MODULE 27 FOUNDATION

ETHICAL HACKER

1.Who is a Hacker? Types of Hackers

A Hacker is a person who finds and exploits the weakness in computer systems and/or networks

to gain access. Hackers are usually skilled computer programmers with knowledge of computer

security.

Hackers are classified according to the intent of their actions. The following list classifies

hackers according to their intent.

• Ethical Hacker (White hat): A hacker who gains access to systems with a view to fix the

identified weaknesses. They may also perform penetration testing and vulnerability

assessments.

• Cracker (Black hat): A hacker who gains unauthorized access to computer systems for

personal gain. The intent is usually to steal corporate data, violate privacy rights, transfer

funds from bank accounts etc.

• Grey hat: A hacker who is in between ethical and black hat hackers. He/she breaks into

computer systems without authority with a view to identify weaknesses and reveal them to

the system owner.

2.What is ethical hacking?

Ans: Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers.

3. How many types of phases of Ethical Hacking?

Ans: There are 5 types of phases in Ethical Hacking.

1.Reconnaissance

2.Scaning

3.Gaining access

4.Maintaining of access

5.Covering tracks

4.What are the Roles and Responsibilities of an Ethical Hacker?

Ethical Hackers must follow certain guidelines in order to perform hacking legally. A good hacker knows his or her responsibility and adheres to all of the ethical guidelines. Here are the most important rules of Ethical Hacking:

- An ethical hacker must seek authorization from the organization that owns the system. Hackers should obtain complete approval before performing any security assessment on the system or network.
- Determine the scope of their assessment and make known their plan to the organization.
- Report any security breaches and vulnerabilities found in the system or network.

- Keep their discoveries confidential. As their purpose is to secure the system or network, ethical hackers should agree to and respect their non-disclosure agreement.
- Erase all traces of the hack after checking the system for any vulnerability. It prevents malicious hackers from entering the system through the identified loopholes.

5. Difference between hardware and software.

Ans: Computer Hardware and software both are essential parts of computer system. Hardware and Software make a system compatible with the user. we are going do discuss the basic differences between computer hardware and computer software.

Computer Hardware

Hardware refers to the physical components of a computer. Computer Hardware is any part of the computer that we can touch these parts. These are the primary electronic devices used to build up the computer. Examples of hardware in a computer are the Processor, Memory Devices, Monitor, Printer, Keyboard, Mouse, and Central Processing Unit.

Types of Computer Hardware

- Input Devices
- Output Devices
- Storage Devices
- Internal Component

1. **Input Devices:** Input Devices are those devices through which a user enters data and information into the computer or simply, User interacts with the computer. Examples of Input Devices are Keyboard, Mouse, Scanner, etc.
2. **Output Devices:** Output Devices are devices that are used to show the result of the task performed by the user. Examples of Output Devices are Monitors, Printers, Speakers, etc.

3. **Storage Devices:** Storage Devices are devices that are used for storing data and they are also known as Secondary Storage Data. Examples of Storage Devices are CDs, DVDs, Hard Disk, etc.
4. **Internal Component:** Internal Components consists of important hardware devices present in the System. Examples of Internal Components are the CPU, Motherboard, etc.

Computer Software

Software is a collection of instructions, procedures, and documentation that performs different tasks on a computer system. we can say also Computer Software is a programming code executed on a computer processor. The code can be machine-level code or code written for an operating system. Examples of software are MS- Word, Excel, PowerPoint, Google Chrome, Photoshop, MySQL, etc.

Types of Computer Software

- System Software
- Application Software

1. System Software: System Software is a component of Computer Software that directly operates with Computer Hardware which has the work to control the Computer's Internal Functioning and also takes responsibility for controlling Hardware Devices such as Printers, Storage Devices, etc. Types of System Software include Operating systems, Language processors, and Device Drivers.

2. Application Software: Application Software are the software that works the basic operations of the computer. It performs a specific task for users. Application Software basically includes Word Processors, Spreadsheets, etc. Types of

Application software include General Purpose Software, Customized Software, etc.

