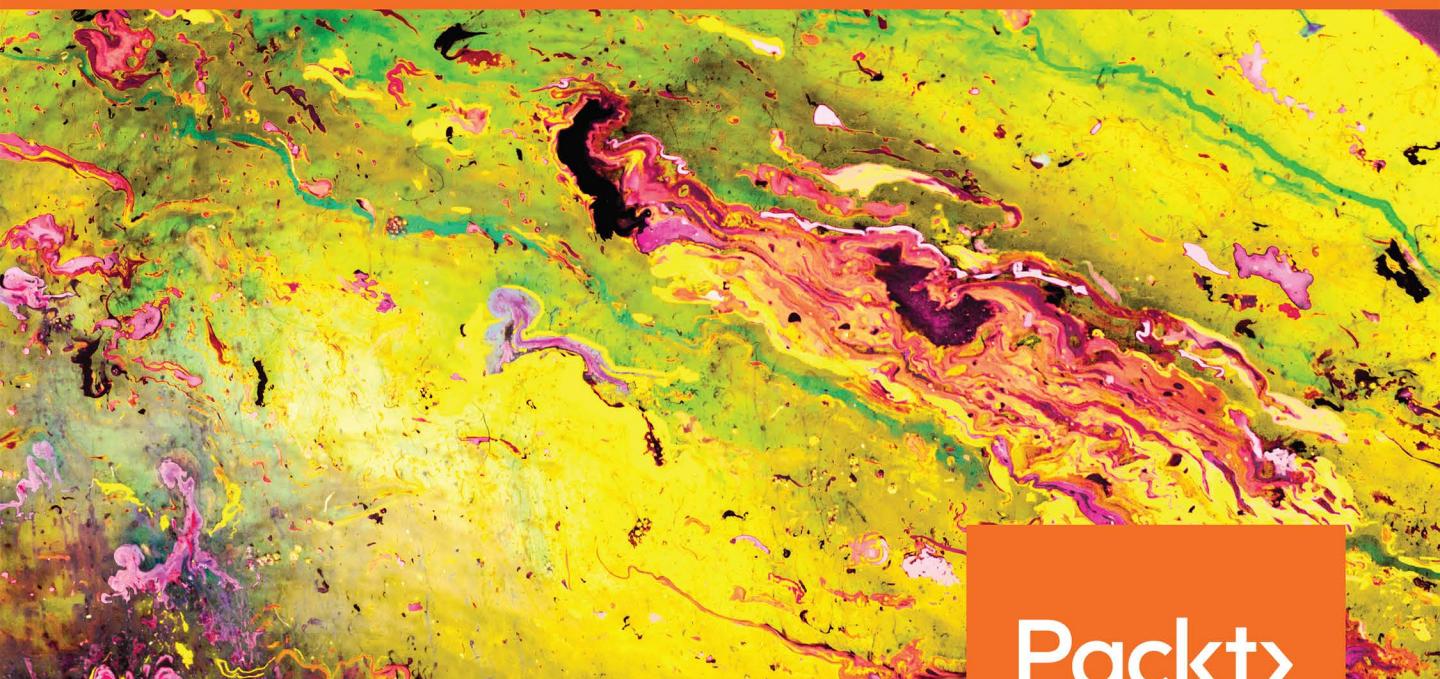


Security+® Practice Tests

Prepare for, practice, and pass the CompTIA Security+ exam



Packt

www.packt.com

Mike Chapple

Security+® Practice Tests

Prepare for, practice, and pass the CompTIA
Security+ exam

Mike Chapple

Packt®

Security+® Practice Tests

Copyright © 2018 Mike Chapple. All rights reserved.

No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without prior written permission, except in the case of brief quotations embedded in critical articles or reviews.

The information contained in this book is sold without warranty, either express or implied. Neither the authors, nor Packt Publishing, and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Author: Mike Chapple

Managing Editor: Snehal Tambe

Acquisitions Editor: Bridget Neale

Production Editor: Samita Warang

Editorial Board: Shubhopriya Banerjee, Bharat Botle, Ewan Buckingham, Megan Carlisle, Simon Cox, Mahesh Dhyani, Manasa Kumar, Alex Mazonowicz, Dominic Pereira, Shiny Poojary, Abhishek Rane, Erol Staveley, Ankita Thakur, Nitesh Thakur, and Jonathan Wray

First Published: October 2019

Production Reference: 1301019

ISBN: 978-1-83921-346-5

Published by Packt Publishing Ltd.

Livery Place, 35 Livery Street

Birmingham B3 2PB, UK

Get Certified!



Security +



CySA +



CISSP



SSCP



PenTest+



A black and white photograph of Mike Chapple, a man with short brown hair, smiling. He is wearing a dark suit jacket, a light-colored shirt, and a tie. To his left is a graphic element consisting of a circular seal with a scalloped edge. Inside the seal, the word "CertMike" is written in a bold, sans-serif font, with a registered trademark symbol (®) to the right. Below "CertMike", the words "PREPARE, PRACTICE, PASS!" are written in a smaller, all-caps font. The background behind him is a gradient from light to dark grey.

**90 Days To Your
Security Certification**

Mike Chapple offers **FREE ONLINE STUDY GROUPS** that complement this book and will help prepare you for your security certification.

Visit CertMike.com to learn more!

Table of Contents

Introduction	i
Preface	xii
Chapter 1: Threats, Attacks, and Vulnerabilities	1
Domain 1 Questions	2
Domain 1 Answers and Explanations	35
Chapter 2: Technologies and Tools	51
Domain 2 Questions	52
Domain 2 Answers and Explanations	85
Chapter 3: Architecture and Design	101
Domain 3 Questions	102
Domain 3 Answers and Explanations	132
Chapter 4: Identity and Access Management	149
Domain 4 Questions	150
Domain 4 Answers and Explanations	180
Chapter 5: Risk Management	195
Domain 5 Questions	196
Domain 5 Answers and Explanations	224
Chapter 6: Cryptography and PKI	241
Domain 6 Questions	242
Domain 6 Answers and Explanations	265

Chapter 7: Practice Exam 1 **277**

Practice Exam 1 Questions 278

Practice Exam 1 Answers and Explanations 310

Chapter 8: Practice Exam 2 **325**

Practice Exam 2 Questions 326

Practice Exam 2 Answers and Explanations 355

Introduction

Welcome to **Security+® Practice Tests!** I've prepared these practice tests to help you prepare for the CompTIA Security+ exam and hope that you find them a useful aid as you get ready for test day.

What's in This Book?

In this book, you'll find over 700 practice exam questions written using the style and format of the Security+ exam. I've organized the book in a manner designed to help you study effectively. The first six chapters each cover one of the six Security+ domains. Each of those chapters contains 100 practice test questions covering the material from that domain. *Chapter 7, Practice Exam 1* and *Chapter 8, Practice Exam 2* each contain a full-length Security+ practice test that's designed to assess your readiness to take the actual test.

At the end of each chapter, you'll find the answers to all of the questions along with detailed explanations to help reinforce your learning of the material.

What Is Security+ Certification?

Security+ certification is the most popular entry-level certification for cybersecurity professionals. It covers foundational knowledge for the field and has no work experience requirements, making it accessible to anyone who is willing to put in the time to prepare for the exam. Sponsored by the Computing Technology Industry Association (CompTIA), the Security+ exam covers six domains of crucial cybersecurity knowledge:

- Threats, Attacks, and Vulnerabilities
- Technologies and Tools
- Architecture and Design
- Identity and Access Management
- Risk Management
- Cryptography and Public Key Infrastructure

Today, employers and IT professionals around the world recognize Security+ as a premier certification program that allows candidates to demonstrate a breadth of knowledge in cybersecurity that prepares them for a career in the field.

The Security+ Exam Environment

You'll take the computer-based Security+ exam at a Pearson Vue testing center (<https://home.pearsonvue.com>), probably not far from your home or office. These centers, typically located in office buildings and strip malls, are nondescript locations that conduct testing for a wide variety of programs. You might find yourself sitting for the exam wedged in between a healthcare professional taking a nursing exam and a student tackling a graduate school admissions test.

When you arrive at the test center, you'll go through a check-in process at the front desk where the exam staff will check your identification, take your photograph, and electronically capture your signature. After all, this is an information security exam. You didn't expect to get away without multifactor authentication, did you?

Speaking of identification, you'll need to bring two forms of identification along with you to the exam. You will not be admitted to the exam without them. Your primary identification must be a government-issued identification card that contains both a photo and a signature. For example, you might use:

- A driver's license
- A national or state-issued identification card

- A learner's permit (if it contains a photo and signature)
- A passport
- A military identification card
- An alien registration card

If you have two items on that list, you're good to go. If you can only come up with one of those items, you may use any other form of identification for your second source. Any form of identification that you use must be current – not expired – and contain your name and either a photo or a signature. The first and last names on your identification must exactly match the first and last names on your test registration. If you recently changed your name, you must bring proof of a legal name change with you to the testing center.

After completing the identification process, you may have to wait a short time until your testing station is ready for use. Once it's time to sit the exam, you'll be asked to use a locker to store any personal items that aren't allowed in the exam room and then shown to the system where you will take the exam.

The testing software used for the Security+ exam is the same software used for many exams administered by Pearson. You'll have up to 90 minutes to navigate through the exam and you are allowed to return to previous items and make as many passes through the questions as you like during that time. Here's a screenshot of the Pearson software to give you a feel for it:

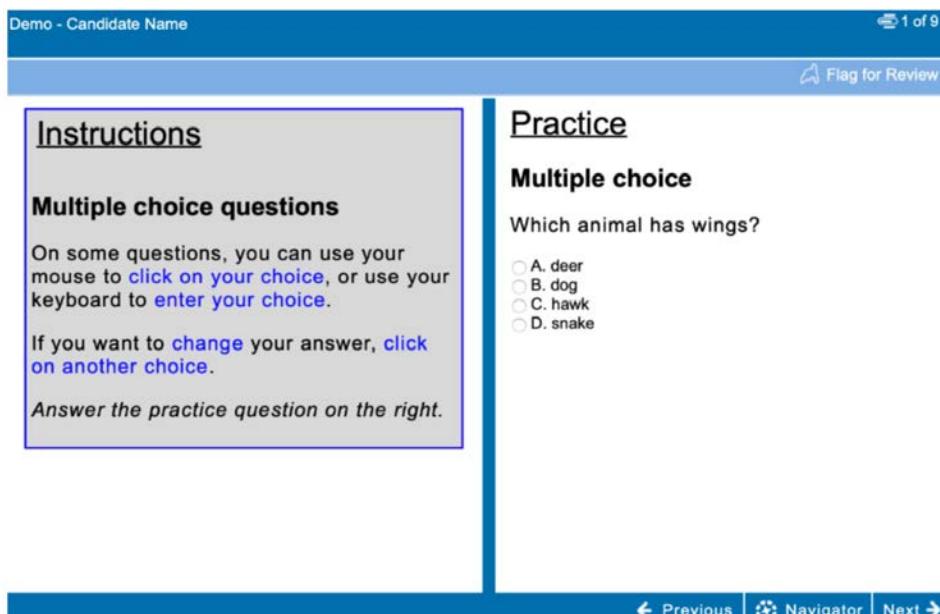


Figure 1: Pearson Vue testing software

If you have any questions or technical difficulties during the exam, raise your hand and a proctor will assist you. The test center proctors administer many different types of exams and have no specialized knowledge of information security. They can help you with the software, but they cannot and will not discuss any exam questions with you.

You may take breaks at your own discretion during the exam but the clock will not stop. You may leave the testing room but you may not leave the testing center during your break. You also may not open your locker and access any of your belongings. If you leave the room, the proctor will reverify your identity before allowing you to return.

When you complete the exam, you'll check out at the front desk and the exam proctor will give you a score report indicating whether you passed the exam. CompTIA will also send you an official notification of your results via email:



CompTIA Security+ Certification Exam Score Report SY0-401

CANDIDATE: MICHAEL J CHAPPLE
CANDIDATE ID: [REDACTED]
REGISTRATION NUMBER: [REDACTED]

EXAM: CompTIA Security+ Certification Exam

DATE: 8/7/15
SITE NUMBER: 45283

PASSING SCORE: 750
CANDIDATE SCORE: 850
PASS/FAIL: Pass

The CompTIA Security+ Certification Exam has a scaled score between 100 and 900.

You incorrectly answered one or more questions in the following objective areas:

- 1.2 Given a scenario, use secure network administration principles.
- 2.1 Explain the importance of risk related concepts.
- 2.4 Given a scenario, implement basic forensic procedures.
- 3.6 Analyze a scenario and select the appropriate type of mitigation and deterrent techniques.
- 3.7 Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities.
- 6.1 Given a scenario, utilize general cryptography concepts.
- 6.2 Given a scenario, use appropriate cryptographic methods.

For a complete listing of CompTIA Security+ Certification Exam objectives, please visit certification.comptia.org.

Figure 2: CompTIA Score Report

Security+ Question Types

The Security+ exam contains two different types of questions: standard multiple-choice questions and some specialized performance-based questions. Let's take a look at each of these categories.

The multiple-choice questions are usually pretty straightforward. For most of them, you'll simply be presented with a fact-based question, such as the one shown in Figure 1, and asked to choose the correct answer from four possible choices.

The second type of question you'll face is the performance-based exam question. On some CompTIA exams, such as the A+ exam, you might be asked to perform a task on a simulated computer system. Fortunately, the Security+ exam doesn't currently include these tasks. Instead, you'll find questions where you're asked to drag items into the right order, sort things by category, indicate different components on a network diagram, or perform similar, vendor-agnostic tasks. Figure 3 shows an example of one of these performance-based questions:

Demo - Candidate Name
7 of 9

Flag for Review

Instructions

Drag-and-drop questions

On some questions you will **drag answers** to new locations.

Click on an answer, then **drag it to the location** of your choice and **drop** it there.

Sometimes, a copy of the answer will still be in its starting place. On these questions, you can **drag another copy** of the answer.

Repeat these steps for **each** answer you wish to move.

To change an answer, **drag an answer to another location**, or **drag the answer back** to its starting place.

Answer the practice question on the right.

Practice

Drag-and-drop

Place the following letters in alphabetical order from left to right.

← Previous
Navigator
Next →

Figure 3: Performance-based test question

When answering exam questions, remember to use solid test-taking strategies. Here are a few pointers for you.

First, read the question very carefully. Pay attention to exactly what the question is asking and remember that one or more of the wrong answers may be based upon common misinterpretations of the question. Don't get tricked by the exam because you didn't read the question closely enough!

Second, read all of the answer choices before you commit to the correct one. If you're unsure of the answer, try to eliminate one or more of the answers that you think are obviously incorrect. If you can eliminate two of the answer choices, you just improved your odds from 1 in 4 to 50/50.

Third, answer every question, even if you have no idea what the question is asking you. There is no penalty for guessing, so you might as well answer each one.

Fourth, the exam software offers you the ability to move back and forth between questions and revisit those that you're unsure of. Additionally, you can mark questions that you'd like to review later. Be sure to use this feature. If you're not confident in your answer, go back later and give it another read.

Finally, make at least three passes through the exam during your 90 minutes. Taking a quick first run through the exam and knocking out the easy questions will build your confidence and help you get a feel for the contents of the entire exam. I've heard from many test-takers that they've encountered exams where all of the performance-based questions appeared at the beginning of the exam. If you don't do a quick pass through the entire exam, you might become very discouraged because these questions tend to be more difficult. It's absolutely fine to just skip them entirely during your first pass.

During your second run-through, try to answer every question on the exam. Finally, your third pass through the exam will help you clean up any errors you made.

Answering other questions during the first and second passes might also jog your memory and help you answer questions that were sticking points earlier.

Following my Security+ preparation process

You're welcome to use this book however you'd like. If you're sitting for the exam soon, you might want to skip right to the full-length practice tests found in *Chapter 7, Practice Exam 1* and *Chapter 8, Practice Exam 2* and use them to zero in on areas where you need to study up before the exam.

On the other hand, if you're just getting started with your Security+ certification journey, I encourage you to use a variety of resources as you prepare for the exam. I've created a video course series on LinkedIn Learning (<https://www.linkedin.com/learning/patterns/become-a-comptia-security-plus-certified-security-professional>) that walks through all of the knowledge you'll need to pass the exam.

I also recommend the Security+ Study Guide by Darril Gibson (<https://www.amazon.com/CompTIA-Security-Certified-Ahead-SY0-401/dp/1939136024/>) as a companion reference as you prepare for the exam. Finally, make sure that you have a copy of my CertMike Security+ Last Minute Review Guide (<https://app.simplegoods.co/i/JBASPD?ref=PTbook>). It's less than ten bucks and provides all of the crucial knowledge that you should review the night before the exam.

Your Free Bonus: Join My Security+ Study Group

I've helped thousands of students earn their Security+ certifications and I've learned quite a bit about test preparation along the way. I've put together a step-by-step process that guides you through the study process week by week, using a combination of this book, my video course series, and Darril's study guide.

As a small token of my thanks for buying this book, I'd like to offer you a free bonus gift. Visit my website at <https://www.certmike.com/> and sign up for my free Security+ Study Group (<https://www.certmike.com/securityplus>). I'll email you new assignments each week along with some extra exam tips and practice test questions. You'll get weekly reminders from me that will walk you through the Security+ exam preparation process, step-by-step. You'll also get the opportunity to interact with other technology professionals who are also preparing for the exam.

The assignments I provide are in a convenient checklist format that guides you through the week. Here's an example of a checklist from the course:

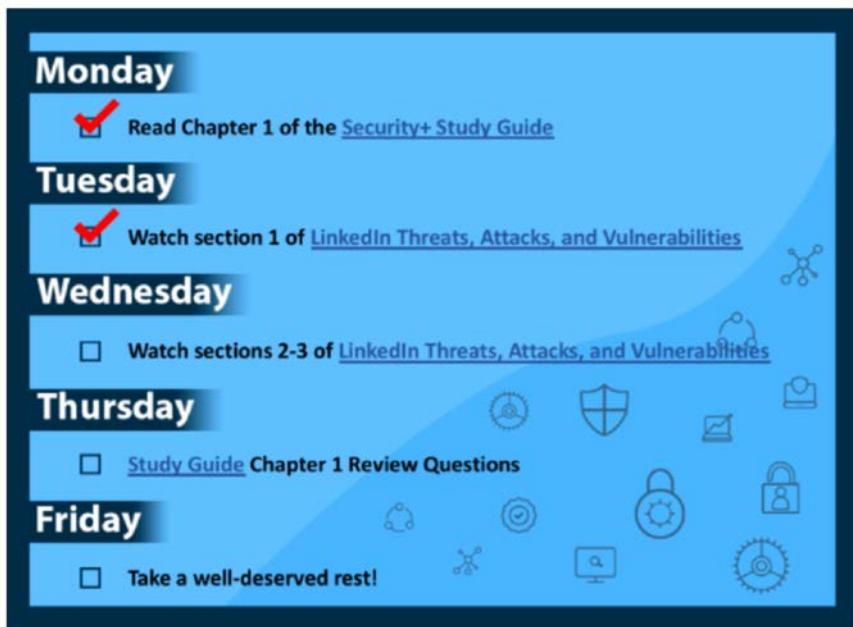
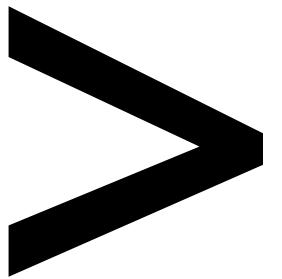


Figure 4: Sample CertMike Study Group checklist

If you sign up for the free study group, I'll email you a new checklist every Monday. If you'd prefer to follow the checklists at your own pace, you'll find a complete set in Appendix A.



Preface

About

This section briefly introduces the authors, the coverage of this book, the technical skills you'll need to get started.

About the Book

Security+ certification is the most popular entry-level certification for cybersecurity professionals. It has no work experience requirement, making it accessible to anyone willing to put in the time to prepare for the exam. Security+® Practice Tests is the perfect tool to prepare for the CompTIA Security+ exam.

The first six chapters each cover one of the six Security+ domains. Each of these chapters contains around 100 practice test questions covering the material from that domain. The final two chapters each contain a full-length Security+ practice test that's designed to assess your readiness to take the actual test. At the end of each chapter, you'll find the answers to all of the questions along with detailed explanations to help reinforce your learning of the material.

By the end of the book, you'll have enough practice to easily ace the CompTIA Security+ exam.

About the Author

Mike Chapple holds the CISSP, CySA+, CISM, PenTest+ and Security+ certifications and has helped thousands of students earn their own certifications through his books, courses, and practice tests. On the CISSP front, Mike is the author of the Official (ISC)2 CISSP Study Guide, Official (ISC)2 CISSP Practice Tests and LinkedIn's CISSP video training series. In the Security+ space, Mike developed the LinkedIn Learning Security+ training series. Mike also authored the CySA+ Study Guide from Sybex and is the author of the book CySA+ Practice Tests and the LinkedIn CySA+ video training series. Mike has 20 years of experience as an educator, author, and hands-on practitioner in cybersecurity across the public and private sectors. He began his career as an information security research scientist with the U.S. National Security Agency. Mike then went into private industry as the Chief Information Officer of the Brand Institute. He currently serves as a faculty member at the University of Notre Dame, specializing in cybersecurity and business analytics.

Learning Objectives

By the end of this book, you will be able to:

- Familiarize yourself with the format of the Security+ exam
- Target your test preparation on each of the Security+ domains
- Brush up on your understanding by testing yourself on realistic practice questions
- Discover areas for improvement by comparing your responses to the answers provided
- Measure your readiness with full-length practice tests
- Know what to expect on test day and
- Learn helpful strategies for tackling the different question types

Audience

This book is designed for service desk analysts, system support engineers, and other IT professionals who want to start their career in managing the IT infrastructure of an organization. Basic knowledge of hardware, software and other relevant components of the IT industry will help you easily grasp the concepts explained in this book.

Approach

The questions in this book are written using the style and format of the Security+ exam. The structure of the book enables you to study effectively. At the end of each chapter, you'll find the answers to all of the questions along with detailed explanations to help reinforce your learning of the material.

Conventions

New terms and important words in the book are highlighted in bold as follows:

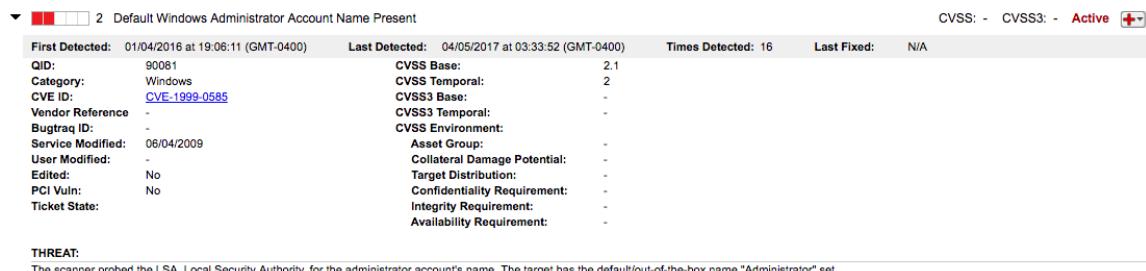
"A **business partnership agreement (BPA)** spells out the relationship between two organizations that are entering into a joint venture or other partnership."

1

Threats, Attacks, and Vulnerabilities

Domain 1 Questions

- After conducting a vulnerability scan of her network, Wendy discovered the issue shown here on several servers. What is the most significant direct impact of this vulnerability?



The screenshot shows a network vulnerability scan result. At the top, there are four colored squares (red, yellow, green, blue) followed by the text "2 Default Windows Administrator Account Name Present". To the right, it says "CVSS: - CVSS3: - Active" with a red warning icon.

First Detected:	01/04/2016 at 19:06:11 (GMT-0400)	Last Detected:	04/05/2017 at 03:33:52 (GMT-0400)	Times Detected:	16	Last Fixed:	N/A
QID:	90081	CVSS Base:	2.1				
Category:	Windows	CVSS Temporal:	2				
CVE ID:	CVE-1999-0585	CVSS3 Base:	-				
Vendor Reference	-	CVSS3 Temporal:	-				
Bugtraq ID:	-	CVSS Environment:	-				
Service Modified:	06/04/2009	Asset Group:	-				
User Modified:	-	Collateral Damage Potential:	-				
Edited:	No	Target Distribution:	-				
PCI Vuln:	No	Confidentiality Requirement:	-				
Ticket State:	-	Integrity Requirement:	-				
		Availability Requirement:	-				

THREAT:
The scanner probed the LSA, Local Security Authority, for the administrator account's name. The target has the default/out-of-the-box name "Administrator" set.

Figure 1.1

- Attackers may eavesdrop on network communications.
Attackers may use this information to gain administrative privileges.
Encryption will not protect credentials for this account.
Automated attacks are more likely to succeed.
- Pete is investigating a domain hijacking attack against his company that successfully redirected web traffic to a third-party website. Which one of the following techniques is the most effective way to carry out a domain hijacking attack?
ARP poisoning
Network eavesdropping
DNS poisoning
Social engineering
- Which one of the following characters is the most important to restrict when performing input validation to protect against XSS attacks?
<
!
\$
'

4. Darren is investigating an attack that took place on his network. When he visits the victim's machine and types www.mybank.com into the address bar, he is directed to a phishing site designed to look like a legitimate banking site. He then tries entering the IP address of the bank directly into the address bar and the legitimate site loads. What type of attack is likely taking place?
 - A. IP spoofing
 - B. DNS poisoning
 - C. ARP spoofing
 - D. Typosquatting
5. Which one of the following technologies must be enabled on a wireless network for a Pixie Dust attack to succeed?
 - A. SSID broadcasting
 - B. WPS
 - C. WPA
 - D. WEP
6. During forensic analysis, Drew discovered that an attacker intercepted traffic headed to networked printers by modifying the printer drivers. His analysis revealed that the attacker modified the code of the driver to transmit copies of printed documents to a secure repository. What type of attack took place?
 - A. Refactoring
 - B. Shimming
 - C. Swapping
 - D. Recoding
7. What type of scan can best help identify cases of system sprawl in an organization?
 - A. Database scan
 - B. Web application scan
 - C. Detailed scan
 - D. Discovery scan

8. Scott is reviewing a list of cryptographic cipher suites supported by his organization's website. Which one of the following algorithms is not secure and may expose traffic to eavesdropping attacks?
 - A. ECC
 - B. 3DES
 - C. AES
 - D. DES
9. Brenda is selecting the tools that she will use in a penetration test and would like to begin with passive techniques. Which one of the following is not normally considered a passive reconnaissance technique?
 - A. Social engineering
 - B. Wireless network eavesdropping
 - C. Open source intelligence
 - D. Domain name searches
10. Scott is a security administrator for a federal government agency. He recently learned of a website that advertises jobs for former government employees. When he accessed the site, the site launched code in his browser that attempted to install malicious software on his system. What type of attack took place?
 - A. Denial of service
 - B. Watering hole
 - C. Spyware
 - D. Trojan horse
11. Paul received an email warning him that a new virus is circulating on the internet and that he needs to apply a patch to correct the problem. The message is branded with a Microsoft header. The virus message is actually a hoax and the patch contains malicious code. What principle of social engineering best describes what the attacker is trying to exploit by including the Microsoft header?
 - A. Consensus
 - B. Scarcity
 - C. Trust
 - D. Intimidation

12. Kristen conducts a vulnerability scan against her organization's network and discovers a file server with the vulnerability shown here. Which one of the following actions is the best way to remediate this vulnerability?

LOW FTP Supports Cleartext Authentication >

Description

The remote FTP server allows the user's name and password to be transmitted in cleartext, which could be intercepted by a network sniffer or a man-in-the-middle attack.

Figure 1.2

- A. Discontinue the file transfer service
 - B. Require strong passwords
 - C. Switch to SFTP
 - D. Require multifactor authentication
13. Frank is the new CISO at a mid-sized business. Upon entering his role, he learns that the organization has not conducted any security training for their sales team. Which one of the following attacks is most likely to be enabled by this control gap?
- A. Buffer overflow
 - B. Social engineering
 - C. Denial of service
 - D. ARP poisoning
14. After conducting security testing, Bruce identifies a memory leak issue on one of his servers that runs an internally developed application. Which one of the following team members is most likely able to correct this issue?
- A. Developer
 - B. System administrator
 - C. Storage administrator
 - D. Security analyst

15. Greg recently detected a system on his network that occasionally begins sending streams of TCP SYN packets to port 80 at a single IP address for several hours and then stops. It later resumes, but directs the packets to a different address. What type of attack is taking place?
 - A. Port scanning
 - B. DDoS
 - C. IP scanning
 - D. SQL injection
16. During a security assessment, Ryan learns that the Accounts Receivable department prints out records containing customer credit card numbers and files them in unlocked filing cabinets. Which one of the following approaches is most appropriate for resolving the security issues this situation raises?
 - A. Physically secure paper records
 - B. Encrypt sensitive information
 - C. Modify business process
 - D. Monitor areas containing sensitive records
17. Jaime is concerned that users in her organization may fall victim to DNS poisoning attacks. Which one of the following controls would be most helpful in protecting against these attacks?
 - A. DNSSEC
 - B. Redundant DNS servers
 - C. Off-site DNS servers
 - D. Firewall rules

18. Irene is reviewing the logs from a security incident and discovers many entries in her database query logs that appear similar to the ones shown here. What type of attack was attempted against her server?

```
SELECT CASE WHEN SUBSTRING(password) = 'a' THEN WAITFOR DELAY  
'00:00:10' ELSE NULL END FROM users WHERE id = 1928 ;  
SELECT CASE WHEN SUBSTRING(password) = 'b' THEN WAITFOR DELAY  
'00:00:10' ELSE NULL END FROM users WHERE id = 1928 ;  
SELECT CASE WHEN SUBSTRING(password) = 'c' THEN WAITFOR DELAY  
'00:00:10' ELSE NULL END FROM users WHERE id = 1928 ;  
SELECT CASE WHEN SUBSTRING(password) = 'd' THEN WAITFOR DELAY  
'00:00:10' ELSE NULL END FROM users WHERE id = 1928 ;
```

Figure 1.3

- A. Error-based SQL injection
 - B. Timing-based SQL injection
 - C. TOC/TOU
 - D. LDAP injection
19. Carl is concerned that his organization's public DNS servers may be used in an amplification attack against a third party. What is the most effective way for Carl to prevent these servers from being used in an amplification attack?
- A. Disable open resolution
 - B. Block external DNS requests
 - C. Block internal DNS requests
 - D. Block port 53 at the firewall
20. What is the purpose of a DNS amplification attack?
- A. Resource exhaustion
 - B. Host redirection
 - C. Record poisoning
 - D. Man-in-the-middle attack

21. Angie is investigating a piece of malware found on a Windows system in her organization. She determines that the malware forced a running program to load code stored in a library. What term best describes this attack?
 - A. DLL injection
 - B. SQL injection
 - C. Pointer dereference
 - D. Buffer overflow
22. Which one of the following threat sources is likely to have the highest level of sophistication?
 - A. Organized crime
 - B. Hacktivist
 - C. APT
 - D. Script kiddie
23. In which of the following types of penetration test does the attacker not have any access to any information about the target environment prior to beginning the attack?
 - A. Grey box
 - B. White box
 - C. Red box
 - D. Black box
24. Bill is securing a set of terminals that are being used to access a highly sensitive web application. He would like to protect against a man-in-the-browser attack. Which one of the following actions would be most effective in meeting Bill's goal?
 - A. Disabling browser extensions
 - B. Requiring multifactor authentication
 - C. Requiring TLS encryption
 - D. Disabling certificate pinning

25. Kevin runs a vulnerability scan on a system on his network and identifies a SQL injection vulnerability. Which one of the following security controls is likely not present on the network?
- TLS
 - DLP
 - IDS
 - WAF
26. Maureen is implementing TLS encryption to protect transactions that are being run against her company's web services infrastructure. Which one of the following cipher suites would not be an appropriate choice?
- AES256-CCM
 - ADH-RC4-MD5
 - ECDHE-RSA-AES256-SHA384
 - DH-RSA-AES256-GCM-SHA384
27. Val runs a vulnerability scan of her network and finds issues similar to the one shown here on many systems. What action should Val take?

SSL Certificate - Self-Signed Certificate

First Detected: 02/16/2015 at 12:59:07 (GMT-0400) Last Detected: 04/05/2017 at 05:08:25 (GMT-0400) Times Detected: 25 Last Fixed: 9.4 [!]

N/A

CVSS

CVSS Base: 9.4 [!] CVSS Temporal: 6.8

CVSS3 Base: CVSS3 Temporal:

CVSS Environment:

Asset Group: -

Metadata:

QID: 38169 Category: General remote services CVSS Base: 9.4 [!] CVSS Temporal: 6.8

CVE ID: - CVSS3 Base: - CVSS3 Temporal: -

Vendor Reference: - CVSS Environment: Asset Group: -

Bugtraq ID: - Collateral Damage Potential: -

Service Modified: 05/24/2009 Target Distribution: -

User Modified: - Confidentiality Requirement: -

Edited: No Integrity Requirement: -

PCI Vuln: Yes Availability Requirement: -

THREAT:

An SSL Certificate associates an entity (person, organization, host, etc.) with a Public Key. In an SSL connection, the client authenticates the remote server using the server's Certificate and extracts the Public Key in the Certificate to establish the secure connection.

The client can trust that the Server Certificate belongs to the server only if it is signed by a mutually trusted third-party Certificate Authority (CA). Self-signed certificates are created generally for testing purposes or to avoid paying third-party CAs. These should not be used on any production or critical servers.

By exploiting this vulnerability, an attacker can impersonate the server by presenting a fake self-signed certificate. If the client knows that the server does not have a trusted certificate, it will accept this spoofed certificate and communicate with the remote server.

Figure 1.4

- Immediately replace all certificates
- Conduct a risk assessment
- No action is necessary
- Replace certificates as they expire

28. Barry would like to identify the mail server being used by an organization. Which one of the following DNS record types identifies a mail server?
- MX
 - A
 - CNAME
 - SOA
29. Gina runs a vulnerability scan of a server in her organization and receives the results shown here. What corrective action could Gina take to resolve these issues without disrupting the service?

Vulnerabilities (4)	
▶ 3 Birthday attacks against TLS ciphers with 64bit block size vulnerability (Sweet32)	port 3389/tcp over SSL CVSS: - CVSS3: - New
▶ 3 SSL/TLS Server supports TLSv1.0	port 3389/tcp over SSL CVSS: - CVSS3: - Active

Figure 1.5

- Update RDP encryption
 - Update HTTPS encryption
 - Disable the network port
 - No action is necessary
30. Carl is a help desk technician and received a call from an executive who received a suspicious email message. The content of the email appears as follows. What type of attack most likely took place?

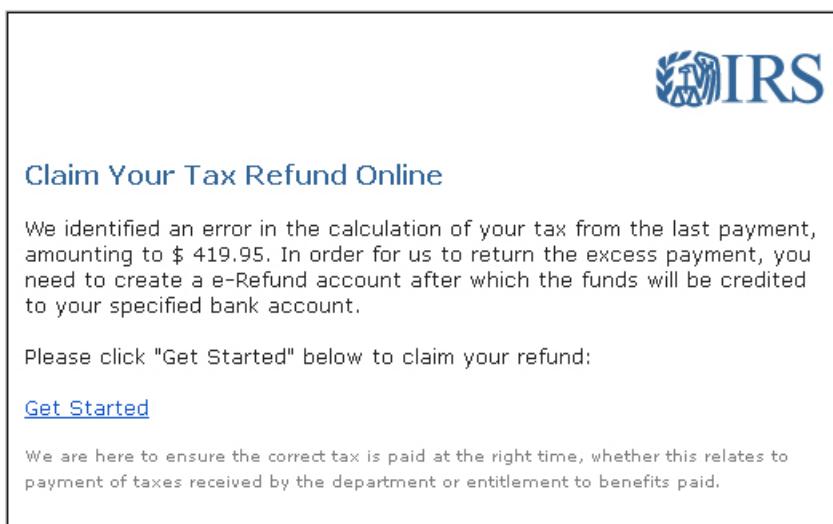


Figure 1.6

- A. Whaling
 - B. Spear phishing
 - C. Vishing
 - D. Phishing
31. Dan is a cybersecurity analyst. Each day, he retrieves log files from a wide variety of security devices and correlates the information they contain, searching for unusual patterns of activity. What security control is likely lacking in Dan's environment?
- A. Firewall management tools
 - B. IPS
 - C. SIEM
 - D. NAC
32. Which one of the following security controls would be MOST effective in combatting buffer overflow attacks?
- A. IDS
 - B. VPN
 - C. DLP
 - D. ASLR
33. Mary believes that her network was the target of a wireless networking attack. Based upon the Wireshark traffic capture shown here, what type of attack likely took place?

```
[+] Frame 981: 26 bytes on wire (208 bits), 26 bytes captured (208 bits)
[+] 802.11 radio information
[+] IEEE 802.11 Deauthentication, Flags: .....C
[+] IEEE 802.11 wireless LAN management frame
```

Figure 1.7

- A. Disassociation
- B. IV accumulation
- C. Replay
- D. Bluesnarfing

34. Gary is concerned about the susceptibility of his organization to phishing attacks. Which one of the following controls will best defend against this type of attack?
- A. Encryption
 - B. User training
 - C. Firewall
 - D. Background checks
35. In which one of the following types of spoofing attack is the attacker often able to establish two-way communication with another device?
- A. Email spoofing
 - B. MAC spoofing
 - C. IP spoofing
 - D. RFID spoofing
36. Rob is conducting a penetration test against a wireless network and would like to gather network traffic containing successful authentication attempts, but the network is not heavily trafficked and he wants to speed up the information gathering process. What technique can he use?
- A. Replay
 - B. Brute force
 - C. Rainbow table
 - D. Disassociation
37. Joe considers himself a hacker but generally does not develop his own exploits or customize exploits that have been developed by others. Instead, he downloads exploits from hacker sites and attempts to apply them to large numbers of servers around the internet until he finds one that is vulnerable. What type of hacker is Joe?
- A. 31337 h4x0r
 - B. APT
 - C. Script kiddie
 - D. Penetration tester

38. Julie is beginning a penetration test against a client and would like to begin with passive reconnaissance. Which one of the following tools may be used for passive reconnaissance?
- A. Metasploit
 - B. Nmap
 - C. Nessus
 - D. Aircrack-ng
39. Jake is responsible for the security of his organization's digital certificates and their associated keys. Which one of the following file types is normally shared publicly?
- A. PEM file
 - B. CRT file
 - C. CSR file
 - D. KEY file
40. Which one of the following malware tools is commonly used by attackers to escalate their access to administrative privileges once they have already compromised a normal user account on a system?
- A. Bot
 - B. Rootkit
 - C. RAT
 - D. Logic bomb

41. Paul has detected the vulnerability shown here in one of his systems. He has several other high priority projects waiting for his attention and needs to prioritize this issue. What should he do?

Vulnerabilities (1)

1 Non-Zero Padding Bytes Observed in Ethernet Packets

	CVSS: -	CVSS3: -	Active
First Detected: 02/04/2017 at 19:40:46 (GMT-0400)	Last Detected: 04/04/2017 at 19:46:13 (GMT-0400)	Times Detected: 3	Last Fixed:
N/A	0	0	-
QID: 82048	CVSS Base:	CVSS Temporal:	0
Category: TCP/IP	CVSS3 Base:	CVSS3 Temporal:	-
CVE ID: -	CVSS Environment:	CVSS3 Environment:	-
Vendor Reference: -	Asset Group:	Collateral Damage Potential:	-
Bugtraq ID: -	Target Distribution:	Confidentiality Requirement:	-
Service Modified: 05/26/2009	Integrity Requirement:	Integrity Requirement:	-
User Modified: -	Availability Requirement:	Availability Requirement:	-
Edited: No			
PCI Vuln: No			
Ticket State:			

THREAT:
Ethernet standards impose strict limitations on the size of encapsulated packets, requiring small packets to be padded up to a minimum size using zero padding bytes (for example, 0x00).
The service detected that the small packets from the host were padded to the minimum size using non-zero padding bytes, as shown in the Results section.

IMPACT:
This weakness may be exploited to fingerprint the Ethernet cards and device drivers.

SOLUTION:
Contact the vendor of the Ethernet cards and device drivers for the availability of a patch.

Figure 1.8

- A. Immediately prioritize the remediation of this vulnerability over all other tasks.
- B. Take no action.
- C. Complete the pressing tasks on his current projects and then correct this vulnerability.
- D. Hire a vendor to remediate the vulnerability.
42. Gary recently gained access to a salted and hashed password file from a popular website and he would like to exploit it in an attack. Which one of the following attacks would be most productive if the website has a password policy requiring complex passwords?
- A. Offline brute force
- B. Online brute force
- C. Dictionary
- D. Rainbow table

43. Vivian is investigating a website outage that brought down her company's e-commerce platform for several hours. During her investigation, she noticed that the logs are full of millions of connection attempts from systems around the world, but those attempts were never completed. What type of attack likely took place?
- A. Cross-site scripting
 - B. DDoS
 - C. DoS
 - D. Cross-site request forgery
44. In which one of the following attacks against Bluetooth technology is the attacker able to steal information from the device?
- A. Blueballing
 - B. Bluejacking
 - C. Bluesnarfing
 - D. Bluefeeding
45. What is the most dangerous consequence that commonly occurs as the result of a buffer overflow attack?
- A. Account enumeration
 - B. Denial of service
 - C. Information disclosure
 - D. Arbitrary command execution
46. Which one of the following would not be considered an OSINT tool?
- A. Website perusal
 - B. WHOIS lookups
 - C. Google searches
 - D. Vulnerability scans
47. Which one of the following is not a likely consequence of system sprawl?
- A. Improper input validation
 - B. Undocumented assets
 - C. Excess costs
 - D. Unsupported systems

48. Tonya is developing a web application and is embedding a session ID in the application that is exchanged with each network communication. What type of attack is Tonya most likely trying to prevent?
- A. Man-in-the-middle
 - B. Replay
 - C. Buffer overflow
 - D. SQL injection
49. Carla found the following page on her web server. What type of attacker most likely waged this attack?



Figure 1.9

Note

The above question is included as an example of a security attack. The publisher does not endorse the political message conveyed by the image, nor wish to cause any offence.

- A. Hactivist
- B. APT
- C. Script kiddie
- D. Organized crime

50. Which one of the following attackers is most likely to understand the design of an organization's business processes?
- A. Script kiddie
 - B. APT
 - C. Insider
 - D. Hacktivist
51. Kevin is configuring a vulnerability scan of his network. He would like the scan to be a non-intrusive scan and is using the configuration settings shown here. Which setting should he modify?

The screenshot shows the 'General Settings' section of the Nessus configuration interface. It contains three checkboxes:

- Enable safe checks
- Stop scanning hosts that become unresponsive during the scan
- Scan IP addresses in a random order

Below this is a 'Performance Options' section with several settings:

- Slow down the scan when network congestion is detected
- Network timeout (in seconds)
- Max simultaneous checks per host
- Max simultaneous hosts per scan
- Max number of concurrent TCP sessions per host
- Max number of concurrent TCP sessions per scan

At the bottom is a 'Debug Settings' section with two checkboxes:

- Log scan details
Logs the start and finish time for each plugin used during a scan to nessusd.messages.
- Enable plugin debugging
Attaches available debug logs from plugins to the vulnerability output of this scan.

Figure 1.10

- A. Enable safe checks.
- B. Stop scanning hosts that become unresponsive during the scan.
- C. Scan IP addresses in a random order.
- D. Slow down the scan when network congestion is detected.

52. Frank is responsible for administering his organization's domain names. He recently received a message from their registrar indicating that a transfer request was underway for one of their domains, but Frank was not aware of any request taking place. What type of attack may be occurring?
- A. DNS spoofing
 - B. IP spoofing
 - C. Domain hijacking
 - D. ARP spoofing
53. Morgan is a web developer who's responsible for implementing an authentication system. She knows that she should store hashed versions of passwords rather than the passwords themselves but chooses to use unsalted passwords. What type of attack does this make the application more susceptible to?
- A. Offline brute force attack
 - B. Online brute force attack
 - C. Rainbow table
 - D. Collision
54. Kelly detected an attack on her network where the attacker used aircrack-ng to create a wireless network bearing her company's SSID. The attacker then boosted the power of that access point so that it was the strongest signal in an executive office area, prompting executive devices to connect to it. What type of attack took place?
- A. Bluesnarfing
 - B. Jamming
 - C. Evil twin
 - D. WPS
55. Which one of the following attributes is NOT a characteristic of APT attackers?
- A. Patience
 - B. Large amounts of money
 - C. Sophisticated exploits
 - D. Brute force

56. Which one of the following security controls is most effective against zero-day attacks?
- A. Vulnerability scans
 - B. Signature-based antivirus software
 - C. Application control
 - D. Intrusion prevention systems
57. Chris is investigating a security incident at his organization where an attacker entered the building wearing a company uniform and demanded that the receptionist provide him access to a network closet. He told the receptionist that he needed to access the closet immediately to prevent a major network disaster. Which one of the following principles of social engineering did the attacker NOT exploit?
- A. Consensus
 - B. Authority
 - C. Intimidation
 - D. Urgency
58. Ann works for an organization that recently opted to discontinue the support service on their network devices to control costs. They realized that it would be less expensive to replace devices when they fail than to use the costly replacement plan that was included in their support contract. What should be Ann's primary concern from a security perspective?
- A. Time required to replace a failed device
 - B. Cost of replacing devices
 - C. Lack of access to vendor patches
 - D. Lack of access to vendor support personnel
59. Which one of the following controls would be LEAST effective against a privilege escalation attack?
- A. HIPS
 - B. Patching
 - C. Data Execution Prevention
 - D. Firewall rule

60. Warren is conducting a penetration test and has gained access to a critical file server containing sensitive information. He is now installing a rootkit on that server. What phase of the penetration test is Warren conducting?
- A. Active reconnaissance
 - B. Persistence
 - C. Escalation of privilege
 - D. Pivot
61. Which one of the following security vulnerabilities is NOT a common result of improper input handling?
- A. DDoS
 - B. SQL injection
 - C. Cross-site scripting
 - D. Buffer overflow
62. What type of access must an attacker have to successfully carry out an ARP poisoning attack against a target?
- A. Access to the target's LAN
 - B. Administrative access on the target's system
 - C. Normal user access on the target's system
 - D. Access to the target's network firewall
63. Which one of the following cryptographic attacks may be used to find collisions in a hash function?
- A. Birthday attack
 - B. Meet-in-the-middle attack
 - C. Man-in-the-middle attack
 - D. Chosen plaintext attack

64. Bob is charged with protecting the service shown here from an attack being waged by Mal. What control would best protect against this threat?

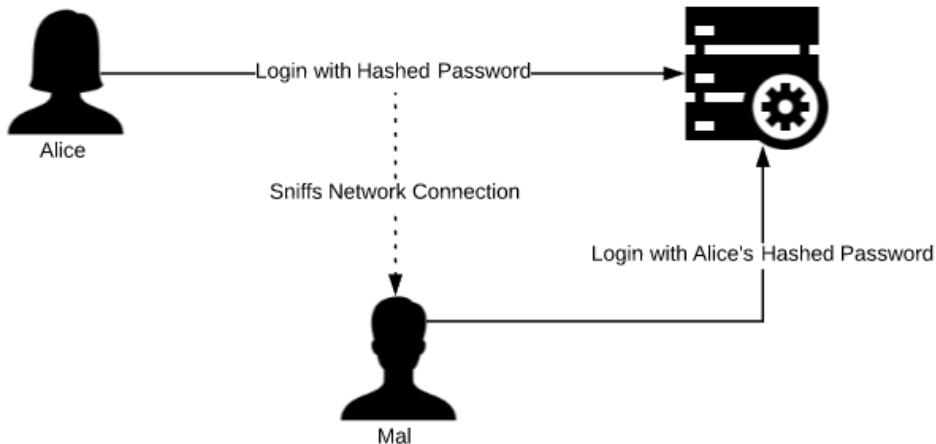


Figure 1.11

- A. Adding TLS encryption
 - B. Changing the hash algorithm
 - C. Changing Alice's password
 - D. Using a shadow password file
65. After running a vulnerability scan, Charlie identified 10 Windows XP systems running on the network. Those systems support critical business hardware that is over 10 years old and it is not possible to replace the hardware. What is the primary issue that Charlie needs to address?
- A. Obsolete operating system
 - B. Incorrectly configured firewall
 - C. Outdated hardware
 - D. User security awareness

66. Patty is approached by an end user who is trying to visit a banking website and sees the following error message. What type of attack is most likely taking place?



Figure 1.12

- A. Social engineering
 - B. This is a routine error and no attack is likely
 - C. Man-in-the-middle
 - D. Certificate pinning
67. During a security review, Terry identified a system that is using the RC4 cipher with a 40-bit key to protect communications between systems using the Remote Desktop Protocol. Which one of the following findings would be appropriate for Terry to include in his report on the risk of this service?
- A. There is not enough information to reach a conclusion.
 - B. The key length is too short and should be increased to 1,024 bits.
 - C. RC4 is an insecure cipher and should not be used.
 - D. The system is using a secure cipher with an appropriate key length.

68. Joan is trying to break a cryptographic algorithm where she has the encryption key but does not have the decryption key. She is generating a series of encrypted messages and using them in her cryptanalysis. Which term best describes Joan's attack?
- A. Known plaintext
 - B. Chosen plaintext
 - C. Chosen ciphertext
 - D. Known ciphertext
69. Kristen is investigating wireless signal interference in her building and suspects that jamming might be taking place. Which one of the following actions can help her rule out the intentional jamming of her wireless signal?
- A. Moving antenna locations
 - B. Changing the Wi-Fi channel
 - C. Changing power levels
 - D. Testing a variety of devices
70. While investigating a security incident, Ryan discovers that the attacker entered the information shown here in the login box for a web application. What type of attack was likely taking place?



The image shows a login interface. At the top, there is a text input field containing the string "comptia)(&". Below it is another text input field containing several dots, indicating a password or sensitive information. At the bottom of the interface is a large, dark blue rectangular button with the word "LOGIN" written in white capital letters.

Figure 1.13

- A. LDAP injection
- B. Blind SQL injection
- C. SQL injection
- D. Cross-site scripting

71. Melanie is designing an authentication scheme for a web application and wishes to protect the site against session hijacking attacks. She would like to ensure that cookies containing session credentials are only sent via encrypted connections. What attribute should she set on cookies that are used for session identification?
- A. Expire
 - B. HttpOnly
 - C. SameSite
 - D. Secure
72. Ken is conducting a penetration test of one of his organization's clients. He gains access to a web server located in the DMZ using a buffer overflow attack and is now attempting to gain access to systems on the internal network. What stage of the attack has Ken reached?
- A. Reconnaissance
 - B. Pivot
 - C. Persistence
 - D. Escalation of privilege
73. Rob is troubleshooting a production application in his organization. He discovers that after the application has been running for about a week, it begins producing repeated errors. When he reboots the system, it works fine for another week, until the errors start recurring. What is the most likely cause of this issue?
- A. Insider attack
 - B. Logic bomb
 - C. Buffer overflow
 - D. Memory leak

74. Vince runs the MD5 hash function against three files on his system. He knows that each of the three files contains log entries from different days. What has occurred?

```
> md5(file1)
fc3b6237c730b6c527856173ff0a1b28

> md5(file2)
dd0e42333f49952523ddf8a33496cf6a

> md5(file3)
fc3b6237c730b6c527856173ff0a1b28
```

Figure 1.14

- A. Use of a secure hash function
 - B. Decryption
 - C. Collision
 - D. Syntax error
75. After running an Nmap scan of a new web server being commissioned on her network, Karen discovered the results shown here. Which port should Karen prioritize for investigation and remediation?

```
Starting Nmap 7.70 ( https://nmap.org ) at 2018-12-05 18:51 EST
Nmap scan report for scan1.certmike (192.168.119.84)
Host is up (0.045s latency).
Not shown: 996 filtered ports
PORT      STATE
22/tcp    open
23/tcp    open
80/tcp    open
443/tcp   open

Nmap done: 1 IP address (1 host up) scanned in 5.10 seconds
```

Figure 1.15

- A. 443
- B. 22
- C. 80
- D. 23

76. The POODLE attack rendered the SSL protocol insecure and prompted many websites to replace SSL with TLS. What type of attack is POODLE?
- A. Disassociation
 - B. Downgrade
 - C. Bluesnarfing
 - D. Evil twin
77. Vince is investigating the compromise of a user's account credentials. The user reports that, in addition to her corporate account, the passwords to many of her online banking and bill payment accounts were also compromised. Vince examines her computer and determines that there is an unusual piece of hardware connected between the keyboard and the computer. What type of attack has most likely taken place?
- A. Bot
 - B. Spyware
 - C. Keylogger
 - D. Adware
78. Larry is evaluating a dynamic web application that uses a web server with a database back end, as shown in the following diagram. The web server is configured to connect to the database server with a database administrative account. Which one of the following statements is correct about this configuration?



Figure 1.16

- A. The web server should use an OS administrator account to connect to the database.
- B. The web server should use a limited privilege account to connect to the database.
- C. This configuration is reasonable.
- D. The web server should not connect directly to the database server.

79. Which one of the following attacks allows the theft of information from a mobile device over a wireless connection that directly connects the attacker to the device?
- A. Bluejacking
 - B. Evil twin
 - C. Bluesnarfing
 - D. Session hijacking
80. In a recent social engineering attack, the attacker found an employee of the target company at his gym and struck up a friendship there for several months before trying to slowly extract sensitive corporate information from the employee. What principle of social engineering is the attacker trying to exploit?
- A. Consensus
 - B. Authority
 - C. Urgency
 - D. Familiarity
81. During a penetration test, the testers sent the following email to a clerk in an organization's Accounts Payable department. What type of attack took place?

----- Forwarded message -----

From: John Lyons <jlyons@yourcompany.com>
Date: Wed, Feb 21, 2018 at 9:29 AM
Subject: Request
To: jsmith@yourcompany.com

Hi Jason,

I hope you are having a pleasant day.

I am currently traveling on business in Europe and need to send an urgent wire transfer to one of our business partners here. What information do you need to process the request? Also, what time would you need to have the information in order to send the money prior to the close of business in Europe today?

I know that this is unusual but appreciate your attending to this right away. It's critical to our relationship with Acme Corp.

Thanks!

John Lyons

President & Chief Executive Office

YourCompany.com

Figure 1.17

A. Spear phishing

B. Whaling

C. Vishing

D. Smishing

82. Which one of the following device types is most susceptible to a pass-the-hash attack?

A. VPN concentrator

B. Network firewall

C. Windows server

D. Hardware security module

83. Vince is concerned about the execution of SQL injection attacks against the database supporting his organization's e-commerce website. Which one of the following controls would NOT be an effective defense against these attacks?

A. Parameterized queries

B. WAF

C. Indexing

D. Stored procedures

84. Norm is concerned that his organization may be the target of a theft of trade secrets by a competitor working with an insider to steal sensitive files. What security control would be the most helpful in detecting attempts to remove that sensitive information from the organization?

A. IPS

B. DLP

C. Firewall

D. TLS

85. Elliott is frustrated by the number of false positive reports being returned by his vulnerability scans. Which one of the following actions is MOST likely to reduce the number of false positive reports?
- A. Implement credentialed scanning
 - B. Decrease the scan's sensitivity
 - C. Disable safe checks
 - D. Increase the size of the target network
86. During a recent security investigation, Cam discovered the device shown here sewn into a briefcase belonging to a senior executive. What type of transmission was most likely used to communicate with this device?



Figure 1.18

- A. Cellular
- B. Bluetooth
- C. Wi-Fi
- D. RFID

87. Dave discovers that a piece of malware running on a system has been loading the feeds of strange Twitter accounts that contain tweets similar to the one shown here. What type of malware likely exists on this system?



Figure 1.19

- A. Trojan horse
 - B. Virus
 - C. Worm
 - D. Botnet
88. Rick would like to use vulnerability scanning results as part of a penetration test he is undertaking. The penetration test is scoped as a black box test. Which one of the following scan reports would be the most useful and appropriate for Rick to obtain from management before conducting the test?
- A. Internal scan report
 - B. External scan report
 - C. Credentialed scan report
 - D. Agent-based scan report
89. After running a vulnerability scan, Carl detects a missing patch on a Windows server. When he investigates the server, he determines that the patch is actually applied. What condition has occurred?
- A. True positive
 - B. False negative
 - C. False positive
 - D. True negative

90. After conducting a vulnerability scan, Kaiden discovers the vulnerability shown here on several of his organization's web servers. What is the most likely direct impact of these vulnerabilities?

MEDIUM Web Application SQL Backend Identification < >

Description
At least one web application hosted on the remote web server is built on a SQL backend that Nessus was able to identify by looking at error messages.

Figure 1.20

- A. An attacker can disrupt access to the web server.
 - B. An attacker can obtain information about the inner functioning of the web application.
 - C. An attacker can steal information from the database supporting this application.
 - D. An attacker can gain administrative access to the web server.
91. Carla noticed unusual spikes in network activity and, upon further investigation, determined that there is an unusually high number of outbound DNS query responses. She also noticed that the query responses are significantly larger than the queries themselves. What type of attack should Carla suspect?
- A. Cross-site scripting
 - B. Amplification
 - C. DNS poisoning
 - D. Pass-the-hash
92. Shortly after Trish's organization fired a software developer, code on a server activated that determined that the developer was no longer employed and deleted the source code from her projects. What type of attack did Trish's organization experience?
- A. Logic bomb
 - B. Trojan horse
 - C. Worm
 - D. RAT

93. Dawn is conducting the reconnaissance phase of a penetration test and would like to identify the registered owner of a domain name. Which one of the following tools would be the most likely to provide her with this information?
- A. Whois
 - B. Nslookup
 - C. Dig
 - D. Ping
94. Which one of the following controls is the most effective way to protect against security-related architectural and design weaknesses?
- A. Deploying intrusion prevention systems
 - B. Carefully maintaining network firewall rules
 - C. Implementing employee background checks
 - D. Including security team members in the project management process
95. Barry is the administrator of a message board that's used by his organization's clients to communicate with each other. One client posted a message on the board that contained script code that caused the browsers of other users to carry out malicious actions when they viewed the message. What type of attack took place?
- A. XSRF
 - B. Reflected XSS
 - C. DOM XSS
 - D. Stored XSS
96. Mal is an attacker associated with an advanced persistent threat (APT) organization. Her team recently discovered a new security vulnerability in a major operating system and has not informed anyone of this vulnerability. What type of attack is Mal's organization in a position to wage?
- A. SQL injection
 - B. Zero-day
 - C. Man-in-the-browser
 - D. Spoofing

97. Which one of the following technologies would be the most useful in preventing man-in-the-middle attacks?
- A. TLS
 - B. SSL
 - C. Digital certificates
 - D. Input validation
98. Harold is examining the web server's logs after detecting unusual activity on the system. He finds the log excerpt shown here. What type of attack did someone attempt against this system based upon the data shown in these logs?

```
10.90.158.182 -- [21/Jan/2018:03:29:56 -0500] "GET /wp-admin HTTP/1.1" 301 241 "-" "Python-urllib/2.7"
10.90.158.182 -- [21/Jan/2018:03:29:56 -0500] "GET /wp-admin/ HTTP/1.1" 302 "-" "Python-urllib/2.7"
10.90.158.182 -- [21/Jan/2018:03:29:56 -0500] "GET /wp-login.php&uid=20%20UNION%20SELECT%201,2
,3,4,5 HTTP/1.1" 200 7255 "-" "Python-urllib/2.7"
10.90.158.182 -- [21/Jan/2018:03:29:56 -0500] "GET / HTTP/1.1" 200 48816 "-" "Python-urllib/2.7"
10.90.158.182 -- [21/Jan/2018:03:29:56 -0500] "GET / HTTP/1.1" 301 "-" "Python-urllib/2.7"
10.196.57.217 -- [21/Jan/2018:03:30:37 -0500] "GET /category/white-papers/feed/ HTTP/1.1" 304
- "https://www.google.com/" "Mozilla/5.0 (Macintosh; U; PPC Mac OS X Mach-0; en-US; rv:1.8.1.7p
re) Gecko/20070815 Firefox/2.0.0.6 Navigator/9.0b3"
```

Figure 1.21

- A. Cross-site scripting
 - B. Domain hijacking
 - C. SQL injection
 - D. Directory traversal
99. Which one of the following attacks exploits a race condition in a software implementation?
- A. Integer overflow
 - B. Buffer overflow
 - C. SQL injection
 - D. TOC/TOU

100. Which one of the following devices is capable of carrying out a rogue AP attack against a Wi-Fi network with minimal configuration?
- A. Switch
 - B. Router
 - C. Orange
 - D. Pineapple
101. Carla's firm is preparing to deploy a large network of Internet of Things sensors. Which one of the following is the least common security concern with IoT deployments?
- A. Data encryption
 - B. Patches to embedded operating systems
 - C. Network segmentation
 - D. Multifactor authentication
102. Hank ran a vulnerability scan of one of his organization's web servers and found the two vulnerabilities shown here. What is the most expedient way for Hank to correct this issue?
- ▶ 3 SSL/TLS use of weak RC4 cipher
 - ▶ 3 SSL/TLS Server supports TLSv1.0
- Figure 1.22
- A. Modify the ciphers used by SSL/TLS
 - B. Upgrade to SSL 3.0
 - C. Upgrade to TLS 1.2
 - D. Replace the digital certificate
103. Mal is engaging in an IP spoofing attack against a target organization over the internet. Which one of the following limitations does the attack have if Mal has complete control of her own network?
- A. Mal will not be able to receive responses to requests.
 - B. Mal will not be able to send packets onto the internet with spoofed addresses.
 - C. Mal will not be able to insert a spoofed IP address into her network traffic.
 - D. Mal will not be able to conduct a denial of service attack.

104. Nate is the first person to arrive in the office one morning and he discovers that a piece of malware is spreading from system to system on his network, exploiting the MS08-067 vulnerability in Microsoft Windows. What term best describes this malware?
- A. Virus
 - B. Trojan horse
 - C. Worm
 - D. Logic bomb
105. Noah is a cybersecurity analyst for a mid-sized business. He is working with the user of a machine that is exhibiting suspicious behavior. The anomalous activity began immediately after the user downloaded and installed software from the internet and Noah suspects that it contained malware. What term best describes the malware in this situation?
- A. Trojan horse
 - B. Virus
 - C. Worm
 - D. Logic bomb

Domain 1 Answers and Explanations

1. D. Most automated attacks assume that a Windows system still contains a default account named Administrator and try to exploit that account. Changing the name makes it less likely that these attacks will stumble upon the account.
2. D. In a domain hijacking attack, the attacker changes the registration of a domain with the registrar. DNS and ARP poisoning attacks may redirect web traffic, but they would do so by providing bogus address information, not by hijacking the domain. Network eavesdropping could theoretically be used to steal credentials that are used to alter information with a registrar, but this is unlikely. The most likely source of a domain hijacking attack is using social engineering with the registrar to gain access to the account being used to manage registration information.
3. A. Cross-site scripting relies upon embedding HTML tags in stored or reflected input. The < and > characters are used to denote HTML tags and should be carefully managed when seen in user input.

