (Vulnerability feeds, Threat feeds, Adversary tactics, techniques, and procedures (TTP))
- 1.6 Explain the security concerns associated with various types of vulnerabilities.
 - Weak configurations (Open permissions, Unsecure root accounts, Errors, Weak encryption, Unsecure protocols, Default settings, Open ports and services)
 - Improper or weak patch management (Firmware, Operating system (OS), Applications), Legacy platforms
- 1.7 Summarize the techniques used in security assessments.
 - Threat hunting (Intelligence fusion, Threat feeds, Advisories and bulletins, Maneuver)
 - Vulnerability scans (False positives, False negatives, Log reviews, Credentialed vs. non-credentialed, Intrusive vs. non-intrusive, Application, Web application, Network, Common Vulnerabilities and Exposures (CVE)/Common Vulnerability Scoring System (CVSS), Configuration review)
- 1.8 Explain the techniques used in penetration testing.
 - Penetration testing (Known environment, Unknown environment, Partially known environment, Rules of engagement, Lateral movement, Privilege escalation, Persistence, Cleanup, Bug bounty, Pivoting)

- Passive and active reconnaissance (Footprinting)
- Exercise types (Red team, Blue team, White team, Purple team)

4.1 Given a scenario, use the appropriate tool to assess organizational security.

- Network reconnaissance and discovery (nmap, netcat, IP scanners, curl, theHarvester, sn1per, scanless, dnsenum, Nessus)
- Packet capture and replay (Tcpreplay, Tcpdump, Wireshark)
- Exploitation frameworks, Password crackers

4.3 Given an incident, utilize appropriate data sources to support an investigation.

- Vulnerability scan output, Netflow/sFlow (Netflow, sFlow, IPFIX), Protocol analyzer output

5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.

- Regulations, standards, and legislation (Payment Card Industry Data Security Standard (PCI DSS))
- Key frameworks (Center for Internet Security, National Institute of Standards and Technology (NIST) Risk Management Framework (RMF)/Cybersecurity Framework (CSF), International Organization for Standardization (ISO) 27001/27002/27701/31000, SSAE SOC 2 Type I/II, Reference architecture)
- Benchmarks/secure configuration guides (Platform/vendor-specific guides, Web server, OS, Application server, Network infrastructure devices)

.4 Summarize risk management processes and concepts.

- Risk types (External, Internal, Legacy systems, Multiparty, IP theft, Software compliance/licensing)
- Risk management strategies (Acceptance, Avoidance, Transference (Cybersecurity insurance), Mitigation)
- Risk analysis (Risk register, Risk matrix/heat map, Risk control assessment, Risk control self-assessment, Risk awareness, Inherent risk, Residual risk, Control risk, Risk appetite,
- Risk assessment types (Qualitative, Quantitative)
- Likelihood of occurrence, Impact, Asset value, Single loss expectancy (SLE), Annualized loss expectancy (ALE), Annualized rate of occurrence (ARO)

**

As a security professional, you need to be aware of the different security issues associated with threats, vulnerabilities, risks, and the tools available to combat them. This chapter digs into risk management concepts, including risk assessment methods. You'll learn about vulnerability scanners and penetration testers, including key differences between them. This chapter also covers some specific tools used to assess networks and manage risks.

Understanding Risk Management

Risk is the likelihood that a threat will exploit a vulnerability. A vulnerability is a weakness, and a threat is a potential danger. The result is a negative impact on the organization. Impact refers to the magnitude of harm that can be caused if a threat exploits a vulnerability.

For example, a system without up-to-date antivirus software is vulnerable to malware. Malware written by malicious attackers is the threat. The likelihood that the malware will reach a vulnerable system represents the risk. Depending on what the malware does, the impact may be an unbootable computer, loss of data, or infection of all computers within a network. However, the likelihood of a risk occurring isn't 100 percent. An isolated system without Internet access, network connectivity, or USB ports has a very low likelihood of malware infection.

The likelihood significantly increases for an Internet-connected system, and it increases even more if a user visits risky websites and downloads and installs unverified files.

It's important to realize that you can't eliminate risk. Sure, you can avoid information technology (IT) risks completely by unplugging your computer and burying it. However, that wouldn't be very useful. Instead, users and organizations practice risk management to reduce the risks.

You probably practice risk management every day. Driving or walking down roads and streets can be a very dangerous activity. Car-sized bullets are speeding back and forth, representing significant risks to anyone else on the road. However, you mitigate these risks with caution and vigilance. The same occurs with computers and networks. An organization mitigates risks using different types of security controls.

Threats

A **threat** is a potential danger. Within the context of risk management, a threat is any circumstance or event that can compromise the confidentiality, integrity, or availability of data or a system. Threats come in different forms, including the following:

- **Malicious human threats.** Chapter 6, “Comparing Threats, Vulnerabilities, and Common Attacks,” discusses various types of threat actors. They include relatively inexperienced script kiddies, dedicated criminals working within an organized crime group, and sophisticated advanced persistent threats (APTs) sponsored by a government. These are all malicious human threats. Malicious human threats regularly launch different types of attacks, including network attacks, system attacks, and the release of malware.
- **Accidental human threats.** Users can accidentally delete or corrupt data, or accidentally access data that they shouldn’t be able to access. Even administrators can unintentionally cause system outages. The common cause is by a well-meaning administrator making a configuration change to fix one problem but inadvertently causing another one.
- **Environmental threats.** This includes long-term power failure, which could lead to chemical spills, pollution, or other possible threats to the environment. It also includes natural threats such as hurricanes, floods, tornadoes, earthquakes, landslides, electrical storms, and other similar events.

A **threat assessment** helps an organization identify and categorize threats. It attempts to predict the threats against an organization’s assets, along with the likelihood the threat will occur. Threat assessments also attempt to identify the potential impact from these threats. Once the organization identifies and prioritizes threats, it identifies security controls to protect against the most serious threats.

Risk Types

There are several different risk types or risk categories. They include:

- **Internal.** Internal risks are any risks from within an organization. This includes employees and all the hardware and software used within the organization. Internal risks are generally predictable and can be mitigated with standard security controls.
- **External.** External risks are from outside the organization. This includes any threats from external attackers. It also includes any natural threats, such as hurricanes, earthquakes, and tornadoes. While some external risks are predictable, many are not. Attackers are constantly modifying attack methods and trying to circumvent existing security controls.
- **IP theft.** Intellectual property (IP) includes things like copyrights, patents, trademarks, and trade secrets. Intellectual property is valuable to an organization, and IP theft represents a significant risk.
- **Software compliance/licensing.** Organizations typically put in a lot of time and effort when developing software. They make their money back by selling the licenses to use the software. However, if individuals or organizations use the software without buying a license, the development company loses money. Similarly, an organization can lose money if it purchases licenses, but doesn't protect them. Imagine your organization purchased 10 licenses for a software application, but several people used 5 of the licenses without authorization. Later, your supervisor gives you one of the licenses, but the application gives an error saying the license has already been used when you try to use it. In this scenario, the organization loses the cost of five licenses.
- **Legacy systems and legacy platforms.** The primary risk related to legacy systems and platforms is that the vendor doesn't support them. If vulnerabilities become known, the vendor doesn't release patches, and anyone using the legacy system is at risk.
- **Multiparty.** Multiparty (often referred to as third-party) risks occur when an organization contracts with an external organization for

goods or services. If the third-party suffers an attack, it may expose the contracting organization to additional threats.

Vulnerabilities

A **vulnerability** is a flaw or weakness in software, hardware, or a process that a threat could exploit, resulting in a security breach. Examples of vulnerabilities include:

- **Default configurations.** Hardening a system includes changing systems from their default hardware and software configurations, including changing default usernames and passwords. If systems aren't hardened, they are more susceptible to attacks. Chapter 5, "Securing Hosts and Data," covers hardening systems in more depth.
- **Lack of malware protection or updated definitions.** Antivirus and anti-malware methods protect systems from malware, but if they aren't used and kept up to date, systems are vulnerable to malware attacks. Chapter 6 covers malware types and methods used to protect systems from malware attacks.
- **Improper or weak patch management.** If systems aren't kept up to date with patches, hotfixes, and service packs, they are vulnerable to bugs and flaws in the software. Attackers can exploit operating systems, applications, and firmware that have known bugs but aren't patched.
- **Lack of firewalls.** If host-based and network firewalls aren't enabled or configured properly, systems are more vulnerable to network and Internet-based attacks. Chapter 3, "Exploring Network Technologies and Tools," covers firewalls in more depth.
- **Lack of organizational policies.** If job rotation, mandatory vacations, and least privilege policies aren't implemented, an organization may be more susceptible to fraud and collusion from employees. Chapter 11, "Implementing Policies to Mitigate Risks," covers organizational policies.

Not all vulnerabilities are exploited. For example, a user may install a wireless router using the defaults. It is highly vulnerable to an attack, but that doesn't mean that an attacker will discover it and attack. In other words, just because the wireless router has never been attacked, it doesn't

mean that it isn't vulnerable. At any moment, a war driving attacker can drive by and exploit the vulnerability.

Risk Management Strategies

Risk management is the practice of identifying, monitoring, and limiting risks to a manageable level. It doesn't eliminate risks but instead identifies methods to limit or mitigate them. There are several basic terms that you should understand related to risk management. They are:

- **Risk awareness** is the acknowledgment that risks exist and must be addressed to mitigate them. Senior personnel need to acknowledge that risks exist. Before they do, they won't dedicate any resources to manage them.
- **Inherent risk** refers to the risk that exists before controls are in place to manage the risk.
- **Residual risk** is the amount of risk that remains after managing or mitigating risk to an acceptable level. Senior management is ultimately responsible for residual risk, and they are responsible for choosing a level of acceptable risk based on the organization's goals. They decide what resources (such as money, hardware, and time) to dedicate to manage the risk.
- **Control risk** refers to the risk that exists if in-place controls do not adequately manage risks. Imagine systems have antivirus software installed, but they don't have a reliable method of keeping it up to date. Additional controls are needed to manage this risk adequately.
- **Risk appetite** refers to the amount of risk an organization is willing to accept. This varies between organizations based on their goals and strategic objectives.

There are multiple risk management strategies available to an organization. They include:

- **Avoidance.** An organization can avoid a risk by not providing a service or not participating in a risky activity. For example, an organization may evaluate an application that requires multiple open ports on the firewall and decide the application is too risky. It can avoid the risk by purchasing a different application that doesn't require opening any additional firewall ports.
- **Mitigation.** The organization implements controls to reduce risks. These controls either reduce the vulnerabilities or reduce the impact

of the threat. For example, up-to-date antivirus software mitigates the risks of malware. Similarly, a security guard can reduce the risk of an attacker accessing a secure area.

- **Acceptance.** When the cost of a control outweighs a risk, an organization will often accept the risk. For example, spending \$100 in hardware locks to secure a \$15 mouse doesn't make sense. Instead, the organization accepts the risk of someone stealing a mouse. Similarly, even after implementing controls, residual risk remains, and the organization accepts this residual risk.
- **Transference.** The organization transfers the risk to another entity or at least shares the risk with another entity. The most common method is by purchasing insurance. Another method is by outsourcing or contracting a third party.
- **Cybersecurity insurance.** Cybersecurity insurance helps protect businesses and individuals from losses related to cybersecurity incidents such as data breaches and network damage. Traditional insurance policies often exclude cybersecurity risks such as the loss of data or extortion from criminals using ransomware. Organizations purchase cybersecurity insurance to cover the gaps left by traditional insurance.

Remember this

It is not possible to eliminate risk, but you can take steps to manage it. An organization can avoid a risk by not providing a service or not participating in a risky activity. Insurance transfers the risk to another entity. You can mitigate risk by implementing controls, but when the cost of the controls exceeds the cost of the risk, an organization accepts the remaining, or residual, risk.

Risk Assessment Types

A risk assessment, or risk analysis, is an important task in risk management. It quantifies or qualifies risks based on different values or judgments. A risk assessment starts by first identifying assets and asset values.

An **asset** includes any product, system, resource, or process that an organization values, and the asset value identifies the worth of the asset to

the organization. It can be a specific monetary value or subjective value, such as Low, Medium, and High. The asset value helps an organization focus on the high-value assets and avoid wasting time on low-value assets.

After identifying asset values, the risk assessment then identifies threats and vulnerabilities and determines the likelihood a threat will attempt to exploit a vulnerability. A risk assessment attempts to identify the impact of potential threats, identify the potential harm, and prioritize risks based on the likelihood of occurrence and impact. Last, a risk assessment includes recommendations on what controls to implement to mitigate risks.

A risk assessment is a point-in-time assessment or a snapshot. In other words, it assesses the risks based on current conditions, such as current threats, vulnerabilities, and existing controls. For example, consider a library computer that has up-to-date antivirus protection and cannot access the Internet. Based on these conditions, the risks are low. However, if administrators connect the system to the Internet, or fail to keep the antivirus software up to date, the risk increases.

It's common to perform risk assessments on new systems or applications. For example, if an organization is considering adding a new service or application that can increase revenue, it will often perform a risk assessment. This helps it determine if the potential risks may offset the potential gains.

Risk assessments use quantitative measurements or qualitative measurements. Quantitative measurements use numbers, such as a monetary figure representing cost and asset values. Qualitative measurements use judgments. Both methods have the same core goal of helping management make educated decisions based on priorities.

A **risk control assessment** (sometimes called a risk and control assessment) examines an organization's known risks and evaluates the effectiveness of in-place controls. If a risk assessment is available, the risk control assessment will use it to identify the known risks. It then focuses on the in-place controls to determine if they adequately mitigate the known risks.

As a simple example, imagine a risk assessment identified malware as a risk. Further, imagine the organization installed antivirus software on its mail server to block all incoming emails containing malware. The risk control assessment would likely point out that malware comes from

multiple sources, so antivirus software on the mail server alone is not adequate to mitigate risks from malware. It may recommend installing antivirus software on all internal hosts and using a network appliance to scan all incoming traffic for malicious traffic.

The **risk control self-assessment** is a risk control assessment, but employees perform it. In contrast, a risk control assessment is performed by a third-party. The danger of doing a self-assessment is that the same employees who installed the controls may be asked to evaluate their effectiveness.

Quantitative Risk Assessment

A **quantitative risk assessment** measures the risk of using a specific monetary amount. This monetary amount makes it easier to prioritize risks. For example, a risk with a potential loss of \$30,000 is much more important than a risk with a potential loss of \$1,000.

The asset value is an important element in a quantitative risk assessment. It may include the revenue value or replacement value of an asset. A web server may generate \$10,000 in revenue per hour. If the web server fails, the company will lose \$10,000 in direct sales each hour it's down, plus the cost to repair it. It can also result in the loss of future business if customers take their business elsewhere. In contrast, a library workstation's failure may cost a maximum of \$1,000 to replace.

One commonly used quantitative model uses the following values to determine risks:

- **Single loss expectancy (SLE).** The SLE is the cost of any single loss.
- **Annual rate of occurrence (ARO).** The ARO indicates how many times the loss will occur in a year. If the ARO is less than 1, the ARO is represented as a percentage. For example, if you anticipate the occurrence once every two years, the ARO is 50 percent or .5.
- **Annual loss expectancy (ALE).** The ALE is the value of SLE × ARO.

Imagine that employees at your company lose, on average, one laptop a month. Thieves have stolen them when employees left them in conference rooms during lunch, while they were on-site at customer locations, and from training rooms.

Someone suggested purchasing hardware locks to secure these laptops for a total of \$1,000. These locks work similar to bicycle locks and allow employees to wrap the cable around a piece of furniture and connect into the laptop. A thief needs to either destroy the laptop to remove the lock or take the furniture with him when stealing the laptop. Should your company purchase them? With a little analysis, the decision is easy.

You have identified the average cost of these laptops, including the hardware, software, and data, is \$2,000 each. This assumes employees do not store entire databases of customer information or other sensitive data on the systems, which can easily result in much higher costs. You can now calculate the SLE, ARO, and ALE as follows:

- **SLE.** The value of each laptop is \$2,000, so the SLE is \$2,000.
- **ARO.** Employees lose about one laptop a month, so the ARO is 12.
- **ALE.** You calculate the ALE as $SLE \times ARO$, so $\$2,000 \times 12 = \$24,000$.

Security experts estimate that these locks will reduce the number of lost or stolen laptops from 12 a year to only 2 a year. This changes the ALE from \$24,000 to only \$4,000 (saving \$20,000 a year). In other words, the organization can spend \$1,000 to save \$20,000. It doesn't take a rocket scientist to see that this is a good fiscal decision, saving a net of \$19,000. Buy them.

Managers use these two simple guidelines for most of these decisions:

- If the cost of the control is less than the savings, purchase it.
- If the cost of the control is greater than the savings, accept the risk.

The organization might be considering other controls, such as a combination of hardware locks, biometric authentication, LoJack for Laptops, and more. The final cost of all of these controls is \$30,000 per year. Even if a laptop is never stolen again, the company is spending \$30,000 to save \$24,000, resulting in a higher net loss—they're losing \$6,000 more a year.

Admittedly, a company could choose to factor in other values, such as the sensitivity of data on the laptops, and make a judgment to purchase these additional controls. However, if they're using a quantitative risk assessment, these values would need to be expressed in monetary terms.

Although you would normally know the SLE and ARO and use these to calculate the ALE, you might occasionally have the SLE and ALE, but

not know the ARO. Using basic algebra, you can reformat the formula. Any of these are valid:

- $ALE = SLE \times ARO$
- $ARO = ALE / SLE$
- $SLE = ALE / ARO$

Remember this

A quantitative risk assessment uses specific monetary amounts to identify cost and asset values. The SLE identifies each loss's amount, the ARO identifies the number of failures in a year, and the ALE identifies the expected annual loss. You calculate the ALE as $SLE \times ARO$. A qualitative risk assessment uses judgment to categorize risks based on the likelihood of occurrence and impact.

Qualitative Risk Assessment

A ***qualitative risk assessment*** uses judgment to categorize risks based on the **likelihood of occurrence** (or probability) and impact. The likelihood of occurrence is the probability that an event will occur, such as the likelihood that a threat will attempt to exploit a vulnerability. ***Impact*** is the magnitude of harm resulting from a risk. It includes the negative results of an event, such as the loss of confidentiality, integrity, or availability of a system or data.

Notice that this is much different from the exact numbers provided by a quantitative assessment that uses monetary figures. You can think of quantitative as using a quantity or a number, whereas qualitative is related to quality, which is often a matter of judgment.

Some qualitative risk assessments use surveys or focus groups. They canvass experts to provide their best judgments and then tabulate the results. For example, a survey may ask the experts to rate the probability and impact of risks associated with a web server selling products on the Internet and a library workstation without Internet access. The experts would use words such as low, medium, and high to rate them.

They could rate the probability of a web server being attacked as high, and if the attack takes the web server out of service, the impact is also high. On the other hand, the probability of a library workstation being attacked is

low, and, even though a library patron may be inconvenienced, the impact is also low.

It's common to assign numbers to these judgments. For example, you can use low, medium, and high terms and give them values of 1, 5, and 10, respectively. The experts assign a probability and impact of each risk using low, medium, and high, and when tabulating the results, you change the words to numbers. This makes it a little easier to calculate the results.

In the web server and library computer examples, you can calculate the risk by multiplying the probability and the impact:

- **Web server.** High probability and high impact: $10 \times 10 = 100$
- **Library computer.** Low probability and low impact: $1 \times 1 = 1$

Management can look at these numbers and easily determine how to allocate resources to protect against the risks. They would allocate more resources to protect the web server than the library computer.

One of the challenges with a qualitative risk assessment is gaining consensus on the probability and impact. Unlike monetary values that you can validate with facts, probability and impact are often subject to debate.

Documenting the Assessment

The final phase of the risk assessment is the report. This identifies the risks discovered during the assessment and the recommended controls. As a simple example, a risk assessment on a database-enabled web application may discover that it's susceptible to SQL injection attacks. The risk assessment will then recommend rewriting the web application with input validation techniques and stored procedures to protect the database.

Management uses this to decide which controls to implement and which risks to accept by not implementing controls. In many cases, a final report documents the managerial decisions. Of course, management can decide not to implement a control but instead accept a risk.

Think how valuable this report will be for an attacker. They won't need to dig to identify vulnerabilities or controls. Instead, the report lists all the details. Even when management approves controls to correct the vulnerabilities, it may take some time to implement them. Because of this, it's important to protect the risk assessment report. Normally, only executive management and security professionals will have access to these reports.

Risk Analysis

Risk assessments use a variety of techniques to analyze risks.

Generically, a **risk analysis** identifies potential issues that could negatively impact an organization's goals and objectives. However, different disciplines define it a little differently. As an example, project management professionals would tell you that a risk analysis identifies potential risks that may impact a project's outcomes and objectives instead of the organization's goals and objectives.

Similarly, the following terms might have slightly different definitions within project management circles or with financial management specialists. However, these definitions are valid within cybersecurity:

- **Risk register.** A **risk register** lists all known risks for a system or an organization. It's often in a table format or as a risk log and is a living document. A table format would have predefined columns such as the risk, the risk owner, mitigation measures, the impact, the likelihood of occurrence, and a risk score. The risk owner is responsible for implementing security controls to mitigate the risk. As security professionals investigate new risks, they add new rows to the table. A risk log format is similar to a file and allows personnel to document risk management activities using free-flowing text instead of formalized columns in a table.
- **Risk matrix.** A **risk matrix** plots risks onto a graph or chart. As a simple example, it can plot the likelihood of occurrence data against the impact of a risk, as shown in Figure 8.1. The letters (A to D) represent specific risks documented elsewhere (such as in the risk register). However, it's easy to see that personnel should spend most of their time on risk D, but risk has already been mitigated to an acceptable level.

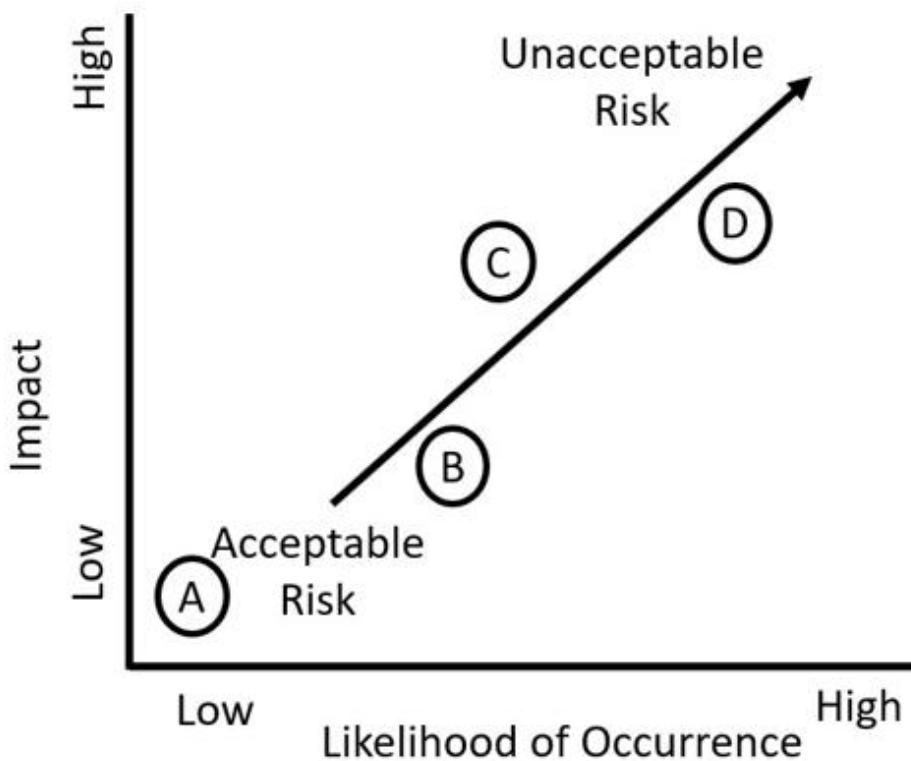


Figure 8.1: Risk Matrix

- **Heat map.** A *heat map* is similar to a risk matrix. However, instead of using words such as acceptable risk and unacceptable risk, they use colors such as green and red, respectively. For example, the risk matrix shown in Figure 8.1 would be colored green in the bottom-left area and red in the top-right area. The middle area would be yellow.

Remember this

A risk register is a comprehensive document listing known information about risks such as the risk owner. It typically includes risk scores along with recommended security controls to reduce the risk scores. A risk matrix plots risks onto a graph or chart, and a risk heat map uses color-coding to plot the risks.

Supply Chain Risks

A *supply chain* includes all the elements required to produce and sell a product. As a simple example, consider the Lard Lad Donuts store. They require a steady supply of flour, sugar, eggs, milk, oil, and other ingredients.

They also require refrigerators to store raw materials, space to manufacture the donuts, and fryers to cook them. Last, they need a method to sell the donuts to customers. If any of these items fail, the company won't be able to make and sell donuts.

It's important to realize that the supply chain isn't only the supply of raw materials. It also includes all the processes required to create and distribute a finished product.

A supply chain can become an attack vector if an attacker can disrupt the supply chain. If an attacker wanted to stop the donut store from producing donuts, it isn't necessary to attack the donut store. Instead, an attacker can attack one of the third-party suppliers in a supply chain attack. A potential indicator of a supply chain attack is a disruption in the supply chain.

Organizations can eliminate the supply chain as a third-party risk simply by ensuring that it has multiple sources for everything that it needs. While this is relatively simple when looking for alternate sources to purchase flour and sugar, it can be difficult when an organization needs complex materials.

For example, General Motors chose to build some 2021 vehicles without the GM Active Fuel Management module due to a worldwide chip shortage. Ford reported the chip shortage could lower its earnings by more than a billion dollars. Most of these chips are produced in Asian nations such as Taiwan and China. While the chip shortage was mainly due to automakers miscalculating supply and demand, it could just as easily be due to an attack. If an attacker destroys one or two factories producing these chips, it could impact the bottom line of automakers on the other side of the world.

Chapter 11 discusses third-party risks in more depth.

Threat Hunting

Threat hunting is the process of actively looking for threats within a network before an automated tool detects and reports on the threat.

An important part of threat hunting is gathering data on the threat through threat intelligence. This refers to information on a threat's capabilities, motives, goals, and resources. This knowledge comes from both internal and external sources.

Internal sources include device logs, IDS alerts, and data from past incidents. Historical data on incidents can help you understand what happened, what worked to mitigate the incident, and what didn't work.

External sources are generated from outside the organization. Chapter 6 discussed ***open source intelligence (OSINT)***, which includes anything available on the Internet such as blogs from researchers and vendors, media reports, and more.

Data feeds provide subscribers regular data on a wide variety of topics. As a generic example, a news feed provides subscribers with a regular stream of up-to-date news. ***Threat feeds*** provide subscribers with up-to-date information on current threats. Many security organizations publish feeds and anyone with an email address can subscribe to them.

Threat feeds use both structured data reports and unstructured reports. A structured report uses a structured language such as Structured Threat Information eXpression (STIX) and unstructured reports use white papers released as Word documents or PDF files.

Security advisories and bulletins are also valuable sources of data. As an example, the United States Computer Emergency Readiness Team (US-CERT) maintains the National Cyber Awareness System. They regularly release free information on threats and vulnerabilities through alerts, bulletins, analysis reports, tips, and other general publications. Anyone can sign up for these here: <https://us-cert.cisa.gov/mailing-lists-and-feeds>.

Adversary tactics, techniques, and procedures (TTPs) refer to attackers' methods when exploiting a target. The National Institute of Standards and Technology (NIST) SP 800-150, "Guide to Cyber Threat Information Sharing," defines TTPs as "...the behavior of an actor. Tactics are high-level descriptions of behavior, techniques are detailed descriptions

of behavior in the context of a tactic, and procedures are even lower-level, highly detailed descriptions in the context of a technique.” By analyzing the TTPs, security analysts often identify how attackers maneuver through a network. Because attackers often use similar TTPs in different attacks, analysts can sometimes predict the attackers’ next steps.

Threat feeds commonly describe threats and list TTPs used by attackers. Additionally, they include specific indicators of compromise that threat hunters can use to detect the presence of attackers in a network.

Threat *intelligence fusion* combines all this data to create a picture of likely threats and risks for an organization. This helps the cybersecurity analysts understand how threat actors may maneuver through the network, how to detect them, and how to mitigate their efforts once they’re discovered.

Comparing Scanning and Testing Tools

Security administrators use tools to test their networks. Two common categories of tools are vulnerability scanners, which check for weaknesses, and penetration tests, which attempt to exploit the vulnerabilities. This section covers vulnerability scanners and penetration tests in more depth.

Checking for Vulnerabilities

Vulnerabilities are weaknesses, and by reducing vulnerabilities, you can reduce risks. That sounds simple enough. However, how do you identify the vulnerabilities that present the greatest risks? Some common methods are vulnerability assessments and various scans such as network scans and vulnerability scans.

The overall goal of a vulnerability assessment is to assess the security posture of systems and networks. They identify vulnerabilities or weaknesses within systems, networks, and organizations and are part of an overall risk management plan.

Vulnerability assessments can include information from a wide variety of sources. This includes reviewing security policies and logs, interviewing personnel, and testing systems. Assessments often use a variety of scans and penetration tests, all discussed in this section. A vulnerability assessment typically includes the following high-level steps:

- Identify assets and capabilities.
- Prioritize assets based on value.
- Identify vulnerabilities and prioritize them.
- Recommend controls to mitigate serious vulnerabilities.

Many organizations perform vulnerability assessments internally. Organizations also hire external security professionals to complete external assessments. The following sections discuss many of the common tools used for vulnerability assessments and vulnerability scans.

Password Crackers

A ***password cracker*** attempts to discover a password. Passwords are typically hashed so that they aren't easily readable. Some hashing methods are stronger than others. If weak methods are used to protect passwords, a password cracker can discover the password or at least discover another password that will create the same hash.

As an example, Message Digest 5 (MD5) is a weak hashing algorithm. When executed against a password of P@ssw0rd, it creates the following MD5hash: 161ebd7d45089b3446ee4e0d86dbcf92. A password cracker can

analyze the MD5 hash of 161ebd7d45089b3446ee4e0d86dbcf92 and discover that the password of P@ssw0rd creates the same hash.

There are two categories of password crackers—offline and online:

- An offline password cracker attempts to discover passwords by analyzing a database or file containing passwords. For example, attackers often obtain large volumes of data during a data breach. This includes files that include hashed or encrypted passwords. They can then analyze the protected passwords to discover the actual passwords. A key benefit of an offline password cracking attack is that attackers have unlimited time to analyze the passwords.
- An online password cracker attempts to discover passwords by guessing them in a brute force attack. For example, some online password crackers attempt to discover the passwords for specific accounts by trying to log on to the accounts remotely. Other online password crackers collect network traffic and attempt to crack any passwords sent over the network.

Chapter 10, “Understanding Cryptography and PKI,” covers password attacks and how hashing methods attempt to thwart password attacks. The point here is that password crackers are one of the tools security administrators use during a vulnerability assessment. Of course, attackers can use the same password crackers.

Network Scanners

A **network scanner** uses various techniques to gather information about hosts within a network. As an example, Nmap is a popular network scanning tool that can give you a lot of information about hosts within a network. Network scanners typically use the following methods:

- **Arp ping scan.** Chapter 1, “Mastering Security Basics,” discusses the Address Resolution Protocol (ARP) and how systems use it to resolve IP addresses to media access control (MAC) addresses. Any host that receives an ARP packet with its IP address responds with its MAC address. If the host responds, the network scanner knows that a host is operational with that IP address.
- **Syn stealth scan.** Chapter 3 discusses the Transmission Control Protocol (TCP) three-way handshake. As a reminder, one host sends

out a SYN (synchronize) packet to initiate a TCP session. The other host responds with a SYN/ACK (synchronize/acknowledge) packet. The first host then completes the handshake with an ACK packet to establish the connection. A syn stealth scan sends a single SYN packet to each IP address in the scan range. If a host responds, the scanner knows that a host is operational with that IP address. However, instead of responding with an ACK packet, a scanner typically sends an RST (reset) response to close the connection.

- **Port scan.** A port scan checks for open ports on a system. Each open port indicates the underlying protocol is running on the system. For example, if port 443 is open, it indicates the host is running HTTPS, meaning it is probably a web server. A port scan typically uses the ports identified as well-known ports by the Internet Assigned Numbers Authority (IANA) and discussed in Appendix D.
- **Service scan.** A service scan is like a port scan, but it goes a step further. A port scan identifies open ports and gives hints about what protocols or services might be running. The service scan verifies the protocol or service. For example, if a port scan identifies port 443 is open, a service scan will send an HTTPS command, such as “Get /.” If HTTPS is running on port 443, it will respond to the Get command verifying that it is a web server.
- **OS detection.** Operating system (OS) detection techniques analyze packets from an IP address to identify the OS. This is often referred to as TCP/IP fingerprinting. As a simple example, the TCP window size (the size of the receive window in the first packet of a TCP session) is not fixed. Different operating systems use different sizes. Some Linux versions use a size of 5,840 bytes, some Cisco routers use a size of 4,128 bytes, and different Windows versions use sizes of 8,192 and 65,535. OS detection techniques don’t rely on a single value but typically evaluate multiple values included in systems responses.

Remember this

Password crackers attempt to discover passwords and can identify weak passwords, or poorly protected passwords. Network scanners can detect all

the hosts on a network, including the operating system and services or protocols running on each host.

Vulnerability Scanning

Security administrators often use a vulnerability scanner to identify which systems are susceptible to attacks. Vulnerability scanners identify a wide range of weaknesses and known security issues that attackers can exploit. Most vulnerability scanners combine multiple features into a single package. A vulnerability scan often includes the following actions:

- Identify vulnerabilities.
- Identify misconfigurations.
- Passively test security controls.
- Identify lack of security controls.

Identifying Vulnerabilities and Misconfigurations

Vulnerability scanners utilize a database or dictionary of known vulnerabilities and test systems against this database. For example, the MITRE Corporation maintains the Common Vulnerabilities and Exposures (CVE) list, which is a dictionary of publicly known security vulnerabilities and exposures. This is similar to how antivirus software detects malware using virus signatures. The difference is that the CVE is one public list funded by the U.S. government, whereas antivirus vendors maintain proprietary signature files.

The Common Vulnerability Scoring System (CVSS) assesses vulnerabilities and assigns severity scores in a range of 0 to 10, with 10 being the most severe. This helps security professionals prioritize their work in mitigating known vulnerabilities.

Other standards used by vulnerability scanners include the Security Content Automation Protocol (SCAP). SCAP utilizes the National Vulnerability Database (NVD), which includes lists of common misconfigurations, security-related software flaws, and impact ratings or risk scores. The risk scores quantify risks, allowing security experts to prioritize vulnerabilities. The SCAP uses both CVE and CVSS data.

Additionally, attackers often look for misconfigured systems. Vulnerability scanners help them detect common misconfiguration settings. Some of the vulnerabilities related to weak configurations include:

- **Open ports and services.** Open ports can signal a vulnerability, especially if administrators aren't actively managing the services associated with these ports. For example, all web servers do not use File Transfer Protocol (FTP), so if TCP ports 20 and 21 are open, it indicates a potential vulnerability related to FTP. Similarly, Telnet uses port 23, so if this port is open, an attacker can try to connect to the server using Telnet.
- **Unsecure root accounts.** Root accounts such as Administrator accounts on Windows systems or the Root account on Linux systems have full control over systems. If they aren't protected with strong passwords, attackers may be able to access these accounts and exploit the systems.
- **Default accounts and passwords.** Operating systems and applications can have default usernames and passwords. Basic operating system and application hardening steps should remove the defaults, and a scan can discover the weaknesses if operating systems and applications aren't secured properly. For example, some SQL database systems allow the sa (system administrator) account to be enabled with a blank password. Scanners such as Nessus will detect this.
- **Default settings.** In addition to changing default accounts and passwords, it's also important to change many default settings. Administrators often use baselines to harden systems and make them more secure from the default configuration.
- **Unpatched systems.** Vulnerability scanners can also identify missing security controls, such as the lack of up-to-date patches or the lack of antivirus software. Although many patch management tools include the ability to verify systems are up to date with current patches, vulnerability scanners provide an additional check to detect unpatched systems.
- **Errors.** Vulnerability scans can also check the system against a configuration or security baseline to identify common security and configuration errors.
- **Open permissions.** It's common to secure files with permissions to prevent unauthorized access. However, there have been many instances where files have remained available to anyone who found

them. This happens when people use unfamiliar technologies. As an example, Amazon Web Services (AWS) allows people to store data in buckets. When people started using AWS buckets, they often left the data available to everyone with open permissions. However, personnel using AWS buckets are more knowledgeable today so this isn't as common.

- **Unsecure protocols.** Unsecure protocols are protocols that have known issues. These have typically been deprecated and are no longer recommended for use. For example, Telnet sends all data across the network in cleartext and shouldn't be used.
- **Weak encryption.** Chapter 10 covers encryption protocols such as Secure Sockets Layer (SSL) and its designated replacement Transport Layer Security (TLS). Both have been used to encrypt Hypertext Transfer Protocol Secure (HTTPS). However, SSL has been deprecated and should not be used because of known weaknesses. Any applications using SSL instead of TLS are susceptible to attacks.
- **Weak passwords.** Many scanners include a password cracker that can discover weak passwords or verify that users are creating strong passwords in compliance with an organization's policy. It is more efficient to use a technical password policy to require and enforce the use of strong passwords. However, if this isn't possible, administrators use a separate password cracker to discover weak passwords.
- **Sensitive data.** Some scanners include data loss prevention (DLP) techniques to detect sensitive data sent over the network. For example, a DLP system can scan data looking for patterns such as Social Security numbers or key words that identify classified or proprietary data.

Administrators can scan specific systems or an entire network. For example, many organizations perform periodic scans on the entire network to detect vulnerabilities. If an administrator makes an unauthorized change resulting in a vulnerability, the scan can detect it. Similarly, if a rebuilt system is missing some key security settings, the scan will detect them. It's also possible to scan a new system before or right after it's deployed.

Analyzing Vulnerability Scan Outputs

A vulnerability scan creates a report showing the results of the scan. The output of the scan typically shows the following information:

- A list of hosts that it discovered and scanned
- A detailed list of applications running on each host
- A detailed list of open ports and services found on each host
- A list of vulnerabilities discovered on any of the scanned hosts
- Recommendations to resolve any of the discovered vulnerabilities

Some vulnerability scanners include the ability to run at preconfigured times automatically. Administrators can use predefined vulnerability reports or create customized reports based on their needs. These reports are typically available in logs, and administrators perform log reviews periodically.

When analyzing the scan outputs, it's important to compare them with previous scans. In some cases, you may notice that scans report the same vulnerability. There are two primary reasons for this. It could be that a patch has undesired side effects, so management has decided to accept the risk and not apply the patch. It could also be that the vendor has not created a patch.

Passively Testing Security Controls

An important point about a vulnerability scan is that it does not attempt to exploit any vulnerabilities. Instead, a vulnerability scan is a passive attempt to identify weaknesses. This ensures that the testing does not interfere with normal operations. Security administrators then assess the vulnerabilities to determine which ones to mitigate. In contrast, a penetration test (covered later in this chapter) is an active test that attempts to exploit vulnerabilities.

Remember this

A vulnerability scanner can identify vulnerabilities, misconfigured systems, and the lack of security controls such as up-to-date patches. Vulnerability scans are passive and have little impact on a system during a test. In contrast, a penetration test is intrusive and can potentially compromise a system.

False Positives and False Negatives

Unfortunately, scanners aren't perfect. Occasionally, they report a vulnerability when it doesn't actually exist. In other words, a scan may indicate a system has a known vulnerability, but the report is false. This is a ***false positive***. As an example, a vulnerability scan on a server might report that the server is missing patches related to a database application, but the server doesn't have a database application installed.

This is similar to false positives in an intrusion detection system (IDS), where the IDS alerts on an event, but the event isn't an actual intrusion. Similarly, an antivirus scanner can identify a useful application as malware, even though it does not have any malicious code. False positives can result in higher administrative overhead because administrators have to investigate them.

Scanners can give false negatives also. If a vulnerability exists but the scanner doesn't detect it, this is a ***false negative***. As an example, imagine that when patches are applied to an application server, it breaks the application. Management decides to accept the risk of not applying these patches to keep the application running. Even though these patches are missing, the vulnerability scanner doesn't report that the patches are missing.

The following list describes the four possibilities when a scanner scans a system looking for vulnerabilities. Refer to Figure 8.2 as you're reading them:

	Scanner Not Accurate	Scanner Accurate
Vulnerability Exists	False Negative	True Positive
Vulnerability Does Not Exist	False Positive	True Negative

Figure 8.2: False Positives and False Negatives

- **False positive.** A false positive is when a vulnerability scanner incorrectly reports that a vulnerability exists, but the vulnerability does not exist on the scanned system.
- **False negative.** A false negative is when a vulnerability exists, but the scanner doesn't detect it and doesn't report the vulnerability.
- **True positive.** A true positive indicates that the vulnerability scanner correctly identified a vulnerability.

- **True negative.** A true negative indicates that a system doesn't have a vulnerability, and the vulnerability scanner did not report the vulnerability.

Credentialed Versus Non-Credentialed

Vulnerability scanners can run as a credentialed scan using an account's credentials or as non-credentialed without any user credentials. Attackers typically do not have an internal account's credentials, so when they run scans against systems, they run non-credentialed scans.

Security administrators often run credentialed scans with the privileges of an administrator account. This allows the scan to check security issues at a much deeper level than a non-credentialed scan. For example, a credentialed scan can list the software versions of installed programs. Additionally, because the credentialed scan can access a system's internal workings, it results in a lower impact on the tested systems, along with more accurate test results and fewer false positives.

It's worth mentioning that attackers typically start without any credentials but use privilege escalation techniques to gain administrative access. This allows them to run a credentialed scan against a network if desired. Similarly, even though a credentialed scan is typically more accurate, administrators often run non-credentialed scans to see what an attacker without credentials would see.

Remember this

A false positive from a vulnerability scan indicates that a scan detected a vulnerability, but the vulnerability doesn't exist. Credentialed scans run under the context of a valid account and can get more detailed information on targets, such as the software versions of installed applications. They are typically more accurate than non-credentialed scans and result in fewer false positives.

Configuration Review

A configuration compliance scanner performs a configuration review of systems to verify that they are configured correctly. They will often use a file that identifies the proper configuration for systems. When running the scan, the scanner will verify that systems have the same configuration

defined in the configuration file. This is also known as configuration validation. Security administrators often configure these tools to use automation or scripting methods so that they automatically run on a set schedule.

Configuration review scans typically need to be run as credentialed scans. This helps ensure they can accurately read the configuration of systems during the scan.

Penetration Testing

Penetration testing actively assesses deployed security controls within a system or network. It starts with reconnaissance to learn about the target but takes it a step further and tries to exploit vulnerabilities by simulating or performing an attack.

Security testers typically perform a penetration test to demonstrate the actual security vulnerabilities within a system. This can help the organization determine the impact of a threat against a system. In other words, it helps an organization determine the extent of damage that an attacker could inflict by exploiting a vulnerability.

Although it's not as common, it's also possible to perform a penetration test to determine how an organization will respond to a compromised system. This allows an organization to demonstrate security vulnerabilities and flaws in policy implementation. For example, many organizations may have perfect policies on paper. However, if employees aren't consistently following the policies, a penetration test can accurately demonstrate the flaws.

Because a penetration test can exploit vulnerabilities, it has the potential to disrupt actual operations and cause system instability. Because of this, it's important to strictly define the boundaries for a test. Ideally, the penetration test will stop right before performing an exploit that can cause damage or result in an outage. However, some tests cause unexpected results.

Testers sometimes perform penetration tests on test systems rather than the live production systems. For example, an organization may be hosting a web application accessible on the Internet. Instead of performing the test on the live server and affecting customers, penetration testers or administrators configure another server with the same web application. If a penetration test cripples the test server, it accurately demonstrates security vulnerabilities, but it doesn't affect customers.

Remember this

A penetration test is an active test that can assess deployed security controls and determine the impact of a threat. It starts with reconnaissance and then tries to exploit vulnerabilities by attacking or simulating an attack.

Rules of Engagement

It's important to obtain authorization before beginning any vulnerability or penetration testing. This outlines the *rules of engagement* or the boundaries of the tests. If testing results in an outage even though the testers followed the engagement rules, repercussions are less likely.

In most cases, this consent is in writing. If it isn't in writing, many security professionals won't perform any testing. A penetration test without consent is an attack, and an organization may perceive a well-meaning administrator doing an unauthorized penetration test as an attacker. The administrator might be updating his résumé after running an unauthorized scan or penetration test.

Reconnaissance

Penetration testers use a variety of methods for *reconnaissance* (sometimes called *footprinting*). During the reconnaissance phase, the penetration tester (or attacker) attempts to learn as much as possible about a network. Testers use both passive reconnaissance and active network reconnaissance and discovery when gathering information on targets.

Passive and Active Reconnaissance

Passive reconnaissance collects information about a targeted system, network, or organization using open source intelligence (OSINT). This includes viewing social media sources about the target, news reports, and even the organization's website. If the organization has wireless networks, it could include passively collecting information from the network, such as network SSIDs. Note that because passive reconnaissance doesn't engage a target, it isn't illegal.

As an example, theHarvester is a passive reconnaissance command-line tool used by testers in the early stages of a penetration test. It uses OSINT methods to gather data such as email addresses, employee names, host IP addresses, and URLs. It uses popular (and not so popular) search engines for queries and then correlates the results in a comprehensive report.

Passive reconnaissance does not include using any tools to send information to targets and analyze the responses. However, passive

reconnaissance can include using tools to gather information from systems other than the target. For example, you can sometimes gain information about a domain name holder using the Whois lookup site (<https://www.whois.com>). Other times, you can gain information by querying Domain Name System (DNS) servers.

Active reconnaissance methods use tools to engage targets. The next section describes many tools used to gather information about networks using active reconnaissance methods.

Network Reconnaissance and Discovery

Network reconnaissance and discovery methods use tools to send data to systems and analyze the responses. This phase typically starts by using various scanning tools such as network scanners and vulnerability scanners. It's important to realize that network reconnaissance engages targets and is almost always illegal. It should never be started without first getting explicit authorization to do so.

The “Network Scanners” section earlier in this chapter discussed how tools gather a significant amount of information about networks and individual systems. This includes identifying all IP addresses active in a network, the ports and services active on individual systems, and the operating system running on individual systems.

Some tools used during this phase include:

- **IP scanner.** An ***IP scanner*** (sometimes called a ping scanner) searches a network for active IP addresses. It typically sends an Internet Control Message Protocol (ICMP) ping to a range of IP addresses in a network. If the host responds, the network scanner knows there is a host operational with that IP address. A problem with ping scans is that firewalls often block ICMP, so the scan may give inconsistent results.
- **Nmap.** ***Nmap*** is a network scanner that you can run from the command prompt. It includes many capabilities, including identifying all the active hosts on a network, their IP addresses, the protocols and services running on each of these hosts, and the host's operating system. When running the command, you include the scan type(s), options, and target specifications.

- **Netcat.** *Netcat* (nc) is a command-line tool that administrators often use for remotely accessing Linux systems. Testers often use it for banner grabbing, a technique used to gain information about remote systems. Banner grabbing will identify the target's operating system along with information about some applications. It can also be used to transfer files and check for open ports.
- **Scanless.** Penetration testers often use *scanless*, a Python-based command-line utility to perform port scans. A benefit is that scanless uses an online website (with or without the website owner's permission) to perform the scans so that the scans don't come from the tester's IP address. Instead, they appear to originate from the website's IP address.
- **Dnsenum.** The *dnsenum* command will enumerate (or list) Domain Name System (DNS) records for domains. It lists the DNS servers holding the records and identifies the mail servers (if they exist) by listing the mx records. Next, it attempts to do an AXFR transfer to download all DNS records from the DNS servers holding the records. However, unauthenticated AXFR transfers are usually blocked on DNS servers so the AXFR requests will normally fail.
- **Nessus.** Nessus is a vulnerability scanner developed by Tenable Network Security. It uses plug-ins to perform various scans against both Windows and Unix systems and is often used for configuration reviews. AutoNessus is a free tool that can be used to automate Nessus scans.
- **hping.** Chapter 1 discusses the hping command and you can use it to send pings using TCP, UDP, or ICMP. You can also use it to scan systems for open ports on remote systems.
- **Sn1per.** Sn1per is a robust automated scanner used for vulnerability assessments and to gather information on targets during penetration testing. It combines the features of many common tools into a single application. It comes in two editions: Community and Professional. The Community edition performs vulnerability assessments, listing all discovered vulnerabilities and detailed information on the targets. The Professional edition also includes the ability to exploit the vulnerabilities.

- **Curl.** The Client URL command (curl) is used to transfer and retrieve data to and from servers, such as web servers. The Uniform Resource Locator (URL) is the address of a webpage. Penetration testers can use scripts to identify all of the URLs of a website and then use curl to retrieve all of the pages. Most websites prevent unauthorized personnel from posting data to them, but blocking curl requests isn't as easy.

Footprinting Versus Fingerprinting

Penetration testers often combine footprinting with fingerprinting techniques to identify targets. Network footprinting provides a big-picture view of a network, including the Internet Protocol (IP) addresses active on a target network. Fingerprinting then homes in on individual systems to provide details of each. This is similar to how fingerprints identify an individual.

Operating system fingerprinting identifies the operating system. For example, is this a Linux system or a Windows system? A fingerprinting attack sends protocol queries or port scans to a server and analyzes the responses. These responses can verify that a service is running and often include other details about the operating system because different operating systems often respond differently to specific queries. The “Network Scanners” section described how many scanners do this to identify operating systems.

It's worth noting that fingerprinting techniques are active. Intrusion detection systems (IDSs) and intrusion prevention systems (IPSs) can detect them and reduce port scanning and fingerprinting scans' success.

Remember this

Penetration tests include passive methods and active network reconnaissance and discovery methods. Passive reconnaissance uses open source intelligence methods, such as social media and an organization's website. Network reconnaissance and discovery methods use tools such as network scanners to gain information on the target.

Initial Exploitation

After scanning the target, testers discover vulnerabilities. They then take it a step further and look for a vulnerability that they can exploit. For example, a vulnerability scan may discover that a system doesn't have a patch installed for a known vulnerability. The vulnerability allows attackers (and testers) to remotely access the system and install malware on it.

With this knowledge, the testers can use known methods to exploit this vulnerability. This gives the testers full access to the system. They can then install additional software on the exploited system.

Persistence

Persistence is an attacker's ability to maintain a presence in a network for weeks, months, or even years without being detected. Penetration testers use similar techniques to maintain persistence within a network.

A common technique used to maintain persistence is to create a backdoor into the network. For example, a tester may create alternate accounts and access them remotely. It's also possible for testers or attackers to install or modify services to connect back into a system in some cases. For example, a tester may enable Secure Shell (SSH) and then create a method used to log on to a system using SSH.

Lateral Movement

When an attacker first exploits a user's computer, he has the credentials of the user. The attacker uses the credentials to access the targeted system and then uses the targeted system for lateral movement.

Lateral movement refers to the way attackers maneuver throughout a network. As an example, Windows Management Instrumentation (WMI) and PowerShell are frequently used to scan a Windows network.

After discovering other systems, the attacker looks for vulnerabilities and exploits them if possible. By exploiting multiple systems, the attacker has a better chance of maintaining persistence in a network.

Privilege Escalation

In many penetration tests, the tester first gains access to a low-level system or low-level account. For example, a tester might gain access to Homer's computer using Homer's user account. Homer has access to the network, but doesn't have any administrative privileges. However, testers

use various techniques to gain more and more privileges on Homer’s computer and his network.

Chapter 6 discusses ***privilege escalation*** tactics that attackers often use. The “One Click Lets Them In” section discusses how advanced persistent threats (APTs) often use remote access Trojans (RATs) to gain access to a single system. Attackers trick a user into clicking a malicious link, which gives them access to a single computer. Attackers then use various techniques to scan the network looking for vulnerabilities. By exploiting these vulnerabilities, the attackers gain more and more privileges on the network.

Penetration testers use similar tactics. Depending on how much they are authorized to do, testers can use other methods to gain more and more access to a network.

Pivoting

Pivoting is the process of using various tools to gain additional information. For example, imagine a tester gains access to Homer’s computer within a company’s network. The tester can then pivot and use Homer’s computer to gather information on other computers. Homer might have access to network shares filled with files on nuclear power plant operations. The tester can use Homer’s computer to collect this data and then send it back out of the network from Homer’s computer.

Testers (and attackers) can use pivoting techniques to gather a wide variety of information. Many times, the tester must first use privilege escalation techniques to gain more privileges. However, after doing so, the tester can access databases (such as user accounts and password databases), email, and any other type of data stored within a network.

Remember this

After exploiting a system, penetration testers use privilege escalation techniques to gain more access to target systems. Pivoting is the process of using an exploited system to target other systems.

Known, Unknown, and Partially Known Testing Environments

It's common to identify testing based on the testers' level of knowledge before starting the test. These testers could be internal employees or external security professionals working for a third-party organization hired to perform the test. Testing types are defined based on how much the testers know about the environment. The three types of testing are:

- **Unknown environment testing.** Testers have zero knowledge of the environment prior to starting an *unknown environment test* (sometimes called a black box test). Instead, they approach the test with the same knowledge as an attacker. When testing new applications, they wouldn't have any prior experience with the application. When testing networks, they aren't provided any information or documentation on the network before the test. These testers often use fuzzing to check for application vulnerabilities. This has been commonly called a black box test.
- **Known environment testing.** Testers have full knowledge of the environment before starting a *known environment test* (sometimes called a white box test). For example, they would have access to product documentation, source code, and possibly even logon details.
- **Partially known environment testing.** Testers have some knowledge of the environment prior to starting a *partially known environment test* (sometimes called a gray box test). For example, they might have access to some network documentation but not know the full network layout.

Remember this

Unknown environment testers have zero prior knowledge of a system prior to a penetration test. Known environment testers have full knowledge of the environment, and partially known environment testers have some knowledge.

Cleanup

Cleanup is one of the last steps of a penetration test. It includes removing all traces of the penetration tester's activities. Of course, this is

dependent on what the penetration tester did during the test and the rules of engagement. Cleanup activities include:

- Removing any user accounts created on systems in the network
- Removing any scripts or applications added or installed on systems
- Removing any files, such as logs or temporary files, created on systems
- Reconfiguring all settings modified by testers during the penetration test

This is an extensive list, and testers should not rely on their memory. Instead, it's common for testers to create a log of what they're doing as they're doing it. This makes it easier to reverse all their actions.

Bug Bounty Programs

A *bug bounty* program provides a monetary incentive for security researchers to discover bugs or vulnerabilities. One of the benefits is that bug bounty programs only pay researchers when they find vulnerabilities. Companies don't pay researchers for their time.

Some are open to the public, while other programs are by invitation only. This effectively creates a crowdsourced model of experts looking for vulnerabilities.

Intrusive Versus Non-Intrusive Testing

Scans can be either intrusive or non-intrusive. You can also think of these terms as invasive and non-invasive, respectively. Tools using intrusive methods can potentially disrupt the operations of a system. In contrast, tools using non-intrusive methods will not compromise a system. These terms also apply to penetration testing (intrusive) and vulnerability scanning (non-intrusive).

When comparing penetration testing and vulnerability scanning, it's important to remember that penetration tests are intrusive and more invasive than vulnerability scans. They involve probing a system and attempting to exploit any vulnerabilities they discover. If they successfully exploit a vulnerability, a penetration test can potentially disrupt services and even take a system down.

Vulnerability scans are generally non-intrusive and less invasive than penetration tests. They never attempt to exploit a vulnerability. Because of this, a vulnerability scan is much safer to run on a system or network because it is significantly less likely that it will affect services.

Remember this

A vulnerability scanner is passive and non-intrusive and has little impact on a system during a test. In contrast, a penetration test is active and intrusive, and can potentially compromise a system. A penetration test is more invasive than a vulnerability scan.

Exercise Types

Many organizations perform exercises to test their cybersecurity readiness. These can be competitions hosted as games or training events designed to help employees increase their knowledge and skills. These types of exercises typically have four teams identified by colors:

- **Red team.** The *red team* attacks. Personnel on a red team are experts in attacking systems, breaking into defenses, and exploiting vulnerabilities. They often use known tactics, techniques, and procedures (TTPs) of attackers to simulate actual attacks. They can be internal employees or experts hired from outside the organization.
- **Blue team.** The *blue team* defends. These are usually employees of the organization and they know about security controls used to protect network resources.
- **Purple team.** People on the *purple team* can do either red team or blue team activities.
- **White team.** *White team* personnel establish the rules of engagement for a test and oversee the testing.

Remember this

Red teams attack using known TTPs and blue teams defend against these attacks. Members of the purple team can perform as either red team members or blue team members. White team personnel set the rules and oversee testing.

Capturing Network Traffic

Several tools are available for use by security professionals and attackers alike. This chapter covered vulnerability scanners, including their use as ping scanners and port scanners. However, other tools are available. This section discusses tools used to capture network traffic.

Packet Capture and Replay

Packet capture refers to capturing network packets transmitted over a network, and packet replay refers to sending packets back out over the network. You can capture packets using a ***protocol analyzer***, which is sometimes called sniffing or using a sniffer.

Protocol analyzers provide administrators and attackers with the ability to analyze and modify packet headers and their payloads. They typically modify them before sending them back out as a packet replay. Administrators can use a protocol analyzer to troubleshoot communication issues between network systems or identify potential attacks using manipulated or fragmented packets.

Attackers can use a protocol analyzer to capture data sent across a network in cleartext. For example, unencrypted credentials are usernames and passwords sent across a network in cleartext. One of the ways attackers can view this data is by connecting an unauthorized switch within a network to capture traffic and forward it to a system running a protocol analyzer. If cabling isn't protected, they might be able to simply connect a switch above a drop-down ceiling. Wireshark is a free protocol analyzer that you can download from the Wireshark site: <https://www.wireshark.org/>.

Figure 8.3 shows the Wireshark protocol analyzer output after it captured packets transmitted over the network. It includes about 150 packets and has packet 121 selected in the top pane. The top pane shows the source and destination IP addresses and the Server Message Block (SMB) protocol. Many networks use SMB to send files over the network, and this packet includes the contents of that file. The middle pane shows details from this packet with the Internet Protocol version 4 header information partially expanded. The bottom pane shows the packet's entire contents (including the unencrypted credentials) displayed in hexadecimal and ASCII characters.

