

CS5460 –Assignment 6



April 24, 2016

Varun GATTu

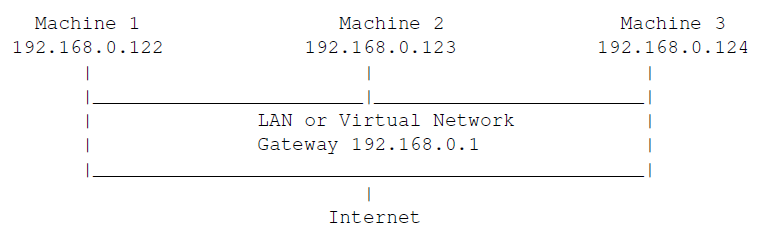
A02092613

**Attack Lab: Attacks on TCP/IP Protocols**

**2. Lab Environment**

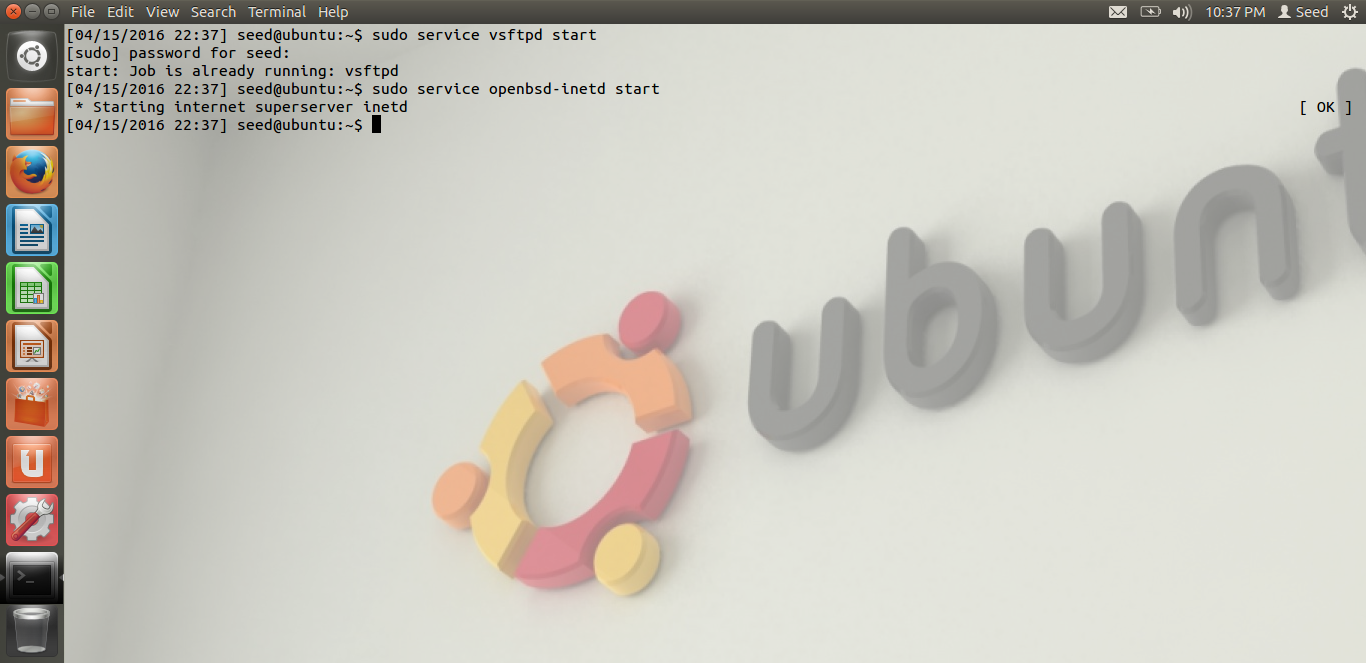
**2.1. Environment Setup**

For this assignment, I have cloned two VM’s as shown in the following image:



The IP addresses were: 192.168.56.101, 192.168.56.102 and 192.168.56.103 with the network 192.168.56.255 and server address 192.168.56.100.

