Luke Evans

February 14, 2021

Lab 3 – TCP/IP Attacks

**Attacker IP = 10.0.2.15**

**Victim IP = 10.0.2.4**

**Server = 10.0.2.5**

* 1. *SYN Flooding Attack*

We check the size of the half open connection queue on our victim machine in the screenshot below:

Text

Description automatically generated

We can check the half open connections using the command nestat -at, shown in the screenshot below:

A picture containing table

Description automatically generated

Next we will launch the attack from our attacking VM:

Text

Description automatically generated with low confidence

We can again run the netstat -at command to view the states of the connections while the attack is being launched:

Text

Description automatically generated

TCP syn cookies was enabled on our victim machine by default so for example purposes we first turn it off.

Graphical user interface, text

Description automatically generated with medium confidence

We then try to telnet to the machine from our server computer and are unable to connect because the half open connection queue is full and no other connection to port 23 can be made:

Graphical user interface, text

Description automatically generated

Next, we turn tcp syn cookies back on on our victim machine:

Text

Description automatically generated with medium confidence

Then we try to telnet to the victim machine again from the server and we are able to make a connection:

Text

Description automatically generated

Observations: The screenshots above show an example of a SYN flood attack. We used the netwox tool to send many TCP SYN packets from spoofed source IP addresses which causes the victim machines half open connection queue to fill up. We target port 23 specifically so when we try to telnet to the victim machine from our server machine it does not work because the victim machine is no longer able to accept any other connections and we disabled the tcp syn cookie counter measure. When we reenable the tcp syn cookie counter measure, we can then make a telnet connection from our server VM to our victim VM even though our attacker is flooding the victim with TCP SYN packets.

Explanation: The TCP SYN flooding attack targets the bottle neck in the three way handshake. By filling the half open connection queue for a specific port, the victim machine will no longer be able to accept any other connections to that port number even though the machine has plenty of computing resources available. When the TCP SYN cookie counter measure is enabled our attack is unsuccessful because once the half open connection queue fills up, the victim machines OS will automatically start attaching tcp session cookies to the syn ack request and will no longer buffer the half open connections. Then when the victim machine receives an ACK packet it can check the SYN cookie to verify if it is a valid connection request before establishing a TCP session.

*2.1 TCP Reset Attacks on Telnet and SSH*