Quiz 3

CSE-644 INTERNET SECURITY

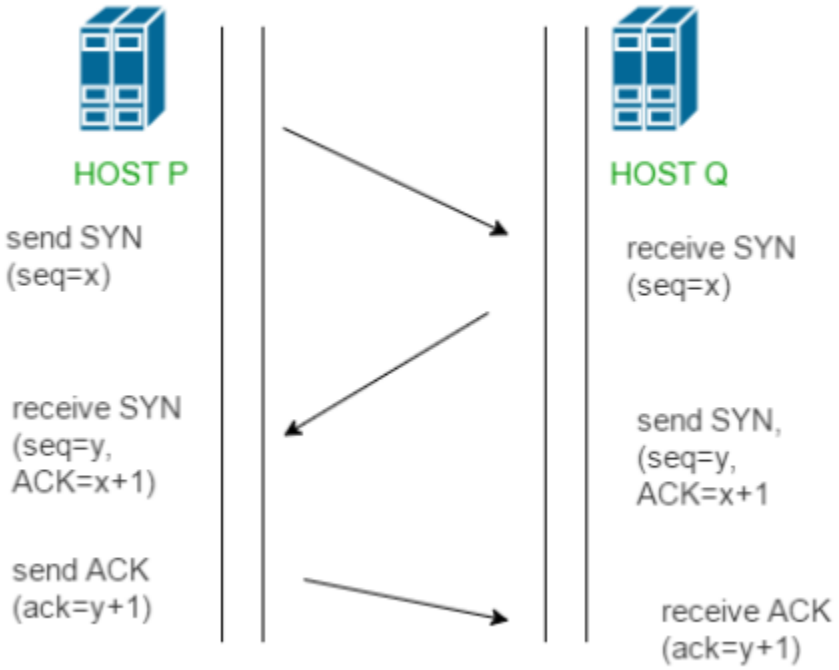
DR. SYED SHAZLI

2/12/2023

Anthony Redamonti
SYRACUSE UNIVERSITY

1) What is TCP three-way handshaking? What is the reason for that?

The three-way handshake is used to establish a TCP connection between the client and server. First, the SYN message (SYN bit is set) is sent from the client to the server with an initial sequence number "X". The server will reply with an ACK message (ACK and SYN bits are set) containing a sequence number "Y" and acknowledge number X+1. Lastly, the client will respond by sending an ACK message with an acknowledge number Y+1.



There is a half-open connection queue on the server side, which contains all the half-open connections. There is also a connection queue which stores information relating to established TCP connections.

The TCP three-way handshake ensures that the client machine is following the proper TCP protocol when it attempts to establish a connection. The mechanism prevents connections from being established with only one SYN message.

