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

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.

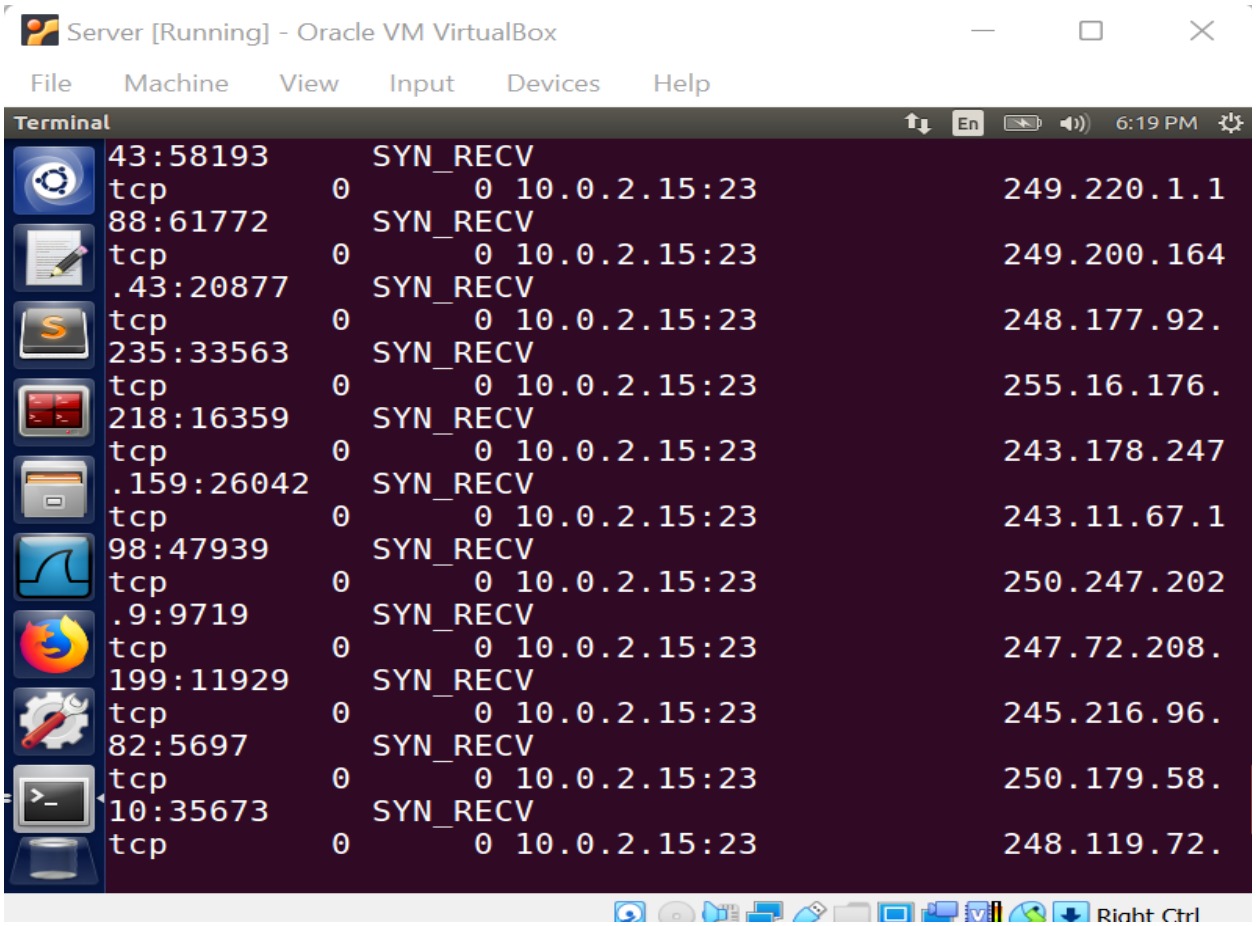

Figure 1. SYN_RECV status of server

