Name: Syeda Nowshin Ibnat

ID: 17183103020

Intake: 39 Section: 02

Dept. Of CSE, BUBT

Semester: Fall 2021-2022

Home Work-4

1 NO Q Ans

Soln: Analyzing the above situation we can say that port scanning is the solution of this problem. A port scan is a method for determining which ports on a network are open. A port scan sends a carefully prepared packet to each destination ~~port~~ port number. Some commonly used port scanning softwares are: Vanilla, SYN Scan etc.

Port scan results reveal the status of the network and can be decribed in three categories:-

① Open ports:	② Closed Ports:	③ Filtered Ports:
It indicate that the target server on network is actively accepting connections on listening.	It indicate that server on network received the request, but there is no service "listening" on that port.	It indicate that a request packet was sent, but ~~host~~ the host did not respond and is not listening.

Some port scanning techniques:

1. Ping Scan: ~~Thi~~ The simplest scan. It looks for any ICMP replies indicating if a target is alive.

2. TCP Half Open: This common scan that requests an Ack packet from a computer.

3. TCP connect: It is similar to TCP Half Open Scan, but the TCP connect scan completes the TCP connection.

4. UDP: It is slower than TCP scan. but it works best when we send a specific payload to a target, such as DNA request.

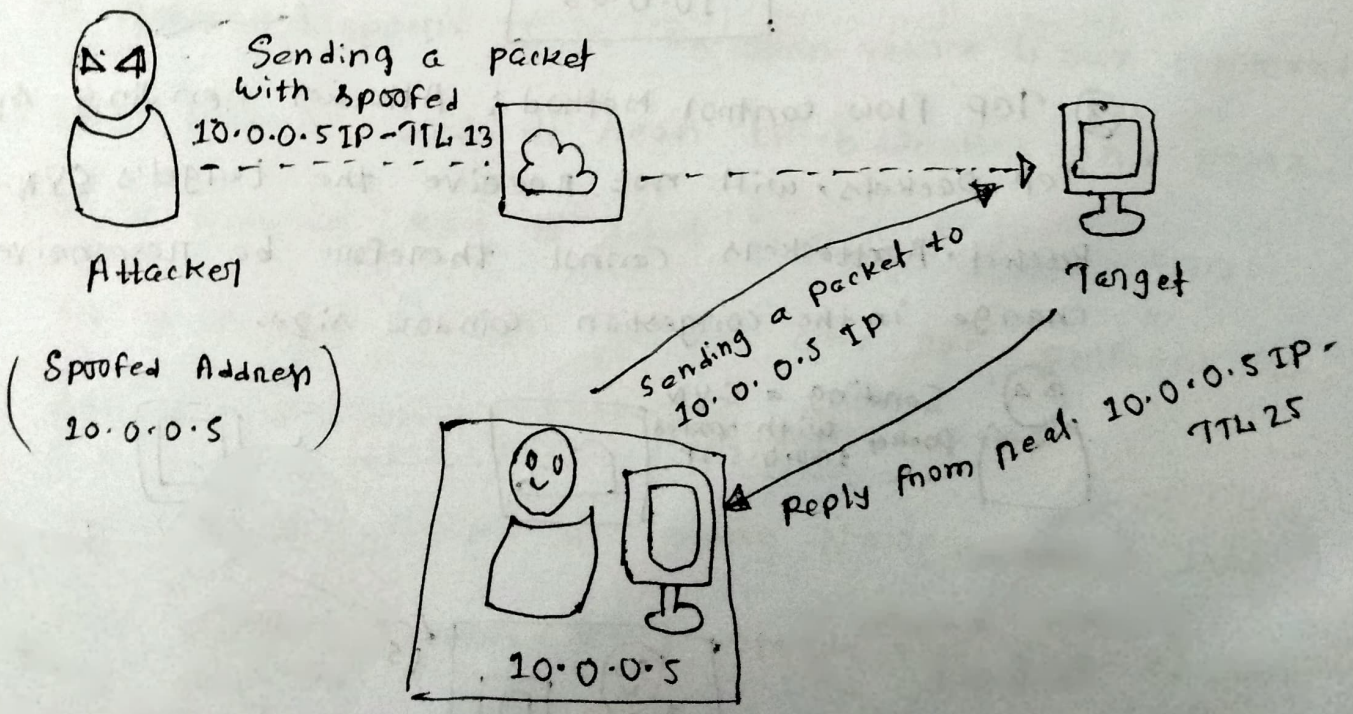
5. Stealth scanning: ~~St~~ ~~Quit~~ Quiet and unobvious, stealth scanning is commonly used by hackers for this reason.

