

# ITIS 6167/8167: Network Security

## Project 3 - SYN Flood Attack

Professor: Dr. Michael Young

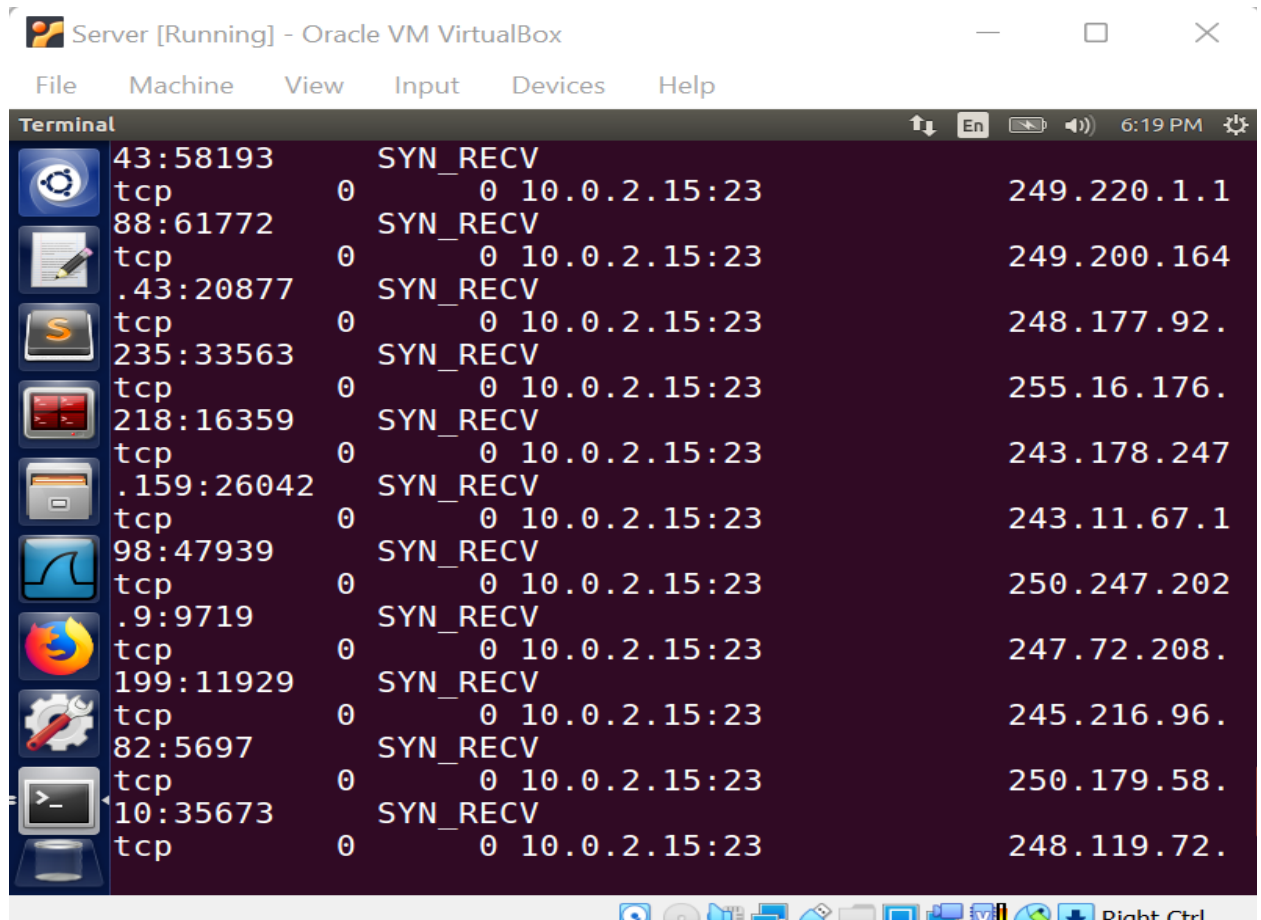
Student Name: Sireesha Ponnaganti

Student ID: 801310488

Student Email : [sponnaga@uncc.edu](mailto:sponnaga@uncc.edu)

### 1. SYN Flood Attack (SYN Cookie = 0):

The screenshot below displays the output of the netstat -tna command on the Server computer when the SYN Cookie is disabled.