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

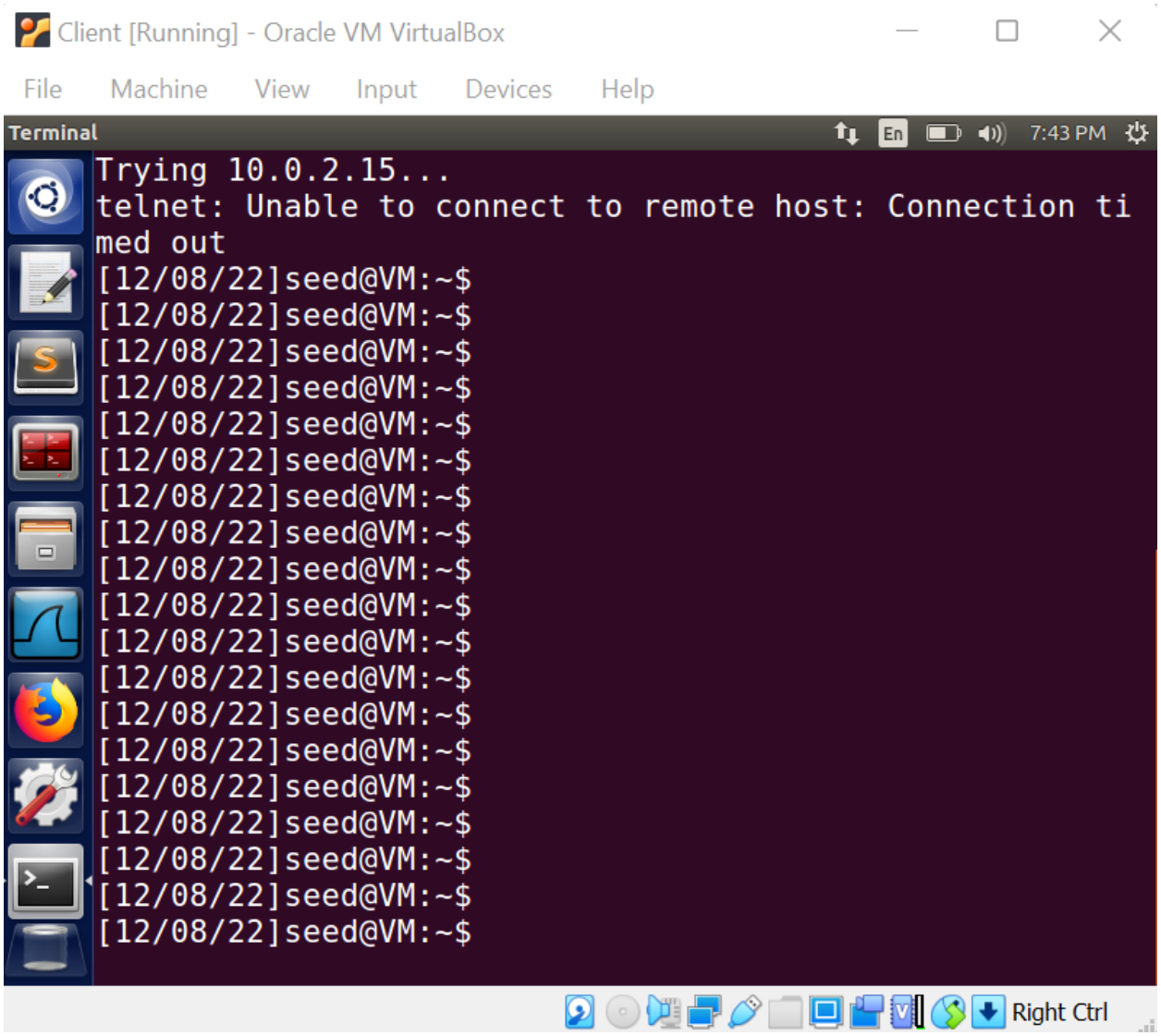

Figure 2 Client is unable to establish a Telnet connection with the server

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.

