Module 1 CS- Introduction

1 what is meaning of cyber security

Ans- **Cybersecurity** is the practice of **protecting computers, networks, data, and systems** from **unauthorized access, attacks, or damage**.

2.what are the main objectives of cyber security?

Ans- **1. Confidentiality**

- Protect data from unauthorized access.
- Example: Data encryption, access control.

2. Integrity

- Ensure data is accurate and unaltered.
- Example: Hashing, version control.

3. Availability

- Ensure systems and data are accessible when needed.
- Example: Backup, redundancy, DDoS protection.

3.What is offensive and defensive in cyber security?

Ans- **Offensive Cybersecurity:**

- **Purpose:** Simulate attacks to find weaknesses.
- **Activities:** Ethical hacking, penetration testing, red teaming.
- **Goal:** Identify and exploit vulnerabilities before real attackers do.

Defensive Cybersecurity:

- **Purpose:** Protect systems from attacks.
- **Activities:** Firewalls, antivirus, monitoring, incident response.
- **Goal:** Detect, block, and recover from threats.

4.what is cyberspace and low

Ans- **Cyberspace:**

- A **virtual environment** where digital communication and activities happen over the internet.

- Includes **networks, computers, software, and data**.
- Example: Social media, online banking, email, websites.

Cyber Law:

- Laws that **govern behavior in cyberspace**.
- Covers **data protection, cybercrime, online privacy, and digital transactions**.
- Example: IT Act 2000 (India), GDPR (Europe).

5. What is cyber welfare?

Ans- **Cyber Welfare** refers to ensuring the **safe, responsible, and ethical use of digital technology** to protect individuals' **well-being, privacy, and rights** online.

6.Explain the Types of Hacker

Ans- **1. White Hat (Ethical Hacker):**

- Works with permission to find and fix security flaws.
- **Goal:** Improve security.
- Example: Penetration testers.

2. Black Hat:

- Breaks into systems **illegally** for personal gain or harm.
- **Goal:** Steal data, damage systems, etc.
- Example: Cybercriminals.

3. Grey Hat:

- Mix of white and black hat.
- Accesses systems **without permission** but doesn't harm — may report issues.
- **Goal:** Curiosity or to alert owners.

4. Script Kiddie:

- Uses existing tools/scripts without real hacking skills.
- **Goal:** Impress or cause mischief.

5. Hacktivist:

- Hacks to promote **political or social causes**.
- **Goal:** Spread messages, protest.

7.What is the full form of SOC in cyber security

Ans- **SOC = Security Operations Center**

It is a **centralized team or facility** that monitors, detects, analyzes, and responds to cybersecurity threats **24/7**.

8.What are the Challenges of Cyber Security

Ans- **Key Challenges:**

1. **Evolving Threats** – New types of malware and hacking methods appear constantly.
2. **Lack of Awareness** – Users may fall for phishing, scams, or weak passwords.
3. **Shortage of Experts** – Not enough skilled cybersecurity professionals.
4. **Insider Threats** – Risks from employees or trusted users.
5. **Cloud Security** – Managing security across shared, remote environments.
6. **Data Privacy** – Protecting sensitive data from leaks and misuse.
7. **IoT Devices** – Many are unsecured and easy to hack.