

... of the CIA triad is/are primarily affected. ... reputation, and

- 1.1) A malicious actor gains unauthorized access to an employee's account by guessing weak passwords and views sensitive customer data. (1)
- 1.2) Attackers alter financial records stored in a company's database, causing discrepancies in monthly reports without detection. (1)
- 1.3) A critical cloud-based service suffers downtime due to a sophisticated Distributed Denial of Service (DDoS) attack, halting user access for hours. (1)
- 1.4) Employees accidentally send unencrypted confidential project files to an external email address, exposing trade secrets. (1)
- 1.5) A system administrator uses elevated privileges to delete audit logs, preventing detection of unauthorized activities. (1)

Question # 2 [Marks 8]

2.1) A medium-sized company uses Digital Signatures with the DSA algorithm to secure confidential emails between Finance and HR departments. A security audit was recently conducted where a digital signature was generated for a message with hash value $H(m) = 5$, private key $x = 7$, and random number $k = 3$. The resulting digital signature pair was found to be $(r = 8, s = 4)$.

- 2.1.1) Explain what this result indicates about the authenticity and integrity of the signed message. (1)
- 2.1.2) Describe what it would suggest if the verification process using the public key (y) failed. (1)
- 2.1.3) Explain why it is important that the random number (k) is kept secret and not reused? (1)

2.2) A logistics company secures data communication between its warehouse management system and delivery trucks, ensuring protection of real-time schedules and sensitive customer information for critical shipments. Due to moderate processing power on trucks and intermittent connectivity in remote areas, the company aims to achieve secure communication with computational efficiency to avoid



ADEEL AHMED

Block

Room

AB-11

0-06

207

'pus

5

1 hours

transmission delays. The IT team is comparing Advanced Encryption Standard (AES) and Data Encryption Standard (DES) for their suitability in this environment.

2.2.1) Which encryption algorithm, AES or DES, would you recommend for this scenario? Provide reasons considering both security strength and performance efficiency. (1.5)

2.2.2) Explain how the differences in key length between AES and DES influence their effectiveness for long-term protection of sensitive logistics data. (1.5)

2.3) A drone delivery company uses lightweight IoT drones to transmit real-time location and package status to the central hub. The system must protect this data from tampering and eavesdropping during transmission. Drones have limited processing power and operate in high-speed environments. The communication channels are exposed to potential man-in-the-middle attacks, especially in urban areas. Security audits stress the need for both fast encryption and sender authenticity verification.

2.3.1) Which cryptographic method is more suitable for this scenario? Justify your answer with reasons based on performance and security needs. (2)

CLO-2 Apply appropriate security measures to identify threats and vulnerabilities using attack prevention techniques.

- Provide reasons considering both security strength and performance efficiency. (1.5)
- 2.2.2) Explain how the differences in key length between AES and DES influence their effectiveness for long-term protection of sensitive logistics data. (1.5)

2.3) A drone delivery company uses lightweight IoT drones to transmit real-time location and package status to the central hub. The system must protect this data from tampering and eavesdropping during transmission. Drones have limited processing power and operate in high-speed environments. The communication channels are exposed to potential man-in-the-middle attacks, especially in urban areas. Security audits stress the need for both fast encryption and sender authenticity verification.

- 2.3.1) Which cryptographic method is more suitable for this scenario? Justify your answer with reasons based on performance and security needs. (2)

CLO-2 Apply appropriate security measures to identify threats and vulnerabilities using attack prevention techniques.

Question # 3 [Marks 10]

3.1) A ride-hailing company faced a cyberattack where hackers exploited the driver app to inject malicious code into the backend. This gave access to real-time user data and ride history. The issue was linked to poor input validation, raising concerns about app security and data privacy. The breach also highlighted the absence of a proper intrusion detection system (IDS) to identify and block abnormal traffic patterns.

