IP configuration

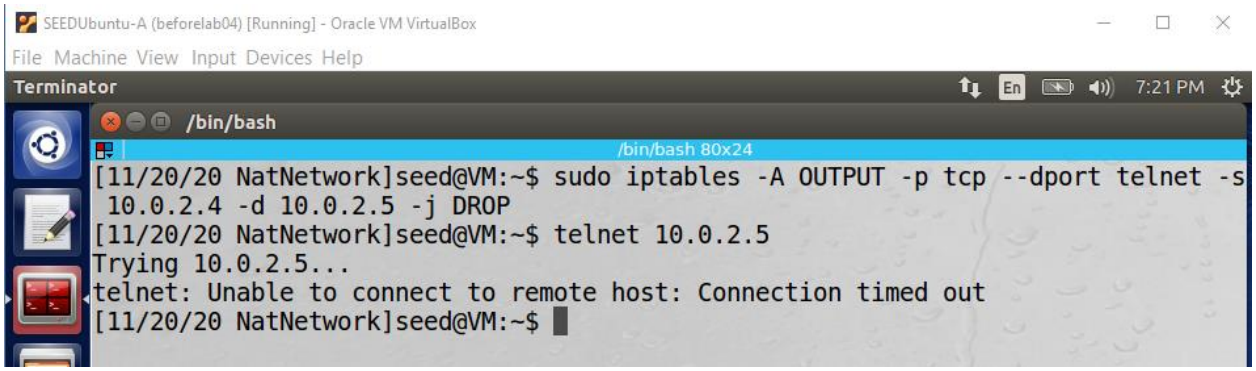
A : 10.0.2.4

B : 10.0.2.5

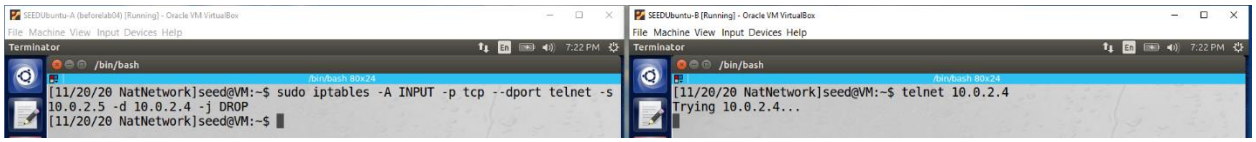
C : 10.0.2.6

2.1 Task 1: Using Firewall

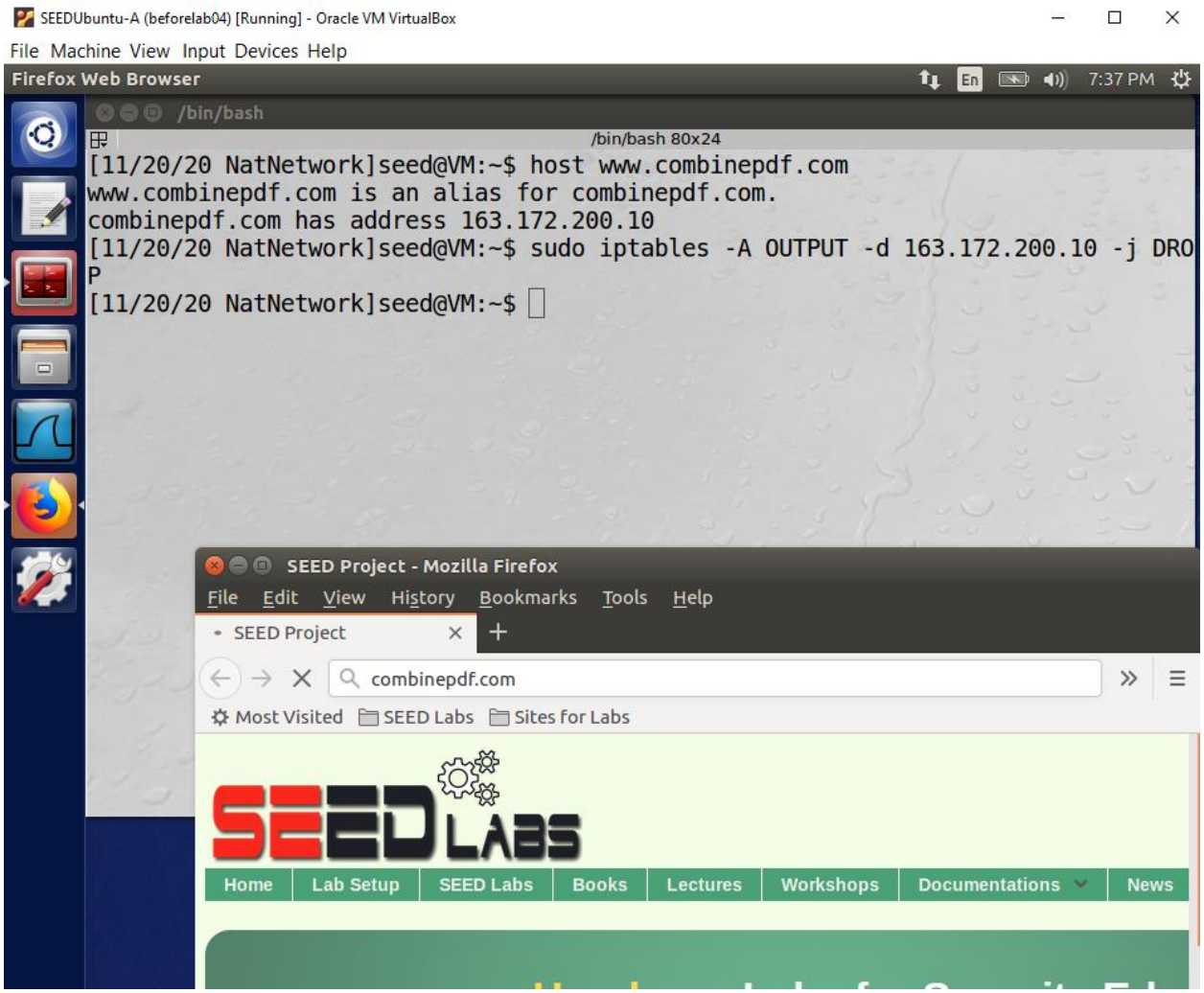
- Prevent A from doing telnet to Machine B.
  - A was not able to telnet to B




- Prevent B from doing telnet to Machine A.
  - B was not able to telnet to A




- Prevent A from visiting an external web site. I chose combinepdf.com
  - Was not able to access to www.combinepdf.com




2.2 Task 2: Implementing a Simple Firewall

- wrote a C program to implement packet filtering module that supports 5 difference rules using LKM and Netfilter

- program named “task2.c”

2.3 Task 3: Evading Egress Filtering

- block all the outgoing traffic to external telnet servers and to www.facebook.com