The screenshot shows a terminal window titled "Server [Running] - Oracle VM VirtualBox". The terminal displays the output of the netstat -tna command, showing a list of TCP connections in the SYN\_RECV state. The output is as follows:

Port	State	Recv-Q	Send-Q	Local Address	Foreign Address
43:58193	SYN_RECV	0	0	10.0.2.15:23	249.220.1.1
88:61772	SYN_RECV	0	0	10.0.2.15:23	249.200.164
.43:20877	SYN_RECV	0	0	10.0.2.15:23	248.177.92.
235:33563	SYN_RECV	0	0	10.0.2.15:23	255.16.176.
218:16359	SYN_RECV	0	0	10.0.2.15:23	243.178.247
.159:26042	SYN_RECV	0	0	10.0.2.15:23	243.11.67.1
98:47939	SYN_RECV	0	0	10.0.2.15:23	250.247.202
.9:9719	SYN_RECV	0	0	10.0.2.15:23	247.72.208.
199:11929	SYN_RECV	0	0	10.0.2.15:23	245.216.96.
82:5697	SYN_RECV	0	0	10.0.2.15:23	250.179.58.
10:35673	SYN_RECV	0	0	10.0.2.15:23	248.119.72.

Figure 1. SYN\_RECV status of server

The snapshot below shows the Client computer unable to connect to the Server's telnet connection.

