**Ethical Hacking Assignment**

**Module 27 Foundation**

* 1. Difference between hardware and software.

Hardware and software are two fundamental components of a computer system. While they work together to perform various functions, they have some fundamental differences:

Definition: Hardware refers to the physical components of a computer system, such as the motherboard, CPU, memory, hard drive, and peripheral devices like keyboard, mouse, and monitor. Software refers to the intangible components of a computer system, such as programs, applications, and operating systems.

Physical presence: Hardware components are tangible and can be touched, felt, and seen. Software, on the other hand, is intangible and cannot be touched or seen.

Function: Hardware components perform physical tasks and provide input and output capabilities. Software provides the instructions and commands that control hardware components and enable them to perform specific tasks.

Upgrades and maintenance: Hardware components can be upgraded or replaced to improve the performance of a computer system. Software can be updated or upgraded to fix bugs, add new features or enhance performance.

Cost: Hardware components are expensive compared to software. They require physical manufacturing and assembly. Software, on the other hand, can be produced and distributed at a much lower cost.

In summary, hardware and software are two different components of a computer system that work together to perform various tasks. While hardware is the physical component of a computer system, software is the set of instructions that control and interact with hardware to perform tasks.

* 1. Define IP address range and private address range.

IP address range refers to a range of IP addresses that are available for use in a particular network. An IP address is a unique numerical identifier that is assigned to each device connected to a network, such as a computer or a printer. IP addresses are used to enable communication between devices on the network.

The private address range is a range of IP addresses that are reserved for private use within a network. These addresses are not meant to be used on the public internet. The private address range includes the following IP address ranges:

10.0.0.0 - 10.255.255.255 (10.0.0.0/8)

172.16.0.0 - 172.31.255.255 (172.16.0.0/12)

192.168.0.0 - 192.168.255.255 (192.168.0.0/16)

These IP address ranges are commonly used in local area networks (LANs) and are assigned by routers or other network devices in the network. Private IP addresses are used to enable communication between devices on the same local network and are not routable on the public internet. Private IP addresses can be reused in different networks, which helps to conserve IP address space.

* 1. Explain Network protocol and Port number.

A network protocol is a set of rules and standards that govern how devices communicate and exchange data on a network. Network protocols define the format and structure of data packets that are transmitted over the network, as well as the procedures and rules for managing communication between devices.

Examples of commonly used network protocols include:

TCP/IP (Transmission Control Protocol/Internet Protocol)

HTTP (Hypertext Transfer Protocol)

FTP (File Transfer Protocol)

DNS (Domain Name System)

SMTP (Simple Mail Transfer Protocol)

Each network protocol has a specific purpose and is designed to perform certain tasks or functions. For example, TCP/IP is a suite of protocols that is used to enable communication on the internet and other networks, while HTTP is used to enable communication between web servers and clients.

A port number is a numerical identifier that is used to identify a specific process or application running on a device. Port numbers are used in conjunction with IP addresses to enable communication between devices on a network. When a device sends data to another device, it includes the port number of the process or application that is sending the data.

There are two types of port numbers: well-known ports and dynamic or private ports. Well-known ports are reserved for specific protocols and services, and range from 0 to 1023. For example, port 80 is used for HTTP traffic, while port 25 is used for SMTP traffic. Dynamic or private ports, on the other hand, are used by applications or processes that are not associated with a specific protocol or service, and range from 1024 to 65535.

In summary, network protocols define the rules and standards for communication between devices on a network, while port numbers are used to identify specific processes or applications running on devices and enable communication between them.

* 1. Explain Types of Network Devices

There are various types of network devices that are used to connect and manage communication between devices on a network. Some of the most commonly used network devices include:

Switches: Switches are used to connect devices on a network and enable communication between them. They operate at the data link layer of the OSI model and use MAC addresses to forward data packets between devices.

Routers: Routers are used to connect multiple networks together and enable communication between them. They operate at the network layer of the OSI model and use IP addresses to forward data packets between networks.

Firewalls: Firewalls are used to protect networks from unauthorized access and malicious traffic. They monitor and filter incoming and outgoing network traffic based on predefined security policies.

Access Points: Access points are used to provide wireless connectivity to devices on a network. They enable devices to connect to the network via Wi-Fi and typically include features such as WPA/WPA2 encryption, MAC address filtering, and guest network access.

Hubs: Hubs are used to connect devices on a network and forward data packets between them. However, unlike switches, hubs operate at the physical layer of the OSI model and do not perform any packet filtering or forwarding based on MAC addresses.

Modems: Modems are used to connect a computer or other network device to the internet via a telephone line, cable, or other type of communication channel. They convert digital signals from the device into analog signals that can be transmitted over the communication channel, and vice versa.

Load Balancers: Load balancers are used to distribute network traffic across multiple servers or network devices to ensure optimal performance and availability. They monitor network traffic and distribute it based on predefined load balancing algorithms.

In summary, network devices are used to connect and manage communication between devices on a network. Some of the most commonly used network devices include switches, routers, firewalls,