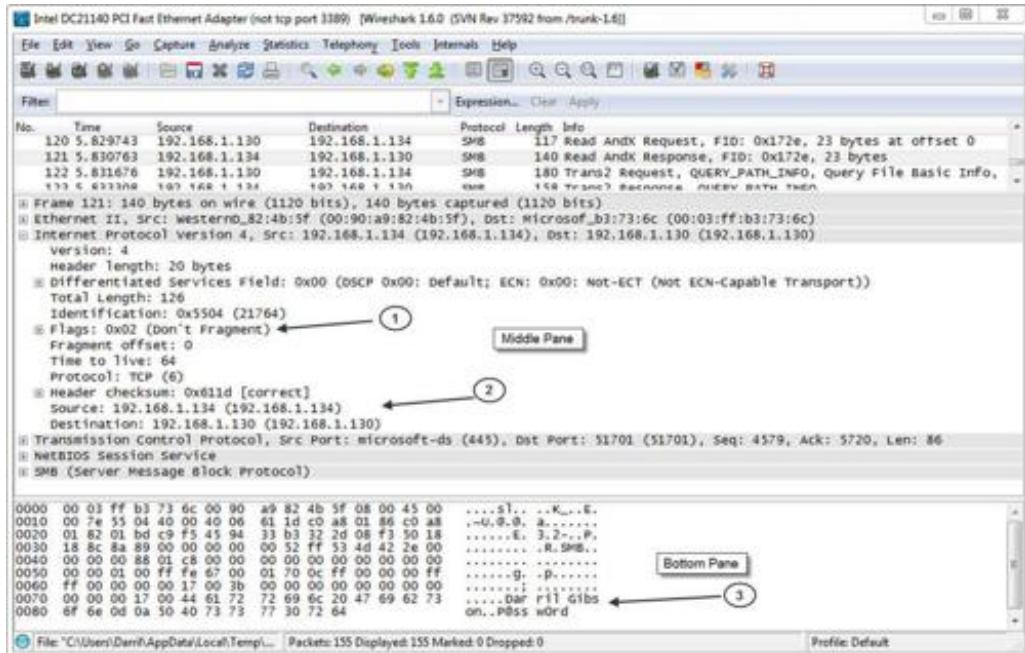


Figure 8.3: Wireshark capture

Although it can be tedious to analyze a packet capture, there is a lot of information in it for anyone willing to take the time to do so. Occasionally, attackers manipulate flags (arrow 1) within the headers for different types of attacks, and the protocol analyzer allows you to verify header manipulation attacks. You can also see the source and destination IP addresses (arrow 2) within the IP header field. You can expand the Ethernet II section to show the media access control (MAC) addresses of the source and destination computers.

Notice that you can view the unencrypted credentials—username (DarrilGibson) and password (P@ssw0rd)—in the bottom pane (arrow 3) because SMB sends it in cleartext. However, if an application encrypted the data before sending it across the network, it would not be readable.

Although this packet capture only includes about 150 packets, a packet capture can easily include thousands of packets. Wireshark includes filters that administrators use to focus on specific types of traffic. These filters also allow them to quantify the traffic. For example, they can determine the percentage of SMTP traffic or HTTPS traffic on the network.

In addition to seeing a capture using the Wireshark graphical interface, you can also view them as text files. The text file's information is usually filtered but normally includes the time, source information labeled as src,

destination information labeled as dst, and sometimes protocol information. Here's an example:

22:33:44, src 192.168.5.55:3389, dst 192.168.7.17:8080, syn/ack

The time is shown in a 24-hour clock as 10:33 p.m. and 44 seconds.

Notice the source and destination includes an IP address and a port number as a socket. It also shows you how you can identify the source of traffic. For example, if an attacker is manipulating or fragmenting packets as part of an attack, you can use the src IP address to identify the attack's potential source.

It's worth noting that the source IP address doesn't always identify the actual attacker. For example, attackers often take control of other computers and launch attacks from them without the owner's knowledge. Similarly, Port Address Translation (PAT) translates public and private IP addresses. If the traffic goes through a device using PAT, the protocol analyzer only captures the translated IP address, not the original IP address.

When using a protocol analyzer, you need to configure the network interface card (NIC) on the system to use promiscuous mode. Normally, a NIC uses non-promiscuous mode, and only processes packets addressed directly to its IP address. However, when you put it in promiscuous mode, it processes all packets regardless of the IP address. This allows the protocol analyzer to capture all packets that reach the NIC.

Remember this

Administrators use a protocol analyzer to capture, display, and analyze packets sent over a network. It is useful when troubleshooting communications problems between systems. It is also useful to detect attacks that manipulate or fragment packets. A capture shows information such as the type of traffic (protocol), flags, source and destination IP addresses, and source and destination MAC addresses. The NIC must be configured to use promiscuous mode to capture all traffic.

Tcpreplay and Tcpdump

Tcpreplay is a suite of utilities used to edit packet captures and then send the edited packets over the network. It includes tcpreplay, tcpprep, tcprewrite, and more. It is often used for testing network devices.

As an example, administrators can modify packets to mimic known attacks and then send them to an intrusion detection system (IDS). Ideally, an IDS should always detect a known attack and send an alert. Using tcpreplay, security administrators can prove that an IDS can detect specific attacks.

The ***tcpdump*** command is a command-line protocol analyzer. It allows you to capture packets like you can with Wireshark. The difference is that Wireshark is a Windows-based tool and tcpdump is executed from the command line. Many administrators use tcpdump to capture the packets and later use Wireshark to analyze the packet capture.

Kali Linux includes tcpdump, and as with most Linux command-line tools, tcpdump is case sensitive. You need to enter tcpdump in all lowercase. Additionally, the switches must be entered with the proper case. For example, -c (lowercase c) represents count and indicates the capture should stop after receiving the specified number of packets. However, -C (uppercase C) represents file size and indicates the maximum size (in millions of bytes) of a packet capture. When the file reaches this size, tcpdump closes it and starts storing packets in a new file. It's not available on Windows systems by default, but there are versions for Windows available for download.

NetFlow, sFlow, and IPFIX

NetFlow is a feature available on many routers and switches that can collect IP traffic statistics and send them to a NetFlow collector. The NetFlow collector receives the data and stores it, and analysis software on the NetFlow collector allows administrators to view and analyze the network activity.

Protocol analyzers like Wireshark allow you to capture and view all data, including headers and payloads of individual packets. In contrast, NetFlow doesn't include payload data and doesn't even include individual packet headers. Instead, a NetFlow record only shows counts, or statistics, related to data a device receives. Cisco created NetFlow, but several other vendors have adopted it.

NetFlow uses templates to identify what data to include in a NetFlow packet, but you'll typically see the following information:

- Timestamps identifying the start and finish time of the flow
- Input interface identifier (on router or switch)
- Output interface identifier (will be zero if a packet is dropped)
- Source information (source IP address and port number, if used)
- Destination information (destination IP address and port, if used)
- Packet count and byte count
- Protocol (such as TCP, UDP, ICMP, or any other Layer 3 protocol)

NetFlow packets report all traffic reaching the device. An alternative is ***sFlow***, a sampling protocol. It provides traffic information based on a preconfigured sample rate. For example, it may capture 1 packet out of every 10 packets it receives and send this sampled data count to the sFlow collector. Because sFlow only captures and sends samples of the data, it is less likely to impact the device's performance, allowing it to work on devices with a high volume of data.

IP Flow Information Export (IPFIX) is very similar to NetFlow v9. Analysis software installed on collectors typically support both protocols. The IETF created an informational document (RFC 3954, “Cisco Systems NetFlow Services Export Version 9”) to describe NetFlow, but it isn't on a standards track. Instead, the IETF created two RFCs to describe the IP Flow Information Export (IPFIX) Protocol, as a replacement for NetFlow. RFC

5101 “Specification of the IP Flow Information Export (IPFIX) Protocol” and RFC 5102 “Information Model for IP Flow Information Export” were derived from RFC 3954.

Because IPFIX is a proposed standard, the IETF can make changes to it as needed. In contrast, Cisco created NetFlow and updates it.

Understanding Frameworks and Standards

A ***framework*** is a structure used to provide a foundation.

Cybersecurity frameworks typically use a structure of basic concepts, and they provide guidance to professionals on how to implement security in various systems. There are multiple frameworks available that describe best practices and provide instructions on how to secure systems. The following sections document many of them.

Some frameworks and standards only apply to specific industries. As an example, organizations that handle credit cards typically comply with the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS includes 12 requirements and over 220 subrequirements that organizations follow to protect credit card data. PCI DSS isn't foolproof, but it has helped reduce many of the risks associated with credit card fraud.

Key Frameworks

Frameworks provide organizations with structure and methodologies they can use to protect cybersecurity assets. This section describes some frameworks.

The International Organization for Standardization (ISO) is an independent organization that establishes standards. They develop standards for a wide variety of industrial and commercial applications, and some directly address cybersecurity topics. However, these documents are not available for free but must be purchased online. In contrast, documents created by NIST are all free to download and use. The following list shows some standards relevant to cybersecurity.

- **ISO 27001.** ISO 27001, “Information Security Management,” provides information on information security management system (ISMS) requirements. Organizations that implement the ISMS requirements can go through a three-stage certification process, indicating they are ISO 27001 compliant.
- **ISO 27002.** ISO 27002, “Information Technology Security Techniques,” is a complement to ISO 27001. While ISO 27001 identifies the requirements to become certified, ISO 27002 provides organizations with best practices guidance.
- **ISO 27701.** ISO 27701, “Privacy Information Management System (PIMS),” is based on ISO 27001, and it outlines a framework for managing and protecting Personally Identifiable Information (PII). It provides organizations with guidance to comply with global privacy standards, such as the European Union General Data Protection Regulation (EU GDPR).
- **ISO 31000.** ISO 31000 is a family of standards related to risk management. It provides guidelines that organizations can adopt to manage risk.

The Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA) has published several auditing standards. The Statement on Standards for Attestation Engagements (SSAE) provides organizations and auditors with guidance on creating various reports.

While many of these reports are focused on financial reporting, the System and Organization Controls (SOC) 2 report covers organizational cybersecurity controls. The auditor creates the SOC 2 report after evaluating an organization's security controls. The SOC 2 report indicates that the organization is SOC 2 compliant and gives customers a level of assurance that the organization has adequate security controls in place. SOC 2 addresses five trust service principles: confidentiality, integrity, availability, security, and privacy. There are two versions of this report:

- **SOC 2 Type I.** The Type I report describes an organization's systems and covers the design effectiveness of security controls on a specific date, such as March 30. In this context, *design* effectiveness refers to how well the security controls address the risks, but not necessarily how well they work when mitigating risks.
- **SOC 2 Type II.** The Type II report describes an organization's systems and covers security controls' operational effectiveness over a range of dates, such as 12 months. In this context, *operational* effectiveness refers to how well the security controls worked when mitigating risks during the range of dates. Soc 2 Type 2 compliance gives a higher level of assurance than SOC 2 Type I.

The Center for Internet Security (CIS) has a stated mission to "identify, develop, validate, promote, and sustain best practice solutions for cyber defense and build and lead communities to enable an environment of trust in cyberspace." They provide several free downloads outlining best practices and maintain up-to-date information on cybersecurity threats. Members include corporations, government agencies, and academic institutions and members have access to additional CIS resources.

Risk Management Framework

NIST SP 800-37, “Risk Management Framework for Information Systems and Organizations,” covers the Risk Management Framework (RMF). While U.S. federal government agencies must adopt the RMF, many private sector organizations adopt it as well. RMF provides organizations with a seven-step process to identify and mitigate risks. The seven steps are:

- **Prepare.** During this step, an organization identifies key roles for implementing the framework, identifies risk tolerance strategies, updates (or creates) risk assessments, and identifies in-place controls. It also creates a continuous monitoring strategy.
- **Categorize information systems.** Personnel determine the adverse impact to operations and assets if there is a loss of confidentiality, integrity, and availability to these operations or assets. This allows them to prioritize the systems.
- **Select security controls.** Personnel select and tailor the controls necessary to protect their operations and assets. They typically start with baselines and then tailor the baselines as needed.
- **Implement security controls.** In this step, personnel implement the selected controls. If changes are required, personnel document them.
- **Assess security controls.** Next, personnel assess the controls to see if they are producing the desired outcome. This includes verifying they are implemented correctly and operating as expected.
- **Authorize information systems.** A senior management official determines if the system is authorized to operate. The official makes this decision based on the output of the previous steps. Government agencies place a higher emphasis on this step than private organizations.
- **Monitor security controls.** Monitoring is an ongoing step where personnel constantly assess changes in the system and environment. This typically includes performing periodic risk assessments and analyzing risk responses.

The NIST Cybersecurity Framework (CSF) aligns with the RMF. Many private sector organizations have adopted it to improve their ability to

prevent, detect, and respond to cyberattacks.

The CSF includes three components:

- **Framework core.** The core is a set of activities that an organization can select to achieve desired outcomes. It includes five functions: identify, protect, detect, respond, and recover.
- **Framework implementation tiers.** The tiers help an organization identify how it views risk. The four tiers are Partial (Tier 1), Risk Informed (Tier 2), Repeatable (Tier 3), and Adaptive (Tier 4). Tier 4 is the highest and indicates the organization has (or desires) a mature risk management program.
- **Framework profiles.** The profiles provide a list of outcomes for an organization based on its needs and risk assessments. Current profiles describe the current state of cybersecurity activities, and target profiles describe the desired outcomes. By comparing current profiles with target profiles, an organization can identify gaps in its risk management program. Organizations can use different profiles for different systems based on their value.

Remember this

When using credit cards, a company would comply with the Payment Card Industry Data Security Standard (PCI DSS). Many organizations use the Risk Management Framework (RMF) and the Cybersecurity Framework (CMF) to identify and mitigate risks.

Reference Architecture

In cybersecurity, ***reference architecture*** is a document or set of documents that provides a set of standards. As an example, a software reference architecture documents high-level design decisions. It may stress the need to create reusable modules and follow a specific standard related to interfaces. Some software reference architecture documents list procedures, functions, and methods that a software project should use.

You won't find a single reference architecture that meets the needs of all projects. Instead, the key is that complex projects often use one to standardize everyone's efforts on a project.

Exploitation Frameworks

An exploitation framework is a tool used to store information about security vulnerabilities. It is often used by penetration testers (and attackers) to detect and exploit software. Exploitation frameworks typically include tools used to check for vulnerabilities and execute exploits on any discovered vulnerabilities. Chapter 4, “Securing Your Network,” discusses intrusion detection systems (IDSs) and many IDSs use information from an existing framework to detect attacks. Some commonly used exploitation frameworks are:

- **Metasploit Framework.** Metasploit is an open source project that runs on Linux systems. It has data on over 1,600 exploits and includes methods to develop, test, and use exploit code. Rapid7 acquired Metasploit in 2009. Although the framework is still free and open source, there are more advanced editions available for purchase.
- **BeEF (Browser Exploitation Framework).** BeEF is an open source web browser exploitation framework. It focuses on identifying web browser vulnerabilities. Successful attacks allow testers (and attackers) to launch attacks from within an exploited web browser.
- **w3af (Web Application Attack and Audit Framework).** This open source framework focuses on web application vulnerabilities. The stated goal is to find and exploit all web application vulnerabilities and make this information known to others. Web application developers can then ensure their web applications are not vulnerable to the exploits.

Benchmarks and Configuration Guides

In addition to frameworks, you can also use various guides to increase security. This includes benchmarks or secure configuration guides, platform- or vendor-specific guides, and general-purpose guides. On the surface, this is quite simple. When configuring Windows systems, use a Windows guide to identify secure settings. When configuring Linux systems, use a Linux guide.

Additionally, when configuring a specific role system (such as a web server, application server, or network infrastructure device), follow the appropriate guide for that role. As an example, a web server would need ports 80 and 443 open for HTTP and HTTPS, respectively. However, a database application server would not typically need these ports open, so they should be closed on a database application server. The individual guides for each of the roles provide this information.

Chapter 8 Exam Topic Review

When preparing for the exam, make sure you understand these key concepts covered in this chapter.

Understanding Risk Management

- A risk is the likelihood that a threat will exploit a vulnerability. A threat is a potential danger that can compromise confidentiality, integrity, or availability. A vulnerability is a weakness in software or hardware or a weakness in a process that a threat could exploit, resulting in a security breach.
- Impact refers to the magnitude of harm that can be caused if a threat exploits a vulnerability.
- Risk management attempts to reduce risk to a level that an organization can accept, and the remaining risk is known as residual risk. Senior management is responsible for managing risk and the losses associated from residual risk.
- You can avoid a risk by not providing a service or participating in a risky activity. Purchasing insurance, such as fire insurance, transfers the risk to another entity. Cybersecurity controls mitigate or reduce risks. When the cost of a control outweighs a risk, it is common to accept the risk.
- A risk assessment quantifies or qualifies risks based on different values or judgments. It starts by identifying asset values and prioritizing high-value items.
- Quantitative risk assessments use numbers, such as costs and asset values. The single loss expectancy (SLE) is the cost of any single loss. The annual rate of occurrence (ARO) indicates how many times the loss will occur annually. You can calculate the annual loss expectancy (ALE) as $SLE \times ARO$.
- Qualitative risk assessments use judgments to prioritize risks based on likelihood of occurrence and impact. These judgments provide a subjective ranking.
- Risk assessment results are sensitive. Only executives and security professionals should be granted access to risk assessment reports.

- A risk register is a detailed document listing information about risks. It typically includes risk scores along with recommended security controls to reduce the risk scores. A risk matrix plots risks on a graph, and a heat map uses colors on the graph.
- A supply chain assessment evaluates a supply chain needed to produce and sell a product. It includes raw materials and all the processes required to create and distribute a finished product.
- Threat hunting is the process of actively looking for threats within a network before an automated tool detects and reports on the threat.

Comparing Scanning and Testing Tools

- A port scanner scans systems for open ports and attempts to discover what services and protocols are running on a system.
- Vulnerability scanners passively test security controls to identify vulnerabilities, a lack of security controls, and common misconfigurations. They are effective at discovering systems susceptible to an attack without exploiting the systems.
- A false positive from a vulnerability scan indicates the scan detected a vulnerability, but the vulnerability doesn't exist. A false negative indicates a vulnerability exists, but the scanner did not detect it.
- Credentialled scans run under an account's context and can get more detailed information on targets, such as the software versions of installed applications. They are also more accurate than non-credentialled scans, giving fewer false positives.
- Penetration testers should gain consent prior to starting a penetration test. A rules of engagement document identifies the boundaries of the test.
- A penetration test is an active test that attempts to exploit discovered vulnerabilities. It starts with a vulnerability scan and then bypasses or actively tests security controls to exploit vulnerabilities.
- Passive reconnaissance gathers information from open source intelligence. Active network reconnaissance and discovery uses scanning techniques to gather information.

- After initial exploitation, a penetration tester uses privilege escalation techniques to gain more access. Pivoting during a penetration test is the process of using an exploited system to access other systems.
- In unknown environment testing, testers perform a penetration test with zero prior knowledge of the environment. Known environment testing indicates that the testers have full knowledge of the environment, including documentation and source code for tested applications. Partially known environment testing indicates testers have some knowledge of the environment.
- Scans can be either intrusive or non-intrusive. Penetration testing is intrusive (also called invasive) and can potentially disrupt operations. Vulnerability testing is non-intrusive (also called non-invasive).
- Exploitation frameworks store information about security vulnerabilities. They are often used by penetration testers (and attackers) to detect and exploit software.
- Red teams attack using known TTPs and blue teams defend against these attacks. Members of the purple team can perform as either red team members or blue team members. White team personnel set the rules of engagement and oversee testing during an exercise.

Capturing Network Traffic

- Protocol analyzers (sniffers) can capture and analyze data sent over a network. Testers (and attackers) use protocol analyzers to capture cleartext data sent across a network.
- Administrators use protocol analyzers for troubleshooting communication issues by inspecting protocol headers to detect manipulated or fragmented packets.
- Captured packets show the type of traffic (protocol), source and destination IP addresses, source and destination MAC addresses, and flags.
- Tcpdump is a suite of utilities used to edit packet captures and then send the edited packets over the network. Tcpreplay is a command-line protocol analyzer. Captured packet files can be analyzed in a graphical protocol analyzer such as Wireshark.

- NetFlow captures IP traffic statistics on routers and switches and sends them to a NetFlow collector. You can capture a sample of NetFlow traffic using sFlow. Cisco created and maintains NetFlow. IPFIX is an IETF standard based on NetFlow.

Understanding Frameworks and Standards

- Frameworks are references that provide a foundation. Cybersecurity frameworks typically use a structure of basic concepts and provide guidance on how to implement security.
- Organizations that handle credit cards typically comply with the Payment Card Industry Data Security Standard (PCI DSS).
- Vendor-specific guides should be used when configuring specific systems.

Online References

- Don't forget to check out the online resources. They include additional free practice test questions, labs, and other resources to help you pass the CompTIA Security+ exam. You can access them at <https://greatadministrator.com/601-extras>.

Chapter 8 Practice Questions

1. A server within your organization has suffered six hardware failures in the past year. IT management personnel have valued the server at \$4,000, and each failure resulted in a 10 percent loss. What is the ALE?
 - A. \$400
 - B. \$2,400
 - C. \$4,000
 - D. \$6,000

2. Maggie is performing a risk assessment on a database server. While doing so, she created a document showing all the known risks to this server, along with the risk score for each risk. Which of the following BEST identifies the name of this document?
 - A. Qualitative risk assessment
 - B. Quantitative risk assessment
 - C. Risk register
 - D. Residual risk

3. Your organization hosts an e-commerce website used to sell digital products. You are tasked with evaluating all the elements used to support this website. What are you performing?
 - A. Quantitative assessment
 - B. Qualitative assessment
 - C. Threat hunting
 - D. Supply chain assessment

4. Which of the following elements are used as part of threat hunting?
(Choose two.)
 - A. Intelligence fusion
 - B. Vulnerability scan
 - C. Advisories and bulletins
 - D. Configuration review

5. Maggie suspects that a server may be running unnecessary services. Which of the following tools is the BEST choice to identify the services running on the server?

- A. Dnsenum
- B. IP scanner
- C. Passive reconnaissance
- D. Nmap

6. You want to identify all the services running on a server in your network. Which of the following tools is the BEST choice to meet this goal?

- A. Penetration test
- B. Protocol analyzer
- C. Non-credentialed scan
- D. Port scanner

7. You recently completed a vulnerability scan on a database server. The scan didn't report any issues. However, you know that it is missing a patch. The patch wasn't applied because it causes problems with the database application. Which of the following BEST describes this?

- A. False negative
- B. False positive
- C. Credential scan
- D. Non-credentialed scan

8. You suspect that a database server used by a web application is not up to date with current patches. Which of the following is the BEST action to take to verify the server has up-to-date patches?

- A. Network scan
- B. Port scan
- C. Protocol analyzer
- D. Vulnerability scan

9. Lisa periodically runs vulnerability scans on the organization's network. Lately, she has been receiving many false positives. Which of the following actions can help reduce the false positives?

- A. Run the scans as credentialed scans.

- B. Run the scans as non-credentialed scans.
- C. Run the scans using passive reconnaissance.
- D. Run the scans using active reconnaissance.

10. Your organization has hired outside penetration testers to identify internal network vulnerabilities. After successfully exploiting vulnerabilities in a single computer, the testers attempt to access other systems within the network. Which of the following BEST describes their current actions?

- A. Partially known environment testing
- B. Persistence
- C. Lateral movement
- D. Privilege escalation

11. Bart, a database administrator in your organization, told you about recent attacks on the network and how they have been disrupting services and network connectivity. In response, he said he has been using Nmap to run vulnerability scans and identify vulnerabilities. Which of the following is wrong with this scenario?

- A. The database administrator was pivoting from his primary job.
- B. A network scan wasn't done first.
- C. Scans weren't done as credentialed scans.
- D. Rules of engagement weren't obtained.

12. Your organization outsourced the development of a software module to modify an existing proprietary application's functionality. The developer completed the module and is now testing it with the entire application.
What type of testing is the developer performing?

- A. Known environment
- B. Unknown environment
- C. Partially known environment
- D. Red team

13. The IT department at your organization recently created an isolated test network that mimics the DMZ. They then hired an outside company to perform a simulated cyberattack on this isolated test network as part of a

testing campaign. Which of the following BEST describes the role of personnel from the outside company?

- A. Red team
- B. Blue team
- C. Purple team
- D. White team

14. Your organization is setting up an e-commerce site to sell products online. Management wants to ensure the website can accept credit cards for payment. Which of the following standards are they MOST likely to follow?

- A. ISO 27001
- B. PCI DSS
- C. ISO 31000
- D. SSAE SOC 2 Type I

15. Your organization recently purchased and deployed an IDS within the network. Security administrators want to verify it will detect a syn stealth scan. Which of the following tools will BEST meet your need?

- A. Tcpreplay
- B. Tcpdump
- C. Wireshark
- D. Netcat

Chapter 8 Practice Question Answers

1. **B** is correct. The annual loss expectancy (ALE) is \$2,400. It is calculated as single loss expectancy (SLE) × annual rate of occurrence (ARO). Each failure has resulted in a 10 percent loss (meaning that it cost 10 percent of the asset value to repair it). The SLE is 10 percent of \$4,000 (\$400), and the ARO is 6. $6 \times \$400$ is \$2400.
2. **C** is correct. A risk register lists all known risks for an asset, such as a database server, and it typically includes a risk score (the combination of the likelihood of occurrence and the impact of the risk). Risk assessments (including qualitative and quantitative risk assessments) might use a risk register, but they are not risk registers. Residual risk refers to the remaining risk after applying security controls to mitigate a risk.
3. **D** is correct. A supply chain assessment evaluates all the elements used to create, sell, and distribute a product. The National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) (NIST SP 800-37 r2) provides steps for reducing supply chain risks. Risk assessments (including both quantitative and qualitative risk assessments) evaluate risks, but don't evaluate the supply chain required to support an e-commerce website. Threat hunting is the process of actively looking for threats within a network before an automated tool detects and reports on the threat.
4. **A** and **C** are correct. Intelligence fusion and advisories and bulletins are part of threat hunting. Threat hunting is the process of actively looking for threats within a network before an automated tool detects and reports on the threat. Vulnerability scans are used as part of a security assessment. Although a history of vulnerability scans and related logs may be part of the intelligence fusion, CompTIA objectives specifically list the following four elements: intelligence fusion, advisories and bulletins, threat feeds, and predictions of how attackers may maneuver through the network. A configuration review verifies that systems are configured correctly.

5. **D** is correct. Nmap is a network scanner, and it can detect the protocols and services running on a server. The **dnsenum** command will enumerate (or list) Domain Name System (DNS) records for domains. An IP scanner detects IPs active on a network but not the services running on the individual hosts. Passive reconnaissance uses open source intelligence (OSINT) instead of active tools.
6. **D** is correct. A port scanner identifies open ports on a system and is commonly used to determine what services are running on the system. Vulnerability scanners often include port-scanning capabilities, and they can help identify potential weak configurations. A penetration test attempts to exploit a vulnerability. A protocol analyzer can analyze traffic and discover protocols in use, but this would be much more difficult than using a port scanner. A non-credentialed scan refers to a vulnerability scan, and while a vulnerability scan may reveal services running on a server, it won't be as specific as a port scan.
7. **A** is correct. A false negative occurs if a vulnerability scanner does not report a known vulnerability. A false positive occurs when a vulnerability scanner reports a vulnerability that doesn't exist. The scenario doesn't indicate if the scan was run under the context of an account (credentialed) or anonymously (non-credentialed), so these answers aren't relevant to the question.
8. **D** is correct. A vulnerability scan determines if the system has current patches. None of the other answers will detect missing patches. A network scan will discover devices on the network. It might look for and detect vulnerabilities on network devices, but it would not be used to scan a single server for patches. A port scan identifies open ports. A protocol analyzer (sniffer) captures traffic for analysis.
9. **A** is correct. Running the scans as credentialed scans (within the context of a valid account) allows the scan to see more information and typically results in fewer false positives. A false positive indicates the scan reported a vulnerability that doesn't exist. Non-credentialed scans run without any user

credentials and can be less accurate. Choosing either passive or active scans won't reduce false positives.

10. **C** is correct. Lateral movement refers to actions taken to move through a network after successfully exploiting a single system. While not available as a possible answer, this could also be described as pivoting, which is the process of accessing other systems through a single compromised system. Partially known environment testing (sometimes called gray box testing) indicates the testers have some knowledge of a system or network before starting, but there is no indication in the scenario about their level of knowledge. Persistence refers to maintaining a presence on the system or network after the initial exploit. Privilege escalation refers to gaining higher privileges after an initial exploit.

11. **D** is correct. Bart should have gotten authorization before doing any scans, and the authorization should outline the rules of engagement. Pivoting refers to an attacker accessing other systems in a network through a single compromised system. While Bart is a database administrator and doing vulnerability scans is outside his normal job functions, his actions wouldn't be described as pivoting. Nmap can do a network scan. The scenario doesn't indicate the scans were credentialed or non-credentialed or what they should have been.

12. **C** is correct. The developer is performing a partially known environment test (sometimes called a gray box test). A partially known environment tester has some knowledge of the application. In this scenario, the tester needs some knowledge of the application (such as input and output data) to develop and test the module. Known environment testers (sometimes called white box testers) have full knowledge about the product or network they are testing, but because this is a proprietary application, it is unlikely the tester has full knowledge. Unknown environment testers (sometimes called black box testers) do not have any knowledge about the product or network they are testing, but this isn't feasible for a developer who needs to develop and test a module to modify an existing application. Red team refers to an exercise type and members on the red team are experts in attacking systems.

13. **A** is correct. A red team attacks and many cybersecurity companies have red teams that can be hired to perform simulated attacks on networks such as a simulated demilitarized zone (DMZ). A blue team defends, and members are usually employees of the organization. A purple team is composed of people who can perform either red team testing or blue team testing. White team personnel oversee testing campaigns and establish the rules of engagement.

14. **B** is correct. When using credit cards, a company would comply with the Payment Card Industry Data Security Standard (PCI DSS). International Organization for Standardization (ISO) 27001 provides information on information security management system (ISMS) requirements. ISO 31000 is a family of standards related to risk management. A Statement on Standards for Attestation Engagements (SSAE) System and Organization Controls (SOC) 2 Type I report describes an organization's systems and covers the design effectiveness of security controls on a specific date.

15. **A** is correct. Tcpreplay is a suite of utilities used to edit packet captures and resend them. It can be used to modify a packet capture to mimic known attacks such as a syn stealth scan. A syn stealth scan finds active hosts on a network by sending a SYN (synchronize) packet to an IP address to initiate a Transmission Control Protocol (TCP) session, waits for a SYN/ACK (synchronize/acknowledge) packet to verify the IP address is in use, and then sends a RST (reset) packet to cancel the TCP handshake. The **tcpdump** command-line tool is a command-line packet analyzer (or protocol analyzer) and its primary purpose is to capture packets. Wireshark is a graphic-based packet analyzer used to capture packets, but it doesn't send packets. Netcat is useful for remotely accessing systems, but it doesn't capture or replay packets.

Chapter 9

Implementing Controls to Protect Assets

CompTIA Security+ objectives covered in this chapter:

.2 Given a scenario, analyze potential indicators to determine the type of attack.

- Physical attacks (Malicious universal serial bus (USB) cable, Malicious flash drive, Card cloning, Skimming)

.1 Explain the importance of security concepts in an enterprise environment.

- Data sovereignty, Geographical considerations, Site resiliency (Hot site, Cold site, Warm site)

.5 Given a scenario, implement cybersecurity resilience.

- Redundancy (Geographic dispersal), Disk (Redundant array of inexpensive disks (RAID) levels, Multipath), Network (Load balancers, Network interface card (NIC) teaming, Power (Uninterruptible power supply (UPS), Generator, Dual supply, Managed power distribution units (PDUs)), Replication (Storage area network))
- Backup types (Full, Incremental, Snapshot, Differential, Tape, Disk, Copy, Network attached storage (NAS), Storage area network, Cloud, Image, Online vs. offline, Offsite storage (Distance considerations))
- High availability (Scalability), Restoration order, Diversity (Technologies, Vendors, Controls)

.7 Explain the importance of physical security controls.

- Bollards/barricades, Badges, Alarms, Signage, Cameras (Motion recognition, Object detection), Closed-circuit television (CCTV), Industrial camouflage

- Personnel (Guards, Robot sentries, Reception, Two-person integrity/control)
- Locks (Biometrics, Electronic, Physical, Cable locks), Lighting, Fencing, Fire suppression
- Sensors (Motion detection, Noise detection, Proximity reader, Moisture detection, Cards, Temperature)
- Drones, Visitor logs, Faraday cages, Air gap, Protected cable distribution
- Secure areas (Air gap, Vault, Safe, Hot aisle, Cold aisle)

.3 Given a scenario, implement secure network designs.

- Load balancing (Active/active, Active/passive, Scheduling, Virtual IP, Persistence)

.2 Summarize the importance of policies, processes, and procedures for incident response.

- Exercises (Tabletop, Walkthroughs, Simulations)
- Disaster recovery plan, Business continuity plan, Continuity of operation planning (COOP)

.1 Compare and contrast various types of controls.

- Control type (Physical)

.3 Explain the importance of policies to organizational security.

- Organizational policies (Asset management)

.4 Summarize risk management processes and concepts.

- Disasters (Environmental, Person-made, Internal vs. external)
- Business impact analysis (Recovery time objective (RTO), Recovery point objective (RPO), Mean time to repair (MTTR), Mean time between failures (MTBF), Functional recovery plans, Single point of failure, Disaster recovery plan (DRP), Mission essential functions, Identification of critical systems, Site risk assessment)

**

You can't eliminate risk to an organization's assets. However, you can reduce the impact of many threats by implementing security controls. It's common to implement several controls using a layered strategy with a diverse assortment of controls, vendors, and technologies. Physical security controls help protect access to secure areas. Redundancy and fault-tolerance

strategies help eliminate single points of failure for critical systems. Backups ensure that data remains available even after data is lost. More in-depth business continuity strategies help ensure mission-critical functions continue to operate even if a disaster destroys a primary business location. This chapter covers these concepts.

Comparing Physical Security Controls

A physical security control is something you can physically touch, such as a hardware lock, a fence, an identification badge, and a security camera. Physical security access controls attempt to control entry and exits, and organizations commonly implement different controls at different boundaries, such as the following:

- **Perimeter.** Military bases and many other organizations erect a fence around the entire perimeter of their land. They often post security guards at gates to control access. In some cases, organizations install barricades to block vehicles.
- **Buildings.** Buildings commonly have additional controls for both safety and security. For example, guards and locked doors restrict entry so only authorized personnel enter. Many buildings include lighting and video cameras to monitor the entrances and exits.
- **Secure work areas.** Some companies restrict access to specific work areas when employees perform classified or restricted access tasks. In some cases, an organization restricts access to all internal work areas. In other words, visitors can enter the lobby of a building, but they are not able to enter internal work areas without an escort.
- **Server rooms.** Servers and network devices such as routers and switches are normally stored in areas where only the appropriate IT personnel can access them. These spaces may be designated as server rooms or wiring closets. It's common for an organization to provide additional physical security for these rooms to prevent attackers from accessing the equipment. For example, locking a wiring closet prevents an attacker from installing illicit monitoring hardware, such as a protocol analyzer, to capture network traffic.
- **Hardware.** Additional physical security controls protect individual systems. For example, server rooms often have locking cabinets to protect servers and other equipment installed in the equipment bays. Cable locks protect laptop computers, and smaller devices can be stored in safes.

Many organizations use camouflage techniques (sometimes called ***industrial camouflage***) to hide buildings, parts of a building, and a wide variety of other items. Generically, camouflage is the use of materials to conceal items or disguise them as something else.

Landscaping can camouflage a building or parts of it. Imagine a strong security fence surrounds an organization. Organizations can conceal it with landscaping such as tall bushes, ornamental grasses, or perennials. This provides aesthetic benefits and obscures the fact that the organization has invested in such a strong security fence.

As another example, phone cell towers in Arizona have been hidden inside fake cactus plants since 2009 or earlier. Some cell towers look like palm trees in the south, and some northern locations use fake pine trees. As the next generation of wireless rolls out (5G), this is no longer efficient, so telecommunications companies are working with cities and utility companies to install the 5G hardware on street lights.

Securing Door Access with Cards

It's possible to secure access to areas with proximity cards or smart cards. ***Proximity cards*** are small credit card-sized cards that activate when they are close to a proximity card reader. Many organizations use these for access points, such as the entry to a building or the entry to a controlled area within a building. The door uses an electronic lock that only unlocks when the user passes the proximity card in front of a card reader.

Similarly, it's possible to use smart cards or physical tokens (described in Chapter 2, "Understanding Identity and Access Management") for door access. In some scenarios, the smart cards include proximity card electronics. In other scenarios, users must insert the smart card into a smart card reader to gain access.

You've probably seen proximity card readers implemented with credit card readers. Many self-serve gasoline stations and fast-food restaurants use them. Instead of swiping your credit card through a magnetic reader, you simply pass it in front of the reader (in close proximity to the reader), and the reader extracts your credit card's information.

These are becoming popular elsewhere, too. For example, if you stay at a Walt Disney World property, they can issue you a bracelet that includes a proximity card's functionality. To enter your hotel room, you wave your bracelet in front of the door. If you want to buy food or souvenirs or pay for almost anything, you can simply wave your bracelet in front of a card reader to complete your purchase.

The card (and bracelet) doesn't require its own power source. Instead, the electronics in the card include a capacitor and a coil that can accept a charge from the proximity card reader. When you pass the card close to the reader, the reader excites the coil and stores a charge in the capacitor. Once charged, the card transmits the information to the reader using a radio frequency. When used with door access systems, the proximity card can send just a simple signal to unlock the door. Some systems include details on the user and record when the user enters or exits the area. When used this way, it's common to combine the proximity card reader with a keypad requiring the user to enter a personal identification number (PIN). This

identifies and authenticates the user with multifactor authentication. The user has something (the proximity card) and knows something (a PIN).

Many organizations use proximity cards with turnstiles to provide access for a single person at a time. These are the same type of turnstiles used as entry gates in subways, stadiums, and amusement parks.

Remember this

Proximity cards are credit card-sized access cards. Users pass the card near a proximity card reader, and the card reader then reads data on the card. Some access control points use proximity cards with PINs for authentication.

Comparing Locks

It's common to secure access to controlled areas of a building with locks, and there are many different lock types. A door access system is one that only opens after some access control mechanism is used. Some common door access systems are physical locks, electronic locks, biometric locks, and cable locks.

When implementing door access systems, it's important to limit the number of entry and exit points. As an example, if a data center has only one entrance and exit, it is much easier to monitor this single access point. You can control it with door locks, video surveillance, and guards. On the other hand, if the data center has two entry/exit points, you need another set of controls to control access in both places.

Another important consideration with door access systems is related to personnel safety and fire. In the event of a fire, door access systems should allow personnel to exit the building without any form of authentication.

Physical Locks

Physical locks are similar to what you use to secure your home, and they can secure buildings as well as rooms within buildings. Companies that don't have the resources to employ advanced security systems use these types of hardware locks.

As an example, it's easy to use physical locks to secure access to wiring closets or small server rooms to restrict access. Although these locks aren't as sophisticated as the ones used by large organizations, they are much better than leaving the rooms open and the equipment exposed.

Physical Cipher Locks

Physical cipher locks often have four or five buttons labeled with numbers. Employees press the numbers in a certain order to unlock the door. For example, the cipher code could be 1, 3, 2, 4. Users enter the code in the correct order to gain access. Cipher locks can be electronic or manual. An electronic cipher lock automatically unlocks the door after you enter the correct code into the keypad. A manual cipher lock requires the user to turn a handle after entering the code.

Many manual cipher locks include a code that requires two numbers entered at the same time. Instead of just 1, 3, 2, 4, the code could be 1/3 (pressed simultaneously), then 2, 4, 5. This adds complexity to the lock and reduces brute force attacks.

One challenge with cipher locks is that they don't identify the users. Further, uneducated users can give out the cipher code to unauthorized individuals without understanding the risks. Shoulder surfers might attempt to discover the code by watching users as they enter.

Biometric Locks

It's also possible to use biometric methods as an access control system. One of the benefits is that some biometric methods provide both identification and authentication. These systems can record who entered and when they entered a secure area.

For example, you can install a retina scanner at the entrance to a secure server room. When individuals want to enter, the biometric scanner identifies and authenticates them. It's essential to ensure you use an accurate biometric system and configure it to use a low false acceptance rate, as described in Chapter 2. Otherwise, it might falsely identify unauthorized individuals and grant them access.

Remember this

Door access systems include physical locks, cipher locks, and biometrics. Biometric locks can provide both the identification and authentication of users to track who entered a secure area and when they entered.

Cable Locks

Cable locks are a great theft deterrent for mobile computers and even many desktop computers at work. Computer cable locks work similarly to how a bicycle cable lock works. However, instead of securing a bicycle to a bike rack or post, a computer cable lock secures a computer to a piece of furniture.

The user wraps the cable around a desk, table, or something heavy and then plugs it into an opening in the laptop specifically created for this purpose. Most cable locks have a four-digit combo. If you (or anyone) remove the cable lock without the combo, it will likely destroy the laptop.

Another common use of cable locks is for computers in unsupervised labs. For example, you can secure laptop or desktop computers with cable locks in a training lab. This allows you to leave the room open so that students can use the equipment, but the cable locks prevent thieves from stealing the equipment.

Remember this

Physical locks can help prevent access to secure areas by unauthorized individuals. Cable locks are effective threat deterrents for small equipment such as laptops and some workstations. When used properly, they prevent losses due to theft of small equipment.

Increasing Security with Personnel

Many organizations use security guards to control access to buildings and secure spaces. If employees have ID badges, guards can check these badges before granting the employees access. Even if ID badges aren't used, guards can still verify people's identities using other identification. Similarly, the security guards can restrict access by checking people's identities against a preapproved access control list.

Security guards can also take a less-active role to deter security incidents. For example, a security guard can deter tailgating incidents by observing personnel when they use their proximity card to gain access to a secure area. Chapter 6, "Comparing Threats, Vulnerabilities, and Common Attacks," discusses tailgating. In some cases, guards record access in visitor logs. This provides a written record of any visitors.

Instead of guards, many organizations use a reception desk or reception area to control access. Visitors need to check in with the receptionist before they're allowed into secure areas. While receptionists aren't guards, they typically have easy access to security personnel with a quick phone call.

Robot sentries first made their appearance in military situations, such as the demilitarized zone between North and South Korea. They are now available to businesses and even homes, though not with the same armaments used in military applications. Some are stationary but guard the entry of secure spaces, recording all activity by people entering or leaving. Mobile robot sentries are starting to appear in large data centers. They use laser light detection sensors and 3D mapping to learn and navigate the environment, along with a variety of sensors to detect activity. They also include video and two-way audio so that security personnel can communicate with intruders from a remote security office.

Two-person integrity is a security control that requires the presence of at least two authorized individuals to perform tasks. The National Institute of Standards and Technology (NIST) online glossary mentions that "Two-Person Integrity refers only to the handling of COMSEC keying material." COMSEC is communications security, and keying material refers to the materials used to encrypt and decrypt classified communications. Two-

person integrity prevents any individual person to access COMSEC keying material.

A two-person control is similar, but it typically refers to nuclear command and control. The military uses this to prevent accidental launches of nuclear weapons. Many movies show this in action requiring two people to agree before they can launch.

Monitoring Areas with Cameras

Organizations are increasingly using security cameras in the workplace and surrounding areas for video surveillance. This includes areas outside of a building, such as a parking lot and all building entrances and exits. Additionally, many organizations use cameras to monitor entrances of high-security areas, such as the entrance of a data center or server room.

A closed-circuit television (CCTV) system transmits signals from video cameras to monitors that are similar to TVs. In addition to providing security, a CCTV system can also enhance safety by deterring threats.

Organizations often use video cameras within a work environment to protect employees and enhance security in the workplace. In addition to live monitoring, most systems include a recording element, and they can verify if someone is stealing the company's assets. By recording activity, videos can be played back later for investigation and even prosecution.

Video surveillance provides the most reliable proof of a person's location and activity. Digital access logs provide a record, but it's possible to circumvent these logs. For example, if Bart used your proximity card to access a secure space, the log will indicate you entered, not Bart. In contrast, if the video shows that Bart entered the room at a certain time of day, it's not easy for Bart to refute the video.

It's also possible to use a CCTV system as a compensating control. Imagine an organization wants to implement a door access system requiring users to use smart cards to enter secure areas. However, this may take months to implement. The organization can implement a CCTV system to record access until the card access system is installed.

Cameras can be connected to motion detection systems so that they only turn on when they detect motion. This can be effective as a burglary detection system.

Object detection uses camera images and software to detect specific objects. Some can detect still images, but it's more common for them to analyze frames to detect common objects' predictable movement. As an example, some cars use this to detect pedestrians walking into the path of a car.

Remember this

Video surveillance provides reliable proof of a person's location and activity. It can identify who enters and exits secure areas and can record theft of assets. Many cameras include motion detection and object detection capabilities. CCTV systems can be used as a compensating control in some situations.

Sensors

Many physical security controls use sensors to detect changes in an environment. It's common to use sensors with cameras, alarms, fire detection, and more. The following bullets describe many common sensors:

- **Motion detection.** Many organizations use a combination of automation, light dimmers, and motion sensors to save on electricity costs without sacrificing security. The lights automatically turn on at dusk but in a low, dimmed mode. When the motion sensors detect any movement, the lights turn on at full capacity, and they automatically turn off at dawn. Motion detection sensors can also trigger alarms. Of course, they are only enabled when an area is empty.
- **Noise detection.** Noise detection sensors can detect any noise or when noise exceeds a certain level. They work like motion detection sensors and alert on any sound to control lights or set off alarms. Some Airbnb hosts don't want renters throwing parties in their houses. They can use noise sensors to detect when the noise levels exceed a certain level. Some noise sensors can detect specific sounds, such as smoke alarms or the sound of glass breaking.
- **Temperature.** Heating, ventilation, and air conditioning (HVAC) systems have temperature and humidity controls to maintain proper temperature and humidity values. Computing systems need to be kept cool, and excessive humidity causes moisture. Some temperature sensors are tied into fire detection systems as a backup to smoke detection.
- **Moisture detection.** Some organizations are located within flood zones and use moisture detection methods to detect flood events. In some cases, they can turn on water pumps before the water causes damage. In other cases, they turn off equipment before the water reaches it.
- **Proximity reader.** Proximity cards are small credit card-sized cards that activate when they are close to a card reader. Many organizations use these with proximity readers for access points.

The door uses an electronic lock that only unlocks when the user passes the proximity card in front of a card reader.

- **Cards.** Some smart cards and badges include sensors that can also be used for access. Users insert the cards or badges into a reader instead of waving them in front of a proximity reader.

Remember this

Sensors monitor the environment and can detect changes. They can detect motion, noise, moisture, temperature changes, and more.

Fencing, Lighting, and Alarms

Fences provide a barrier around a property and deter people from entering. When using a fence, it's common to control access to the area via specific gates. Guards often monitor these gates and ensure only authorized individuals can enter. When additional security is required, organizations sometimes configure dual gates, allowing access into one area where credentials are checked before allowing full access. This effectively creates a cage preventing full access but also prevents unauthorized individuals from escaping.

Installing lights at all the entrances to a building can deter attackers from trying to break in. Similarly, lighting at the entrances of any internal restricted areas can deter people from trying to enter. Many organizations use a combination of automation, light dimmers, and motion sensors to save on electricity costs without sacrificing security. The lights automatically turn on at dusk, but in a low, dimmed mode. When the motion sensors detect any movement, the lights turn on at full capacity. They automatically turn off at dawn.

It's important to protect the lights. For example, if an attacker can remove the light bulbs, it defeats the control. Either place the lights high enough so that they can't be reached or protect them with a metal cage.

Alarms provide additional physical security protection. This includes alarms that detect fire and alarms that detect unauthorized access. Fire alarms detect smoke and/or heat and trigger fire suppression systems. Burglary prevention systems monitor entry points such as doors and windows, detecting when someone opens them.

You can also combine motion detection systems with burglary prevention systems. They detect movement within monitored areas and trigger alarms. Obviously, you wouldn't have motion detection systems turned on all the time. Instead, you'd turn them on when people will not be working in the area, such as during nights or weekends.

You might have noticed that fencing, lighting, and alarms can all be combined with motion detection. At the most basic level, motion detection methods detect moving objects. Many motion detectors use microwave

technologies to detect movement. This is similar to the technology used in some police radar speed guns.

A more advanced method is temperature detection using infrared detection. Infrared detectors sense infrared radiation, sometimes called infrared light, which effectively sees a difference between objects of different temperatures. As an example, a person is much warmer than objects in a room and easily stands out using an infrared detector. This can help eliminate false alarms by sensing more than just motion but motion from objects of different temperatures.

Remember this

Fencing, lighting, and alarms all provide physical security. They are often used together to provide layered security. Motion detection methods are also used with these methods to increase their effectiveness. Infrared detectors detect movement by objects of different temperatures.

Securing Access with Barricades

In some situations, fencing isn't enough to deter potential attackers. To augment fences and other physical security measures, organizations erect stronger barricades. As an example, military bases often erect strong, zigzag barricades that require vehicles to slow down to navigate through them. This prevents attackers from trying to ram through the gates.

Businesses and organizations need to present an inviting appearance, so they can't use such drastic barricades. However, they often use ***bollards***, which are short vertical posts composed of reinforced concrete and/or steel. They often place the bollards in front of entrances about three or four feet apart and paint them with colors that match their store so that they blend in. You've probably walked through a set of bollards multiple times without giving them a second thought. However, thieves who are contemplating driving a car or truck through the entrance see them.

Many thieves have driven vehicles right through the front of buildings and then proceeded to steal everything in sight. Depending on the walls' strength, criminals might even be able to drive through a wall with a truck. Strategically placed bollards will prevent these types of attacks.

Remember this

Barricades provide stronger barriers than fences and attempt to deter attackers. Bollards are effective barricades that can block vehicles.

Using Signage

A simple physical security control is signage. For example, an “Authorized Personnel Only” sign will deter many people from entering a restricted area. Similarly, “No Trespassing” signs let people know they shouldn’t enter. Of course, these signs won’t deter everyone, so an organization typically uses additional physical security measures.

Drones

Drones are small flying vehicles, sometimes called unmanned aerial vehicles (UAVs). Most drones have onboard cameras and include the ability to transmit images to operators. They are typically piloted by remote control, but sophisticated drones can use onboard computers. They can add to physical security, but they can also be physical security threats.

As an example of adding to physical security, drones can provide a bird's-eye view of an area to assess damage after a disaster. They can also observe potential threats in the area. For example, some fences include sensors that can detect suspicious activity, such as someone cutting the fence or climbing over it. Security personnel can launch a drone to observe the area.

Unfortunately, attackers can use drones, too. Attackers can use them to observe an area looking for vulnerabilities.

Asset Management

Asset management is the process of tracking valuable assets throughout their life cycles. For example, organizations commonly implement processes to track hardware such as servers, desktop computers, laptop computers, routers, and switches. An effective asset management system can help reduce several vulnerabilities:

- **Architecture and design weaknesses.** Asset management helps reduce architecture and design weaknesses by ensuring that purchases go through an approval process. The approval process does more than just compare costs. It also evaluates the purchase to ensure it fits in the overall network architecture. Unapproved assets often weaken security by adding in additional resources that aren't managed.
- **System sprawl and undocumented assets.** System sprawl occurs when an organization has more systems than it needs, and the systems it owns are underutilized. Asset management begins before the hardware is purchased and helps prevent system sprawl by evaluating the purchase. Additionally, after the purchase is completed, asset management processes ensure the hardware is added to the asset management tracking system. This ensures that the assets are managed and tracked from the cradle to the grave.

Many organizations use automated methods for inventory control. For example, radio-frequency identification (RFID) methods can track the movement of devices. These are the same types of devices used in stores to prevent shoplifting. If someone exits without paying, the RFID device transmits when the shoplifter gets close to the exit door and sounds an alarm. Organizations won't necessarily have an alarm, but they can track devices' movement by placing RFID tags on the equipment.

Mobile devices are easy to lose track of, so organizations often use asset-tracking methods to reduce losses. For example, when a user receives a mobile device, asset-tracking methods record it. Similarly, if the user leaves the company, asset-tracking methods ensure the user returns the device.

Chapter 6 discusses unauthorized systems known as shadow IT. An effective asset management system can help identify these unauthorized systems. As an example, if authorized devices have an RFID tag, the absence of one indicates the device may not be authorized.

Implementing Diversity

Defense in depth (also known as layered security) refers to the security practice of implementing several layers of protection. You can't simply take a single action, such as installing locks at the entrance of a building and consider yourself protected. You must implement security at several different layers. This way, if one layer fails, you still have additional layers to protect you.

If you drive your car to a local Walmart, put a five-dollar bill on the dash, and leave the keys in the car and the car running, there is a very good chance the car won't be there when you come out of the store. On the other hand, if you ensure nothing of value is visible from the windows, the car is locked, it has an alarm system, and it has stickers on the windows advertising the alarm system, it's less likely that someone will steal it. Not impossible, but less likely.

One of the ways of applying layered security is with diversity. This includes using different vendors, different technologies, and different controls.

Vendor diversity is the practice of implementing security controls from different vendors to increase security. As an example, Chapter 3, "Exploring Network Technologies and Tools," describes a screened subnet (sometimes known as a demilitarized zone). Many screened subnets use two firewalls, and vendor diversity dictates the use of firewalls from different vendors. For example, one firewall could be a Cisco firewall, and the other one could be a Check Point firewall. If a vulnerability is discovered in one of these firewalls, an attacker might be able to exploit it. However, it's unlikely that both firewalls would develop a vulnerability at the same time.

Technology diversity is the practice of using different technologies to protect an environment. For example, an organization may choose a data server room. They may start by limiting the access points, adding biometric locks to open the doors, and monitoring the access points with a CCTV system.

Control diversity is the use of different security control types, such as technical controls, physical controls, and administrative controls. For example, technical security controls such as firewalls, intrusion detection

systems (IDSs), and proxy servers help protect a network. Physical security controls can provide extra protection for the server room or other areas where these devices are located. Administrative controls such as vulnerability assessments and penetration tests can help verify that these controls are working as expected.

Creating Secure Areas

Physical security measures are available to protect secure areas. The following sections describe some methods you should know for the exam.

Air Gap

An ***air gap*** is a physical security control that ensures that a computer or network is physically isolated from another computer or network. Cables to one network never touch cables to another network, but instead, there is a gap of air between the cables. As an example, you can isolate a computer from a network by ensuring that it is not connected to any other system in the network. This lack of connectivity provides an air gap. Organizations often separate classified networks from unclassified networks to ensure that classified networks are not accessible by other internal networks or the Internet.

Vaults

A vault is a room or a large compartment used to store valuables. As an example, many banks use walk-in vaults to protect money and other valuables. Similarly, organizations use vaults to protect valuables, such as proprietary data.

Many vaults are used to store and access classified information. For example, the U.S. Department of Defense (DoD) uses Sensitive Compartmented Information Facilities (SCIFs), which are rooms within a building used to process classified information. Access to SCIFs is tightly controlled based on an individual's clearance and need-to-know.

Faraday Cage

A ***Faraday cage*** is typically a room that prevents radio frequency (RF) signals from entering into or emanating beyond a room. It includes electrical features that cause RF signals that reach the boundary of the room to be reflected back. This prevents signals from emanating outside the Faraday cage and protects equipment in the cage from damage from external signals such as lightning. A Faraday cage can also be a small enclosure.

Some elevators act as a Faraday cage (though I seriously doubt the designers were striving to do so). You might have stepped into an elevator and found that your cell phone stopped receiving and transmitting signals. The metal shielding around the elevator prevents signals from emanating out or signals such as the cell phone tower signal from entering the elevator.

Remember this

A Faraday cage can be a large room or a box, and it prevents signals from emanating beyond the enclosure. An air gap is a physical security control that ensures that a network is physically isolated from other networks, including the Internet.

Safes

Locking file cabinets or safes used in many offices help prevent the theft of smaller devices. For example, you can store smaller devices such as external USB drives or USB flash drives in an office safe or locking file cabinet when they aren't in use. Depending on the size of the office safe and office cabinet, you might also be able to secure laptops within them.

Hot and Cold Aisles

Hot and cold aisles help regulate the cooling in data centers with multiple rows of cabinets. The back of all the cabinets in one row faces the back of all the cabinets in an adjacent row. Because the hot air exits out the back of the cabinet, the aisle with the backs facing each other is the hot aisle.

Similarly, the front of the cabinets in one row faces the front of the cabinets in the adjacent row. Cool air is pumped through the floor to this cool aisle using perforated floor tiles in the raised flooring. This is the cold aisle. In some designs, cool air is also pumped through the base of the cabinets. This depends on the design of the cabinets and the needs of the equipment. Consider what happens if all the cabinets had their front facing the same way without a hot/cold aisle design. The hot air pumping out the back of one row of cabinets would be sent to the front of the cabinets behind them. The front row would have very cold air coming in the front, but other rows would have warmer air coming in the front.

Physical Attacks

A few physical attacks use smaller devices that appear to be normal. Some can install malware onto systems, and some can steal credit card data.

Malicious Universal Serial Bus (USB) Cable

A **malicious Universal Serial Bus (USB)** cable has an embedded Wi-Fi controller capable of receiving commands from nearby wireless devices, such as a smartphone. A computer detects this as a Human Interface Device as if it is a keyboard or mouse. If an attacker can connect to the malicious USB cable, he can send commands to the computer.

You don't need to be logged in to your computer in order to use your keyboard. Otherwise, how could you log in? Similarly, an attacker can access your computer via a malicious USB cable even if you're not logged on.

Penetration testers (and attackers) sometimes use a USB Ninja cable that looks like a normal USB cable. However, the cable delivers the malware to the system when a wireless signal triggers it. These are programmable, allowing testers and attackers to install different firmware onto the cable.

Malicious Flash Drive

A malicious flash drive is one that includes malware configured to infect a computer when the drive is plugged in. Years ago, attackers dropped infected drives in business or bank parking lots. If just a single employee picked up the drive and plugged it into a computer, it would infect that computer and potentially spread malware throughout the network from there.

Operating systems and antivirus software try to block malware from running automatically when USB drives are plugged into a computer. However, if someone reports erratic behavior after plugging in a USB drive, it's possible it installed malware on the user's system.

Card Skimming and Card Cloning

Credit card skimming is the practice of capturing credit card data at the point of sale. Attackers often place a skimmer on automated teller machines (ATMs) or gas stations when users swipe their credit cards. The skimmer captures the data on the magnetic strip but also allows the transaction to go through. Some signs of a credit card skimmer are a broken security seal, a loose credit card reader, or a credit card reader that extends past the panel.

Card cloning refers to making a copy of a credit card using data captured from a magnetic strip. Attackers copy the data onto a blank card or overwrite the data on a stolen card. This is relatively easy to do when using the magnetic strip of a credit card. However, the use of chips in credit cards makes it much harder to copy because the chip encrypts the data. The primary indicator of a cloned credit card is unauthorized or fraudulent charges.

Fire Suppression

You can fight fires with individual fire extinguishers, with fixed systems, or both. Most organizations included fixed systems to control fires and place portable fire extinguishers in different areas around the organization. A fixed system can detect a fire and automatically activate it to extinguish the fire. Individuals use portable fire extinguishers to extinguish or suppress small fires.

The different fire components are heat, oxygen, fuel, and a chain reaction creating the fire. Fire suppression methods attempt to remove or disrupt one of these elements to extinguish a fire:

- **Remove the heat.** Fire extinguishers commonly use chemical agents or water to remove the heat. However, water should never be used on an electrical fire.
- **Remove the oxygen.** Many methods use a gas, such as carbon dioxide (CO₂), to displace the oxygen. This is a common method of fighting electrical fires because CO₂ and similar gases are harmless to electrical equipment.
- **Remove the fuel.** Fire-suppression methods don't typically fight a fire this way, but of course, the fire will go out once all the material is burned.
- **Disrupt the chain reaction.** Some chemicals can disrupt the chain reaction of fires to stop them.