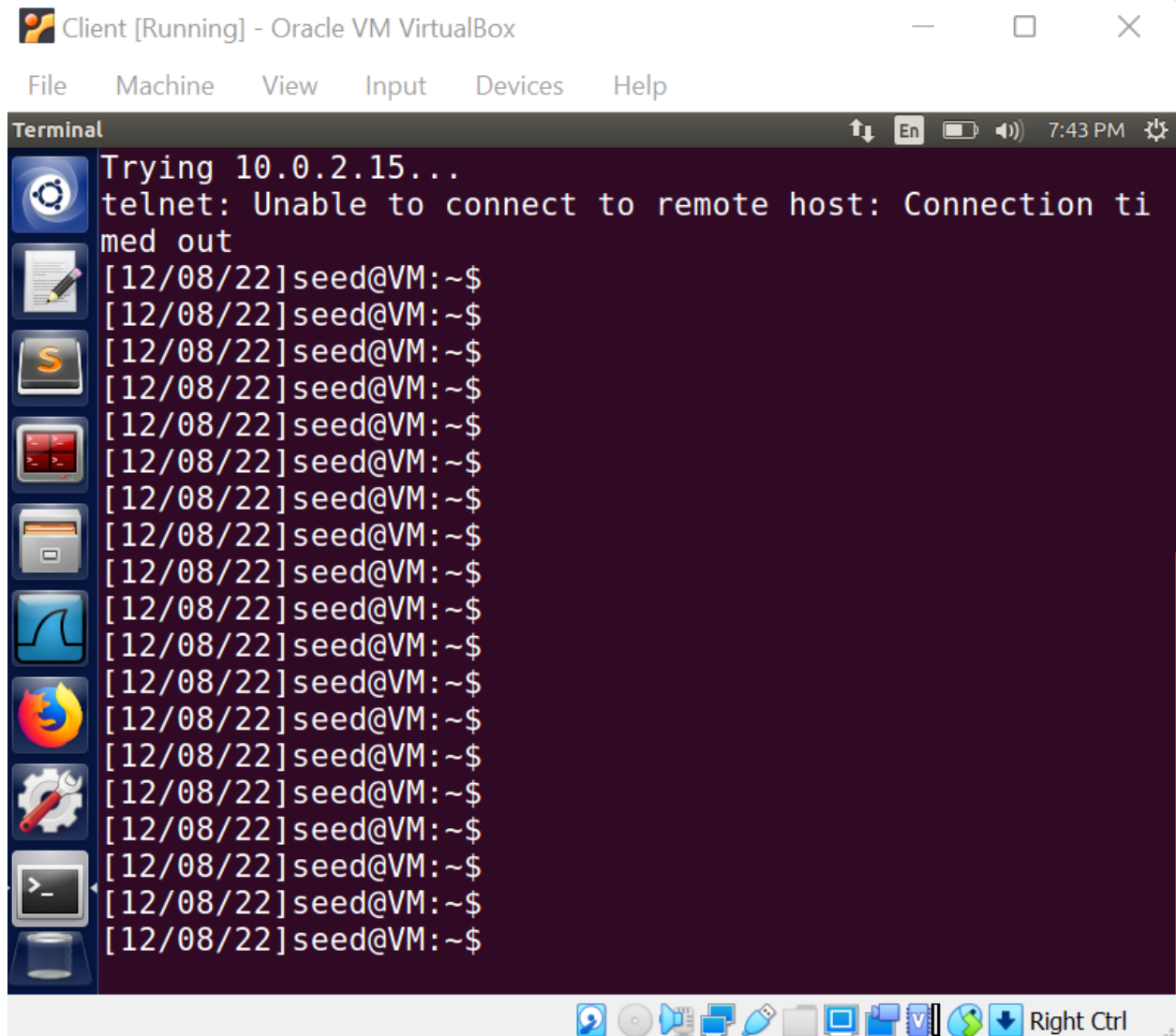
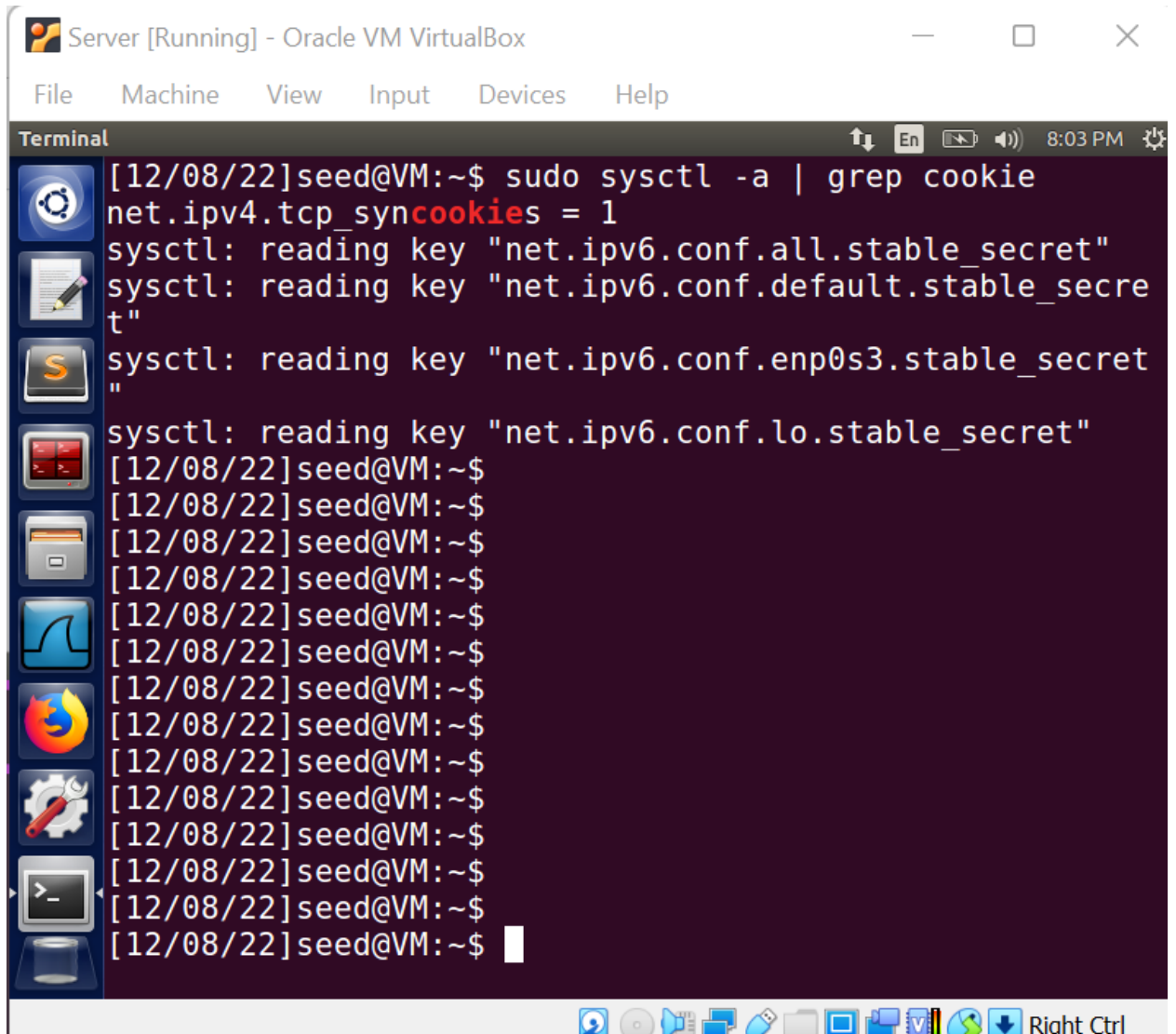


Figure 2 Client is unable to establish a Telnet connection with the server

## 2. SYN Flood Attack (SYN Cookie = 1):

The client can connect to the server's telnet connection when the SYN Cookie is turned on, as seen in the following screenshot of the server machine.