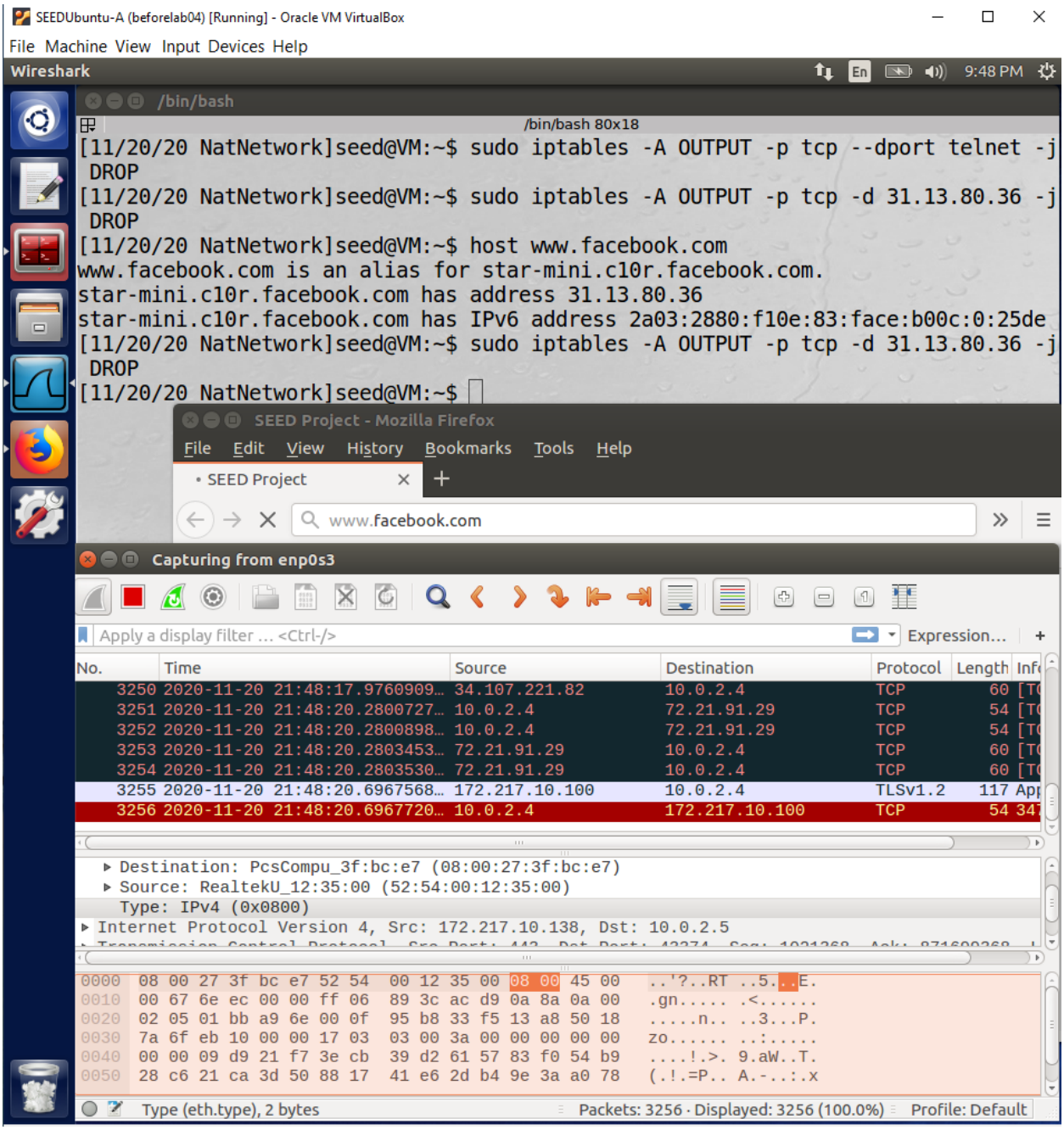
- Task 3.a: Telnet to Machine B through the firewall
  - Got facebook's ip address from "host facebook.com"
  - After blocking the outgoing traffics

```
[11/20/20 NatNetwork]seed@VM:~$ sudo iptables -A OUTPUT -p tcp --dport telnet -j
 DROP
[11/20/20 NatNetwork]seed@VM:~$ sudo iptables -A OUTPUT -p tcp -d 31.13.80.36 -j
 DROP
[11/20/20 NatNetwork]seed@VM:~$ telnet 10.0.2.5
Trying 10.0.2.5...
```

  - After establishing an SSH tunnel between A and B to make the all telnet traffic going through this tunnel => evade

```
[11/20/20 NatNetwork]seed@VM:~$ ssh -L 8000:10.0.2.6:23 seed@10.0.2.5
seed@10.0.2.5's password:
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.

Last login: Fri Nov 20 20:54:11 2020 from 10.0.2.4
[11/20/20 NatNetwork]seed@VM:~$ telnet 10.0.2.5
Trying 10.0.2.5...
Connected to 10.0.2.5.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login:
```