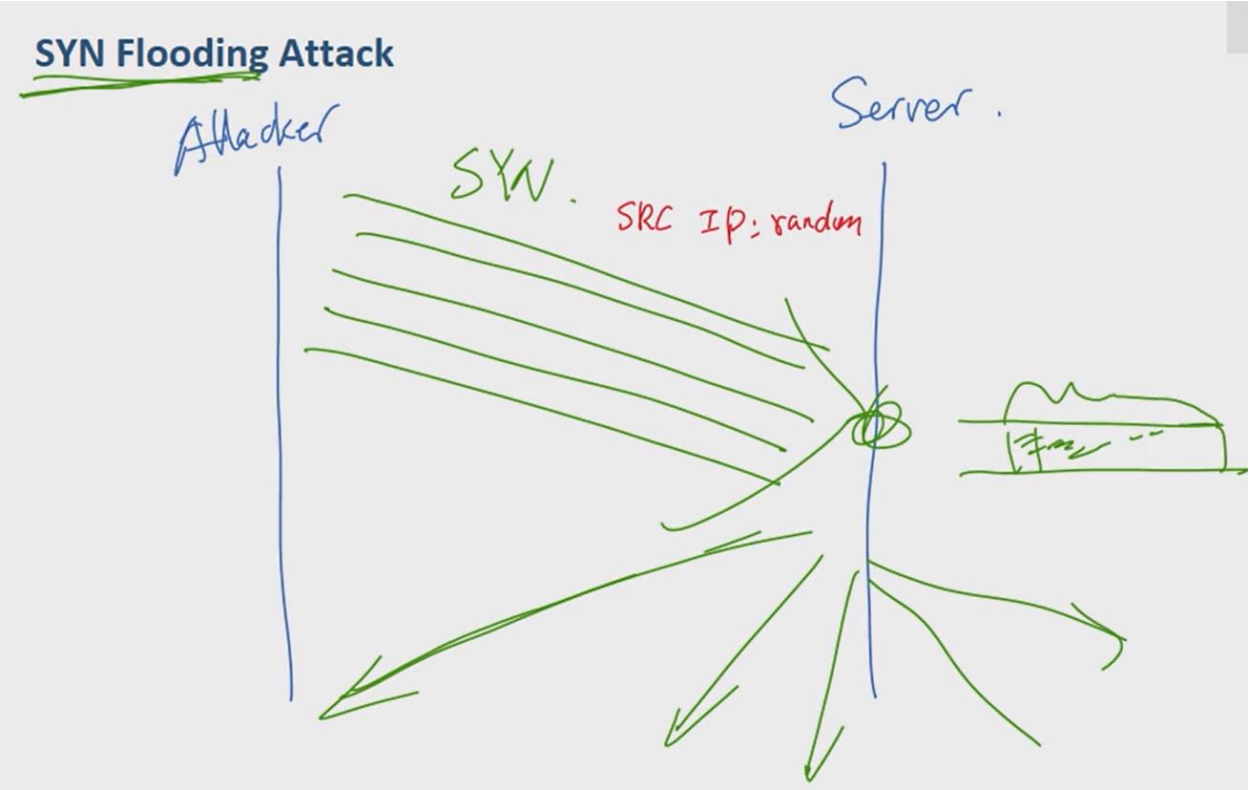
2) What is the sequence number in TCP header?

The 32-bit sequence number is part of the TCP header. Every octet in the data stream has a unique sequence number. It keeps track of how much data has been sent.

3) What is SYN flood attack? (can use diagram to answer if you need). Will the resource of the victim machine all run out? Why and why not?

The SYN flooding attack is when an attacker sends many spoofed SYN messages to the server. The spoofed SYN messages may have random source IP's or a fake source IP belonging to another machine. The server will send messages back to the fake source IP with ACK messages. The fake source IP will not complete the three-way handshake because it did not initiate the handshake process.