- 3.1.1) How might the attacker have exploited the mobile app to gain backend access? (2)
- 3.1.2) Which type of cyber-attack could be used in this case, and how does it affect the system? (2)
- 3.1.3) Name and explain two basic security principles that were violated in this scenario. (2)

3.2) A hospital's internal messaging app was compromised after an attacker intercepted communications between doctors and staff. Sensitive patient reports were leaked, and some messages were altered without detection. The breach exposed weaknesses in the app's communication security. The hospital now aims to strengthen its data protection measures.

- 3.2.1) What method could the attacker have used to intercept these communications? (1.5)
- 3.2.2) Suggest two protocols or techniques to secure communication in such systems. (1.5)
- 3.2.3) Why is encryption important in medical communication platforms? (1)

Question #4 [Marks 2.5 + 2.5 = 5]

3.1.2) Which type of cyber-attack could be used in this case, and how does it affect the system? (2)

3.1.3) Name and explain two basic security principles that were violated in this scenario. (2)

3.2) A hospital's internal messaging app was compromised after an attacker intercepted communications between doctors and staff. Sensitive patient reports were leaked, and some messages were altered without detection. The breach exposed weaknesses in the app's communication security. The hospital now aims to strengthen its data protection measures.

3.2.1) What method could the attacker have used to intercept these communications? (1.5)

3.2.2) Suggest two protocols or techniques to secure communication in such systems. (1.5)

3.2.3) Why is encryption important in medical communication platforms? (1)

Question #4 [Marks 2.5 + 2.5 = 5]

4.1) TechCore Inc., a mid-sized IT firm, discovered unusual file deletions and unauthorized access attempts on their internal file servers. The IT team suspects an insider threat combined with malware infection targeting sensitive client data. Critical system logs showed multiple failed login attempts followed by privilege escalation activity. The company urgently needs to identify the source and

oad
Spring

prevent further damage.

4.1.1) Based on the symptoms, what type of malware might be involved? Explain its possible consequences on the company's data. (2.5)

4.1.2) Recommend two security measures TechCore Inc. should implement to prevent such insider threats and malware infections in the future. (2.5)

Question #5 [Marks 10]

1) Suppose the following groups are defined in a system:

- **Group A:** Majeed, Amna, Hira, Usman , **Group B:** Majeed, Amna, Hira, **Group C:** Amna, Usman, **Group D:** Usman, Zara

prevent further damage.

4.1.1) Based on the symptoms, what type of malware might be involved? Explain its possible consequences on the company's data. (2.5)

4.1.2) Recommend two security measures TechCore Inc. should implement to prevent such insider threats and malware infections in the future. (2.5)

Question #5 [Marks 10]

5.1) Suppose the following groups are defined in a system:

- **Group A:** Majeed, Amna, Hira, Usman, **Group B:** Majeed, Amna, Hira, **Group C:** Amna, Usman, **Group D:** Usman, Zara

Access Control List (ACL) for File X:

- **File X:** **Group A**, R; **Group B**, RW; **Group C**, RWE

ACL for File Y:

- **File Y:** Group D, RW; Group C, R

5.1.1) If **Amna** tries to **execute File X**, state whether she will be allowed to do so under the following two policies: i) First-match policy (first matching entry is enforced), ii) Any-match policy (user gets all permissions from any group they belong to) (2.5)

5.1.2) Can **Usman** delete File Y if the delete operation requires **W (write) + E (execute)** permission together? Justify your answer based on his group membership and file permissions. Also, show how **access to File Y can be restricted to Amna only** without creating a new group. (2.5)

5.2) The network administrator of "CyberSecure Pvt. Ltd." has deployed the following firewall types

- File Y: Group D, RW; Group C, R

5.1.1) If Amna tries to execute File X, state whether she will be allowed to do so under the following two policies: i) First-match policy (first matching entry is enforced), ii) Any-match policy (user gets all permissions from any group they belong to) (2.5)

5.1.2) Can Usman delete File Y if the delete operation requires W (write) + E (execute) permission together? Justify your answer based on his group membership and file permissions. Also, show how access to File Y can be restricted to Amna only without creating a new group. (2.5)

5.2) The network administrator of "CyberSecure Pvt. Ltd." has deployed the following firewall types to protect their network. For each traffic request, apply the firewall type and policy to decide whether to Allow or Reject, provide a brief reason for your decision, and name one possible attack that could target or bypass that firewall type (5)

