Module: Malware And Threat Detection

1. Explain CIA triad.

Ans- The **CIA Triad** in cybersecurity stands for:

- **Confidentiality** → Ensuring information is accessible only to authorized users (protecting data from unauthorized access).
- **Integrity** → Maintaining accuracy and trustworthiness of data (no unauthorized changes or corruption).
- **Availability** → Ensuring information and systems are accessible when needed (preventing downtime or disruptions).

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

Ans- **Firewall**
A firewall is a network security device (hardware, software, or both) that monitors and filters incoming and outgoing network traffic based on security rules. It acts as a barrier between a trusted internal network and untrusted external networks (like the internet).

Why it is used:

- To block unauthorized access.
- To allow safe communication.
- To protect systems from malware, hackers, and cyberattacks.

3. What is the difference between VA(Vulnerability Assignment) and PT(Penetration Testing)?

Ans- **Difference between VA and PT**

- **Vulnerability Assessment (VA):**
    - Process of scanning and identifying weaknesses or security flaws in a system, application, or network.
    - It only reports the vulnerabilities but does not exploit them.
    - Example: A scan shows outdated software versions or weak passwords.
- **Penetration Testing (PT):**
    - Simulates real-world attacks by exploiting vulnerabilities to check the actual impact and risk.
    - Goes beyond identifying flaws by testing how far an attacker can go.
    - Example: Attempting to hack into a system using a weak password to gain unauthorized access.

4. What is the difference between HIDS and NIDS?

Ans- **Difference between HIDS and NIDS**

- **HIDS (Host-Based Intrusion Detection System):**
    - Installed on individual devices (hosts/servers).
    - Monitors logs, files, and system activities for suspicious behavior.
    - Detects attacks targeting a specific host.
- **NIDS (Network-Based Intrusion Detection System):**
    - Installed at strategic points in a network.
    - Monitors network traffic in real-time for malicious activity.
    - Detects attacks happening across the network.

5. Explain SSL Encryption

Ans- **SSL Encryption**
SSL (**Secure Socket Layer**) is a security protocol that encrypts the data transmitted between a web browser and a web server. It ensures that sensitive information such as usernames, passwords, and credit card details cannot be intercepted or read by unauthorized parties.

How it works:

- SSL uses **public and private key encryption**.
- Data is converted into unreadable form during transmission.
- Only the intended recipient (server or client) with the correct key can decrypt it.

Purpose:

- Provides **confidentiality** (data privacy).
- Ensures **integrity** (data is not altered).
- Confirms **authentication** (verifies website identity).

6. What is Data Leakage?

Ans- **Data Leakage**
Data leakage is the **unauthorized transmission of sensitive information** from within an organization to an external source. It can happen accidentally (human error) or intentionally (malicious insider/attacker).

Examples:

- Sending confidential files to the wrong email address.
- Uploading sensitive data to unsecured cloud storage.
- Using infected USB drives.

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

Ans- **Brute Force Attack**
A brute force attack is a hacking method where an attacker tries all possible combinations of usernames and passwords until the correct one is found. It is a **trial-and-error** technique used to gain unauthorized access to accounts or systems.

Prevention Methods:

- Use **strong, complex passwords** (mix of letters, numbers, symbols).
- Enable **Multi-Factor Authentication (MFA)**.
- Implement **account lockout** after multiple failed attempts.
- Use **CAPTCHA** to block automated login attempts.
- Regularly **monitor login activity** for unusual behavior.

8. Explain MITM attack and how to prevent it?

Ans- **MITM Attack (Man-in-the-Middle Attack)**
A MITM attack occurs when a hacker secretly intercepts and possibly alters communication between two parties (e.g., user and website) without their knowledge. The attacker can steal sensitive information such as passwords, banking details, or personal data.

Example: A hacker sitting on public Wi-Fi intercepts your login credentials while you log into your email.