2 No Q Ans

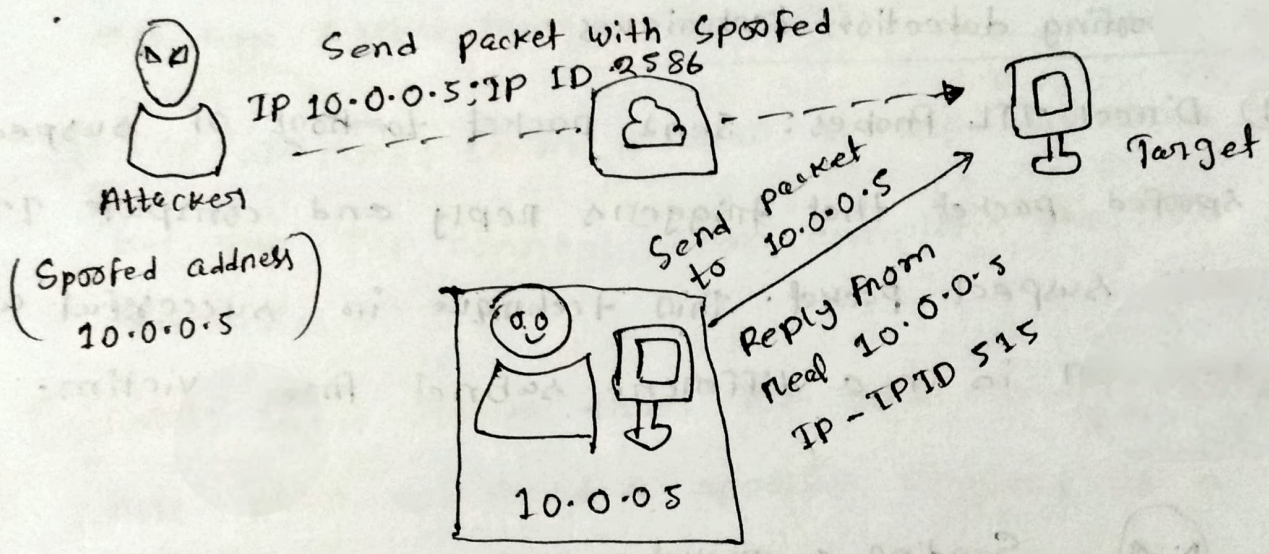
Soln: IP spoofing refers to changing so that the attack appears to come from someone else. When the victim replies to the address, it goes back to the spoofed address and not to the attacker's real address.

IP spoofing detection techniques:

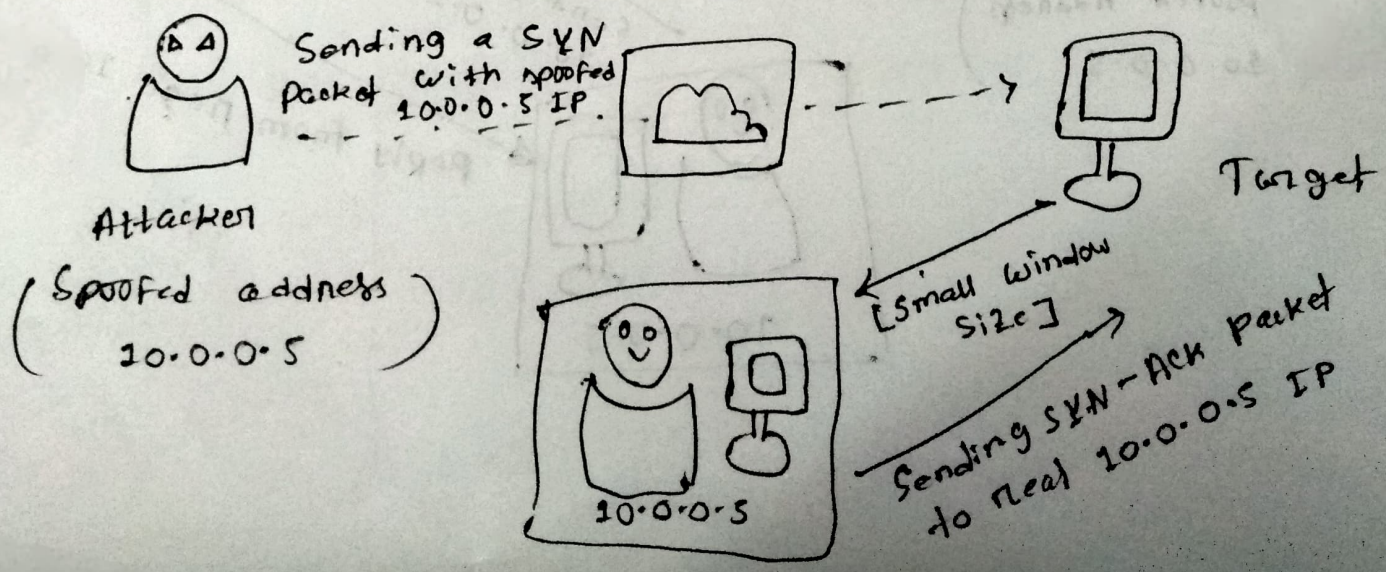
1. Direct TTL Probes: Send packet to host of suspect spoofed packet that triggers reply and compare TTL with suspect packet. This technique is successful when attacker is in a different subnet from victim.