When implementing any fire suppression system, it's important to consider the safety of personnel. As an example, if a fire suppression system uses a gas such as carbon dioxide (CO₂) to displace the oxygen, it's important to ensure that personnel can get out before the oxygen is displaced.

Similarly, consider an exit door secured with a proximity card. Normally, employees open the door with the proximity card, and the system records their exit. What happens if a fire starts and power to the building is lost? The proximity card reader won't work, and if the door can't open, employees will be trapped. It's important to ensure that an alternative allows personnel to exit even if the proximity card reader loses power. Of course, this might introduce a vulnerability to consider. You don't want an

attacker to access a secure data center just by removing power to the proximity reader.

Protected Cable Distribution

Physical security includes planning where you route cables and how you route them. Skilled network administrators can cut a twisted-pair cable, attach an RJ-45 connector to each end, and connect them back together with an adapter in less than 5 minutes. Experienced fiber-optic cable technicians can do the same thing with a fiber-optic cable within 10 minutes. If an attacker did this, he could connect the cut cable to a network device and then capture all the traffic with a protocol analyzer. This represents a significant risk.

One method of reducing this risk is to run cables through cable troughs or wiring ducts. A cable trough is a long metal container, typically about four inches wide by four inches high. If you run data cables through the cable trough, they aren't as accessible to potential attackers. In contrast, many organizations simply run the cable through a false ceiling or a raised floor.

In addition to considering physical security, it's important to keep the cables away from electromagnetic interference (EMI) sources. For example, if technicians run cables over or through fluorescent lighting fixtures, the lights' EMI can disrupt the cables' signals. The result is intermittent connectivity for users.

Adding Redundancy and Fault Tolerance

One of the constants with computers, subsystems, and networks is that they will fail. It's one of the few things you can count on. It's not a matter of if they will fail, but when. However, by adding redundancy into your systems and networks, you can increase the system's reliability even when they fail. By increasing reliability, you increase a system's resiliency or availability.

Redundancy adds duplication to critical system components and networks and provides ***fault tolerance***. If a critical component has a fault, the duplication allows the service to continue as if a fault never occurred. In other words, a system with fault tolerance can suffer a fault, but it can tolerate it and continue to operate. Organizations often add redundancies to eliminate single points of failure:

- Disk redundancies using RAID
- NIC redundancy with NIC teaming
- Server redundancies by adding load balancers
- Power redundancies by adding generators or an UPS
- Site redundancies by adding hot, cold, or warm sites

Single Point of Failure

A ***single point of failure*** is a component within a system that can cause the entire system to fail if the component fails. When designing redundancies, an organization will examine different components to determine if they are a single point of failure. If so, they take steps to provide redundancy or fault-tolerance capabilities. The goal is to increase the reliability and availability of the systems.

Some examples of single points of failure include:

- **Disk.** If a server uses a single drive, the system will crash if the single drive fails. A redundant array of inexpensive disks (RAID) provides fault tolerance for hard drives and is a relatively inexpensive method of adding fault tolerance to a system.
- **Server.** If a server provides a critical service and its failure halts the service, it is a single point of failure. Load balancing provides fault tolerance for critical servers.
- **Power.** If an organization only has one source of power for critical systems, the power is a single point of failure. However, elements such as uninterruptible power supplies (UPSs) and power generators provide fault tolerance for power outages.
- **Personnel.** If there are tasks within an organization that only one person can perform, that person becomes a single point of failure. For example, imagine an organization purchased a sophisticated remote-controlled helicopter used to assess damage after storms or disasters. Arnie Pye is the only person who knows how to fly this helicopter. After winning the lottery a week ago, he quit work, and no one can reach him. Because no one knows how to fly the helicopter, the organization cannot assess the damage as planned. Similarly, imagine Apu is the only person in the IT department that knows how to run vulnerability scans. If Apu is no longer available, the organization can no longer run vulnerability scans.

Although IT personnel recognize the risks with single points of failure, they often overlook them until a disaster occurs. However, tools such as business continuity plans (covered later in this chapter) help an organization identify critical services and address single points of failure.

Remember this

A single point of failure is any component whose failure results in the failure of an entire system. Elements such as RAID, load balancing, UPSs, and generators remove many single points of failure. RAID is an inexpensive method used to add fault tolerance and increase availability. If only one person knows how to perform specific tasks, that person can become a single point of failure.

Disk Redundancies

Any system has four primary resources: processor, memory, disk, and the network interface. Of these, the disk is the slowest and most susceptible to failure. Because of this, administrators often upgrade disk subsystems to improve their performance and redundancy.

A redundant array of independent disks (**RAID**) subsystem provides fault tolerance for disks and increases system availability. Even if a disk fails, most RAID subsystems can tolerate the failure, and the system will continue to operate. RAID systems are becoming much more affordable as the price of drives falls and disk capacity steadily increases. The following sections discuss common RAID levels and how they can contribute to cybersecurity resilience.

RAID-0

RAID-0 (striping) is somewhat of a misnomer because it doesn't provide any redundancy or fault tolerance. It includes two or more physical disks. Files stored on a RAID-0 array are spread across each of the disks.

The benefit of a RAID-0 is increased read and write performance. Because a file is spread across multiple physical disks, the different parts of the file can be read from or written to each of the disks simultaneously. If you have three 500-GB drives used in a RAID-0, you have 1,500 GB (1.5 TB) of storage space.

RAID-1

RAID-1 (mirroring) uses two disks. Data written to one disk is also written to the other disk. If one of the disks fails, the other disk still has all the data, so the system can continue to operate without any data loss. With this in mind, if you mirror all the drives in a system, you can actually lose half of the drives and continue to operate.

You can add an additional disk controller to a RAID-1 configuration to remove the disk controller as a single point of failure. In this configuration, each of the disks has its own disk controller. Adding a second disk controller to a mirror is called disk duplexing.

If you have two 500-GB drives used in a RAID-1, you have 500 GB of storage space. The other 500 GB of storage space is dedicated to the fault-tolerant, mirrored volume.

RAID-2, RAID-3, and RAID-4 are rarely used.

RAID-5 and RAID-6

A RAID-5 is three or more disks that are striped together, similar to RAID-0. However, the equivalent of one drive includes parity information. This parity information is striped across each of the drives in a RAID-5 and provides fault tolerance. If one of the drives fails, the disk subsystem can read the remaining drives' information and re-create the original data. If two of the drives fail in a RAID-5, the data is lost.

RAID-6 is an extension of RAID-5. The big difference is that it uses an additional parity block and requires an additional disk. A huge benefit is that the RAID-6 disk subsystem will continue to operate even if two disk drives fail. RAID-6 requires a minimum of four disks.

Remember this

RAID subsystems, such as RAID-1, RAID-5, and RAID-6, provide fault tolerance and increased data availability. RAID-1 and RAID-5 can survive the failure of one disk, and RAID-6 can survive the failure of two disks.

RAID-10

A RAID-10 configuration combines the features of mirroring (RAID-1) and striping (RAID-0). RAID-10 is sometimes called RAID 1+0. A variation of RAID-10 is RAID-01 or RAID 0+1 that also combines mirroring and striping features but implements the drives differently.

The minimum number of drives in a RAID-10 is four. When adding more drives, you add two more (or multiples of two, such as four, six, and so on). If you have four 500-GB drives used in a RAID-10, you have 1 TB of usable storage.

Disk Multipath

Multipath input/output (I/O) is another fault-tolerance method for disks. In simple terms, it uses a separate data transfer path to and from the

storage hardware. If one of the paths fails, the second path handles the transfer. If both paths are operational, it provides increased performance.

However, multipath I/O isn't so simple. One method of implementing multipath I/O is via a storage area network (SAN) using Fibre Channel. Setting up a SAN with Fibre Channel is both complex and expensive.

Server Redundancy and High Availability

High availability refers to a system or service that needs to remain operational with almost zero downtime. It's possible to achieve 99.999 percent uptime, commonly called five nines by implementing redundancy and fault-tolerance methods. This equates to less than 6 minutes of downtime a year: $60 \text{ minutes} \times 24 \text{ hours} \times 365 \text{ days} \times .00001 = 5.256 \text{ minutes}$.

Although five nines is achievable, it's expensive. However, if the potential cost of an outage is high, the high cost of the redundant technologies is justified. For example, some websites generate a significant amount of revenue, and every minute a website is unavailable represents lost money. High-capacity load balancers ensure the service is always available even if a server fails.

Active/Active Load Balancers

An ***active/active load balancer*** can optimize and distribute data loads across multiple computers or multiple networks. For example, if an organization hosts a popular website, it can use multiple servers hosting the same website in a web farm. Load-balancing software distributes traffic equally among all the servers in the web farm, typically located in a DMZ.

The term ***load balancer*** makes it sound like it's a piece of hardware, but a load balancer can be hardware or software. A hardware-based load balancer accepts traffic and directs it to servers based on factors such as processor utilization and the number of current connections to the server. A software-based load balancer uses software running on each of the servers to balance the load. Load balancing primarily provides scalability, but it also contributes to high availability. Scalability refers to the ability of a service to serve more clients without any decrease in performance. Availability ensures that systems are up and operational when needed. By spreading the load among multiple systems, it ensures that individual systems are not overloaded, increasing overall availability.

Consider a web server that can serve 100 clients per minute, but if more than 100 clients connect at a time, performance degrades. You need to either scale up or scale out to serve more clients. You scale the server up by adding additional resources, such as processors and memory, and you scale out by adding additional servers in a load balancer.

Figure 9.1 shows an example of a load balancer with multiple web servers configured in a web farm. Each web server includes the same web application.

A load balancer uses a scheduling technique to determine where to send new requests. Some load balancers simply send new requests to the servers in a round-robin fashion. The load balancer sends the first request to Server 1, the second request to Server 2, and so on. Other load balancers automatically detect the load on individual servers and send new clients to the least used server.

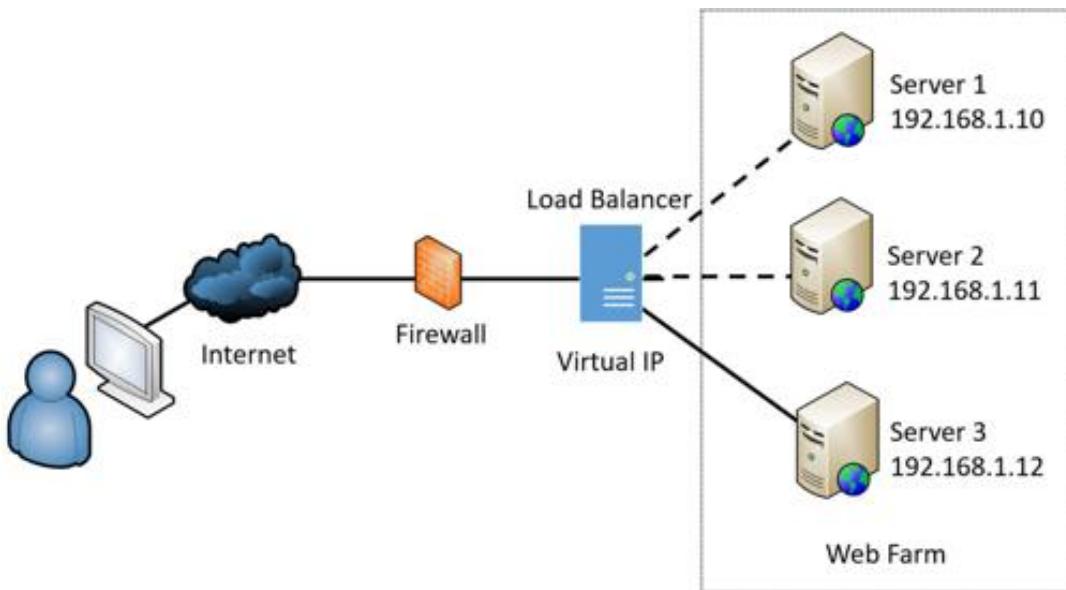


Figure 9.1: Load balancing

Some load balancers use source address affinity to direct the requests. Source affinity sends requests to the same server based on the requestor's IP address and provides the user with session persistence. As an example, imagine that Homer sends a request to retrieve a webpage. The load balancer records his IP address and sends his request to Server 3. When he interacts with the page and sends another request, the load balancer identifies his IP address and sends his request to Server 3 again. Source affinity effectively sticks users to a specific server ensuring session persistence.

A software-based load balancer uses a virtual IP. For example, imagine the IP address of the website is 72.52.206.134. This IP address isn't assigned to a specific server. Instead, clients send requests to this IP address, and the load-balancing software redirects the request to one of the servers in the web farm using their private IP addresses. In this scenario, the actual IP address is referred to as a virtual IP.

An added benefit of many load balancers is that they can detect when a server fails. If a server stops responding, the load-balancing software no longer sends clients to this server. This contributes to overall high availability.

Active/Passive Load Balancers

Load balancers can also be configured in an active/passive configuration. In an active/passive configuration, one server is active, and the other server is inactive. If the active server fails, the inactive server takes over.

Consider Figure 9.2, which shows a two-node active-passive configuration. (Load balancers can include more than two nodes, but these examples use only two to keep them simple.) Both nodes are individual servers, and they both have access to external data storage used by the active server. Additionally, the two nodes have a monitoring connection to each other used to check each other's health or heartbeat.

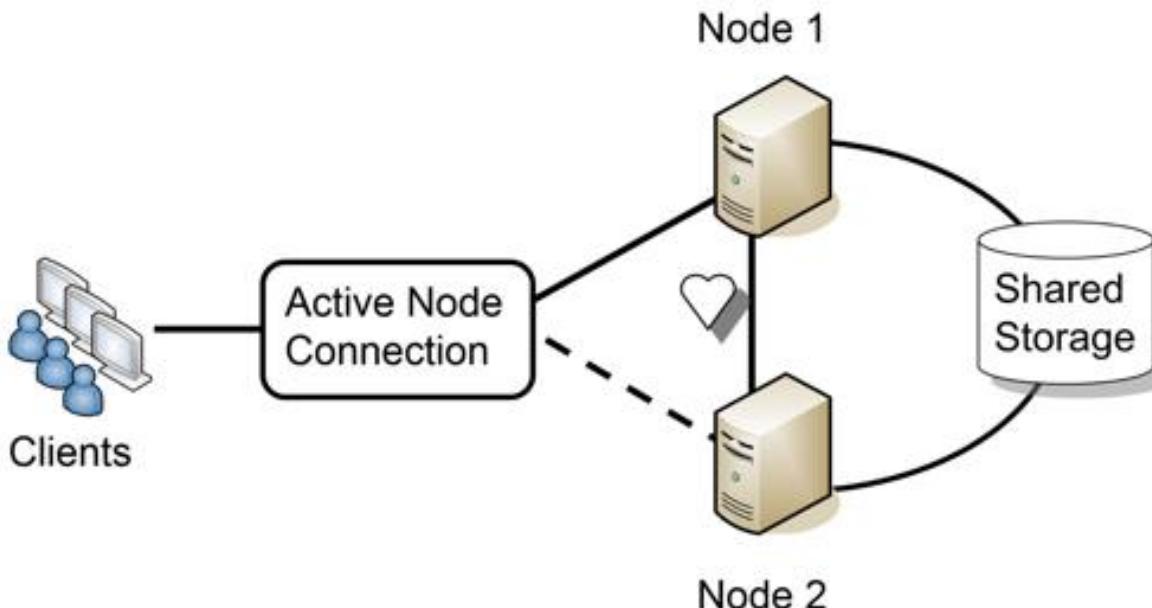


Figure 9.2: Active/passive configuration

Imagine that Node 1 is the active node. When any of the clients connect, the load balancer ensures that the clients connect to the active node. If Node 1 fails, Node 2 senses the failure through the heartbeat connection and configures itself as the active node. Because both nodes have access to the shared storage, there is no loss of data for the client. Clients may notice a momentary hiccup or pause, but the service continues.

You might notice that the shared storage in Figure 9.1 represents a single point of failure. It's not uncommon for this to be a robust hardware RAID-10. This ensures that even if a hard drive in the shared storage fails, the service will continue. Additionally, if both nodes are plugged into the same power grid, the power represents a single point of failure. They can each be protected with a separate UPS and use a separate power grid.

Remember this

Load balancing increases the overall processing power of a service by sharing the load among multiple servers. Configurations can be active/passive or active/active. Scheduling methods include round-robin and source IP address affinity. Source IP address affinity scheduling ensures clients are redirected to the same server for an entire session.

NIC Teaming

NIC teaming allows you to group two or more physical network adapters into a single software-based virtual network adapter. This provides increased performance because the NIC team handles all the individual NICs' bandwidth as if the NIC team is a single physical network adapter. Additionally, the NIC team uses load-balancing algorithms to distribute outgoing traffic equally among the NICs.

The NIC team also eliminates any physical NIC as a single point of failure. If one NIC in the NIC team fails, the software detects the failure and logically removes the team's failed NIC.

Power Redundancies

Power is a critical utility to consider when reviewing redundancies. For mission-critical systems, you can use uninterruptible power supplies, generators, and managed power distribution units (PDUs) to provide both fault tolerance and high availability:

- **Uninterruptible power supplies.** An uninterruptible power supply (UPS) provides short-term power and can protect against power fluctuations. UPS systems give computing devices enough time to perform a logical shutdown or keep them powered until longer-term power systems come online.
- **Dual supply.** Within the context of power redundancies, a dual power supply (or a redundant power supply) is a second power supply that can power a device if the primary power supply fails. During normal operations, each power supply provides power to the device. Most redundant power supplies are hot-swappable, allowing administrators to replace a failed device without removing power to the system. Within electronics, a dual power supply provides both positive voltage and negative voltage to devices. This allows it to use the entire alternating current (AC) cycle (positive and negative) before converting the power to direct current (DC). However, this is unrelated to a redundant power supply.
- **Generators.** Generators provide long-term power during extended outages. For example, during natural disasters such as hurricanes and floods, communities may experience power outages for days or even weeks. Generators can provide power to critical systems during these outages.
- **Managed power distribution units.** Server racks within a data center house multiple computing devices, and it's common to use power distribution units (PDUs) within the racks to power the devices. Basic PDUs distribute power to devices, similar to how a power strip delivers power via multiple outlets. Managed PDUs (sometimes called switched PDUs) monitor the quality of power such as voltage, current, and power consumption and report these measurements to a central monitoring console. This allows

administrators to use a single application to monitor power in all the racks within a data center.

Protecting Data with Backups

Backups are copies of data created to ensure that if the original data is lost or corrupted, it can be restored. The truth is, if you work with computers long enough, you will lose data. The difference between a major catastrophe and a minor inconvenience is the existence of a usable backup.

Ransomware has exploded in recent years. Attackers infect a single system and then move throughout a network looking for data files. As mentioned in Chapter 6, attackers have been launching ransomware attacks against hospitals, cities, and schools, effectively crippling these networks. The primary protection is to prevent ransomware attacks. However, once they succeed, the best corrective control is up-to-date backups of all critical data.

It's important to realize that redundancy and backups are not the same things. Protecting data with a RAID-1 or RAID-10 does not negate the need for backups. If a fire destroys a server, it also destroys the data on the RAID. Without a backup, all of the data is gone. Forever.

Backup Media

The most common media used for backups is tape. Tapes store more data and are cheaper than other media. Other types of media used to store backups are:

- **Disk.** Backups can also be stored on disks. A benefit is that disk access is much quicker than tape. However, disks are more expensive. The disks can be located on servers or simple USB disk drives.
- **Network-attached storage.** *Network-attached storage (NAS)* is a dedicated computer used for file storage and is accessible on a network. It can have multiple drives and often runs a stripped-down version of Linux for simplicity and to reduce costs. A NAS provides file-based data storage allowing users to access files on NAS devices and copy backup files to NAS devices.
- **Storage area network.** A *storage area network (SAN)* provides block-level data storage via a full network. Organizations use SANs to provide high-speed access to disk arrays or tape libraries. SANs can also be used for real-time replication of data. As soon as data changes in its primary location, it is replicated to the SAN. A primary difference between a NAS and a SAN is that a SAN requires dedicated hardware and uses different protocols such as Fibre Channel. In contrast, a NAS uses standard network protocols such as TCP and IP.
- **Cloud.** It's also possible to store backups in the cloud. Many companies such as Microsoft and Google provide free cloud storage to individuals. Similarly, many companies rent storage space from third-party providers. Chapter 5, “Securing Hosts and Data,” discusses cloud concepts in more depth.

Online Versus Offline Backups

Offline backups use traditional backup media within a network such as tapes, local disks, drives in a NAS, and even backup targets within a SAN. Offline backups provide an organization with easy access to the backups, better control of the backup media, and relatively fast backup and restore capabilities. Unfortunately, backup media can fail, be destroyed, or even be stolen.

In contrast, online backups are stored within the cloud. Most cloud providers provide data storage that you can access via the Internet from anywhere. Even if a natural disaster destroys all online backups, they remain available in the cloud. Additionally, most cloud providers automatically encrypt the data preventing unauthorized access to the backups.

Online and offline backups have a slightly different meaning in the context of databases. An online database backup is a hot backup, meaning that it backs up the database while it is operational. It captures the changes while they're occurring and applies them to the backup when it's done. In contrast, an offline backup is a cold backup or a backup performed while the database is offline. You can also think of an offline backup of a database as a local backup.

Comparing Backup Types

Backup utilities support several different types of backups. Even though third-party backup programs can be quite sophisticated in what they do and how they do it, you should have a solid understanding of the basics. As an introduction, many of these utilities commonly use the following backup types:

- **Full backup.** A full (or normal backup) backs up all the selected data.
- **Differential backup.** This backs up all the data that has changed or is different since the last full backup.
- **Incremental backup.** This backs up all the data that has changed since the last full or incremental backup.
- **Snapshot and image backup.** A snapshot backup captures the data at a point in time. It is sometimes referred to as an image backup.

Full Backups

A *full backup* backs up all data specified in the backup. For example, you could have several folders on the D: drive. If you specify these folders in the backup program, the backup program backs up all the data in these folders.

Although it's possible to do a full backup on a daily basis, it's rare to do so in most production environments. This is because of two limiting factors:

- **Time.** A full backup can take several hours to complete and can interfere with operations. However, administrators don't always have unlimited time to do backups and other system maintenance. For example, if a system is online 24/7, administrators might need to limit the amount of time for full backups to early Sunday morning to minimize the impact on users.
- **Money.** Backups need to be stored on some type of media, such as tape or hard drives. Performing full backups every day requires more media, and the cost can be prohibitive. Instead, organizations often combine full backups with differential or incremental backups.

Incremental and differential backup strategies must start with a full backup.

Restoring a Full Backup

A full backup is the easiest and quickest to restore. You only need to restore the single full backup, and you're done. If you store backups on tapes, you only need to restore a single tape. However, most organizations need to balance time and money and use either a full/differential or a full/incremental backup strategy.

Differential Backups

A *differential backup* strategy starts with a full backup. After the full backup, differential backups back up data that has changed or is different since the last full backup.

For example, a full/differential strategy could start with a full backup on Sunday night. On Monday night, a differential backup would back up all files that changed since the last full backup on Sunday. On Tuesday night, the differential backup would again back up all the files that changed since the last full backup. This repeats until Sunday when another full backup starts the process again. As the week progresses, the differential backup steadily grows in size.

Order of Restoration for a Full/Differential Backup Set

Assume for a moment that administrators store each of the backups on different tapes. If the system crashes on Wednesday morning, how many tapes would they need to recover the data?

The answer is two. They would first recover the full backup from Sunday. Because the differential backup on Tuesday night includes all the files that changed after the last full backup, they would then restore that tape to restore all the changes up to Tuesday night.

Incremental Backups

An *incremental backup* strategy also starts with a full backup. After the full backup, incremental backups then back up data that has changed

since the last backup. This includes either the last full backup or the last incremental backup.

As an example, a full/incremental strategy could start with a full backup on Sunday night. On Monday night, an incremental backup would back up all the files that changed since the last full backup. On Tuesday night, the incremental backup would back up all the files that changed since the incremental backup on Monday night. Similarly, the Wednesday night backup would back up all the files that changed since the last incremental backup on Tuesday night. This repeats until Sunday, when another full backup starts the process again. As the week progresses, the incremental backups stay about the same size.

Order of Restoration for a Full/Incremental Backup Set

Assume for a moment that administrators store each of the backups on different tapes. If the system crashes on Thursday morning, how many tapes would they need to recover the data?

The answer is four. They would first need to recover the full backup from Sunday. Because the incremental backups would be backing up different data each day of the week, each of the incremental backups must be restored and restored in chronological order.

Sometimes, people mistakenly think the last incremental backup would have all the relevant data. Although it might have some relevant data, it doesn't have everything.

As an example, imagine you worked on a single project file each day of the week, and the system crashed on Thursday morning. In this scenario, the last incremental backup would hold the most recent copy of this file. However, what if you compiled a report every Monday but didn't touch it again until the following Monday? Only the incremental backup from Monday would include the most recent copy. An incremental backup from Wednesday night or another day of the week wouldn't include the report.

Remember this

If you have unlimited time and money, the full backup alone provides the fastest recovery time. Full/incremental strategies reduce the amount of time

needed to perform backups. Full/differential strategies reduce the amount of time needed to restore backups.

Choosing Full/Incremental or Full/Differential

You may wonder “Why are there so many choices for backups?” The answer is that different organizations have different needs. For example, imagine two organizations perform daily backups to minimize losses. They each do a full backup on Sunday but are now trying to determine if they should use a full/incremental or a full/differential strategy.

The first organization doesn’t have much time to perform maintenance throughout the week. In this case, the backup administrator needs to minimize the amount of time required to complete backups during the week. An incremental backup only backs up the data that has changed since the last backup. In other words, it includes changes only from a single day. In contrast, a differential backup contains all the changes since the last full backup. Backing up the changes from a single day takes less time than backing up changes from multiple days, so a full/incremental backup is the best choice.

In the second organization, they want to recover failed systems quickly. If a failure requires restoring data, they want to minimize the amount of time needed to restore the data. A full/differential is the best choice in this situation because it only requires the restoration of two backups, the full and the most recent differential backup. In contrast, a full/incremental can require the restoration of several different backups, depending on when the failure occurs, taking much more time.

Snapshot and Image Backups

A ***snapshot backup*** (also known as an ***image backup***) captures the data at a moment in time. It is commonly used with virtual machines, but many backup utilities can perform snapshot backups on data. Chapter 5 discusses virtual machines (VMs) in more depth. Administrators often take a snapshot of a VM before a risky operation, such as an update. If the update causes problems, it’s relatively easy to revert the VM to the state it was in before the update.

Copy Backup

A copy backup copies files to backup media. As a simple example, when I'm working on a project such as this book, I'm frequently making backups to different drives. Sometimes I copy them to a NAS server in my office network. Other times I copy them to USB disk drives I've purchased specially for backups. As I get closer to the end of a project, I tend to get a little paranoid about losing files, and I typically have backups scattered in multiple locations.

It's worth mentioning that malware such as ransomware will look for, and infect, all drives connected to a computer. This includes local drives, USB disk drives, and drives on NAS devices. However, if you disconnect a USB disk drive after copying files, the malware can't reach them. Chapter 6 discusses malware types, including ransomware, in more depth.

Testing Backups

I've heard many horror stories in which personnel are regularly performing backups thinking all is well. Ultimately, something happens, and they need to restore some data. Unfortunately, they discover that none of the backups hold valid data. People have been going through the motions, but something in the process is flawed.

The only way to validate a backup is to perform a test restore. Performing a test restore is nothing more than restoring the data from a backup and verifying its integrity. If you want to verify that you can restore the entire backup, you perform a full restore of the backup. If you want to verify that you can restore individual files, you perform a test restore of individual files. It's common to restore data to a different location than the original source location. This still validates the quality of the backup.

As a simple example, an administrator can retrieve a random backup and attempt to restore it. There are two possible outcomes of this test, and both are good:

- **The test succeeds.** Excellent! You know that the backup process works. You don't necessarily know that every backup tape is valid, but at least you know that the process is sound and at least some of your backups work.
- **The test fails.** Excellent! You know there's a problem that you can fix before a crisis. If you discovered the problem after you actually lost data, it wouldn't help you restore the data.

An additional benefit of performing regular test restores is that it allows administrators to become familiar with the process. The first time they do a restore shouldn't be in the middle of a crisis with several high-level managers peering over their shoulders.

Backups and Geographic Considerations

Organizations typically create a backup policy to answer critical questions related to backups. The backup policy is a written document and will often identify what data to back up, how often to back up the data, how to test the backups, and how long to retain the backups.

Additionally, it's important to address special geographic considerations, such as the following:

- **Off-site storage.** At least one copy of backups should be stored off-site. Storing backups in a separate geographic location protects them against a disaster such as a fire or a flood. Even if a disaster destroys the site, the organization will still have another copy of the critical data.
- **Distance.** Many organizations have specific requirements related to geographic dispersal or the distance between the main site and the off-site location. In some scenarios, the goal is to have the off-site location relatively close so that personnel can easily retrieve the backups. However, in other scenarios, the off-site location must be far away, such as 25 miles or further away. This ensures that a disaster destroying a primary location won't impact the backup's location.
- **Location selection.** The location is often dependent on environmental issues. As an example, consider an organization located in California near the San Andreas fault. The off-site backup location should be far enough away that an earthquake at the primary location doesn't affect the off-site location.
- **Legal implications.** The legal implications related to backups depend on the data stored in the backups. For example, if the backups include Personally Identifiable Information (PII) or Protected Health Information (PHI), the backups need to be protected according to governing laws.
- **Data sovereignty.** Data sovereignty refers to the legal implications when data is stored off-site. If the backups are stored in a different country, they are subject to that country's laws. This can be a concern if the backups are stored in a cloud location and the cloud

servers are in a different country. For example, imagine that an organization is located in the United States. It routinely does backups and stores them with a cloud provider. The cloud provider has some servers in the United States, some in Canada, and some in Mexico. If the organization's backups are stored in other countries, the organization can be subject to additional laws and regulations.

Remember this

Test restores are the best way to test the integrity of a company's backup data. Backup media should be protected with the same level of protection as the data on the backup. Geographic considerations for backups include storing backups off-site, choosing the best location, and considering legal implications and data sovereignty.

Comparing Business Continuity Elements

Business continuity planning helps an organization predict and plan for potential outages of critical services or functions. The goal is to ensure that critical business operations continue and the organization can survive the outage. Organizations often create a business continuity plan (BCP). This plan includes disaster recovery elements that provide the steps used to return critical functions to operation after an outage.

Disasters and outages can come from many sources, including:

- **Environmental.** This can include natural disasters, such as hurricanes, floods, tornadoes, and earthquakes. It can also include things like fires caused by lightning strikes rather than by humans. On a larger scale, it can include major environmental disasters such as the Fukushima Daiichi Nuclear Power Plant's nuclear meltdown after an earthquake and tsunami in 2011.
- **Person-made.** Person-made disasters refer to those caused by human activity. This includes fires (caused by people) and train wrecks caused by human error, such as the May 2015 Amtrak derailment. Within an organization, human error can cause hardware and software failures, and data loss. Attacks are also person-made.
- **Internal versus external.** An internal disaster occurs within an organization. For example, a fire within an organization's data center is an internal disaster that may result in hardware failure and data loss. In contrast, an external disaster is a disaster that occurs outside of an organization but still impacts the organization. As an example, a wildfire near an organization may damage utility lines impacting the stability of power or communication lines.

Addressing all of these possible sources takes a lot of time and effort. The goal is to predict the relevant disasters as well as their impact and then develop recovery strategies to mitigate them. One of the first things an organization completes is a business impact analysis.

Business Impact Analysis Concepts

A ***business impact analysis (BIA)*** is an important part of a BCP. It helps an organization identify critical systems and components that are essential to the organization's success. These critical systems support ***mission-essential functions***. Mission-essential functions are the activities that must continue or be restored quickly after a disaster. The BIA also helps identify vulnerable business processes, which are the processes that support mission-essential functions.

As an example, imagine an organization that has an online e-commerce business. Some basic mission-essential functions might include serving webpages, providing a shopping cart path, accepting purchases, sending email confirmations, and shipping purchases to customers. The shopping cart path alone is a business process. Because it is essential to the mission of e-commerce sales, management will likely consider it a vulnerable business process to protect. The customer needs to view products, select a product, enter customer information, enter credit card data, and complete the purchase. Some critical systems that support the website are web servers and a back-end database application hosted on one or more database servers.

If critical systems and components fail and cannot be restored quickly, it impacts mission-essential functions. If this lasts too long, the organization may not be able to survive the disaster.

For example, if a disaster such as a hurricane hit, which services must the organization restore to stay in business? Imagine a financial institution. It might decide that customers must have uninterrupted access to account data through an online site. If customers can't access their funds online, they might lose faith with the company and leave in droves.

However, the company might decide to implement alternate business practices in other elements of the business. For example, management might decide that accepting and processing loan applications is not important enough to continue during a disaster. Loan processing is still important to the company's bottom line, but a delay will not seriously affect its ability to stay in business. In this scenario, continuous online access is a

mission-essential function, but processing loan applications during a disaster is not mission-essential.

The time to make these decisions is not during a crisis. Instead, the organization completes a BIA in advance. The BIA involves collecting information from throughout the organization and documenting the results. This documentation identifies core business or mission requirements. The BIA does not recommend solutions. However, it provides management with valuable information so that they can focus on critical business functions. It helps them address some of the following questions:

- What are the critical systems and functions?
- Are there any dependencies related to these critical systems and functions?
- What is the maximum downtime limit of these critical systems and functions?
- What scenarios are most likely to impact these critical systems and functions?
- What is the potential loss from these scenarios?

As an example, imagine an organization earns an average of \$5,000 an hour through online sales. In this scenario, management might consider online sales to be a mission-essential function, and all systems that support online sales are critical systems. This includes web servers and back-end database servers. These servers depend on the network infrastructure connecting them, Internet access, and access to payment gateways for credit card charges.

After analysis, they might determine that the maximum allowable outage for online sales is five hours. Identifying the maximum downtime limit is extremely important. It drives decisions related to recovery objectives and helps an organization identify various contingency plans and policies.

Site Risk Assessment

Chapter 8, “Using Risk Management Tools,” covers risk assessments such as qualitative and quantitative risk assessments. These are used to assess a wide variety of risks. However, a site risk assessment is a focused assessment of a specific location or site.

For example, the environmental risks for a site in Florida include hurricanes and floods, and these are items an organization should address. However, a San Francisco site doesn't need to worry about hurricanes, but earthquakes are a real risk.

Similarly, if an organization has multiple locations, each site probably has different mission-essential functions. One site may be focused on online sales so a site risk assessment would focus on protecting everything related to online sales. Another location may only focus on warehousing and shipping products after sales are completed. The warehouse site risk assessment will be quite different than the online site risk assessment.

Impact

The BIA evaluates various scenarios, such as natural disasters, fires, attacks, power outages, data loss, and hardware and software failures. Additionally, the BIA attempts to identify the impact of these scenarios. When evaluating the impact, a BIA looks at multiple items. For example, it might attempt to answer the following questions related to any of the scenarios:

- Will a disaster result in loss of life?
- Will a disaster result in loss of property?
- Is there a way to minimize the risk to personnel?
- Will a disaster reduce safety for personnel or property?
- What are the potential financial losses to the organization?
- What are the potential losses to the organization's reputation?

For example, a database server might host customer data, including credit card information. If an attacker accesses this customer data, the cost to the organization might exceed millions of dollars. According to a Ponemon Institute report, the average total cost of a data breach in 2020 was \$3.86 million. For health care organizations, the average cost was \$7.13 million. Of course, these are only averages. Many data breaches cost much more.

Remember this

The BIA identifies mission-essential functions and critical systems that are essential to the organization's success. It also identifies maximum downtime limits for these systems and components, various scenarios that

can impact these systems and components, and the potential losses from an incident.

Recovery Time Objective

The recovery time objective (RTO) identifies the maximum amount of time it can take to restore a system after an outage. Many BIAs identify the maximum acceptable outage or maximum tolerable outage time for mission-essential functions and critical systems. If an outage lasts longer than this maximum time, the impact is unacceptable to the organization.

For example, imagine an organization that sells products via a website that generates \$10,000 in revenue an hour via online sales. It might decide that the maximum acceptable outage for the web server is five minutes. This results in an RTO of five minutes, indicating any outage must be limited to less than five minutes.

Imagine that the organization has a database server only used by internal employees, not online sales. Although the database server may be valuable, it is not critical. Management might decide they can accept an outage for as long as 24 hours, resulting in an RTO of less than 24 hours.

Recovery Point Objective

A recovery point objective (**RPO**) identifies a point in time where data loss is acceptable. Imagine a server hosting archived data that has very few changes weekly. Management might decide that some data loss is acceptable, but they always want to recover data from at least the previous week. In this case, the RPO is one week.

With an RPO of one week, administrators would ensure that they have at least weekly backups. In the event of a failure, they will be able to restore recent backups and meet the RPO.

In some cases, the RPO is up to the minute of the failure. For example, any data loss from an online database recording customer transactions might be unacceptable. In this case, the organization can use various techniques to ensure administrators can restore data up to the moment of failure.

Remember this

The recovery time objective (RTO) identifies the maximum amount of time it should take to restore a system after an outage. It is derived from the maximum allowable outage time identified in the BIA. The recovery point objective (RPO) refers to the amount of data you can afford to lose.

Comparing MTBF and MTTR

When working with a BIA, experts often attempt to predict the possibility of a failure. For example, what is the likelihood that a hard disk within a RAID configuration will fail? The following two terms are often used to predict potential failures:

- **Mean time between failures (MTBF).** The MTBF provides a measure of a system's reliability and is usually represented in hours. More specifically, the MTBF identifies the average (the arithmetic mean) time between failures. Higher MTBF numbers indicate higher reliability of a product or system. Administrators and security experts attempt to identify the MTBF for critical systems with the goal of predicting potential outages.
- **Mean time to repair (MTTR).** The MTTR identifies the average (the arithmetic mean) time it takes to restore a failed system. In some cases, people interpret MTTR as the mean time to recover, and both mean essentially the same thing. Organizations that have maintenance contracts often specify the MTTR as a part of the contract. The supplier agrees that it will, on average, restore a failed system within the MTTR time. The MTTR does not provide a guarantee that it will restore the system within the MTTR every time. Sometimes, it might take a little longer, and sometimes it might be a little quicker, with the average defined by the MTTR.

Remember this

The mean time between failures (MTBF) provides a measure of a system's reliability and would provide an estimate of how often the systems will experience outages. The mean time to recover (MTTR) refers to the time it takes to restore a system.

Continuity of Operations Planning

Continuity of operations planning (COOP) focuses on restoring mission-essential functions at a recovery site after a critical outage. For example, suppose a hurricane or other disaster prevents the company from operating in the primary location. In that case, the organization can continue to operate the mission-essential functions at an alternate location that management previously identified as a recovery site. Failover is the process of moving mission-essential functions to the alternate site.

Site Resiliency

A ***recovery site*** is an alternate processing site that an organization uses for ***site resiliency***. If one site suffers a catastrophic failure, an alternate site can take over after the disaster. The three primary types of recovery sites are hot sites, cold sites, and warm sites. These alternate locations could be office space within a building, an entire building, or even a group of buildings. Other types of recovery sites are mobile sites and mirrored sites. The following sections provide more details on these sites.

Hot Site

A ***hot site*** would be up and operational 24 hours a day, seven days a week and would be able to take over functionality from the primary site quickly after a primary site failure. It would include all the equipment, software, and communication capabilities of the primary site, and all the data would be up to date. In many cases, copies of backup tapes are stored at the hot site as the off-site location.

In many cases, a hot site is another active business location that has the capability to assume operations during a disaster. For example, a financial institution could have locations in two separate cities. The second location provides noncritical support services, but also includes all the resources necessary to assume the functions of the first location.

Some definitions of hot sites indicate they can take over instantaneously, though this isn't consistent. In most cases, it takes a little bit of time to transfer operations to the hot site, and this can take anywhere from a few minutes to an hour.

Clearly, a hot site is the most effective disaster recovery solution for high-availability requirements. If an organization must keep critical systems with high-availability requirements, the hot site is the best choice. However, a hot site is the most expensive to maintain and keep up to date.

Remember this

A hot site includes personnel, equipment, software, and communication capabilities of the primary site with all the data up to date. A hot site provides the shortest recovery time compared with warm and cold sites. It is the most effective disaster recovery solution, but it is also the most expensive to maintain.

Cold Site

A ***cold site*** requires power and connectivity but not much else. Generally, if it has a roof, electricity, running water, and Internet access, you're good to go. The organization brings all the equipment, software, and data to the site when it activates it.

I often take my dogs for a walk at a local army base and occasionally see soldiers activate an extreme example of a cold site. On most weekends, the fields are empty. Other weekends, soldiers have transformed one or more fields into complete operational sites with tents, antennas, cables, generators, and porta-potties.

Because the army has several buildings on the base, they don't need to operate in the middle of fields, but what they're really doing is testing their ability to stand up a cold site wherever they want. If they can do it in the field, they can do it in the middle of a desert, or anywhere else they need to.

A cold site is the cheapest to maintain, but it is also the most difficult to test.

Warm Site

You can think of a ***warm site*** as the Goldilocks solution—not too hot and not too cold, but just right. Hot sites are generally too expensive for most organizations, and cold sites sometimes take too long to configure for full operation. However, the warm site provides a compromise that an organization can tailor to meet its needs.

For example, an organization can place all the necessary hardware at the warm site location but not include up-to-date data. If a disaster occurs, the organization can copy the data to the warm site and take over operations. This is only one example, but there are many different possibilities of warm site configurations.

Site Variations

Although hot, cold, and warm sites are the most common, you might also come across two additional alternate site types: mobile and mirrored.

A mobile site is a self-contained transportable unit with all the equipment needed for specific requirements. For example, you can outfit a semitrailer with everything needed for operations, including a satellite dish for connectivity. Trucks, trains, or ships haul it to its destination and it only needs power to start operating.

Mirrored sites are identical to the primary location and provide 100 percent availability. They use real-time transfers to send modifications from the primary location to the mirrored site. Although a hot site can be up and operational within an hour, the mirrored site is always up and operational.

Restoration Order

After the disaster has passed, you will want to return all the functions to the primary site. As a best practice, organizations return the least critical functions to the primary site first. Remember, the critical functions are operational at the alternate site and can stay there as long as necessary. If a site has just gone through a disaster, it's very likely that there are still some unknown problems. By moving the least critical functions first, undiscovered problems will appear and can be resolved without significantly affecting mission-essential functions.

Remember this

A cold site will have power and connectivity needed for a recovery site, but little else. Cold sites are the least expensive and the hardest to test. A warm site is a compromise between a hot site and a cold site. Mobile sites do not have dedicated locations but can provide temporary support during a disaster.

Disaster Recovery

A disaster recovery plan (DRP) identifies how to recover critical systems and data after a disaster. Disaster recovery is a part of an overall business continuity plan. Often, the organization will use the business impact analysis to identify the critical systems and components and then develop disaster recovery strategies and DRPs to address the systems hosting these functions.

In some cases, an organization will have multiple DRPs within a BCP, and in other cases, the organization will have a single DRP. For example, it's possible to have individual DRPs that identify the steps to recover individual critical servers and other DRPs that detail the recovery steps after different disasters such as hurricanes or tornadoes. A smaller organization might have a single DRP that simply identifies all the steps used to respond to any disruption.

A DRP or a BCP will include a hierarchical list of critical systems. This list identifies what systems to restore after a disaster and in what order. For example, should a server hosting an online website be restored first, or a server hosting an internal application? The answer is dependent on how the organization values and uses these servers. In some cases, systems have interdependencies requiring administrators to restore systems in a specific order.

If the DRP doesn't prioritize the systems, individuals restoring the systems will use their own judgment, which might not meet the organization's overall needs. For example, Nicky New Guy might not realize that a web server is generating \$5,000 an hour in revenue but does know that he's responsible for keeping a generic file server operational. Without an ordered list of critical systems, he might spend his time restoring the file server and not the web server.

This hierarchical list is valuable when using alternate sites such as warm or cold sites, too. When the organization needs to move operations to an alternate site, the organization will want the most important systems and functions restored first.

Similarly, the DRP often prioritizes the services to restore after an outage. As a rule, critical business functions and security services are

restored first. Support services are restored last.

The different phases of a disaster recovery process typically include the following steps:

- **Activate the disaster recovery plan.** Some disasters, such as earthquakes or tornadoes, occur without much warning, and a DRP is activated after the disaster. Other disasters, such as hurricanes, provide a warning, and the DRP is activated when the disaster is imminent.
- **Implement contingencies.** If the recovery plan requires the implementation of an alternate site, critical functions are moved to these sites. If the disaster destroyed on-site backups, this step retrieves the off-site backups from the off-site location.
- **Recover critical systems.** After the disaster has passed, the organization begins recovering critical systems using the prioritization listed in the DRP. This also includes reviewing change management documentation to ensure that recovered systems include approved changes.
- **Test recovered systems.** Before bringing systems online, administrators test and verify them. This may include comparing the restored system with a performance baseline to verify functionality.
- **After-action report.** The final phase of disaster recovery includes a review of the disaster, sometimes called an after-action review. This often includes a lessons learned review to identify what went right and what went wrong. After reviewing the after-action report, the organization often updates the plan to incorporate any lessons learned.

Some organizations use functional recovery plans to address items that another organization may include in a standard DRP. It may include the hierarchical list of critical systems to ensure that personnel know the systems' priorities and the order of restoration.

Remember this

A disaster recovery plan (DRP) identifies how to recover critical systems after a disaster and often prioritizes services to restore after an outage. Testing validates the plan. The final phase of disaster recovery includes a

review to identify any lessons learned and may include an update of the plan.

Testing Plans with Exercises

Business continuity plans and disaster recovery plans include testing. Testing validates that the plan works as desired and will often include testing redundancies and backups. Several types of testing are used with BCPs and DRPs, including tabletop exercises, walk-throughs, and simulations.

If you search the Internet for these testing types, you'll find various definitions. Of course, anyone can write and post a webpage, so it's best to seek authoritative sources for definitions. I derived the definitions for these terms using two sources for business continuity exercises I trust:

- NIST SP 800-34, "Contingency Planning Guide for Federal Information Systems."
- Ready.gov (specifically <https://www.ready.gov/exercises>)

A ***tabletop exercise*** (also called a desktop exercise) is discussion-based. A coordinator gathers participants in a classroom or conference room and leads them through one or more hypothetical scenarios such as a cyberattack or a natural disaster. As the coordinator introduces each stage of the scenario, the participants identify how they would respond based on an organization's plan. This generates discussion about team members' roles and responsibilities and the decision-making process during an incident.

During a tabletop exercise, the coordinator may inject additional information. As an example, imagine the initial scenario is about a wildfire threatening a remote office. As participants discuss their responses, the coordinator may announce that the winds shifted and the wildfire is now threatening the organization's main location. This additional scenario is planned in advance and mimics potential events that may occur in a real-life situation.

Ideally, the exercise validates that the plan adequately addresses the scenario. However, it sometimes reveals flaws. The BCP coordinator ensures the plans are rewritten if necessary after the tabletop exercise.

Prior to doing a tabletop exercise, it's common to do walk-throughs. ***Walk-throughs*** are workshops or orientation seminars that train team members about their roles and responsibilities. They familiarize personnel with an organization's business continuity plans and their roles and

responsibilities. A walk-through can also help personnel planning the tabletop exercise to develop a formal tabletop test plan.

Simulations are functional exercises that allow personnel to test the plans in a simulated operational environment. There is a wide range of functional exercises, from simple simulations to full-blown tests. In a simulation, the participants go through the steps in a controlled manner without affecting the actual system. For example, a simulation can start by indicating that a server failed. Participants then follow the steps to rebuild the server on a test system. A full-blown test goes through all the steps of the plan. In addition to verifying that the test works, this also shows the amount of time it will take to execute the plan.

As a summary, these three exercises are:

- **Walk-throughs.** A walk-through is training provided to personnel in a classroom setting before a tabletop exercise. They can also be used to help develop a formal tabletop test plan.
- **A tabletop exercise.** This is a discussion-based exercise where participants sit around a table and talk through one or more scenarios.
- **Simulations.** Simulations allow personnel to go through the actual steps of an exercise but in a simulated environment. Unlike walk-throughs and tabletop exercises, they allow personnel to perform response and recovery steps rather than just talk about them.

Some common elements of testing plans include:

- **Backups.** Backups are tested by restoring the backup data, as discussed in the “Testing Backups” section earlier in this chapter.
- **Server restoration.** A simple disaster recovery exercise rebuilds a server. Participants follow the steps to rebuild a server using a test system without touching the live system.
- **Server redundancy.** If a server is using active/passive load balancing, you can test it by taking a primary node offline. Another node within the cluster should automatically assume the role of this offline node.
- **Site resiliency.** You can test site resiliency by moving some of the functionality to the alternate site and ensuring the alternate site works as desired. It’s also possible to test individual elements of an

alternate site, such as Internet connectivity or the ability to obtain and restore backup media.

Remember this

You can validate business continuity plans through testing. Tabletop exercises are discussion-based only and are typically performed in a conference setting. Walk-throughs provide training to personnel prior to a tabletop exercise or to create a formal tabletop exercise plan. Simulations are hands-on exercises.

Chapter 9 Exam Topic Review

When preparing for the exam, make sure you understand these key concepts covered in this chapter.

Comparing Physical Security Controls

- Physical security controls are controls you can physically touch. They often control entry and exit points and include various types of locks. Controlled areas such as data centers and server rooms should only have a single entrance and exit point. Door lock types include physical locks, cipher locks, and biometric locks.
- Cable locks secure mobile computers such as laptop computers in a training lab. Small devices can be stored in safes or locking office cabinets to prevent the theft of unused resources.
- A proximity card can electronically unlock a door and helps prevent unauthorized personnel from entering a secure area. By themselves, proximity cards do not identify and authenticate users. Some systems combine proximity cards with PINs for identification and authentication.
- Security guards are a preventive physical security control, and they can prevent unauthorized personnel from entering a secure area. A benefit of guards is that they can recognize people and compare an individual's picture ID for people they don't recognize.
- Cameras and closed-circuit television (CCTV) systems provide video surveillance and can give reliable proof of a person's identity and activity. Many cameras include motion detection and object detection capabilities. It's also possible to use CCTV systems as a compensating control.
- Sensors can detect changes in the environment, such as motion, noise, and temperature changes.
- Fencing, lighting, and alarms are commonly implemented with motion detection systems for physical security. Infrared motion detection systems detect human activity based on temperatures.
- Barricades provide stronger physical security than fences and attempt to deter attackers. Bollards are effective barricades that

- allow people through but block vehicles.
- Asset management processes protect against vulnerabilities related to architecture and design weaknesses, system sprawl, and undocumented assets. They can also help detect shadow IT.
- Organizations use diversity methods to provide layered security. Vendor diversity is the practice of implementing security controls from different vendors to increase security. Technology diversity uses different technologies to protect an environment, and control diversity uses different security control types, such as technical controls, administrative controls, and physical controls.
- An air gap is a physical security control that ensures that a computer or network is physically isolated from other computers or networks.
- A Faraday cage prevents signals from emanating beyond a room or enclosure.
- Hot and cold aisles provide more efficient cooling of systems within a data center.

Adding Redundancy and Fault Tolerance

- A single point of failure is any component that can cause the entire system to fail if it fails. It normally refers to hardware but can be a person. If one person is the only person that can perform a task, that person can be a single point of failure.
- RAID disk subsystems provide fault tolerance and increase availability. RAID-1 (mirroring) uses two disks. RAID-5 uses three or more disks and can survive the failure of one disk. RAID-6 and RAID-10 use four or more disks and can survive the failure of two disks.
- Load balancers spread the processing load over multiple servers. In an active/active configuration, all servers are actively processing requests. In an active/passive configuration, at least one server is not active but is instead monitoring activity ready to take over for a failed server. Software-based load balancers use a virtual IP.
- Affinity scheduling sends client requests to the same server based on the client's IP address. This is useful when clients need to access

the same server for an entire online session. Round-robin scheduling sends requests to servers using a predefined order.

- NIC teaming groups two or more physical network adapters into a single software-based network adapter. It provides load balancing for outgoing traffic and fault tolerance if one of the NICs fail.
- Power redundancies include a UPS, a dual power supply, and generators. Managed PDUs monitor the quality of power delivered to devices within a server rack.

Protecting Data with Backups

- Offline backups use traditional backup media such as tapes, local disks, drives in a NAS, and even backup targets within a SAN. Online backups are stored in the cloud.
- Traditional backup methods include full, full/differential, full/incremental, snapshot, and image strategies. A full backup strategy alone allows the quickest recovery time.
- Full/incremental backup strategies minimize the amount of time needed to perform daily backups. Full/differential backup strategies minimize the amount of time required to restore backups.
- A copy of backups should be kept off-site and should be kept far enough away so that a disaster impacting the primary site doesn't impact the backups.
- It's important to consider the distance between the main site and the off-site location.
- The location of the data backups affects data sovereignty. If backups are stored in a different country, the backups' data is now subject to the laws and regulations of that country.

Comparing Business Continuity Elements

- A business impact analysis (BIA) is part of a business continuity plan (BCP), and it identifies mission-essential functions, critical systems, and vulnerable business processes that are essential to the organization's success.
- The BIA identifies maximum downtimes for these systems and components. It considers various scenarios that can affect these

systems and components, and the impact to life, property, safety, finance, and reputation from an incident.

- A recovery time objective (RTO) identifies the maximum amount of time it should take to restore a system after an outage. The recovery point objective (RPO) refers to the amount of data you can afford to lose.
- The mean time between failures (MTBF) identifies the average (the arithmetic mean) time between failures. The mean time to recover (MTTR) identifies the average (the arithmetic mean) time it takes to restore a failed system.
- Continuity of operations planning identifies alternate processing sites (used for site resiliency) and alternate business practices. Recovery sites provide alternate locations for business functions after a major disaster.
- A hot site includes everything needed to be operational within 60 minutes and is the most effective recovery solution but is also the most expensive. A cold site has power and connectivity requirements and little else and is the least expensive to maintain. Warm sites are a compromise between hot sites and cold sites.
- A disaster recovery plan (DRP) identifies how to recover critical systems after a disaster and often prioritizes services to restore after an outage.
- Periodic testing validates continuity of operations plans. Exercises validate the steps to restore individual systems, activate alternate sites, and document other actions within a plan. Tabletop exercises are discussion-based only, and walk-throughs provide training to personnel before a tabletop exercise. Simulations are hands-on exercises.

ine References

- Do you know how to answer performance-based questions? Check out the online extras at <https://greatadministrator.com/601-extras>.

Chapter 9 Practice Questions

1. Employees access the data center by entering a cipher code at the door. However, everyone uses the same code, so it does not identify individuals. After a recent security incident, management has decided to implement a key card system that will identify individuals who enter and exit this secure area. However, the installation might take six months or longer. Which of the following choices can the organization install immediately to identify individuals who enter or exit the secure area?
 - A. Access control vestibule
 - B. Access list
 - C. CCTV
 - D. Bollards
 - E. Compensating control

2. Your local library is planning to purchase new laptops that patrons can use for Internet research. However, management is concerned about possible theft. Which of the following is the BEST choice to prevent theft of these laptops?
 - A. Mantrap
 - B. Anti-malware software
 - C. Cable locks
 - D. Disk encryption

3. Your organization needs to create a design for a high-security network for a U.S. government contract. The network should not be accessible by your organization's existing networks or the Internet. Which of the following options will BEST meet this need?
 - A. Faraday cage
 - B. Air gap
 - C. Protected cable distribution
 - D. Vault

4. You need to secure access to a data center. Which of the following choices provides the BEST physical security to meet this need? (Select

THREE.)

- A. Biometrics
- B. Cable locks
- C. Access control vestibule
- D. CCTV
- E. HVAC

5. You need to add disk redundancy for a critical server in your organization's screened subnet. Management wants to ensure it supports two-drive failure. Which of the following is the BEST solution for this requirement?

- A. RAID-0
- B. RAID-1
- C. RAID-5
- D. RAID-6

6. Your organization hosts several databases on two servers. Management wants to increase the redundancy of data storage for these servers. Which of the following is the BEST choice to meet this requirement?

- A. NIC teaming
- B. Managed PDUs
- C. UPS
- D. Multipath

7. Your organization hosts an e-commerce website that has been receiving a significant increase in traffic. The CPU is handling the load, but the server is unable to process the bandwidth consistently. Which of the following is the BEST choice to solve this problem?

- A. SAN
- B. NIC teaming
- C. Multipath
- D. Managed PDUs

8. Your organization is planning to deploy a new e-commerce website. Management anticipates heavy processing requirements for a back-end application used by the website. The current design will use one web server

and multiple application servers. Additionally, when beginning a session, a user will connect to an application server and remain connected to the same application server for the entire session.

Which of the following BEST describes the configuration of the application servers?

- A. Load balancing
 - B. Active/active
 - C. Active/passive
 - D. Persistence
9. Your organization recently implemented two servers in an active/passive load-balancing configuration. What security goal does this support?
- A. Obfuscation
 - B. Integrity
 - C. Confidentiality
 - D. Resilience
10. Your database backup strategy includes full backups performed on Saturdays at 12:01 a.m. and differential backups performed daily at 12:01 a.m. If the database fails on Thursday afternoon, how many backups are required to restore it?
- A. 1
 - B. 2
 - C. 3
 - D. 5
11. After reading about increased ransomware attacks against the health sector, hospital administrators want to enhance organizational resilience against these attacks. Which of the following could IT personnel implement to support this goal?
- A. Use email filtering to block malicious emails
 - B. Perform regular testing and validation of full backups
 - C. Ensure all systems are patched
 - D. Increase end-user training related to ransomware and other risks

12. Your organization hired a security consultant to create a BIA. She is trying to identify processes that can potentially cause losses in revenue if they stop functioning. Which of the following BEST describes what she is identifying?

- A. Single points of failure
- B. Critical systems
- C. Mission-essential functions
- D. MTBF

13. After a recent attack causing a data breach, an executive is analyzing the financial losses. She determined that the attack is likely to result in losses of at least \$1 million. She wants to ensure that this information is documented for future planning purposes. Which of the following documents is she MOST likely to use?

- A. DRP
- B. BIA
- C. MTTR
- D. RTO

14. A project manager is reviewing a business impact analysis. It indicates that a key website can tolerate a maximum of three hours of downtime. Administrators have identified several systems that require redundancy additions to meet this maximum downtime requirement. Of the following choices, what term refers to the maximum of three hours of downtime?

- A. RPO
- B. MTTR
- C. MTBF
- D. RTO
- E. DRP

15. Lisa has scheduled quarterly meetings with department leaders to discuss how they would respond to various scenarios such as natural disasters or cyberattacks. During the meetings, she presents a scenario and asks attendees to indicate their responses. Also, during the meetings, she injects variations on the scenario similar to what may happen during a live

event and encourages attendees to discuss their responses. What does this describe?

