Assignment: Ethical hacking

**1. Explain CIA Triad**

The **CIA Triad** is a fundamental concept in cybersecurity, consisting of three key principles:

* **Confidentiality**: Ensures that data is only accessible to authorized users.
* **Integrity**: Ensures that data remains unaltered and trustworthy.
* **Availability**: Ensures that data and resources are accessible to authorized users when needed.

**2. What is a Firewall and Why is it Used?**

A **firewall** is a security device (software or hardware) that monitors and controls incoming and outgoing network traffic based on predefined security rules. It is used to:

* Block unauthorized access
* Prevent cyber threats like malware and hackers
* Allow legitimate traffic while blocking harmful traffic

**3. Difference Between VA (Vulnerability Assessment) and PT (Penetration Testing)**

* **Vulnerability Assessment (VA)**: Identifies and categorizes security vulnerabilities in a system but does not exploit them.
* **Penetration Testing (PT)**: Simulates real-world attacks by exploiting vulnerabilities to assess their impact.

**4. Difference Between HIDS and NIDS**

* **HIDS (Host-based Intrusion Detection System)**: Monitors a specific host or system for suspicious activities.
* **NIDS (Network-based Intrusion Detection System)**: Monitors network traffic for malicious activity across an entire network.

**5. Explain SSL Encryption**

**SSL (Secure Sockets Layer)** encryption is a security protocol that encrypts data transmitted between a web browser and a server. It ensures secure communication by preventing eavesdropping and data tampering. It has been replaced by **TLS (Transport Layer Security)** for better security.

**6. What is Data Leakage?**

**Data leakage** is the unauthorized transmission of sensitive information outside an organization. It can occur due to human error, malicious intent, or weak security policies.

**7. What is a Brute Force Attack? How Can You Prevent It?**

A **brute force attack** is a hacking method that involves systematically trying different passwords until the correct one is found. Prevention methods include:

* Implementing **strong password policies**
* Using **account lockout mechanisms**
* Deploying **CAPTCHAs**
* Enforcing **multi-factor authentication (MFA)**

**8. Explain MITM Attack and How to Prevent It**

A **Man-in-the-Middle (MITM) attack** occurs when an attacker intercepts and alters communication between two parties without their knowledge. Prevention methods include:

* Using **HTTPS and TLS encryption**
* Implementing **VPNs**
* Avoiding **public Wi-Fi without encryption**
* Enabling **two-factor authentication (2FA)**

**9. Explain XSS Attack and How to Prevent It**

**Cross-Site Scripting (XSS)** is a web security vulnerability where attackers inject malicious scripts into web pages viewed by users. Prevention methods include:

* **Input validation and sanitization**
* **Using Content Security Policy (CSP)**
* **Escaping user input in HTML and JavaScript**

**10. What is a Botnet?**

A **botnet** is a network of compromised computers (bots) controlled by a hacker (botmaster) to perform malicious activities like **DDoS attacks, spam distribution, or data theft**.

**11. Explain SSL and TLS**

* **SSL (Secure Sockets Layer)**: A cryptographic protocol that provides secure communication over the internet.
* **TLS (Transport Layer Security)**: A more secure and updated version of SSL, offering better encryption and security features.

**12. Define the Terms Virus, Malware, and Ransomware**

* **Virus**: A type of malware that attaches itself to a file and spreads when executed.
* **Malware**: A general term for malicious software, including viruses, worms, trojans, and spyware.
* **Ransomware**: A type of malware that encrypts a victim's data and demands a ransom for decryption.