Student Study Guide and Assessment Bank

CompTIA Security+ Guide to Network Security Fundamentals

Chapter 1: Introduction to Security

Section A: Chapter Summary

Key Concepts

- **Information Security Definition:** The process of securing digital information (manipulated by a processor, stored on a device, or transmitted over a network) to protect it from harm.
- **The CIA Triad:**
  - **Confidentiality:** Ensures that only authorized parties can view the information.
  - **Integrity:** Ensures that the information is correct and no unauthorized person or malicious software has altered the data.
  - **Availability:** Ensures that data is accessible to authorized users when needed.
- **Security vs. Convenience:** There is an inversely proportional relationship between security and convenience; as security increases, convenience typically decreases.
- **Threat Actors:**
  - **Script Kiddies:** Unskilled individuals who use automated tools/scripts written by others.
  - **Hacktivists:** Attackers motivated by ideology or principles.
  - **State Actors:** Government-sponsored attackers targeting foreign governments or corporations for espionage or sabotage (often associated with Advanced Persistent Threats or APTs).
  - **Insiders:** Employees, contractors, or partners who pose a threat from within the organization.
  - **Competitors:** Launch attacks to steal proprietary information for financial gain.
- **Social Engineering:** Psychological manipulation of people into performing actions or divulging confidential information.
  - **Phishing:** Sending fraudulent emails appearing to be from reputable sources.
  - **Vishing (Voice Phishing):** Phishing conducted via phone calls.
  - **Smishing (SMS Phishing):** Phishing conducted via text messages.
  - **Whaling:** Phishing targeting high-profile individuals (e.g., CEOs).
- **Physical Social Engineering:** Includes dumpster diving (searching trash for data), tailgating (following an authorized person into a secure area), and shoulder surfing (watching someone enter credentials).

Section B: Test Bank

I. Multiple Choice

1. Which element of the CIA Triad ensures that data has not been altered by unauthorized persons?

   (a) Confidentiality
   (b) Availability
   (c) Authentication
   (d) Integrity

   Answer: d

2. Which type of threat actor lacks technical expertise and relies on automated tools written by others?

   (a) State Actor
   (b) Script Kiddie
   (c) Hacktivist
   (d) Insider

   Answer: b

3. What is the term for a phishing attack that targets a specific group or individual with customized information?

   (a) Whaling
   (b) Spear Phishing
   (c) Vishing
   (d) Smishing

   Answer: b

4. Following an authorized person through a secure door without presenting credentials is known as:

   (a) Dumpster Diving
   (b) Shoulder Surfing
   (c) Tailgating
   (d) Impersonation

   Answer: c

5. Which social engineering principle relies on the victim's desire to be helpful or liked?

   (a) Intimidation
   (b) Scarcity
   (c) Urgency
   (d) Familiarity

   Answer: d

6. State-sponsored attackers are most often associated with which type of threat?

   (a) Script Kiddie attacks
   (b) Advanced Persistent Threat (APT)
   (c) Insider Threat
   (d) Accidental data loss

   Answer: b

7. What type of attack involves digging through trash receptacles to find useful information?

   (a) Dumpster Diving
   (b) Shoulder Surfing
   (c) Tailgating
   (d) Pretexting

   Answer: a

8. A user receives a text message claiming their bank account is locked and asking them to click a link. This is an example of:

   (a) Vishing
   (b) Phishing
   (c) Smishing
   (d) Whaling

   Answer: c

9. Which security layer involves policies, procedures, and awareness training?

   (a) Products
   (b) People
   (c) Procedures
   (d) Perimeters

   Answer: c

10. Which threat actor is motivated primarily by ideology or a cause?

    (a) Cybercriminal
    (b) Hacktivist
    (c) State Actor
    (d) Competitor

    Answer: b

II. True/False

1. Security and convenience are inversely proportional. **Answer: True**
2. Confidentiality ensures that data is accessible to authorized users when needed. **Answer: False** (This is Availability)
3. A ”White Hat” hacker is an ethical attacker who probes systems with permission. **Answer: True**
4. Vishing is a form of phishing that uses email as the primary vector. **Answer: False** (Uses voice/phone)
5. Insiders are often considered a significant threat because they already have authorized access. **Answer: True**
6. Pretexting involves creating a fabricated scenario to steal information. **Answer: True**
7. A zero-day vulnerability is one that is known to the vendor and has a patch available. **Answer: False**
8. Brokers sell their knowledge of vulnerabilities to other attackers or governments. **Answer: True**
9. The ”Urgency” principle in social engineering attempts to give the victim time to think rationally. **Answer: False**
10. Integrity ensures data is correct and unaltered. **Answer: True**

III. Fill-in-the-Blank

1. The three protections of the CIA Triad are Confidentiality, _____, and Availability. **Answer: Integrity**
2. _____ are unskilled attackers who use scripts or programs developed by others to attack computer systems. **Answer: Script kiddies**
3. _____ is the practice of sending emails that appear to be from a legitimate source to trick users into revealing sensitive information. **Answer: Phishing**
4. _____ involves an attacker watching a user enter a password or PIN from a nearby location. **Answer: Shoulder surfing**
5. _____ is a social engineering attack that targets high-profile individuals like CEOs. **Answer: Whaling**
6. The _____ is the relationship between security and convenience; as one increases, the other decreases. **Answer: Inverse relationship**
7. _____ actors are government-sponsored attackers who launch cyberattacks against the foes of the state. **Answer: State**
8. _____ is the act of unauthorized individuals entering a restricted area by following closely behind an authorized person. **Answer: Tailgating**
9. _____ refers to hiding the existence of data, often within image or audio files. **Answer: Steganography**

10. _____ involves masquerading as a real or fictitious character to trick a victim. **Answer: Impersonation**

IV. Short Answer

1. Define "Information Security." **Answer: The process of securing digital information to protect it from harm, ensuring its integrity, confidentiality, and availability.**
2. What is the difference between a vulnerability and a threat? **Answer: A vulnerability is a flaw or weakness in a system; a threat is an action or event that has the potential to exploit that weakness.**
3. Explain the concept of "Defense in Depth" or "Layered Security." **Answer: Using multiple layers of security controls (products, people, procedures) so that if one fails, others are still in place to protect assets.**
4. What distinguishes a "Gray Hat" hacker from a "Black Hat" hacker? **Answer: A Black Hat hacks for malicious gain; a Gray Hat hacks without permission but often not for malicious destruction, sometimes revealing vulnerabilities publicly.**
5. Describe "Watering Hole" attacks. **Answer: An attack where the aggressor infects a website that a specific group of victims is known to visit.**
6. What is an "Advanced Persistent Threat" (APT)? **Answer: A sophisticated, long-term attack, often state-sponsored, where the attacker establishes a foothold in a network to steal data over time.**
7. Define "Typo Squatting." **Answer: Registering domain names that are very similar to popular domains (e.g., goggle.com) to capture traffic from users who make typing errors.**
8. What is "Social Engineering"? **Answer: The psychological manipulation of people into performing actions or divulging confidential information.**
9. List three principles of social engineering effectiveness. **Answer: Authority, Intimidation, Consensus, Scarcity, Familiarity, Trust, Urgency (Any three).**
10. What is a "Zero Day" attack? **Answer: An attack that exploits a previously unknown vulnerability for which no patch or fix currently exists.**

V. Matching

Terms:

A. Confidentiality
B. Availability
C. Integrity
D. Obfuscation
E. Authentication
F. Nonrepudiation
G. Accounting
H. Authorization
I. Identification
J. Threat Actor

Definitions:

1. Ensures information is correct and unaltered.

2. Ensures only authorized parties can view information.
3. Ensures data is accessible when needed.
4. Making something obscure or unclear.
5. The inability to deny an action.
6. Proving a user is genuine (e.g., password).
7. Granting permission to take action.
8. Review of credentials.
9. Record of user actions.
10. Entity responsible for a cyber incident.

Answers: 1-C, 2-A, 3-B, 4-D, 5-F, 6-E, 7-H, 8-I, 9-G, 10-J

Chapter 2: Threat Management and Cybersecurity Resources

Section A: Chapter Summary

Key Concepts

- **Threat Management:** The process of identifying and responding to potential cyber threats.
- **Penetration Testing (Pen Test):** An authorized simulated cyberattack on a computer system, performed to evaluate the security of the system.
  - **Black Box:** Tester has no prior knowledge of the network.
  - **White Box:** Tester has full knowledge of the network (source code, IP schemes).
  - **Gray Box:** Tester has limited knowledge (e.g., user credentials).
  - **Active Reconnaissance:** Directly probing the system.
  - **Passive Reconnaissance:** Gathering information from open sources (OSINT) without directly interacting with the target.
- **Teams in Pen Testing:**
  - **Red Team:** Attackers (offensive security).
  - **Blue Team:** Defenders (defensive security).
  - **White Team:** Referees/observers.
  - **Purple Team:** Collaboration between Red and Blue teams.
- **Vulnerability Scanning:** Automated process to identify known weaknesses.
  - **Credentialed Scan:** Scanner authenticates to the system (more thorough).
  - **Non-credentialed Scan:** Scanner acts as an outsider.
  - **Intrusive vs. Non-intrusive:** Intrusive attempts to exploit vulnerabilities (risk of disruption); Non-intrusive only identifies them.
- **Cybersecurity Resources:**
  - **NIST (National Institute of Standards and Technology):** Provides frameworks like CSF (Cybersecurity Framework).
  - **ISO (International Organization for Standardization):** Provides standards like ISO 27001.
  - **Regulations:** GDPR (EU privacy), PCI DSS (Credit card security), HIPAA (Health information).
- **Threat Intelligence:** Information about threats and threat actors. Sources include OSINT (Open Source Intelligence), dark web, and closed/proprietary feeds.

Section B: Test Bank

I. Multiple Choice

1. Which penetration testing team is responsible for defending the network?

   (a) Red Team
   (b) Blue Team
   (c) White Team
   (d) Purple Team

   Answer: b

2. A penetration test where the tester has no prior knowledge of the target system is called:

   (a) White Box
   (b) Black Box
   (c) Gray Box
   (d) Clear Box

   Answer: b

3. Which type of vulnerability scan uses valid authentication credentials to scan the system?

   (a) Non-credentialed scan
   (b) Credentialed scan
   (c) Passive scan
   (d) External scan

   Answer: b

4. Which organization publishes the Cybersecurity Framework (CSF)?

   (a) ISO
   (b) IEEE
   (c) NIST
   (d) PCI

   Answer: c

5. What is the primary difference between a vulnerability scan and a penetration test?

   (a) Vulnerability scans are manual; pen tests are automated.
   (b) Vulnerability scans identify weaknesses; pen tests attempt to exploit them.
   (c) Vulnerability scans are illegal; pen tests are legal.
   (d) Vulnerability scans require full knowledge; pen tests require no knowledge.

   Answer: b

6. What does OSINT stand for?

   (a) Operating System Intelligence

(b) Open Source Intelligence
(c) Operational Security Intelligence
(d) Open Standards Integration

Answer: b

7. Which regulation protects the privacy of personal data for European Union residents?

(a) HIPAA
(b) SOX
(c) GDPR
(d) PCI DSS

Answer: c

8. In the context of threat hunting, what is a ”False Positive”?

(a) A vulnerability that is missed by the scanner.
(b) An alert raised when there is no actual problem.
(c) An attack that is successfully blocked.
(d) A scanner failing to run.

Answer: b

9. Which type of reconnaissance involves gathering information without directly interacting with the target system?

(a) Active
(b) Passive
(c) Intrusive
(d) Dynamic

Answer: b

10. The process of actively searching for cyber threats that have evaded existing security defenses is called:

(a) Vulnerability Management
(b) Threat Hunting
(c) Risk Assessment
(d) Penetration Testing

Answer: b

II. True/False

1. A White Box test simulates an insider threat with full knowledge of the system. **Answer: True**
2. Intrusive vulnerability scans attempt to exploit vulnerabilities and may disrupt services. **Answer: True**
3. The Red Team acts as the referee during a penetration test exercise. **Answer: False** (The White Team is the referee)
4. PCI DSS is a regulation governing health insurance portability. **Answer: False** (PCI DSS governs payment cards; HIPAA governs health)
5. Passive reconnaissance engages the target system directly. **Answer: False**
6. A false negative occurs when a scanner fails to identify a real vulnerability. **Answer: True**
7. Threat hunting is a reactive process that waits for alerts to fire. **Answer: False** (It is proactive)
8. The Purple Team creates a bridge between the Red and Blue teams for feedback. **Answer: True**
9. Vulnerability scans should be conducted continuously or on a frequent schedule. **Answer: True**
10. Credentialed scans generally provide less detailed information than non-credentialed scans. **Answer: False**

III. Fill-in-the-Blank

1. _____ is the process of simulating an attack to identify vulnerabilities and attempt to exploit them. **Answer: Penetration testing**
2. The _____ team is responsible for attacking the network in a war game scenario. **Answer: Red**
3. _____ refers to information gathered from publicly available sources. **Answer: Open Source Intelligence (OSINT)**
4. _____ scans allow the scanner to log in to the system to check for internal vulnerabilities. **Answer: Credentialed**
5. The _____ regulation applies to any organization handling credit card information. **Answer: PCI DSS**
6. A _____ is an automated tool used to identify open ports and missing patches. **Answer: Vulnerability scanner**
7. _____ involves pivoting from a compromised system to other systems within the network. **Answer: Lateral movement**
8. _____ provides a framework of security controls for cloud computing. **Answer: Cloud Security Alliance (CSA) / Cloud Controls Matrix**

9. A _____ box test provides the tester with no prior knowledge of the system. **Answer: Black**
10. _____ are monetary rewards offered to researchers who find vulnerabilities in software. **Answer: Bug bounties**

IV. Short Answer

1. Define "Vulnerability Scanning." **Answer: An automated process of identifying and reporting known security weaknesses in systems and networks.**
2. What is the difference between Active and Passive reconnaissance? **Answer: Active interacts directly with the target (e.g., port scanning); Passive gathers info without direct interaction (e.g., OSINT).**
3. Explain the purpose of a "Rules of Engagement" document in penetration testing. **Answer: To define the scope, timing, authorized targets, and limitations of the test to ensure legality and safety.**
4. What is "Threat Hunting"? **Answer: The proactive search for cyber threats that are lurking undetected in a network.**
5. Describe "Privilege Escalation." **Answer: The act of exploiting a bug or design flaw to gain higher-level access (e.g., from user to admin) than intended.**
6. What is "SIEM"? **Answer: Security Information and Event Management; a solution that aggregates and analyzes log data from various sources.**
7. What is the function of the "White Team" in a cybersecurity exercise? **Answer: To act as judges or referees, enforcing rules and observing the exercise.**
8. Why might an organization choose a "Gray Box" penetration test? **Answer: To simulate an attacker with some insider knowledge or to save time in the reconnaissance phase.**
9. What is "SOAR" in the context of threat management? **Answer: Security Orchestration, Automation, and Response; tools that automate incident response workflows.**
10. Define "False Positive" in vulnerability scanning. **Answer: An error where the scanner reports a vulnerability that does not actually exist.**

V. Matching

Terms:

A. NIST

B. GDPR

C. PCI DSS

D. ISO 27001

E. HIPAA

F. CVE

G. CVSS

H. STIX

I. TAXII

J. OSINT

Definitions:

1. Standard for Information Security Management Systems.
2. US Health information privacy regulation.
3. National Institute of Standards and Technology.
4. Common Vulnerabilities and Exposures list.
5. Language format for exchanging threat intelligence.
6. European data privacy regulation.
7. Standard for credit card data security.
8. Scoring system for vulnerability severity.
9. Protocol for exchanging threat intelligence.
10. Intelligence from public sources.

