Internal Assessment Test 2 – Nov. 2025

| USN | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|

CMRIT
CMR INSTITUTE OF TECHNOLOGY, BENGALURU.
ACCREDITED WITH A+ GRADE BY NAAC

| Subject/Code: Computer and Network Security/BEC714B | | | | |
|---|---|---|---|---|
| Date: 28/11/2025 | Duration: 90 mins | Max. Marks: 50 | Semester: 07 | Branch: ECE |

| Sl. | **Answer any FIVE FULL Questions** | **Marks** | **CO** | **RBT** |
|---|---|---|---|---|
| 1 | Explain the fundamental principles of intrusion detection, including the difference between misuse detection and anomaly detection. | [10] | CO3 | L2 |
| 2 | Describe the process of security policy development. Explain the importance of data classes, user classes and consistency checks. | [10] | CO4 | L2 |
| 3 | Explain the architecture and purpose of a DMZ in network security. Discuss the roles of DMZ servers and firewall configurations. | [10] | CO4 | L3 |
| 4 | Describe the security of files and devices in detail. Explain permissions, deletion policies, writable devices, and risks. | [10] | CO4 | L2 |
| 5 | Explain the working of firewalls and proxies in protecting a network. Compare different firewall configurations. | [10] | CO5 | L2 |
| 6 | What does anticipating attacks mean? Explain strategies, tools and proactive methods used to anticipate and detect attacks. | [10] | CO5 | L2 |
| 7 | Explain the role of encryption in system security. Discuss cryptographic keys and secure key management. | [10] | CO5 | L2 |

CI CCI HOD


| USN | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|

Internal Assessment Test 2 – Nov. 2025

CMRIT
CMR INSTITUTE OF TECHNOLOGY, BENGALURU.
ACCREDITED WITH A+ GRADE BY NAAC


| Subject/Code: Computer and Network Security/BEC714B | | | | |
|---|---|---|---|---|
| Date: 28/11/2025 | Date: 28/11/2025 | Date: 28/11/2025 | Date: 28/11/2025 | Date: 28/11/2025 |


| Sl. | **Answer any FIVE FULL Questions** | **Marks** | **CO** | **RBT** |
|---|---|---|---|---|
| 1 | Explain the fundamental principles of intrusion detection, including the difference between misuse detection and anomaly detection. | [10] | CO3 | L2 |
| 2 | Describe the process of security policy development. Explain the importance of data classes, user classes and consistency checks. | [10] | CO4 | L2 |
| 3 | Explain the architecture and purpose of a DMZ in network security. Discuss the roles of DMZ servers and firewall configurations. | [10] | CO4 | L3 |
| 4 | Describe the security of files and devices in detail. Explain permissions, deletion policies, writable devices, and risks. | [10] | CO4 | L2 |
| 5 | Explain the working of firewalls and proxies in protecting a network. Compare different firewall configurations. | [10] | CO5 | L2 |
| 6 | What does anticipating attacks mean? Explain strategies, tools and proactive methods used to anticipate and detect attacks. | [10] | CO5 | L2 |
| 7 | Explain the role of encryption in system security. Discuss cryptographic keys and secure key management. | [10] | CO5 | L2 |

CI CCI HOD

# Solutions

Q 1. Explain the fundamental principles of intrusion detection, including the difference between misuse detection and anomaly detection.

Ans:

Intrusion Detection is a security mechanism used to monitor network or system activities to identify unauthorized access, malicious behavior, or policy violations. It helps organizations detect attacks in real time and respond before major damage occurs.

