**Module :-Ethical Hacking**

1. **CIA Triad**

* **Confidentiality**: Ensures that data is only accessible to authorized users. It can be achieved using encryption, access control lists, and authentication mechanisms.  
  **Example**: Encrypting sensitive emails or files to ensure only the recipient can access them.
* **Integrity**: Ensures that data remains accurate and unaltered during storage or transmission. This can be achieved through checksums, hash functions, and version controls.  
  **Example**: Using a hash algorithm (e.g., SHA-256) to verify that a file has not been tampered with.
* **Availability**: Ensures that data is accessible when needed by authorized users. This involves maintaining hardware, software, and network systems, as well as creating backup solutions.  
  **Example**: Setting up redundant systems or cloud storage to ensure that a service is always available, even during system failures.

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

* A **Firewall** is a security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It is often deployed to protect an internal network from external threats.
* **Why is it used?**
  + It acts as a barrier to prevent unauthorized access to internal systems.
  + It can filter traffic based on IP addresses, ports, and protocols.
  + It can block malicious traffic, such as DDoS attacks, viruses, and malware.
* **Practical Example**: If you set up a home router, it likely has a built-in firewall that blocks incoming requests from unknown or untrusted sources.

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

* **Vulnerability Assessment (VA)**: A systematic process used to identify, quantify, and prioritize vulnerabilities in a system. It provides a report of potential weaknesses but does not attempt to exploit them.
  + **Example**: Running an automated tool like **Nessus** to scan a network for known vulnerabilities.
* **Penetration Testing (PT)**: A simulated cyber attack that exploits vulnerabilities to assess the effectiveness of security defenses. It attempts to break into systems or applications.
  + **Example**: A penetration tester using **Metasploit** to exploit a vulnerability in a web application to gain unauthorized access.

**4. Difference Between HIDS and NIDS**

* **HIDS (Host-based Intrusion Detection System)**: Monitors the activities of individual systems (e.g., a computer or server). It checks for suspicious behavior or changes in the host, such as unauthorized file access or system configuration changes.
  + **Example**: Using **OSSEC** to monitor system logs and file integrity on a server.
* **NIDS (Network-based Intrusion Detection System)**: Monitors network traffic for signs of malicious activity, such as unusual data flows or network scans.
  + **Example**: Using **Snort** to detect a DDoS attack by analyzing network packets.

**5. Explain SSL Encryption**

* **SSL (Secure Sockets Layer)** is a protocol used to secure communication over a network, primarily the internet. SSL encrypts the data transmitted between a client (browser) and a server to prevent eavesdropping and tampering.
  + **Example**: When you visit an HTTPS website, SSL encrypts the communication between your browser and the server to protect sensitive information like login credentials.

**6. What is Data Leakage?**

* **Data Leakage** refers to the unauthorized transmission of data from within an organization to external parties. This can occur due to improper security controls or accidental sharing of sensitive information.
* **Practical Example**: Sending an email containing confidential company data to the wrong recipient or using a personal cloud service to store company files.

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

* **Brute Force Attack**: An attack where an attacker tries every possible combination of characters to guess a password or encryption key.
* **Prevention**:
  + Use long, complex passwords (e.g., a mix of uppercase, lowercase, numbers, and symbols).
  + Enable account lockout after several failed attempts.
  + Use Multi-Factor Authentication (MFA) to add an extra layer of security.
  + Use CAPTCHAs to limit automated attempts.
* **Practical Example**: Using a password manager to generate a strong password and enforce MFA on your accounts.

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

* **MITM (Man-in-the-Middle) Attack**: Occurs when an attacker intercepts and potentially alters communication between two parties without their knowledge.
* **Prevention**:
  + Use **SSL/TLS** to encrypt communication, ensuring that even if intercepted, the data is unreadable.
  + Implement **Public Key Infrastructure (PKI)** to authenticate users and servers.
  + Use VPNs to secure communication over untrusted networks like public Wi-Fi.
* **Practical Example**: Using HTTPS when accessing online banking to prevent an attacker from reading or altering your transaction.

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

* **XSS (Cross-Site Scripting)** is an attack where an attacker injects malicious scripts into a trusted website, typically targeting users who visit the website.
* **Prevention**:
  + Validate and sanitize user inputs to prevent malicious script execution.
  + Use **Content Security Policy (CSP)** headers to restrict the sources of executable scripts.
  + Implement proper output encoding on user-generated content.
* **Practical Example**: Ensuring that input fields on a website do not accept HTML or JavaScript code by escaping characters like <, >, etc.