The next task involved enabling the FTP and Telnet Servers like the follows:



**3. Lab Tasks**

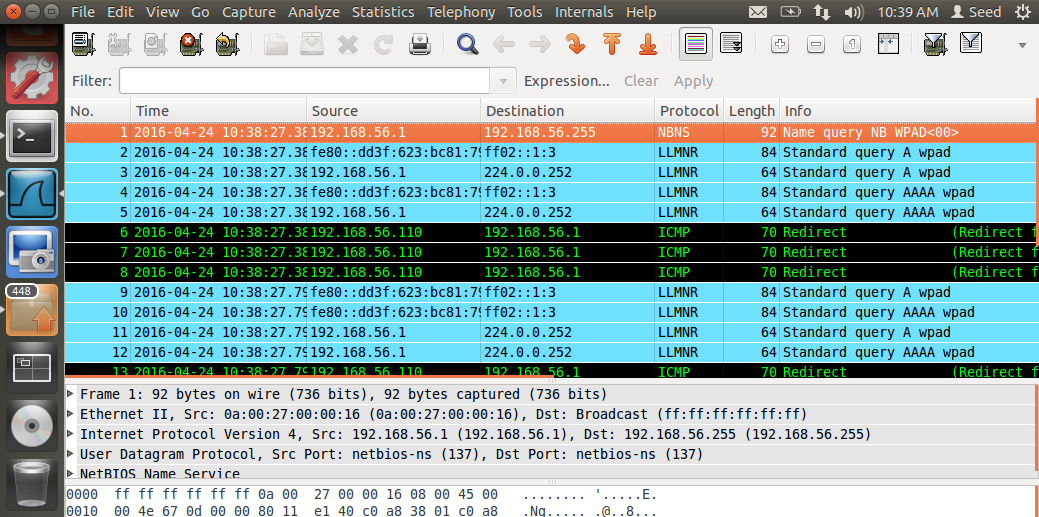
**3.2 Task (2): ICMP Redirect Attack**

Here, I used the netwox 86 command to redirect the ICMP messages and spoof with a different

IP address and modify the victim’s routing table as follows:

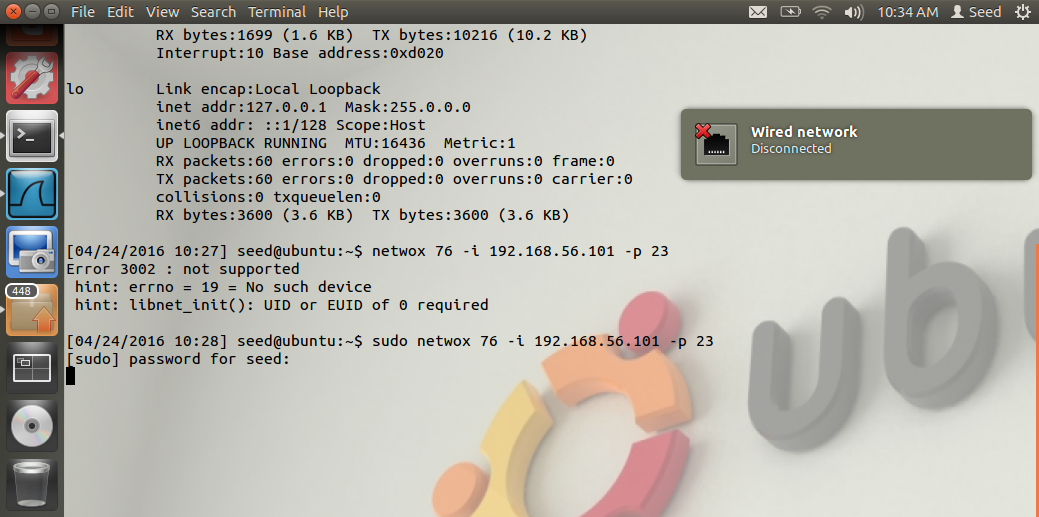


We can now verify the activity using Wireshark.

