1. netwox 76 -i 10.0.0.3 -p 80

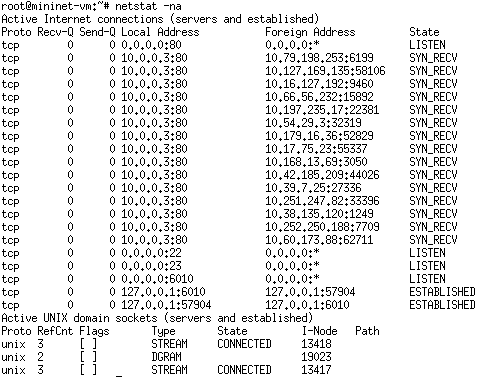


Figure 1 Half-open TCP ports from SYN FLood Attack

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.

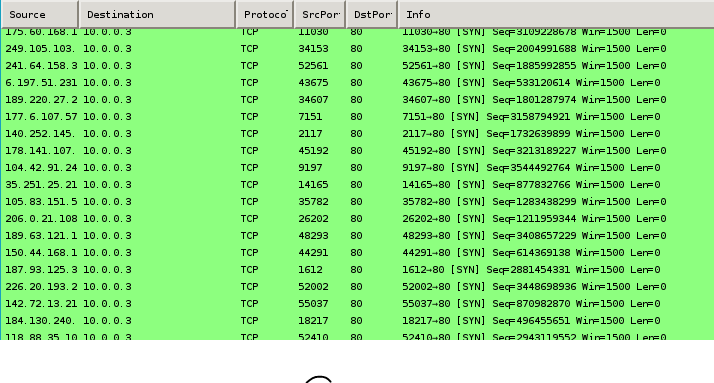


Figure 2 DoS Attack SYN packets to vic

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.

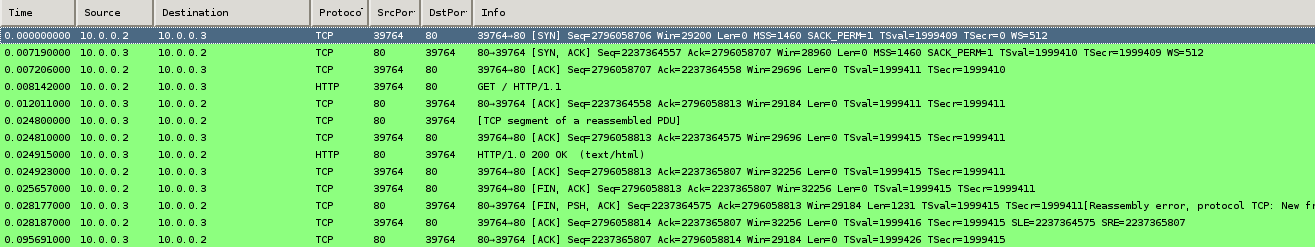


Figure 3 HTTP Connection with DoS Attack

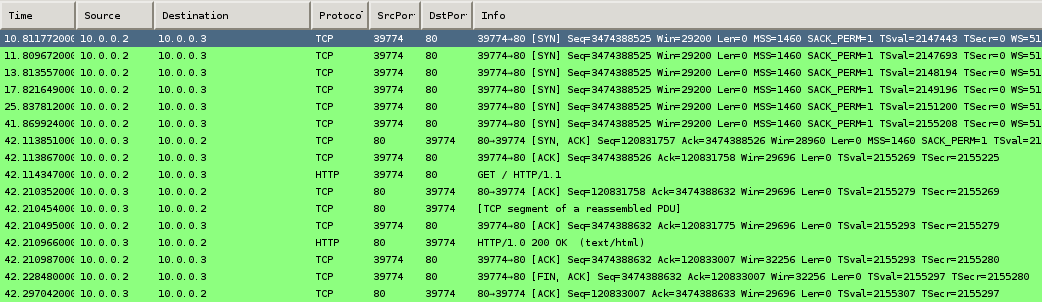


Figure 4 HTTP Connection with DoS Attack

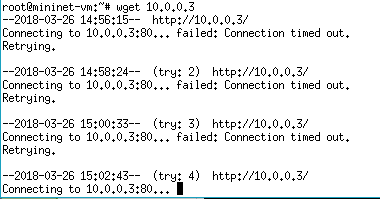


Figure 5 leg fails to connect to vic during DoS Attack

* Telnet:

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

telnet 10.0.0.3 -l mininet

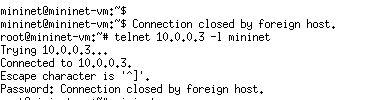


In the att terminal, run an RST attack on port 23 of vic:

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



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



* SSH:

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

ssh mininet@10.0.0.3

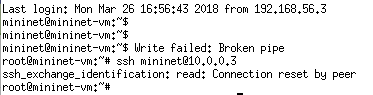


In the att terminal, run an RST attack on port 22 of vic:

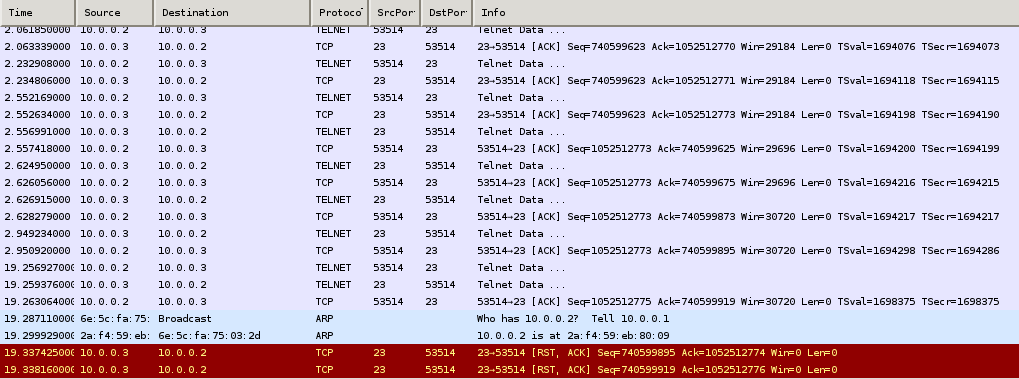
netwox 78 --device “att-eth0” --filter “dst host 10.0.0.3 and dst port 22”



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



* Telnet:



* SSH:



1. ???
2. ???