- A. Simulation
- B. Tabletop exercise
- C. Incident response
- D. Testing site resiliency

Chapter 9 Practice Question Answers

1. **C** is correct. Closed-circuit television (CCTV) or a similar video surveillance system can monitor the entrance and record who enters and exits the area. An access control vestibule (sometimes called a mantrap) prevents tailgating, but it doesn't necessarily identify individuals. An access list is useful if a guard identifies users and allows access based on the access list, but the access list does not identify users. Bollards are a type of barricade that protects building entrances. Using a CCTV until the key card system is installed is an example of a compensating control, but all compensating controls do not identify people.
2. **C** is correct. A cable lock attaches to a computer and wraps around a piece of furniture to secure it to deter and prevent theft. This is like a bike lock used to secure a bicycle to a bike rack. A mantrap prevents tailgating but is unrelated to this question. Anti-malware software protects the systems from viruses and other malware. Disk encryption is useful if the computers have confidential information, but it wouldn't be appropriate to put confidential information on a public computer.
3. **B** is correct. An air gap is a physical security control that ensures that a network is physically isolated from other networks, including the Internet. A Faraday cage prevents radio frequency (RF) signals from entering or emanating beyond an enclosure, but a network within a Faraday cage can still be connected to external networks. Protected cable distribution practices isolate cables from electromagnetic interference (EMI) sources but don't isolate networks. Vaults are rooms or large compartments used to store valuables, not isolate networks.
4. **A, C, and D** are correct. A biometric reader used for access control, an access control vestibule (sometimes called a mantrap), and a closed-circuit television (CCTV) system all provide strong physical security for accessing a data center. Cable locks are effective theft deterrents for mobile devices such as laptops, but they don't protect data centers. Heating, ventilation,

and air conditioning (HVAC) systems can control the data center's environment, but they don't secure access.

5. **D** is correct. A redundant array of independent disks 6 (RAID-6) is the best solution of the available answers. It supports two-drive failure meaning that two drives can fail in the RAID-6, and the disk subsystem will continue to operate. RAID-0 (disk striping) doesn't have any fault tolerance and will fail completely if a single drive fails. RAID-1 (disk mirroring) uses only two drives. If one drive fails in a RAID-1, the data is preserved, but if two drives fail, all data is lost. RAID-5 (striping with parity) will continue to operate if one drive fails, but all data is lost if two drives fail.

6. **D** is correct. Multipath is a fault-tolerance technique that provides more than one path for a system to the data storage system. It could be two Small Computer System Interface (SCSI) controllers providing a path to SCSI disks, or two storage area network (SAN) switches providing redundant paths to a SAN. Network interface card (NIC) teaming combines the bandwidth of two or more NICs to increase the throughput, but the NICs won't necessarily be used to access disks. Managed power distribution units (PDUs) provide the ability to monitor energy consumption in a data center remotely. An uninterruptible power supply (UPS) provides short-term power to systems after a power failure.

7. **B** is correct. Network interface card (NIC) teaming combines the bandwidth of two or more NICs to increase the throughput and would solve this problem. A storage area network (SAN) is a computer network that provides block-level data storage. A SAN can increase disk performance, not bandwidth performance. Multipath is a fault-tolerance technique used for data storage. Managed power distribution units (PDUs) provide the ability to remotely monitor energy consumption in a data center.

8. **D** is correct. This describes a load-balancing configuration using persistence so that a user will connect to the same application server for an entire session. All the answers are related to load balancing, but the scenario describes load balancing with persistence, so persistence is more correct than load balancing. An active/active load-balancing configuration

indicates all the servers are handling user requests. An active/passive load-balancing configuration has at least one server that is not actively serving clients but can take over if another server fails. However, the scenario didn't give enough information to determine if the application servers were configured as active/active or active/passive.

9. **D** is correct. An active/passive load-balancing configuration supports resilience and high availability. An active/passive load-balancing configuration uses redundant servers to ensure a service continues to operate even if one of the servers fails. Obfuscation methods attempt to make something unclear or difficult to understand and are not related to load balancing. Integrity methods ensure that data has not been modified. Confidentiality methods such as encryption prevent the unauthorized disclosure of data.

10. **B** is correct. Two backups are required, the full backup performed on Sunday at 12:01 a.m. and the differential backup performed on Thursday at 12:01 a.m. If you perform only one backup, it would be the full backup. You can't restore a differential backup without restoring the full backup first. This wouldn't include all the changes that occurred during the week. If you were using a full/incremental strategy, you would apply five backups: the full backup, and each of the incremental backups performed daily (Monday, Tuesday, Wednesday, and Thursday).

11. **B** is correct. Performing regular testing and validation of full backups will enhance organizational resilience against ransomware attacks. Resiliency techniques help ensure an organization can recover from a security incident and minimize downtime after an outage. The other answers all refer to preventive methods taken before an outage. Email filtering blocks spam and malicious emails can prevent ransomware attacks. Keeping systems patched helps ensure they aren't susceptible to known vulnerabilities. Training users decreases the possibility that they may respond inappropriately to malicious emails.

12. **C** is correct. The security consultant is identifying mission-essential functions, which is a key part of a business impact analysis (BIA). A single

point of failure is a component within a system that can cause the entire system to fail if the component fails. It's common to eliminate single points of failure of critical systems, but not all single points of failure are supporting mission-essential functions. Critical systems support mission-essential functions. However, if single points of failure have been eliminated, a critical system can fail but the mission-essential function will continue to operate. The mean time between failures (MTBF) identifies the average (the arithmetic mean) time between failures.

13. **B** is correct. A business impact analysis (BIA) includes information on potential losses and is the most likely document of those listed where this loss would be documented. A disaster recovery plan (DRP) includes methods used to recover from an outage. The mean time to repair (MTTR) identifies the average (the arithmetic mean) time it takes to restore a failed system. The recovery time objective (RTO) identifies the maximum amount of time it should take to restore a system after an outage.

14. **D** is correct. The recovery time objective (RTO) identifies the maximum amount of time it can take to restore a system after an outage. Because the business impact analysis states that the website can only tolerate three hours of downtime, this also identifies the RTO. The recovery point objective (RPO) identifies a point in time where data loss is acceptable, but it doesn't refer to downtime. The mean time to recover (MTTR) metric identifies the average (the arithmetic mean) time it takes to restore a failed system, but not a maximum amount of time a system can be down. The mean time between failures (MTBF) metric provides a measure of a system's reliability and is usually represented in hours. A disaster recovery plan (DRP) details the recovery steps to take after different types of disasters.

15. **B** is correct. This is a tabletop exercise. A tabletop exercise is discussion-based, and participants discuss their responses to various scenarios. A simulation is a hands-on exercise, not a meeting. Incident response refers to the actual steps taken in response to an incident (preparation, identification, containment, eradication, recovery, lessons learned), not a meeting discussing steps to take. Site resiliency is tested by

seeing if an alternate site (such as a hot site, cold site, or warm site) can take over if necessary, but the scenario doesn't discuss alternate sites.

Chapter 10

Understanding Cryptography and PKI

CompTIA Security+ objectives covered in this chapter:

1.2 Given a scenario, analyze potential indicators to determine the type of attack

- Password attacks (Spraying, Dictionary, Brute force, Offline, Online, Rainbow table, Plaintext/unencrypted)
- Cryptographic attacks (Birthday, Collision, Downgrade)

1.3 Given a scenario, analyze potential indicators associated with application attacks.

- Pass the hash

2.1 Explain the importance of security concepts in an enterprise environment.

- Data protection (Encryption, At rest, In transit/motion, In processing)
- Hashing

2.5 Given a scenario, implement cybersecurity resilience.

- Diversity (Crypto)

2.8 Summarize the basics of cryptographic concepts.

- Digital signatures, Key length, Key stretching, Salting, Hashing, Key exchange, Elliptical curve cryptography, Perfect forward secrecy, Quantum (Communications, Computing), Post-quantum, Ephemeral, Modes of operation (Authenticated, Unauthenticated, Counter), Blockchain (Public ledgers), Cipher suites (Stream, Block), Symmetric vs. asymmetric, Lightweight cryptography, Steganography (Audio, Video, Image), Homomorphic encryption
- Common use cases (Low power devices, Low latency, High resiliency, Supporting confidentiality, Supporting integrity, Supporting obfuscation, Supporting non-repudiation), Limitations (Speed, Size, Weak keys, Time, Longevity, Predictability, Reuse, Entropy, Computational overheads, Resource vs. security constraints)

3.1 Given a scenario, implement secure protocols.

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

3.9 Given a scenario, implement public key infrastructure.

- Public key infrastructure (PKI) (Key management, Certificate authority (CA), Intermediate CA, Registration authority (RA), Certificate revocation list (CRL), Certificate attributes, Online Certificate Status Protocol (OCSP), Certificate signing request (CSR), CN, Subject alternative name, Expiration)
- Types of certificates (Wildcard, Subject alternative name, Code signing, Self-signed, Machine/computer, Email, User, Root, Domain validation, Extended validation)
- Certificate formats (Distinguished encoding rules (DER), Privacy enhanced mail (PEM), Personal information exchange (PFX), .cer, P12, P7B), Concepts (Online vs.

offline CA, Stapling, Pinning, Trust model, Key escrow, Certificate chaining)

4.4 Given an incident, apply mitigation techniques or controls to secure an environment.

- Configuration changes (Update or revoke certificates)

**

Cryptography and Public Key Infrastructure (PKI) topics are challenging for many test takers, mostly because they include topics that aren't familiar to many system administrators. When tackling these topics, don't lose sight of the basics. The first section in this chapter, "Introducing Cryptography Concepts," outlines and summarizes these basics. Don't worry if they aren't clear to you right away—they should be once you complete the chapter. Passwords are commonly hashed and password attacks often try to exploit weaknesses in hashes. After hashes are explained, password attacks are explored. Other sections dig into the details of hashing, encryption, and Public Key Infrastructure (PKI) components.

Introducing Cryptography Concepts

Cryptography includes several important concepts that you need to grasp for the CompTIA Security+ exam, but the topics are often new to many information technology (IT) professionals.

As an introduction, the following bullets identify the important core cryptography concepts. Remember, this is only an overview. If these bullets don't make sense to you now, they should after you complete this chapter:

- **Integrity** provides assurances that data has not been modified.
Hashing ensures that data has retained integrity.
 - A **hash** is a number derived from performing a calculation on data, such as a message, patch, or file.
 - Hashing creates a fixed-length string of bits or hexadecimal characters, which cannot be reversed to re-create the original data.
 - A common hashing algorithm in use today is the Secure Hash Algorithm 3 (SHA-3).
- **Confidentiality** ensures that data is only viewable by authorized users. Encryption protects the confidentiality of data.
 - **Encryption** scrambles data to make it unreadable if intercepted. Encryption normally includes an algorithm and a key.
 - **Symmetric encryption** uses the same key to encrypt and decrypt data. Most symmetric algorithms use either a block cipher or a stream cipher.
 - **Stream ciphers** encrypt data 1 bit at a time. Block ciphers encrypt data in blocks.
 - **Asymmetric encryption** uses two keys (public and private) created as a matched pair.
 - Asymmetric encryption requires a Public Key Infrastructure (PKI) to issue certificates.
 - Anything encrypted with the public key can only be decrypted with the matching private key.
 - Anything encrypted with the private key can only be decrypted with the matching public key.

- **Steganography** provides a level of confidentiality by hiding data within other files. For example, it's possible to embed data within the white space of a picture file.
- A digital signature provides authentication, non-repudiation, and integrity.
 - **Authentication** validates an identity.
 - **Non-repudiation** prevents a party from denying an action.
 - Users sign emails with a digital signature, which is a hash of an email message encrypted with the sender's private key.
 - Only the sender's public key can decrypt the hash, providing verification it was encrypted with the sender's private key.

Providing Integrity with Hashing

You can verify integrity with hashing. Hashing is an algorithm performed on data such as a file or message to produce a number called a hash. The hash is used to verify that data is not modified, tampered with, or corrupted. In other words, you can verify the data has maintained integrity.

A key point about a hash is that no matter how many times you execute the hashing algorithm against the data, the hash will always be the same if the data is the same.

Hashes are created at least twice so that they can be compared. For example, imagine a software company is releasing a patch for an application that customers can download. They can calculate the hash of the patch and post both a link to the patch file and the hash on the company site. They might list it as:

- **Patch file.** Patch_v2_3.zip
- **SHA-3-256 hash.** d4723ac6f72daea2c779 ... 3ac113863c

The Secure Hash Algorithm 3 (SHA-3) hash is the calculated number displayed in hexadecimal. A SHA-3-256 hash is typically displayed as 64 hexadecimal characters, but I've shortened it for brevity. Customers can download the patch file and then calculate the hash on the downloaded file. If the calculated hash is the same as the hash posted on the web site, it verifies the file has retained integrity. In other words, the file has not changed. If you did the labs in Chapter 1, "Mastering Security Basics," you had an opportunity to do this yourself.

Remember this

Hashing verifies integrity for data such as email, downloaded files, and files stored on a disk. A hash is a number created with a hashing algorithm.

Hash Versus Checksum

Hashes and checksums are similar, but there are some differences. In general, hashes are much longer numbers and used in strong cryptographic implementations. A ***checksum*** is typically a small piece of data, sometimes only 1 or 2 bits, and is used to quickly verify the integrity of data.

As an example of a checksum, RAID-5 disk subsystems, described in Chapter 9, “Implementing Controls to Protect Assets,” use a single parity bit per byte and can identify corrupted data.

Similarly, the initial check for credit cards often uses a checksum. In a 16-digit credit card, the first six digits identify the institution that issued the card, the next nine represent the account number, and the 16th digit is a check digit or checksum. Imagine Homer enters his credit card online but inadvertently enters it incorrectly. One way this is checked is by calculating the checksum twice. First, it is calculated without the check digit, then it is calculated with the check digit. If both calculations are the same, it indicates the card number was entered correctly. If they’re different, the application typically displays an error before even trying to submit the charge.

Checksums are not intended to be cryptographically secure. Instead, they give a quick indication when data integrity has been lost. In contrast, strong hashing algorithms such as SHA-3 are cryptographically secure.

MD5

Message Digest 5 (**MD5**) is a common hashing algorithm that produces a 128-bit hash. Hashes are commonly shown in hexadecimal format instead of a stream of 1s and 0s. For example, an MD5 hash is displayed as 32 hexadecimal characters instead of 128 bits. Hexadecimal characters are composed of 4 bits and use the numbers 0 through 9 and the characters a through f.

MD5 has been in use since 1992. Experts discovered significant vulnerabilities in MD5 in 2004 and later years. As processing power of computers increased, it became easier and easier to exploit these vulnerabilities. Security experts now consider it cracked and discourage its use as a cryptographic hash.

However, it is still sometimes used to verify the integrity of files as a quick checksum. This includes email, files stored on disks, files downloaded from the Internet, executable files, and more. The “Hashing Files” section shows how you can manually calculate hashes.

Secure Hash Algorithms

Secure Hash Algorithms (**SHA**) are a group of hashing algorithms with variations in grouped four families—SHA-0, SHA-1, SHA-2, and SHA-3:

- SHA-0 is not used.
- SHA-1 is an updated version that creates 160-bit hashes. It is similar to the MD5 algorithm. Weaknesses were discovered and it is no longer approved for most cryptographic uses.
- SHA-2 improved SHA-1 to overcome potential weaknesses. It includes four versions. SHA-256 creates 256-bit hashes and SHA-512 creates 512-bit hashes. SHA-224 (224-bit hashes) and SHA-384 (384-bit hashes) create truncated versions of SHA-256 and SHA-512, respectively.
- SHA-3 (previously known as Keccak) is an alternative to SHA-2. The U.S. National Security Agency (NSA) created SHA-1 and SHA-2. SHA-3 was created outside of the NSA and was selected in a non-NSA public competition. It can create hashes of the same size as SHA-2 (224 bits, 256 bits, 384 bits, and 512 bits).

Just as MD5 is used to verify the integrity of files, SHA also verifies file integrity. As an example, it's rare for executable files to be modified. However, some malware modifies executable files by adding malicious code into the file.

Some host-based intrusion detection systems (HIDSs) and antivirus software capture hashes of files on a system when they first scan it and include valid hashes of system files in signature definition files. When they scan a system again, they can capture hashes of executable and system files and compare them with known good hashes. If the hashes are different for an executable or system file, it indicates the file has been modified, and it may have been modified by malware.

HMAC

Another method used to provide integrity is with a Hash-based Message Authentication Code (**HMAC**). An HMAC is a fixed-length string of bits similar to other hashing algorithms such as MD5 and SHA-256 (known as HMAC-MD5 and HMAC-SHA256, respectively). However, HMAC also uses a shared secret key to add some randomness to the result and only the sender and receiver know the secret key.

For example, imagine that one server is sending a message to another server using HMAC-MD5. It starts by first creating a hash of a message with MD5 and then uses a secret key to complete another calculation on the hash. The server then sends the message and the HMAC-MD5 hash to the second server. The second server performs the same calculations and compares the received HMAC-MD5 hash with its result. Just as with any other hash comparison, if the two hashes are the same, the message retained integrity, but if the hashes are different, the message lost integrity.

The HMAC hash provides both integrity and authenticity of messages. The MD5 portion of the hash provides integrity just as MD5 does. However, because only the server and receiver know the secret key, if the receiver can calculate the same HMAC-MD5 hash as the sender, it knows that the sender used the same key. If an attacker were trying to impersonate the sender, the message wouldn't pass this authenticity check because the attacker wouldn't have the secret key. Even though MD5 by itself isn't cryptographically secure, HMAC-MD5 is secure if the secret key is long enough.

Internet Protocol security (IPsec) and Transport Layer Security (TLS) often use a version of HMAC such as HMAC-MD5 and HMAC-SHA256.

Remember this

Two popular hashing algorithms used to verify integrity are MD5 and SHA-256. HMAC verifies both the integrity and authenticity of a message with the use of a shared secret. Other protocols such as IPsec and TLS use HMAC-MD5 and HMAC-SHA256.

Hashing Files

Many applications calculate and compare hashes automatically without any user intervention. For example, digital signatures (described later) use hashes within email, and email applications automatically create and compare the hashes.

Additionally, there are several applications you can use to manually calculate hashes. As an example, *sha256sum.exe* is a free program anyone can use to create hashes of files. If you did the lab “Create a Bootable USB” from Chapter 1, you saw this in action.

For example, the Kali Linux image I downloaded had the following hash:

acf455e6f9ab0720df0abed15799223c2445882b44dfcc3f2216f9464db79152 . Administrators at *kali.org* calculated the hash on the image and then posted both the image and the hash.

After I downloaded the image file, I calculated the hash on the downloaded file. Thankfully, it was the same. This provided proof that the file I downloaded was the file that the *kali.org* administrators posted on their site. If my hash was different, it would have indicated that the image file lost integrity. Either it had been modified after it was posted, or it lost some bits during the download. Either way, the file should not be trusted and should not be used.

Figure 10.1 shows this. By running the **sha256sum** command against the file, I calculated the hash. I first used the **dir** command to list the files in the directory. I then ran **sha256sum** against the Kali Linux file three times. Each time, **sha256sum** calculated the same hash, as shown in Figure 10.1.

```
Command Prompt
C:\Users\Darrell>cd /kaliiso

C:\KaliISO>dir
Volume in drive C is Windows
Volume Serial Number is 260A-97DE

Directory of C:\KaliISO

03/11/2020  01:18 PM    <DIR>      .
03/11/2020  01:18 PM    <DIR>      ..
03/09/2020  03:38 PM  2,948,083,712 kali-linux-2020.1-live-amd64.iso ←
03/11/2020  01:18 PM          73,216 sha256sum.exe ←
              2 File(s)  2,948,156,928 bytes
              2 Dir(s)  2,406,252,290,048 bytes free

C:\KaliISO>sha256sum kali-linux-2020.1-live-amd64.iso
acf45e6f9ab0720df0abed15799223c2445882b44dfcc3f2216f9464db79152 *kali-linux-2020.1-live-amd64.iso 1

C:\KaliISO>sha256sum kali-linux-2020.1-live-amd64.iso
acf45e6f9ab0720df0abed15799223c2445882b44dfcc3f2216f9464db79152 *kali-linux-2020.1-live-amd64.iso 2

C:\KaliISO>sha256sum kali-linux-2020.1-live-amd64.iso
acf45e6f9ab0720df0abed15799223c2445882b44dfcc3f2216f9464db79152 *kali-linux-2020.1-live-amd64.iso 3

C:\KaliISO>
```

Figure 10.1: Calculating a hash with sha256sum

Figure 10.1 demonstrates two important points:

- **The hash will always be the same no matter how many times you calculate it.**

In the figure, I ran sha256sum three times, but it would give me the same result if I ran it 3,000 times.

- **Hashing verifies the file has retained integrity.**

Because the calculated hash is the same as the hash posted on the download site, it verifies the file has not lost integrity.

It's worth stressing that hashes are one-way functions. In other words, you can calculate a hash on a file or a message, but you can't use the hash to reproduce the original data. The hashing algorithms always create a fixed-size bit string regardless of the size of the original data. The hash doesn't give you a clue about the size of the file, the type of the file, or anything else.

As an example, the SHA-1 hash from the message "I will pass the Security+ exam" is: 765591c4611be5e03bea41882ffdaa159352cf49.

However, you can't look at the hash and identify the message, or even know that it is a hash of a six-word message. Similarly, you can't look at the hash shown in Figure 10.1 and know that it was calculated from a 2.9-GB executable file.

Again, if you want to work with hashes yourself, check out the labs in the online resources for this book at <https://greatadministrator.com/sy0->

601-labs/

Hashing Messages

Hashing provides integrity for messages. It provides assurances to someone receiving a message that the message has not been modified. Imagine that Lisa is sending a message to Bart, as shown in Figure 10.2. The message is “The price is \$75.” This message is not secret, so there is no need to encrypt it. However, we do want to provide integrity, so this explanation is focused only on hashing.

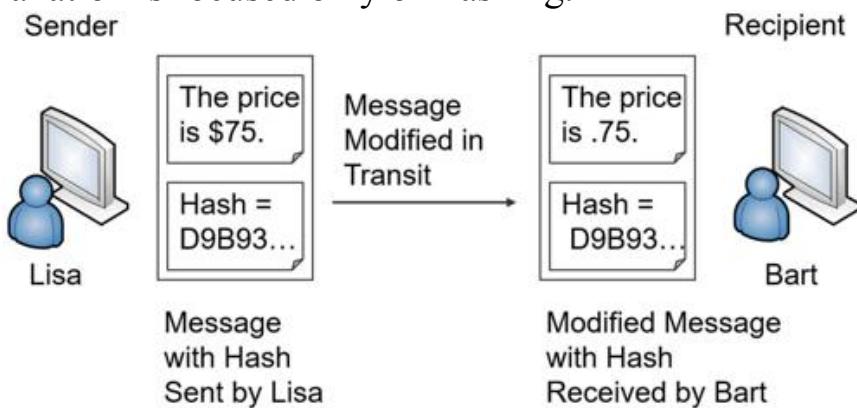


Figure 10.2: Simplified hash process

An application on Lisa’s computer calculates the MD5 hash as:

D9B93C99B62646ABD06C887039053F56.

In the figure, I’ve shortened the full hash down to just the first five characters of “D9B93.” Lisa then sends both the message and the hash to Bart.

In this example, something modified the message before it reaches Bart. When Bart receives the message and the original hash, the message is now “The price is .75.” Note that the message is modified in transit, but the hash is not modified.

A program on Bart’s computer calculates the MD5 hash on the received message as 564294439E1617F5628A3E3EB75643FE. It then compares the received hash with the calculated hash:

- The hash created on Lisa’s computer, and received by Bart’s computer is: D9B93C99B62646ABD06C887039053F56
- The hash created on Bart’s computer is:
564294439E1617F5628A3E3EB75643FE

Clearly, the hashes are different, so you know the message lost integrity. The program on Bart’s computer would report the discrepancy.

Bart doesn't know what caused the problem. It could have been a malicious attacker changing the message, or it could have been a technical problem. However, Bart does know the received message isn't the same as the sent message and he shouldn't trust it.

Using HMAC

You might have noticed a problem in the explanation of the hashed message. If an attacker can change the message, why can't the attacker change the hash, too? In other words, if Hacker Harry changed the message to "The price is .75," he could also calculate the hash on the modified message and replace the original hash with the modified hash. Here's the result:

- The hash created on Lisa's computer is:
D9B93C99B62646ABD06C887039053F56
- The modified hash inserted by the attacker after modifying the message is: 564294439E1617F5628A3E3EB75643FE
- The hash created for the modified message on Bart's computer is:
564294439E1617F5628A3E3EB75643FE

The calculated hash on the modified message would be the same as the received hash. This erroneously indicates that the message has maintained integrity. HMAC helps solve this problem.

With HMAC, both Lisa and Bart's computers would know the same secret key and use it to create an HMAC-MD5 hash instead of just an MD5 hash. Figure 10.3 shows the result.

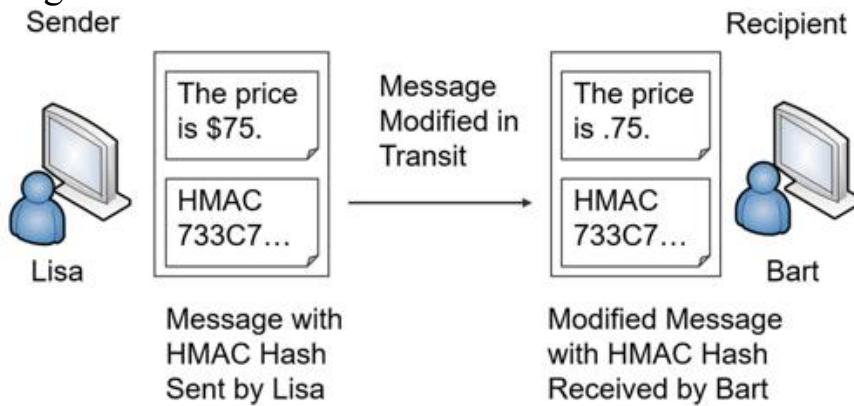


Figure 10.3: Using HMAC

Note that Lisa is still sending the same message. The MD5 hash is D9B93C99B62646ABD06C887039053F56. However, after applying the HMAC secret key, the HMAC-MD5 hash is 733C70A54A13744D5C2C9C4BA3B15034. For brevity, I shortened this to only the first five characters (733C7) in the figure.

An attacker can modify the message in transit just as before. However, the attacker doesn't know the secret key, so he can't calculate the HMAC hash.

Bart's computer calculates the HMAC-MD5 hash on the received message using the shared secret key. It then compares the calculated hash with the hash received from Lisa:

- The HMAC-MD5 hash created on Lisa's computer is:
733C70A54A13744D5C2C9C4BA3B15034
- The HMAC-MD5 hash created on Bart's computer is:
1B4FF0F6C04434BF97F1E3DDD4B6C137

Again, you can see that the hashes are different indicating the message has lost integrity. If the messages weren't modified, the HMAC-MD5 hash would be the same.

Remember this

If you can recognize the hashing algorithms such as MD5, SHA, and HMAC, it will help you answer some exam questions. For example, if a question asks what you would use to encrypt data and it lists three hashing algorithms, you can quickly eliminate them because hashing algorithms don't encrypt data.

Hashing Passwords

Most systems don't store the actual password for an account. Instead, they store a hash of the password. When a user creates a new password, the system calculates the hash for the password and then stores the hash. Similarly, passwords are rarely sent over the network in cleartext. Instead, the password hash is sent.

Later, when the user authenticates by entering a username and password, the system calculates the hash of the entered password, and then compares it with the stored hash. If the hashes are the same, it indicates that the user entered the correct password.

Unfortunately, tools are available to discover many hashed passwords. For example, MD5 Online <https://www.md5online.org/> allows you to enter a hash and it gives you the text of the password. If the password is 12345, the hash is 827ccb0eea8a706c4c34a16891f84e7b. If you enter that hash into MD5 Online, it returns the password of 12345 in less than a second. MD5 Online uses a database of hashed words from a dictionary. If the hash matches a database entry, the site returns the password.

Because of this, only strong hashing algorithms, such as SHA-3, should be used to store password hashes. However, even this isn't enough, and passwords are commonly salted, as described later in this chapter.

Remember this

Hashing is a one-way function that creates a string of characters. You cannot reverse the hash to re-create the original file. Passwords are often stored as hashes instead of storing the actual password. Additionally, applications often salt passwords with extra characters before hashing them.

Understanding Hash Collisions

A hash ***collision*** occurs when the hashing algorithm creates the same hash from different inputs. This is not desirable.

As an example, imagine a simple hashing algorithm creates three-digit hashes. The password “success” might create a hash of 123 and the password “passed” might create the same hash of 123. In this scenario, an attacker could use either “success” or “passed” as the password and both would work. The attacker doesn’t need to guess the correct password, only a password that creates the same hash.

MD5 is highly susceptible to collision attacks, which is why it is no longer recommended as a cryptographic hash.

Understanding Password Attacks

Password attacks attempt to discover, or bypass, passwords used for authentication on systems and networks, and for different types of files. Some password attacks are sophisticated cryptographic attacks, while others are rather simple brute force attacks.

An ***online password attack*** attempts to discover a password from an online system. For example, an attacker can try to log on to an account by repeatedly guessing the username and password. Many tools are available that attackers can use to automate the process. For example, ncrack is a free tool that can be used to run online brute force password attacks.

Offline password attacks attempt to discover passwords from a captured database or captured packet scan. For example, when attackers hack into a system or network causing a data breach, they can download entire databases. They then perform offline attacks to discover the passwords contained within these downloaded databases.

A primary indicator of online password attacks can be found in system logs that record successful and unsuccessful logons. These logs will show repeated attempts to guess passwords. In Windows systems, this is recorded as Event ID 4625 in the Security log available in Event Viewer. If the attacker enters the wrong password too many times, the system will lock the user account. This is recorded as Event ID 4740. The online labs show you how to create a custom filter to view these events.

Dictionary Attacks

A ***dictionary attack*** is one of the original password attacks. It uses a dictionary of words and attempts every word in the dictionary to see if it works. A dictionary in this context is simply a list of words and character combinations.

Dictionaries used in these attacks have evolved over time to reflect user behavior. Today, they include many of the common passwords that uneducated users configure for their accounts. For example, even though 12345 isn't a dictionary word, many people use it as a password, so character sets such as these have been added to many dictionaries used by dictionary attack tools.

These attacks are thwarted by using complex passwords. A complex password will not include words in a dictionary.

Brute Force Attacks

A ***brute force attack*** attempts to guess all possible character combinations. One of the first steps to thwart offline brute force attacks is to use complex passwords and to store the passwords in an encrypted or hashed format. Complex passwords include a mix of uppercase letters, lowercase letters, numbers, and special characters. Additionally, longer passwords are much more difficult to crack than shorter passwords.

Spraying Attacks

A password **spraying attack** is a special type of brute force or dictionary attack designed to avoid being locked out. An automated program starts with a large list of targeted user accounts. It then picks a password and tries it against every account in the list. It then picks another password and loops through the list again.

Chapter 2, “Understanding Identity and Access Management,” discusses account lockout policies used in Windows systems. They are effective against online brute force and dictionary attacks. An account lockout setting locks an account after the user enters the incorrect password a preset number of times in a short period of time. For example, if the user enters the wrong password three times in 30 minutes, the lockout policy locks the account.

Because a spraying attack loops through a long list of accounts, it takes a while before it hits the same account twice. This normally exceeds the time limit of account lockout settings, effectively bypassing the account lockout policy. However, you’ll still see Event ID 4625 indicating failed logon attempts but there will be a time lapse between each entry.

Remember this

Online attacks guess the password of an online system. Offline attacks guess the password stored within a downloaded file, such as a database. Logs will show a large volume of failed logon attempts as Event ID 4625 and/or several accounts being locked out as Event ID 4740. Spraying attacks attempt to avoid account lockout policies, but logs will still show a large volume of failed logon attempts, but with a time lapse between each entry.

Pass the Hash Attacks

In a ***pass the hash attack***, the attacker discovers the hash of the user's password and then uses it to log on to the system as the user. Any authentication protocol that passes the hash over the network in an unencrypted format is susceptible to this attack. It has been widely associated with Microsoft LAN Manager (LM) and NT LAN Manager (NTLM), two older security protocols used to authenticate Microsoft clients. However, this attack has enjoyed success against other protocols, such as Kerberos.

Attackers first try to gain administrative access to a system, either by gaining access as a member of the local Administrators group or gaining certain equivalent privileges. This is trivial if a user is logged on with an account that has administrator privileges. If the computer is infected with malware, the attacker has the same privileges as the logged-on user.

Once attackers have these privileges, they use them to steal password hashes stored in multiple locations on the computer, such as the Security Accounts Manager (SAM) database, the Local Security Authority Subsystem (LSASS) process, the Credential Manager (CredMan) store, and the LSA Secrets stored in the Registry.

A strong indicator of a pass the hash attack is the usage of NTLM as the Authentication Package and/or a Logon Process of NtLmSSP shown in Event ID 4624 in the Windows Security log. This can be correlated with Event ID 4672 to determine the privileges used with this connection. Normal users wouldn't use administrative privileges when connecting to other computers. However, an active pass the hash attack would use administrative privileges when moving laterally to similar computers around the network. The online labs show you how to search for and detect these events.

Remember this

Passwords are typically stored as hashes. A pass the hash attack attempts to use an intercepted hash to access an account. These attacks can be detected in Event ID 4624 with a Logon Process of NtLmSSP and/or an Authentication Package of NTLM.

Birthday Attacks

A ***birthday attack*** is named after the birthday paradox in mathematical probability theory. The birthday paradox states that for any random group of 23 people, there is a 50 percent chance that 2 of them have the same birthday. This is not the same year, but instead one of the 366 days in a year, including February 29.

In a birthday attack, an attacker attempts to create a password that produces the same hash as the user's actual password. This is also known as a hash collision, as described earlier. Using the knowledge of the birthday paradox, the attacker doesn't need to guess every possible password before discovering a collision. If the password could only be one of 366 possibilities, the attacker has a 50 percent chance of guessing it after only 23 attempts.

Birthday attacks on hashes are thwarted by increasing the number of bits used in the hash to increase the number of possible hashes. For example, the MD5 algorithm uses 128 bits and is susceptible to birthday attacks. SHA-3 can use as many as 512 bits and is not susceptible to birthday attacks.

Rainbow Table Attacks

Rainbow table attacks are a type of attack that attempts to discover the password from the hash. A rainbow table is a huge database of possible passwords with the precomputed hashes for each. It helps to look at the process of how some password cracker applications discover passwords without a rainbow table. Assume that an attacker has the hash of a password. The application can use the following steps to discover the password that matches the hash:

1. The application guesses a password (or uses a password from a dictionary).
2. The application hashes the guessed password.
3. The application compares the original password hash with the guessed password hash. If they are the same, the application now knows the password.
4. If they aren't the same, the application repeats steps 1 through 3 until finding a match.

From a computing perspective, the most time-consuming part of these steps is hashing the guessed password in step 2. However, by using rainbow tables, applications eliminate this step. Rainbow tables are huge databases of passwords and their calculated hashes. Some rainbow tables are as large as 690 GB in size, and they include hashes for every possible combination of characters up to nine characters in length. Larger rainbow tables are also available using more characters.

Rainbow table attacks are often performed offline on stolen or compromised databases. In a rainbow table attack, the application simply compares the hash of each password in the database against hashes stored in the rainbow table. When the application finds a match, it identifies the password used to create the hash (or at least text that can reproduce the hash of the original password). Admittedly, this is a simplistic explanation of a rainbow table attack, but it is adequate unless you plan on writing an algorithm to create your own rainbow table attack software.

Salting Passwords

Salting passwords is a common method of preventing rainbow table attacks, along with other password attacks such as brute force and dictionary attacks. A salt is a set of random data such as two additional characters. Password salting adds these additional characters to a password before hashing it. These additional characters add complexity to the password, and result in a different hash than the system would create using only the original password. This causes password attacks that compare hashes with a rainbow table to fail.

Remember this

Birthday attacks exploit collisions in hashing algorithms. A hash collision occurs when the hashing algorithm creates the same hash from different passwords. Salting adds random text to passwords before hashing them and thwarts many password attacks, including rainbow table attacks.

Key Stretching

Key stretching is an advanced technique used to increase the strength of stored passwords. Instead of just adding a salt to the password before hashing it, key stretching applies a cryptographic stretching algorithm to the salted password. The benefit of key stretching is that it consumes more time and computing resources—frustrating attackers who are trying to guess passwords.

Three common key stretching techniques are bcrypt, Password-Based Key Derivation Function 2 (PBKDF2), and Argon2.

Bcrypt is based on the Blowfish block cipher and is used on many Unix and Linux distributions to protect the passwords stored in the shadow password file. Bcrypt salts the password by adding additional random bits before encrypting it with Blowfish. Bcrypt can go through this process multiple times to further protect against attempts to discover the password. The result is a 60-character string.

As an example, if your password is IL0ve\$ecurity, an application can encrypt it with bcrypt and a salt. It might look like this, which the application stores in a database:

\$2b\$12\$HXIKtJr93DH59BzzKQhehOI9pGjRA/03ENcFRby1jH7nXwt1Tn0kG

Later, when a user authenticates with a username and password, the application runs bcrypt on the supplied password and compares it with the stored bcrypt-encrypted password. If the bcrypt result of the supplied password is the same as the stored bcrypt result, the user is authenticated.

As an added measure, it's possible to add some pepper to the salt to further randomize the bcrypt string. In this context, the pepper is another set of random bits stored elsewhere.

PBKDF2 uses salts of at least 64 bits and uses a pseudo-random function such as HMAC to protect passwords. Many algorithms such as Wi-Fi Protected Access II (WPA2), Apple's iOS mobile operating system, and Cisco operating systems use PBKDF2 to increase the security of passwords. Some applications send the password through the PBKDF2 process as many as 1,000,000 times to create the hash. The size of the resulting hash

varies with PBKDF2 depending on how it is implemented. Bit sizes of 128 bits, 256 bits, and 512 bits are most common.

A weakness with PBKDF2 is that it can be configured to use less computing time and less RAM. While this may seem beneficial to users, it also makes it easier for attackers, allowing them to guess many passwords in a short amount of time.

A Password Hashing Competition (PHC) in 2015 selected *Argon2* as an alternative key stretching algorithm. Like bcrypt and PBKDF2, Argon2 uses a password and salt that is passed through an algorithm several times. Argon2 has been improved with each new version using a lowercase letter such as Argon2d and Argon2i.

Remember this

Bcrypt, PBKDF2, and Argon2 are key stretching techniques that help prevent brute force and rainbow table attacks. They salt the password with additional bits and then send the result through a cryptographic algorithm.

Providing Confidentiality with Encryption

Encryption provides confidentiality and prevents unauthorized disclosure of data. Plaintext is human-readable data. An encryption algorithm scrambles the data, creating ciphertext, which is unreadable. Attackers can't read encrypted traffic sent over a network or encrypted data stored on a system. In contrast, if data is sent in cleartext, an attacker can capture and read the data using a protocol analyzer.

Data at rest refers to any data stored on media and it's common to encrypt sensitive data. For example, it's possible to encrypt individual fields in a database (such as the fields holding customer credit card data), individual files, folders, or a full disk.

Data in transit or **data in motion** refers to any data sent over a network and it's common to encrypt sensitive data in transit. For example, e-commerce web sites commonly use Hypertext Transfer Protocol Secure (HTTPS) sessions to encrypt transactions that include credit card data. If attackers intercept the transmissions, they only see ciphertext.

Data in processing (sometimes called data in use) refers to data being used by a computer. Because the computer needs to process the data, it is not encrypted while in use. If the data is encrypted, an application will decrypt it and store it in memory while in use. If the application changes the data, it will encrypt it again before saving it. Additionally, applications usually take extra steps to purge memory of sensitive data after processing it.

The two primary encryption methods are symmetric and asymmetric. Symmetric encryption encrypts and decrypts data with the same key. Asymmetric encryption encrypts and decrypts data using a matched key pair of a public key and a private key.

These encryption methods include two elements:

- **Algorithm.** The algorithm performs mathematical calculations on data. The algorithm is always the same.
- **Key.** The key is a number that provides variability for the encryption. It is either kept private and/or changed frequently.

Remember this

Encryption provides confidentiality and helps ensure that data is viewable only by authorized users. This applies to any data at rest (such as data stored in a database) or data in transit being sent over a network.

Symmetric Encryption

Symmetric encryption uses the same key to encrypt and decrypt data. In other words, if you encrypt data with a key of three, you decrypt it with the same key of three. Symmetric encryption is also called secret-key encryption or session-key encryption.

As a simple example, when I was a child, a friend and I used to pass encoded messages back and forth to each other. Our algorithm was:

- **Encryption algorithm.** Move X spaces forward to encrypt.
- **Decryption algorithm.** Move X spaces backward to decrypt.

On the way to school, we would identify the key (X) we would use that day. For example, we may have used the key of three one day. If I wanted to encrypt a message, I would move each character three spaces forward, and he would decrypt the message by moving three spaces backward.

Imagine the message “PASS” needs to be sent:

- Three characters past “P” is “S”—Start at P (Q, R, S)
- Three characters past “A” is “D”—Start at A (B, C, D)
- Three characters past “S” is “V”—Start at S (T, U, V)
- Three characters past “S” is “V”—Start at S (T, U, V)

The encrypted message is SDVV. My friend decrypted it by moving backward three spaces and learned that “PASS” was the original message.

We were using a simple substitution cipher. A substitution cipher replaces **plaintext** with **ciphertext** using a fixed system. In the example, “PASS” is the plaintext, “SDVV” is the ciphertext, and the fixed system is three letters.

The **ROT13** (short for rotate 13 places) cipher uses the same substitution algorithm, but always uses a key of 13. To encrypt a message, you would rotate each letter 13 spaces. To decrypt a message, you would rotate each letter 13 spaces. However, because ROT13 uses both the same algorithm and the same key, it doesn’t provide true encryption but instead just obfuscates the data.

Obfuscation methods attempt to make something unclear or difficult to understand. This is sometimes referred to as security through obscurity.

However, security through obscurity is rarely a reliable method of maintaining security.

Rotating letters with a key shows how symmetric encryption methods fail if the same key isn't used for encryption and decryption. If I encrypted the message with a key of three, and my friend tried to decrypt it with a key of six, he would get a completely different message.

Sophisticated symmetric encryption techniques use the same components of an algorithm and a key. However, the algorithms and keys are much more complex. For example, the Advanced Encryption Standard (AES) symmetric algorithm typically uses 128-bit keys but can use keys with 192 or 256 bits.

Imagine two servers sending encrypted traffic back and forth to each other using AES symmetric encryption. They both use the same AES algorithm and the same key for this data. The data is encrypted on one server with AES and a key, sent over the wire or other transmission medium, and the same key is used to decrypt it on the other server. Similarly, if a database includes encrypted data, the key used to encrypt this data is the same key used to decrypt the data.

However, symmetric encryption doesn't use the same key to encrypt and decrypt all data. For example, my friend and I used a different key each day. On the way to school, we decided on a key to use for that day. The next day, we picked a different key. If someone cracked our code yesterday, they couldn't crack our code today using the same key.

Symmetric encryption algorithms change keys much more often than once a day. For example, imagine an algorithm uses a key of 123 to encrypt a project file. It could then use a key of 456 to encrypt a spreadsheet file. The key of 123 can only decrypt the project file and the key of 456 can only decrypt the spreadsheet file.

On the other hand, if symmetric encryption always used the same key of 123, it would add significant vulnerabilities. First, when keys are reused, the encryption is easier to crack. Second, once the key is cracked, all data encrypted with this key is compromised. If attackers discover the key of 123, not only would they have access to the project file, but they would also have access to the spreadsheet file and any other data encrypted with this same key.

As a more realistic example, Chapter 4, “Securing Your Network,” describes how Remote Authentication Dial-In User Service (RADIUS) encrypts password packets. RADIUS uses shared keys for symmetric encryption. When users authenticate, RADIUS servers and clients use the shared key to encrypt and decrypt data exchanged in a challenge/response session. Without the shared key, clients are unable to decrypt the data and respond appropriately.

Comparing Symmetric Encryption to a Door Key

Occasionally, security professionals compare symmetric keys to a house key, and this analogy helps some people understand symmetric encryption a little better. For example, imagine Marge moves into a new home. She'll receive a single key that she can use to lock and unlock her home. Of course, Marge can't use this key to unlock the Flanders' home.

Later, Marge marries Homer, and Homer moves into Marge's home. Marge can create a copy of her house key and give it to Homer. Homer can now use that copy of the key to lock and unlock the house. By sharing copies of the same key, it doesn't matter whether Marge or Homer is the one who locks the door; they can both unlock it.

Similarly, symmetric encryption uses a single key to encrypt and decrypt data. If a copy of the symmetric key is shared, others who have the key can also encrypt and decrypt data.

Remember this

Symmetric encryption uses the same key to encrypt and decrypt data. For example, when transmitting encrypted data, symmetric encryption algorithms use the same key to encrypt and decrypt data at both ends of the transmission media. RADIUS uses symmetric encryption.

Block Versus Stream Ciphers

Most symmetric algorithm cipher suites use either a block cipher or a stream cipher. They are both symmetric, so they both use the same key to encrypt or decrypt data. However, they divide data in different ways.

A ***block cipher*** encrypts data in specific-sized blocks, such as 64-bit blocks or 128-bit blocks. The block cipher divides large files or messages into these blocks and then encrypts each individual block separately. A ***stream cipher*** encrypts data as a stream of bits or bytes rather than dividing it into blocks.

In general, stream ciphers are more efficient than block ciphers when the size of the data is unknown or sent in a continuous stream, such as when streaming audio and video over a network. Block ciphers are more efficient when the size of the data is known, such as when encrypting a file or a specific-sized database field.

An important principle when using a stream cipher is that encryption keys should never be reused. If a key is reused, it is easier to crack the encryption.

Remember this

Stream ciphers encrypt data a single bit, or a single byte, at a time in a stream. Block ciphers encrypt data in a specific-sized block such as 64-bit or 128-bit blocks. Stream ciphers are more efficient than block ciphers when encrypting data in a continuous stream.

Common Symmetric Algorithms

The following sections describe some commonly used symmetric algorithms. This isn't meant to be an exhaustive list of all symmetric algorithms, but instead a short listing of some that are commonly used.

AES

The Advanced Encryption Standard (*AES*) is a strong symmetric block cipher that encrypts data in 128-bit blocks. The National Institute of Standards and Technology (NIST) adopted AES from the Rijndael encryption algorithm after a lengthy evaluation of several different algorithms.

AES can use key sizes of 128 bits, 192 bits, or 256 bits, and it's sometimes referred to as AES-128, AES-192, or AES-256 to identify how many bits are used in the key. When more bits are used, it makes it more difficult to discover the key and decrypt the data. AES-128 provides strong protection, but AES-256 provides stronger protection.

In general, the size of the key for any encryption directly corresponds to the key strength. Longer keys for a specific algorithm result in stronger key strength.

Because of its strengths, AES has been adopted in a wide assortment of applications. For example, many applications that encrypt data on USB drives use AES. Some of the strengths of AES are:

- **Fast.** AES uses elegant mathematical formulas and only requires one pass to encrypt and decrypt data. In contrast, 3DES (mentioned later in this chapter) requires multiple passes to encrypt and decrypt data.
- **Efficient.** AES is less resource intensive than other encryption algorithms such as 3DES. AES encrypts and decrypts quickly even when ciphering data on small devices, such as USB flash drives.
- **Strong.** AES provides strong encryption of data, providing a high level of confidentiality.

3DES

3DES (pronounced as “Triple DES”) is a symmetric block cipher designed as an improvement over the known weaknesses of the legacy Data Encryption Standard (DES). In basic terms, it encrypts data using the DES algorithm in three separate passes and uses multiple keys. 3DES encrypts data in 64-bit blocks.

Although 3DES is a strong algorithm, it isn’t used as often as AES today. AES is much less resource intensive. However, if hardware doesn’t support AES, 3DES is a suitable alternative. 3DES uses key sizes of 56 bits, 112 bits, or 168 bits.

Remember this

AES is a strong symmetric block cipher that encrypts data in 128-bit blocks. AES uses 128-bit, 192-bit, or 256-bit keys. 3DES is a block cipher that encrypts data in 64-bit blocks. 3DES was originally designed as a replacement for DES, but NIST selected AES as the current standard. However, 3DES is still used in some applications, such as when legacy hardware doesn’t support AES.

Blowfish and Twofish

Blowfish is a strong symmetric block cipher that is still widely used today. It encrypts data in 64-bit blocks and supports key sizes between 32 and 448 bits. Bruce Schneier (a widely respected voice in IT security) designed Blowfish as a general-purpose algorithm to replace DES.

Interestingly, Blowfish is faster than AES in some instances. This is especially true when comparing Blowfish with AES-256. Part of the reason is that Blowfish encrypts data in smaller 64-bit blocks, whereas AES encrypts data in 128-bit blocks.

Twofish is related to Blowfish, but it encrypts data in 128-bit blocks, and it supports 128-, 192-, or 256-bit keys. It was also one of the finalist algorithms evaluated by NIST.

Asymmetric Encryption

Asymmetric encryption uses two keys in a matched pair to encrypt and decrypt data—a public key and a private key. There are several important points to remember with these keys:

- If the ***public key*** encrypts information, only the matching private key can decrypt the same information.
- If the ***private key*** encrypts information, only the matching public key can decrypt the same information.
- Private keys are always kept private and never shared.
- Public keys are freely shared by embedding them in a shared certificate.

Remember this

Only a private key can decrypt information encrypted with a matching public key. Only a public key can decrypt information encrypted with a matching private key. A key element of several asymmetric encryption methods is that they require a certificate and a PKI.

Although asymmetric encryption is strong, it is also very resource intensive. It takes a significant amount of processing power to encrypt and decrypt data, especially when compared with symmetric encryption. Most cryptographic protocols that use asymmetric encryption only use it for key exchange.

Key Exchange

Key exchange is a cryptographic method used to share cryptographic keys between two entities. In this context, asymmetric encryption uses key exchange to share a symmetric key. The cryptographic protocol then uses the symmetric encryption to encrypt and decrypt data because symmetric encryption is much more efficient.

The key is that the two entities need to be able to identify a symmetric key that they both know and can use. However, the exchange needs to be encrypted so that no one else knows the symmetric key. The “Encrypting HTTPS Traffic with TLS” section later in this chapter digs deeper into the key exchange method.

Some of the more advanced topics related to asymmetric encryption become harder to understand if you don't understand the relationship of matched public and private key pairs. However, because you can't see these keys, the concepts are hard to grasp for some people. The Rayburn box demonstrates how you can use physical keys for the same purposes as these public and private keys.

The Rayburn Box

I often talk about the Rayburn box in the classroom to help people understand the usage of public and private keys. A Rayburn box is a lockbox that allows people to securely transfer items over long distances. It has two keys. One key can lock the box but can't unlock it. The other key can unlock the box but can't lock it.

Both keys are matched to one box and won't work with other boxes:

- Only one copy of one key exists—think of it as the private key.
- Multiple copies of the other key exist, and copies are freely made and distributed—think of these as public keys.

The box comes in two different versions. In one version, it's used to send secrets in a confidential manner to prevent unauthorized disclosure. In the other version, it's used to send messages with authentication, so you know the sender sent the message and that the message wasn't modified in transit.

The Rayburn Box Used to Send Secrets

Imagine that I wanted you to send some proprietary information and a working model of an invention to me. Obviously, we wouldn't want anyone else to be able to access the information or the working model. I could send you the empty open box with a copy of the key used to lock it. You place everything in the box and then lock it with the public key I've sent with the box.

This key can't unlock the box, so even if other people had copies of the public key that I sent to you, they couldn't use it to unlock the box. When I receive the box from you, I can unlock it with the only key that will unlock it—my private key.

This is similar to how public and private keys are used to send encrypted data over the Internet to ensure confidentiality. The public key

encrypts information. Information encrypted with a public key can only be decrypted with the matching private key. Many copies of the public key are available, but only one private key exists, and the private key always stays private. The “Encrypting HTTPS Traffic with TLS” section later in this chapter shows this process in more depth.

The Rayburn Box Used for Authentication

With a little rekeying of the box, I can use it to send messages while giving assurances to recipients that I sent the message. In this context, the message isn’t secret and doesn’t need to be protected. Instead, it’s important that you know I sent the message.

When used this way, the private key will lock the Rayburn box, but it cannot unlock the box. Instead, only a matching public key can unlock it. Multiple copies of the public key exist and anyone with a public key can unlock the box. However, after unlocking the box with a matching public key, it isn’t possible to lock it with the public key.

Imagine that you and I are allies in a battle. I want to give you a message of “SY0-601,” which is a code telling you to launch a specific attack at a specific time. We don’t care if someone reads this message because it’s a code. However, we need you to have assurances that I sent the message.

I write the message, place it in the box, and lock it with my private key. When you receive it, you can unlock it with the matching public key. Because the public key opens it, you know this is my box and it was locked with my private key—you know I sent the message.

If an enemy spy intercepted the box and opened it with the public key, the spy wouldn’t be able to lock it again using the public key, so you’d receive an open box. The spy could replace the message with something else. However, an open box with a message inside it doesn’t prove I sent it. The only way you know that I sent it is if you receive a locked box that you can unlock with the matching public key.

This is similar to how digital signatures use public and private keys. The “Signing Email with Digital Signatures” section later in this chapter explains digital signatures in more depth. In short, I can send you a message digitally signed with my private key. If you can decrypt the digital signature with my matching public key, you know it was encrypted, or signed, with

my private key. Because only one copy of the private key exists, and I'm the only person who can access it, you know I sent the message.

The Rayburn Box Demystified

Before you try to find a Rayburn box, let me clear something up. The Rayburn box is just a figment of my imagination. Rayburn is my middle name.

I haven't discovered a real-world example of how public/private keys work, so I've created the Rayburn box as a metaphor to help people visualize how public/private keys work. Feel free to build one if you want.

Certificates

A key element of asymmetric encryption is a certificate. A certificate is a digital document that typically includes the public key and information on the owner of the certificate. Certificate authorities (CAs, explored in greater depth later in this chapter) issue and manage certificates.

Certificates are used for a variety of purposes beyond just asymmetric encryption, including authentication and digital signatures.

Figure 10.4 shows a sample certificate with the public key selected. Users and applications share the certificate file to share the public key. They do not share the private key.

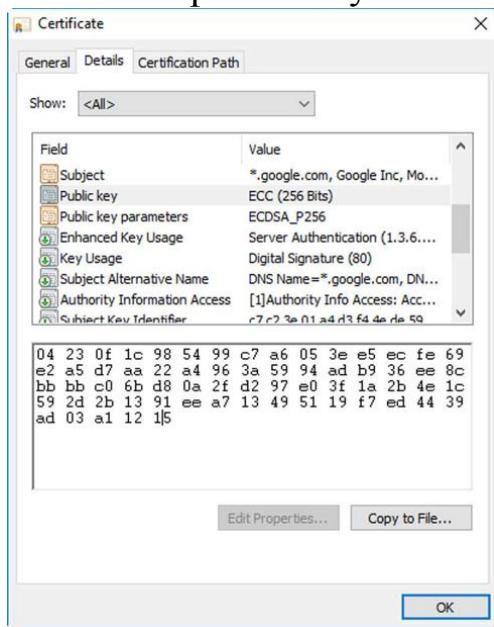


Figure 10.4: Certificate with public key selected

There is much more information in the certificate than just the public key, but not all of it is visible in the figure. Common elements within a certificate include:

- **Serial number.** The serial number uniquely identifies the certificate. The CA uses this serial number to validate a certificate. If the CA revokes the certificate, it publishes this serial number in a certificate revocation list (CRL).
- **Issuer.** This identifies the CA that issued the certificate.

- **Validity dates.** Certificates include “Valid From” and “Valid To” dates. These identify expiration dates.
- **Subject.** This identifies the owner of the certificate. In the figure, it identifies the subject as Google, Inc and indicates this is a wildcard certificate used for all web sites with the google.com root domain name.
- **Public key.** Asymmetric encryption uses the public key in combination with the matching private key.
- **Usage.** Some certificates are only for encryption or authentication, whereas other certificates support multiple usages.

Certificate attributes identify the issuer using Distinguished Name attributes. Some common attributes are:

- CN: CommonName (also known as the Fully Qualified Domain Name such as letsencrypt.org)
- o: Organization (such as the Internet Security Research Group)
- L: Locality (such as Mountain View)
- S: StateOrProvinceName (such as CA)
- C: CountryName (such as US)

If you want to view a certificate, check out the “How to View a Certificate” lab in the online labs for this book at <https://greatadministrator.com/sy0-601-labs/>.

Remember this

Certificates are an important part of asymmetric encryption. Certificates include public keys along with details on the owner of the certificate and on the CA that issued the certificate. Certificate owners share their public key by sharing a copy of their certificate.

Ephemeral Keys

Ephemeral refers to something that lasts a short time. In the context of cryptography, an ephemeral key has a short lifetime and is re-created for each session. In contrast, a static key is semipermanent and stays the same over a long period of time.

An ephemeral key pair includes a private ephemeral key and a public ephemeral key. Systems use these key pairs for a single session and then discard them. Some versions of Diffie-Hellman use ephemeral keys.

Certificates are based on static keys. A certificate includes an embedded public key matched to a private key and this key pair is valid for the lifetime of a certificate, such as a year. Certificates have expiration dates and systems continue to use these keys until the certificate expires. A benefit of static keys is that a CA can validate them as discussed in the “Validating a Certificate” section later in this chapter.

Perfect forward secrecy is an important characteristic that ephemeral keys comply with in asymmetric encryption. Perfect forward secrecy indicates that a cryptographic system generates random public keys for each session, and it doesn’t use a deterministic algorithm to do so. In other words, given the same input, the algorithm will create a different public key. This helps ensure that systems do not reuse keys. The result is that the compromise of a key does not compromise any past keys.

Elliptic Curve Cryptography

Elliptic curve cryptography (ECC) doesn't take as much processing power as other cryptographic methods. It uses mathematical equations to formulate an elliptical curve. It then graphs points on the curve to create keys. A key benefit is that ECC keys can be much smaller when compared with non-ECC keys.

Digital signatures (described later in this chapter) are commonly used to sign emails. The Digital Signature Algorithm (DSA) uses key pairs managed by a PKI with the public key distributed in a certificate. The Elliptic Curve Digital Signature Algorithm (ECDSA) can also be used for digital signatures. A 256-bit elliptic curve public key is said to provide the same security benefit of a 3072-bit key used with DSA.

Because of this, ECC is often considered with common use cases of low power devices. For example, ECC is sometimes used with small wireless devices because it doesn't take much processing power to achieve the desired security.

Quantum Computing

Quantum cryptography uses quantum mechanical properties to perform cryptographic tasks. Don't worry, you don't need to be a quantum physicist to understand the basics.

In regular computing, any single bit can be either a 0 or a 1. In quantum computing, quantum bits (or qubits) are used. A qubit can be two values at the same time. Superposition allows qubits to be superposed (or added together), creating the second quantum state.

Additionally, in regular computing, the value of any single bit is not dependent on other bits. However, in quantum computing, a qubit can be entangled with other qubits. This entanglement creates a dependency between the qubits, with the value of one qubit dependent on the value of other entangled qubits.

Another quirk about quantum computing is that it is impossible to copy data when it's stored in a quantum state. Any attempt to read the data changes it. This is also known as the no cloning theorem.

Quantum communication takes advantage of superposition, entanglement, and the no cloning theorem. It transfers the qubits and if the data is intercepted or read by an attacker, the data changes—leaving a clear indication of the possible hack.

