**What is Cybersecurity?**

**Cybersecurity** refers to the practice of protecting systems, networks, programs, devices, and data from **digital attacks, unauthorized access, damage, or theft.** It involves implementing technologies, processes, and controls to safeguard computers, servers, mobile devices, and sensitive information from cyber threats such as:

* **Malware** (viruses, ransomware, spyware)
* **Phishing** and social engineering attacks
* **Hacking** and data breaches
* **Denial-of-Service (DoS/DDoS) attacks**
* **Insider threats** and human error

**Key Goals of Cybersecurity (CIA Triad)**

**1. Confidentiality** – Ensuring only authorized users can access data.

**2. Integrity** – Protecting data from being altered or corrupted.

**3. Availability** – Ensuring systems and data are accessible when needed.

**Types of Cybersecurity**

* **Network Security** – Protects networks from intrusions.
* **Application Security** – Secures software and apps from threats.
* **Information Security** – Protects sensitive data.
* **Cloud Security** – Secures cloud-based systems and data.
* **Endpoint Security** – Protects devices like laptops and smartphones.

**Why is Cybersecurity Important?**

With increasing cyber threats, cybersecurity helps prevent financial losses, reputational damage, and legal consequences for businesses and individuals.

**Question and Answer**

**Basic Cybersecurity Concepts**

**1. What is cybersecurity?**

The practice of protecting systems, networks, and data from digital attacks.

**2. What are the three main goals of cybersecurity (CIA Triad)?**

Confidentiality, Integrity, Availability.

**3. What is a cyber threat?**

Any potential malicious attack that seeks to damage or steal data.

**4. What is a vulnerability in cybersecurity?**

A weakness in a system that can be exploited by attackers.

5. **What is an exploit?**

A method or tool used to take advantage of a vulnerability.

6. **What is a zero-day vulnerability?**

A flaw in software that is unknown to the vendor and has no patch yet.

**7. What is risk in cybersecurity?**

The potential for loss or damage due to a cyber threat.

**8. What is encryption?**

Converting data into a coded form to prevent unauthorized access.

**9. What is multi-factor authentication (MFA)?**

A security method that requires two or more verification steps to access an account.

**10. What is a firewall?**

A network security device that monitors and filters incoming/outgoing traffic.

**Cyber Threats & Attacks**

**11. What is malware?**

Malicious software designed to harm systems (e.g., viruses, ransomware).

**12. What is ransomware?**

Malware that encrypts files and demands payment to unlock them.

**13. What is phishing?**

A fraudulent attempt to steal sensitive information via fake emails or websites.

**14. What is spear phishing?**

A targeted phishing attack aimed at a specific individual or organization.

**15. What is a brute-force attack?**

A trial-and-error method to guess passwords or encryption keys.

**16. What is a DDoS attack?**

**Distributed Denial of Service** – Overwhelming a server with traffic to crash it.

**17. What is social engineering?**

Manipulating people into revealing confidential information.

**18. What is a man-in-the-middle (MITM) attack?**

An attacker secretly intercepts and alters communications between two parties.

**19. What is SQL injection?**

A code injection attack that exploits vulnerabilities in database queries.

**20. What is a botnet?**

A network of infected computers controlled by an attacker for malicious purposes.

**Security Measures & Best Practices**

**21. What is antivirus software?**

A program that detects and removes malware.

**22. What is a VPN?**

**Virtual Private Network** – Encrypts internet traffic for privacy and security.

**23. Why is patch management important?**

Updating software fixes security vulnerabilities.

**24. What is a strong password?**

A long, complex password with letters, numbers, and symbols.

**25. What is the principle of least privilege?**

Users should have only the minimum access needed to perform their jobs.

**26. What is endpoint security?**

Protecting devices (laptops, phones) from cyber threats.

**27. What is network segmentation?**

Dividing a network into smaller parts to limit attack spread.

**28. What is a honeypot**?

A decoy system to attract and study hackers.

**29. What is incident response?**

A plan to detect, respond to, and recover from cyber incidents.

**30. What is penetration testing?**

Ethical hacking to find security weaknesses before attackers do.

**Data Protection & Privacy**

**31. What is Personally Identifiable Information (PII)?**

Data that can identify an individual (e.g., name, SSN, address).

**32. What is GDPR?**

**General Data Protection Regulation** – EU law for data privacy.

**33. What is data encryption at rest?**

Encrypting stored data to prevent unauthorized access.

**34. What is data masking?**

Hiding sensitive data with random characters (e.g., credit card numbers).

**35. What is a data breach?**

Unauthorized access to confidential data.

**36. What is tokenization?**

Replacing sensitive data with unique tokens for security.

**37. What is a security audit?**

A systematic evaluation of security policies and controls.

**38. What is a security policy?**

A set of rules to protect an organization’s data and systems.

**39. What is biometric authentication?**

Using fingerprints, facial recognition, or iris scans for security.

**40. What is a security token?**

A physical or digital device used for authentication (e.g., RSA token).