

Malware And Threat Detection

1. Define Types of Viruses.

ANS: A **computer virus** is a malicious program that can copy itself and infect a computer without the user's consent.

Types of Viruses:

- **Boot Sector Virus** – Infects the system boot record.
- **File Infector Virus** – Attaches to executable files (.exe, .com).
- **Macro Virus** – Written in macro language, targets applications like MS Word or Excel.
- **Polymorphic Virus** – Changes its code to avoid detection.
- **Resident Virus** – Hides in system memory and infects files automatically.
- **Multipartite Virus** – Infects both boot sector and files.

2. Create virus using Http Rat Trojan tool.

ANS: An **HTTP RAT (Remote Access Trojan)** is a tool that allows remote control of a target computer.

Process (for lab demonstration only):

- Install the RAT tool on your system.
- Create a **payload** (infected file) using the tool.
- Configure the **server (attacker)** and **client (victim)** connection using IP/Port.
- Send the payload to the victim's computer.
- Once executed, the attacker gains remote access.

3. Explain any one Antivirus with example.

ANS: **Antivirus software** detects, prevents, and removes malware from computers.

Example – Avast Antivirus:

- Provides real-time protection.
- Detects viruses, spyware, and ransomware.
- Offers a firewall, email shield, and web protection.
- Automatically updates virus definitions.

4. What is a Firewall and why is it used?

ANS: A **firewall** is a network security device or software that monitors and controls incoming and outgoing network traffic based on security rules.

Purpose:

- Blocks unauthorized access.
- Protects systems from external attacks.
- Filters harmful or suspicious traffic.

Example: Windows Defender Firewall, Cisco ASA Firewall.

5. What is the difference between VA (Vulnerability Assessment) and PT (Penetration Testing)?

ANS:

Aspect	Vulnerability Assessment (VA)	Penetration Testing (PT)
Purpose	Identify security weaknesses.	Exploit weaknesses to find real risks.
Approach	Automated scanning and analysis.	Manual and simulated attack testing.
Outcome	List of vulnerabilities.	Proof of exploitation and security impact.
Frequency	Regular and continuous.	Periodic (quarterly or yearly).

6. What is the difference between HIDS and NIDS?

ANS:

Type	Full Form	Monitors	Location
HIDS	Host-based Intrusion Detection System	Activities on a single host or server.	Installed on host machines.
NIDS	Network-based Intrusion Detection System	Network traffic for suspicious activity.	Placed on network boundaries.

Example:

- HIDS – OSSEC
- NIDS – Snort

7. What is Data Leakage?

ANS: Data Leakage is the unauthorized transmission of data from inside an organization to an external destination.

Causes:

- Weak security policies
- Insider threats
- Misconfigured cloud storage

Prevention:

- Data Loss Prevention (DLP) tools
- Encryption
- Access control and monitoring

8. What is a Brute Force Attack? How can you prevent it?

ANS: A Brute Force Attack is a trial-and-error method used to guess passwords or encryption keys by trying all possible combinations.

Prevention:

- Use strong, complex passwords.
- Enable account lockout after failed attempts.
- Use CAPTCHA and multi-factor authentication (MFA).

9. Explain MITM (Man-in-the-Middle) attack and how to prevent it?

ANS: A **MITM attack** occurs when an attacker secretly intercepts and relays communication between two parties.

Example: Capturing login credentials on an unsecured Wi-Fi network.

Prevention:

- Use HTTPS and SSL/TLS encryption.
- Avoid public Wi-Fi for sensitive tasks.
- Use VPNs and secure authentication.

10. Explain XSS (Cross-Site Scripting) attack and how to prevent it?

ANS: **XSS Attack** happens when an attacker injects malicious scripts into a trusted website.

Effect: Steals cookies, session tokens, or user data.

Prevention:

- Validate and sanitize all user inputs.
- Use output encoding (HTML escaping).
- Implement Content Security Policy (CSP).

11. What is a Botnet?

ANS: A **Botnet** is a network of infected computers (bots) controlled remotely by an attacker.

Uses:

- Launching DDoS attacks
- Sending spam
- Stealing data

Detection & Prevention:

- Use IDS/IPS and updated antivirus.
- Monitor unusual network activity.

12. What is a DDoS (Distributed Denial of Service) attack and how does it work?

ANS: A **DDoS attack** floods a target server or network with massive traffic from multiple compromised systems, causing it to slow down or crash.

Working:

- Attacker controls many infected devices (botnet).
- All devices send requests simultaneously to overload the target.

Prevention:

- Use firewalls and DDoS protection services (e.g., Cloudflare).
- Rate limiting and traffic filtering.

13. What is a Zero-Day Vulnerability?

ANS: A **Zero-Day Vulnerability** is a software flaw unknown to the vendor and has no patch available.

Risk: Attackers exploit it before developers can fix it.

Prevention:

- Regular software updates.
- Use behaviour-based threat detection tools.
- Employ Intrusion Detection and Prevention Systems (IDPS).