Parameters	Hardware	Software
Basic Definition	Hardware is a physical part of the computer that causes the processing of data.	Software is a set of instructions that tells a computer exactly what to do.
Development	It is manufactured.	It is developed and engineered.
Dependency	Hardware cannot perform any task without software.	The software cannot be executed without hardware.
Process of creating	Electronic and other materials are used to create hardware.	Created by utilizing a computer language to write instructions.
Tangible	Hardware is tangible as hardware is a physical electronic device, that can be touched.	Software is intangible as we can see and also use the software but can’t touch them.

Parameters	Hardware	Software
Durability	Hardware typically wears out over time.	The software does not wear out with time. However, it may contain flaws and glitches.
Types	It has four main categories: 1. Input Devices 2. Output Devices 3. Storage Devices 4. Internal Components.	It is mainly divided into 1. System software 2. Application software.
Virus effect	Hardware is not affected by computer viruses.	Software is affected by computer viruses.
Transfer	It cannot be transferred from one place to another electrically through the network.	It can be transferred via a network means.

Parameters	Hardware	Software
Machine-Level language	Only machine-level language is known to be understood by hardware.	The program accepts human-readable input, interprets it in machine-level language, and sends it to hardware for additional processing.
Replacement	If the hardware is damaged, it is replaced with a new one.	If the software is damaged, its backup copy can be reinstalled.
Failures	Dust, overheating, humidity, and other factors are commonly responsible for hardware failures.	Overloading, systematic error, major-minor version error, and other factors are commonly responsible for software failures.
Examples	Ex: Keyboard, Mouse, Monitor, Printer, CPU, Hard disk, RAM, ROM, etc.	Ex: MS Word, Excel, PowerPoint, Photoshop, MySQL, etc.

6. Define IP address range and private address range.

Ans: An IP address range, also known as an IP address space or IP address block, refers to a range of IP addresses that are assigned or available within a certain network or subnet. These addresses are typically defined by a starting address and an ending address, representing the range of usable IP addresses within that network.

A private address range, also known as a private IP address range or private network range, refers to a set of IP addresses designated for private use within a local network, such as a home or corporate intranet. These addresses are reserved for use within private networks and are not routable over the internet.

The most commonly used private address ranges, as defined by the Internet Assigned Numbers Authority (IANA), are:

1. **IPv4 Private Address Ranges**:
    - **Class A**: 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
    - **Class B**: 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
    - **Class C**: 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)

These private IPv4 address ranges are commonly used in home and corporate networks for internal communication, allowing multiple devices to share a single public IP address for internet connectivity through network address translation (NAT).

2. **IPv6 Unique Local Addresses (ULA)**:
    - **Prefix**: fc00: :/7 (fd00: :/8 for locally assigned ULA prefixes)

IPv6 also supports private addressing using Unique Local Addresses (ULA). Unlike IPv4, IPv6 has a massive address space, and the concept of private addressing is slightly different. ULAs are used for local communication within a single site or organization and are not routable outside of that scope.

In summary, an IP address range refers to a range of IP addresses within a network, while a private address range specifically refers to reserved IP address ranges for

use within private networks, such as those defined by IANA for IPv4 and Unique Local Addresses (ULAs) for IPv6

7. Explain Network protocol and Port number.

Ans: **Network Protocol**:

A network protocol is a set of rules and conventions that govern the communication between devices or systems over a network. These protocols define the format and meaning of the data exchanged between devices, ensuring that information can be transmitted, received, and understood reliably.

Network protocols operate at different layers of the OSI (Open Systems Interconnection) model or the TCP/IP (Transmission Control Protocol/Internet Protocol) model. Each layer of these models corresponds to specific functions and protocols that handle different aspects of network communication.

Some common network protocols include:

1. **Internet Protocol (IP)**: This protocol defines the addressing scheme and routing of data packets across networks. It ensures that data packets are correctly delivered from the source to the destination.
2. **Transmission Control Protocol (TCP)**: TCP is a connection-oriented protocol that provides reliable, ordered, and error-checked delivery of data between devices. It establishes a connection between the sender and receiver, manages the flow of data, and ensures that packets are delivered in the correct order.
3. **User Datagram Protocol (UDP)**: UDP is a connectionless protocol that provides a simpler, faster, and less reliable method of data transmission compared to TCP. It does not establish a connection before transmitting data and does not guarantee delivery or order of packets. UDP is commonly used for real-time communication, such as streaming media or online gaming.
4. **Hypertext Transfer Protocol (HTTP)**: HTTP is an application-layer protocol used for transmitting hypermedia documents, such as web pages and multimedia content, over the internet. It defines how clients (web browsers)

request resources from web servers and how servers respond to those requests.

