CMR INSTITUTE OF TECHNOLOGY	USN										

Internal Assesment Test-III

Sub: Network Security Code: 21EC732

Date: 16/12/2024 Duration: 90 mins Max Marks: 50 Sem: 7th Branch: ECE(A,B,C,D)

Answer any **FIVE FULL** Questions

		Marks	OBE CO	OBE RBT
1.	Explain and describe the three classes of Intruders and their behavior patterns. Ans: Intruders are individuals or entities that attempt to gain unauthorized access to systems, networks, or data. They can be broadly categorized into the following three classes based on their motivations, objectives, and behavior patterns. **Masqueraders:** Masqueraders are unauthorized users who gain access to a system by exploiting stolen credentials or bypassing authentication mechanisms. **Behavior Patterns:** Use stolen or guessed login credentials to impersonate legitimate users. Exploit system vulnerabilities to bypass authentication mechanisms. **Misfeasors:** Misfeasors are authorized users of a system who misuse their privileges to perform unauthorized actions. These are typically insiders who abuse their access rights. **Behavior Patterns:** Access sensitive data beyond the scope of their job responsibilities (e.g., viewing confidential company files). Alter or delete data they are authorized to access. Share internal system information with external parties or use it for personal gain. **Clandestine Users:** Clandestine users are skilled attackers, often with advanced knowledge of systems, who aim to bypass security mechanisms undetected. They can be internal or external users and often focus on maintaining long-term access. **Behavior Patterns:** Exploit system vulnerabilities to install backdoors or maintain persistent access. Disable or manipulate audit logs and security alerts to avoid detection.	[10]	CO4	L2
2.	Explain the rule based intrusion detection techniques in Intrusion detection. Ans: Rule-Based Intrusion Detection Techniques **are a key approach used in** Intrusion Detection Systems (IDS) to identify malicious activity in a network or system by analyzing events and comparing them against predefined rules or patterns. Rule-based techniques can be broadly classified into the following: **Rule-Based Anomaly Detection** Focuses on identifying deviations from normal behavior defined by rules. A baseline of normal behavior is created based on system performance, network traffic, or user actions. Rules are applied to detect activities that deviate from this baseline. Example: A rule might alert if a user logs in at an unusual time or accesses a resource they rarely use. **Advantage**: Can detect new attacks or zero-day threats.	[10]	CO4	L2

Limitation: Prone to false positives because unusual behavior isn't always malicious.

Rule-Based Signature Detection

Matches activities against a database of known attack patterns or signatures.

Predefined rules are created based on known threats, like specific malware or attack vectors.

The system scans activities for these specific patterns and generates alerts for matches.

Example: A rule might flag packets containing a certain malicious payload.

3. Discuss the firewall configurations with examples and neat sketches. [05] CO5 L1

Ans:

Firewall configurations are critical in safeguarding networks from unauthorized access and cyber threats. Different firewall configurations cater to varying security needs, ensuring both internal and external network protection.

1. Packet Filtering Firewall: A packet-filtering firewall examines individual packets of data, allowing or blocking them based on predefined rules. These rules are applied to parameters like source/destination IP address, protocol, and port number.

Example: Blocking incoming traffic to port 22 (SSH) to prevent unauthorized remote access.

Allowing HTTP (port 80) and HTTPS (port 443) traffic for a web server.

2. Stateful Inspection Firewall: A stateful inspection firewall monitors the **state** of active connections and uses this information to decide whether to allow or block packets. It inspects traffic flow rather than just individual packets.

Example:

Allowing return traffic only for outbound requests initiated by internal hosts.

3. Proxy Firewall: A proxy firewall acts as an intermediary between users and the internet. It processes requests from internal users and forwards them to the external network, effectively hiding internal network details.

Example:

Using a proxy server to filter and monitor web traffic for compliance with company policies.

4. Network Address Translation (NAT) Firewall: A NAT firewall translates private IP addresses into a public IP address to communicate with external networks. This ensures that internal addresses are not exposed to the internet.

Example: Allowing multiple devices to access the internet through a single public IP.

4. Explain the types of malicious software in detail. [10] CO4 L2

Ans:

Malicious software, or malware, refers to any program or code intentionally designed to harm, exploit, or disrupt systems, networks, or devices. Here are the main types of malicious software explained in detail:

1. Viruses: A virus is a type of malware that attaches itself to legitimate programs or files and spreads when the infected file or program is executed.

It Requires a host program to spread.Can corrupt, delete, or modify files.

Often spreads through infected attachments, downloads, or USB drives.

2. Worms: A worm is a self-replicating malware that spreads across networks without requiring a host program or user interaction. It exploits vulnerabilities in networks or software. Can spread rapidly, consuming bandwidth and system resources.

3. Trojans: A Trojan horse, or Trojan, disguises itself as legitimate software to trick users into installing it, granting attackers unauthorized access to systems.

4. Ransomware: Ransomware encrypts a victim's data or locks their system, demanding a ransom payment in exchange for decryption keys or system access.

5. Spyware: Spyware is designed to secretly monitor user activity and collect

sensitive information without consent.

6. Adware: Adware displays unwanted advertisements, often generating revenue for attackers, and may collect user data without consent.

7. Keyloggers: Keyloggers record keystrokes to capture sensitive information, such as passwords, PINs, and credit card details.

5.a) List out the characteristics of firewall and explain in brief. [06] CO5 L2

Ans:

A firewall is a security device that filters incoming and outgoing traffic based on predefined rules to protect networks from unauthorized access. It enforces access control by allowing only authorized users or devices to access specific resources while blocking others. Firewalls inspect data packets, checking details such as IP addresses, ports, and protocols, and can track active connections to ensure only valid sessions are allowed. They often support features like Network Address Translation (NAT) to hide internal IPs and Virtual Private Network (VPN) support for secure remote access. Firewalls also log and monitor network activity, helping detect suspicious behavior and potential threats. Some firewalls include content filtering to block specific websites or applications and intrusion detection systems to identify malicious activities. Advanced firewalls offer application-layer filtering, spoofing protection, and multi-layer security to safeguard networks comprehensively. They also provide scalability and redundancy for uninterrupted operation and can enforce user authentication for added security.

b) Discuss the limitations of firewall in detail. [04] CO5 L1

Ans:

Firewalls are vital for network security but have limitations as standalone defenses. They cannot detect threats within allowed traffic, like encrypted malware or phishing attacks, and are ineffective against insider threats. Sophisticated attacks, such as zero-day exploits, often bypass them. Firewalls rely on correct configurations, and errors can create vulnerabilities or block legitimate traffic. They may struggle with performance in high-traffic environments and lack protection against application-specific attacks and human errors. While they help mitigate minor DDoS attacks, they cannot handle large-scale threats or provide real-time threat intelligence. These limitations make additional security tools and a multi-layered approach essential.