Ech

- Information Gathering

1. Meaning of Cybersecurity
Cybersecurity is the practice of protecting systems, networks, and data from cyber threats, including hacking, malware, and data breaches.

2. Main Objectives of Cybersecurity (CIA Triad)
Confidentiality – Protecting sensitive data from unauthorized access.
Integrity – Ensuring data is accurate and not altered.
Availability – Keeping systems and data accessible to authorized users.

3. Offensive vs. Defensive Cybersecurity
Offensive Security – Ethical hacking, penetration testing, and red teaming to find vulnerabilities.
Defensive Security – Protecting systems using firewalls, monitoring, and incident response.

4. Cyberspace & Cyber Law
Cyberspace – The digital world where computers, networks, and users interact.
Cyber Law – Legal regulations for online activities, covering data privacy, cybercrime, and digital rights.
5. Cyber Warfare
Cyber warfare involves nation-states or groups using cyber attacks to disrupt or damage enemy systems, such as infrastructure hacking and misinformation campaigns.

6. Types of Hackers
White Hat – Ethical hackers securing systems.
Black Hat – Malicious hackers breaking into systems.
Grey Hat – In-between, sometimes breaking rules but not always malicious.
Script Kiddies – Inexperienced hackers using pre-made tools.
Hacktivists – Hackers promoting political or social causes.

7. Full Form of SOC
SOC – Security Operations Center, a team monitoring, detecting, and responding to cyber threats 24/7.

8. Challenges of Cybersecurity
Sophisticated Cyber Attacks – AI-powered and evolving threats.
Lack of Awareness – Human errors leading to security breaches.
Cloud & IoT Security Risks – Protecting expanding digital environments.
Compliance & Regulations – Adhering to data protection laws.
Zero-Day Vulnerabilities – Unknown security flaws being exploited.