4. B. The fact that the legitimate server responds to requests made by an IP address indicates that the attacker is not performing IP spoofing or ARP spoofing. There is no indication that the URL is incorrect, so Darren can rule out typosquatting. The most likely attack in this scenario is DNS poisoning. Darren can verify this by manually changing the system to a different DNS server, clearing the system's DNS cache, and attempting to resolve the name again.
5. B. Pixie Dust attacks are a specialized attack that's used to retrieve the **Wi-Fi Protected Setup (WPS)** PIN code for a network. Pixie Dust attacks will not work if WPS is not enabled on the network.
6. A. The two major categories of attack against device drivers are shimming and refactoring. In a shimming attack, the attacker wraps his or her own malicious code around the legitimate driver. Shimming attacks do not require access to the driver's source code. In a refactoring attack, such as this one, the attacker actually modifies the original driver's source code.
7. D. Discovery scans are designed to identify systems on the network and can be used to detect undocumented assets that are the result of system sprawl.
8. D. The **Data Encryption Standard (DES)** is an outdated, insecure algorithm that should not be used in modern applications. **Triple DES (3DES)** is a secure alternative that uses three rounds of DES encryption. The **Advanced Encryption Standard (AES)** and **Elliptic Curve Cryptosystem (ECC)** are also modern, secure cipher suites.
9. A. Social engineering is an active technique because it involves interaction with the target organization. Attackers may conduct open source intelligence gathering, including domain name searches, using only external resources that will not alert the target organization. Wireless network eavesdropping may also be conducted from a location outside of the organization's facilities without alerting the organization to their presence or interacting with target systems.
10. B. This is an example of a watering hole attack. These attacks place malicious code on a website frequented by members of the target audience. There is not sufficient information to determine whether the malicious code was spyware or a Trojan horse, or whether it delivered a denial of service payload.
11. C. The social engineer is using the Microsoft header in an attempt to exploit the trust that the recipient has for Microsoft. This attack also exploits the principles of authority, familiarity, and urgency. There is no note of scarcity or consensus in the message. The attacker is indeed trying to intimidate the recipient, but the intimidation is contained within the virus hoax message, not the Microsoft header.

12. C. The root cause of this issue is that FTP is an insecure protocol and Kristen can resolve this problem by replacing it with a secure alternative, such as SFTP. Requiring strong passwords or multifactor authentication would not resolve this problem as an attacker could still eavesdrop on those connections and obtain user passwords. Discontinuing the file transfer service would resolve the vulnerability, but it is not a good solution because it would unnecessarily disrupt whatever business processes take place on this server.
13. B. Social engineering attacks depend on user error, and training can dramatically reduce the success rate of these attacks. Buffer overflow attacks, denial of service attacks, and ARP poisoning attacks are not generally preventable by end users and, therefore, training the sales team would not be an effective defense against them.
14. A. A memory leak is a software flaw and, since this is an internally developed application, the developer is the person who's the most likely to be able to correct it. If the issue were in a commercially purchased application, a system administrator may be able to correct the issue by applying a patch, but that is not the case in this scenario.
15. B. This is a clear example of a **distributed denial of service (DDoS)** attack. The system is flooding the target with connection requests, hoping to overwhelm it. The port and IP address are not changing, so this is not indicative of a scanning attack. There is no indication that the connection is completed, so it cannot be a SQL injection attack.
16. C. All of the controls mentioned in this question would improve the security of this scenario. However, the best way to handle sensitive information is to not retain it in the first place. It is unlikely that there is a valid business reason for storing copies of records containing customer credit card information. Therefore, the most appropriate solution would be to modify the business process to avoid this inappropriate data retention.
17. A. DNS poisoning works by injecting false information into a user's local DNS servers. Adding redundant or off-site DNS servers would not reduce the likelihood of a successful attack. Blocking DNS traffic with firewall rules would disrupt the service for legitimate users. The DNSSEC protocol adds a verification layer to ensure that DNS updates come from trusted sources, reducing the likelihood of a successful DNS poisoning attack.
18. B. This is an example of a SQL injection attack because the attacker is inserting his or her own commands into a SQL database query. This particular example is slowing down responses when the answer is correct to ferret out the characters of a password, one by one. That is an example of a timing-based SQL injection attack.

19. A. All of the possible answers have the effect of blocking some DNS requests. The most effective technique to prevent DNS amplification is to disable open resolution so that external users may not make arbitrary recursive requests against the server. Blocking internal requests would have no effect on the attack. Blocking all external requests or blocking port 53 at the firewall would prevent all external requests, preventing the server from fulfilling its purpose as a public DNS server.
20. A. DNS amplification is a denial of service technique that sends small queries with spoofed source addresses to DNS servers, generating much larger, amplified responses back to the spoofed address. The purpose is to consume all of the bandwidth available to the target system, resulting in a resource exhaustion denial of service attack.
21. A. This attack is a DLL injection attack. In a DLL injection, the attacker forces an existing process to load a dynamically linked library that contains unauthorized code.
22. C. **Advanced persistent threats (APTs)** are characterized by a high level of sophistication and significant financial and technical resources. Other attackers, including script kiddies, criminals, and hacktivists, are not likely to have anywhere near the same sophistication as an APT attacker (such as a national government).
23. D. In a black box attack, the attacker does not have access to any information about the target environment before beginning the attack. In a grey box attack, the attacker has limited information. In a white box attack, the attacker has full knowledge of the target environment before beginning the attack.
24. A. In a man-in-the-browser attack, the attacker manages to gain a foothold inside the user's browser, normally by exploiting a browser extension. This gives him or her access to all of the information that's accessed with the browser, regardless of whether the site uses strong authentication or transport encryption (such as TLS). Certificate pinning is a technique that's used to protect against inauthentic digital certificates and would not protect against a man-in-the-browser attack.
25. D. A **web application firewall (WAF)**, if present, would likely block SQL injection attack attempts, making SQL injection vulnerabilities invisible to a vulnerability scanner. A **data loss prevention system (DLP)** does not protect against web application vulnerabilities such as SQL injection. An **intrusion detection system (IDS)** might identify a SQL injection exploit attempt, but it is not able to block the attack. **Transport layer security (TLS)** encrypts web content but encryption would not prevent an attacker from engaging in SQL injection attacks.

26. B. The key to this question is focusing on the encryption algorithms used by each option. Three of the four options use AES 256-bit encryption, which provides strong cryptography. One uses RC4 encryption, which is a weak implementation of cryptography and should be avoided.
27. B. The use of self-signed certificates is not, by itself, cause for alarm. It is acceptable to use self-signed certificates for internal use. Val should conduct a risk assessment to identify whether this use is appropriate and replace any certificates used by external users.
28. A. The MX record identifies the mail server for a domain. A records are used to identify domain names associated with IP addresses, while CNAMEs are used to create aliases. **Start of Authority (SOA)** records contain information about the authoritative servers for a DNS zone.
29. A. These vulnerabilities both relate to the encryption of the service running on port 3389, which is used by the **Remote Desktop Protocol (RDP)**. Upgrading this encryption should resolve these vulnerabilities. There is no indication that an HTTPS service is running on this device. Disabling the network port would disrupt the service. Gina should take action because this is an easily corrected vulnerability.
30. D. This is most likely a straightforward phishing attack. The message is generic and not targeted at a specific user, as you would find in a spear phishing attack. Although the user is an executive, there is no indication that the message was specifically sent to this user because of his status as an executive, so it is not likely to be a whaling attack. The attack was sent over email, not the telephone, so it is not an example of vishing.
31. C. If Dan's organization used a **security information and event management (SIEM)** solution, Dan would not need to gather information from this wide variety of sources. Instead, the SIEM would collect and correlate this information, providing Dan with a single place to review correlated data.
32. D. **Address space layout randomization (ASLR)** is a security technique that randomizes the location of objects in memory, making a buffer overflow attack less likely to succeed. **Virtual private networks (VPN)** provide transport encryption and **data loss prevention (DLP)** systems provide protection against data exfiltration. Neither would be effective against buffer overflow attacks. **Intrusion detection systems (IDS)** may identify a buffer overflow attack but would not prevent it from succeeding.

33. A. The message shown in the capture is a deauthentication message. These messages are often used in disassociation attacks, where the attacker attempts to force the disconnection of a client from a legitimate access point. IV attacks use cryptanalysis on the **initialization vectors (IVs)** that are used in establishing a Wi-Fi session. Replay attacks attempt to reuse credentials captured during a legitimate session to establish unauthorized wireless connections. Bluesnarfing attacks leverage Bluetooth technology, which is not in use in this scenario.
34. B. Phishing is a form of social engineering, and its effectiveness depends upon the susceptibility of users to this type of attack. While some technical controls, such as email content filtering, may be useful against phishing attacks, the most effective defense is user awareness training.
35. B. In a MAC spoofing attack, the local switch is normally fooled into believing the spoofed address and will route reply traffic back to the device spoofing an address. IP spoofing and email spoofing work at the application layer and, in most cases, the attacker will not receive any responses to spoofed messages. RFID spoofing is not a common type of attack.
36. D. Disassociation attacks intentionally disconnect a wireless user from their access point to force a reauthentication that the attacker may collect with a wireless eavesdropping tool. Brute force attacks, rainbow table attacks, and replay attacks do not gather network traffic and, therefore, would not be useful in this scenario.
37. C. Joe is a script kiddie because he does not leverage his own knowledge but merely applies tools written by others. Advanced persistent threats or elite hackers (31337 h4x0r) use sophisticated, customized tools. Joe is not a penetration tester because he does not have authorization to perform the scans.
38. D. Nmap, Nessus, and Metasploit are all active reconnaissance tools that interact with their target environments. Aircrack-ng may be used to passively gather information about a wireless network and crack a pre-shared key.
39. B. Jake may safely share the CRT file, which contains a copy of the organization's public X.509 certificate. The KEY and PEM files contain copies of the organization's private keys, which must be kept secret and secure. The CSR file is a certificate signing request, which is sent to the CA when requesting a signed digital certificate. There is no need to share this file publicly.
40. B. Rootkits are specialized attack tools that allow an attacker to escalate privileges. They exploit system vulnerabilities to leverage a normal user account to gain administrative privileges on the system.

41. B. This is a very low priority vulnerability. The report shows that it has a severity of one on a five-point scale, placing it into the category of informational messages. There are likely hundreds or thousands of similar issues elsewhere on the network. Therefore, there is no need for Paul to take any action.
42. A. In this case, Gary should use an offline bruteforce attack against the password file. An online attack would not leverage the password file that he obtained and would likely be slower and attract attention. A dictionary attack is not effective against a site with a strong password complexity policy. A rainbow table attack suffers the same deficiency as a dictionary attack with the added problem that the site uses salted hashes, rendering the rainbow table ineffective.
43. B. This is a clear example of a **distributed denial of service (DDoS)** attack. The half-open connections indicate the use of a denial of service attack. The fact that the requests came from all over the world makes it clear that it is more than a standard denial of service attack. There is no indication that there was a web application flaw, such as cross-site request forgery or cross-site scripting.
44. C. In a bluesnarfing attack, the attacker establishes a Bluetooth connection to a target device and then retrieves information from that device. Bluejacking attacks only allow the attacker to display a message on the device. Blueballing attacks allow an attacker to break an existing Bluetooth connection between two devices. Bluefeeding attacks do not exist.
45. D. While any of these actions may result from a buffer overflow attack, they are all the result of the more general arbitrary command's execution capability. After a successful buffer overflow, the attacker can typically execute any commands they would like on the system. This effectively gives the attacker full control of the device.
46. D. **Open source intelligence (OSINT)** includes the use of any publicly available information. This includes domain registration records found in WHOIS entries, the contents of public websites, and the use of Google searches. Vulnerability scans are an active reconnaissance technique and are not considered OSINT.
47. A. System sprawl may lead to undocumented systems that are running without the knowledge of the IT organization. These systems may serve no useful purpose, contributing to excess costs. They may also have no assigned IT support personnel, leading to unpatched systems and security vulnerabilities. Input validation is an application security technique and system sprawl would not necessarily lead to increased failures to perform proper input validation.

48. B. Session tokens, or session IDs, are used to prevent an eavesdropper from stealing authentication credentials and reusing them in a different session in what is known as a replay attack. The use of session IDs would not prevent an attacker from carrying out an application layer attack, such as a buffer overflow or injection. It also would not be effective against a man-in-the-middle attack, as the attacker could simply establish a secure session with the server and would, therefore, have access to the session ID.
49. A. This website defacement attack has a clear political message, making the attacker a hacktivist. It is unlikely that an advanced persistent threat or organized crime ring conducted this attack because there is no obvious non-activist motive. There is not enough information to conclude that the attack was waged by a script kiddie because we do not know how the site was compromised.
50. C. Insider attacks are particularly dangerous because they involve internal employees, contractors, or other individuals with access to systems and knowledge of business processes. Other attackers are less likely to have access to this information.
51. A. Enabling safe checks tells the scanner to only use scan plugins that are non-intrusive. The other settings would not change the plugins that are used by the scanner. Configuring the scanner to stop scanning hosts that become unresponsive implies that the scan has already disrupted the host. Changing the order or speed of the scan would not change the tests that are performed.
52. C. This is not likely to be a spoofing attack because there is no evidence that an attacker is falsifying address information in network traffic. However, it is quite possible that an attacker is attempting to steal a domain registration using a domain hijacking attack. Frank should contact the registrar and cancel the request. He should also consider locking the domain to prevent any future unauthorized transfer.
53. C. In a rainbow table attack, the attacker computes the hash values of common passwords and then searches the password file for those values. Adding a random salt to the password eliminates the performance benefit of this attack. Brute force attacks (online or offline) would not be more or less effective either way. The use of salting does not decrease the likelihood of a collision.
54. C. In this attack, the perpetrator created a false wireless network, otherwise known as an evil twin. Although the attacker boosted the power of the signal to make the evil twin signal stronger than other signals, there is no indication of attempts to jam signals from legitimate access points. There is no indication in the scenario that Bluetooth or WPS technology was involved.

55. D. **Advanced persistent threat (APT)** attackers are sophisticated attackers who generally have the support of a nation-state or other large organization that provides them with significant financial resources and sophisticated tools. They often pursue their targets very patiently until they are able to exploit a vulnerability. APT attackers operate stealthily and would avoid using brute force techniques.
56. C. Zero-day attacks are attacks that are not previously known to the security community. Therefore, signature-based controls, such as vulnerability scans, antivirus software, and intrusion prevention systems, are not effective against these attacks. Application control software may use whitelisting to limit software running on a system to a list of known good applications. This technique may prevent zero-day malware from running on the protected system.
57. A. The attacker entered the building wearing a uniform, which is a sign of authority. He threatened the receptionist (intimidation) with an impending network outage (urgency). There is no indication that he tried to build consensus.
58. C. While all of these concerns are legitimate, the lack of access to vendor patches should be Ann's primary security concern. Most vendors require a valid support agreement to obtain firmware updates and devices without those updates may have serious security vulnerabilities. Ann should consider pursuing a less costly support agreement that does not include the expensive hardware replacement feature but does provide access to security updates.
59. D. Patching operating systems will address security vulnerabilities that may allow privilege escalation attacks. **Host intrusion prevention systems (HIPS)** may detect and block privilege escalation attempts. **Data Execution Prevention (DEP)** prevents the system from executing unauthorized code that could result in privilege escalation. Firewalls do not offer an effective defense because an attacker attempting privilege escalation already has a foothold on the system.
60. C. Warren is using a rootkit to attempt to gain administrative privileges on the server. This is an example of an escalation of privilege attack.
61. A. SQL injection, cross-site scripting, and buffer overflow attacks all occur when applications do not properly screen user-provided input for potentially malicious content. DDoS attacks use botnets of compromised systems to conduct a brute force resource exhaustion attack against a common target.
62. A. ARP poisoning attacks work by broadcasting false MAC address information on the **local area network (LAN)**. ARP traffic does not travel over the internet or across broadcast domains, so the attacker must have access to the local network segment to carry out an ARP poisoning attack. The attacker does not need access to the target system or any network devices, including firewalls.

63. A. A birthday attack is used to find collisions in a hash function. If successful, a birthday attack may be used to find substitute content that matches a digital signature. It takes its name from the mathematical birthday problem, which states that it only takes 70 people in a room to have a 99.9% probability that two will share the same birthday.
64. A. The image shows an example of a replay attack, where Mal obtains a copy of Alice's hashed password by sniffing a network connection and then reuses that hash to log in to the server. Changing Alice's password or the hash algorithm would prevent Mal from using the hash he already captured, but he could just repeat the attack to obtain the new hash. Using a shadow password file is good practice but it would not be effective against this attack because Mal is not accessing a password store on the server. Using TLS encryption to protect the session would prevent Mal from sniffing the hashed password.
65. A. While any of these issues may exist, the pressing issue that Charlie must resolve is the fact that the computers are running Windows XP, an end-of-life operating system. Microsoft no longer releases security patches for the OS, and this may cause a critical security issue. If Charlie cannot upgrade the operating system, he should implement other compensating controls, such as placing these systems on an isolated network.
66. C. This is a serious error, indicating that the name on the certificate does not match the name on the server and that the certificate was not issued by a trusted CA. It is very possible that a man-in-the-middle attack is taking place and that the certificate is being presented by an attacker. Patty should warn the user not to visit the site and investigate further.
67. C. The RC4 cipher has inherent security vulnerabilities and is not considered secure, regardless of the key length. Therefore, Terry should include a recommendation in his report that the cipher is replaced with a secure alternative.
68. B. This is a tricky question because any of the answers other than chosen ciphertext could be correct. We can rule out that answer because Joan cannot choose her own ciphertext. She can, however, choose the plaintext that's used to create the ciphertext. When she does choose her own plaintext, she must, therefore, have knowledge of the plaintext. Once she encrypts the message, she also has access to the ciphertext. However, the best term to describe this attack is a chosen plaintext attack because it is the most specific of the three names. Every chosen plaintext attack is also a known plaintext and a known ciphertext attack.

69. B. While all of these are reliable troubleshooting tools, changing the Wi-Fi channel is the best way to detect intentional interference. If Kristen changes the channel and the interference initially goes away but later reappears, it is possible that an attacker is intentionally jamming her network.
70. A. The code shown here is a clear example of an LDAP injection attack. The attacker is attempting to bypass the password security controls of the application by modifying the LDAP query to accept any password provided by the attacker as authentic.
71. D. The Secure attribute instructs the browser to only transmit the cookie via an encrypted HTTPS connection. The HttpOnly attribute does not affect encryption but rather restricts scripts from accessing the cookie via DOM objects. The SameSite attribute prevents the cookie from being shared with other domains, while the Expire attribute sets an expiration date for the cookie.
72. B. Ken is at the pivot stage of the attack. He has gained a foothold in one system and is now attempting to use that access to pivot, or gain access to, other systems.
73. D. The symptoms described here are the classic symptoms of a memory leak. The system is slowly depleting memory as it runs until it finally runs out of available memory, resulting in errors. When Rob reboots the system, it clears out available memory and begins the cycle anew.
74. C. Files 1 and 3 have identical hash values but different content. This is a security issue known as a collision and indicates that the hash function is not secure. There is no syntax error as the hashes were computed properly. Hash functions produce message digests. They do not perform encryption or decryption.
75. D. Port 23 is used by telnet, an insecure protocol for administrative connections to a server. This service should be disabled and replaced with SSH, which uses port 22. Ports 80 and 443 are commonly open on a web server.
76. B. POODLE is a downgrading attack that forces sites using SSL to revert to insecure cipher suites, rendering their communications susceptible to eavesdropping attacks.
77. C. While any type of malware could be responsible for the symptoms described by the user, the compelling piece of evidence in this scenario is that Vince discovered an unusual hardware device attached to the keyboard. This is most likely a keylogger.

78. B. This is a common and reasonable architecture for a dynamic web application where the web server initiates a connection to the database server. However, the connection should not take place with an administrative account. Instead, the database administrator should create a limited privilege service account that restricts the activity performed by the web application. This limits the impact of an attack that compromises the web server and takes over the database connection.
79. C. Bluesnarfing attacks use Bluetooth connections to steal information stored on the target device. Bluejacking attacks also exploit Bluetooth connections but they only allow people to send messages to the device and do not allow the theft of information. Evil twin attacks set up false SSIDs but do not necessarily directly connect the attacker to the target device. Session hijacking attacks do not necessarily take place over a wireless connection and involve a third-party website rather than a direct connection.
80. D. This is a clear example of familiarity and liking. The attacker built up a relationship over time with the employee until they had a strong bond. He then leveraged that relationship to slowly extract information from the target.
81. A. This is an example of a spear phishing attack that was designed specifically for someone in the Accounts Payable department of this firm. It is not a whaling attack because it is targeting a clerk, not a senior executive. It was not conducted by telephone or SMS, so it is not a vishing or smishing attack.
82. C. Pass-the-hash attacks exploit a vulnerability in the NTLM authentication protocol that's used by Windows systems. The attack is not possible against non-Windows systems.
83. C. Web application firewalls are capable of detecting and filtering SQL injection attack attempts and would be an effective control. Stored procedures and parameterized queries both limit the information sent from the web application to the database and also serve as an effective control against SQL injection attacks. Indexes are used to enhance database performance and would not prevent an injection attack.
84. B. **Data loss prevention (DLP)** systems are designed to detect and block the exfiltration of sensitive information. While an **intrusion prevention system (IPS)** or firewall may be able to reduce the likelihood of a successful attack, they are not designed for this purpose. The use of TLS encryption would not prevent an attack as it protects data while in transit but not at rest.

85. A. Implementing credentialled scanning would improve the quality of the information provided to the scanner and, therefore, would lower the false positive rate. Decreasing the scan's sensitivity would lower the threshold for an alert and increase the false positive rate. Disabling safe checks and increasing the size of the target network would both increase the number of scan tests performed and, absent of any other change, would have the effect of increasing the number of false positive reports.
86. D. This is an example of a **radio frequency identification (RFID)** transmitter. RFID is a form of **near-field communication (NFC)** that is used to communicate over short distances. This device could be used to track the physical presence of the executive when within range of a receiver.
87. D. These tweets are an example of botnet command and control traffic. The Twitter account is directing the infected system to engage in distributed denial of service attacks.
88. B. During a black box test, the attacker should not have access to any non-public information. It is reasonable to assume that any member of the public could conduct an external vulnerability scan, and so there is no harm in expediting the penetration test by providing Rick with the results of an external scan. However, he should not have access to scans that would require additional access. These include credentialled scans, agent-based scans, and internal scans.
89. C. A false positive error occurs when a security system reports a condition that does not actually exist. In this case, the vulnerability scanner reported a missing patch, but that report was in error and, therefore, a false positive report.
90. B. This issue means that the web server will provide detailed error messages when an error condition occurs. These error messages may disclose information about the structure of the web application and supporting databases to an attacker that the attacker could then use to wage an attack.
91. B. The fact that the traffic is exceeding normal baselines and that the responses are much larger than the queries indicates that a DNS amplification attack may be underway. In this type of attack, the attacker sends spoofed DNS queries, asking for large amounts of information. The source address on those queries is the IP address of the target system, which then becomes overwhelmed by the response packets.
92. A. This is an example of a logic bomb, that is, code that remains dormant until certain logical conditions are met and then releases its payload. In this case, the logic bomb was configured to release if the developer was no longer employed by the organization.

93. A. Whois queries provide information about the registered owners of domain names and are a useful open source intelligence tool. The **nslookup** and **dig** commands perform standard DNS queries and can determine the IP addresses associated with domain names but do not normally reveal registration information. The **ping** command is used to test network connectivity.
94. D. Including security team members in the project management process allows them to review and comment on proposed system designs and architectures before a project is implemented. This increases the likelihood that the design will be secure. Technical controls, such as firewalls and intrusion prevention systems, may not protect against architectural weaknesses. Design flaws are generally not caused by employee malfeasance, so background checks would not be an effective control.
95. D. This type of attack, which causes a user's browser to execute a script, is known as a **cross-site scripting (XSS)** attack. This particular variant stores the script on the server (in the form of a message board posting) and, therefore, is a stored XSS attack.
96. B. Zero-day attacks occur when an attacker exploits a vulnerability for which there is no security patch, leaving users defenseless. As Mal's organization is the only entity aware of the attack, there is no security update from the vendor to resolve the problem. Therefore, she is in a position to conduct a zero-day attack. The question does not provide enough information about the vulnerability to determine whether it would allow SQL injection, man-in-the-browser, or spoofing attacks.
97. C. **Man-in-the-middle (MITM)** attacks occur when an interloper is able to trick both client and server systems into establishing a connection with the interloper but believing that they are actually communicating with each other. SSL and TLS may be used to protect the contents of communications with encryption but they do not, by themselves, offer protection against MITM attacks. If the parties use digital certificates signed by a trusted certificate authority, this provides an added degree of trust and protects against MITM attacks. Input validation is a useful control to protect against application layer attacks but is not helpful against MITM attacks.
98. C. The third log entry shows clear signs of a SQL injection attack. Notice that the parameters passed to the web page include an appended SQL command: **UNION SELECT 1,2,3,4,5**. This is designed to retrieve the first five columns from the database table and will likely succeed if the web application is not performing proper input validation.

99. D. Race conditions occur when a security issue exists that allows an attacker to exploit the timing of commands to obtain unauthorized access. A **time-of-check/time-of-use (TOC/TOU)** attack exploits a time lag between when an application verifies authorization and then allows the use of privileges. Therefore, this timing-based attack exploits a race condition.
100. D. A Wi-Fi pineapple is a device specifically designed to carry out rogue AP attacks against wireless networks. The pineapple functions by forcing clients to disassociate from their current access points and connect to a network run by the pineapple.
101. D. Generally speaking, IoT deployments do not typically require multifactor authentication. They do, however, call for maintenance of the embedded operating systems, network segmentation, and the encryption of sensitive information.
102. C. The core issue underlying these vulnerabilities is that SSL is no longer considered secure and that TLS version 1.0 is also insecure. Therefore, the most expedient way to address this problem is to upgrade to TLS 1.2 and make that the only transport encryption protocol supported by the server.
103. A. The main limitation of IP spoofing over the internet is that the attacker will not be able to receive responses to their requests because they will be routed to a different network location. If Mal controls her own network, she will be able to bypass any local firewall egress filters that would prevent her from sending the spoofed packets, which she can create with any packet generation tool. IP spoofing is commonly used in denial of service attacks.
104. C. Answering this question doesn't require any knowledge of the specific vulnerability described in MS08-067. Instead, the key is that the worm was spreading overnight while nobody was in the office. The key characteristic of a worm is that it spreads on its own power, without user intervention.
105. A. From the description provided, we have sufficient information to identify this as a Trojan horse. Trojans are a type of malware that disguise themselves as a benign application, such as a game, but then carry a malicious payload.

2

Technologies and Tools

Domain 2 Questions

1. In which one of the following mobile device deployment models does the organization allow employees to use corporate-owned devices for personal use?
 - A. BYOD
 - B. CYOD
 - C. COPE
 - D. Corporate-owned
2. Bruce would like to implement an authentication mechanism that requires that users connecting via mobile devices use a second authentication factor when they are connecting from an unfamiliar IP address. What term best describes this technique?
 - A. Context-based authentication
 - B. Role-based authentication
 - C. Rule-based authentication
 - D. Device-based authentication
3. Rob is tracking down the unauthorized exfiltration of sensitive information from his organization and found suspicious emails sent by an employee to a Gmail address. The emails seem to only contain photos, but Rob suspects that the photos contain sensitive information. What technique might the employee have used to embed sensitive information within a photograph?
 - A. Cartography
 - B. Cryptography
 - C. Steganography
 - D. Psychology

4. Brad received a call from the Help Desk that users are suddenly calling to report that they are receiving an Access Denied message when trying to access several popular websites, although they are able to access other sites. It seems that everyone in the organization is experiencing the same symptoms on different devices and operating systems and the sites that are being blocked are consistent from user to user. Of the components listed here, which is the most likely culprit?
 - A. Content filter
 - B. Network firewall
 - C. GPO
 - D. IPS
5. Ryan is reviewing logs for his wireless network controller and discovers that a single system attempted to connect to the wireless network once every minute with incorrect credentials until finally logging in successfully after several hours. While reviewing the logs, Ryan noticed that the system had been used by the same user on the network several days ago. What is the most likely explanation of these log entries?
 - A. The user's password was compromised via a brute force attack.
 - B. The user fell victim to a social engineering attack.
 - C. The user changed his or her password.
 - D. The user's device was stolen.
6. Mary's organization uses a specialized statistical software package for their research. Mary discovered that users pass around installation media within their departments rather than deploying the software via a centralized tool. What is the greatest risk facing the organization?
 - A. Social engineering
 - B. Malware infection
 - C. License violation
 - D. Faulty software

7. Sandra is deploying cellular devices to her firm's salesforce. She is concerned that the employees will install apps on the devices that jeopardize security. Which one of the following technologies will allow her to control the configuration of the device and prevent the installation of unwanted apps?
 - A. ERP
 - B. BYOD
 - C. MDM
 - D. CRM
8. Which one of the following tools would be the most helpful in detecting missing operating system patches?
 - A. Documentation review
 - B. Network vulnerability scanner
 - C. Port scanner
 - D. Configuration management tool
9. Tina is deploying an NAC solution for a university network and she wishes to perform host health checking. The network has many unmanaged student machines and students do not want to have software installed on their systems that remains behind after they leave the network. Which one of the following approaches would be best for Tina to use?
 - A. Dissolvable NAC
 - B. Permanent NAC
 - C. Captive portal
 - D. Active Directory NAC
10. Which one of the following elements of an LDAP entry can be reconstructed to determine the domain name of a system?
 - A. CN
 - B. OU
 - C. DC
 - D. ST

11. Charlie received an alert from file integrity monitoring software running on a server in his organization. Which one of the following is NOT a likely reason for this alert?
- A. Operating system update
 - B. CPU failure
 - C. Application update
 - D. Security incident
12. Which one of the following features is not typically supported by mobile device management solutions?
- A. Remote wiping
 - B. Carrier unlocking
 - C. Application management
 - D. Configuration management
13. Consider the load balanced server situation shown here. The load balancer sent the last user request to Server A. If the server is using round-robin load balancing, which server will receive the next request?

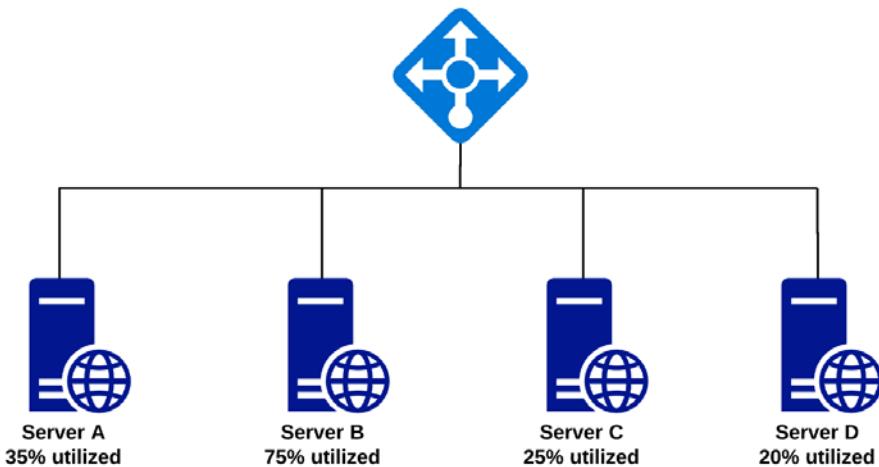


Figure 2.1

- A. Server A
- B. Server B
- C. Server C
- D. Server D

14. Ben would like to identify all of the active network connections and services listening for connections on a Linux system that he is analyzing. What command-line utility can he use to meet this need?
- A. pstools
 - B. tcpdump
 - C. netstat
 - D. netcat
15. Carl is troubleshooting a Windows device that is having issues connecting to the network. He runs the **ipconfig** commands and finds the information shown here for the problematic interface. How did the system receive this IP address?

```
Ethernet adapter Ethernet 3:

Connection-specific DNS Suffix . . . :
Link-local IPv6 Address . . . . . : fe80::d50a:1b66:8185:4ae3
IPv4 Address . . . . . : 169.254.188.19(Preferred)
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :
```

Figure 2.2

- A. Active Directory preferred address
- B. DHCP
- C. Static assignment
- D. APIPA

16. Tim is planning the deployment of a new VPN that is illustrated in the high-level diagram shown here. What type of VPN is Tim deploying?

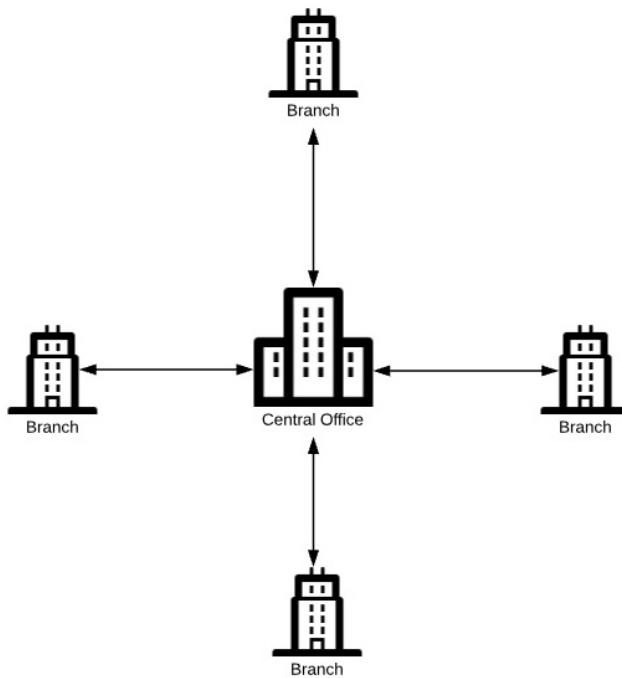


Figure 2.3

- A. TLS VPN
 - B. Remote access VPN
 - C. Site-to-site VPN
 - D. IPsec VPN
17. Vince is concerned that attackers might be able to gain access to the password file for a service that he runs and he would like to protect it as much as possible. Which one of the following controls provides the most effective protection against the success of rainbow table attacks?
- A. Salting
 - B. Hashing
 - C. Shadow passwords
 - D. Password expiration

18. Which one of the following techniques often reveals both the type and version of a service running on a particular port?
- A. Traceroute
 - B. Port scanning
 - C. Steganography
 - D. Banner grabbing
19. Jena would like to configure her organization's switches so that they do not allow systems connected to a switch to spoof MAC addresses. Which one of the following features would be helpful in this configuration?
- A. Loop protection
 - B. Port security
 - C. Flood guard
 - D. Traffic encryption
20. What type of proxy server is shown in the following illustration?

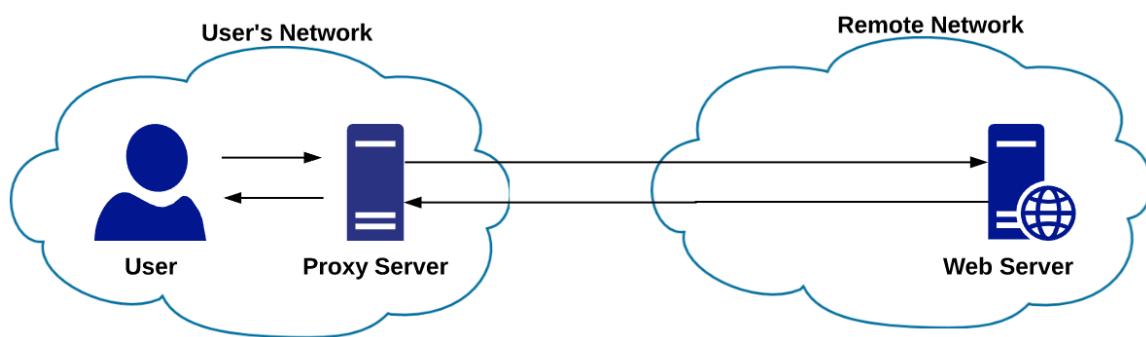


Figure 2.4

- A. Caching proxy
- B. Reverse proxy
- C. Content filtering proxy
- D. Forward proxy

21. Bill is inspecting a new tablet computer that was brought to him by an employee wishing to connect it to the network. The device has the logo shown here on its back panel. What does this logo indicate?



Figure 2.5

- A. The device has the ability to upload data to cloud services.
 - B. The device is portable.
 - C. The device can be recharged through the USB port.
 - D. The device may be used as a server to access other USB devices.
22. Drew is concerned that users in his organization may send customers sensitive email messages that travel over the internet in an unencrypted form. What technology can he use to intercept these messages and provide encrypted delivery to the recipient?
- A. Firewall
 - B. Email gateway
 - C. IPS
 - D. TLS
23. What transport protocol is used by the **traceroute** command by default?
- A. No transport protocol is used
 - B. ICMP
 - C. TCP
 - D. UDP

24. Helen is working with a user who reported that strange messages were appearing on his mobile device. After troubleshooting, Helen determines that the messages were sent over Bluetooth. There is no indication that any information on the device was accessed by the attacker. What type of attack likely took place?
- A. Bluelining
 - B. Bluesnarfing
 - C. Bluescreening
 - D. Bluejacking
25. Alan is running a system audit and detects a user workstation that deviates from the organization's security standard. What action should he take next?
- A. Identify the cause of the deviation.
 - B. Report the issue to his manager.
 - C. Reimage the workstation.
 - D. Reconfigure the device to meet the baseline.
26. Brian recently established a transport mode IPsec connection between his system and a remote VPN concentrator. Which one of the following statements is correct about this connection?
- A. The payload of the packet is not encrypted.
 - B. The IP header of the packet is not encrypted.
 - C. The connection supports NAT traversal.
 - D. No encryption is in use.
27. Gwen is crafting a social media policy for her organization and is considering including the following provisions. Which one of these provisions is most likely to be problematic from a legal perspective?
- A. Restricting the use of personal social media accounts outside of working hours.
 - B. Requiring disclosure of company affiliation on social media.
 - C. Requiring the approval of posts that are sent out via corporate social media accounts.
 - D. Blocking social media sites at the perimeter firewall.

28. Nancy issues the command shown here to determine whether a system is live on the network. What type of packet is sent out by her system?

```
$ ping 10.36.16.1
PING 10.36.16.1 (10.36.16.1): 56 data bytes
64 bytes from 10.36.16.1: icmp_seq=0 ttl=255 time=46.363 ms
64 bytes from 10.36.16.1: icmp_seq=1 ttl=255 time=2.172 ms
64 bytes from 10.36.16.1: icmp_seq=2 ttl=255 time=1.613 ms
64 bytes from 10.36.16.1: icmp_seq=3 ttl=255 time=6.930 ms
64 bytes from 10.36.16.1: icmp_seq=4 ttl=255 time=2.834 ms
64 bytes from 10.36.16.1: icmp_seq=5 ttl=255 time=1.612 ms
^C
--- 10.36.16.1 ping statistics ---
6 packets transmitted, 6 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.612/10.254/46.363/16.251 ms
$ █
```

Figure 2.6

- A. ICMP echo reply
 - B. ICMP echo request
 - C. ICMP information request
 - D. ICMP information reply
29. What type of social engineering attack always occurs via telephone calls?
- A. Spear phishing
 - B. Vishing
 - C. Smishing
 - D. Whaling

30. What type of Wi-Fi antenna is shown in the following image?

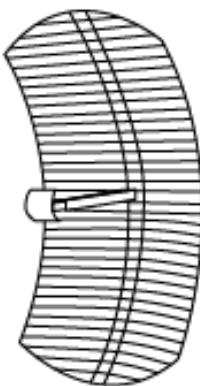


Figure 2.7

- A. Omnidirectional
 - B. Parabolic
 - C. Pulse width
 - D. Yagi
31. Hannah is investigating a security incident and discovers that a network client sent false MAC address information to a switch. What type of attack likely took place?
- A. DNS poisoning
 - B. ARP poisoning
 - C. Man-in-the-middle
 - D. Eavesdropping
32. Laura is performing a DNS query using the **nslookup** command and she would like to identify the SMTP server(s) associated with a domain. What type of records should she retrieve?
- A. MX
 - B. A
 - C. CNAME
 - D. NS

33. Helen would like to sideload an app onto an Android device. What format must the application be in for her to successfully sideload it?
- A. EXE
 - B. IPA
 - C. ZIP
 - D. APK
34. Raj is troubleshooting authentication problems with his organization's VPN. All of the users are receiving password authentication failures. What is the most likely cause of this problem?
- A. Password expiration
 - B. Incorrect passwords
 - C. RADIUS server failure
 - D. VPN server failure
35. Carla learns that a user in her organization is about to be terminated at 3:00 and she wants to properly time the disablement of that user's account. What would be the best time to terminate access?
- A. During the termination conversation
 - B. Immediately
 - C. At the end of the day
 - D. Tomorrow morning
36. Ricky is configuring a directory server that must be accessible to users passing through a firewall. He would like to allow only encrypted LDAPS sessions through the firewall. What port should Ricky enable?
- A. TCP port 3389
 - B. TCP port 389
 - C. TCP port 636
 - D. TCP port 443

37. Which one of the following security controls can best protect against the risk of unauthorized software installation?
- A. Content filters
 - B. Application blacklisting
 - C. Host firewalls
 - D. Application whitelisting
38. During a security audit of his organization's web environment, Robert discovers that his web server supports SSL v2.0. What action should he recommend based upon this information?
- A. The organization should replace SSL with TLS.
 - B. The organization should disable SSL v2.0 and support only SSL v3.0 or higher.
 - C. The organization should replace SSL with SSH.
 - D. No action is necessary.
39. Ryan is experiencing interference on his Wi-Fi network. Which one of the following options is not an effective solution to the problem?
- A. Change wireless channels
 - B. Relocate access points
 - C. Increase bandwidth
 - D. Relocate wireless clients
40. Which one of the following statements about IPsec protocols is correct?
- A. AH supports authentication, integrity, and confidentiality. ESP supports confidentiality and authentication.
 - B. AH supports authentication, integrity, and confidentiality. ESP supports confidentiality and integrity.
 - C. AH supports authentication and integrity. ESP supports confidentiality, authentication, and integrity.
 - D. AH supports authentication and confidentiality. ESP supports integrity and authentication.

41. Barry is reviewing log records in the wake of a security incident. He suspects that the attackers attempted a SQL injection attack that was blocked. Which one of the following log sources is likely to contain the best information about the attempted attack?
- A. Host firewall logs
 - B. Web server logs
 - C. Database logs
 - D. Web application firewall logs
42. After implementing a SIEM solution, Amanda discovers that the timestamps on log entries are not synchronized. What protocol can Amanda deploy in her organization to ensure clock synchronization?
- A. DHCP
 - B. DNS
 - C. NTP
 - D. BGP
43. Colleen's company is considering deploying a BYOD mobile device strategy. She is concerned about the intermingling of corporate and personal data on mobile devices. What security control can help resolve this situation?
- A. Application control
 - B. Full device encryption
 - C. Storage segmentation
 - D. Multifactor authentication

44. Renee ran a wireless network scan in her office and found the results shown in the following table. Which one of the following networks has the strongest signal?

Network Name	BSSID	Security	Protocol	RSSI	Noise	Channel
CAFwifi	1c:b9:c	WPA2 Personal	802.11b/g/n	-67	0	9
CAFwifi-Guest	1c:b9:c	WPA2 Personal	802.11b/g/n	-74	0	4
CAFwifi-Guest	1c:b9:c	WPA2 Personal	802.11ac	-89	0	36
CAFwifi-Guest	1c:b9:c	WPA2 Personal	802.11b/g/n	-73	0	4
CAFwifi-Guest	1c:b9:c	WPA2 Personal	802.11ac	-81	0	157
CAFwifi-Guest	1c:b9:c	WPA2 Personal	802.11b/g/n	-68	0	9
cathy	f8:a0:8	WPA/WPA2 Personal	802.11ac	-89	-99	48
CBCI-3CD8-2.4	20:25:	WPA/WPA2 Personal	802.11b/g/n	-69	0	6
CBD	1c:b9:c	WPA2 Personal	802.11b/g/n	-78	0	4
CBD	1c:b9:c	WPA2 Personal	802.11ac	-88	0	36
CNA_Corporate	68:bd:	WPA2 Enterprise	802.11a/n	-83	0	60
CornerBakeryCafeWiFi	00:11:7	Open	802.11ac	-72	0	1
CornerBakeryCafeWiFi	00:11:7	Open	802.11ac	-83	-99	48

Figure 2.8

A. CAFwifi-Guest

B. cathy

C. CornerBakeryCafeWiFi

D. CAFwifi

45. Dylan is helping his organization select a secure video conferencing solution that will be used to meet both internally and with customers. He would like to choose a technology that uses a protocol that supports secure video conferencing and will most likely be allowed through the network firewalls of customer organizations. Which one of the following protocols is his best option?

A. RTPS

B. HTTPS

C. H.323

D. SIP

46. Sally is planning to deploy an advanced malware protection system. What feature of these systems would allow Sally to leverage information obtained from malware monitoring that was conducted by other customers of the same vendor?
- A. Sandboxing
 - B. Threat intelligence
 - C. Quarantining
 - D. Behavioral detection
47. Ron is selecting an email data loss prevention (DLP) solution for use in his organization. He is specifically concerned about preventing the loss of a set of product plans that are contained in a single repository. Which DLP technology would be the most effective at meeting his needs?
- A. Pattern recognition
 - B. Watermarking
 - C. Host-based
 - D. Network-based
48. Visitors to Patricia's organization's website are seeing the following error message. What is the simplest way that Patricia can resolve this issue?

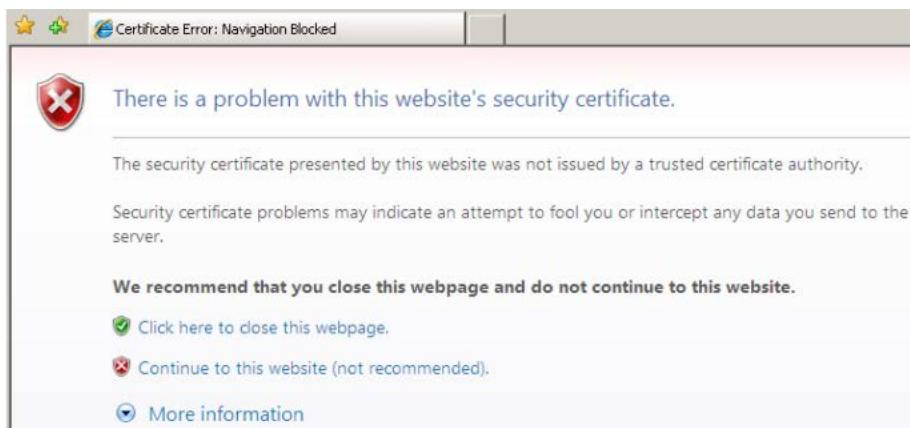


Figure 2.9

- A. Require the use of TLS
- B. Renew the certificate
- C. Replace the certificate
- D. Block insecure ciphers

49. Dennis is reviewing the logs from a content filter and notices that a user has been visiting pornographic websites during business hours. What action should Dennis take next?

- A. Take no action
- B. Discuss the issue with the user
- C. Block access to the websites
- D. Report the issue to management

50. Review the ifconfig results shown here. What is the primary IP address for this machine?

```
lo0: flags=8049<UP,LOOPBACK,RUNNING,MULTICAST> mtu 16384
    options=1203<RXCSUM,TXCSUM,TXSTATUS,SW_TIMESTAMP>
    inet 127.0.0.1 netmask 0xffffffff
        inet6 ::1 prefixlen 128
            inet6 fe80::1%lo0 prefixlen 64 scopeid 0x1
                nd6 options=201<PERFORMNUD,DAD>
gif0: flags=8010<POINTOPOINT,MULTICAST> mtu 1280
stf0: flags=0<> mtu 1280
XHC20: flags=0<> mtu 0
en0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    ether 98:e0:d9:87:8a:73
    inet 10.36.23.22 netmask 0xfffffff800 broadcast 10.36.23.255
        media: autoselect
        status: active
p2p0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 2304
    ether 0ae0:d9:87:8a:73
        media: autoselect
        status: inactive
awdl0: flags=8943<UP,BROADCAST,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1484
    ether 62:9f:a8:6b:94:08
    inet6 fe80::609f:a8ff:fe6b:9408%awdl0 prefixlen 64 scopeid 0x9
        nd6 options=201<PERFORMNUD,DAD>
        media: autoselect
        status: active
en1: flags=8963<UP,BROADCAST,SMART,RUNNING,PROMISC,SIMPLEX,MULTICAST> mtu 1500
    options=60<TS04,TS06>
    ether 9a:00:01:99:02:70
        media: autoselect <full-duplex>
        status: inactive
bridge0: flags=8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=63<RXCSUM,TXCSUM,TS04,TS06>
    ether 9a:00:01:99:02:70
    Configuration:
        id 0:0:0:0:0:0 priority 0 hellotime 0 fwddelay 0
        maxage 0 holdcnt 0 proto stp maxaddr 100 timeout 1200
        root id 0:0:0:0:0:0 priority 0 ifcost 0 port 0
        ipfilter disabled flags 0x2
    member: en1 flags=3<LEARNING,DISCOVER>
        ifmaxaddr 0 port 10 priority 0 path cost 0
        nd6 options=201<PERFORMNUD,DAD>
        media: <unknown type>
        status: inactive
utun0: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 2000
    inet6 fe80::11f19:7c86:94a1:3708%utun0 prefixlen 64 scopeid 0xd
        nd6 options=201<PERFORMNUD,DAD>
utun1: flags=8051<UP,POINTOPOINT,RUNNING,MULTICAST> mtu 1380
    inet6 fe80::c277:463f:341a:4c99%utun1 prefixlen 64 scopeid 0xe
        nd6 options=201<PERFORMNUD,DAD>
```

Figure 2.10

- A. 127.0.0.1
- B. 10.36.23.255
- C. 10.36.23.22
- D. 98:e0:d9:87:8a:73

51. Alan created a system named PersonnelDatabase that is designed to attract attackers, but there is no real sensitive information on the server. When someone attempts to connect to the system, Alan analyzes their activity. What type of system has Alan created?
- A. Honeypot
 - B. Darknet
 - C. Sinkhole
 - D. Honeynet
52. Tom would like to deploy NAC technology that is capable of constantly monitoring the configuration of endpoint machines and quarantining machines that fail to meet a security baseline. Which technology would be the most appropriate for Tom to deploy?
- A. Dissolvable NAC
 - B. Agentless NAC
 - C. Captive portal
 - D. Agent-based NAC
53. Flo is investigating an alert that was generated by her organization's NIDS. The system was alerted to a distributed denial of service attack and Flo's investigation revealed that this type of attack did take place. What type of report has the system generated?
- A. False positive
 - B. True negative
 - C. True positive
 - D. False negative
54. Kyle would like to capture network traffic to assist with troubleshooting a firewall issue. What command-line utility can he use to capture traffic?
- A. netcat
 - B. Wireshark
 - C. nmap
 - D. tcpdump

55. Which one of the following IP addresses should never be seen as the destination address of a packet leaving an organization's network over the internet?
- A. 192.168.10.6
 - B. 12.8.1.42
 - C. 129.53.100.15
 - D. 154.42.190.5
56. Trevor is planning the deployment of a Wi-Fi network. Which one of the following encryption technologies provides the highest level of security?
- A. WPA2
 - B. WEP
 - C. TKIP
 - D. WPA
57. Wendy is deploying mobile devices to field workers who must travel in rural areas and require constant data service availability. Which one of the following technologies can provide that access?
- A. Cellular
 - B. SATCOM
 - C. Wi-Fi
 - D. Bluetooth
58. Which one of the following tools is an exploitation framework commonly used in penetration testing?
- A. Metasploit
 - B. Cain and Abel
 - C. Nessus
 - D. Sysinternals

59. Tim is concerned about the integrity of log records written by a database that stores sensitive information. What technology can he use to best prevent unauthorized changes to log entries?
- A. TLS
 - B. Cryptographic hashing
 - C. File integrity monitoring
 - D. WORM
60. Brian would like to restrict access to his Wi-Fi network to three specific devices that he controls. This network is small and Brian would like to control costs and preserve simplicity. What is the best way to restrict access?
- A. PSK
 - B. MAC filtering
 - C. NAC
 - D. Kerberos
61. Victor's organization is experiencing a rash of misplaced devices. What IT management discipline can help them maintain an accurate inventory?
- A. Configuration management
 - B. Asset management
 - C. Change management
 - D. Firewall management
62. Barry is using Nmap to scan systems and is experiencing difficulty because some systems are not responding to **ping** requests. He knows the hosts are active. What flag can he use to skip the discovery step entirely?
- A. -Pn
 - B. -PS
 - C. -PA
 - D. -PU

63. Carrie is setting up a site-to-site VPN between two of her organization's offices and wishes to establish the connection using IPsec-based VPN concentrators. Which IPsec mode should Carrie use?
- A. Tunnel mode
 - B. Transport mode
 - C. Split tunnel
 - D. TLS
64. Maddox is configuring an internal firewall that will restrict access to a network subnet populated with database servers. Which one of the following ports is not commonly associated with database traffic?
- A. 1433
 - B. 1521
 - C. 1701
 - D. 3306
65. Tammy is running a set of three load-balanced web servers for her domain. The first server is the primary server and handles requests until it reaches capacity, and then new requests are assigned to the second server. The third server remains idle unless the other two servers are fully utilized. What IP address should Tammy use for the DNS entry for the domain?
- A. Second server's IP
 - B. First server's IP
 - C. Virtual IP
 - D. Third server's IP
66. Alan is checking the NTFS permissions for a file and finds that the permissions for a problematic user are as follows. What is the end result of these permissions?

Permissions:	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Modify	<input type="checkbox"/>	<input type="checkbox"/>
Read & Execute	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Figure 2.11

- A. The user cannot read or write the file.
 - B. The user can read the file but not write to it.
 - C. The user can write to the file but cannot read it.
 - D. The user can read and write the file.
67. Eric would like to determine whether the users on his network are transmitting sensitive information without the use of encryption. What technology, of the following choices, can best assist Eric in completing this task?
- A. Exploitation framework
 - B. Port scanner
 - C. Protocol analyzer
 - D. Honeypot
68. Laurie is considering using the S/MIME standard to provide secure email capability for her organization. Which one of the following statements best describes the security capabilities of S/MIME?
- A. S/MIME provides confidentiality, integrity, and non-repudiation.
 - B. S/MIME provides confidentiality and integrity, but not non-repudiation.
 - C. S/MIME provides integrity and non-repudiation, but not confidentiality.
 - D. S/MIME provides confidentiality and non-repudiation, but not integrity.
69. Tom is conducting a security audit of network devices in a hospital and discovers that the devices are using SNMPv3 for management. What conclusion can he reach from this information alone?
- A. SNMPv3 is insecure because it contains injection vulnerabilities.
 - B. SNMPv3 is insecure because it uses plaintext community strings.
 - C. SNMPv3 is insecure because it transfers commands in unencrypted form.
 - D. The hospital is using a secure network management protocol.

70. Greg is concerned that users might connect USB drives to their workstations in an attempt to steal sensitive information without being detected on the network. What technology can Greg use to block USB device use?
- A. Host-based DLP
 - B. Network-based DLP
 - C. Host-based IPS
 - D. Network-based IPS
71. Which one of the following approaches provides the greatest security for a two-factor authentication system based upon the use of mobile devices?
- A. TLS notification
 - B. SMS notification
 - C. MMS notification
 - D. Push notification
72. Dave's organization uses Android devices from a manufacturer who is very slow to provide operating system updates. Users in his organization are very tech-savvy and want the most recent version of Android. What technique might they wind up adopting to obtain those updates that might also jeopardize Dave's ability to manage them through his MDM platform?
- A. Custom firmware
 - B. Application sideloading
 - C. Bluejacking
 - D. Bluesnarfing
73. Scott is creating a VPN policy for end users. He would like to provide maximum protection for mobile devices running Windows by automatically establishing VPN connections when the users of those devices open applications that are known to process sensitive data. What technology can best assist Scott with this task?
- A. Split tunnel VPN
 - B. TLS VPN
 - C. IPsec VPN
 - D. Always On VPN

74. Alan's organization is deploying a BYOD policy for mobile devices, and he would like to protect corporate data stored on those devices in the event of a compromise. Which one of the following features would be the least appropriate for meeting this goal?
- A. Remote wiping
 - B. Containerization
 - C. Geofencing
 - D. Encryption
75. Molly's security team is overwhelmed by the number of sources of security information that they receive. She would like to select a tool that can aggregate and correlate log entries. What tool is the most appropriate for her needs?
- A. DLP
 - B. SIEM
 - C. IPS
 - D. NAC
76. Which feature of Microsoft operating systems prevents the execution of code stored in regions of memory not specifically designated for executable code?
- A. PCI
 - B. ASLR
 - C. DEP
 - D. PGP
77. Libby is reviewing the logs that were generated by her organization's application whitelisting system. Which one of the following circumstances is most likely to generate a false positive alert?
- A. Software update to authorized application
 - B. Downloading software from the web
 - C. Execution of malware on a system
 - D. Installation of a rootkit

78. Juan is running two load balancers in active/passive mode. Which one of the following terms does NOT describe this situation?
- A. High availability
 - B. Fully utilized
 - C. Fault tolerant
 - D. Easily maintained
79. Carl is configuring security permissions for his network and comes across the ruleset shown here. What type of device is most likely executing this policy?

```
access-list 100 deny ip 10.0.0.0 0.255.255.255 any
access-list 100 deny ip 172.16.0.0 0.15.255.255 any
access-list 100 deny ip 192.168.0.0 0.0.255.255 any
access-list 100 deny ip 127.0.0.0 0.255.255.255 any
access-list 100 permit ip any any
```

Figure 2.12

- A. IDP
- B. Firewall
- C. DLP
- D. Router

80. In the following image, what term is used to describe the Wi-Fi network names being displayed to the user?



Figure 2.13

- A. Broadcast name
 - B. MAC
 - C. IP address
 - D. SSID
81. Bev is analyzing host IPS logs from endpoints in her network and notices that many are receiving port scans from external hosts. Which one of the following circumstances is likely present?
- A. Compromised internal system
 - B. Misconfigured host firewall
 - C. Misconfigured IPS
 - D. Misconfigured network firewall

82. Greg is reviewing smartphone security controls for users who take photos at sensitive locations. He is concerned about the type of information that might be included in the EXIF metadata associated with each image. Which one of the following data elements is not commonly included in EXIF metadata?
- A. Ambient temperature
 - B. GPS coordinates
 - C. Camera model
 - D. Shutter speed
83. Ricky works for a defense contractor that would like to disable the use of cameras on all mobile devices owned by the organization. They are doing this to prevent the theft of confidential information through device cameras. What technology can Ricky use to best enforce this requirement?
- A. IPS
 - B. DLP
 - C. MDM
 - D. WAF
84. Which one of the following firewall types is capable of monitoring connection statuses by tracking the stages of the TCP handshake and then using that information when deciding whether to allow future packets that are part of an active connection?
- A. Stateless firewall
 - B. Packet filter
 - C. Stateful inspection
 - D. Router ACL
85. Barbara is the cybersecurity manager for a retail chain that is considering deploying contactless payment systems that support Apple Pay, Google Wallet, and similar solutions. What type of communication technology do these solutions use to communicate between a user's smartphone and the payment terminal?
- A. NFC
 - B. Bluetooth
 - C. Infrared
 - D. Wi-Fi

86. After reviewing the results of a system scan, Mike determines that a server in his organization supports connections using the FTP service. What is the primary risk associated with this service?
- A. Buffer overflow
 - B. Unencrypted credentials
 - C. Cross-site scripting
 - D. Privilege escalation
87. Tina is selecting a firewall for her organization and would like to choose a technology that is capable of serving as her organization's front line connection to the internet and blocking a variety of attacks, including SYN floods, TCP probes, and SQL injection. Which one of the following devices would best meet her needs?
- A. Packet filter
 - B. Next-generation firewall
 - C. Router ACL
 - D. Web application firewall
88. Sam is reviewing the logs from his organization's unified threat management system. Which one of the following functions is not typically performed by a UTM device?
- A. Sandboxing
 - B. Content filter
 - C. Firewall
 - D. Intrusion prevention
89. Jaime is creating a firewall ruleset that is designed to allow access from external networks to a web server that responds to both encrypted and unencrypted requests. What ports should Jaime fill for the boxes currently labeled X and Y in the following diagram?

Rule	Source IP	Source Port	Dest IP	Dest Port	Action
1	any	any	10.0.0.1	X	allow
2	any	any	10.0.0.1	Y	allow
3	any	any	any	any	block

Figure 2.14

- A. 80 and 443
 - B. 80 and 8080
 - C. 53 and 443
 - D. 53 and 80
90. Which one of the following data sanitization techniques uses strong magnetic fields to remove remnant data from a device?
- A. Pulverizing
 - B. Degaussing
 - C. Wiping
 - D. Overwriting
91. Tom purchased a mobile device from a carrier under a contract that expired last year. He attempted to transfer the device to a new carrier but was told that the device is locked. Who must unlock the device in order for Tom to complete the transfer?
- A. The new carrier
 - B. The original carrier
 - C. Tom's employer
 - D. Tom
92. Norma is comparing the security characteristics of different Wi-Fi networks. Which one of the following types of Wi-Fi network allows the use of enterprise authentication protocols?
- A. PSK
 - B. WPA
 - C. Ad hoc
 - D. Direct

93. Tim is installing a data loss prevention system in his organization and is concerned about the likelihood of false positive reports. Which one of the following techniques is most likely to generate false positive alerts?
- A. Removable media control
 - B. Watermarking
 - C. Pattern matching
 - D. Software updates
94. Which one of the following network device features is NOT used to prevent routing loops from occurring in a network or to correct them when they do occur?
- A. Split horizon
 - B. Loop prevention
 - C. Flood guard
 - D. Hold-down timers
95. Samantha would like to add security to her organization's voice over IP (VoIP) telephony system. What protocol is specifically designed to assist with securing VoIP implementations?
- A. SNMP
 - B. SRTP
 - C. SSH
 - D. TLS
96. Which one of the following services is not normally performed by email security gateways?
- A. Network firewall
 - B. Data loss prevention
 - C. Encryption
 - D. Spam filtering

97. In the firewall ruleset shown here, what name is typically used to refer to rule number 4?

Rule	Source IP	Source Port	Dest IP	Dest Port	Action
1	any	any	10.0.0.1	25	allow
2	any	any	10.0.0.1	465	allow
3	10.0.0.0/24	any	any	any	allow
4	any	any	any	any	block

Figure 2.15

- A. SMTP
 - B. Stealth
 - C. Promiscuous
 - D. Implicit deny
98. John would like to identify a subscription service that helps him block known malicious systems from accessing his network by automatically updating his firewall rules. What type of service would best meet this need?
- A. Malware signature
 - B. IP reputation
 - C. IDS signature
 - D. Behavioral analysis
99. Ralph runs a large-scale Wi-Fi network and is having difficulty with interference between access points. What is the most effective and efficient way for Ralph to address these issues?
- A. Use a Wi-Fi controller
 - B. Modify access point power levels
 - C. Reposition access points
 - D. Modify access point antenna configuration

100. Gavin is choosing a model that will allow employees to access corporate systems remotely. He would like to allow employees to use their own devices but would like to provision access in a way that allows them to use the data through a corporate-controlled computing environment without them having to transfer data to their own devices. Which one of the following models would best meet Gavin's needs?
- A. COPE
 - B. CYOD
 - C. BYOD
 - D. VDI
101. Justin is searching for rogue systems on his network and would like to detect devices that are responding to network requests but are not on his approved list. What tool can he use to identify the systems on a network that are responding to requests?
- A. sqlmap
 - B. OpenSSL
 - C. netcat
 - D. nmap
102. Nina is assisting a user who reports that he cannot connect to the wireless network in his building. The network continually shows a message requesting a network password. What is the most likely issue with this connection?
- A. Expired user account
 - B. Incorrect PSK
 - C. Incorrect user password
 - D. Incorrect SSID

103. An attacker has compromised a system on an organization's local network and has set up an encrypted tunnel to that system. He is now attempting to pivot by exploiting a zero-day vulnerability on a system located on the same LAN as the already compromised system. What type of intrusion detection system would be the most likely to detect the pivot attack?
- A. Signature HIDS
 - B. Heuristic HIDS
 - C. Heuristic NIDS
 - D. Signature NIDS
104. Greg is working with remote users to troubleshoot issues that they are experiencing with VPN connections when traveling to customer sites. He believes that customer firewalls are interfering with the VPN connection and is considering altering the VPN configuration to prevent this issue. What type of VPN connection is the least susceptible to this problem?
- A. TLS
 - B. IPsec
 - C. Split tunnel
 - D. Full tunnel
105. Mark is analyzing host antivirus logs in the aftermath of a system compromise. He discovers that the antivirus software did not detect malicious software that infected the system. Which one of the following is the least likely cause of this failure?
- A. Antivirus software failure
 - B. Outdated antivirus signatures
 - C. Zero-day attack
 - D. APT attack

Domain 2 Answers and Explanations

1. C. The **corporate-owned, personally enabled (COPE)** model allows employees to make personal use of corporate-owned devices. While **choose-your-own-device (CYOD)** and corporate-owned models do not preclude personal use, they do not necessarily allow it. **Bring-your-own-device (BYOD)** models use personally owned equipment, rather than corporate-owned equipment.
2. A. The use of different authentication requirements depending on the circumstances of the user's request is known as context-based authentication. In this scenario, authentication requirements are changing based upon the user's IP address, making it an example of context-based authentication.
3. C. Steganography is a set of techniques that are used to hide information within other files, in plain sight. The most common application of steganography is hiding information within images.
4. A. Any of these devices could conceivably be the culprit, but the most likely case is that a content filter is suddenly blocking sites that should be allowed. This often happens when the filter policy is incorrectly configured. A network firewall is less likely to block traffic based upon the identity of the website. An **intrusion prevention system (IPS)** may be conducting this type of filtering, but it is a less likely candidate than the content filter. A GPO could also be restricting access to websites, but this is not likely to happen across different operating systems as GPOs are a Windows technology.
5. C. While any of these explanations are plausible, this pattern of activity is indicative of a password change. Once the user changed his or her password, authentication began to fail and continued to fail as the device retried the connection automatically. The user eventually noticed and updated the password on the device, allowing it to resume normal connectivity.
6. C. The scenario gives us no reason to believe that the installation media is faulty or malicious. However, deploying the software in this way does run the risk of exceeding the organization's licensed allocation, putting them in jeopardy of violating the terms of their license agreement.
7. C. **Mobile device management (MDM)** solutions allow administrators to set policies that manage the configuration of mobile devices, as well as control the apps installed on those devices.
8. D. All of these tools may be useful in detecting missing patches. However, the most useful tool is a configuration management system. These tools have the ability to directly query the operating system to obtain real-time information on their patch level.