**10. What is a Botnet?**

* A **Botnet** is a network of compromised devices (computers, IoT devices, etc.) controlled remotely by an attacker, often used to perform large-scale attacks like DDoS.
* **Practical Example**: A hacker infects hundreds of machines with malware, creating a botnet, and uses it to flood a website with traffic, making it unavailable.

**11. Explain SSL and TLS**

* **SSL (Secure Sockets Layer)**: An older cryptographic protocol used to secure data between a client and a server.
* **TLS (Transport Layer Security)**: The modern, more secure version of SSL. TLS is what most websites and services use today to encrypt communication.
* **Practical Example**: When you visit a website using **https://**, the browser uses TLS to secure the connection between your browser and the server.

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

* **Virus**: A self-replicating program that attaches itself to other programs and spreads when executed. It can corrupt files or damage systems.
* **Malware**: Any malicious software designed to cause harm, steal data, or gain unauthorized access to systems. Examples include viruses, worms, and trojans.
* **Ransomware**: A type of malware that encrypts a victim’s files and demands payment (ransom) for their decryption.
* **Practical Example**: **WannaCry** is a well-known example of ransomware that spread globally, encrypting users’ files and demanding payment.

**13. What is Phishing? Provide an Example**

* **Phishing** is a type of social engineering attack where attackers impersonate a legitimate entity to steal sensitive information such as usernames, passwords, and credit card details.
* **Example**: Receiving an email that looks like it’s from your bank, asking you to click a link and provide your account credentials.

**14. Define the Terms Encryption and Decryption**

* **Encryption**: The process of converting plain text into an unreadable format to prevent unauthorized access.
* **Decryption**: The process of converting encrypted data back into its original, readable format.
* **Practical Example**: Sending an encrypted email so that only the recipient with the decryption key can read it.

**15. What is a DDoS Attack and How Does it Work?**

* A **DDoS (Distributed Denial of Service)** attack is when multiple systems are used to flood a server or network with traffic, making it unavailable.
* **Practical Example**: An attacker uses a botnet to send millions of requests to a website, causing it to crash or become unresponsive.

**16. What is a Zero-Day Vulnerability?**

* A **Zero-Day Vulnerability** is a flaw in software that is unknown to the software vendor and thus has no fix or patch available. These vulnerabilities are often exploited by attackers before they are discovered.
* **Practical Example**: An attacker exploits a vulnerability in a web browser before the vendor releases a patch to fix it.

**17. What is Network Sniffing?**

* **Network Sniffing** is the practice of intercepting and analyzing packets of data traveling over a network.
* **Practical Example**: Using tools like **Wireshark** to capture and analyze network traffic for troubleshooting or identifying vulnerabilities.

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

* A **SOC** is a centralized unit within an organization responsible for monitoring and responding to security incidents. It uses tools to detect, analyze, and mitigate security threats.
* **Practical Example**: A SOC might use SIEM (Security Information and Event Management) systems to monitor log data for suspicious activities.

**19. What is the Importance of Forensics in Cybersecurity?**

* **Cyber Forensics** involves investigating and analyzing cybercrimes and security incidents. It helps organizations understand how an attack occurred, the impact of the attack, and provides evidence for legal proceedings.
* **Practical Example**: Using forensic tools to recover deleted files from a compromised computer to understand how the attacker gained access.

**20. Future Trends in Cybersecurity and Key Skills**

* **Future Trends**:
  + The rise of **AI and machine learning** in threat detection.
  + Increased focus on securing **IoT devices**.
  + Expansion of **cloud security** as more organizations migrate to the cloud.
  + **Quantum computing** will challenge traditional encryption methods.
* **Key Skills**:
  + Ethical hacking and penetration testing.
  + Knowledge of encryption and cryptography.
  + Threat intelligence and incident response.
  + Cloud security and IoT security.

**21. Difference Between IDS and IPS**

* **IDS (Intrusion Detection System)**: Monitors network or system activities for signs of suspicious behavior or attacks and generates alerts but does not actively block the attacks.
* **IPS (Intrusion Prevention System)**: Monitors and analyzes network traffic in real-time and actively blocks potential threats based on predefined security rules.
* **Practical Example**: **Snort** can be configured as both an IDS and IPS depending on how it is set up.