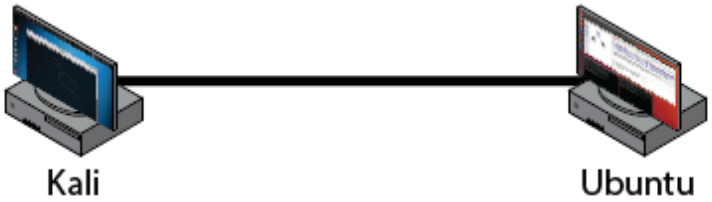
SIT716 Computer Networks and Security

Week 4: TCP SYN Flood

Below you will find instructions for conducting an experiment designed to explore concepts of networking and/or security. Before referring to the instructions below, make sure you take the time to research and design your own experiment – even if you can't work out everything that is required. After completing your study of this unit, the skills you develop in designing your own experiments will be a critical skill for learning about new network protocols and security attacks, enabling you to work successfully as a valued professional in these fields.



Host	IP Address	Role
Ubuntu	192.168.1.1/24	Victim machine
Kali	192.168.1.2/24	Attacker that will perform a TCP SYN Flood

Outline:

In this lab we will using Kali to execute a TCP SYN Flood attack against our Ubuntu VM. TCP connections are initiated by the requester sending a TCP segment with the SYN flag attached. This is usually followed by the remaining two segments in the TCP three-way handshake, however in a SYN Flood the attacker ignores any SYN-ACK responses, leaving the receiver with a partially opened connection. Each device usually only has a limited capacity to process incoming requests, and so the resources reserved for handling new connections are quickly exhausted, denying legitimate connection requests from other hosts (a denial of service attack).

There are several tools available that can allow us to perform a SYN Flood attack, however our focus will be on hping3 and Metasploit, both of which are available within Kali.

Instructions:

1. Load VirtualBox, Ubuntu, and Kali as required.
2. Confirm that they Ubuntu and Kali are isolated to the internal network and are connected together correctly by performing a simple `ping` against each other. If this does not work, go back to the Connecting Ubuntu and Kali screencast before continuing.

Using hping3 to perform a SYN Flood attack

1. Within Ubuntu, start Wireshark to monitor traffic it receives.
2. Have Kali send a ping to Ubuntu. Ensure that the traffic is detected by Wireshark in Ubuntu. To ping, open a terminal in Kali, and enter the following command:

```
ping 192.168.1.1
```

3. Within Ubuntu, open the System Monitor (in bottom-left, press 'Show Applications', and search). This will give a real-time view of the CPU and memory being used by the instance.
4. Within Kali, open a terminal window. We will use hping3 to launch a SYN flood attack against Ubuntu. Enter in the commands below to start a SYN flood attack with hping3:

```
hping3 -c 10000 -S 192.168.1.1 --flood
```

5. Monitor on Ubuntu the traffic coming in Wireshark. You should see a huge amount of packets being detected, and in the System Monitor there should be a large increase in CPU and memory usage. Remember not to leave the SYN flood attack running for too long as it will consume your computer's resources. Remember: to cancel a command press Ctrl + C. Don't let the flood run for too long else you may crash the Ubuntu instance or your host PC.
6. hping3 has many parameters that can be set for configuring the attack:

```
-c: number of packets to send
d: size of the each packet to send (e.g. 100)
-S: the type of packets you are sending, in this can SYN packets
-p: port (defaults to port 80)
--flood: sends packets continuously and as fast as possible
--rand-source: spoofs the IP of the sender (highly recommend giving this
parameter a try, and analysing the packets received in Wireshark)
```

   Experiment with these parameters and determine differences in the affects on the Ubuntu victim.
7. When you are finished, cancel any running commands (Ctrl + c), close all terminals, and close Wireshark. Ensure that it is all reset before continuing with the Metasploit instructions below.

Using Metasploit to perform a SYN Flood attack

1. Within Ubuntu, start Wireshark to monitor traffic it receives.
2. Have Kali send a ping to Ubuntu. Ensure that the traffic is detected by Wireshark in Ubuntu. To ping, open a terminal in Kali, and enter the following command:

```
ping 192.168.1.1
```

3. Within Ubuntu, open the System Monitor (in bottom-left, press 'Show Applications', and search). This will give a real-time view of the CPU and memory being used by the instance.
4. Within Kali, open a terminal window. We will use Metasploit to perform our attack. Enter in the commands below to start Metasploit:

```
service postgresql start

msfdb

msfconsole
```

5. To search for the right tool that we are after (as Metasploit has 1000+ included), run the following command:

```
search synflood
```

6. "auxiliary/dos/tcp/synflood" was returned in our search. This is the tool (and the path where it exists) that allows us to do a SYN flood attack. To execute the tool and perform a SYN flood attack, enter in the command:

```
use auxiliary/dos/tcp/synflood

show options
```

7. The command "show options" brings up the parameters that can be set with the synflood tool. We need to set the RHOST (which is the remote host we plan to attack, in our case Ubuntu). Do so with the command:

```
set RHOST 192.168.1.1
```

8. Execute the synflood tool to begin the attack:

```
exploit
```

9. Return to Ubuntu. Monitor the activity on Wireshark and the System Monitor as Ubuntu receives the large volume of packets. Remember to cancel the attack with Ctrl + C in the terminal where Metasploit was executed (do not let it run for too long).