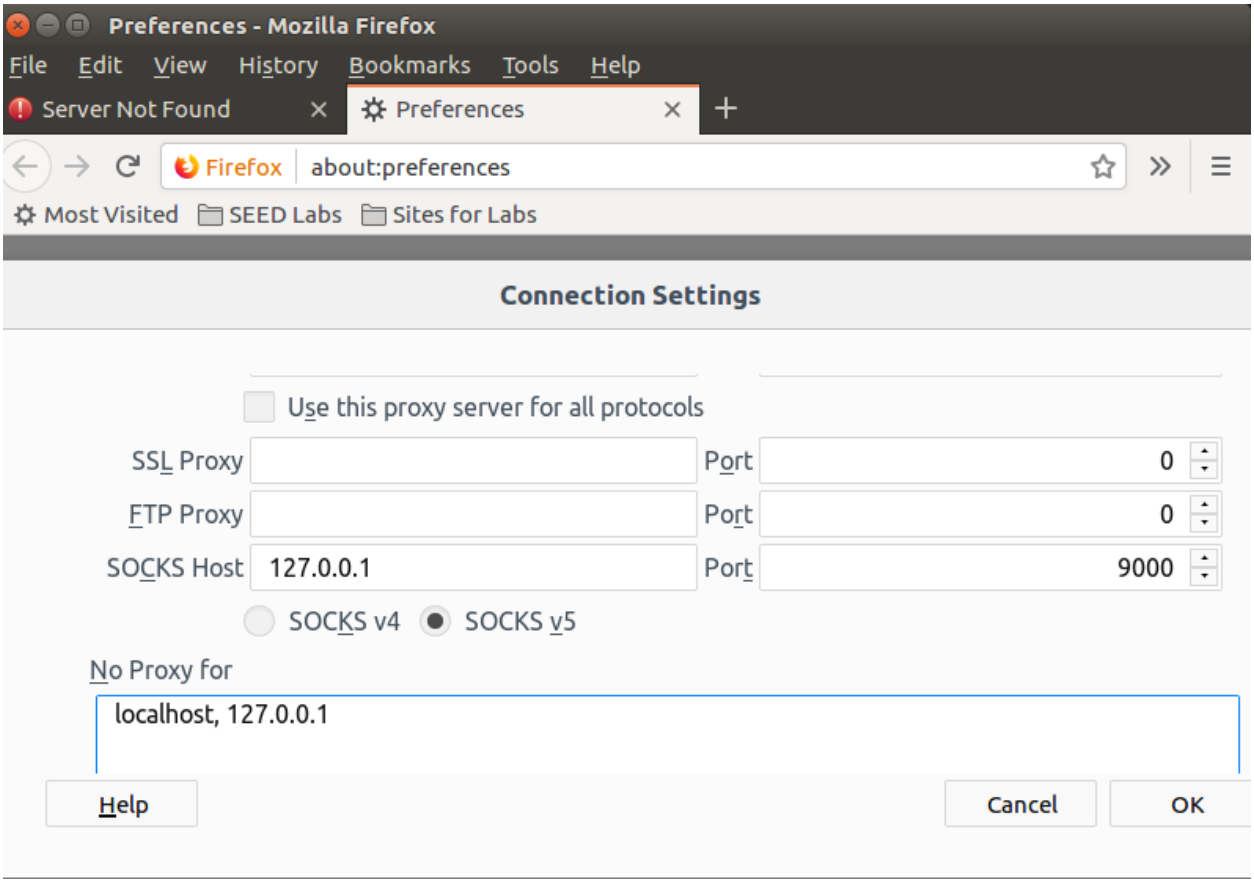
- Task 3.b: Connect to Facebook using SSH Tunnel.
  - Before establishing a SSH tunnel, was not able to connect to facebook.com



