1. **Explain CIA triad:**  
   The CIA triad is a model for information security that consists of **Confidentiality**, **Integrity**, and **Availability**:
   * **Confidentiality**: Ensuring only authorized users have access to sensitive information.
   * **Integrity**: Ensuring that data is accurate and has not been tampered with.
   * **Availability**: Ensuring that data and services are accessible when needed.
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 security rules. It is used to protect networks from unauthorized access, cyber threats, and malware.
3. **What is the difference between VA (Vulnerability Assessment) and PT (Penetration Testing)?**
   * **Vulnerability Assessment (VA)**: Identifies and ranks security vulnerabilities in a system but does not exploit them.
   * **Penetration Testing (PT)**: Simulates real cyberattacks by actively exploiting vulnerabilities to evaluate security.
4. **What is the difference between HIDS and NIDS?**
   * **HIDS (Host-based Intrusion Detection System)**: Monitors individual devices for suspicious activity.
   * **NIDS (Network-based Intrusion Detection System)**: Monitors network traffic to detect threats.
5. **Explain SSL Encryption:**  
   SSL (Secure Sockets Layer) encryption secures data transmission between a web browser and a server by encrypting the communication, preventing eavesdropping and data tampering.
6. **What is Data Leakage?**  
   Data leakage occurs when sensitive information is unintentionally exposed to unauthorized users, leading to security risks.
7. **What is a Brute Force Attack? How can you prevent it?**  
   A brute force attack is a hacking method where attackers try all possible password combinations to gain access. Prevention methods include:
   * Using strong, complex passwords
   * Implementing account lockouts after multiple failed attempts
   * Using multi-factor authentication (MFA)
8. **Explain MITM attack and how to prevent it?**  
   A **Man-in-the-Middle (MITM) attack** is when an attacker intercepts and possibly alters communication between two parties. Prevention methods:
   * Using encrypted connections (SSL/TLS)
   * Avoiding public Wi-Fi without a VPN
   * Implementing strong authentication mechanisms
9. **Explain XSS attack and how to prevent it?**  
   **Cross-Site Scripting (XSS)** is an attack where malicious scripts are injected into trusted websites to steal user data. Prevention methods:
   * Input validation and sanitization
   * Using Content Security Policy (CSP)
   * Escaping special characters in web inputs
10. **What is a Botnet?**  
    A **botnet** is a network of compromised computers controlled by an attacker to launch cyberattacks such as DDoS attacks or spam campaigns.
11. **Explain SSL and TLS:**

* **SSL (Secure Sockets Layer)**: An older encryption protocol for securing internet communications.
* **TLS (Transport Layer Security)**: The successor to SSL, offering better security and performance.

1. **Define the terms Virus, Malware, and Ransomware:**

* **Virus**: A malicious program that attaches to legitimate files and spreads when executed.
* **Malware**: A broad term for malicious software, including viruses, worms, and trojans.
* **Ransomware**: A type of malware that encrypts files and demands a ransom for decryption.

1. **What is Phishing? Provide an example.**  
   **Phishing** is a cyberattack where attackers trick users into providing sensitive information by pretending to be a trusted entity.  
   **Example**: A fake email from "your bank" asking for login credentials.
2. **Define the terms Encryption and Decryption:**

* **Encryption**: The process of converting data into an unreadable format to protect it.
* **Decryption**: Converting encrypted data back into a readable format.

1. **What is a DDoS attack and how does it work?**  
   A **Distributed Denial of Service (DDoS) attack** overwhelms a target server with excessive traffic from multiple sources, making it inaccessible.
2. **What is a zero-day vulnerability?**  
   A **zero-day vulnerability** is a software flaw unknown to developers, making it a prime target for cybercriminals before a patch is released.
3. **What is network sniffing?**  
   **Network sniffing** is the practice of capturing and analyzing network traffic, which can be used for legitimate monitoring or malicious eavesdropping.
4. **What is a Security Operations Center (SOC)?**  
   A **SOC** is a centralized team and facility responsible for monitoring, detecting, and responding to cybersecurity threats in an organization.
5. **What is the importance of forensics in cybersecurity?**  
   **Cyber forensics** helps investigate cybercrimes, collect evidence, and understand attack patterns to improve security measures.

**Assignment: Ethical Hacking**

1. **Discuss future trends in cybersecurity. Which skills are important for cybersecurity professionals?**  
   **Future trends in cybersecurity:**

* AI-driven threat detection
* Quantum computing risks
* Zero-trust security models
* Cloud security advancements
* Increased focus on privacy laws

**Important skills for cybersecurity professionals:**

* Ethical hacking and penetration testing
* Incident response and forensics
* Security architecture and risk assessment
* Programming (Python, Java, C)
* Knowledge of compliance regulations

1. **What is the difference between IDS and IPS?**

* **IDS (Intrusion Detection System)**: Monitors network traffic for threats but does not take action.
* **IPS (Intrusion Prevention System)**: Detects threats and actively blocks them.