Exam Questions Based on Slides (Chapters 1-5)

1. Ransomware Attack on a University

The university's student portal and research data servers were encrypted in a ransomware attack. The attackers are demanding payment to restore access.

a. Which two elements of the CIA triad are most directly violated? Justify your answer.

b. Referring to the Parkerian Hexad, which additional principle is compromised if the attackers also exfiltrate (steal) the data before encrypting it?

c. What is the primary purpose of cryptography that could have mitigated the impact of this attack on the stolen data, even if the servers were encrypted?

2. Weak Authentication at an E-Commerce Company

An online retailer uses only simple username and password authentication for its customers and administrative staff.

a. This practice relies on only one factor of authentication. Name the factor and explain why it is considered weak.

b. Describe two other factors of authentication the company could implement for its administrators to create a multifactor system. Provide a specific example for each.

c. The company's CEO argues, "Our passwords are very long and complex, so we are secure." Using Kerckhoffs's Principle, explain why this argument is flawed.

3. Flawed Access Control in a Bank

A junior bank teller's computer account has been compromised. The investigation reveals the teller had access to:

· The internal customer database (read/write)

· The software used to approve small loans

· The audit logs of all transactions

a. Which fundamental security principle (Principle of Least Privilege) was violated in this scenario? Explain.

b. For each of the three resources listed, recommend a more appropriate access control model (e.g., RBAC, MAC, ABAC) that could limit access and justify your choice.

c. Beyond technical controls, name one administrative control (policy or procedure) the bank should implement to prevent such over-provisioning of access in the future.

4. Data Protection and Regulations

A healthcare clinic stores patient records digitally. A laptop containing unencrypted patient records is stolen from a doctor's car.

a. Which U.S. regulation (HIPAA) was likely violated in this incident? What is its primary purpose?

b. Explain the difference between due care and due diligence in the context of the clinic's responsibility to protect patient data.

c. Name two cryptographic methods (one for data at rest, one for data in motion) the clinic should have used to protect this data and prevent a breach even if the device was stolen.

5. Cryptography Concepts You intercept the following ciphertext, encrypted with a Caesar Cipher: GRRQ BRX VHH D WIZARD?

a. Determine the shift key used and decrypt the message. Explain your method (e.g., brute force, common word patterns).

b. Explain the critical weakness of a Caesar Cipher that makes it trivial to break, especially when compared to modern symmetric encryption algorithms like AES.

c. Differentiate between a Block Cipher and a Stream Cipher. For which type of data (e.g., large files, real-time communication) is each best suited?

6. Incident Response & Defense in Depth An attacker gained access to your corporate network by phishing an employee's credentials.

a. Describe three distinct layers from a defense-in-depth strategy that could have prevented, detected, or contained this attack. (One must be non-technical).

b. The attack was successful and data was stolen. You are now in the Containment phase of the Incident Response process. What are two key actions to take during this phase?

c. In the Post-Incident Activity phase, what is the primary goal, and what is one important question to ask to achieve it?

7. Ethics and Professional Conduct A friend who works at a different company asks you for a copy of your employer's proprietary security policy document to "get some ideas."

a. Referring to the codes of ethics from professional organizations like (ISC)², explain two ethical canons that would be violated if you complied with this request.

b. Differentiate between a law and a policy. Why is "I didn't know the policy" sometimes an acceptable defense within an organization, while "I didn't know the law" is not?

c. What is the concept of organizational liability? How does demonstrating due care with employee security training help reduce this liability?

Exam Questions Set 2 (Based on Slides Chapters 1-5)

1. Multifactor Authentication Design

You are tasked with designing a multifactor authentication system for a remote access portal for a financial institution.

a. Identify three different factors of authentication (e.g., something you know) and provide a specific, robust example of each that would be appropriate for this high-security environment.

b. The CFO is concerned about accessibility for an employee with severe arthritis who has difficulty typing and handling small tokens. For two of the factors you listed, suggest an alternative implementation that maintains security but accommodates this user's needs.

c. Explain how this multifactor system provides stronger security than a password alone by referencing the concept of falsifying identification.

2. Cryptanalysis and Hashing

You receive a message that has been encrypted with a Caesar cipher: WKHFHDUHU LV RXWIRUWRGD\.

a. Use a brute force method to find the shift key and decrypt the message. Detail the number of shifts you tried to find the correct one.

b. The message is also accompanied by a hash value. Explain the purpose of this hash in ensuring integrity. What property of a cryptographic hash function ensures that even a small change in the message will be detected?

c. Differentiate between the goals of encryption (as used in the Caesar cipher) and a hash function. Does a hash provide confidentiality? Why or why not?

3. Physical and Logical Access Control Failure

An unauthorized individual tailgates an employee into a secure server room and plugs a malicious device into a network port.

a. Identify one physical and one logical access control that failed to prevent this incident.

b. The device intercepts network traffic that is encrypted. However, the attacker is still able to capture the data. Which cryptographic concept (Confidentiality, Integrity, or Authentication) is still being upheld, and which one is potentially compromised? Justify your answer.

c. Referring to the Principle of Least Privilege, what network-level control could be implemented so that even if a device is plugged in, it cannot communicate with sensitive servers?

4. Risk Management of a Lost Backup Tape

A company loses a shipment of backup tapes containing customer personal data. The data on the tapes is encrypted with a strong algorithm.

a. Based on the Parkerian Hexad, which security principle is NOT violated by this incident? Explain why.

b. Now, identify two principles from the Hexad that are violated and justify your reasoning for each.

c. Outline the risk management process the company should follow post-incident by listing the four steps (Identify Assets, Identify Threats, Assess Vulnerabilities, Mitigate Risks) and provide an example for each step relevant to this scenario.

5. Laws, Ethics, and Professional Responsibility

A software developer at a social media company is asked to create a feature that aggregates user data without explicit consent to build detailed profiles for targeted advertising.

a. This request potentially violates which major U.S. privacy regulation (HIPAA, GLBA, etc.)? Why?

b. Differentiate between a law and a code of ethics from a professional organization like the ACM. If no law is broken, does that mean the action is ethical?

c. The developer is uncomfortable with the task. According to the concept of organizational liability, what is the responsibility of the company's management to encourage the developer to report this concern?