Systems that do intrusion detection are called intrusion detection systems (IDS). Their goals are fourfold

- Detect wide variety of intrusions
  - Previously known and unknown attacks
  - Suggests need to learn/adapt to new attacks or changes in behavior
- Detect intrusions in timely fashion
  - May need to be real-time, especially when system responds to intrusion
  - Problem: analyzing commands may impact response time of system
  - May suffice to report intrusion occurred a few
- Present analysis in simple, easy-to-understand format
  - Ideally a binary indicator
  - Usually more complex, allowing analyst to examine suspected attack
  - User interface critical, especially when monitoring many systems
- Be accurate
  - Minimize false positives, false negatives
  - Minimize time spent verifying attacks, looking for them
- **Anomaly detection**
  - What is usual, is known
  - What is unusual, is bad
- **Misuse detection**
  - What is bad, is known
  - What is not bad, is good
- **Misuse Detection (Signature-based Detection)**
  - Detects intrusions by **matching activities against known attack patterns/signatures**.
  - Works only when the attack is **already known and documented**.
  - Very **accurate for known threats** but **cannot detect new or unknown attacks**.
  - Example: Antivirus identifying malware using a stored signature.
- ◆ Anomaly Detection (Behavior-based Detection)
  - Analyzes characteristics of the system
  - Compares current activity with expected/normal values
  - Reports deviations when computed statistics do not match expected statistics
  - Can detect new or unknown attacks, because it flags abnormal behavior.
  - But may produce **false positives**, since unusual but legitimate behavior may also be flagged.

Q 2. Describe the process of security policy development. Explain the importance of data classes, user classes and consistency checks.

Ans: Security Policy Development: Security policy development involves systematically identifying organizational information assets, classifying them, defining who can access them, and controlling how information flows to minimize security risks such as unauthorized data leakage. The Drib case illustrates a policy created by analysing organizational structure, information needs, and security requirements. The security policy development process involves classifying information, defining user roles, and enforcing controlled interactions between data and users. By incorporating least privilege, separation of privilege, and consistency checks, The Drib ensures information flows only as necessary for business operations while minimizing the risk of unauthorized disclosure.

1. Role of Data Classes

Data classification is central to policy development because it applies the principle of least privilege by ensuring access is granted strictly on a need-to-know basis.

- Five data classes are defined — Public Data (PD), Development Data for Existing Products (DDEP), Development Data for Future Products (DDFP), Corporate Data (CpD), and Customer Data (CuD).

- Each class reflects confidentiality levels and legal/business sensitivity.
- Data can be reclassified only under controlled conditions; for example, DDFP becomes DDEP when a product moves from concept to realization.

Thus, classifying data ensures controlled exposure, preventing sensitive product, legal, corporate and customer information from leaking to unauthorized entities.

2. Role of User Classes

User classes define who can access what, based on job responsibilities. The Drib defines four user classes — Outsiders, Developers, Corporate Executives, and Employees. An access control matrix is used to map permissions (read/write) for each user class to each data class. This reflects a mandatory access control (MAC) policy, preventing discretionary, unmonitored sharing of sensitive information. The use of user classes enforces separation of privilege and reduces insider misuse by ensuring no group automatically inherits rights beyond its scope.

3. Consistency Checks

Consistency mechanisms ensure that data flow rules are enforced correctly within the organization:

- Reclassification of information requires approval from more than one party, ensuring separation of privilege.
- Checks prevent conflicting access assignments that could bypass confidentiality or integrity safeguards.
- Decisions on reclassification are role-dependent (e.g., corporate executives may declassify legal information but require concurrence of another corporate executive).

These controls ensure the security model remains logically consistent and resistant to accidental or intentional violations.

Q3. Explain the architecture and purpose of a DMZ in network security. Discuss the roles of DMZ servers and firewall configurations.

Ans: A DMZ (Demilitarized Zone) is a separate, controlled sub-network positioned between an organization's internal trusted network and the external untrusted network (Internet). Its fundamental purpose is to provide a buffer layer of security, ensuring that external users can access public services without exposing the internal network to threats The DMZ is typically created using firewalls and network segmentation. The most common architecture includes:

1. Two-Firewall Architecture
   - An external firewall separates the Internet → DMZ
   - An internal firewall separates the DMZ → Internal Network
   - Public servers such as web servers, mail servers, DNS servers, and proxy servers are placed inside the DMZ.
   - Even if an attacker compromises a DMZ server, the internal firewall prevents penetration into the corporate network.
2. Three-Interface / Single-Firewall Architecture
   - A single firewall configured with three network interfaces:
     - Outside interface (Internet)
     - DMZ interface
     - Inside interface (Internal network)
   - Firewall rules strictly control packet movement among the three zones, giving controlled access to DMZ resources while blocking direct access to the internal network.