Answers: 1-D, 2-E, 3-A, 4-F, 5-H, 6-B, 7-C, 8-G, 9-I, 10-J

Chapter 3: Threats and Attacks on Endpoints

Section A: Chapter Summary

Key Concepts

- **Malware Classifications:**
  - **Ransomware:** Encrypts data and demands payment for the key.
  - **Cryptomalware:** Similar to ransomware but may run silently to mine cryptocurrency (cryptojacking).
  - **Trojan:** Malicious code disguised as legitimate software.
  - **Worm:** Self-replicating malware that spreads across networks without user interaction.
  - **Botnet:** Network of infected computers (zombies) controlled by a Command and Control (C&C) server.
  - **Rootkit:** Malware that hides deep in the OS to conceal its presence and grant persistent access.
  - **Logic Bomb:** Malicious code triggered by a specific event or time.
  - **Spyware/Keyloggers:** Software that monitors user activity and captures keystrokes.
  - **Fileless Virus:** Operates in memory using native system tools (e.g., PowerShell) to avoid detection.
- **Application Attacks:**
  - **Cross-Site Scripting (XSS):** Injecting malicious scripts into trusted websites to execute on client browsers.
  - **Injection Attacks (SQLi, XML, DLL):** Injecting malicious commands into input fields to manipulate databases or applications.
  - **Buffer Overflow:** Writing data past the buffer boundary to overwrite memory and crash systems or execute code.
  - **Cross-Site Request Forgery (CSRF):** Tricking a user into executing unwanted actions on a web application where they are authenticated.
  - **Replay Attack:** Intercepting and retransmitting data to impersonate a legitimate user.
- **Adversarial Artificial Intelligence:** Attacks that manipulate AI/ML algorithms, such as poisoning training data to cause incorrect classifications.

Section B: Test Bank

I. Multiple Choice

1. Which type of malware disguises itself as legitimate software to trick the user into installing it?

   (a) Worm

   (b) Trojan

(c) Rootkit

(d) Logic Bomb

Answer: b

2. Which attack involves injecting malicious scripts into a website that are later executed by a visitor's browser?

   (a) SQL Injection

   (b) Buffer Overflow

   (c) Cross-Site Scripting (XSS)

   (d) Bluejacking

   Answer: c

3. What is the primary characteristic of a "Worm"?

   (a) It encrypts files for ransom.

   (b) It self-replicates and spreads without user interaction.

   (c) It disguises itself as utility software.

   (d) It waits for a specific date to trigger.

   Answer: b

4. Which type of attack attempts to overflow a memory buffer to overwrite adjacent memory?

   (a) SQL Injection

   (b) Buffer Overflow

   (c) Replay Attack

   (d) Pass the Hash

   Answer: b

5. A group of compromised computers controlled by a central attacker is known as a:

   (a) Rootkit

   (b) Botnet

   (c) Logic Bomb

   (d) Honeypot

   Answer: b

6. Which malware type is designed to hide its presence and grant persistent administrative access?

   (a) Adware

   (b) Rootkit

   (c) Worm

   (d) Ransomware

   Answer: b

7. Inserting malicious SQL statements into an entry field for execution is known as:

   (a) XSS
   (b) CSRF
   (c) SQL Injection
   (d) XML Injection

   Answer: c

8. What is a ”Fileless Virus”?

   (a) A virus that deletes all files.
   (b) Malware that operates in memory and uses native tools like PowerShell.
   (c) A virus transmitted only via hardware.
   (d) A macro virus.

   Answer: b

9. Which attack tricks a user into performing an action on a web application where they are authenticated?

   (a) XSS
   (b) CSRF (Cross-Site Request Forgery)
   (c) SQLi
   (d) Replay

   Answer: b

10. Malware that lies dormant until a specific condition is met is called a:

    (a) Logic Bomb
    (b) Rootkit
    (c) Trojan
    (d) Keylogger

    Answer: a

II. True/False

1. A worm requires a host file and user interaction to spread. **Answer: False** (Viruses require hosts; worms do not)
2. Ransomware encrypts user data and demands payment for decryption. **Answer: True**
3. SQL Injection attacks target the database layer of an application. **Answer: True**
4. A keylogger is a hardware device or software that records keystrokes. **Answer: True**
5. Rootkits operate at the application level and are easy to detect with standard antivirus. **Answer: False** (They operate at OS/kernel level)
6. A botnet consists of ”zombie” computers controlled by a bot herder. **Answer: True**

7. Cross-Site Scripting (XSS) attacks occur when the server trusts data from the client without validation. **Answer: False** (Usually described as the client browser trusting scripts sent from the server/application)
8. A Logic Bomb executes immediately upon installation. **Answer: False**
9. Adversarial AI involves manipulating AI algorithms or training data. **Answer: True**
10. Replay attacks involve capturing valid data and retransmitting it later. **Answer: True**

III. Fill-in-the-Blank

1. _____ is malware that restricts access to a computer system until a fee is paid. **Answer: Ransomware**
2. A _____ creates a backdoor that gives an attacker remote control over a victim's computer. **Answer: Remote Access Trojan (RAT)**
3. _____ involves injecting malicious code into a website that is then executed by the visitor's browser. **Answer: Cross-Site Scripting (XSS)**
4. A _____ is a network of infected computers used for malicious purposes like DDoS. **Answer: Botnet**
5. _____ exploits involve sending more data to a buffer than it can handle. **Answer: Buffer Overflow**
6. _____ is the process of manipulating inputs to a machine learning model to cause it to make errors. **Answer: Adversarial AI**
7. _____ are typically used to automate tasks but can be malicious if they execute unwanted code (often in documents). **Answer: Macros**
8. A _____ captures every key pressed by a user. **Answer: Keylogger**
9. _____ uses native OS tools like PowerShell to run malicious code in memory. **Answer: Fileless malware**
10. _____ attacks involve an attacker sitting between two parties and intercepting communications. **Answer: On-path / Man-in-the-Middle**

IV. Short Answer

1. Explain the difference between a Virus and a Worm. **Answer: A Virus requires a host file and user action to spread; a Worm is self-replicating and spreads automatically over networks.**
2. What is "Cryptojacking"? **Answer: The unauthorized use of a victim's computer resources to mine cryptocurrency.**
3. Describe a "Driver Manipulation" attack (Shimming/Refactoring). **Answer: Modifying or creating drivers to execute malicious code or maintain persistence, often using shims (compatibility code) or rewriting internal code.**
4. What is the goal of a "Replay Attack"? **Answer: To capture valid credentials or session data and reuse them later to impersonate the user.**

5. Define ”Privilege Escalation.” **Answer: Exploiting a bug to gain higher permissions (e.g., root/admin) than authorized.**
6. What is ”Bluejacking”? **Answer: Sending unsolicited messages to Bluetooth-enabled devices.**
7. Explain ”Bluesnarfing.” **Answer: Unauthorized access of information from a wireless device through a Bluetooth connection.**
8. What is a ”Logic Bomb”? **Answer: Malicious code inserted into a system that executes only when specific conditions or times are met.**
9. How does ”SQL Injection” work? **Answer: The attacker enters SQL commands into an input field (like a login box) to manipulate the backend database.**
10. What is a ”Botnet”? **Answer: A collection of internet-connected devices infected and controlled by a common type of malware.**

V. Matching

Terms:

A. Rootkit

B. Spyware

C. Adware

D. Bot

E. Crypto-malware

F. Trojan

G. Worm

H. Keylogger

I. Logic Bomb

J. Backdoor

Definitions:

1. Self-replicating malware spreading via networks.
2. Hides processes/files from the OS kernel.
3. Records user keystrokes.
4. Uses system resources to mine currency.
5. Automatically displays unwanted advertisements.
6. Disguised as legitimate software.
7. Collects user data without consent.
8. A zombie computer in a network.
9. Bypasses normal authentication.
10. Executes when a specific event occurs.

Answers: 1-G, 2-A, 3-H, 4-E, 5-C, 6-F, 7-B, 8-D, 9-J, 10-I

Chapter 4: Endpoint and Application Development Security

Section A: Chapter Summary

Key Concepts

- **Threat Intelligence Sources:**
  - **Open Source Intelligence (OSINT):** Publicly available information (e.g., social media, news).
  - **Closed Source:** Proprietary information gathered by security firms or governments.
  - **Automated Indicator Sharing (AIS):** Standardized exchange of cyber threat indicators (uses STIX/TAXII).
  - **Dark Web:** Part of the web requiring specific software (like Tor) to access; often used for illicit activities.
- **Securing Endpoint Computers:**
  - **Boot Integrity:** Ensuring the boot process is secure.
    - **UEFI (Unified Extensible Firmware Interface):** Replaced BIOS; supports Secure Boot to validate drivers/OS.
    - **Measured Boot:** Logs the boot process for verification by a remote server.
  - **Endpoint Protection:** Antivirus (AV), Antimalware, Host-based Firewalls, EDR (Endpoint Detection and Response), HIDS/HIPS.
  - **Hardening:** Reducing the attack surface.
    - **Patch Management:** Automated updates for OS and applications.
    - **Disabling Unnecessary Ports/Services.**
    - **Least Privilege:** Limiting user account permissions.
    - **Whitelisting/Blacklisting:** Controlling allowed applications.
- **Application Development Security (SecDevOps):**
  - **DevOps:** Integrating software development (Dev) and IT operations (Ops).
  - **SecDevOps:** Integrating security into the DevOps process ("Security as Code").
  - **Code Analysis:**
    - **Static Analysis:** Analyzing source code without executing it.
    - **Dynamic Analysis:** Analyzing code while it is running (e.g., Fuzzing).
  - **Fuzzing:** Sending random, invalid data to an application to crash it or find vulnerabilities.
- **Development Models:**
  - **Waterfall:** Sequential stages (inflexible).
  - **Agile:** Iterative, incremental changes (flexible).

Section B: Test Bank

I. Multiple Choice

1. Which technology allows for the automated exchange of cyber threat indicators between organizations?

   (a) UEFI
   (b) AIS (Automated Indicator Sharing)
   (c) Fuzzing
   (d) Waterfall

   Answer: b

2. What replaced the legacy BIOS to provide enhanced boot security features like Secure Boot?

   (a) MBR
   (b) UEFI
   (c) CMOS
   (d) EDR

   Answer: b

3. Which type of code analysis is performed while the software is running?

   (a) Static Analysis
   (b) Dynamic Analysis
   (c) Passive Analysis
   (d) Waterfall Analysis

   Answer: b

4. A security approach that approves only specific applications to run on an endpoint is called:

   (a) Blacklisting
   (b) Whitelisting
   (c) Fuzzing
   (d) Sandboxing

   Answer: b

5. Which development model relies on short cycles or ”sprints” to allow for rapid adjustments?

   (a) Waterfall
   (b) Agile
   (c) Monolithic
   (d) Legacy

   Answer: b

6. What is ”Fuzzing”?

   (a) Encrypting data at rest.
   (b) Sending random input to an application to test for vulnerabilities.
   (c) Analyzing code without running it.
   (d) A boot integrity check.

   Answer: b

7. Which endpoint protection tool is designed to detect and respond to advanced threats by analyzing behavior?

   (a) Antivirus (AV)
   (b) EDR (Endpoint Detection and Response)
   (c) Firewall
   (d) DLP

   Answer: b

8. STIX and TAXII are standards associated with:

   (a) Secure Boot
   (b) Threat Intelligence Sharing
   (c) Application Fuzzing
   (d) Database Encryption

   Answer: b

9. Which term describes removing unnecessary services, accounts, and drivers to improve security?

   (a) Hardening
   (b) Provisioning
   (c) Sandboxing
   (d) Virtualization

   Answer: a

10. In the context of SecDevOps, what does ”Infrastructure as Code” imply?

    (a) Managing hardware via physical switches.
    (b) Managing infrastructure using machine-readable definition files.
    (c) Writing code to build physical servers.
    (d) Using only software firewalls.

    Answer: b

II. True/False

1. Static code analysis requires the application to be compiled and running. **Answer: False**
2. The Waterfall model is considered more flexible than Agile. **Answer: False**
3. Secure Boot checks the digital signatures of drivers and the OS loader. **Answer: True**
4. A sandbox is an isolated environment used to test suspicious files. **Answer: True**
5. OSINT stands for Operating System Internal Technologies. **Answer: False** (Open Source Intelligence)
6. Fuzzing is a type of static analysis. **Answer: False** (Dynamic analysis)
7. Whitelisting is generally considered more secure than blacklisting. **Answer: True**
8. A Trusted Platform Module (TPM) is a hardware chip used for cryptographic functions and boot integrity. **Answer: True**
9. Patch management should only be performed manually to ensure quality. **Answer: False** (Automated is preferred for scale/speed)
10. ”Dark Web” content is indexed by standard search engines like Google. **Answer: False**

III. Fill-in-the-Blank

1. _____ is the process of integrating security practices into the DevOps software development lifecycle. **Answer: SecDevOps (or DevSecOps)**
2. The _____ boot process logs the boot sequence to a trusted server (TPM) to verify the system’s health. **Answer: Measured**
3. _____ analysis involves reviewing source code for vulnerabilities without executing the program. **Answer: Static**
4. _____ is the practice of providing random or unexpected input to a computer program to uncover errors. **Answer: Fuzzing**
5. _____ refers to publicly available information that can be used for threat intelligence. **Answer: OSINT**
6. _____ prevents specific applications from running on a system (default allow). **Answer: Blacklisting**
7. _____ is a hardware chip on the motherboard that stores cryptographic keys and supports Secure Boot. **Answer: TPM (Trusted Platform Module)**
8. The _____ development model uses a linear, sequential approach to software design. **Answer: Waterfall**
9. _____ is a machine-to-machine exchange of cyber threat intelligence information. **Answer: Automated Indicator Sharing (AIS)**
10. _____ involves creating a secure baseline image and deploying it to multiple endpoints. **Answer: Imaging / Provisioning**

IV. Short Answer

1. Define ”Hardening” in the context of endpoint security. **Answer: The process of securing a system by reducing its surface of vulnerability (e.g., disabling unnecessary services, patching).**
2. What is the difference between Static and Dynamic code analysis? **Answer: Static analyzes source code at rest (not running); Dynamic tests the application while it is executing.**
3. Explain the purpose of a ”Sandbox.” **Answer: A restricted, isolated environment where code or files can be executed safely without affecting the host system.**
4. What is the role of a TPM (Trusted Platform Module)? **Answer: A hardware chip that provides cryptographic functions, stores keys, and ensures boot integrity.**
5. Describe the ”Agile” development methodology. **Answer: An iterative approach to software development that emphasizes flexibility, collaboration, and rapid delivery of small functional blocks.**
6. What is ”Application Whitelisting”? **Answer: A security practice where only pre-approved applications are allowed to run on a system.**
7. Define ”Fuzzing.” **Answer: An automated software testing technique that involves providing invalid, unexpected, or random data as inputs to finding bugs.**
8. What is ”Secure Boot”? **Answer: A UEFI feature that prevents a system from booting with unauthorized or malicious drivers/OS loaders.**
9. What is the ”Dark Web”? **Answer: Encrypted online content that is not indexed by conventional search engines and requires specific software (e.g., Tor) to access.**
10. Explain ”Patch Management.” **Answer: The process of distributing and applying updates to software to correct errors or security vulnerabilities.**

V. Matching

Terms:

A. UEFI

B. SecDevOps

C. Fuzzing

D. Whitelisting

E. Blacklisting

F. Waterfall

G. Agile

H. TPM

I. STIX/TAXII

J. EDR

Definitions:

1. Hardware chip for crypto operations.
2. Standards for sharing threat intelligence.
3. Allows only approved apps to run.
4. Sequential software development model.
5. Testing with random input data.
6. Modern firmware replacing BIOS.
7. Integrating security into DevOps.
8. Iterative software development model.

