COMSATS UNIVERSITY ISLAMABAD (CUI)

DEPARTMENT OF COMPUTER SCIENCE
FINAL TERM EXAMINATION FALL-2025
BS-AI, BSSE, BCS

Course: CSC232-Information Security
Maximum Marks: 50
Instructors: *Dr. Quratulain Alam, Ms. Sara Ali, Ms. Haseena Kainat*

Dated: 3rd January, 2026
Time Allowed: 180 Minutes

- *All questions are self-explanatory and require no further explanations during exam time.*
- *Return the question paper along with the answer sheet.*
- *Attempt all questions, in sequence.*

CLO-1

(Explain key concepts of cyber security and cryptography.)

Question No 1.

i) You are a cybersecurity analyst at **TechSecure Corp**, preparing to migrate key organizational assets to a cloud environment. Management wants to ensure that critical information is protected and proper security measures are applied. Management wants to move **five key assets** to the cloud for remote access. Each asset has different sensitivity and business impact: **Financial Data** – includes transaction records, client invoices, and bank details. **Employee Records** – personal information, payroll data, and performance reports. **Software Source Code** – proprietary code for company's products. **Marketing Materials** – presentations, brochures, and campaigns. **Internal Project Plans** – confidential plans for new products under development.
Complete the table below by identifying the **criticality**, **CIA priority**, and suggest suitable **security measures**.
[3 Marks]

Asset/Resource	Criticality (High/Medium/Low)	CIA Priority (C/I/A)	Suggested Security Measure(s)
Financial Data			
Employee Records			
Software Source Code			
Marketing Materials			
Internal Project Plans			

ii) A multinational organization, **GlobalTech**, is planning a fully digital transformation over the next 5 years, moving all sensitive operations and client data to cloud-based systems. They are worried about future threats, insider misuse, and maintaining trust with clients. Management wants to ensure proper accountability and control over data access, while keeping information authentic, confidential, and properly authorized.

a) Explain how **Information Security** ensures **authenticity, authorization, and accountability** in this digital transformation. Identify which aspects of the **CIA triad** are most critical for protecting future digital assets and why.

b) Discuss at least **two cybersecurity principles** and **two security strategy measures** that GlobalTech should adopt to maintain the integrity and reliability of their systems in the future.
[1.5+1.5 = 3 Marks]

NIST

Question No 2.

Alice (Branch A) and Bob (Branch B) of a financial company want to establish a secure session over the Internet. They plan to use the **Diffie-Hellman key exchange** to agree on a shared secret key. Once the session key is established, messages will be protected using a **MAC** for integrity, and the company is considering **HMAC** for stronger authentication and integrity.

a) Explain how Alice and Bob would use **Diffie-Hellman** to establish a shared secret key.

b) Describe how a **MAC** can be used to ensure that messages exchanged are not tampered with. Analyze how **HMAC** strengthens message compared to a simple MAC.

c) Identify **the likely threat or attack** that could occur if Diffie-Hellman is used **without authentication**. Suggest a **practical mitigation technique** that the company could implement to prevent this threat in a real-world business environment.

[1+1+2=4 Marks]

----------CLO-2 ----------

(Apply appropriate security measures to identify threat and vulnerabilities using Attack Prevention techniques)

Question No 3. While sitting in a café, a user notices that their phone suddenly prompts them to connect to a free Wi-Fi network named "Cafe_Free_WiFi_5G." When they connect, a pop-up appears asking them to enter their email and password to "verify access." The user becomes suspicious because the café normally requires no login. **Identify** the type of wireless attack taking place and briefly explain how the user could protect themselves from it.

[3 Marks]

Question No 4. A company employee downloads free utility software from an untrusted website. Shortly after installation, the employee notices unusual activity: files are being deleted, sensitive company data is being sent over the internet, and the system runs slower than usual.

a) Identify the type of malware likely responsible for this behavior.

b) Explain how this malware could have entered the system and what immediate steps the organization should take to contain the threat.

[6 Marks]

Question No 5. FinTech Corp uses Kerberos for SSO across its internal network with a Key Distribution Center (KDC). Alice wants to access the Accounting Server. Draw a **Kerberos authentication flow diagram** including all messages between the user, KDC (AS & TGS), and the service. Explain **step by step** how Kerberos **applies security measures** to:

a) Ensure mutual authentication between Alice and the service.

b) Protect against replay attacks.

c) Distribute keys securely without transmitting passwords in plaintext.

d) Explain the **role of the KDC** in this process and **identify one potential security weakness**. Suggest a **practical way to apply mitigation** to prevent this weakness.

[5 Marks]

Question No 6. A small bank wants to control access to its customer database: **[6 Marks]**

- Branch managers can **read and modify** all customer records.
- Teller staff can **only read** customer records.
- Interns **cannot access** customer records.

a) Identify the most appropriate **access control model** for this scenario.

b) Create a simple **Access Control List (ACL)** showing the permissions for each user role.

c) Using your understanding of different types of firewalls, fill in the table below by identifying the OSI layer(s) each firewall type primarily operates on and its key feature or function. **[5 Marks]**

Firewall Type	Primary OSI Layer(s) It Operates On	Key Feature / Function
Packet Filtering Firewall		
Circuit-Level Gateway		
Application Proxy Gateway		
MAC Layer Firewall		
Hybrid Firewall		

---------- **CLO-3** ----------

(Describe Legal , ethical and professional issues and obligations)

Question No 7. XYZ Corporation manages a critical customer database that contains sensitive information. The company has identified that the value of this asset is $500,000, and in the event of a security breach, they could potentially lose 30% of the asset's value. Currently, security analysts estimate that an attack occurs once every 5 years. To reduce this risk, the company is considering implementing Snort (an IDS/IPS system), which would cost $25,000. Snort is expected to reduce the frequency of attacks to half.

a) Calculate the Single Loss Expectancy (SLE) for the database.

b) Calculate the Annual Loss Expectancy (ALE) without implementing Snort.

c) Calculate the Annual Loss Expectancy (ALE) after implementing Snort.

d) Based on your calculations, determine whether Snort is cost-effective. Show all steps.

[10 Marks]

Question No 8. A healthcare technology company is preparing to launch a new **patient-record management system**. During an internal audit, the security manager emphasizes that the system must follow a **formal set of technical controls** and **procedures** to manage cyber security risks, especially for **access control**, **incident response**, and **data protection**. At the same time, the legal team reminds the company that storing and processing patient data requires **compliance with a specific law** designed to protect individual's health information.

a) Identify which **cyber security standard** is the security manager likely referring to, and which **Law** is the legal team referring to?

[5 Marks]

---------- END ----------

CLO 3 15

CLO 2

CLO 1 10