quiz Student name: Kevin Martin

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

In order to establish a TCP connection, the three way handshake protocol must be followed. The first packet sent by the client to the server is a special packet, the SYN packet, which stands for Synchronization. Within that packet lies the Initial Sequence number. Next, the server will acknowledge this request by sending back the ACK package. This contains the Initial sequence number plus 1. This also tells the client the server's Initial sequence number (SYN). Finally, the client will send back the server's Initial sequence number plus 1, in the form of the client's ACK package.

This is done to establish a secure TCP connection.

2) What is the sequence number in TCP header?

The sequence number in the TCP header is the index for every single octet in the buffer. This will maintain the correct order of the data to be processed.

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 attacker floods the server with many SYN packets (the initial conatct for a TCP connection). The server will automatically reply even though the attacker has no intention of replying again (which would establish a three way handshake). The attacker will also use multiple IP addresses to avoid blacklisting.

The attack does not necessarily consume all of the memory of the server, but only the memory that is reserved for the buffer. The server could have lots and lots of memory, but has an "Achille's Heel" for smaller amounts allocated to the buffer only. That is the resource that will run out after enough SYN flooding packets.

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?

An attacker spoofs a reset packet from the server to the client, which causes the client to immediately terminate the connection to the server. This attack is launched unbeknownst to the server, because the attacker intercepts the transmission from the client without the server knowing.

This works because the reset packet forces the receiver to automatically drop the connection as soon as it is received.

The important areas of the reset packet are the source IP address (now spoofed from the attacker), destination IP address, source port, destination port, sequence number, and of course the reset bit (indicating this is a reset packet).

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 injecting malicious code, such as a command to remove a file directory, into the connection between two machines. The attack targets one of the machines and forces the execution of the code.

The purpose of “\n” in front and at the end of the commands is to prevent the command from being obscured by the client. For example if the user enters a series of characters that would negate the malicoius command, the newline forces a break from the user-entered characters and solely executes the malicious command, thus ensuring its effectiveness.

6) How to achieve TCP session hijacking?

To achieve TCP session hijacking, a reverse shell must be created. This enables the attacker to get full control of the server. To do this, several pieces must be put in place. First, the redirection of the server’s shell to the attacker (via /dev/tcp/ip address). Next, the input needs to be redirected from the server to the attacker (via 2>&1). Finally, the output also needs to be sent to the attacker (via 0<&1). If all these parts are in place, the attacker will have successfully hijacked the session.