## Role of a DMZ

The DMZ is designed **to** minimize the attack surface by isolating public-facing services from internal systems. Its purposes include:

Protect internal network: External users cannot directly access the internal LAN even if DMZ hosts are compromised.

Support public services: Hosts in DMZ provide services (e.g., website, email, FTP) to customers/outsiders securely.

Limit damage: Compromise of a DMZ server does not imply compromise of internal systems.

Control traffic: Access rules regulate inbound and outbound traffic to internal, DMZ, and external networks.

Enable monitoring: DMZ servers are ideal points for logging, IDS/IPS, and intrusion monitoring.

A DMZ introduces defense-in-depth:

- Even if an attacker penetrates the external firewall, they reach only the DMZ, not the internal network.
- Internal systems remain shielded from direct exposure to the Internet.
- Strict firewall rules prevent unnecessary inbound/outbound communication.

A DMZ in network security is an isolated sub-network placed between the internal network and the Internet. It is constructed using one or two firewalls and hosts public-facing services while protecting sensitive internal resources. Its design follows the principles of **least privilege**, **segmentation**, and **defense-in-depth**, ensuring that any breach in publicly accessible services does not compromise the organization's internal systems.

Roles of Firewall Configurations in DMZ

Firewalls are responsible for controlling traffic between the Internet, the DMZ, and the internal network. Their configurations are based on the principle of least privilege.

1. External Firewall

- Separates Internet → DMZ
- Allows only necessary inbound traffic (e.g., HTTP to web server, SMTP to mail server)
- Blocks direct access to the internal network

2. Internal Firewall

- Separates DMZ → Internal Network
- Allows only specific, controlled communications (e.g., web server request to internal database)
- Prevents attackers in the DMZ from moving laterally into the private network

Q4. Describe the security of files and devices in detail. Explain permissions, deletion policies, writable devices, and risks.

Ans: Securing files and devices is a crucial aspect of operating system and network security, as unauthorized access or misuse can result in data theft, alteration, or destruction. Security mechanisms ensure that only authorized users can read, modify, execute, or delete sensitive information.

File permissions are the primary control mechanism to regulate access to stored information.

Permissions specify **who** can access a file and **how** they can access it.bCommon types of permissions:

Read (R): View the contents of the file

Write (W): Modify or append data

Execute (X): Run the file if it is a program

Copying and Moving Files: Copying cp and to move the file mv has to be used.

Most systems support permission categories such as:

Owner; Group; Others (public)

For example, in UNIX: -rwxr-x—x grants full permissions to owner, read/execute to group, and only execute to others. Access control prevents unauthorized reading of proprietary or personal data and restricts accidental or malicious modification and execution.

Deletion policies determine how files are removed and whether deleted files can be recovered.

- In many systems, deleting a file only removes its **directory entry**, while the data blocks remain on disk until overwritten. Attackers may recover such data using **file recovery tools**.
- Secure deletion policies include:
  - Immediate overwrite of file contents multiple times
  - Scrubbing free space periodically
  - Preventing non-privileged users from recovering deleted files
  - Logging deletion operations for traceability

Mandatory deletion of temporary, cached, and confidential files minimizes risk of data leakage.

For example, in UNIX: rm * .o This command says to delete all files in the current directory

Writable devices refer to any medium that can store data, such as:

- USB drives, CDs/DVDs, SD cards
- External hard drives
- Network storage
- Cloud storage

Smart Terminals: Smartphones and removable media: provides built-in mechanisms for performing special functions.