9. A. Dissolvable NAC uses a temporary agent that is removed immediately after the health check completes. This would be the best solution for Tina to deploy. A captive portal solution does not necessarily have the ability to perform health checking unless it is combined with a dissolvable agent. Permanent NAC would install software that remains on the student computers. Active Directory NAC would not be appropriate because the systems are unmanaged and, therefore, not accessible through AD.
10. C. The **domain component (DC)** of an LDAP entry contains portions of the domain name of a system. The OU component contains information about the organizational unit, while the CN component contains the common name. The ST component contains information about the state or territory.
11. B. Operating system updates and application updates frequently trigger file integrity alerts, as do system compromises. A CPU failure would result in a system crash, rather than a file integrity alert.
12. B. Mobile device management products do typically support remote wiping, application management, and configuration management, among other features. They do not provide carrier unlocking functionality, as this may only be performed by the wireless carrier that activated the device.
13. B. In round-robin load balancing, the load balancer assigns requests to servers sequentially. The load balancer does not use capacity information to determine scheduling. It simply assigns each incoming request to the next server in line.
14. C. The **netstat** command lists all of the active network connections on a system, as well as the status of ports that are listening for requests. The **tcpdump** command captures network traffic and would see active network connections but does not identify ports that are listening without an active connection. The **pstools** command is used to find information about processes running on a system but does not provide network port or version information. The **netcat** command is used to send information via a network pipe.
15. D. Addresses in the range of 169.254.0.0/16 are assigned by the **Automatic Private IP Assignment (APIPA)** protocol when a system is unable to receive an address via other means. An address that's received via DHCP or static assignment would override this address. An Active Directory preferred address is not a valid IP address assignment mechanism.
16. C. The illustration shows a VPN that connects multiple branches of the organization to a central office. This is a site-to-site VPN. Remote access VPNs are used to connect individual devices. It is not possible to tell from the diagram whether the VPN is using TLS or IPsec transport.

17. A. Rainbow table attacks use precomputed hash values to identify commonly used passwords in password files. They are quite effective against password files or shadow password files that contain passwords that have been hashed but have not been salted. Password expiration limits the length of time that a compromised password may be used for but does not prevent rainbow table attacks from being successful.
18. D. Banner grabbing queries a service for header information provided to clients. This information often includes the specific service running on a port, as well as version information. Port scanning will reveal the existence of a service on a port, but port scanning alone cannot identify version information unless it is supplemented with banner grabbing information. Steganography is a technique that's used for hiding data within images or other binary files. **Traceroute** is a command that's used to find the path between two systems on a network.
19. B. Port security restricts the number of unique MAC addresses that may originate from a single switch port. It is commonly used to prevent someone from unplugging an authorized device from the network and connecting an unauthorized device but may also be used to prevent existing devices from spoofing the MAC addresses of other devices.
20. D. This is a forward proxy because the proxy server is located on the same network as the user. It connects to remote web servers on behalf of the end user. It is not possible to determine whether this proxy server is performing caching and/or content filtering based upon this illustration.
21. D. While all of the attributes listed in the scenario may be true of the device, the USB on-the-go logo indicates that the device supports the USB OTG standard for acting as a host server for other devices, such as cameras, flash drives, or peripherals.
22. B. One of the functions provided by email gateways is the interception of sensitive messages destined for external locations. The gateway then informs the recipient that they have a secure message and the recipient logs into a website to receive the message over an HTTPS-protected connection. Firewalls and intrusion prevention systems do not provide this technology. While TLS is used in this solution, TLS alone is not capable of intercepting messages.
23. D. By default, the **traceroute** command uses UDP connections. This is different from the **ping** command, which uses ICMP by default.

24. D. In a bluejacking attack, the attacker uses a Bluetooth connection to display messages to the end user. This attack does not grant the attacker access to information stored on the device, as would occur in a bluesnarfing attack. Bluescreening and bluelining are made-up terms in the context of Bluetooth technology.
25. A. There are sometimes legitimate reasons for a system to deviate from a security baseline. Alan should investigate this issue and determine the reason for the deviation before taking more drastic action.
26. B. VPN connections established in transport mode encrypt the payload of data packets but do not provide encryption for packet headers. Transport mode connections do not support NAT traversal.
27. A. It is difficult for companies to restrict the social media activity of employees who are accessing the networks outside of working hours and without using corporate resources. It is perfectly reasonable to limit the use of corporate accounts, block social media use on corporate networks, and require the disclosure of corporate affiliations when discussing related matters.
28. B. The **ping** command transmits an ICMP echo request message to the target system, which may then respond with an ICMP echo reply message.
29. B. Vishing, or voice phishing, attacks always take place over telephone calls. Smishing attacks use SMS messages. Spear phishing or whaling attacks normally occur over email but may use any communications mechanism.
30. B. The antenna that's shown here is an example of a parabolic antenna.
31. B. Based on the information provided, we can only conclude that an ARP poisoning attack took place. This attack could have been used to conduct eavesdropping or man-in-the-middle attacks but there is not enough information provided to draw that conclusion. There is no evidence that DNS poisoning took place.
32. A. **Mail eXchanger (MX)** records contain information about the SMTP servers associated with a domain. A records are standard address mapping records. **Canonical name (CNAME)** records are used to create aliases for DNS names. Name Server (NS) records are used to identify DNS servers for a domain
33. D. Android applications must be in **Android Application Package (APK)** format to be sideloaded onto a device. IPA files are used for iOS applications, not Android applications. EXE files are applications designed for use on Windows systems. The ZIP format is a generic file compression format that is used in APK files, but Android applications are not stored in pure ZIP format.

34. C. The most likely problem is that the RADIUS server is not properly authenticating accounts. It is not likely to be a VPN server problem because users are able to contact the server but are failing at the authentication step. It is unlikely that users are entering their passwords incorrectly or using expired passwords because the issue is occurring for all users.
35. A. The primary risk that Carla must avoid is that the user may have access to systems after being terminated. In addition, Carla should avoid tipping off the user to the pending termination. Therefore, she should wait until she can verify that the termination meeting has started and then cut off the user's access during the meeting.
36. C. Encrypted LDAPS sessions use TCP port 636. Unencrypted LDAP sessions use TCP port 389. Port 3389 is used for GUI connections to devices using the **Remote Desktop Protocol (RDP)**. Port 443 is used for encrypted web connections using HTTPS.
37. D. Application whitelisting prevents the installation of any software that is not on a list of preapproved applications and would prevent users from installing software that is not on the authorized list. Blacklisting takes the opposite approach, where administrators list the software that may not be installed. Host firewalls and content filters do not generally block the installation of software.
38. A. The **Secure Sockets Layer (SSL)** is now considered an insecure protocol and should no longer be used. The secure replacement for SSL is **Transport Layer Security (TLS)**. The **Secure Shell (SSH)** protocol is a secure means for establishing connections between two systems, but it does not provide the same transport layer functionality as SSL and TLS.
39. C. Moving the access point or the client may resolve the interference, as might changing the wireless channel/band in use. Increasing bandwidth will only provide more capacity. Additional capacity will not resolve interference.
40. C. The **Authentication Headers (AH)** protocol supports only authentication and integrity for IPsec connections. The **Encapsulating Security Payload (ESP)** protocol supports confidentiality, integrity, and authentication.
41. D. The web application firewall is the device that most likely blocked the attack and would contain detailed information about the attack. If the WAF blocked the attack, records would not appear in the logs of the web server, the database server, or the host firewalls on any devices.

42. C. The **Network Time Protocol (NTP)** performs clock synchronization across devices. The Domain Name Service performs translations between domain names and IP addresses. The **Dynamic Host Configuration Protocol (DHCP)** provides IP addresses to systems. The **Border Gateway Protocol (BGP)** is used to configure network routing.
43. C. Storage segmentation provides separate storage areas on the mobile device for personal and corporate information, preventing the two from becoming intermingled. Application control would limit the applications that users may install on devices but would not control where those applications store data. Full device encryption would add security to all data stored on the device but would not differentiate between personal and corporate data. Multifactor authentication does add a layer of security to the device but does not distinguish between categories of information.
44. D. When measuring RSSI, the network with the strongest signal is the one with the highest value. Since RSSI is measured in negative numbers, this will be the number closest to zero which, in this case, is -67, corresponding to the CAFwifi network.
45. B. All of the protocols listed here have the capability of supporting secure video conferencing. Of the options, HTTPS is the most likely to be fully supported by customer firewalls because it is the same port that's used for secure web connections. Therefore, this would be the best option for Dylan to choose.
46. B. All of the capabilities listed here are features of advanced malware prevention systems. However, only threat intelligence directly leverages information obtained from systems deployed at other customer sites.
47. B. There is not enough information in the scenario to determine whether host-based or network-based DLP would be more appropriate. The main choice facing Ron is whether to use pattern matching or watermarking. Pattern matching looks for data that matches the format of known sensitive data elements, such as Social Security numbers or credit card numbers. Watermarking tags sensitive documents and then watches for those tags in network traffic. In this case, Ron has a specific set of documents that he would like to protect, so watermarking would be the best solution.
48. C. This error message indicates that the website is using a certificate from an untrusted certificate authority. Patricia should replace the certificate with one from a trusted CA.

49. D. Dennis should consult his manager to determine the appropriate next steps. He should not confront the user directly. While his manager may direct him to block the websites, this is a management decision that Dennis should not take on himself.
50. C. The IP address for this machine is shown in the record for the Ethernet interface en0. It is 10.36.23.22. The address 10.36.23.255 is the broadcast address associated with that adapter and not the IP address of the machine. 127.0.0.1 is the local loopback address for any system. 98:e0:d9:87:8a:73 is the MAC address for the en0 interface and not an IP address.
51. A. Honeypots are systems that are deliberately designed to attract attackers and monitor their activity. Honeynets are entire networks of decoy systems. Darknets are unused portions of IP space that are used to identify scanning attempts. Sinkholes are false DNS entries that are created to prevent users from accidentally contacting malicious systems.
52. D. Tom should deploy an agent-based NAC solution or, more specifically, a permanent agent. This technology leaves software running on the endpoint that may remain in constant contact with the NAC solution. Agentless NAC, captive portal solutions, and dissolvable agents do not maintain a constant presence on the system and would not meet Tom's requirements.
53. C. In a true positive report, the system reports an attack when an attack actually exists. A false positive report occurs when the system reports an attack that did not take place. A true negative report occurs when the system reports no attack and no attack took place. A false negative report occurs when the system does not report an attack that did take place.
54. D. Both the tcpdump and Wireshark utilities can be used to capture network traffic. Of those two, only tcpdump is a command-line utility. Wireshark uses a graphical interface. Nmap is a network port scanner, while netcat is used to redirect data to a network connection. Neither Nmap nor netcat can capture traffic.
55. A. The IP address 192.168.10.6 falls within the private IP address range of 192.168.0.0/16. This address range is only for use on a local area network and should never be seen on a public network, such as the internet. The other addresses provided in this question are all valid public IP addresses.
56. A. **Wi-Fi Protected Access version 2 (WPA2)** uses the AES encryption standard and provides the highest level of security for a Wi-Fi network. WPA version 1 uses the **Temporal Key Integrity Protocol (TKIP)**, which is secure but not as strong as WPA2. **Wired Equivalent Privacy (WEP)** is an insecure encryption technique.

57. B. **Satellite communications (SATCOM)** have the widest availability, as they may be used from any region of the world with satellite coverage. For large satellite networks, this covers the entire planet. Cellular signals do travel long distances but may not have constant availability in rural areas. Wi-Fi and Bluetooth are only useful over short distances and would not be appropriate for this scenario.
58. A. Metasploit is an exploitation framework commonly used in penetration testing. Cain and Abel is a password cracking utility. Nessus is a vulnerability scanner. Sysinternals is a set of Windows system administration tools.
59. D. **Write once, read many (WORM)** storage devices allow us to write data in a permanent fashion where modification is impossible. Cryptographic hashing and file integrity monitoring solutions may detect unauthorized changes, but they are unable to prevent unauthorized changes. **Transport layer security (TLS)** is an encryption protocol that would not prevent changes to stored data.
60. A. Brian can use a **preshared key (PSK)** known only by him to restrict network access. Kerberos or NAC authentication would require configuration and a costly infrastructure. MAC address filtering is easily defeated and should not be relied upon for secure network access controls.
61. B. Asset management practices include tracking a physical hardware inventory, which would help maintain accurate device location information. Change and configuration management systems would not generally track the physical location of a device. Firewalls are network security devices, which would not help meet this requirement.
62. A. The -Pn flag disables the host discovery step and scans every specified system. The -PS flag conducts a TCP SYN ping, while the -PA flag conducts a TCP ACK ping. The -PU flag conducts a UDP ping.
63. A. IPsec has two modes of operation: tunnel mode and transport mode. Tunnel mode is primarily used for site-to-site connections, such as the one that Carrie is establishing here. Transport mode is normally used for connections involving endpoint devices.
64. C. Port 1433 is commonly associated with Microsoft SQL Server databases, while port 1521 is used by Oracle databases. Port 3306 is the default port for MySQL databases. Port 1701 is used by the L2TP protocol, which is associated with VPN access, not databases.
65. C. When registering DNS entries for a load-balanced service, administrators should assign the entry to a virtual IP address that maps to the public interface of the load balancer.

66. D. In this case, the explicit permission that's granted to the user to write the file overrides the deny permission, which is inherited (denoted by the grey shading). Therefore, the user can both read and write the file.
67. C. Eric can use a protocol analyzer to sniff network traffic and search the contents for unencrypted sensitive information. A **data loss prevention (DLP)** solution could automate this work, but that is not one of the options available to Eric.
68. A. The S/MIME secure email standard allows organizations to achieve confidentiality, integrity, and non-repudiation for email communications.
69. D. SNMPv3 is the current standard for network management and is a secure protocol. Older versions of SNMP did not provide secure authentication due to their use of plaintext community strings.
70. A. Data loss prevention systems are designed to prevent the exfiltration of sensitive information, while intrusion prevention systems are designed to block attack traffic. Since Greg is attempting to block the exfiltration of sensitive information, he should choose a DLP solution. The threat that Greg wants to defend against does not use the network, so he should choose a host-based DLP that offers USB blocking capabilities.
71. D. Push notification uses a secure mechanism to notify users of mobile devices. The **Apple Push Notification Service (APNS)** is an example of a secure push notification mechanism. SMS (text messaging) notifications have insecurities, particularly when used with VoIP numbers. MMS is used for multimedia messages and is not appropriate for an authentication solution. TLS is a generic transport layer security protocol and cannot be used to directly deliver notifications to mobile devices.
72. A. Users may bypass the manufacturer's installed operating system by installing their own custom firmware on the device. This may remove any MDM configuration that Dave places on the device before providing it to the user. Application sideloading can install illicit applications on a device but does not replace the operating system. Bluejacking and Bluesnarfing are attacks against Bluetooth connections but do not alter the operating system on a device.
73. D. In this scenario, Scott would like to choose a technology that automatically triggers VPN connections based upon security policies. Microsoft's Always On VPN technology provides this feature. TLS and IPsec VPNs are different VPN protocols but they do not inherently have the ability to trigger a VPN connection. Split tunneling policies control what information is routed through the VPN connection but they do not have the ability to require or initiate a VPN connection.

74. C. Mobile device management products support all four of these features. Containerization may be used to isolate corporate content from personal content. Remote wiping may be used to remove data from a lost or stolen device. Encryption may be used to protect data from theft. Geofencing does not prevent the theft of data.
75. B. **Security information and event management (SIEM)** solutions aggregate and correlate log entries that are received from a wide variety of sources. **Data loss prevention (DLP)** systems seek to prevent the exfiltration of sensitive information from the organization. **Intrusion prevention systems (IPS)** block potentially malicious network traffic. **Network access control (NAC)** solutions prevent unauthorized systems from connecting to the network.
76. C. **Data execution prevention (DEP)** requires the explicit marking of memory regions as executable, preventing malicious attacks that seek to execute code out of other regions of memory.
77. A. The most common false positive report for application whitelisting results from an unexpected update from the software vendor that changes the signature of the application. A user downloading software from the web should generate an alert, so this would not be a false positive. The same thing is true for malicious activity, such as the execution of malware or the installation of a rootkit.
78. B. In an active/passive configuration, one load balancer remains unused while the other load balancer handles all traffic. If the active load balancer fails, the passive load balancer takes over. This is a high availability, fault-tolerant configuration and it is easily maintained. It does not, however, use the full capacity of both devices.
79. D. This is an example of an access control list from a router. Of the devices listed, only routers and firewalls perform network filtering of the type that would be defined by these types of rules. However, if these rules had come from a firewall, they would contain more detail, including source and destination ports.
80. D. Wi-Fi networks use the **service set identifier (SSID)** to broadcast a network name to all the devices in the area. SSID broadcasting advertises the presence of the Wi-Fi network.
81. D. Hosts on an internal network should never see port scans coming from external networks. The fact that these packets are reaching the host indicates that the network perimeter firewall is improperly configured.

82. A. EXIF metadata includes a wide variety of technical and environmental information about photos that have been shot with digital cameras and smartphones. This information commonly includes geolocation information obtained from the device's GPS, as well as the camera's make and model, shutter speed, and other technical characteristics. It does not normally include temperature information as these devices typically do not include thermometers that measure ambient temperature.
83. C. **Mobile device management (MDM)** technology allows administrators to control the configuration of mobile devices, such as disabling device cameras. **Data loss prevention (DLP)** systems may be useful in preventing the theft of confidential information but cannot disable device cameras. **Intrusion prevention systems (IPS)** and **web application firewalls (WAF)** are also good security controls but do not manage mobile device configurations.
84. C. Stateful inspection firewalls monitor the connection status by tracking the TCP handshake. They maintain a table of active connections and automatically allow traffic that is part of an established connection without requiring the reevaluation of the ruleset for each packet. The other firewall types listed here are more primitive and do not track connection status. They simply reevaluate every packet that they receive.
85. A. Apple Pay, Google Wallet, and similar contactless payment technologies rely upon **near-field communication (NFC)** to facilitate communications between a user's smartphone and the payment terminal.
86. B. The primary issue with FTP is that it does not support the use of encryption. Credentials and other information sent via FTP are transmitted in cleartext and are open to eavesdropping attacks.
87. B. **Next-generation firewalls (NGFW)** are traditional firewalls with advanced capabilities, including defense against application layer attacks, such as SQL injection. Of the choices listed, an NGFW is the best solution to meet all of these requirements. Packet filters and router ACLs would not be effective against all of the attacks listed here. A web application firewall does not normally contain the routing technology necessary to be the organization's main connection to the internet.
88. A. UTM solutions typically perform a wide variety of security functions, including content filtering, intrusion prevention, and firewalling. They do not typically perform sandboxing, as this is typically a capability of more advanced malware prevention systems.

89. A. Web servers use port 80 for unencrypted communications using the HTTP protocol and port 443 for encrypted communications using the HTTPS protocol. Those are the two ports that Jaime should allow through the firewall. Port 53 is used for DNS, while port 8080 is a non-standard port that's sometimes used for proxies or as an alternate location for web services. Neither of those situations are mentioned in the scenario.
90. B. Degaussing applies strong magnetic fields to a storage device in order to remove the data that is stored magnetically on that device.
91. B. Mobile devices purchased under contract are locked by the carrier to prevent transfers to other carriers while the contract is in place. After the expiration of the contract, the original carrier must unlock the device before the user may transfer it to another carrier.
92. B. Ad hoc and direct Wi-Fi networks allow the establishment of Wi-Fi connectivity between devices without the use of enterprise infrastructure. Therefore, these Wi-Fi operating modes do not support the use of enterprise authentication. Wi-Fi networks using **preshared keys (PSKs)** use these PSKs in lieu of enterprise authentication. WPA and WPA2 both support the use of enterprise authentication in place of a PSK.
93. C. Data loss prevention systems that use pattern matching are most likely to generate false positive reports because data in a file might match a pattern by happenstance. Watermarking and removable media control techniques do not typically generate false positive reports. Software updates would not be detected by a DLP system.
94. C. Flood guard technology is used to block denial of service attacks on a network. Loop prevention, hold-down timers, and split horizon are all used to prevent and correct routing loops.
95. B. The **Secure Real-Time Protocol (SRTP)** is a secure, encrypted protocol designed specifically to support VoIP communications. The Simple Network Management Protocol is designed to facilitate management of network devices. **Secure Shell (SSH)** is a tool for encrypted administrative connections to systems. **Transport Layer Security (TLS)** may be used to encrypt VoIP communications, but it is a general-purpose encryption protocol and is not specifically designed to secure VoIP communications.
96. A. Email security gateways commonly perform spam filtering, malware filtering, data loss prevention, and encryption. They do not typically serve as a network firewall.

97. D. The implicit deny rule is the last rule that's found in a firewall rulebase and is part of the firewall's default configuration. It specifies that any traffic that was not explicitly allowed by an earlier rule should be blocked.
98. B. IP reputation services are a form of threat intelligence that provides organizations with a frequently updated list of known malicious IP addresses that can be automatically blocked at the firewall. Malware and IDS signature updates are also important security controls but they do not identify known malicious systems and rather identify patterns of suspicious activity. Behavioral analysis systems watch for anomalous patterns of activity rather than relying upon lists of known malicious systems.
99. A. Any of the solutions presented may resolve the issue that Ralph is experiencing, but deploying a Wi-Fi controller is the most efficient approach. Wireless controllers allow the automated modification of access point settings so that they can be adapted to the changing radio frequency environment.
100. D. **Virtual Desktop Infrastructure (VDI)** environments allow employees to access a remote desktop computing environment and work within that environment without transferring data to the device used to access the VDI desktop. The **choose-your-own-device (CYOD)** and **corporate-owned, personally enabled (COPE)** models do not involve employee-owned devices. The **bring-your-own-device (BYOD)** model does allow the use of personal devices but does not necessarily prevent the transfer of corporate information to the device.
101. D. The Nmap tool performs network mapping and is the ideal way for Justin to develop a list of systems providing network services. OpenSSL is an encryption tool that would not help Justin meet his goal. Netcat lists the open connections and listening services on a single system but does not do this across a network. The sqlmap tool is used to scan database applications for vulnerabilities.
102. B. The use of a network password indicates that this network is using a **preshared key (PSK)** rather than user authentication. Therefore, the most likely issue is that the user is entering the PSK incorrectly.
103. B. This attack is taking place between two systems located on the same LAN, so it is unlikely that a **network-based IDS (NIDS)** would detect the traffic. A **host-based IDS (HIDS)** would be much more likely to do so. Signature-based systems are not capable of detecting zero-day attacks, so a heuristic system would be the most likely to detect the attack.

104. A. TLS VPNs typically use port 443, the same port that's used for HTTPS web traffic. This port is commonly allowed full outbound access through firewalls. IPsec VPNs use UDP port 500, as well as IP protocols 50 and 51. It is much more likely that this traffic will be blocked at a firewall. It is irrelevant whether Greg uses a split tunnel or full tunnel policy in this case as the policy will not help establish the connection through the firewall; it will only control what traffic is routed through the VPN connection once it is established.
105. A. There is no indication in this scenario that Mark discovered log entries indicating any type of software failure. The failure most likely resulted from the use of malware for which the scanner did not have current signatures. This could be because the scanner had not been updated or it may be because the attacker used a zero-day/APT attack.

3

Architecture and Design

Domain 3 Questions

1. Ralph is working with his organization to implement a new cloud storage solution. He would like to protect the data stored in this cloud service against an attack being waged by a malicious insider employed by the vendor. What is the best control to provide this defense?
 - A. Two-factor authentication
 - B. Encryption
 - C. Least-privilege access controls
 - D. Strong passwords
2. Ron is concerned about the potential of attackers exploiting issues in the operating system supporting a virtualization hypervisor to gain access to information stored by guest operating systems. What type of hypervisor can he use to minimize this risk?
 - A. Type 1 hypervisor
 - B. Type 2 hypervisor
 - C. Type 3 hypervisor
 - D. Type 4 hypervisor
3. Which one of the following temperature and humidity readings falls outside of the recommended environmental ranges for data centers set by the **American Society of Heating, Refrigeration, and Air Conditioning Engineers (ASHRAE)**?
 - A. 80 degrees Fahrenheit and 45% relative humidity
 - B. 65 degrees Fahrenheit and 55% relative humidity
 - C. 60 degrees Fahrenheit and 25% relative humidity
 - D. 75 degrees Fahrenheit and 55% relative humidity
4. James would like to implement RAID 5 redundancy for the hard drives he is placing in a server. What is the minimum number of disks necessary to implement this approach?
 - A. 1
 - B. 2
 - C. 3
 - D. 5

5. Ed is selecting a load balancing algorithm for use in his organization's web environment. There are substantial differences between the performance characteristics of the servers in the web farm, and there are also significant differences in the lengths of user connections. Which load balancing algorithm would produce the best results for Ed?
 - A. Weighted Round Robin
 - B. Least Connections
 - C. Round Robin
 - D. Weighted Least Connections
6. Which one of the following combinations of controls introduces control diversity across the major control categories?
 - A. Background checks and security training
 - B. DLP and IPS
 - C. IPS and backups
 - D. DLP and background checks
7. Barry's organization follows the Center for Internet Security's benchmarks for Windows Server security. He is working with a developer who insists that a security setting must be changed to allow an application to function properly. What should Barry do next?
 - A. Allow the change
 - B. Implement a compensating control
 - C. Deny the change
 - D. Evaluate the change and determine whether it is appropriate
8. Which one of the following approaches to hard drive encryption uses a drive that performs the encryption itself?
 - A. Chipset FDE
 - B. Enclosed FDE
 - C. SED
 - D. Bridge FDE

9. What is the primary risk associated with storing API keys in a public GitHub code repository?
 - A. Unauthorized provisioning of resources
 - B. Theft of sensitive information
 - C. Unauthorized API use
 - D. Denial-of-service attacks
10. Which one of the following biometric security controls requires users to come into the closest physical proximity of the device?
 - A. Retinal scanning
 - B. Iris scanning
 - C. Facial recognition
 - D. Voice recognition
11. Betty is responsible for managing the digital certificates on her organization's servers. The certificate on the main public web server is about to expire. What must Betty do?
 - A. Obtain a new certificate from the CA
 - B. Generate a new certificate using the server's private key
 - C. Renew the certificate using the server's private key
 - D. Place the certificate on the CRL

12. Gina is preparing an application server that will be used by employees within her organization to manage payroll. Review the basic network diagram shown here. Gina will place the server on a protected subnet of one of these network zones. Which zone is the most appropriate?

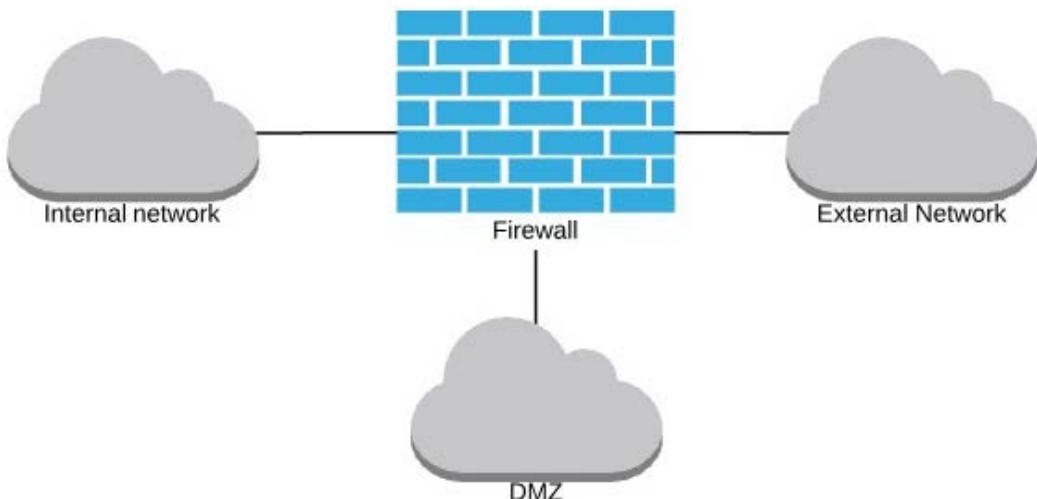


Figure 3.1

- A. Internal network
 - B. External network
 - C. DMZ
 - D. None of the above
13. Which one of the following is a compiled programming language?
- A. JavaScript
 - B. C++
 - C. R
 - D. PHP
14. Which one of the following is an example of a platform-as-a-service (PaaS) computing environment?
- A. Slack
 - B. Microsoft Office 365
 - C. Amazon EC2
 - D. Google App Engine

15. Denise is reviewing the security of her network's management plane against the vendor's security baseline. Which one of the following protocols should she not expect to see allowed on the management plane?

- A. RADIUS
- B. NTP
- C. SSH
- D. RTP

16. Refer to the network shown here. What technology must be supported by the firewall in order for this network to function properly?

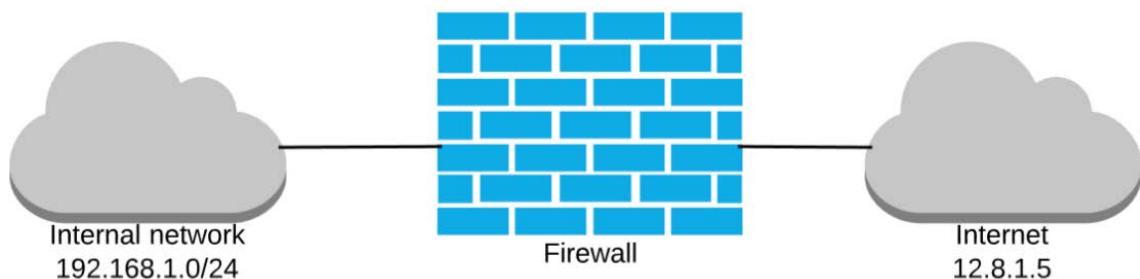


Figure 3.2

- A. IPS
 - B. NAC
 - C. NAT
 - D. WAF
17. Carl is designing a database-driven web application. If he follows the principle of least functionality, what is the minimum number of servers he should use?
- A. 1
 - B. 2
 - C. 3
 - D. 4

18. Ingrid is preparing a standby server that her organization will activate to achieve redundancy in the event of a system failure. The server will be placed in the rack in a configured state and may be turned on for immediate functionality when needed. What type of server has Ingrid prepared?
- A. Active spare
 - B. Hot spare
 - C. Cold spare
 - D. Warm spare
19. Barry is designing a site-to-site VPN to support remote office access to corporate resources, as shown here. Which one of the following devices would be the best place to terminate the VPN connection at the central office?

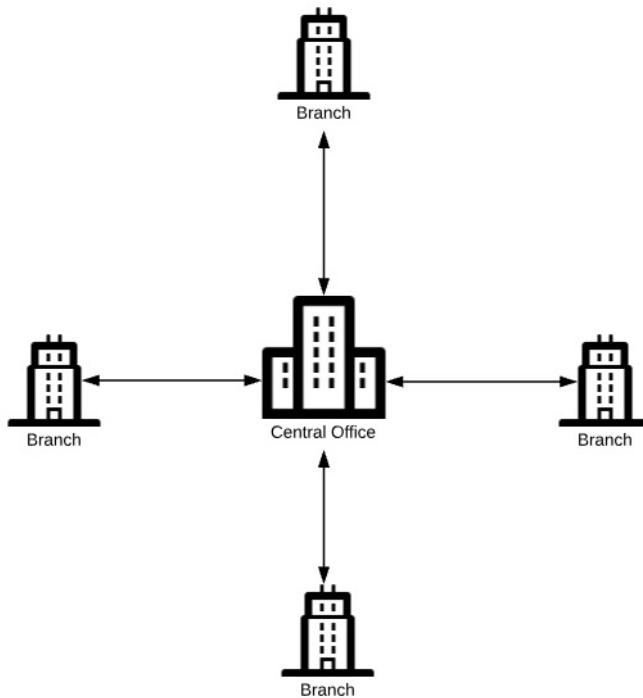


Figure 3.3

- A. VPN server
- B. Router
- C. Firewall
- D. VPN concentrator

20. Gina receives a piece of digitally signed code from one of her suppliers and would like to verify the digital signature on the code. What key should she use to verify the signature?
- A. Her own public key
 - B. The supplier's private key
 - C. The supplier's public key
 - D. Her own private key
21. Paul's organization has a high availability web server cluster composed of six servers that all handle user requests. In a high-availability configuration, how many servers can Paul lose without causing a complete loss of service to end users?
- A. 1
 - B. 2
 - C. 4
 - D. 5

22. Which element of the NIST Cybersecurity Framework, shown below, involves the development and implementation of appropriate safeguards to ensure the delivery of critical services?



Figure 3.4

- A. Identify
- B. Protect
- C. Respond
- D. Recover

23. Paul's company offers an unencrypted wireless network for use by visitors to their chain of retail stores. Employees sometimes use this network for convenience because the secured wireless network is known to have authentication issues. When an employee connects to the unencrypted network, what network zone should they be placed on?
- A. Guest network
 - B. Intranet
 - C. Extranet
 - D. DMZ
24. In a data center using the hot aisle/cold aisle approach, where should air conditioner vents be positioned to distribute cold air?
- A. Above racks
 - B. At the back of racks
 - C. At the front and back of racks
 - D. At the front of racks
25. Tony would like to use input validation to prevent SQL injection attacks against his organization's web applications. Where should Tony place input validation code to ensure maximum effectiveness?
- A. Within JavaScript code
 - B. Database server
 - C. Endpoint systems
 - D. Web server
26. Elaine is installing an intrusion detection system and would like to ensure that her device sees all network traffic crossing a link. She is also concerned about the system causing a network outage if it fails. Which installation approach would be the most appropriate in this situation?
- A. TAP
 - B. SPAN
 - C. Port mirroring
 - D. Inline installation

27. Dylan is working to protect his organization against integer overflow attacks. He has a web application that stores the weight of an individual in a database. The weight value is stored as an 8-bit positive integer. What is the maximum weight that may be stored in this field?
- A. 255
 - B. 127
 - C. 511
 - D. 1,023
28. Which one of the following security tools is best able to perform file integrity monitoring?
- A. Wireshark
 - B. Snort
 - C. Tripwire
 - D. QRadar
29. Devin manages a shared computing environment for multiple customers and is worried about one of his customers accessing virtual machines owned by other customers. He would like to protect against these virtual machine escape attacks. What is the best control that he can implement?
- A. Hypervisor patching
 - B. Network firewall
 - C. Input validation
 - D. Port security
30. Upon booting a laptop, Yvonne sees the password prompt shown here. What is presenting this prompt?

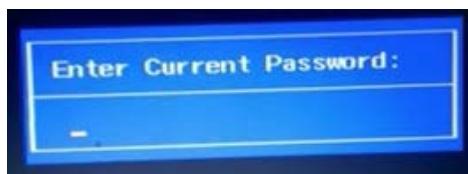


Figure 3.5

- A. Active Directory
 - B. BIOS
 - C. TPM
 - D. HSM
31. Kassie's company is considering the use of a cloud service to manage their hotel reservations. Employees would use a web interface to access the application located in the vendor data center. The vendor handles all installation tasks, deploys and scales the infrastructure, and maintains the source code. Kassie's company is only responsible for application configuration and authorization control. What type of cloud computing environment is Kassie's organization using?
- A. PaaS
 - B. IaaS
 - C. SaaS
 - D. SecaaS
32. Brandy is using a computer at a hotel business center and she is concerned that the operating system on the device may be compromised. What is the best way for her to use this computer in a secure fashion?
- A. Use live boot media
 - B. Run a malware scan
 - C. Connect to a VPN
 - D. Only access secure websites
33. Which one of the following characteristics does not describe a hardware root of trust?
- A. It should be secure by design.
 - B. It should be implemented in hardware.
 - C. It should contain as much of the operating system as possible.
 - D. It should be trusted by components at higher layers of abstraction.

34. Fran is working with her organization's IT operations team to troubleshoot an issue on their web servers. They discover that the CPU load on all of their web servers is quite high and they would like to reduce that load without purchasing additional web servers. Which one of the following technologies would best address this situation?
- A. Weighted least connections load balancing
 - B. Round-robin load balancing
 - C. SSL acceleration
 - D. Web application firewall
35. Katie is testing a new application and recently completed unit testing. She would now like to run a series of tests designed to confirm that the tested units will work together properly. What type of software testing should Katie run next?
- A. Design testing
 - B. Functional testing
 - C. Acceptance testing
 - D. Integration testing
36. Helen is the developer of a new application that recently completed all testing and now resides in a staging environment. She is ready to release the code to production. Who is the most appropriate person to trigger the code transfer?
- A. Helen's supervisor
 - B. Change manager
 - C. Another developer on Helen's team
 - D. Helen

37. Martha is placing an IPS sensor on her network and would like to place it in a location where it will receive the least traffic, but is likely to intercept any SQL injection attack that might reach the web server located in the DMZ. Which network location is the best place to position the sensor, given the network diagram shown here?

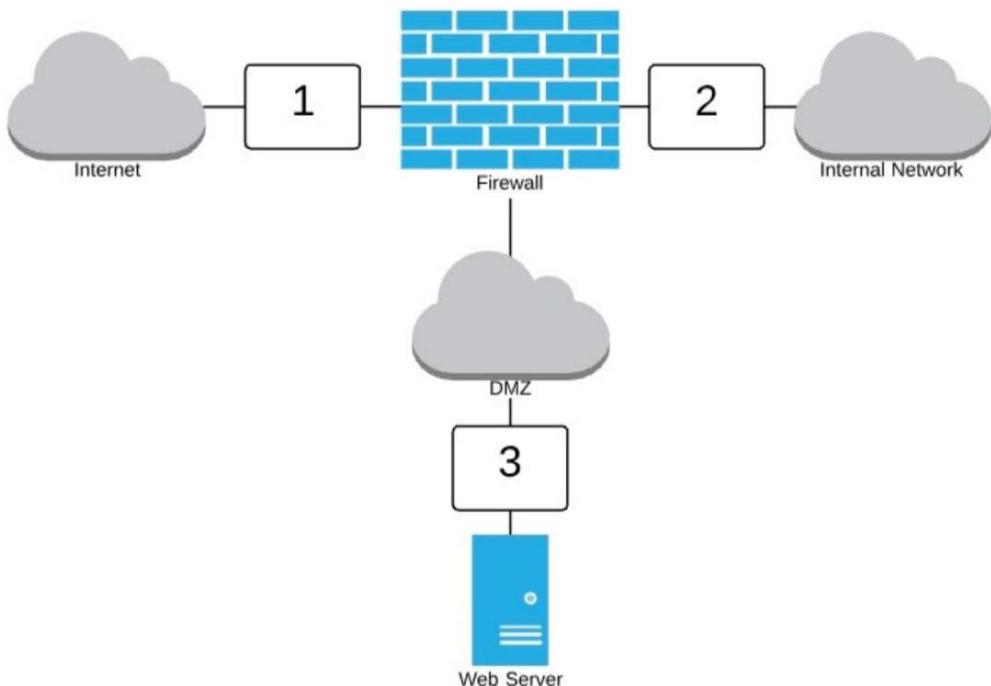


Figure 3.6

- A. Location 1
 - B. Location 2
 - C. Location 3
 - D. Locations 1 and 2
38. Which one of the following security devices is least likely to perform content filtering services to protect end users against malware infections?
- A. IPS
 - B. Firewall
 - C. Proxy
 - D. Router

39. Which one of the following is not an example of a physical security control?

- A. Exterior lighting
- B. System ACL
- C. Secure equipment enclosures
- D. Faraday cageS

40. When configuring **access control lists (ACLs)** on a Cisco router, what limitation of standard ACLs does not exist for extended ACLs?

- A. Standard ACLs cannot perform outbound filtering.
- B. Standard ACLs cannot filter based upon the source IP address.
- C. Standard ACLs cannot perform inbound filtering.
- D. Standard ACLs cannot filter based upon the destination IP address.

41. Carl is selecting a computing environment for a machine learning workload. The nature of the workload is that it uses resources intensely for several hours each evening and does not need resources at other times of the day. What computing model would be the most cost-effective for this type of workload?

- A. Remote data center
- B. On-premises computing
- C. Cloud computing
- D. Colocation facility

42. Tonya is considering the use of a security-as-a-service deployment model for her organization's identity and access management solutions. She is planning to use a well-respected vendor with a mature service. Which one of the following attributes should cause her the greatest concern?

- A. Confidentiality
- B. Latency
- C. Non-repudiation
- D. Reliability

43. Devin is a developer who recently received some code from an overseas partner, and he is suspicious that it may contain malicious content. He would like to run the code to confirm or deny his suspicions. What environment should he use to perform this testing?
- A. Production
 - B. Test
 - C. Development
 - D. Sandbox
44. What IPSec mode is most commonly used to create site-to-site VPNs between locations?
- A. Tunnel mode
 - B. Transport mode
 - C. Internet key exchange mode
 - D. Security association mode
45. In a virtualized environment, what is the easiest way to restore a virtual system to a previous known good state?
- A. Rebuild the system.
 - B. Restore from full backup and then apply differential backups.
 - C. Restore from full backup and then apply incremental backups.
 - D. Revert to a snapshot.
46. Zack is concerned about the potential for DDoS attacks against his organization that may consume all of their available network bandwidth. What entity is in the best position to implement controls to limit the impact of these attacks?
- A. Zack's ISP.
 - B. Zack's organization.
 - C. Nobody is able to mitigate the impact of a distributed attack.
 - D. The attacker's ISP.

47. Katie encounters a fire in her building that appears to have started in a bundle of electrical wires. Which one of the following fire extinguishers would be the most appropriate to combat this fire?
- A. Class A
 - B. Class B
 - C. Class C
 - D. Class D
48. Trevor is seeking an open source version control system for use in his software development environment. Which one of the following tools would not meet his requirements?
- A. Git
 - B. Visual SourceSafe
 - C. Subversion
 - D. CVS
49. Liam is securing a series of endpoints that run Microsoft Windows operating systems. He would like to use an automated mechanism to apply security settings to those systems. What technology can he use to do this?
- A. FQDNs
 - B. GPOs
 - C. MACs
 - D. TLS
50. Carla is the firewall administrator for a large university. She has recently seen a flurry of activity from student networks sending spam print jobs to printers located in administrative offices. She would like to block printer traffic between network segments using the standard HP JetDirect port. What port should she block?
- A. UDP port 9100
 - B. TCP port 9100
 - C. TCP port 8080
 - D. UDP port 8080

51. Which one of the following automation techniques provides a preconfigured baseline version of an operating system that is configured to meet the organization's security standards and is ready for customization to perform workload-specific tasks?
- A. Template
 - B. Live boot media
 - C. Master image
 - D. Standard
52. Tim is performing input validation for a free-text field in a web application. He would like to protect against SQL injection attacks. Which one of the following characters is the most crucial to sanitize?
- A. >
 - B. "
 - C. <
 - D. '
53. Travis is placing a new web server on his organization's network. The server will provide information to the general public. Which network zone is the most appropriate placement for this server?
- A. Extranet
 - B. Intranet
 - C. DMZ
 - D. Guest network

54. What type of security control is shown here?



Figure 3.7

- A. Airgap
 - B. Mantrap
 - C. Bollard
 - D. Hot aisle
55. Which one of the following tools can be used to perform DNS queries on a Windows system without requiring the installation of non-standard software?
- A. Dig
 - B. Nslookup
 - C. Nbtstat
 - D. Arp
56. Norma is employed by an online retailer that processes credit card payments thousands of times each day. Which one of the following regulations definitely applies to her organization?
- A. PCI DSS
 - B. HIPAA
 - C. FERPA
 - D. Sarbanes-Oxley

57. What do most physical security professionals consider the minimum fence height to slow down a determined intruder?
- A. 12 feet
 - B. 4 feet
 - C. 6 feet
 - D. 8 feet
58. When deploying a wireless network, which network zone offers the most appropriate placement for wireless users?
- A. Wireless users should be placed on the extranet.
 - B. Wireless users should be placed on the guest network.
 - C. Wireless users should be placed on the intranet.
 - D. Wireless users should be placed on the same network zone they would be placed on if they connected to a wired network.
59. What security standard provides the requirements for an operating system to be certified as a trusted operating system according to the federal government?
- A. Common Criteria
 - B. TCSEC
 - C. CIS
 - D. Windows Secure Configuration Guide
60. Which one of the following technologies separates applications into their own virtualized environment where each uses the kernel of the underlying operating system?
- A. Type 2 virtualization
 - B. Bare metal virtualization
 - C. Type 1 virtualization
 - D. Application containers

61. When using Windows BitLocker in transparent operation mode, what is used to decrypt the key protecting data stored on the disk?

- A. USB key
- B. Active Directory
- C. User password
- D. Trusted Platform Module

62. What type of hypervisor is shown in the following diagram?

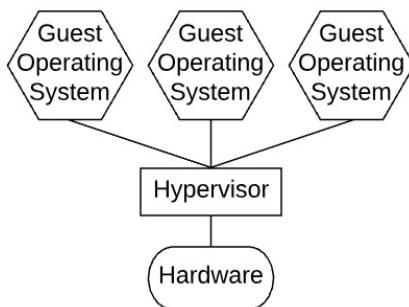


Figure 3.8

- A. Type 1 Hypervisor
- B. Type 2 Hypervisor
- C. Type 3 Hypervisor
- D. Type 4 Hypervisor

63. Which one of the following features is not normally included in a proxy server?

- A. Caching
- B. Content filtering
- C. Route optimization
- D. Anonymization

64. Wanda would like to disable unnecessary services on a Windows 10 system in her organization. What tool should she use to do this?

- A. Event Viewer
- B. Programs and Features
- C. Computer Management
- D. Disk Management

65. Tim is designing a remote access VPN for use by employees traveling to customer sites on sales calls. His primary objective is to ensure that employees will be able to access the VPN from customer networks without requiring that the customers reconfigure their networks to allow this access. What type of VPN would best meet Tim's needs?
- A. TLS
 - B. IPSec
 - C. PPTP
 - D. L2TP
66. Consider the application input shown here:
- \uFE64script\uFE65
- What technique should a developer use prior to submitting this string for input validation?
- A. Normalization
 - B. Concatenation
 - C. Tokenization
 - D. Substitution
67. Joan is designing the fire suppression system for a new data center in Missouri and would like to choose a system that, if discharged, would be the least damaging to the equipment in the data center. What is her best option?
- A. FM-200
 - B. Halon
 - C. Wet pipe
 - D. Dry pipe
68. Florence is installing a concealed CCTV system outside her organization's data center. Which one of the following statements is the most likely to be correct as regards this system?
- A. The system will be helpful in preventing security violations.
 - B. The system will be helpful in deterring security violations.
 - C. The system will be helpful in detecting security violations.
 - D. The system will be extremely expensive.

69. Rob's organization is considering the deployment of software-defined networking (SDN). Which one of the following statements is not correct as regards SDN?
- A. SDN facilitates network segmentation.
 - B. SDN combines the control plane and the data plane.
 - C. SDN creates a programmable network environment.
 - D. SDN increases network complexity.
70. Ben is designing a network that will support the ICS and SCADA systems at a nuclear power plant. What security technology should he use to segment these networks from other systems?
- A. Physical segmentation
 - B. VLANs
 - C. VPNs
 - D. IPS
71. Jamie is concerned about attackers using a web application to engage in cross-site scripting attacks against her organization. Which one of the following techniques is not a good defense against these attacks?
- A. Server-side input validation
 - B. Client-side input validation
 - C. Query parameterization
 - D. Stored procedures
72. Why should administrators only allow employees to download digitally signed applications to mobile devices?
- A. Digitally signed applications are certified to function properly.
 - B. Digitally signed applications are free of malware.
 - C. Digitally signed applications come from known sources.
 - D. Digitally signed applications are guaranteed by Apple.

73. Fran recently completed development of a new code module and the module successfully completed user acceptance testing. Now that testing is complete, she would like to request that the module be moved to the next step in the process. What environment is the most appropriate for the code at this stage of the process?
- A. Staging environment
 - B. Development environment
 - C. Production environment
 - D. Test environment
74. Joe is responsible for providing end user computing to a large organization that allows a BYOD approach for most users. He needs to provide users with a way to access a very expensive desktop software package that has limited licenses and may not be installed on personally owned devices due to license restrictions. He wants to provide users with a desktop environment where they can log in and interact with the software while being isolated from each other. What type of environment is the most appropriate for this purpose?
- A. DLP
 - B. Web-based client
 - C. VPN-based client
 - D. VDI
75. Which one of the following devices would be the least likely to run a desktop or server operating system?
- A. Endpoint computing device
 - B. Multifunction printer
 - C. IoT sensor
 - D. Kiosk computer
76. What step in the user life cycle process should be triggered any time that an employee is terminated?
- A. Management
 - B. Provisioning
 - C. Deprovisioning
 - D. Support

77. Laura is developing a firewall strategy for her organization using the approach shown here. Which one of the following statements should be Laura's primary concern when selecting firewall products in this scenario?

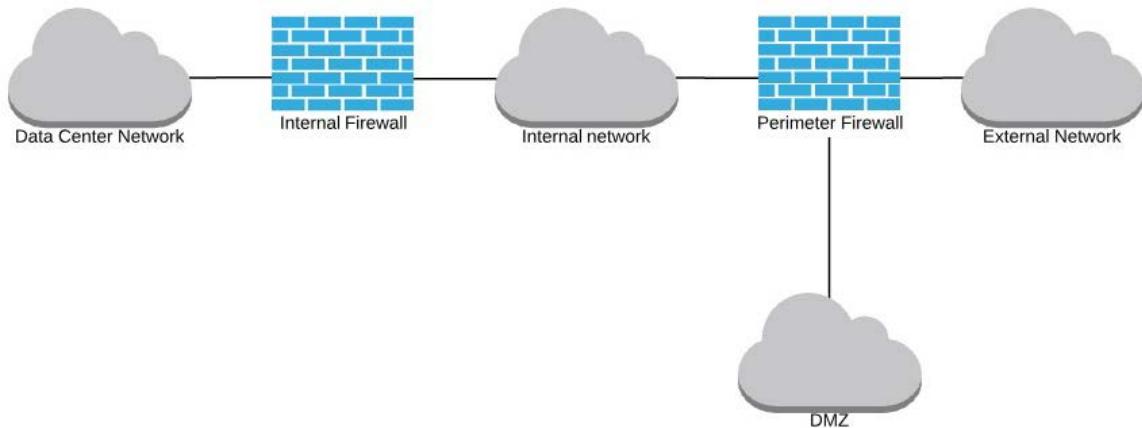


Figure 3.9

- A. Using two different brands of firewall increases the cost.
 - B. Using two different brands of firewall introduces an opportunity for configuration incompatibility.
 - C. Using two different brands of firewall introduces vendor diversity.
 - D. Using two different brands of firewall increases training requirements.
78. Andy works for an online retailer and has configured his organization's cloud computing environment to automatically purchase additional servers when necessary to meet periods of increased demand. Those servers are automatically deprovisioned when it's no longer necessary to meet demand. What term best describes what Andy is trying to achieve with this design?
- A. Scalability
 - B. Elasticity
 - C. Redundancy
 - D. Flexibility

79. What kind of card reader is shown here?



Figure 3.10

- A. Magnetic stripe card
 - B. Smart card
 - C. Proximity card
 - D. RFID card
80. Paul is helping to develop the security controls for a new high-security facility. The requirements specify that some equipment must be housed in a Faraday cage. What is the primary purpose of this control?
- A. Block electromagnetic radiation
 - B. Block physical access to equipment
 - C. Prevent tailgating attacks
 - D. Prevent the theft of equipment

81. Which one of the following is not a benefit of an infrastructure-as-code approach to computing?
- A. Reduced reliance on version control
 - B. Reduced risk of error
 - C. Reduction in cost
 - D. Increase in agility
82. Gavin is part of a consortium of health care providers in his region who are working together to build and host their own cloud computing environment that will be open only to members of the consortium. What type of cloud environment is Gavin helping to build?
- A. Community cloud
 - B. Hybrid cloud
 - C. Public cloud
 - D. Private cloud
83. Consider the query shown here:
- https://twitter.com/1.1/statuses/user_timeline.json?screen_name=mchapple
- What technology is this query using to retrieve information from Twitter?
- A. SDK
 - B. API
 - C. JSON
 - D. XML
84. Dennis is evaluating the physical security of a wiring closet inside his office building and would like to implement a preventive control. Which one of the following controls would best meet his needs?
- A. Guard dogs
 - B. Warning signs
 - C. Intrusion alarms
 - D. Door locks

85. Joyce is planning to implement a cloud access security broker and would like to deploy the technology using a model that will function with the largest possible variety of cloud applications. Which one of the following approaches should Joyce select?
- A. Forward proxy
 - B. Reverse proxy
 - C. API
 - D. Firewall
86. John is assisting a senior executive who must store some sensitive files on a USB flash drive for transfer to a remote location. The executive will hand-carry the drive and is the only person who needs to access the contents. Which one of the following encryption technologies would be the most appropriate for this application?
- A. TLS
 - B. DES
 - C. AES
 - D. RSA
87. Katie is reviewing the security of a web server used by her organization. She discovers each of the items listed here. Which one of these items poses the greatest security risk and should be prioritized for remediation?
- A. The server runs Apache and MySQL.
 - B. The server supports access on port 80.
 - C. The server supports access on port 443.
 - D. The server uses TLS 1.2.
88. Brian is designing a security awareness training program for his organization. Which one of the following statements is not true regarding awareness training best practices?
- A. Users should receive initial training shortly after joining the organization.
 - B. Employees in some job categories do not need to receive awareness training.
 - C. Awareness training efforts should be customized based upon an individual's role in the organization.
 - D. Privileged users should be singled out for focused training efforts.

89. Randy wishes to segment his organization's network to enforce isolation between different classes of users. Users are scattered around the building and Randy must support each of these network segments anywhere within the facility. Which one of the following technologies will best meet Randy's needs?
- WAF
 - Physical segmentation
 - VPN
 - VLANs
90. Consider the firewall rulebase shown here. Assuming the firewall is positioned to intercept the request, if a user on a system located at 192.168.100.1 attempts to make an HTTPS connection to the web server located at 192.168.15.5, how will the firewall react?

Rule	Source IP	Source Port	Dest IP	Dest Port	Action
1	any	any	192.168.15.5	80	allow
2	any	any	192.168.15.5	443	allow
3	192.168.100.1	any	192.168.15.5	any	deny
4	any	any	any	any	deny

Figure 3.11

- The firewall will allow the traffic according to rule 1.
 - The firewall will allow the traffic according to rule 2.
 - The firewall will deny the traffic according to rule 3.
 - The firewall will deny the traffic according to rule 4.
91. Nancy's organization uses the device shown here to store encryption keys in a secure manner. What type of device is this?



Figure 3.12

- A. HSM
 - B. TPM
 - C. SSL accelerator
 - D. BIOS
92. Air gaps are used by security professionals to perform what information security task?
- A. Virtual network implementation
 - B. Intrusion detection
 - C. Network separation
 - D. Non-repudiation
93. Christina is building a new capability for her organization's data centers that allows for the automatic shifting of workloads to Amazon Web Services when the organization's own resources are overwhelmed. What type of environment is Christina building?
- A. Public cloud
 - B. Hybrid cloud
 - C. Private cloud
 - D. Community cloud
94. What static code analysis technique seeks to identify the variables in a program that may contain user input?
- A. Signature detection
 - B. Lexical analysis
 - C. Control flow analysis
 - D. Taint analysis

95. Sarah's boss asked her to identify a security technology that can block users from installing three specific pieces of undesirable software on their laptops without affecting other uses of the devices. Which one of the following security technologies would best meet this requirement?

- A. Application blacklisting
- B. Application whitelisting
- C. Host firewall
- D. Host IPS

96. Frank is responsible for the security of a Windows domain. He would like to use a tool to assess the compliance of servers in his environment against the organization's security standards. Which Microsoft tool can best assist him with this task?

- A. LAPS
- B. MBSA
- C. SCT
- D. SysInternals

97. Which one of the following statements is not generally correct regarding the systems that are used to control HVAC environments?

- A. They often run outdated operating systems.
- B. They often embed strict host firewalls.
- C. They often contain security vulnerabilities.
- D. They are often actively managed.

98. Kevin is an application developer and would like to digitally sign code so that users know that it originated from his organization. What key should Kevin use to sign the code?

- A. The web server's private key
- B. The company's public key
- C. The company's private key
- D. The web server's public key

99. What term is used to describe a network of decoy systems that's used to attract and study the activity of intruders?
- A. Honeypot
 - B. Honeynet
 - C. Darknet
 - D. Darkpot
100. Fred is evaluating the effectiveness of a biometric system. Which one of the following metrics would provide him with the best measure of the system's effectiveness?
- A. IRR
 - B. FAR
 - C. FRR
 - D. CER
101. What software security technique can be added to a Secure DevOps approach to automate the evaluation of how software will respond to mutated input?
- A. Decompilation
 - B. Penetration testing
 - C. Vulnerability scanning
 - D. Fuzz testing
102. Which one of the following tools can be used to easily determine the patch level of Windows systems across an enterprise?
- A. APT
 - B. Windows Update
 - C. Yum
 - D. SCCM

103. What technology do Mac OS X systems use to prevent applications that have been downloaded from the App Store from accessing critical system resources directly?
- A. Sandboxing
 - B. TCP wrappers
 - C. Virtualization
 - D. Taint analysis

Domain 3 Answers and Explanations

1. B. Ralph should use encryption to protect the data and then store the encryption keys in a location other than the cloud service. With this control in place, a rogue employee of the cloud service may be able to access the organization's data, but will not be able to decrypt it. The other controls listed here are all good security practices, but an insider may be able to bypass them.
2. A. In a type 1 hypervisor, the hypervisor runs directly on the system hardware, eliminating the need for an underlying operating system and reducing the environment's attack surface. Type 2 hypervisors require the use of a host operating system. Type 3 and 4 hypervisors do not exist.
3. C. ASHRE recommends that data centers maintain temperatures within the range of 64.4 and 80.6 degrees Fahrenheit and keep relative humidity between 8% and 80%.
4. C. RAID level 5 is also known as disk striping with parity. This approach requires a minimum of two disks for data storage and an additional disk for parity, requiring a total of three disks minimum. It is important to note that RAID 5 actually distributes parity information across all of the disks to prevent a single disk from becoming a bottleneck, but it does require the use of three disks.

5. D. The fact that the servers have different performance characteristics indicate that Ed should choose a weighted algorithm that allows him to specify that some servers should handle more load than others. The fact that users have sessions of differing length indicates that he should use a least connections approach that tracks the number of active sessions instead of a round-robin approach that simply balances the number of assignments made. Therefore, Ed should choose the Weighted Least Connections algorithm.
6. D. This is a tricky question, similar to ones that you might find in the exam. From a defense-in-depth perspective, it's likely that any of these combinations would be appropriate. However, when CompTIA asks about control diversity, they are looking for a mixture of controls across administrative, technical, and physical controls. Of the controls included in this question, background checks and security training are administrative controls, while the remainder are all technical controls. Therefore, the only option that mixes controls across two of the CompTIA categories is the use of **data loss prevention (DLP)** and background checks.
7. D. Barry should perform an additional analysis of the change before taking any action. He should determine whether the change is truly necessary and the impact on the organization if it is denied. He should also determine the security impact of allowing the change and investigate whether a compensating control can mitigate the security risk introduced by allowing the variance from the standard.
8. C. **Self-encrypting drives (SEDs)** contain encryption technology built into the drive and, therefore, provide a high degree of security. Enclosed **full disk encryption (FDE)** technology uses a standard drive that is bundled with an encryption module. Chipset and bridge FDE place a bridge that performs encryption between the computer and the drive.
9. C. This is a tricky question to answer, similar to some of the ones that you'll see in the exam. The reason this is difficult is because all of the answer choices are possible risks associated with storing an API key in a public code repository. However, the primary risk that occurs in all cases is allowing anyone who's accessing the key to make unauthorized use of the API using the owner's key. This MIGHT make it possible to steal sensitive information, provision unauthorized resources, or conduct a denial-of-service attack, but that depends upon the nature of the API, which we do not know of in this example.
10. A. Facial and voice recognition can normally be done from a distance without requiring close user interaction. Retina and iris recognition require the user to expose his or her eye to the reader. However, iris scanning can often be done from a distance, while retinal scanning requires intrusive interaction with the scanner.