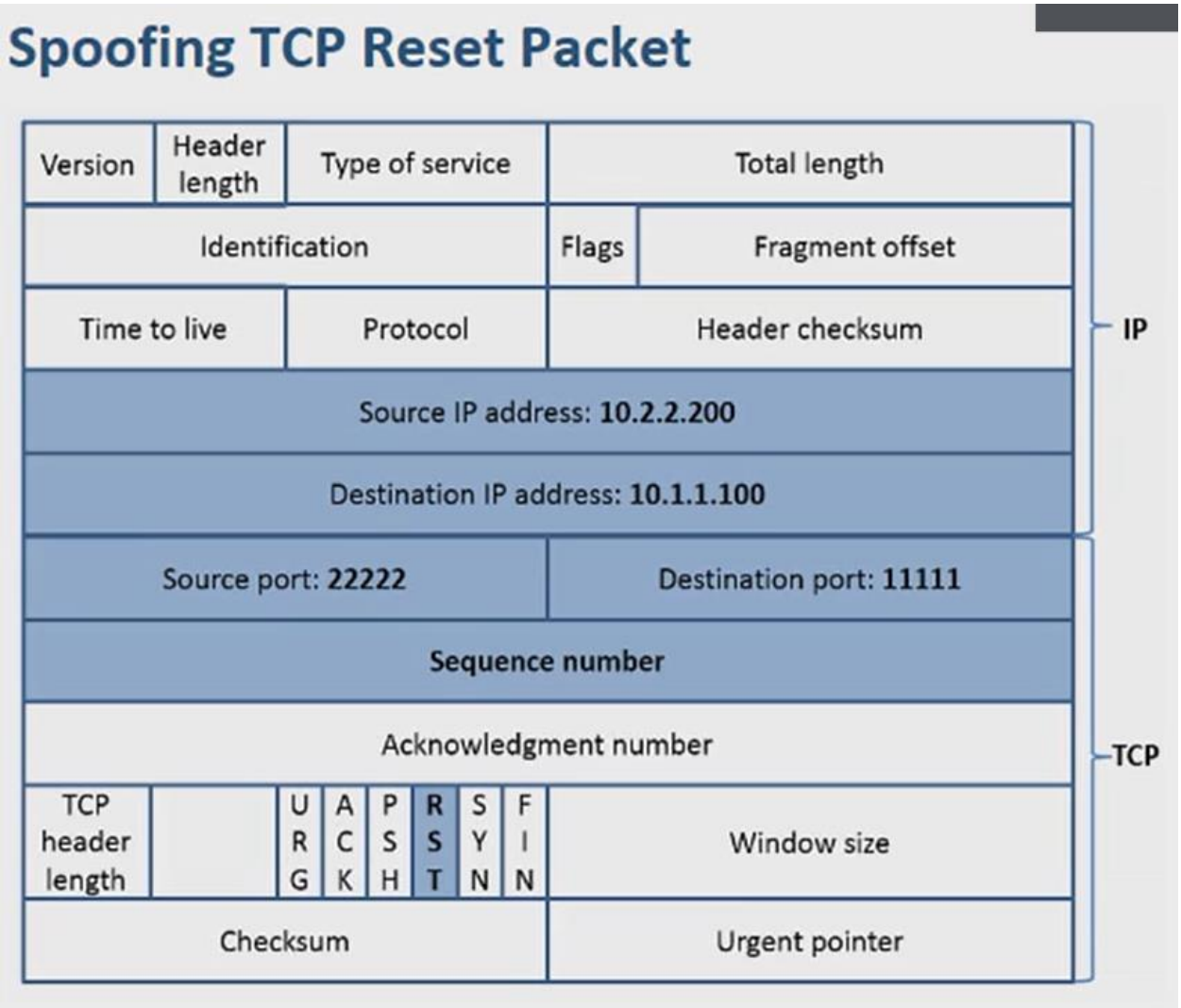
The only resource of the victim machine that will be exhausted by the attack is the half-open connection queue. When the half-open connection queue is full, the victim machine can no longer accept any incoming TCP connection requests. However, many operating systems use cookies that protect against these types of attacks.



4) What is TCP Reset Attacks? How does it work? What are those important areas of your Reset packet need to be very careful about?

A TCP reset attack is when the attacker spoofs a message from the client machine to the server with the RST bit set, signifying a reset command. The reset command has no payload and is used to end an established TCP connection during an emergency. Using the reset command is not the typical method of closing a TCP connection.

The important areas of the packet that the attacker must replicate are the source/destination IP addresses, sequence number, and source/destination port numbers in use. The source and destination IP addresses and port numbers must match the client/server IP addresses and port numbers in use. The sequence number must match the sequence number in the last packet sent between the client and server to be treated as a valid reset command (not dropped).



5) What is TCP session hijacking? What is the purpose of "\n" in front of your commands and at the end of your commands when you use "netwox"?

TCP session hijacking is used to hijack an existing TCP connection (telnet connection, for example). The attacker injects a command into the TCP stream, mimicking one of the two machines. The important data to replicate in the spoofed packet is the source and destination IP addresses, destination and source port numbers, and sequence number in use.

After the attack takes place, the sequence number is incremented by one of the machines. The other machine is therefore using an invalid sequence number, so all future attempts at communication fail (all TCP packets will be dropped due to invalid sequence number). The attacker knows the valid sequence number, so it can continue the conversation on behalf of the victim machine.

The purpose of the return character (\n) in the front and back of the injected command is so the injected command is treated as a new command and is not appended to the end of an existing command.