Prevention Methods:

- Use **HTTPS / SSL/TLS** for secure communication.
- Avoid using **public Wi-Fi** for sensitive transactions (or use a **VPN**).
- Enable **end-to-end encryption** in messaging apps.
- Keep systems and browsers **updated** with latest security patches.
- Use **strong authentication methods** like MFA.

9. Explain XSS attack and how to prevent it?

Ans- **XSS Attack (Cross-Site Scripting)**
An **XSS attack** happens when an attacker injects malicious scripts (usually JavaScript) into a trusted website. When users visit the site, the script runs in their browser, allowing the attacker to steal cookies, hijack sessions, redirect users, or display fake content.

Example: A comment box on a website where the attacker inserts <script> code that steals session cookies of users who view the comment.

Prevention Methods:

- **Input Validation:** Check and sanitize all user inputs.

- **Output Encoding:** Convert special characters (<, >, ") into safe formats before displaying.
- **Use Content Security Policy (CSP):** Restrict what scripts can run on a site.
- **Web Application Firewall (WAF):** Detects and blocks malicious scripts.

10. What is a Botnet?

Ans- **Botnet**
A **botnet** is a network of computers, servers, or IoT devices that have been **infected with malware** and are remotely controlled by a hacker (called a "botmaster"). The infected devices, known as "bots" or "zombies," work together without the owner's knowledge.

Uses of Botnets:

- Launching **DDoS attacks** (flooding websites with traffic).
- Sending large-scale **spam emails**.
- Stealing sensitive data (like banking info).
- Spreading malware to other devices.

11. Explain SSL and TLS

Ans- **SSL and TLS**

- **SSL (Secure Socket Layer):**
  An older security protocol that encrypts communication between a web browser and a server. It ensures data privacy, integrity, and authentication during transmission. Websites using SSL show **HTTPS** in the URL.
- **TLS (Transport Layer Security):**
  The improved and more secure version of SSL. TLS uses stronger encryption algorithms, better authentication methods, and is the current standard for securing online communications.

12. Define the terms Virus, Malware, and Ransomware.

Ans- **Virus, Malware, and Ransomware**

- **Virus:**
  A type of malicious program that attaches itself to files or software and spreads when the infected file is executed. It can corrupt files, slow down systems, or delete data.
- **Malware:**
  A general term for **any kind of malicious software** (viruses, worms, Trojans, spyware, ransomware, etc.) designed to harm, steal, or disrupt computer systems.
- **Ransomware:**
  A specific type of malware that **encrypts a user's files or locks the system**, then demands payment (ransom) to restore access.

13. What is Phishing? Provide an example.

Ans-**Phishing**
Phishing is a **social engineering attack** where cybercriminals trick people into sharing sensitive information such as passwords, credit card details, or banking credentials by pretending to be a trusted entity (like a bank, company, or government). It is usually carried out through fake emails, messages, or websites.

Example:
You receive an email that looks like it's from your bank, asking you to *"click the link and verify your account."* The link leads to a fake website that steals your login details.

14. Define the terms Encryption and Decryption.

Ans- **Encryption:**
The process of converting **plain text (readable data)** into **cipher text (unreadable form)** using an algorithm and a key. It protects sensitive information from unauthorized access.

Decryption:
The reverse process of encryption. It converts **cipher text back into plain text** using a key, making the data readable again for authorized users.

15. What is a DDoS attack and how does it work?

Ans- **DDoS Attack (Distributed Denial of Service Attack)**
A **DDoS attack** is a cyberattack where multiple compromised systems (often part of a botnet) flood a target server, website, or network with massive traffic.

How it works:

- The attacker infects many devices with malware, turning them into "bots."
- All these bots are controlled remotely and instructed to send requests to the target at the same time.
- The huge traffic overloads the server, causing it to slow down, crash, or become unavailable to legitimate users.

Example: An e-commerce website taken down during a sale due to a DDoS attack.

16. What is a zero-day vulnerability?

Ans- **Zero-Day Vulnerability**
A **zero-day vulnerability** is a security flaw in software or hardware that is **unknown to the vendor or developer**. Since no patch or fix exists at the time of discovery, attackers can exploit it immediately, leaving the system highly vulnerable.