11. A. Betty must obtain a new certificate from a **certificate authority (CA)**. While this may be called "renewing" the certificate, it requires a new certificate to be obtained that replaces the expiring certificate. She should not place the certificate on the **certificate revocation list (CRL)** unless it has been compromised.
12. A. An application server designed only for use by internal users should be placed on the internal network. The DMZ is only appropriate for servers that require external access, while the external network zone is not an appropriate place to host any servers as it is not protected from external access by the firewall.
13. B. Compiled languages are converted from source code into machine language before execution using a program called a compiler. C++ is an example of a compiled language. Interpreted languages run the source code directly using an interpreter. JavaScript, R, and PHP are all examples of interpreted languages.
14. D. In a **platform-as-a-service (PaaS)** computing environment, the vendor maintains an environment where customers can develop, run, and manage their own applications. The vendor manages all of the infrastructure and the code execution environment. Google App Engine is an example of a PaaS service. Microsoft Office 365 and Slack are **software-as-a-service (SaaS)** services. Amazon's **Elastic Compute Cloud (EC2)** is an **infrastructure-as-a-service (IaaS)** environment.
15. D. The **Real-Time Protocol (RTP)** is an application protocol used for videoconferencing and should not be found on a management plane. The **Network Time Protocol (NTP)**, **Secure Shell (SSH)**, and **Remote Access Dial In User Service (RADIUS)** are all administrative protocols that would be expected traffic on a management plane.
16. C. This network uses a private IP range (192.168.1.0/24) on the internal network and a public IP address (12.8.1.5) on the external network. The firewall must support **Network Address Translation (NAT)** so that it can convert between public and private addresses or this network will not function properly. The firewall may also support **Intrusion Prevention System (IPS)** and **Web Application Firewall (WAF)** technology, but those are not required for proper network functioning. **Network Admission Control (NAC)** is normally performed by switches, rather than firewalls.
17. B. The principle of least functionality says that each server should offer only one primary function. This requires having at least two servers: a database server and a web server. Carl might choose to have additional servers for redundancy or capacity purposes, but only two servers are required to follow the principle of least functionality.

18. D. A warm spare server is configured and ready to operate, but is not turned on until it is needed. Hot spare (or active spare) servers are identically configured, but are powered on and ready to take over operations, perhaps on an automated basis. Cold spare servers are on hand, but not yet configured.
19. D. Any of the devices listed here is capable of serving as an endpoint for a VPN connection. However, a VPN concentrator is specifically well-suited for this task because it contains dedicated hardware that's been optimized for performing the cryptographic calculations required by a VPN. This would place an unnecessary burden on a firewall or router. A VPN server is also dedicated to this purpose, but does not contain the specialized, optimized hardware of a VPN concentrator.
20. C. Digital signatures are always verified using the public key of the individual or organization who created the signature. In this case, Gina should use the supplier's public key to verify the signature.
21. D. Because these servers are configured in a high availability manner, the web cluster will continue to operate as long as at least one server is functioning properly and answering user requests. The server may not be able to handle the full load, but there will not be a complete loss of service unless all six servers are lost.
22. B. During the Protect phase of the CSF, organizations develop and implement appropriate safeguards to ensure the delivery of critical services. In the Identify phase, they develop an organizational understanding to manage cybersecurity risks to systems, people, assets, data, and capabilities. The Detect phase allows them to develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. During the Respond phase, organizations develop and implement appropriate activities to take action regarding a detected cybersecurity incident. Finally, during the Recover phase, organizations develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.
23. A. In almost all cases, users should be placed into network zones based on their role in the organization. However, this scenario presents the exception to that rule. Because employees are connecting to an unsecured wireless network, they should be placed in a guest zone where they will not have access to sensitive information. If employees need to access sensitive information, they should either connect to a secured wireless network or use a VPN to make an external connection to the secured network.

24. D. In a hot aisle/cold aisle layout, cold air should be distributed at floor level in the front of racks (cold aisle) so that it is pulled into the front of the equipment and vented out the back, into the hot aisle.
25. D. Input validation should always be performed on the web server. If it is placed on the endpoint or within JavaScript code, the attacker may modify or remove the input validation code. Input validation cannot be performed on the database server because the database server will not be able to tell the difference between SQL code provided by the web server and code provided by the user as part of the attack.
26. A. Elaine should use a network **terminal access point (TAP)** to create a monitor port that allows the intrusion detection system to see all network traffic. Port mirroring (also known as SPAN) would allow the IDS to see network traffic, but it runs the risk of dropped packets. Inline installation would not have this disadvantage, but does pose a higher risk of network interruption if the IDS fails to pass traffic properly.
27. A. An 8-bit number can have 256 possible values (calculated as 2 to the 8th power). When used as a positive integer, this means that it can hold values between 0 and 255.
28. C. Tripwire is a file integrity monitoring solution that is also able to perform system configuration monitoring. It is the most appropriate tool for this task. Snort is an intrusion detection and prevention system. Wireshark is a network packet sniffing tool. QRadar is a **security information and event management (SIEM)** system.
29. A. **Virtual machine (VM)** escape attacks target vulnerabilities in the hypervisor supporting a virtualized environment. The strongest control to protect hypervisors against these attacks is to keep them patched. Network firewalls and port security are network security controls that occur outside of the virtualized environment and would not be effective in this case. Input validation is an application security control.
30. B. The password shown here is a BIOS password presented through the UEFI interface. This is not an especially secure way of securing access to a system as there are many techniques to bypass BIOS passwords.
31. C. In a **software-as-a-service (SaaS)** environment, the customer is only responsible for configuring the application and managing authorization controls. The vendor develops and maintains the application and infrastructure environment.

32. A. If Brandy's major concern is a compromised operating system, she can bypass the operating system on the device by booting it from live boot media and running her own operating system on the hardware. Running a malware scan may provide her with some information, but may not detect all compromises, and Brandy likely does not have the necessary permissions to correct any issues. Using a VPN or accessing secure sites would not protect her against a compromised operating system as the operating system would be able to view the contents of her communication prior to encryption.
33. C. The hardware root of trust is a core building block of the security of a system and must be designed securely so that system components that build upon it (operating at higher levels of abstraction) may trust it. The root of trust should be implemented in hardware and it should be as small as possible. The root of trust should not be large and, therefore, should not contain the operating system.
34. C. SSL acceleration uses hardware to reduce the computational burden on web servers and other devices using **Transport Layer Security (TLS)**. Note that this technology is still called SSL acceleration even though SSL has been replaced by TLS. Load balancing strategies would not be effective in this case because all of the servers are experiencing the problem equally. There is no indication in the scenario that a **web application firewall (WAF)** would reduce the load.
35. D. Integration testing occurs after unit testing and is designed to confirm that units of code will work together properly. Functional testing takes place upon the conclusion of requirement development, while design testing takes place once the design is complete. Both functional and design testing should be completed before – not after – unit testing. Acceptance testing occurs as the next step after successful integration testing.
36. B. Development environments are designed for active use by developers who are creating new code. These environments are the only location where code should be modified. Once the code is ready for testing, it is released from the development environment into a test environment for software testing. After the completion of user acceptance testing, the code is moved from the test environment into a staging environment where it is prepared for its final deployment into the production environment. Developers should never have permission to move code themselves and should only be able to move code between environments through the use of a managed change control system.

37. C. Placing the sensor on the DMZ allows it to see traffic before it reaches the web server but minimizes the amount of traffic that it sees because the sensor will not observe traffic that is blocked first by the network firewall. Placing the sensor on the external network would still allow it to see external attacks, but would expose it to traffic destined to be blocked by the firewall. Placing it on the internal network would not allow it to see external traffic headed to the web server.
38. D. Firewalls, proxy servers, and intrusion prevention systems all offer content filtering functionality. Routers generally do not perform content filtering as they do not operate at the application layer.
39. B. A system **access control list (ACL)** is an example of a logical security control. Lighting, equipment enclosures, and Faraday cages are all examples of physical security controls.
40. D. Standard ACLs are able to filter traffic based only on the source address. They cannot filter based on the destination address. Extended ACLs do not have this limitation. Both standard and extended ACLs may apply to either inbound or outbound traffic.
41. C. Cloud computing environments provide on-demand computing and allow users to pay for resources on an as-needed basis. In that model, Carl can power down servers that are not needed and reduce his costs. Other computing models have high fixed costs that would not be as cost-effective for this type of bursty workload.
42. B. If the service is not designed and/or implemented well, any of these issues could become a concern. However, a mature service from a well-respected vendor should not have design flaws that cause confidentiality, non-repudiation, or reliability concerns. Latency is a potential issue with any cloud service and should be carefully evaluated in an identity and access management deployment.
43. D. Testing suspicious software should only take place within an isolated sandbox environment that is specifically designed for testing suspicious code in a manner where it cannot impact other systems. Test, development, and production environments should never be used for testing potentially malicious software.
44. A. Organizations deploying IPsec for site-to-site VPNs typically use tunnel mode to connect two VPN concentrators to each other and then route traffic through that tunnel in a manner that is transparent to the communicating devices. Transport mode is more commonly used for remote access VPNs. **Internet key exchange (IKE) and security associations (SAs)** are not modes of IPsec VPN operation.

45. D. All of the options presented here are possible ways to restore a system to a previously known good state, but the simplest way to do so is to restore the system from a snapshot as this is a file that captures the complete state of the system. Applying backups or rebuilding the system may achieve the same goal, but would be more time-consuming.
46. A. Internet service providers are best positioned to mitigate the effects of an attack against their customers by blocking the traffic before it reaches the customer network.
47. C. Class C fire extinguishers are designed for use against electrical fires. Class A extinguishers are for ordinary combustible materials, such as wood. Class B are for flammable liquids, such as grease, while Class D are specialized extinguishers for flammable metals.
48. B. Git, **Subversion (SVN)**, and **Concurrent Versions System (CVS)** are all open source version control systems. Visual SourceSafe is a version control system from Microsoft, but it is not open source.
49. B. **Group Policy Objects (GPOs)** may be used to automatically assign security settings to systems through Active Directory. **Fully qualified domain names (FQDNs)** are not used to apply security settings, nor are **media access control (MAC)** addresses or **Transport Layer Security (TLS)**.
50. B. HP JetDirect printer traffic uses TCP port 9100 to transfer data from clients to printers.
51. C. A master image is a preconfigured version of an operating system that meets the organization's standard configuration requirements and may be customized for workload-specific use. A template or standard may contain information about the organization's security requirements, but does not provide a working copy of the operating system. Live boot media is a media device that contains an operating system and may be used to boot a device. It does not necessarily meet the organization's security configuration requirements.
52. D. The single quotation mark ('') is commonly used to escape a SQL query and should be carefully handled during input validation. The greater than (>) and less than (<) characters should also be handled carefully, but these are used in **cross-site scripting (XSS)** rather than SQL injection attacks.
53. C. Servers that provide services to the general public should be placed in the DMZ. Intranet servers should have access restricted to internal users. Extranet servers may be accessed by vendors and other business partners. Guest networks are designed for visitors to a facility to gain internet access.

54. C. The image shows an example of a bollard, a physical barrier placed near a street to block vehicle access without inhibiting pedestrian access.
55. B. The nslookup and dig utilities both perform domain name resolution, but dig is not included on Windows systems by default and must be installed manually. Nbtstat is used for NetBIOS name lookups, while ARP is used for MAC address lookups.
56. A. All organizations involved in the processing of credit card transactions are contractually obligated to comply with the **Payment Card Industry Data Security Standard (PCI DSS)**. There is no information provided in the scenario that Norma is employed by a health care organization that would be covered under the **Health Insurance Portability and Accountability Act (HIPAA)**. Similarly, she is not employed by an educational institution covered by the **Family Educational Rights and Privacy Act (FERPA)**. The scenario does not state whether her employer is a publicly traded company, so we cannot conclude that her firm is subject to the **Sarbanes-Oxley (SOX)** Act.
57. D. Most security professionals consider eight feet to be the minimum height for a fence protecting critical assets. It is trivial for an intruder to climb a fence of six feet or less. A fence that stands twelve feet high is likely unnecessary and aesthetically unpleasant. For added security, organizations may add barbed wire to the top of the fence.
58. D. When assigning users to network zones, the method of accessing the network (wired or wireless) should not be a primary concern. Rather, users should be placed in network zones based upon their role in the organization and security policies. These zone assignments should be consistent across wired and wireless networks.
59. A. The Common Criteria lays out the requirements for an operating system to be certified by the government as a Trusted Operating System. The Trusted Computer System Evaluation Criteria (also known as the orange book) served a similar purpose, but is now outdated. CIS and Windows standards are not government sources.
60. D. Application containers virtualize the user space for an application, but each container uses the kernel of the underlying operating system. In type 1 or type 2 virtualization, the hypervisor supports different guest operating systems, but does not perform application isolation. Bare metal virtualization is another term for type 1 virtualization.

61. D. In transparent operation mode, BitLocker uses the **Trusted Platform Module (TPM)** to decrypt the encryption key. Active Directory does not store disk encryption keys. User passwords are used to protect the key in user authentication mode, while USB keys are used in USB Key Mode.
62. A. In a Type 1 hypervisor, the hypervisor runs directly on the physical hardware. In a Type 2 hypervisor, the hypervisor runs on a host operating system which, in turn, runs on the physical hardware. In both cases, guest operating systems run on top of the hypervisor.
63. C. Proxy servers do not perform route optimization as this is the function of network routing devices. They do, however, accept requests from users for websites, anonymize those requests, and pass them to the remote site. This allows the proxy server to perform anonymization to protect the identity of the end user and content filtering to block access to undesirable content.
64. B. Wanda can disable services using the Windows Programs and Features tool.
65. A. TLS VPNs are unique because they rely upon the same Transport Layer Security protocol used by HTTPS connections. Because of this, most customer networks will allow access by default. Other VPN types would likely require the configuration of customer firewalls to allow access.
66. A. String normalization processes input in different Unicode character sets and convert it into a standard format prior to performing input validation. Normalizing the string shown here results in <script> as input, which may be part of a cross-site scripting attack.
67. A. Wet pipe and dry pipe systems both use water and may damage or destroy equipment in the data center if discharged. FM-200 and Halon systems both use gas, which is not likely to damage equipment, but it is illegal to construct new Halon systems in the United States. Therefore, Joan should choose an FM-200 system.
68. C. **Closed circuit television (CCTV)** systems are useful controls for monitoring a facility and detecting potential intrusions. Therefore, Florence's system is best described as a detective control. CCTV may be a deterrent control as well, but this system is concealed, so it has no deterrent purpose. A video surveillance system cannot actually stop an intrusion, so it is not a preventive control. CCTV systems are usually fairly cost-effective and not overwhelmingly expensive.
69. B. Software-defined networking does facilitate network segmentation. It allows for the rapid realignment of network functionality by creating a programmable network, but this flexibility also adds complexity to the network. SDN separates, rather than combines, the data and control planes of the network.

70. A. **Virtual LANs (VLANs)**, **Virtual Private Networks (VPNs)**, and physical segmentation are all technologies that can isolate networks. However, the extremely sensitive nature of **industrial control systems (ICS)** and **supervisory control and data acquisition (SCADA)** systems in a nuclear power plant call for the greatest degree of segmentation possible – physical segmentation. This approach is usually too costly for most applications, but it is appropriate in this case. An **intrusion prevention system (IPS)** does not provide the required functionality.
71. B. Query parameterization and stored procedures store the SQL code on the database server, preventing a user from supplying additional code through a web application. Input validation is used to filter out potentially malicious input, but it must be performed on the server to prevent attackers from tampering with the validation code.
72. C. Digital signatures validate the fact that the application came from the entity that signed the application. Security professionals should not draw any other conclusions from the fact that an application is digitally signed.
73. A. Development environments are designed for active use by developers who are creating new code. These environments are the only location where code should be modified. Once the code is ready for testing, it is released from the development environment into a test environment for software testing. Following the completion of user acceptance testing, the code is moved from the test environment to a staging environment where it is prepared for its final deployment into the production environment. Developers should never have permission to move code themselves and should only be able to move code between environments through the use of a managed change control system.
74. D. In a **virtual desktop infrastructure (VDI)** approach, each user logs in to the system and has access to his or her own interactive desktop. This approach best meets Joe's requirements. The software being used is desktop software, so there is no reason to believe that a web-based client is available. Using a VPN-based approach would require installation of the software on the devices connecting to the VPN, which is prohibited by the license agreement. **Data loss prevention (DLP)** systems are not relevant in this scenario.
75. C. Kiosk computers and endpoint computing devices all commonly run desktop and server operating systems. Multifunction printers often have embedded computer systems running standard operating systems. **Internet of Things (IoT)** sensors usually do not have the memory or processing power to run a standard operating system and normally run specialized operating systems designed for IoT applications.

76. C. Provisioning is the process of adding a new user to the organization and should be triggered for new hires. Deprovisioning is the process of removing a user from the organization and should be triggered on termination. Management and support are ongoing activities.
77. C. All of the statements listed in this scenario may be true to one extent or another. However, Laura's overriding concern here should be introducing vendor diversity into the environment to provide additional security. Using two different products increases the likelihood that her data center network will be robustly defended following a defense-in-depth strategy. Watch out for questions like this in the exam as CompTIA stresses the need for vendor diversity in the exam objectives.
78. B. Andy may very well be attempting to achieve all of these goals. However, the term *elasticity* best describes this environment because it both provisions new servers when necessary, and deprovisions them when they are no longer needed. Scalability is a very similar term, but it describes the provisioning of servers to meet demand and does not include the deprovisioning of unnecessary servers.
79. B. The card reader shown here requires the user to insert the card into the reader and leave it there. This indicates that the card is a smart card containing a chip that interacts with the reader. Magnetic stripe cards are swiped through a reader and do not remain in the reader. Proximity and RFID cards are waved in front of the reader.
80. A. Faraday cages are enclosures designed to prevent electromagnetic radiation from entering or leaving an area. They are used to shield very sensitive equipment and to prevent electromagnetic signals that might be intercepted from leaving a facility.
81. A. Infrastructure-as-code approaches reduce risk by decreasing manual work, lowering costs by automating activity, and increasing agility by providing rapid flexibility. However, they increase, rather than decrease, the importance of using version control systems to manage the code that defines infrastructure.
82. A. In a public cloud environment, providers offer services on the same shared computing platform to all customers. Customers do not necessarily have any relationship to, or knowledge of, each other. In a private cloud environment, an organization builds its own computing environment. In a hybrid cloud environment, an organization combines elements of public and private cloud computing. In a community cloud environment, a group of related organizations build a shared cloud environment that is not open for general public use.

83. B. This query is using the Twitter **application programming interface (API)** to retrieve data for the user with the Twitter handle, mchapple. We can tell that this is an API call because the query is in an HTTP request. A **software development kit (SDK)** would use function calls in the language of the SDK. The query is retrieving results in JSON format, rather than XML format, but this is the standard that's used to format the results, not the technology that's used to retrieve them.
84. D. All of the controls listed here are physical security controls. However, warning signs are a deterrent control, and an intrusion alarm is a detective control. Neither are preventive controls. Guard dogs and door locks may both be considered preventive controls, but it is not normally practical to have guard dogs in an office building. Therefore, the best choice for Dennis is to use hardware door locks.
85. A. A forward proxy approach can work with any type of cloud application and would best meet Joyce's requirements. Reverse proxies and API-based approaches work with a limited subset of applications. A firewall is not a CASB deployment model.
86. C. Because the executive is the only person who requires access to the information, the simplest solution would be to use a symmetric encryption algorithm, such as the **Advanced Encryption Standard (AES)**. It is also a symmetric algorithm, but it is insecure and not suitable for use. The **Rivest, Shamir, Adelman (RSA)** algorithm would work for this application, but it is asymmetric and has unnecessary complexity. **Transport Layer Security (TLS)** is designed for use on data in transit over a network and not data stored on a device.
87. A. One of the basic server security principles is that each server should support only one primary function. Best practice dictates separating the web server (Apache) from the database server (MySQL). It is normal and standard for a web server to support both unencrypted access on port 80, and encrypted access on port 443. TLS 1.2 is a modern version of the protocol and is secure and acceptable for use.
88. B. Every employee in an organization should receive at least a basic level of security awareness training shortly after they join the organization and on a recurring basis. This training should be customized to a user's role and may be more frequent for individuals with sensitive roles, such as privileged users.
89. D. **Virtual LANs (VLANs)** provide the segmentation Randy desires at the logical level, allowing them to appear anywhere in the building. Physical segmentation is likely too costly and inflexible for these requirements. **Virtual private networks (VPNs)** are unwieldy and unnecessary in a fixed office environment. **Web application firewalls (WAFs)** do not provide the required segmentation functionality.

90. B. Firewall rules are always processed in a top-down fashion, with the first rule matching the network traffic taking precedence. In this case, rule 1 does not apply because the request is for HTTPS traffic, which takes place on port 443, while rule 1 is for port 80. Rule 2 does apply because the destination IP address and port match. Therefore, the traffic is allowed. Rules 3 and 4 would also match this traffic, but they are not effective in this case because rule 2 supersedes them.
91. A. **Hardware security modules (HSMs)**, such as the one shown here, are used to protect encryption keys and perform cryptographic processing. **Trusted Platform Modules (TPMs)** do store encryption keys for use in disk encryption, but they are chips contained within another device, rather than a standalone device. SSL accelerators and BIOS chips do not serve as key repositories.
92. C. Air gaps are a security control that uses physical separation between networks to prevent the flow of information or network traffic between the networks. Air gapping is used in high security environments to protect critically sensitive systems from the potential of external access and other threats.
93. B. In a public cloud environment, providers offer services on the same shared computing platform to all customers. Customers do not necessarily have any relationship to, or knowledge of, one another. In a private cloud environment, an organization builds its own computing environment. In a hybrid cloud environment, an organization combines elements of public and private cloud computing. In a community cloud environment, a group of related organizations builds a shared cloud environment that is not open for general public use.
94. D. Taint analysis traces variables that may contain user input and ensures that they are sanitized before being used by a potentially vulnerable function. Lexical analysis converts source code into a tokenized form. Control flow analysis traces the execution path of code. Signature detection looks for known patterns of malicious activity.
95. A. Application blacklisting is used to block specific applications from devices. Sarah has a list of three specific applications she must block, and blacklisting would be the least disruptive way to achieve her goal. Application whitelisting would block all applications not on an approved list, and would likely cause unintended disruptions. Host firewalls and intrusion prevention systems generally do not block the installation and use of software.

96. C. The Microsoft **Security Compliance Toolkit (SCT)** is a modern tool designed to assess compliance with security baselines and is ideal for Frank's task. The **Microsoft Baseline Security Analyzer (MBSA)** performed a similar purpose, but is outdated and no longer maintained. The Local Administrator **Password Store (LAPS)** is a security tool for managing local administrator accounts and does not assess systems against a security baseline. Neither does the SysInternals suite, which provides a series of one-off system administration tools.
97. B. The controllers for **heating, ventilation, and air conditioning (HVAC)** systems often run on outdated hardware and software and contain security vulnerabilities because they are commonly not actively managed. These systems do not usually have host firewalls and should be segmented on a specialized network.
98. C. When digitally signing code, the developer uses the private key belonging to the organization that is vouching for the code. In this case, Kevin should sign the code using the organization's private key.
99. B. Honeynets are networks of decoy systems designed to attract intruders so that security analysts may study their activity. Honeypots are single systems designed for the same purpose. Darknets are unused portions of IP address space designed to detect scanning activity when a scanner attempts to access those unused addresses. Darkpots are what occur when I attempt to cook and leave a pot unattended on the stove for too long.
- 100.D. The **false rejection rate (FRR)** identifies the number of times that an individual who should be allowed access to a facility is rejected. The **false acceptance rate (FAR)** identifies the number of times that an individual who should not be allowed access to a facility is admitted. Both the FAR and FRR may be manipulated by changing system settings. The **crossover error rate (CER)** is the rate at which the FRR and FAR are equal and is less prone to manipulation. Therefore, the CER is the best measure for Fred to use. IRR is not a measure of biometric system effectiveness.
101. D. Fuzz testing specifically evaluates the performance of applications in response to mutated input combinations. Penetration testing is a manual, and not an automated, process. Vulnerability scanning may be automated, but does not necessarily include the use of mutated input. Decompilation attempts to reverse engineer code.

102. D. Windows System Center Configuration Manager allows administrators to easily determine the patch level of multiple systems. Windows Update is an updating mechanism for individual systems that does not provide automated monitoring. Yum and APT are package managers that allow updates for Linux systems.
103. A. Sandboxing isolates an application, preventing it from accessing protected system resources. Mac OS X uses sandboxing for all applications that are installed through the App Store. TCP wrappers are a firewall technology. Virtualization is a general term that's used to refer to running multiple operating systems on a single hardware platform. Taint analysis is a technique that's used to trace user input through code execution.

4

Identity and Access Management

Domain 4 Questions

1. Ryan is concerned about integrity attacks against his organization's sales database. Which one of the following SQL commands is least likely to result in an integrity issue?
 - A. SELECT
 - B. INSERT
 - C. UPDATE
 - d. DELETE
2. Which one of the following technologies is not commonly used as part of a **single sign-on (SSO)** implementation?
 - A. OAuth
 - B. IPSec
 - C. OpenID
 - D. SAML
3. Consider the statistics shown in the following table for a biometric authentication system. What is the system's FRR based upon for this data?

	Authorized User	Unauthorized User
Accept	98	16
Reject	2	84

Figure 4.1

- A. 1%
 - B. 2%
 - C. 8%
 - D. 16%
4. In an authentication system using the **mandatory access control (MAC)** model, who determines what users may access an object?
 - A. The user
 - B. The object owner
 - C. The system administrator
 - D. The system

5. TJ is designing the authentication system for an online gambling website that is restricted for use by residents of a single US state. What type of access control should TJ implement to ensure that his organization does not run afoul of the law?
 - A. Role-based access control
 - B. Multifactor authentication
 - C. Token-based authentication
 - D. Location-based access control
6. Thelma is configuring a new web server running Apache. Apache requires an account to read the files contained in the /var/www directory. What type of account should Thelma use for this access?
 - A. Root account
 - B. Guest account
 - C. Service account
 - D. Administrator account
7. Helen's organization has a password policy that does not enforce complexity requirements. What is the major disadvantage of this approach?
 - A. Attackers can use social engineering to extract simple passwords from users.
 - B. Attackers can easily brute force passwords that are short.
 - C. Attackers can easily brute force passwords that draw from a limited character set.
 - D. Attackers may use reverse hashing to decrypt simple passwords.
8. Victoria is implementing an authentication system where the user is asked to speak a predefined passcode into a microphone. The system then verifies that the speaker's voice matches their enrollment sample and that the passcode is correct. How many authentication factors are at play in this scenario?
 - A. Zero
 - B. One
 - C. Two
 - D. Three

9. Lila is concerned about the security of a database table that contains Social Security Numbers. The organization needs to maintain this information for tax reporting purposes, but Lila wants to make sure that the database administrators are unable to access this very sensitive field. Which one of the following security controls would best meet Lila's need?
 - A. Database activity monitoring
 - B. Field-level hashing
 - C. Database access controls
 - D. Field-level encryption
10. Which one of the following account types should be assigned the highest priority for account activity logging?
 - A. Temporary user accounts
 - B. Guest accounts
 - C. Service accounts
 - D. Standard user accounts
11. Colleen's company would like to manage administrator credentials by creating them in such a manner that nobody has knowledge of the root password for a system and the password is stored in an electronic vault. What mechanism should Colleen implement to ensure that administrators are not locked out of the system in the event of an access control failure?
 - A. Emergency access procedure
 - B. Redundant passwords
 - C. Give a manager the passwords
 - D. Multifactor authentication
12. Which one of the following assertions can NOT be made by validating the card authentication certificate on a US government PIV card?
 - A. The holder of the credential is the same individual the card was issued to.
 - B. The card has not expired.
 - C. The card has not been revoked.
 - D. The card was issued by an authorized entity.

13. Carla is examining a point-of-sale terminal and sees the prepopulated login screen shown here. What type of account is most likely being used in this scenario?



Figure 4.2

- A. Privileged account
 - B. Shared account
 - C. Guest account
 - D. Superuser account
14. Wanda is concerned about the likelihood of privilege creep in her organization. Which one of the following activities is likely to uncover the most comprehensive listing of privilege creep situations that can then be remediated?
- A. Permission auditing
 - B. Usage auditing
 - C. Policy review
 - D. User termination audit

15. Tim is a member of several NTFS groups and is attempting to access a file stored on an NTFS volume. The set of permissions that apply from each of his group memberships are shown here. What is the end result of these permissions when Tim attempts to access the file?

Accounting Group

Inherited deny read and write permission

Tim's Account

Explicit allow read and write permission

Managers Group

Explicit deny write permission

Figure 4.3

- A. Tim can't read or write to the file.
 - B. Tim can read the file but not write to it.
 - C. Tim can write to the file but not read it.
 - D. Tim can both read and write the file.
16. What network port is used for communications related to the Kerberos authentication process?
- A. UDP port 636
 - B. TCP port 88
 - C. UDP port 88
 - D. TCP port 636
17. Paula is reviewing her organization's account management life cycle. She is paying particular attention to the timeliness of account management activities and would like to prioritize areas that have the greatest risk. Which one of the following activities should be her highest priority?
- A. Access modifications
 - B. Onboarding
 - C. Access reviews
 - D. Offboarding

18. Nancy is configuring a user account and is setting the permissions that are shown here. What type of permissions is Nancy setting?

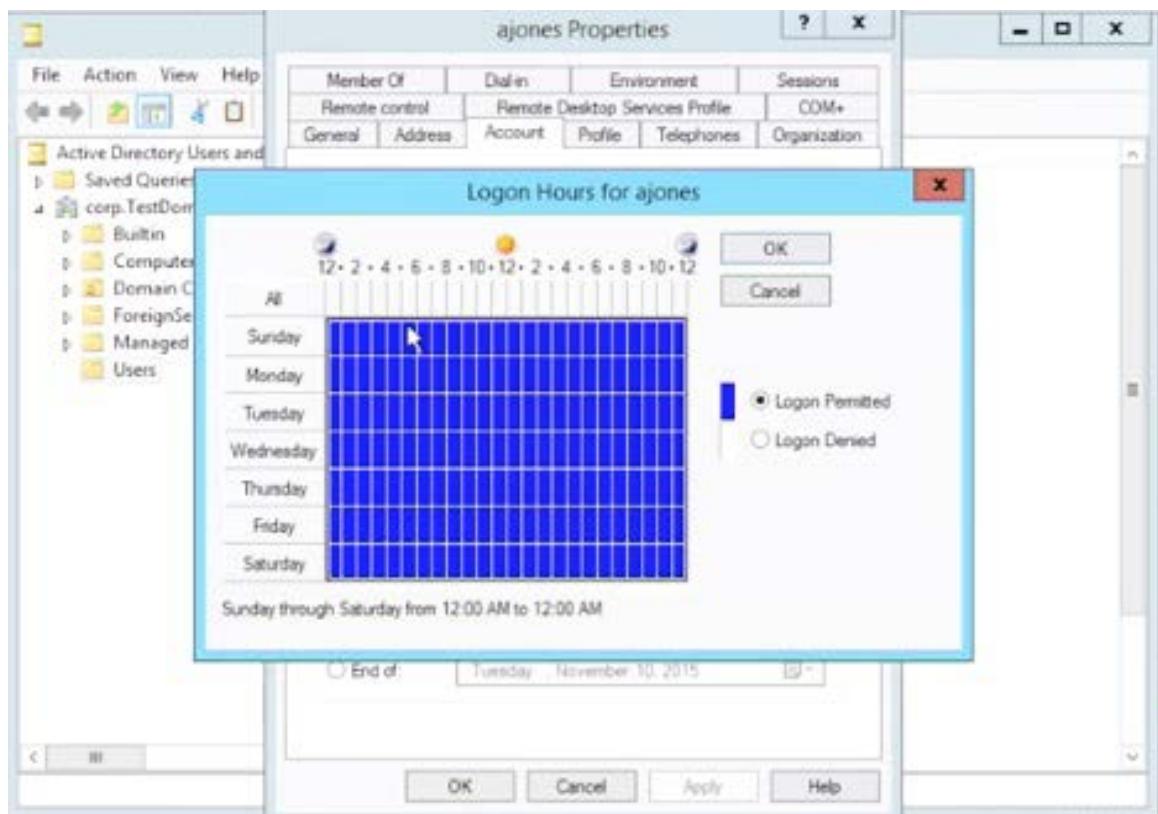


Figure 4.4

- A. Location-based restrictions
- B. Content-based restrictions
- C. Role-based restrictions
- D. Time-based restrictions

19. When using CHAP authentication, what does the server send to the client in the second step of the handshake?
 - A. Password
 - B. Hash
 - C. Challenge
 - D. Certificate
20. Barry is reviewing the password settings on his Windows domain and discovers that the domain is set to expire passwords every 60 days. Which one of the following actions should Barry take to align his organization with industry best practices?
 - A. Remove the password expiration period.
 - B. Extend the password expiration period to 180 days or more.
 - C. Shorten the password expiration period to 30 days or less.
 - D. No action is necessary.
21. Brian is implementing geofencing as a component of his access control system. What type of control is he implementing?
 - A. Role-based access control
 - B. Group-based access control
 - C. Location-based access control
 - D. Time-based access control
22. Molly's organization has a shared account that they use to provide access to vendors. What is the primary security objective that is sacrificed using this model, assuming that the password is not shared with unauthorized individuals?
 - A. Integrity
 - B. Least privilege
 - C. Confidentiality
 - D. Accountability

23. Review the Google Authenticator screenshot shown here. What protocol is being used to generate passcodes by this software token?

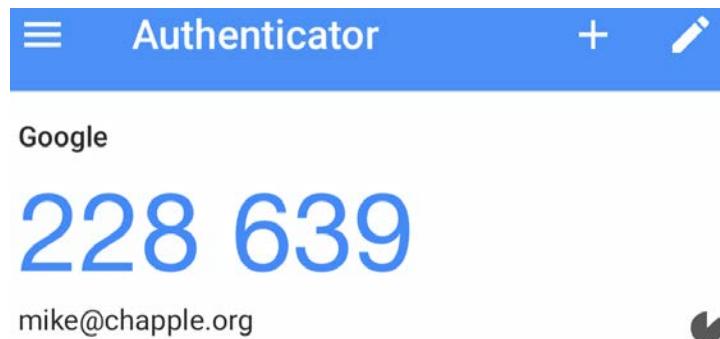


Figure 4.5

- A. LOTP
 - B. HOTP
 - C. KOTP
 - D. TOTP
24. Which one of the following biometric technologies is most likely to be affected by a person's race?
- A. Facial recognition
 - B. Fingerprint recognition
 - C. Iris recognition
 - D. Hand geometry
25. When digital certificates are used for the authentication of a user to a server, what is the primary purpose of the digital certificate?
- A. To convey a signed copy of the server's public key
 - B. To convey a signed copy of the user's private key
 - C. To convey a signed copy of the user's public key
 - D. To convey a signed copy of the server's private key

26. Tina is designing a recovery mechanism for her organization's authentication system and provides each user with a card containing several one-time use passwords for use in the event their smartphone app malfunctions. What type of authentication factor are these one-time passwords?
- A. Something you have
 - B. Something you know
 - C. Somewhere you are
 - D. Something you are
27. Taylor is accessing a website that would like to access information stored in her Google account. The site makes a request to access that information using the OAuth protocol. In this scenario, who is the OAuth resource owner?
- A. Taylor
 - B. Google
 - C. Website
 - D. Both Google and the website
28. What is the primary feature that distinguishes a smart card from other types of access card?
- A. Presence of a magnetic stripe
 - B. Presence of an integrated circuit
 - C. The requirement to enter a PIN or password
 - D. Compatibility with biometric authentication
29. Corey would like to implement a multifactor authentication system for physical access to his data center. He is currently using a fingerprint scanner. Which one of the following would be the best second authentication technique to use in combination with the fingerprint scanner?
- A. Voiceprint analysis
 - B. Security question
 - C. ID card
 - D. Retinal scan

30. Consider the US government personal identity verification (PIV) card shown here. When the individual presents a card to an appropriate system for verification, what element allows the validator to verify the identity of the PIV user?



Figure 4.6

- A. Encryption certificate
- B. Card authentication certificate
- C. Digital signature certificate
- D. PIV authentication certificate

31. Barry is troubleshooting authentication problems for his organization's VPN. The VPN uses a RADIUS backend for authentication and Barry would like to monitor this traffic. What ports are associated with RADIUS?
 - A. UDP ports 1812 and 1813
 - B. TCP ports 1812 and 1813
 - C. UDP ports 1433 and 1521
 - D. TCP ports 1433 and 1521
32. Ken would like to configure his organization's password security policy to be in line with current NIST guidelines. What is the minimum password length that Ken should require to be consistent with those guidelines?
 - A. 6 characters
 - B. 8 characters
 - C. 12 characters
 - D. No minimum
33. Which of the following services are supported by the TACACS+ protocol?
 - A. Authentication, authorization, and accounting
 - B. Authentication only
 - C. Authentication and authorization
 - D. Authentication and accounting
34. Which one of the following techniques is the least secure approach to a "something you have" authentication factor?
 - A. SMS message
 - B. Physical token
 - C. Smartphone app
 - D. Smartcard

35. Erin would like to assess the impact of several overlapping Windows GPOs and determine the effective result of those policies. Which tool is best suited for this task?
- A. dcpromo
 - B. gpedit
 - C. gpresult
 - D. gpupdate
36. Roger uses his fingerprint to unlock his laptop. What authentication factor was used in this example?
- A. Biometric authentication
 - B. Token-based authentication
 - C. Location-based authentication
 - D. Knowledge-based authentication
37. Which one of the following biometric access control mechanisms generally takes the longest time to recognize a user?
- A. Fingerprint scan
 - B. Iris scan
 - C. Facial recognition
 - D. Retinal scan
38. Before accessing a wire transfer website, Harry's bank requires that he provide a password, a security PIN, and answer several security questions. How many distinct authentication factors is this system using?
- A. 0
 - B. 1
 - C. 2
 - D. 3

39. Tim recently set the attribute shown here on a group of Windows user accounts. His organization has the following security requirements:

1. Passwords must be at least 10 characters.
2. Passwords must contain characters from three different character classes.
3. Passwords may not contain the user's account name.

Which of these requirements are met by the setting shown here?

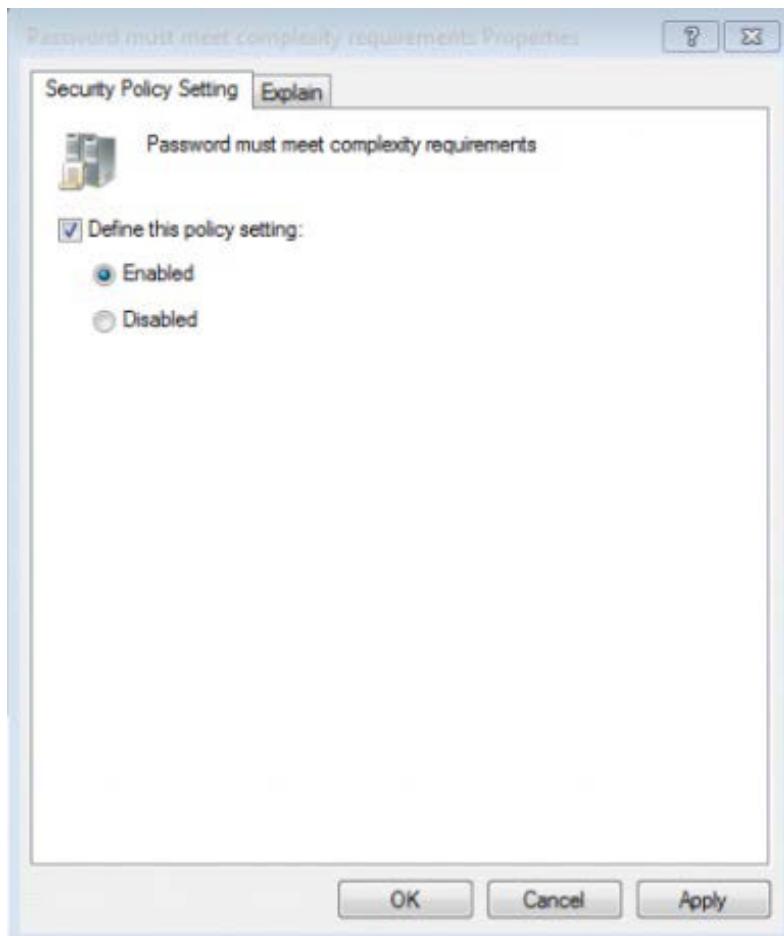


Figure 4.7

- A. Requirements 1 and 2
- B. Requirements 2 and 3
- C. Requirements 1, 2, and 3
- D. Requirements 1 and 3

40. Carl would like to implement a recertification process for vendors with accounts allowing access to systems in his organization. What access management control can best facilitate this?
- A. Password complexity
 - B. Account expiration
 - C. Least privilege
 - D. Job rotation
41. Which one of the following protocols is considered secure for use in an authentication system without the use of any compensating controls?
- A. PAP
 - B. MS-CHAP
 - C. MS-CHAP v2
 - D. Kerberos
42. Which one of the following is a large-scale federated identity management solution that is widely used mainly in academic institutions?
- A. Kerberos
 - B. Shibboleth
 - C. OAuth
 - D. OpenID Connect
43. Martin is concerned about the misuse of legitimate privileges by employees, otherwise known as the insider threat. Which one of the following activities would best serve as a control against this threat?
- A. Privilege auditing
 - B. Usage auditing
 - C. Multifactor authentication
 - D. Credential management

44. Lisa is evaluating a set of Group Policy Objects that have been applied to a Windows account. Which one of the following policies will be processed first?
- A. Organizational Unit policy
 - B. Site policy
 - C. Domain policy
 - D. Local policy
45. Tom is designing a password reset mechanism for his organization and would like to require a personal visit to a help desk. Which one of the following statements is not correct?
- A. Users should be permitted to reset passwords in person.
 - B. Users reporting to the help desk should be asked for proof of identification.
 - C. Use of a help desk reset approach is burdensome on both users and staff.
 - D. Users reporting to the help desk should provide an old, expired password if possible.
46. Which one of the following is a best practice for the management of privileged accounts on a server?
- A. Privileged accounts should be shared between administrators.
 - B. Administrative users should have both privileged and unprivileged accounts.
 - C. Privileged accounts should not be protected by passwords.
 - D. Privileged accounts should be exempted from standard password management practices.
47. Frank would like to set his organization's password length requirements to align with industry best practices. What should he set as the maximum password length?
- A. 8 characters
 - B. 16 characters
 - C. 255 characters
 - D. No maximum

48. Greg is designing authentication controls for a system that is accessed by employees in branch offices. There is no need for mobile or remote users to access the system. What authentication factor could Greg implement to prevent users from accessing the system remotely?
- A. Something you have
 - B. Something you are
 - C. Somewhere you are
 - D. Something you know
49. Which one of the following is an implementation of a mandatory access control system?
- A. SELinux
 - B. NTFS
 - C. Google Drive
 - D. Mac OS X
50. Taylor works for an organization that experiences high turnover in employees, particularly at their call center and retail stores. She would like to implement an access control system that minimizes work. Which one of the following actions will best reduce the workload on the access management team while maintaining security?
- A. Implement group-based access control
 - B. Implement a permissive access control model
 - C. Implement mandatory access control
 - D. Implement personalized access control for each employee
51. In a normal RADIUS authentication session, what is the first message that's sent by the client to the server?
- A. Access-Reject
 - B. Access-Request
 - C. Access-Challenge
 - D. Access-Accept

52. Tom is deciding whether to implement a standard account naming practice for his organization. Which one of the following statements best reflects the accepted best practices regarding this topic?
- A. Organizations should adopt standard naming conventions to make account identification easier.
 - B. Organizations should not adopt standard naming conventions because it makes account names easy to guess.
 - C. Organizations should not adopt standard naming conventions because it facilitates social engineering.
 - D. Organizations should not adopt standard naming conventions because it violates the principle of security through obscurity.
53. In a **discretionary access control (DAC)** system, who is primarily responsible for assigning permissions to access objects for a user?
- A. User
 - B. Object owners
 - C. System administrator
 - D. The system itself
54. What type of access control is performed by a standard network firewall?
- A. Role-based access control
 - B. Rule-based access control
 - C. Mandatory access control
 - D. Attribute-based access control
55. **Group Policy Objects (GPOs)** are components of what access control system?
- A. Active Directory
 - B. Kerberos
 - C. RADIUS
 - D. TACACS+

56. Tonya is considering the use of a voice recognition system for authentication purposes. She is concerned about the use of recordings to fool the system. What technology can she include in her design to best reduce the risk of this type of attack?
- A. Passcode
 - B. Hashing
 - C. Encryption
 - D. Challenge/response
57. Helen recently moved from the marketing department to the sales department and retained the permissions that were assigned to her previous job, despite the fact that they are no longer necessary. What security principle does this violate?
- A. Security through obscurity
 - B. Separation of duties
 - C. Two-person control
 - D. Least privilege
58. Brenda is assisting a user who is traveling on business and is unable to access a critical system. Brenda is able to access the system herself and the user was able to access it last week from the office. The user is connected to the VPN and is still having the same issue. What type of access restriction is most likely in place?
- A. Role-based restriction
 - B. Time-based restriction
 - C. Location-based restriction
 - D. Content-based restriction

59. This diagram shows the results of testing the accuracy of a biometric authentication system. What characteristic is designated by the arrow?

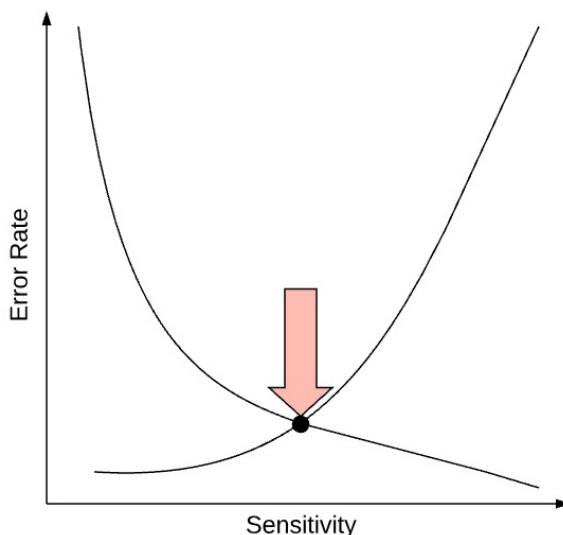


Figure 4.8

- A. FAR
 - B. CER
 - C. FRR
 - D. IRR
60. When using an **attribute-based access control (ABAC)** model, what attributes are available to the authorization system for analysis?
- A. User and system attributes only
 - B. User attributes, system attributes, and environmental attributes
 - C. User attributes only
 - D. System attributes only
61. Which one of the following principles describes the basic concept of access control that should be enforced by every network firewall?
- A. Explicit deny
 - B. Implicit deny
 - C. Implicit allow
 - D. Explicit allow

62. In a Kerberos authentication scheme, the client sends an authenticator to the **ticket-granting server (TGS)** when requesting a service ticket. How does the client encrypt this authenticator?
- A. The client encrypts the authenticator with the client's private key.
 - B. The client encrypts the authenticator with the TGS public key.
 - C. The client encrypts the authenticator with the TGS session key.
 - D. The client does not encrypt the authenticator.
63. In a network using 802.1x authentication, which device normally contains the 802.1x supplicant?
- A. Authenticator
 - B. End-user system
 - C. Authentication server
 - D. Service server
64. When you enter a password into a system, what activity are you engaged in?
- A. Authentication
 - B. Identification
 - C. Authorization
 - D. Accounting
65. Randi is configuring authentication for a SQL Server database and would like to ensure that user accounts are disabled when they leave the organization. Which one of the following approaches would best meet her requirement?
- A. Windows authentication
 - B. SQL server authentication
 - C. Mixed mode authentication
 - D. No authentication

66. Brent is the CISO for Sorin Sprockets, a manufacturer of industrial products. He is designing a federated authentication system where users from Domer Industries, one of his organization's suppliers, will use their accounts to access systems in the Sorin Sprockets domain. Which one of the following statements is correct about this relationship?
- A. There must be a transitive trust relationship between Domer Industries and Sorin Sprockets.
 - B. Domer Industries must have a trust relationship with Sorin Sprockets.
 - C. There must be a two-way trust relationship between Domer Industries and Sorin Sprockets.
 - D. Sorin Sprockets must have a trust relationship with Domer Industries.
67. Which one of the following authentication protocols is an appropriate protocol for performing administrator authentication on network devices?
- A. STACACS
 - B. XTACACS
 - C. TACACS
 - D. TACACS+
68. Ryan attempts to log in to AcmeSocial, a social networking website. The website allows him to log in with his HMail account through the use of SAML authentication. In this scenario, who is the SAML principal?
- A. Both HMail and Acme Social
 - B. AcmeSocial
 - C. HMail
 - D. Ryan
69. During what stage of the account management life cycle should a user receive their first exposure to security awareness training?
- A. Onboarding
 - B. Deprovisioning
 - C. Renewal
 - D. Privilege assignment

70. What protocol is normally used for communication between an authenticator and authentication server on a network using 802.1x authentication?
- A. XTACACS
 - B. TACACS
 - C. RADIUS
 - D. TACACS+
71. Thomas is configuring the security for a specialized computing system that will be used in a high-security environment. This system will assign tags to each file based upon their classification and users will only be able to access information that matches their security clearance. What type of security model is Thomas implementing?
- A. ABAC
 - B. DAC
 - C. MAC
 - D. RBAC
72. Which one of the following statements about iris recognition technology is incorrect?
- A. Iris recognition technology has a very low false acceptance rate.
 - B. Iris patterns may be recognized from a distance.
 - C. Iris patterns change gradually during a person's lifetime.
 - D. Iris recognition scanners can be fooled by an image of a face.
73. Carrie approaches the door to a physical facility and places her finger on a scanner. When she does so, the scanner displays the message "OK" and the door unlocks. Which one of the following steps has not occurred?
- A. Authentication
 - B. Authorization
 - C. Identification
 - D. Two-factor authentication

74. Yolanda is concerned about brute force attacks against her Windows system. Which one of the following controls is a good security practice that reduces the likelihood of a successful brute force attack?
- A. Expire the Administrator account password monthly.
 - B. Rename the Administrator account.
 - C. Disable the Administrator account.
 - D. Encrypt the contents of the Administrator account.
75. Which one of the following is a reasonable approach to handling failed authentication attempts against a password-based authentication system?
- A. Disabling a user account after three incorrect attempts.
 - B. Require an exponentially increasing timeout period between login attempts.
 - C. Lock a user account after five incorrect login attempts.
 - D. Require 5 seconds between login attempts.
76. Riley is securing an application that uses PAP authentication. Which one of the following statements is correct about PAP?
- A. PAP can't perform reliable, repeatable authentication.
 - B. PAP does not encrypt credentials and is insecure.
 - C. PAP implementations are only possible on Token Ring networks.
 - D. PAP is widely used for VPN authentication.
77. Which one of the following is an example of biometric authentication control?
- A. Password
 - B. Fingerprint scan
 - C. Smart card
 - D. Keyfob token

78. Gavin is managing the access control system for his organization. Users often change jobs and he would like to select an approach that will make it easy to reassign permissions when users move around the organization. Which access control model is best suited for his needs?
- A. MAC
 - B. ABAC
 - C. DAC
 - D. RBAC
79. After a user enters an incorrect password, many authentication systems record this activity in an authentication log. What phase of the identity and access management process is taking place?
- A. Identification
 - B. Authentication
 - C. Accounting
 - D. Authorization
80. Kip is preparing to conduct a privilege usage audit of his organization's database servers. Which one of the following data sources would be least helpful to him in this exercise?
- A. Organization chart
 - B. Database access logs
 - C. Network firewall logs
 - D. Asset classification information
81. Ron is designing a user awareness program intended to improve password security practices. Of the practices listed here, which poses the greatest risk to organizations?
- A. Use of passwords that are more than a year old
 - B. Use of passwords less than 12 characters long
 - C. Use of passwords that do not contain special characters
 - D. Reuse of passwords on multiple sites

82. Randy is building a multifactor authentication system that requires users to enter a passcode and then verifies that their face matches a photo stored in the system. What two factors is this system using?
- A. Something you know and something you have
 - B. Something you have and something you know
 - C. Something you have and something you are
 - D. Something you know and something you are
83. When creating a web application based upon the OAuth 2.0 standard, what authentication protocol is often the simplest choice?
- A. Digital certificates
 - B. RADIUS
 - C. Kerberos
 - D. OpenID Connect
84. Which one of the following authentication factors is the most difficult to practically implement?
- A. Something you are
 - B. Something you do
 - C. Something you have
 - D. Something you know
85. Val would like to configure her organization's password security policy to comply with industry best practices. How many passwords should she keep in a password history to prevent password reuse?
- A. 0
 - B. 1
 - C. 5
 - D. 8

86. Which one of the following devices is most likely to serve as an authenticator in an 802.1x network authentication scenario?

- A. Laptop with a wireless connection
- B. Desktop with a wired connection
- C. Wireless access point
- D. RADIUS server

87. What type of security card is shown here?



Figure 4.9

- A. Proximity card
- B. Smart card
- C. Magnetic stripe card
- D. Common access card (CAC)

88. Consider the statistics shown here for a biometric authentication system. What is the system's FAR based upon for this data?

	Authorized User	Unauthorized User
Accept	45	2
Reject	5	48

Figure 4.10

- A. 2%
- B. 4%
- C. 5%
- D. 10%

89. Consider the OpenLDAP password hashes shown here. Which user has the most secure password storage mechanism?

User 1

```
userPassword: {MD5}af14621b429c5a5cb94e2f46ddd52885
```

User 2

```
userPassword: {SSHA}hnN1pf1+l3Pg8H/wr6Z7YqyC4PJLYtFx
```

User 3

```
userPassword: {SHA}6EDC6DEAB58E4C149032FE96981F20B708678769
```

User 4

```
userPassword: {CRYPT}bIxoer4Wdls3Y
```

Figure 4.11

- A. User 1
 - B. User 2
 - C. User 3
 - D. User 4
90. Beth used the sign in with Facebook feature to access a website hosted by The Washington Post. This feature uses SAML-based authentication. In this scenario, what is the role that's being played by The Washington Post?
- A. Identity provider
 - B. User agent
 - C. Service provider
 - D. Certificate authority
91. In Kerberos authentication, which one of the following components is responsible for verifying that a user's password (or other credentials) is valid and correct?
- A. Client
 - B. AS
 - C. Service
 - D. TGS

92. Gina is configuring an access control system for a college that will examine a user's identity profile when determining whether to grant access to resources. Students will be granted access to limited files, while faculty and staff will have broader access. Faculty and staff access may be further segmented based upon their department, title, and other identity attributes. What type of access control system is Gina designing?

- A. ABAC
- B. DAC
- C. MAC
- D. SLAC

93. Consider the transitive trust relationships shown here. Ben has a user account in Domain D. Which domains can Ben use his account in so that he can access resources?

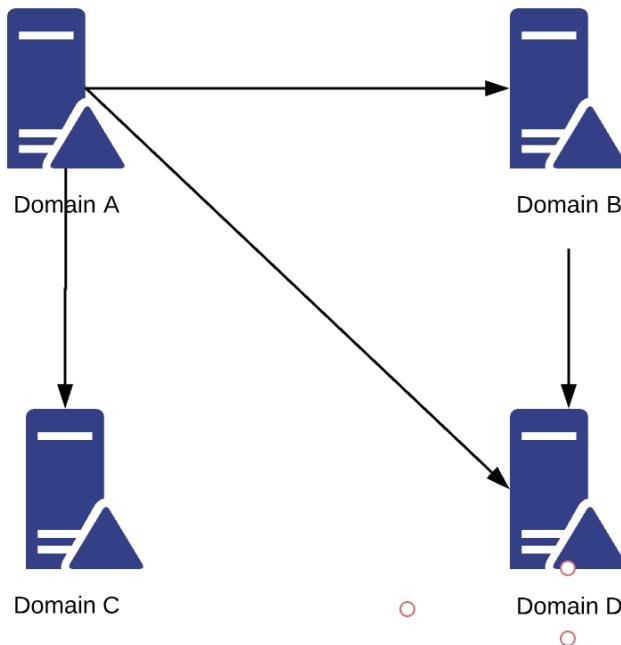


Figure 4.12

- A. Domains A, B, C, and D
- B. Domain D only
- C. Domains A, B, and D only
- D. Domains A and B only

94. When creating a role-based access control system, what mechanism can best be used to assign permissions to individuals in the same job role?

- A. Policy templates
- B. Group policy
- C. Standard procedures
- D. Administrator training

95. Jane is seeking to enforce role-based access restrictions in her organization.

Which one of the following technologies would allow her to enforce these restrictions across a variety of systems?

- A. Oracle database permissions
- B. NTFS access control lists
- C. Cisco access controls lists
- D. Active Directory group policy

96. John approaches a security guard and hands her the smart card shown here. The guard conducts a physical inspection of the card and pulls up an image of it on her system to verify that it is authentic. How many authentication factors has John successfully completed at this point?



Figure 4.13

- A. Zero
 - B. One
 - C. Two
 - D. Three
97. Which one of the following is not an example of a privileged account on a server?
- A. Shared account
 - B. Root account
 - C. Service account
 - D. Administrator account
98. Paul is designing a system that will allow users from Acme Corporation, one of his organization's vendors, to access Paul's accounts payable system using the accounts provided by Acme Corporation. What type of authentication system is Paul attempting to design?
- A. Single sign-on
 - B. Transitive trust
 - C. Federated authentication
 - D. Multifactor authentication
99. Which one of the following attacks is a critical threat that applies specifically to NTLM authentication?
- A. Rainbow table
 - B. Brute force
 - C. Pass-the-hash
 - D. Man-in-the-middle

Domain 4 Answers and Explanations

1. A. The INSERT, UPDATE, and DELETE commands all have the ability to modify information in a database, potentially resulting in an integrity violation. The SELECT command is used to retrieve, but not modify, information, so it is unlikely to result in an integrity issue. The use of the SELECT command is more likely to result in a confidentiality issue.
2. B. OAuth is commonly used to provide API-based SSO for web applications. OpenID is used for consumer-grade SSO implementations, while SAML is used for enterprise-grade SSO implementations. IPSec is a network security protocol used for VPN connections, among other purposes, but is not associated with SSO implementations.
3. A. The false rejection rate (FRR) of a system is calculated by dividing the number of false rejections by the total number of authentication attempts. In this dataset, there are 200 total authentication attempts, of which two were false rejections of an authorized user. Therefore, the false acceptance rate is 1%.
4. D. In a **mandatory access control (MAC)** model, the system determines access authorization based upon the security labels applied to objects.
5. D. All of the options presented here are good security practices, and TJ should consider each of them. However, only location-based access control will help prevent TJ's organization from running afoul of the law restricting access to residents of a single state.
6. C. Service accounts are used to provide applications with access to resources necessary for the provision of their services. This example clearly calls for a service account. Guest accounts should never be used on a server, barring extenuating circumstances. The web server service should not run with unrestricted root/administrator access.
7. C. The major issue with simple passwords is that they are far easier to break in a brute force attack than complex passwords that draw from multiple character classes. Complexity requirements do not affect the minimum length of a password or make passwords less susceptible to social engineering. Reverse hashing is not possible for any password as secure hash functions are not reversible.
8. C. This does qualify as multifactor authentication because it is based upon a passcode known only to the user (something you know) and the user's voice (something you are). However, it is not an ideal solution because an attacker could record the user speaking the passcode and replay it to gain access to the system.

9. D. Lila should encrypt the Social Security Number field using an encryption key that is not known to the database administrators. Hashing is not a good solution because it would not be possible to reverse the hash and retrieve the SSN for tax reporting purposes. Database access controls would not be effective against a database administrator, who likely has the privileges necessary to bypass those controls. Database activity monitoring might detect unauthorized access but cannot prevent it.
10. C. Service accounts are an example of privileged accounts and should be subject to strict logging requirements. Activity from other account types may certainly be logged, but this is not as high a priority as it is for privileged accounts.
11. A. Colleen should implement an emergency access procedure to allow access to the passwords. A common way to do this is to require the concurrence of two authorized individuals to retrieve the password from the vault. Providing a manager with the passwords would defeat the design requirement of nobody having knowledge of the password. Multifactor authentication would still require knowledge of the password. Redundant passwords are not a security mechanism.
12. A. PIVs contain four digital certificates. The card authentication certificate is used to verify that the PIV credential was issued by an authorized entity, has not expired, and has not been revoked. The PIV authentication certificate is used to verify that the PIV credential was issued by an authorized entity, has not expired, has not been revoked, and that the holder of the credential (YOU) is the same individual it was issued to. The digital signature certificate allows the user to digitally sign a document or email, providing both integrity and non-repudiation. The encryption certificate allows the user to digitally encrypt documents or email.
13. B. An account with a generic role-based name, such as cashier, is likely shared among many users. There is no reason to believe that this is a privileged administrator or superuser account. There is also no reason to believe that non-employee guests have access to this account.
14. A. Privilege creep occurs when an employee retains permissions from prior jobs after shifting roles within an organization. User termination audits are more likely to turn up examples of accounts that were not deprovisioned than privilege creep. Usage auditing may discover some examples of privilege creep but is designed to uncover privilege misuse. Policy reviews will not discover examples of privilege creep. Permission auditing is the most comprehensive way to discover unnecessary privileges that have been assigned to user accounts.

15. B. In NTFS permissions, explicit permissions always take precedence over inherited permissions and deny permissions take precedence over allow permissions. Therefore, in this case, the explicit deny from the manager's group blocks Tim from writing to the file, regardless of any other permissions. Then, the explicit permission assigned to Tim's account to read the file takes precedence over the inherited deny read permission on the accounting group.
16. C. Kerberos uses UDP port 88 for authentication-related communications. Port 636 is associated with the secure LDAP (LDAPS) protocol.
17. D. The offboarding process is the area of greatest risk to the organization because failure to execute deprovisioning activities in a prompt manner may mean that employees who have left the organization retain access to sensitive information or systems.
18. D. In this image, Nancy is setting logon hour restrictions for the ajones account. This is an example of a restriction based upon the time of day.
19. C. In the **Challenge Handshake Authentication Protocol (CHAP)**, the client makes an authentication request and the server responds with a challenge message. The client must then combine its password with the challenge message and hash it, providing this hashed response to the server.
20. A. The **National Institute for Standards and Technology (NIST)** issued guidelines for digital identity in 2017 that state that organizations should not set password expiration dates under normal circumstances. Organizations should only require password changes if there are signs of a potential compromise.
21. C. Geofencing places specific geographic constraints around access to a system or resource. Therefore, this is an example of location-based access control.
22. D. If the password remains known only to authorized individuals, this does not violate the principles of confidentiality or integrity. There is no indication from the scenario that the account has excess privileges, so least privilege is not violated. However, the use of a shared account prevents security staff from determining which individual performed an action, violating the principle of accountability.
23. D. The two main technologies that are used to generate one-time passwords are the **HMAC-Based One Time Password (HOTP)** algorithm and the **Time-Based One Time Password (TOTP)** algorithm. HOTP passcodes are generated sequentially and do not expire until used. TOTP passcodes are based upon the time of authentication and expire frequently. Google Authenticator uses TOTP expiring passcodes, as shown by the pie chart icons to the right of each code.

24. A. Academic studies have demonstrated that the accuracy of facial recognition technology may be significantly affected by a person's race. Ethnicity is less likely to impact other biometric techniques, such as fingerprint recognition, iris recognition, and hand geometry analysis.
25. C. When a user presents a digital certificate for authentication purposes, the primary purpose of that certificate is to provide a signed copy of the user's public key.
26. A. This is a difficult question, as it is likely that many people will automatically assume that this is a knowledge-based factor because it involves passwords. However, since those passwords are provided on a card, this approach is considered a possession-based approach (something you have). For a reference on this, see page 15 of NIST SP800-63b.
27. A. In this scenario, the website would like to access information in Taylor's Google account. This makes Taylor, as the account owner, the resource owner. Google, the service that maintains the account, is the resource provider, and the third-party website is the application.
28. B. Smart cards contain an integrated circuit that interactively authenticates with the reader. They do not necessarily contain a magnetic stripe. There is no requirement that a smart card be combined with a PIN/passcode or biometric authentication, although this is often done to achieve multifactor authentication.
29. C. Retinal scans and voiceprint analysis are both examples of biometric controls and, when used in combination with a fingerprint scan, would not constitute multifactor authentication. Security questions are a knowledge-based factor but would be difficult to implement for physical access and are generally not a very secure authentication technique due to the ease of a third party discovering correct answers in many cases. ID cards are a "something you have" factor and would be an ideal pairing for the fingerprint scan.
30. D. PIVs contain four digital certificates. The card authentication certificate is used to verify that the PIV credential was issued by an authorized entity, has not expired, and has not been revoked. The PIV authentication certificate is used to verify that the PIV credential was issued by an authorized entity, has not expired, has not been revoked, and holder of the credential (YOU) is the same individual it was issued to. The digital signature certificate allows the user to digitally sign a document or email, providing both integrity and non-repudiation. The encryption certificate allows the user to digitally encrypt documents or emails.
31. A. RADIUS uses UDP port 1812 for authentication and UDP port 1813 for accounting services. TCP ports 1433 and 1521 are associated with Microsoft SQL Server and Oracle databases, respectively.