5. **File Transfer Protocol (FTP)**: FTP is a protocol used for transferring files between a client and a server on a computer network. It provides a set of commands for accessing, uploading, downloading, and managing files on remote servers.

These are just a few examples of the many network protocols that exist to facilitate communication between devices on a network.

Port Number:

In computer networking, a port number is a 16-bit unsigned integer assigned to each network communication endpoint, or port, within a device. Ports allow multiple network services or applications to operate simultaneously on a single device, each using a unique port number to distinguish between them.

Port numbers are used in conjunction with the IP address of a device to enable communication between devices over a network. When a device sends data to another device, it specifies both the IP address of the destination device and the port number of the receiving service or application.

Port numbers are divided into three ranges:

1. **Well-Known Ports (0-1023)**: Reserved for system services and applications commonly used by users or administrators. For example, port 80 is reserved for HTTP, port 443 for HTTPS, and port 22 for SSH.
2. **Registered Ports (1024-49151)**: Assigned by the Internet Assigned Numbers Authority (IANA) to specific services or applications upon request. These ports are commonly used by third-party applications and services.
3. **Dynamic (or Private) Ports (49152-65535)**: Also known as ephemeral ports, these are used by client applications or services temporarily for communication with servers. Operating systems typically assign these ports dynamically to outgoing connections.

Port numbers, in combination with IP addresses, facilitate the routing and delivery of data packets between devices on a network, ensuring that they reach the intended service or application running on a specific port.

8. Explain Types of Network Devices

1. Ans: **Router**:
    - A router is a networking device that connects multiple networks together and directs traffic between them. It operates at the network layer (Layer 3) of the OSI model and uses routing tables to determine the best path for data packets to reach their destination across interconnected networks. Routers can also provide functions such as network address translation (NAT), firewalling, and VPN (Virtual Private Network) connectivity.
2. **Switch**:
    - A switch is a networking device that connects multiple devices within a single local area network (LAN) and forwards data packets between them. It operates at the data link layer (Layer 2) of the OSI model and uses MAC addresses to forward packets only to the device intended to receive them, improving network efficiency compared to traditional hubs. Switches come in various configurations, including unmanaged, managed, and layer 3 switches.
3. **Hub**:
    - A hub is a basic networking device that connects multiple devices within a LAN and broadcasts data packets to all connected devices. Unlike switches, hubs operate at the physical layer (Layer 1) of the OSI model and do not have intelligence to selectively forward packets based on MAC addresses. As a result, they are less efficient and more prone to network congestion compared to switches. Hubs are now mostly obsolete and replaced by switches in modern networks.
4. **Access Point (AP)**:
    - An access point is a networking device that allows wireless devices to connect to a wired network using Wi-Fi technology. It operates at the

data link layer (Layer 2) of the OSI model and functions as a bridge between wireless devices and the wired network infrastructure. Access points are commonly used in wireless LANs (WLANs) to provide wireless connectivity to devices such as laptops, smartphones, and IoT devices.

5. **Modem**:
    - A modem (short for modulator-demodulator) is a networking device that converts digital data from a computer into analog signals for transmission over analog communication lines, such as telephone lines or cable lines, and vice versa. Modems are commonly used to provide internet connectivity over DSL (Digital Subscriber Line) or cable broadband connections.
6. **Firewall**:
    - A firewall is a network security device that monitors and controls incoming and outgoing network traffic based on predetermined security rules. It acts as a barrier between a trusted internal network and untrusted external networks, such as the internet, to prevent unauthorized access and protect against various cyber threats, including malware, viruses, and intrusions.
7. **Proxy Server**:
    - A proxy server is a network device or software application that acts as an intermediary between clients and servers, forwarding client requests to servers and returning responses to clients. Proxy servers can provide various functions, including caching commonly accessed web content to improve performance, filtering and blocking undesirable content, and enhancing security by hiding client IP addresses from external servers.

These are just a few examples of the many types of network devices used in modern computer networks. Each device plays a crucial role in enabling communication, connectivity, and security within and across networks of varying sizes and complexities.


Thank
You