Module : 29 Advanced Cybersecurity Concepts

1) Hardware

- Refers to the physical components of a computer or device that you can see and touch.
- Examples include the CPU (central processing unit), RAM (random access memory), hard drive, monitor, keyboard, and mouse.
- Hardware requires software to function properly.
- Software
- Refers to the intangible instructions, programs, or data that run on the hardware and enable it to perform specific tasks.
- Examples include operating systems (like Windows or macOS), applications (like web browsers or games), and programming languages.
- Software depends on hardware to execute its functions.

2) An IP address range refers to a block of IP addresses available for use within a network. IP addresses are unique numerical identifiers used to communicate between devices over a network, and they are defined in two versions: IPv4 (e.g., 192.168.0.1) and IPv6 (e.g., 2001:db8::1).

- The range specifies the starting and ending addresses within a block.
- Private IP address ranges are specific ranges of IP addresses reserved for use within private networks (e.g., home or office LANs) and are not directly routable on the internet. These ranges are defined by the Internet Assigned Numbers Authority (IANA) and are commonly used to avoid conflicts when devices communicate internally. Here are the private IP address ranges for IPv4:
- Class A: 10.0.0.0 – 10.255.255.255
- Class B: 172.16.0.0 – 172.31.255.255
- Class C: 192.168.0.0 – 192.168.255.255
- For IPv6, the private address range is called Unique Local Addresses (ULAs), and the reserved range is fc00::/7.

3) Network Protocol

- A network protocol is a set of rules and conventions that governs how data is transmitted, received, and processed across a network. These protocols ensure seamless communication between devices, irrespective of differences in hardware, software, or operating systems. They can operate at various layers of a network, based on the OSI model or TCP/IP model, and include well-known examples like:

- HTTP/HTTPS (HyperText Transfer Protocol): Used for web browsing.
- FTP (File Transfer Protocol): Used to transfer files.
- SMTP/IMAP/POP3: Used for email communication.
- TCP/IP (Transmission Control Protocol/Internet Protocol): Fundamental for internet communication, managing connections and addressing.
- DNS (Domain Name System): Resolves domain names to IP addresses.
- Port Number
- A port number is a numerical identifier (ranging from 0 to 65535) that specifies a specific process or service running on a device in a network. Ports help differentiate multiple services or applications communicating over the same network. For example:
- HTTP: Port 80
- HTTPS: Port 443
- FTP: Port 21
- SMTP: Port 25

4) 9 Types of network devices.

- Router
- Switch
- Hub
- Modem
- Access Point

- Gateway
- Firewall
- Network Interface Card (NIC)
- Repeater

5) 6 Tools use for Data Backup and Recovery

- Recoverit Data Recovery
- Cobian Backup
- EaseUS Todo Backup
- Acronis Cyber Protect
- Disk Drill
- Redo Rescue

6) HTTP (HyperText Transfer Protocol)

- Purpose: HTTP is the protocol used for transferring data between a client (like a browser) and a web server.
- Function: It allows users to load web pages, send form data, and interact with websites.
- Security: HTTP data is transmitted in plain text, making it vulnerable to interception by hackers during transmission.
- Port Number: HTTP uses port 80 by default.
- HTTPS (HyperText Transfer Protocol Secure)

- Purpose: HTTPS is the secure version of HTTP, designed to encrypt data transmission for safer communication.
- Function: In addition to HTTP's functionality, HTTPS ensures that the data sent between a client and server is encrypted, protecting it from unauthorized access.
- Security: It uses SSL (Secure Sockets Layer) or TLS (Transport Layer Security) protocols to provide encryption, authentication, and data integrity.
- Port Number: HTTPS uses port 443 by default.

7) SSL (Secure Sockets Layer)

- SSL is a cryptographic protocol designed to secure communication over the internet. It encrypts data transferred between a client (like a browser) and a server (like a website), ensuring that any intercepted data is unreadable by unauthorized parties. SSL was widely used for secure transactions like online banking and e-commerce.
- Key Features:
- Encryption: Protects data during transmission.
- Authentication: Verifies the identity of the server (and optionally the client) using digital certificates.
- Integrity: Ensures data is not altered during transfer.
- TLS (Transport Layer Security)

- TLS is the successor to SSL and provides stronger encryption and improved security. It has become the modern standard for securing communications. Like SSL, TLS encrypts data, authenticates parties, and ensures data integrity. TLS versions (e.g., TLS 1.2, TLS 1.3) are widely used in HTTPS today.
- Differences from SSL:
- Enhanced cryptographic algorithms.
- Better performance.
- Resistance to vulnerabilities found in SSL protocols.

8) A MAC Address (Media Access Control Address) is a unique identifier assigned to a network interface card (NIC) of a device. It is used for communication within a local network (e.g., a LAN). Think of it as the device's "physical address" on a network, helping devices identify and communicate with each other.