32. B. NIST's digital identity security guidelines suggest that organizations set a minimum password length of 8 characters for passwords that are memorized by the user (NIST SP 800-63B).
33. A. TACACS+ is a AAA protocol. Therefore, it supports authentication, authorization, and accounting services.
34. A. SMS-based approaches to authentication are vulnerable to attacks where the attacker hijacks the telephone number associated with an individual and then uses that hijacked number to receive an authentication message. The other techniques listed here are all considered secure.
35. C. The gresult command computes and displays **Resultant Set of Policy (RSoP)** information for a remote user and computer. This allows administrators to determine the end result of a set of policies that have been applied to a user account.
36. A. This use of a fingerprint scan is an example of a measurement of Roger's physical body, or "something you are" authentication. Therefore, it is an example of a biometric authentication technique.
37. D. Retinal scans are generally perceived as the slowest and most intrusive biometric technique because they require the individual to make physical contact with an eye scanner. Iris scanning and facial recognition can typically be accomplished from a distance. Fingerprint scanning does require physical contact with the scanner but is generally faster than retinal scanning.
38. B. All of the authentication techniques described in this scenario are knowledge-based authentication techniques. Therefore, the only factor being used in this scenario is "something you know."
39. B. The passwords must meet complexity requirements settings, which establishes a policy that user passwords must contain characters from three different character classes and that the password may not contain the user's account name or display name. It does not enforce a minimum password length.
40. B. Recertification requires that a user's access be renewed periodically to ensure that a business need still exists. The best way that Carl can enforce this is to implement account expiration controls on the vendor accounts and require that the account sponsor recertify the need on a periodic basis to extend the expiration date. Accounts that are not recertified will then be automatically disabled.

41. D. Kerberos is a widely used authentication system that is considered secure by modern standards. The **Password Authentication Protocol (PAP)** is an insecure protocol that does not encrypt passwords as they are transmitted over the network. The **Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)** and MS-CHAP v2 both have known security vulnerabilities that make them unacceptable for standalone use today.
42. B. Shibboleth is an open source federated identity management solution that is most commonly used in academic institutions. OAuth and OpenID Connect are broadly used solutions for web-based authentication. Kerberos is mainly used as an internal authentication solution.
43. B. Martin is concerned about the misuse of legitimately assigned privileges. Credential management and privilege auditing activities would turn up improperly assigned privileges but would not identify the misuse of legitimate privileges. The use of auditing, however, analyzes the actual use of privileges and would detect insider misuse.
44. D. Group Policy Objects are processed in the following order: local policies are processed first, followed by site GPOs, domain GPOs, and **Organizational Unit (OU) GPOs**.
45. D. The use of a help desk password reset process is burdensome on staff and users but does provide security if users are asked to prove their identity with documentation. Users should never be asked to provide a current or expired password, as this promotes poor password security practices.
46. B. It is a standard practice for administrative users to have both privileged and non-privileged accounts. They may use the non-privileged account for routine activities and only use the privileged account when necessary. There is no reason that privileged accounts should not be protected by passwords. They should not be shared by multiple users or exempt from password management policies.
47. D. The best source for guidance on passwords and other authentication techniques is NIST Special Publication 800-63B: Digital Identity Guidelines. In the most recent revision of this document, NIST states that users should not be subjected to a maximum password length requirement and should be allowed to choose passwords as lengthy as they would like.
48. C. While these are all valid authentication factors, the only one that would implement Greg's location-based requirement is "somewhere you are" authentication, which takes the user's physical location into account. These factors may be used to implement context-based authentication that either blocks user access or requires additional authentication measures based upon location.

49. A. Most modern filesystems, including the Windows NTFS, Mac OS X, and cloud services such as Google Drive, allow the owner of objects to set the access permissions for those objects. These are examples of **discretionary access control (DAC)**. **Security-enhanced Linux (SELinux)** allows the system owner to set authorization based upon security labels. This is an example of mandatory access control.
50. A. The most effective way to implement access controls in this situation is to use group-based access control. This way, every new user is simply added to the appropriate group and then receives the necessary permissions. Permissive access control would violate the security principle of least privilege. Mandatory and personalized access control approaches would increase the burden on staff, rather than reduce it.
51. B. The RADIUS Access-Request message is sent by a client to the server requesting RADIUS authentication. The server then normally responds with an Access-Accept or Access-Reject message, depending on whether the authentication was successful or unsuccessful. When a system is using two-factor authentication, the RADIUS server may respond to the client's request with an Access-Challenge message asking for additional authentication.
52. A. Security professionals generally agree that the transparency benefits of standard naming conventions outweighs any risks associated with the practice by making it easier to identify users. It is true that naming conventions might make it easier to guess usernames or conduct social engineering, but these risks are generally minimal compared to the benefits of easy user identification.
53. B. In a **discretionary access control (DAC)** system, the owners of individual objects are delegated the authority to grant other users access to those objects. This is the primary means of managing authorization on most modern systems.
54. B. Rule-based access control uses a standard set of rules to determine what access is authorized. This is the access control mechanism that's enforced by a firewall, which consults a rule base each time a network connection request is received.
55. A. Active Directory uses Group Policy Objects to assign permissions and policy controls to groups of user accounts and systems.
56. D. Hashing and encryption are not practical for an interactive system because the human who's speaking cannot perform these operations. The use of a passcode does not protect against this attack if someone is able to record the person saying the passcode. Challenge/response systems prompt the user to answer a simple, randomly generated question, similar to a CAPTCHA. They increase the difficulty of a replay attack.

57. D. There is no evidence presented that this violates any separation of duties or two-person control requirements. Security through obscurity is the idea that the details of security controls should be kept secret, which is not an issue in this scenario. The fact that Helen is retaining privileges from a prior position violates the principle of least privilege.
58. C. The only factor that changed is the user's location, making a location-based restriction the most likely culprit. This type of restriction can apply even when a user connects to a VPN. We know that it is not a content-based restriction or role-based restriction because the user was able to access the same system when in the office. We can also surmise that it is not likely a time-based restriction because Brenda is able to access the system at the same time.
59. B. The accuracy of a biometric authentication system is described using three metrics. The **false acceptance rate (FAR)** is the frequency at which the system admits a person who should not be admitted. The **false rejection rate (FRR)** is the frequency at which the system denies access to an authorized user incorrectly. The FAR can be improved by increasing the sensitivity of the system, while the FRR can be improved by decreasing the sensitivity of the system. Because of this, the best measure of accuracy is the **crossover error rate (CER)**, which is the sensitivity point at which FAR and FRR are equal.
60. B. When making attribute-based authorization decisions, the ABAC system may analyze user attributes (such as job position or group membership), system attributes (such as the sensitivity level of information processed), and environmental attributes (such as the date or time).
61. B. The implicit deny principle is the cornerstone of firewall access control. This principle states that any activity that is not explicitly authorized should be blocked. Explicit allow does describe the way that access is granted, but this is only effective if the firewall uses the implicit deny principle as its foundation.
62. C. When a Kerberos client requests a session key, the client creates an authenticator consisting of the client's ID and a timestamp. The client then encrypts this authenticator with the TGS session key, which the client obtained earlier from the authentication server.
63. B. In 802.1x authentication, the end user's system contains a component called the supplicant, which initiates the authentication process. The supplicant connects to the authenticator, normally a network switch or wireless access point, that then reaches out to an authentication server to confirm the user's identity. The communication between the authenticator and authentication server normally takes place using the RADIUS and EAP protocols.

64. A. Identification occurs when a user makes a claim of identity. This claim is then proven during the authentication phase, through the use of one or more authentication factors, such as a password, smart card, or biometric reading. The system then determines the specific activities that the authenticated user is authorized to engage in by consulting **access control lists (ACLs)** and other mechanisms and then tracks user access in an accounting system.
65. A. Using the Windows authentication mode ties database accounts to domain user accounts and provides the greatest level of assurance that user accounts will be promptly disabled. Both SQL Server authentication and mixed mode authentication allow the use of local accounts that may not be promptly disabled.
66. D. Brent is creating a federated authentication system. For this system to function properly, the domain that contains resources (Sorin Sprockets) must have a trust relationship with the domain that contains the user accounts (Domer Industries). While there may also be a trust relationship in the reverse direction (which would create a two-way trust), this is not required for the federation described in the scenario. There are only two domains described here, so there is no need for transitive trust relationships, which would involve three or more domains.
67. D. The TACACS+ protocol is an authentication protocol developed by Cisco for use with network devices. It replaced the older TACACS and XTACACS protocols, which should no longer be used. STACACS is not a protocol.
68. D. In SAML authentication, the user requesting authentication (Ryan) is the principal. The organization providing the request service (AcmeSocial) is the service provider and the organization providing the login account (HMail) is the identity provider.
69. A. Security awareness training should begin at the earliest possible stage of the account management life cycle. Onboarding is this earliest step and should be the first opportunity for security awareness training.
70. C. In 802.1x authentication, the end user's system contains a component called the supplicant that initiates the authentication process. The supplicant connects to the authenticator, normally a network switch or wireless access point, that then reaches out to an authentication server to confirm the user's identity. The communication between the authenticator and authentication server normally takes place using the RADIUS and EAP protocols.

71. C. In a **mandatory access control (MAC)** system, such as the one that Thomas is implementing, the system itself sets authorizations based upon object labels. In a **discretionary access control (DAC)** system, file owners set authorizations for other users. In an **attribute-based access control (ABAC)** system, authorization is set based upon user attributes. In a **role-based access control system (RBAC)**, authorization is based upon the role of a user in the organization.
72. C. Iris recognition technology is a widely used biometric authentication technique because it is nonintrusive and has a low false positive rate. Iris patterns remain stable throughout a person's life and may be scanned from a distance. One disadvantage of this technology is that scanners may be fooled by an image of a person's face.
73. D. When Carrie places her finger on the scanner, she is using this as both an identification and authentication technique. The fact that the door opens means that authentication was successful and Carrie was authorized to access the facility. Carrie did not provide a PIN, ID card, or other authentication technique, so this is only single-factor authentication.
74. B. Yolanda should rename the Administrator account to prevent brute force attempts to guess the password for that account. Expiring the password would limit the effective length of a successful attack but would not prevent an attack from succeeding. Disabling the Administrator account would prevent legitimate administrative access to the system. Encrypting the contents of the account would not prevent someone from accessing the account.
75. B. Best practices in authentication security dictate that user accounts should be subject to an exponentially increasing login delay after failed login attempts. This greatly reduces the effectiveness of brute force password guessing attacks. Locking out or disabling user accounts after a small number of incorrect logins is likely to cause false positive alerts when users accidentally lock themselves out. This approach also facilitates denial of service attacks where an attacker can easily trigger the lockout mechanism, denying users access to their accounts.
76. B. The **Password Authentication Protocol (PAP)** is a legacy protocol that was commonly used for authentication many years ago but is no longer used today because it does not use encryption to protect passwords in transit. There are no issues with PAP's reliability or use on Ethernet networks, but is it not widely used for any purpose today.
77. B. A fingerprint scan is a measurement of an individual's physical characteristics and, therefore, is a biometric security control. Passwords are an example of something you know. Smart cards and keyfobs are examples of something you have.

78. D. This situation calls for role-based access control, where authorizations are assigned based upon a user's role in the organization. This approach would allow Gavin to simply change a user's role when they switch jobs and then the permissions would automatically update based upon the user's new role.
79. C. Logging is an example of an accounting mechanism, creating an unalterable record of authentication activity. The user already completed the identification and authentication phases and authentication was unsuccessful, so no authorization takes place.
80. C. During a privilege usage review, Kip will determine whether any employees misused legitimately assigned privileges. To do this, he would need access logs that detail privilege usage. It would also be helpful for him to have access to an organizational chart to determine employee job roles and asset classification information to identify sensitive assets. Firewall logs aren't likely to be helpful in this situation because he is looking for insider misuse, which would appear to be legitimate activity from a network perspective.
81. D. One of the greatest risks to password security occurs when users reuse passwords across multiple sites. If an attacker compromises a third-party site, they may attempt to reuse those passwords on other sites. NIST password security guidelines recommend a minimum password length of 8 characters, so a 12-character password does not pose excessive risk. Those guidelines also call for using non-expiring passwords and not requiring enhanced complexity requirements, such as the use of special characters. These practices reduce the likelihood that users will remember their passwords.
82. D. Facial recognition technology is an example of a biometric authentication technique, or "something you are." A passcode is an example of a knowledge-based authentication technique, or "something you know."
83. D. OpenID Connect is an authentication protocol built directly on top of the OAuth 2.0 framework, making it the simplest choice for user authentication.
84. B. The most commonly used authentication factors are something you know (such as a password), something you have (such as an authentication token or smartcard), and something you are (such as a fingerprint). Behavioral factors, known as something you do, are more difficult to measure and implement effectively.
85. A. Current guidance from the National Institute for Standards and Technology suggests that user passwords should not expire as a matter of best practice. Therefore, users should also not be prohibited from reusing prior passwords, unless those passwords are known to be compromised.

86. C. In 802.1x authentication, the end user's system contains a component called the supplicant, which initiates the authentication process. The supplicant connects to the authenticator, normally a network switch or wireless access point, that then reaches out to an authentication server to confirm the user's identity. The communication between the authenticator and authentication server normally takes place using the RADIUS and EAP protocols.
87. A. This is an example of a proximity card. It lacks the magnetic strip that would be found on a magnetic swipe card or the integrated circuit that would be found on a smart card or CAC.
88. A. The **false acceptance rate (FAR)** of a system is calculated by dividing the number of false acceptances by the total number of authentication attempts. In this dataset, there are 100 total authentication attempts, of which two were false acceptances of an unauthorized user. Therefore, the false acceptance rate is 2%.
89. B. User 2's password is stored using the salted SHA algorithm, which is resistant to both brute-force and dictionary attacks. The unsalted MD5 and SHA algorithms are vulnerable to dictionary attacks. The MD5 and CRYPT algorithms are vulnerable to brute force attacks.
90. C. In SAML authentication, the user agent is the web browser, application, or other technology being used by the end user. The service provider is the service that the user would like to access. The identity provider is the organization providing the authentication mechanism. The certificate authority issues digital certificates required to secure the connections.
91. B. In Kerberos authentication, the **authentication server (AS)** is responsible for validating user credentials. The **ticket granting server (TGS)** issues authentication tickets to clients after the authentication server completes this validation. The client then provides authentication tickets to the service as proof of identity, rather than providing the service with authentication credentials directly.
92. A. There is not enough information provided to determine whether this system uses **mandatory access control (MAC)** where permissions are set only by the system or **discretionary access control (DAC)**, where permissions are set by resource owners. We can determine based upon the analysis of the user's identity that this system is using **attribute-based access control (ABAC)**. SLAC is not an access control model.
93. A. Ben can access resources in Domain D because his account is located there. He can also access resources in Domain A and Domain B because those domains have direct trust relationships with Domain D. Domain C has a transitive trust relationship with Domain A, which trusts Domain D. Ben can follow this transitive trust relationship and use his account to access resources in Domain C as well.

94. B. While all of these techniques may be used to assign user permissions, the best way to achieve this goal is to use a group policy to assign permissions to role-based groups and then add users to the appropriate group(s) for their role.
95. D. All of these technologies enable the enforcement of access controls, but most are limited to a specific domain, such as Windows filesystems, Oracle databases, or network access. Active Directory group policies, on the other hand, may apply across a wide variety of Windows-based systems and applications.
96. C. While John and the guard are not using the smart capabilities of this card, they have still achieved multifactor authentication. John has presented a physical token (the card) and has also passed a biometric screening when the guard performed facial recognition by comparing him to the photo in her database.
97. A. Administrative (or root) accounts are clear examples of privileged accounts due to their superuser privileges. Service accounts also have elevated privilege levels. Shared accounts do not normally have privileged access and should not be used on secured servers.
98. C. This type of authentication, where one domain trusts users from another domain, is called federation. Federation may involve transitive trusts, where the trusts may be followed through a series of domains, but this scenario only describes the use of two domains. This scenario only describes use of credentials for a single system and does not describe a multiple-system scenario where single sign-on would be relevant. No requirement is described for the use of multifactor authentication, which would require the use of two or more diverse authentication techniques.
99. C. All of these attacks are authentication attacks. Brute force and rainbow table attacks are generic attacks that may be used against any authentication system that stores hashed passwords. Man-in-the-middle attacks are generally used against web applications. Pass-the-hash attacks are specifically effective against NTLM authentication.

5

Risk Management

Domain 5 Questions

1. Which one of the following risk assessment activities does not require advanced authorization from the target organization?
 - A. Penetration testing
 - B. Open source reconnaissance
 - C. Social engineering
 - D. Vulnerability scanning
2. Ryan is developing a security awareness training program and would like to include information about the person employees should approach if they need to clarify who may access different types of information. What role in an organization has this responsibility?
 - A. Privileged user
 - B. System owner
 - C. Data owner
 - D. Executive user
3. Which one of the following statements is not true about security awareness programs?
 - A. Some categories of employee do not require any security training.
 - B. System administrators should receive specialized technical training.
 - C. Awareness training should be customized to a user's role in the organization.
 - D. Training updates should occur when there are significant new threats.
4. Belinda is negotiating with an **internet service provider (ISP)** regarding the terms of service they will provide to her organization. Belinda would like the agreement to spell out the specific requirements for the service and include financial penalties if the service does not meet those requirements. What tool would best meet Belinda's needs?
 - A. SLA
 - B. BPA
 - C. ISA
 - D. MOU

5. Which one of the following statements about risk management is true?
 - A. Risk acceptance should only be done after careful analysis of other options.
 - B. Insurance policies are an example of risk avoidance.
 - C. Firewalls and intrusion prevention systems are examples of risk avoidance.
 - D. Risk avoidance is always preferable to risk acceptance.
6. Sonia is concerned that users in her organization are connecting to corporate systems over insecure networks and begins a security awareness campaign designed to encourage them to use the VPN. What type of control has Sonia implemented?
 - A. Technical
 - B. Administrative
 - C. Physical
 - D. Detective
7. Greg believes that a recently departed employee is likely to sue the company for employment law violations because the employee threatened to do so during an exit interview. When should the company issue a legal hold to preserve evidence?
 - A. When the employee issues a formal notice of intent to sue
 - B. When a lawsuit is filed
 - C. When they receive a subpoena
 - D. Immediately

Questions 8 through 11 refer to the following scenario:

Gary is conducting a business impact assessment for his organization. During this assessment, he identifies the risk of a power supply failure in a critical database server. He determines that the power supply is likely to fail once every three years and that it will take two days to obtain and install a replacement part.

After consulting with functional experts, Gary determines that the database server is crucial to business functions and would cause considerable disruption if it were down for more than a day. No new transactions would occur during a failure. In the event of a failure, clerks could retrieve the last four hours of transactions from an application log file and use those to recover lost data. Therefore, it would be acceptable to lose four hours of information prior to the failure.

8. What is the MTTR in this scenario?

- A. 4 hours
- B. 1 day
- C. 2 days
- D. 3 years

9. What is the MTBF in this scenario?

- A. 4 hours
- B. 1 day
- C. 2 days
- D. 3 years

10. What is the RTO in this scenario?

- A. 4 hours
- B. 1 day
- C. 2 days
- D. 3 years

11. What is the RPO in this scenario?

- A. 4 hours
- B. 1 day
- C. 2 days
- D. 3 years

12. During an incident response effort, Tony discovers that many systems on his network have different times set on their internal clocks. He wants to avoid the hassle of recording time offsets during future investigations by synchronizing clocks. What protocol would meet this need?
- A. NTP
 - B. TLS
 - C. SMTP
 - D. BGP
13. Andy is developing requirements for a disaster recovery site and needs to be able to recover operations as quickly as possible. Which one of the following recovery site options provides the quickest activation time?
- A. Warm site
 - B. Mobile site
 - C. Hot site
 - D. Cold site
14. Rhonda is preparing a role-based awareness training program and recently developed a module designed to raise awareness among users of wire transfer fraud schemes where the attacker poses as a business leader seeking to transfer money to a foreign account. Of the following audiences, which would be the most likely to need this training?
- A. System administrator
 - B. Executive user
 - C. Accounts payable clerk
 - D. Sales director

15. Tom is conducting an incident response effort and believes that a crime may have been committed against his organization involving the theft of intellectual property. Which one of the following statements best describes Tom's obligation based upon the information available at this point?
 - A. Tom must contact federal law enforcement.
 - B. Tom must contact local law enforcement.
 - C. Tom does not have a specific legal obligation to report the incident to anyone outside the organization.
 - D. Tom must notify customers of the breach.
16. Scott's company is entering into a joint venture with another organization and he would like to create a document that spells out the relationship between the two firms. Scott would like the agreement to be enforceable in court. What type of document would be best suited for this task?
 - A. SLA
 - B. BPA
 - C. ISA
 - D. MOU
17. When capturing a system image for forensic purposes, what tool should the analyst use to avoid unintentionally altering the original evidence?
 - A. Write blocker
 - B. Imaging software
 - C. Clean media
 - D. Labels
18. Brenda is a security analyst and is reviewing the alerts that were generated by a content filtering system on her corporate network. She notices that one employee has accessed a large number of sports gambling websites. What action should Brenda take next?
 - A. Disable the employee's account pending an investigation.
 - B. Inform the employee that this activity is not acceptable.
 - C. Consult her manager.
 - D. Take no action, as this would be an invasion of the employee's privacy.

19. Howard is conducting an asset valuation exercise as part of his organization's risk assessment process. He would like to ensure that the valuations included in insurance policies are sufficient to cover the restoration of operations after asset destruction. Which one of the following asset valuation techniques is most appropriate for Howard's use?
- A. Replacement cost
 - B. Original purchase price
 - C. Depreciated value
 - D. Subject matter expert estimated value
20. Jane is designing an inventory control system and wants to reduce the risk of employee theft. She designs the access controls so that a person who has the ability to order supplies from vendors does not also have the ability to log received shipments into the system. This attempts to prevent someone from ordering supplies, diverting them for their own use, and logging them into the inventory system as received. What principle is Jane most directly enforcing?
- A. Least privilege
 - B. Two-person control
 - C. Job rotation
 - D. Separation of duties
21. Jake is helping his organization move out of an office complex they are leaving and has a large quantity of sensitive paper records to dispose of. Which one of the following destruction methods would not be appropriate to sufficiently destroy the information?
- A. Degaussing
 - B. Burning
 - C. Pulping
 - D. Shredding

22. Consider the NIST incident response process shown here. Which step in the process is indicated by the question mark?

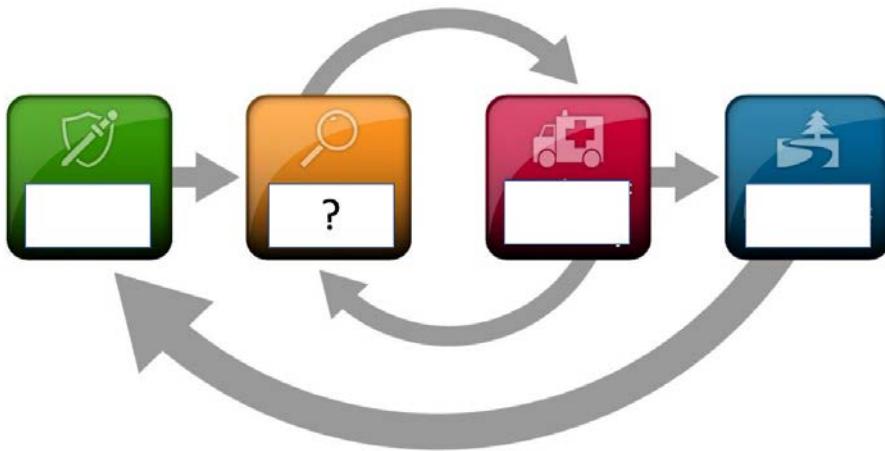


Figure 5.1

- A. Post-incident activity
 - B. Preparation
 - C. Containment, Eradication, and Recovery
 - D. Detection and Analysis
23. Which one of the following data governance roles would normally be assigned to someone of the most senior rank in the organization?
- A. Data custodian
 - B. Data steward
 - C. Data owner
 - D. Data user
24. When labeling sensitive information using the US military classification scheme, which one of the following is the lowest level of classification?
- A. Confidential
 - B. Secret
 - C. Top Secret
 - D. Top Secret SCI

25. Which one of the following categories of information is explicitly governed by HIPAA's security and privacy rules?
- A. PDI
 - B. PCI
 - C. PII
 - D. PHI
26. Gordon is considering a variety of techniques to remove information stored on hard drives that are being discarded by his company and donated to a charity for reuse. Which one of the following techniques would not be an effective way to meet this goal?
- A. Wiping
 - B. Encryption
 - C. Degaussing
 - D. Purging
27. Which one of the following activities would not typically be a component of an employee onboarding process?
- A. Deprovisioning accounts
 - B. Security training
 - C. Computer issuance
 - D. Credential generation
28. Bill is concerned about his organization's practices regarding the timing of disposing records that are no longer necessary for business purposes. Which one of the following policies would be most relevant to this issue?
- A. Data retention policy
 - B. Data encryption standards
 - C. Data access policy
 - D. Acceptable use policy

29. Which one of the following elements would not be found at a warm disaster recovery site?
- A. Computing hardware
 - B. Electrical infrastructure
 - C. Current data
 - D. Software
30. Who has the primary responsibility for ensuring that the security requirements for a system are designed in a manner that is consistent with the organization's security policy?
- A. System owner
 - B. Business owner
 - C. System administrator
 - D. Data owner
31. Kate is conducting an investigation of activity on her network. She is looking for an information source that might provide the identity of the systems that a user connected to and the times of those connections. Which one of the following data sources is LEAST likely to have this information?
- A. Wireless access point logs
 - B. NetFlow logs
 - C. Firewall logs
 - D. Content filter logs
32. Wanda is developing an incident response team for her organization. Which one of the following individuals would be the best person to have direct oversight of the team's activities?
- A. CEO
 - B. CIO
 - C. CISO
 - D. CFO

33. Don maintains a database of information about the spending habits of individual consumers. Which term would best describe this information?
- A. PHI
 - B. PII
 - C. PCI
 - D. PDI
34. Vincent is tasked with establishing a disaster recovery site but is charged with providing bare-bones functionality at a minimal cost. Which option should he consider?
- A. Hot site
 - B. Cold site
 - C. Warm site
 - D. Mobile site
35. Tom is attempting to comply with a requirement of the Payment Card Industry Data Security Standard (PCI DSS) that requires that credit card information not be stored in a system. He is unable to remove the data due to a variety of technical issues and works with regulators to implement encryption as an interim measure while he is working to fully comply with the requirement. What term best describes this control?
- A. Detective control
 - B. Corrective control
 - C. Preventive control
 - D. Compensating control
36. Sandy is working with her leadership team on documenting the relationship between her firm and a new partner who will be co-marketing products. They would like to document the relationship between the firms but do so in a less formal way than a contract. Which tool would be the most appropriate for this task?
- A. ISA
 - B. BPA
 - C. MOU
 - D. SLA

37. Which one of the following disaster recovery exercise types will have the greatest impact on an organization's operations?
- A. Parallel test
 - B. Full interruption test
 - C. Checklist review
 - D. Structured walkthrough
38. Which one of the following statements is correct about evidence gathering and litigation holds?
- A. Attorneys should review documents for privilege during the collection phase.
 - B. Most litigation holds never move forward to the production phase.
 - C. System administrators do not need to disable log file deletion during a litigation hold if the deletion process is part of a standard business practice.
 - D. Corporate attorneys bear primary responsibility for preserving evidence during a litigation hold.
39. Harold is designing an access control system that will require the concurrence of two system administrators to gain emergency access to a root password. What security principle is he most directly enforcing?
- A. Two-person control
 - B. Least privilege
 - C. Separation of duties
 - D. Security through obscurity
40. Which one of the following data destruction technique requires the use of chemicals?
- A. Pulverizing
 - B. Pulping
 - C. Degaussing
 - D. Wiping

41. Thomas is considering using guard dogs to patrol the fenced perimeter of his organization's data processing facility. What category best describes this control?
- A. Corrective
 - B. Deterrent
 - C. Compensating
 - D. Preventive
42. Which one of the following regulations contains specific provisions requiring that the organization maintain the availability of protected information to facilitate medical treatment?
- A. GDPR
 - B. PCI DSS
 - C. HIPAA
 - D. GLBA
43. Gavin is planning to upgrade the operating system on a production server and would like to obtain approval from the change advisory board. What type of document should he submit to obtain this approval?
- A. CRC
 - B. RFP
 - C. RFC
 - D. CMA
44. Ron has a hard disk that contains sensitive information. He tried connecting the drive to a computer but a component failure will not allow him to access the drive. Which one of the following destruction techniques would be the most effective?
- A. Wiping
 - B. Purging
 - C. Degaussing
 - D. Pulping

45. When choosing an appropriate off-site storage location for backup media, which one of the following factors is most important when choosing the distance between the storage location and the primary facility?
- Facility usage fees
 - Nature of the risk
 - Convenience
 - Transportation fees
46. Consider the evidence log shown here. What is the primary purpose of this tool during a forensic investigation?

EVIDENCE LOG (For Non-Photographic Evidence)						
Incident Identification: _____						
Evidence Custodian: _____						
Description of Item	Evidence ID #	Name of Person Logging Item Out	Name & Signature of Person Receiving Item	Date Item Received	Name & Signature of Person Receiving Item Back In	Date Item Received

Figure 5.2

- A. Ensure evidence is timely
 B. Prevent the alteration of evidence
 C. Document the chain of custody
 D. Ensure evidence is relevant
47. Matt is ranking systems in his organization in order of priority for disaster recovery. Which one of the following systems should have the highest impact rating?
- Enterprise resource planning
 - Routing and switching
 - Fire suppression
 - Customer relationship management

48. Which one of the following elements is least likely to be found in a security awareness training program that's been designed for end users?
- A. Confidentiality requirements
 - B. Password management requirements
 - C. Social engineering education
 - D. Patching requirements
49. What type of risk assessment focuses on evaluating the security controls put in place by vendors and contractors?
- A. Penetration test
 - B. Quantitative assessment
 - C. Supply chain assessment
 - D. Qualitative assessment
50. Randy is working within a virtualized server environment and would like to back up complete images of his virtual servers so that he can easily restore them in the event of failure. What type of backup is the most appropriate for his needs?
- A. Full backup
 - B. Snapshot backup
 - C. Differential backup
 - D. Incremental backup

Questions 51-55 refer to the following scenario.

Tonya is performing a quantitative risk assessment for her organization's new data processing facility. Due to the proximity of this facility to the coast, she is concerned about the risk of flooding.

Tonya consults flood maps from the **Federal Emergency Management Agency (FEMA)** and determines that the facility lies within the 100-year flood plain. She also reviews a replacement cost estimate for the facility and determines that the cost to replace the facility would be \$12 million. Tonya estimates that a typical flood would cause approximately \$2 million in damage to the facility and that purchasing an insurance policy would incur a premium of \$10,000 annually.

51. What is the asset value (AV) in this scenario?

- A. \$20,000
- B. \$100,000
- C. \$2 million
- D. \$12 million

52. What is the annualized rate of occurrence (ARO) in this scenario?

- A. 0.01
- B. 0.1
- C. 1
- D. 100

53. What is the single loss expectancy in this scenario?

- A. \$20,000
- B. \$100,000
- C. \$2 million
- D. \$12 million

54. What is the annualized loss expectancy in this scenario?

- A. \$20,000
- B. \$100,000
- C. \$2 million
- D. \$12 million

55. Which one of the following statements best describes the risk situation Tonya is in?
- A. Tonya should recommend that the business always purchases insurance for any risk with an ALE greater than 0.005.
 - B. The purchase of insurance in this scenario is not cost-effective from a purely financial viewpoint.
 - C. The purchase of insurance in this scenario makes good financial sense.
 - D. Tonya should recommend against the purchase of insurance because the SLE is less than the AV.
56. Wayne was called to visit the workstation of a user who believes that an attacker is remotely controlling his computer. Which one of the following evidence-gathering techniques would best document what is appearing on the user's screen?
- A. Witness interview
 - B. Operating system logs
 - C. Screen capture
 - D. CCTV
57. Gordon is considering the implementation of exit interviews for staff who voluntarily resign from his organization. Who would be best suited to perform this exit interview?
- A. Immediate supervisor
 - B. Second-level supervisor
 - C. Human resources representative
 - D. Co-worker
58. Where is the most appropriate place for an organization to keep track of risks across a wide variety of risk management disciplines?
- A. Audit reports
 - B. Risk assessment reports
 - C. Incident tracking system
 - D. Risk register

59. Which one of the following security policies is specifically designed to prevent the unintentional unauthorized observation of sensitive information?

- A. Mandatory vacations
- B. Separation of duties
- C. Least privilege
- D. Clean desk policy

60. Renee is reviewing the diagram shown here for a critical web application that's used by her company. She is performing a SPOF analysis on this environment. In the context of this analysis, what should raise the most concern?

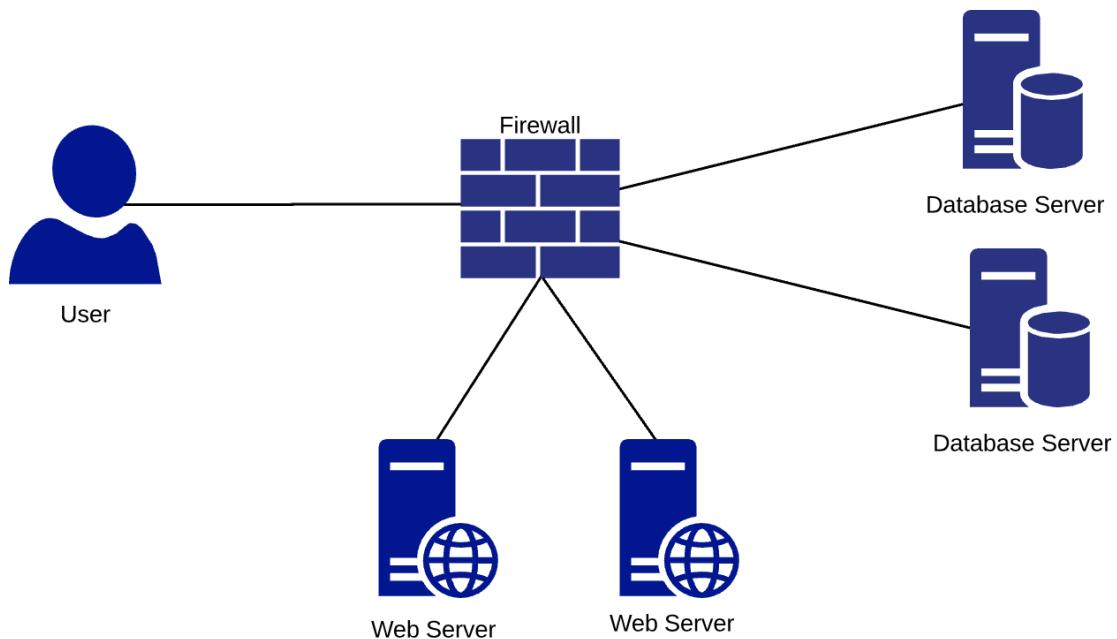


Figure 5.3

- A. User
- B. Firewall
- C. Web server
- D. Database server

61. When designing a security awareness program for employees, which one of the following groups would generally receive the most technical security training?
- A. Users
 - B. System administrators
 - C. Data owners
 - D. Executives
62. Wendy is seeking to design a compensating control for a PCI DSS requirement that she cannot meet. Which one of the following statements is incorrect about compensating controls in this situation?
- A. The compensating control must meet the intent of the original control.
 - B. The compensating control may be used to meet another PCI DSS requirement simultaneously.
 - C. The compensating control must be commensurate with the additional risk that's introduced by failing to meet the original requirement.
 - D. The compensating control must meet the rigor of the original control.
63. Steven is conducting a forensic investigation and believes that a hard drive may contain critical evidence. Which one of the following statements correctly describes how Steven should analyze this evidence?
- A. Steven should not attempt to make a forensic image because it may tamper with the evidence.
 - B. Steven should make a forensic image of the drive, lock away the image, and conduct analysis on the original.
 - C. Steven should make a forensic image of the drive, lock away the original, and conduct analysis on the image.
 - D. Steven should create two forensic images, one for storage and one for analysis, and return the original drive to the user immediately.
64. Which one of the following is the best example of a technical security control?
- A. Firewall rules
 - B. Employee credit checks
 - C. Asset inventory
 - D. Fire detection system

65. Which one of the following activities is the best example of a corrective security control?

- A. Vulnerability remediation
- B. Perimeter protection
- C. Background checks
- D. Intrusion prevention system

66. What is the primary risk associated with using motion detectors to automatically unlock a data center door when a person is attempting to exit?

- A. An employee may exit the facility with unauthorized materials.
- B. An intruder may attempt to trigger the motion detector from the outside to gain entry.
- C. The motion detector may not work during a power failure.
- D. The motion detector may not sense some employees based upon their physical characteristics.

67. Which one of the following techniques for destroying physical records is considered the least secure?

- A. Pulping
- B. Incineration
- C. Straight-cut shredding
- D. Cross-cut shredding

68. Gwen is reviewing her organization's security policies and would like to update them to restrict the web browsing of employees. Specifically, she would like to prohibit the use of pornographic websites. Where would be the most common place to detail this type of restriction?

- A. AUP.
- B. NDA.
- C. BYOD.
- D. This type of policy is an invasion of privacy and should not be implemented.

69. Evan is conducting a business impact analysis for an industrial products manufacturer. Which one of the following business functions would likely be ranked highest on a list of mission critical functions?
- A. IPS systems
 - B. Billing systems
 - C. ICS systems
 - D. HVAC systems
70. Patty is the information security officer for a bank. She is concerned about the possibility that a bank teller might be colluding with a customer to commit fraud and using his position to cover up that fraud by updating records each day to shuffle around funds. Which one of the following controls would be the most likely to uncover this type of malfeasance?
- A. Intrusion detection
 - B. Clean desk policy
 - C. Multifactor authentication
 - D. Mandatory vacations

Questions 71-74 refer to the following scenario.

Brian is the risk manager for a firm that is considering locating personnel in a country where there is a high risk of kidnapping. He is considering a variety of controls designed to manage this risk.

71. Brian is considering using armed bodyguards to protect his organization's employees. What type of risk management strategy is this?
- A. Risk acceptance
 - B. Risk avoidance
 - C. Risk transference
 - D. Risk mitigation

72. Brian is also consulting with senior managers to determine whether the business value of this effort justifies the risk. If the value is not sufficient, he is planning to propose not sending employees on this trip. What type of risk management strategy is this?
- A. Risk acceptance
 - B. Risk avoidance
 - C. Risk transference
 - D. Risk mitigation
73. After consulting with business leaders, Brian learns that the risk is justified and that the organization will send the employees. He considers purchasing an insurance policy to cover ransoms and other related costs. What type of risk management strategy is this?
- A. Risk acceptance
 - B. Risk avoidance
 - C. Risk transference
 - D. Risk mitigation
74. In the end, Brian determines that insurance policies and armed guards are not cost-effective, and the employees leave for the target country without those controls in place. What type of risk management strategy is this?
- A. Risk acceptance
 - B. Risk avoidance
 - C. Risk transference
 - D. Risk mitigation
75. Which one of the following disaster recovery test types has the least impact on business operations?
- A. Full interruption test
 - B. Structured walk-through
 - C. Parallel test
 - D. Checklist review

76. Which one of the following is the biggest disadvantage of relying on witness interviews during a forensic investigation?
- A. Witness testimony is not admissible in civil court.
 - B. Witnesses usually want to deceive the interviewer.
 - C. Witnesses interviews are costly.
 - D. Witnesses have unreliable memories.
77. Bob is performing regular backups of a system and is asked by his boss to create an emergency backup. Which one of the following backup types will consume the most disk space?
- A. Full backup
 - B. Differential backup
 - C. Incremental backup
 - D. Transaction log backup
78. Helen is examining the contract for a new SaaS provider and is scrutinizing a clause about data sovereignty. What is her primary concern?
- A. Vendor viability
 - B. Resiliency
 - C. Fault tolerance
 - D. Retaining ownership of data
79. Dylan is designing a social media security policy for his organization. Which one of the following elements would not be appropriate to include in that policy?
- A. Complete ban on use of social media by employees
 - B. Prohibition of users identifying themselves as an employee of the company on social media
 - C. Approval requirements for posts from corporate accounts
 - D. Restrictions on accessing personal social media accounts

80. Vivian's organization is about to begin a period of hiring. They will be bringing in a large number of new employees who will handle sensitive financial information. Which one of the following controls may be used as a pre-employment screening technique to reduce the risk of future fraud?
- A. Separation of duties
 - B. Time-of-day restrictions
 - C. Privileged user monitoring
 - D. Background checks
81. Hayley's team is analyzing the results of a qualitative risk assessment. The assessment uses the reporting structure shown here. Which quadrant should Hayley's team look to first when prioritizing remediation initiatives?

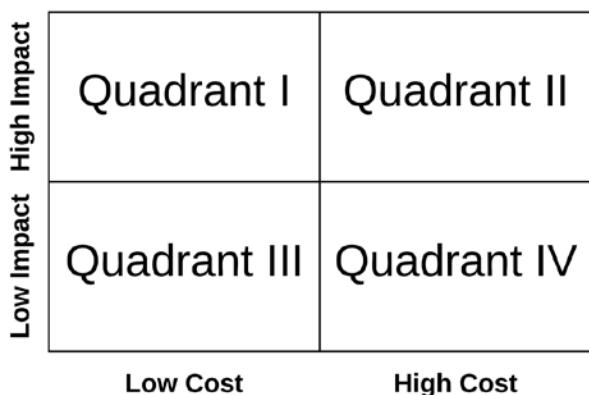


Figure 5.4

- A. Quadrant I
- B. Quadrant II
- C. Quadrant III
- D. Quadrant IV

Questions 82–84 refer to the following scenario.

John's organization performs full backups at midnight on the first day of every month and incremental backups every night at midnight (other than the first night of the month). The organization also performs differential backups every two hours, beginning at 2A.M. and ending at 10P.M. each day.

John is working to restore a system that failed at 9:30A.M. on Wednesday, November 14th.

82. How many different backups must John apply to restore the system to the most current possible status?
- A. 1
 - B. 3
 - C. 6
 - D. 15
83. How long is the time period where data may have been permanently lost?
- A. 30 minutes
 - B. 90 minutes
 - C. 2 hours
 - D. 9.5 hours
84. If the system failure occurred at 12:30A.M. instead of 9:30A.M., how many backups would John have needed to restore?
- A. 1
 - B. 2
 - C. 3
 - D. 14
85. Which one of the following sources of evidence contains the least volatile information?
- A. Archival media
 - B. Memory contents
 - C. Files stored on disk
 - D. ARP tables

86. Brianna recently accepted a position at a US financial institution that handles checking the account records of US consumers. Which one of the following laws regulates this type of information?
- A. GDPR
 - B. PCI DSS
 - C. SOX
 - D. GLBA
87. Frank is collecting digital evidence and would like to use a technical control that would allow him to conclusively demonstrate that the evidence he later presents in court is identical to the evidence he collected. Which one of the following controls would best meet this requirement?
- A. Digital certificates
 - B. Hashing
 - C. Write blocking
 - D. Evidence logs
88. Barry recently accepted a new position with a marketing agency that collects data from residents of the European Union. Which data processing law most directly applies to this situation?
- A. HIPAA
 - B. PCI DSS
 - C. GDPR
 - D. GLBA
89. Nolan's business maintains trade secret information about their manufacturing process. Which one of the following categories would best describe this information?
- A. Classified
 - B. Proprietary
 - C. Public
 - D. Internal

90. Yvonne is the business continuity analyst for a web hosting company. She is conducting an analysis to identify and prioritize mission-critical systems. Which one of the following systems should be highest on her list?
- A. A web server supporting the company's own site
 - B. Billing system
 - C. A web server supporting a single client
 - D. Firewall
91. Carla is concerned about the exfiltration of sensitive information from her corporate network by employees. Which one of the following controls would be least effective at meeting this requirement?
- A. Encrypting data in transit
 - B. Blocking the use of personal email accounts
 - C. Implementing data loss prevention systems
 - D. Building least-privilege access controls
92. As part of a business partnership, Norm is working with his counterparts at another firm to interconnect the two networks. He would like to document the security requirements for that interconnection. What tool would best meet Norm's needs?
- A. ISA
 - B. BPA
 - C. MOU
 - D. SLA
93. Donna was recently approached by the manager of a former employee who was seeking access to that employee's email account. She believes there is a valid business need for the access but is unsure how to obtain approval. What type of control would assist Donna and others in her organization in making these decisions?
- A. Service level agreement
 - B. Data handling guidelines
 - C. Data classification policy
 - D. Standard operating procedure

94. Roger is wrapping up an incident response effort. The business is now functioning normally again and affected systems and data have been restored. What activity should come next in the process?
- A. Containment
 - B. Recovery
 - C. Eradication
 - D. Lessons learned
95. Which one of the following actions would not normally occur during the recovery phase of an incident response effort?
- A. Remediate vulnerabilities
 - B. Restore from backups
 - C. Shutting down systems
 - D. Modify firewall rules
96. Under the Sarbanes Oxley Act, which one of the following corporate officers bears personal liability for the accuracy of the content of the firm's annual report?
- A. CIO
 - B. CFO
 - C. CISO
 - D. CPO
97. When designing a continuity of operations plan, which one of the following would be best described as an alternate business practice?
- A. Filing an after action report
 - B. Moving data processing to a failover site
 - C. Moving data processing to a mobile recovery facility
 - D. Using paper-based forms while systems are down

98. Which one of the following backup types typically takes the shortest amount of time to perform when done several times per day?
 - A. Complete backup
 - B. Full backup
 - C. Incremental backup
 - D. Differential backup
99. Under GDPR, which individual bears responsibility for ensuring that the company understands its privacy responsibilities and serves as the primary liaison to the supervising authority?
 - A. Data protection officer
 - B. Chief executive officer
 - C. Chief information officer
 - D. Chief information security officer
100. When providing security awareness training to privileged users, what threat should be emphasized that is a more likely risk with these employees than standard users?
 - A. Water cooler attack
 - B. Spear phishing attack
 - C. Brute force attack
 - D. Man-in-the-middle attack
101. Darren is an intrusion analyst and feels overwhelmed by the amount of information presented to him by various tools. He would like to find a solution that can correlate information from various other sources. Which one of the following tools would best meet his needs?
 - A. DLP
 - B. SIEM
 - C. IPS
 - D. IDS

102. After an incident responder identifies that a security incident is in progress, what is the next step in the incident response process?
- Eradication
 - Containment
 - Recovery
 - Preparation

Domain 5 Answers and Explanations

1. B. Any active testing that's done against an organization should only be conducted with advance approval. This includes penetration testing, vulnerability scanning, and social engineering. Open source intelligence involves consulting publicly available information sources and is passive in nature. It does not require any prior approval.
2. C. The responsibility of determining appropriate access to information is the data owner. This data owner may, by the nature of their job, fit into other categories, such as system owner, privileged user, or executive user, but it is the person's assignment to the data owner role that gives them this authority and responsibility.
3. A. Continuing education is an important component of security awareness training. All users should receive some level of awareness training on a recurring basis, but users with privileged access, such as system administrators, should receive more frequent training. This training should be based on a user's role, and technical users should receive more technical training. Training should be conducted periodically and should be updated whenever there is a significant change in the security landscape.
4. A. A **service-level agreement (SLA)** spells out the requirements for a service provider who will be offering services to a customer and frequently includes penalties for the vendor failing to meet the SLA requirements. It is the most appropriate tool for this task. An **interconnection security agreement (ISA)** spells out the security requirements for interconnecting the networks of two organizations. A **business partnership agreement (BPA)** spells out the relationship between two organizations that are entering into a joint venture or other partnership. A **memorandum of understanding (MOU)** is a document that spells out an agreement between two organizations but is typically informal and less enforceable than other agreement types. It might be possible to use an MOU in this case, but it is not the best tool for the job because it is less enforceable than a BPA.

5. A. Risk acceptance should always be done in an educated manner after the organization excludes other options. It may or may not be preferable to risk avoidance, depending on the specific circumstances. Insurance policies are an example of risk transference, not risk avoidance. Firewalls and intrusion prevention systems are examples of risk mitigation, not risk avoidance.
6. B. Security awareness training is an example of an administrative security control. The subject of the training is the use of the VPN, which is a technical control, but the training itself is administrative in nature.
7. D. An organization is required to issue a legal hold as soon as they have reason to believe that they may have evidence that will be used in a legal proceeding.
8. C. The **mean time to repair (MTTR)** is the amount of time that it will typically take to restore service after a failure. In this case, the MTTR is 2 days: the amount of time to obtain and install a replacement part.
9. D. The **mean time between failures (MTBF)** is the amount of time that typically passes between failure events. In this scenario, Gary has determined that events typically occur once every three years.
10. B. From his conversations with business leaders, Gary determined that the business can tolerate an outage of one day, making this the **recovery time objective (RTO)**.
11. A. From his conversations with business leaders, Gary determined that the business can tolerate the loss of four hours' data, making this the **recovery point objective (RPO)**.
12. A. The **Network Time Protocol (NTP)** is used to synchronize system clocks. **Transport Layer Security (TLS)** is used to encrypt network communications. The **Simple Mail Transfer Protocol (SMTP)** is used to exchange email messages. **The Border Gateway Protocol (BGP)** is used to coordinate network routing.
13. C. Cold sites have only basic infrastructure available and require the longest period of time to activate operations. They are also the cheapest option. Warm sites add hardware – and possible software – to the mix but do not have a current copy of the data that's running. They require hours to activate. Hot sites are up and running at all times and can assume operations at a moment's notice. They are the most expensive option. Mobile sites are transportable on trailers and are a good choice for a last-minute recovery plan.

14. C. While it may be reasonable for anyone in the company to have basic awareness of these attacks, the user role that's most in need of this training is the accounts payable clerk. This is the individual who is in a position to actually initiate wire transfers and, therefore, must be aware that these transfers are a common target of fraudsters.
15. C. Based upon the information presented in this scenario, Tom is under no obligation to report the incident to anyone outside of his organization. There is no indication that any of the stolen information involved personal data that would trigger a breach notification law. Tom is also not obligated to report the potential crime and should consult legal counsel on the best course of action.
16. B. A **business partnership agreement (BPA)** spells out the relationship between two organizations that are entering into a joint venture or other partnership. It is the most appropriate tool for this task. A **service-level agreement (SLA)** spells out the requirements for a service provider who will be offering services to a customer and frequently includes penalties for the vendor failing to meet the SLA requirements. An **interconnection security agreement (ISA)** spells out the security requirements for interconnecting the networks of two organizations. A **memorandum of understanding (MOU)** is a document that spells out an agreement between two organizations but is typically informal and less enforceable than other agreement types. It might be possible to use an MOU in this case, but it is not the best tool for the job because it is less enforceable than a BPA.
17. A. An analyst capturing a forensic image should use all of the tools listed here. However, the write blocker is the only tool specifically designed to preserve the original evidence by preventing the system creating the image from accidentally altering the original drive.
18. C. Brenda has detected a potential violation of the organization's acceptable use policy, so she should take action. The employee has no expectation of privacy on a corporate network, so there are no issues with doing so. However, Brenda should not unilaterally take action to disable a user's account or confront the user directly. She should consult with her manager and determine the appropriate next steps.
19. A. Replacement cost is the most reliable valuation technique to use when an organization is primarily concerned with replacing assets after a disaster. This ensures that the insurance payout is sufficient to cover the costs of replacing the asset. The replacement cost may be higher or lower than the original purchase price.

20. D. This is a clear example of separation of duties: preventing a single employee from having the ability to place orders and receive inventory. Two-person control would require the concurrence of two employees to perform a single task, while this scenario is requiring two employees to each perform two different tasks. There is no discussion of changing job assignments in the scenario, so job rotation is not at play. It is possible to describe this as an implementation of least privilege, but separation of duties is the more directly applicable security principle. Remember, the exam may include many questions that ask you to choose the BEST answer. It's important to read all of the answer options and recognize that more than one may be partially correct.
21. A. Burning, shredding, and pulping are all acceptable ways to destroy paper records. Degaussing is a magnetic destruction technique that is only appropriate for digital records.
22. D. The first phase in the NIST incident response process is preparation, which is followed by the detection and analysis phase. The final phases are containment, eradication, and recovery and post-incident activity.
23. C. The data owner is a very senior position that's assigned to someone who bears overall responsibility for the quality and security of a category of information. The data owner often oversees data stewards, custodians, and users in the performance of their duties.
24. A. The lowest level of classified information in the US military system is Confidential. Information may also be marked as Unclassified or For Official Use Only, but these are not levels of classified information.
25. D. The **Health Insurance Portability and Accountability Act (HIPAA)** contains security and privacy provisions covering **protected health information (PHI)**. It does not apply to more general **personally identifiable information (PII)** or **payment card information (PCI)**. PDI is not a common category of information.
26. C. Purging/wiping uses overwriting to remove data from a disk and is an acceptable technique to use. Encryption renders data inaccessible and is acceptable, provided that strong encryption is used. Degaussing can destroy data on the drive but it also will likely destroy the drive, preventing reuse by the charity.
27. A. During an employee onboarding process, the organization typically conducts a number of startup activities for the new employee. These commonly include issuing a computer, generating account credentials, and conducting initial security training. Deprovisioning is the removal of user access and accounts and occurs during the offboarding process.

28. A. Data retention policies govern the maintenance and disposal of records and normally reference retention schedules that specify the minimum and maximum retention periods for different categories of information.
29. C. Cold sites have only a basic infrastructure available and require the longest period of time to activate operations. They are also the cheapest option. Warm sites add hardware – and possible software – to the mix but do not have a current copy of the data that's running. They require hours to activate. Hot sites are up and running at all times and can assume operations at a moment's notice. They are the most expensive option. Mobile sites are transportable on trailers and are a good choice for a last-minute recovery plan.
30. A. The system owner is responsible for ensuring that a system's security requirements are aligned with the organization's security policy. The system administrator may be responsible for implementing these requirements, but does not set or align the requirements. The data owner may share some responsibility with the system owner but does not have primary responsibility. The business owner does not normally create system security requirements.
31. A. Wireless access points are generally not configured to log network traffic. They typically record only diagnostic information. The other data sources are far more likely to contain network traffic records.
32. C. The incident response team should be overseen by an executive with authority and responsibility for cybersecurity activities. Of the choices presented, the **Chief Information Security Officer (CISO)** is the individual who most directly meets these requirements.
33. B. This type of information certainly fits into the category of **personally identifiable information (PII)**. There is no indication that the records contain health information, so they would not qualify as **protected health information (PHI)**. There is also no indication that the records contain credit card information, so they would not constitute **payment card information (PCI)**. PDI is not a common category of information.
34. B. Cold sites have only basic infrastructure available and require the longest period of time to activate operations. They are also the cheapest option. Warm sites add hardware – and possible software – to the mix but do not have a current copy of the data running. They require hours to activate. Hot sites are up and running at all times and can assume operations at a moment's notice. They are the most expensive option. Mobile sites are transportable on trailers and are a good choice for a last-minute recovery plan.

35. D. The best way to describe this situation is as a compensating control. Tom cannot meet the original requirement and implemented an additional control to help mitigate the risk. This is the definition of a compensating control.
36. C. A **memorandum of understanding (MOU)** is a document that spells out an agreement between two organizations but is typically informal and less enforceable than other agreement types. It seems to be the most appropriate option for Sandy. An **interconnection security agreement (ISA)** spells out the security requirements for interconnecting the networks of two organizations. It is not appropriate tool for this task. A **service-level agreement (SLA)** spells out the requirements for a service provider who will be offering services to a customer and frequently includes penalties for the vendor failing to meet the SLA requirements. There is no vendor/client relationship here, so an SLA would not be the appropriate tool. A **business partnership agreement (BPA)** spells out the relationship between two organizations that are entering into a joint venture or other partnership, but it is a more formal contract, so it would not meet Sandy's requirements.
37. B. The full interruption test has the potential to disrupt all of the business activities of an organization by moving processing to the alternate facility. A parallel test also activates the alternate facility but does not switch over operations to that facility. A structured walkthrough gathers everyone together to discuss an exercise in a tabletop format. A checklist review is the least disruptive test because people simply review their disaster recovery checklists in their own time.
38. B. Litigation holds occur quite often, but very few of them actually move to the production phase. Attorneys should review documents for privilege prior to production, but it would be unnecessarily costly and time-consuming to do this during the collection phase. System administrators must disable the automatic deletion of logs or other materials subject to a litigation hold. It is the responsibility of all employees, not just attorneys, to preserve evidence when a litigation hold is in place.
39. A. Systems that require two individuals to concur before performing a single action follow the principle of two-person control. There is no indication in the question that the control also enforces separation of duties or least privilege. There is also no indication that the mechanism relies upon the dangerous practice of security through obscurity.
40. B. Pulping reduces paper to a slurry of fibers and requires the use of chemicals and water. Degaussing and wiping are digital destruction techniques and require no chemicals. Pulverizing reduces an object to dust and does not require the use of chemicals.

41. B. Guard dogs may be described as either a deterrent or preventive control, depending on the context. They do serve in a preventive role because they have the ability to corner a potential intruder. However, this is not their primary role. Their main function is to serve as a deterrent to intrusion attempts through their menacing appearance. When taking the exam, remember that you may face questions like this, asking you to choose the BEST answer from among several correct possibilities.
42. C. The **Health Insurance Portability and Accountability Act (HIPAA)** governs health information and includes specific provisions requiring that organizations preserve the availability of that data. PCI DSS governs credit card information, while GLBA covers financial records. GDPR is a European privacy regulation that is most concerned with the confidentiality and integrity of information and does not contain specific provisions about the availability of health records for medical treatment.
43. C. A **request for change (RFC)** is the standard document that's used to document the need for a change, the test plan, implementation plan, and rollback procedure. The change advisory board will review the RFC and either approve or reject the proposed change.
44. C. Degaussing uses strong magnetic fields to destroy data on a device and will work even if the drive is not functioning properly. Purging or wiping will not work if the drive is not accessible. Pulping is effective only on paper records.
45. B. All of these factors are important when performing off-site storage facility location selection. However, the primary consideration should be the nature of the risk. The off-site facility must be located far away enough from the primary facility that it would not be impacted by the same disaster.
46. C. While all of these goals are important for those handling forensic evidence, the primary purpose of an evidence log is to document the chain of custody from the time of collection to the time of use.
47. C. Life safety systems should always have a higher impact rating than other systems. Therefore, Matt should prioritize the fire suppression system over other restoration efforts.
48. D. Security awareness training should be customized for an individual's role in the organization. An end user would be responsible for protecting the confidentiality of information, managing his or her own password, and staying vigilant for social engineering attempts. Therefore, all three of these topics should be included in security awareness training for end users. An end user would not normally be responsible for applying security patches, so this topic is not necessary in training that's focused on the end user role.

49. C. Supply chain assessments specifically focus on the security controls put in place by vendors and other suppliers. Penetration tests, quantitative assessments, and qualitative assessments may indeed look at supplier controls, but they are not necessarily the focus of the assessment.
50. B. A snapshot backup is a specialized type of backup that takes a complete image of the system, rather than just storing files from the filesystem. This approach is commonly used in virtualized environments because the virtualization platform can launch a new system directly from that image.
51. D. The **asset value (AV)** is the full value of the facility. In this scenario, Tonya determined that the facility value is \$12 million using the replacement cost method.
52. A. The annualized rate of occurrence is the number of events expected in a given year. The facility lies within the 100-year flood plain, meaning that risk managers should expect a flood once every 100 years. This is equivalent to a 0.01 annual risk of flood.
53. C. The **single loss expectancy (SLE)** is the amount of damage, in dollars, that the organization should expect as the result of a single incident. From this scenario, we know that a single flood would cause approximately \$2 million in damage.
54. A. The annualized loss expectancy is the amount of damage expected to occur in any given year. It is computed by multiplying the single loss expectancy by the annualized rate of occurrence (or $ALE = SLE * ARO$). In this scenario, this is an ALE of \$2 million * 0.01 or \$20,000.
55. C. The purchase of an insurance policy is never purely a financial decision, but in this case, it does make good financial sense because the annualized loss expectancy (\$20,000) exceeds the policy premium cost (\$10,000). Tonya should not use the ALE or SLE alone to make this decision and must do so in the context of the control costs and other business factors.
56. C. Screen capture technology allows the analyst to capture what is appearing on a user's screen directly and is a good source of evidence. Operating system logs may provide information about the activity but they will not directly document what the user saw. Witness interviews may be useful, but the user's memory is not as reliable as a screen capture. It is unlikely that a CCTV camera would be positioned in such a manner as to capture the activity on a user's screen.

57. B. Exit interviews should be conducted by someone who is in a position to collect and use information about the employee's experience to positively influence the organization. This rules out a co-worker. They should also be conducted by someone who is independent of the situation, ruling out the employee's immediate supervisor, who may be part of the reason for the departure. HR is a viable option, but they do not have direct knowledge of the employee's work duties and may not capture all of the insight that's provided during an exit interview. The best choice would be the employee's second-level supervisor, who is in a direct position to implement changes, but is separated from the management of the employee by a level of supervision. HR may sit in on the interview if they wish to ensure objectivity.
58. D. The best place to track the status of all risks facing an organization is in a formal risk register. The other documents listed here may include information about risks but good practice suggests extracting that information from these sources and placing it in a risk register.
59. D. Clean desk policies require that employees clean off their desktops when leaving the immediate vicinity and secure all papers and other materials. The purpose of this policy is to prevent anyone walking by from observing sensitive information. Separation of duties and least privilege practices also protect against unauthorized access to information, but they generally protect against *intentional* unauthorized access.
60. B. In a **single point of failure (SPOF)** analysis, technologists should review an infrastructure by looking for components where a single failure could cause service disruption. In this case, the web and database servers are redundant, but the firewall is not. Therefore, the firewall should be the greatest concern. Users would not be included in a SPOF analysis.
61. B. All employees should receive security awareness training that is tailored to their role in the organization. System administrators are the most technical employees mentioned here, so they should receive the most technical training.
62. B. PCI DSS requires that compensating controls must be above and beyond the other PCI DSS requirements. Organizations may not use controls that are required by another section of PCI DSS to compensate controls for a different requirement that they cannot meet. Controls must be commensurate with the new risk that's introduced and must meet the intent and rigor of the original requirement.
63. C. In order to ensure preservation of evidence, Steven should make a forensic image of the original drive and lock the original away for safekeeping. He should then perform his analysis on the image. If the end user needs the drive back immediately, Steven should provide the user with another drive made from the image and should retain the original drive as evidence.

