Module – 1

1. What is the meaning of Cybersecurity?

Cybersecurity refers to the practice of protecting systems, networks, programs, and data from cyber-attacks or unauthorized access. It involves implementing measures, policies, and controls to safeguard information from theft, damage, or disruption.

2. What are the main objectives of Cybersecurity?

The main objectives of cybersecurity can be categorized under the CIA triad:

Confidentiality: Ensuring that sensitive information is only accessible to authorized users.

Integrity: Ensuring the accuracy and trustworthiness of data by protecting it from being altered or tampered with.

Availability: Ensuring that systems, data, and services are available to authorized users when needed.

3. What is Offensive and Defensive in Cybersecurity?

Offensive Cybersecurity: This involves actively testing and exploiting vulnerabilities in systems to assess and improve security. This could involve penetration testing (ethical hacking), vulnerability assessments, or red team exercises

Defensive Cybersecurity: This focuses on protecting, detecting, and responding to cyber-attacks. Defensive strategies include deploying firewalls, antivirus software, intrusion detection systems (IDS), encryption, and monitoring networks for suspicious activity. The goal is to block attacks, minimize damage, and recover from incidents.

4. What is Cyberspace and Cyber Law?

Cyberspace: Refers to the virtual environment of information systems, including the internet, computer networks, and digital communication platforms. It's the domain where data is exchanged, and cyber activities (both malicious and legitimate) occur.

Cyber Law: Cyber laws are legal frameworks and regulations governing activities in cyberspace. These laws address issues such as:

Data protection and privacy

Intellectual property rights in digital content

Cybercrime and its prevention (e.g., hacking, identity theft)

Electronic transactions and e-commerce regulations

Cyber defamation and other offenses online

5. What is Cyber Warfare?

Cyber Warfare refers to the use of cyber tools and techniques by a nation-state or organized group to attack or disrupt the information systems of another entity for political, military, or strategic advantage. It can be a form of cyber-terrorism and is often part of larger military or geopolitical conflicts.

6. Explain the Types of Hackers

White Hat Hackers: Ethical hackers who use their skills to identify and fix security vulnerabilities. They work within legal boundaries and are often hired by companies for penetration testing and security assessments.

Black Hat Hackers: Malicious hackers who exploit vulnerabilities for personal gain, financial theft, or to cause harm. They operate outside the law and are responsible for illegal activities such as data breaches, ransomware attacks, and fraud.

Gray Hat Hackers: Hackers who fall between white and black hat. They may identify vulnerabilities without malicious intent but could exploit them without permission, often to expose flaws or gain recognition.

Script Kiddies: Unskilled individuals who use pre-written scripts or tools created by others to hack systems. They typically lack deep technical expertise.

Hacktivists: Individuals or groups who use hacking techniques for political or social causes. Their goal is to promote an agenda or cause, such as exposing corrupt practices or censorship.

State-sponsored Hackers: Hackers employed or funded by governments to conduct espionage, cyber warfare, or intelligence-gathering activities.

7. What is the full form of SOC in Cybersecurity?

SOC stands for Security Operations Center. A SOC is a centralized unit that monitors, detects, and responds to cybersecurity incidents on an ongoing basis

8. What are the Challenges of Cybersecurity?

The key challenges of cybersecurity include:

Evolving Threat Landscape: New types of malware, ransomware, and advanced persistent threats (APTs) are constantly emerging, making it difficult to keep defenses up to date.

Insider Threats: Employees or trusted insiders with access to sensitive data can pose risks, either intentionally or accidentally.

Complexity of Networks: Modern networks are large, complex, and interconnected, which increases the attack surface for hackers.

Third-party Risks: Many organizations rely on third-party vendors and partners, which can introduce vulnerabilities if not properly managed.

Module – 2

1. Difference Between Hardware and Software

Hardware: Refers to the physical components of a computer or network system. These are tangible parts you can touch and interact with, such as:

Examples: CPU, RAM , hard drives

Software: Refers to the set of instructions or programs that tell the hardware what to do. Software is intangible and cannot be touched.

Examples: Operating systems, applications

2. Define IP Address Range and Private Address Range

IP Address Range: An IP address (Internet Protocol address) is a unique numerical label assigned to every device connected to a network that uses the Internet Protocol. IP addresses are either IPv4 (32-bit) or IPv6 (128-bit).

Public IP Address Range: IP addresses that are routable on the public internet and are assigned by the Internet Assigned Numbers Authority (IANA). They range from 1.0.0.0 to 255.255.255.255.

Private IPv4 Address Ranges:

Class A: 10.0.0.0 to 10.255.255.255 (for large networks)

Class B: 172.16.0.0 to 172.31.255.255 (for medium-sized networks)

Class C: 192.168.0.0 to 192.168.255.255 (for small home or office networks)

A device on a home network may have the private IP address 192.168.1.10, which is non-routable on the internet.

3. Explain Network Protocol and Port Number

Network Protocol: A network protocol is a set of rules and conventions that govern communication between devices on a network. Protocols define how data is formatted, transmitted, and received, ensuring that devices can understand each other.

Examples of Network Protocols:

TCP (Transmission Control Protocol), UDP (User Datagram Protocol) , HTTP/HTTPS (Hypertext Transfer Protocol) ,FTP (File Transfer Protocol)

Port Number: A port number is a numerical identifier used in conjunction with an IP address to direct network traffic to the correct service or application on a device. Ports are used by protocols to identify the destination of data packets.

Types of Ports:

Well-known ports: Ports 0 to 1023

Registered ports: Ports 1024 to 49151

Dynamic/Private ports: Ports 49152 to 65535

4. Explain Types of Network Devices

Network devices are hardware components used to connect and manage network traffic between devices in a network. Some key types of network devices include:

Router:

Directs data packets between different networks, often between a local area network (LAN) and the internet. Routers determine the best path for data and can connect multiple networks.

A home router connects your devices to the internet.

Switch:

Operates at the data link layer (Layer 2) to connect devices within a local network (LAN). A switch uses MAC addresses to forward data to the correct destination within the same network.

A switch can connect multiple computers in an office network to enable data sharing.

Firewall:

Monitors and controls incoming and outgoing network traffic based on security rules. Firewalls can be hardware or software-based and are used to protect networks from unauthorized access or cyber threats.

Access Point (AP):

Allows wireless devices to connect to a wired network using Wi-Fi. Access points are often used in large buildings or campuses to provide wireless coverage.

5. Which Tools are Used for Data Backup and Recovery?

Bacula, amanda, veeam, windows backup and restore

6. Explain HTTP and HTTPS Protocols.

HTTP is an application layer protocol used for transmitting hypertext (HTML) between clients and servers. HTTP transmits data in plain text, which makes it vulnerable to attacks like man-in-the-middle (MitM) attacks.

HTTPS is an extension of HTTP that adds security through encryption. It is used for secure communication over the web. Data transmitted using HTTPS is encrypted, making it secure from hackers who may try to intercept the communication.

7. **What is SSL and TLS Security?**

SSL establishes an encrypted connection between a web server and a client to ensure that data is secure during transmission.

TLS is the successor to SSL and is a more secure and efficient cryptographic protocol. It provides encryption, authentication, and data integrity during data transmission.

8. Explain the MAC Address.

A MAC address is a unique hardware identifier assigned to a network interface card (NIC) of a device. It is used at the data link layer (Layer 2) of the OSI model for communication within a local network (LAN).

A MAC address is typically represented as six pairs of hexadecimal digits, separated by colons or hyphens (e.g., 00:1A:2B:3C:4D:5E or 00-1A-2B-3C-4D-5E).