S.No	Firewall Type	Source IP	Destination IP	Destination Port	Rule/Policy Description
1	Packet Filtering Firewall	10.10.1.5	192.168.0.10	80	Allow HTTP traffic to internal web server
2	Stateful Inspection Firewall	172.16.5.3	10.10.1.100	443	Allow HTTPS only if the session was initiated internally
3	Application Proxy Firewall	192.168.0.9	203.0.113.20	21	Block all FTP traffic
4	Packet Filtering Firewall	10.0.0.25	192.168.0.8	23	Reject all Telnet connections
5	Application Proxy Firewall	172.16.0.15	203.0.113.50	80	Allow only if HTTP request passes proxy authentication

CLO3 Describe legal, ethical, professional issues, and obligations.

Question #6 [Marks 6]

6.1) As a cybersecurity consultant for a retail company, you discover a manager storing sensitive customer data, including payment details, on an unsecured personal cloud storage account. The company has delayed applying critical security patches to its e-commerce platform, fearing service disruptions during peak sales periods. The platform processes thousands of transactions daily. Recent reports indicate competitors faced similar breaches, raising concerns. The company is subject to data protection regulations. Customer trust is critical to business success.

6.1.1) How would you ethically address the manager's use of personal cloud storage for sensitive data, considering professional responsibilities and data privacy? (2)

6.2) SecureNet Co., a cybersecurity firm, experienced a Credential Exposure Breach due to unpatched vulnerabilities on public-facing servers. This incident disrupted client services and severely impacted the company's reputation. A risk assessment scored key factors on a scale of 1 to 5: Threat Capability: 3 (automated tools), Vulnerability: 4 (unpatched servers), Exposure: 5 (public servers with weak authentication), Mitigation: 2 (basic firewall and antivirus, no intrusion detection). Serving regulated clients, the company must ensure strict compliance with security standards.

6.2.1) Based on the given scores, describe the likelihood of a Credential Exposure Breach occurring again at SecureNet Co. Also, name any one type of security audit that should be conducted after this incident to identify weaknesses and improve system defenses. (2)

6.2.2) As a cybersecurity professional, how would you advise SecureNet Co. to balance the risk of applying critical updates on public-facing servers with the need to maintain uninterrupted client services? Describe your approach while considering both ethical responsibilities and security obligations. (2)

Question #7 [Marks 3+3=6]

the firm must ensure to protect sensitive student

6.2.1) Based on the given scores, describe the likelihood of a Credential Exposure Breach occurring again at SecureNet Co. Also, name any one type of security audit that should be conducted after this incident to identify weaknesses and improve system defenses.

(2)

6.2.2) As a cybersecurity professional, how would you advise SecureNet Co. to balance the risk of applying critical updates on public-facing servers with the need to maintain uninterrupted client services? Describe your approach while considering both ethical responsibilities and security obligations.

(2)

Question #7 [Marks 3+3=6]

7.1) EduTech, an educational technology provider, is upgrading its systems to protect sensitive student data in its learning management system. A recent audit found weak encryption and gaps in governance and compliance. Serving schools across multiple countries, EduTech needs to align with international IT governance standards while managing budget constraints to maintain trust.

7.1.1) Explain how the COBIT framework can help EduTech improve its IT governance and cybersecurity posture. In your answer, mention two COBIT principles and describe how they support alignment between IT goals and business objectives in an educational organization. (3)

7.2) EduTech's vulnerability scan revealed weak encryption in its learning management system's database, risking unauthorized access to student data. The company serves schools across multiple countries and must meet regulatory requirements while addressing system vulnerabilities. A recent audit found compliance gaps. EduTech aims to maintain student and parent trust despite budget constraints.

7.2.1) Explain the importance of ISO 27001 in strengthening EduTech's information security management. Which specific ISO 27001 control addresses weak encryption, and how can compliance with the Pakistan Electronic Crimes Act (PECA) further enhance data protection?

(3)