1.Explain CIA triad?

- The CIA Triad—Confidentiality, Integrity, and Availability—is a guiding model in information security. A comprehensive information security strategy includes policies and security controls that minimize threats to these three crucial components.

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

- The primary use of a firewall in networking is to secure the network from cyberattacks. For example, a firewall prevents malicious and unwanted content from entering your environment. As well, a firewall protects vulnerable systems and private data in the network from unauthorized access–such as hackers or insiders.

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

- The key difference between vulnerability assessment and penetration testing is that vulnerability assessments search for potential weak points in your security, while penetration testing identifies weaknesses and then attempts to exploit them.

4. What is the difference between HIDS and NIDS?

- HIDS protects against host-level attacks while NIDS (Network-Based Intrusion Detection System) protects against attacks to a network segment.

5. Explain SSL Encryption?

- SSL is standard technology for securing an internet connection by encrypting data sent between a website and a browser (or between two servers). It prevents hackers from seeing or stealing any information transferred, including personal or financial data.

6. What is Data Leakage?

- A data leak unintentionally exposes sensitive, protected, or confidential information outside its intended environment. This happens for various reasons, such as internal human errors, software vulnerabilities, or poor data security measures.

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

- A brute force attack is a hacking method that uses trial and error to crack passwords, login credentials, and encryption keys. It is a simple yet reliable tactic for gaining unauthorized access to individual accounts and organizations' systems and networks.

The most obvious way to block brute-force attacks is to simply lock out accounts after a defined number of incorrect password attempts. Account lockouts can last a specific duration, such as one hour, or the accounts could remain locked until manually unlocked by an administrator.

8. Explain MITM attack and how to prevent it?

- Man-in-the-middle attacks (MITM) are a [common type of cybersecurity attack](https://www.rapid7.com/fundamentals/types-of-attacks/) that allows attackers to eavesdrop on the communication between two targets. The attack takes place in between two legitimately communicating hosts, allowing the attacker to “listen” to a conversation they should normally not be able to listen to, hence the name “man-in-the-middle.”

MITM attack prevention:

1. Strong wep/wpa encryption on access point
2. Strong router login credential
3. Virtual private network
4. Force HTTPS

9. Explain XSS attack and how to prevent it?

- Cross-site scripting (also known as XSS) is a web security vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. It allows an attacker to circumvent the same origin policy, which is designed to segregate different websites from each other. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, to carry out any actions that the user is able to perform, and to access any of the user's data. If the victim user has privileged access within the application, then the attacker might be able to gain full control over all of the application's functionality and data.

10. What is a Botnet?

- A **botnet** is a group of [Internet](https://en.wikipedia.org/wiki/Internet)-connected devices, each of which runs one or more [bots](https://en.wikipedia.org/wiki/Internet_bot). Botnets can be used to perform [distributed denial-of-service](https://en.wikipedia.org/wiki/Distributed_denial-of-service_attack) (DDoS) attacks, steal data, send [spam](https://en.wikipedia.org/wiki/Spamming), and allow the attacker to access the device and its connection. The owner can control the botnet using command and control (C&C) software. The word "botnet" is a [portmanteau](https://en.wikipedia.org/wiki/Portmanteau) of the words "[robot](https://en.wikipedia.org/wiki/Robot)" and "[network](https://en.wikipedia.org/wiki/Computer_network)". The term is usually used with a negative or malicious connotation.

11. Explain SSL and TLS?

- SSL/TLS stands for secure sockets layer and transport layer security. It is a protocol or communication rule that allows computer systems to talk to each other on the internet safely. SSL/TLS certificates allow web browsers to identify and establish encrypted network connections to web sites using the SSL/TLS protocol.

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

- A virus is designed as a malicious code attached to a separate file. A virus can format a hard drive, or it can be harmless. Impact on the system. Malware can control and steal data, use the resources of a computer, destroy the system, etc. Ransomware locks the system and encrypts all data.

13. What is Phishing? Provide an example?

- Phishing happens when a victim acts on a fraudulent email that demands urgent action. Examples of requested actions in a phishing email include: Clicking an attachment. Enabling macros in a Word document.

14. Define the terms Encryption and Decryption?

- Encryption is the process of translating plain text data (plaintext) into something that appears to be random and meaningless (ciphertext). Decryption is the process of converting ciphertext back to plaintext.

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

- DDoS Attack means "Distributed Denial-of-Service (DDoS) Attack" and it is a cybercrime in which the attacker floods a server with internet traffic to prevent users from accessing connected online services and sites

16. What is a zero-day vulnerability?

- A zero-day vulnerability is a security loophole in software, hardware or firmware that threat actors exploit before the vendors can identify and patch it.

17. What is network sniffing?

- Sniffing is a process of monitoring and capturing all data packets passing through given network. Sniffers are used by network/system administrator to monitor and troubleshoot network traffic. Attackers use sniffers to capture data packets containing sensitive information such as password, account information etc.

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

- A security operations center (SOC) improves an organization's [threat detection](https://www.ibm.com/services/threat-intelligence?utm_content=SRCWW&p1=Search&p4=43700074604548183&p5=e&gad_source=1&gclid=CjwKCAiAivGuBhBEEiwAWiFmYf5-CFHXYzvS212eJrA3vSOQDZutpGjBXTgNz8VXy7jXnJCbntBroBoC2eMQAvD_BwE&gclsrc=aw.ds), response and prevention capabilities by unifying and coordinating all cybersecurity technologies and operations.

19. What is the importance of forensics in cyber security? Assignment: Ethical hacking

- Forensic cybersecurity is uncovering, analyzing, and preserving digital evidence following a cyberattack. It helps organizations mitigate the damage, understand how the attack occurred, and prevent future incidents

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

- Professionals need to understand key concepts like public key infrastructure (PKI), symmetric and asymmetric encryption, digital signatures, and hashing algorithms. These skills are critical for protecting sensitive data, ensuring security protocols are adhered to, and mitigating risks in malware analysis.

21. What is the difference between IDS and IPS?

- An IDS is designed to only provide an alert about a potential incident, which enables a security operations center (SOC) analyst to investigate the event and determine whether it requires further action. An IPS, on the other hand, takes action itself to block the attempted intrusion or otherwise remediate the incident.