9. Blocks specific known bad apps.
10. Advanced endpoint monitoring/response.

Answers: 1-H, 2-I, 3-D, 4-F, 5-C, 6-A, 7-B, 8-G, 9-E, 10-J

Chapter 5: Mobile, Embedded, and Specialized Device Security

Section A: Chapter Summary

Key Concepts

- **Enterprise Deployment Models:**
  - **BYOD (Bring Your Own Device):** Employees use personal devices for work. Low cost, high security risk.
  - **COPE (Corporate Owned, Personally Enabled):** Company provides device; limited personal use allowed.
  - **CYOD (Choose Your Own Device):** Employee chooses from approved list; company manages it.
  - **Corporate Owned:** Strictly for work use; highest security control.
  - **VDI (Virtual Desktop Infrastructure):** Mobile device accesses a remote virtual desktop; data stays on server.
- **Mobile Risks & Attacks:**
  - **Jailbreaking/Rooting:** Removing OS restrictions (iOS/Android), which weakens security.
  - **Sideloading:** Installing apps from unofficial sources.
  - **Bluejacking:** Sending unsolicited messages via Bluetooth.
  - **Bluesnarfing:** Stealing data via Bluetooth.
  - **Geolocation/Geotagging:** Risks regarding privacy and location tracking.
- **Mobile Protections:**
  - **MDM (Mobile Device Management):** Centralized control of devices (remote wipe, enforce passwords).
  - **MAM (Mobile Application Management):** Controls specific corporate apps/data (containerization) rather than the whole device.
  - **Geofencing:** Triggering actions based on physical location.
  - **Screen Locks/Biometrics:** Fundamental access control.
- **Embedded & Specialized Systems:**
  - **Embedded Systems:** Computer hardware/software integrated into a larger system (e.g., medical devices, cars).
  - **IoT (Internet of Things):** Everyday objects connected to the internet (smart home, wearables). Often lack robust security.
  - **SCADA (Supervisory Control and Data Acquisition) / ICS (Industrial Control Systems):** Systems managing industrial infrastructure (power plants, factories).
- **Constraints:** Embedded systems often have constraints in power, compute, network, and patching capabilities, making security difficult.

Section B: Test Bank

I. Multiple Choice

1. Which deployment model allows employees to use their personal devices for work?

   (a) COPE
   (b) CYOD
   (c) BYOD
   (d) VDI

   Answer: c

2. What is the term for removing software restrictions on an iOS device?

   (a) Rooting
   (b) Jailbreaking
   (c) Sideloading
   (d) Unlocking

   Answer: b

3. Which attack involves stealing data from a device via a Bluetooth connection?

   (a) Bluejacking
   (b) Bluesnarfing
   (c) Phishing
   (d) Smishing

   Answer: b

4. A system used to control industrial processes such as power plants is called:

   (a) IoT
   (b) SCADA / ICS
   (c) VDI
   (d) MDM

   Answer: b

5. Installing an application on a mobile device from a source other than the official app store is called:

   (a) Jailbreaking
   (b) Bootloading
   (c) Sideloading
   (d) Carrier Unlocking

   Answer: c

6. Which technology creates a virtual barrier based on real-world geographic coordinates?

   (a) Geotagging

(b) Geolocation
(c) Geofencing
(d) GPS Spoofing

Answer: c

7. What is a primary security constraint of embedded systems and IoT devices?

(a) Excessive processing power
(b) Frequent automatic updates
(c) Inability to be patched
(d) Large storage capacity

Answer: c

8. Which mobile management tool focuses specifically on securing corporate data within applications rather than the entire device?

(a) MDM
(b) MAM
(c) UEM
(d) MCM

Answer: b

9. Sending unsolicited messages to a Bluetooth-enabled device is known as:

(a) Bluejacking
(b) Bluesnarfing
(c) Whitewashing
(d) Sandboxing

Answer: a

10. Which connectivity method uses close-proximity radio waves (approx. 4 cm) often for payments?

(a) Bluetooth
(b) WiFi
(c) NFC
(d) Cellular

Answer: c

II. True/False

1. Rooting refers to gaining administrative privileges on an Android device. **Answer: True**
2. SCADA systems are typically found in home automation environments. **Answer: False** (Industrial environments)

3. Containerization allows separating corporate data from personal data on a mobile device. **Answer: True**
4. VDI stores all data locally on the mobile device. **Answer: False** (Data stays on the remote server)
5. Embedded systems usually have high power capabilities and easy patch management. **Answer: False**
6. USB On-The-Go (OTG) allows mobile devices to connect directly to external media. **Answer: True**
7. Geotagging adds geographical identification metadata to media like photos. **Answer: True**
8. COPE stands for "Choose Own Personal Equipment." **Answer: False** (Corporate Owned, Personally Enabled)
9. Zigbee is a high-power wireless standard used for streaming video. **Answer: False** (Low-power, for IoT/sensors)
10. A Faraday cage can block wireless signals from reaching a mobile device. **Answer: True**

III. Fill-in-the-Blank

1. _____ is the process of gaining root access on an iOS device. **Answer: Jailbreaking**
2. _____ involves sending unsolicited messages via Bluetooth. **Answer: Bluejacking**
3. _____ allows a mobile device to be wiped of data from a central location. **Answer: Remote wipe**
4. _____ systems control critical infrastructure like water treatment and power grids. **Answer: SCADA / ICS**
5. _____ uses GPS to define geographical boundaries for app usage or alerts. **Answer: Geofencing**
6. _____ is the installation of apps from unofficial sources. **Answer: Sideloading**
7. _____ is a low-power wireless protocol often used in home automation and IoT. **Answer: Zigbee / Z-Wave**
8. The _____ deployment model involves the company purchasing the device but allowing personal use. **Answer: COPE**
9. _____ separates personal and corporate information on a single device (often used in MAM). **Answer: Containerization / Storage Segmentation**
10. _____ is a short-range wireless technology used for contactless payments. **Answer: NFC (Near Field Communication)**

IV. Short Answer

1. Explain the difference between MDM and MAM. **Answer: MDM manages the entire device (settings, wipe); MAM manages specific applications and their data.**
2. What is ”Context-aware authentication”? **Answer: Authentication that changes requirements based on context, such as location, time of day, or behavior.**
3. Define ”Embedded System.” **Answer: A computer system with a dedicated function within a larger mechanical or electrical system (e.g., car engine controller).**
4. What are the risks of ”Jailbreaking” or ”Rooting”? **Answer: It bypasses security controls, voids warranties, and exposes the device to malware.**
5. Describe the ”BYOD” model. **Answer: Bring Your Own Device; employees use personal devices for work tasks.**
6. What is ”Geofencing”? **Answer: Creating a virtual perimeter that triggers an action (like locking a device) when a device enters or leaves the area.**
7. What is the purpose of ”Remote Wipe”? **Answer: To delete data from a lost or stolen device remotely to prevent unauthorized access.**
8. Describe ”Sideloading.” **Answer: Installing mobile applications directly via a file (e.g., APK) rather than through the official app store.**
9. What is ”IoT” (Internet of Things)? **Answer: A network of physical objects embedded with sensors/software that connect and exchange data over the internet.**
10. Why are SCADA systems difficult to secure? **Answer: They often use legacy hardware/software, cannot be easily patched, and prioritize availability over security.**

V. Matching

Terms:

A. NFC

B. ANT+ / Zigbee

C. SCADA

D. BYOD

E. COPE

F. VDI

G. Geofencing

H. Containerization

I. Sideloading

J. Rooting

Definitions:

1. Gaining admin rights on Android.
2. Industrial Control System.
3. Employees use personal phones for work.
4. Data stays on a remote server, not device.
5. Installing apps from unofficial sources.
6. Short-range wireless (payments).
7. Corporate owned, personal use allowed.
8. Isolating corporate app data.
9. Low-power IoT wireless protocols.
10. Virtual geographic boundary.

Answers: 1-J, 2-C, 3-D, 4-F, 5-I, 6-A, 7-E, 8-H, 9-B, 10-G

Chapter 6: Basic Cryptography

Section A: Chapter Summary

Key Concepts

- **Cryptography Definition:** The practice of transforming information so that it is secure and cannot be understood by unauthorized persons (scrambling data).
- **Core Protections:**
  - **Confidentiality:** Only authorized users can read data.
  - **Integrity:** Data has not been altered.
  - **Authentication:** Proof of sender's identity.
  - **Nonrepudiation:** Sender cannot deny sending the message.
  - **Obfuscation:** Making something unclear (e.g., Security through obscurity).
- **States of Data:** Data at Rest (storage), Data in Transit (network), Data in Use (memory).
- **Cryptographic Algorithms:**
  - **Hashing:** One-way function to create a unique digital fingerprint (digest). Used for Integrity.
    - Examples: MD5 (weak), SHA-1 (weak), SHA-2, SHA-3, RIPEMD.
  - **Symmetric Encryption:** Uses a *single* shared key for encryption and decryption. Fast. Used for Confidentiality (bulk data).
    - Examples: DES (weak), 3DES, AES (standard), Blowfish, RC4.
  - **Asymmetric Encryption:** Uses a key *pair* (Public and Private). Public key encrypts; Private key decrypts. Slower. Used for Key Exchange and Digital Signatures.
    - Examples: RSA, ECC (Elliptic Curve), DSA, Diffie-Hellman (Key Exchange).
- **Attacks on Cryptography:**
  - **Collision Attack:** Finding two different inputs that produce the same hash.
  - **Birthday Attack:** A probability-based collision attack.
  - **Downgrade Attack:** Forcing a system to use weaker, older protocols.
- **Implementation:**
  - **Hardware Encryption:** TPM (Trusted Platform Module) on motherboard; HSM (Hardware Security Module) external device.
  - **Full Disk Encryption (FDE):** Encrypting the entire drive (e.g., BitLocker).
  - **Blockchain:** Shared, immutable ledger relying on hashes.

Section B: Test Bank

I. Multiple Choice

1. Which concept ensures that data is not altered without authorization?

   (a) Confidentiality
   (b) Integrity
   (c) Availability
   (d) Nonrepudiation

   Answer: b

2. Which type of algorithm uses a single shared key for both encryption and decryption?

   (a) Hashing
   (b) Asymmetric
   (c) Symmetric
   (d) Digital Signature

   Answer: c

3. Which of the following is a Hashing algorithm?

   (a) AES
   (b) RSA
   (c) SHA-256
   (d) Diffie-Hellman

   Answer: c

4. What is the primary use of Asymmetric cryptography?

   (a) Bulk data encryption
   (b) Integrity checking
   (c) Key exchange and digital signatures
   (d) Creating rainbows tables

   Answer: c

5. Which cryptographic attack relies on the probability of two different inputs producing the same hash value?

   (a) Brute Force
   (b) Birthday Attack
   (c) Dictionary Attack
   (d) Replay Attack

   Answer: b

6. Which hardware component on a motherboard provides cryptographic services and stores keys?

(a) CPU
(b) GPU
(c) TPM
(d) RAM

Answer: c

7. Making data unclear or difficult to understand without necessarily encrypting it is called:

(a) Obfuscation
(b) Authentication
(c) Nonrepudiation
(d) Integrity

Answer: a

8. Which algorithm is currently the standard for symmetric encryption (used by US gov)?

(a) DES
(b) 3DES
(c) AES
(d) RC4

Answer: c

9. Elliptic Curve Cryptography (ECC) is an example of which type of encryption?

(a) Symmetric
(b) Asymmetric
(c) Hashing
(d) Obfuscation

Answer: b

10. What is ”Steganography”?

(a) Encrypting a hard drive.
(b) Hiding data inside another file (like an image).
(c) Using quantum computing to crack codes.
(d) A type of digital signature.