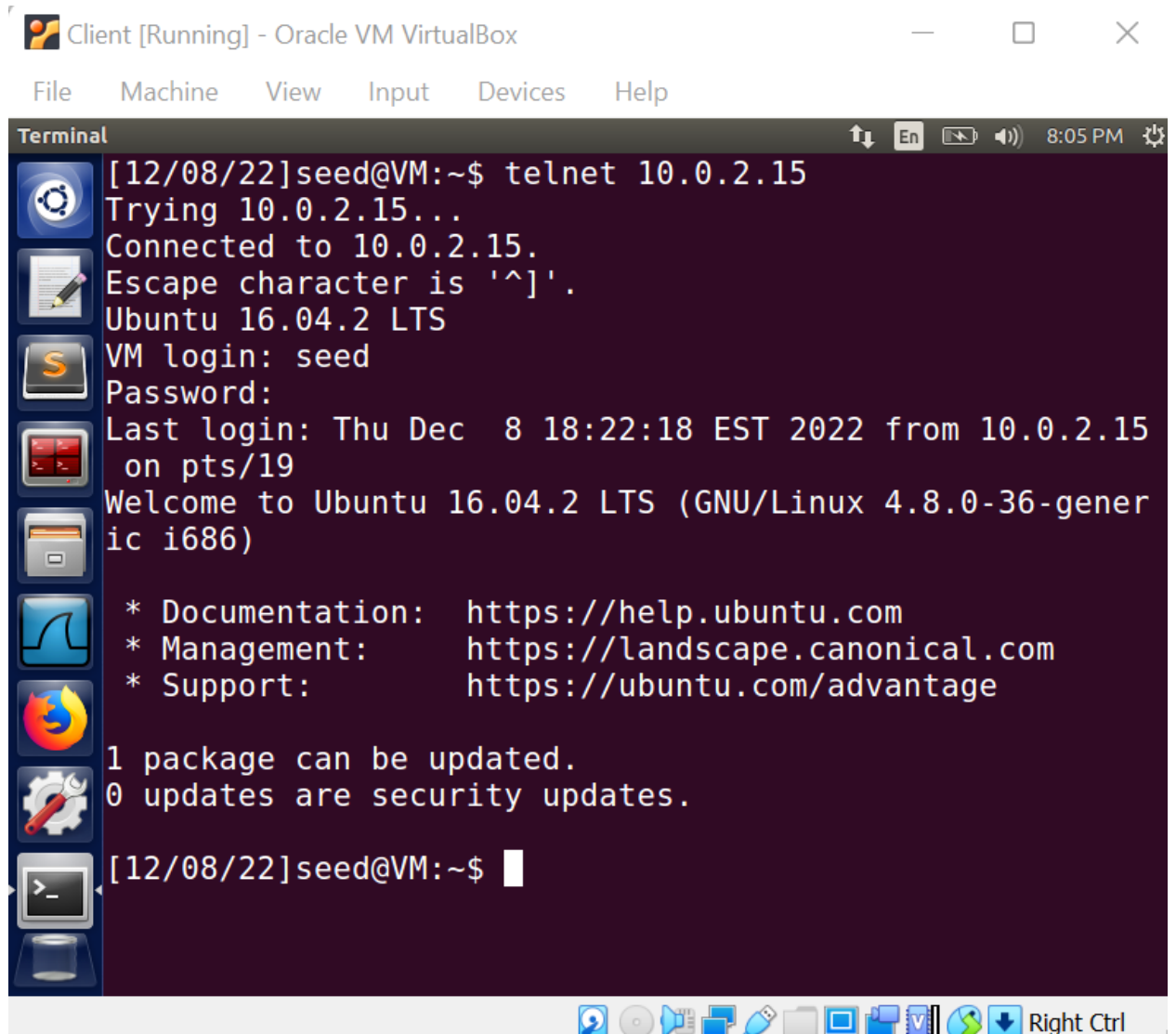


The image shows a screenshot of a VirtualBox window titled "Server [Running] - Oracle VM VirtualBox". The window contains a terminal window with a dark background and a light blue sidebar on the left. The terminal displays the following text:

```
[12/08/22]seed@VM:~$ sudo sysctl -a | grep cookie
net.ipv4.tcp_syncookies = 1
sysctl: reading key "net.ipv6.conf.all.stable_secret"
sysctl: reading key "net.ipv6.conf.default.stable_secret"
sysctl: reading key "net.ipv6.conf.enp0s3.stable_secret"
sysctl: reading key "net.ipv6.conf.lo.stable_secret"
[12/08/22]seed@VM:~$
[12/08/22]seed@VM:~$
[12/08/22]seed@VM:~$
[12/08/22]seed@VM:~$
[12/08/22]seed@VM:~$
[12/08/22]seed@VM:~$
[12/08/22]seed@VM:~$
[12/08/22]seed@VM:~$
[12/08/22]seed@VM:~$
[12/08/22]seed@VM:~$
[12/08/22]seed@VM:~$
[12/08/22]seed@VM:~$
[12/08/22]seed@VM:~$
[12/08/22]seed@VM:~$
```

The terminal window has a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". The status bar at the bottom of the terminal shows "8:03 PM" and a "Right Ctrl" button. The sidebar on the left contains icons for various applications, including a terminal, a file manager, a web browser, and a settings application.

Figure 3: checking SYNC cookie which is 1



The screenshot shows a VirtualBox window titled "Client [Running] - Oracle VM VirtualBox". Inside the window is a terminal window titled "Terminal". The terminal output shows a telnet connection from a client to a server at 10.0.2.15. The client is identified as "seed@VM". The server is identified as "Ubuntu 16.04.2 LTS". The user "seed" logs in with the password "seed". The last login was on Thursday, December 8, 2022, at 18:22:18 EST from 10.0.2.15 on pts/19. The terminal also displays the Ubuntu logo, the version number "16.04.2 LTS", and the kernel version "GNU/Linux 4.8.0-36-generic i686". The terminal also shows the documentation, management, and support URLs for Ubuntu. The terminal also shows the update status: "1 package can be updated. 0 updates are security updates." The terminal prompt is "[12/08/22]seed@VM:~\$".

```
[12/08/22]seed@VM:~$ telnet 10.0.2.15