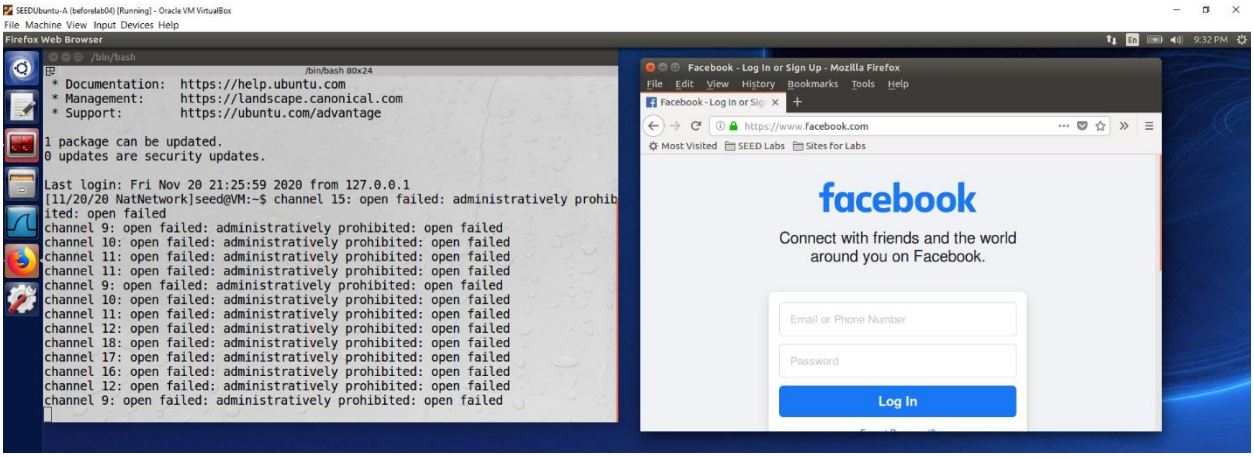

- After establishing a SSH tunnel by calling dynamic port forwarding

```
[11/20/20 NatNetwork]seed@VM:~$ ssh -D 9000 -C seed@vmb
ssh: Could not resolve hostname vmb: Name or service not known
[11/20/20 NatNetwork]seed@VM:~$ ssh -D 9000 -C seed@10.0.2.5
seed@10.0.2.5's password:
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.

Last login: Fri Nov 20 21:25:59 2020 from 127.0.0.1
```

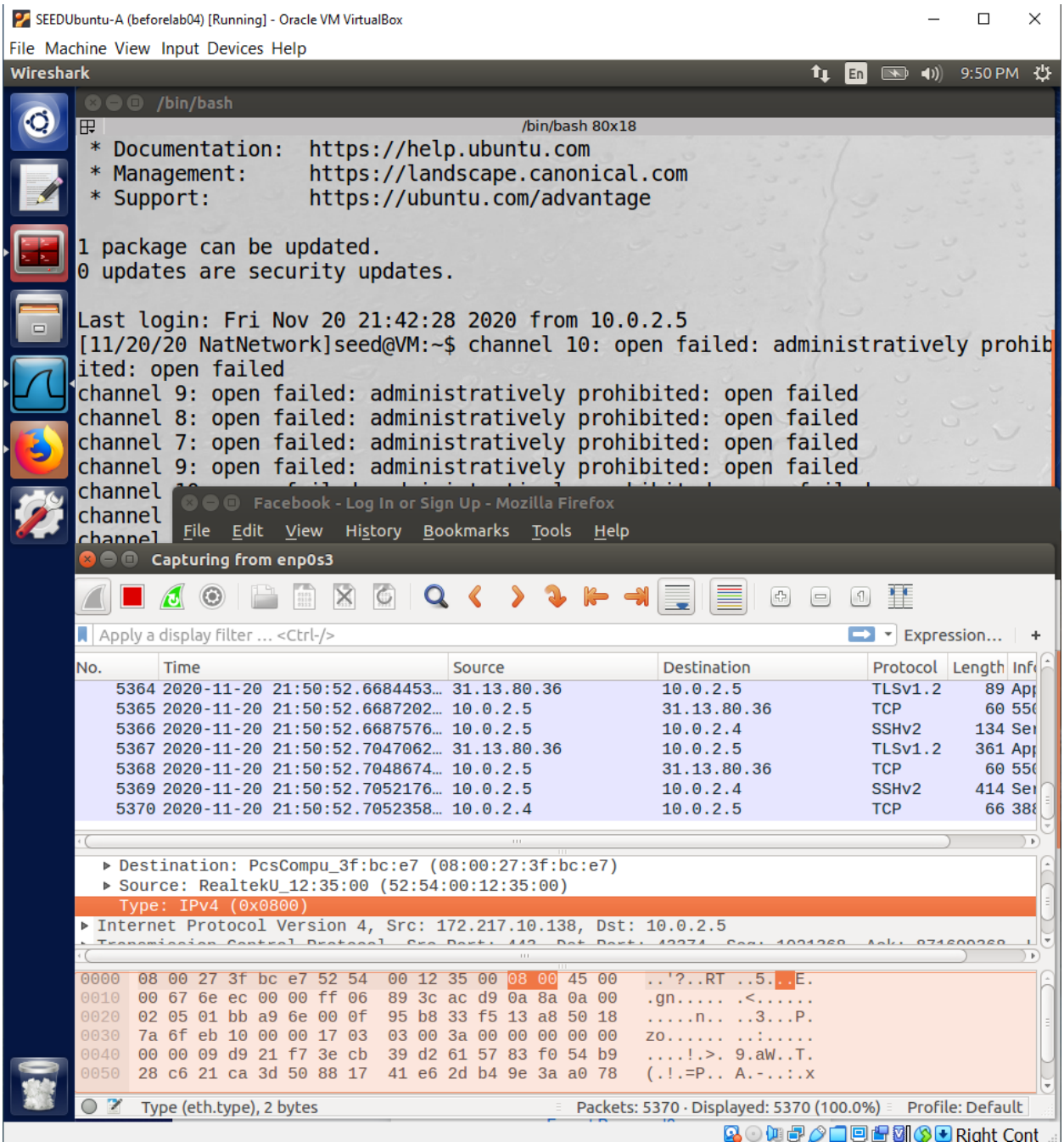
- Run the Firefox, under the setting shown below



