**NED University of Engineering and Technology**
**Department of Computer and Information Systems Engineering**

# Lab 4

**Sheikh Muhammad Farjad**
**CS-16059**
**Section A**
**Batch 2016-17**

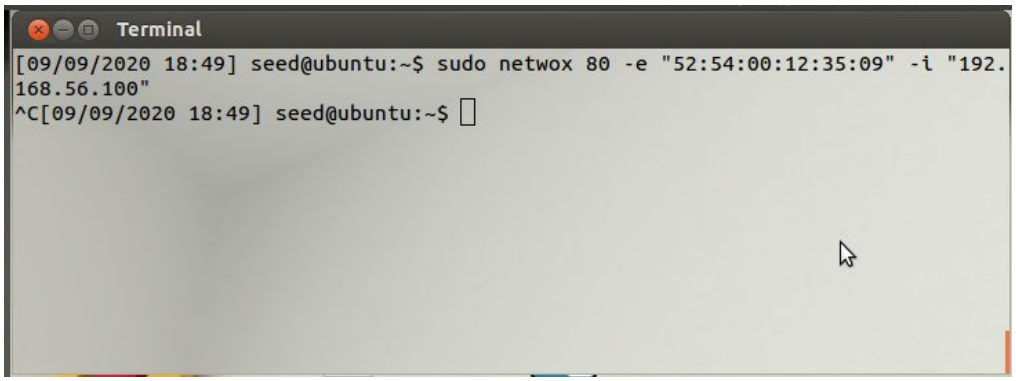
**Course Instructor: Sir Umar Iftikhar**
**Computer Systems Security**

| Virtual Machine | IP Address |
|---|---|
| VM1 | 192.168.56.101 |
| VM2 | 192.168.56.103 |

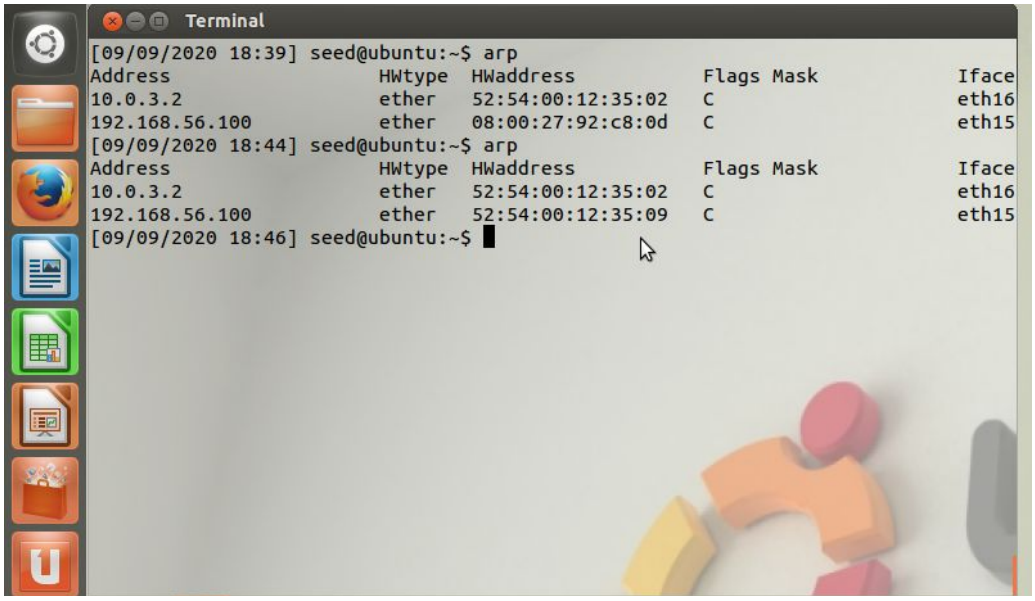
# Task (1): ARP cache poisoning

In this task, netwox utility was used in VM1 for poisoning the ARP table of VM2 with the manipulated MAC address against the entry of 192.168.56.100..