Trying 10.0.2.15...
Connected to 10.0.2.15.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Dec  8 18:22:18 EST 2022 from 10.0.2.15
on pts/19
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.

[12/08/22]seed@VM:~$
```

Figure 4 Client connected to Server's Telnet connection

3. The SYN Flood attack was successful when the SYN Cookie was disabled. The SYN Flood assault, however, failed when the SYN Cookie was activated. There are a lot of half-opened SYN RECV connections because the attacker is using the netwox tool to conduct a SYN Flood attack by sending a lot of SYN packets and not responding to the server's SYN/ACK packets. We receive "unable to connect to remote host" when the client computer attempts to connect to the server's telnet connection because the server stops accepting incoming connections once the maximum number is reached.

Additionally, the connection will be successful if the client machine attempts to connect to the server right after the attack begins because the server has not yet reached its maximum capacity to reject incoming connections. However, after a while, the server can no longer maintain the resources allocated to partially opened connections due to its maximum capacity, and so it rejects the initiated telnet connection.

When the SYN Cookie is disabled, this occurs. However, when enabled, the SYN Cookie enables a server to keep connections open even when the SYN queue becomes overloaded. A SYN queue entry is encoded into the sequence number sent in the SYN/ACK response rather than being stored alongside other connections. The information encoded in the TCP sequence number can be used by the server to reconstruct the SYN queue entry and carry on with the connection as usual if the server then receives a subsequent ACK response from the client with the incremental sequence number.

### **References:**

PURPLESEC(2022, Feb 28).How To Prevent A SYN Flood Attack - PurpleSec.<https://purplesec.us/prevent-syn-flood-attack/>

A10(2019, Oct 2).What are SYN Cookies and How are they Used? - A10 Networks.<https://www.a10networks.com/blog/what-are-syn-cookies-and-how-are-they-used/>