64. A. The installation and operation of a firewall is an example of a technical security control: the use of technology to meet security objectives. Credit checks for prospective employees and conducting an asset inventory are examples of administrative controls. Fire detection systems are an example of a physical security control.
65. A. Vulnerability remediation is an example of a corrective control because it takes actions to fix – or correct – security issues. Perimeter protection, background checks, and **intrusion prevention systems (IPS)** are all examples of preventive controls.
66. B. The primary risk associated with automated exit motion detectors is that an intruder outside the facility may be able to gain access by triggering the motion detector. For example, if it is possible to slide a piece of paper under the door, it may be possible to forcefully push the paper through so it flies up in the air and triggers the detector.
67. C. Straight-cut shredding produces long strips of paper that may be reassembled and, therefore, is not considered a secure document destruction technique. Cross-cut shredding, pulping, and incineration are all considered secure.
68. A. Gwen should place this restriction in her organization's **acceptable use policy (AUP)**. It would not be appropriate to place usage restrictions in a **non-disclosure agreement (NDA)** or a **bring your own device (BYOD)** policy. Employers are well within their rights to impose usage limits on their own networks. Employees do not have an expectation of privacy on a corporate network so there are no privacy issues with such a restriction.
69. C. The purpose of a manufacturer is to produce products. **An industrial control system (ICS)** is directly tied to this mission and would most likely be ranked highest on a list of mission critical functions. Billing is an important activity, but could be delayed due to having lower priority if a manufacturing line is idled. **Heating, ventilation, and air conditioning (HVAC)** and **intrusion prevention systems (IPS)** are important functions, but do not impact the mission as directly as an ICS.
70. D. The best way to uncover this type of fraud is through a mandatory vacation policy. If the teller is forced to take a vacation of a week or more each year, it would be difficult to continue to perpetrate the fraud during that time, increasing the likelihood that it would come to light. An intrusion detection system may uncover this type of fraud but it is generally more tuned to identifying anomalous network traffic than anomalous transactions. Multifactor authentication requirements and clean desk policies would not be effective against this risk.

71. D. Risk mitigation strategies seek to reduce the likelihood or impact of a risk. In this case, armed guards reduce the likelihood of a successful kidnapping and are, therefore, an example of risk mitigation.
72. B. Risk avoidance seeks to change business practices to eliminate a risk. By not sending employees to the affected country, Brian avoids the risk of a kidnapping there.
73. C. Purchasing insurance moves the financial risk from Brian's organization to an insurance company and is, therefore, an example of risk transference.
74. A. Risk acceptance is a deliberate decision to incur risk after considering the costs and benefits of other risk management strategies. That is what occurred in this case.
75. D. The full interruption test has the potential to disrupt all of the business activities of an organization by moving processing to the alternate facility. A parallel test also activates the alternate facility but does not switch over operations to that facility. A structured walkthrough gathers everyone together to discuss an exercise in a tabletop format. A checklist review is the least disruptive test because people simply review their disaster recovery checklists in their own time.
76. D. Generally speaking, witnesses are not trying to deceive the interviewer unless they are accused of wrongdoing. Generally, they want to assist, but suffer from unreliable memories. Interviews are generally not expensive to conduct and are definitely admissible in court.
77. A. Full backups always include all the data that's stored on the backed up media and, therefore, are always at least as large as any other backup type. This system is being regularly backed up, so other backup types will be smaller than a full backup.
78. D. While Helen is right to be concerned about all of these issues while examining a vendor contract, her primary concern here is data sovereignty. This means that she wishes to ensure that her company retains ownership of data that is stored in the vendor's systems and has the ability to retrieve that data when necessary.
79. A. Employers are able to place a variety of restrictions on social media use by employees. It is entirely appropriate to restrict use during work hours, or prevent employees from mentioning an affiliation with the company on their personal accounts. It is also appropriate to require approval for posts from corporate accounts. Employers generally may not, however, completely block employees from using personal social media accounts in their own time.

80. D. All of the techniques described here may be used to reduce the likelihood of fraud. However, background checks are the only control listed that are a pre-employment technique. The remainder of the controls are used to limit risk with current employees, rather than prospective employees.
81. A. Hayley's team should first look for high impact, low-cost remediation efforts. These are found in Quadrant I in the diagram.
82. D. John must first restore the full backup from November 1st and then apply the incremental backups from each of the 13 days up until the morning of November 14th. Then, he must apply the differential backup from 8A.M. This is a total of 15 backups that he must restore.
83. B. The most recent backup occurred at 8A.M. There is no way for John to recover any information that was created or modified between 8:00 and the failure time at 9:30, which is an interval of 90 minutes.
84. D. The only difference in this scenario is that there are no differential backups to apply. Therefore, John only needs to restore the full backup and the 13 incremental backups.
85. A. Volatile information is information that is likely to be altered or lost as time passes. Archival media is designed for long-term storage and is the least volatile data source listed here. ARP tables in a router and the contents of system memory may change frequently and are the most volatile. Files stored on disk fall in-between these two extremes.
86. D. Financial institutions are required to preserve the privacy of consumer records by the **Gramm-Leach-Bliley Act (GLBA)**. The **Payment Card Industry Data Security Standard (PCI DSS)** does apply to financial records, but its scope is limited to credit and debit card records. The **General Data Protection Regulation (GDPR)** would apply to these records if they were about European Union residents, but that is not the case here. The **Sarbanes Oxley Act (SOX)** regulates the financial accounting practices of publicly traded companies and is not applicable here.
87. B. If Frank takes a hash of the evidence as he collects it, he may then take a hash at a later date. If the two hashes match, he can demonstrate that the evidence was not altered. A write blocker may prevent tampering but it does not provide a means for Frank to demonstrate the integrity of the evidence.

88. C. The **General Data Protection Regulation (GDPR)** is a European law governing the privacy of personally identifiable information about residents of the European Union. It applies to that data worldwide. The **Health Insurance Portability and Accountability Act (HIPAA)** regulates health information in the United States. The **Gramm Leach Bliley Act (GLBA)** covers financial records in the United States. The **Payment Card Industry Data Security Standard (PCI DSS)** applies worldwide but only to credit and debit card information.
89. B. Trade secrets are normally classified as proprietary information. While the term internal may apply to trade secrets, this is not the best term to use because it normally applies to a wide range of information and the term proprietary is more specific. The term classified is normally used to refer only to government information. Trade secrets are certainly not public information.
90. D. Yvonne should first limit her prioritization to mission-critical systems. The billing system is important, but not directly tied to the mission of delivering web hosting services. Therefore, she can rank this system as having a low priority. Web servers are clearly quite important to the company's operations and Yvonne should likely rank a client's web server above the company's own server. However, none of these servers will be accessible without a functioning firewall, so the firewall should have the highest priority.
91. A. Carla should implement least privilege access controls to limit the amount of information that's available to any individual user. She can also use a **data loss prevention (DLP)** system to detect the exfiltration of sensitive information. Blocking the use of personal email accounts limits a common method for exfiltrating sensitive information. Adding encryption in transit is not likely to reduce the risk of internal theft, as employees may still access stored sensitive information.
92. A. An **interconnection security agreement (ISA)** spells out the security requirements for interconnecting the networks of two organizations. It is the most appropriate tool for this task. A **service-level agreement (SLA)** spells out the requirements for a service provider who will be offering services to a customer and frequently includes penalties for the vendor failing to meet the SLA requirements. There is no vendor/client relationship here, so an SLA would not be the most appropriate tool. A **business partnership agreement (BPA)** spells out the relationship between two organizations that are entering into a joint venture or other partnership, but does not generally include technical requirements. A **memorandum of understanding (MOU)** is a document that spells out an agreement between two organizations but is typically informal and less enforceable than other agreement types.

93. D. Donna's organization should consider implementing a **standard operating procedure (SOP)** for data access requests. This procedure could spell out the appropriate approval process for granting access to data stored in another user's account. A guideline is not mandatory and would not be appropriate in this case. A data classification policy would generally not cover access request procedures, nor would a service level agreement.
94. D. At the conclusion of an incident response, the organization should conduct a thorough lessons learned process that's designed to evaluate the response and identify opportunities for improvement.
95. C. According to the NIST incident response guide, shutting down systems would normally occur during the containment phase. In the recovery phase, administrators restore systems to normal operation, confirm that the systems are functioning normally, and (if applicable) remediate vulnerabilities to prevent similar incidents. Recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security (for example, firewall rulesets, boundary router access control lists, and so on).
96. B. The **Sarbanes-Oxley (SOX)** Act requires that the **Chief Executive Officer (CEO)** and **Chief Financial Officer (CFO)** certify that the information contained within an annual report is accurate and assigns them personal liability for these statements. The CIO, CISO, and CPO do not bear this responsibility.
97. D. During a business continuity event, organizations may choose to adopt alternate business practices that modify their normal business processes. Switching to paper-based forms is a good example of this type of practice. Moving to a failover or mobile processing facility is not a change in business practice but the use of an alternate processing facility. After action reports are a standard part of continuity operations and should be filed after any continuity event.
98. C. Incremental backups only back up files that were changed since the most recent full or incremental backup. Therefore, they are faster than full/complete backups, which would back up all files. Differential backups contain all the files that have been modified since the last full or incremental backup and would therefore take longer as each differential backup in a series grows larger since it includes all the files from previous incremental backups. Each differential backup in a series contains all of the files included in prior differential backups, while each file is only contained in one incremental backup from a series.

99. A. The **data protection officer (DPO)** is a formal designation under GDPR and the individual designated as DPO bears significant responsibilities for GDPR compliance.
100. B. Privileged users are clearly susceptible to all of these attacks. However, there is no reason to believe that they are more likely to be victims of water cooler attacks, brute force attacks, or man-in-the-middle attacks than any other user. Spear phishing attacks target specific people and are more likely to target privileged users because of their elevated privileges.
101. B. A **security information and event management (SIEM)** system receives information from other security tools and correlates across systems to discover trends and patterns that might indicate an attack. **Data loss prevention (DLP)** systems, **intrusion detection systems (IDS)**, and **intrusion prevention systems (IPS)** all generate data that might be fed to a SIEM.
102. B. After identifying an incident, the team should move into the containment phase, where they seek to limit the damage caused by the incident. Containment occurs prior to the eradication and recovery phases. The preparation phase occurs before incident identification.

6

Cryptography and PKI

Domain 6 Questions

1. Adam created a message and then computed a message digest based upon that message. He then altered a single character at the end of the message and then recomputed the message digest. Which one of the following statements about the second message digest is correct?
 - A. The second message digest should be one character different from the first digest.
 - B. The second message digest will be completely different from the first digest.
 - C. There may be minor differences in the second message digest, but they will be toward the end of the digest.
 - D. The two digests will essentially be the same, with minor differences.
2. Which one of the following encryption algorithms does not rely upon the difficulty of factoring large prime numbers to achieve its secrecy?
 - A. RSA
 - B. PGP
 - C. ECC
 - D. Diffie-Hellman
3. Helen is concerned about an attack that may retrieve credit card numbers from memory in a point-of-sale terminal. What term best describes this scenario?
 - A. Data-in-transit
 - B. Data-at-rest
 - C. Data-in-use
 - D. Data-on-disk

Questions 4-7 refer to the following scenario:

Renee and Mike are communicating using an asymmetric encryption algorithm. They each have the appropriate keys to participate in the communication.

Renee would like to send a message to Mike and make use of encryption for several purposes.

4. Renee would like confidentiality protection on the message that she sends Mike, and would like to achieve this by encrypting the message. What key should she use to encrypt the message?
 - A. Mike's public key
 - B. Mike's private key
 - C. Renee's public key
 - D. Renee's private key
5. When Mike receives the message, what key should he use to decrypt it?
 - A. Mike's public key
 - B. Mike's private key
 - C. Renee's public key
 - D. Renee's private key
6. Renee would also like to achieve non-repudiation by applying a digital signature to the message. What key should she use to encrypt the message digest?
 - A. Mike's public key
 - B. Mike's private key
 - C. Renee's public key
 - D. Renee's private key

7. When Mike receives the message, he would like to verify the digital signature. What key should he use to decrypt the signature?
 - A. Mike's public key
 - B. Mike's private key
 - C. Renee's public key
 - D. Renee's private key
8. Carol is designing a wireless network for use in a coffee shop. Her primary concern is ensuring that users have easy access to the network. Which one of the following wireless network types is most appropriate for her needs?
 - A. WPA-PSK
 - B. Open
 - C. WPA-Enterprise
 - D. WPA2-Enterprise
9. Which one of the following statements about the Blowfish algorithm is incorrect?
 - A. The algorithm is covered by a patent.
 - B. The algorithm uses a 64-bit block size.
 - C. The algorithm allows the use of any length key between 32 and 448 bits.
 - D. The developer of the algorithm does not recommend it for use today.
10. Norm would like to allow users to memorize passwords that may be used to protect strong encryption keys. What technique could he use to generate strong keys from those relatively short passwords?
 - A. Key stretching
 - B. Key escrow
 - C. Key exchange
 - D. Key revocation

11. Which one of the following properties should NOT be found in a cryptographic hash function?
 - A. Defined range
 - B. One-way
 - C. Collision
 - D. Reproducible
12. Darryl is concerned about the level of security provided by the encryption of Microsoft Office documents. What component of Windows could he upgrade to allow the use of stronger encryption with these documents?
 - A. CRL
 - B. CSP
 - C. PKI
 - D. SP
13. When creating a digital certificate, what key does the certificate authority use to prevent the public disclosure of the certificate's public key?
 - A. The certificate owner's private key
 - B. The CA's private key
 - C. The CA's public key
 - D. No key
14. Solve the exclusive or (XOR) operation shown here:

$$\begin{array}{r} 0110 \\ \oplus \quad 0101 \\ \hline \end{array}$$

Figure 6.1

- A. 0011
- B. 1100
- C. 0111
- D. 1000

15. As you increase the length of a key by a single bit, how much more resilient does that key become against a brute force attack?
 - A. Twice as strong
 - B. One percent stronger
 - C. 10 times stronger
 - D. Four times stronger
16. David encountered a cryptographic implementation using the RC4 stream cipher with a weak key and he would like to secure this implementation. What action should he take?
 - A. Apply the algorithm three times
 - B. Increase the key length
 - C. Replace the cipher algorithm
 - D. Apply the algorithm twice
17. Will is creating a digital certificate for his web server. He will request the certificate from his internal corporate CA, which is an intermediate CA validated by the GeoTrust root CA. Who would create the CSR in this case?
 - A. GeoTrust creates the CSR after receiving a request from Will
 - B. Will creates the CSR on the GeoTrust website
 - C. Will creates the CSR on the web server
 - D. The internal CA creates the CSR after receiving a request from Will
18. Which one of the following approaches to cryptography is least useful for data in transit over a network?
 - A. FDE
 - B. File encryption
 - C. TLS
 - D. AES

19. Kaitlyn is selecting a wireless encryption algorithm for use in her organization. If she is able to choose from the following options, which would be the best choice?
- A. WPA
 - B. WPA2
 - C. WEP
 - D. WPS
20. Which one of the following block cipher modes of operation may NOT be used to turn a block cipher into a stream cipher?
- A. OFB
 - B. GCM
 - C. CTM
 - D. ECB
21. Ron is troubleshooting an application that is having trouble communicating with a RADIUS authentication server to validate user credentials. He believes that the issue may be a firewall problem. What port should he verify is accessible through the firewall from the application to the RADIUS server?
- A. 1812
 - B. 1521
 - C. 1433
 - D. 3389
22. Which one of the following statements about block and stream ciphers is correct?
- A. Most modern ciphers are block ciphers
 - B. Stream ciphers commonly use Feistel networks
 - C. Block ciphers are faster than equivalent stream ciphers
 - D. Block ciphers encrypt 1 byte at a time

23. Paul is sending a message to Kathy using asymmetric cryptography. In the final stage of the process, he uses Kathy's public key to encrypt the message. What goal(s) of cryptography are met by this encryption?
- A. Confidentiality, integrity, and non-repudiation
 - B. Confidentiality only
 - C. Non-repudiation only
 - D. Confidentiality and integrity only
24. When configuring cipher suites for a web server, which one of the following key exchange approaches would produce the strongest security?
- A. DHE Group 1
 - B. DHE Group 2
 - C. Export cipher suite
 - D. ECDHE
25. Harold is connecting to a wireless network that uses the 802.1x protocol. What term best describes the operating system component on his computer that interacts with the 802.1x service?
- A. The authentication server
 - B. The client
 - C. The supplicant
 - D. The access server
26. Which one of the following message-digest sizes is supported by the SHA-3 hash algorithm?
- A. 256 bits
 - B. 224 bits
 - C. SHA-3 supports any size digest
 - D. 384 bits

27. Alan is developing a new application that will rely upon cryptography. Which one of the following techniques is the best way for him to ensure that the cryptography is properly implemented?
- A. Write the cryptographic code directly in his application
 - B. Hire a vendor to develop a custom cryptographic module
 - C. Use a popular open source cryptographic module
 - D. Test the software prior to use
28. Greg is using a pseudorandom number generator (PNRG) to create cryptographic keying material. Which element of the algorithm must be varied with each use to prevent reproduction attacks?
- A. The hash
 - B. The algorithm
 - C. The key
 - D. The seed
29. What block size is used by the Advanced Encryption Standard when encrypting and decrypting data?
- A. 64 bits
 - B. 128 bits
 - C. 192 bits
 - D. 256 bits
30. When designing an encryption algorithm, which elements of the algorithm should be preserved as secrets?
- A. Both keys and encryption techniques should be kept secret
 - B. Encryption techniques
 - C. Decryption techniques
 - D. Cryptographic keys

31. Andy is implementing a new VPN server and would like to use the Diffie-Hellman algorithm. Which one of the following DH groups is most secure?
- A. Group 2
 - B. Group 14
 - C. Group 19
 - D. Group 5
32. Rob is sending a message to Gary and, as part of that communication, he computes the hash value of the message using the SHA-1 algorithm. Which of the following options best describes the set of people who are able to compute that hash value if they have the original message?
- A. Only Rob can compute the hash
 - B. Anyone can compute the hash
 - C. Only Rob or Gary can compute the hash
 - D. Only someone with the encryption key can compute the hash
33. Seth is encrypting a document to provide confidentiality using a symmetric encryption algorithm. He is sending the document to Helena. Which key should he use to perform this encryption?
- A. A shared secret key
 - B. Seth's public key
 - C. Seth's private key
 - D. Helena's public key
34. Which one of the following cryptographic algorithms was chosen as the winner of the contest to implement the Advanced Encryption Standard (AES)?
- A. Twofish
 - B. Rijndael
 - C. Blowfish
 - D. Serpent

35. When storing passwords in a password file, what term is used to describe a random value combined with a password to reduce the risk of rainbow table attacks?
- A. Cream
 - B. IV
 - C. Nonce
 - D. Salt
36. What is the encrypted version of the message shown here when the ROT13 algorithm is used?

S E C R E T

Figure 6.2

- A. SECRET
 - B. FRPERG
 - C. \$TR#T%
 - D. XJHWJY
37. What encryption protocol does the WPA2 algorithm use to provide confidentiality for wireless communications?
- A. 3DES
 - B. TKIP
 - C. DES
 - D. CCMP
38. What is the most commonly used secure message-digest length with the RIPEMD algorithm?
- A. 128 bits
 - B. 160 bits
 - C. 256 bits
 - D. 320 bits

39. What protocol was designed as an efficient and secure replacement for the use of CRLs to determine whether a digital certificate has been revoked by the certificate authority?
- A. CSR
 - B. OSCP
 - C. CSP
 - D. TACACS
40. Don would like to ensure that traveling users are provided with encryption services for all of their network connections while on the road. Which one of the following cryptographic technologies would best meet this need?
- A. SSH
 - B. An encrypted web proxy
 - C. A web browser supporting HTTPS
 - D. A VPN
41. Carl connects to a wireless network that is using strong encryption and encounters the message shown here. Which type of network might he be connecting to?



Figure 6.3

- A. WPA2-PSK
- B. WPA-Enterprise
- C. WEP2-PSK
- D. WEP-Enterprise

42. Bill is designing a security solution that must be able to encrypt network traffic without introducing a delay into the transmission of that traffic. What term best describes Bill's requirement?
- A. Low resiliency
 - B. High latency
 - C. Low latency
 - D. High resiliency
43. Nick is using AES encryption to protect files stored on his network. What is the simplest step he can take to improve the strength of that encryption?
- A. Apply a second encryption algorithm on top of AES
 - B. Change algorithms
 - C. Increase the key length
 - D. Use two rounds of AES encryption
44. Zack is purchasing a digital certificate for his organization's web server from a trusted certificate authority. He would like to choose the certificate that provides the highest degree of trust to site visitors. Which certificate type should he choose?
- A. EV
 - B. OV
 - C. DV
 - D. NV
45. Vincent and Fred would like to communicate with each other using the 3DES encryption algorithm. What key must Vincent have in order to successfully communicate with Fred?
- A. Vincent's private key
 - B. A shared secret key
 - C. Fred's public key
 - D. Fred's private key

46. ROT 13 is an example of what type of cipher?
- A. Cryptographically strong
 - B. Transposition
 - C. Substitution
 - D. Hashing
47. Which one of the following is not a disadvantage of using a CRL to revoke digital certificates?
- A. Fails to open if the client can't retrieve the CRL
 - B. Slow updating
 - C. Does not work for EV certificates
 - D. Requires the client to search the CRL
48. Ben is conducting forensic analysis and discovers an image stored on a computer entitled "Drug Formula." When he opens the file, he sees the image shown here. If someone did embed a formula in the file, what technique did they likely use?



Figure 6.4

- A. A stream cipher
- B. Hashing
- C. Obfuscation
- D. Steganography

49. Which one of the following risks would be addressed by applying full disk encryption to a computer?
- A. Malware infection on the device
 - B. The theft of the device
 - C. Eavesdropping on the network segment used by the device
 - D. An insider attack
50. Which one of the following security principles does NOT describe a standard best practice in cybersecurity?
- A. Least privilege
 - B. Security through obscurity
 - C. Separation of duties
 - D. Defense in depth
51. Sam is designing a new certificate authority (CA). He creates an initial CA and uses that CA to authorize several subordinate CAs that issue certificates to end users. He then disconnects the initial CA from the network to protect it against attack. Which one of the following terms best describes the initial CA?
- A. Online CA
 - B. Intermediate CA
 - C. Offline CA
 - D. Unauthorized CA
52. The Tor network allows both participants in the communication to remain anonymous by filtering traffic through a number of relay nodes. What term describes the technology used by Tor to ensure anonymity?
- A. Perfect forward secrecy
 - B. Security through obscurity
 - C. Obfuscation
 - D. Non-repudiation

53. Brianne is accessing a website over a TLS connection. When her browser retrieves the digital certificate from the website, what key should she use to verify that the certificate may be trusted?

- A. The CA's public key
- B. The CA's private key
- C. The website's public key
- D. The website's private key

54. Carla is examining her wireless access point and notices that it bears the logo shown here. What technology does this access point support?



Figure 6.5

- A. WPS
- B. WPA2
- C. WPA
- D. WEP

55. How many times must the DES encryption algorithm be applied to data in order to achieve a reasonable level of security?

- A. 1
- B. 2
- C. 3
- D. It is not possible to implement DES in a secure manner

56. What does the PGP algorithm use to facilitate the trusted exchange of public keys between users?
- A. Certificate authorities
 - B. Web of trust
 - C. A central key management server
 - D. BitTorrent
57. What standard is used to define the format of a digital certificate?
- A. X.509
 - B. 802.1x
 - C. RFC 1918
 - D. RFC 783
58. What mathematical principle does the RSA algorithm rely upon for security?
- A. Cosine law
 - B. Prime factorization
 - C. Elliptic curve
 - D. Ohm's law
59. Brian is designing a communications system for the exchange of stock transactions. He wants to implement a system where a customer cannot later claim that someone else placed an order on their behalf. What goal of cryptography is he attempting to achieve?
- A. Integrity
 - B. Authentication
 - C. Confidentiality
 - D. Non-repudiation
60. Barry is configuring 802.1x authentication for his wireless network. In a typical wireless authentication scenario, what device would act as the 802.1x client?
- A. The backend authentication server
 - B. Mobile devices connecting to the network
 - C. The router
 - D. A wireless access point

61. Victor is evaluating the encryption algorithm options available for use in his organization. Of the options presented here, which would provide Victor with the strongest level of encryption?
- A. AES
 - B. 2DES
 - C. DES
 - D. RC4

62. Which mode of cipher operation is shown here?

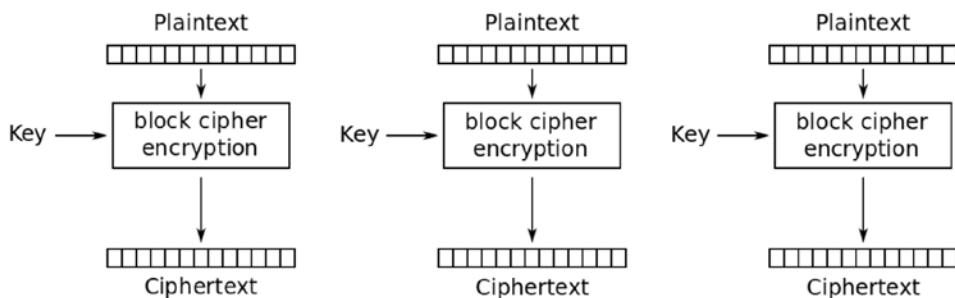


Figure 6.6

- A. OFB
 - B. CFB
 - C. ECB
 - D. CBC
63. Which one of the following keying options creates the most secure implementation of the 3DES encryption algorithm?
- A. K1=K2=K3
 - B. K1, K2, and K3 are independent
 - C. K1=K2; K2 is not equal to K3
 - D. K2=K3; K1 is not equal to K3

64. Which one of the following is not a secure technique for exchanging encryption keys?
- A. An emailed key
 - B. The Diffie-Hellman algorithm
 - C. Digital certificates
 - D. In-person exchange
65. Frank accesses a website over HTTPS using a standard web browser. After his browser retrieves the site's digital certificate and validates the signature, what piece of critical information does it extract from the certificate to continue the communication session?
- A. The web server's private key
 - B. The web server's public key
 - C. The CA's public key
 - D. The CA's private key
66. What encryption key length is used by the original Data Encryption Standard (DES)?
- A. 16 bits
 - B. 56 bits
 - C. 112 bits
 - D. 128 bits
67. What technology does the PEAP protocol combine with EAP to provide the secure communication of authentication credentials?
- A. IDEA
 - B. SSL
 - C. LEAP
 - D. TLS

68. Shannon is assisting a business unit with the implementation of an approach that may be used to verify the integrity and authenticity of a message. Which one of the following algorithms would best meet this need?
- A. SHA-3
 - B. AES
 - C. SHA-2
 - D. HMAC
69. Jerry is examining the cipher suites available for use on his organization's web server and finds the following supported options. Which one of these is it most important for him to remove?
- A. TLS_DHE_RSA_WITH_AES_128_GCM-SHA256
 - B. TLS_RSA_WITH_RC4_128_SHA
 - C. TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
 - D. TLS_RSA_WITH_3DES_EDE_CBC_SHA
70. Riley would like to perform port-based authentication on her network and is seeking an authentication protocol specifically designed for this purpose. Which protocol would best meet her needs?
- A. RADIUS
 - B. 802.1x
 - C. Kerberos
 - D. TACACS
71. Bill is configuring a web server to use TLS cryptography. When the server is up and running, how many users will share each ephemeral session key?
- A. 1
 - B. 2
 - C. 4
 - D. All users use the same session key

72. What is the main reason for using an ephemeral symmetric session key within a TLS session rather than simply using asymmetric encryption keys for communication?
- A. Symmetric cryptography is more secure than asymmetric cryptography
 - B. Symmetric cryptography is faster than asymmetric cryptography
 - C. Asymmetric cryptography can only be used to exchange keys and not to transfer data
 - D. Ephemeral keys can be reused
73. Mike accesses the wireless network in a local coffee shop and sees the login screen shown here. What type of authentication is in use on this network?



Figure 6.7

- A. WPA-PSK
- B. WPA-Enterprise
- C. Captive portal
- D. WPA2-Enterprise

74. Examine the digital certificate shown here. What organization is asserting that the public key presented in this certificate actually belongs to Bank of America?

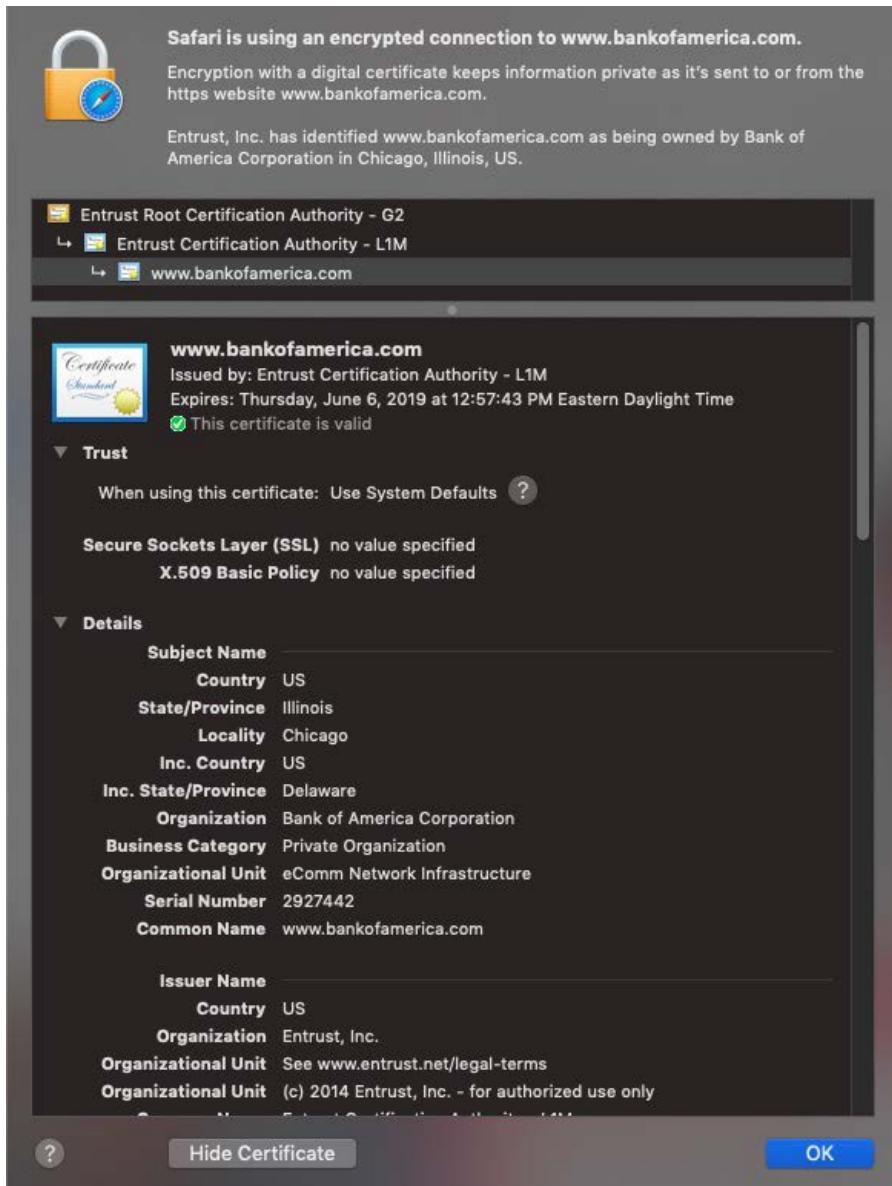


Figure 6.8

- A. No such assertion is being made
- B. Bank of America Corporation
- C. eComm Network Infrastructure
- D. Entrust Certification Authority

75. What cipher does EAP use to protect the confidentiality of authentication credentials passed using the protocol?
- A. 3DES
 - B. AES
 - C. No cipher
 - D. RC4
76. Which one of the following digital certificate types offers the lowest degree of assurance?
- A. EV
 - B. OV
 - C. DV
 - D. XV
77. Examine the digital certificate shown here. Which one of the following URLs would not be covered by this certificate?

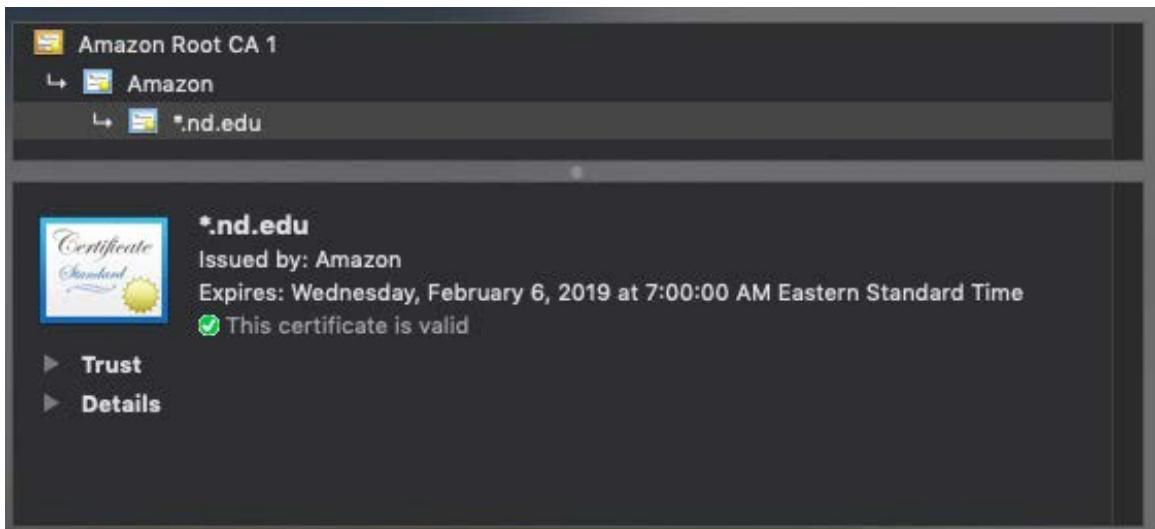


Figure 6.9

- A. <https://www.mike.nd.edu/>
- B. <https://www.nd.edu/>
- C. <https://www.nd.edu/mike>
- D. <https://mike.nd.edu/>

78. Ray is configuring a highly secure web application that is being used by a limited number of users. He would like to apply a client-side control that informs the client browser exactly what certificate to expect from the server. Which one of the following controls meets his requirement?
- A. Certificate stapling
 - B. Certificate pinning
 - C. Certificate folding
 - D. Certificate chaining
79. Consider the digital certificate shown here. What format is the file used for this digital certificate?

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAmxYcf8/qYv9kvXKat0panz+f/Bq6yZbfCdAz+Xnla7iokSb8ZmZ/N7/pBmYo
HIkrPTnUpAkUHlyiiot4GpkLttQNRrND8gYQ0mn1MHZJlvr52DLuBuJzbFu1+rKQLUmyVt9oHOp
3aBdpWcz3d4MjgmzQPgJAC0tSD0LKMzP3JbHkoK70gEqc4cBEfCL4MlzsAYkqhWnQ/QgYnrII278
l7CanwFFlinFNp0EPEneN3uvoslM1W81k7ie1/T2VLVLLftB1PZY+df5o7vLweF4ffbaUilvbLCsn
xHk/FSiWF3d9XQePUhjInKbg9UeJZCcSbWXH9cV2dAgPqo7VIWpZwIDAQABAoIBACicFKBfSEfe
CnoVLW+cQlia54CzWx/4crT2IPX9tjtq0guwAr2przxg81rqmyxFut3Qa976mK93aqndlPhgao9s1
MI6HUxD214AES0EEyEfxokS7qVoW7S790Nxhr6E8QAfBfl18CMJn9jr+kXRXEZBQgAMMwcpzUay
PV7UqsVfCb+Xy3i2y//YXZkYb0WLAFjuLh28nXvx/NcGTJ2SmIU3Cj3suqIQ0L4u70X784Cw9p3x
BEa4FFB84aWbImrfciRmoGOFU7nvrYTgDbTxAR6HqQkD1NIZZPhia3D7XEvqzbL9lXzLaXLVXPuW
HoZMENAiDTWF5dUKz1EpAP1GMtkCgYEAzjP5yrnXjjaDgR7zJGMrRWZAWllReRW+DXkIZaHVHZch
LTcWf6qEKPbHmW8ayD8xzSwQs38hg9ItqgrKiV5GgWmqflfPxR07Fckzm7dLsmn0iTfIsKTjhT5W
ibvRp83AyuR5pw+KUWzeF2rw4b1tfA569JZPS+pCW/VQ+4ZATI0CgaEAwIn3etXdakC81CqxNm7r
f4vdSOrhI7cHJX+9L82taWUkEuqnppjCIr0CXrnTt5qgD5Y2BPGvDrkt0Li55c+bNXccbL71jHNY
4EiRuPXogh+ELD7bg4d1C6xwIg/jdwDLkpC7P9r20I8jWpNvyhcRh6vX9xTQX05YXxnrxHLLQsMC
gYA/S5sQjI0rUK57MxnlgIIqD2IPmb01kuP81LssH0oAxERN0cwZMilRPbc1NPKepy9NUIpr3s1V
4m1cLogxtHuNbWcFU04Wt4tMe61YzCHzSSzj9ALH/z1QprsAGmQrwa07w/hHrLBzoByINjZswkzX
eMzrT7xVjDoaakAKhUI1fQKBgQCxTxzi0Qum4E1E0d/l283x0prBITg2LLpffSjjWfTlh2fWJ9Sm
fiziCg/4LgdEIRhf4kPy/6Ln2y709R70/0ABMahMGPtGEX96ZDoWbBcljpiIqoY6tUbbrjxBkgI2
uDvAyJo3mTla0r6LDhW3tNDG8UDcYIWYDy0gv104t0JqQwKBgHXfmoLKG8iGCjn8AB6KryK7BTiK
ULHuklkIcHHFh8mdQJd9VzaAlilqvny7b9aTwq0RB9c8PvBAbexD6v5ti+0KiPCJfiZiNIS2K07q
9ICEyB2dPA1kYLkfAfRVr0P6oIKN1l7PMCY/6PykRc1/xVZ+kLwecBR5CtRSfxsqMc9
-----END RSA PRIVATE KEY-----
```

Figure 6.10

- A. .DER
- B. .PEM
- C. .P12
- D. .PFX

Questions 80 and 81 refer to the following scenario:

Ryan is evaluating potential encryption algorithms for use in his organization and would like to choose an approach that provides strong security.

80. Ryan would like to ensure that the relationship between the encryption key and the ciphertext is quite complex so as to avoid reverse engineering. What property is he seeking to enforce?
 - A. Diffusion
 - B. Collusion
 - C. Obfuscation
 - D. Confusion

81. Ryan would also like to prevent statistical analysis attacks by choosing an algorithm that prevents patterns in the plaintext from also appearing in the ciphertext. What property is he seeking to enforce?
 - A. Diffusion
 - B. Collusion
 - C. Obfuscation
 - D. Confusion

Domain 6 Answers and Explanations

1. B. Message digests are one-way functions where it is not possible to reproduce the input by observing the output. To facilitate this, the digests produced by messages with even slight differences are completely different from each other. There is no way to assess the similarity of two messages by comparing their message digests.

2. C. The Pretty Good Privacy (PGP), Rivest Shamir Adelman (RSA), and Diffie-Hellman algorithms all depend upon the difficulty of the prime factorization problem to achieve secrecy. The Elliptic Curve Cryptography (ECC) algorithm does not use prime numbers, and instead depends upon the mathematical properties of an elliptic curve.

3. C. Data stored in memory is considered data in use, and is the most difficult scenario to protect against. Data at rest is data stored on a disk or other storage device, while data in transit is data being sent over a network.

4. A. In an asymmetric encryption algorithm, the sender of a message achieves confidentiality by encrypting the message with the recipient's public key.

5. B. In an asymmetric encryption algorithm, the recipient of a message decrypts the message by using the recipient's private key.
6. D. In an asymmetric encryption algorithm, the sender of a message may achieve non-repudiation by digitally signing the message. To do this, the sender creates a message digest using a secure hash function and then signs that message digest their own private key.
7. C. In an asymmetric encryption algorithm, the recipient of a digitally signed message decrypts the digital signature using the sender's public key. The recipient then computes the hash of the message using the same hash function used by the sender and compares the hash with the decrypted signature. If the hash and decrypted signature are identical, the message is authentic.
8. B. In an open environment such as a coffee shop, the most effective approach is likely to use an unauthenticated, unencrypted network that users can connect to easily and simply. While this leaves communication unsecured, it minimizes the support needed and increases the likelihood that users will successfully connect. In this setup, users are responsible for providing their own encryption, if desired. This is an excellent example of conducting a risk/benefit analysis – the most secure option is not always the best choice!
9. A. Bruce Schneier designed the Blowfish algorithm as an open source alternative to other patented encryption algorithms. The algorithm supports a 64-bit block size and variable length keys between 32 and 448 bits. Schneier does not recommend that people use Blowfish today, instead recommending the Twofish algorithm.
10. A. Key stretching is a cryptographic technique used to turn a relatively weak key, such as a short password, into a stronger cryptographic key used to protect the confidentiality of information.
11. C. Collisions occur when a hash function produces the same output for two different input values. This is a serious failure of the algorithm. Hash functions should have a defined range, as they often produce fixed-length output values. They should be one-way functions, meaning that it is not possible to obtain the plaintext from the hash. They should also be reproducible, meaning that anyone using the same hash function on the same input should receive the same hash value as output.
12. B. Cryptographic Service Providers (CSPs) are components of Microsoft Windows that add support for specific encryption algorithms. Darryl can ensure that his systems are configured to use strong CSPs.

13. D. The purpose of a digital certificate is to share a public key freely with the world. Therefore, the public key is not encrypted at all – it is freely given to anyone who receives the certificate.
14. A. The exclusive or (XOR) operation is true when one, and only one, of the inputs is true. This means that one input must have a value of 1, while the other has a value of 0. Applying this operation to the problem shown here gives the answer of 0011.
15. A. Adding a single bit to a cryptographic key doubles the number of possible keys, making the new key length twice as strong as the previous key length.
16. C. The RC4 algorithm has inherent insecurities and should not be used under any circumstances. David should replace RC4 with another algorithm that meets modern security standards.
17. C. In the process of creating a digital certificate, the requester creates a certificate signing request (CSR) on the device that will receive the certificate and then sends this CSR to the CA for use in creating the certificate.
18. A. Full disk encryption is designed to protect data stored on a disk and would not affect data transmitted over a network. Transport Layer Security (TLS) is designed specifically to protect data being sent over network connections. File encryption may also be used to protect the contents of files being sent over a network. TLS and file encryption may both make use of the Advanced Encryption Standard (AES) to provide encryption and decryption functionality.
19. B. The WPA2 algorithm is the current best practice standard for wireless encryption. The WPA algorithm is also considered secure, but is not the current best practice. The Wi-Fi Protected Setup (WPS) protocol is used to establish a wireless connection and is not an encryption standard. The Wired Equivalent Privacy (WEP) protocol is an outdated wireless encryption standard.
20. D. The counter mode (CTM), Galois/counter mode (GCM), and output feedback (OFB) modes of operation may all be used to turn a block cipher into a stream cipher. The Electronic Code Book (ECB) mode retains the characteristics of a block cipher.
21. A. RADIUS authentication may take place over TCP or UDP, and uses port 1812 in either case. TCP port 1521 is reserved for Oracle database communication, while TCP port 1433 is reserved for Microsoft SQL Server. TCP port 3389 is used by the Remote Desktop Protocol (RDP).
22. A. It is true that block ciphers make up the vast majority of modern encryption algorithms. Stream ciphers are faster, not slower, than block ciphers. Block ciphers may make use of Feistel networks, while stream ciphers cannot. Block ciphers work on chunks of data, rather than a single byte at a time.

23. D. When Paul encrypts the message with Kathy's public key, he provides confidentiality for the message because Kathy is the only one with the corresponding decryption key. When Kathy decrypts the message successfully, she also receives a guarantee of integrity because the message would not decrypt properly if it were altered. There is no guarantee of non-repudiation because Paul did not digitally sign the message.
24. D. The Elliptic Curve Diffie-Hellman algorithm (ECDHE) is a strong, modern approach to key exchange. Export cipher suites are intentionally weak and should always be avoided. DHE groups 1 and 2 are also outdated and inappropriate for use in modern applications.
25. C. In an 802.1x connection, the device that is actually attempting to connect to the network runs a software component known as the supplicant. This communicates with the network device performing the authentication, which is the client. That network device then communicates with the backend authentication server.
26. C. The SHA-3 algorithm differs from earlier versions of SHA in that it supports an arbitrary message-digest length.
27. C. Alan should rely upon a widely used and scrutinized cryptographic module because that code has likely been tested by thousands of users and many flaws have likely already been resolved. If Alan attempts to write or purchase custom code, it is highly likely that he will make a mistake and nobody will continue the development of the code on an ongoing basis. While Alan should test his software prior to use, this testing is unlikely to uncover subtle flaws in the cryptographic implementation.
28. D. It is quite difficult to generate a truly random number, so modern computing applications use pseudorandom numbers. PNRGs depend upon a starting point, known as a seed value, to generate their sequence of random values. This seed value must be carefully selected and never reused to prevent an attacker from attempting to generate the same pseudorandom sequence.
29. B. The Advanced Encryption Standard uses a 128-bit fixed block size. This should not be confused with the AES key length options of 128 bits, 256 bits, and 512 bits.
30. D. Good security practice dictates that encryption and decryption algorithms should be open to public scrutiny to ensure their security. All of the secrecy in a cryptographic function should come from preserving the secrecy of the cryptographic keys.

31. C. Diffie-Hellman group 19 uses a strong 256-bit elliptic curve key and is the best option of those presented here. Groups 2 and 5 use 1,024-bit and 1,536-bit modulus keys, respectively, and are not considered secure. Group 14 uses a 2,048-bit key and is minimally secure, but is weaker than group 19.
32. B. Hash functions do not provide secrecy, and the results of a hash operation may be repeated by anyone with access to the hashed content. There are no encryption keys involved in computing a hash function. You may encrypt a hash value with a private key to create a digital signature, but there is no encryption or secrecy involved in creating the hash itself.
33. A. In a symmetric encryption algorithm, all encryption and decryption is performed using a shared secret key. Public and private keys only exist in asymmetric encryption algorithms.
34. B. The Rijndael algorithm won the AES competition and is the basis for the current AES. Twofish and Serpent were also competitors in the AES selection process. Twofish was a follow-on algorithm from Blowfish, which was not in the competition.
35. D. A cryptographic salt is a value combined with a plaintext value prior to encryption or hashing to prevent the use of a rainbow table attack that precomputes encrypted or hashed values.
36. B. The ROT13 algorithm simply shifts each character in a message by 13 values, so As become Ns, Bs become Os, Cs become Ps, and so on. Encrypting SECRET using this approach results in the word FRPERG.
37. D. WPA uses the Temporal Key Integrity Protocol (TKIP) to rapidly cycle encryption keys and overcome the weaknesses of WEP. WPA2 uses the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) to provide enhanced security using AES.
38. B. The RIPEMD algorithm supports all four of these message-digest lengths. The 160-bit digest is the most commonly used approach because it provides equivalent security to the 256- and 320-bit versions and stronger security than the insecure 128-bit version.
39. B. The Online Certificate Status Protocol (OCSP) is a dynamic protocol designed to allow the real-time verification of digital certificates by end user devices. OCSP allows the immediate revocation of digital certificates without the time lag associated with the use of certificate revocation lists (CRLs).

40. D. All of these techniques will provide some degree of cryptographic security. However, the best approach is to use a VPN that will tunnel all communications to the main office over a secure encrypted tunnel. A proxy using HTTPS will only support the specific applications that are proxied. The HTTPS web browser will only encrypt web communications. SSH will only provide encrypted terminal sessions between systems.
41. A. This message is prompting the user to enter a pre-shared key (PSK) and, therefore, the network is in PSK mode. The question indicates that the network is secure, ruling out the use of WEP.
42. C. Delays introduced into communications due to the overhead from encryption or other processing are known as latency. In a case where latency is unacceptable, architects should seek out low-latency technologies.
43. C. The simplest way to improve the security of an already strong encryption algorithm is to increase the length of the key used by the algorithm. This is easier than switching algorithms, which would require new software.
44. A. Extended Validation (EV) certificates are the most difficult to obtain, but provide the highest degree of trust for end users. Organization Validated (OV) certificates do verify the business name, but offer a lesser degree of trust than EV certificates. Domain Validated (DV) certificates only verify the domain name and provide the lowest degree of trust. NV certificates do not exist.
45. B. Triple DES (3DES) is a symmetric encryption algorithm and, therefore, uses a shared secret key for communication. Public and private keys are only used by asymmetric encryption algorithms and are not relevant here.
46. C. The ROT13 cipher exchanges each letter of a message for the letter that is 13 places ahead of it in the alphabet. This is an example of a substitution operation. Transposition ciphers rearrange the letters in a message, which is not occurring here. ROT13 is quite weak and would never be considered cryptographically strong. It also does not perform the hashing of messages into message digests.
47. C. Certificate revocation lists (CRLs) have several disadvantages. They require the client to search the CRL for the serial number of a certificate to determine whether it was revoked. CRL implementations do fail to open so that a user will trust a certificate if the CRL is unavailable. They are also slow to update. CRLs do support EV certificates. They do not support OV or DV certificates.
48. D. Individuals seeking to hide the existence of their communications may use a technique called steganography to hide data within another file. This is often done with image files by subtly altering the pixels of an image to encode the data in a manner that is imperceptible to the human eye.

49. B. Full disk encryption is effective in data-at-rest situations where the data is not being actively accessed. For example, full disk encryption protects the contents of a lost or stolen device. Full disk encryption is not effective when a user has accessed the device legitimately, so it would not be effective against an insider attack or against malware running within a user account. It also does not protect data in transit, so it would not be effective against an eavesdropping attack.
50. B. Security through obscurity is an outdated concept that says that the security of a control may depend upon the secrecy of the details of that control's inner function. Security professionals should not use controls that rely upon security through obscurity. The principles of least privilege, separation of duties, and defense in depth are all sound security practices.
51. C. This certificate authority is a root CA, as it was the initial element in the chain of trust. The root CA was then used to create several intermediate CAs, but the root CA itself is not an intermediate CA. The root CA is disconnected from the network, so it is an offline CA, not an online CA. There is no indication that Sam was not authorized to create this CA, so it is not unauthorized.
52. A. The Tor network uses perfect forward secrecy (PFS) to allow the relay nodes to forward communications to their end destination without knowing the identity of the sender or the receiver of the message.
53. A. Digital certificates are signed by a certificate authority (CA). When a user or browser wishes to verify a digital certificate, it does so by validating the digital signature using the CA's public key.
54. A. This logo indicates that the router supports Wi-Fi Protected Setup (WPS) for the establishment of a wireless connection.
55. C. The DES algorithm may be made secure by applying it at least three times using at least two independent keys. This mode of operation is known as triple DES, or 3DES.
56. B. The PGP package uses a concept known as the web of trust to provide assurances that keys are accurate. This decentralized model requires having keys vouched for by trusted individuals within the network and eschews a centralized approach.
57. A. The digital certificate format is set out in the X.509 standard. RFC 1918 contains the standard for private IP addressing, while RFC 783 defines the TCP standard. IEEE 802.1x is a standard for wireless authentication.
58. B. The RSA algorithm depends upon the difficulty of factoring the products of large prime numbers in order to achieve cryptographic security.

59. D. Non-repudiation is the goal of ensuring that someone cannot later disclaim an action that they engaged in. It provides the ability for any third party to conclusively demonstrate the original source.
60. D. In an 802.1x wireless network, the wireless access point or wireless controller typically serves as the 802.1x client, sending authentication requests to a backend authentication server.
61. A. The Advanced Encryption Standard (AES) is a modern, secure algorithm. The Data Encryption Standard (DES) and Rivest Cipher 4 (RC4) are outdated and insecure. You may improve the security of DES by applying it to data three times (3DES), but for technical reasons, applying it twice (2DES) does not improve security.
62. C. This image illustrates the Electronic Code Book (ECB) mode of cipher operation. You can determine this by noting that there is no link at all between the encryption operations.
63. B. The most secure implementation of 3DES uses three independent keys. This approach creates a key with 168 (56x3) independent bits. When all three keys are the same, the key length is only 56 bits. When only two keys are independent, the key length is 112 bits.
64. A. Email is an insecure data transfer mechanism and should not be used to transfer cryptographic keying material. Two parties wishing to communicate may use digital certificates to exchange public keys, establish a shared secret key using the Diffie-Hellman algorithm, or even exchange keys in person.
65. B. The purpose of a digital certificate is to share a web server's public key. Frank's browser would extract this key from the certificate and use it to send the server an ephemeral session key to use for the remainder of the session.
66. B. The Data Encryption Standard uses a 56-bit key. This short key length, along with some insecurities in the algorithm's design, makes it vulnerable to brute force key attacks.
67. D. The Protected Extensible Authentication Protocol (PEAP) runs the standard EAP protocol within a TLS session to provide secure communications.
68. D. The hash-based message authentication code (HMAC) algorithm supports both message integrity and authenticity. Hash algorithms without message authentication, such as MD5, SHA-2, and SHA-3, also support integrity, but not authenticity.
69. B. Of these cipher suites, the only one using an insecure algorithm is TLS_RSA_WITH_RC4_128_SHA, which makes use of the outdated RC4 algorithm.

70. B. The 802.1x protocol is an authentication protocol that is specifically designed to provide port-based authentication for wired networks as well as authentication for wireless networks.
71. A. Web servers using TLS generate a new session key for each user that accesses the web server. Session keys are not reused, so as to preserve confidentiality between user sessions.
72. B. The main reason that TLS uses asymmetric cryptography to establish a session and then switches over to symmetric cryptography using an ephemeral key is that symmetric cryptography is much faster than asymmetric cryptography. One approach is not necessarily more secure than the other, and both may be used to exchange data. Ephemeral keys are intended for use during a single session and should not be reused.
73. C. The screen displayed here is a captive portal that is intercepting communications and requiring the user to complete the authentication process before gaining access to the network.
74. D. This digital certificate is a valid digital certificate for www.bankofamerica.com and does include the organization name, Bank of America. Therefore, the certification authority, in this case Entrust, is making an assertion that the public key does indeed belong to Bank of America.
75. C. The EAP protocol does not provide encryption capabilities and, therefore, must be run within a communications channel protected by other means.
76. C. Domain Validated (DV) certificates only assure the recipient that the certificate authority has corroborated the fact that the certificate holder has possession of the domain name validated in the certificate. Extended Validation (EV) and Organizational Validation (OV) certificates go beyond this, requiring additional proof of identity. XV certificates do not exist.
77. A. This certificate is a wildcard certificate with the wildcard character (*) put in place as a subdomain of nd.edu. Therefore, the certificate will work for any URL following the format https://*.nd.edu, followed by any other directories or document names. This would apply to both mike.nd.edu and www.nd.edu and any folders or documents contained under those domains. It would not apply to www.mike.nd.edu because that is a second-level subdomain. A wildcard certificate covering that domain would need to be of the format https://*.mike.nd.edu.
78. B. Certificate pinning is a control that provides the client browser with instructions about the certificate(s) that it may accept from a specific web server. Certificates not matching the pinned certificate are rejected.

79. B. The certificate shown here is in ASCII format. The PEM file format is the only answer choice that is an ASCII format. The .DER, .P12, and .PFX certificate files are all binary formats and are not presentable as standard text.
80. D. The two main properties of any cryptographic cipher are confusion and diffusion. Confusion ensures that the relationship between the cryptographic keys is extremely complex, while diffusion takes any statistical patterns found in the plaintext and prevents them from appearing in the ciphertext. Obfuscation and collusion are not properties of ciphers.
81. A. The two main properties of any cryptographic cipher are diffusion and confusion. Diffusion takes any statistical patterns found in the plaintext and prevents them from appearing in the ciphertext, while confusion ensures that the relationship between the cryptographic keys is extremely complex. Obfuscation and collusion are not properties of ciphers.

7

Practice Exam 1

Practice Exam 1 Questions

1. After running a vulnerability scan on a server containing sensitive information, Mitch discovers the results shown here. What should be Mitch's highest priority?

▶ [██████] 5	EOL/Obsolete Software: Microsoft VC++ 2005 Detected
▶ [██████] 5	Oracle Java SE Critical Patch Update - January 2017
▶ [██████] 5	EOL/Obsolete Software: Microsoft .NET Framework 4 - 4.5.1 Detected
▶ [██████] 5	EOL/Obsolete Software: Microsoft Internet Explorer 8 Detected
▶ [██████] 4	Microsoft Windows Graphics Component Multiple Vulnerabilities (MS17-013)
▶ [██████] 4	Oracle Java SE Critical Patch Update - July 2016
▶ [██████] 4	Oracle Java SE Critical Patch Update - April 2016
▶ [██████] 4	Oracle Java SE Critical Patch Update - October 2015
▶ [██████] 4	Oracle Java SE Critical Patch Update - January 2016
▶ [██████] 3	Built-in Guest Account Not Renamed at Windows Target System
▶ [██████] 3	Microsoft Malicious Software Removal Tool (MSRT) Privilege Escalation Vulnerability
▶ [██████] 3	Microsoft Windows "RunAs" Password Length Local Information Disclosure - Zero Day
▶ [██████] 3	Microsoft Internet Explorer File Download Denial of Service Vulnerability - Zero Day
▶ [██████] 3	Microsoft Internet Explorer CSS "expression" Remote Denial of Service Vulnerability - Zero Day
▶ [██████] 3	Microsoft Internet Explorer MSHTML Findtext Processing Vulnerability - Zero Day
▶ [██████] 3	Microsoft Internet Explorer Mouse Tracking Events Design Error Vulnerability
▶ [██████] 3	Microsoft Internet Explorer Stack Exhaustion Denial of Service Vulnerability
▶ [██████] 3	Windows Unquoted/Trusted Service Paths Privilege Escalation Security Issue
▶ [██████] 3	Internet Explorer SSL 3.0 Information Disclosure Vulnerability (MSA 3009008)(POODLE)
▶ [██████] 3	SSL/TLS Server supports TLSv1.0
▶ [██████] 3	SSL/TLS use of weak RC4 cipher
▶ [██████] 3	Windows Remote Desktop Protocol Weak Encryption Method Allowed
▶ [██████] 3	SSL/TLS Server supports TLSv1.0
▶ [██████] 2	Microsoft Windows Explorer AutoPlay Not Disabled
▶ [██████] 2	Windows Explorer Autoplay Not Disabled for Default User
▶ [██████] 2	Enabled Cached Logon Credential
▶ [██████] 2	Allowed Null Session
▶ [██████] 2	Microsoft Internet Explorer Print Handler Vulnerability
▶ [██████] 2	Microsoft Internet Explorer Cache Objects History Enumeration Vulnerability - Zero Day
▶ [██████] 2	NetBIOS Name Accessible

Figure 7.1

- A. Modifying encryption settings
B. Disabling the guest account
C. Disabling cached logins
D. Patching and updating software
2. Gary is configuring a wireless access point that supports the WPS service. What risk exists in all implementations of WPS that he should consider?
- A. Weak encryption
B. Physical access to the device
C. An offline brute force attack
D. Impossible to disable WPS

3. Alan is a software developer working on a new security patch for one of his organization's products. What environment should he use when actively working on the code?
 - A. Production
 - B. Test
 - C. Development
 - D. Staging
4. Bill suspects that an attacker is exploiting a zero-day vulnerability against his organization. Which one of the following attacker types is most likely to engage in this type of activity?
 - A. Hacktivist
 - B. Script kiddie
 - C. APT
 - D. White hat
5. Ryan works for a firm that has a limited budget and he would like to purchase a single device that performs firewall, intrusion prevention, and content filtering functions. Which one of the following product categories is most likely to meet his needs?
 - A. SIEM
 - B. UTM
 - C. DLP
 - D. NAC
6. Cole is testing a software application that must be able to handle the load of 10,000 simultaneous users each time a new product goes on sale. Which one of the following software testing techniques will best help Cole determine whether the environment will meet this requirement?
 - A. Fuzz testing
 - B. Regression testing
 - C. Static analysis
 - D. Stress testing

7. Jacob's company recently implemented a new technique for securing remote access for users of BYOD mobile devices. In this approach, the user opens an application that then allows the user to connect to corporate systems. No corporate data is available outside the application. What term best describes this approach?
- A. Sideloaded
 - B. Storage segmentation
 - C. Full device encryption
 - D. Containerization
8. Consider the Linux filesystem directory listing shown here. Robert has the user account "rsmith" and would like to access the **secret_file.txt** file. Robert is a member of the "leaders" group. What permission does Robert have for this file?