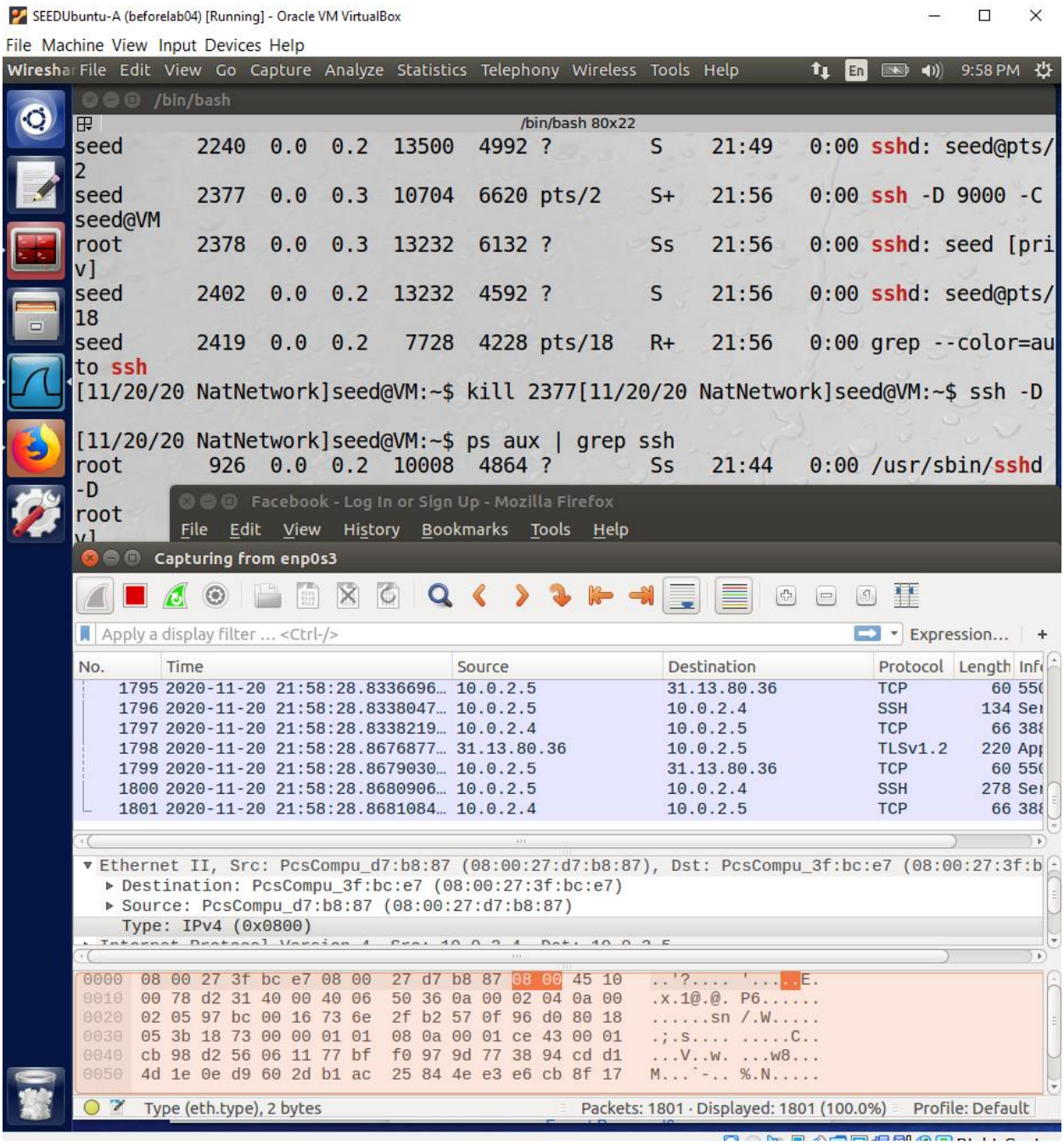

- Then, was able to access to facebook.com




- Tunnel forwards the HTTP request to facebook via 10.0.2.5, relay the results back to the browser. => firewall becomes seeing the ssh traffic between 10.0.2.4 and 10.0.2.5 rather than 10.0.2.4 and facebook