Quantum Cryptography

Quantum key distribution (QKD) is one example of quantum cryptography. It allows two parties to establish a shared key, similar to how asymmetric encryption is used to allow two parties to establish a shared key used with symmetric encryption.

As an example, imagine Bart and Lisa are in different cities. They can use QKD to establish a quantum connection and share a symmetric key. Once it's established, only Bart and Lisa know the symmetric key and they can use it to share encrypted data.

What if Hacker Harry established a man-in-the-middle connection and attempted to intercept the shared key? Because of the no cloning theorem, when Hacker Harry intercepts the QKD connection, he changes the data.

However, this also alerts Bart and Lisa that something is wrong. Once the data is changed, it corrupts the QKD connection.

Post-Quantum Cryptography

Post-quantum cryptography (also known as quantum-proof or quantum-resistant) refers to cryptographic algorithms that are likely to be resistant to attacks using a quantum computer.

Physicists estimate that a quantum computer could easily exceed the power of the most powerful computers. Google reportedly built a 53-qubit quantum computer proving this, solving a complex mathematical calculation in about 3 ½ minutes. It's estimated that Summit, one of the world's fastest supercomputers, would take about 10,000 years to solve the same problem.

Quantum computers are currently extremely expensive. However, as with other computing resources, the cost will come down. And when they do, attackers are likely to start using them in cryptographic attacks.

NIST released a "Call for Proposals Announcement" in 2017, which "initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms." The goal is to identify new algorithms that will be able to protect data, even if attackers are using quantum computers.

Round 2 candidates were announced in January 2019 and NIST began collecting comments on them. They expect to whittle this down and announce Round 3 candidates in 2020 or 2021. Sometime in 2022 to 2024, they expect to release a draft of selected standards.

Lightweight Cryptography

Lightweight cryptography refers to cryptography deployed to smaller devices such as radio frequency identification (RFID) tags, sensor nodes, smart cards, health care devices, and Internet of Things (IoT) devices.

Unlike servers and desktop computers, these smaller devices have limited processing power. The smaller devices either don't have the ability to implement strong cryptography, or when they do, it severely limits the device's performance.

NIST has been digging into the needs related to lightweight cryptography for years. In 2017, they published a white paper asking for algorithms that could be used for lightweight cryptography. Round 1 ended with 56 candidates and 32 were selected to continue to Round 2. They are expected to announce finalists in September 2020.

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) have published ISO/IEC 29192- "Information technology – Security Techniques – Lightweight cryptography." It includes multiple parts that have been released over the years on various cryptographic functions that can be considered for lightweight cryptography. However, unlike NIST, which is available to the public domain, ISO/IEC documents must be purchased.

ISO/IEC 29192-2:2019 identifies several lightweight block ciphers that are suitable for lightweight cryptography, such as:

- Present has a block size of 64 bits and a key size of 80 or 128 bits. It is said to be about 2.5 times smaller than AES.
- CLEFIA has a block size of 128 bits and a key size of 128, 192, or 256 bits. Clefia was developed by Sony. Its name is derived by the French word clef, meaning key.
- LEA, short for lightweight encryption algorithm, has a block size of 128 bits and a key size of 128, 192, or 256 bits.

Homomorphic Encryption

Homomorphic encryption allows data to remain encrypted while it is being processed. This allows people to access and manipulate the data without being able to see it because it remains encrypted.

Most homomorphic encryption methods work best when data is stored and manipulated as integers. Encryption schemes typically focus on a single mathematical computation such as addition, multiplication, subtraction, or division, while some have modules that allow them to do all the basic computations.

Some industries want to share data, but data privacy issues prevent them from doing so. As an example, health care organizations often want to share data such as how many patients have a disease, how many are in specific age groups, how many responded to certain therapies, and so on. A centralized system using homomorphic encryption can allow multiple health care organizations to submit their data in an encrypted form and the centralized database can be updated in real time.

Remember this

Lightweight cryptography refers to cryptographic methods that can be deployed on smaller devices such as wireless devices and IoT devices. Homomorphic encryption allows data to remain encrypted while it is being processed.

Key Length

Because the algorithm always stays the same, the way that any individual algorithm is strengthened is by increasing the length of a key. As an example, consider RSA (Rivest-Shamir-Adleman), the primary public key cryptography algorithm used on the Internet. It supports key sizes of 1024, 2048, and 4096.

NIST indicated that 1024 keys were strong enough through 2010, but they predicted that computing power would be strong enough in 2011 that attackers could crack it. They recommended deprecating 1024-bit keys by 2011 and implementing 2048 keys.

Based on the expected advances of computer technologies, NIST predicts that 2048-bit keys should be safe until 2030. After then, 4096-bit keys will be needed if RSA is still in widespread use.

Modes of Operation

Authenticated encryption modes ensure the confidentiality of data and the authenticity of the data. Confidentiality is provided with encryption. In this context, authenticity allows you to verify that data came from a trusted entity and that the data hasn't lost integrity.

Many authenticated encryption implementations are in use with symmetric block ciphers. They commonly combine a symmetric encryption algorithm with a message authentication code (MAC) but can use various methods. The key is that the authentication is performed on each block when used with block ciphers.

As one example, imagine Homer is visiting a web site using TLS. His computer and the web site establish a session and share symmetric keys. One key is used to encrypt the web pages before sending them. The second key is used with a hash function on the ciphertext to create a MAC. Note that at this point, only the web site and Homer's computer know these keys. The web site then sends the ciphertext and the MAC to Homer.

Homer's computer uses the second key with the hash function to recalculate the MAC. If the recalculated MAC is the same as the sent MAC, it provides authenticity by proving that the data was sent by the web site and that the data hasn't changed. The first key is then used to decrypt the ciphertext.

A counter mode cipher (CTR) effectively converts a block cipher into a stream cipher. It combines an initialization vector (IV) with a counter and uses the result to encrypt each plaintext block. The IV is a fixed-size random or pseudo-random number that helps create random encryption keys and it provides a starting value for a cryptographic algorithm.

Each block uses the same IV, but CTR combines it with the counter value, resulting in a different encryption key for each block. Multiprocessor systems can encrypt or decrypt multiple blocks at the same time, allowing the algorithm to be quicker on multiprocessor or multicore systems. CTR is widely used and respected as a secure mode of operation.

CTR provides authenticated encryption. The IV and the starting counter are known to parties in the conversation, like the symmetric key in the authenticated encryption model is known to both entities.

The unauthenticated mode is sometimes referred to as better-than-nothing security. It provides confidentiality with encryption but doesn't provide authenticity.

Remember this

Three common encryption modes of operation used with encryption are authenticated, counter, and unauthenticated. Authenticated encryption provides both confidentiality and authenticity. Counter (CTR) mode is a form of authenticated encryption and CTR modes allow block ciphers to function as stream ciphers. Unauthenticated mode provides confidentiality, but not authenticity.

Steganography

Steganography hides data inside other data, or, as some people have said, it hides data in plain sight. The goal is to hide the data in such a way that no one suspects there is a hidden message. However, if other people know what to look for, they will be able to retrieve the message.

It doesn't encrypt the data, so it can't be classified as either symmetric or asymmetric. However, it can effectively hide information using obfuscation. Obfuscation methods attempt to make something unclear or difficult to understand.

Security professionals use steganalysis techniques to detect steganography, and the most common method is with hashing. If a single bit of a file is modified, the hashing algorithm creates a different hash. By regularly taking the hashes of different files and comparing them with previous hashes, it's easy to detect when a file has been modified.

There are three primary types of files used with steganography. They are audio files, image files, and video files.

Audio Steganography

Audio steganography takes advantage of the limitations of a human ear. Ideally, a human ear can detect sounds in the frequency range of 20 Hz and 20 KHz. Most humans can't detect sounds between 18 KHz and 20 KHz, but these sounds can be detected by most microphones. These sounds, commonly called audio beacons, are used to identify user activity.

SilverPush, an India-based advertising company, used this to track users. Its software developer kit (SDK) includes the ability to hear the audio beacons, and once the apps are installed, the app constantly listens for them. Some television advertisements include audio beacons and the SilverPush apps reported back to SilverPush servers when a user device heard the beacon. This helped them determine what commercials and, ultimately, what shows users were watching.

SilverPush claimed to have stopped doing this in 2016 but other app developers were still using the SilverPush SDK. In 2017, researchers found over 200 Android-based apps that included this SDK were downloaded millions of times from Google Play.

Some audio beacons are used by marketers within stores. They track the location of shoppers as they move through a large store. Apps then send ads or coupons based on the shopper's location.

This technology can also be used to perform cross-device tracking to determine what devices belong to an individual. Apps send audio beacons from one device. When another device repeatedly hears this same beacon, it indicates it is owned by the same user.

Image Steganography

Image steganography is the practice of hiding data within image files such as a .jpeg or .gif file. Two common ways this is done is by manipulating the bits of a file or by hiding data in the white space.

You can embed a message into a file by modifying the least significant bit in some of the individual bytes of a file. Because you are modifying the least significant bit, the changes to the file won't be perceptible to anyone viewing the image. As an example, imagine a pixel of an image is red (having the RGB value of 255, 0, 0). If you change the least significant bit of red from 255 to 254, giving the pixel a value of 254, 0, 0, the change can't be perceived on a monitor. If the image file is large, it's possible to hide a large file within it.

Many files have unused space (called white space) at the end of file clusters. Imagine a small 6-KB file stored in two 4-KB clusters. It has an extra 2 KB of unused space and it's possible to fill this white space with a message. A benefit of using this method is that it is possible to embed a message without altering the size of the file.

Check out the "Hiding Files with Steganography" lab at <https://greatadministrator.com/sy0-601-labs/> to see how to embed a message into an image file.

Video Steganography

Video steganography is an extension of image steganography and it embeds messages into videos. Videos have become quite popular on the Internet through sites such as Facebook, YouTube, and TikTok.

Because video files are typically large, a common method is to modify the least significant bits of some bytes within the file to embed a message. A drawback of video steganography is that it can cause noise in the audio.

To avoid this, many video steganography methods only modify the image portion of video files and they leave the audio portion intact.

Remember this

Steganography hides messages or other data within a file. Security professionals use hashing to detect changes in files that may indicate the use of steganography. The three methods of steganography are audio, image, and video.

Using Cryptographic Protocols

With a basic understanding of hashing, symmetric encryption, and asymmetric encryption, it's easier to grasp how cryptography is used. Many applications use a combination of these methods, and it's important to understand how they're intertwined.

When describing public and private keys earlier, it was stressed that one key encrypts and the other key decrypts. A common question is “which one encrypts, and which one decrypts?” The answer depends on what you’re trying to accomplish. The following sections describe the details, but as an overview, these are the important points related to these keys:

- Email digital signatures
 - The *sender's private key* encrypts (or signs).
 - The *sender's public key* decrypts.
- Email encryption
 - The *recipient's public key* encrypts.
 - The *recipient's private key* decrypts.
- Web site encryption
 - The *web site's public key* encrypts.
 - The *web site's private key* decrypts.
 - The symmetric key encrypts data in the web site session.

Email and web site encryption commonly use a combination of both asymmetric and symmetric encryption. They use asymmetric encryption for key exchange, privately sharing a symmetric key. Symmetric encryption encrypts the data.

Remember this

Knowing which key encrypts and which key decrypts will help you answer some questions on the exam. For example, just by knowing that a private key is encrypting, you know that it is being used for a digital signature.

Protecting Email

Cryptography provides two primary security methods you can use with email: digital signatures and encryption. These are separate processes, but you can digitally sign and encrypt the same email.

Signing Email with Digital Signatures

Digital signatures are similar in concept to handwritten signatures on printed documents that identify individuals, but they provide more security benefits. The Digital Signature Algorithm (DSA) uses an encrypted hash of a message. The hash is encrypted with the sender's private key. If the recipient of a digitally signed email can decrypt the hash, it provides the following three security benefits:

- **Authentication.** This identifies the sender of the email. Email recipients have assurances the email came from who it appears to be coming from. For example, if an executive digitally signs an email, recipients know it came from the executive and not from an attacker impersonating the executive.
- **Non-repudiation.** The sender cannot later deny sending the message. This is sometimes required with online transactions. For example, imagine Homer sends an order to sell stocks using a digitally signed email. If the stocks increase after his sale completes, he can't deny the transaction.
- **Integrity.** This provides assurances that the message has not been modified or corrupted. Recipients know that the message they received is the same as the sent message.

Digital signatures are much easier to grasp if you understand some other cryptography concepts discussed in this chapter. As a short review, these concepts are:

- **Hashing.** Digital signatures start by creating a hash of the message. A hash is simply a number created by executing a hashing algorithm on the message.
- **Certificates.** Digital signatures need certificates, and certificates include the sender's public key.

- **Public/private keys.** In a digital signature, the sender uses the sender's private key to encrypt the hash of the message. The recipient uses the sender's public key to decrypt the hash of the message. The public key is often distributed in an S/MIME.p7s formatted file.

Figure 10.5 shows an overview of this process. In the figure, Lisa is sending a message to Bart with a digital signature. Note that the message "I passed" is not secret. If it was, Lisa would encrypt it, which is a separate process. The focus in this explanation is only the digital signature.

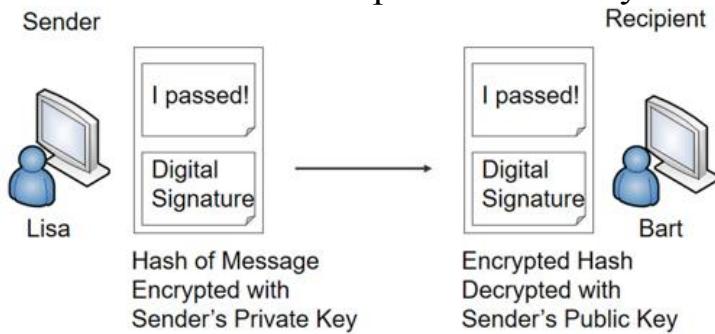


Figure 10.5: Digital signature process

Lisa creates her message in an email program, such as Microsoft Outlook. Once the email program is configured, all she does is click a button to digitally sign the message. Here is what happens when she clicks the button:

1. The application hashes the message.
2. The application retrieves Lisa's private key and encrypts the hash using this private key.
3. The application sends both the encrypted hash (which is the digital signature) and the unencrypted message to Bart.

When Bart's system receives the message, it verifies the digital signature using the following steps:

4. Bart's system retrieves Lisa's public key, which is in Lisa's public certificate. In some situations, Lisa may have sent Bart a copy of her certificate with her public key. In domain environments, Bart's system can automatically retrieve Lisa's certificate from a network location.
5. The email application on Bart's system decrypts the encrypted hash with Lisa's public key.
6. The application calculates the hash on the received message.

7. The application compares the decrypted hash with the calculated hash.

If the calculated hash of the received message is the same as the encrypted hash of the digital signature, it validates several important checks:

- **Authentication.** Lisa sent the message. The public key can only decrypt something encrypted with the private key, and only Lisa has the private key. If the decryption succeeded, Lisa's private key must have encrypted the hash. On the other hand, if another key was used to encrypt the hash, Lisa's public key could not decrypt it. In this case, Bart will see an error indicating a problem with the digital signature.
- **Non-repudiation.** Lisa cannot later deny sending the message. Only Lisa has her private key and if her public key decrypted the hash, the hash must have been encrypted with her private key. Non-repudiation is valuable in online transactions.
- **Integrity.** Because the hash of the sent message matches the hash of the received message, the message has maintained integrity. It hasn't been modified.

At this point, you might be thinking, if we do all of this, why not just encrypt the message, too? The answer is resources. It doesn't take much processing power to encrypt 256 bits in a SHA-256 hash. In contrast, it would take quite a bit of processing power to encrypt a lengthy email and its attachments. However, if you need to ensure confidentiality of the email, you can encrypt it.

Remember this

A digital signature is an encrypted hash of a message. The sender's private key encrypts the hash of the message to create the digital signature. The recipient decrypts the hash with the sender's public key. If successful, it provides authentication, non-repudiation, and integrity. Authentication identifies the sender. Integrity verifies the message has not been modified. Non-repudiation prevents senders from later denying they sent an email.

Encrypting Email

There are times when you want to ensure that email messages are only readable by authorized users. You can encrypt email and just as any other time encryption is used, encryption provides confidentiality.

Encrypting Email with Only Asymmetric Encryption

Imagine that Lisa wants to send an encrypted message to Bart. The following steps provide a simplified explanation of the process if only asymmetric encryption is used:

1. Lisa retrieves a copy of Bart's certificate that contains his public key.
2. Lisa encrypts the email with Bart's public key.
3. Lisa sends the encrypted email to Bart.
4. Bart decrypts the email with his private key.

This works because Bart is the only person who has access to his private key. If attackers intercepted the email, they couldn't decrypt it without Bart's private key. It's important to remember that when you're encrypting email contents, the recipient's public key encrypts and the recipient's private key decrypts. The sender's keys are not involved in this process. In contrast, a digital signature only uses the sender's keys but not the recipient's keys.

Remember this

The recipient's public key encrypts when encrypting an email message and the recipient uses the recipient's private key to decrypt an encrypted email message.

Encrypting Email with Asymmetric and Symmetric Encryption

The previous description provides a simplistic explanation of email encryption used by some email applications. However, most email applications combine both asymmetric and symmetric encryption. You may remember from earlier in this chapter that asymmetric encryption is slow and inefficient, but symmetric encryption is very quick.

Instead of using only symmetric encryption, most email applications use asymmetric encryption to privately share a session key. They then use

symmetric encryption to encrypt the data with this session key. For example, imagine that Lisa is sending Bart an encrypted message. Figure 10.6 shows the process of encrypting the message and encrypting the symmetric key. Figure 10.7 shows the process of sending the encrypted message and encrypted session key, and identifies how the recipient can decrypt the data:

1. Lisa's system identifies a symmetric key to encrypt her email. For this example, assume it's a simplistic symmetric key of 53, though a symmetric algorithm like AES would use 128-bit or larger keys.
2. Lisa encrypts the email contents with the symmetric key of 53.
3. Lisa retrieves a copy of Bart's certificate that contains his public key.
4. She uses Bart's public key to encrypt the symmetric key of 53.
5. Lisa sends the encrypted email and the encrypted symmetric key to Bart.
6. Bart decrypts the symmetric key with his private key.
7. He then decrypts the email with the decrypted symmetric key.

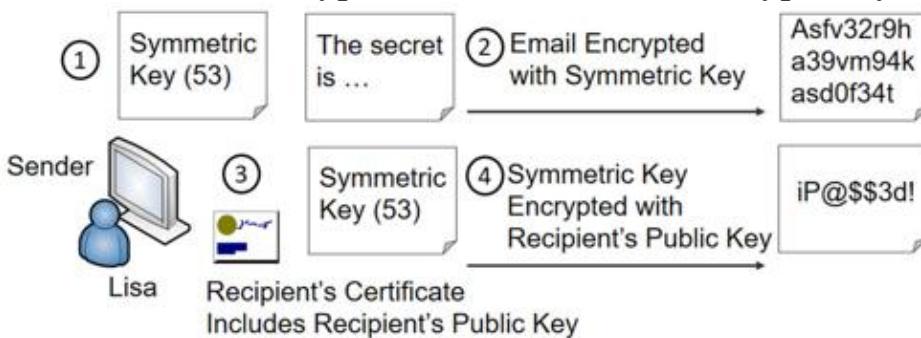


Figure 10.6: Encrypting email

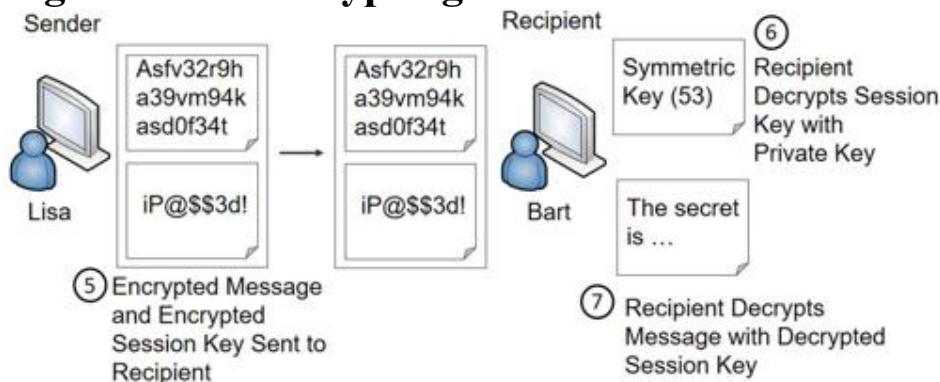


Figure 10.7: Decrypting email

Unauthorized users who intercept the email sent by Lisa won't be able to read it because it's encrypted with the symmetric key. Additionally, they can't read the symmetric key because it's encrypted with Bart's public key, and only Bart's private key can decrypt it.

S/MIME

Secure/Multipurpose Internet Mail Extensions(S/MIME) is one of the most popular standards used to digitally sign and encrypt email. Most email applications that support encryption and digital signatures use S/MIME standards.

S/MIME uses both asymmetric encryption and symmetric encryption. It can encrypt email at rest (stored on a drive) and in transit (data sent over the network). The current version uses the Cryptographic Message Syntax (CMS), which allows it to use a wide variety of different hashing algorithms and encryption algorithms. Many asymmetric algorithms use certificates and require a PKI to distribute and manage certificates.

When implementing S/MIME, you typically use the following ports:

- Port 995 for Post Office Protocol 3 (POP3) over Transport Layer Security (TLS), or POP3-over-TLS
- Port 587 for Simple Mail Transfer Protocol (SMTP) over Transport Layer Security (TLS), or SMTP-over-TLS
- Port 993 for Internet Message Access Protocol (IMAP) over Transport Layer Security (TLS), or IMAP-over-TLS

HTTPS Transport Encryption

Transport encryption methods encrypt data in transit to ensure transmitted data remains confidential. This includes data transmitted over the Internet and on internal networks. As an example, Chapter 3, “Exploring Network Technologies and Tools,” discusses the use of Secure Shell (SSH) to encrypt traffic, such as Secure File Transfer Protocol (SFTP). This section focuses on transport encryption methods used with HTTPS.

TLS Versus SSL

Transport Layer Security (TLS) and Secure Sockets Layer (SSL) are encryption protocols that have been commonly used to encrypt data sent over the Internet. SSL has significant vulnerabilities and should not be used anymore. However, many people commonly refer to TLS as SSL/TLS as if they are the same. If you see this, you can consider almost all references to SSL as a reference to TLS.

It is common to encrypt HTTPS with TLS to ensure confidentiality of data transmitted over the Internet. It can also be used to encrypt other transmissions such as File Transfer Protocol Secure (FTPS).

TLS provides certificate-based authentication and encrypts data with a combination of both symmetric and asymmetric encryption during a session. It uses asymmetric encryption for the key exchange (to privately share a session key) and symmetric encryption to encrypt data displayed on the web page and transmitted during the session. The next section shows this process.

It's important to remember that TLS requires certificates. Certificate authorities (CAs) issue and manage certificates, so a CA is required to support TLS. These CAs can be internal or external third-party CAs.

Remember this

TLS is the replacement for SSL. TLS requires certificates issued by certificate authorities (CAs). TLS encrypts HTTPS traffic, but it can also encrypt other traffic.

Encrypting HTTPS Traffic with TLS

HTTP Secure (HTTPS) is commonly used on the Internet to secure web traffic. It commonly uses TLS to encrypt the traffic, with both asymmetric and symmetric encryption. If you’re able to grasp the basics of how HTTPS combines both asymmetric and symmetric encryption, you’ll have what you need to know for most protocols that use both encryptions.

Because asymmetric encryption isn’t efficient to encrypt large amounts of data, symmetric encryption is used to encrypt the session data. However, both the client and the server must know what this symmetric key is before they can use it. They can’t whisper it to each other over the Internet. That’s like an actor on TV using a loud whisper, or stage whisper, to share a secret. Millions of TV viewers can also hear the secret.

Instead, HTTPS uses asymmetric encryption to transmit a symmetric key using a secure key exchange method. It then uses the symmetric key with symmetric encryption to encrypt all the data in the HTTPS session.

Figure 10.8 and the following steps show the overall process of establishing and using an HTTPS session. As you read these steps, try to keep these two important concepts in mind:

- TLS uses asymmetric encryption to securely share the symmetric key.
- TLS uses symmetric encryption to encrypt the session data.

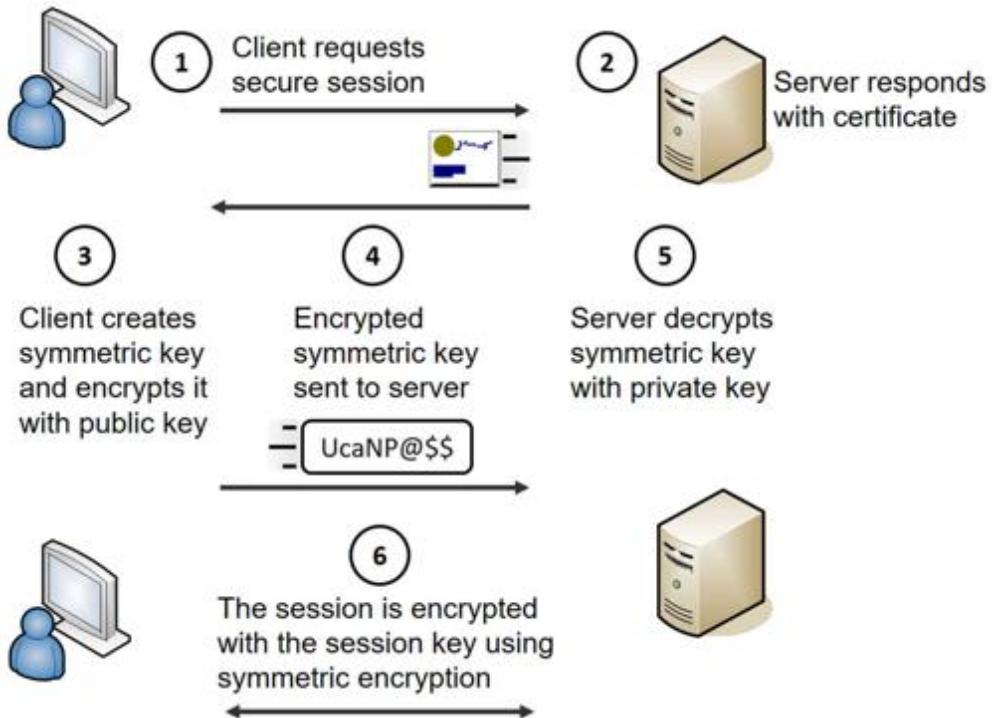


Figure 10.8: Simplified TLS handshake process used with HTTPS

1. The client begins the process by requesting an HTTPS session. This could be by entering an HTTPS address in the URL or by clicking on an HTTPS link.
2. The server responds by sending the server's certificate. The certificate includes the server's public key. The matching private key is on the server and only accessible by the server.
3. The client creates a symmetric key and encrypts it with the server's public key. As an example, imagine that the symmetric key is 53 (though it would be much more complex in a live session). The client encrypts the symmetric key of 53 using the web server's public key creating ciphertext of UcaNP@\$\$. This symmetric key will be used to encrypt data in the HTTPS session, so it is sometimes called a session key.
4. The client sends the encrypted session key (UcaNP@\$\$) to the web server. Only the server's private key can decrypt this. If attackers intercept the encrypted key, they won't be able to decrypt it because they don't have access to the server's private key.
5. The server receives the encrypted session key and decrypts it with the server's private key. At this point, both the client and the server know the session key.
6. All the session data is encrypted with this symmetric key using symmetric encryption.

The amazing thing to me is that this happens so quickly. If a web server takes as long as five seconds, many of us wonder why it's taking so long. However, a lot is happening to establish this session.

Downgrade Attacks on Weak Implementations

A *downgrade attack* is a type of attack that forces a system to downgrade its security. The attacker then exploits the lesser security control. It is most often associated with cryptographic attacks due to weak implementations of cipher suites.

An example is with Transport Layer Security (TLS) and Secure Sockets Layer (SSL). Imagine a server has both SSL and TLS installed. If a

client is not able to use TLS, the server would downgrade its security and use SSL to accommodate the client.

Attackers exploited this vulnerability by configuring their systems so that they could not use TLS. When they communicate with the server, the server downgrades security to use SSL instead of TLS. This allows attackers to launch SSL-based attacks such as the Padding Oracle On Downgraded Legacy Encryption (POODLE) attack. After the server downgrades to SSL, the attacker can initiate a man-in-the-middle attack.

One way to ensure that SSL isn't used on a site is to ensure that SSL is disabled. Disabling SSL prevents any SSL-based downgrade attacks. Similarly, cipher suites with known vulnerabilities, such as using other deprecated encryption algorithms, should be disabled. If weak cipher suites are enabled on a server, it increases the vulnerabilities.

Remember this

Administrators should disable weak cipher suites and weak protocols on servers. When a server has both strong and weak cipher suites, attackers can launch downgrade attacks bypassing the strong cipher suite and exploiting the weak cipher suite.

Blockchain

Blockchain is commonly defined as a distributed, decentralized, public ledger. In other words, it is a public record-keeping technology. Banks commonly use ledgers to record transactions such as deposits and withdrawals and blockchain **public ledgers** are similar. The word *block* refers to pieces of digital information (the ledger), and *chain* refers to a public database. Together they create a database of public records.

Each block has three parts:

- Information about a transaction, or transactions, such as the date, time, and amount.
 - Information on the parties involved with the transaction(s). However, this doesn't include actual names but instead uses a digital signature.
 - A unique hash that distinguishes the block from other blocks.
- A block is added to the blockchain after four things happen:
- A transaction occurred.
 - The transaction has been verified by a network of computers.
 - The transaction is accurately recorded in a block.
 - The block is assigned a unique hash.

The block also includes the hash of the most recent block added just before it. This is what creates the chain. Every block has a unique hash, and every block has the hash of the block right before it. These connected hashes create the chain.

Bitcoin is a cryptocurrency that uses blockchain. The network of computers that verify and record transactions are referred to as miners. However, it costs money to maintain all these computers and miners earn money (in the form of bitcoin) through transaction fees and rewards. Rewards are issued for the blocks and each block includes multiple transactions.

The block reward started at 50 bitcoins per block. The reward is cut in half after 210,000 blocks are mined, which occurs about every four years. In May 2020, it was cut in half again dropping to 6.25 bitcoins per block. Eventually, the rewards will stop, and no more bitcoins will be created. However, miners will still earn money through transaction fees.

Crypto Diversity

Cryptographic diversity typically refers to using different methods to protect security keys. The idea is that if a vulnerability appears in one method, the diversified methods still protect the key. As an example, NISTIR 8214A (Roadmap Toward Criteria for Threshold Schemes for Cryptographic Primitives) suggests the use of multiple hardware security modules (HSMs) to protect keys.

If three different HSMs are used, each one would hold part of the key. If a vulnerability occurs in one of the HSMs, it still wouldn't reveal the entire key.

Identifying Limitations

When evaluating different algorithms, it is important to consider their possible limitations. When you understand these, it becomes much easier to identify the best algorithm to meet specific requirements. The following sections identify many of the common limitations to consider.

Resource Versus Security Constraints

Organizations frequently need to balance resource availability with security constraints. Consider using encryption to maintain the confidentiality of data. If this is possible, why not just encrypt all the data? The reason is that encryption consumes resources.

As an example, the above paragraph is about 260 characters in cleartext. Encrypted using one algorithm, it is about 360 characters in ciphertext. That's an increase of about 40 percent, which is typical with many encryption methods. If a company decides to encrypt all data, it means that it will need approximately 40 percent more disk space to store the data. Additionally, when processing the data, it consumes more memory. Last, it takes additional processing time and processing power to encrypt and decrypt the data.

Security experts might say the cost for additional resources is worth it, but executives looking to increase the value of the company don't. Instead, executives have a responsibility to minimize costs without sacrificing security. They do this by looking for the best balance between resource costs and security needs.

Speed and Time

Speed refers to how long an algorithm takes to compute the result. As an example, encryption algorithms typically perform several rounds, or iterations, on data. How fast the algorithm can perform a round and how many rounds it performs determine its speed. You generally want a quick algorithm when encrypting and decrypting data.

When salting and hashing passwords, a slower algorithm is desirable. The slower speed is not perceptible when validating a single password. However, the slower speed thwarts attackers who are using the algorithm

trying to guess the correct password from tens of thousands (or more) of possibilities.

Size and Computational Overhead

Size in cryptography typically relates to the amount of memory space the algorithm needs to execute. On most desktops and servers, the size required is trivial. However, many smaller devices don't have adequate memory and processing power to run the same algorithms. Lightweight cryptography methods are smaller, requiring a smaller overhead.

In some cases, size relates to the size of the output compared with the input. This is relevant when encrypting data. As mentioned previously, encrypted data is larger than unencrypted data and it requires more storage space.

Entropy

Entropy refers to the randomness of a cryptographic algorithm. A higher level of randomness results in a higher level of security when using the algorithm. A lack of entropy results in a weaker algorithm and makes it much easier for the algorithm to be cracked.

Cryptographic algorithms are published so anyone can access them. This results in a significant amount of testing by cryptanalysts. When they discover a weakness or vulnerability, they publish their findings. Other cryptanalysts then peer-review their work attempting to prove or disprove the findings. Weak algorithms are deprecated and eventually fall into disuse.

As an example, cryptographic weaknesses were discovered in SHA-1. It hasn't been approved for most uses since about 2010.

Predictability

In general, predictability refers to knowing what will likely happen based on repeating the same events. When applied to cryptography, it is commonly associated with random number generators used to create encryption keys.

Random number generators are either pseudo-random number generators or true random number generators. A pseudo-random number generator uses a deterministic algorithm. In other words, given the same

input, a pseudo-random number generator will produce the same output. If attackers know what is being used as an input to a pseudo-random number generator to create an encryption key, it increases the likelihood that they can predict the key.

True random number generators often use environmental factors such as atmospheric noise or cosmic background radiation as inputs. When used properly, these sources can add true entropy into random number generators and cryptographic algorithms.

Weak Keys

Even the strongest algorithms can be easily cracked when weak keys are used. A weak key is a short or small key. When weak keys are used, it increases the possibility that an attacker can decrypt the data and read it. As an example, NIST recommends using at least 2048-bit keys with RSA since 2010. At this point, 1024-bit keys are weak and shouldn't be used.

Longevity

Longevity refers to how long you can expect to use an algorithm. This is typically related to the expected improvements in processing power. RSA provides a good example when considering just the keys. By doubling the key size, it increases the longevity of the algorithm.

However, all cryptographic algorithms don't support larger keys. As an example, the Data Encryption Standard (DES) supports key sizes of 56 bits only. The U.S. government approved it as a federal standard in November 1976. AES was chosen as the successor to DES in 2002 and the U.S. government removed its approval of DES in 2005. It is no longer recommended for use.

Reuse

When using symmetric encryption, the same keys shouldn't be reused. This is especially true with stream ciphers. If any key is used twice in the same stream, the algorithm is vulnerable to attacks. This was the problem with the legacy Wired Equivalent Privacy (WEP) algorithm used with early implementations of wireless networks. Because keys were reused in the same stream, it was vulnerable to attacks. Indeed, attackers created apps

making it trivial for attackers to discover the passwords used WEP-based wireless networks. WEP was deprecated in 2004.

Plaintext Attack

A plaintext attack (also called a known plaintext) attack is possible if an attacker has some known plaintext data and the ciphertext created from this plaintext. As an example, if an attacker captures an encrypted message (the ciphertext) and knows the unencrypted plaintext of the message, he can use both sets of data to discover the encryption and decryption method. If successful, he can use the same decryption method on other ciphertext.

A chosen plaintext attack is similar, but the attacker doesn't have access to all the plaintext. As an example, imagine a company includes the following sentences at the end of every email:

“The information contained in this email and any accompanying attachments may contain proprietary information about the Pay & Park & Pay parking garage. If you are not the intended recipient of this information, any use of this information is prohibited.”

If the entire message is encrypted, the attacker can try various methods to decrypt the chosen plaintext (the last two sentences included in every email). When he's successful, he can use the same method to decrypt the entire message.

In a ciphertext only attack, the attacker doesn't have any information on the plaintext. Known plaintext and chosen plaintext attacks are almost always successful if an attacker has the resources and time. However, ciphertext only attacks are typically only successful on weak encryption algorithms. They can be thwarted by not using legacy and deprecated encryption algorithms.

Common Use Cases

The SY-601 exam objectives list several common uses cases you should understand related to cryptographic concepts. While these have often been mentioned in other sections, I'm summarizing them here for clarity:

- **Supporting integrity.** Hashing protocols are used to support integrity. They can verify that data has been changed by an unauthorized entity.
- **Supporting confidentiality.** Encryption protocols are used to provide confidentiality. This prevents unauthorized users from accessing data.
- **Supporting non-repudiation.** Digital signatures are used to support non-repudiation. When someone sends an email with a digital signature, recipients know it was sent by that person. Additionally, a person can't later deny sending the email, at least not believably.
- **Supporting high resiliency.** A common use case for encryption algorithms is to provide high resiliency. Within cryptography, high resiliency refers to the security of an encryption key even if an attacker discovers part of the key. Ideally, keys are not susceptible to leakage, preventing attackers from gaining information on any part of a key. However, there are many situations that can cause leakage. A strong algorithm implements high-resiliency techniques that ensure this leakage does not compromise the encryption key.
- **Supporting obfuscation.** Steganography is used to support obfuscation. It allows people to hide data in plain sight and obscure the fact that a file is holding a hidden message. Messages can be hidden in audio, image, and video files.
- **Supporting low power devices.** ECC and other lightweight cryptography algorithms support deploying cryptography on low power devices. This includes wireless devices, and just about any IoT device.
- **Supporting low latency.** OCSP supports a use case of low latency. When a certificate is revoked, it adds the certificate to a CRL.

However, CRLs are cached so clients using the CRL won't know the certificate is revoked until the CRL is refreshed. OCSP provides a real-time response eliminating this latency.

Exploring PKI Components

A ***Public Key Infrastructure (PKI)*** is a group of technologies used to request, create, manage, store, distribute, and revoke digital certificates. Asymmetric encryption depends on the use of certificates for a variety of purposes, such as protecting email and protecting Internet traffic with TLS. For example, HTTPS sessions protect Internet credit card transactions, and these transactions depend on a PKI.

A primary benefit of a PKI is that it allows two people or entities to communicate securely without knowing each other previously. In other words, it allows them to communicate securely through an insecure public medium such as the Internet.

For example, you can establish a secure session with Amazon.com even if you've never done so before. Amazon is using certificates issued by a trusted certificate authority (CA). As shown in the "Encrypting HTTPS Traffic with TLS" section previously, the certificate provides the ability to establish a secure session. A key element in a PKI is a certificate authority.

Certificate Authority

A ***certificate authority (CA)*** issues, manages, validates, and revokes certificates. In some contexts, you might see a CA referred to as a certification authority, but they are the same thing. CAs can be large, such as Comodo, DigiCert, or Symantec, which are public CAs. A CA can also be small, such as a single service running on a server within a private network.

Public CAs make money by selling certificates. For this to work, the public CA must be trusted. If the CA is trusted, all certificates issued by the CA are trusted.

This is similar to how a driver's license is trusted. The Department of Motor Vehicles (DMV) issues driver's licenses after validating a person's identity. If you want to cash a check, you might present your driver's license to prove your identity. Businesses trust the DMV, so they trust the driver's license. On the other hand, if you purchased an ID from Gibson's Instant IDs, businesses might not trust it.

Although we might trust the DMV, why would a computer trust a CA? The answer is based on the certificate trust path.

Certificate Trust Models

CAs are trusted by placing a copy of their root certificate into a trusted root CA store. The root certificate is the first certificate created by the CA that identifies it, and the store is just a collection of these root certificates. If the CA's root certificate is placed in this store, all certificates issued by this CA are trusted.

Figure 10.9 shows the Trusted Root Certification Authority store on a Windows computer. You can see that there are many certificates from many different CAs. In the figure, I've selected one of the certificates from COMODO Certification Authority. One of the labs for this chapter (available at <https://greatadministrator.com/sy0-601-labs>) shows how to access this on a Windows computer.

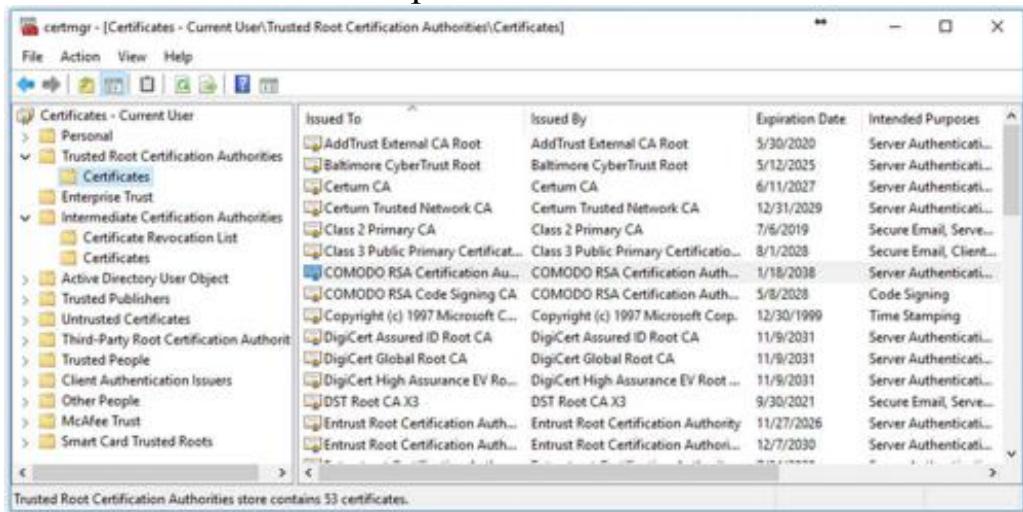


Figure 10.9: Trusted Root Certification Authorities

Public CAs such as Symantec and Comodo negotiate with web browser developers to have their certificates included with the web browser. This way, any certificates that they sell to businesses are automatically trusted.

The most common trust model is the hierarchical trust model, also known as a centralized trust model. In this model, the public CA creates the first CA, known as the root CA. If the organization is large, it can create an **intermediate CA** and child CAs. If you look back at Figure 10.9, you can see that it includes a section used to store intermediate CA certificates. A large trust model works like this:

- The root CA issues certificates to intermediate CAs.
- Intermediate CAs issue certificates to child CAs.
- Child CAs issue certificates to devices or end users.

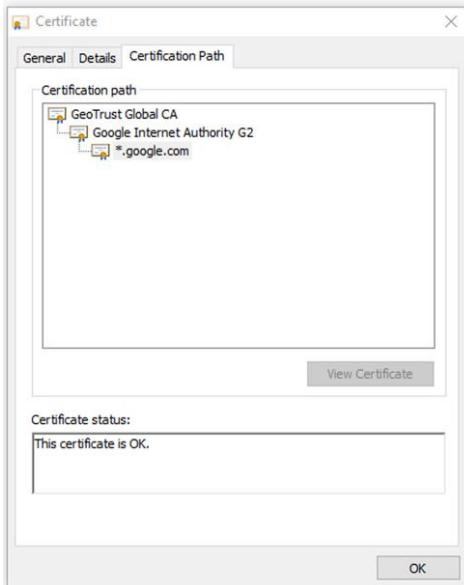


Figure 10.10: Certificate Path

Certificate chaining combines all the certificates from the root CA down to the certificate issued to the end user. For example, Figure 10.10 shows the certificate chain for a wildcard certificate issued to google.com. A certificate chain would include all three certificates. In a small organization, the root CA can simply issue certificates to the devices and end users. It's not necessary to have intermediate and child CAs.

Registration Authority and CSRs

Users and systems request certificates from a CA using a registration process. In some cases, a user enters information manually into a web site form. In other cases, a user sends a specifically formatted file to the CA. Within a domain, the system handles much of the process automatically.

As an example, imagine I wanted to purchase a certificate for *GetCertifiedGetAhead.com* for secure HTTPS sessions. I would first create a public and private key pair. Many programs are available to automate this process. For example, ***OpenSSL*** is a software library accessible via the command line in many Linux distributions. It creates key pairs in one command and allows you to export the public key to a file in a second command. Technically, OpenSSL and similar applications create the private key first. However, these applications appear to create both keys at the same time.

I would then put together a ***certificate signing request (CSR)*** for the certificate, including the purpose of the certificate and information about the web site, the public key, and me. Most CAs require CSRs to be formatted using the Public-Key Cryptography Standards (PKCS) #10 specification. The CSR includes the public key, but not the private key. A CA typically publishes a certificate template showing exactly how to format the CSR.

After receiving the CSR, the CA validates my identity and creates a certificate with the public key. The validation process is different based on the usage of the certificate. In some cases, it includes extensive checking, and in other cases, verification comes from the credit card I use to purchase it.

I can then register this certificate with my web site along with the private key. Any time someone initiates a secure HTTPS connection, the web site sends the certificate with the public key and the TLS/SSL session creates the session.

In large organizations, a ***registration authority (RA)*** can assist the CA by collecting registration information. The RA never issues certificates. Instead, it only assists in the registration process.

Online Versus Offline CAs

If the CA is online, meaning it is accessible over a network, it's possible to submit the CSR using an automated process. However, an organization may choose to keep some CAs offline to protect them from attacks. Offline CAs can only accept CSRs manually.

Large organizations typically keep the root CA offline to reduce the risk of compromise. The root CA issues certificates to the intermediate and child CAs that are online and accessible. If an intermediate or child CA becomes compromised, the entire certification path isn't compromised. The root CA can issue new certificates to replace the compromised certificates. However, if the root CA is compromised, the entire certification path is compromised.

Remember this

You typically request certificates using a certificate signing request (CSR). The first step is to create the RSA-based private key, which is used to create the public key. You then include the public key in the CSR and the CA will embed the public key in the certificate. The private key is not sent to the CA.

Updating and Revoking Certificates

Two common configuration changes related to certificates are updating and revoking them. Certificates normally expire based on the Valid From and Valid To dates and can be updated by replacing them with newer certificates. If a certificate is compromised, the CA can revoke it.

Many web sites use certificates from Let's Encrypt, a nonprofit certificate authority that provides free TLS-based certificates. These certificates are valid for 90 days, but automated processes can be used to automatically update the certificate without additional site administrator interaction.

When desired, the CA can revoke a certificate before it expires. As an example, if a private key is somehow leaked to the public, the key pair is compromised. It no longer provides adequate security because the private key is no longer private. Similarly, if the CA itself is compromised through a security breach, certificates issued by the CA may be compromised, so the CA can revoke certificates.

In general, any time a CA does not want anyone to use a certificate, the CA revokes it. Although the most common reasons are due to compromise of a key or compromise of the CA, there are others. A CA can use any of the following reasons when revoking a certificate:

- Key compromise
- CA compromise
- Change of affiliation
- Superseded
- Cease of operation
- Certificate hold

Certificate Revocation List

CAs use certificate revocation lists (CRLs) to revoke a certificate. The CRL is a version 2 certificate that includes a list of revoked certificates identified by their serial numbers. For example, Figure 10.11 shows a copy of a CRL. One of the labs for this chapter shows you how to download and view a CRL.

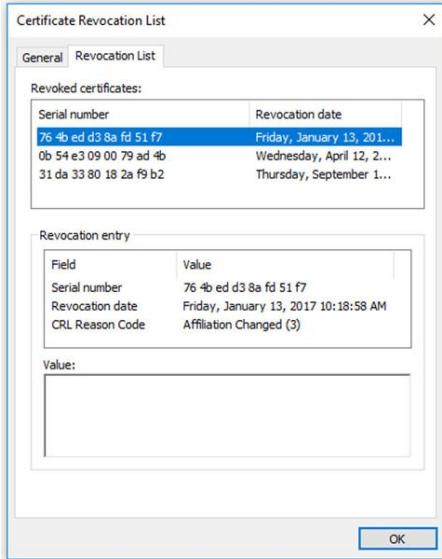


Figure 10.11: Certificate revocation list

Validating a Certificate

Before clients use a certificate, they first verify it is valid with some checks. There are many different certificate issues that can result in an invalid certificate. Browsers typically display an error describing the issue and encouraging users not to use the certificate. Applications that detect a certificate issue might display an error using a certificate, but they are typically coded to not use it. Some of the common issues are:

- **Expired.** The first check is to ensure that it isn't expired. If the certificate is expired, the computer system typically gives the user an error indicating the certificate is not valid.
- **Certificate not trusted.** The next check is to see if the certificate was issued by a trusted CA. For example, a Windows system will look in the Trusted Root Certification Authority store and the Intermediate Certification Authorities store shown previously in Figure 10.9. If the system doesn't have a copy of the CA's certificate, it will indicate the certificate is not trusted. Users can override this warning, though there are often warnings encouraging users not to continue.
- **Certificate revoked.** Clients also validate certificates through the CA to ensure they haven't been revoked.

A common method of validating a certificate is by requesting a copy of the CRL, as shown in Figure 10.12. The following steps outline the process:

1. The client initiates a session requiring a certificate, such as an HTTPS session.
2. The server responds with a copy of the certificate that includes the public key.
3. The client queries the CA for a copy of the CRL.
4. The CA responds with a copy of the CRL.

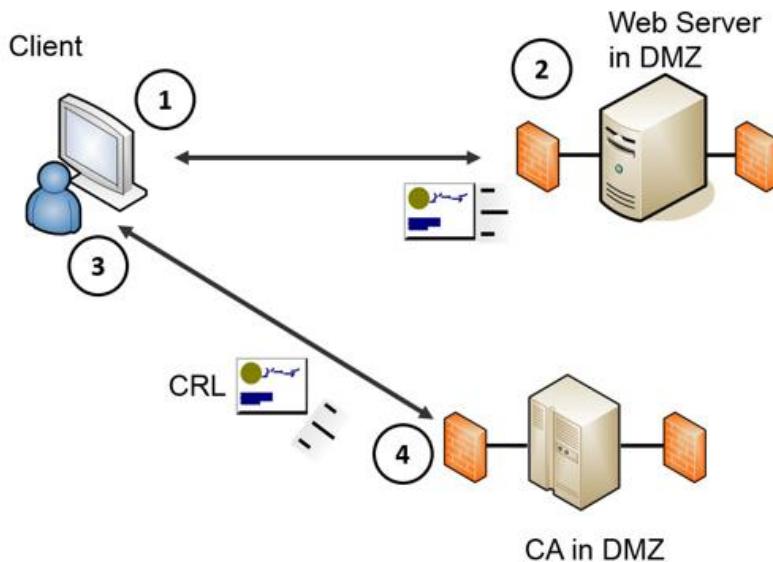


Figure 10.12: Validating a certificate

The client then checks the serial number of the certificate against the list of serial numbers in the CRL. If the certificate is revoked for any reason, the application gives an error message to the user.

CRLs are typically cached after being downloaded the first time. Instead of requesting another copy of the CRL, clients use the cached copy. This reduces the amount of traffic sent between clients and the CA.

Another method of validating a certificate is with the ***Online Certificate Status Protocol (OCSP)***. OCSP allows the client to query the CA with the serial number of the certificate. The CA then responds with an answer of “good,” “revoked,” or “unknown.” A response of “unknown” could indicate the certificate is a forgery.

Because OCSP provides a real-time response, it is an excellent example of supporting a common use case of low latency. If a CA revokes a certificate, clients using OCSP will know immediately. In contrast, if clients are using a cached CRL, they will be unaware of the revoked certificate until another copy of the CRL is downloaded.

Over time, authorities realized that OCSP was generating a lot of real-time traffic to the CA because it requires a CA to respond to every request. **OCSP stapling** solves this problem. The certificate presenter (such as the web server in Figure 10.12) obtains a timestamped OCSP response from the CA. Before sending it, the CA signs it with a digital signature. The certificate presenter then appends (or metaphorically staples) a timestamped

OCSP response to the certificate during the TLS handshake process. This eliminates the need for clients to query the CA.

Remember this

CAs revoke certificates for several reasons such as when the private key is compromised or the CA is compromised. The certificate revocation list (CRL) includes a list of revoked certificates and is publicly available. An alternative to using a CRL is the Online Certificate Status Protocol (OCSP), which returns answers such as good, revoked, or unknown.

Public Key Pinning

Public key *pinning* is a security mechanism designed to prevent attackers from impersonating a web site using fraudulent certificates. When configured on a web site server, the server responds to client HTTPS requests with an extra header. This extra header includes a list of hashes derived from valid public keys used by the web site. It also includes a max-age field specifying how long the client should store and use the data.

When clients connect to the same web site again, they recalculate the hashes and then compare the recalculated hashes with the stored hashes. If the hashes match, it verifies that the client is connected to the same web site.

Web site administrators create hashes of one or more certificates used by the web site. This can be the public key used by the web site's certificate. It can also include any public keys from certificates in the certificate chain such as the public key from the root CA certificate, and/or the public key from intermediate CA certificates. Last, it must include a backup key that can be used if the current key becomes invalid.

Remember this

Certificate stapling is an alternative to OCSP. The certificate presenter (such as a web server) appends the certificate with a timestamped digitally signed OCSP response from the CA. This reduces OCSP traffic to and from the CA. Public key pinning helps prevent attackers from impersonating a web site with a fraudulent certificate. The web server sends a list of public key hashes that clients can use to validate certificates sent to clients in subsequent sessions.

Key Escrow

Key escrow is the process of placing a copy of a private key in a safe environment. This is useful for recovery. If the original key is lost, the organization retrieves the copy of the key to access the data. Key escrow isn't required, but if an organization determines that data loss is unacceptable, it will implement a key escrow process.

In some cases, an organization provides a copy of the key to a third party. Another method is to designate employees within the organization who will be responsible for key escrow. These employees maintain and protect copies of the key, and if the original key is lost, they check out a copy of the key to an administrator or user.

A key recovery agent is a designated individual who can recover or restore cryptographic keys. In the context of a PKI, a recovery agent can recover private keys to access encrypted data. The recovery agent may be a security professional, administrator, or anyone designated by the company.

In some cases, the recovery agent can recover encrypted data using a different key. For example, Microsoft BitLocker supports encryption of entire drives. It's possible to add a data recovery agent field when creating a BitLocker encrypted drive. In this case, BitLocker uses two keys. The user has one key and uses it to unlock the drive during day-to-day use. The second key is only accessible by the recovery agent and is used for recovery purposes if the original key is lost or becomes inaccessible.

Key Management

Key management within a PKI refers to all the steps taken to manage public and private keys used within the PKI. This includes keeping private keys private, distributing public keys in certificates, and revoking certificates when keys are compromised.

Comparing Certificate Types

Certificates are sometimes identified based on their usage. The following bullets describe some common certificate types:

- **Machine/Computer.** Certificates issued to a device or a computer are commonly called machine certificates or computer certificates. The certificate is typically used to identify the computer within a domain.
- **User.** Certificates can also be issued to users. They can be used for encryption, authentication, smart cards, and more. For example, Microsoft systems can create user certificates allowing the user to encrypt data using Encrypting File System (EFS).
- **Email.** Email certificates are used for encryption of emails and digital signatures, as described earlier in this chapter.
- **Code signing.** Developers often use code signing certificates to validate the authentication of executable applications or scripts. The code signing certificate verifies the code has not been modified. As an example, a PowerShell script can use a code signing certificate to prove the script hasn't been modified before it is run.
- **Self-signed.** A self-signed certificate is not issued by a trusted CA. Private CAs within an enterprise often create self-signed certificates. They aren't trusted by default. However, administrators can use automated means to place copies of the self-signed certificate into the trusted root CA store for enterprise computers. Self-signed certificates from private CAs eliminate the cost of purchasing certificates from public CAs.
- **Root.** The root certificate is the certificate issued by the root CA.
- **Wildcard.** A wildcard certificate starts with an asterisk (*) and can be used for multiple domains if each domain name has the same root domain. For example, Google uses a wildcard certificate issued to *.google.com. This same certificate can be used for other Google domains, such as accounts.google.com and support.google.com. Wildcard certificates can reduce the administrative burden associated with managing multiple certificates.

- **Subject alternative name.** A subject alternative name (SAN) certificate is used for multiple domains that have different names but are owned by the same organization. For example, Google uses SANs of *.google.com, *.android.com, *.cloud.google.com, and more. It is often used for systems with the same base domain names, but different top-level domains. For example, if Google used names such as google.com and google.net, it could use a single SAN certificate for both domain names.
- **Domain validation.** A domain-validated certificate indicates that the certificate requestor has some control over a DNS domain. The CA takes extra steps to contact the requestor such as by email or telephone. The intent is to provide additional evidence to clients that the certificate and the organization are trustworthy.
- **Extended validation.** Extended validation (EV) certificates use additional steps beyond domain validation. Some browsers display the name of the company before the URL when an extended validation certificate is used. Usage of EV certificates is on the decline. Most web browsers stopped including the name in the URL. Part of the reason is that the absence of the company name doesn't mean anything to many users. Think of the user who clicks on a phishing email. He probably doesn't know to look for a company name in the URL, so its absence doesn't alarm him.

Comparing Certificate Formats

Most certificates use one of the X.509 v3 formats. The primary exception is certificates used to distribute certificate revocation lists that use the X.509 v2 format.

Certificates are typically stored as binary files or as BASE64 American Standard Code for Information Interchange (ASCII) encoded files. Binary files are stored as 1s and 0s. BASE64 encoding converts the binary data into an ASCII string format. Additionally, some certificates are also encrypted to provide additional confidentiality.

The base format of certificates is ***Canonical Encoding Rules (CER)*** or ***Distinguished Encoding Rules (DER)***. CER and DER formats are defined by the International Telegraph Union Telecommunication Standardization Sector (ITU-T) in the X.690 standard. They use a variant of the Abstract Syntax Notation One (ASN.1) format, which defines data structures commonly used in cryptography. CER is an ASCII format and DER is a binary format.

Some certificates include headers and footers to identify the contents. As an example, the following text shows a header and a footer for a certificate:

```
-----BEGIN CERTIFICATE-----  
MIIDdTCCAI2gAwIBAgILBAAAAAAABFUtaw5QwDQYJKoZIhvcNAQEFBQAwVzEL  
... additional ASCII Characters here... HMUfpIBvFSDJ3gyICh3WZlXi/EjJKSzp4A==  
-----END CERTIFICATE-----
```

Each header starts with five dashes (-----), BEGIN, a label, and five more dashes. The footer starts with five dashes, End, the same label, and five more dashes. In the previous example, the label is CERTIFICATE. Other labels include PUBLIC KEY, PRIVATE KEY, ENCRYPTED PRIVATE KEY, CERTIFICATE REQUEST, and X509 CRL. DER-based certificates are binary encoded, so they do not have headers and footers.

Certificate files can have many extensions, such as .crt, .cer, .pem, .key, .p7b, .p7c, pfx, and .p12. However, it's worth stressing that a certificate with the.cer extension doesn't necessarily mean that it is using the CER format.

When comparing the different formats, it's important to know what they can contain and how to identify them. Table 10.1 provides an overview

of the primary formats and the following sections describe these in more depth.