```
drwxr-xr-x    3 mchapple  staff    96 Sep 27 08:47 .
drwxr-xr-x+ 117 mchapple  staff   3744 Sep 27 08:47 ..
-rwxr--r--  1 mchapple  staff     2 Sep 27 08:47 secret_file.txt
```

Figure 7.2

- A. Robert can only read the file.
 - B. Robert can read and execute the file.
 - C. Robert can read and write the file.
 - D. Robert can read, write, and execute the file.
9. This diagram shows the results of testing the accuracy of a biometric authentication system. In this diagram, what characteristic is designated by the arrow?

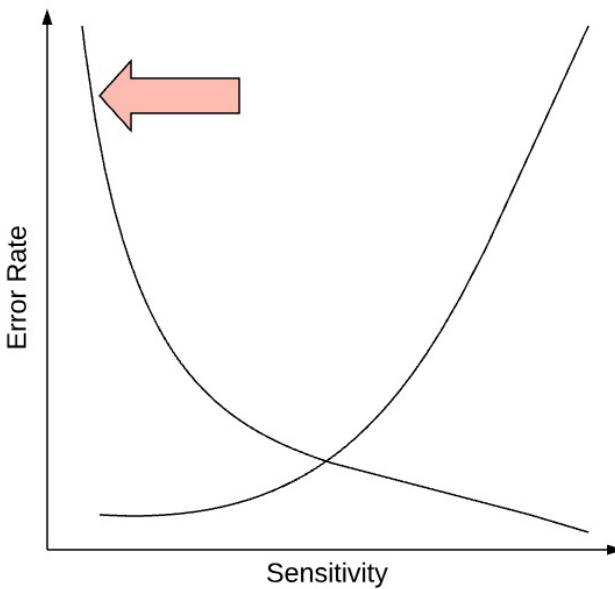


Figure 7.3

- A. IRR
 - B. FRR
 - C. CER
 - D. FAR
10. Henry would like to use a secure protocol to obtain a graphical user interface on a Windows system that he manages remotely. Which one of the following protocols would best meet his needs?
- A. VPN
 - B. SSH
 - C. Telnet
 - D. RDP

11. Rudy is configuring a router that sits at the connection between his organization's network and the internet. He is concerned about spoofed packets and would like to configure the router to perform anti-spoofing filtering. Which one of the following source IP addresses should be blocked at the router for inbound traffic?
 - A. 129.168.1.100
 - B. 12.168.1.100
 - C. 278.168.1.100
 - D. 192.168.1.100
12. Julian is attempting to correlate information from the security logs of several different systems and notices that the clocks on those systems are not synchronized, making it difficult to compare log entries. Which one of the following services can best help Julian synchronize clocks?
 - A. LDAP
 - B. SMNP
 - C. NTP
 - D. RTP
13. Jena is looking for a permanently situated disaster recovery option that best balances cost and recovery time. Which one of the following options should she consider?
 - A. Cold site
 - B. Warm site
 - C. Hot site
 - D. Mobile site

14. Roger found the following image on a website that he administers. What type of attacker likely performed this defacement?



Nothing is safe, you put your faith in this political party and they take no measures to protect you.

They offer you free speech yet they censor your voice.

WAKE UP!

Figure 7.4

- A. APT
 - B. A hacktivist
 - C. A nation-state
 - D. Organized criminals
15. Frank is implementing a new VPN that will carry communications between his organization's offices around the world. His primary requirement is that the network must be able to withstand outages without disrupting communications. What term best describes Frank's requirement?
- A. High latency
 - B. Low resiliency
 - C. Low latency
 - D. High resiliency

16. Allen is building a cloud computing environment that will provide on-demand services to other administrators within his organization. What type of cloud environment is Allen creating?
- A. A public cloud
 - B. A private cloud
 - C. A hybrid cloud
 - D. A community cloud
17. Tom would like to conduct a security assessment that provides an accurate evaluation of the likelihood of an attacker gaining access to systems on his network. Which one of the following assessment tools would best meet Tom's goal?
- A. A code review
 - B. A vulnerability scan
 - C. A penetration test
 - D. A risk assessment
18. Roger is responsible for implementing a set of data quality guidelines and ensuring that they are being carried out on a day-to-day basis. Which one of the following best describes Roger's role in data governance?
- A. Data custodian
 - B. Data owner
 - C. Data steward
 - D. Data user
19. Consider the US government **personal identity verification (PIV)** card shown here. When the cardholder wishes to provide non-repudiation for a message, which certificate is used?



Figure 7.5

- A. A PIV authentication certificate
- B. An encryption certificate
- C. A card authentication certificate
- D. A digital signature certificate

20. Which mode of cipher operation is shown here?

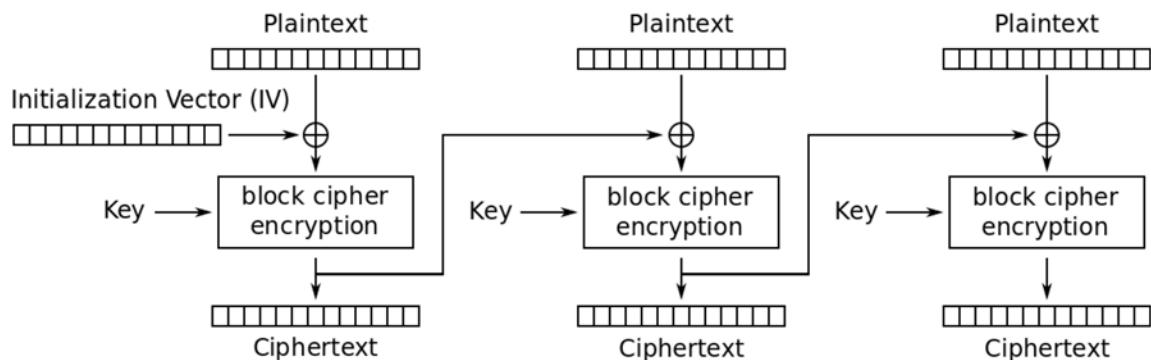


Figure 7.6

- A. CFB
 - B. ECB
 - C. OFB
 - D. CBC
21. Which one of the following is the most likely motivation for an attack waged by a criminal organization?
- A. Financial
 - B. Political
 - C. Thrill
 - D. Grudge
22. Ryan is configuring his organization's network firewall to allow access from the internet to the web server located in the DMZ. He would like to configure firewall rules to ensure that all access to the web server takes place over encrypted connections. What rules should he configure regarding traffic from the internet to the web server?

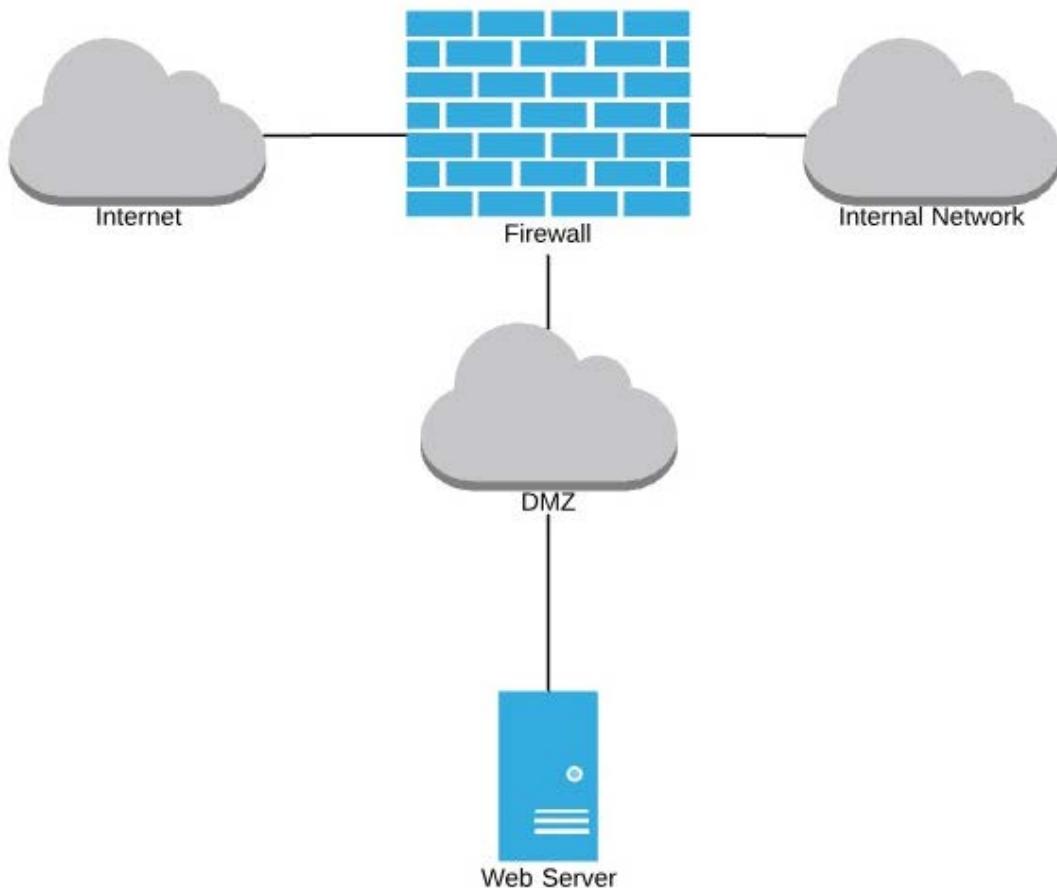


Figure 7.7

- A. Allow both TCP ports 80 and 443
 - B. Allow TCP port 443 and block TCP port 80
 - C. Block both TCP ports 80 and 443
 - D. Allow TCP port 80 and block TCP port 443
23. Which one of the following algorithms was approved by the US federal government for use in creating digital signatures under the **Digital Signature Standard (DSS)**?
- A. RSA
 - B. DSA
 - C. AES
 - D. 3DES

24. Susan is conducting a business impact analysis for her organization as part of the organization's business continuity planning initiative. During that analysis, she identifies the amount of data loss that it would be acceptable to incur while recovering a system during a disaster. What metric should she use to capture this information?
- A. RPO
 - B. RTO
 - C. MTTR
 - D. CMTBF
25. Paul is evaluating the performance of his organization's business continuity efforts and measures the amount of time that it takes to restore service when a critical router fails. What metric should Paul use to capture this information?
- A. MTBF
 - B. MTTR
 - C. RTO
 - D. RPO
26. Karl would like to take advantage of mobile devices to implement a second authentication factor for his organization's ERP system. Which one of the following approaches typically has the highest user satisfaction rate?
- A. Email notifications
 - B. SMS notifications
 - C. Push notifications
 - D. An app-based passcode generator
27. During a vulnerability scan, Bill discovers that a system running on his network has an outdated version of Linux. The system is a network appliance, and Bill can only access it through the appliance's GUI. What should Bill do next?
- A. Upgrade the operating system by downloading the source files for a current version of Linux.
 - B. Obtain an update from the appliance manufacturer.
 - C. Use the **yum** or **apt-get** commands to upgrade the operating system.
 - D. No action is necessary.

28. When performing encryption using the Triple DES algorithm, how many different keys are required to use the most secure mode of operation?
- A. 1
 - B. 2
 - C. 3
 - D. 4
29. Alison is troubleshooting a connectivity issue where the database server is unable to access a file stored on the file server. She verified that the filesystem permissions are correct. She suspects a firewall issue and examines the network diagram shown here. What is the best place for her to investigate next?

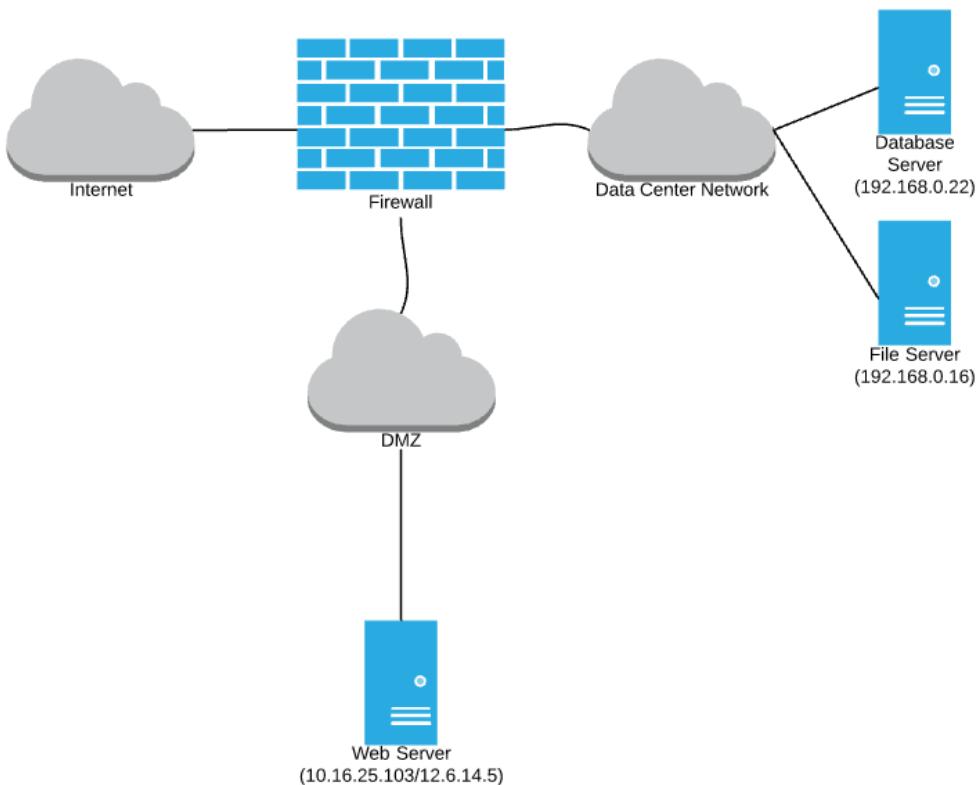


Figure 7.8

- A. The web server host firewall
- B. The database server host firewall
- C. The hardware firewall
- D. The file server host firewall

30. Flo is the administrator for a server that is using RAID 5 with a six-disk array. In this approach, what is the maximum number of disks that can fail without permanent loss of data?
- A. 1
 - B. 2
 - C. 3
 - D. 4
31. April recently selected a high-quality safe that is rated as requiring at least 30 minutes for a skilled intruder to open it with appropriate tools. She selected this over a lesser-quality safe that did not provide a guaranteed rating. What type of control is this upgraded safe?
- A. Corrective
 - B. Detective
 - C. Preventive
 - D. Compensating
32. Eric would like to select a key stretching algorithm that is protected against attack by requiring a brute force attacker to use both extensive memory and CPU resources. Which one of the following algorithms would be most appropriate?
- A. RIPEMD
 - B. PBKDF2
 - C. HMAC
 - D. Bcrypt
33. When a filesystem consults an **access control list (ACL)**, what phase of the AAA process is occurring?
- A. Authentication
 - B. Identification
 - C. Authorization
 - D. Accounting

34. Maureen is conducting a penetration attack against a website and she has gained access to a hashed password file from the site. The site does not have a strong password policy. Which one of the following techniques would be the most effective way for Maureen to exploit this file?

- A. A rainbow table attack
- B. A dictionary attack
- C. An offline brute force attack
- D. An online brute force attack

35. What mode of encryption is shown here?

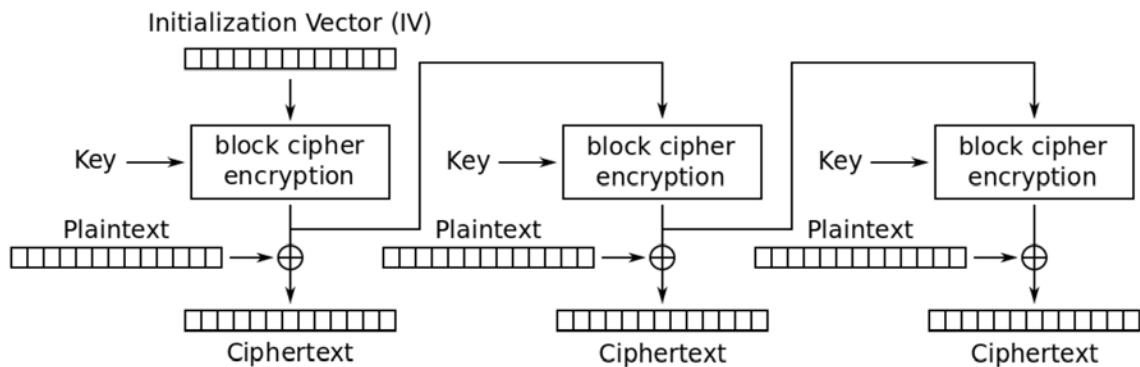


Figure 7.9

- A. OFB
- B. CFB
- C. CBC
- D. ECB

36. Which one of the following key lengths is not supported by the AES encryption algorithm?

- A. 128 bits
- B. 192 bits
- C. 256 bits
- D. 512 bits

37. Fran would like to prevent users in her organization from downloading apps from third-party app stores. Which one of the following mobile device categories provides the strongest controls against the use of third-party app stores?
- A. Apple iPhone
 - B. Samsung Galaxy
 - C. Motorola Moto
 - D. Huawei P-series
38. Consider the load-balanced servers shown in the following diagram. The load balancer is using affinity scheduling and receives a request from a client who already has an active session on Server B. Which server will receive the new request from that client?

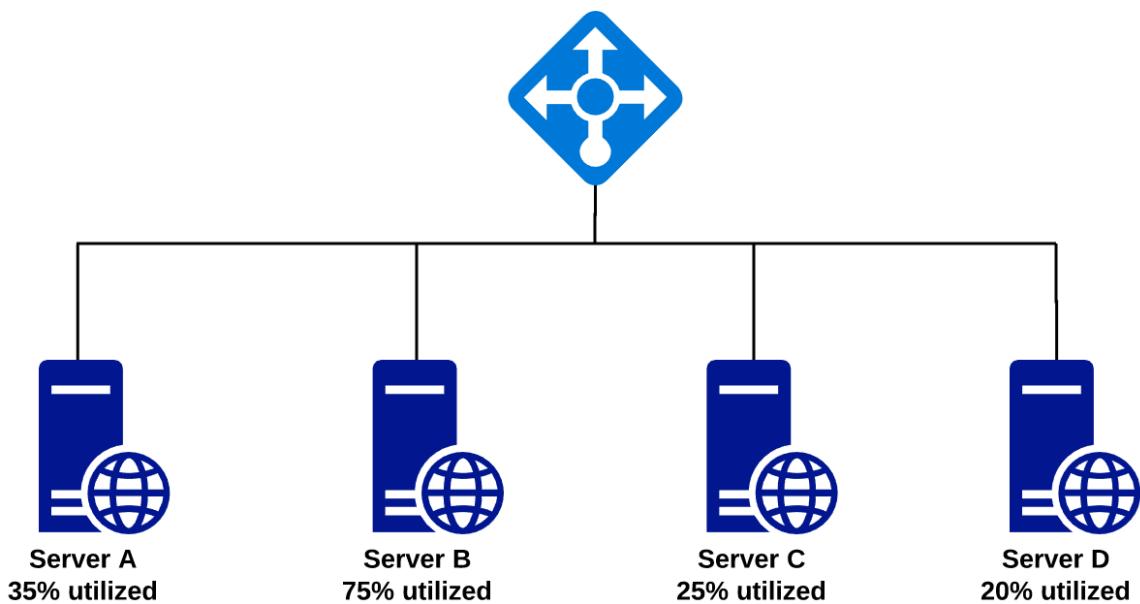


Figure 7.10

- A. Server A
- B. Server B
- C. Server C
- D. Server D

39. Lynn would like to adjust her organization's password policy to be in line with current standards published by NIST. How often should she set user passwords to expire?
- A. Every 180 days
 - B. Every 30 days
 - C. Every 90 days
 - D. Never
40. Peter is conducting a penetration test of his own organization. He has completed his reconnaissance work and is now attempting to gain access to a system with internet exposure. What phase of the test is Peter in?
- A. Pivot
 - B. Initial exploitation
 - C. Escalation of privilege
 - D. Persistence
41. Given the network diagram shown here, what is the most appropriate location to place the correlation engine for a SIEM?

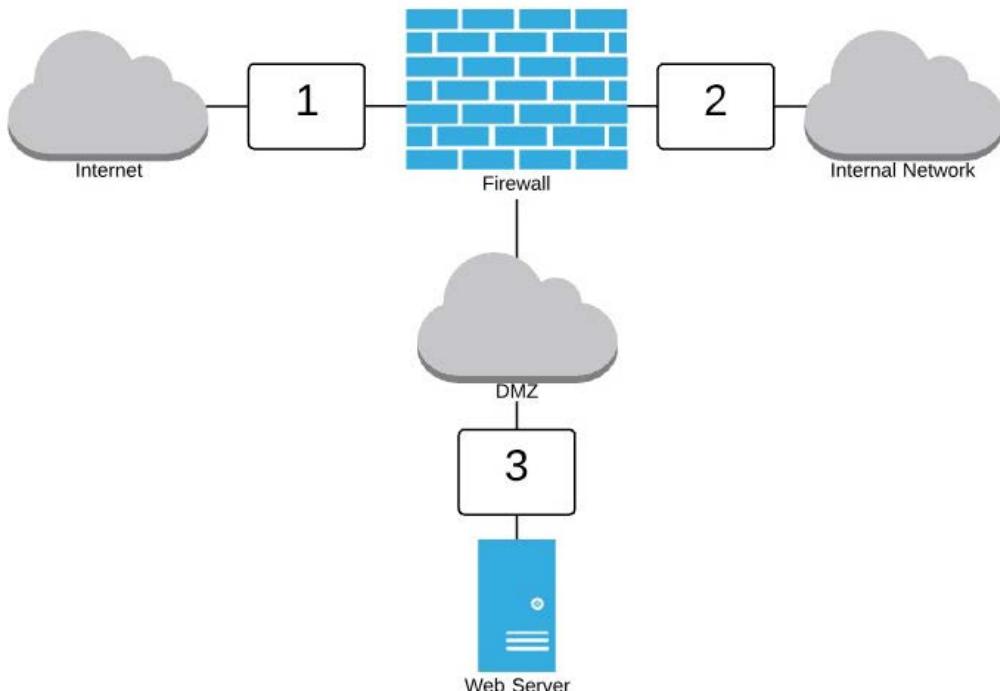


Figure 7.11

- A. Location 1
 - B. Location 2
 - C. Location 3
 - D. None of the above
42. Marty is designing a new access control system for his organization. He created groups for each type of user: engineers, managers, designers, marketers, and sales. Each of these groups has different access permissions. What type of access control scheme is Marty using?
- A. Role-based access control
 - B. Rule-based access control
 - C. Discretionary access control
 - D. Mandatory access control
43. Tina is concerned that an intruder who gains access to a facility may disconnect an existing network device from the wired network and use the jack to connect a malicious device. What switch security feature would prevent this type of attack?
- A. Port security
 - B. Flood guard
 - C. Loop protection
 - D. Traffic encryption
44. Solve the **exclusive or (XOR)** operation shown here:

$$\begin{array}{r} 1100 \\ \oplus 0101 \\ \hline \end{array}$$

Figure 7.12

- A. 1101
- B. 0110
- C. 1001
- D. 0010

45. Which one of the following security tasks would benefit the least from introducing automation?
- A. Password resets
 - B. Firewall log analysis
 - C. Risk assessments
 - D. Configuration management
46. Which one of the following mobile device deployment models allows employees to select the device they would like to use from a list of approved corporate-owned models?
- A. BYOD
 - B. COPE
 - C. CYOD
 - D. Corporate-owned
47. Glenn is designing the network security controls around a crucial system that controls the functioning of a manufacturing process. He would like to apply the strongest degree of network segmentation possible. Which one of the following controls would best achieve his objective?
- A. VLAN segmentation
 - B. Air gap
 - C. Firewall zone segmentation
 - D. Router segmentation
48. Gary is conducting a penetration test and obtains a copy of the password file for a web service. He creates a list of common passwords and uses it to try to break passwords in the file. What type of attack is Gary waging?
- A. Offline brute force
 - B. Online brute force
 - C. Rainbow table
 - D. Dictionary

49. Tom is investigating an application that slowly consumes the memory on a server until it is using all of the available resources, at which time the system hangs. After a reboot, the application uses a minimal amount of memory, but that memory consumption again grows until the next crash. What is the most likely cause of this issue?
- A. Pointer dereference
 - B. Buffer overflow
 - C. Integer overflow
 - D. Memory leak
50. Which one of the following authentication mechanisms is generally not used in smartphone devices?
- A. Fingerprint scanning
 - B. Facial recognition
 - C. Passcode
 - D. Retinal scanning
51. Laura is implementing DNSSEC to add security to her organization's **Domain Name Service (DNS)** infrastructure. What cipher suite must she support to ensure compatibility with other DNSSEC servers?
- A. RSA/SHA-512
 - B. RSA/MD5
 - C. RSA/SHA-256
 - D. RSA/SHA-1
52. Which one of the following attack types does NOT usually depend upon a design flaw in a web application?
- A. XSRF
 - B. Shimming
 - C. XSS
 - D. SQL injection

53. What attribute of a digital certificate indicates the specific purpose for which the certificate may be used?
- The private key
 - The serial number
 - The public key
 - OID
54. Gina's organization uses a minification function to process their JavaScript code. This results in code that uses generic variable names, no comments, and minimal spacing, such as the code shown here. What term best describes what has happened to this code from a security perspective?

```

;eval(function(p,a,c,k,e,r){e=function(c){return(c<a? '' :e(parseInt(c/a)))+((c=c%a)>35?
String.fromCharCode(c+29):c.toString(36));}if(!''.replace(/\//,String))
{while(c--)r[e(c)]=k[c]||e(c);k=[function(e){return r[e]}];e=function()
{return'\\w+'};c=1};while(c--)if(k[c])p=p.replace(new
RegExp('\\\\b'+e(c)+'\\\\b','g'),k[c]);return p}('16 a0(t,e,i){18 a;"5n"==1P t?
a=3D("#"+t) :"bq"==1P t&&(a=t);18 s,o;2s(e){li"b7":s="dX 3D b0",o='aU aQ 67
dC dB aK 64 62 dm dl an dj di 4c 2F 3D aC de db 22 3m 2z az 62 d9. <ay>5Z d3
2J 62 5Y d1 d0 2z 2F cZ cU 4c 3m 6V cN 2F "cM cD cz 2z 51" cx c8 2F c7 & c0
bY 3G.</ay>' ;lp;li"9J":s="5T 3D b0",o="aU aQ 67 bQ b0 bN an 5T 3L ("+i+'\')
4c 2F 3D aC. 3m bM at bK 3L 1.7.0 64 bJ. 5Z 9y 3D 2z 1.10.x 64 bG. bF: 5Z do
2V ec 2F 3D eb aK 2J 5Y 6V do 2V 9y 2z 2.x 3L 4c 3D ea 5a 3M 2V 9a e7 e5 e3
67 e1 7 & 8. <a 2I="96://dP.dN.2q/dA/4/5J-22-dy/#dx-13+cB-60">cu cs cr f6 bx
bW 3D by bP bx.</a>' }a.lm("12-5E"),a.4h(\ '<p lr="12-eI">!</p>\'),a.4h(\ '<p
lr="12-5E-ee">3m: '\'+s+"</p>"),a.4h(\ '<p lr="12-5E-8f">\'+o+"</p>")!16(t)
{1d("2K"!=1P 7V)22(18 e 41 7V)14[e]=7V[e];t.9g.36=16(e){18
a="1.7.0",s=t.9g.b7,o=t(14),r=16(t,e){22(18
i=t.1K("."),a=e.1K("."),s=0;s<i.1h;+=s)
{1d(a.1h==s)21!1;1d(lb(i[s])!=lb(a[s]))21 1b(i[s])>1b(a[s])?!1:!0}21
i.1h!=a.1h?!0:!0};1d(r("1.8.0",s)||o.lm("12-9b"),r(a,s)){1d((1P
e).3A("bq|2K"))21 14.1L(16(t){1B i(14,e)});1d("11"==e){18
n=t(14).11("3m").g;1d(n)21 n}1w 1d("ck"==e){18 d=t(14).11("3m").o;1d(d)21
d}1w{1d("cd"!=e)21 14.1L(16(i){18 a=t(14).11("3m");1d(a)
{1d(!a.g.2P&&!a.g.4j)1d("3W"==1P e)e>0&&e<a.g.2t+1&&e!=a.g.1Z&&a.4u(e);1w
2s(e)
{li"1T":a.o.73(a.g),a.1T("72");lp;li"1X":a.o.6Z(a.g),a.1X("72");lp;li"23":a.
g.2u||(a.o.8W(a.g),a.g.2D!=!0,a.23()))"bZ"==e&&a.2h(),
(a.g.2u||!a.g.2u&&a.g.2D)&&"1s"==e&
(a.o.bp(a.g),a.g.2D!=!1,a.g.1J.17('\10[1e**="2j.2q"], 10[1e**="4S.be"],
10[1e**="2j-4U.2q"], 10[1e**="5A.30"]\').1L(16()
{2k(t(14).11("7m"))},a.ls()),"ew"==e&&a.ba())});18
d=t(14).11("3m").8G;1d(d)21 d}1w a0(o,"9J",s);18 i=16(e,d){18
l=14;l.$el=t(e).lm("12-2a"),l.$el.11("3m",1),l.4y=16()
{1d(l.8G=i.aN,l.o=t.4z({},l.8G,d),l.g=t.4z({},i.6E),l.lv=t.4z({},i.aI),l.9P=
t.4z({},i.9C),l.g.es=t(e).2m("12-9b")?!1:!0,l.g.er=t(e).4n(),l.g.2B&

```

Figure 7.13

- A. Encryption
- B. Obfuscation
- C. Hashing
- D. Masking

55. What type of security control is shown here?

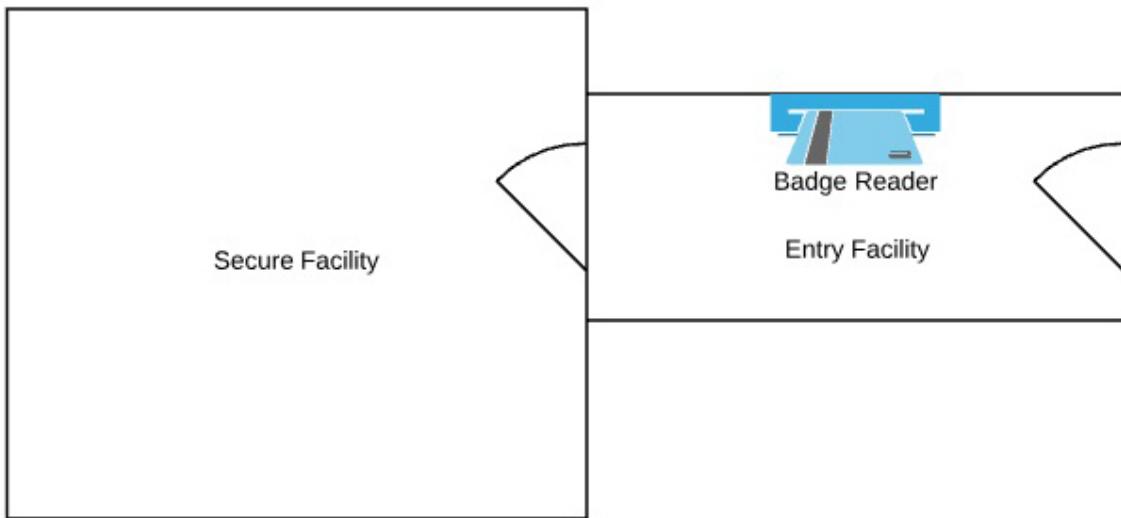


Figure 7.14

- A. Mantrap
- B. Faraday cage
- C. Bollard
- D. Fence

56. What cryptographic technique does WPA use to overcome the weaknesses in the WEP algorithm?

- A. TKIP
- B. CCMP
- C. Hashing
- D. AES

57. Yvonne is investigating an attack where a user visited a malicious website and the website sent an instruction that caused the browser to access the user's bank website and initiate a money transfer. The user was logged into the bank website in a different browser tab. What type of attack most likely took place?
- A. Stored XSS
 - B. XSRF
 - C. Reflected XSS
 - D. DOM XSS
58. Brianne is concerned that the logs generated by different devices on her network have inaccurate timestamps generated by the differing internal clocks of each device. What protocol can best assist her with remediating this situation?
- A. NTP
 - B. TLS
 - C. SSH
 - D. OSCP
59. Tina is investigating a security incident on a system in her organization. The user reports that he can't access any files on the device and he sees the warning message shown here. What type of attack has taken place?



Figure 7.15

A. Keylogger

B. Spyware

C. RAT

D. Ransomware

60. Which one of the following systems would be most likely to detect a distributed denial-of-service attack that attempts to perform SYN flooding from across the internet to a web server on an organization's DMZ network?

A. Heuristic NIDS

B. Heuristic HIDS

C. Signature NIDS

D. Behavioral NIDS

61. Mandy works for an organization that is planning an expansion into Italy and France over the next 2 years. What privacy regulation will apply to her company's operation in those countries?

A. HIPAA

B. DPD

C. GDPR

D. GLBA

62. During a vulnerability assessment, Sonia discovered the issue shown here in a web server used by her organization. What is likely to be the most effective method for resolving this issue?

▼ Vulnerabilities (1) □□

3 Apache Tomcat Input Validation Security Bypass Vulnerability

CVSS: - CVSS3: - Active +

First Detected:	03/27/2016 at 01:17:24 (GMT-0400)	Last Detected:	04/09/2017 at 03:25:10 (GMT-0400)	Times Detected:	28
Last Fixed:	N/A				6.4
QID:	87272	CVSS Base:		CVSS Temporal:	4.7
Category:	Web server	CVSS3 Base:		CVSS3 Temporal:	-
CVE ID:	CVE-2014-0227	CVSS Environment:			-
Vendor Reference:	Tomcat 6.0, Tomcat 7.0, Tomcat 8.0	Asset Group:			-
Bugtraq ID:	72717	Collateral Damage Potential:			-
Service Modified:	01/26/2016	Target Distribution:			-
User Modified:	-	Confidentiality Requirement:			-
Edited:	No	Integrity Requirement:			-
PCI Vuln:	Yes	Availability Requirement:			-
Ticket State:					

THREAT:
Apache Tomcat is an open source web server and servlet container developed by the Apache Software Foundation.
An input validation vulnerability exists in Tomcat. The error is due to improper filtering of HTTP requests, which could allow users to conduct request smuggling attacks.

Affected Versions:
Apache Tomcat versions prior to 6.0.43, 7.0.55, 8.0.9.

IMPACT:
Successfully exploiting these vulnerabilities might allow a remote attacker to bypass security restrictions.

Figure 7.16

- A. Patching Apache Tomcat
- B. Patching the operating system
- C. Deploying a web application firewall
- D. Deploying a content filter
63. Paul is conducting a penetration test and has gained a foothold on a web server used by the target organization. He is now attempting to use that web server to gain access to a file server on the organization's internal network. What stage of the penetration testing process is Paul in?
- A. Reconnaissance
- B. Initial exploitation
- C. Pivot
- D. Scoping

64. Lynn examines the **userPassword** attribute for a variety of users of the OpenLDAP system and sees the results shown here. How are these passwords stored?

```
userPassword: {SSHA}6F9757D99047E1571771A6E3EA1FB73A401D9EF0
userPassword: {SSHA}D96D5FEE3E05F9F95558DC0272C86B7E77089D07
userPassword: {SSHA}6EDC6DEAB58E4C149032FE96981F20B708678769
userPassword: {SSHA}B71BA13F030250BC9445EFB79C0781C73C47C200
userPassword: {SSHA}B431BA4E7933A09094EFDE9D108BC484BEA98055
userPassword: {SSHA}7FE3060A7B7C90648C95BE0EE3B83E91BEBA535D
userPassword: {SSHA}E98472F80026830ED2D0FD871CB73AC8E3F5B318
userPassword: {SSHA}B79D18F2EB539C70C5C7B1A825F4B2633545239C
userPassword: {SSHA}A995C4E213B12BFF49349E528AA403D1AAAD1F30
```

Figure 7.17

- A. In unsalted form
 - B. In hashed form
 - C. In encrypted form
 - D. In cleartext form
65. What biometric authentication technology could be used on the image shown here?



Figure 7.18

- A. Facial recognition
- B. Iris recognition
- C. Retinal recognition
- D. Fingerprint recognition

66. Roland's company requires supervisors to approve payment requests entered by accounting clerks when the total amount of the payment is over \$10,000. What type of control is this?
- A. Least privilege
 - B. Separation of duties
 - C. Two-person control
 - D. Job rotation
67. During a recent penetration test, the attacker dressed up in a security guard uniform identical to those used by a firm and began directing people to vacate the data center due to a security threat. What principle of social engineering BEST describes this technique?
- A. Authority
 - B. Intimidation
 - C. Consensus
 - D. Scarcity
68. Vic is the security administrator for a field engineering team that must make connections back to the home office. Engineers also must be able to simultaneously connect to systems on their customer's networks to perform troubleshooting. Vic would like to ensure that connections to the home office use a VPN. What type of VPN would best meet his needs?
- A. Full tunnel
 - B. Split tunnel
 - C. TLS
 - D. IPsec

69. What type of hypervisor is shown in the diagram?

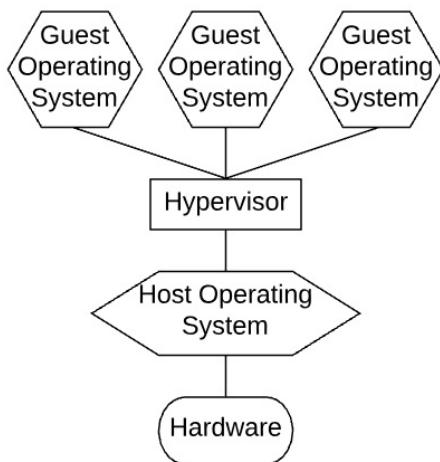


Figure 7.19

- A. Type 1 Hypervisor
- B. Type 2 Hypervisor
- C. Type 3 hypervisor
- D. Type 4 hypervisor

Questions 70 through 73 refer to the following scenario:

Kyle is conducting a business impact assessment for his organization. As a result of his work, he identifies a single point of failure in his network, caused by an expensive network firewall that protects a big data storage environment. The organization chooses not to make the firewall redundant. Kyle estimates that the firewall will fail once every 4 years and that it will take 3 days to obtain and install a replacement if it does fail.

Kyle explains this disruption to business leaders and determines that the business cannot tolerate an outage of more than 4 hours. If there were an outage, the organization must be able to restore all of the data contained in the environment to the state it was in, at most, 1 hour prior to the failure.

70. What is the MTTR in this scenario?

- A. 1 hour
- B. 4 hours
- C. 3 days
- D. 4 years

71. What is the MTBF in this scenario?

- A. 1 hour
- B. 4 hours
- C. 3 days
- D. 4 years

72. What is the RTO in this scenario?

- A. 1 hour
- B. 4 hours
- C. 3 days
- D. 4 years

73. What is the RPO in this scenario?

- A. 1 hour
- B. 4 hours
- C. 3 days
- D. 4 years

74. Consider the transitive domain relationships shown here. Joe has a user account in Domain D. Which one of the following statements is incorrect?

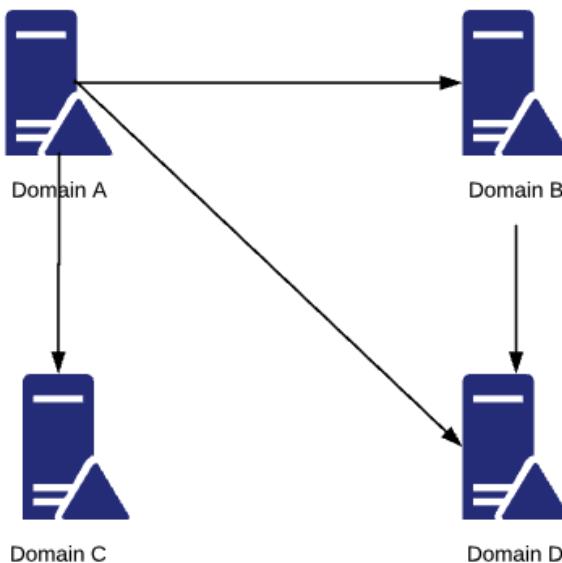


Figure 7.20

- A. Joe can use his account in Domain A.
- B. Joe can use his account in Domain B.
- C. Joe can use his account in Domain C.
- D. Joe can use his account in Domain D.

75. Molly's organization has a shared account that they use to provide access to vendors. What is the primary security objective that is sacrificed using this model, assuming that the password is not shared with unauthorized individuals?

- A. Least privilege
- B. Accountability
- C. Confidentiality
- D. Integrity

76. Donna is looking for a secure way to transfer files between systems. The systems in question are already configured for SSH connections. What file transfer method could she use that would leverage the SSH protocol?

- A. SFTP
- B. FTPS
- C. Dropbox
- D. HTTPS

77. Kristen's organization recently entered into a business partnership with a new shipping vendor. She is placing a server on the network that will facilitate shipping transactions and must be accessed by both the vendor and internal users. Which network zone is the most appropriate placement for this server?

- A. The guest network
- B. The intranet
- C. DMZ
- D. The extranet

78. Tonya is analyzing host firewall logs in an effort to diagnose a service that is not responding to user requests. She finds entries in the host firewall logs indicating that the traffic was allowed. What is the most likely cause of the service not responding?
- A. Application failure
 - B. Host firewall misconfiguration
 - C. Network IPS misconfiguration
 - D. Network firewall misconfiguration
79. Which one of the following security controls would be the least effective at detecting fraud committed by an employee?
- A. Separation of duties
 - B. Job rotation
 - C. Mandatory vacation
 - D. Privileged access monitoring
80. Brian is the physical security official for a data center hosting organization. While entering the building this morning, he noticed that one employee used his badge to enter the building and then held the door open for two other employees. Which one of the following situations occurred?
- A. Piggybacking
 - B. Dumpster diving
 - C. Shoulder surfing
 - D. Impersonation
81. Consider the statistics shown here for a biometric authentication system. What is the system's FRR based upon this data?

	Authorized User	Unauthorized User
Accept	45	2
Reject	5	48

Figure 7.21

- A. 2%
- B. 4%
- C. 5%
- D. 10%

82. Carl is selecting a data loss prevention (DLP) system for use in his organization. He would like to choose an approach that requires the least maintenance effort from his team. Which solution would best meet Carl's needs?

- A. Host-based DLP
- B. Network-based DLP
- C. Cloud-based DLP
- D. Signature-based DLP

83. Ryan would like to restrict the use of a sensitive mobile application so that users may only use it when they are located in a building on his company's corporate campus. Which one of the following technologies can he use to best enforce this restriction?

- A. Application control
- B. Geofencing
- C. Remote wiping
- D. Containerization

84. Val is conducting a black-box penetration test on a website and would like to try to gain access to a user account. If she has not yet gained access to any systems on the target network, which one of the following attacks would be most effective?

- A. Rainbow table
- B. Offline brute force
- C. Offline dictionary
- D. Online brute force

85. Gayle is logging onto a website managed by a third-party vendor using credentials provided by her employer. The authentication system uses SAML-based authentication. In this scenario, who is the identity provider?
- A. Gayle's web browser
 - B. The vendor
 - C. Gayle's employer
 - D. The certificate authority
86. Corwin is beginning a penetration test and is reviewing the technical documentation provided by management that explains how the systems are designed and laid out. What type of test is Corwin most likely performing?
- A. Red box
 - B. Grey box
 - C. White box
 - D. Black box
87. Sandra would like to prevent users of her organization's mobile devices from using those devices to connect laptops and other systems to the network. What feature of mobile devices should she disable through her mobile device management platform?
- A. Split tunneling
 - B. Tethering
 - C. Split horizon DNS
 - D. TLS

Questions 88 through 90 refer to the following scenario.

Gavin is considering different options for backing up the file server used by his organization. This server exhibits the normal usage patterns of an office file server. The four strategies he is considering are shown here:

Option	Monday	Tuesday	Wednesday	Thursday	Friday
A	Full	Full	Full	Full	Full
B	Full	Incremental	Incremental	Incremental	Incremental
C	Full	Differential	Differential	Differential	Differential
D	Full	Differential	Full	Differential	Full

Figure 7.22

88. If Gavin's primary concern is conserving disk space, which option should he choose?
- A. Option A
 - B. Option B
 - C. Option C
 - D. Option D
89. If Gavin's primary concern is the speed of recovering the system after a failure, which option should he choose?
- A. Option A
 - B. Option B
 - C. Option C
 - D. Option D
90. If Gavin's primary concern is the amount of time required to perform the backups, which option should he choose?
- A. Option A
 - B. Option B
 - C. Option C
 - D. Option D

Practice Exam 1 Answers and Explanations

1. D. In this scenario, there are several critical vulnerabilities that all relate to the system running unsupported or unpatched components. While the other issues presented in this question do also appear in the scan results, updating this software and applying necessary security patches would result in the greatest risk reduction and should be Mitch's highest priority.
2. B. Several vulnerabilities exist in different implementations of WPS. Some allow an offline brute force attack known as Pixie Dust. Others may make it impossible for device administrators to disable WPS. Others may use weak encryption. The risk that applies to all WPS devices is the risk of physical access. If an attacker gains physical access to the device, they can join the network.

3. C. Development environments are designed for active use by developers who are creating new code. These environments are the only location where code should be modified. Once code is ready for testing, it is released from the development environment into a test environment for software testing. After the completion of user acceptance testing, the code is moved from the test environment into a staging environment, where it is prepared for final deployment into the production environment. Developers should never have permission to move code themselves but should only be able to move code between environments through the use of a managed change control system.
4. C. While it is possible that any type of attacker might engage in a zero-day attack, it is most likely to find these vulnerabilities exploited by an advanced persistent threat (APT). APT attackers are more likely to have the technical resources to discover and use zero-day vulnerabilities.
5. B. Unified threat management (UTM) solutions combine the features of many different security technologies into a single, cost-effective platform. They are most appropriate for use in small businesses, as they typically are not capable of high-performance activities.
6. D. Stress testing, otherwise known as load testing, is a technique designed to determine the maximum capacity of an application. Cole can use stress testing to evaluate the performance of the application environment under the pressure of 10,000 simultaneous users. Static analysis, regression testing, and fuzz testing all test applications but are not able to determine an application's performance under load.
7. D. Containerization approaches embed all access to corporate systems with a secure application container. No data from inside the container is accessible from other applications on the device. The entire container is controlled by the organization's mobile device management solution. Storage segmentation is a similar solution that provides separate storage for different data classifications but this approach goes beyond storage segmentation. Sideloaded is a technique for loading applications and data onto a device outside of normal channels. Full device encryption provides encrypted storage for all data on a device but does not differentiate between corporate and personal data.

8. A. Robert is not the file's owner, nor is he a member of the file's group. Therefore, the permissions that he has are those that apply to all users. In a Linux permission string, the first character indicates whether an object is a directory or not. The next three characters indicate the permissions assigned to the file's owner. The three characters after that assign permissions to members of the file's group. The next three characters indicate the all users permissions. The all users permissions for this file are 'r--'. Therefore, Robert can read the file but cannot write to it or execute it.
9. D. The accuracy of a biometric authentication system is described using three metrics. The false acceptance rate (FAR) is the frequency at which the system admits a person who should not be admitted. The false rejection rate (FRR) is the frequency at which the system denies access to an authorized user incorrectly. The FAR can be improved by increasing the sensitivity of the system, while the FRR can be improved by decreasing the sensitivity of the system. Because of this, the best measure of accuracy is the crossover error rate (CER), which is the sensitivity point at which the FAR and FRR are equal.
10. D. The Remote Desktop Protocol (RDP) provides a secure graphical user interface connection to a remote Windows system and would meet Henry's needs out of the box. It may be possible to configure remote access via a secure shell (SSH) connection, but this would require an additional tool and configuration. A virtual private network (VPN) could provide a secure connection to the remote network but does not inherently offer a graphical interface to manage a system. Telnet is not a secure protocol.
11. D. 12.168.1.100 and 129.168.1.100 are valid public IP addresses and should be permitted as inbound source addresses. 278.168.1.100 is not a valid IP address because the first octet is greater than 255. It does not need to be blocked because it is not possible. This leaves 192.168.1.100. This address is a private address and should never be seen as a source address on packets crossing an external network connection.
12. C. The Network Time Protocol (NTP) is designed to synchronize clocks on systems and devices with a centralized source. The Simple Network Management Protocol (SNMP) is designed for the management of network devices and does not synchronize time across a variety of devices. The Lightweight Directory Access Protocol (LDAP) is a directory services protocol and does not perform time synchronization. The Real-Time Protocol (RTP) is an application protocol designed for videoconferencing and, despite the name, does not perform time synchronization.

13. B. Cold sites have only basic infrastructure available and require the longest period of time to activate operations. They are also the cheapest option. Warm sites add hardware, and possibly software, to the mix but do not have a current copy of the data running. They require hours to activate. Hot sites are up and running at all times and can assume operations at a moment's notice. They are the most expensive option. Mobile sites are transportable on trailers and do provide a cost/benefit balance but they are not permanently situated like cold, hot, and warm sites.
14. B. This is a classic example of a hacktivist attack where the attacker was motivated by an ideological agenda. There does not seem to be any financial motivation here, which would be the primary sign of organized criminal activity. The attack is also prominent and obvious, lacking the stealthy characteristics of an attack waged by a nation-state or other APT.
15. D. Resiliency is the ability of a system to withstand potentially disruptive actions. In this scenario, Frank is seeking to design a VPN solution that exhibits high levels of resiliency.
16. B. In a public cloud environment, providers offer services on the same shared computing platform to all customers. Customers do not necessarily have any relationship to, or knowledge of, each other. In a private cloud environment, an organization builds its own computing environment. In a hybrid cloud environment, an organization combines elements of public and private cloud computing. In a community cloud environment, a group of related organizations builds a shared cloud environment that is not open for general public use.
17. C. Penetration tests take an attacker's perspective on the network and actually seek to bypass security controls and gain access to systems. This would be the best way for Tom to determine the likelihood of a successful attack.
18. C. Data owners and data stewards both bear responsibility for data quality standards. However, day-to-day data quality issues are the domain of a data steward, while a data owner bears executive-level responsibility. Data custodians and users generally do not have overarching data quality responsibilities.
19. D. PIVs contain four digital certificates. The card authentication certificate is used to verify that the PIV credential was issued by an authorized entity, has not expired, and has not been revoked. The PIV authentication certificate is used to verify that the PIV credential was issued by an authorized entity, has not expired, has not been revoked, and that the holder of the credential (you) is the same individual it was issued to. The digital signature certificate allows the user to digitally sign a document or email, providing both integrity and non-repudiation. The encryption certificate allows the user to digitally encrypt documents or emails.

20. D. This image shows the cipher block chaining (CBC) mode of cipher operation. You can determine this by noting that the plaintext block being encrypted is XORed with the ciphertext of the preceding block.
21. A. Attacks sponsored by organized crime groups almost always have financial motivations.
22. B. Web servers use TCP port 80 for unencrypted HTTP communications and they use TCP port 443 for encrypted HTTPS communications. If Ryan would like to require the use of encrypted connections to the web server, he should allow TCP port 443 and block TCP port 80.
23. B. The US federal government's Digital Signature Standard (DSS) endorses the use of the Digital Signature Algorithm (DSA) for the creation of digital signatures.
24. A. The recovery time objective (RTO) is the amount of time that it is acceptable for a system to be down prior to recovery during a disaster. The recovery point objective (RPO) is the amount of acceptable data loss during a recovery effort. The RTO and RPO are targets rather than measures of actual performance. The mean time between failures (MTBF) is the average amount of time that elapses between the failures of a system or component. The mean time to repair (MTTR) is the amount of time that it takes to recover a failed system. The MTBF and MTTR are measures of actual performance.
25. B. The recovery time objective (RTO) is the amount of time that it is acceptable for a system to be down prior to recovery following a disaster. The recovery point objective (RPO) is the amount of acceptable data loss during a recovery effort. The RTO and RPO are targets rather than measures of actual performance. The mean time between failures (MTBF) is the average amount of time that elapses between the failures of a system or component. The mean time to repair (MTTR) is the amount of time that it takes to recover a failed system. The MTBF and MTTR are measures of actual performance.
26. C. Push notifications are a secure way to implement a second authentication factor and also have high user satisfaction because they typically only require the user to click **approve** on a notification pushed to their device. SMS notifications and app-based passcode generators have lower user satisfaction because they require the user to enter a passcode to complete the authentication process. Email notifications are not an acceptable way to implement multifactor authentication with mobile devices because an email account is not tied to a specific device and, therefore, does not constitute a "something you have" authentication approach.

27. B. Bill should definitely update the operating system to bring it into compliance with current security standards. However, he does not have console access to the device, so the only way he can do this is to obtain the update from the device vendor.
28. C. The Triple DES algorithm performs three different rounds of DES encryption. The most secure way of doing this is with three different keys. A less secure mode of operation uses only two keys, while an insecure mode of operation uses a single key to replicate the functionality of DES. It is not possible to use Triple DES with four encryption keys.
29. D. Communication between the database server and the firewall server would not travel through the hardware firewall because they are located on the same network segment. In this case, the database server is attempting to connect to the file server, so the file server's host firewall is the most likely culprit.
30. A. In a RAID 5 array, all of the disks contain data except for the parity disk. Therefore, regardless of the number of disks in the array, only a single disk may fail before data is permanently lost.
31. C. This upgraded safe is best described as a preventive control because it is designed to prevent an intruder from successfully cracking it in less than 30 minutes. This time period allows detective controls the time to work and identify the intrusion.
32. D. Bcrypt is a key stretching algorithm that is both memory-hardened and CPU-hardened. PBKDF2 is CPU-hardened but not memory-hardened. HMAC and RIPEMD are not key stretching algorithms.
33. C. Identification occurs when a user makes a claim of identity. This claim is then proven during the authentication phase, through the use of one or more authentication factors, such as a password, smart card, or biometric reading. The system then determines the specific activities that the authenticated user is authorized to engage in by consulting access control lists (ACLs) and other mechanisms and then tracks user access in an accounting system.
34. A. Maureen can use a rainbow table attack against this website because she has access to the password file. This would be more productive than a dictionary attack because it precomputes the password hashes. Both dictionary and rainbow table attacks are more productive than brute force attacks when the site does not have a strong password policy.
35. A. This is the output feedback (OFB) mode of encryption. You can determine this because it generates keystream blocks to combine with the plaintext and arrive at ciphertext.

36. D. The Advanced Encryption Standard (AES) supports key sizes of 128, 192, and 256 bits. It does not support 512-bit keys.
37. A. Apple's iOS platform limits users to installing applications downloaded from Apple's App Store. The other three device types listed – Samsung Galaxy, Motorola Moto, and Huawei P-series – are all Android devices, which allow users to download apps from a variety of third-party app stores.
38. B. In a load-balanced network that uses server affinity, client requests are assigned to the server that is already handling requests from that same client to minimize the number of network connections.
39. D. NIST changed their password security guidelines in 2017 and now recommends that organizations do not enforce the expiration of user passwords.
40. B. In this scenario, Peter has already completed his reconnaissance but has not yet gained access to any systems on the target network. Therefore, he is still in the initial exploitation phase of the penetration test.
41. B. The SIEM correlation engine is a sensitive device that should be accessed only by security personnel. Therefore, it should be placed on the internal network where it is not exposed to external traffic.
42. A. The assignment of permissions based upon a user's job indicates that this is a role-based access control system. There is not enough information provided to come to the conclusion that this is a mandatory or discretionary access control system. There is also no indication that the attributes of the user's account are scrutinized during the authorization process.
43. A. Port security restricts the number of unique MAC addresses that may originate from a single switch port. It is commonly used to prevent someone from unplugging an authorized device from the network and connecting an unauthorized device but may also be used to prevent existing devices from spoofing the MAC addresses of other devices.
44. C. The exclusive or (XOR) operation is true when one and only one of the inputs is true. This means that one input must have a value of 1 while the other has a value of 0. Applying this operation to the problem shown here gives the answer of 1001.
45. C. Firewall log analysis can be easily automated to identify common configuration issues and attack signatures. Password reset automation is a very commonly used technique to reduce the burden on help desks. Configuration management is generally only possible through automation. Risk assessments are an inherently time-intensive activity that would not likely benefit from automation.

46. C. In a choose-your-own-device (CYOD) model, the employee is permitted to choose from a selection of approved devices. The company owns the device. In a bring-your-own-device (BYOD) model, the employee owns the device. In corporate-owned, personally-enabled (COPE) and corporate-owned models, the company owns the device but the employee does not necessarily have the ability to choose the device.
47. B. While Glenn may use any of the technologies described here to segment the sensitive network, the question specifically asks for the strongest degree of separation possible. This is achieved by designing an air-gapped network that is not connected to any other network.
48. D. Gary is engaging in a dictionary attack because he begins the attack with a dictionary of possible passwords. This is not a brute force attack because Gary begins with a list of possible passwords. A brute force attack would simply try every possible value. It is not a rainbow table attack because Gary did not create a rainbow table: a prehashed file of possible password values.
49. D. This is a classic example of a memory leak. The application is not releasing memory that it no longer needs, and it continues to make requests for new memory allocations. This activity persists until the system runs out of memory and is rebooted.
50. D. Retinal scanning is a slow, intrusive technique that requires specialized hardware and cannot be performed with a standard smartphone. Smartphones do commonly use passcodes, fingerprint scanning, and facial recognition for authentication.
51. D. All DNSSEC implementations must support the RSA/SHA-1 cipher suite to maintain compatibility between systems. The RSA/MD5 cipher suite should never be used due to insecurities in the MD5 hash algorithm. The RSA/SHA-256 and RSA/SHA-512 cipher suites are recommended for use but are not required.
52. B. Cross-site scripting (XSS), cross-site request forgery (XSRF), and SQL injection attacks all exploit vulnerabilities in web applications. Shimming is a technique used to manipulate device drivers.
53. D. The object identifier (OID) indicates the specific purpose of the digital certificate. For example, OID 1.3.6.1.5.5.7.3.1 is for server authentication, while 1.3.6.1.5.5.7.3.4 is for email protection.
54. B. Minifying code makes it very difficult for humans to interpret, but not impossible. This is an example of obfuscation. If the code were encrypted, it would require decryption prior to execution. If the code were hashed or masked, it would not function because those operations are irreversible.

55. A. The image shows a mantrap, a physical security control designed to limit access to a facility to one person at a time. This control prevents tailgating by preventing one individual from holding the door open, intentionally or accidentally, for a second person.
56. A. WPA uses the Temporal Key Integrity Protocol (TKIP) to rapidly cycle encryption keys and overcome the weaknesses of WEP. WPA2 uses the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) to provide enhanced security using AES. Hashing is not an integral component of the cryptographic improvements.
57. B. In this attack, the attacker executed a request against a third-party website by taking advantage of the fact that the user already had an established session with that site. This is an example of a cross-site request forgery (XSRF) attack.
58. A. The Network Time Protocol (NTP) is used to synchronize the clocks of devices to a standardized time source. NTP is quite useful in helping to ensure consistent timestamps on log entries.
59. D. The image explains that the malware encrypted the contents of the computer and will only restore access after the user pays a ransom. This is an example of ransomware, a category of crypto-malware.
60. C. Any of these systems would be capable of detecting the attack. However, a SYN flood attack is a well-documented attack and any signature-based IDS would have a built-in signature that defines the attack precisely. Therefore, a signature-based system is most likely to successfully detect this attack.
61. C. The General Data Protection Regulation (GDPR) is a sweeping privacy regulation covering operations in the European Union. It replaced the older Data Protection Directive (DPD) in 2018. The Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA) are US, not European, laws.
62. A. The most effective way to address this issue is to deploy a patch that corrects the vulnerability. Since this vulnerability is in Apache Tomcat, the patch must be applied to that service. Patching the operating system will not correct an issue with the service. Web application firewalls and content filters, if deployed in the correct location, may block an attack from exploiting this vulnerability but they do not remediate the root issue.
63. C. Paul has already gained initial access to a system: the web server. He is now attempting to take that access and pivot from the initial compromise to a more lucrative target: the file server.

64. B. The passwords shown here are hashed using the salted SHA hash algorithm, as described by the {SSHA} attribute. They are neither encrypted (because the hash cannot be reversed) nor stored in cleartext form (because you can't examine the value and determine the password). If they were hashed using an unsalted version of SHA, the attribute before the hash would read {SHA} instead of {SSHA}.
65. B. This image clearly shows the patterns in an individual's iris. Retinal scanning requires images of the blood vessels inside the eye, which are not visible in this image. Facial recognition requires an image of a significant portion of the individual's face.
66. C. Two-person control requires the concurrence of two individuals for sensitive actions. That is the scenario described here. Separation of duties says that an individual should not have both permissions necessary to perform a sensitive action. This is a closely related but distinct principle. There is no evidence given that supervisors do not have the ability to create payments, so separation of duties is not in play here.
67. A. This attack leveraged the implied authority of someone wearing a security guard's uniform. It may also have leveraged intimidation by threatening employees, or consensus when employees followed each other's lead, but this is not clear in the scenario. There is no indication of scarcity being used in this particular attack.
68. B. A split tunnel VPN policy allows Vic to specify that only traffic destined for the home office should be routed through the VPN. If Vic used a full tunnel policy, engineers would not be able to access systems on the customer's local network. Vic may use either an IPsec or TLS VPN to meet this requirement. That technology decision is separate from determining what traffic is sent through the VPN.
69. B. In a Type 1 hypervisor, the hypervisor runs directly on the physical hardware. In a Type 2 hypervisor, the hypervisor runs on a host operating system which, in turn, runs on the physical hardware. In both cases, guest operating systems run on top of the hypervisor.
70. C. The mean time to repair (MTTR) is the amount of time that it will typically take to restore service after a failure. In this case, the MTTR is 3 days: the amount of time to obtain and install a replacement firewall.
71. D. The mean time between failures (MTBF) is the amount of time that typically passes between failure events. In this scenario, Kyle has determined that events typically occur once every 4 years.
72. B. From his conversations with business leaders, Kyle determined that the business can tolerate an outage of 4 hours, making this the recovery time objective (RTO).

73. A. From his conversations with business leaders, Kyle determined that the business can tolerate the loss of 1 hour of data, making this the recovery point objective (RPO).
74. C. The diagram shows federated trust relationships. Arrows with only one arrowhead are one-way trusts. Joe's account is in Domain D and the relationships show that Domains A and B have one-way trust in Domain D. Therefore, Joe can use his account to access resources in Domains A and B. Domain A trusts Domain C, but Domain C does not trust Domain A, so Joe can't use his account to access resources in Domain C.
75. B. If the password remains known only to authorized individuals, this does not violate the principles of confidentiality or integrity. There is no indication from the scenario that the account has excess privileges, so least privilege is not violated. However, the use of a shared account prevents security staff from determining which individual performed an action, violating the principle of accountability.
76. A. The Secure File Transfer Protocol (SFTP) provides a file transfer capability through a Secure Shell (SSH) connection. The File Transfer Protocol Secure (FTPS) also provides secure file transfers, but does so through a modified version of the FTP protocol and does not use SSH. Dropbox is a proprietary file sharing service that does not use SSH. The HyperText Transfer Protocol Secure (HTTPS) is a secure web protocol that may be used for file transfers but does not leverage SSH.
77. D. Servers that provide services to business partners should be placed on the extranet. Intranet servers should have access restricted to internal users. DMZ servers may be accessed by the general public. Guest networks are designed for visitors to a facility to gain internet access.
78. A. The fact that the packets are reaching the host rules out a network firewall or IPS issue. The fact that the logs indicate that the traffic was allowed rules out a host firewall issue. Therefore, the most likely remaining cause is an issue with the application.
79. A. Mandatory vacation and job rotation policies seek to uncover fraud by requiring employees to be unable to perform their normal job functions for an extended period of time, subjecting those functions to scrutiny by other employees. Privileged access monitoring tracks the activity of users with special privileges and may also uncover fraud. Separation of duties seeks to prevent fraudulent activity before it occurs and would not detect the misuse of privileges in a fraudulent manner.

80. A. This is a classic example of a piggybacking attack where one person enters a physical facility and then holds the door open for others to enter without requiring them to also use the access control system. In a dumpster diving attack, individuals rummage through the trash searching for sensitive information. In a shoulder surfing attack, the perpetrator looks over the shoulder of an individual while they use a computer. There is no sign that the individuals entering the building without authenticating were making false claims of identity, so there is no evidence of an impersonation attack.
81. C. The false rejection rate (FRR) of a system is calculated by dividing the number of false rejections by the total number of authentication attempts. In this dataset, there are 100 total authentication attempts, of which 5 were false rejections of an authorized user. Therefore, the false acceptance rate is 5%.
82. C. Cloud-based DLP solutions are updated and maintained by the cloud vendor and would involve the least maintenance effort from Carl's team. Host-based and network-based DLP would require the local team to install the solution and keep it updated. The use of signature-based DLP technology does not have a significant impact on the amount of maintenance time.
83. B. Geofencing allows an organization to restrict certain actions so that they may only take place when the device is in a specified area. If a user exits the geofenced area, the action is no longer possible. This technology is ideal for limiting the use of an application to a specific geographic area, such as a corporate campus.
84. D. While it is not an incredibly productive attack, an online brute force attack is Val's only option of the choices provided. Val does not have access to a password file, which would be a requirement for an offline attack, such as an offline dictionary attack, a rainbow table attack, or an offline brute force attack.
85. C. In SAML authentication, the user agent is the web browser, application, or other technology used by the end user. The service provider is the service that the user would like to access. The identity provider is the organization providing the authentication mechanism. The certificate authority issues the digital certificates required to secure the connections.
86. C. In a black-box attack, the attacker does not have access to any information about the target environment before beginning the attack. In a grey-box attack, the attacker has limited information. In a white-box attack, the attacker has full knowledge of the target environment before beginning the attack.

87. B. Tethering allows mobile devices to share their network connection with other devices. Split tunneling allows a device to send traffic through a VPN tunnel only when connecting to corporate systems, while split-horizon DNS allows the use of different DNS servers for different networks. Transport layer security (TLS) is an important encryption protocol used to secure communications between devices.
88. B. The use of incremental backups is the best way to conserve disk space. If Gavin chooses this option, he will back up the entire file server on Monday. Then, each of the other day's backups will include only the files added or modified on those days, which is the approach used by incremental backups.
89. A. If Gavin performs a full backup each day, when he recovers the system, he will only need to restore the single full backup that occurred most recently before the failure. All of the other strategies require restoring multiple backups.
90. B. Each strategy requires performing a full backup on the first day, which is the most time-consuming operation. Options A and D require performing additional full backups, so those options may be eliminated immediately. This leaves us with a choice between strategies that perform incremental backups and differential backups. Differential backups only back up files that have changed since the last full backup, making them a faster choice than full backups. However, incremental backups only back up files that have changed since the last full or incremental backup, making them even faster to perform.

8

Practice Exam 2

Practice Exam 2 Questions

1. Ralph is reviewing user accounts and matching up the permissions assigned to those accounts in the ERP to access requests made by managers. What activity is Ralph undertaking?
 - A. Credential management
 - B. Usage auditing
 - C. Privilege auditing
 - D. Multifactor authentication

2. Tom is concerned about the fact that executives routinely leave their mobile devices unattended on their desks in the office. What control can he enforce through his MDM tool to prevent misuse of those devices?
 - A. Remote wipe
 - B. Geofencing
 - C. Screen locking
 - D. Application control

3. Taylor is conducting a business impact analysis for her organization as part of the organization's business continuity planning initiative. During that analysis, she identifies the amount of time that would be acceptable for a system to be down during a disaster. What metric should she use to capture this information?
 - A. RPO
 - B. RTO
 - C. MTTR
 - D. MTBF

4. George is evaluating the performance of his organization's business continuity efforts and measures the amount of time that passes between each time that a web server experiences a hard drive failure. What metric should George use to capture this information?
 - A. RPO
 - B. MTTR
 - C. MTBF
 - D. RTO

5. Ralph comes across a legacy infrastructure that uses telnet to create an administrative connection between a client and a server. Even though this connection takes place over a private network link, Ralph would like to replace telnet with a secure protocol to prevent eavesdropping. What protocol would be the easiest drop-in replacement for telnet?
- A. TLS
 - B. FTPS
 - C. SSL
 - D. SSH
6. Will is selecting a new encryption algorithm for use in his organization. Which one of the following algorithms is weak and should not be considered for use?
- A. DES
 - B. 3DES
 - C. AES
 - D. RSA
7. What type of proxy server is shown in the following illustration?

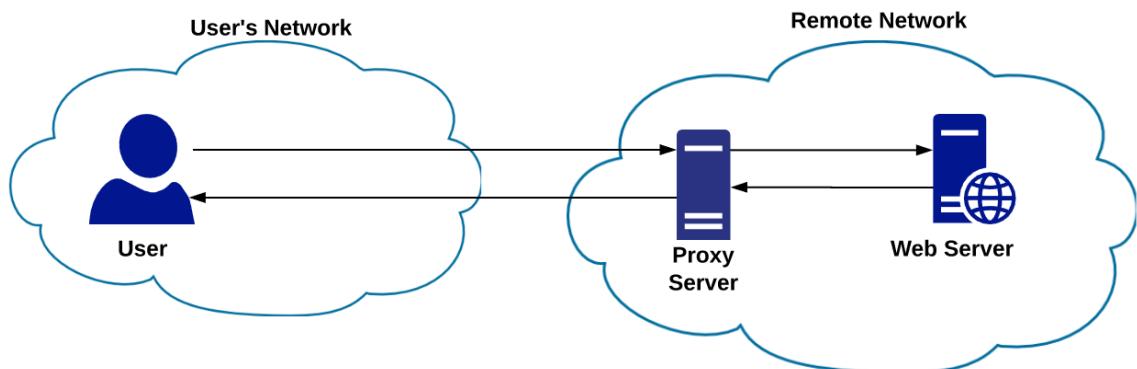


Figure 8.1

- A. Forward proxy
- B. Reverse proxy
- C. Caching proxy
- D. Content filtering proxy

8. Fred created a set of IP restrictions on his Cisco router using Cisco's extended access control list (ACL) functionality. What type of access control model is Fred enforcing?
 - A. Role-based access control
 - B. Rule-based access control
 - C. Attribute-based access control
 - D. Discretionary access control
9. Sandy is designing a new computing environment for his company. He is contracting with XYZ Cloud Services, who will be providing him with the ability to provision servers on a self-service basis. What type of cloud provider is XYZ?
 - A. SaaS
 - B. IaaS
 - C. PaaS
 - D. SecaaS
10. Tom is investigating a report from his organization's intrusion detection system. After an exhaustive investigation, he determines that the activity detected by the system was actually not an attack. What type of report took place?
 - A. False negative
 - B. True positive
 - C. True negative
 - D. False positive
11. What common clause in software is used specifically for error handling?
 - A. Try...catch
 - B. If...then
 - C. Do...while
 - D. For loop

12. Which one of the following EAP protocols does not take advantage of transport layer security?
 - A. EAP-FAST
 - B. EAP-IKEv2
 - C. EAP-TLS
 - D. EAP-TTLS
13. Linda is investigating a security incident that took place in her organization. The attacker issued himself checks from an organization account and then created false journal entries in the accounting system to cover them up. There are no signs of unauthorized activity in IPS or firewall logs. What type of attacker most likely conducted this attack?
 - A. Script kiddie
 - B. Organized crime
 - C. Insider
 - D. Competitor
14. Carla is conducting a penetration test and she has successfully gained access to a jumpbox system through the use of social engineering. Her current access is as a standard user and she is attempting to gain administrative access to the server. What penetration testing activity is Carla engaged in?
 - A. Initial exploit
 - B. Pivot
 - C. Persistence
 - D. Escalation of privilege
15. Kevin is deploying a new customer relationship management (CRM) server. The services offered by this device will be accessible only to employees of Kevin's company. What network zone offers the most appropriate placement for this server?
 - A. DMZ
 - B. Extranet
 - C. Intranet
 - D. Guest network

16. Samantha is the administrator of her organization's mobile devices and wants to ensure that users have current versions of the operating system firmware. Which one of the following approaches will best meet this need?
 - A. Administrator installation
 - B. OTA upgrades
 - C. User installation
 - D. Sideloaded
17. Which one of the following data destruction techniques produces waste material that requires wearing a respirator during exposure?
 - A. Pulverization
 - B. Wiping
 - C. Purging
 - D. Degaussing
18. Tim is investigating an ARP spoofing attack that took place on his organization's network. What is the maximum scope of a single ARP spoofing attack?
 - A. The attacker and the victim must be using the same router.
 - B. The attacker and the victim must be behind the same firewall.
 - C. The attacker and the victim must be connected to the same switch.
 - D. The attacker and the victim must be sharing a switch port.
19. Which one of the following is not an appropriate use of the MD5 hash function?
 - A. Verifying file checksums against corruption
 - B. Partitioning database records
 - C. Creating digital signatures
 - D. Identifying duplicate records

20. What type of lock is shown here?



Figure 8.2

- A. Preset lock
 - B. Cipher lock
 - C. Biometric lock
 - D. Smartcard lock
21. What cryptographic cipher is used in the Bcrypt key stretching function?
- A. 3DES
 - B. AES
 - C. Blowfish
 - D. RSA
22. Patrick is investigating a security incident and is able to monitor an intruder's activity on one of his servers. The intruder wrote a script that is attempting to log into a web application using an administrator account. It first attempted the password *aaaaaaaa*, followed by *aaaaaaab*, *aaaaaaac*, and so on. What type of attack is taking place?
- A. Offline brute force
 - B. Online brute force
 - C. Dictionary
 - D. Rainbow table

23. Which one of the following activities is not a passive test of security controls?
- A. Configuration analysis
 - B. Penetration testing
 - C. Network monitoring
 - D. Intrusion detection
24. Which one of the following is an example of a privilege escalation attack against a mobile device?
- A. Jailbreaking
 - B. Sideloaded
 - C. Man-in-the-middle
 - D. Tethering
25. Which one of the following is an example of a platform-as-a-service (PaaS) computing environment?
- A. Amazon EC2
 - B. Amazon Lambda
 - C. Microsoft Azure Virtual Machine
 - D. Microsoft Azure DNS
26. Which one of the following techniques is an example of dynamic code testing?
- A. Fuzzing
 - B. Data flow analysis
 - C. Taint analysis
 - D. Lexical analysis

27. David is purchasing cloud infrastructure services from Microsoft Azure. Use of the servers he purchases will be strictly limited to employees of his company. What type of cloud environment is this?
- A. Hybrid cloud
 - B. Private cloud
 - C. Public cloud
 - D. Community cloud
28. Which one of the following tools is useful in testing the security of a wireless network's encryption key?
- A. nmap
 - B. NetStumbler
 - C. Aircrack
 - D. QualysGuard
29. Frances is investigating a security incident where a former employee accessed a critical system after termination, despite the fact that the employee's account was disabled. Frances learned that the employee, a software engineer, created a dummy username and password that was hardcoded into the application and used those credentials to log in. What type of attack took place?
- A. Logic bomb
 - B. Backdoor
 - C. Remote access Trojan
 - D. Ransomware

30. Orlando is configuring his network firewall to allow access to the organization's email server, as shown in the following image. He would like to allow internet users to send emails to the organization but would like to only allow internal users to access emails on the server. What protocol(s) should Orlando allow to access the email server from the internet?

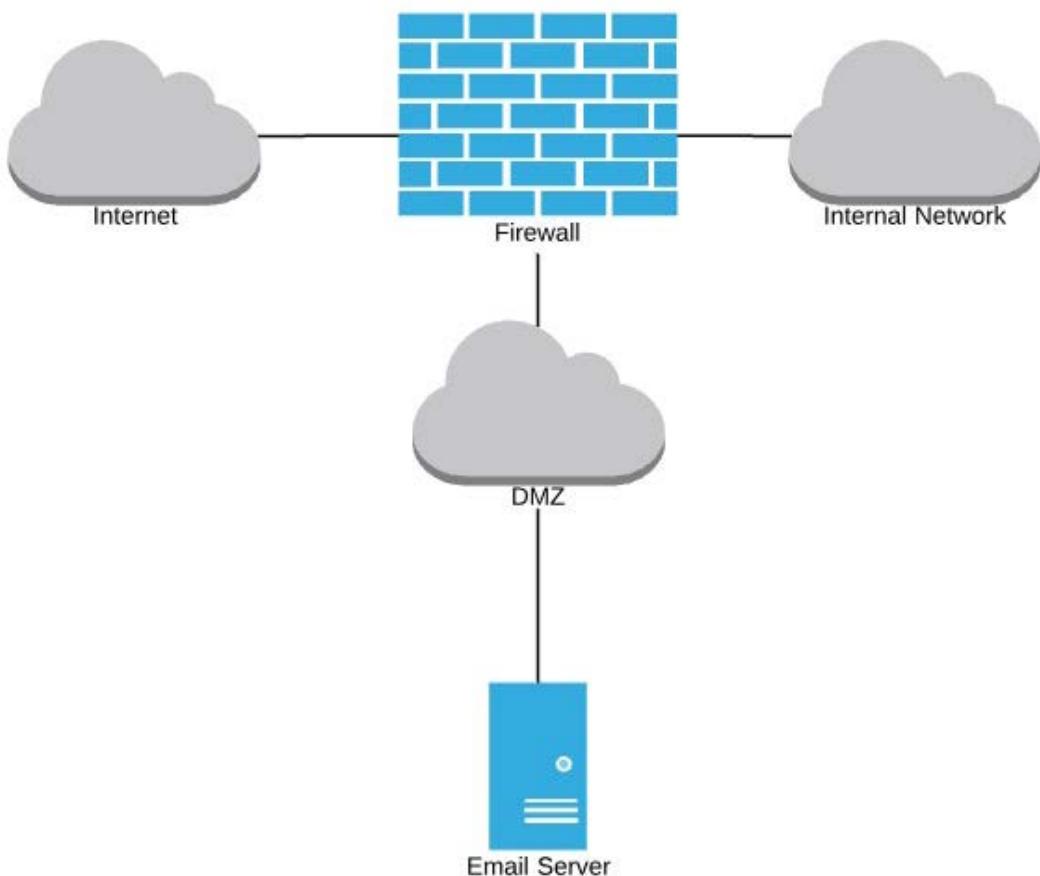


Figure 8.3

- A. IMAP only
- B. SMTP only
- C. POP3 only
- D. IMAP and POP3

31. Which one of the following RADIUS messages is normally found only in situations where an organization is implementing multifactor authentication?
 - A. Access-Accept
 - B. Access-Request
 - C. Access-Challenge
 - D. Access-Reject
32. Visitors to the website arifrance.com found themselves directed to a website containing discount travel information when they expected to find the Air France corporate website. What type of attack took place?
 - A. Typosquatting
 - B. Website defacement
 - C. Clickjacking
 - D. Session hijacking
33. Which one of the following terms best describes the level of firewall protection that is typically found in router access control lists?
 - A. Stateful
 - B. Stateless
 - C. Next-generation
 - D. Proxying
34. Norm is designing a file transfer mechanism to facilitate the flow of information between the hospital where he works and an X-ray service provider with locations around the city. Which one of the following protocols does NOT provide a secure option for these file transfers?
 - A. SFTP
 - B. SCP
 - C. FTP
 - D. FTPS

35. After running a vulnerability scan of a copy machine, Tom discovers the results shown in the following screenshot. What is the most likely cause of these results?

- ▶  5 Microsoft Cumulative Security Update for Internet Explorer (MS17-006)
- ▶  5 Microsoft Cumulative Security Update for Windows (MS17-012)
- ▶  4 Microsoft Uniscribe Multiple Remote Code Execution and Information Disclosure Vulnerabilities (MS17-011)
- ▶  4 Microsoft Security Update for Windows Kernel-Mode Drivers (MS17-018)
- ▶  4 Microsoft Windows DirectShow Information Disclosure Vulnerability (MS17-021)
- ▶  4 Microsoft XML Core Services Information Disclosure Vulnerability (MS17-022)
- ▶  4 Microsoft Windows Kernel Elevation of Privileges (MS17-017)

Figure 8.4

- A. The copy machine has an embedded operating system.
- B. The results are false positives.
- C. Tom scanned the wrong IP address.
- D. The results are true negatives.
36. Colleen is running two load balancers in active/active mode. What is the most significant risk that she is likely facing?
- A. Servers must be manually assigned to load balancers.
- B. Network traffic may be misrouted.
- C. The load balancers may not have the capacity to survive the failure of one device.
- D. The two load balancers may become out of sync.
37. Which one of the following cipher types works on plaintext one bit or byte at a time?
- A. Block cipher
- B. Stream cipher
- C. AES
- D. Blowfish

38. What mode of cipher operation is shown here?

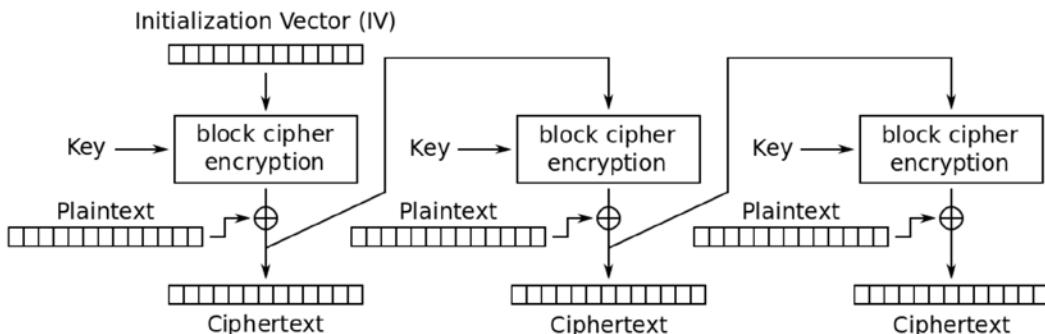


Figure 8.6

- A. CBC
 - B. OFB
 - C. ECB
 - D. CFB
39. Which one of the following tools may be used to scan a system over the network and detect potential vulnerabilities in that system?
- A. Nessus
 - B. Nmap
 - C. Jack the Ripper
 - D. Kismet
40. Which one of the following mobile device deployment models allows employees to bring personally owned devices into the corporate environment?
- A. COPE
 - B. CYOD
 - C. BYOD
 - D. Corporate-owned

41. Roger is conducting a penetration test and has gained administrative access to a system on his target network. He is now using those administrative privileges to set up a back door. What stage of the attack is Roger in?
- A. Persistence
 - B. Initial exploitation
 - C. Privilege escalation
 - D. Pivot
42. During a web application security review, Crystal discovered that one of her organization's applications is vulnerable to SQL injection attacks. Where would be the best place for Crystal to address the root cause issue?
- A. Database server configuration
 - B. Web server configuration
 - C. Application code
 - D. Web application firewall
43. Tim is choosing a card-based control system for physical access to his facility. His primary concern is the speed of authentication. Which type of card would be most appropriate for this situation?
- A. Proximity card
 - B. Smart card
 - C. Magnetic stripe card
 - D. Photo ID card
44. Which one of the following types of access is necessary to engage in a pass-the-hash attack?
- A. Access to a domain workstation
 - B. Access to a domain controller
 - C. Access to a network segment
 - D. Access to a public website

45. This diagram shows the results of testing the accuracy of a biometric authentication system. In this diagram, what characteristic is designated by the arrow?

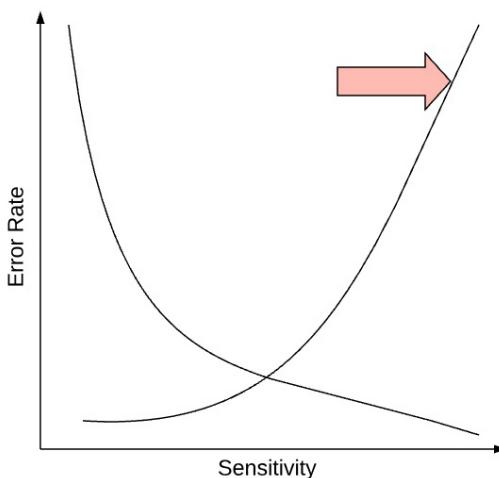


Figure 8.7

- A. CER
 - B. FAR
 - C. IRR
 - D. FRR
46. Gail is a software developer who recently completed the coding of a new module that will be incorporated into one of her organization's products. Now that her work is complete, she is ready to request that the code be moved to the next environment. Where should the code go next?
- A. Development environment
 - B. Test environment
 - C. Staging environment
 - D. Production environment
47. What is the primary purpose of the Diffie-Hellman (DH) algorithm?
- A. Digital signatures
 - B. Key exchange
 - C. Message confidentiality
 - D. Authentication

48. Which one of the following characteristics does not accurately describe an Agile approach to software development?
- A. Features are prioritized by the value added.
 - B. Customers should be available throughout the project.
 - C. Requirements are clearly defined before beginning development.
 - D. Changes are welcomed in the process.
49. Carl is creating an authentication system where users seeking to access web applications will be redirected to a login page, such as the one shown here. What type of authentication is Carl seeking to implement?

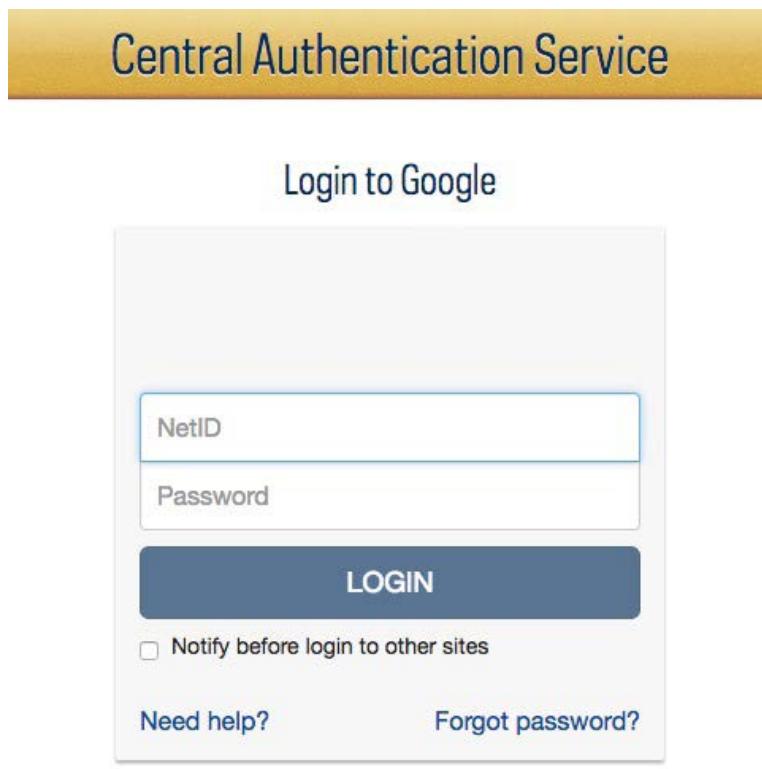


Figure 8.8

- A. SAML
- B. SSO
- C. Federation
- D. RADIUS

50. Which one of the following wireless networking protocols makes use of a backend authentication server?
- A. WPA-PSK
 - B. WPA-Enterprise
 - C. WEP-PSK
 - D. WPS
51. Nadine recently accepted a new position as the CISO of a financial institution. What regulatory body produces information security standards that specifically apply to financial institutions?
- A. FDA
 - B. FERC
 - C. FFIEC
 - D. FRA
52. Roger recently deployed an IDS on his organization's network and tuned it to reduce the false positive rate. Which one of the following categories best describes this control?
- A. Corrective
 - B. Preventive
 - C. Detective
 - D. Compensating
53. Xavier is concerned about the security of a wireless network in his organization's conference facility that uses WPS to connect new clients. What is the best action that Xavier can take to protect this network?
- A. Remove WPS stickers from wireless access points.
 - B. Disable WPS.
 - C. Use a strong WPS PIN.
 - D. Change the PSK.

54. Bruce is investigating a security incident that involves the embezzlement of funds from his organization. Which one of the following groups should be the first focus of his investigation?
- A. Script kiddies
 - B. APTs
 - C. Insiders
 - D. Hacktivists
55. Consider the hardware passcode generator shown here. What algorithm does this token use to generate passcodes?



Figure 8.9

- A. LOTP
 - B. TOTP
 - C. HOTP
 - D. KOTP
56. Which one of the following categories of account should normally exist on a secured server?
- A. Guest account
 - B. Service account
 - C. Generic account
 - D. Shared account

57. Which encryption mode of operation is shown in the following figure?

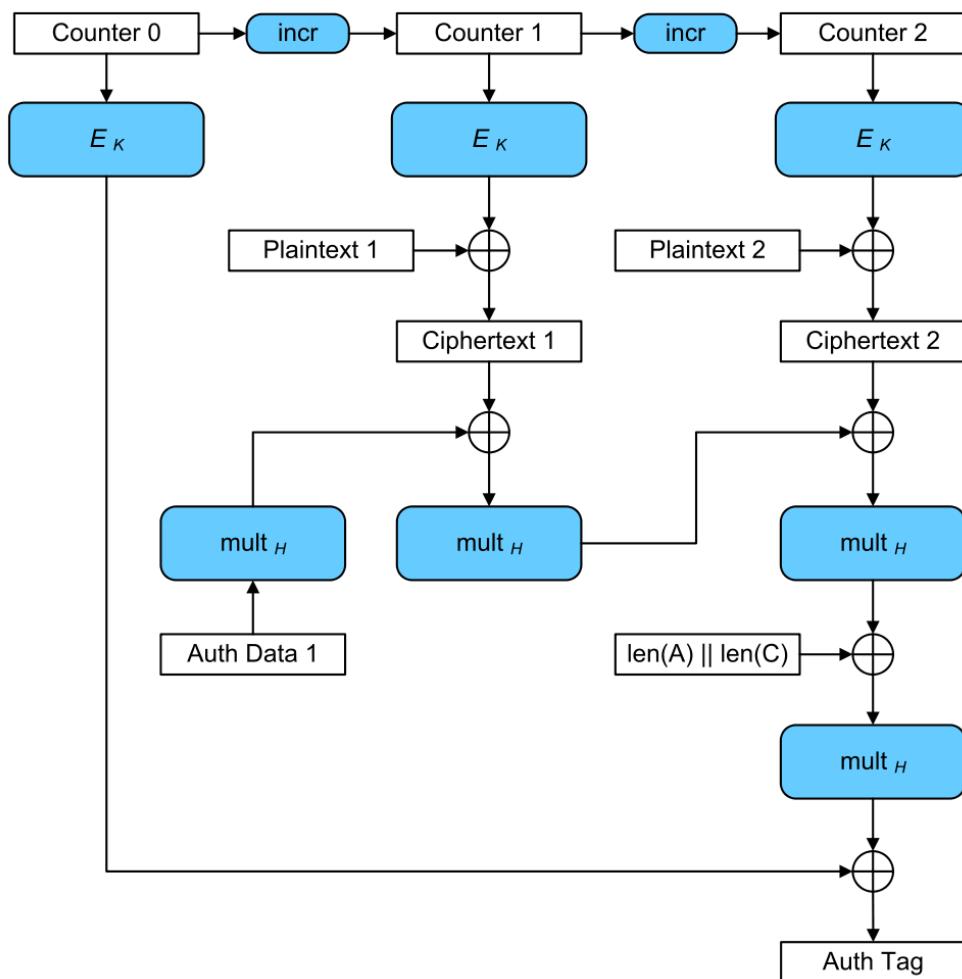


Figure 8.10

- A. CTM
- B. GCM
- C. ECB
- D. OFB

58. Roger's digital forensics team places any mobile devices collected as evidence in bags such as the one shown here. What is the primary purpose of this bag?



Figure 8.11

- A. Prevent communication with the device.
 - B. Maintain the chain of custody.
 - C. Categorize the evidence.
 - D. Prevent others from seeing the evidence.
59. Mike would like to allow users on his network to securely access their personal Gmail accounts using the service's standard interface. What protocol must he allow through his network firewall to Google's servers to allow this access?
- A. IMAP
 - B. SMTP
 - C. HTTPS
 - D. POP3
60. Taylor is building a server where data will be infrequently written but frequently read. He would like to use a redundant storage solution that maximizes read performance. Which one of the following approaches would best meet his needs?
- A. RAID 0
 - B. RAID 1
 - C. RAID 3
 - D. RAID 5

61. In the following diagram, what type of attack is Mal waging against Alice?

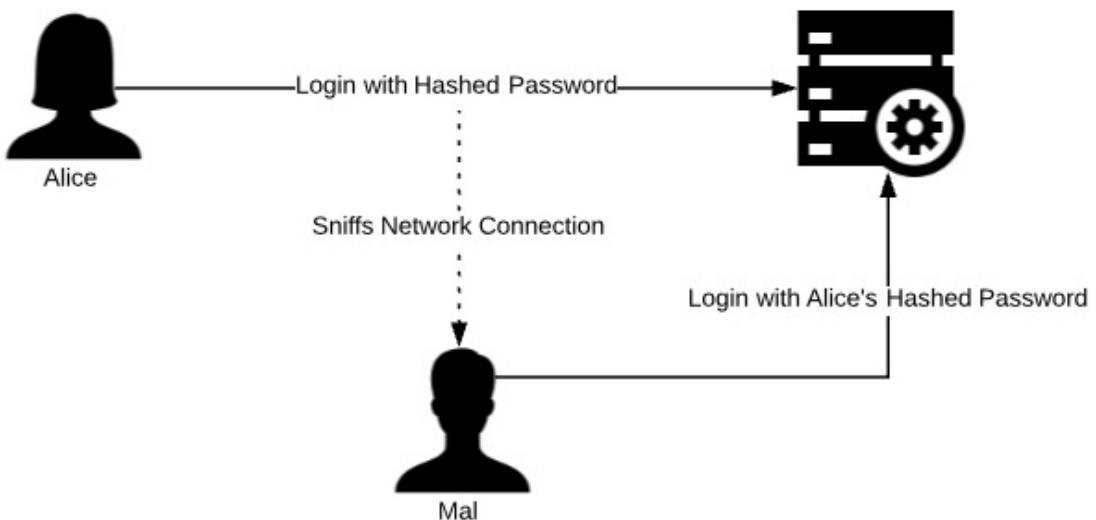


Figure 8.12

- A. Man-in-the-middle
 - B. Social engineering
 - C. Replay attack
 - D. Dictionary
62. Which one of the following statements is true about NTLM authentication?
- A. NTLMv2 is protected against pass-the-hash attacks that exist in the original version of NTLM.
 - B. NTLM uses SHA-512 hashing to protect passwords.
 - C. NTLM and NTLMv2 are both insecure and should not be used.
 - D. NTLM is only available for Windows systems.
63. When a certificate authority creates a digital certificate for a web server, what key does it use to apply the CA's digital signature to the certificate?
- A. Server's private key
 - B. CA's public key
 - C. CA's private key
 - D. Server's public key

64. Which one of the following authentication techniques generally provides the least degree of security for a mobile device?
- A. Password authentication
 - B. Fingerprint authentication
 - C. PIN authentication
 - D. Facial recognition

65. Mike stores some sensitive passwords in a text file called mypasswords.txt. The permissions for this file are shown here. Mike's user ID is mchapple. Which statement best describes the access permissions for this file?