Answer: b

II. True/False

1. Symmetric encryption is generally faster than asymmetric encryption. **Answer: True**
2. Hashing is a two-way function; you can decrypt a hash to get the original text. **Answer: False** (One-way)
3. A digital signature provides nonrepudiation. **Answer: True**
4. MD5 is considered a secure hashing algorithm for modern use. **Answer: False** (It has collision vulnerabilities)
5. The private key in asymmetric encryption can be shared with anyone. **Answer: False** (Public key is shared; private is kept secret)
6. Diffie-Hellman is used primarily for encrypting hard drives. **Answer: False** (Used for key exchange)
7. Full Disk Encryption (FDE) protects data at rest. **Answer: True**
8. High resiliency in cryptography means the algorithm works well with low latency/low power resources. **Answer: True**
9. A collision occurs when two different inputs result in the same hash digest. **Answer: True**
10. Quantum computing poses no threat to current cryptographic standards. **Answer: False**

III. Fill-in-the-Blank

1. _____ is the process of changing plaintext into ciphertext. **Answer: Encryption**
2. _____ algorithms create a unique digital fingerprint of data to verify integrity. **Answer: Hashing**
3. _____ encryption uses a pair of keys: a public key and a private key. **Answer: Asymmetric**
4. _____ provides proof that a user performed an action and prevents them from denying it. **Answer: Nonrepudiation**
5. _____ is a dedicated cryptographic processor chip on the motherboard. **Answer: TPM (Trusted Platform Module)**
6. _____ is hiding the existence of data, often within image or audio files. **Answer: Steganography**
7. A _____ attack forces a system to abandon a higher security mode for a legacy, less secure one. **Answer: Downgrade**
8. _____ is a shared, immutable ledger that relies on cryptographic hashes (used in cryptocurrency). **Answer: Blockchain**
9. _____ refers to data currently being used by the CPU/RAM. **Answer: Data in Use / Processing**
10. The _____ algorithm is a symmetric cipher that creates a stream of bits (Stream Cipher), once popular in WEP/TLS. **Answer: RC4**

IV. Short Answer

1. What is the difference between Symmetric and Asymmetric encryption? **Answer: Symmetric uses one shared key; Asymmetric uses a key pair (public/private).**
2. Define "Hashing." **Answer: A one-way mathematical function that converts data into a fixed-length string (digest) to verify integrity.**
3. What is "Salting" passwords? **Answer: Adding random data to a password before hashing it to protect against rainbow table attacks.**
4. Describe a "Collision Attack." **Answer: An attempt to find two different input messages that hash to the same digest.**
5. What is "Perfect Forward Secrecy"? **Answer: A property where compromising long-term keys does not compromise past session keys (uses ephemeral keys).**
6. What is the purpose of a "Digital Signature"? **Answer: To verify the sender's identity (authentication) and ensure the message hasn't changed (integrity).**
7. Explain "Diffie-Hellman." **Answer: A protocol that allows two parties to securely establish a shared secret key over an insecure channel.**
8. What is an "HSM" (Hardware Security Module)? **Answer: A physical computing device that manages digital keys and performs cryptographic operations.**
9. Define "Obfuscation." **Answer: Making code or data difficult for humans to understand (e.g., masking variables) without encryption.**
10. Why is MD5 no longer recommended? **Answer: It is vulnerable to collision attacks (it is easy to generate two files with the same MD5 hash).**

V. Matching

Terms:

A. AES
B. RSA
C. SHA-256
D. Diffie-Hellman
E. TPM
F. Nonrepudiation
G. Obfuscation
H. Collision
I. Symmetric
J. Asymmetric

Definitions:

1. Hashing algorithm used for integrity.
2. Standard symmetric block cipher.
3. Asymmetric algorithm based on prime numbers.
4. Hardware chip for crypto storage on PC.
5. Two inputs producing the same hash.
6. Proof of origin (cannot deny action).
7. Uses one key for lock and unlock.
8. Uses a public and private key.
9. Hiding meaning (e.g., ROT13).
10. Key exchange protocol.

Answers: 1-C, 2-A, 3-B, 4-E, 5-H, 6-F, 7-I, 8-J, 9-G, 10-D

Student Study Guide and Assessment Bank

Modules 7 & 8

Contents

Chapter 7: Public Key Infrastructure and Cryptographic Protocols

Section A: Chapter Summary

Key Concepts

- **Digital Certificates:**
  - Used to associate a user's identity with a public key, digitally signed by a trusted third party (Certificate Authority).
  - **X.509:** The standard format for digital certificates.
  - **Certificate Life Cycle:** Creation, Suspension, Revocation, Expiration.
- **Public Key Infrastructure (PKI):**
  - **Certificate Authority (CA):** The trusted entity that issues and manages certificates.
  - **Registration Authority (RA):** Verifies the identity of the requester before a certificate is issued.
  - **Certificate Repository (CR):** Publicly accessible directory of certificates.
  - **Certificate Revocation List (CRL):** A list of serial numbers of certificates that have been revoked.
  - **OCSP (Online Certificate Status Protocol):** Real-time check of a certificate's status (often uses "Stapling" to reduce traffic).
- **Trust Models:**
  - **Hierarchical:** Single root CA.
  - **Distributed:** Multiple CAs.
  - **Bridge:** Connects different trust models.
- **Key Management:**
  - **Key Escrow:** Storing keys with a third party (for recovery).
  - **M-of-N Control:** Recovering a key requires multiple people (M) out of a group (N).
  - **Expiration/Renewal:** Keys should have a limited lifespan.
- **Cryptographic Protocols (Data in Transit):**
  - **SSL/TLS:** Secure Sockets Layer (deprecated) and Transport Layer Security (current standard) for securing web traffic.
  - **HTTPS:** HTTP over SSL/TLS (Port 443).
  - **SSH (Secure Shell):** Secure remote login (Port 22).
  - **S/MIME:** Secure email (encryption/digital signatures).
  - **IPsec:** Secures IP communications (Tunnel mode vs. Transport mode; uses AH and ESP protocols).

Section B: Test Bank

I. Multiple Choice

1. Which entity is responsible for verifying the identity of an applicant before a digital certificate is issued?

   (a) Certificate Authority (CA)
   (b) Registration Authority (RA)
   (c) Certificate Repository (CR)
   (d) Key Escrow Agent

   Answer: b

2. Which protocol provides a real-time method for checking the revocation status of a digital certificate?

   (a) CRL
   (b) HTTP
   (c) OCSP
   (d) SSH

   Answer: c

3. In a hierarchical trust model, what is the single master CA called?

   (a) Bridge CA
   (b) Root CA
   (c) Intermediate CA
   (d) Distributed CA

   Answer: b

4. Which IPsec protocol provides confidentiality (encryption)?

   (a) AH (Authentication Header)
   (b) ESP (Encapsulating Security Payload)
   (c) IKE (Internet Key Exchange)
   (d) ISAKMP

   Answer: b

5. What is the standard format for digital certificates?

   (a) X.500
   (b) X.509
   (c) PGP
   (d) PKCS#12

   Answer: b

6. Which protocol is used to secure email messages with encryption and digital signatures?

(a) HTTPS
(b) SSH
(c) S/MIME
(d) SNMPv3

Answer: c

7. ”Key Escrow” refers to:

(a) Destroying keys securely.
(b) A third party holding a copy of a private key for recovery purposes.
(c) Generating new keys every session.
(d) Using ephemeral keys for perfect forward secrecy.

Answer: b

8. Which version of SSL/TLS is currently considered secure and is the industry standard?

(a) SSL v3.0
(b) TLS v1.0
(c) TLS v1.2 / v1.3
(d) SSL v2.0

Answer: c

9. What is ”OCSP Stapling”?

(a) The web server sends the OCSP response to the client, reducing burden on the CA.
(b) The client queries the CA directly for every request.
(c) Attaching a physical token to the server.
(d) Revoking a certificate permanently.

Answer: a

10. Which secure protocol replaces Telnet for remote server administration?

(a) HTTP
(b) FTP
(c) SSH
(d) RDP

Answer: c

II. True/False

1. A digital certificate binds a public key to a user’s identity. **Answer: True**
2. The Root CA’s certificate is self-signed. **Answer: True**
3. CRLs (Certificate Revocation Lists) are updated in real-time. **Answer: False** (They are periodic snapshots)

4. IPsec in Transport Mode encrypts the entire IP packet (header and payload). **Answer: False** (Tunnel mode does this; Transport encrypts payload only)
5. S/MIME uses a web of trust model. **Answer: False** (Usually relies on PKI/CA hierarchy)
6. SSH uses port 22 by default. **Answer: True**
7. If a user's private key is compromised, their certificate should be suspended, not revoked. **Answer: False** (It should be revoked immediately)
8. M-of-N control ensures that a single person cannot recover a key alone. **Answer: True**
9. HTTPS uses port 80. **Answer: False** (Uses port 443)
10. A "Wildcard" certificate can be used for multiple subdomains (e.g., *.example.com). **Answer: True**

III. Fill-in-the-Blank

1. _____ is the framework for managing all entities involved in digital certificates (hardware, software, people, policies). **Answer: PKI (Public Key Infrastructure)**
2. A _____ certificate is used to digitally sign software code to prove its origin and integrity. **Answer: Code Signing**
3. _____ is an attack where a user is tricked into using an unencrypted HTTP connection instead of HTTPS. **Answer: SSL Stripping**
4. The _____ is the entity responsible for issuing digital certificates. **Answer: CA (Certificate Authority)**
5. In the _____ trust model, there is no single CA that signs digital certificates, but a CA acts as a facilitator. **Answer: Bridge**
6. _____ requires the browser to query the CA's responder to check certificate status. **Answer: OCSP**
7. _____ provides authentication, integrity, and non-repudiation for IPsec. **Answer: AH (Authentication Header)**
8. _____ keys are temporary keys used only once for a single session. **Answer: Ephemeral**
9. _____ is a protocol for securing VoIP communications. **Answer: SRTP (Secure Real-time Transport Protocol)**
10. A _____ request is sent by a user to a CA to apply for a digital certificate. **Answer: CSR (Certificate Signing Request)**

IV. Short Answer

1. Define "Certificate Chaining." **Answer: Linking a user certificate back to the trusted Root CA through one or more Intermediate CAs.**
2. What is the difference between IPsec Transport Mode and Tunnel Mode? **Answer: Transport mode encrypts only the payload (data); Tunnel mode encrypts the entire packet including the header.**

3. Explain the purpose of ”Key Escrow.” **Answer: To allow an authorized third party (like a CA or government) to access a decryption key for data recovery.**
4. What is ”Pinning” in the context of digital certificates? **Answer: Hard-coding a digital certificate (or public key) within an application to prevent MITM attacks using fraudulent certificates.**
5. Why is SSL considered obsolete? **Answer: It has known security vulnerabilities (e.g., POODLE attack) and has been replaced by TLS.**
6. What is an ”Extended Validation (EV)” certificate? **Answer: A certificate requiring a rigorous identity verification process, often displaying the company name in the browser address bar.**
7. Define ”Session Key.” **Answer: A symmetric key generated for use during a single communication session (e.g., during an SSL/TLS handshake).**
8. What is the function of the ”Registration Authority” (RA)? **Answer: To verify the identity of a prospective certificate holder before the CA issues the certificate.**
9. What is a ”Self-Signed Certificate”? **Answer: A certificate signed by the entity that created it, rather than by a trusted third-party CA (often used for testing).**
10. Explain ”Perfect Forward Secrecy.” **Answer: A property where the compromise of a long-term key does not compromise past session keys (typically uses ephemeral keys).**

V. Matching

Terms:	**Definitions:**
A. Root CA	1. Standard for digital certificates.
B. OCSP	2. Secures IP traffic (VPNs).
C. CRL	3. Trusted anchor of the PKI hierarchy.
D. SSH	4. Real-time certificate status check.
E. HTTPS	5. Application for a certificate.
F. IPsec	6. List of invalid certificates.
G. S/MIME	7. Secure web browsing protocol.
H. Key Escrow	8. Secure email protocol.
I. X.509	9. Secure remote terminal protocol.
J. CSR	10. Archiving keys for recovery.

Answers: 1-I, 2-F, 3-A, 4-B, 5-J, 6-C, 7-E, 8-G, 9-D, 10-H

Chapter 8: Networking Threats, Assessments, and Defenses

Section A: Chapter Summary

Key Concepts

- **Network Attacks:**
  - **Interception:**
    - **Man-in-the-Middle (MITM):** Intercepting communications between two parties.
    - **Man-in-the-Browser (MITB):** Malware in the browser intercepts data.
    - **Replay Attack:** Capturing and resending valid data (e.g., authentication tokens).
  - **Layer 2 Attacks:**
    - **ARP Poisoning:** Corrupting the ARP cache to link the attacker's MAC to a legitimate IP.
    - **MAC Flooding:** Overwhelming a switch's MAC table to force it to act like a hub (fail-open).
  - **DNS Attacks:**
    - **DNS Poisoning:** Altering DNS records to redirect traffic to malicious sites.
    - **DNS Hijacking:** Taking over the DNS server itself.
  - **DDoS (Distributed Denial of Service):** Using a botnet to overwhelm a target.
- **Assessment Tools:**
  - **Reconnaissance:** `ping`, `tracert`/`traceroute`, `nslookup`/`dig`, `ipconfig`/`ifconfig`, `nmap` (port scanner), `netstat`.
  - **Packet Capture:** Wireshark (GUI analyzer), `tcpdump` (command line).
  - **File Manipulation (Linux):** `grep`, `cat`, `chmod`, `logger`.
- **Physical Security Controls:**
  - **Perimeter:** Fencing, Bollards (stop vehicles), Lighting, Signs.
  - **Internal:** Locks (physical/electronic), Mantraps (access control vestibules), Safe areas.
  - **Surveillance:** CCTV (Video), Guards, Robot Sentries.
  - **Hardware Security:** Cable locks, Faraday cages (block EM signals), Air gaps.

Section B: Test Bank

I. Multiple Choice

1. Which attack involves overwhelming a switch's MAC address table to force it into fail-open mode?

(a) ARP Poisoning
(b) MAC Flooding
(c) DNS Poisoning
(d) Replay Attack

Answer: b

2. Which command-line tool is used to trace the path a packet takes to a destination?

(a) ping
(b) ipconfig
(c) traceroute
(d) netstat

Answer: c

3. What is the primary function of a ”Mantrap”?

(a) To extinguish fires.
(b) To prevent tailgating by using two interlocking doors.
(c) To capture network packets.
(d) To block electromagnetic signals.

Answer: b

4. Which attack alters the ARP cache of a victim to redirect traffic to the attacker?

(a) DNS Poisoning
(b) ARP Poisoning
(c) MAC Cloning
(d) Session Replay

Answer: b

5. Which physical security control consists of short, sturdy vertical posts used to prevent vehicles from ramming a building?

(a) Fencing
(b) Bollards
(c) Mantraps
(d) Air gaps

Answer: b

6. Which tool is a command-line packet analyzer common on Linux systems?

(a) Wireshark
(b) Nmap
(c) tcpdump
(d) Nessus

Answer: c

7. An attack where valid data transmission is maliciously or fraudulently repeated or delayed is called:

   (a) Replay Attack
   (b) DDoS
   (c) SQL Injection
   (d) Cross-Site Scripting

   Answer: a

8. Which command displays current network connections and listening ports?

   (a) ping
   (b) netstat
   (c) nslookup
   (d) dig

   Answer: b

9. What is a ”Faraday Cage” used for?

   (a) Blocking physical entry.
   (b) Blocking electromagnetic fields/signals.
   (c) Filtering web traffic.
   (d) Storing cryptographic keys.

