1. What is cybersecurity and why is it important?

→ Cybersecurity refers to the practice of protecting networks, digital information and systems from unauthorized access or disruption.
It is essential to safeguard sensitive data, prevent financial losses and maintain trust in systems. Ultimately, effective safeguards privacy, and maintains national security.

2. What is the difference between a threat, a vulnerability and a risk?

→ A threat is a potential occurance that could compromise security and a vulnerability is a weakness in a system that can be exploited by a threat where in essence, threat exploits a vulnerability which creates a risk as likelihood.

3. Define CIA triad (Confidentiality, Integrity, Availability)

→ The CIA triad is a foundational model for guiding information security policies.

- Confidentiality: data is accessible only to authorized users
- Integrity: Ensuring data accuracy and preventing unauthorized modifications.
- Availability: Data & systems are accessible when needed.

4. What is the difference between IDS and IPS?

→ An intrusion detect system (IDS) is a passive system that monitors network traffic for signs of unauthorized access or malicious activity alerting administrators. In contrast, IPS is an active system which takes an action to block intrusion from succeeding in real-time.

5. What is the difference between symmetric and asymmetric encryption?

⇒ Symmetric encryption uses a single, shared secret key for both encrypting and decrypting data, making it very fast for large dataset.
Asymmetric encryption uses a pair of keys eg. RSA; more secure for key exchange but slower.

6. What is the principle of least privilege?

→ It involves granting users and system only the minimum level of access and permission necessary to perform their task.
It minimizes the potential damage from a malicious attack or an accidental error.

7. Explain the difference between hashing and encryption.

→ Hashing: A one-way process that converts data into fixed size string of characters (hash), which cannot be reversed.

Encryption: A two way process where data can be encrypted and then decrypted back to its original form using a key.

8. What is 2FA and how does it work?

→ It is a security process that requires users to provide two different authentication factors to verify their identity, adding a second layer of security to a password.

9. What is the difference between black hat, white hat and grey hat hackers?

→ The difference lies their motivation and legality.

Black hat hackers: Malicious hackers exploiting vulnerabilities.

White hat hackers: Ethical hackers fixing security issues.

Grey hat hackers: who may exploit vulnerabilities without malicious intent but often without permission, operating in a legal grey area.