```
drwxr-xr-x    3 mchapple  staff   96 Sep 27 08:54 .
drwxr-xr-x+ 117 mchapple  staff  3744 Sep 27 08:54 ..
-rw-r--r--    1 mchapple  staff   104 Sep 27 08:54 mypasswords.txt
```

Figure 8.13

- A. Anyone on the system can read the file.
 - B. Only Mike can read the file.
 - C. Mike and any member of the staff group can read the file.
 - D. Only Mike and system administrators can read this file.
66. In what type of attack does the attacker place malicious content on a website that is frequented by individuals in the target organization in the hopes that one of those individuals will visit the site with a vulnerable system and become compromised?
- A. Man-in-the-middle attack
 - B. DDoS attack
 - C. Watering hole attack
 - D. Man-in-the-browser attack

67. During a vulnerability scan of an internal web application, Christine discovers the issues shown in the following screenshot. What action should she recommend to correct the issue while minimizing cost and labor?

- ▶  2 SSL Certificate - Self-Signed Certificate
- ▶  2 SSL Certificate - Subject Common Name Does Not Match Server FQDN
- ▶  2 SSL Certificate - Signature Verification Failed Vulnerability

Figure 8.14

- A. Replace the certificate with a certificate from a third-party CA.
 - B. Replace the certificate with a certificate from the same source.
 - C. No change is required. These are false positive reports.
 - D. Replace the certificate with a certificate supporting stronger encryption.
68. Consider the statistics shown here for a biometric authentication system. What is the system's FAR based upon this data?

	Authorized User	Unauthorized User
Accept	98	16
Reject	2	84

Figure 8.15

- A. 1%
- B. 2%
- C. 8%
- D. 16%

69. Examine the digital certificate shown here. How many intermediate CAs were involved in the creation of this certificate?

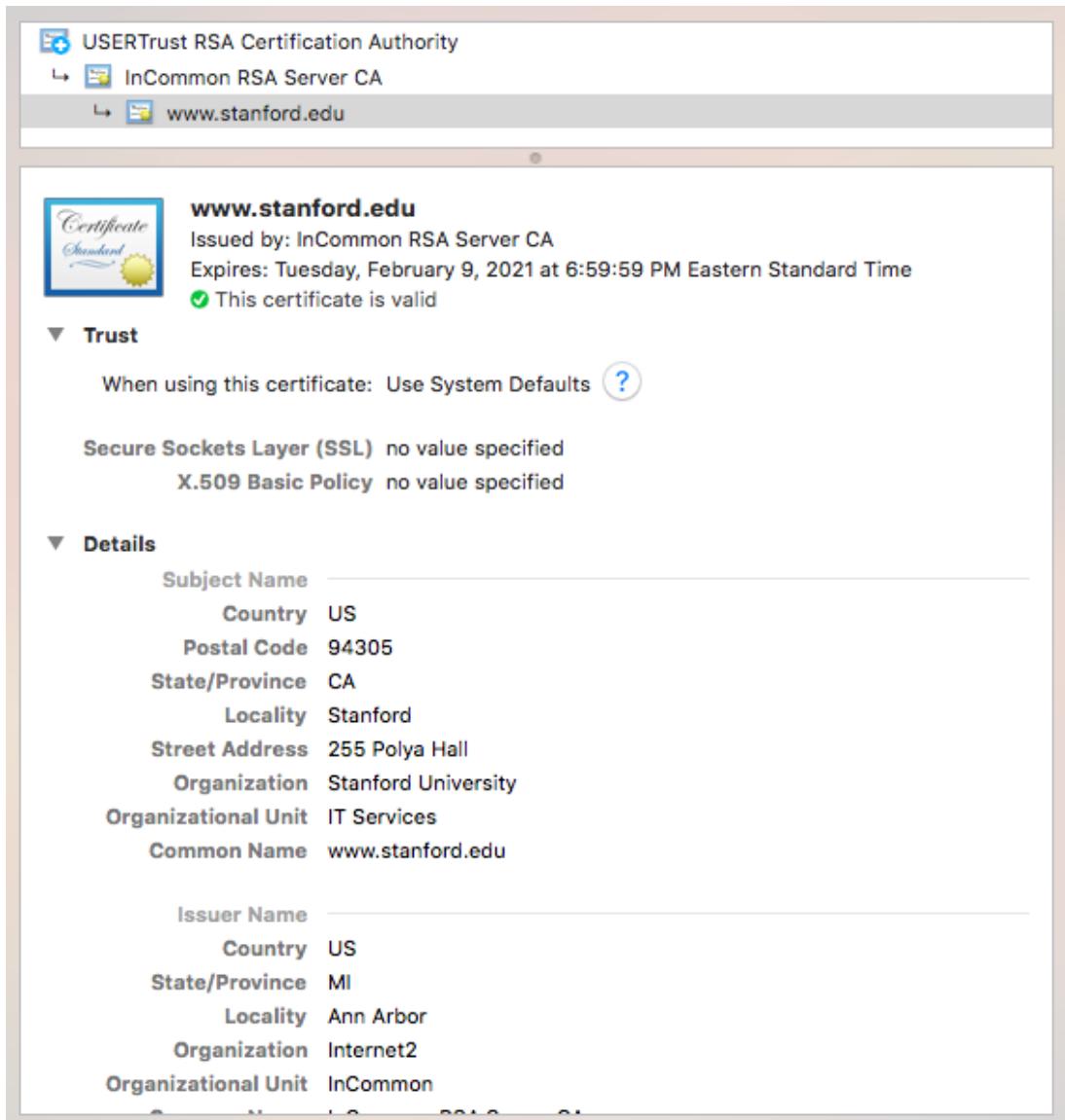


Figure 8.16

- A. 0
- B. 1
- C. 2
- D. 3

70. Frank is revising an application that currently stores Social Security numbers in a database. This is the only unique identifier available to him but he would like to store it in a way that nobody can determine the original Social Security numbers, but it remains useful as a unique identifier. What technology can Frank apply to best meet this requirement?
- A. Steganography
 - B. Encryption
 - C. Decryption
 - D. Hashing
71. Roger's company did not have a strong disaster recovery plan and suffered a catastrophic data center outage. With no plan in place, what option likely allows them the quickest recovery at their primary site?
- A. Warm site
 - B. Hot site
 - C. Mobile site
 - D. Cold site
72. Henrietta is concerned about the possibility that an attacker will obtain a copy of her password file and conduct a rainbow table attack against it. What technique can she use to best prevent this type of attack?
- A. Salting
 - B. Hashing
 - C. Password complexity requirements
 - D. Encryption
73. Flora is conducting a penetration test of a client and wishes to gain physical access to the building during daylight hours. Which one of the following techniques is least likely to arouse suspicion?
- A. Pretexting
 - B. Lock picking
 - C. Tailgating
 - D. Climbing in an open window

74. Andrea was investigating the IP address(es) associated with a domain name and obtained the results shown in the following screenshot. What tool did she use to obtain these results?

```
; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 20426
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;certmike.com.           IN      A

;; ANSWER SECTION:
certmike.com.        1799    IN      A      162.255.119.225

;; Query time: 118 msec
;; SERVER: 66.205.160.99#53(66.205.160.99)
;; WHEN: Wed Aug 22 11:16:43 EDT 2018
;; MSG SIZE  rcvd: 57
```

Figure 8.17

- A. dig
 - B. nslookup
 - C. dnsquery
 - D. resolve
75. Which one of the following objects, if successfully stolen, would be most useful in a session hijacking attack?
- A. IP address
 - B. Public key
 - C. Digital certificate
 - D. Cookie

76. Dan recently received a digitally signed message and when he attempted to verify the digital signature received an error that the hash values did not match. What can Dan conclude from this error?
- A. The message was accidentally corrupted in transit.
 - B. The message was altered by a malicious individual after being sent.
 - C. Dan can't draw one of these specific conclusions.
 - D. There was an error creating the digital signature.
77. Which one of the following technologies can be used to mitigate the effects of a denial-of-service attack on a local area network?
- A. Flood guard
 - B. Loop prevention
 - C. Split horizon
 - D. Hold-down timers
78. Melanie is the system administrator for a database containing sensitive information. She is responsible for implementing security controls to protect the contents of the database. Which term best describes her role?
- A. Data owner
 - B. Data steward
 - C. Data user
 - D. Data custodian

79. Greg visits a website and sees the error shown in the following screenshot. What is the most likely cause of this error message?

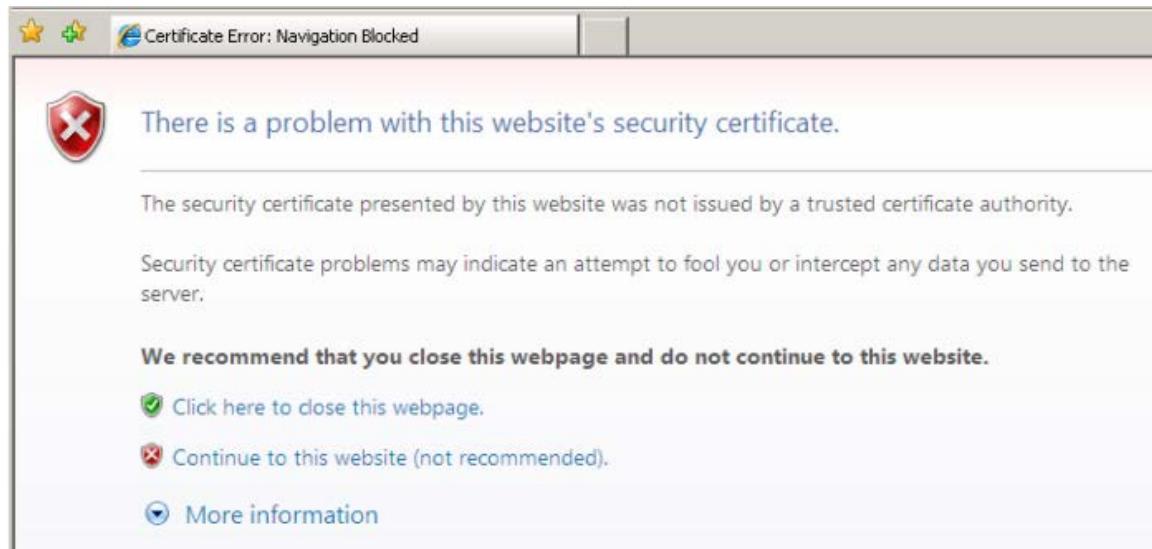


Figure 8.18

- A. The certificate uses an insecure cipher, such as DES.
- B. The website is using a self-signed certificate.
- C. The certificate is expired.
- D. The certificate does not support TLS communication.
80. Brendan is helping a colleague troubleshoot a connectivity issue for two systems using the Secure File Transfer Protocol (SFTP). He would like to check whether the traffic is being blocked by his network firewall. What TCP port is used for these connections?
- A. 22
- B. 21
- C. 20
- D. 23

81. Ben finds that the DNS servers in his organization are configured to allow unrestricted recursive queries. What type of attack are these servers vulnerable to as a result of this configuration?
- A. ARP poisoning
 - B. CDNS poisoning
 - C. DNS amplification
 - D. Man-in-the-middle
82. In a Kerberos authentication scheme, who provides the client with the TGS session key?
- A. Authentication server
 - B. Ticket granting server
 - C. Service server
 - D. Key generation server
83. Ron would like to implement a security control that requires that employees protect the confidentiality of corporate information, even after they leave the organization. Which one of the following agreements would best meet his needs?
- A. SLA
 - B. NDA
 - C. BPA
 - D. ICA
84. Norma has held several positions in her company and is still able to carry out system actions that were granted to her based upon her previous roles. She no longer has a job-based requirement to perform those activities. What term describes what has happened here?
- A. Privileged account
 - B. Least privilege
 - C. Privilege creep
 - D. Privilege migration

Questions 85–90 refer to the following scenario:

Melanie is conducting a quantitative risk assessment for her organization. She is specifically focusing on the risk of an earthquake damaging her Southern California data center. After consulting geologists, she estimates that her area is likely to experience a significant earthquake once every 50 years.

Melanie asked an architect to help her develop a replacement cost estimate for the facility and determined that the cost is \$5 million. She also consulted a structural engineer who estimated that a typical earthquake would cause approximately \$1 million in damage to the facility. An earthquake insurance policy would require payment of a \$75,000 annual premium.

85. What is the asset value in this scenario?

- A. \$20,000
- B. \$75,000
- C. \$1,000,000
- D. \$5,000,000

86. What is the single loss expectancy in this scenario?

- A. \$20,000
- B. \$75,000
- C. \$1,000,000
- D. \$5,000,00

87. What is the annualized rate of occurrence in this scenario?

- A. 0.02
- B. 0.05
- C. 0.20
- D. 0.50

88. What is the exposure factor in this scenario?

- A. 0.02
- B. 0.05
- C. 0.20
- D. 0.50

89. What is the annualized loss expectancy in this scenario?
- A. \$20,000
 - B. \$75,000
 - C. \$1,000,000
 - D. \$5,000,000
90. Which one of the following statements best describes the risk situation Melanie is in?
- A. Melanie should recommend that the business always purchases insurance for any risk with an ALE greater than 0.005.
 - B. The purchase of insurance in this scenario is not cost-effective from a purely financial viewpoint.
 - C. The purchase of insurance in this scenario makes good financial sense.
 - D. Melanie should recommend against the purchase of insurance because the SLE is less than the AV.

Practice Exam 2 Answers and Explanations

1. C. Ralph is conducting a privilege audit by ensuring that each permission assigned to a user account is backed by an approved access request. Usage auditing is a similar activity but it analyzes actual privilege usage, rather than privilege existence.
2. C. Tom can use screen locking to prevent someone walking by from using a device that he or she is not authorized to use. Remote wiping is not an effective control for this scenario, as it would destroy all data on the device and is only effective when actively triggered. Geofencing is not an effective control because the device is located in the office where it is expected to be. Application control would limit the applications that users can install on the device but would not prevent an unauthorized user from accessing the device.
3. B. The recovery time objective (RTO) is the amount of time that it is acceptable for a system to be down prior to recovery during a disaster. The recovery point objective (RPO) is the amount of acceptable data loss during a recovery effort. The RTO and RPO are targets, rather than measures of actual performance. The mean time between failures (MTBF) is the average amount of time that elapses between failures of a system or component. The mean time to repair (MTTR) is the amount of time that it takes to recover a failed system. The MTBF and MTTR are measures of actual performance.

4. C. The recovery time objective (RTO) is the amount of time that it is acceptable for a system to be down prior to recovery during a disaster. The recovery point objective (RPO) is the amount of acceptable data loss during a recovery effort. The RTO and RPO are targets, rather than measures of actual performance. The mean time between failures (MTBF) is the average amount of time that elapses between failures of a system or component. The mean time to repair (MTTR) is the amount of time that it takes to recover a failed system. The MTBF and MTTR are measures of actual performance.
5. D. The secure shell (SSH) functions in a manner that is functionally equivalent to telnet but adds encryption and other security features. SSL and TLS may be used to encrypt communications but they do not provide the connection features of SSH on their own. The file transfer protocol – secure (FTPS) is used for transferring files and does not allow interactive administrative sessions similar to the ones provided by telnet.
6. A. The Data Encryption Standard (DES) is a weak algorithm that is no longer considered secure. The Triple DES (3DES) algorithm is a stronger variant of DES that is acceptable. The Advanced Encryption Standard (AES) and Rivest Shamir Adelman (RSA) algorithm are both considered secure.
7. B. This is a reverse proxy because the proxy server is located on the same network as the web server. Users connect directly to the reverse proxy and the proxy server then connects to the web server. This process is transparent to the end user. It is not possible to determine whether this proxy server is performing caching and/or content filtering based upon this illustration.
8. B. Network access control lists are examples of rule-based access control because the router will make decisions based upon the rules that Fred provides. The router does not know the identity of the user, so it cannot perform role-based or attribute-based access control. Users have no authority to delegate access control decisions, so this is not an example of discretionary access control.
9. B. XYZ Cloud Services is allowing Sandy to provision servers on his own, as he needs them. This is an example of providing customers with the basic building blocks of a computing environment as a cloud service and, therefore, is an example of infrastructure as a service (IaaS).
10. D. In a true positive report, the system reports an attack when an attack actually exists. A false positive report occurs when the system reports an attack that did not take place. A true negative report occurs when the system reports no attack and no attack took place. A false negative report occurs when the system does not report an attack that did take place.

11. A. While it is possible to perform error handling with a variety of constructs, the most appropriate tool is the use of the try...catch construct. In this approach, developers include the code that might generate an error in the try clause and then provide error handling code in the catch clause.
12. B. The EAP-TLS, EAP-TTLS, and EAP-FAST protocols all use transport layer security (TLS) to provide security for the EAP session. EAP-IKEv2 relied upon the Internet Key Exchange (IKE) protocol.
13. C. The most likely culprit is an insider with access to the accounting system. There are no signs of IPS or firewall anomalies, which reduces the likelihood that this was an external attack.
14. D. Carla has already completed the initial exploitation phase of the test. She is now attempting to expand her permissions on the compromised system. This is an example of escalation of privilege.
15. C. Servers that provide services only to internal users should be placed on the intranet. DMZ servers provide services to the general public. Extranet servers may be accessed by vendors and other business partners. Guest networks are designed for visitors to a facility to gain internet access.
16. B. Over-the-air (OTA) upgrades occur automatically and without user or administrator intervention, making them the best way to ensure that devices remain current. If Samantha wants to control when these updates occur, she can manage OTA updates through her mobile device management (MDM) platform. Manual installation or sideloading by users or administrators is not likely to keep devices consistently updated.
17. A. Pulverizing materials reduces them to a fine dust, which may pose an inhalation hazard. Anyone working around pulverized materials should wear a respirator.
18. C. ARP spoofing attacks occur by poisoning the MAC address table either on an individual host or on the switch used by the victim. In order for this attack to be successful, the attacker and victim must be attached to the same switch, although they do not need to be sharing the same switch port.
19. C. The MD5 algorithm is cryptographically broken and should never be used for secure applications, such as creating a digital signature. It is still appropriate for use in non-cryptographic applications, such as identifying duplicate records, partitioning database keys, and verifying file checksums to detect unintentional corruption.

20. A. This is an example of a preset lock, where a locksmith sets the lock to work with a specific key or keys. Cipher locks use a keypad that requires individuals to enter a code. Biometric locks use fingerprint readers or some other form of biometric identification, while smartcard locks require the user to insert a smartcard or place one in the immediate proximity of the lock.
21. C. The Bcrypt algorithm relies upon the Blowfish cipher to perform key stretching of passwords.
22. B. This is a brute force attack because the intruder seems to be generating possible passwords sequentially without using a dictionary or rainbow table. It is an online attack because the intruder is conducting the hacking attempt against the live service.
23. B. Penetration tests interact with systems and seek to exploit vulnerabilities. Therefore, they are an active test of security controls. Configuration analysis, network monitoring, and intrusion detection are passive activities.
24. A. Jailbreaking a mobile device breaks the user out of the controls imposed by the operating system developer, granting the user root privileges on the device. This is an example of privilege escalation. Sideload is the process of loading information on a device via USB or another non-wireless mechanism. It is a capability included in devices by design and is not an example of privilege escalation. Man-in-the-middle attacks are used to eavesdrop on network connections and do not require privilege escalation. Tethering is an intended capability of mobile devices that allow users to connect other devices to the network through the mobile device's network connection.
25. B. Amazon's Lambda service is a serverless computing platform offered to customers on a platform-as-a-service (PaaS) basis. Microsoft Azure Virtual Machines and Amazon EC2 are both virtual server environments that offer infrastructure-as-a-service (IaaS). Microsoft Azure DNS is also an infrastructure service offering for name resolution.
26. A. Fuzzing uses artificially generated input to a program to test it for security purposes. Fuzzing executes the code, so it is an example of dynamic code analysis. Data flow analysis, lexical analysis, and taint analysis are all examples of static code-testing techniques.

27. C. In a public cloud environment, providers offer services on the same shared computing platform to all customers. Customers do not necessarily have any relationship to, or knowledge of, each other. In a private cloud environment, an organization builds its own computing environment. In a hybrid cloud environment, an organization combines elements of public and private cloud computing. In a community cloud environment, a group of related organizations builds a shared cloud environment that is not open for general public use. Despite the fact that David is limiting access to these servers to his own organization, Microsoft Azure is still a public cloud computing environment.
28. C. Aircrack is specifically designed to test the security of WiFi encryption keys and would be the ideal tool in this situation. NetStumbler is an outdated tool used to survey wireless networks but is no longer supported. Nmap is a network mapping tool and QualysGuard is a network vulnerability scanner, neither of which has a wireless encryption testing capability.
29. B. The developer created a backdoor in the system by hardwiring credentials into the application that allowed later access. A logic bomb is set to automatically trigger when certain conditions are met, which is not the case in this scenario. A remote access Trojan (RAT) is a type of malware that establishes a backdoor but there is no indication that one was used in this case, as the engineer added the backdoor directly into the code. Ransomware is a form of cryptomalware that encrypts files and then demands payment of a ransom before restoring access. There is no indication of a ransomware attack in this scenario.
30. B. The Simple Mail Transfer Protocol (SMTP) is used to relay inbound emails and should be allowed from the internet. The Internet Message Access Protocol (IMAP) and the Post Office Protocol version 3 (POP3) are used to retrieve messages from an email server and should only be allowed from the internal network.
31. C. The RADIUS Access-Request message is sent by a client to the server requesting RADIUS authentication. The server then normally responds with an Access-Accept or Access-Reject message, depending upon whether the authentication was successful or unsuccessful. When a system is using two-factor authentication, the RADIUS server may respond to the client's request with an Access-Challenge message asking for additional authentication.

32. A. The individual who set up this website registered a domain name that was extremely similar to a legitimate domain: arifrance.com instead of airfrance.com. This is an example of typosquatting (or URL hijacking), an attack that hopes to garner web traffic by having a name that is quite similar to that of a legitimate site. This is a different website than the legitimate site, so no defacement took place. In a clickjacking attack, the attacker seeks to fool individuals into clicking links on a website. In a session hijacking attack, the attacker attempts to interfere with ongoing communication between a client and web server.
33. B. Router access control lists are only capable of performing stateless filtering, which does not take connection status into account. Other firewall technologies, including stateful inspection firewalls, next-generation firewalls, and proxy firewalls, all track connection state and typically require dedicated firewall hardware.
34. C. The basic File Transfer Protocol (FTP) does not provide encryption for data in transit and exposes both transferred files and authentication credentials to eavesdropping attacks. The Secure File Transfer Protocol (SFTP) and File Transfer Protocol – Secure (FTPS) offer the same functionality over a secure, encrypted connection. The Secure Copy (SCP) protocol copies files over a secure SSH connection and is also a viable alternative to FTP.
35. A. While it is possible that Tom scanned the wrong IP address or that these are false positive results, the most likely explanation is that the copy machine contains an embedded Windows operating system that is vulnerable to these issues. True negative reports occur when a scanner does not report an issue that does not exist; therefore, they would not appear in a scan report.
36. C. Active/active mode is a perfectly acceptable way to operate two load balancers and the load balancers will take care of synchronization issues between themselves and the servers. The major risk with active/active mode is that if both load balancers run at greater than 50% capacity, a single load balancer will not be able to handle the full workload in the event that one device fails.
37. B. Stream ciphers work on a single bit or byte of plaintext at a time, while block ciphers work on plaintext in chunks. AES and Blowfish are examples of block ciphers.

38. D. This illustration shows the cipher feedback (CFB) mode of encryption. You can determine this by noting that in each encryption operation, the ciphertext from the previous operation is encrypted and then XORed with the plaintext block to produce the next ciphertext block.
39. A. Nessus is a vulnerability scanner designed to scan systems over the network and identify potential vulnerabilities. Nmap performs a similar function but only identifies open ports on remote devices without probing for vulnerabilities. Jack the Ripper is a password cracking tool. Kismet is a wireless network assessment tool.
40. C. In a bring-your-own-device (BYOD) model, employees are able to bring personally owned devices into a corporate computing environment. The other models listed all involve the use of corporate-owned equipment.
41. A. Roger is installing a back door so that he can regain access to the system at a later date. This is an example of persistence. He will be able to use this back door to regain access even if the initial vulnerability that he exploited is patched.
42. C. While it may be possible to mitigate this issue by adjusting the settings on any of the devices mentioned here, the root cause of a SQL injection vulnerability is faulty input validation in the application's source code. This root cause may only be addressed by modifying the application code.
43. A. The proximity card provides the fastest scanning time, as the user simply needs to hold it near the reader. Smart cards and magnetic stripe cards require more time-consuming interaction with the reader. Photo ID cards require scrutiny by a human guard.
44. A. In a pass-the-hash attack, the attacker must gain access to a hashed Windows account passwords. This is possible by gaining access to a Windows workstation where the target user logs into his or her domain account. Access to a domain controller is not necessary. Access to a network segment or public website is not sufficient because hashed passwords are not generally found in those locations in unencrypted form.
45. D. The accuracy of a biometric authentication system is described using three metrics. The false acceptance rate (FAR) is the frequency at which the system admits a person who should not be admitted. The false rejection rate (FRR) is the frequency at which the system denies access to an authorized user incorrectly. The FAR can be improved by increasing the sensitivity of the system, while the FRR can be improved by decreasing the sensitivity of the system. Because of this, the best measure of accuracy is the crossover error rate (CER), which is the sensitivity point at which the FAR and FRR are equal.

46. B. Development environments are designed for active use by developers who are creating new code. These environments are the only location where code should be modified. Once code is ready for testing, it is released from the development environment into a test environment for software testing. After the completion of user acceptance testing, the code is moved from the test environment into a staging environment where it is prepared for final deployment into the production environment. Developers should never have permission to move code themselves but should only be able to move code between environments through the use of a managed change control system.
47. B. The Diffie-Hellman (DH) algorithm is a key exchange algorithm designed to facilitate the creation of a mutually shared secret.
48. C. An Agile approach to software development embraces change and prioritizes feature requests by the value added to the deliverable. Customers are encouraged to engage throughout the process. Agile projects often begin without clearly defined requirements and requirements evolve as the project unfolds.
49. B. This approach, redirecting users to a central authentication service, is an example of single sign-on (SSO), where a user authenticates once and may use that authenticated session to access a variety of services. While this authentication may be part of a federated environment, there is no indication of this and there is no description of the specific technologies used to support this SSO environment.
50. B. The WPA-Enterprise and WPA2-Enterprise standards both rely upon an enterprise authentication server. Pre-shared key (PSK) mode uses a shared secret key. WPS is not a wireless encryption standard.
51. C. The Federal Financial Institutions Examination Council (FFIEC) is responsible for overseeing the audits of financial institutions and produces a series of information security standards that apply to those institutions. The Federal Energy Regulatory Commission (FERC) produces security standards for the energy industry. The Food and Drug Administration (FDA) regulates healthcare products and food items, while the Federal Railroad Administration (FRA) regulates rail transportation.
52. C. An intrusion detection system (IDS) has the ability to identify suspicious network traffic but cannot take any preventive action to block the traffic. Therefore, it is best classified as a detective control.
53. B. Recent attacks against WPS have rendered it insecure and made it unsuitable for use. Xavier should discontinue the use of WPS and switch to a more secure authentication and access control technology.

54. C. Most embezzlement attacks are waged either entirely by insiders or with significant support from an insider with access to the organization's financial systems and accounts.
55. C. The two main technologies used to generate one-time passwords are the HMAC-Based One Time Password (HOTP) algorithm and the Time-Based One Time Password (TOTP) algorithm. HOTP passcodes are generated sequentially and do not expire until use. TOTP passcodes are based upon the time of authentication and expire frequently. This hardware token requires that the user press a button to generate a passcode sequentially, rather than generating them continuously. Therefore, it is an HOTP token.
56. B. Generic, shared, and guest accounts should not be used on secure servers due to their lack of accountability to an individual user. Service accounts normally exist on all servers and are required for routine operation of services.
57. B. This image shows the Galois/Counter Mode (GCM) cipher mode of operation. The distinguishing feature of this approach is that block numbers are generated by a counter and those numbers are combined with an initialization vector using a block cipher.
58. A. While this bag may be used to perform all of the functions listed in the question, the primary purpose of this bag is to serve as a portable Faraday cage that prevents electromagnetic signals from reaching the device. This allows the forensic analysts to leave the device powered on without worrying that someone will remote wipe the device. Powering the device off may lose critical evidence stored in memory.
59. C. The standard access mechanism for Gmail accounts is to use a web browser over a secure connection. This traffic occurs using the HTTPS protocol. While it is possible to access Gmail through the SMTP, IMAP, and POP3 protocols, the basic version of those protocols are not secure and do not use the standard web interface. There are secure, encrypted alternatives to SMTP, IMAP, and POP3, but those still do not use the Gmail web interface.
60. B. RAID 1, also known as disk mirroring, writes identical data to two disks. This approach allows read operations to recover all data by accessing a single disk and is quite efficient for that use. RAID 3 and RAID 5 stripe data across multiple disks and incur overhead in reassembling information that reduces read performance. RAID 0 does not provide redundancy, as it simply stripes data across multiple disks without parity information.
61. C. In this attack, Mal is obtaining Alice's hashed password by sniffing the network connection. He then reuses the hashed password to log in to the service. This is an example of a replay attack.

62. C. NTLM and NTLM v2 both contain critical security vulnerabilities that make them poor choices for authentication protocols. They use the MD4 and MD5 hash algorithms. While NTLM is most commonly found on Windows systems, there are NTLM implementations for Linux systems as well.
63. C. The purpose of a CA signing a certificate is to prove that the CA was involved in the certificate's creation. The CA uses its own private key to create the digital signature and then other users may verify the signature using the CA's public key.
64. C. Facial recognition and fingerprint-based authentication both use acceptably strong biometric authentication techniques. The remaining two options, passwords and PINs, both use knowledge-based authentication. Passwords allow users to select from a wider range of characters than PINs, which only allow the use of digits. Therefore, PINs provide the weakest level of security of all of these techniques.
65. A. The three "r" values in this permission string indicate that the file's owner can read the file, members of the file's group can read the file, and all system users can read the file. Therefore, anyone on the system has permission to read this file.
66. C. Watering hole attacks take advantage of the fact that many people are predictable in their web surfing patterns. They place malicious content at a site likely to attract the target audience (the watering hole) and then wait for a compromise to occur.
67. B. This is an internal application, so the use of a self-signed certificate is likely appropriate. However, this certificate issued for an incorrect domain name and, therefore, should be replaced. Using a certificate from the same self-signing source will minimize costs compared to the use of a third-party CA. There is no sign in this report that the certificate does not support strong encryption.
68. C. The false acceptance rate (FAR) of a system is calculated by dividing the number of false acceptances by the total number of authentication attempts. In this dataset, there are 200 total authentication attempts, of which 16 were false acceptances of an unauthorized user. Therefore, the false acceptance rate is 8%.
69. B. This certificate was issued by an intermediate CA known as the InCommon RSA Server CA. This intermediate CA was certified by the USERTrust RSA Certification Authority root CA.
70. D. Hashing would allow Frank to create a unique value from each SSN that would still uniquely identify each record but would not be reversible by anyone. Encryption would also protect the data but could be reversed by someone with the decryption key. Steganography is used to hide data within images.

71. C. Cold sites have only basic infrastructure available and require the longest period of time to activate operations. They are also the cheapest option. Warm sites add hardware, and possibly software, to the mix but do not have a current copy of the data running. They require hours to activate. Hot sites are up and running at all times and can assume operations at a moment's notice. They are the most expensive option. Mobile sites are transportable on trailers and are a good choice for a last-minute recovery plan. They would work well in this scenario because Roger could bring a mobile site to their primary facility and use it to recover operations during the restoration effort at the primary site.
72. A. While all of these techniques will help reduce the likelihood of a password cracking attack, the best defense against rainbow tables is to implement salting. Rainbow table attacks precompute hashes and then check the password file for those values. Salting adds a value (the salt) to each password prior to hashing to make rainbow table attacks no more effective than a brute force attack.
73. C. During a tailgating attack, the attacker simply blends in with a crowd of people entering a facility and hopes they will hold the door open for him or her. This is the least likely way to arouse suspicion during daylight hours when the office is occupied. Lockpicking, pretexting, and climbing in a window are all likely to attract unwanted attention.
74. A. Both the **dig** and **nslookup** tools are useful when seeking to determine the IP address(es) associated with a domain name. However, the results shown in the figure are formatted as output from the dig tool. Dnsquery and resolve are not domain lookup tools.
75. D. If an eavesdropper gains access to the cookie used to authenticate a session, the attacker could use that cookie to take over the session. Public encryption keys, digital certificates, and IP addresses are all commonly shared publicly and would not be very useful in a session hijacking attack.
76. C. Any one of these scenarios is a plausible reason that the digital signature would not verify. Dan cannot draw a specific conclusion other than that the message he received is not the message that was sent by the originator.
77. A. Flood guard prevents a single device from flooding the network with traffic, which may cause a denial of service. Loop prevention, hold-down timers, and split horizon routing are all used to detect and correct routing loops.
78. D. System administrators are examples of data custodians: individuals who are charged with the safekeeping of information under the guidance of the data owner.

79. B. This error message indicates that the certificate was not issued by a trusted certificate authority. This error most often occurs when a certificate was self-issued.
80. A. The SFTP protocol uses SSH connections to transfer files securely. Therefore, it works over the same port used by SSH, TCP port 22. Ports 20 and 21 are used for traditional FTP connections and would not apply here. Port 23 is used by the insecure Telnet protocol.
81. C. In a DNS amplification attack, the attacker sends short queries to servers that allow unrestricted recursive queries. Those queries include forged source addresses, causing the third-party DNS servers to unwittingly flood the victim system with lengthy and unsolicited DNS responses.
82. A. When a Kerberos client requests a session key, the client creates an authenticator consisting of the client's ID and a timestamp. The client then encrypts this authenticator with the TGS session key, which the client obtained earlier from the authentication server.
83. B. A non-disclosure agreement (NDA) is a confidentiality agreement between two organizations or between an individual and an organization. NDAs are commonly used to enforce employee confidentiality and typically remain in effect after the end of an employment relationship.
84. C. Privilege creep is the term used to describe the situation where a user moves through various job roles and accumulates permissions over time without having unnecessary permissions revoked. Privilege creep is a violation of the principle of least privilege.
85. D. The asset value (AV) is the full value of the facility. In this scenario, Melanie consulted with an architect and determined that the facility value is \$5 million using the replacement cost method.
86. C. The single loss expectancy (SLE) is the amount of damage, in dollars, that the organization should expect as the result of a single incident. From the scenario, we know that a single earthquake would cause approximately \$1 million in damage.
87. A. The annualized rate of occurrence is the number of events expected in a given year. Geologists expect an earthquake once every 50 years. This is equivalent to a 0.02 annual risk of an earthquake.
88. C. The exposure factor is calculated by dividing the single loss expectancy (\$1,000,000) by the asset value (\$5,000,000), resulting in a value of 0.20, or 20%.

89. A. The annualized loss expectancy is the amount of damage expected to occur in any given year. It is computed by multiplying the single loss expectancy by the annualized rate of occurrence (or $ALE=SLE*ARO$). In this scenario, that is $ALE=\$1\text{ million} * 0.02$ or $\$20,000$.
90. B. The purchase of an insurance policy is never purely a financial decision; however, in this case, it does not make good financial sense because the annualized loss expectancy ($\$20,000$) is less than the policy premium cost ($\$75,000$). Tonya should not use the ALE or SLE alone to make this decision and must do so in the context of the control costs and other business factors.