Security concerns arise because data can be copied and transported outside the organization without detection. Therefore, systems often employ:

- Device access control policies (allow/block)
- Encryption of portable storage
- Automatic scanning using antivirus tools

- Access monitoring and logging

Some organizations disable USB ports entirely or allow writing only from approved devices.

Q 5 Explain the working of firewalls and proxies in protecting a network. Compare different firewall configurations.

A firewall is a network security mechanism that filters traffic between a trusted internal network and an untrusted external firewall network (such as the Internet). It protects the network by monitoring, permitting, or blocking traffic based on security rules.

How Firewalls Work

- Every incoming or outgoing packet is inspected.
- The firewall checks the packet's source/destination IP address, port number, protocol, and connection state.
- If the packet matches the defined security policies, it is allowed; otherwise it is blocked.
- Firewalls prevent unauthorized access, restrict unsafe services, block scanning attempts, and protect internal hosts from direct exposure to attacks.

Firewalls ensure perimeter defence and least-privilege access by allowing only necessary communication.

A proxy server acts as an intermediary between internal users and external systems. Instead of the user directly accessing Internet resources, the proxy communicates on their behalf.

How Proxies Work

- A client sends a request (e.g., a web request) to the proxy.
- The proxy evaluates the request, applies filtering rules, and then forwards it to the remote server if safe.
- The response from the Internet is returned to the proxy, which sends it to the client.

Security Advantages of Proxies

- Anonymity: Internal IP addresses remain hidden from external systems.
- Filtering: Blocks malicious URLs and content.
- Caching: Frequently accessed pages are stored to improve speed.
- Logging: User activity can be monitored for auditing and compliance.

| Firewall Configuration | Working | Security Level | Advantages | Disadvantages |
|---|---|---|---|---|
| Packet-Filtering Firewall | Filters based on IP, ports, and protocol | Low–Medium | Simple, fast | Stateless, cannot detect application-layer attacks |
| Stateful Inspection Firewall | Tracks connection state and allows only valid active sessions | Medium–High | Prevents spoofing, more secure than packet filtering | Higher processing load |
| Application-Level Firewall (Proxy Firewall) | Examines traffic at application layer (HTTP, FTP, SMTP etc.) | High | Deep inspection, strong filtering | Slower, requires per-service proxy |
| Next-Generation Firewall (NGFW) | Integrates firewall + intrusion prevention + deep packet inspection + application awareness | Very High | Protects from modern threats like malware, ransomware | Expensive and complex to configure |

Q6. What does anticipating attacks mean? Explain strategies, tools and proactive methods used to anticipate and detect attacks.

Anticipating Attacks

Anticipating attacks means predicting and preparing for security breaches before they actually occur. Instead of waiting for an attack to succeed and then reacting, the goal is to identify possible threats, analyze vulnerabilities, observe suspicious behavior, and take preventive action.

It is a proactive approach to computer security that focuses on minimizing exposure and preventing attackers from exploiting weaknesses.

Strategies for Anticipating Attacks

1. Threat Modeling
   - Identifying potential attackers, their goals, and the likely attack paths.
   - Helps prioritize the assets and areas requiring strong protection.
2. Risk Assessment
   - Estimating the likelihood and impact of attacks.
   - Guides where to apply security resources effectively.
3. Vulnerability Assessment
   - Systematically examining software, hardware, and configurations for weaknesses.
   - Eliminates exploitable loopholes before attackers find them.
4. Defense-in-Depth
   - Using multiple layers of security (firewalls, IDS, authentication, encryption, etc.) so a single failure does not compromise the whole system.
5. Security Auditing and Patch Management
   - Regular reviews of system logs, permissions, and code quality.
   - Updating and patching software reduces attack surface.