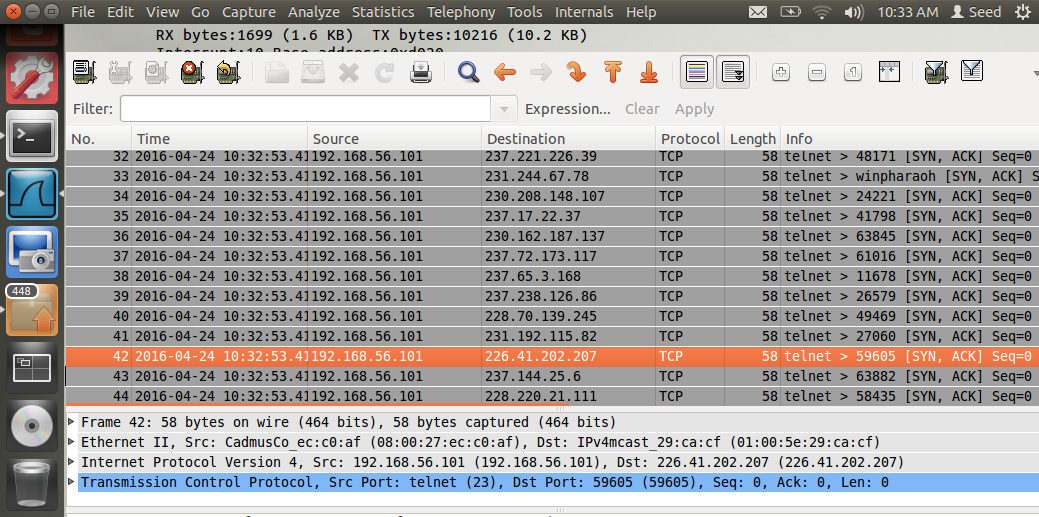


**3.3 Task (3): SYN Flooding Attack**

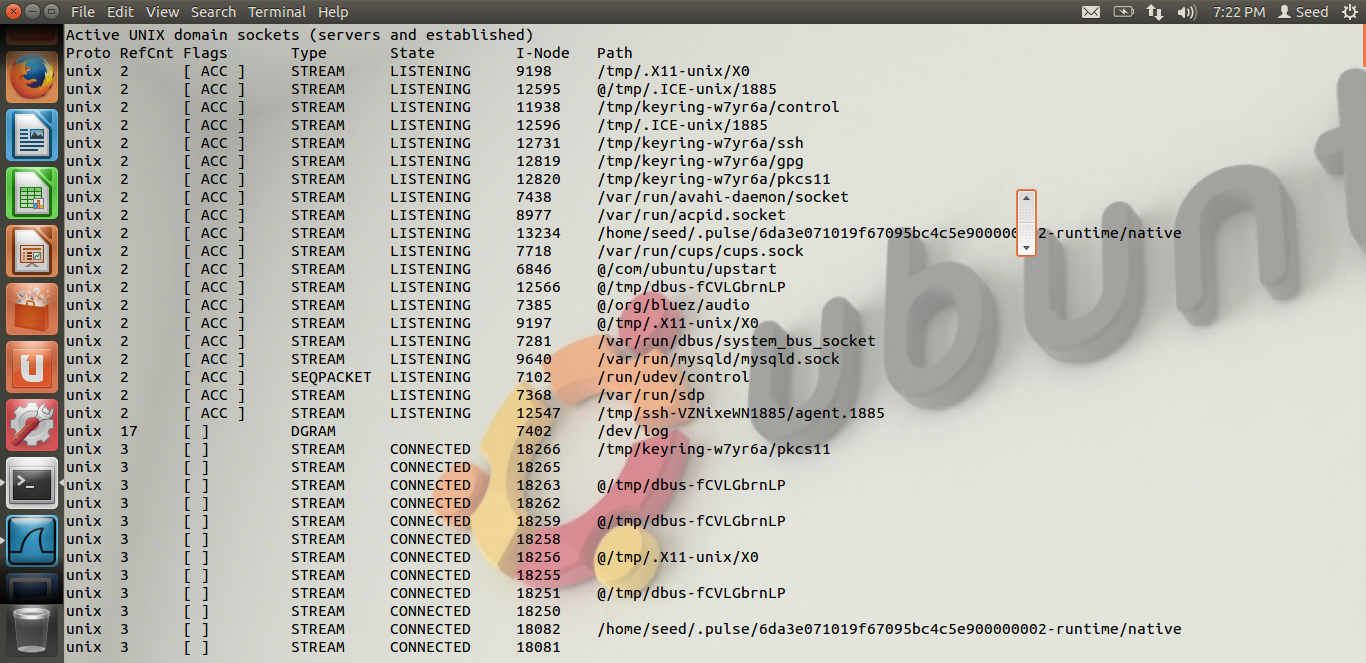
Here, I used the netwox 76 command to attack an IP on the TCP port which is 23. This causes DOS attack on the target machine to use up its queue and not have a 3 way handshake.



