**Module:Term - 4 ====&Gt; Ech - Introduction To Ethical Hacking**

**1. Explain CIA Triad**

The CIA Triad is a fundamental model in information security, representing the three core principles to protect data:

* **Confidentiality**: Ensures that sensitive information is accessed only by authorized individuals.
* **Integrity**: Ensures that the data is accurate and cannot be modified without authorization.
* **Availability**: Ensures that data and resources are accessible when needed by authorized users.

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

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

* To block unauthorized access.
* To prevent cyberattacks, such as malware, worms, and DDoS attacks.
* To allow legitimate traffic while blocking suspicious activities.

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

* **Vulnerability Assessment (VA)**:  
  Identifies, quantifies, and prioritizes vulnerabilities in a system or network. It focuses on finding potential risks but doesn’t exploit them.
  + **Example**: Scanning for unpatched software.
* **Penetration Testing (PT)**:  
  Simulates real-world attacks by exploiting vulnerabilities to assess the system's resilience.
  + **Example**: Attempting to hack into a system to find exploitable gaps.

**4. What is the difference between HIDS and NIDS?**

* **HIDS (Host-based Intrusion Detection System)**:  
  Monitors and detects suspicious activities on a single host or device (e.g., file changes).
  + Example: Antivirus software.
* **NIDS (Network-based Intrusion Detection System)**:  
  Monitors and detects malicious activity on an entire network by analyzing traffic.
  + Example: Snort.

**5. Explain SSL Encryption**

**SSL (Secure Sockets Layer)** encryption ensures secure communication over the internet by encrypting the data exchanged between a user’s browser and a server.

* It uses **public key** and **private key** encryption.
* SSL is commonly used in HTTPS to secure online transactions, passwords, and sensitive data.

**6. What is Data Leakage?**

**Data leakage** occurs when sensitive information is unintentionally or maliciously exposed to unauthorized individuals.

* **Examples**: Emailing confidential data to the wrong recipient, insider threats, or poor data protection practices.
* **Prevention**: Data Loss Prevention (DLP) solutions, encryption, and access control policies.

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

A **Brute Force Attack** is a trial-and-error method where an attacker repeatedly tries to guess passwords or encryption keys until they succeed.

* **Prevention**:
  + Implement account lockout policies.
  + Use strong, complex passwords.
  + Enable multi-factor authentication (MFA).
  + Deploy rate-limiting mechanisms.

**8. Explain MITM attack and how to prevent it?**

A **Man-in-the-Middle (MITM) Attack** occurs when an attacker intercepts and manipulates communication between two parties without their knowledge.

* **Example**: Eavesdropping on unencrypted Wi-Fi.
* **Prevention**:
  + Use HTTPS and SSL/TLS for secure communication.
  + Avoid public Wi-Fi or use VPNs.
  + Implement strong encryption and authentication protocols.

**9. Explain XSS attack and how to prevent it?**

A **Cross-Site Scripting (XSS) Attack** occurs when an attacker injects malicious scripts into a legitimate website or web application, which then executes on the user’s browser.

* **Types**:
  + **Stored XSS**: Malicious script is permanently stored on the server.
  + **Reflected XSS**: Malicious script is reflected off a web application.
* **Prevention**:
  + Sanitize user input.
  + Use Content Security Policy (CSP).
  + Implement proper input validation and escaping.

**10. What is a Botnet?**

A **Botnet** is a network of compromised devices (bots) controlled by an attacker (botmaster). These devices are often used for malicious purposes like:

* Distributed Denial-of-Service (DDoS) attacks.
* Spamming or phishing campaigns.
* Data theft or credential harvesting