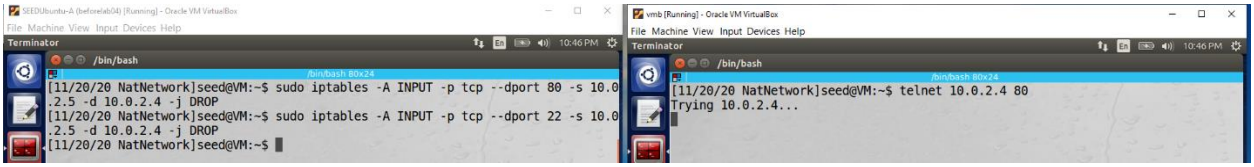



- Broke the SSH tunnel, cleared the Firefox cache, and tried to connect again
  - Was still able to access to facebook, which was unexpected


SEEDUbuntu-A (beforelab04) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
9:58 PM
/bin/bash
/bin/bash 80x22
seed 2240 0.0 0.2 13500 4992 ? S 21:49 0:00 sshd: seed@pts/2
seed 2377 0.0 0.3 10704 6620 pts/2 S+ 21:56 0:00 ssh -D 9000 -C seed@VM
root 2378 0.0 0.3 13232 6132 ? Ss 21:56 0:00 sshd: seed [priv]
seed 2402 0.0 0.2 13232 4592 ? S 21:56 0:00 sshd: seed@pts/18
seed 2419 0.0 0.2 7728 4228 pts/18 R+ 21:56 0:00 grep --color=auto ssh
[11/20/20 NatNetwork]seed@VM:~$ kill 2377[11/20/20 NatNetwork]seed@VM:~$ ssh -D
[11/20/20 NatNetwork]seed@VM:~$ ps aux | grep ssh
root 926 0.0 0.2 10008 4864 ? Ss 21:44 0:00 /usr/sbin/sshd -D
root
Facebook - Log In or Sign Up - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Capturing from enp0s3
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length
1795 2020-11-20 21:58:28.8336696… 10.0.2.5 31.13.80.36 TCP 60
1796 2020-11-20 21:58:28.8338047… 10.0.2.5 10.0.2.4 SSH 134
1797 2020-11-20 21:58:28.8338219… 10.0.2.4 10.0.2.5 TCP 66
1798 2020-11-20 21:58:28.8676877… 31.13.80.36 10.0.2.5 TLSv1.2 220
1799 2020-11-20 21:58:28.8679030… 10.0.2.5 31.13.80.36 TCP 60
1800 2020-11-20 21:58:28.8680906… 10.0.2.5 10.0.2.4 SSH 278
1801 2020-11-20 21:58:28.8681084… 10.0.2.4 10.0.2.5 TCP 66
Ethernet II, Src: PcsCompu_d7:b8:87 (08:00:27:d7:b8:87), Dst: PcsCompu_3f:bc:e7 (08:00:27:3f:b
Destination: PcsCompu_3f:bc:e7 (08:00:27:3f:bc:e7)
Source: PcsCompu_d7:b8:87 (08:00:27:d7:b8:87)
Type: IPv4 (0x0800)
0000 08 00 27 3f bc e7 08 00 27 d7 b8 87 08 00 45 10
0010 00 78 d2 31 40 00 40 06 50 36 0a 00 02 04 0a 00
0020 02 05 97 bc 00 16 73 6e 2f b2 57 0f 96 d0 80 18
0030 05 3b 18 73 00 00 01 01 08 0a 00 01 ce 43 00 01
0040 cb 98 d2 56 06 11 77 bf f0 97 9d 77 38 94 cd d1
0050 4d 1e 0e d9 60 2d b1 ac 25 84 4e e3 e6 cb 8f 17
Type (eth.type), 2 bytes
Packets: 1801 · Displayed: 1801 (100.0%)
Profile: Default

2.4 Task 4: Evading Ingress Filtering

- blocked B from accessing A's port 80(web server) and 22(ssh server)




- set up a reverse SSH tunnel on A