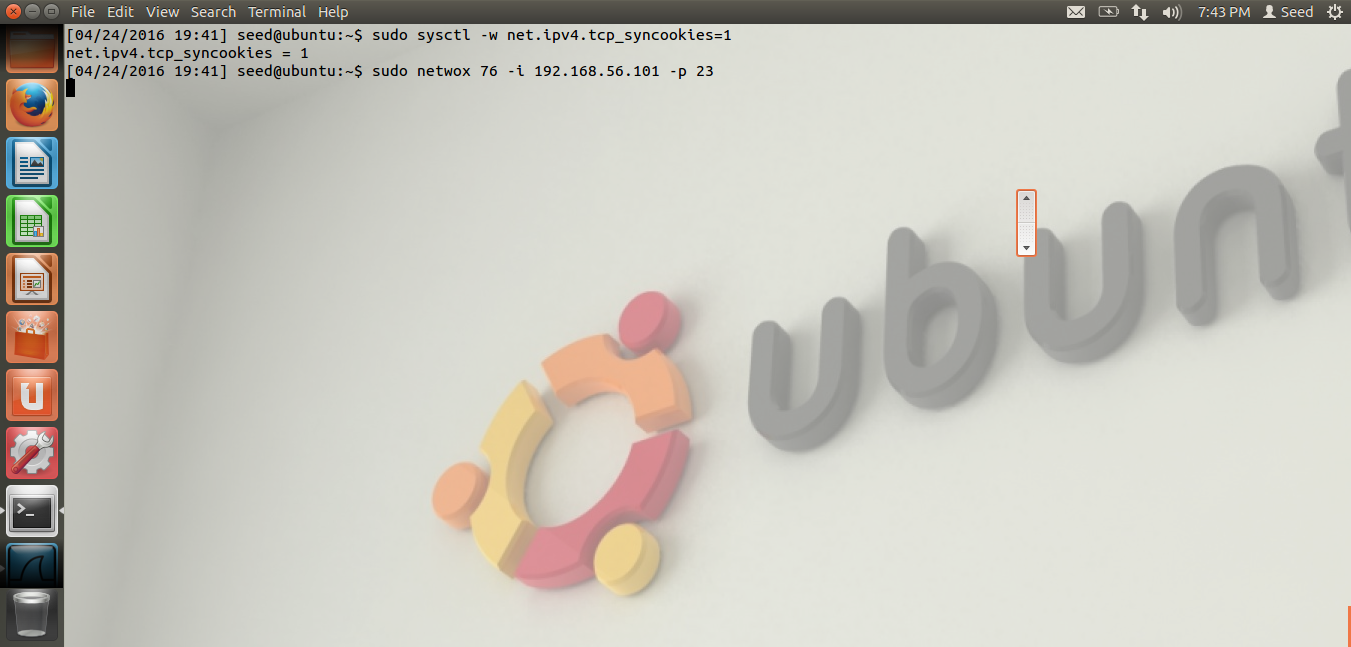
The Wireshark trace can be seen here:

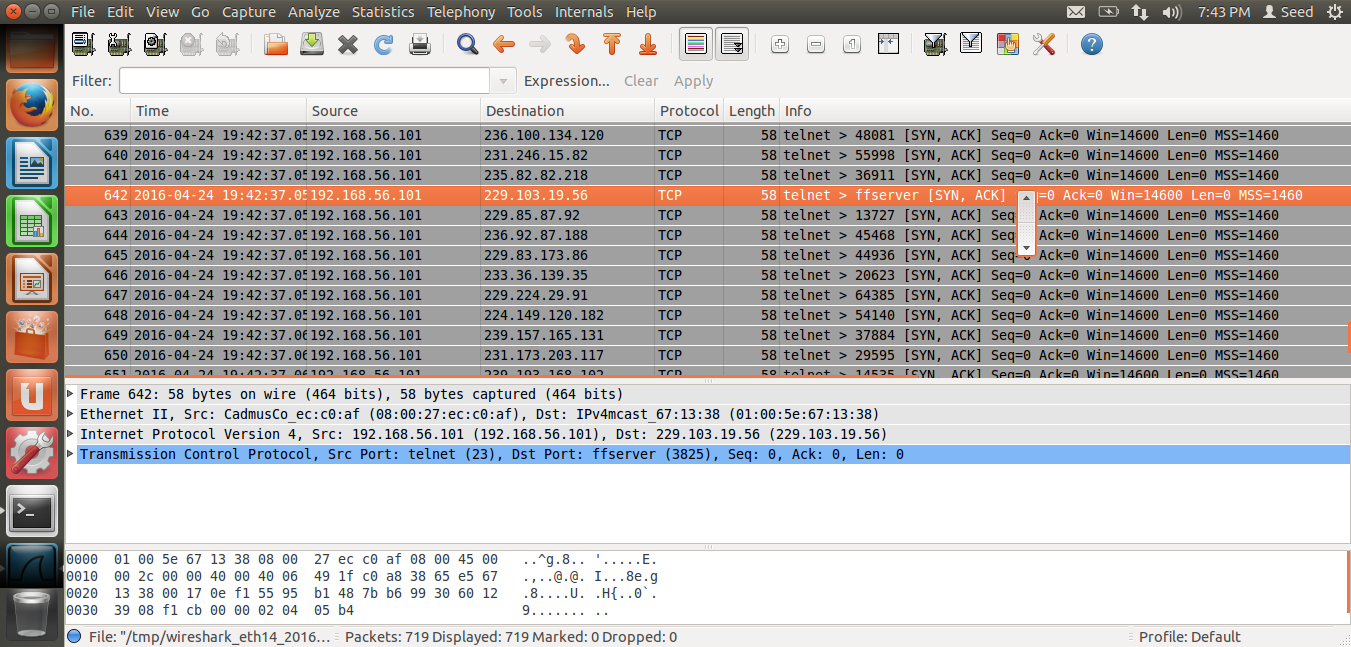


The output of netstat-na is as follows:



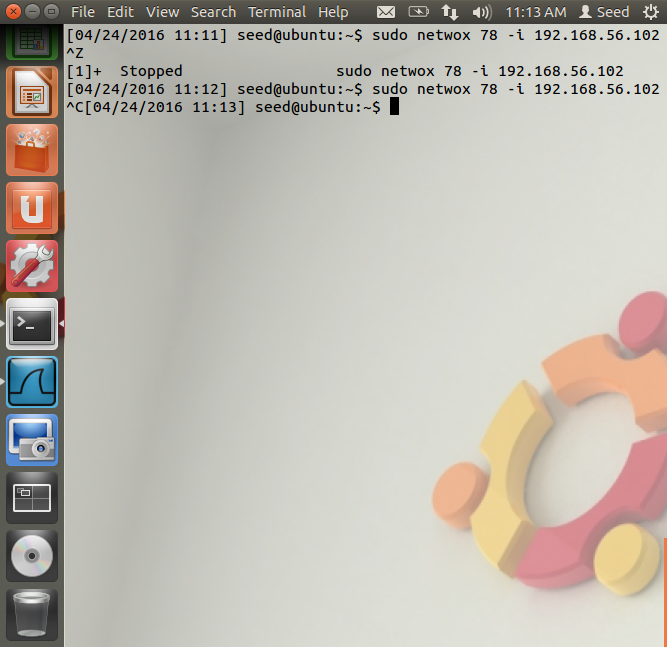
Now, I have made the syncookies as one and tried following the same steps again.

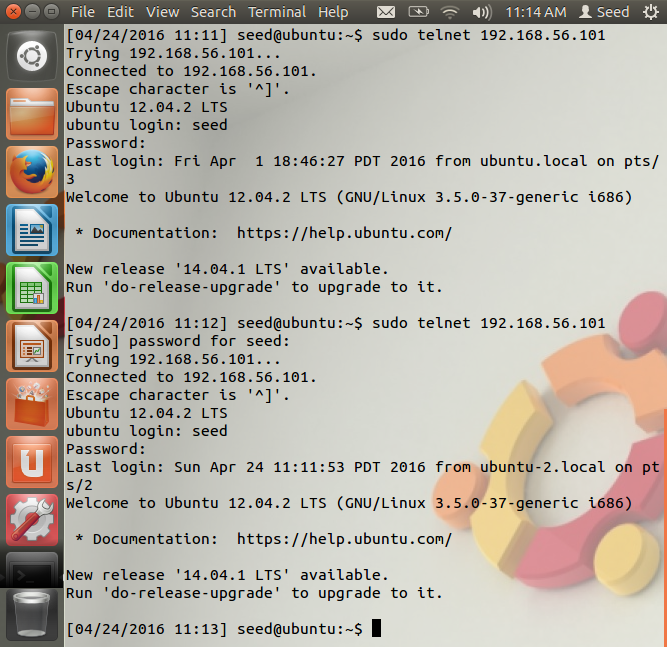




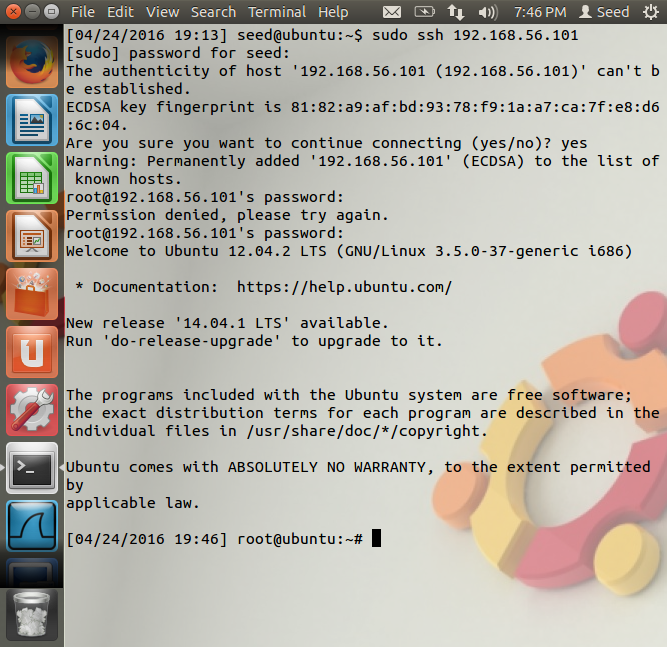
**3.4 Task 4: TCP RST Attacks on telnet and SSH connections**

Here, we use two virtual machines to capture the activity. The first machine will use the netwox command 78 with the second machines IP address. Now, when the connection is open, we telnet the first machines IP address from the second one to raise a new connection. When we stop the activity in the first machine, we can see that the second machine’s activity completely stops.





Now, I have tried to use SSH instead of telnet and found the output as follows:



SSH has some additional authentication before trying to login to the other device.