**CS 409**

**Ethical Hacking**

**Homework 2 (30 pts)**

**1. What are the communication identifiers that are used in the Data link layer, Network layer and Transport layer? How does Internet Assigned Numbers Authority (IANA) maintain a list of port number assignments?**

Communication identifiers used in

1. Data Link Layer: MAC Adress

2. Network Layer: IP Adress

3. Transport Layer: Port Number (choose from multiple processes running on the destination host)

**IANA (Internet Assigned Numbers Authority):**

Is the organization who handles all the ports and assigns the ports using some standards. Every protocol has a distinct set of bits and memory. IP4 has 32-bit port number and IP6 has 128-bit port number.

IANA helps in assigning those bits using the standards. The whole address is divided into several sectors to identify the part of the network.

In which we have IP addresses, Host Id, Network Id, Mac addresses and all. Subnet helps in finding Network component and Host part of the address.

We have some well-known ports, Registered ports, and Dynamic Ports.

**2. What is an IP address? Describe the general structure of IP address. How does the IP address divide during subnetting?**

**IP address:**

An Ip address is an internet protocol, which helps us to send or receive data through the internet. It is a unique value given to a system to identify it on the internet while sending or receiving the packets.

It is a 32-bit address with 0 and 1. It is divided into 4 sections with 8-bits each separated by dots. And it looks like below:

10110010.11000011.11100110.10101010

While Ip address subnetting, it is divided into Network Id and Host Id. For example, 1.122.2.1 is the Ip address of system, then 1.122.2 is the Network Id and the last number is Host Id.

So, the first 3 sections of the Ip address are referred as Host Id (Which helps to identify the system on the network), and the last section helps us in identifying the network.

**3. Describe the TCP connection establishment, termination and reset mechanisms.**

TCP (Transfer Control Protocol) connection happens in three-way handshake.

In TCP, the information is initially sent to the network and waits for the acknowledgment.

SYN flag bit x.

The network once validating the connection it will send the acknowledgement (ACK) to the data packet (SYN).

So, the network sends x+ as the ACK packet and y as its SYN packet.

Then the client sends the acknowledgment (ACK) to the network that we can terminate the connection.

That is y+1.

In TCP connection termination, Initially an FIN is sent to server from the client. That the client is done with the connection.

And the server sends the FIN by the acknowledging the client.

And the client responds with ACK packet and states to cut the connection.

For TCP reset mechanism, we use RST packet.

1. SYN packet is sent in the first stage.

2. SYN/ACK is received in the second stage.

3. RST is sent to the server from the client.

**4. Describe the major differences between TCP and UDP. Mention four disadvantages of UDP port scanning.**

Please find the differences along with the advantages and disadvantages discussed in the points.

**TCP (Transfer Control Protocol):**

1. TCP port scan is a connection-oriented scanning, which is a three-way handshake. So, the scanning was fast in TCP port scan.
2. TCP arranges the packets. So, while receiving the packets in the same order.
3. TCP needs to have 3 packets to establish a socket connection before even sending the data.
4. TCP has many error checks while sending and receiving the data through the network.

**UDP (User Datagram Protocol):**

1. UDP port scan is a connectionless port scan, so it takes lot of time to scan the system or network.
2. In UDP as do not have connection, so the packets will be received randomly.
3. In UDP we do not need any packets to ACK, SYN or order the messages.
4. UDP does not have any error checks for the data sent through the connections.

**5. Explain the stages of a hacking cyber-operation in your own language.**

Hacking can be done in 5 stages.

Initially stage of hacking is like Reconnaissance, where we look for some details about the network like finding the Ip address of the system and any open port numbers.

Reconnaissance have 2 types active and passive Reconnaissance. Active Reconnaissance in which we close all the traces of the hack and in passive Reconnaissance we do not bother much about the traces.

Once, Hacker gets the details of the systems. Hackers start scanning to find the vulnerabilities present in the system.

Gaining Access: After finding the weak points and vulnerabilities in the network. Hackers start finding access to the weak points in the network.

Maintain Access: Hackers start to maintain access by implanting bugs or malware into the system.

Covering Tracks: Once, he is done with all the process and getting what needs to be attained. A hacker covers all the tracks implanted by him while doing the process.

**6. What is port scanning? Mention** **distinct types of port scanning techniques with their advantages and disadvantages.**

Port scanning is a technique used frequently by hackers to find weak points and open doors in a network.

So, depending on the reaction from the network, the hacker sends some signals to the network. A hacker can identify some weaknesses or potential network access points, which allows them to get access to the system.

TCP Half Open:

$nmap –sS <traget\_host> is the command used to find the vulnerable ports.

TCP half open scan is the simplest port scanning technique.

In TCP half open scan the information is initially sent to the network and waits for the acknowledgment.

The network once validating the connection it will send the acknowledgement (ACK) to the data packet (SYN).

Then the client sending the acknowledgment (ACK) to the service port stage is missing in the TCP half open scan.

Ping scans: One of the easiest port scanning methods is the ping scan. They are also known as ICMP (Internet Control Message Protocol) requests, which are used to identify problems with networks.

Ping scans conduct many ICMP requests to numerous servers throughout the network in search of any responses.

A ping scan might be compared to the administrator blocking and deactivating the firewalls to investigate problems.

Ping scan will help ICMP, which is used to discover network problems, but we also leave traces that hackers might use to conduct malicious actions on the network.