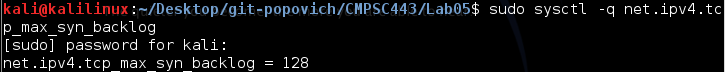
**TCP/IP Attack Lab:**

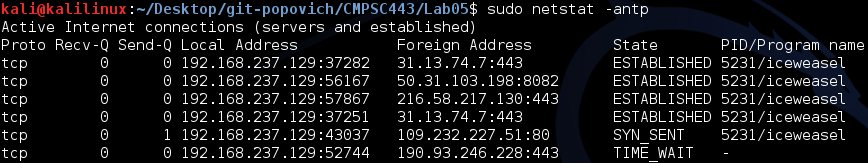
This lab begins with explaining a SYN (synchronize) flooding attack. This is a limitation of the TCP/IP protocol. It happens whenever a server receives many SYN requests, acknowledges them, but never receives an acknowledgement back. Because of this, the server’s queue grows until it cannot take any more connections.

Using the command ‘sysctl –q net.ipv4.tcp\_max\_syn\_backlog’, we can view the system queue size. An example of this is below in figure 1.



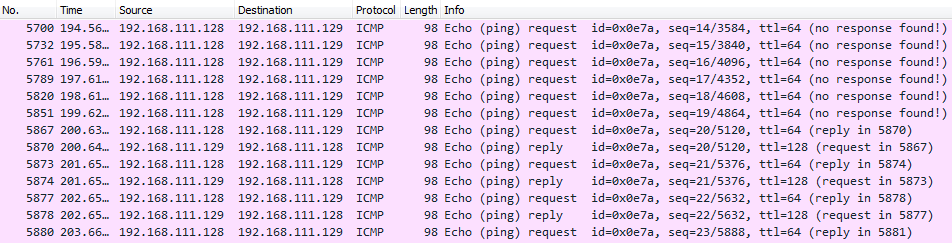
**Figure 1:** System TCP queue size

We can also view the number of half opened connections associated with the listening port by running the command ‘netstat –antp’. Figure 2 shows the current connections open on my virtual machine. If the 3-way handshake is finished, their state will be ‘ESTABLISHED’. If we are waiting on an ACK, their state will be ‘SYN-RECV’.



**Figure 2:** Opened connections

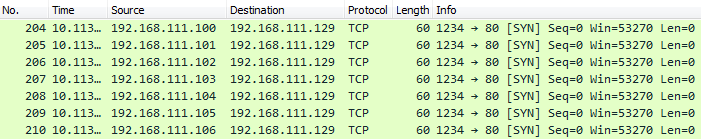
Next, we are instructed to write a SYN-flood program in python with the help of <http://www.binarytides.com/python-syn-flood-program-raw-sockets-linux/>. The target of this attack will be Ollydbg - a Windows 7 virtual machine running on my computer. The source will be a Kali Linux virtual machine also running on my computer. The first thing I did was to test that I could ping between the two virtual machines. I could ping from Windows to Kali, but not from Kali to Windows. However, as soon as I turned off Windows Firewall the pings began to go through. A screenshot of this activity via Wireshark is below in Figure 3.



**Figure 3:** Windows Firewall blocking ping requests (up to packet 5891)

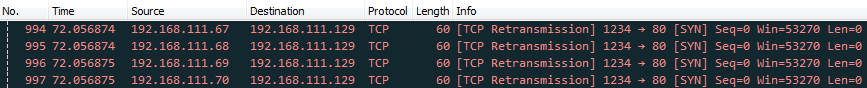
With communication between the two virtual machines, the lab can now continue. I ran the SYN flood script from Kali Linux directed towards the Windows VM. I viewed the active connections on the Windows VM by running ‘netstat –an 1’ which refreshes the command every second. The open connection did not show up.

However, I viewed the packets being sent in Wireshark and figure 4 shows that the SYN flood is occurring over multiple IP addresses, as desired.



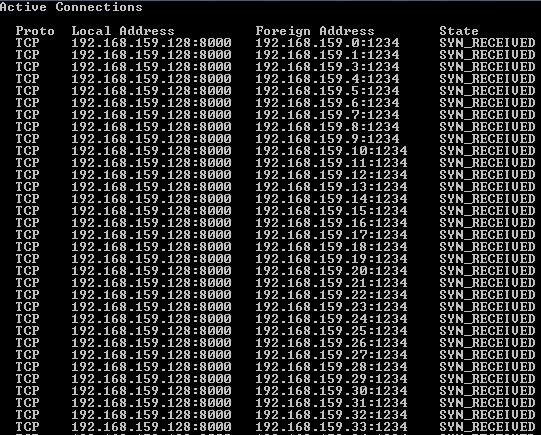
**Figure 4:** Successful SYN flood from Kali Linux VM to Windows 7 VM

Also to note, figure 5 shows that after a few SYN floods, the packets begin to be flagged by Wireshark as “TCP Retransmission” packets.



**Figure 5:** Multiple SYN floods begin to be flagged as “TCP Retransmission” packets

After receiving more info during lab, it was suggested to run a simple python server with the command “python –m SimpleHTTPServer”. I began the server on the Windows VM, it runs on port 8000. The script was then modified to be directed to that port. Running “netstat –n 1” on the Windows VM shows that the attack was successful! As figure 5 shows, there are now many connections to the Windows VM and all of them are at the “SYN\_RECEIVED” state waiting for an ACK.



**Figure 5:** Successful SYN flood to the Python server on the Windows VM

However, even during the flood the Windows VM can still browse the internet. Interesting to note that after about 18 seconds, the SYN\_RECEIVED connections are dropped.