**VM1:**




**VM2:**

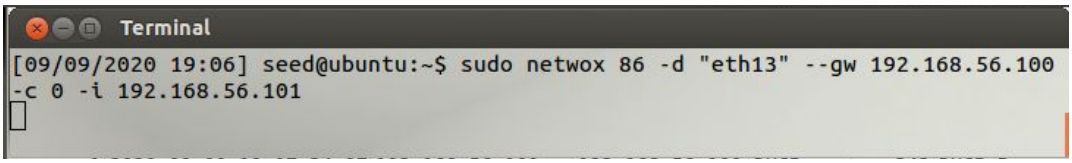


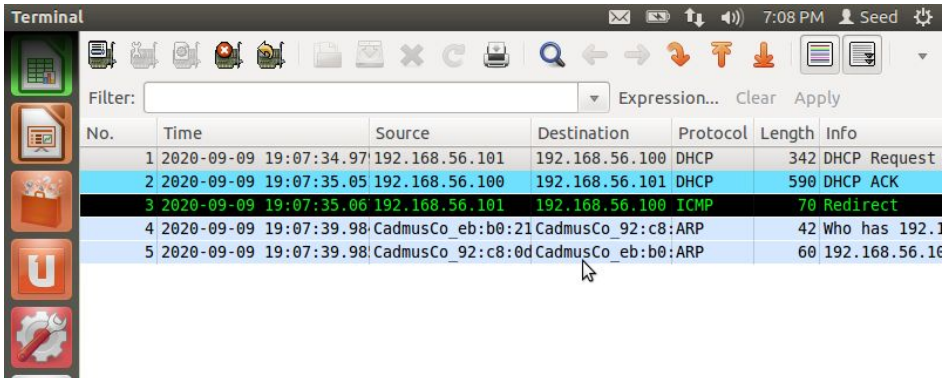
The first arp command was prior to executing netwox command in VM1. After executing the netwox command in VM1, the modified arp table was observed by re-entering the arp command in VM2. A different MAC address (HWaddress) can be observed against the entry of 192.168.56.100.

# Task (2): ICMP Redirect Attack

In this task, netwox command was used in VM1 for transmitting the ICMP redirect message to the gateway 192.168.56.100. The evidence of the attack can also be observed in the screenshot of wireshark utility.

**VM1:**

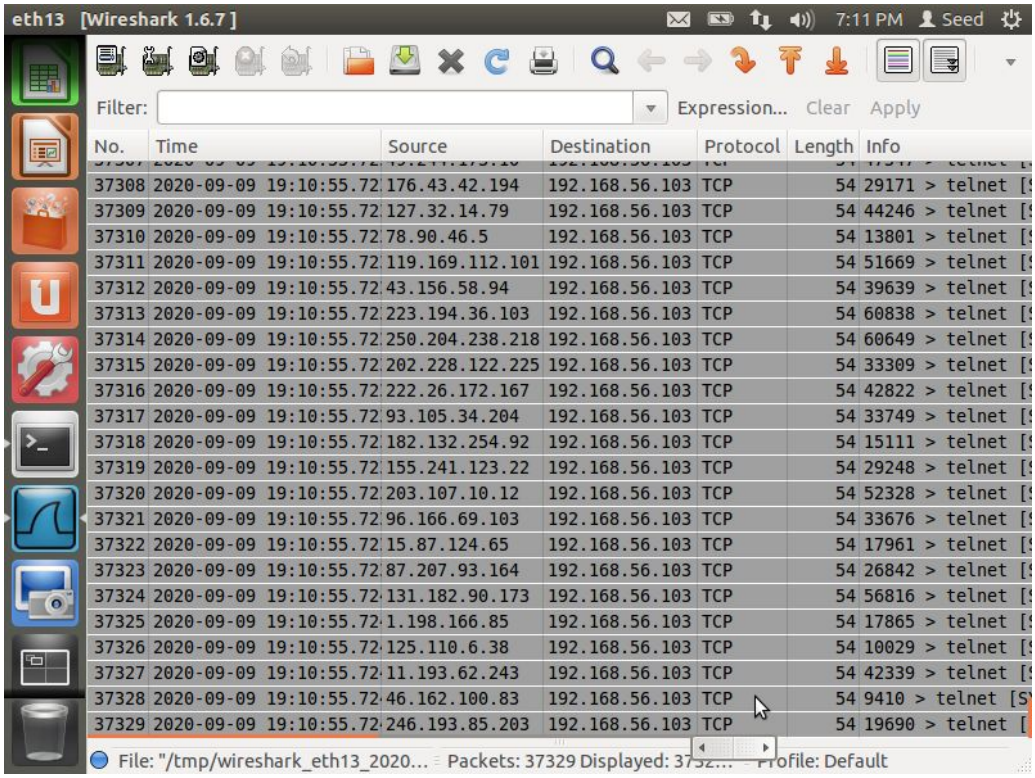



# Task (3): SYN Flooding Attack

In this task, netwox command was used in VM1 for transmitting the SYN flood to VM2 (192.168.56.103). While executing this attack, wireshark utility was also run for capturing the packets. Wireshark reported the transmission of bulk of packets towards VM2.