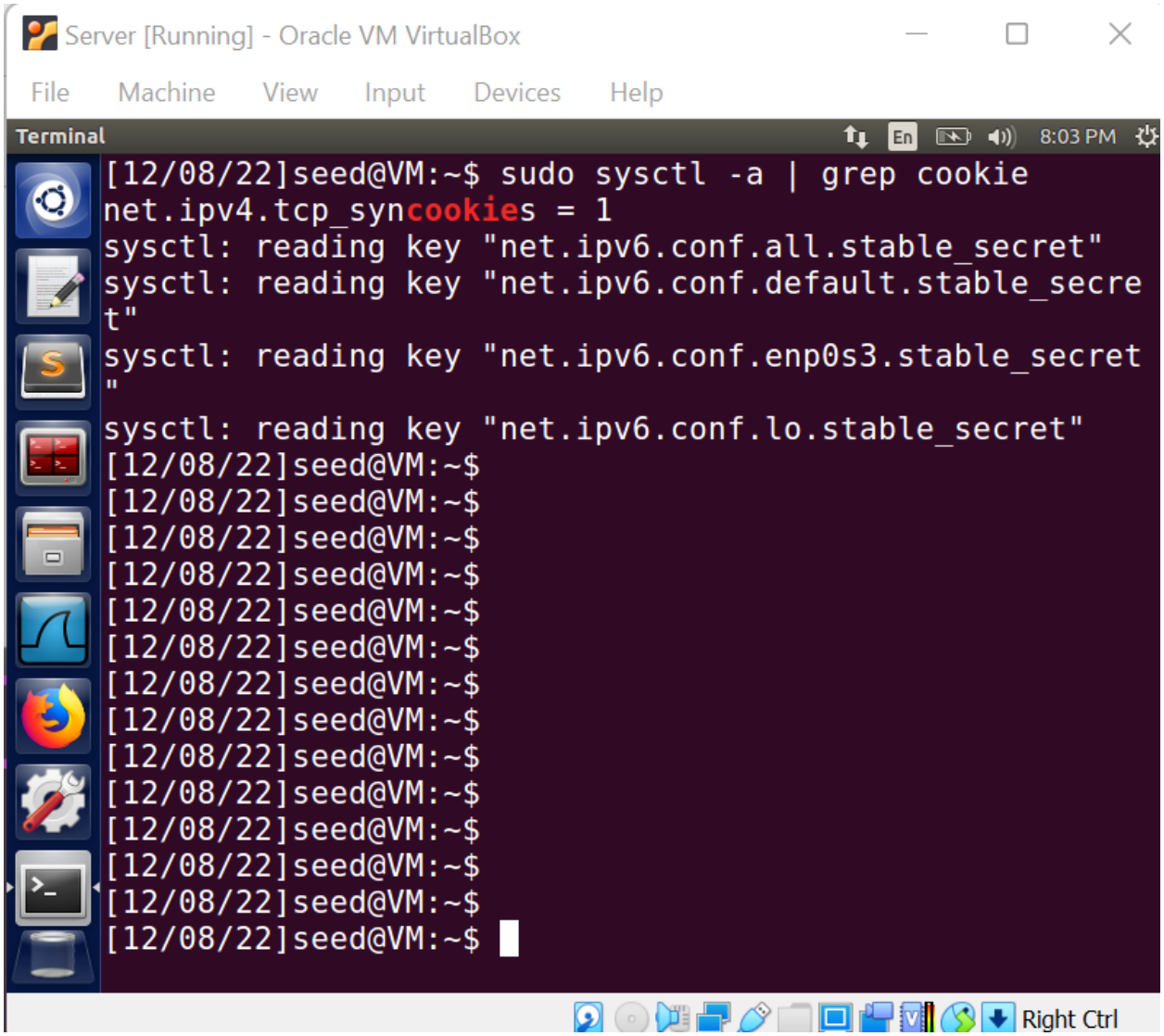

Figure 3: checking SYNC cookie which is 1

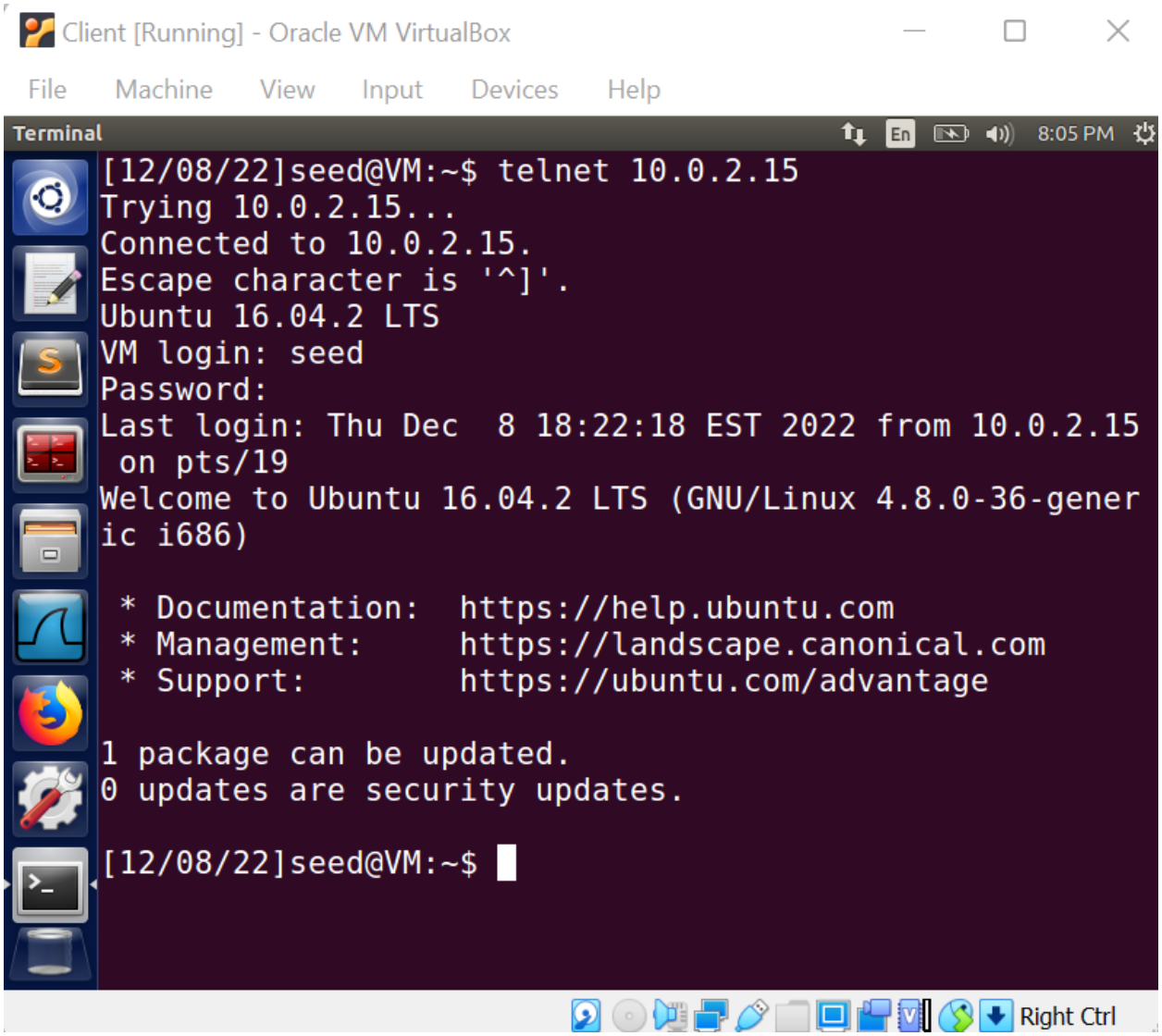

Figure 4 Client connected to Server's Telnet connection

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/