   Answer: b

10. Which Linux command is used to change file permissions?

    (a) chown
    (b) grep
    (c) chmod
    (d) cat

    Answer: c

II. True/False

1. ARP Poisoning is a Layer 3 (Network Layer) attack. **Answer: False** (It is a Layer 2 attack)
2. A DDoS attack uses a single computer to overwhelm a target. **Answer: False** (Uses multiple computers/botnet)
3. Nmap is a popular tool for network discovery and port scanning. **Answer: True**
4. An ”Air Gap” refers to physically isolating a secure network from unsecure networks. **Answer: True**
5. DNS Poisoning redirects a user to a malicious website by corrupting name resolution. **Answer: True**
6. Wireshark is a command-line only tool. **Answer: False** (It is a GUI tool)

7. Tailgating can be mitigated by using a mantrap. **Answer: True**
8. The `ping` command uses ICMP Echo Request packets. **Answer: True**
9. MAC Cloning involves spoofing a valid MAC address to bypass access control lists. **Answer: True**
10. Motion detection sensors are a type of administrative control. **Answer: False** (Physical/Technical control)

III. Fill-in-the-Blank

1. _____ is the act of intercepting communication between two parties, often without their knowledge. **Answer: Man-in-the-Middle (MITM)**
2. The Linux command _____ is used to search for text or patterns within files. **Answer: grep**
3. A _____ is a physical enclosure designed to block wireless signals. **Answer: Faraday cage**
4. _____ involves flooding a switch with fake MAC addresses to overflow the CAM table. **Answer: MAC Flooding**
5. The _____ command in Windows displays IP configuration details. **Answer: ipconfig**
6. _____ is a physical security device consisting of a small room with two doors, where one must close before the other opens. **Answer: Mantrap**
7. _____ involves using a botnet to flood a target with traffic, rendering it unavailable. **Answer: Distributed Denial of Service (DDoS)**
8. _____ is the process of gathering information about a network to identify vulnerabilities (often using Nmap). **Answer: Reconnaissance / Scanning**
9. A _____ attack redirects users to a fake website by corrupting the Domain Name System cache. **Answer: DNS Poisoning**
10. The Linux command _____ displays the contents of a file. **Answer: cat**

IV. Short Answer

1. Explain "ARP Poisoning." **Answer: An attack that associates the attacker's MAC address with the IP address of a legitimate device (like a gateway) in the victim's ARP cache.**
2. What is a "Replay Attack"? **Answer: An attack where valid data (like an auth token) is captured and retransmitted later to impersonate the user.**
3. Describe the function of "Nmap." **Answer: A network scanning tool used for network discovery, port scanning, and security auditing.**
4. What is an "Air Gap" in security? **Answer: A physical isolation measure where a secure network is physically disconnected from unsecured networks (like the internet).**

5. Define ”Man-in-the-Browser” (MITB). **Answer: A Trojan that infects a web browser to intercept or modify web pages and transaction data.**
6. What is the difference between `ping` and `traceroute`? **Answer: Ping tests connectivity/reachability; traceroute maps the path (hops) packets take to the destination.**
7. How does a ”Mantrap” enhance security? **Answer: It controls access by ensuring only one person enters at a time, preventing tailgating.**
8. What is ”MAC Flooding”? **Answer: Sending many fake MAC addresses to a switch to fill its CAM table, forcing it to broadcast traffic (fail open).**
9. Explain ”DNS Hijacking.” **Answer: An attack where the attacker changes DNS settings to redirect traffic to a malicious server.**
10. What is ”Wireshark” used for? **Answer: Capturing and analyzing network packets in real-time for troubleshooting and security analysis.**

V. Matching

Terms:

A. Nmap
B. Wireshark
C. ARP Poisoning
D. DDoS
E. Mantrap
F. Faraday Cage
G. Bollard
H. DNS Poisoning
I. Grep
J. Traceroute

Definitions:

1. Blocks electromagnetic signals.
2. Maps the path to a remote host.
3. Physical barrier against vehicles.
4. Network scanner and mapper.
5. Packet analyzer (GUI).
6. Redirects web traffic via corrupted cache.
7. Prevents tailgating.
8. Links attacker MAC to victim IP.
9. Overwhelms target with traffic.
10. Linux text search tool.

Answers: 1-F, 2-J, 3-G, 4-A, 5-B, 6-H, 7-E, 8-C, 9-D, 10-I

Chapter 9: Network Security Appliances and Technologies

Section A: Chapter Summary

Key Concepts

- **Firewalls:**
  - **Stateless vs. Stateful:** Stateless examines packets in isolation based on rules; Stateful tracks the state of active connections (SPI).
  - **Next-Generation Firewall (NGFW):** Deep packet inspection, application awareness (Layer 7), and intrusion prevention.
  - **Web Application Firewall (WAF):** Protects web servers from HTTP-specific attacks (SQLi, XSS).
  - **Unified Threat Management (UTM):** All-in-one device (Firewall, IDS/IPS, AV, Spam filter, URL filter).
- **Proxies and Gateways:**
  - **Forward Proxy:** Filters internal client traffic to the internet (caching, content filtering).
  - **Reverse Proxy:** Handles requests from the internet to internal servers (load balancing, SSL offloading).
  - **NAT Gateway:** Translates private internal IPs to public IPs.
- **Intrusion Detection/Prevention:**
  - **NIDS (Network IDS):** Passive monitoring of network traffic; alerts on threats.
  - **NIPS (Network IPS):** Inline monitoring; blocks malicious traffic automatically.
  - **Detection Methods:** Signature-based (known threats), Anomaly/Behavioral (baseline deviations), Heuristic (experience-based algorithms).
- **Deception & Disruption:**
  - **Honeypot:** A decoy system configured to be vulnerable to attract and study attackers.
  - **Sinkhole:** Redirects malicious traffic (e.g., botnet C&C traffic) to a dead-end address.
- **Network Access & Design:**
  - **NAC (Network Access Control):** Assesses device health (patches, AV) before granting network access (Agent vs. Agentless).
  - **VPN (Virtual Private Network):** Secure tunnel. Split Tunneling (only secure traffic goes through VPN) vs. Full Tunneling (all traffic).
  - **DLP (Data Loss Prevention):** Inspects packets to prevent sensitive data exfiltration.
  - **DMZ (Demilitarized Zone):** Subnet for public-facing services (web, email) separated from the internal LAN.
  - **Zero Trust:** Security model assuming no user or device is trusted by default, regardless of location.
- **Load Balancing:** Distributes traffic across multiple servers (Scheduling: Round-robin, Affinity; Config: Active-Active, Active-Passive).

Section B: Test Bank

I. Multiple Choice

1. Which device sits inline on the network and actively blocks malicious traffic based on signatures or anomalies?

   (a) NIDS
   (b) NIPS
   (c) Sniffer
   (d) Tap

   Answer: b

2. Which type of firewall filters traffic based on the state of the connection (e.g., ensuring an inbound packet matches an outbound request)?

   (a) Stateless
   (b) Packet Filter
   (c) Stateful
   (d) WAF

   Answer: c

3. A system designed to lure attackers away from critical systems to study their behavior is called a:

   (a) Bastion Host
   (b) Jump Server
   (c) Honeypot
   (d) Proxy

   Answer: c

4. Which technology allows an administrator to copy all traffic from a switch port to a monitoring port for analysis?

   (a) Port Security
   (b) Port Mirroring (SPAN)
   (c) VLAN Tagging
   (d) Trunking

   Answer: b

5. In a Load Balancing "Active-Passive" configuration, what happens?

   (a) All servers handle traffic simultaneously.
   (b) One node handles traffic while the other waits on standby for failover.
   (c) Traffic is split 50/50 between nodes.
   (d) Nodes are geographically separated.

   Answer: b

6. Which security appliance specifically protects web applications against XSS and SQL Injection attacks?

   (a) NGFW
   (b) WAF
   (c) VPN Concentrator
   (d) Spam Filter

   Answer: b

7. What does ”NAC” stand for?

   (a) Network Address Configuration
   (b) Network Access Control
   (c) Network Authentication Center
   (d) Node Access Check

   Answer: b

8. Which proxy server type is typically used to retrieve resources on behalf of a client from the internet (hiding the client)?

   (a) Reverse Proxy
   (b) Forward Proxy
   (c) Application Proxy
   (d) Open Proxy

   Answer: b

9. ”Zero Trust” architecture is based on which principle?

   (a) Trust but verify.
   (b) Never trust, always verify.
   (c) Trust internal users implicitly.
   (d) Verification is optional for known devices.

   Answer: b

10. Which VPN configuration routes only corporate traffic through the VPN tunnel while internet traffic goes directly to the ISP?

    (a) Full Tunnel
    (b) Split Tunnel
    (c) Site-to-Site
    (d) Always-on

    Answer: b

II. True/False

1. A NIDS can automatically block traffic that matches a signature. **Answer: False** (NIDS is passive; NIPS blocks)
2. A Reverse Proxy sits in front of web servers to protect them and distribute load. **Answer: True**
3. Signature-based detection is effective against zero-day (unknown) attacks. **Answer: False** (It requires a known signature)
4. Port Security relies on MAC addresses to authorize devices on a switch port. **Answer: True**
5. A UTM (Unified Threat Management) device combines multiple security functions into one appliance. **Answer: True**
6. In an "Active-Active" load balancing cluster, only one node processes traffic at a time. **Answer: False** (Both process traffic)
7. A DMZ is a highly secure zone where internal databases are stored. **Answer: False** (It is a buffer zone for public services; databases stay in the internal secure network)
8. DLP (Data Loss Prevention) systems can inspect outgoing emails for sensitive data. **Answer: True**
9. Heuristic monitoring uses a baseline of normal traffic to detect deviations. **Answer: False** (That is Anomaly/Behavioral; Heuristic uses algorithms/experience)
10. A Jump Server is used to access and manage devices in a separate security zone (like a DMZ). **Answer: True**

III. Fill-in-the-Blank

1. A _____ acts as an intermediary for requests from clients seeking resources from other servers. **Answer: Proxy Server**
2. _____ is the process of combining multiple network cards to increase bandwidth and redundancy. **Answer: NIC Teaming (or Port Aggregation)**
3. A _____ firewall inspects traffic up to Layer 7 (Application Layer). **Answer: Next-Generation (NGFW)**
4. _____ is a physical device that intercepts traffic between two network points for monitoring (unlike port mirroring). **Answer: Network TAP**
5. _____ refers to directing malicious traffic (like a botnet command) to a non-existent address to nullify it. **Answer: Sinkholing**
6. The _____ protocol helps prevent switching loops in a network. **Answer: Spanning Tree Protocol (STP)**
7. A _____ allows multiple internal hosts to share a single public IP address. **Answer: NAT Gateway**
8. _____ affinity is a load balancing method where a user is kept connected to the same server for the duration of their session. **Answer: Session (or Source IP)**

9. _____ is a set of rules on a router or firewall used to permit or deny traffic. **Answer: ACL (Access Control List)**
10. _____ monitoring detects attacks by comparing current activity against a ”normal” baseline. **Answer: Anomaly-based (or Behavioral)**

IV. Short Answer

1. What is the difference between a Firewall and a Network Access Control (NAC) system? **Answer: A firewall filters traffic based on rules; NAC validates the health/identity of the device before connection.**
2. Explain the purpose of a ”DMZ” (Demilitarized Zone). **Answer: To isolate public-facing services from the private internal network to minimize risk if they are compromised.**
3. What is ”SSL/TLS Offloading”? **Answer: The process of shifting the burden of encrypting/decrypting traffic from the web server to a load balancer or proxy.**
4. Define ”Zero Trust.” **Answer: A security concept where no user or device is trusted by default, requiring verification for every request.**
5. What is a ”Hardware Security Module” (HSM)? **Answer: A physical computing device that safeguards and manages digital keys for strong authentication and cryptoprocessing.**
6. Describe ”Port Mirroring” (SPAN). **Answer: Copying network packets from one switch port to another for analysis by a network probe or IDS.**
7. What is the function of ”DLP” (Data Loss Prevention)? **Answer: To identify, monitor, and protect data in use, data in motion, and data at rest from unauthorized exfiltration.**
8. Explain ”Split Tunneling” in VPNs. **Answer: Routing only critical/corporate traffic through the VPN while allowing other traffic (like web browsing) to go directly to the internet.**
9. What is ”MAC Filtering”? **Answer: A security method that allows or blocks access to a network based on the hardware address (MAC) of the device.**
10. What is the difference between ”Inline” and ”Passive” monitoring? **Answer: Inline traffic flows *through* the device (can block); Passive receives a *copy* of traffic (cannot block).**

V. Matching

Terms:

A. VPN
B. NIPS
C. WAF
D. DLP
E. Honeypot
F. Proxy
G. Load Balancer
H. NAT
I. NAC

J. HSM

Definitions:

1. Distributes traffic for high availability.
2. Encrypted tunnel for remote access.
3. Translates private IP to public IP.
4. Manages crypto keys in hardware.
5. Protects web apps from SQLi.
6. Prevents sensitive data leaks.
7. Checks device health before connect.
8. Intermediary that hides client identity.
9. Decoy system to trap attackers.
10. Inline device that blocks attacks.

Answers: 1-G, 2-A, 3-H, 4-J, 5-C, 6-D, 7-I, 8-F, 9-E, 10-B

Chapter 10: Cloud and Virtualization Security

Section A: Chapter Summary

Key Concepts

- **Cloud Computing Models:**
  - **SaaS (Software as a Service):** Vendor manages everything (apps, runtime, OS, hardware). Examples: Gmail, Office 365.
  - **PaaS (Platform as a Service):** Vendor manages OS/Hardware; Customer manages apps/data. Example: Google App Engine.
  - **IaaS (Infrastructure as a Service):** Vendor manages hardware; Customer manages OS, apps, data. Example: AWS EC2.
  - **XaaS (Anything as a Service):** Broad category for any service delivered via cloud.
- **Deployment Models:** Public (shared), Private (single org), Community (shared interest group), Hybrid (combination).
- **Virtualization:**
  - **Hypervisor Type I (Bare Metal):** Runs directly on hardware (e.g., ESXi). More efficient/secure.
  - **Hypervisor Type II (Hosted):** Runs on top of a host OS (e.g., VMware Workstation).
  - **VDI (Virtual Desktop Infrastructure):** Hosting user desktops on central servers.
  - **Containerization:** Isolating applications sharing the same OS kernel (lighter than VMs).
- **Security Issues:**
  - **VM Sprawl:** Unmanaged/undocumented VMs consuming resources and creating vulnerabilities.
  - **VM Escape:** An attacker breaks out of a VM to access the host system.
- **Cloud Security Controls:**
  - **CASB (Cloud Access Security Broker):** Intermediary software enforcing security policies between on-prem users and cloud services.
  - **SECaaS (Security as a Service):** Outsourcing security functions (e.g., email filtering) to the cloud.
- **Software-Defined Networking (SDN):** Separates the control plane from the data plane for programmable network management.

Section B: Test Bank

I. Multiple Choice

1. Which cloud service model gives the customer the most control over the operating system?

   (a) SaaS
   (b) PaaS
   (c) IaaS
   (d) DaaS

   Answer: c

2. Which type of hypervisor runs directly on the hardware without a host operating system?

   (a) Type I
   (b) Type II
   (c) Hosted
   (d) Application-based

   Answer: a

3. A security policy enforcement point positioned between enterprise users and cloud service providers is called a:

   (a) Firewall
   (b) CASB (Cloud Access Security Broker)
   (c) VPN Concentrator
   (d) Hypervisor

   Answer: b

4. Which virtualization risk involves an attacker moving from a virtual machine to the host system?

   (a) VM Sprawl
   (b) VM Escape
   (c) Buffer Overflow
   (d) Bluejacking

   Answer: b

5. Gmail and Microsoft Office 365 are examples of which cloud model?

   (a) IaaS
   (b) PaaS
   (c) SaaS
   (d) SECaaS

   Answer: c

6. Which deployment model involves a cloud infrastructure shared by several organizations with specific shared concerns?

   (a) Public Cloud
   (b) Private Cloud
   (c) Hybrid Cloud
   (d) Community Cloud

   Answer: d

7. What is ”VM Sprawl”?

   (a) When VMs crash simultaneously.
   (b) The uncontrolled creation of VMs leading to management and security issues.
   (c) When a VM consumes all host CPU.
   (d) The process of live migration.