Why it's called "zero-day":
Because developers have **"zero days"** to fix the flaw before it is exploited.

Example: Hackers exploiting a newly discovered bug in Windows or a web browser before Microsoft/Google releases a security update.

17. What is network sniffing

Ans- **Network Sniffing**
Network sniffing is the process of **capturing and monitoring data packets** that travel across a network. It can be used by administrators for troubleshooting and performance analysis, but attackers use it to steal sensitive information such as usernames, passwords, or credit card details.

Types:

- **Active Sniffing:** Interferes with network traffic to capture data.
- **Passive Sniffing:** Simply listens and records traffic without altering it.

18. What is a Security Operations Center (SOC)?

Ans- **Security Operations Center (SOC)**
A **Security Operations Center (SOC)** is a centralized team or facility within an organization that is responsible for **monitoring, detecting, analyzing, and responding to cybersecurity threats** in real time.

Functions of SOC:

- Continuous monitoring of networks, servers, and devices.
- Detecting suspicious or malicious activity.
- Incident response and threat containment.
- Forensics and reporting after an attack.

19. What is the importance of forensics in cyber security?

Ans- **Importance of Forensics in Cybersecurity**

Digital forensics is a crucial part of cybersecurity because it helps in **investigating, analyzing, and preserving digital evidence** after a cyber incident or attack. Its importance can be understood in the following points:

- **Incident Investigation:** Identifies how an attack happened, who was involved, and what systems were affected.
- **Evidence Preservation:** Collects and safeguards digital evidence that can be used in court or legal proceedings.
- **Attack Prevention:** Analyzing past attacks helps in improving defenses and preventing future incidents.
- **Tracing Attackers:** Forensics techniques can trace IPs, logs, and malicious files to identify attackers.
- **Compliance:** Many industries (banking, healthcare) require digital forensics for regulatory compliance.

20.Discuss the future trends in cyber security. Which skills are important for cyber security professionals?

Ans- **Future Trends in Cybersecurity**
The field of cybersecurity is constantly evolving due to the rise of new technologies and advanced threats. Some key future trends include:

- **AI and Machine Learning in Security:** Used to detect and respond to threats faster.
- **Cloud Security:** Growing need to protect data stored on cloud platforms.
- **IoT Security:** With billions of connected devices, securing IoT networks is critical.
- **Zero Trust Architecture:** "Never trust, always verify" model for stronger access control.
- **Quantum-Safe Cryptography:** Preparing for future quantum computers that may break current encryption.
- **Automation & SOAR (Security Orchestration, Automation, and Response):** Speeding up incident response.

Skills Important for Cybersecurity Professionals
To keep up with these trends, cybersecurity professionals need:

- **Ethical Hacking & Penetration Testing** (to identify vulnerabilities).
- **Incident Response & Digital Forensics** (to handle breaches).
- **Cloud Security Skills** (AWS, Azure, GCP).
- **Threat Intelligence & Malware Analysis**.
- **Knowledge of AI/ML in Cybersecurity**.
- **Soft Skills:** Problem-solving, communication, and analytical thinking.

Conclusion
The future of cybersecurity will focus heavily on **automation, AI, and securing cloud/IoT environments**. Professionals with **technical expertise and adaptive skills** will be in high demand to combat ever-evolving cyber threats.

21. What is the difference between IDS and IPS?

Ans- **Difference between IDS and IPS**

- **IDS (Intrusion Detection System):**
    - Monitors network traffic for suspicious activity or policy violations.
    - Generates alerts when a threat is detected but does not take direct action.
    - Works in a **passive** mode.
    - Example: An IDS detects a SQL injection attempt and alerts the admin.

- **IPS (Intrusion Prevention System):**
    - Monitors and actively blocks or prevents malicious traffic in real time.
    - Can drop malicious packets, block IPs, or reset connections.
    - Works in an **active (inline)** mode.
    - Example: An IPS detects and blocks a SQL injection attempt automatically.