Module: Penetration Testing Basics

1. Difference between hardware and software.

Ans- **Difference between Hardware and Software**

- **Hardware:**
    - The **physical components** of a computer system that you can touch and see.
    - Examples: Keyboard, Mouse, CPU, Monitor, Hard Drive.
    - Without hardware, software cannot run.
- **Software:**
    - The set of **programs, instructions, or applications** that tell the hardware what to do.
    - Examples: Windows, MS Word, Chrome, Antivirus.
    - Without software, hardware is useless.

2. Define IP address range and private address range.

Ans- **IP Address Range**
An **IP address** is a unique number assigned to each device on a network. The IP address range refers to the set of addresses available within a specific network. For example, a network with IP 192.168.1.0/24 has a range of 192.168.1.1 – 192.168.1.254.

Private IP Address Range
Private IP addresses are reserved for use within **local/private networks** (like homes, offices) and are not routable on the public internet. They are defined by IANA (Internet Assigned Numbers Authority).

Private IPv4 ranges are:

- **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

3. Explain Network protocol and Port number.

Ans- **Network Protocol**
A **network protocol** is a set of rules and standards that define how data is transmitted and communicated between devices over a network.

- Examples: **HTTP** (web browsing), **FTP** (file transfer), **SMTP** (email), **TCP/IP** (internet communication).
- Purpose: Ensures devices from different vendors can communicate properly.

Port Number
A **port number** is a logical number assigned to network services to identify specific processes or applications on a device.

- Ports help multiple services run on the same IP address without conflict.
- Example: **Port 80 (HTTP)**, **Port 443 (HTTPS)**, **Port 25 (SMTP)**.
- Range: 0 – 65535 (Well-known ports: 0–1023).

4. Explain Types of Network Devices

Ans- **Types of Network Devices**

1. **Router**
   - Connects different networks (e.g., home network to the internet).
   - Forwards data packets based on IP addresses.
2. **Switch**
   - Connects multiple devices (computers, printers, servers) within a local network (LAN).
   - Forwards data using **MAC addresses**.
3. **Hub**
   - A basic device that broadcasts data to all connected devices.
   - Less secure and less efficient compared to a switch.
4. **Access Point (AP)**
   - Provides **wireless connectivity** to devices (Wi-Fi).
   - Extends the range of a network.

5. **Modem**
    - Connects a network to the **Internet Service Provider (ISP)**.
    - Converts digital signals to analog and vice versa.
6. **Firewall (Hardware/Software)**
    - Monitors and filters incoming/outgoing traffic.
    - Provides security by blocking unauthorized access.
7. **Gateway**
    - Connects two different types of networks and translates protocols.

5. Which Tools use for Data Backup and Recovery

Ans- **Tools Used for Data Backup and Recovery**

Data backup and recovery tools help in creating copies of data and restoring them in case of accidental loss, system failure, or cyberattack. Commonly used tools include:

1. **Acronis Cyber Protect** – Backup, recovery, and ransomware protection.
2. **Veeam Backup & Replication** – Popular for virtual machines and cloud backup.
3. **Commvault** – Enterprise-level backup and disaster recovery.
4. **Veritas NetBackup** – Scalable solution for large organizations.
5. **EaseUS Todo Backup** – User-friendly backup for personal and business use.
6. **Nakivo** – Backup for VMware, Hyper-V, and cloud.
7. **Duplicati** – Free, open-source backup tool with encryption support.
8. **Windows Backup & Restore / File History** – Built-in backup feature in Windows.
9. **Time Machine (macOS)** – Built-in backup solution for Apple systems.

6. Explain HTTP and HTTPS Protocols

Ans- **HTTP (HyperText Transfer Protocol)**

- A protocol used for transferring data (web pages, images, etc.) between a web browser and a web server.
- Works on **Port 80**.
- Data is sent in **plain text**, so it can be intercepted by attackers.
- Less secure, mainly used for non-sensitive communication.

HTTPS (HyperText Transfer Protocol Secure)

- A secure version of HTTP that uses **SSL/TLS encryption** to protect data.
- Works on **Port 443**.
- Encrypts communication, ensuring **confidentiality, integrity, and authentication**.
- Used for sensitive transactions like online banking, shopping, and logins.

7. What is SSL and TLS Security?

Ans- **SSL and TLS Security**

- **SSL (Secure Socket Layer):**
  A security protocol that encrypts the communication between a web browser and a server. It ensures data privacy, prevents eavesdropping, and verifies the identity of websites. However, SSL is now outdated.
- **TLS (Transport Layer Security):**
  The upgraded and more secure version of SSL. TLS provides stronger encryption, better authentication, and is widely used today to secure online communication (e.g., HTTPS websites, emails, VPNs).

Purpose of SSL/TLS Security:

- Protects data from interception (confidentiality).
- Ensures data is not altered (integrity).
- Confirms the identity of the website/server (authentication).

8. Explain the MAC ADDRESS?

Ans- **MAC Address (Media Access Control Address)**

- A **unique physical identifier** assigned to every network device's **Network Interface Card (NIC)** by the manufacturer.

- It is a **12-digit hexadecimal number** (48-bit) written as pairs (e.g., 00:1A:2B:3C:4D:5E).
- Works at the **Data Link Layer (Layer 2)** of the OSI model.
- Used to uniquely identify devices within a **local network (LAN)**.

Example:

- 08:00:27:5A:9B:6C