   Answer: b

8. Which technology allows applications to run in isolated user spaces while sharing the same OS kernel?

   (a) Type I Hypervisor
   (b) Containerization
   (c) VDI
   (d) Sandboxing

   Answer: b

9. In a ”Shared Responsibility Model” for IaaS, who is responsible for patching the Guest OS?

   (a) The Cloud Provider
   (b) The Customer
   (c) The ISP
   (d) The Auditor

   Answer: b

10. What does VDI stand for?

    (a) Virtual Disk Interface
    (b) Virtual Desktop Infrastructure
    (c) Virtual Data Integration
    (d) Verified Digital Identity

    Answer: b

II. True/False

1. A Type II hypervisor is typically used in enterprise data centers for high performance. **Answer: False** (Type I is used for performance; Type II is for desktops)
2. In a SaaS model, the customer is responsible for patching the application. **Answer: False** (The vendor manages patches)
3. VM Escape allows an attacker to access other VMs on the same host. **Answer: True**
4. A Hybrid Cloud combines public and private cloud infrastructures. **Answer: True**
5. VDI stores user desktops on the local client machine. **Answer: False** (Stored on a central server)
6. SDN separates the control plane from the data plane. **Answer: True**
7. Fog computing brings processing closer to the edge/IoT devices rather than a centralized cloud. **Answer: True**
8. A private cloud is always hosted on-premises. **Answer: False** (Can be hosted externally but dedicated to one org)
9. Containers are generally more resource-heavy than Virtual Machines. **Answer: False** (Lighter)
10. SECaaS stands for Security as a Service. **Answer: True**

III. Fill-in-the-Blank

1. _____ is the delivery of computing services over the internet (servers, storage, databases). **Answer: Cloud Computing**
2. A _____ hypervisor runs on top of a host operating system. **Answer: Type II**
3. _____ is a technology that separates the control plane from the data plane in networking. **Answer: Software-Defined Networking (SDN)**
4. The phenomenon where the number of virtual machines grows beyond the administrator's ability to manage them is called _____. **Answer: VM Sprawl**
5. _____ is a cloud model where the vendor provides the platform/tools for development, but the customer manages the application. **Answer: PaaS (Platform as a Service)**
6. _____ computing processes data near the edge of the network, close to where it is generated. **Answer: Edge (or Fog)**
7. A _____ cloud is infrastructure provisioned for exclusive use by a single organization. **Answer: Private**
8. _____ enables running multiple operating systems on a single physical server. **Answer: Virtualization**
9. _____ is the process of moving a live VM from one physical server to another without downtime. **Answer: Live Migration**
10. A _____ acts as a gatekeeper, enforcing security policies for cloud services. **Answer: CASB**

IV. Short Answer

1. Explain the difference between IaaS and SaaS. **Answer: IaaS provides raw infrastructure (servers/network) for customers to manage; SaaS provides fully managed software applications.**
2. What is a ”Container”? **Answer: A lightweight virtualization method where applications share the host OS kernel but run in isolated user spaces.**
3. Define ”VM Escape.” **Answer: An attack where code running in a VM breaks out of the virtual environment to interact with the host hypervisor or hardware.**
4. What is the role of a ”Hypervisor”? **Answer: Software/Firmware that creates and manages virtual machines, allocating hardware resources to them.**
5. Describe ”VDI” (Virtual Desktop Infrastructure). **Answer: Hosting user desktop environments on a centralized server, accessible remotely by clients.**
6. What is ”Edge Computing”? **Answer: Processing data closer to the source (IoT devices) to reduce latency and bandwidth usage.**
7. Explain the ”Shared Responsibility Model.” **Answer: A security framework where the cloud provider protects the infrastructure, and the customer protects the data/configuration within it.**
8. What is a ”Hybrid Cloud”? **Answer: An environment combining a private cloud and a public cloud, allowing data/apps to share between them.**
9. What is a ”Thin Client”? **Answer: A lightweight computer that relies on a server (like VDI) for processing and storage, rather than local resources.**
10. Define ”Microservices.” **Answer: An architecture style where an application is built as a collection of small, independent services.**

V. Matching

Terms:

A. SaaS

B. IaaS

C. PaaS

D. Type I Hypervisor

E. Type II Hypervisor

F. VM Sprawl

G. VM Escape

H. CASB

I. Private Cloud

J. Community Cloud

Definitions:

1. Dedicated to a single organization.
2. Runs on host OS (e.g., VMware Workstation).
3. Vendor provides OS and tools (e.g., Azure App Service).
4. Unmanaged growth of VMs.
5. Enforces policy between user and cloud.
6. Vendor manages app (e.g., Salesforce).
7. Shared by organizations with common goals.
8. Bare metal (e.g., ESXi).

9. Breaking out of a VM to the host.
10. Vendor provides hardware (e.g., AWS EC2).

Answers: 1-I, 2-E, 3-C, 4-F, 5-H, 6-A, 7-J, 8-D, 9-G, 10-B

Chapter 11: Wireless Network Security

Section A: Chapter Summary

Key Concepts

- **Wireless Standards:** IEEE 802.11 family (a, b, g, n, ac, ax).
- **Wireless Attacks:**
  - **Rogue Access Point:** Unauthorized AP connected to the wired network (backdoor).
  - **Evil Twin:** Attacker sets up an AP with the same SSID as a legitimate AP to eavesdrop.
  - **Jamming:** Intentional interference to create a Denial of Service (DoS).
  - **Bluejacking:** Sending unsolicited messages via Bluetooth.
  - **Bluesnarfing:** Unauthorized theft of data via Bluetooth.
  - **War Driving:** Searching for Wi-Fi networks while moving (vehicle).
  - **Disassociation Attack:** Forcing a client to disconnect to capture the handshake.
- **Wireless Encryption Protocols:**
  - **WEP (Wired Equivalent Privacy):** Obsolete/Weak. Uses RC4 and static IVs (easy to crack).
  - **WPA (Wi-Fi Protected Access):** Interim replacement for WEP. Uses TKIP (Temporal Key Integrity Protocol).
  - **WPA2:** Uses AES (Advanced Encryption Standard) and CCMP. Current standard for many.
  - **WPA3:** Newest standard. Uses SAE (Simultaneous Authentication of Equals) to replace the 4-way handshake, preventing offline dictionary attacks.
- **Authentication Modes:**
  - **PSK (Pre-Shared Key):** Personal mode; everyone uses the same passphrase.
  - **Enterprise (802.1x):** Uses a RADIUS server for individual authentication.
- **Wireless Technologies:**
  - **NFC (Near Field Communication):** Very short range (payments).
  - **RFID (Radio Frequency Identification):** Inventory/tracking tags.
  - **WPS (Wi-Fi Protected Setup):** Push-button/PIN setup (Vulnerable to brute force).

Section B: Test Bank

I. Multiple Choice

1. Which wireless encryption standard uses AES and CCMP?

   (a) WEP
   (b) WPA
   (c) WPA2
   (d) TKIP

   Answer: c

2. An unauthorized access point connected to a corporate network by an employee is known as a:

   (a) Evil Twin
   (b) Rogue Access Point
   (c) Honeypot
   (d) Bluejack

   Answer: b

3. Which Bluetooth attack involves stealing data from a device?

   (a) Bluejacking
   (b) Bluesnarfing
   (c) Bluebugging
   (d) Pairing

   Answer: b

4. What is ”SAE” (Simultaneous Authentication of Equals) used in?

   (a) WPA
   (b) WPA2
   (c) WPA3
   (d) WEP

   Answer: c

5. Which authentication protocol is used in WPA2-Enterprise?

   (a) PSK
   (b) RADIUS (802.1x)
   (c) TACACS+
   (d) Kerberos

   Answer: b

6. What is the primary vulnerability of WPS (Wi-Fi Protected Setup)?

   (a) Weak encryption algorithm

(b) Vulnerable to PIN brute force attacks
(c) Requires a RADIUS server
(d) Does not support WPA2

Answer: b

7. An attacker sets up a fake AP with the same SSID as the coffee shop Wi-Fi to steal credentials. This is a:

(a) Rogue AP
(b) Evil Twin
(c) Replay Attack
(d) Jamming Attack

Answer: b

8. Which technology uses electromagnetic fields to identify and track tags attached to objects?

(a) NFC
(b) Bluetooth
(c) RFID
(d) Wi-Fi Direct

Answer: c

9. Which wireless standard operates exclusively in the 5 GHz band and offers high speeds (up to 7 Gbps)?

(a) 802.11g
(b) 802.11n
(c) 802.11ac
(d) 802.11b

Answer: c

10. Sending unsolicited messages to a Bluetooth device is called:

(a) Bluesnarfing
(b) Bluejacking
(c) War Driving
(d) Jamming

Answer: b

II. True/False

1. WEP is considered a secure protocol for modern wireless networks. **Answer: False** (It is obsolete/weak)
2. An Evil Twin is an AP configured to look like a legitimate AP. **Answer: True**
3. WPA3 uses SAE to prevent offline dictionary attacks against the handshake. **Answer: True**
4. 802.1x authentication allows every user to have a unique username/password. **Answer: True**
5. Disabling SSID broadcasting completely secures a wireless network. **Answer: False** (SSID can still be sniffed)
6. Bluejacking causes data theft. **Answer: False** (It only sends messages)
7. NFC has a longer range than Bluetooth. **Answer: False** (NFC is 4cm; Bluetooth is 10m+)
8. A ”Deauthentication Attack” is a type of Denial of Service. **Answer: True**
9. MAC Filtering is an effective method for stopping sophisticated attackers. **Answer: False** (MACs can be spoofed easily)
10. A heat map is used to visualize wireless signal coverage. **Answer: True**

III. Fill-in-the-Blank

1. _____ is the encryption protocol used by WPA2. **Answer: CCMP (or AES-CCMP)**
2. A _____ Access Point is an unauthorized AP installed on a network. **Answer: Rogue**
3. _____ involves driving around searching for open wireless networks. **Answer: War Driving**
4. The _____ protocol in WPA was a temporary replacement for WEP. **Answer: TKIP**
5. _____ is the IEEE standard for port-based network access control (used in Enterprise mode). **Answer: 802.1x**
6. _____ is the short-range wireless technology often used for ”tap to pay.” **Answer: NFC (Near Field Communication)**
7. An _____ attack forces a client to disconnect from an AP to capture the re-connection handshake. **Answer: Disassociation / Deauthentication**
8. _____ is the process of sending radio noise to block wireless signals (DoS). **Answer: Jamming**
9. _____ is the strongest wireless security standard currently available. **Answer: WPA3**
10. _____ refers to the name of the wireless network broadcast by the AP. **Answer: SSID (Service Set Identifier)**

IV. Short Answer

1. What is the main difference between WPA2-Personal and WPA2-Enterprise? **Answer: Personal uses a Pre-Shared Key (PSK); Enterprise uses a RADIUS server (802.1x) for individual authentication.**
2. Explain an ”Evil Twin” attack. **Answer: An attacker sets up a fake AP with the same SSID as a trusted network to trick users into connecting.**
3. Why is WEP insecure? **Answer: It uses RC4 with a short, static Initialization Vector (IV) that repeats, allowing keys to be cracked easily.**
4. What is ”Bluesnarfing”? **Answer: The unauthorized access and theft of information from a wireless device via a Bluetooth connection.**
5. Describe ”WPS” risks. **Answer: The PIN method is vulnerable to brute force attacks, allowing attackers to recover the WPA passphrase.**
6. What is the purpose of a ”Site Survey”? **Answer: To analyze the radio frequency environment (coverage, noise, interference) to optimize AP placement.**
7. Define ”Jamming” in wireless security. **Answer: A DoS attack where the attacker broadcasts RF noise to drown out legitimate signals.**
8. How does ”MAC Filtering” work? **Answer: The AP is configured to allow or deny connections based on the hardware MAC address of the client.**
9. What is ”RFID” used for? **Answer: Tracking objects (inventory, badges) using radio waves and tags.**
10. What does ”SAE” do in WPA3? **Answer: It replaces the PSK handshake, preventing offline dictionary attacks by requiring interaction for every guess.**

V. Matching

Terms:

A. WEP
B. WPA2
C. WPA3
D. SSID
E. Rogue AP
F. Evil Twin
G. Bluejacking
H. Bluesnarfing
I. NFC
J. 802.1x

Definitions:

1. Uses SAE for better security.
2. Unauthorized AP on the network.
3. Sending annoying Bluetooth messages.
4. The network name.
5. Obsolete/weak encryption.
6. Stealing data via Bluetooth.
7. Fake AP mimicking a real one.
8. Uses AES-CCMP encryption.
9. Authentication standard (Enterprise).
10. Very short-range wireless.

Answers: 1-C, 2-E, 3-G, 4-D, 5-A, 6-H, 7-F, 8-B, 9-J, 10-I

Chapter 12: Authentication

Section A: Chapter Summary

Key Concepts

- **Authentication Factors (MFA):**
  - **Something you Know:** Passwords, PINs, security questions.
  - **Something you Have:** Smart cards, hardware tokens, smartphones (push notifications/SMS).
  - **Something you Are:** Physiological biometrics (fingerprint, retina, iris, facial recognition).
  - **Somewhere you Are:** Geolocation, geofencing.
  - **Something you Do:** Behavioral biometrics (keystroke dynamics, gait analysis).
- **Password Security:**
  - **Attacks:** Brute force, Dictionary, Rainbow Tables (precomputed hashes), Password Spraying (common password against many accounts).
  - **Defenses:** Complexity, Expiration, **Salting** (adding random data before hashing to stop rainbow tables), **Key Stretching** (slowing down hashing with algorithms like Bcrypt, PBKDF2).
- **Biometric Metrics:**
  - **FAR (False Acceptance Rate):** Imposter allowed in (Type II error).
  - **FRR (False Rejection Rate):** Legitimate user denied (Type I error).
  - **CER (Crossover Error Rate):** The rate where FAR equals FRR; lower CER indicates a more accurate system.
- **Authentication Protocols & Services:**
  - **RADIUS:** Centralized AAA (Authentication, Authorization, Accounting) protocol using UDP. Encrypts only the password.
  - **TACACS+:** Cisco proprietary AAA protocol using TCP. Encrypts the entire packet. Separates authentication and authorization.
  - **Kerberos:** Network authentication protocol using ”tickets” to prevent replay attacks. Relies on a KDC (Key Distribution Center) and time synchronization.
  - **LDAP:** Protocol for accessing and maintaining distributed directory information services (e.g., Active Directory).
- **Federation & SSO:**
  - **SAML (Security Assertion Markup Language):** XML-based standard for exchanging authentication data between an Identity Provider (IdP) and a Service Provider (SP).
  - **OAuth / OpenID Connect:** Standards for authorization and authentication (commonly used for ”Log in with Google/Facebook”).
  - **Shibboleth:** Open-source software implementing SAML for single sign-on.