Type	Common Extensions	Format	Common Purpose	Can Contain
CER	.cer	ASCII	Used for ASCII certificates	Varies
DER	.der	Binary	Used for binary certificates	Varies
PEM	.pem, .cer, .crt, .key	Binary (DER) or ASCII (DER)	Can be used for almost any certificate purpose	Server certificates, certificate chains, keys, CRL
P7B	.p7b, .p7c	ASCII (CER)	Used to share the public key	Certificates, certificate chains, CRL, but never the private key
P12	.p12, .pfx	Binary (DER)	Commonly used to store private keys with a certificate	Certificates, certificate chains, and private keys
PFX				

Table 10.1: Certificate formats

The ***Privacy Enhanced Mail (PEM)*** certificate name implies that PEM-based certificates are used for email only, but that is misleading. PEM-based certificates can be used for just about anything. They can be formatted as CER (ASCII files) or DER (binary files). They can also be used to share public keys within a certificate, request certificates from a CA as a CSR, install a private key on a server, publish a CRL, or share the full certificate chain.

You might see a PEM-encoded certificate with the .pem extension. However, it's more common for the certificate to use other extensions. For example, a PEM-encoded file holding the certificate with the public key typically uses the .cer or .crt extension. A PEM file holding just the private key typically uses the .key extension.

P7B certificates use the PKCS version 7 (PKCS#7) format and they are CER-based (ASCII). They are commonly used to share public keys with proof of identity of the certificate holder. Recipients use the public keys to encrypt or decrypt data. For example, a web server might use a P7B certificate to share its public key. P7B certificates can also contain a certificate chain or a CRL. However, they never include the private key.

P12 certificates use the PKCS version 12 (PKCS#12) format and they are DER based (binary). They are commonly used to hold certificates with the private key. For example, when installing a certificate on a server to support HTTPS sessions, you might install a P12 certificate with the private

key. Because it holds the private key, it's common to encrypt P12 certificates. It's also possible to include the full certificate chain in a P12 certificate.

Personal Information Exchange (PFX) is a predecessor to the P12 certificate and it has the same usage. Administrators often use this format on Windows systems to import and export certificates.

Remember this

CER is an ASCII format for certificates and DER is a binary format. PEM is the most used certificate format and can be used for just about any certificate type. P7B certificates are commonly used to share public keys. P12 and PFX certificates are commonly used to hold the private key.

Chapter 10 Exam Topic Review

When preparing for the exam, make sure you understand these key concepts covered in this chapter.

Introducing Cryptography Concepts

- Integrity provides assurances that data has not been modified.
Hashing ensures that data has retained integrity.
- Confidentiality ensures that data is only viewable by authorized users. Encryption protects the confidentiality of data.
- Symmetric encryption uses the same key to encrypt and decrypt data.
- Asymmetric encryption uses two keys (public and private) created as a matched pair.
- A digital signature provides authentication, non-repudiation, and integrity.
 - Authentication validates an identity.
 - Non-repudiation prevents a party from denying an action.
 - Users sign emails with a digital signature, which is a hash of an email message encrypted with the sender's private key.
 - Only the sender's public key can decrypt the hash, providing verification it was encrypted with the sender's private key.

Providing Integrity with Hashing

- Hashing verifies the integrity of data, such as downloaded files and email messages.
- A hash is a fixed-length string of numbers or hexadecimal characters, which cannot be reversed to re-create the original data.
- A checksum is similar to a hash but is typically smaller. It is used to verify the integrity of data but is not intended to be cryptographically secure.
- Hashing algorithms are one-way functions used to create a hash. You cannot reverse the process to re-create the original data.
- A hash collision occurs when a hashing algorithm creates the same hash from different inputs.

- Common hashing algorithms are Message Digest 5 (MD5), Secure Hash Algorithm (SHA), and Hash-based Message Authentication Code (HMAC). HMAC provides both integrity and authenticity of a message.

Understanding Password Attacks

- Password attacks attempt to discover passwords. An online password attack attempts to discover a password from an online system. An offline password attack attempts to discover passwords from a captured database or captured packet scan.
- Passwords are often stored as a hash. Weak hashing algorithms are susceptible to collisions, which allow different passwords to create the same hash.
- A brute force attack attempts to guess all possible character combinations and a dictionary attack uses all the words and character combinations stored in a file. Account lockout policies thwart online brute force attacks and complex passwords thwart offline password attacks.
- A spraying attack attempts to bypass account lockout policies. An automated program starts with a large list of targeted user accounts. It then picks a password and tries it against every account in the list. It then picks another password and loops through the list again.
- In a pass the hash attack, the attacker discovers the hash of the user's password and then uses it to log on to the system as the user.
- In a birthday attack, an attacker attempts to create a password that produces the same hash as the user's actual password.
- Password salting adds additional characters to passwords before hashing them and prevents many types of attacks, including dictionary, brute force, and rainbow table attacks.
- Three commonly used key stretching techniques are bcrypt, Password-Based Key Derivation Function 2 (PBKDF2), and Argon2. They protect passwords against brute force and rainbow table attacks.

Providing Confidentiality with Encryption

- Confidentiality ensures that data is only viewable by authorized users.
- Encryption provides confidentiality of data, including data at rest (any type of data stored on disk) or data in transit (any type of transmitted data).
- Symmetric encryption uses the same key to encrypt and decrypt data.
- Block ciphers encrypt data in fixed-size blocks. Advanced Encryption Standard (AES) encrypts data in 128-bit blocks and 3DES encrypts data in 64-bit blocks.
- Stream ciphers encrypt data 1 bit or 1 byte at a time. They are more efficient than block ciphers when encrypting data of an unknown size or when sent in a continuous stream.
- Asymmetric encryption uses public and private keys as matched pairs.
 - If the public key encrypts information, only the matching private key can decrypt it.
 - If the private key encrypts information, only the matching public key can decrypt it.
 - Private keys are always kept private and never shared.
 - Public keys are freely shared by embedding them in a certificate.
- Asymmetric encryption is used to share symmetric keys between two entities. After both parties know the symmetric key, they use it to encrypt data within the session because symmetric encryption is much faster than asymmetric encryption.
- Certificates distribute public keys and the same public key is used for months or years.
- Ephemeral keys last only a short time, such as a few minutes within a session. Perfect forward secrecy ensures that the compromise of a key does not compromise any keys used in the past. It depends on the use of ephemeral keys.
- Elliptic curve cryptography (ECC) is an encryption technology that doesn't take as much processing power as other cryptographic methods. It is commonly used with low power devices.
- Quantum computing uses quantum bits (or qubits) instead of bits. A qubit can be two values at the same time and any qubit can be

dependent on the value of another qubit. Quantum computers are much faster than even the world's fastest supercomputers.

- Post-quantum cryptography refers to cryptographic algorithms that are likely to be resistant to attacks using a quantum computer. Quantum computers are rare, but one day they'll be easily accessible by attackers, and these newer algorithms are intended to thwart any attacks using quantum computers.
- Lightweight cryptography refers to cryptography deployed to smaller devices, including IoT devices.
- Homomorphic encryption allows data to remain encrypted while it is being processed.
- Steganography is the practice of hiding data within a file. Current steganography methods include audio steganography, image steganography, and video steganography.

Using Cryptographic Protocols

- When using digital signatures with email:
 - The sender's private key encrypts (or signs).
 - The sender's public key decrypts.
- A digital signature provides authentication (verified identification) of the sender, non-repudiation, and integrity of the message.
 - Senders create a digital signature by hashing a message and encrypting the hash with the sender's private key.
 - Recipients decrypt the digital signature with the sender's matching public key.
- When encrypting email:
 - The recipient's public key encrypts.
 - The recipient's private key decrypts.
 - Many email applications use the public key to encrypt a symmetric key, and then use the symmetric key to encrypt the email contents.
- S/MIME is used to secure email with encryption and digital signatures. It uses certificates and depends on a PKI. When deploying, use port 587 for SMTP-over-TLS and port 993 for IMAP-over-TLS.
- When encrypting web site traffic with TLS:

- The web site's public key encrypts a symmetric key.
- The web site's private key decrypts the symmetric key.
- The symmetric key encrypts data in the session.

Exploring PKI Components

- A Public Key Infrastructure (PKI) is a group of technologies used to request, create, manage, store, distribute, and revoke digital certificates. A PKI allows two entities to privately share symmetric keys without any prior communication.
- Most public CAs use a hierarchical centralized CA trust model, with a root CA and intermediate CAs. A CA issues, manages, validates, and revokes certificates. Certificate chaining combines all the certificates from the root CA to the certificate issued to the end user.
- You request a certificate with a certificate signing request (CSR). You first create a private/public key pair and include the public key in the CSR.
- An online CA is accessible over a network, including the Internet. Many root CAs are taken offline to reduce the risk of compromise.
- Configuration changes related to certificates are updating them and revoking them. Certificates are renewed before their expiration dates to update them. Certificates are revoked if they are compromised.
- A certificate revocation list (CRL) identifies revoked certificates with a list of serial numbers.
- The CA publishes the CRL, making it available to anyone. Web browsers can check certificates they receive from a web server against a copy of the CRL to determine if a certificate is revoked.
- As an alternative to the CRL, the Online Certificate Status Protocol (OCSP) allows clients to query the CA with the serial number of the certificate to determine if it is valid.
- Certificate stapling provides clients with a timestamped, digitally signed OCSP response. This is from the CA and appended to the certificate.
- Public key pinning provides clients with a list of hashes for each public key it uses.

- A key escrow stores a copy of private keys used within a PKI. If the original private key is lost or inaccessible, the copy is retrieved from escrow, preventing data loss.
- Wildcard certificates use an asterisk (*) for child domains to reduce the administrative burden of managing certificates. Subject alternative name (SAN) certificates can be used for multiple domains with different domain names.
- CER is an ASCII format and DER is a binary format.
- PEM is the most commonly used certificate format and can be used for just about any certificate type.
- P7B certificates are commonly used to share public keys. P12 and PFX certificates are commonly used to hold the private key.

Online References

- Remember, there are additional resources at <https://greatadministrator.com/sy0-601-extras>. Resources include labs, sample performance-based questions, and more.

Chapter 10 Practice Questions

1. GCGA, a software development company, occasionally updates its software with major updates and minor patches. Administrators load these updates to the company web site along with a hash associated with each update. Which of the following BEST describes the purpose of the hash?
 - A. Availability of updates and patches
 - B. Integrity of updates and patches
 - C. Confidentiality of updates and patches
 - D. Integrity of the application

2. Users in your organization sign their emails with digital signatures. Which of the following provides integrity for these digital signatures?
 - A. Hashing
 - B. Encryption
 - C. Non-repudiation
 - D. Private key

3. While reviewing logs on a web server hosted by your organization, you notice multiple logon failures to an FTP account, but they're only happening about once every 30 minutes. You also see that the same password is being tried against the SSH account right after the FTP account logon failure. What BEST describes what is happening?
 - A. Brute force attack
 - B. Dictionary attack
 - C. Plaintext attack
 - D. Spraying attack

4. An online application requires users to log on with their email address and a password. The application encrypts the passwords in a hashed format. Which of the following can be added to decrease the likelihood that attackers can discover these passwords?
 - A. Rainbow tables
 - B. Salt
 - C. Digital signatures

D. Input validation

5. What is the primary difference between a block cipher and a stream cipher?
 - A. A stream cipher encrypts data 1 bit or 1 byte at a time.
 - B. A block cipher encrypts data 1 bit or 1 byte at a time.
 - C. Stream ciphers are used for symmetric encryption, but block ciphers are used for asymmetric encryption.
 - D. Block ciphers are used for symmetric encryption, but stream ciphers are used for asymmetric encryption.

6. A developer is creating an application that will encrypt and decrypt data on mobile devices. These devices don't have a lot of processing power. Which of the following cryptographic methods has the LEAST overhead and can provide encryption for these mobile devices?
 - A. Elliptic curve cryptography
 - B. Perfect forward secrecy
 - C. Salting
 - D. Digital signatures

7. You are configuring a web server that will be used by salespeople via the Internet. Data transferred to and from the server needs to be encrypted, so you are tasked with requesting a certificate for the server. Which of the following would you MOST likely use to request the certificate?
 - A. CA
 - B. CRL
 - C. CSR
 - D. OCSP

8. Users within an organization frequently access public web servers using HTTPS. Management wants to ensure that users can verify that certificates are valid even if the public CAs are temporarily unavailable. Which of the following should be implemented to meet this need?
 - A. OCSP
 - B. CRL
 - C. Private CA

D. CSR

9. Your organization hosts an internal web site used only by employees. The web site uses a certificate issued by a private CA and the network downloads a CRL from the CA once a week. However, after a recent compromise, security administrators want to use a real-time alternative to the CRL. Which of the following will BEST meet this need?

- A. SAN
- B. CSR
- C. RA
- D. OCSP

10. An organization hosts several web servers in a web farm used for e-commerce. Due to recent attacks, management is concerned that attackers might try to redirect web site traffic, allowing the attackers to impersonate their e-commerce site. Which of the following methods will address this issue?

- A. Stapling
- B. Perfect forward secrecy
- C. Pinning
- D. Key stretching

11. Management has mandated the use of digital signatures by all personnel within your organization. Which of the following use cases does this support?

- A. Supporting confidentiality
- B. Supporting availability
- C. Supporting obfuscation
- D. Supporting non-repudiation

12. A DLP system detected confidential data being sent out via email from Bart's account. However, he denied sending the email. Management wants to implement a method that would prevent Bart from denying accountability in the future. Which of the following are they trying to enforce?

- A. Confidentiality

- B. Encryption
- C. Access control
- D. Non-repudiation

13. Your organization recently updated the security policy and mandated that emails sent by all upper-level executives include a digital signature. Which security goal does this policy address?

- A. Confidentiality
- B. Hashing
- C. Obfuscation
- D. Authentication

14. You are tasked with getting prices for certificates. You need to find a source that will provide a certificate that can be used for multiple domains that have different names. Which of the following certificates is the BEST choice?

- A. SAN
- B. Domain validation
- C. Extended validation
- D. Wildcard

15. Your organization recently lost access to some decryption keys, resulting in the loss of some encrypted data. The chief information officer (CIO) mandated the creation of a key escrow. Which of the following cryptographic keys are MOST likely to be stored in key escrow?

- A. Public
- B. Private
- C. Ephemeral
- D. Session

Chapter 10 Practice Question Answers

1. **B** is correct. The hash provides integrity for the updates and patches so that users can verify they have not been modified. Installing updates and patches increases the availability of the application. Confidentiality is provided by encryption. The hashes are for the updates and patches, so they do not provide integrity for the application.
2. **A** is correct. Hashing provides integrity for digital signatures and other data. A digital signature is a hash of the message encrypted with the sender's private key, but the encryption doesn't provide integrity. The digital signature provides non-repudiation, but non-repudiation does not provide integrity. The private key and public key are both needed, but the private key does not provide integrity.
3. **D** is correct. This indicates a password spraying attack. It loops through a list of accounts, guessing a password for one account at a time, and then guessing the same password for a different account. In this scenario, the attack may be guessing passwords for other servers before it returns to the web server. A brute force attack attempts to guess all possible character combinations for a password, and a dictionary attack uses a dictionary of words trying to discover the correct password. A spraying attack could use either a brute force method or a dictionary method when guessing the password; however, these methods do not loop through a list of user accounts. In a plaintext attack (also called a known plaintext attack), an attacker has samples of known plaintext and can use these samples to decrypt ciphertext that includes this plaintext.
4. **B** is correct. A password salt is additional random characters added to a password before hashing the password, and it decreases the success of password attacks. Rainbow tables are used by attackers and contain precomputed hashes, and salting is intended to specifically thwart rainbow table attacks. A digital signature provides authentication, non-repudiation, and integrity, but it doesn't protect passwords. Input validation techniques

verify data is valid before using it, and they are unrelated to protecting hashed passwords.

5. **A** is correct. A stream cipher encrypts data a single bit or a single byte at a time and is more efficient when the size of the data is unknown, such as streaming audio or video. A block cipher encrypts data in specific-sized blocks, such as 64-bit blocks or 128-bit blocks. Both are used with symmetric encryption algorithms.
6. **A** is correct. Elliptic curve cryptography (ECC) has minimal overhead and is often used with mobile devices for encryption. Perfect forward secrecy refers to session keys and provides assurances that session keys will not be compromised even if a private key is later compromised. Salting adds random characters to a password before hashing it to thwart rainbow table attacks. Digital signatures provide integrity, authentication, and non-repudiation, but not encryption.
7. **C** is correct. You would request a certificate with a certificate signing request (CSR). It uses a specific format to request a certificate. You submit the CSR to a certificate authority (CA), but the request needs to be in the CSR format. A certificate revocation list (CRL) is a list of revoked certificates. The Online Certificate Status Protocol (OCSP) is an alternate method of validating certificates and indicates if a certificate is good, revoked, or unknown.
8. **B** is correct. A certificate revocation list (CRL) can meet this need because CRLs are cached. If the public certificate authority (CA) is not reachable due to any type of connection outage or CA outage, the cached CRL can be used if the cache time has not expired. The Online Certificate Status Protocol (OCSP) works in real time where the client queries the CA with the serial number of the certificate. If the CA is unreachable, the certificate cannot be validated. A private CA is used within an organization and cannot validate certificates from a public CA. You request a certificate with a certificate signing request (CSR), but the CSR doesn't validate an issued certificate.

9. **D** is correct. The Online Certificate Status Protocol (OCSP) provides real-time responses to validate certificates issued by a certificate authority (CA). A certificate revocation list (CRL) includes a list of revoked certificates, but if it is only downloaded once a week, it can quickly be out of date. None of the other answers validates certificates. In the context of certificates, a subject alternative name (SAN) certificate is used for multiple domains that have different names but are owned by the same organization. A certificate signing request (CSR) is used to request a certificate. A registration authority (RA) accepts CSRs for a CA.

10. **C** is correct. Public key pinning provides clients with a list of public key hashes that clients can use to detect web site impersonation attempts. Stapling reduces Online Certificate Status Protocol (OCSP) traffic by appending a timestamped, digitally signed OCSP response to a certificate. Perfect forward secrecy ensures that the compromise of one session key does not compromise other session keys used in the past. Key stretching techniques add additional bits (salts) to passwords, making them harder to crack.

11. **D** is correct. Digital signatures will support a use case of supporting non-repudiation. Digital signatures also provide integrity and authentication, but these weren't available answers. Digital signatures don't encrypt data, so they do not support a use case of supporting confidentiality. Redundancy and fault-tolerance solutions will increase availability. Steganography is one way of supporting obfuscation.

12. **D** is correct. Non-repudiation methods such as digital signatures prevent users from denying they took an action. In this scenario, if a data loss protection (DLP) system detected the outgoing email and it was signed with Bart's account using a digital signature, he couldn't believably deny sending it. Encryption methods protect confidentiality. Access control methods protect access to data.

13. **D** is correct. A digital signature is an encrypted hash of a message and it can be used to provide authentication, integrity, and non-repudiation. Authentication identifies the sender of the email. Encryption provides

confidentiality and prevents unauthorized disclosure. Obfuscation methods attempt to make something harder to read, but a digital signature doesn't provide obfuscation. Hashing is a method used to provide integrity, but hashing by itself isn't a security goal.

14. **A** is correct. A subject alternative name (SAN) certificate is used for multiple domains that have different names but are owned by the same organization. A domain-validated certificate indicates that the certificate requestor has some control over a Domain Name System (DNS) domain. Extended validation certificates use additional steps beyond domain validation. A wildcard certificate starts with an asterisk (*) and can be used for multiple domains, but each domain name must have the same root domain.

15. **B** is correct. Copies of private keys are typically stored in a key escrow so that data encrypted with a private key can be retrieved if the original private key is no longer accessible. Public keys are available to anyone so there is no need to store them in a key escrow. An ephemeral key has a short lifetime and is re-created for each session. A session key is only used for a single session so wouldn't be stored in a key escrow.

Chapter 11

Implementing Policies to Mitigate Risks

CompTIA Security+ objectives covered in this chapter:

- 1.5 Explain different threat actors, vectors, and intelligence sources.**
 - Vectors (Supply chain)
- 1.6 Explain the security concerns associated with various types of vulnerabilities.**
 - Impacts (Data breaches, Reputation) Third-party risks (Vendor management, System integration, Lack of vendor support, Supply chain)
- 1.7 Summarize the techniques used in security assessments.**
 - Security orchestration, automation, response (SOAR)
- 2.1 Explain the importance of security concepts in an enterprise environment.**
 - Data protection (Masking, Tokenization)
- 2.5 Given a scenario, implement cybersecurity resilience.**
 - Diversity (Vendors)
- 2.7 Explain the importance of physical security controls.**
 - Secure data destruction, Burning, Shredding, Pulping, Pulverizing, Degaussing, Third-party solutions
- 3.2 Given a scenario, implement host or application security solutions.**
 - Database (Tokenization)
- 4.1 Given a scenario, use the appropriate tool to assess organizational security.**
 - Forensics (dd, Memdump, WinHex, FTK imager, Autopsy), Data sanitization
- 4.2 Summarize the importance of policies, processes, and procedures for incident response.**
 - Incident response plans, Incident response process (Preparation, Identification, Containment, Eradication, Recovery, Lessons learned), Stakeholder management, Communication plan, Incident response team, Retention policies
- 4.3 Given an incident, utilize appropriate data sources to support an investigation.**
 - Log files (Dump files), Bandwidth monitors, Metadata (Email, Mobile, Web, File)
- 4.4 Given an incident, apply mitigation techniques or controls to secure an environment.**
 - Isolation, Containment, SOAR (Runbooks, Playbooks)
- 4.5 Explain the key aspects of digital forensics.**
 - Documentation/evidence (Legal hold, Video, Admissibility, Chain of custody, Tags, Reports, Event logs, Interviews),
 - Timelines of sequence of events (Time stamps, Time offset),

- Acquisition (Order of volatility, Disk, Random-access memory (RAM), Swap/pagefile, OS, Device, Firmware, Snapshot, Cache, Network, Artifacts)
- On-premises vs. cloud (Right to audit clauses, Regulatory/jurisdiction, Data breach notification laws),
- Integrity (Hashing, Checksums, Provenance), Preservation, E-discovery, Data recovery, Non-repudiation Strategic intelligence/counterintelligence

5.2 Explain the importance of applicable regulations, standards, or frameworks that impact organizational security posture.

- Regulations, standards, and legislation (General Data Protection Regulation (GDPR), National, territory, or state laws)

5.3 Explain the importance of policies to organizational security.

- Personnel (Acceptable use policy, Job rotation, Mandatory vacation, Separation of duties, Least privilege, Clean desk space, Background checks, Non-disclosure agreement (NDA), Social media analysis, Onboarding, Offboarding)
- User training (Gamification, Capture the flag, Phishing campaigns, Phishing simulations, Computer-based training (CBT), Role-based training), Diversity of training techniques
- Third-party risk management (Vendors, Supply chain, Business partners, Service level agreement (SLA), Memorandum of understanding (MOU), Measurement systems analysis (MSA), Business partnership agreement (BPA), End of life (EOL), End of service (EOSL), NDA)
- Data (Classification, Governance, Retention)

5.4 Summarize risk management processes and concepts.

- Risk analysis (Regulations that affect risk posture)

5.5 Explain privacy and sensitive data concepts in relation to security.

- Organizational consequences of privacy breaches (Reputation damage, Identity theft, Fines, IP theft), Notifications of breaches (Escalation, Public notifications and disclosures)
- Data types (Classifications, Public, Private, Sensitive, Confidential, Critical, Proprietary, Personally identifiable information (PII), Health information, Financial information, Government data, Customer data)
- Privacy enhancing technologies (Data minimization, Data masking, Tokenization, Anonymization, Pseudo-anonymization)
- Roles and responsibilities (Data owners, Data controller, Data processor, Data protection officer (DPO), Data custodian/steward)
- Information life cycle, Impact assessment, Terms of agreement, Privacy notice

**

Organizations often develop written security policies. These provide guiding principles to the professionals who implement security throughout the organization. These policies include personnel management policies and data protection policies. Combined with training for personnel to raise overall security awareness, they help mitigate risk and reduce security

incidents. However, security incidents still occur, and incident response policies and forensic data policies provide the direction on how to handle them.

Exploring Security Policies

Security policies are written documents that lay out a security plan within a company. They are one of many administrative controls used to reduce and manage risk. When created early enough, they help ensure that personnel implement security throughout the life cycle of various systems in the company. When employees follow the policies and procedures, they help prevent incidents, data loss, and theft.

Policies include brief, high-level statements that identify goals based on an organization's overall beliefs and principles. After creating the policy, personnel within the organization create plans and procedures to support the policies. Although the policies are often high-level statements, the plans and procedures provide details on policy implementation.

A security policy can be a single large document or be divided into several smaller documents, depending on the needs of the company. The following sections identify many of the common elements of a security policy.

Personnel Policies

Companies frequently develop policies to define and clarify issues related to personnel. This includes personnel behavior, expectations, and possible consequences. Personnel learn these policies when they are hired and as changes occur. The following sections cover common personnel policies in more depth.

Acceptable Use Policy

It often describes the purpose of computer systems and networks, how users can access them, and the responsibilities of users when they access the systems.

Many organizations monitor user activities, such as what websites they visit and what data they send out via email. For example, a proxy server would typically log websites visited by users. The AUP may include statements informing users that systems are in place monitoring their activities.

In some cases, the AUP might include privacy statements informing users of the computer activities they can consider private. Many users have an expectation of privacy when using an organization's computer systems and networks that isn't justified. The ***privacy policy*** statement helps to clarify the organization's stance.

It's common for organizations to require users to read and sign a document indicating they understand the acceptable use policy when they're hired and in conjunction with annual security training. Other methods, such as logon banners or periodic emails, help reinforce an AUP.

Mandatory Vacations

Mandatory vacation policies help detect when employees are involved in malicious activity, such as fraud or embezzlement. As an example, employees in positions of fiscal trust, such as stock traders or bank employees, are often required to take an annual vacation of at least five consecutive workdays.

For embezzlement actions of any substantial size to succeed, an employee would need to be constantly present to manipulate records and

respond to different inquiries. On the other hand, if a policy forces an employee to be absent for at least five consecutive workdays, someone else would be required to answer any queries during the employee's absence. This increases the likelihood of discovering illegal activities by employees. It also acts as an effective deterrent.

Mandatory vacations aren't limited to only financial institutions, though. Many organizations require similar policies for administrators. For example, an administrator might be the only person required to perform sensitive activities such as reviewing certain logs. A malicious administrator can overlook or cover up certain activities revealed in the logs. However, a mandatory vacation policy would require someone else to perform these activities, which increases the chance of discovery.

Of course, mandatory vacations by themselves won't prevent fraud. Most companies will implement the principle of defense in depth by using multiple layers of protection. Additional policies may include separation of duties and job rotation to provide as much protection as possible.

Remember this

Mandatory vacation policies require employees to take time away from their job. These policies help to deter fraud and discover malicious activities while the employee is away.

Separation of Duties

Separation of duties is a principle that prevents any single person or entity from being able to complete all the functions of a critical or sensitive process. It helps prevent fraud, theft, and errors.

Two people perform separate actions to prevent inventory fraud. One person is authorized to order goods from suppliers, but someone else would record the receipt of goods. This prevents one person from ordering goods for himself and then logging them as received.

Similarly, when receiving inventory, one person would record the receipt of goods when they are received. Another person would approve the payment for these goods, and a third person could make the payments. If Homer oversaw all three processes, he could approve and make payments to Homer's Most Excellent Retirement Account for goods that were never

received. If Homer doesn't go to jail, he may indeed retire early at the expense of the financial health of the company.

Separation of duties policies also apply to IT personnel. For example, it's common to separate application development tasks from application deployment tasks. In other words, developers create and modify applications and then pass the compiled code to administrators. Administrators then deploy the code to live production systems. Without this policy in place, developers might be able to make quick, untested changes to code, resulting in unintended outages. This provides a high level of version control and prevents potential issues created through uncontrolled changes.

As another example, a group of IT administrators may be responsible for maintaining a group of database servers. However, they would not be granted access to Security logs on these servers. Instead, security administrators regularly review these logs, but these security administrators would not have access to data within the databases.

Imagine that Bart has been working as an IT administrator but recently changed jobs and is now working as a security administrator. What should happen? Based on the separation of duties principle, Bart should now have access to the security logs, but database administrators should revoke his access to the data in the databases. If database administrators don't revoke his database permissions, he will have more access than he needs, violating the principle of least privilege. An account audit would often discover these types of issues.

Remember this

Separation of duties prevents any single person or entity from controlling all the functions of a critical or sensitive process by dividing the tasks between employees. This helps prevent potential fraud, such as if a single person prints and signs checks.

Least Privilege

The principle of ***least privilege*** specifies that individuals and processes are granted only the privileges needed to perform assigned tasks or functions, but no more. Privileges are the rights and permissions assigned to authorized users and processes. For example, if Lisa needs read access to a

folder on a server, you should grant her read access to that folder, but nothing else.

A primary goal of implementing least privilege is to reduce risks. As an example, imagine that Carl works at the Nuclear Power Plant, but administrators have improperly configured accounts ignoring the principle of least privilege. In other words, Carl has access to all available data within the Nuclear Power Plant, not just the limited amount of data he needs to perform his job. Later, Lenny gets into trouble and needs money, so he convinces Carl to steal data from the power plant so that they can sell it. In this scenario, Carl can steal and sell all the data at the plant, which can result in serious losses.

In contrast, if administrators applied the principle of least privilege, Carl would only have access to a limited amount of data. Even if Lenny convinces him to steal the data, Carl wouldn't be able to steal very much simply because he doesn't have access to it. This limits the potential losses for the power plant.

This principle applies to regular users and administrators. As an example, if Marge administers all the computers in a training lab, it's appropriate to give her administrative control over all these computers. However, her privileges don't need to extend to the domain, so she wouldn't have administrative control over all the computers in a network. Additionally, she wouldn't have the privileges required to add these computers to the domain, unless that was a requirement in the training lab. Similarly, if a network administrator needs to review logs and update specific network devices, it's appropriate to give the administrator access to these logs and devices, but no more.

Many services and applications run under the context of a user account. These services have the privileges of this user account, so it's important to ensure that these accounts are granted only the privileges needed by the service or the application. In the past, many administrators configured these service and application accounts with full administrative privileges. When attackers compromised a service or application configured this way, they gained administrative privileges and wreaked havoc on the network.

SQL Server sa Account

Microsoft SQL Server includes a built-in system administrator account named sa. By default, this account is a member of the sysadmin fixed server role, giving it full administrative privileges on the server. SQL Server uses the sa account in SQL Server Authentication mode only.

Windows Authentication mode uses a Windows account to access SQL Server, and SQL Server Authentication mode uses a SQL Server account (such as the built-in sa account) to access SQL Server. You select either Windows Authentication mode or SQL Server and Windows Authentication mode when you install SQL Server.

When you install newer versions of SQL Server, the installation program forces you to assign a strong password if you select SQL Server and Windows Authentication mode. It will then enable the account. If you choose Windows Authentication mode, the installation sets a strong password and disables the account.

Unfortunately, there are many scenarios where the account is enabled with a blank password. Early versions of SQL Server allowed you to leave the password blank. Additionally, some versions of the Microsoft SQL Server Desktop Engine enable the account with a blank sa password.

It's a well-known vulnerability, and if attackers compromise a system, you can bet that it is one of the things they'll check. If it is enabled with a blank password, they can use it to escalate their privileges and move laterally throughout the network.

Remember this

Least privilege specifies that individuals or processes are granted only those rights and permissions needed to perform their assigned tasks or functions. By implementing the least privilege policy, it limits potential losses if any individual or process is compromised.

Job Rotation

Job rotation is a concept that has employees rotate through different jobs to learn the processes and procedures in each job. From a security perspective, job rotation helps to prevent or expose dangerous shortcuts or even fraudulent activity. Employees might rotate through jobs temporarily or permanently.

For example, your company could have an Accounting department. As mentioned in the “Separation of Duties” section, you would separate job tasks so that no individual would control all the functions of critical processes. Additionally, you could rotate personnel in and out of jobs performing these tasks. This would ensure more oversight over past transactions and help ensure that employees are following rules and policies.

In contrast, imagine a single person always performs the same function without any expectation of oversight. This increases the temptation to go outside the bounds of established policies.

Job rotation policies work well together with separation of duties policies. A separation of duties policy helps prevent a single person from controlling too much. However, if an organization only uses a separation of duties policy, two people can collude in a scheme to defraud the company. If a job rotation policy is also used, these two people will not be able to continue the fraudulent activity indefinitely.

Job rotation policies also apply to IT personnel. For example, the policy can require administrators to swap roles regularly, such as annually or quarterly. This prevents any single administrator from having too much control over a system or network.

Remember this

Job rotation policies require employees to change roles regularly. Employees might change roles temporarily, such as for three to four weeks, or permanently. This helps ensure that employees cannot continue with fraudulent activity indefinitely.

Clean Desk Space

A *clean desk space* policy directs users to keep their areas organized and free of papers. The primary security goal is to reduce threats of security incidents by ensuring the protection of sensitive data. More specifically, it helps prevent the possibility of data theft or inadvertent disclosure of information.

Imagine an attacker who goes into a bank and meets a loan officer. The loan officer has stacks of paper on his desk, including loan applications from various customers. If the loan officer steps out for a moment, the

attacker can easily grab some of the documents or simply take pictures of the documents with a mobile phone.

Beyond security, organizations want to present a positive image to customers and clients. Employees with cluttered desks with piles of paper can easily turn off customers. However, a clean desk space policy doesn't just apply to employees who meet and greet customers. It also applies to employees who don't interact with customers. Just as dumpster divers can sort through trash to gain valuable information, anyone can sort through papers on a desk to learn information. It's best to secure all documents to keep them away from prying eyes. Some items left on a desk that can present risks include:

- Keys
- Cell phones
- Access cards
- Sensitive papers
- Logged-on computer
- Printouts left in the printer
- Passwords on Post-it notes
- File cabinets left open or unlocked
- Personal items such as mail with Personally Identifiable Information (PII)

Some people want to take a clean desk space policy a step further by scrubbing and sanitizing desks with antibacterial cleaners and disinfectants daily. They are free to do so, but that isn't part of a security-related clean desk space policy.

Remember this

A clean desk space policy requires users to organize their areas to reduce the risk of possible data theft. It reminds users to secure sensitive data and may include a statement about not writing down passwords.

Background Check

It's common for organizations to perform background checks on potential employees and even after employees are hired. ***Background checks*** investigate employees' histories to discover anything about them that might make them less-than-ideal for any given job.

A background check will vary depending on job responsibilities and the sensitivity of data that an employee can access. For example, a background check for an associate at Walmart will be significantly less than a background check for a government employee who will handle Top Secret Sensitive Compartmented Information.

However, background checks will typically include a query to law enforcement agencies to identify a person's criminal history. In some cases, this is only to determine if the person is a felon. In other instances, it checks for all potential criminal activity, including a review of a person's driving records.

Many organizations check a person's financial history by obtaining a credit report. For example, someone applying for a job in an Accounting department might not be a good fit if his credit score is 350 and he has a string of unpaid loans.

It is also common for employers to check a person's online activity. This includes social media sites, such as Facebook, LinkedIn, and Twitter. Some people say and do things online that they would rarely do in public. One reason is a phenomenon known as the online disinhibition effect. Just as a beer or glass of wine releases inhibitions in many people, individuals are often less inhibited when posting comments online. And what they post often reflects their true feelings and beliefs. Consider a person who frequently posts hateful comments about others. A potential employer might think that this person is unlikely to work cohesively in a team environment and choose to hire someone else.

Note that some background checks require written permission from the potential employee. For example, the Fair Credit Reporting Act (FCRA) requires organizations to obtain written permission before getting a credit report on a job applicant or employee. However, other background checks don't need consent. For example, anyone can look at an individual's social media profile.

Onboarding

Onboarding is the process of granting individuals access to an organization's computing resources after being hired. This includes providing the employee with a user account and granting access to appropriate resources. One of the key considerations during the onboarding

process is to follow the principle of least privilege. In other words, it's appropriate to grant the new employees access to what they need for their job, but no more.

Offboarding

Offboarding is the process of removing an employee's access when he leaves the company. This includes disabling the user's account or deleting it depending on company policy. It also includes collecting any equipment (such as smartphones, tablets, or laptops), security badges, or proximity cards the organization issued to the employee. This is more than just a cost issue. Equipment often has proprietary data on it, and the company needs to take steps to protect the data. Additionally, smart cards and proximity cards can allow individuals access to protected areas.

It's common to remove an employee's access during an exit interview. Organizations sometimes do this by informing senior personnel in the IT department of the scheduled interview a day before. An administrator then disables the account after the interview starts. The key is that a departing employee should not have access to computing and network resources after the interview.

Remember this

Background checks investigate the history of an individual prior to employment and, sometimes, during employment. They may include criminal checks, credit checks, and an individual's online activity. Onboarding is the process of granting new employees access to resources. Offboarding removes this access often by disabling or deleting a user's account. Offboarding also includes collecting everything issued to the employee.

Non-Disclosure Agreement

A ***non-disclosure agreement (NDA)*** is used between two entities to ensure that proprietary data is not disclosed to unauthorized entities. For example, imagine BizzFad wants to collaborate with Costington's on a project. BizzFad management realizes they need to share proprietary data with Costington's personnel, but they want to ensure that the distribution of

the data is limited. The NDA is a legal document that BizzFad can use to hold Costington's legally responsible if the proprietary data is shared.

Similarly, many organizations use an NDA to prohibit employees from sharing proprietary data either while they are employed or after leaving the organization. It's common to remind employees of an existing NDA during offboarding or an exit interview.

Social Media Analysis

In the context of personnel security policies, social media analysis refers to monitoring employee activity on social media networks such as Facebook, LinkedIn, Instagram, and Twitter. As mentioned previously, employers often check social media networks during a background check process. However, some employers monitor social media activity during employment.

As an example, a company fired a woman after a video of her went viral. A bird-watcher in Central Park asked her to leash her dog. She responded, saying she would call 911 telling them a man is threatening her life. The video shows her calling while dragging and choking her dog, holding it by the collar. After an internal review, her company fired her the next day.

AUPs often specify what employees can and cannot do with social media. These policies might include:

- Employees cannot use company resources (such as computers or networks) to post to an employee's personal social media account.
- Employees cannot engage in illegal activities. This includes engaging in hate speech against others based on race, religion, or gender.
- Employees cannot divulge any confidential information or trade secrets.
- Employees cannot misrepresent their employer.
- Employees cannot defame competitors.

With a policy in place, security professionals may use social media analysis to verify that policies are followed. One simple method is to use a tool to regularly search social media sites for any mention of the organization and investigate any hits. If the organization receives any

specific complaints about an employee, such as an employee bullying someone else, they can narrow their search based on the complaint.

Third-Party Risk Management

Organizations interact with entities outside the organization (commonly called third parties) for various reasons, such as purchasing supplies, creating partnerships, and more. These relationships can often introduce risks that need to be managed, and security policies sometimes address these risks.

Supply Chain and Vendors

A ***supply chain*** includes all the elements required to produce and sell products and services. In some cases, the supply chain becomes an attack vector. By exploiting vulnerabilities in the supply chain, attackers can impact the primary organization.

Supply chain policies vary depending on the vendors. A vendor is an entity in the supply chain that provides goods or services to an organization. In general, it's best to limit the amount of access that vendors have to internal networks or data to only what they need, and vendor management systems provide vendors with limited access.

Vendors often need to provide feedback to an organization, such as order status, and vendor management systems provide vendors with limited system integration. As an example, some organizations use web-based applications, allowing vendors to enter data. These web-based applications limit access with credentials. Additionally, these web applications have limited integration with internal systems.

Organizations sometimes implement policies requiring ***vendor diversity*** to provide cybersecurity resilience. Using more than one vendor for the same supply reduces the organization's risk if that vendor can no longer provide the product or service.

Supply chain policies will also provide guidelines on limiting vendor access to an organization's network and data. The goal is to limit damage to the organization if an attacker exploits a vendor. Vendor management policies include limiting system integration and understanding when vendor support stops.

When working with vendors, it's also important to be aware of *end of life (EOL)* and *end of service life (EOSL)* policies. EOL generally refers to the date when a product will no longer be offered for sale. You can think of this as the shelf life of the product. EOSL indicates the date when you expect a lack of vendor support because vendors no longer create patches or upgrades to resolve vulnerabilities for the product.

Attack on Vendor Exposes Customer Data

M. J. Brunner, Inc., is a software development and marketing agency and is a vendor for multiple companies. They developed and maintained the online enrollment portal of SEI Investments Co., a vendor for other clients such as Pacific Investment Management Co. (PIMCO), Fortress Investment Group LLC, and more. In May 2020, attackers launched a successful ransomware attack against M. J. Brunner, Inc. Before encrypting the data, attackers exfiltrated it and gained access to customer data from SEI Investments Co. and their clients.

In this case, attackers accessed PIMCO investor data, but not due to a vulnerability at PIMCO. It wasn't even due to a vulnerability of their vendor, SEI Investments Co. Instead, this ransomware attack on M. J. Brunner, Inc., caused this data breach.

Attackers reportedly collected information such as names, usernames, emails, physical addresses, and phone numbers. While attackers may not have collected passwords in this data breach, they could still use the other information to target individuals in smishing, vishing, or phishing attacks.

Third-Party Agreements

Organizations often utilize different types of agreements to help identify various responsibilities. Organizations use them when working with other organizations, but they can also use them when working with different departments within the same organization. These include:

- **Service level agreement (SLA).** An SLA is an agreement between a company and a vendor that stipulates performance expectations, such as minimum uptime and maximum downtime levels.

Organizations use SLAs when contracting services from service providers, such as Internet Service Providers (ISPs). Many SLAs

include a monetary penalty if the vendor is unable to meet the agreed-upon expectations.

- **Memorandum of understanding (MOU).** An MOU, sometimes called a memorandum of agreement (MOA), expresses an understanding between two or more parties indicating their intention to work together toward a common goal. You can also compare an MOU with an SLA because it defines the responsibilities of each of the parties. However, it is less formal than an SLA and does not include monetary penalties.
- **Business partners agreement (BPA).** A BPA is a written agreement that details the relationship between business partners, including their obligations toward the partnership. It typically identifies the shares of profits or losses each partner will take, their responsibilities to each other, and what to do if a partner chooses to leave the partnership. One of the primary benefits of a BPA is that it can help settle conflicts when they arise.

Terms of Agreement

A *term of agreement* refers to the period that an agreement shall be in effect. It is frequently added as a clause in a legal document. NDAs, SLAs, BPAs, and other types of agreements can include it.

Measurement Systems Analysis

A *measurement systems analysis (MSA)* evaluates the processes and tools used to make measurements. The MSA uses various methods to identify variations within a measurement process that can result in invalid results. Ideally, a measurement system should produce the same values when measuring the same sample. If it doesn't, it results in inaccurate data. Worse, decision makers may make decisions based on the faulty data.

As a simple example, imagine an organization decides to take employees' temperatures as they walk in, and they do so with a no-touch forehead thermometer. An MSA would evaluate the accuracy of the thermometer by verifying it gives consistent, accurate readings.

Additionally, the MSA would evaluate how the thermometer is used by observing how people take the measurements. Everyone should follow the manufacturer's directions in the same way, such as pointing the

thermometer toward the forehead in the same way and taking the temperature from the same distance.

In practice, MSAs involve a lot more than just a single tool and a single process. An MSA policy would provide guidelines to personnel performing the analysis.

Remember this

Supply chain and vendor policies typically provide guidance on how to limit access given to vendors. An SLA is an agreement between a company and a vendor that stipulates performance expectations, such as minimum uptime and maximum downtime levels. A memorandum of understanding (MOU) expresses an understanding between two or more parties indicating their intention to work together toward a common goal. A measurement systems analysis (MSA) evaluates the processes and tools used to make measurements.

Incident Response Policies

Many organizations create ***incident response*** policies to help personnel identify and respond to incidents. A ***security incident*** is an adverse event or series of events that can negatively affect the confidentiality, integrity, or availability of data or systems within the organization, or that has the potential to do so.

As an example, a ***data breach*** is a security incident where unauthorized entities access data. Common data breaches occur after an attacker gains access to a network, finds vulnerable systems holding data, and exfiltrates or extracts it.

Other examples of security incidents include cyberattacks, the release of malware, security policy violations, and inappropriate usage of systems. For example, an attack resulting in a data breach is a security incident. Once the organization identifies a security incident, it will respond based on the incident response policy.

Organizations regularly review and update the policy. Reviews might occur on a routine schedule, such as annually, or in response to an incident after performing a lessons learned review of the incident.

As an example, in the early days of computers, one hacker broke into a government system, and the first thing he saw was a welcome message. He started poking around, but authorities apprehended him. Later, when the judge asked him what he was doing, he replied that when he saw the welcome message, he thought it was inviting him in. The lesson learned here was that a welcome message can prevent an organization from taking legal action against an intruder. Government systems no longer have welcome messages. Instead, they have warning banners stressing that only authorized personnel should be accessing the system. It's common to see similar warning banners when logging on to any system today.

NIST SP 800-61 Revision 2, “Computer Security Incident Handling Guide,” provides comprehensive guidance on responding to incidents. It is 79 pages long, so it’s obviously more in-depth than this section, but if you want to dig deeper into any of these topics, it’s an excellent resource. Use your favorite search engine and search for “NIST SP 800-61.”

Remember this

An incident response policy defines a security incident and incident response procedures. Incident response procedures start with preparation to prepare for and prevent incidents. Preparation helps prevent incidents such as malware infections. Personnel review the policy periodically and in response to lessons learned after incidents.

Incident Response Plan

An *incident response plan* provides more detail than the incident response policy. It provides organizations with a formal, coordinated plan that personnel can use when responding to an incident. Some of the common elements included with an incident response plan include:

- **Definitions of incident types.** This section helps employees identify the difference between an event (that might or might not be a security incident) and an actual incident. Some types of incidents include attacks from botnets, malware delivered via email, data breaches, and a ransom demand after a criminal encrypts an organization's data. The plan may group these incident types using specific category definitions, such as attacks, malware infections, and data breaches.
- **Incident response team.** An incident response team is composed of employees with expertise in different areas. Organizations often refer to the team as an incident response team, a computer incident response team (CIRT), or a security incident response team. Combined, they have the knowledge and skills to respond to an incident. Due to the complex nature of incidents, the team often has extensive training. Training includes concepts, such as how to identify and validate an incident, how to collect evidence, and how to protect the collected evidence.
- **Roles and responsibilities.** Many incident response plans identify specific roles for an incident response team along with their responsibilities. For example, an incident response team might include someone from senior management with enough authority to get things done, a network administrator or engineer with the technical expertise necessary to understand the problems, a security expert who knows how to collect and analyze evidence, and a communication expert to relay information to the public if necessary.

Communication Plan

A communication plan is part of an incident response plan, and it provides direction on how to communicate issues related to an incident. As with all elements of an incident response plan, it's important to create the communication plan before an incident. If a plan isn't in place, the wrong people may talk to the media and give the impression that the incident is causing chaos within the organization.

It's common for a communication plan to include the following elements:

- **First responders.** Initial responders, such as a help-desk technician, should know when to inform incident response entities of an incident and who to contact. While a single malware infection may not seem serious, it could easily be the first hint of a significant attack or data breach. If first responders report all incidents, it increases the possibility of catching and thwarting an incident early.
- **Internal communication.** The incident response team should know when to inform senior personnel of an incident. As an example, it's unnecessary to inform the chief executive officer (CEO) of a distributed denial of service (DDoS) attack on a web server that is being blocked by automated response systems. Then again, it's appropriate to inform all senior management of a data breach exposing private data of thousands of customers, or serious incidents that have the potential to affect critical operations.
- **Reporting requirements.** Often, a security incident needs to be reported to external entities such as law enforcement. If customer data is exposed, customers need to be notified. Laws often drive the reporting requirements, and the incident response plan outlines who needs to be notified and when.
- **External communication.** It should be clear who can talk to external entities, such as the media. Just as important, everyone should know they should refer all external queries to the appropriate internal personnel.
- **Law enforcement.** Law enforcement personnel can often provide significant help after an incident. They typically have teams with digital forensics tools and knowledge. However, bringing in law enforcement increases the chance that the incident may get increased public scrutiny. With this mind, a communication plan

will typically designate who can authorize bringing law enforcement into the picture.

- **Customer communication.** In some cases, laws dictate when an organization must inform customers of a data breach. In other cases, it becomes a judgment call. Because informing (or not informing) customers of an incident may affect an organization's reputation, a communication plan may designate senior executives as the only people authorized to approve this communication.

Data Breach Responses

There are multiple consequences related to data breaches. If intellectual property (IP), such as trade secrets and software algorithms, is stolen, the organization will suffer direct losses. If personal information about customers is accessed, attackers can impersonate them and steal their identity. This can result in lawsuits and monetary settlements, causing more direct losses.

As an example, Equifax suffered a massive data breach in 2017 that exposed the personal information of about 147 million people. Exposed data included names, birth dates, Social Security numbers, addresses, and other data that attackers use for identity theft. Lawsuits were settled in 2019 when Equifax agreed to give as much as \$425 million to help people impacted by the data breach. In the settlement, Equifax also agreed to pay at least \$575 million (and potentially as much as \$700 million) in global fines.

When employees discover an incident, they need to identify the extent of the loss. It's common to escalate any data breach to C-Level personnel (such as the chief information officer or the chief executive officer). Depending on the laws applying to the organization and the extent of the incident, it may need to be reported to outside agencies. Public notifications and disclosures are released according to the communication plan.

Stakeholder Management

A stakeholder is any entity with an interest or concern in an organization and can include owners, stock owners, employees, creditors, suppliers, and more. Stakeholder management refers to creating and maintaining positive relationships with stakeholders. Creating and

following a communication plan with stakeholders in mind is an important stakeholder management strategy.

Incident Response Process

Incident response includes multiple phases. It starts with creating an incident response policy and an incident response plan. With the plan in place, personnel are trained and given the tools necessary to handle incidents. Ideally, incident response preparation will help an organization prevent all incidents. However, this isn't realistic for most organizations, but with an effective plan in place, the organization will effectively handle any incidents that occur.

Some of the common phases of an incident response process are:

- **Preparation.** This phase occurs before an incident and provides guidance to personnel on how to respond to an incident. It includes establishing and maintaining an incident response plan and incident response procedures. It also includes establishing procedures to prevent incidents. For example, preparation includes implementing security controls to prevent malware infections.
- **Identification.** All events aren't security incidents, so when a potential incident is reported, personnel take the time to verify it is an actual incident. For example, intrusion detection systems (IDSs) might falsely report an intrusion, but administrators would investigate it and verify if it is a false positive or an incident. If the incident is verified, personnel might try to isolate the system based on established procedures.
- **Containment.** After identifying an incident, security personnel attempt to isolate or contain it. This protects critical systems while maintaining business operations. Containment might include quarantining a device or removing it from the network. This can be as simple as unplugging the system's network interface card to ensure it can't communicate on the network. Similarly, you can isolate a network from the Internet by modifying access control lists on a router or a network firewall. This is similar to how you'd respond to water spilling from an overflowing sink. You wouldn't start cleaning up the water until you first turn off the faucet. The goal of isolation is to prevent the problem from spreading to other

areas or other computers in your network or to simply stop the attack.

- **Eradication.** After containing the incident, it's often necessary to remove components from the attack. For example, if attackers installed malware on systems, it's important to remove all remnants of the malware on all hosts within the organization. Similarly, an attack might have been launched from one or more compromised accounts. Eradication would include deleting or disabling these accounts.
- **Recovery.** During the recovery process, administrators return all affected systems to normal operation and verify they are operating normally. This might include rebuilding systems from images, restoring data from backups, and installing updates. Additionally, if administrators have identified the vulnerabilities that caused the incident, they typically take steps to remove the vulnerabilities.
- **Lessons learned.** After personnel handle an incident, security personnel perform a lessons learned review. The incident may provide some valuable lessons, and the organization might modify procedures or add additional controls to prevent a reoccurrence of the incident. A review might indicate a need to provide additional training to users or indicate a need to update the incident response policy. The goal is to learn from the incident and prevent a future reoccurrence of a similar incident.

Remember this

The first step in the incident response process is preparation. After identifying an incident, personnel attempt to contain or isolate the problem to protect critical systems while maintaining business operations.

Eradication attempts to remove all malicious components from an attack, and recovery returns a system to normal operation. Reviewing lessons learned allows personnel to analyze the incident and the response to prevent a future occurrence.

Understanding SOAR

A trend in incident response is the use of Secure Orchestration, Automation, and Response (SOAR) tools to respond to low-level security events automatically. The key is that SOAR tools respond automatically, which frees up administrators to focus on other administrative and cybersecurity tasks. A SOAR platform is typically a combination of tools that can work together to detect and respond to suspicious activity.

As a simple example, SOAR tools can examine and respond to phishing emails, reducing the amount of time needed by personnel to investigate them. By looking at email elements, such as the header, embedded URLs, and attachments, it's possible to detect suspicious emails. These can be forwarded to other tools to investigate further. For example, a SOAR tool can open attachments within a sandbox and observe the activity. Another SOAR tool may dissect the header looking for discrepancies common in phishing emails such as spoofed email addresses.

When the SOAR platform verifies an email is malicious, it can automatically respond. The response is dependent on the organization's available tools and internal guidelines. It may include quarantining or deleting the email and blocking access to the embedded URLs.

Similarly, it's common for a network with Internet traffic to experience a lot of potentially malicious traffic. When a tool raises an alarm, administrators often must go through the same steps to verify if the threat is real or not. If it is, they usually repeat the same steps to mitigate the threat. In contrast, a SOAR platform can do these same steps automatically to verify if the threat is real or not, and if it is real, implement the appropriate steps to mitigate it.

SOAR platforms use playbooks and runbooks. In general terms, a playbook provides general guidelines, and a runbook provides the technical details to implement the playbook guidelines.

Playbooks

As an example, a playbook for phishing may include a checklist of what to check within a suspected phishing email. It may look for discrepancies between the Reply to and the From addresses, indicating a

spoofed email. If it has an attachment, it may dictate that the email needs to be forwarded to another system, which opens the attachment within a sandbox.

These steps document formal procedures to follow for well-known incidents. They typically identify the same steps that human administrators should take for each suspected incident. Of course, humans can make mistakes even when there is a checklist, but automating the playbook reduces potential human error. Appendix A of NIST SP 800-184 provides a checklist of items to include in a playbook.

Although some playbooks can trigger automated actions, they typically document the steps to take in response to the action, and let the runbook automate the response.

Runbooks

Runbooks implement the guidelines documented in the playbooks using the available tools within the organization. As an example, if a phishing email has discrepancies in the header indicating it is a phishing email, it can implement a rule to quarantine or delete the email. If it has an attachment, it can forward the email to a system that can automatically open the attachment within a sandbox.

Ideally, a runbook can automatically respond to all potential incidents. However, there are times when a runbook may instead assign the task to an administrator to investigate.

Remember this

Secure Orchestration, Automation, and Response (SOAR) platforms use internal tools to respond to low-level security events automatically, reducing administrator workload. A SOAR playbook provides a checklist of things to check for suspected incidents. A SOAR runbook implements the playbook checklist using available tools within the organization.

Understanding Digital Forensics

Organizations implement digital forensic techniques when collecting information after an incident. These help an organization collect and analyze data as evidence it can use to prosecute a crime. In general, forensic evaluations proceed with the assumption that the data collected will be used as evidence in court. Because of this, forensic practices ensure that evidence is controlled and not modified during the collection or analysis of digital data.

Once an incident has been contained or isolated, the next step is a forensic evaluation. What do you think of when you hear forensics? Many people think about the TV program *CSI* (short for “crime scene investigation”) and all its spin-offs. These shows demonstrate the phenomenal capabilities of science in criminal investigations.

Computer forensics techniques analyze evidence from computers to gather details on computer incidents, similar to how CSI personnel analyze evidence from crime scenes. Forensic experts use a variety of different tools to gather and analyze computer evidence. Although you might not be the computer forensics expert collecting or analyzing evidence, you should know some of the basic concepts related to gathering and preserving the evidence.

Key Aspects of Digital Forensics

The following sections cover some key aspects of digital forensics. While forensic experts must understand these, it's also important for anyone involved in a security incident to understand these concepts, too. This is especially important if any evidence is collected.

Admissibility of Documentation and Evidence

When collecting documentation and evidence, it's essential to follow specific procedures to ensure that the evidence is admissible in a court of law. If personnel don't follow proper procedures, the evidence won't be admissible. Following proper procedures also ensures that personnel control the evidence after collecting it, maintaining an unaltered original.

This evidence often supports non-repudiation. It includes proof that individuals were involved in an incident, preventing them from believably denying they were involved.

Admittedly, every security incident won't end up in court. However, at the beginning of an investigation, it's almost impossible to know if it will go to court. Because of this, it's important to treat every incident as if it will go to court, and personnel follow all relevant procedures.

Tags

After an item is identified as possible evidence, it needs to be tagged. This can be a formal document, but it's more common to be something simple, such as a sticker. The tag is placed on the item with the date, time, and name of the person placing the tag. It's also common to include a control number that can be included in a chain of custody.

Chain of Custody

A crucial part of incident response is collecting and protecting evidence. A ***chain of custody*** is a process that provides assurances that evidence has been controlled and appropriately handled after collection. Forensic experts establish a chain of custody when they first collect evidence.

Security professionals use a chain of custody form to document this control. The chain of custody form provides a record of every person who was in possession of a physical asset collected as evidence. It shows who had custody of the evidence and where it was stored the entire time since collection. Additionally, personnel often tag the evidence as part of a chain of custody process. A proper chain of custody process ensures that evidence presented in a court of law is the same evidence that security professionals collected.

As an example, imagine that Homer collected a hard drive as part of an investigation. However, instead of establishing a chain of custody, he stores the drive on his desk, intending to analyze it the next day. Is it possible that someone could modify the contents of the drive overnight? Absolutely. Instead, he should immediately establish a chain of custody and lock the drive in a secure storage location.

If evidence is not controlled, someone can modify, tamper, or corrupt it. Courts will rule the evidence inadmissible if there is a lack of adequate control, or even a lack of documentation showing that personnel maintained adequate control. However, the chain of custody provides proof that personnel handled the evidence properly.

Remember this

A tag is placed on evidence items when they are identified. A chain of custody provides assurances that evidence has been controlled and properly handled after collection. It documents who handled the evidence and when they handled it. A legal hold is a court order to preserve data as evidence.

Legal Hold

A ***legal hold*** refers to a court order to maintain different types of data as evidence. As an example, imagine that ZiffCorp is being sued for fraud and the Securities and Exchange Commission is investigating ZiffCorp. A court orders them to maintain digital and paper documents for the past three years related to the case. ZiffCorp now needs to take steps to preserve the data.

This data may include emails, databases, logs, backup tapes, data stored on servers in file shares and document libraries, and data stored on desktop computers, laptops, tablets, and smartphones owned by the

company. The first step management needs to take is to direct the data custodians to preserve this data. On the surface, this might sound easy, but it can be tremendously complex, especially if it is not clear to data custodians what data should be maintained. They might preserve too much data, resulting in a high cost to store it. They might preserve too little data, subjecting the company to more litigation in a suspected cover-up.

Data retention policies also apply here. As an example, imagine that the data retention policy states that email older than six months is deleted. If administrators rigorously followed the policy, the company wouldn't have any emails from more than six months ago. That's OK if the policy is in writing, and administrators are following it.

What if the administrators didn't follow the data retention policy? What if they have emails from as long as two years ago? In this scenario, administrators need to maintain these emails. If they take steps to delete the emails after receiving the court order, it looks like they are trying to withhold evidence, and it puts the organization into legal jeopardy for a cover-up.

