Module : 28 Cyber Security Introduction

1) Cybersecurity is all about protecting systems, networks, and data from digital attacks.

- These attacks can come in many forms, such as hacking, malware, phishing, and more.
- The goal of cybersecurity is to safeguard information from unauthorized access, theft, and damage.
- It involves a combination of technologies, processes, and practices designed to defend against these threats.

2) The main objectives of cyber security

- Confidentiality
- Integrity
- Availability
- Authentication
- Non-repudiation
- Accountability

3) Offensive Cybersecurity

- Offensive strategies involve proactively seeking out vulnerabilities and potential threats before they can cause harm. This can include activities such as penetration testing (pen testing), ethical hacking, and red teaming.

- Penetration Testing: Simulating attacks on a system to identify security weaknesses and fix them before malicious attackers can exploit them.
- Ethical Hacking: Authorized hacking conducted by skilled professionals to discover and address security gaps.
- Red Teaming: A group of security professionals who simulate real-world cyber-attacks to test and improve an organization's defenses.
- Defensive Cybersecurity:
- Defensive strategies focus on protecting systems, networks, and data from attacks. These measures aim to detect, prevent, and respond to cyber threats.
- Firewalls: Hardware or software that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
- Intrusion Detection and Prevention Systems (IDPS): Tools that detect and respond to potential threats or unusual activities on a network.
- Security Information and Event Management (SIEM): Systems that provide real-time analysis of security alerts generated by applications and network hardware.
- Blue Teaming: The defensive side of cybersecurity, where a team of professionals defends against attacks and continuously improves security measures.

4) Cyberspace refers to the virtual environment in which digital information is communicated and exchanged over networks, primarily the internet.

- It's an abstract realm where interactions between computers, systems, and users take place.
- Cyberspace encompasses everything from websites and social media platforms to data storage and digital communication channels.
- Cyber law is crucial for maintaining order and ensuring the legal and ethical use of cyberspace.
- It helps protect users' rights, promote trust in digital transactions, and address the challenges posed by the rapidly evolving digital landscape.

5) Cyber warfare refers to the use of computer technology to disrupt the activities of a state or organization, especially through deliberate attacks on information systems for strategic or military purposes.

6) White Hat Hackers

- Black Hat Hackers
- Grey Hat Hackers
- Script Kiddies
- Hacktivists
- State-Sponsored Hackers
- Cyber Criminals
- Insider Threats

7) SOC stands for Security Operations Center.

- A SOC is a centralized unit that deals with security issues on an organizational and technical level.
- It employs people, processes, and technology to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

8) The Challenges of Cyber Security

- Evolving Threat Landscape
- Sophistication of Attacks
- Shortage of Skilled Professionals
- Complexity of IT Systems
- Insider Threats
- Data Breaches
- Compliance and Regulatory Requirements
- Resource Constraints
- Human Error
- Supply Chain Vulnerabilities
- Rapid Technological Advancements