Ethical Hacking Assignments

Module -1

- Difference between hardware and software.

a. Hardware

- Hardware refers to the tangible parts of a computer system that you can see and touch. Examples include the monitor, keyboard, mouse, CPU (central processing unit), memory, and storage devices like hard drives and solid-state drives (SSDs).
- **Functionality:** Hardware provides the physical structure and components that carry out the computer's operations. It processes data, performs calculations, and interacts with external devices.

Software

- Software is the intangible set of instructions that tells the hardware what to do. It's essentially a collection of programs and data that run on the hardware. Examples include operating systems (like Windows or macOS), application software (like web browsers, word processors, and games), and system utilities.
- **Functionality:** Software provides the instructions and data that the hardware needs to perform specific tasks. It allows users to interact with the computer and carry out various functions.

- Define IP address range and private address range.

a. An IP (Internet Protocol) address range refers to a block of consecutive IP addresses that can be assigned to devices on a network. There are two main versions of IP addresses: IPv4 and IPv6.

IPv4 Address Range

IPv4 addresses are 32-bit numbers, usually written in decimal format as four octets separated by dots (e.g., 192.168.1.1). The range of IPv4 addresses is from 0.0.0.0 to 255.255.255.255, which allows for approximately 4.3 billion unique addresses.

IPv6 Address Range

IPv6 addresses are 128-bit numbers, written in hexadecimal format and separated by colons (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334). The range of IPv6 addresses is much larger, allowing for a virtually unlimited number of unique addresses.

Private Address Range

Private IP address ranges are designated for use within private networks and are not routable on the public Internet. These addresses are reserved by the Internet Assigned Numbers Authority (IANA) and help prevent conflicts between internal and external IP addresses.

IPv4 Private Address Ranges

IPv4 private addresses are specified in RFC 1918 and include the following ranges:

10.0.0.0 to 10.255.255.255

- Class A private address range
- Supports a single large network

172.16.0.0 to 172.31.255.255

- Class B private address range
- Can be divided into 16 contiguous Class B networks

192.168.0.0 to 192.168.255.255

- Class C private address range
- Typically used for smaller networks

IPv6 Private Address Ranges

IPv6 private addresses are specified in RFC 4193 and include Unique Local Addresses (ULAs), which have the following format:

fc00::/7 (or more commonly, fd00::/8)

- The first 7 bits are set to 1111110, making the prefix fc00::/7
- The remaining 121 bits can be used for network addressing within a private network

- Explain Network protocol and Port number.

a. port means to whom you communicate. & Protocol means how to communicate or way of communication. A port is just a channel that you select for the communication, and the protocol determines

how the communication is done. A certain protocol usually uses a specific port, like port 80 for HTTP, port 21 for FTP.

- Explain Types of Network Devices

- Network devices are essential for connecting computers and other devices within a network, enabling communication and data exchange. Here are the primary types of network devices:

  1. Router
  Function: Connects multiple networks together and routes data packets between them.
  Use Case: Typically used to connect local networks to the Internet, directing incoming and outgoing traffic efficiently.

  2. Switch
  Function: Connects devices within a single network and uses MAC addresses to forward data to the correct destination.
  Use Case: Commonly used in local area networks (LANs) to connect computers, printers, and servers within the same network.

  3. Hub
  Function: Broadcasts data to all devices on a network segment, without intelligence to direct the data to a specific device.
  Use Case: An older technology used to connect multiple Ethernet devices in a LAN; largely replaced by switches due to efficiency issues.

  4. Bridge
  Function: Connects two or more network segments, improving traffic flow by reducing collision domains.
  Use Case: Often used to extend or segment networks within an organization to manage traffic more effectively.

5. Modem
Function: Modulates and demodulates signals for data transmission over telephone lines, cable systems, or satellite links.
Use Case: Connects a network to an Internet Service Provider (ISP) via DSL, cable, or fiber.

6. Access Point (AP)
Function: Provides wireless connectivity to devices within a network, extending the reach of the network.
Use Case: Commonly used in wireless LANs to connect Wi-Fi-enabled devices to the wired network.

7. Firewall
Function: Monitors and controls incoming and outgoing network traffic based on predetermined security rules.
Use Case: Protects networks from unauthorized access, cyber-attacks, and data breaches by filtering traffic.

8. Repeater
Function: Amplifies or regenerates signals to extend the range of a network.
Use Case: Used in large networks or areas with weak signals to ensure consistent connectivity.

9. Gateway
Function: Serves as a bridge between different networks, enabling communication between different protocols and formats.
Use Case: Often used to connect a local network to a wide area network (WAN) or the Internet, translating data between disparate systems.

10. Network Interface Card (NIC)
Function: Provides the hardware interface for a device to connect to a network.

Use Case: Installed in computers and other devices to enable wired or wireless network connectivity.

11. Proxy Server
Function: Acts as an intermediary for requests from clients seeking resources from other servers, often providing caching and filtering.
Use Case: Used to improve performance, manage network traffic, and enhance security and privacy for users.

12. Load Balancer
Function: Distributes network or application traffic across multiple servers to ensure no single server becomes overwhelmed.
Use Case: Improves the performance and reliability of websites, applications, and other services by balancing the load.