2. IP Identification Number: Send probe to host of suspect traffic that triggers reply an compare IP ID with suspect traffic. This technique is successful even if the attacker is in the same subnet.



3. TCP Flow control Method: Attacker sending spoofed TCP packets, will not receive the target's SYN-ACK packet. Attackers cannot therefore be responsive to change in the congestion window size.



3 NO Q Ans

Soln: With the growing ~~digitalizat~~ digitization, internet crimes are also increasing at a faster speed. cybercrime is defined as a crime that is committed using a network-connected device such as a computer or a mobile phone. To get rid of cybercrime vulnerability scanning is needed. Vulnerability scanning, ~~als~~ also commonly known as "Vuln scan", is an automated process of proactively identifying network, application and security vulnerabilities. Nmap is a vulnerability scanning tool. ~~Namp~~ Nmap is short for ~~Network~~ Network Mapper. It is an open-source Linux command tool that is used to scan IP addresses and ports in a network and to detect installed applications.

As a digital forensic expert, one can perform the system vulnerability scanning with Nmap:-

Nmap (NSE) script is among Nmap's most used and powerful features, & NSE stands for Nmap Scripting Engine.

Some examples of N-map default script:

1. Nmap Vulnerability Scan using the nmap Vuln script:

```
nmap --script vuln <IP Address>
```

2. Nmap Vulnerability Scan SMB:

```
sudo nmap --script = smb-vuln-ms17-010
                     <IP Address>
```

3. Nmap Vulnerability Scan FTP Backdoor:

```
sudo nmap --script = ftp-vsftpd-backdoor -p 21
                     <IP address>
```

4. Brute Force SSH Password Using Nmap Script:

Using this Nmap Script, we can brute force the SSh password, an example;

```
nmap --script ssh-brute -p22 <IP address>
 --script-args userdb = user.txt, passdb = pass.txt
```

4 NO Q Ans

Soln: Cybercrime is any criminal activity that involves a computer, networked device or a network.

Cybercrimes can generally be divided into two categories:

Crimes that target networks or devices	Crimes using devices to participate in criminal activities
Viruses	Phishing Emails
Malware	Cyberstalking
DoS Attacks	Identity Theft

Cyber ~~at~~ crimes targets both individuals and organizations.

Some cybercrime against organizations ~~are~~ can be:

(1) Unauthorized Accessing of computer.

(2) Denial of ~~se~~ service.

(3) Virus attack.

(4) Email bombing.

(5) Trojan Horse, etc.

Effective cybercrime investigations are usually undertaken using best practice ~~approa~~ approaches such as evidence-based policing.

Port scanning countermeasures:-

(1) configure firewall and IDs rules to detect and block probes.

(2) Run port scanning tools against hosts to determine whether the firewall properly detects the port scan scanning activity.

(3) Ensure that the router, IDs and firewall fireware are updated to their latest releases.

(4) Use a custom rule set to lock down the network and block unwanted ports.

(5) Perform Tcp and UDP scanning to check the network configuration and its available ports.

(6) Ensure that the anti scanning and anti spoofing rules are configured.

Ans: