

# Foundations Network Security

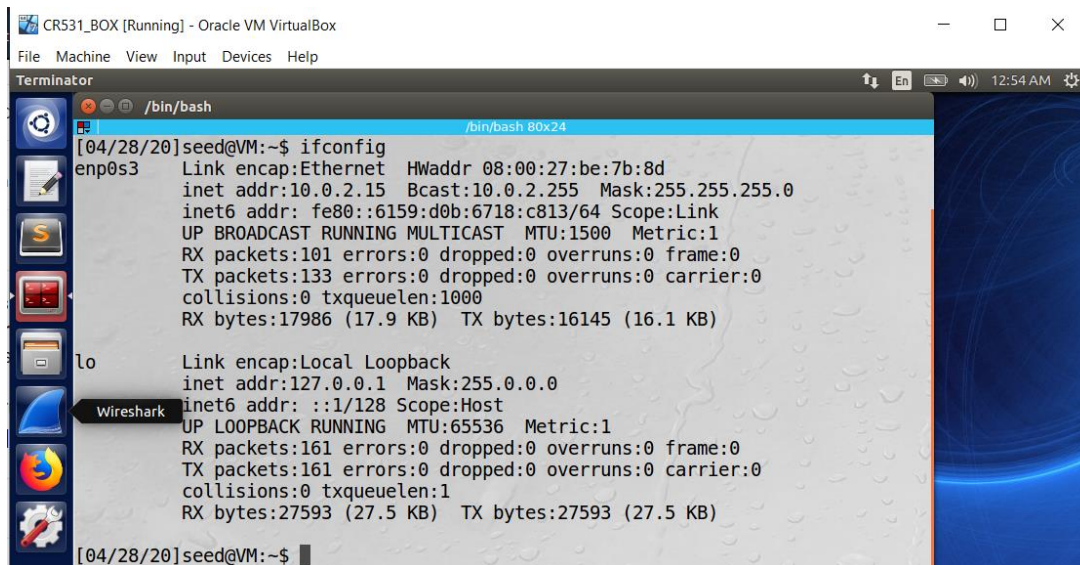
## Linux Firewall Exploration Lab

Chakradhar Reddy Donuri

E949F496

### Task 1: Using a Firewall

VM1 IP address: 10.0.2.15

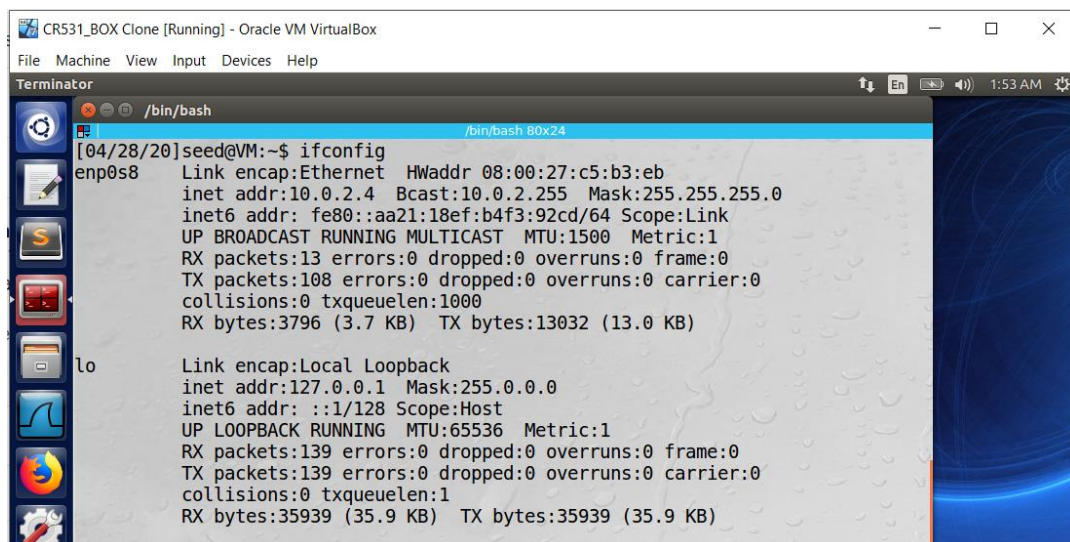


```
CR531_BOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
[04/28/20]seed@VM:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:be:7b:8d
        inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::6159:d0b:6718:c813/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:101 errors:0 dropped:0 overruns:0 frame:0
        TX packets:133 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:17986 (17.9 KB)  TX bytes:16145 (16.1 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:161 errors:0 dropped:0 overruns:0 frame:0
        TX packets:161 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:27593 (27.5 KB)  TX bytes:27593 (27.5 KB)

[04/28/20]seed@VM:~$
```

VM2 IP address: 10.0.2.4

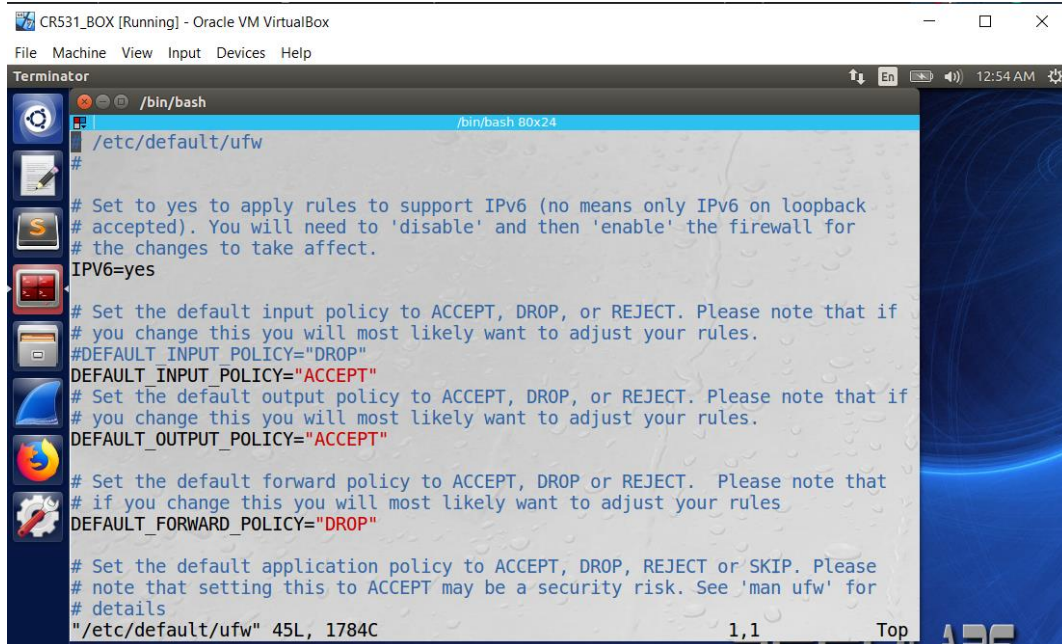


```
CR531_BOX Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
[04/28/20]seed@VM:~$ ifconfig
enp0s8  Link encap:Ethernet  HWaddr 08:00:27:c5:b3:eb
        inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::aa21:18ef:b4f3:92cd/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:13 errors:0 dropped:0 overruns:0 frame:0
        TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:3796 (3.7 KB)  TX bytes:13032 (13.0 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:139 errors:0 dropped:0 overruns:0 frame:0
        TX packets:139 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:35939 (35.9 KB)  TX bytes:35939 (35.9 KB)

[04/28/20]seed@VM:~$
```

Change DEFAULT\_INPUT\_POLICY="ACCEPT" in /etc/default/ufw



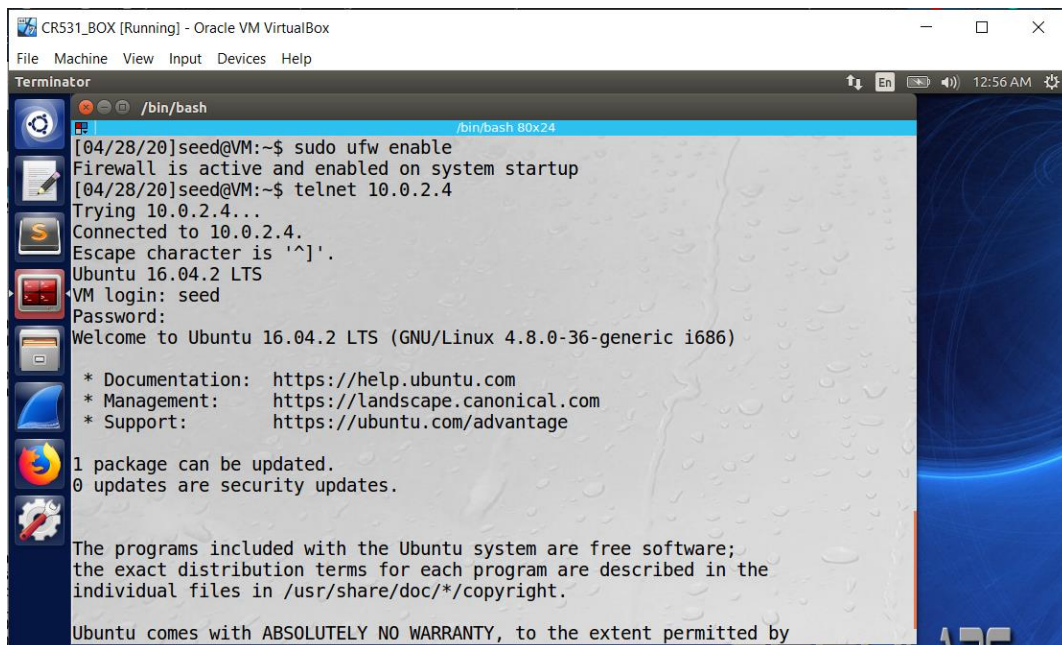
CR531\_BOX [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminator

```
/bin/bash
/etc/default/ufw
#
# Set to yes to apply rules to support IPv6 (no means only IPv6 on loopback
# accepted). You will need to 'disable' and then 'enable' the firewall for
# the changes to take affect.
IPV6=yes
# Set the default input policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
#DEFAULT_INPUT_POLICY="DROP"
DEFAULT_INPUT_POLICY="ACCEPT"
# Set the default output policy to ACCEPT, DROP, or REJECT. Please note that if
# you change this you will most likely want to adjust your rules.
DEFAULT_OUTPUT_POLICY="ACCEPT"
# Set the default forward policy to ACCEPT, DROP or REJECT. Please note that
# if you change this you will most likely want to adjust your rules
DEFAULT_FORWARD_POLICY="DROP"
# Set the default application policy to ACCEPT, DROP, REJECT or SKIP. Please
# note that setting this to ACCEPT may be a security risk. See 'man ufw' for
# details
"/etc/default/ufw" 45L, 1784C 1,1 Top
```

Making sure that VM1 is connecting to VM2



CR531\_BOX [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

Terminator

```
/bin/bash
[04/28/20]seed@VM:~$ sudo ufw enable
Firewall is active and enabled on system startup
[04/28/20]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
Connected to 10.0.2.4.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
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.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
```

## Prevent A from using telnet to connect Machine B.

```
CR531_BOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
[04/28/20]seed@VM:~$ sudo ufw enable
Firewall is active and enabled on system startup
[04/28/20]seed@VM:~$ sudo ufw deny out proto tcp to 10.0.2.4 port 23
Rule added
[04/28/20]seed@VM:~$ sudo ufw status numbered
Status: active

      To      Action      From
      --      -
[ 1] 10.0.2.4 23/tcp      DENY OUT      Anywhere      (out)

[04/28/20]seed@VM:~$ telnet 10.0.2.4
Trying 10.0.2.4...
^C
[04/28/20]seed@VM:~$
```

## Prevent B from doing telnet to Machine A.

```
CR531_BOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
[04/28/20]seed@VM:~$ sudo ufw deny proto tcp to 10.0.2.15 port 23
Rule added
[04/28/20]seed@VM:~$ sudo ufw status numbered
Status: active

      To      Action      From
      --      -
[ 1] 10.0.2.4 23/tcp      DENY OUT      Anywhere      (out)
[ 2] 10.0.2.15 23/tcp      DENY IN       Anywhere

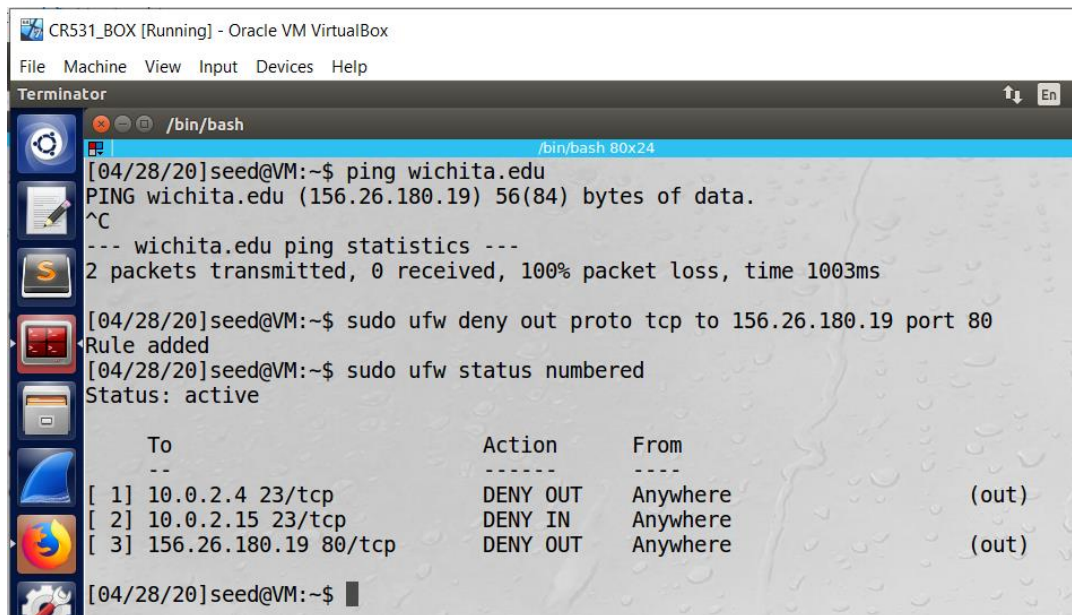
[04/28/20]seed@VM:~$
```

## Checking

```
CR531_BOX Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
[04/28/20]seed@VM:~$ telnet 10.0.2.15
Trying 10.0.2.15...
^C
[04/28/20]seed@VM:~$
```



## Prevent A from visiting an external web site (Wichita.edu)



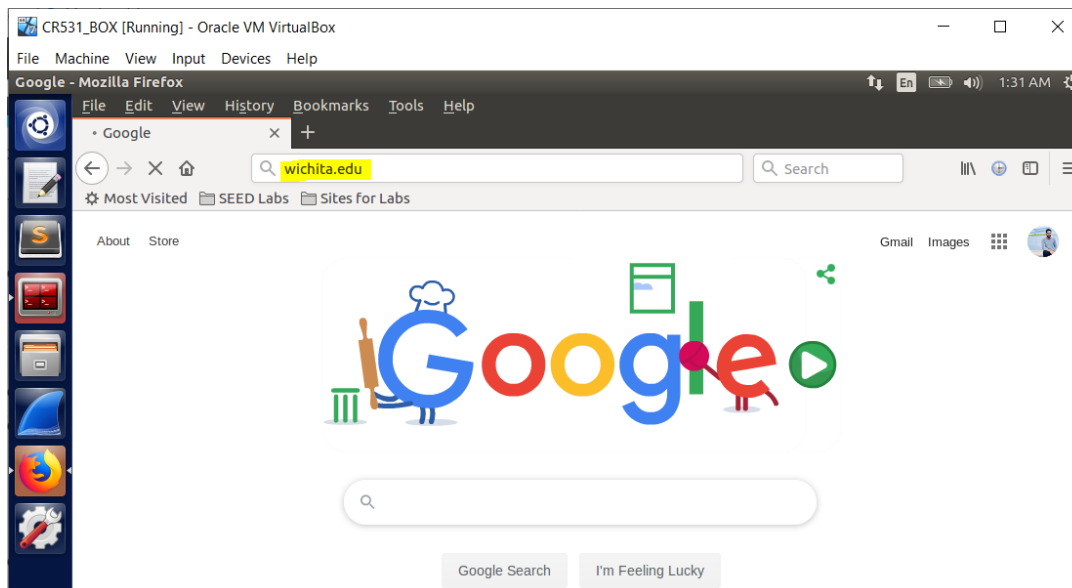
```
CR531_BOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
[04/28/20]seed@VM:~$ ping wichita.edu
PING wichita.edu (156.26.180.19) 56(84) bytes of data.
^C
--- wichita.edu ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1003ms

[04/28/20]seed@VM:~$ sudo ufw deny out proto tcp to 156.26.180.19 port 80
Rule added
[04/28/20]seed@VM:~$ sudo ufw status numbered
Status: active

      To                        Action      From
      --                        -
[ 1] 10.0.2.4 23/tcp            DENY OUT    Anywhere    (out)
[ 2] 10.0.2.15 23/tcp           DENY IN     Anywhere
[ 3] 156.26.180.19 80/tcp       DENY OUT    Anywhere    (out)

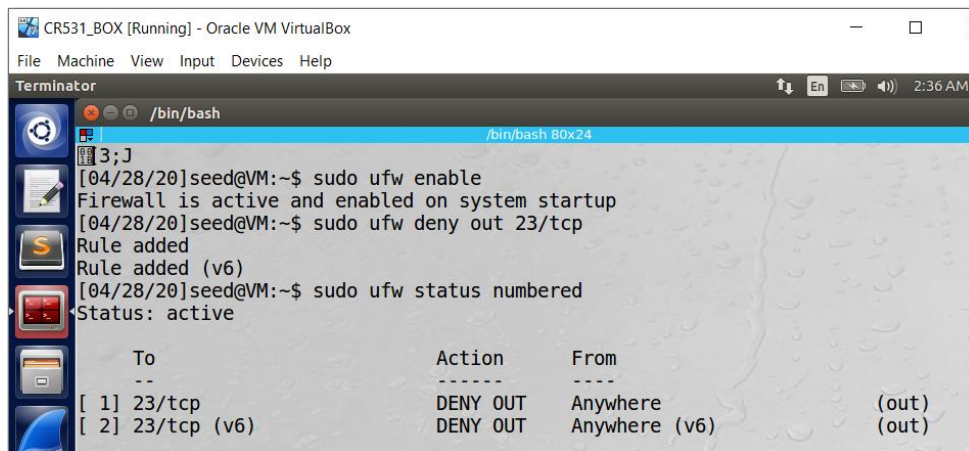
[04/28/20]seed@VM:~$
```

## Checking Wichita.edu in browser



## Task 2: Evading Egress Filtering

### Step 1: blocking outgoing traffic 23/tcp



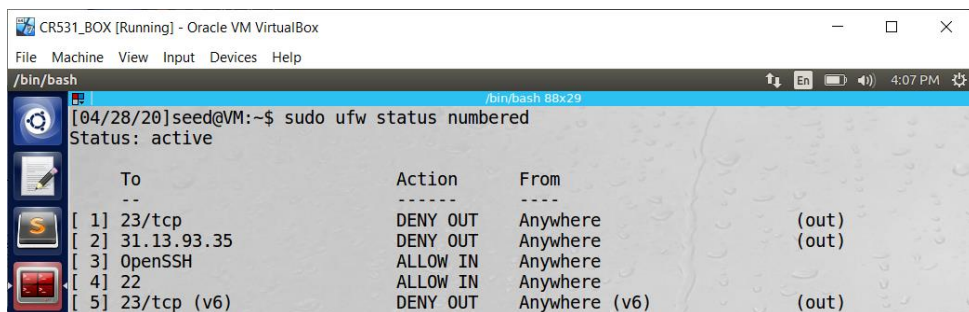
```
CR531_BOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminator
/bin/bash
/bin/bash 80x24

[04/28/20]seed@VM:~$ sudo ufw enable
Firewall is active and enabled on system startup
[04/28/20]seed@VM:~$ sudo ufw deny out 23/tcp
Rule added
Rule added (v6)
[04/28/20]seed@VM:~$ sudo ufw status numbered
Status: active

    To      Action      From
    --      -
[ 1] 23/tcp  DENY OUT    Anywhere    (out)
[ 2] 23/tcp  DENY OUT    Anywhere (v6) (out)
```

Next block [www.facebook.com](http://www.facebook.com) i.e. 31.13.93.35



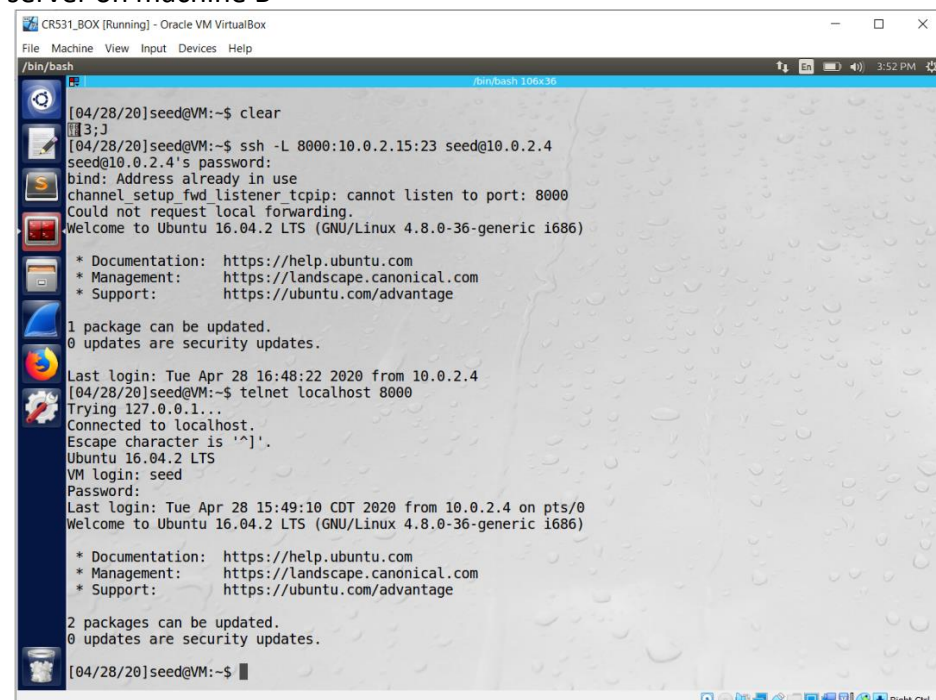
```
CR531_BOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminator
/bin/bash
/bin/bash 88x29

[04/28/20]seed@VM:~$ sudo ufw status numbered
Status: active

    To      Action      From
    --      -
[ 1] 23/tcp  DENY OUT    Anywhere    (out)
[ 2] 31.13.93.35 DENY OUT    Anywhere    (out)
[ 3] OpenSSH ALLOW IN     Anywhere
[ 4] 22      ALLOW IN     Anywhere
[ 5] 23/tcp (v6) DENY OUT    Anywhere (v6) (out)
```

**Task 2.a) Deliverable** Explain what the "-L" option does in the ssh command. Explain how the tunneling approach allows us to bypass the egress filtering. A screen shot of the packet traffic provided by Wireshark on Machine A showing the packet traffic when connecting to the telnet server on machine B



```
CR531_BOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminator
/bin/bash
/bin/bash 106x36

[04/28/20]seed@VM:~$ clear
[04/28/20]seed@VM:~$ ssh -L 8000:10.0.2.15:23 seed@10.0.2.4
seed@10.0.2.4's password:
bind: Address already in use
channel_setup_fwd_listener_tcpip: cannot listen to port: 8000
Could not request local forwarding.
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: Tue Apr 28 16:48:22 2020 from 10.0.2.4
[04/28/20]seed@VM:~$ telnet localhost 8000
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Tue Apr 28 15:49:10 CDT 2020 from 10.0.2.4 on pts/0
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

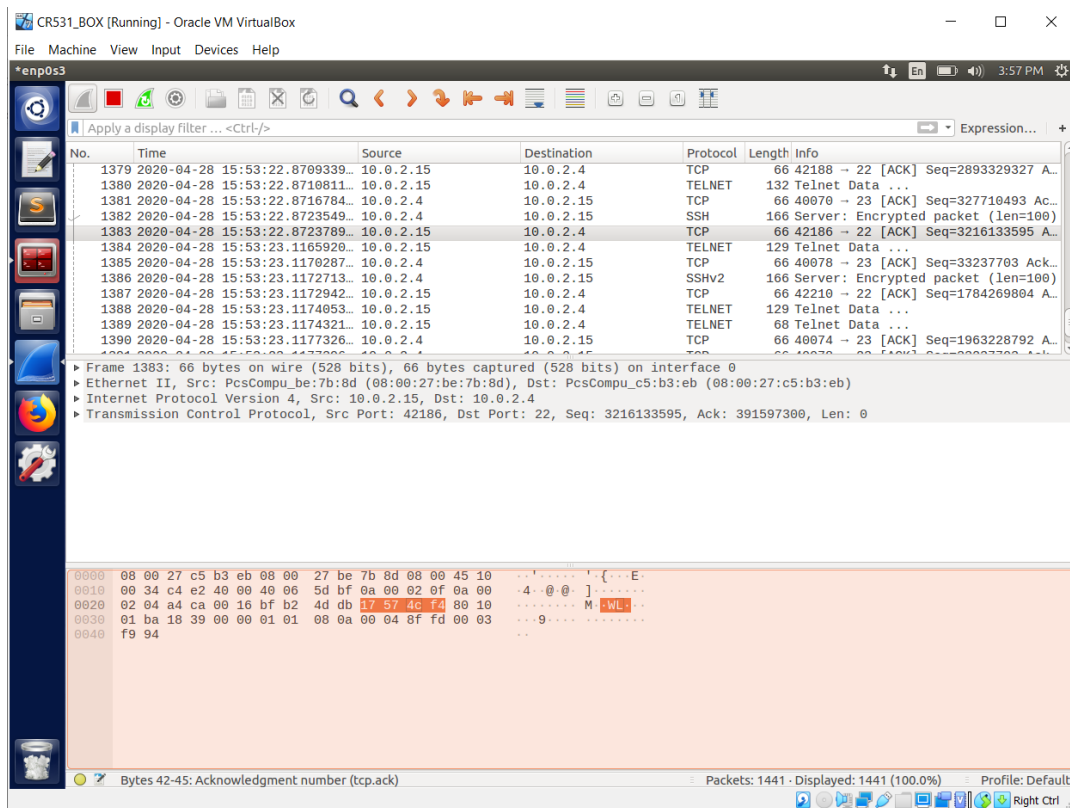
2 packages can be updated.
0 updates are security updates.

[04/28/20]seed@VM:~$
```

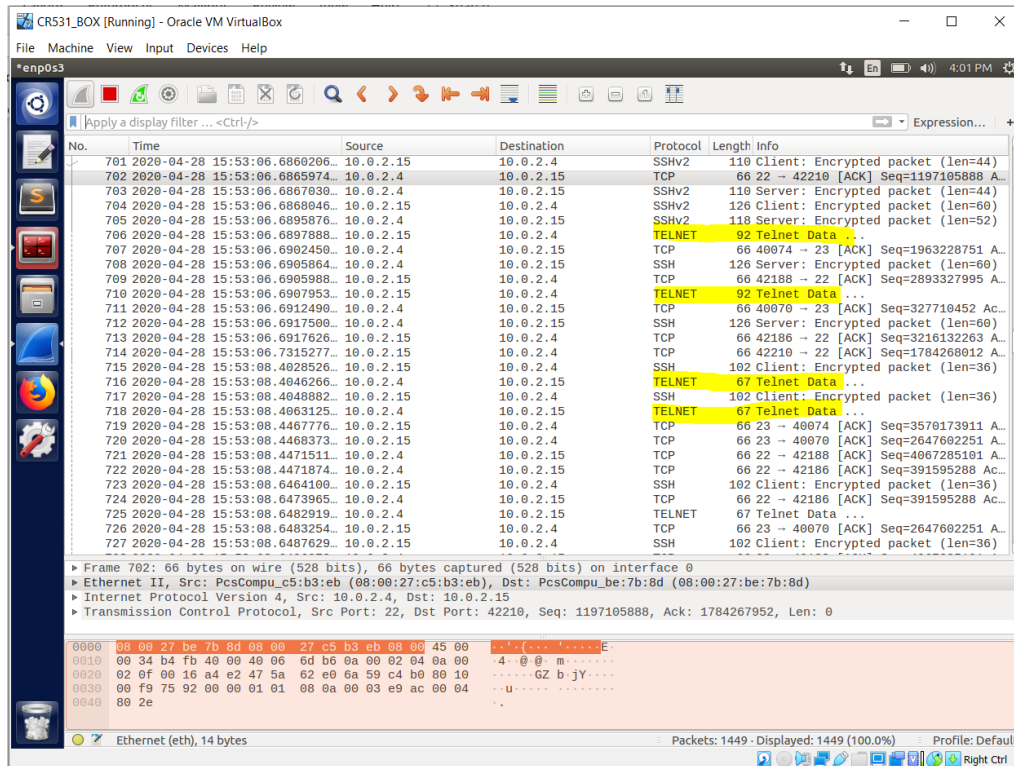
**Answer)** We set up an SSH tunnel through which all telnet communications can pass. The -L flag stands for the local host. i.e. Specifies that the given port on the local (client) host is to be forwarded to the given host and port on the remote side.

Now, if we point the VM to localhost 8000, first it gets forwarded to 10.0.2.4:23 (i.e. telnet port of machine\_B) through after going 10.0.2.4:22 (ssh port of machine\_B) known as port forwarding.

**Below is the screen shot of the packet traffic provided by Wireshark on Machine .A showing the packet traffic when connecting to the telnet server on machine B**

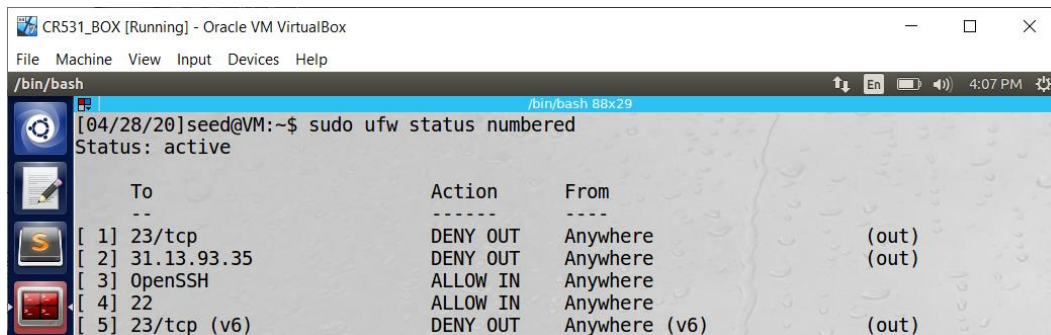


**Observation:** After CR531 i.e. VM1 gains access to CR531\_Clone i.e. VM2 it telnet to localhost and gains access to localhost. Information regarding localhost is passed to VM1 through VM2 and SSH tunnel



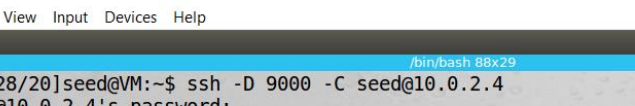
## Task 2.b Connect to Facebook using SSH Tunnel

We have already denied out to facebook.com i.e 31.13.93.35





VM1(10.0.2.15) creates a SSH tunnel to VM2 (10.0.2.4) through port 9000.



CR531\_BOX [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

/bin/bash

[04/28/20]seed@VM:~\$ ssh -D 9000 -C seed@10.0.2.4

seed@10.0.2.4'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>

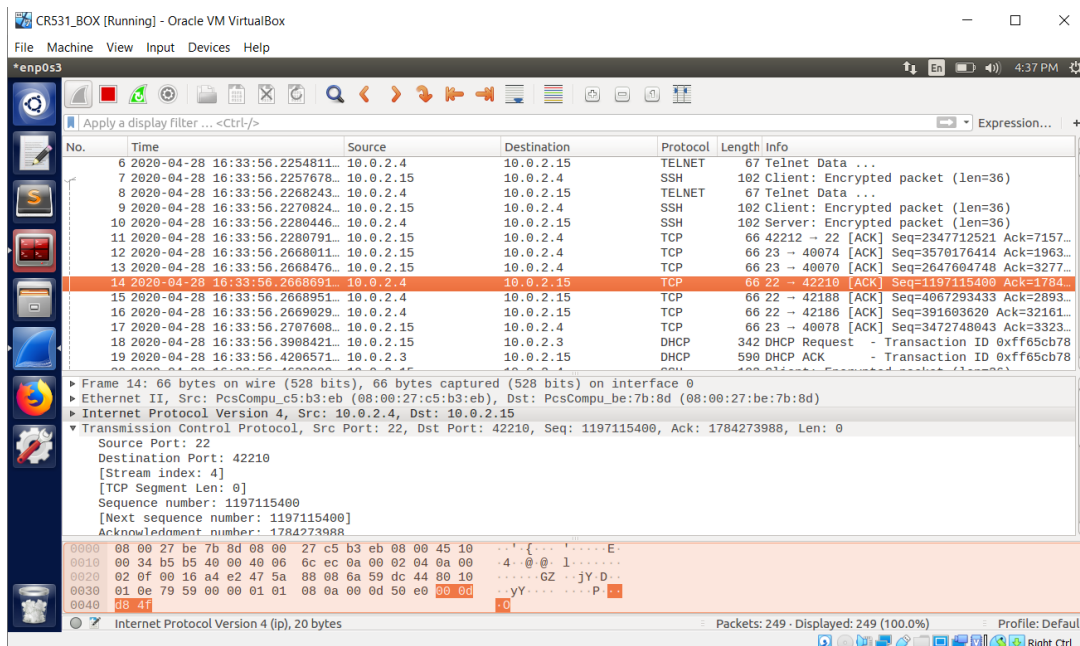
\* Support: <https://ubuntu.com/advantage>

1 package can be updated.

0 updates are security updates.

Last login: Tue Apr 28 16:53:17 2020 from 10.0.2.15

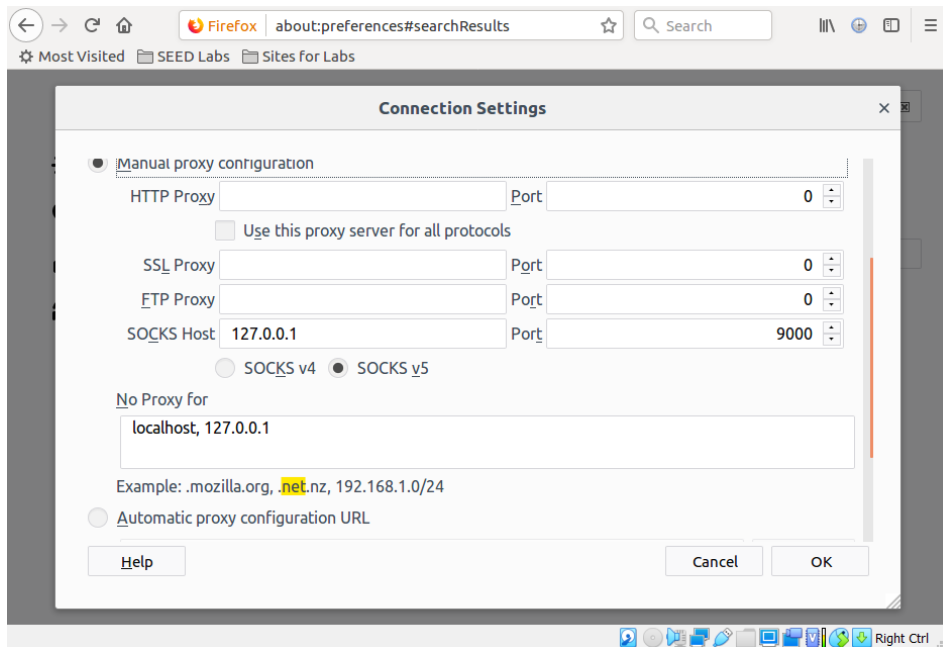
[04/28/20]seed@VM:~\$



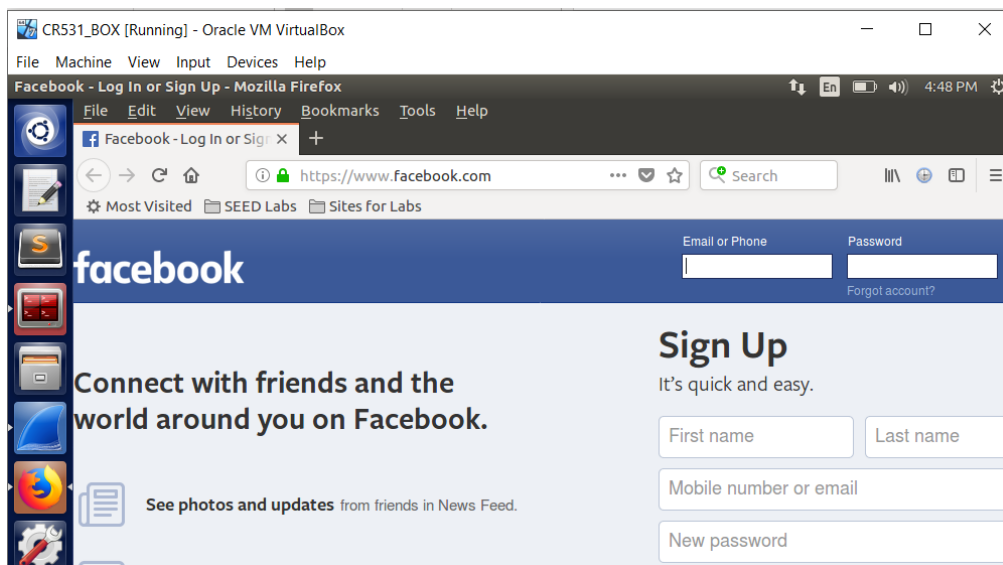
**Observation:** VM1(10.0.2.15) and VM2 (10.0.2.4) performs 3-way handshake and establishes connection using the SSH port 22. After establishing the connection they communicate through TCP protocol.

### Step-1) Changing preferences of firefox



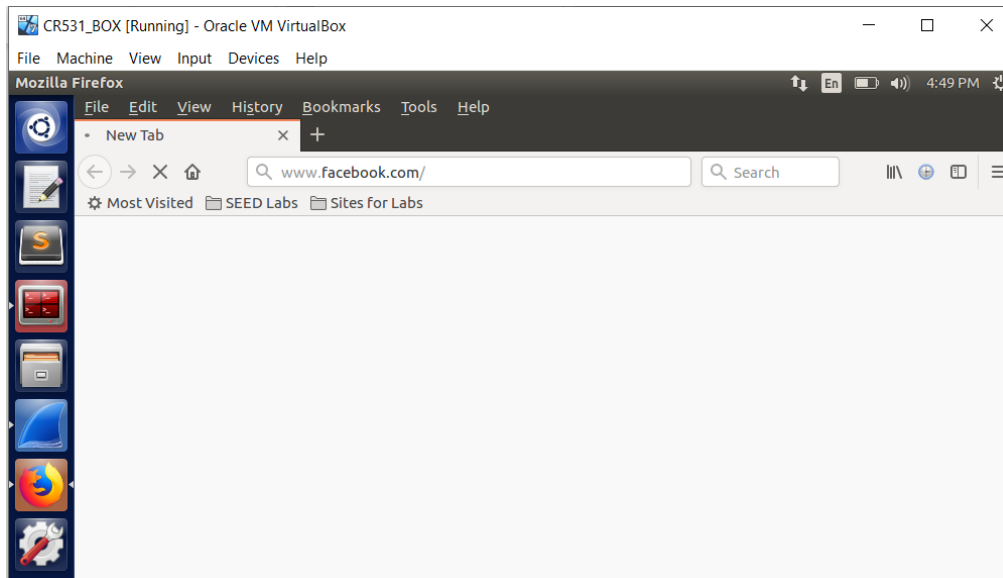


Testing [www.facebook.com](https://www.facebook.com)



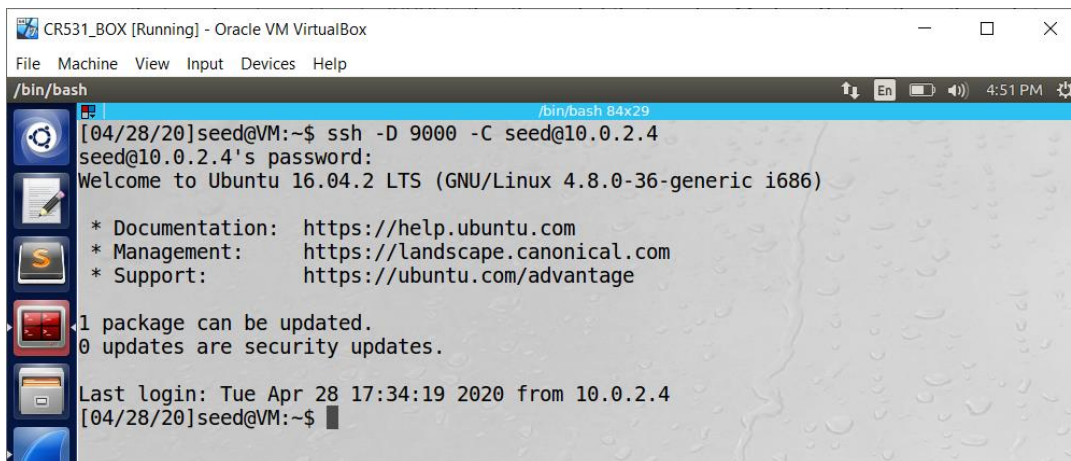
**Observation:** We can see that website is working.

**Step-2)** Now, VM1 (10.0.2.15) breaks the SSH connection from VM2 (10.0.2.4) by exiting VM2



**Observation:** After breaking SSH connection when VM1(10.0.2.15) tries to access facebook.com the proxy and port 9000 refuses the connection since it cannot connect to VM2 (10.0.2.4).

**Step-3)** Now, again VM1 (10.0.2.15) establishes SSH connection to VM2 (10.0.2.4).



After establishing the SSH tunnel between 10.0.2.15 and 10.0.2.4 again performs 3-way handshake. Further communication is done through SSH

### **Explain what the -D and -C options do in the ssh command**

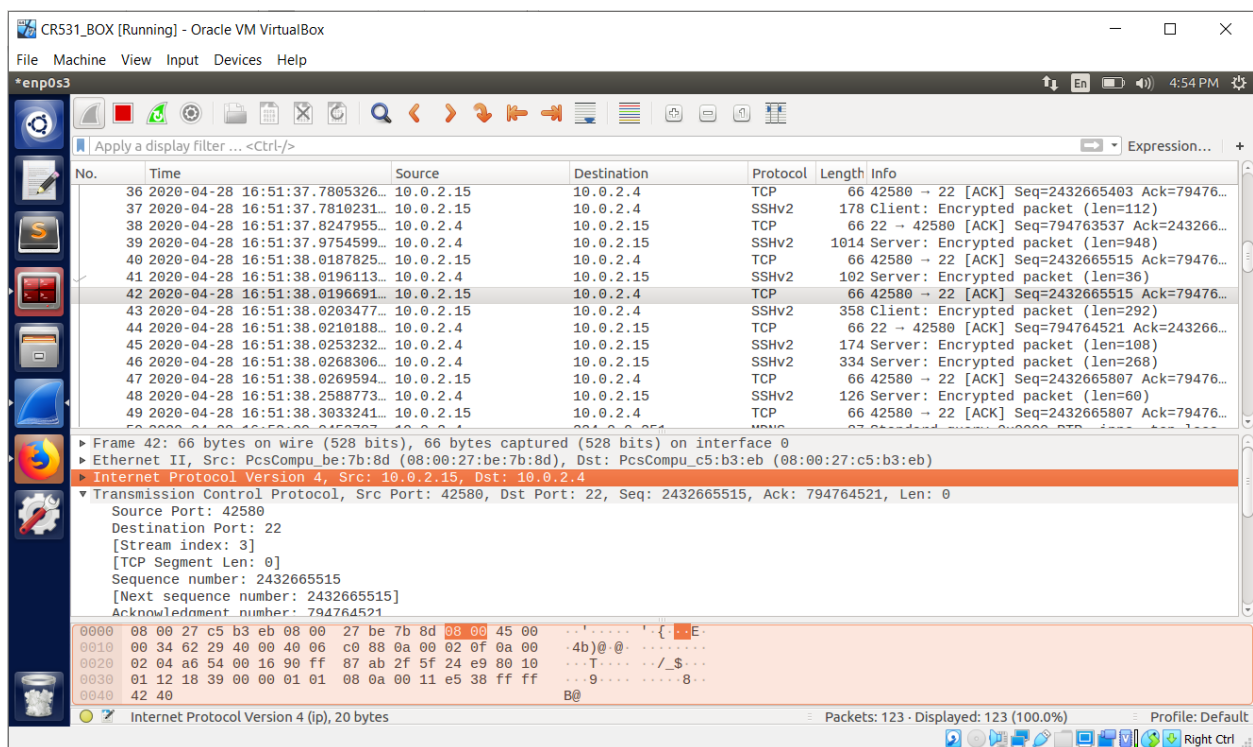
The -D flag stands for dynamic port forwarding which will basically turn your SSH client into a proxy server (SOCKS). i.e. Specifies a local “dynamic” application-level port forwarding.

-C i.e. Requests compression of all data (including stdin, stdout, stderr, and data for forwarded X11 and TCP connections)

**Explain how this approach helps you bypass the firewall rules?**

Many organizations and industries among different countries often block access to some external sites by their internal users. This is called Egress filtering . These businesses set up their egress firewalls to block social network sites, which ensures that their workers can not access such sites from within their network. Unfortunately, it is easy to bypass these firewalls, and services / products that help users bypass firewalls are widely available on the Internet. The most commonly used technology to bypass egress firewalls is Virtual Private Network (VPN)

Egress filtering controls the traffic that is attempting to leave the network. Before an outbound connection is allowed, it has to pass the filter's rules. Pretty much every firewall provides egress filtering. However, it is not enabled by default. The out-of-the-box setup typically allows any machine on the network to connect to any host over any port. Since it is disabled by default, many small & medium-size organizations never use egress filtering.



**Observation:** We can see that packets are sent through SSH which contain information about Ethernet Type, IP, TCP and SSH and with port number 22. There is no information of facebook.com IP address and port 22 is not blocked so the ufw firewall accepts the packet.

### Task 3: Evading Ingress Filtering

**Answer)** First check the ip address of each VM box

VM1- 10.0.2.15

```
CR531_BOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
[04/28/20]seed@VM:~$ ifconfig
enp0s3  Link encap:Ethernet  HWaddr 08:00:27:be:7b:8d
        inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::6159:d0b:6718:c813/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:101 errors:0 dropped:0 overruns:0 frame:0
        TX packets:133 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:17986 (17.9 KB)  TX bytes:16145 (16.1 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:161 errors:0 dropped:0 overruns:0 frame:0
        TX packets:161 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:27593 (27.5 KB)  TX bytes:27593 (27.5 KB)

[04/28/20]seed@VM:~$
```

## VM-2: 10.0.2.4

```
CR531_BOX Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
[04/28/20]seed@VM:~$ ifconfig
enp0s8  Link encap:Ethernet  HWaddr 08:00:27:c5:b3:eb
        inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
        inet6 addr: fe80::aa21:18ef:b4f3:92cd/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:13 errors:0 dropped:0 overruns:0 frame:0
        TX packets:108 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:3796 (3.7 KB)  TX bytes:13032 (13.0 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:139 errors:0 dropped:0 overruns:0 frame:0
        TX packets:139 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1
        RX bytes:35939 (35.9 KB)  TX bytes:35939 (35.9 KB)

[04/28/20]seed@VM:~$
```