---

Tools Used to Anticipate Attacks

| Category | Purpose | Examples |
|---|---|---|
| Vulnerability Scanners | Detect misconfigurations and software weaknesses | Nessus, OpenVAS |
| Penetration Testing Tools | Simulate attacks to test system defenses | Metasploit, Nmap |
| Log and Event Monitoring Tools | Analyze system activity for anomalies | Splunk, Syslog |
| Configuration Management Tools | Maintain secure and consistent system settings | Ansible, SCAP |
| Network Monitoring Tools | Observe network traffic patterns | Wireshark, NetFlow |

Proactive Methods for Anticipating and Detecting Attacks

1. Intrusion Detection Systems (IDS)
   - Monitors network or host activity for attack signatures and abnormal behavior.
   - Can provide real-time alerts.
2. Honeypots and Honeynets
   - Deliberately vulnerable systems set up to attract attackers.
   - Reveal attack patterns, tools, and motivations without putting real assets at risk.
3. Security Information and Event Management (SIEM)
   - Aggregates logs from multiple systems and applies analytics to detect coordinated attacks.
4. Behavioral and Anomaly Detection
   - Builds a baseline of normal system activity; deviations trigger alerts.
   - Useful against zero-day and insider attacks.
5. Threat Intelligence
   - Continuous updates on new malware, vulnerabilities, and attack trends.
   - Helps anticipate emerging threats and adapt defenses.
6. Red Team vs. Blue Team Exercises
   - Red team plays the attacker; blue team defends.
   - Improves preparedness and highlights weaknesses in systems and policies.

Q7. Explain the role of encryption in system security. Discuss cryptographic keys and secure key management.

Encryption plays a fundamental role in system security by ensuring that sensitive information remains protected even if it is intercepted or accessed by unauthorized users. It transforms plaintext into ciphertext using mathematical algorithms, making the information unintelligible unless the recipient has the appropriate decryption key.

Encryption supports three major security goals:

1. Confidentiality – prevents unauthorized disclosure of data.
2. Integrity – detects any unauthorized modification when combined with cryptographic hashes and digital signatures.
3. Authentication & Non-repudiation – ensures the identity of communicating parties and prevents denial of actions.

Encryption can be applied to:

- Data-at-rest (files, disks, backup media)
- Data-in-transit (network communication, email, VPN)
- Data-in-use (trusted execution environments)

Thus, encryption acts as a defensive barrier that protects information irrespective of storage location or transmission medium.

Cryptographic systems depend on keys, not secrecy of algorithms. A key is a value that controls the encryption and decryption process.

Types of Keys

1. Symmetric Keys
   - Same key used for both encryption and decryption.
   - Fast and suitable for bulk encryption (e.g., AES, DES).
   - Requires secure key sharing between parties.
2. Asymmetric Keys (Public–Private Key Pair)
   - Uses two mathematically related keys: a public key for encryption and a private key for decryption.
   - Supports secure key exchange and digital signatures (e.g., RSA, ECC).
   - Computationally slower.
3. Session Keys
   - Temporary symmetric keys generated for a communication session.
   - Often exchanged securely using asymmetric cryptography.

Secure Key Management

Even strong encryption becomes ineffective if keys are poorly managed. Key management ensures that cryptographic keys are generated, stored, distributed, rotated, and destroyed securely.

Key Management Requirements

- Secure Key Generation – using cryptographically strong random number generators.
- Secure Storage of Keys
  - Hardware security modules (HSM), Trusted Platform Modules (TPM)
  - Encrypted databases and device-bound keystores
- Key Distribution
  - Physical distribution (in symmetric systems)
  - Public Key Infrastructure (PKI) for asymmetric systems
- Key Rotation and Expiry
  - Changing keys periodically reduces impact of key compromise.
- Key Backup and Recovery
  - Prevents loss of data due to key damage or corruption.
- Key Revocation
  - Removing compromised keys from circulation using Certificate Revocation Lists (CRL) or OCSP.

Risks of Poor Key Management

- Unauthorized access to encrypted data
- Man-in-the-middle attacks during insecure key exchange
- Insider threats or theft of unprotected private keys