Section B: Test Bank

I. Multiple Choice

1. Which biometric error rate represents the percentage of imposters incorrectly granted access?

   (a) FRR (False Rejection Rate)
   (b) CER (Crossover Error Rate)
   (c) FAR (False Acceptance Rate)
   (d) TGT (Ticket Granting Ticket)

   Answer: c

2. What is the primary benefit of ”Salting” passwords?

   (a) It encrypts the password with a public key.
   (b) It prevents the use of precomputed rainbow tables.
   (c) It forces users to change passwords frequently.
   (d) It speeds up the hashing process.

   Answer: b

3. Which authentication protocol uses a Key Distribution Center (KDC) and Tickets?

   (a) RADIUS
   (b) TACACS+
   (c) Kerberos
   (d) LDAP

   Answer: c

4. A user logging in with a password and a fingerprint scan is using:

   (a) Single-factor authentication
   (b) Multifactor authentication (MFA)
   (c) Mutual authentication
   (d) Federated identity

   Answer: b

5. Which open standard is primarily used for *authorization*, allowing users to share private resources (like photos) with another site without sharing their credentials?

   (a) SAML
   (b) OAuth
   (c) LDAP
   (d) RADIUS

   Answer: b

6. Which AAA protocol encrypts the entire payload and uses TCP for reliability?

   (a) RADIUS

(b) Kerberos
(c) TACACS+
(d) NTLM

Answer: c

7. ”Keystroke Dynamics” is an example of which authentication factor?

(a) Something you Know
(b) Something you Have
(c) Something you Are
(d) Something you Do

Answer: d

8. Which XML-based standard is commonly used for web-based Single Sign-On (SSO)?

(a) SAML
(b) RADIUS
(c) PAP
(d) CHAP

Answer: a

9. What is the purpose of ”Key Stretching” algorithms like Bcrypt or PBKDF2?

(a) To compress the password for storage.
(b) To slow down the hashing process to resist brute-force attacks.
(c) To allow passwords to be recovered by administrators.
(d) To transmit passwords securely over HTTP.

Answer: b

10. A smart card used for entry into a secure building falls under which factor?

(a) Something you Know
(b) Something you Have
(c) Something you Are
(d) Somewhere you Are

Answer: b

II. True/False

1. The Crossover Error Rate (CER) is the point where the FAR and FRR are equal. **Answer: True**
2. RADIUS uses TCP and encrypts the entire packet. **Answer: False** (Uses UDP; encrypts only password)
3. A password is an example of ”Something you Are.” **Answer: False** (Something you Know)

4. Kerberos relies heavily on time synchronization between clients and servers. **Answer: True**
5. Federation allows a user to use one set of credentials across different organizations. **Answer: True**
6. A Dictionary Attack tries every possible combination of characters to crack a password. **Answer: False** (That is Brute Force; Dictionary uses a wordlist)
7. FRR (False Rejection Rate) is also known as a Type I error. **Answer: True**
8. TOTP (Time-based One-Time Password) generates a code that is valid indefinitely. **Answer: False** (Valid for a short window, e.g., 30-60 seconds)
9. LDAP is a protocol used to query and modify items in directory services like Active Directory. **Answer: True**
10. OpenID Connect is built on top of the OAuth 2.0 protocol to provide authentication. **Answer: True**

III. Fill-in-the-Blank

1. _____ is the process of proving a user's identity (e.g., logging in). **Answer: Authentication**
2. A _____ table contains precomputed hashes used to speed up password cracking. **Answer: Rainbow**
3. _____ is a Cisco proprietary protocol that separates authentication, authorization, and accounting. **Answer: TACACS+**
4. _____ biometrics analyzes user behavior, such as typing rhythm or mouse movement. **Answer: Behavioral**
5. In a Kerberos environment, the _____ issues tickets to authenticated users. **Answer: KDC (Key Distribution Center)**
6. _____ involves adding random bits to a password before hashing it to ensure unique hashes. **Answer: Salting**
7. _____ is an XML-based standard for exchanging authentication and authorization data between security domains. **Answer: SAML (Security Assertion Markup Language)**
8. _____ is an attack where an intruder attempts to log in to many different accounts using a few common passwords. **Answer: Password Spraying**
9. A _____ token generates a password that changes at a fixed interval (e.g., every 60 seconds). **Answer: TOTP (Time-based One-Time Password)**
10. _____ is the property of a biometric system where an unauthorized person is incorrectly admitted. **Answer: False Acceptance Rate (FAR)**

IV. Short Answer

1. Explain "Multifactor Authentication" (MFA). **Answer: Authentication requiring two or more *different* types of factors (e.g., password + token).**
2. What is the difference between Identification and Authentication? **Answer: Identification is claiming an identity (username); Authentication is proving it (password).**
3. Define "Single Sign-On" (SSO). **Answer: A property allowing a user to log in once and gain access to multiple related but independent software systems.**
4. What is "Shibboleth"? **Answer: An open-source software project that provides Single Sign-On capabilities (often using SAML).**
5. Why is "RADIUS" commonly used in wireless networks? **Answer: It provides centralized authentication for users connecting to network access points (802.1x).**
6. Describe a "Retina Scan." **Answer: A biometric scan of the blood vessel patterns at the back of the eye.**
7. What is "Geofencing" in authentication? **Answer: Restricting authentication attempts to a specific geographic area using GPS boundaries.**
8. Explain "Credential Stuffing." **Answer: Using stolen username/password pairs from one breach to attempt logins on other unrelated websites.**
9. What is "OpenID Connect"? **Answer: An identity layer on top of the OAuth 2.0 protocol that allows clients to verify the identity of the end-user.**
10. What is the purpose of "CHAP" (Challenge-Handshake Authentication Protocol)? **Answer: To authenticate a user or network host without sending the password over the network (uses a 3-way handshake).**

V. Matching

Terms:

A. Something you Know
B. Something you Have
C. Something you Are
D. Something you Do
E. Somewhere you Are
F. OAuth
G. SAML
H. Kerberos
I. TACACS+
J. RADIUS

Definitions:

1. Authorization standard (e.g., social login).
2. A Smart Card.
3. A Password.
4. Location-based authentication.
5. Fingerprint Scan.
6. Centralized AAA, encrypts whole packet.
7. Typing rhythm (Keystroke dynamics).
8. XML standard for Federation.
9. Centralized AAA, encrypts only password.
10. Uses Tickets and Time-stamps.

Answers: 1-F, 2-B, 3-A, 4-E, 5-C, 6-I, 7-D, 8-G, 9-J, 10-H

Chapter 13: Incident Preparation, Response, and Investigation

Section A: Chapter Summary

Key Concepts

- **Incident Response (IR) Process (PICERL):**
  - **Preparation:** Planning, tools, training, IRP (Incident Response Plan).
  - **Identification:** Detecting and determining if an event is an incident.
  - **Containment:** Limiting damage (Isolation vs. Segmentation).
  - **Eradication:** Removing the root cause (malware, accounts).
  - **Recovery:** Restoring systems and verifying function.
  - **Lessons Learned:** Post-incident analysis to improve future response.
- **IR Exercises:**
  - **Tabletop:** Discussion-based exercise in a conference room.
  - **Walkthrough:** Reviewing processes step-by-step.
  - **Simulation:** Hands-on drill testing the actual response.
- **Attack Frameworks:**
  - **Cyber Kill Chain:** 7 steps (Recon, Weaponization, Delivery, Exploitation, Installation, C2, Actions on Objectives).
  - **MITRE ATT&CK:** Matrix of tactics and techniques based on real-world observations.
  - **Diamond Model:** Analyzing intrusion events (Adversary, Capability, Infrastructure, Victim).
- **Digital Forensics:**
  - **Order of Volatility:** Capture most fleeting data first (CPU Cache $\rightarrow$ RAM $\rightarrow$ Swap $\rightarrow$ HDD $\rightarrow$ Remote Logs).
  - **Chain of Custody:** Documentation of evidence handling to ensure integrity for court (Admissibility).
  - **Legal Hold:** Preserving data relevant to litigation.
- **Data Sources:** Logs (Syslog, Firewall, SIEM), Metadata, NetFlow (traffic statistics).

Section B: Test Bank

I. Multiple Choice

1. Which step of the Incident Response process involves removing the root cause of the incident?

   (a) Containment

   (b) Eradication

(c) Identification

(d) Recovery

Answer: b

2. What is the ”Order of Volatility”?

   (a) The order in which systems should be rebooted.

   (b) The sequence for collecting evidence from most fleeting to least fleeting.

   (c) The priority list for restoring services.

   (d) The chain of command during an incident.

   Answer: b

3. Which attack framework focuses on the four nodes: Adversary, Capability, Infrastructure, and Victim?

   (a) Cyber Kill Chain

   (b) MITRE ATT&CK

   (c) Diamond Model

   (d) OWASP Top 10

   Answer: c

4. Which IR exercise is a discussion-based review of roles and responses without touching live systems?

   (a) Simulation

   (b) Tabletop

   (c) Red Teaming

   (d) Full-scale Drill

   Answer: b

5. Which item is the *most* volatile and should be collected first?

   (a) Hard Drive Data

   (b) CPU Registers / Cache

   (c) RAM

   (d) Archived Backup Tapes

   Answer: b

6. What document tracks the handling of evidence to ensure it is admissible in court?

   (a) Incident Response Plan

   (b) Chain of Custody

   (c) Service Level Agreement

   (d) Non-Disclosure Agreement

   Answer: b

7. ”NetFlow” data is primarily used to analyze:

(a) The content of email messages.
(b) Network traffic metadata (source/dest IP, volume).
(c) The contents of RAM.
(d) Hard drive file structures.

Answer: b

8. Which step of the Cyber Kill Chain involves transmitting the weaponized object to the victim?

(a) Reconnaissance
(b) Exploitation
(c) Delivery
(d) Command and Control

Answer: c

9. Disconnecting a compromised server from the network is an example of:

(a) Identification
(b) Containment
(c) Recovery
(d) Preparation

Answer: b

10. What is a ”Legal Hold”?

(a) A pause on data destruction to preserve evidence for litigation.
(b) Arresting a suspect.
(c) Seizing physical hardware.
(d) A contract dispute resolution.

Answer: a

II. True/False

1. The ”Lessons Learned” phase occurs before the incident happens. **Answer: False** (It happens after recovery)
2. RAM is more volatile than a Hard Disk Drive. **Answer: True**
3. MITRE ATT&CK is a knowledge base of adversary tactics and techniques. **Answer: True**
4. Isolation involves keeping the attacker connected but monitored. **Answer: False** (Isolation disconnects the system)
5. A ”Runbook” typically contains automated or conditional steps for incident response. **Answer: True**
6. The `dd` command is used in Linux for creating bit-by-bit forensic images. **Answer: True**

7. E-discovery is the process of identifying and collecting electronic evidence for legal proceedings. **Answer: True**
8. In the Order of Volatility, remote logs are collected before CPU registers. **Answer: False** (CPU registers are first)
9. Containment strategies can include network segmentation. **Answer: True**
10. The Cyber Kill Chain was developed by Lockheed Martin. **Answer: True**

III. Fill-in-the-Blank

1. The phase of IR where systems are restored to normal operation is called _____. **Answer: Recovery**
2. _____ is the documentation of who handled evidence, when, and why. **Answer: Chain of Custody**
3. A _____ exercise involves role-playing a scenario in a conference room setting. **Answer: Tabletop**
4. _____ is the process of finding the root cause and removing malware from the system. **Answer: Eradication**
5. The _____ model analyzes intrusions using four vertices: Adversary, Capability, Infrastructure, Victim. **Answer: Diamond**
6. A forensic copy of a hard drive is often called a _____ image. **Answer: Bit-stream (or Mirror)**
7. _____ refers to data about data (e.g., email headers, file timestamps). **Answer: Metadata**
8. In the Cyber Kill Chain, the _____ phase involves the attacker communicating with the compromised system remotely. **Answer: Command and Control (C2)**
9. _____ is a standard protocol for forwarding log messages on IP networks. **Answer: Syslog**
10. A _____ is a comprehensive guide or checklist of actions for responding to a specific type of incident. **Answer: Playbook**

IV. Short Answer

1. What is the purpose of the ”Lessons Learned” (Post-Incident Activity) phase? **Answer: To analyze what happened, what went wrong, and how to improve the process for future incidents.**
2. Define ”Order of Volatility.” **Answer: The sequence in which evidence should be collected based on how easily the data is lost (most fugitive to least fugitive).**
3. Explain the difference between ”Containment” and ”Eradication.” **Answer: Containment stops the spread of the threat; Eradication removes the threat from the system completely.**
4. What is a ”Write Blocker” used for in forensics? **Answer: To prevent any modifications to the original evidence drive while creating an image.**

5. Describe the ”MITRE ATT&CK” framework. **Answer: A curated knowledge base of adversarial tactics, techniques, and procedures (TTPs) based on real-world observations.**
6. What is ”SOAR”? **Answer: Security Orchestration, Automation, and Response; tools to automate incident response workflows.**
7. Why is ”Time Synchronization” (NTP) important in forensics? **Answer: To ensure that logs from different devices can be accurately correlated to reconstruct the timeline of an attack.**
8. What is ”Admissibility” in the context of digital evidence? **Answer: The requirement that evidence must be relevant, authentic, and legally obtained to be used in court.**
9. Explain ”Data Sanitization” in recovery. **Answer: Ensuring no malware remains on a system before restoring it to production (or wiping data before disposal).**
10. What is ”Provenance” in forensics? **Answer: The documentation of the origin and history of a piece of evidence (tracing it to the source).**

V. Matching

Terms:

A. Preparation
B. Identification
C. Containment
D. Eradication
E. Recovery
F. Lessons Learned
G. Tabletop
H. Walkthrough
I. Cyber Kill Chain
J. Chain of Custody

Definitions:

1. Removing the root cause of an incident.
2. Restoring systems to business-as-usual.
3. Establishing an IRP and training.
4. Determining if an event is an incident.
5. Limiting the scope/damage of an attack.
6. Documenting evidence handling.
7. Discussion-based training exercise.
8. 7-stage attack framework.
9. Hands-on step-by-step review of a plan.
10. Post-incident analysis/reporting.

