Computer networking II. COMM.NET.400
Reyver Serna (K412764)
reyverarley.sernalerma@tuni.fi

Assignment 1. Network Security

1) What is the difference between a port scan and port sweep?

Portscan sends client request to a range of server port addresses on a host. This aims to find an active port and the services available on a remote device. On the contrary, portsweep scans different host for a specific service in a specific listening port.

2) TCP scanning

The goal of this type of portscanning is to check if the TCP port on the target host is closed or open. This is done by sending TCP SYNC packets to the host's open ports. If it is open, the hosts will reply with a TCP SYN-ACK packet. When it is closed, it will answer with a TCP RST packet. In a stateful firewall, The TCP scanning packets can block these types of packets, if they come from unknown sources. The socket used for this type of scanning is the TCP socket, which is the only one capable of sending and receiving TCP packets.

3) SYN scanning

A more secretive version of TCP scanning. The implementation is similar to the TCP scanning, however, the SYN packets are sent to the target host's open ports do not wait for a response. Instead, it immediately sends TCP RST. These types of packets can be blocked by stateful firewalls if it is sent from an unknown source. However, stateless could also block UDP packets if it is configured to do it. A TCP socket is used to handle the SYN scanning because it involves sending and receiving TCP packets.

4) UDP scanning

To check if the UDP port on a host is open. This is done by retransmitting UDP packets to the port and observe the responses. If it is open the host will respond with an UDP packet. On the contrary, the port will respond with a ICMP message. A stateful firewall can block UDP scanning, although stateless could also block UDP packets if it is configured to do it. Socket used: UDP socket.

5) ACK scanning

The goal of ACK scanning is to determine if a port is filtered or unfiltered. These packets are intended for probing if there is a firewall and its rulesets. The working of this scanning lies on filtering ACK packet bits. It is detected by stateless firewalls.

6) FIN scanning

Different to ACK scanning, FIN scanning is technique used for identifying open ports on a target host. It works by sending TCP packets with the FIN flag set. If these end up in a

closed packet, the system replies with a TCP RST packet. Stateful firewalls can block FIN scanning packets.

7) Chapter 8 of the course book introduces the SCTP protocol. It replaces TCP's three-way handshake with a four-way handshake. It is related to one of the above mentioned port scanning types. Which one and what its idea is?

It is related to UDP or TCP scanning. SCTP aims to identify listening ports on a host by sending packets to several ports and checking their responses. Concretely, SCTP INIT packets are sent to the port. If the response is open, there won't be any response back. On the contrary, if it is closed, the port will answer with a SCTP error message.

8) Define a Snort rule that alerts of a possible UDP scanning. Your network is 193.120.20.0/24.

The snort rule is:
alert udp $EXTERNAL_NET any -> 193.120.20.0/24. (msg: "Possible UDP Scanning Detected"; sid:1000001;)

9) Define a Snort rule that alerts you if Snort suspects that your network (193.120.20.0/24) is the target of port scanning. The network is interpreted as being scanned if there are TCP connection requests to more than 10 different ports in five seconds. In this case, the alert is written to the alert/portscans.log file.

alert tcp 193.120.20.0/24 any -> $HOME_NET any (msg:"Potential Port Scanning Detected"; flow:to_server,established; detection_filter:track by_src, count 10, seconds 5; threshold:type limit, track by_src, count 1, seconds 5; sid:1000002; logto:"alert/portscans.log";)

10) In practice, the home network very rarely receives service requests for UDP ports that are not open, that is, they do not provide any UDP service. So, for UDP scanning, prevent the ICMP port unreachable messages to be sent from your home network to the public network.

/ip firewall filter

add chain=forward action=drop protocol=icmp icmp-options=3:3 comment="Drop ICMP Port Unreachable from Home Network"

11) Non-server machines are rarely the targets of TCP connection requests. Admittedly, such services can sometimes be. For Syn scanning, block requests to open TCP connections from the public network to the home network if there are more than 5 per minute. However, this restriction does not apply to TCP connection requests to Server 193.120.20.10.

/ip firewall filter
add chain=input action=accept protocol=tcp dst-address=193.120.20.10 comment="Allow TCP to Server"

```
add chain=input action=drop protocol=tcp connection-state=new src-
address=193.120.20.0/24 \
   dst-address=!193.120.20.10 limit=5,minute comment="Drop TCP connections exceeding
limit to Home Network"
```