Video

Video surveillance methods such as closed-circuit television (CCTV) systems are often used as a detective control during an investigation. If a person is recorded on video, the video provides reliable proof of the person's location and activity. For example, if a person is stealing equipment or data, the video might provide evidence of the theft.

As an example, I remember a high school student was working nights at a local grocery store. The store had a delivery of beer in a tractor trailer that hadn't been unloaded yet but was kept backed up to the store loading dock overnight. The student stole several cases of beer, thinking the crime was undetectable. However, a video recorded the entire scene. When he showed up for work the next evening, the store promptly called the police and provided a copy of the video. The video offered reliable proof that couldn't be disputed.

Interviews

Another element of an investigation is interviewing witnesses. Witnesses provide firsthand reports of what happened and when it

happened. However, witnesses won't necessarily come forward with relevant information unless someone asks them. Often witnesses don't recognize what information is valuable.

For example, imagine a tailgating incident where an attacker follows closely behind an employee. The employee uses a proximity card to get in, but the attacker just walks right in behind the employee. The employee might notice, but not give it much thought, especially if tailgating is common in the organization. If the attack resulted in the loss of equipment or data, an investigator might get a good description of the attacker just by interviewing witnesses.

Event Logs

A forensic investigation often includes an analysis of available logs. This information helps the investigators re-create events leading up to and during an incident. This can be as simple as looking at Event logs on computers, or Device Logs on routers and firewalls.

Logs record what happened during an event, when it happened, and what account was used during the event. You might remember that a Security log records logon and logoff events. Similarly, many applications require users to authenticate, and Application logs record these authentication events. All these logs can be invaluable in re-creating the details of a security incident, including the identity of the account used in the attack.

Sequence of Events

Digital forensic analysis typically tries to determine the timeline of an event. If the incident results in a data breach or ransomware spread throughout a network, they try to determine how the attacker got in. Today, the first failure is often a user responding inappropriately to a phishing email. By identifying the first failure in the incident, it becomes easier to make recommendations to prevent such a failure in the future.

Logs are one of the primary sources of determining the sequence of events. Log entries include ***timestamps***, so anyone reading the logs can determine when the event occurred. However, it's essential to consider ***time offsets*** based on how the timestamps are recorded.

Imagine you live in Virginia Beach and you see a server log entry of 12:01. You might assume that this indicates 12:01 Eastern Standard Time (EST), but if it's in the winter months, it may be Eastern Daylight Time (EDT). However, the server may be in the cloud and physically located in Las Vegas, which follows Pacific Standard Time (PST) and Pacific Daylight Time (PDT) in the winter months. If you compare this log entry with a log entry on a server located in Pensacola, you need to consider Central Standard Time (CST) and Central Daylight Time (CDT).

To simplify this, many servers use Greenwich Mean Time (GMT) or Coordinated Universal Time (UTC). Neither GMT or UTC observe daylight savings time, and they are both based on the time at the Royal Observatory in Greenwich, London.

If the servers in Virginia Beach, Las Vegas, and Pensacola all use UTC, you don't have to consider a time offset. However, if it's daylight savings time, you'll need to convert the log entry timestamps to UTC for consistency. For Virginia Beach, you add four hours to the EDT time. For Las Vegas, you add seven hours to the PDT time. For Pensacola, you add five hours to the CDT time.

Reports

After analyzing all the relevant evidence, digital forensic experts create a report documenting their findings. These often document the tactics, techniques, and procedures (TTP) used in an attack.

There aren't any specific requirements for the report, but there are some common things you may see, such as:

- An executive summary listing the findings and recommendations
- A listing of the forensic tools used in the investigation
- A list of evidence collected and analyzed
- The findings derived from analyzing each piece of the evidence
- Recommendations based on the findings

A digital forensic analysis report isn't meant to be a legal document. However, if the case goes to court, legal personnel are sure to review every line. The report needs to be technically accurate and focus on the findings

that justify the recommendations. If other experts identify any errors in the reported findings, it can result in the entire report being viewed as tainted.

On-Premises Versus Cloud Concerns

Digital forensics can be challenging enough when all the evidence is on-premises. When an organization uses cloud resources, it can add additional risks. Anytime an organization contracts with a cloud provider, the cloud provider becomes a third-party source providing the service. This includes when the cloud provider holds data or provides any type of service.

The core risk is that an organization rarely knows exactly where their cloud data is stored. Users access it via the Internet, but the data centers holding the data and cloud-based apps can be anywhere.

Right to Audit Clauses

Cloud providers are expected to take precautions to protect any data they maintain in the cloud and ensure all the services they provide are secure. This isn't always apparent, so more and more customers are demanding a ***right to audit*** clause be included in a contract. This allows a customer to hire an auditor and review the cloud provider's records.

Auditing can help the customer ensure that the cloud provider is implementing adequate security. It can also help the customer verify that the cloud provider is implementing the advertised security controls.

Regulatory Jurisdiction

If all data and resources for ZiffCorp are contained and processed within a single building in Virginia Beach, Virginia, the ***regulatory jurisdiction*** is clear. The company must comply with relevant U.S. laws, Virginia laws, and Virginia Beach laws.

However, if ZiffCorp contracts with a cloud provider to store data, things change. Imagine that the cloud provider's headquarters are in San Jose, California, but it runs data centers across the United States and in Canada to hold the data. At this point, ZiffCorp is now responsible for complying with the laws in any location used by the cloud provider.

The European Union (EU) passed the General Data Protection Regulation (GDPR), which clarified requirements to protect the personal data of anyone living in the EU. If a cloud provider stores or processes data

in the EU, the provider must comply with the GDPR. Similarly, an organization that contracts with such a provider must also comply with the GDPR.

Data Breach Notification Laws

Data breach notification laws require organizations to notify customers about a data breach and take steps to mitigate the loss. When the data is stored in the cloud, this could require notification based on several different laws.

All states in the United States have data breach notification laws. In general, they require the notification of affected personnel if an organization believes that an unauthorized entity acquired any unencrypted personal information. However, the laws often allow an organization to delay the notification if a law enforcement agency determines that the notification would impede an investigation.

These laws typically include a time frame where the notification is required, such as within 45 days. Additionally, many laws require organizations to report the breach to the state Attorney General if the data breach affects a certain number of individuals, such as more than 1,000 people.

These laws typically define personal information as information that can be used to identify a person. This includes a name combined with a driver's license number, Social Security number, account number, medical data, and more.

The GDPR requires organizations to report any data breaches to the impacted individuals and appropriate regulatory authorities within 72 hours after discovering the breach. Additionally, organizations must complete a detailed forensic report, including a comprehensive containment plan, within 72 hours.

These laws typically include fines for noncompliance. As an example, the GDPR can impose a penalty of up to 10,000,000 Euro (almost 12 million dollars) or 2 percent of an organization's annual revenue.

Acquisition and Preservation

When performing data acquisition for digital forensics, it's important to follow specific procedures to ensure that the data is not modified. In many cases, this ensures that the evidence is preserved in case it is needed in a legal proceeding. The following sections provide more information on common procedures.

Order of Volatility

Order of volatility refers to the order in which you should collect evidence. Volatile doesn't mean it's explosive, but rather that it is not permanent. In general, you should collect evidence starting with the most volatile and moving to the least volatile.

For example, data in random access memory (RAM) is lost after powering down a computer. Because of this, it is important to realize you shouldn't power a computer down if you suspect it has been involved in a security incident and might hold valuable evidence. Chapter 6, "Comparing Threats, Vulnerabilities, and Common Attacks," discusses fileless viruses, which are often in RAM only. If you power a computer down, you may inadvertently delete all evidence of a fileless virus.

A processor can only work on data in RAM, so all the data in RAM indicates what the system was doing. This includes data that users have been working on, system processes, network processes, application remnants, and much more. All of this can be valuable evidence in an investigation, but if a rookie technician turns the computer off, the evidence is lost.

In contrast, data on a disk drive remains on the drive even after powering a system down. This includes any files and even low-level data such as the Master Boot Record on a drive.

The order of volatility from most volatile to least volatile is:

- **Cache.** This is data in the cache memory, including the processor cache and hard drive cache. Data in the cache is removed as new data is used.
- **RAM.** Data in RAM is used by the operating system (OS) and applications.

- **Swap or pagefile.** A swap file (sometimes called a pagefile) is on the system disk drive. It is an extension of RAM and is stored on the hard drive. However, the pagefile isn't a typical file, and the system rebuilds the pagefile when rebooting. This makes the pagefile more volatile than other files stored on hard drives.
- **Disk.** Data files are stored on local disk drives, and they remain there even after rebooting a system.
- **Attached** devices such as USB drives will also hold data when a system is powered down.
- **Network.** Networks typically have servers and shared folders accessible by users and used to store log files. These remote systems often have more robust backup policies in place, making them the least volatile.

Remember this

When collecting data for forensic analysis, you should collect it from the most volatile to the least volatile. The order of volatility is cache memory, regular RAM, swap file (or paging file), hard drive data, and data stored on network systems.

Data Acquisition

When performing data acquisition for evidence, it's important to follow specific procedures to ensure that the evidence is not modified. Following the order of volatility, you prevent destroying the data before you collect it. It's also important to know the location of additional forensic data.

Security experts sometimes use **snapshots** to capture data for forensic analysis. Various tools are available to capture snapshots of memory (including cache memory), disk contents, cloud-based storage, and more.

Forensic **artifacts** are pieces of data on a device that regular users are unaware of, but digital forensic experts can identify and extract. In general, logs and data files show direct content, but the artifacts are not so easy to see. Some examples are:

- **Web history.** This includes both pages visited and searches.
- **Recycle bin.** You can view the content of deleted files and the metadata of deleted files.

- **Windows error reporting.** These often give insight into what programs were running when a system crashed.
- **Remote desktop protocol (RDP) cache.** This can provide useful information if an attacker moves laterally through a network, or when an attacker is connecting to a system from an Internet server.

OS forensics refers to the process of collecting data from the OS. This includes things like the cache, RAM, swap file, and artifacts. It can also include much more depending on the operating system. As an example, the Windows Registry includes a wealth of information on installed applications and holds user data to enhance the user experience. Linux doesn't have a registry, but many Linux applications do store data in text-based configuration files.

Firmware forensic methods are useful when a forensic specialist suspects malware has infected firmware. It starts by extracting the firmware code. It then attempts to reverse engineer the code to discover what it is doing. In some cases, the firmware has a backdoor embedded in it that attackers can exploit. In other cases, the firmware has malicious code embedded within it.

Forensic Tools

Forensic specialists have a wide variety of tools available to acquire, preserve, and analyze evidence. These tools use special techniques to ensure the data is not changed while forensic specialists are collecting it.

Capturing Data

A forensic image of captured data will collect the data without modifying it all. This includes data within the cache, RAM, and entire disk drives. Some tools use bit-by-bit copy methods that can read the data without modifying it. Other methods include hardware devices connected to the system to write-protect it during the copy process.

These methods capture the entire contents of the disk, including system files, user files, and files marked for deletion but not overwritten. Similarly, many tools include the ability to capture data within volatile memory and save it as an image.

After capturing an image, experts create a copy and analyze the copy. They do not analyze the original disk and often don't even analyze the

original image. They understand that by analyzing the contents of a disk directly, they can modify the contents. By creating and analyzing forensic copies, they never modify the original evidence.

One of the oldest disk imaging tools used for forensics is the ***dd*** command (short for data duplicator) available in Linux systems, including Kali Linux. It can also be installed on Windows systems. To see how ***dd*** works, check out the labs for this chapter at <https://greatadministrator.com/sy0-601-labs/>.

Kali Linux includes the Volatility Framework, which is a collection of open-source tools used to capture and extract memory contents and digital artifacts. One of the tools is ***memdump*** (short for memory dumper), which can dump any addressable memory space to the terminal or redirect the output to a dump file.

WinHex is a Windows-based hexadecimal editor used for evidence gathering, data analysis, editing, recovery of data, and data removal. It can work with data on all drives, such as hard drives, CDs, and DVDs. It can also work directly with memory. It is a proprietary tool.

FTK imager is part of the Forensic Toolkit (FTK) sold by AccessData. It can capture an image of a disk as a single file or multiple files and save the image in various formats. It also gives you the option of creating images of individual folders or files. After capturing the image, it allows you to view and analyze data within the image.

Autopsy is a graphical user interface (GUI) digital forensics platform. It allows users to add command-line utilities from The Sleuth Kit (TSK). The Sleuth Kit includes both Windows- and Linux-based utilities used in forensics, and it can be used to analyze data on Windows, Linux, and some Apple operating systems.

Verifying Integrity

Hashes and checksums are important elements of forensic analysis to provide proof that collected data has retained integrity. Chapter 10, “Understanding Cryptography and PKI,” covers hashes and checksums. As a reminder, a hash is simply a number. You can execute a hashing algorithm against data as many times as you want, and if the data is the same, the hash will be the same. The focus in Chapter 10 is on using hashes with files and

messages. A captured forensic image (from RAM or a disk) is just a file, and you can use hashing with forensic images to ensure image integrity.

Provenance refers to tracing something back to its origin. In the context of digital forensics, hashing and checksums allow you to prove the analyzed copy of data is the same as the original data. This is required if the evidence needs to be admissible in a court of law.

Chapter 10 mentioned MD5 as a popular hashing algorithm. While its use as a cryptographic hash (such as hashing passwords) is not recommended, it is still used in forensics to create checksums.

The dd lab mentioned previously includes steps to create a copy of the image. After creating the copy, you also have a chance to use the **shasum** command to create and compare hashes.

For example, after capturing an image of a disk, an expert can create a hash or checksum of the image. The expert can then write-protect the image to prevent accidental modifications during the analysis. Later, the expert can take another hash of the image and compare it with the original hash. If both hashes are the same, it proves that the image is the same, and the analysis did not modify it.

Forensic analysts sometimes make a copy of the image to analyze, instead of analyzing the first image they capture. If they ever need to verify the integrity of the copy, they run the same hashing algorithm against it. Again, if the hash is the same, they know the analyzed data is the same as the captured data.

Similarly, some tools allow you to create a hash of an entire drive. These verify that the imaging process has not modified data. For example, you can create a hash of a drive before capturing the image and after capturing the image. If the hashes are the same, it verifies that the imaging process did not modify the drive.

Remember this

Forensic experts capture data using tools that don't modify it during the capture process. Some commonly used tools used to capture data on disks and within memory are the **dd** command (short for data duplicator), memdump (short for memory dumper), WinHex, and FTK imager. Autopsy provides a graphical tool to run many of the commands in The Sleuth Kit. Hashes and checksums prove the provenance of data.

Bandwidth Monitors

Chapter 8, “Using Risk Management Tools,” discusses several tools used to capture network traffic, and these can be used as bandwidth monitors forensic investigations. It’s common for administrators to keep these packet captures.

By comparing captures taken at different times, investigators can determine changes in network traffic. If an organization recently suffered a data breach, investigators may be able to identify when there was an increase in outgoing traffic. This may help them determine when the network was first attacked, and maybe even the first computer that was infected with malware.

Electronic Discovery

Electronic discovery, or *eDiscovery*, is the identification and collection of electronically stored information. This includes files of any kind, voice mail, social media entries, and website data.

When collecting this data, it’s vital to preserve the metadata related to all the files. Metadata is data about data instead of the data itself. It’s common to use digital forensic processes to collect the data. This ensures that the files and the associated metadata aren’t modified during the collection.

The following list identifies some metadata that can be useful during an investigation

- **File.** File metadata includes items such as when a file was created, who created it, when it was modified, and when it was last accessed.
- **Email.** Email metadata includes items such as the header, who sent it, who they sent it to, and when they sent it.
- **Web.** Web metadata includes items in the header (or head) of a web page, such as the title, the character set, and any other information developers add in the meta tag.
- **Mobile.** Mobile device metadata is often a treasure trove of evidence for investigators. It includes users’ location (tracked through apps), who they called, who called them, who they messaged, and who messaged them, website history, and more.

Data Recovery

Generically, ***data recovery*** refers to restoring lost data, such as restoring a corrupt file from a backup. In the context of forensics, data recovery goes further. Even without backups, it's often possible to recover data that a user has intentionally or accidentally deleted.

When a user deletes a file, the operating system typically just marks it for deletion and makes the space the file is consuming available to use for other files. However, the file is still there. Many file systems place the file in a recycle bin or trash can, and you can just retrieve it from there. Even if the user empties the trash after deleting a file, forensic experts can use tools to undelete the files.

Formatting a drive appears as though it has overwritten all the data on the drive. However, just as forensic experts have tools to undelete files, they also have tools to unformat drives. It's worth noting that criminals have access to these same tools, too, and can recover data from systems that haven't been sanitized.

Strategic Intelligence and Counterintelligence

Strategic intelligence and counterintelligence in the context of digital forensics aren't terms that you'll come across very often, but they are in the CompTIA Security+ objectives. By breaking down the terms, they become easier to understand.

Intelligence is the ability to learn by acquiring new knowledge and skills. Digital forensic intelligence refers to knowledge and information which has value to investigative personnel and has been gathered using digital forensic methods and techniques.

Generically, ***strategic intelligence*** refers to collecting, processing, and analyzing information to create long-term plans and goals. Digital forensics strategic intelligence is collecting, processing, and analyzing digital forensic data to create long-term cybersecurity goals.

Said another way, it's possible to observe the TTPs used by attackers and develop long-term goals to limit attacker's success. In the current threat environment, it's almost impossible to prevent attacks. However, using strategic intelligence to understand the threats, the threat actors, and the attack vectors, an organization has a better chance of increasing cybersecurity resilience. This will limit the damage of an attack and allow an organization to recover quicker.

Counterintelligence activities assume that attackers are also using strategic intelligence methods. It refers to any activities designed to prevent or thwart spying, intelligence gathering, or attacks. As an example, Chapter 4, "Securing Your Network," discusses honeypots, honeyfiles, and honeynets. These are passive examples of counterintelligence. They typically include fake information, and while the attackers are stealing from them, they aren't accessing any actual data.

Protecting Data

Every company has secrets. Keeping these secrets can often make the difference between success and failure. A company can have valuable research and development data, customer databases, proprietary information on products, and much more. If the company cannot keep private and proprietary data secret, it can directly affect its bottom line.

Data policies assist in the protection of data and help prevent data leakage. This section covers many of the different elements that a data policy may contain.

Classifying Data Types

As a best practice, organizations take the time to identify and classify data they use. Data classifications ensure that users understand the value of data, and the classifications help protect sensitive data. Classifications can apply to data in any form, such as printouts and data files.

As an example, the U.S. government uses classifications such as Top Secret, Secret, Confidential, and Unclassified to identify the sensitivity of ***government data***. Private companies often use terms such as Public, Private, Proprietary, and Sensitive.

The U.S. government identifies classified information using the following three levels:

- **Top secret.** If data in this category is disclosed to unauthorized entities, it could cause exceptionally grave damage to national security.
- **Secret.** If data in this category is disclosed to unauthorized entities, it could cause serious damage to national security.
- **Confidential.** If data in this category is disclosed to unauthorized entities, it could cause damage to national security.

Note that while the U.S. government has published standards for these classifications, there isn't a published standard that all private organizations use. Private organizations can use a wide variety of different terms. The classifications an organization uses are not as important as the fact that they use classifications. Organizations take time to analyze their data, classify it, and provide training to users to ensure the users recognize the value of the data. They also include these classifications within a data policy.

Any organization that has sensitive data needs to take steps to protect it. In this context, ***sensitive data*** is any data that isn't public and that the organization wants to protect against unauthorized access. It may be critical business information, financial data, trade secrets, customer data, or employee data. An organization may want to protect sensitive data to maintain its reputation for moral reasons, ethical reasons, or regulatory and legal reasons.

The following bullets show some identifiers that private companies may use:

- **Public data** is available to anyone. It might be in brochures, press releases, or on websites.
- **Private data** is information about an individual that should remain private. Two classic examples within IT security are Personally Identifiable Information (PII) and health information. Both are covered in more depth later in this chapter.
- **Confidential data** is information that an organization intends to keep secret among a certain group of people. For example, most companies consider salary data confidential. Personnel within the Accounting department and some executives have access to salary data, but they keep it secret. Many companies have specific policies telling people that they shouldn't even tell anyone else their salary amount.
- A proprietor is an owner, and **proprietary data** is owned by an individual, a group, or an organization. Proprietary data can include patents, trade secrets, software algorithms, designs, and more.
- **Financial information** is any data about monetary transactions related to an organization or an individual. Within an organization, financial information is contained within a balance sheet, an income statement, and a cash flow statement. Combined, they give a good picture of the organization's financial health.
- Employee data is all the information collected by an organization about employees. It includes information identifying the employees, such as names, addresses, and birth dates. It also includes payroll information and performance reports.
- **Customer data** is all the information collected and maintained about customers. It typically includes email addresses, usernames (if different from the email addresses), and passwords. It can also include credit card

data, phone numbers, mailing addresses, and much more depending on what the organization decides to collect and maintain.

Remember this

Public data is available to anyone. Sensitive data is any kind of data that needs to be protected against unauthorized access. Confidential data information is kept secret among a certain group of people. Proprietary data is data related to ownership, such as patents or trade secrets. Financial information provides a picture of an organization's financial health.

PII and Health Information

Personally Identifiable Information (PII) is personal information that can personally identify an individual. Health information is PII that includes health information.

Some examples of PII are:

- Full name
- Birthday and birthplace
- Medical and health information
- Street or email address information
- Personal characteristics, such as biometric data
- Any type of identification number, such as a Social Security number (SSN) or driver's license number

In general, you need two or more pieces of information to make it PII. For example, "John Smith" is not PII by itself because it can't be traced back to a specific person. However, when you connect the name with a birth date, a physical address, medical information, or other data, it is PII.

Many governments have enacted laws mandating the protection of both PII and health information. Also, there are many documents that provide guidance on how to protect it. The National Institute of Standards and Technology (NIST) created Special Publication (SP) 800-122 "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)." It identifies many specific safeguards that organizations can implement to protect PII along with steps to take in response to a data breach involving PII. You can access all the NIST publications at

<https://csrc.nist.gov/publications/sp>.

When attackers gain PII, they often use it for financial gain at the expense of the individual. For example, attackers steal identities, access credit cards, and empty bank accounts. Whenever possible, organizations should minimize the use, collection, and retention of PII. If it's not kept, it can't be compromised. On the other hand, if they collect PII and attackers compromise the data, the company is liable.

The Identity Theft Resource Center tracks data breaches and lists them on their site (<https://www.idtheftcenter.org/>). Their 2019 report indicated the number of known U.S. data breaches was 811, and they exposed more than

493 million records containing PII. This represented a 17 percent increase over the previous year. Some data breaches were small, affecting only a few hundred people. Others were large, exposing millions of user records.

Impact Assessment

An impact assessment helps an organization understand the value of data by considering the impact if it is lost or released to the public. Data can be lost due to corruption or technical failures, and data breaches can result in data being released to the public.

NIST SP 800-122 quotes McGeoge Bundy “If we guard our toothbrushes and diamonds with equal zeal, we will lose fewer toothbrushes and more diamonds. Similarly, all data doesn’t need the same protection. Instead data needs to be protected according to its classification and value.

Remember this

Personally Identifiable Information (PII) includes information such as a full name, birth date, biometric data, and identifying numbers such as an SSN. Personal health information is PII, which includes medical or health information. Organizations have an obligation to protect PII and typically identify procedures for handling and retaining PII in data policies.

Data Governance

Data governance refers to the processes an organization uses to manage, process, and protect data. The word *governance* implies the process of governing a state, but it doesn't have anything to do with managing a government, only data.

At a basic level, organizations attempt to ensure that data is stored consistently, even in different databases. This improves the data quality and allows an organization to integrate data from multiple databases and efficiently perform in-depth analysis. However, data governance encompasses much more than just data consistency. It also includes methods used to manage the availability, usability, integrity, and security of data used by an organization.

While data quality is a core goal of data governance, many organizations are motivated to implement data governance to comply with external laws and regulations. Some regulations that affect risk posture are listed here:

- **Health Insurance Portability and Accountability Act (HIPAA).** HIPAA mandates that organizations protect health information. This includes any information related to the health of an individual that might be held by doctors, hospitals, or any health facility. It also applies to any information held by an organization related to health plans offered to employees. Fines for not complying with the law have been as high as \$4.3 million.
- **Gramm-Leach Bliley Act (GLBA).** This is also known as the Financial Services Modernization Act and includes a Financial Privacy Rule. This rule requires financial institutions to provide consumers with a privacy notice explaining what information they collect and how it is used.
- **Sarbanes-Oxley Act (SOX).** SOX was passed after several accounting scandals by major corporations, such as Enron and WorldCom. Companies engaged in accounting fraud to make their financial condition look better than it was and prop up their stock price. For example, Enron's stock value was over \$90 in 2000, but executives knew of problems and began selling their stock. As the

scandal emerged, the stock crashed to \$42 a year later, and \$15 in 2001. In December 2002, the stock was worthless at six cents a share, effectively wiping out \$60 billion in investments. SOX requires that executives within an organization take individual responsibility for the accuracy of financial reports. It also includes specifics related to auditing and identifies penalties to individuals for noncompliance.

- **General Data Protection Regulation (GDPR).** This European Union (EU) directive mandates the protection of privacy data for individuals who live in the EU. It applies to any organization that collects and maintains this data, regardless of the location of the organization.

While this section outlined four specific laws related to data, there are others. The key is that organizations must know which laws apply to them and implement data governance methods to comply with the laws. This includes any national, territory, or state laws.

The GDPR and other laws mandate the use of *privacy notices* on websites. This public document explains what information is being collected, how it is being collected, what it is used for, why it is being collected, how the data will be used, and if it will be shared with third parties. People should also be able to correct any errors in their data.

Critical data is data that is critical to the success of a mission within an organization. This can be the primary mission of the entire organization or any specific function within the organization. Proper data governance practices ensure that critical data elements within an organization are identified. Once they are identified, additional data governance processes can be implemented to manage the availability, usability, integrity, and security of the critical data.

Remember this

Data governance refers to the processes an organization uses to manage, process, and protect data. Some data governance methods help ensure or improve the quality of data. Other methods are driven by regulations and laws. Proper data governance practices ensure that critical data elements are identified.

Privacy Enhancing Technologies

Several methods can be used to provide additional privacy protections for data. One of the easiest ways of protecting data is to implement ***data minimization***. Data minimization is a principle requiring organizations to limit the information they collect and use. If the organization doesn't hold the data, it isn't susceptible to loss due to a data breach. The following sections identify some other methods.

Data Masking

Data masking refers to modifying data to hide the original content. The primary reason for doing so is to protect sensitive information such as PII. The process retains usable data but converts it to inauthentic data.

This is sometimes done to provide realistic data that can be used for testing, but the data doesn't reveal anything if unauthorized users see it. As an example, consider a database containing customer data. A row in a customer table may include a customer number, first and last names, an address, and a phone number.

Substitution is one method used in data masking. Consider Figure 11.1, which shows a fictional row from a customer table, and the same row after data masking has been performed.

CustID	Fname	Lname	Address	City	State	Zip	Phone
8642975	Homer	Simpson	742 Evergreen	Springfield	OR	97475	541-555-4321
Masked Data Below							
1357924	Fred	Kramden	328 Chauncey	Brooklyn	NY	11214	347-555-8765

Figure 11.1: Data Masking

Simplistically, Cust ID is replaced with a different seven-digit number, Homer is replaced with Fred, Simpson is replaced with Kramden, and so on. Most of the masked data typically comes from substitution files, such as a file of first names, a file of last names, and so on. In practice, a data masking process may go through several passes of substitution, applying various rules to ensure the result is usable.

Anonymization

Data anonymization modifies data to protect the privacy of individuals by removing all PII within a data set. The goal is to remove any data that can be traced back to an individual while maintaining other data within the data set.

As an example, medical data may include information on patients from the time they reported to an emergency room to the time they were discharged. This could include information on their illness, how they were diagnosed, medications they were given that helped them, medical protocols followed, and more. If medical professionals have this data on tens of thousands of patients, it provides them with a lot of usable information that can be used with future patients to increase positive medical outcomes. However, due to privacy concerns, this data should not include PII.

By removing all PII, it allows the medical data to be shared but doesn't violate the privacy of the patients. The goal is for anonymization to be permanent. However, it's sometimes possible to use techniques to de-anonymize data. For example, a data set may refer to a middle-aged patient living in Springfield who loves donuts and Duff beer, is almost completely bald, weighs about 240 pounds, has a short attention span, and holds a job of safety inspector at a nuclear power plant. Homer Simpson's name may have been removed, but someone may be able to determine it is him.

Pseudo-Anonymization

Pseudo-anonymization replaces PII and other data with pseudonyms or artificial identifiers. For example, every instance of Homer in a data set could be replaced with a pseudonym of Z1. A separate data set matches the pseudonyms with the original data.

The pseudo-anonymized data sets appear anonymous. If unauthorized personnel gain access to the data, they won't be able to identify people in the data set. However, anyone with the separate data matching the pseudonyms with the original data set can reverse the process and re-create the original data.

Anonymization is used when the intent is to anonymize the data permanently. In contrast, pseudo-anonymization is used when an organization needs the data to be anonymized, but the organization also needs the ability to reverse the process and access the original data.

Tokenization

Data tokenization replaces sensitive data elements with a token. The token is a substitute value used in place of the sensitive data. A tokenization system can convert the token back into its original form.

Consider credit card information stored on a mobile phone and used for payments at point of sale (POS) terminals, such as terminals at fast-food stores. When users first configure a phone app, their phone passes credit card data to a tokenization system and requests a token. This tokenization system stores the token and the credit card data. When a user makes a charge, the phone app sends the token to the credit card processor. The credit card processor then sends the token to the tokenization system to retrieve the credit card data and processes the charge.

The important point here is that the credit card data is never used directly at POS terminals. Years ago, point of sale terminals often sent credit card data over wireless networks allowing attackers to intercept them.

Remember this

Data masking hides sensitive data by permanently replacing it with inauthentic data. Anonymization attempts to permanently remove all PII within a data set to protect the privacy of individuals. Pseudo-anonymization replaces data elements within a data set with pseudonyms or artificial identifiers. Tokenization replaces data elements with a token, or substitute value.

Data Retention Policies

A *data retention policy* identifies how long data is retained, and sometimes specifies where it is stored. This reduces the amount of resources, such as hard drive space or backup tapes, required to retain the data. Retention policies also help reduce legal liabilities. For example, imagine if a retention policy states that the company will only keep emails for one year. A court order requiring all emails from the company can only expect to receive email from the last year.

On the other hand, if the organization doesn't have a retention policy, it might need to provide emails from the past 10 years or longer in response to a court order. This can require an extensive amount of work by administrators to recover archives or search for specific emails. Additionally, investigations can uncover other embarrassing evidence from previous years. The retention policy helps avoid these problems.

Some laws mandate the retention of data for specific time frames, such as three years or longer. Proper data governance practices ensure that these time frames are known and followed.

Data Sanitization

Data sanitization methods ensure that data is removed or destroyed from any devices before disposing of the devices. A computing device's life cycle starts when it's put into service and ends when it is disposed of. Information also has a life cycle. It begins when the data is created and should end when the data is no longer needed. However, if computing devices aren't sanitized when they reach the end of their life cycle, unauthorized entities may gain access to the data.

Organizations may donate the hardware devices, recycle them, or sometimes just throw them away. Data sanitization procedures ensure that the devices don't include any data that might be useful to people outside your organization or damaging to your organization if unauthorized people receive it.

It's common for organizations to have a checklist to ensure that personnel sanitizes a system before disposing of it. The goal is to ensure that personnel remove all usable data from the system.

Hard drives represent the greatest risk because they hold the most information, so it's essential to take additional steps when decommissioning old hard drives. Simply deleting a file on a drive doesn't delete it. Instead, it marks the file for deletion and makes the space available for use. Similarly, formatting a disk drive doesn't erase the data. There are many recovery applications available to recover deleted data, file remnants, and data from formatted drives.

Data destruction isn't limited to only hard drives. Organizations often have a policy related to paper containing any type of sensitive data. Shredding or incinerating these papers prevents them from falling into the wrong hands. If personnel just throw this paper away, dumpster divers can sift through the trash and gain valuable information. An organization also takes steps to destroy other types of data, such as backup tapes, and other types of devices, such as removable media.

Some common methods used to destroy data and sanitize media are:

- **File shredding.** Some applications remove all remnants of a file using a shredding technique. They do so by repeatedly overwriting the space where the file is located with 1s and 0s.

- **Wiping.** Wiping refers to the process of completely removing all remnants of data on a disk. A disk wiping tool might use a bit-level overwrite process that writes different patterns of 1s and 0s multiple times and ensures that the data on the disk is unreadable.
- **Erasing and overwriting.** Solid-state drives (SSDs) require a special process for sanitization. Because they use flash memory instead of magnetic storage platters, traditional drive wiping tools are not effective. Some organizations require personnel to destroy SSDs as the only acceptable method of sanitization physically.
- Paper shredding. You can physically shred papers by passing them through a shredder. When doing so, it's best to use a cross-cut shredder that cuts the paper into fine particles. Large physical shredders can even destroy other hardware, such as disk drive platters removed from a disk drive.
- Burning. Many organizations burn materials in an incinerator. Obviously, this can be done with printed materials, but isn't as effective with all materials.
- Pulping. *Pulping* is an additional step taken after shredding paper. It reduces the shredded paper to mash or puree.
- Pulverizing. *Pulverizing* is the process of physically destroying media to sanitize it, such as with a sledge hammer (and safety goggles). Optical media is often pulverized because it is immune to degaussing methods and many shredders can't handle the size of optical media. It's also possible to remove disk platters from disk drives and physically destroy them.
- Degaussing. A degausser is a very powerful electronic magnet. Passing a disk through a *degaussing* field renders the data on tape and magnetic disk drives unreadable.
- Third-party solutions. Many companies provide data destruction services. As an example, you can drop off documents at almost any United Parcel Service (UPS) store and they will shred them for you. Many other companies, such as Shred-it can destroy everything from paper documents to hard drives.

It's also worth mentioning that hard drives and other media can be in devices besides just computers. For example, many copy machines include disk drives, and they can store files of anything that employees recently

copied or printed. If personnel don't sanitize the drives before disposing of these devices, it can also result in a loss of confidentiality.

Training Users

User training is an essential part of organizational security. This includes training personnel on security policies and training to help ensure personnel remain up to date with current technologies and threats.

When users understand risks related to their actions, they're less likely to take risky actions. As a simple example, attackers are constantly sending out phishing emails with malicious links. If users engage in risky behaviors, such as clicking these links, they can give attackers a path into an organization's network. However, providing regular training to users on common threats and emerging threats helps them avoid these attacks.

People learn differently. Knowing this, it's important to use a diversity of training techniques to ensure all employees within an organization understand cybersecurity threats. The following sections describe some commonly used training methods.

Computer-Based Training

Computer-based training (CBT) refers to any training where an individual interacts with an application on a computer. It can be courseware installed on a single computer or web-based training available over the Internet or an intranet.

One benefit of CBT is that students can learn at their own pace. One person may enjoy a topic and absorb it quickly, while another person may need to take more time with it. Some CBT courseware includes videos, allowing students to pause and rewind the video, and watch videos repeatedly if desired. Similarly, students can typically review any text pages as often as they desire.

CBT courseware often includes quizzes or tests so that students can gauge their understanding of the material. When an organization purchases CBT courseware, they often require students to pass these quizzes or tests to show that they went through the courseware and understand the topic.

Industrial Control Systems Computer Emergency Response Team (ICS-CERT) provides a lot of free training via their site. Their focus is on preventing attacks on industrial control systems (ICSs). However, attacks on many organizations start the same way. As an example, spear-phishing attacks are a risk for any organization, whether it has an ICS or not. You can access the training here: <https://ics-training.inl.gov/learn/>.

Phishing Campaigns

Attackers are constantly launching phishing campaigns trying to trick users into clicking a malicious link or opening malicious attachments. They are continually trying new things and improving their tactics. When cybersecurity personnel learn of new phishing campaigns, they often inform users of these new campaigns and methods.

Phishing Simulations

If a single employee within an organization clicks on a malicious link within an email or responds with private information, it may be enough for an attacker to take over an entire network. Some organizations want to know if any of their employees will be tricked by phishing emails. A phishing simulation sends out fake phishing emails to employees to see if anyone will click a link or respond to it.

Organizations often hire an outside security company to help with phishing simulations. Some security companies provide access to an online app that an organization's representative can use. The representative can choose who to send the phishing emails to (such as everyone or specific groups), how often to send the emails (such as one time or monthly), when to start the simulation, and more. These online apps often have multiple templates that the representatives can choose from, such as emails with attachments, emails with URLs, and emails asking them to respond with information.

This culminates with a report documenting any inappropriate responses. It gives management insight into the effectiveness, or ineffectiveness, of current training.

Gamification

Gamification intertwines game-design elements within user training methods to increase participation and interaction. It is often used in courseware and online training, but it can be used differently depending on the goals.

As an example, imagine a company has tried to educate employees about phishing emails using several different techniques. Unfortunately, for some reason, employees aren't getting the message, and the company just experienced another security incident after an employee responded to a phishing email.

The chief information officer (CIO) could launch occasional unannounced phishing simulations and give some sort of prize to the department with the fewest responses. When one department wins, and other departments lose because someone in the department responded, the "game" is likely to generate more interest and interaction than other training.

Within formal training, the intent is to help make the courseware fun, motivating students to engage with the course. As a simple example, an end-of-topic quiz could include a mini-crossword puzzle instead of multiple-choice or fill-in-the-blank questions. Students would answer questions to fill in the puzzle.

Some gamification techniques include a sense of competition. For example, after students complete a quiz, their names can be added to a leaderboard to show how they performed against their peers. However, this isn't always appreciated. If students score too low and they see their name at the bottom of a leaderboard, they may view it as social pressure making leaderboards a demotivator for some people.

Badges are sometimes used to provide a visual representation of achievement. Students can earn them after completing an entire course or earn individual badges after completing topics within a course. As an example, a student may be able to earn 10 badges within a course. Knowing these 10 badges are available to earn, students may be more motivated to get each one.

Remember this

User training helps keep personnel up to date on security policies and current threats. Computer-based training is on computers or online and allows students to learn at their own pace. Phishing simulations mimic the type of phishing campaigns used by attackers and allow an organization to safely check to see if employees will respond to phishing emails. Gamification adds game-design elements into training to increase user participation and interaction.

Capture the Flag

A capture the flag (CTF) event is an example of gamification used by cybersecurity personnel. The rules may vary depending on who is hosting the event, but there are some common characteristics.

The CTF event includes several challenges that players can solve. When players solve a challenge, they receive a digital flag that they present as proof that they solved the challenge. They then get another challenge that they try to solve. Each solved challenge earns points for the players, with more demanding challenges worth more points. CTF events often include a large scoreboard that everyone can see, adding an element of competition. Players can be individuals or teams depending on the rules of the CTF event organizers.

Many cybersecurity conferences include CTF events. Additionally, the challenges are often based on real-world vulnerabilities and attacks. This allows the players to see exactly how attackers exploit these vulnerabilities and gain insights into how to protect systems from these attacks.

Role-Based Awareness Training

Role-based awareness training is targeted to personnel based on their roles. The primary goal is to minimize the risk to the organization. By giving employees targeted training based on their needs within their jobs, they are better prepared to avoid threats.

In general, all employees need general training on how to avoid threats. Phishing is one of the most pervasive threats to organizations, so training personnel on how to avoid getting fooled by phishing emails is a minimum baseline. Help-desk personnel need to know about the basics related to forensics, such as the order of volatility, and who to contact when a security incident has been verified.

Chapter 8 discusses penetration testing and the roles of red, blue, white, and purple teams. Employees on any of these teams need specialized training related to their roles in penetration testing. Similarly, personnel on incident response teams and forensic analysis teams need specialized training to fulfill their responsibilities.

Personnel in specific data roles often need training on their roles and responsibilities. Some of these roles are GDPR-related. As a reminder, the GDPR applies to any organization that collects or processes data on any EU residents.

- **Data owner.** Data owners need to understand their responsibilities related to data that they own. This includes ensuring that the data is classified correctly and ensuring that the data is labeled to match the classification. They are also responsible for ensuring adequate security controls are implemented to protect the data. While they often delegate day-to-day tasks to data custodians, they cannot delegate their responsibility.
- **Data controller.** The data controller is the entity that determines why and how personal data should be processed. As an example, a business may outsource payroll. They control all employee data and decide what data to release to the payroll company. In many cases, the data owner and the data controller are the same.
- **Data processor.** A data processor is any entity that uses and manipulates the data on behalf of the data controller. A payroll

company would accept the personal data from the data controller and use it to process payroll functions.

- **Data custodian/steward.** A data custodian (also called a data steward) is responsible for routine daily tasks such as backing up data, storage of the data, and implementation of business rules. As an example, a database administrator (DBA) would be the data custodian for all data contained within databases the DBA oversees.
- **Data protection officer.** The data protection officer (DPO) is a role identified in the GDPR. This person is responsible for ensuring the organization is complying with all relevant laws. This person in this role also needs to act as an independent advocate for customer data.

Remember this

Role-based training ensures that employees receive appropriate training based on their roles in the organization. Data owners are responsible for ensuring adequate security controls are in place to protect the data. The data controller determines why and how personal data should be processed. The data processor uses and manipulates the data on behalf of the data controller. A data custodian/steward is responsible for routine daily tasks such as backing up data. The data protection officer acts as an independent advocate for customer data.

Chapter 11 Exam Topic Review

When preparing for the exam, make sure you understand these key concepts covered in this chapter.

Exploring Security Policies

- Written security policies are administrative controls that identify an overall security plan for an organization and reduce overall risk. Plans and procedures identify security controls used to enforce security policies.
- An acceptable use policy defines proper system usage for users and spells out rules of behavior when accessing systems and networks. It often provides specific examples of unacceptable usage, such as visiting certain websites, and typically includes statements informing users that the organization monitors user activities. Users are required to read and sign an acceptable use policy when hired and in conjunction with refresher training.
- Mandatory vacation policies require employees to take time away from their job. These policies help to reduce fraud and discover malicious activities by employees.
- A separation of duties policy separates individual tasks of an overall function between different entities or different people and helps deter fraud. For example, a single person shouldn't be able to approve bills and pay them or print checks and then sign them.
- The principle of least privilege specifies that individuals or processes are granted only the rights and permissions needed to perform assigned tasks or functions, but no more.
- Job rotation policies require employees to change roles regularly. Employees might swap roles temporarily, such as for three to four weeks, or permanently. These policies help to prevent employees from continuing with fraudulent activities and help detect fraud if it occurs.
- Clean desk space policies require users to organize their desks and surrounding areas to reduce the risk of possible data theft and password compromise.

- Background checks are performed before hiring an employee. Once hired, onboarding processes give employees access to resources. An exit interview is conducted before an employee departs the organization, and the account is typically disabled during the interview.
- A non-disclosure agreement helps ensure that proprietary data is not shared.
- Social media analysis practices monitor employee activity on social media networks.
- A service level agreement (SLA) is an agreement between a company and a vendor that stipulates performance expectations, such as minimum uptime and maximum downtime levels.
- Memorandum of understandings (MOUs) expresses an understanding between two or more parties, indicating their intention to work together toward a common goal.
- End of life (EOL) generally refers to the date when a vendor stops offering a product for sale.
- End of service life (EOSL) indicates the date when a vendor will stop supporting a product with patches or upgrades.
- A measurement systems analysis (MSA) evaluates the processes and tools used to make measurements.

Incident Response Policies

- An incident response policy defines an incident and response procedures. Organizations review and update incidents periodically and after reviewing lessons learned after actual incidents.
- A communication plan identifies who to inform when an incident occurs. It also outlines the roles and responsibilities of various personnel, including a communication expert that would communicate with the media.
- The first step in incident response is preparation. It includes creating and maintaining an incident response policy and includes prevention steps such as implementing security controls to prevent malware infections.
- Before acting, personnel verify an event is an actual incident. Next, they attempt to contain or isolate the problem. Disconnecting a

computer from a network will isolate it.

- Eradication attempts to remove all malicious components left after an incident. Recovery restores a system to its original state. Depending on the scope of the incident, administrators might completely rebuild the system, including applying all updates and patches.
- A review of lessons learned helps an organization prevent a reoccurrence of an incident.
- Secure Orchestration, Automation, and Response (SOAR) platforms use internal tools to respond to low-level security events automatically, reducing administrator workload.
- A SOAR playbook provides a checklist of things to check for suspected incidents.
- A SOAR runbook implements the playbook checklist using available tools within the organization.

Understanding Digital Forensics

- When collecting documentation and evidence, it's important to follow specific procedures to ensure that the evidence is admissible in a court of law.
- A chain of custody provides assurances that personnel controlled and handled evidence properly after collecting it. It may start with a tag attached to the physical item, followed by a chain of custody form that documents everyone who handled it and when they handled it.
- A legal hold requires an organization to protect existing data as evidence.
- Video surveillance systems (when available) should be used in forensic investigations. If personnel witnessed an incident, they should be interviewed.
- Event logs often help investigators reconstruct the timeline of an event by looking at the timestamps of entries. However, investigators need to consider any time offsets based on the time zone used by the logs.
- Investigators provide a report on their findings. They typically include tactics, techniques, and procedures (TTPs) used by attackers

and recommendations based on the results.

- When using a cloud provider, organizations should ensure that the contract includes a right to audit clause. Organizations should also know where their data is being housed so that the regulatory jurisdiction is known. If a data breach occurs, organizations need to comply with data breach notification laws based on the location of the data.
- The order of volatility for data from most volatile to least volatile on a system is cache memory, regular RAM, a swap or paging file, and hard drive data.
- Snapshots can capture data from almost any location, and the snapshot can be used for forensic analysis.
- Forensic artifacts are pieces of data that most users are unaware of, but digital forensic experts can extract and analyze the artifacts.
- Firmware forensics extract code from firmware and reverse engineer it.
- Forensic experts capture an image of the data before analysis to preserve the original and maintain its usability as evidence.
- Hard drive imaging creates a forensic copy and prevents the forensic capture and analysis from modifying the original evidence. A forensic image is a bit-by-bit copy of the data and does not modify the data during the capture.
- Some tools used to capture data include dd, memdump, WinHex, and FTK imager. Autopsy is a graphical user interface that simplifies running command-line utilities from The Sleuth Kit.
- Hashes or checksums are used to verify the integrity of captured data. They provide proof the capturing process did not modify data.
- Electronic discovery (eDiscovery) is the identification and collection of electronically stored information. This includes files of any kind.
- Forensic methods support the recovery of data after it has been deleted or a drive has been formatted.

Protecting Data

- Information classification practices help protect sensitive data by ensuring users understand the value of data. Sensitive data is any

data that isn't public. An organization protects sensitive data.

- Public data is available to anyone. Confidential data is information that an organization intends to keep secret among a certain group of people. Proprietary data is data that is related to ownership, such as patents or trade secrets. Private data includes PII and health information.
- Personally Identifiable Information (PII) is used to identify an individual. Examples include a full name combined with a birth date, address, or medical information. Health information is PII that includes medical or health-related information.
- Data governance refers to the processes an organization implements to manage, process, and protect data. Many laws require organizations to implement specific data governance methods.
- PII requires special handling for data retention. Many laws mandate the protection of PII and require informing individuals when an attack results in the compromise of PII.
- Data masking hides sensitive data such as PII by permanently converting it into usable but inauthentic data. Anonymization attempts to permanently remove all PII within a data set to protect the privacy of individuals.
- Pseudo-anonymization replaces data elements within a data set with pseudonyms or artificial identifiers. The pseudonyms and original data elements are retained in a separate data set. This second data set can be used to re-create the original data set.
- Tokenization replaces data elements with a token, or substitute value. A tokenization system retains both the token and the original value. Tokenization is commonly used with credit cards.
- Retention policies identify how long data is retained. They can limit a company's exposure to legal proceedings and reduce the amount of labor required to respond to court orders.
- Data sanitization and destruction methods ensure that sensitive data is removed from decommissioned systems. File shredders remove all remnants of a file. Wiping methods erase disk drives. Degaussing a disk magnetically erases all the data. Physically destroying a drive is the most secure method of ensuring unauthorized personnel cannot access proprietary information.

Training Users

- User training includes training personnel on security policies and reducing risks by training users on current technologies and threats.
- Computer-based training (CBT) allows students to learn at their own pace.
- Phishing simulations mimic the type of phishing campaigns used by attackers and allow an organization to safely check to see if employees will respond to phishing emails.
- Gamification adds game-design elements into training to increase user participation and interaction.
- Role-based training ensures that personnel receive the training they need based on their roles within the organization.
- Organizations doing business in the European Union (EU) must follow data privacy standards described in the General Data Protection Regulation (GDPR). The GDPR describes responsibilities for several specific roles.
- Data owners are responsible for ensuring adequate security controls are in place to protect the data.
- The data controller determines why and how personal data should be processed.
- The data processor uses and manipulates the data on behalf of the data controller.
- A data custodian/steward is responsible for routine daily tasks such as backing up data.
- The data protection officer acts as an independent advocate for customer data.

Online References

- Do you know how to answer performance-based questions? Check out the online extras at <https://greatadministrator.com/sy0-601-extras/>.

Chapter 11 Practice Questions

1. Management within your organization wants to ensure that users understand the rules of behavior when they access the organization's computer systems and networks. Which of the following BEST describes what they would implement to meet this requirement?
 - A. AUP
 - B. NDA
 - C. SLA
 - D. MSA

2. Management recently decided to upgrade the organization's security policy. Among other items, they want to implement a policy that will reduce the risk of personnel within the organization colluding to embezzle company funds. Which of the following is the BEST choice to meet this need?
 - A. AUP
 - B. Training
 - C. Mandatory vacations
 - D. Background check

3. Lisa is a training instructor, and she maintains a training lab with 16 computers. She has enough rights and permissions on these machines to configure them as needed for classes. However, she does not have the rights to add them to the organization's domain. Which of the following choices BEST describes the reasoning for this?
 - A. Least privilege
 - B. MSA
 - C. Diversity of training
 - D. Offboarding

4. Your organization includes a software development division within the IT department. One developer writes and maintains applications for the Sales and Marketing departments. A second developer writes and maintains

applications for the Payroll department. Once a year, they switch roles for at least a month. What is the purpose of this practice?

- A. To enforce a separation of duties policy
 - B. To enforce a mandatory vacation policy
 - C. To enforce a job rotation policy
 - D. To enforce an acceptable use policy
5. Your organization recently suffered a costly malware attack. Management wants to take steps to prevent damage from malware in the future. Which of the following phases of common incident response procedures is the BEST phase to address this?
- A. Preparation
 - B. Identification
 - C. Containment
 - D. Eradication
6. An incident response team is following typical incident response procedures. Which of the following phases is the BEST choice for analyzing an incident to identify steps to prevent a reoccurrence of the incident?
- A. Preparation
 - B. Identification
 - C. Eradication
 - D. Lessons learned
7. After a recent cybersecurity incident resulting in a significant loss, your organization decided to create a security policy for incident response. Which of the following choices is the BEST choice to include in the policy when an incident requires confiscation of a physical asset?
- A. Ensure hashes are taken first.
 - B. Maintain the order of volatility.
 - C. Keep a record of everyone who took possession of the physical asset.
 - D. Require interviews of all witnesses present when the asset is confiscated.

8. A forensic analyst was told of a suspected attack on a Virginia-based web server from IP address 72.52.230.233 at 01:23:45 GMT. However, after investigating the logs, he doesn't see any traffic from that IP at that time. Which of the following is the MOST likely reason why the analyst was unable to identify the traffic?

- A. He did not account for the time offset.
- B. He did not capture an image.
- C. The IP address has expired.
- D. The logs were erased when the system was rebooted.

9. Homer called the help desk complaining his computer is giving random errors. Cybersecurity professionals suspect his system is infected with malware and decide to use digital forensic methods to acquire data on his system. Which of the following should be collected before turning the system off? (Choose TWO.)

- A. Image of disk
- B. RAM
- C. OS
- D. ROM
- E. Cache

10. After a recent incident, a forensic analyst was given several hard drives to analyze. Which of the following actions should she take FIRST?

- A. Capture drive images for integrity.
- B. Take hashes for provenance.
- C. Review the logs on the disks.
- D. Create a chain of custody document.

11. A health care organization manages several hospitals and medical facilities within a state, and they have treated thousands of patients who have suffered from a recent viral outbreak. Doctors from another state are performing studies of this virus and would like to access the information that the health care organization has amassed. Management has authorized the release of this information but has mandated that the data cannot reveal any personal information about patients. Which of the following methods will BEST meet these requirements?

- A. Pseudo-anonymization
- B. Tokenization
- C. Encryption
- D. Masking

12. An urban hospital has recently treated hundreds of patients after a viral outbreak. Researchers trying to learn more about the virus have asked the hospital for information on treatment methods they used and their outcomes. The hospital management has asked the IT department to remove all personal information about patients before releasing this data. Which of the following methods will BEST meet these requirements?

- A. Anonymization
- B. Pseudo-anonymization
- C. Tokenization
- D. Data minimization

13. Investigations have shown that several recent security incidents originated after employees responded inappropriately to malicious emails. The IT department has sent out multiple emails describing what to do with these emails, but employees continue to respond inappropriately. The chief information officer has directed the Human Resources department to find and implement a solution that will increase user awareness and reduce these incidents. Which of the following would be the BEST solution?

- A. Offboarding
- B. Least privilege
- C. Gamification
- D. Role-based training

14. Your organization is updating the data policy, and management wants to ensure that employees get training on their responsibilities based on their role. Which of the following BEST describes the responsibilities of data owners and indicates what training they need?

- A. Ensuring data is backed up in accordance with the data policy
- B. Ensuring data is classified and labeled correctly
- C. Complying with laws related to privacy

D. Understanding common threats, such as malware and phishing attacks

15. Organizations that conduct business in the EU must have a position within the organization that can act as an independent advocate for the proper care and use of customer information. Which of the following BEST identifies this position?

- A. Data owner
- B. Data custodian
- C. Data processor
- D. Data protection officer

Chapter 11 Practice Question Answers

1. **A** is correct. An acceptable use policy (AUP) informs users of company expectations when they use computer systems and networks, and it defines acceptable rules of behavior. A non-disclosure agreement (NDA) ensures that individuals do not share proprietary data with others. A service level agreement (SLA) is an agreement between a company and a vendor that stipulates performance expectations, such as minimum uptime and maximum downtime levels. A measurement systems analysis (MSA) evaluates the processes and tools used to make measurements.
2. **C** is correct. Mandatory vacations help to reduce the possibility of fraud and embezzlement. An acceptable use policy informs users of company policies, and even though users sign them, they don't deter someone considering theft by embezzling funds. Training can help reduce incidents by ensuring personnel are aware of appropriate policies. A background check is useful before hiring employees, but it doesn't directly reduce risks related to employees colluding to embezzle funds.
3. **A** is correct. When following the principle of least privilege, individuals have only enough rights and permissions to perform their job. Lisa needs to maintain the training lab, but there is no indication she needs to join the training lab computers to the domain. A measurement systems analysis (MSA) uses various methods to identify variations within a measurement process and is completely unrelated to this question. Diversity of training techniques refers to using different training techniques for end users. Offboarding is the process of removing employees' access when they leave the company but has nothing to do with the privileges of a training instructor.
4. **C** is correct. This practice enforces a job rotation policy where employees rotate into different jobs, and it is designed to reduce potential incidents. A separation of duties policy prevents any single person from performing multiple job functions to help prevent fraud, but it doesn't force users to switch roles. A mandatory vacation policy requires employees to

take time away from their job. An acceptable use policy informs users of their responsibilities when using an organization's equipment.

5. **A** is correct. The preparation phase is the first phase of common incident response procedures and attempts to prevent security incidents. Incident identification occurs after a potential incident occurs and verifies it is an incident. Containment attempts to limit the damage by preventing an incident from spreading, but it doesn't prevent the original incident. Eradication attempts to remove all malicious elements of an incident after it has been contained. All six steps in order are preparation, identification, containment, eradication, recovery, and lessons learned.

6. **D** is correct. You should analyze an incident during the lessons learned phase of incident response to identify steps to prevent reoccurrence. Preparation is a planning step done before an incident, to prevent incidents and identify methods to respond to incidents. Identification is the first step after hearing about a potential incident to verify it is an incident. Eradication attempts to remove all malicious elements of an incident after containing it.

7. **C** is correct. It's important to keep a chain of custody for any confiscated physical items, and the chain of custody is a record of everyone who took possession of the asset after it was first confiscated. Hashes should be taken before capturing an image of a disk, but hashes are not required before confiscating equipment. Security personnel should be aware of the order of volatility and protect volatile data, but there isn't any way to maintain the order of volatility. It's important to perform interviews of anyone who observed the incident, but it isn't necessary to interview people who were present when the asset is confiscated.

8. **A** is correct. The most likely reason is that he did not account for the time offset. The attack occurred at 01:23:45 Greenwich Mean Time (GMT), which is the same time in London (except when daylight savings time starts). The web server is in the Eastern Standard Time (EST) zone in Virginia, which is five hours different from GMT. There is no need to capture an image to view logs. IP addresses on the Internet do not expire.

Logs are written to a hard drive or a central location; they are not erased when a system is rebooted.

9. **B** and **E** are correct. Random access memory (RAM) and cache are the most volatile of the items listed and should be collected before the system is turned off. You can collect an image of the disk and the operating system (OS) after it is powered off. Read only memory (ROM) will be retained even when the power is removed. While the swap/pagefile is not listed, it should also be collected. If the system is turned back on after it is turned off, the swap/pagefile will be overwritten.

10. **B** is correct. Forensic analysts take hashes to prove provenance of the copy. The hash (or checksum) provides proof that the copy is the same as the original and has not lost integrity. A drive image shouldn't be captured before creating a hash, and just having a drive image doesn't provide integrity or prove that it is the same as the original. Reviewing any data on an original disk will potentially modify the data so it shouldn't be done. A chain of custody document is created when evidence is collected, so it should already exist.

11. **D** is correct. Data masking will modify the original data and can be used to hide Personally Identifiable Information (PII). In this scenario, data masking could modify names, addresses, and phone numbers, while retaining medical data such as treatments and outcomes. Although not available as a choice, anonymization of the data could also meet the requirements. Pseudo-anonymization replaces some data with pseudonyms, or artificial identifiers, but the process can be reversed to identify the original data, so it isn't the best choice. Tokenization replaces data elements with a token, and the token is then used in place of the original data element. Tokenization doesn't protect identities. Encryption would convert cleartext into ciphertext making everything unusable by the outside researchers.

12. **A** is correct. Anonymization of the data would modify it to hide Personally Identifiable Information (PII) and is the best choice of the available options. Although not available as a choice, data masking could

also meet the requirements. Pseudo-anonymization replaces some data with pseudonyms, or artificial identifiers, but the process can be reversed to identify the original data, so it isn't the best choice. Tokenization doesn't protect identities but instead replaces data elements with a token, and the token can then be used in place of the original data element. Data minimization refers to data collection and requires organizations to limit the data they collect and use.

13. **C** is correct. Gamification uses various techniques to increase employee interaction, participation, and understanding of topics. This scenario indicates employees are responding to phishing emails and the IT department has been unsuccessful in getting them to respond to phishing emails appropriately. Offboarding is the process of removing an employee's access when they leave the company but firing employees isn't the best choice here. A principle of least privilege ensures employees have only enough rights and permissions to perform their job and can temporarily limit an attacker's access after a successful phishing attack, but it won't prevent an employee's actions. Role-based training gives users specific training based on their role, but this scenario doesn't indicate the problem is limited to any role.

14. **B** is correct. Owners are responsible for identifying the proper classification of data, ensuring it is labeled correctly, and ensuring security controls are implemented to protect the data. A data custodian (also called a data steward) is responsible for routine daily tasks such as backing up data. A data protection officer (DPO) is responsible for ensuring the organization is complying with relevant laws. End users need to be trained on common threats, such as malware and phishing attacks.

15. **D** is correct. The data protection officer (DPO) is a role identified in the General Data Protection Regulation (GDPR), and the GDPR specifies the person in this role needs to act as an independent advocate for customer information. Data owners are responsible for identifying the proper classification of data, ensuring it is labeled correctly, and ensuring security controls are implemented to protect the data. A data custodian (also called a

data steward) is responsible for routine daily tasks such as backing up data. A data processor is any entity that uses and manipulates the data.

Post-Assessment Questions

1. Your organization hosts an e-commerce web server. The server randomly experiences a high volume of sales and usage from mid-November to the end of December, causing spikes in resource usage. These spikes have resulted in outages during the past year. Which of the following should be implemented to prevent these outages?
 - A. Stored procedures
 - B. Scalability
 - C. Version control
 - D. Memory management

2. Employees currently log in with their username and a password but management wants to increase login security by implementing smart cards. However, the IT department anticipates it will take a long time to purchase the necessary equipment and issue smart cards for everyone. You need to identify a solution that will provide comparable security until the smart cards are implemented. Which of the following is a compensating control that will meet these needs?
 - A. Implement an account lockout policy.
 - B. Increase password policy requirements.
 - C. Implement a TOTP solution.
 - D. Require users to change their password more often.

3. You have configured a firewall in your network to block ICMP traffic. You want to verify that it is working as expected. Which of the following commands would you use?
 - A. arp
 - B. ipconfig
 - C. route
 - D. ping

4. You need to reboot a database server. Before doing so, you need to verify it doesn't have any active network connections. Which of the following commands will BEST meet your needs?

- A. arp
- B. ipconfig
- C. hping3
- D. netstat

5. You are troubleshooting an issue with the ycda application hosted on a Linux system. You suspect that the issue is caused when performing a specific function. You execute the function and see a generic error message. You now want to view the detailed error logged in the messages file. Which of the following commands would be the BEST choice to use?

- A. head
- B. tail
- C. chmod
- D. logger

6. Lisa is installing an application named *gcga.exe* on a Linux server. The documentation indicates that the application should be installed with the following permissions:

- The owner of the application should have read, write, and execute permissions.
- The owner group of the application should have read and execute permissions.
- All other users should not have any permissions for the application.

Which of the following commands should be used to meet these requirements?

- A. chmod 067 gcga.exe
- B. chmod 661 gcga.exe
- C. chmod 750 gcga.exe
- D. chmod 770 gcga.exe

7. Homer is not able to access any network resources from his Linux-based computer. Which of the following commands would he use to view the network configuration of his system?

- A. ifconfig

- B. ipconfig
- C. netstat
- D. tracert

8. Management wants to increase security for any users accessing the network with a VPN. They plan to implement a method that will require users to install an application on their smartphones. This application will generate a key that they'll have to enter in addition to their username and password. What is the BEST description of this added authentication method?

- A. Something you know
- B. Something you have
- C. Something you are
- D. Something you can do

9. Users normally log on using a smart card, a username, and a password. Management wants administrators to use a third factor of authentication. Which of the following will meet this need?

- A. PIN
- B. Token
- C. Fingerprints
- D. Push notification

10. Developers are planning to develop an application using role-based access control. Which of the following would they MOST likely include in their planning?

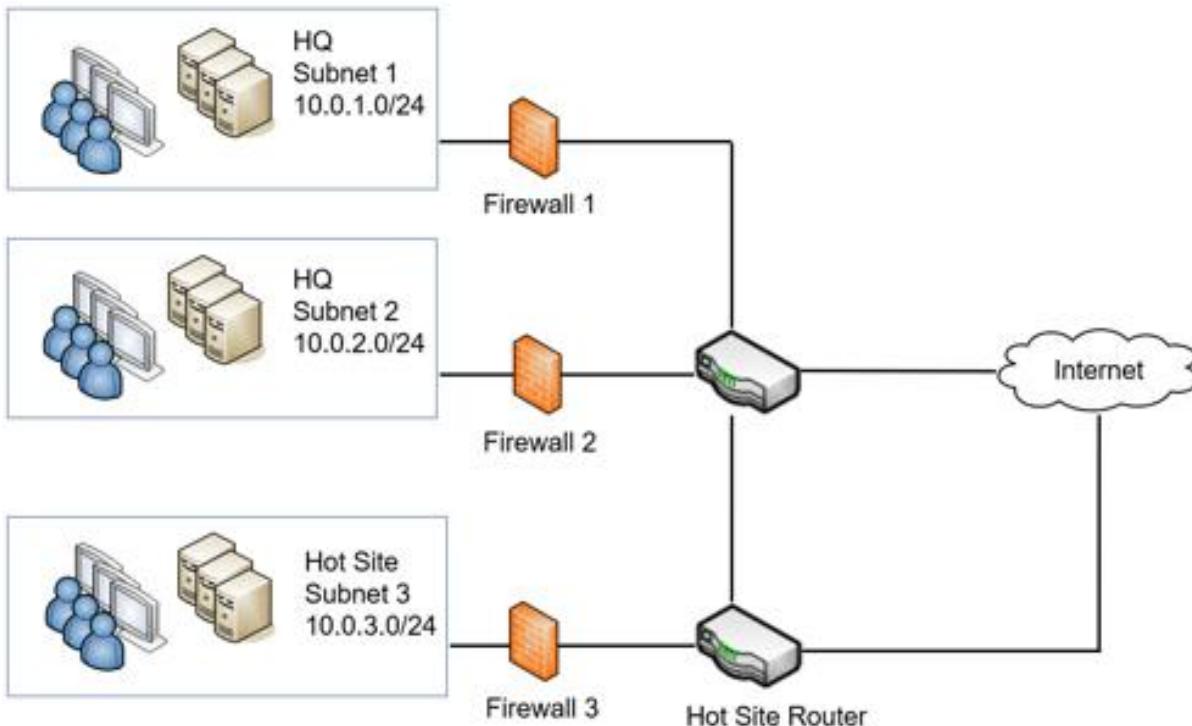
- A. A listing of labels reflecting classification levels
- B. A listing of rules that the application must be able to trigger
- C. A listing of owners
- D. A matrix of functions matched with required privileges

11. Your organization has implemented a system that stores user credentials in a central database. Users log on once with their credentials. They can then access other systems in the organization without logging on again. Which of the following does this describe?

- A. Federation

- B. SAML
- C. SSO
- D. OAuth

12. The Mapple organization is creating a help-desk team to assist employees with account issues. Members of this team need to create and modify user accounts and occasionally reset user passwords. Which of the following is the BEST way to accomplish this goal?
- A. Give each help-desk employee appropriate privileges individually.
 - B. Add each member of the help-desk team to the administrator group within the domain.
 - C. Add members of the help-desk team to a security group that has the appropriate privileges.
 - D. Assign attributes to members of the help-desk team and give these attributes appropriate privileges.
13. Your organization's security policy states that administrators should follow the principle of least privilege. Which of the following tools can ensure that administrators are following the policy?
- A. Account audits
 - B. Risk assessment
 - C. Vulnerability assessment
 - D. Threat assessment
14. Lisa is responsible for managing and monitoring network devices, such as routers and switches, in your network. Which of the following protocols is she MOST likely to use?
- A. NAT
 - B. SRTP
 - C. SNMPv3
 - D. DNSSEC
15. Your organization's network looks like the following graphic and you've been asked to verify that Firewall 2 has the correct settings.



All firewalls should enforce the following requirements:

- Use only secure protocols for remote management.
- Block cleartext web traffic.

The following graphic shows the current rules configured in Firewall 2.

Rule	Destination	Source	Protocol	Action
HTTPS Outbound	Any	10.0.2.0/24	HTTPS	Allow
HTTP Outbound	Any	10.0.2.0/24	HTTP	Block
DNS	Any	10.0.2.0/24	DNS	Allow
HTTPS Inbound	10.0.2.0/24	Any	HTTPS	Allow
HTTP Inbound	10.0.2.0/24	Any	HTTP	Block
Telnet	10.0.2.0/24	Any	Telnet	Allow
SSH	10.0.2.0/24	Any	SSH	Allow

Which rule, if any, should be changed in Firewall 2?

- HTTPS Outbound
- HTTP Outbound
- DNS
- Telnet
- SSH
- None. All rules are correct.

16. Your organization recently landed a contract with the federal government. Developers are fine-tuning an application that will process sensitive data. The contract mandates that all computers using this application must be isolated. Which of the following would BEST meet this need?

- A. Create a bastion host in a screened subnet.
- B. Implement a boundary firewall.
- C. Create an air-gapped network.
- D. Implement an IPS.

17. Your organization wants to increase security for VoIP and video teleconferencing applications used within the network. Which of the following protocols will BEST support this goal?

- A. S/MIME
- B. TLS
- C. SFTP
- D. SRTP

18. Your organization hosts a web server accessed from employees within the network, and via the Internet. Management wants to increase its security. You are tasked with separating all web-facing traffic from internal network traffic. Which of the following provides the BEST solution?

- A. Screened subnet
- B. VLAN
- C. Firewall
- D. WAF

19. Developers recently configured a new service on a server called GCGA1. GCGA1 is in a screened subnet and accessed by employees in the internal network, and by others via the Internet. Network administrators modified firewall rules to access the service. Testing shows the service works when accessed from internal systems. However, it does not work when accessed from the Internet. Which of the following is MOST likely configured incorrectly?

- A. The new service
- B. An ACL

- C. The GCGA1 server
- D. A VLAN

20. Bart recently hooked up a switch incorrectly causing a switching loop problem, which took down part of an organization's network. Management wants to implement a solution that will prevent this from occurring in the future. Which of the following is the BEST choice to meet this need?

- A. Flood guard
- B. SNMPv3
- C. SRTP
- D. RSTP

21. A penetration tester has been hired to perform an assessment on the *greatadministrator.com* site. He used the nslookup command to perform some reconnaissance and received the following output:

```
C:\>nslookup -querytype=mx greatadministrator.com
```

Server: UnKnown

Address: 192.168.1.1

Non-authoritative answer:

```
gcapremium.com MX preference = 20, mail exchanger =  
mx1.emailsrvr.com
```

```
gcapremium.com MX preference = 90, mail exchanger =  
mx2.emailsrvr.com
```

Of the following choices, what BEST describes this output?

- A. The server named mx2.emailsrvr.com is the primary email server for this domain.
- B. The server named mx1.emailsrvr.com is the primary email server for this domain.
- C. The AAAA record is misconfigured for this domain.
- D. The SOA record is hiding the IP address of the domain.
- E. DNSSEC has not been enabled on this domain.

22. Which of the following is an example of a detective control?

- A. An IPS reconfigured to monitor traffic instead of blocking it
- B. A backup solution that includes off-site backups
- C. Security guards

D. A cable lock

23. Your organization is planning to implement a wireless network using WPA2 Enterprise. Of the following choices, what is required?

- A. An authentication server with a digital certificate installed on the authentication server
- B. An authentication server with DHCP installed on the authentication server
- C. An authentication server with DNS installed on the authentication server
- D. An authentication server with WPS running on the access point

24. Bart was in a coffee shop going through emails and messages on his smartphone. He then started receiving several text messages promoting a political party and encouraging him to visit websites. After he left the coffee shop, he didn't receive any more messages. What does this describe?

- A. Bluesnarfing
- B. Bluejacking
- C. Malware
- D. WPS attack

25. Management within your organization wants employees to be able to access internal network resources from remote locations, including from their homes. Which of the following is the BEST choice to meet this need?

- A. NAC
- B. VPN
- C. IDS
- D. IPS

26. Security experts want to reduce risks associated with updating critical operating systems. Which of the following will BEST meet this goal?

- A. Implement patches when they are released.
- B. Implement a change management policy.
- C. Use only trusted operating systems.
- D. Implement operating systems with secure configurations.

27. Your organization has a segmented network used to process highly classified material. Management wants to prevent users from copying documents to USB flash drives from any computer in this network. Which of the following can be used to meet this goal?

- A. DLP
- B. HSM
- C. COPE
- D. SED

28. Your organization hosts an e-commerce website using a back-end database. The database stores product data and customer data, including credit card numbers. Which of the following is the BEST way to protect the credit card data?

- A. Full database encryption
- B. Full disk encryption
- C. Database column encryption
- D. File-level encryption

29. The Springfield Nuclear Power Plant has created and maintains an online application used to teach the basics of nuclear physics. Only students and teachers in Springfield Elementary School can access this application via the cloud. What type of cloud service model is this?

- A. IaaS
- B. PaaS
- C. SaaS
- D. XaaS

30. Your organization has implemented a CYOD security policy. The policy mandates the use of security controls to protect the devices, and any data on them if they are lost or stolen. Which of the following would BEST meet this goal?

- A. Screen locks and GPS tagging
- B. Patch management and change management
- C. Screen locks and device encryption
- D. Full device encryption and XaaS

31. Management within your company wants to implement a method that will authorize employee access to the network based on several elements. These elements include the employee's identity, location, the time of day, and the type of device used by the employee. Which of the following will BEST meet this need?

- A. Geofence
- B. Containerization
- C. Tethering
- D. Context-aware authentication

32. Personnel should be able to run the BizzFadd app from their mobile devices. However, certain features should only be operational when employees are within the company's property. When an employee leaves the property, access to these features should be blocked. Which of the following answers provides the BEST solution to meet this goal?

- A. Geofencing
- B. Geolocation
- C. GPS tagging
- D. Containerization

33. A large city is using a SCADA system to manage a water treatment plant. City managers have asked IT personnel to implement security controls to reduce the risk of cybersecurity attacks against ICSs controlled by the SCADA system. Which of the following security controls would be MOST relevant to protect this system?

- A. DLP
- B. TPM
- C. FPGA
- D. NIPS

34. IT auditors have found several unmanaged VMs in a network. They discovered that these were created by administrators for testing but weren't removed after testing was completed. Which of the following should be implemented to prevent this in the future?

- A. A policy related to VM sprawl
- B. A policy related to VM escape protection

- C. A policy related to XAAS
- D. A policy related to SDNs

35. Bart recently launched an attack on a company website using scripts he found on the Internet. Which of the following BEST describes Bart as a threat actor?

- A. Insider
- B. Hacktivist
- C. Script kiddie
- D. Shadow IT

36. The Marvin Monroe Memorial Hospital recently suffered a serious attack preventing employees from accessing any computer data. The attackers scattered ReadMe files throughout the network that appeared on user screens. They indicated that the attackers encrypted all the data, and it would remain encrypted until the attackers received a hefty sum as payment. Which of the following identifies the MOST likely threat actor in this attack?

- A. Criminal syndicate
- B. Ransomware
- C. Competitors
- D. Hacktivist

37. Gil Gunderson, a salesperson in your organization, received an email on his work computer that included a malicious link. After clicking the link, his computer was infected with malware. The malware was not detected by antivirus software installed on his computer, the organization's email server, or the organization's UTM appliance. After infecting his computer, the malware then searched the network and encrypted data in all the network shares that Gil could access. Which of the following BEST describes how this occurred?

- A. The malware represents a zero-day exploit.
- B. The antivirus software indicated false positives.
- C. The malware infection was the result of a backdoor.
- D. The principle of least privilege was not implemented.

38. Logs on a web server show that it is receiving a significant number of SYN packets from multiple sources on the Internet, but it isn't receiving the corresponding ACK packets. Of the following choices, what is the MOST likely source of these packets?

- A. DDoS
- B. Ransomware
- C. Worm
- D. Bots

39. Management recently mandated that computer monitors be repositioned to ensure they cannot be viewed from outside any windows. Additionally, users are directed to place screen filters over their monitors. What is the purpose of this policy?

- A. Reduce success of phishing
- B. Reduce success of shoulder surfing
- C. Reduce success of dumpster diving
- D. Reduce success of prepadding

40. Bart's supervisor told him to clean his desk to comply with the organization's clean desk space policy. While doing so, he threw several papers containing PII into the recycle bin. Which type of attack can exploit this action?

- A. SPIM
- B. Dumpster diving
- C. Shoulder surfing
- D. Tailgating

41. Your organization's CFO recently received an email indicating the organization is being sued. More, the email names her specifically as a defendant in the lawsuit. It includes an attachment described as a subpoena and encourages her to open it for more information. Which of the following BEST describes the social engineering principle used by the sender in this scenario?

- A. Whaling
- B. Phishing

- C. Authority
- D. Consensus

42. Users are complaining about intermittent connectivity with a web server. After examining the logs, you identify a large volume of connection attempts from public IP addresses. You realize these connection attempts are overloading the server, preventing it from responding to other connections. Which of the following is MOST likely occurring?

- A. DDoS attack
- B. DNS poisoning attack
- C. Replay attack
- D. ARP poisoning attack

43. An application on one of your database servers has crashed several times recently. Examining detailed debugging logs, you discover that just prior to crashing, the database application is receiving a long series of x90 characters. What is MOST likely occurring?

- A. SQL injection
- B. Buffer overflow
- C. XML injection
- D. Zero-day

44. Your organization recently experienced a significant data breach. After an investigation, cybersecurity professionals found that the initial attack originated from an internally developed application. Normally users can only access the application by logging on. However, the application allowed the attacker access to the application without requiring the attacker to log on. Which of the following would have the BEST chance of preventing this attack?

- A. Code review
- B. Backdoor
- C. DDoS protection
- D. Keylogger

45. A software development process merges code changes from developers working on a project several times a day. It uses automation to validate the

code and tracks changes using version control processes. Which of the following BEST describes this process?

- A. Continuous integration
- B. Continuous validation
- C. Continuous delivery
- D. Continuous monitoring

46. Martin is performing a risk assessment. He is trying to identify the number of times a specific type of incident occurred in the previous year. Which of the following BEST identifies this?

- A. ALE
- B. ARO
- C. SLE
- D. RPO

47. Lisa recently received a security advisory. She's using it to review logs and looking for activity mentioned in the security advisory. Which of the following BEST describes what she is doing?

- A. Creating OSINT
- B. Threat hunting
- C. Penetration testing
- D. Performing reconnaissance

48. You recently completed a vulnerability scan on your network. It reported that several servers are missing key operating system patches. However, after checking the servers, you've verified that the servers have these patches installed. Which of the following BEST describes this?

- A. False negative
- B. Misconfiguration on servers
- C. False positive
- D. Non-credentialed scan

49. An external security auditor recently completed a security assessment. He discovered that a system has a vulnerability that two previous security assessments detected. Which of the following BEST explains this?

- A. The scanner is reporting a false negative.

- B. The vendor has not created a security patch.
 - C. The scans ran as credentialed scans.
 - D. The system is misconfigured.
50. Your organization regularly performs training in the form of a game mimicking an exercise. One team oversees the exercise, sets the rules, and identifies the rules of engagement. Another team uses known TTPs to exploit vulnerabilities within the rules of engagement. You are on a team dedicated to defending resources. Which of the following BEST describes your role?
- A. A member of the red team
 - B. A member of the blue team
 - C. A member of the purple team
 - D. A member of the white team
51. You are running a vulnerability scanner with an access level that gives it the best chance of detecting vulnerabilities. Which of the following BEST describes the type of scan you are running?
- A. Non-credentialed scan
 - B. A port scan
 - C. A non-intrusive scan
 - D. Credentialed scan
52. You suspect that an attacker has been sending specially crafted TCP packets to a server trying to exploit a vulnerability. You decide to capture TCP packets being sent to this server for later analysis and you want to use a command-line tool to do so. Which of the following tools will BEST meet your need?
- A. Tcpreplay
 - B. Tcpdump
 - C. Netcat
 - D. Wiredump

53. Your company wants to control access to a restricted area of the building by adding an additional physical security control that includes facial recognition. Which of the following provides the BEST solution?

- A. Bollards
- B. Guards
- C. Retina scanners
- D. Cameras

54. Thieves recently rammed a truck through the entrance of one of your organization's buildings in the middle of the night. They then proceeded to steal a significant amount of IT equipment. Which of the following choices can prevent this from happening again?

- A. Bollards
- B. Guards
- C. CCTV
- D. Alarms

55. Fileserver1 hosts several files accessed by users in your organization, and it's important that they can always access these files. Management wants to implement a solution to increase cybersecurity resilience. Which of the following is the LOWEST cost solution to meet this requirement?

- A. Active/active load balancing
- B. Active/passive load balancing
- C. RAID
- D. Warm site

56. You need to identify and mitigate potential single points of failure in your organization's security operations. Which of the following policies would be the BEST choice to help you find them?

- A. A disaster recovery plan
- B. A business impact analysis
- C. Annualized loss expectancy
- D. Separation of duties

57. Compu-Global-Hyper-Mega-Net hosts a website selling digital products. Marketing personnel have launched several successful sales. The server has been overwhelmed, resulting in slow responses from the server, and lost sales. Management wants to implement a solution that will provide cybersecurity resilience. Which of the following is the BEST choice?

- A. Managed PDUs
- B. Certificates
- C. Web application firewall
- D. Load balancing

58. The backup policy for a database server states that the amount of time needed to perform backups should be minimized. Which of the following backup plans would BEST meet this need?

- A. Full backups on Sunday and full backups on the other six days of the week
- B. Full backups on Sunday and differential backups on the other six days of the week
- C. Full backups on Sunday and incremental backups on the other six days of the week
- D. Differential backups on Sunday and incremental backups on the other six days of the week

59. A security analyst is creating a document that includes the expected monetary loss from a major outage. She is calculating the potential impact on life, property, finances, and the organization's reputation. Which of the following documents is she MOST likely creating?

- A. BCP
- B. BIA
- C. MTBF
- D. RPO

60. You are helping a risk management team update the business impact analysis for your organization. For one system, the plan requires an RTO of five hours and an RPO of one day. Which of the following would meet this requirement?

- A. Ensure the system can be restored within five hours and ensure it does not lose more than one day of data.
- B. Ensure the system can be restored within one day and ensure it does not lose more than five hours of data.
- C. Ensure the system can be restored between five hours and one day after an outage.

D. Ensure critical systems can be restored within five hours and noncritical systems can be restored within one day.

61. Marge is updating the business impact analysis (BIA) for your organization. She needs to document the time needed to return a database server to an operational state after a failure. Which of the following terms would she use?

- A. MTTR
- B. MTBF
- C. SLE
- D. ARO

62. Lisa needs to transmit PII via email and she wants to maintain its confidentiality. Which of the following choices is the BEST solution?

- A. Use hashes.
- B. Encrypt it before sending.
- C. Protect it with a digital signature.
- D. Use RAID.

63. Employees in your organization recently received an email that appeared to come from your organization's CEO. The email mentioned that IT personnel were troubleshooting an authentication issue and needed employees to reply to the email with their credentials. Several employees responded with their credentials. This was a phishing campaign created for user training, and it spoofed the CEO's email. Executives want to ensure that employees have proof that any emails that appear to be coming from the executives, did come from them. Which of the following should be implemented?

- A. Digital signatures
- B. Spam filter
- C. Role-based training
- D. Heuristic-based detection

64. As an administrator, you receive an antivirus alert from a server in your network indicating one of the files has a hash of known malware. The file was pushed to the server from the organization's patch management system

and is scheduled to be applied to the server early the next morning. The antivirus software indicates that the file and hash of the malware on the server are:

- File: gcga_upgrade.exe
- Hash: bd64571e26035d95e5e9232b4aff b915

Checking the logs of the patch management system, you see the following information:

Status	Update Name	Hash
Pushed	gcga_upgrade.exe b815571e26035d95e5e9232b4aff48db	

Which of the following indicates what MOST likely occurred?

- A. The file was infected after it was pushed out to the server.
- B. The file was embedded with crypto-malware before it was pushed to the server.
- C. The file was listed in the patch management system's blacklist.
- D. The file was infected when the patch management system downloaded it.

65. Tony hid several plaintext documents within an image file. He then sent the image file to Louie. Which of the following BEST describes the purpose of his actions?

- A. To support steganography
- B. To support integrity
- C. To support resilience
- D. To support obfuscation

66. Lisa and Bart need to exchange emails over the Internet using a nonsecure channel. These emails need to provide non-repudiation. They decide to use certificates on each of their computers. What would they use to sign their emails?

- A. CRL
- B. OCSP
- C. CSR
- D. CA
- E. DSA

67. Administrators have noticed a significant amount of OCSP traffic sent to an intermediate CA. They want to reduce this traffic. Which of the following is the BEST choice to meet this need?

- A. Pinning
- B. Digital signatures
- C. Stapling
- D. Hashing

68. A company is hosting an e-commerce site that uses certificates for HTTPS. Management wants to ensure that users can verify the validity of these certificates even if elements of the Internet suffer an extended outage. Which of the following provides the BEST solution?

- A. OCSP
- B. PEM
- C. SAN
- D. CRL

69. A security auditor discovered that several employees in the Accounting department can print and sign checks. In her final report, she recommended restricting the number of people who can print checks and the number of people who can sign them. She also recommended that no one should be authorized to both print and sign checks. Which security policy does this describe?

- A. Discretionary access control
- B. Rule-based access control
- C. Separation of duties
- D. Job rotation

70. Bart recently resigned and left your organization. Later, IT personnel determined that he deleted several files and folders on a server share after he left the organization. Further, they determined that he did so during the weekend while the organization was closed. Which of the following account management practices would have prevented his actions?

- A. Onboarding
- B. Time-of-day restrictions
- C. Account audit

D. Offboarding

71. Your organization hired a third-party security professional to assess vulnerabilities. The security professional discovered a server was running an application that hasn't been updated for eight years. Management decided to keep the application online because there isn't a newer version from the vendor. Which of the following BEST describes why the application doesn't have a newer version?

- A. MSA
- B. AUP
- C. MSSP
- D. EOL

72. A help-desk professional has begun to receive several calls from employees related to malware. Using common incident response procedures, which of the following should be her FIRST response to these calls?

- A. Preparation
- B. Identification
- C. Eradication
- D. Recovery

73. Homer reported suspicious activity on his computer. After investigating, you verify that his computer is infected with malware. Which of the following steps should you take NEXT?

- A. Identification
- B. Preparation
- C. Containment
- D. Eradication

74. Security personnel confiscated Bart's workstation after a security incident. Administrators removed the hard drive for forensic analysis but were called away to troubleshoot an outage before capturing an image of the drive. They left it unattended for several hours before returning to begin their analysis. Later, legal personnel stated that the analysis results would

not be admissible in a court of law. What is the MOST likely reason for the lack of admissibility?

- A. Witnesses were not identified.
 - B. A chain of custody was not maintained.
 - C. An order of volatility was not maintained.
 - D. A hard drive analysis was not complete.
75. Your organization is involved in a lawsuit, and a judge issued a court order requiring your organization to keep all emails from the last three years. Your data retention policy states that email should only be maintained from the previous 12 months. After investigating, administrators realize that backups contain emails from the last three years. What should they do with these backups?
- A. Backups older than 12 months should be deleted to comply with the data retention policy.
 - B. Backups for the last 12 months should be protected to comply with the legal hold.
 - C. Backups for the last two years should be protected to comply with the legal hold.
 - D. Backups for the last three years should be protected to comply with the legal hold.

Post-Assessment Answers

1. **B** is correct. Scalability is the best choice because it allows administrators to manually scale the server up or out as needed in response to this predictable high resource usage. Stored procedures are a group of SQL statements that execute as a whole and help prevent SQL injection attacks. Version control tracks software versions as it is updated and is unrelated to this question. Memory management techniques help ensure that applications don't cause memory problems such as memory leaks or integer overflows. See Chapter 1.
2. **C** is correct. A Time-based One-Time Password (TOTP) solution can be implemented as a compensating control. It can be implemented with hardware tokens or with an app on a smartphone. The smart cards provide two-factor authentication, so the compensating control should provide two-factor control, and TOTP fills that need. None of the other answers provides an additional factor of authentication. An account lockout policy locks out users after entering an incorrect password too many times. The password policy can be used to increase password security. Requiring users to change their password more often is in the password policy as password expiration. See Chapter 1.
3. **D** is correct. The **ping** command sends Internet Control Message Protocol (ICMP) echo requests and checks for ICMP echo replies. The Address Resolution Protocol (ARP) resolves IP addresses to media access control (MAC) addresses, and the **arp** command is used to view and manipulate the ARP cache. The **ipconfig** command displays the configuration of a NIC. The **route** command can be used to display and manipulate the routing table on computing systems. See Chapter 1.
4. **D** is correct. The **netstat** command displays active connections on a system. **Arp** displays information related to media access control (MAC) addresses. **Ipconfig** displays TCP/IP configuration information for wired and wireless network interface cards. The **hping3** command is used to identify open and closed ports on remote systems. See Chapter 1.

5. **B** is correct. The **tail** command shows the last 10 lines (by default) of a log file and, in this scenario, is the best choice to show a recent error message. The **head** command shows the beginning lines in a log file and is unlikely to display recent error messages. You would use the **chmod** command (short for change mode) to change permissions on files and directories. The **logger** command is used to add entries into the syslog file. See Chapter 1.

6. **C** is correct. The **chmod 750 gcga.exe** should be used. The 7 (in 760) gives read, write, and execute permissions to the owner. The 5 (in 750) gives read and execute permissions to the owner group. The 0 (in 760) ensures that everyone else has no permissions. The 0 (in 067) denies read, write, and execute permissions for the owner, and the 7 (in 067) grants read, write, and execute permissions for everyone. The first 6 (in 661) grants only read and write permissions but not execute permissions to the owner. The second 7 (in 770) grants read, write, and execute permissions for the owner group, but the scenario says that only read and execute permissions should be granted for this group. See Chapter 1.

7. **A** is correct. The **ifconfig** command displays network settings on a Linux computer. This includes the IP address, subnet mask, and default gateway assigned to the network interface card (NIC). The **ipconfig** command performs similar checks on Windows computers but not on Linux systems. **Netstat** shows network statistics and active connections but not the network settings. The **tracert** command traces the route between systems on a network and can help determine which network devices are failing. See Chapter 1.

8. **B** is correct. This is in the something you have factor of authentication. Users are required to have a smartphone with the authentication application installed. The application generates a key of numbers, users don't know this key until the application generates it. Biometrics are in the something you are factor, but biometric methods aren't mentioned. Something you can do refers to a user's actions, such as making gestures on a screen. See Chapter 2.

9. **C** is correct. Fingerprints are in the something you are factor of authentication and will meet this need. All the other answers are in either the something you have factor (already used by the smart card) or the something you know factor (already used by the password). A personal identification number (PIN) is in the something you know factor. Tokens and push notifications are in the something you have factor. See Chapter 2.

10. **D** is correct. A matrix of functions, roles, or job titles matched with the required access privileges for each of the functions, roles, or job titles is a common planning document for a role-based access control model. The mandatory access control (MAC) model uses sensitivity labels and classification levels. Rule-based access control models use rules, but role-based access control models don't use rules. The discretionary access control (DAC) model specifies that every object has an owner and it might identify owners in a list. See Chapter 2.

11. **C** is correct. This describes a single sign-on (SSO) solution in which users only log on once. Although a federation supports SSO, not all SSO systems use a federation. Security Assertions Markup Language (SAML) is an SSO solution used for web-based applications, but not all SSO solutions use SAML. OAuth (Open Authorization) is an authorization protocol used with HTTP-based apps, not internal organizations. See Chapter 2.

12. **C** is correct. The best solution of the available choices is to add members of the help-desk team to a security group that has the appropriate privileges. Assigning permissions to users individually adds to the administrative workload. Giving members administrator privileges violates the principle of least privilege by giving them too many privileges. An attribute-based access control model can use attributes to grant access but would add to the administrative workload if done individually. See Chapter 2.

13. **A** is correct. Account audits verify users have the permissions they need for their job, and no more, which verifies the principle of least privilege is being followed. Risk, vulnerability, and threat assessments assess current

risks. While they might verify the principle of least privilege is being followed, they do much more. See Chapter 3.

14. **C** is correct. Simple Network Management Protocol version 3 (SNMPv3) is used to securely manage and monitor network devices. None of the other choices is related to managing and monitoring network devices. Network Address Translation (NAT) translates public IP addresses to private IP addresses and private addresses back to public. The Secure Real-time Transport Protocol (SRTP) secures voice and other streaming media transmissions. Domain Name System Security Extensions (DNSSEC) helps prevent DNS cache poisoning attacks. See Chapter 3.

15. **D** is correct. The Telnet rule should be changed to block Telnet traffic. Telnet sends credentialled and other data in cleartext and should not be used. Secure Shell (SSH) encrypts traffic and should be used instead of Telnet. All other rules are correct. See Chapter 3.

16. **C** is correct. An air-gapped network would best meet this need. An air gap indicates that the network is isolated from other networks with space or air. The application would be developed and compiled in this isolated network. All the other answers have a level of connectivity with the Internet and don't provide the best protection. A bastion host is a hardened server that can be accessed via the Internet and it may be directly on the Internet or within a screened subnet (sometimes called a demilitarized zone or DMZ). A boundary firewall (sometimes called a perimeter firewall) is placed at the edge of the network between the Internet and the internal network or within the screened subnet. An intrusion prevention system (IPS) is typically placed inline with traffic between the Internet and the internal network and attempts to detect and block attacks. See Chapter 3.

17. **D** is correct. The Secure Real-Time Transport Protocol (SRTP) provides encryption, message authentication, and integrity for Voice over Internet Protocol (VoIP), video teleconferencing, and other streaming media applications. None of the other answers are related to VoIP or video teleconferencing. Secure/Multipurpose Internet Mail Extensions (S/MIME) secures email. The Transport Layer Security (TLS) protocol is used to

encrypt data in transit but isn't the best choice for streaming media. Secure File Transfer Protocol (SFTP) is a secure implementation of FTP to transfer files. See Chapter 3.

18. **A** is correct. A screened subnet (sometimes called a demilitarized zone, DMZ) is a buffered zone between a private network and the Internet, and it will separate the web server's web-facing traffic from the internal network. You can use a virtual local area network (VLAN) to group computers together based on job function or some other administrative need, but it is created in the internal network. A firewall does provide protection for the web server but doesn't necessarily separate the web-facing traffic from the internal network. A web application firewall (WAF) protects a web server from incoming attacks, but it does not necessarily separate Internet and internal network traffic. See Chapter 3.

19. **B** is correct. The most likely problem of the available choices is that an access control list (ACL) is configured incorrectly. The server is in a screened subnet (sometimes called a demilitarized zone or DMZ) and the most likely problem is an incorrectly configured ACL on the border firewall (between the Internet and the screened subnet). The service is working when accessed by internal systems, so it isn't likely that it is the problem. Also, the GCGA1 server works for internal systems indicating it is working correctly. There isn't any indication a virtual local area network (VLAN) is in use. See Chapter 3.

20. **D** is correct. Rapid Spanning Tree Protocol (RSTP) prevents switching loop problems and should be enabled on the switches to meet this need. While not available as a possible answer, the older Spanning Tree Protocol (STP) also provides loop protection. A flood guard on a switch helps prevent a media access control (MAC) flood attack. Simple Network Management Protocol version 3 (SNMPv3) is used to manage and monitor network devices. The Secure Real-time Transport Protocol (SRTP) provides encryption, message authentication, and integrity for video and voice data. See Chapter 3.

21. **B** is correct. The server named mx1.emailsrvr.com is the primary email server for this domain. The MX record indicates it is a mail server and the preference of 20 (compared with the preference of 90 for mx2) indicates it is the primary email server. A preference of 90 for mx2.emailsrvr.com is higher than 20 (the preference for mx1.emailsrvr.com) and indicates that mx2.emailsrvr.com is the backup email server. An AAAA record maps the IPv6 address to the hostname, but IPv6 is not indicated at all in this question. The start of authority (SOA) record includes information about the DNS zone and some of its settings, but it does not hide the domain's IP address. Domain Name System Security Extensions (DNSSEC) is a suite of extensions to DNS that helps prevent DNS cache poisoning, but the existence (or non-existence) of a DNSSEC record is not indicated in this question. See Chapter 3.

22. **A** is correct. An intrusion prevention system (IPS) is normally placed in line with traffic to block malicious traffic. However, it can be reconfigured to monitor traffic, effectively operating as an intrusion detection system (IDS). A backup solution is a corrective or recovery control. Security guards are preventive and deterrent controls. Cable locks are physical controls that prevent the theft of devices such as laptops. See Chapter 4.

23. **A** is correct. WPA2 Enterprise requires an 802.1x authentication server and most implementations require a digital certificate installed on the server. The network will likely have Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) services, but it isn't necessary to install them on the authentication server. Wi-Fi Protected Setup (WPS) makes it easier to set up wireless devices, but it isn't related to WPA2 Enterprise. See Chapter 4.

24. **B** is correct. Bluejacking is the practice of sending unsolicited messages to other Bluetooth devices. It has a limited range of about 30 feet when sent from one mobile phone to another so the attacker couldn't send additional messages after he left. Bluesnarfing allows attackers to access data (including email contact lists) on a smartphone but the scenario only indicates the user is receiving unwanted messages. Malware would not stop after a person leaves a coffee shop. A Wi-Fi Protected Setup (WPS) attack

attempts to discover an access point WPS PIN by guessing PIN numbers, but this is not related to smartphone messages. See Chapter 4.

25. **B** is correct. A virtual private network (VPN) provides access to a private network over a public network such as the Internet via remote locations and is the best choice to meet this requirement. Network access control (NAC) methods can check VPN clients for health before allowing them access to the network, but it doesn't directly provide the access. Intrusion detection systems (IDSs) and intrusion prevention systems (IPSSs) protect networks but do not provide remote access. See Chapter 4.

26. **B** is correct. A change management policy helps reduce risk associated with making any changes to systems, including updating them. Patches should be tested and evaluated before implementing them and implementing them when they are released sometimes causes unintended consequences. The use of a trusted operating system or operating systems with secure configurations doesn't address how they are updated. See Chapter 5.

27. **A** is correct. A data loss prevention (DLP) solution can prevent users from copying documents to a USB drive. None of the other answers control USB drives. A hardware security module (HSM) is an external security device used to manage, generate, and securely store cryptographic keys. COPE (corporate-owned, personally enabled) is a mobile device deployment model. A self-encrypting drive (SED) includes the hardware and software to encrypt all data on the drive and securely store the encryption keys. See Chapter 5.

28. **C** is correct. Database column (or field) encryption is the best choice because it can be used to encrypt the fields holding credit card data, but not fields that don't need to be encrypted. Full database encryption and full disk encryption aren't appropriate because of the resources needed to encrypt everything compared with the security desire of protecting only the credit card data. File-level encryption isn't appropriate on a database and will often make it inaccessible to the database application. See Chapter 5.

29. **C** is correct. This is a Software as a Service (SaaS) model. The software is the online application and the cloud provider (the Springfield Nuclear Power Plant in this example) maintains it. Infrastructure as a Service (IaaS) provides customers with the hardware via the cloud. Customers are responsible for installing the operating system and any applications. Platform as a Service (PaaS) is a computing platform. Anything as a Service (XaaS) refers to cloud services beyond IaaS, PaaS, and SaaS but this scenario clearly describes a SaaS model. See Chapter 5.

30. **C** is correct. Screen locks provide protection for lost devices by making it more difficult for someone to access the device. Device encryption protects the confidentiality of the data even if someone gets past the screen lock. Global Positioning System (GPS) tagging includes location information on pictures and other files but won't help protect a lost or stolen device. Patch management keeps devices up to date, and change management helps prevent outages from unauthorized changes. Anything as a Service (XaaS) refers to cloud services beyond IaaS, PaaS, and SaaS. See Chapter 5.

31. **D** is correct. Context-aware authentication can authenticate a user and a mobile device using multiple elements, including identity, geolocation, time of day, and type of device. None of the other answers meets all the requirements of the question. A geofence creates a virtual fence, or geographic boundary, and can be used with context-aware authentication. Containerization isolates an application, protecting it and its data. Tethering allows one device to share its Internet connection with other devices. See Chapter 5.

32. **A** is correct. Geofencing can be used to create a virtual fence or geographic boundary, outlining the company's property. Geolocation is used to identify the location of an object, such as a mobile device. Geofencing will use geolocation to determine when a mobile device is within a geographic boundary, but geolocation without geofencing won't detect if a user is on the company's property. Global Positioning System (GPS) tagging adds geographic data (such as latitude and longitude data) to files indicating when the file was created and is unrelated to this question.

Containerization runs applications in a container to isolate them. See Chapter 5.

33. **D** is correct. A network intrusion prevention system (NIPS) is the most relevant security control of those listed to reduce risks related to cybersecurity attacks of the supervisory control and data acquisition (SCADA) system, or industrial control systems (ICSs) controlled by the SCADA system. The SCADA system should be within an isolated network, and the NIPS helps provide that isolation. A data loss prevention (DLP) system helps prevent loss of data but wouldn't protect a SCADA system from potential attacks. A Trusted Platform Module (TPM) is a hardware chip on a computer's motherboard that stores cryptographic keys used for encryption. A field programmable gate array (FPGA) is an integrated circuit that can be configured after it is sold and is unrelated to this question. See Chapter 5.

34. **A** is correct. Virtual machine (VM) sprawl occurs when an organization has many VMs that aren't managed properly, and a policy addressing VM sprawl can reduce or eliminate them. Unmonitored VMs often aren't updated and can be vulnerable to attacks. A policy related to VM escape protection addresses problems that allow successful VM escape protection attacks, such as not keeping VMs updated. Anything as a Service (XaaS) refers to cloud services beyond IaaS, PaaS, and SaaS and is unrelated to VMs. A software-defined network (SDN) creates an infrastructure with code instead of hardware routers and switches and is unrelated to VMs. See Chapter 5.

35. **C** is correct. In this scenario, Bart is acting as a script kiddie because he is using existing scripts. An insider works for an organization, but there isn't any indication that Bart is an employee of the company he attacked. A hacktivist launches attacks as part of an activist movement, but this scenario doesn't indicate Bart's actions are trying to increase awareness about a cause. Shadow information technology (IT) refers to IT systems deployed by non-IT departments to get around shortcomings with IT systems deployed by a central IT department in a large organization. See Chapter 6.

36. **A** is correct. Criminal syndicates most likely launched this attack because their motivation is primarily money. While the scenario describes ransomware, ransomware is the malware, not the threat actor. Competitors often want to obtain proprietary information, but it would be rare for a hospital competitor to put lives at risk by taking down a hospital's network and trying to extort money from another hospital. A hacktivist typically launches attacks to further a cause, not to extort money. See Chapter 6.

37. **A** is correct. The malware is likely a zero-day attack because the malware was not detected by antivirus software, the email server, or the unified threat management (UTM) appliance. A zero-day exploit wouldn't be known by antivirus software, so it wouldn't detect it. A false positive occurs when antivirus software raises an alert indicating a file is malicious when it isn't. However, there isn't any indication that the antivirus software raised an alert. Malware often installs backdoors that allow attackers access to infected systems without user intervention, but the scenario indicates that Gil clicked the malicious link causing the infection. If the malware encrypted all network shares, it would indicate that Gil had too many permissions, and the principle of least privilege wasn't implemented. However, the scenario indicates that the malware only encrypted shares that Gil could access. See Chapter 6.

38. **D** is correct. These packets are most likely coming from bots within a botnet that are launching a distributed denial-of-service (DDoS) attack using a SYN flood attack. The attacker sends the SYN packet, the web server responds with the SYN/ACK packet, but the attacker never finished the TCP handshake with the ACK packet. While this is a DDoS attack, the question is asking for the likely source of the packets, not what type of attack is taking place. Ransomware would encrypt data on the system, not send packets to it. A worm is self-replicating malware that spreads throughout a network. See Chapter 6.

39. **B** is correct. Shoulder surfing is the practice of viewing data by looking over someone's shoulder and it includes looking at computer monitors. Positioning monitors so that they cannot be viewed through a window and/or placing screen filters over the monitors reduces this threat. Phishing

is an email attack. Dumpster diving is the practice of looking through dumpsters. Prepending simply means to add something to the beginning of something else, and social engineers often prepend queries with valid information to make their query seem valid. See Chapter 6.

40. **B** is correct. Dumpster divers look through trash or recycling containers for valuable paperwork, such as documents that include Personally Identifiable Information (PII). Instead, paperwork should be shredded or incinerated. Spam over Internet messaging (SPIM) refers to unwanted text messages sent to mobile devices. Shoulder surfers attempt to view monitors or screens, not papers thrown into the trash or recycling containers. Tailgating is the practice of following closely behind someone else without using proper credentials. See Chapter 6.

41. **C** is correct. The sender is using the social engineering principle of authority in this scenario. A chief financial officer (CFO) would respect legal authorities and might be more inclined to open an attachment from such an authority. The scenario describes whaling, which is a specific type of phishing attack. However, whaling and phishing are attacks, not social engineering principles. The social engineering principle of consensus attempts to show that other people like a product, but this is unrelated to this scenario. See Chapter 6.

42. **A** is correct. A distributed denial-of-service (DDoS) attack includes attacks from multiple systems with the goal of depleting the target's resources, and this scenario indicates multiple connection attempts from different IP addresses. A Domain Name System (DNS) poisoning attack attempts to redirect web browsers to malicious URLs. A replay attack doesn't overload a system but instead allows the attacker to intercept data and use it to impersonate a user or system. An Address Resolution Protocol (ARP) poisoning attack gives clients false hardware address updates, and attackers use it to redirect or interrupt network traffic. See Chapter 7.

43. **B** is correct. Buffer overflow attacks include a series of no operation (NOP) commands, such as hexadecimal 90 (x90). When successful, they can crash applications and expose memory, allowing attackers to run

malicious code on the system. SQL injection attacks and Extensible Markup Language (XML) injection attacks do not use NOP commands. Zero-day attacks are unknown or undocumented, but attacks using NOP commands are known. See Chapter 7.

44. **A** is correct. A code review would have the best chance of preventing this attack. The scenario describes a backdoor in the internally developed application, but the backdoor is a vulnerability that allowed the attack and won't prevent the attack. Distributed denial of service (DDoS) protection can help thwart DDoS attacks, but there's no indication that this is a DDoS attack. A keylogger logs keystrokes of users so would not prevent an attack. See Chapter 7.

45. **A** is correct. This describes continuous integration, which merges changes from multiple developers and uses version control processes to track the changes. Continuous validation revalidates code after every change and is frequently part of CI, but continuous validation by itself doesn't include version control. Continuous delivery comes after CI and provides an automated process that delivers changes to a testing or staging environment. Continuous monitoring monitors code changes to detect compliance issues and security threats. See Chapter 7.

46. **B** is correct. The annual rate of occurrence (ARO) is the best choice to identify how many times a specific type of incident occurs in a year. Annual loss expectancy (ALE) identifies the expected monetary loss for a year and single loss expectancy (SLE) identifies the expected monetary loss for a single incident. $ALE = SLE \times ARO$ and if you know any two of these values, you can identify the third value. For example, $ARO = ALE / SLE$. The recovery point objective (RPO) identifies a point in time where data loss is acceptable, but it doesn't refer to the number of times an incident occurred. See Chapter 8.

47. **B** is correct. Threat hunting is the process of actively looking for threats within a network, and security advisories provide information on threats, including their tactics, techniques, and procedures (TTPs).

Security advisories are one type of open source intelligence (OSINT) used in threat hunting, but she is reading the OSINT, not creating it. Penetration testing actively assesses deployed security controls within a system or network. It is much more than reviewing logs. Reconnaissance methods attempt to learn as much as possible about a target, but Lisa is examining her own network. See Chapter 8.

48. **C** is correct. In this scenario, the vulnerability scanner reported a false positive indicating that the servers had a vulnerability, but the servers did not have the vulnerability. A false negative occurs if a vulnerability scanner does not report a known vulnerability. There isn't any indication that the servers are misconfigured. The scenario doesn't indicate if the scan was run under an account's context (credentialed or non-credentialed), so this answer isn't relevant to the question. See Chapter 8.

49. **B** is correct. If a vendor has not created a patch for a known vulnerability, vulnerability scanners will report the vulnerability (assuming they know about the vulnerability). False negatives are not reported so they will not appear in a vulnerability scanner's output. If scans are reporting the same vulnerability, it may be because a non-credentialed scan is reporting incorrect results, but a credentialed scan is more accurate than a non-credentialed scan. There isn't any indication that the system is misconfigured. See Chapter 8.

50. **B** is correct. A blue team defends and since you are on a team dedicated to defending resources, you are a member of the blue team. A red team attacks and they often use known tactics, techniques, and procedures (TTPs) of attackers to simulate actual attacks. A purple team is a group of people who can perform on either a red team or a blue team. The white team oversees the exercise, sets the rules, and identifies the rules of engagement. See Chapter 8.

51. **D** is correct. A credentialed scan runs with a high level of access and is better at detecting vulnerabilities than a non-credential scan. A non-credentialed scan runs without any account privileges. A port scan detects

open ports on a server. Vulnerability scanners are generally non-intrusive, but this doesn't give a scanner any specific access level. See Chapter 8.

52. **B** is correct. The **tcpdump** command-line tool is the best choice of the given answers. It is a command-line packet analyzer (or protocol analyzer) and its primary purpose is to capture packets. Tcpreplay is a suite of utilities used to edit packet captures and resend them, not capture packets. Netcat is useful for remotely accessing systems and can be used for banner grabbing, but it doesn't capture packets. Wiredump isn't a valid tool name. Wireshark (not included as an answer choice) is a graphic-based packet analyzer that can be started from the command line, but **tcpdump** includes more command-line options than Wireshark. See Chapter 8.

53. **B** is correct. Security guards can protect access to restricted areas with facial recognition and by checking the identities of personnel before letting them in. In some cases, the guards might recognize people, and in other situations, they might compare people's faces with their security badge. None of the other answers use facial recognition. Bollards are effective barricades to block vehicles, but they do not block personnel. Retina scanners are effective biometric access devices, but they only scan part of the eye, not the whole face. Cameras can monitor who goes in and out of an area, but they do not control the access. See Chapter 9.

54. **A** is correct. Bollards are effective barricades that can block vehicles. Guards can restrict access for personnel, but they cannot stop trucks from ramming through a building. Closed-circuit television (CCTV) or a similar video surveillance system can monitor the entrance, but it won't stop the attack. Alarms can go off after the truck rams through the entrance, but they won't stop the attack. See Chapter 9.

55. **C** is correct. A redundant array of inexpensive disks (RAID) subsystem is a relatively low-cost solution for disks' fault tolerance. By providing fault tolerance, it increases availability and resilience. Load balancing (active/active and active/passive) requires additional servers, which are significantly more expensive than RAID. A warm site is a separate location, which can also be expensive. See Chapter 9.

56. **D** is correct. A separation of duties policy is the best answer. In this context, if only one person can perform tasks within the organization's security operations, that person becomes a single point of failure. None of the other answers address a single point of failure. A disaster recovery plan (DRP) identifies how to recover critical systems and data after a disaster. A business impact analysis (BIA) helps an organization identify critical systems and components. An annualized loss expectancy (ALE) identifies the expected annual loss from a known risk. See Chapter 9.

57. **D** is correct. Load balancing shifts the load among multiple servers and provides cybersecurity resilience by increasing the site's availability by adding additional nodes when necessary. Managed power distribution units (PDUs) are used to remotely monitor energy consumption in a data center. Certificates can be used for identity, authentication, confidentiality, and integrity but won't provide resilience due to overloading resources on a server. A web application firewall helps protect a web server against attacks, but it does not increase availability from normal client requests. See Chapter 9.

58. **C** is correct. A full/incremental backup strategy is the best option with one full backup on one day and incremental backups on the other days. The incremental backups will take a relatively short time compared with the other methods. A full backup every day would require the most time every day. Differential backups become steadily larger as the week progresses and take more time to back up than incremental backups. Backups must start with a full backup, so a differential/incremental backup strategy is not possible. See Chapter 9.

59. **B** is correct. A business impact analysis (BIA) includes information on potential monetary losses along with information on essential and critical functions, recovery plans, and more. It is the most likely document of those listed that would include this information. A business continuity plan (BCP) includes a BIA, but the BIA is more likely to include this information than the BCP. The mean time between failures (MTBF) provides a measure of a system's reliability. The recovery point objective (RPO) refers to the

amount of data you can afford to lose, but it does not include monetary losses. See Chapter 9.

60. **A** is correct. The recovery time objective (RTO) identifies the maximum amount of time it should take to restore a system after an outage. The recovery point objective (RPO) refers to the amount of data you can afford to lose. RTO only refers to time, not data. RPO refers to data recovery points, not time to restore a system. See Chapter 9.

61. **A** is correct. The mean time to recover (MTTR) identifies the average time (the arithmetic mean) it takes to restore a failed system and is commonly used when preparing a business impact analysis (BIA). The mean time between failures (MTBF) identifies the average (the arithmetic mean) time between failures. The single loss expectancy (SLE) identifies the cost of any single loss. The annual rate of occurrence (ARO) identifies how many times a loss is expected to occur in a year. Multiplying SLE * ARO identifies the annual loss expectancy (ALE). See Chapter 9.

62. **B** is correct. Encryption is used to maintain confidentiality of any data, including Personally Identifiable Information (PII) with encryption. Hashes provide integrity, not confidentiality. A digital signature provides authentication, non-repudiation, and integrity. A redundant array of inexpensive disks (RAID) provides higher availability for a disk subsystem. See Chapter 10.

63. **A** is correct. A digital signature provides assurances of who sent an email and meets the goal of this scenario. Although a spam filter might filter a spear phishing attack, it does not provide assurances about who sent an email. Role-based training provides targeted training for employees based on their roles, but any type of training wouldn't provide assurances about who sent an email. Some antivirus software includes heuristic-based detection. Heuristic-based detection attempts to detect viruses that were previously unknown and do not have virus signatures. See Chapter 10.

64. **A** is correct. Of the given choices, the file was most likely infected after it was pushed out to the server. This is because the hash of the file is

different on the server than it is on the patch management system. The scenario doesn't indicate what type of infection the malware has, so it isn't possible to tell if it is crypto-malware or another type of malware. A blacklist blocks files so if the file were listed in the patch management system's blacklist, the patch management system wouldn't push it out to systems.

If it were infected before it was pushed out to the server, it would have the same hash. See Chapter 10.

65. **D** is correct. Hiding data within data is one way to support a use case of supporting obfuscation and Tony is attempting to send the text files within the image file to obscure his intent. In this scenario, Tony is using steganography to hide the files within the image, but that is the method, not the purpose. Hashing methods and digital signatures support integrity. Redundancy and fault-tolerance methods increase availability supporting resiliency. See Chapter 10.

66. **E** is correct. A Digital Signature Algorithm (DSA) is used to create a digital signature and they would sign their emails with a digital signature. A certificate revocation list (CRL) is a list of revoked certificates. Online Certificate Status Protocol (OCSP) is an alternative to a CRL and provides a real-time response indicating the validity of a certificate. The certificate signing request (CSR) is used to request a certificate. A certificate authority (CA) manages certificates and would sign certificates issued to users. A certificate is needed to create a digital signature, but the certificate itself can't sign an email. See Chapter 10.

67. **C** is correct. Online Certificate Status Protocol (OCSP) stapling reduces OCSP traffic sent to a certificate authority (CA). Certificate presenters append a timestamped, digitally signed OCSP response to a certificate. Public key pinning includes a list of public key hashes in HTTPS responses from the web server. While pinning helps validate certificates, it is unrelated to OCSP. Neither digital signatures (used for non-repudiation) nor hashing (used for integrity) will reduce OCSP traffic. See Chapter 10.

68. **D** is correct. A certificate revocation list (CRL) provides the best solution in this scenario. After a CRL is retrieved, systems hold a copy of it in cache. Instead of downloading the same CRL every time a system needs to validate a certificate, they just look at the cached copy of the CRL. Online Certificate Status Protocol (OCSP) is an alternative to a CRL and provides a real-time response to validate certificates. Because OCSP responds in real time, it is susceptible to Internet outages. Privacy enhanced mail (PEM) certificates are not used to validate other certificates. A subject alternative name (SAN) certificate is used for multiple domains that have different names but are owned by the same organization. See Chapter 10.

69. **C** is correct. This recommendation enforces the separation of duties principle, which prevents any individual person from performing multiple job functions that might allow the person to commit fraud. Discretionary access control specifies that every object has an owner but doesn't separate duties. Devices such as routers use a rule-based access control model, but it doesn't separate duties. Job rotation policies rotate employees into different jobs, but they don't necessarily separate job functions. See Chapter 11.

70. **D** is correct. Offboarding is the process of removing an employee's access when he leaves the organization, and this is typically done during the exit interview. Because the employee deleted the files and shares after he left the organization, it indicates offboarding processes were not performed. Onboarding is the process of granting appropriate access to employees when they are first hired. Time-of-day restrictions might have prevented the employee from accessing resources during the weekend while the organization was closed. However, there isn't any indication that the organization wanted to restrict employees from accessing resources during off-hours. An account audit might have identified the account but not as quickly as offboarding processes done during an exit interview. Additionally, audits are typically done periodically, such as monthly. See Chapter 11.

71. **D** is correct. When a system reaches its end of life (EOL), a vendor no longer offers it for sale, and the vendor stops releasing updates for it. This scenario indicates management has weighed the risks and decided to keep

the application. While not available as a possible answer, end of service life (EOSL) would be more specific. EOSL is the date when a vendor no longer supports a product and would no longer create patches or upgrades. The other answers are unrelated to the question. Measurement systems analysis (MSA) evaluates processes and tools used to make measurements. An acceptable use policy (AUP) defines proper system usage for employees when using IT systems. A managed security service provider (MSSP) is a third-party vendor that provides security services for smaller companies. See Chapter 11.

72. **B** is correct. At this stage, the first response is incident identification. The preparation phase is performed before an incident and includes steps to prevent incidents. After identifying this as a valid incident (malware infection), the next steps are containment, eradication, recovery, and lessons learned. See Chapter 11.

73. **C** is correct. After identifying an incident, the next step is containment. The scenario indicates you have identified the incident as a malware infection. Preparation is the first step in an incident response process. Eradication attempts to remove all elements of the incident after first containing it. The last two steps in the incident response process are recovery and lessons learned. See Chapter 11.

74. **B** is correct. A chain of custody was not maintained because the hard drive was left unattended for several hours before capturing an image. Witnesses were not mentioned but are not needed for the hard drive if the chain of custody was maintained. The order of volatility does not apply here, but the hard drive is not volatile. Analysis would occur after capturing an image, but there isn't any indication it wasn't done or wasn't complete. See Chapter 11.

75. **D** is correct. The court order specified a legal hold on email from the last three years, so all the backups for the last three years should be kept. If the backups had been destroyed before the court order, they wouldn't be available, so the legal hold wouldn't apply to them. Deleting them after the

court order is illegal. Protecting only the backups from the last 12 months or the last two years doesn't comply with the court order. See Chapter 11.