Now, Deny port 22 and 80 from 10.0.2.4 (VM2) and perform reverse ssh tunnel to VM2



```
CR531_BOX [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
Rule added
[04/29/20]seed@VM:~$ sudo ufw deny from 10.0.2.4 to any port 80
Rule added
[04/29/20]seed@VM:~$ sudo ufw status numbered
Status: active

    To Action From
    --
[ 1] 22 DENY IN 10.0.2.4
[ 2] 80 DENY IN 10.0.2.4

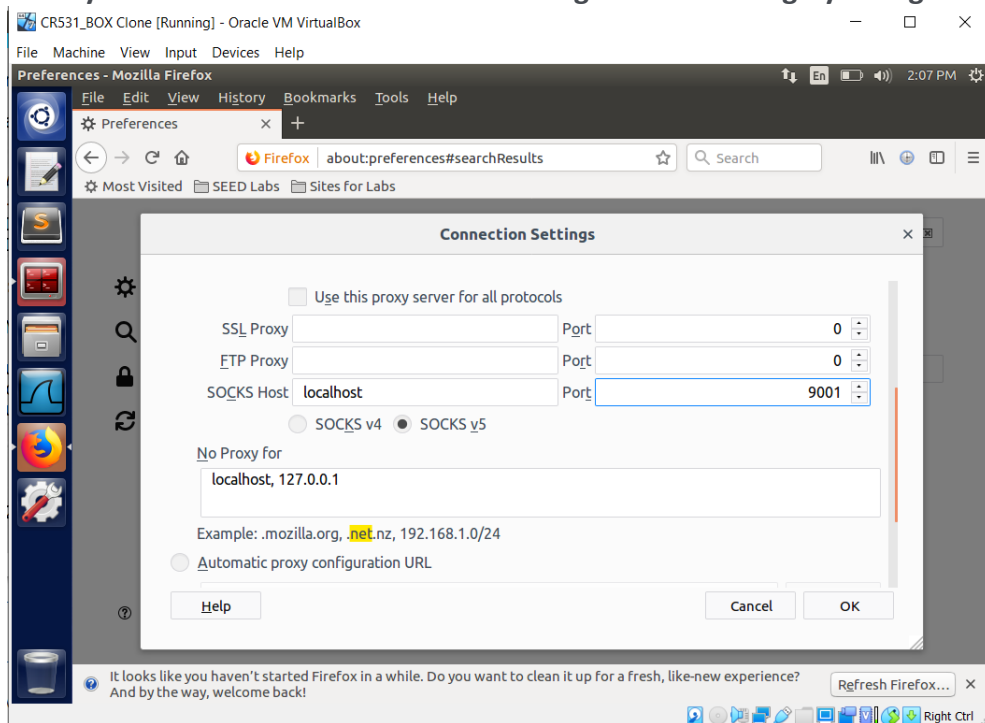
[04/29/20]seed@VM:~$ ssh -R 9000:localhost:22 seed@10.0.2.4
seed@10.0.2.4's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

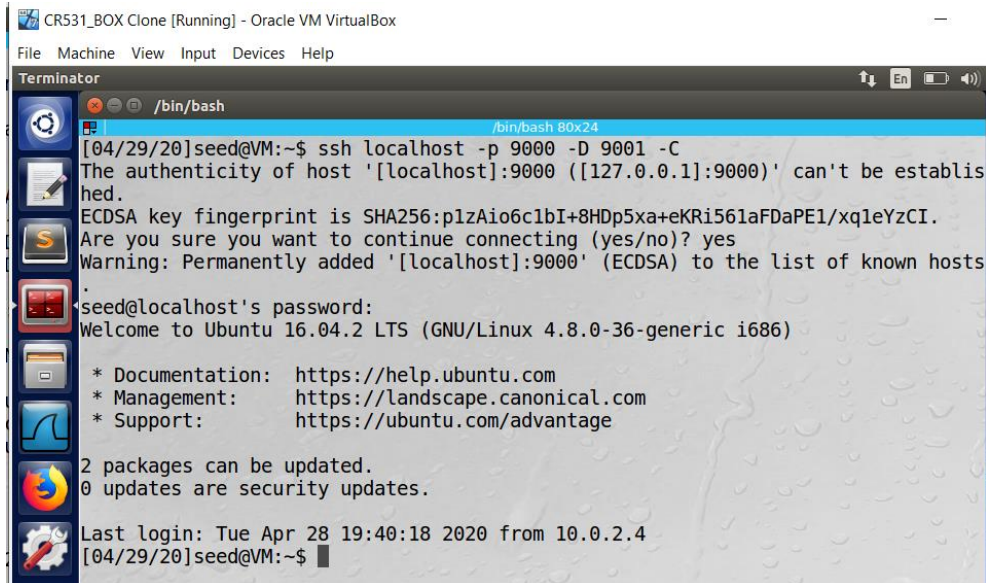
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

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

Last login: Tue Apr 28 20:41:00 2020 from 127.0.0.1
[04/29/20]seed@VM:~$
```

Now you can SSH from VM2 to VM1 through SSH tunneling by change the proxy port to 9001





```
CR531_BOX Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
[04/29/20]seed@VM:~$ ssh localhost -p 9000 -D 9001 -C
The authenticity of host '[localhost]:9000 ([127.0.0.1]:9000)' can't be established.
ECDSA key fingerprint is SHA256:plzAio6c1bI+8HDP5xa+eKRI561aFDaPE1/xqleYzCI.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:9000' (ECDSA) to the list of known hosts
seed@localhost's password:
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

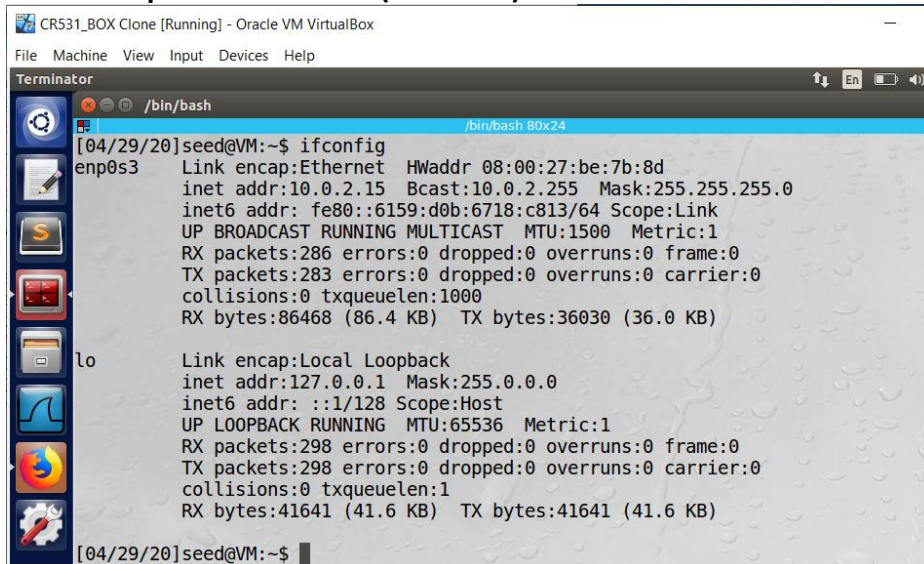
 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

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

Last login: Tue Apr 28 19:40:18 2020 from 10.0.2.4
[04/29/20]seed@VM:~$
```

Now we can see from below screenshots the ip address have be altered from VM1 to VM2

## VM-2 has ip address of VM1(10.0.2.15)



```
CR531_BOX Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
[04/29/20]seed@VM:~$ ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:be:7b:8d
            inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
            inet6 addr: fe80::6159:d0b:6718:c813/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:286 errors:0 dropped:0 overruns:0 frame:0
            TX packets:283 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:86468 (86.4 KB)  TX bytes:36030 (36.0 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:298 errors:0 dropped:0 overruns:0 frame:0
            TX packets:298 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1
            RX bytes:41641 (41.6 KB)  TX bytes:41641 (41.6 KB)

[04/29/20]seed@VM:~$
```

## VM-1 has ip address of VM2(10.0.2.4)

```
[04/29/20]seed@VM:~$ ifconfig
enp0s8    Link encap:Ethernet  HWaddr 08:00:27:c5:b3:eb
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.0
          inet6 addr: fe80::aa21:18ef:b4f3:92cd/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:5899 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2040 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7831951 (7.8 MB)  TX bytes:350037 (350.0 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:639 errors:0 dropped:0 overruns:0 frame:0
          TX packets:639 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:169079 (169.0 KB)  TX bytes:169079 (169.0 KB)

[04/29/20]seed@VM:~$
```

## Check the VM1 ip address from browser