Answers: 1-D, 2-E, 3-A, 4-B, 5-C, 6-J, 7-G, 8-I, 9-H, 10-F

Chapter 14: Cybersecurity Resilience

Section A: Chapter Summary

Key Concepts

- **Business Continuity Plan (BCP):** Strategic document ensuring operations continue during a disaster.
  - **Business Impact Analysis (BIA):** Identifies critical functions and quantifies impact of loss.
  - **Disaster Recovery Plan (DRP):** Focuses specifically on restoring IT functions.
  - **MTBF (Mean Time Between Failures):** Average time a component lasts before failure.
  - **MTTR (Mean Time to Recovery):** Average time to repair a failed device.
  - **RPO (Recovery Point Objective):** Max tolerable data loss (time between backups).
  - **RTO (Recovery Time Objective):** Max tolerable downtime (time to restore).
- **Redundancy (Fault Tolerance):**
  - **Servers:** Clustering (Active/Active or Active/Passive).
  - **Disks (RAID):**
    - **RAID 0:** Striping (Speed, no redundancy).
    - **RAID 1:** Mirroring (Redundancy, costlier).
    - **RAID 5:** Striping with Parity (Redundancy + Speed, requires 3+ disks).
    - **RAID 10:** Mirroring + Striping.
  - **Network:** Load balancers, NIC Teaming, Multipath IO.
  - **Power:** Dual power supplies, UPS (Uninterruptible Power Supply), Generators.
- **Recovery Sites:**
  - **Hot Site:** Fully functional mirror, expensive, near-immediate recovery.
  - **Warm Site:** Has equipment/links but requires data restoration; moderate cost/time.
  - **Cold Site:** Empty facility (power/AC only); cheapest, longest recovery.
- **Backups:**
  - **Full:** Backs up everything; clears archive bit.
  - **Differential:** Backs up changes since last Full; does *not* clear archive bit. (Restore = Full + Last Diff).
  - **Incremental:** Backs up changes since last backup (any type); clears archive bit. (Restore = Full + All Incrementals).
  - **Snapshot:** Image of system state at a specific time.
  - **3-2-1 Rule:** 3 copies of data, 2 different media types, 1 offsite.
- **Policies:**
  - **Types:** Standard (Required), Guideline (Suggested), Policy (Required High-level rule).
  - **Personnel:** Separation of Duties, Job Rotation, Mandatory Vacation, Least Privilege.
  - **Data:** Classification (Public, Private, Confidential), Retention, Gover-

Section B: Test Bank

I. Multiple Choice

1. Which RAID level uses disk striping with parity to provide fault tolerance?

   (a) RAID 0
   (b) RAID 1
   (c) RAID 5
   (d) RAID 10

   Answer: c

2. What is the primary purpose of a ”Warm Site”?

   (a) To provide immediate failover capability with real-time data synchronization.
   (b) To provide a facility with power and cooling but no equipment.
   (c) To provide equipment and connectivity but requires data restoration.
   (d) To store paper records only.

   Answer: c

3. Which backup type backs up all data modified since the last *full* backup and does not clear the archive bit?

   (a) Full Backup
   (b) Incremental Backup
   (c) Differential Backup
   (d) Snapshot

   Answer: c

4. What does ”RPO” (Recovery Point Objective) define?

   (a) The time it takes to restore a system.
   (b) The maximum acceptable amount of data loss measured in time.
   (c) The average time between hardware failures.
   (d) The priority order for restoring servers.

   Answer: b

5. Which personnel policy requires employees to take time off to audit their activities for fraud?

   (a) Separation of Duties
   (b) Least Privilege
   (c) Job Rotation
   (d) Mandatory Vacation

   Answer: d

6. Which device provides short-term battery power to allow for a graceful shutdown during an outage?

(a) Generator
(b) UPS
(c) PDU
(d) RAID Controller

Answer: b

7. A document that outlines specific mandatory requirements or rules that must be met is a:

(a) Guideline
(b) Standard
(c) Procedure
(d) Policy

Answer: d

8. Which data classification level would typically be applied to a company's trade secrets?

(a) Public
(b) Private
(c) Confidential / Proprietary
(d) Unclassified

Answer: c

9. High Availability (HA) is best described as:

(a) Ensuring data is encrypted at rest.
(b) The ability to withstand outages and provide continuous processing.
(c) Storing backups in a remote location.
(d) Preventing unauthorized access to the network.

Answer: b

10. Which redundancy technique involves connecting multiple network interfaces to increase bandwidth and failover?

(a) Clustering
(b) NIC Teaming
(c) RAID
(d) Multipath I/O

Answer: b

II. True/False

1. RAID 0 provides redundancy and fault tolerance. **Answer: False** (Only performance/speed)
2. A Cold Site is the most expensive type of recovery site. **Answer: False** (Cheapest; Hot Site is most expensive)
3. An Incremental backup clears the archive bit after running. **Answer: True**
4. Separation of Duties ensures that no single person has complete control over a critical process. **Answer: True**
5. MTTR stands for Mean Time to Recovery. **Answer: True**
6. A Guideline is a mandatory rule that must be followed. **Answer: False** (Guidelines are recommendations)
7. Active/Passive clustering involves all servers handling traffic simultaneously. **Answer: False** (Active/Passive has standby servers)
8. Data Retention policies specify how long data must be kept and how it should be destroyed. **Answer: True**
9. A full backup is the fastest to restore from. **Answer: True**
10. Air gapping involves physically isolating a secure network from unsecured networks. **Answer: True**

III. Fill-in-the-Blank

1. _____ is the average time a device is expected to function before it fails. **Answer: MTBF (Mean Time Between Failures)**
2. A _____ site is a fully operational facility with real-time data replication, ready for immediate switchover. **Answer: Hot**
3. _____ is the practice of limiting user access rights to only what is necessary to perform their job. **Answer: Least Privilege**
4. _____ backups save all data that has changed since the last backup of any type. **Answer: Incremental**
5. _____ is a RAID level that uses disk mirroring. **Answer: RAID 1**
6. _____ analysis is the first step in BCP, identifying critical functions and the impact of downtime. **Answer: Business Impact (BIA)**
7. A _____ is a snapshot of a system's state (files, registry) used to revert changes. **Answer: System Image / Restore Point**
8. The _____ rule suggests having 3 copies of data, on 2 different media, with 1 offsite. **Answer: 3-2-1**
9. _____ involves organizing data into categories (e.g., Public, Secret) to apply appropriate protections. **Answer: Data Classification**
10. _____ ensures that if one power supply fails, the server remains operational. **Answer: Dual Power Supply / Redundant Power**

IV. Short Answer

1. Explain the difference between RTO and RPO. **Answer: RTO is the target time to restore service; RPO is the target time limit for data loss (backup frequency).**
2. What is the difference between a Differential and an Incremental backup? **Answer: Differential captures changes since the last Full backup; Incremental captures changes since the last backup of any kind.**
3. Define "High Availability." **Answer: A system design that ensures a certain degree of operational continuity (uptime) during a given measurement period.**
4. What is "Job Rotation" and why is it used? **Answer: Moving employees between jobs to prevent fraud (no one person controls a process indefinitely) and cross-train.**
5. Describe "Tabletop Exercises." **Answer: Discussion-based sessions where team members talk through their roles during an emergency scenario without touching live systems.**
6. What is a "Cold Site"? **Answer: A recovery facility that provides space and power but lacks equipment and data; it takes the longest to activate.**
7. Why is "RAID 5" popular for file servers? **Answer: It balances fault tolerance (can lose 1 disk) with efficient storage usage (striping with parity).**
8. Explain "Clean Desk Policy." **Answer: A policy requiring sensitive information (papers, electronics) to be secured/locked away when the user leaves their workspace.**
9. What is "Cloud Storage" in the context of resilience? **Answer: Offsite storage of data backups over the internet, providing geographic separation and scalability.**
10. Define "Single Point of Failure." **Answer: A part of a system that, if it fails, will stop the entire system from working.**

V. Matching

Terms:

A. RAID 0

B. RAID 1

C. Hot Site

D. Cold Site

E. Full Backup

F. Differential Backup

G. RPO

H. RTO

I. BIA

J. AUP

Definitions:

1. Mirroring.
2. Striping (No redundancy).
3. Immediate recovery site.
4. Empty facility recovery site.
5. Clears archive bit.
6. Does not clear archive bit.

7. Max tolerable data loss.
8. Target recovery time.
9. Identifies critical functions.
10. Rules for system usage.

Answers: 1-B, 2-A, 3-C, 4-D, 5-E, 6-F, 7-G, 8-H, 9-I, 10-J

Chapter 15: Risk Management and Data Privacy

Section A: Chapter Summary

Key Concepts

- **Risk Terminology:**
  - **Asset:** Something of value.
  - **Threat:** Potential danger.
  - **Vulnerability:** Weakness.
  - **Risk:** Probability of a threat exploiting a vulnerability.
  - **Inherent Risk:** Risk before controls.
  - **Residual Risk:** Risk remaining after controls.
  - **Risk Appetite:** Level of risk an org is willing to accept.
- **Risk Assessment (Quantitative):**
  - **SLE (Single Loss Expectancy):** Asset Value (AV) $\times$ Exposure Factor (EF).
  - **ALE (Annualized Loss Expectancy):** SLE $\times$ ARO (Annualized Rate of Occurrence).
- **Risk Strategies:**
  - **Accept:** Acknowledge and do nothing (low impact/cost).
  - **Transfer:** Shift liability (Cyber insurance).
  - **Avoid:** Eliminate the cause (stop the activity).
  - **Mitigate:** Implement controls to reduce risk.
- **Security Controls:**
  - **Technical:** Firewall, Encryption, IDS.
  - **Managerial (Administrative):** Policies, Background checks.
  - **Operational:** Guards, Training.
  - **Types:** Preventative, Detective, Corrective, Deterrent, Compensating, Physical.
- **Data Privacy:**
  - **PII (Personally Identifiable Information):** Data identifying a person.
  - **Privacy Impact Assessment (PIA):** Analyzing risks to PII.
  - **Data Destruction:** Shredding, Degaussing (magnets), Wiping (overwriting), Pulping.

Section B: Test Bank

I. Multiple Choice

1. Which risk calculation represents the expected monetary loss for a single event?

(a) ARO
(b) ALE
(c) SLE
(d) MTBF

Answer: c

2. Buying cyber insurance is an example of which risk management strategy?

(a) Avoidance
(b) Acceptance
(c) Mitigation
(d) Transference

Answer: d

3. Which type of control allows a security guard to check IDs at the door?

(a) Technical
(b) Operational
(c) Managerial
(d) Logical

Answer: b

4. What is ”Residual Risk”?

(a) The risk before any controls are applied.
(b) The risk transferred to an insurance company.
(c) The risk remaining after security controls are implemented.
(d) The total asset value.

Answer: c

5. Which data destruction method involves using strong magnets to scramble data on magnetic media?

(a) Shredding
(b) Pulping
(c) Degaussing
(d) Burning

Answer: c

6. A security camera (CCTV) is primarily which type of control?

(a) Preventative
(b) Detective
(c) Corrective
(d) Compensating

Answer: b

7. Which agreement defines the level of service expected from a vendor (e.g., 99.9% uptime)?

   (a) NDA
   (b) SLA (Service Level Agreement)
   (c) MOU
   (d) ISA

   Answer: b

8. Which formula calculates ALE?

   (a) SLE $\times$ ARO
   (b) AV $\times$ EF
   (c) SLE / ARO
   (d) AV + EF

   Answer: a

9. What is ”Data Sovereignty”?

   (a) The right to be forgotten.
   (b) Encrypting data in transit.
   (c) Data being subject to the laws of the country where it is stored.
   (d) Backup retention policies.

   Answer: c

10. Which privacy-enhancing technology replaces sensitive data with a non-sensitive equivalent (a token)?

    (a) Degaussing
    (b) Tokenization
    (c) Shredding
    (d) Hashing

    Answer: b

II. True/False

1. Qualitative risk assessment uses numerical values and monetary costs. **Answer: False** (Quantitative uses numbers; Qualitative uses high/med/low)

2. Risk Mitigation involves implementing controls to reduce the likelihood or impact of a risk. **Answer: True**

3. Degaussing is effective for destroying data on SSDs (Solid State Drives). **Answer: False** (Degaussing works on magnetic media; SSDs need wiping/shredding)

4. An NDA (Non-Disclosure Agreement) is a legal contract outlining confidential material. **Answer: True**

5. ARO represents how often a risk is expected to occur in a year. **Answer: True**

6. PII stands for Protected Internet Information. **Answer: False** (Personally Identifiable Information)
7. A Corrective control restores systems after an incident occurs (e.g., backups). **Answer: True**
8. Risk Acceptance is typically chosen when the cost of the control exceeds the cost of the risk. **Answer: True**
9. GDPR is a US federal law protecting health information. **Answer: False** (GDPR is EU privacy; HIPAA is US health)
10. Data Masking hides data by replacing actual characters with other characters (e.g., asterisks). **Answer: True**

III. Fill-in-the-Blank

1. _____ is the probability of a threat exploiting a vulnerability. **Answer: Risk**
2. _____ risk is the level of risk before any measures are taken. **Answer: Inherent**
3. A _____ control discourages an attacker from attempting an attack (e.g., a warning sign). **Answer: Deterrent**
4. _____ is the process of overwriting storage media with random data to make it unrecoverable. **Answer: Wiping**
5. The formula for SLE (Single Loss Expectancy) is Asset Value $\times$ _____. **Answer: Exposure Factor (EF)**
6. _____ is a risk strategy where an organization decides to stop engaging in the risky activity. **Answer: Avoidance**
7. A _____ is a document identifying potential risks, their severity, and mitigation status. **Answer: Risk Register**
8. _____ is a method of verifying that a user is human (e.g., selecting traffic lights). **Answer: CAPTCHA**
9. _____ refers to turning paper documents into pulp to destroy data. **Answer: Pulping**
10. _____ Agreement is a contract between two or more parties establishing a business partnership. **Answer: BPA (Business Partnership Agreement)**

IV. Short Answer

1. Define ”Risk Appetite.” **Answer: The amount of risk an organization is willing to accept in pursuit of its objectives.**
2. Explain ”Risk Transference.” **Answer: Moving the financial impact of a risk to a third party, typically through insurance.**
3. What is the difference between SLE and ALE? **Answer: SLE is the cost of a single event; ALE is the expected yearly cost (SLE $\times$ Frequency).**

4. What does a ”Privacy Impact Assessment” (PIA) do? **Answer: It identifies and evaluates the risks associated with collecting, maintaining, and disseminating PII.**
5. Describe ”Data Minimization.” **Answer: Collecting only the data that is strictly necessary for the specified purpose.**
6. What is a ”Compensating Control”? **Answer: An alternative control used when a primary control cannot be implemented (e.g., isolation instead of patching).**
7. Define ”Degaussing.” **Answer: Using a strong magnetic field to erase data from magnetic media (hard drives, tapes).**
8. What is the purpose of an ”Acceptable Use Policy” (AUP)? **Answer: To define how employees are permitted to use company systems and the consequences of misuse.**
9. Explain ”Supply Chain Risk.” **Answer: The risk associated with third-party vendors, hardware, or software introduced into the organization’s environment.**
10. What is ”Data Anonymization”? **Answer: The process of removing PII from data sets so that the people described remain anonymous.**

V. Matching

Terms:

A. SLA
B. NDA
C. ISA
D. MOU
E. SLE
F. ALE
G. ARO
H. PII
I. PHI
J. GDPR

Definitions:

1. Service Level Agreement (uptime guarantee).
2. Non-Disclosure Agreement (confidentiality).
3. Single Loss Expectancy (cost per incident).
4. Annualized Loss Expectancy (cost per year).
5. Annualized Rate of Occurrence (frequency).
6. Personally Identifiable Information.
7. Protected Health Information.
8. EU Data Protection Regulation.
9. Memorandum of Understanding (mutual goal).
10. Interconnection Security Agreement.

Answers: 1-A, 2-B, 3-E, 4-F, 5-G, 6-H, 7-I, 8-J, 9-D, 10-C