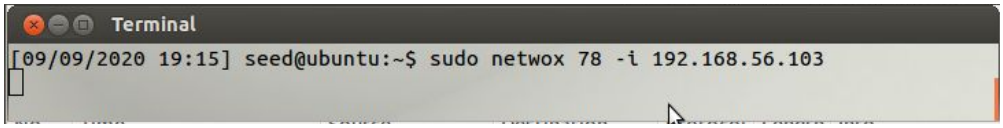
**VM1:**




# Task (4): TCP RST Attacks on telnet and ssh Connections

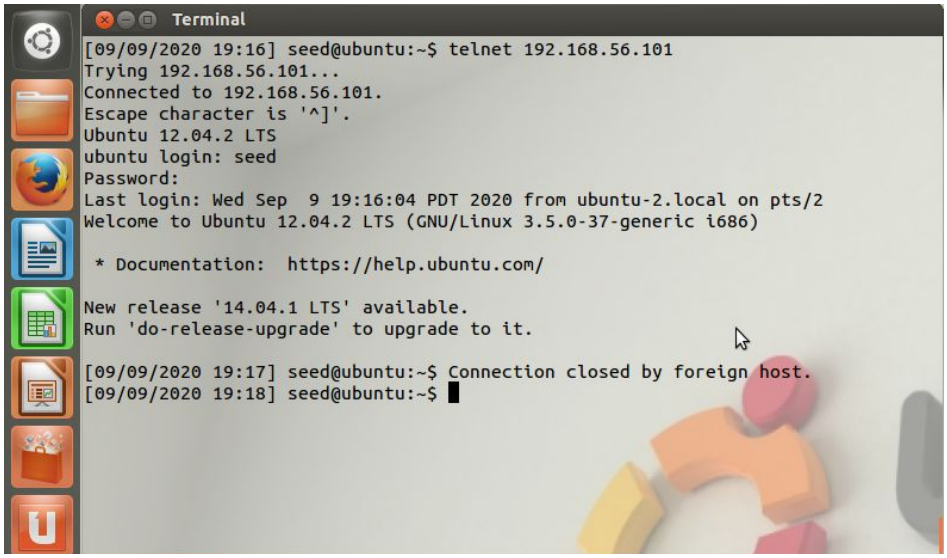
In this task, netwox command was used in VM1 for executing TCP RST attack that breaks or aborts the TCP connection. This attack was executed in two scenarios: telnet and ssh. The VM2 was used for establishing the telnet and ssh connection to VM1. After establishing the connection, netwox command was executed in VM1, which broke the connection by resetting the connection.

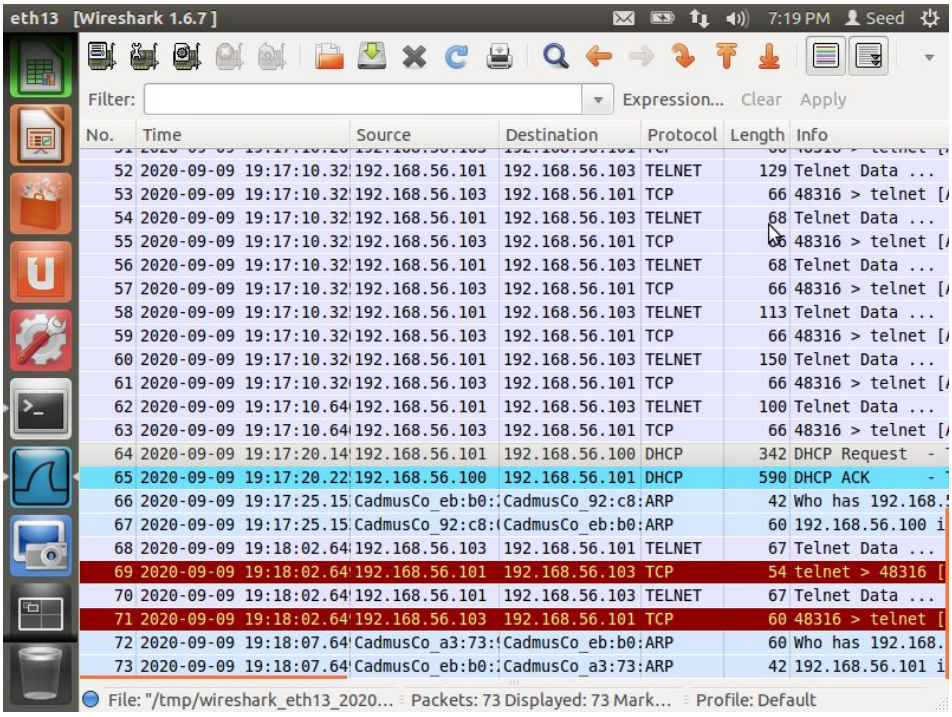
**VM1:**



# Telnet:

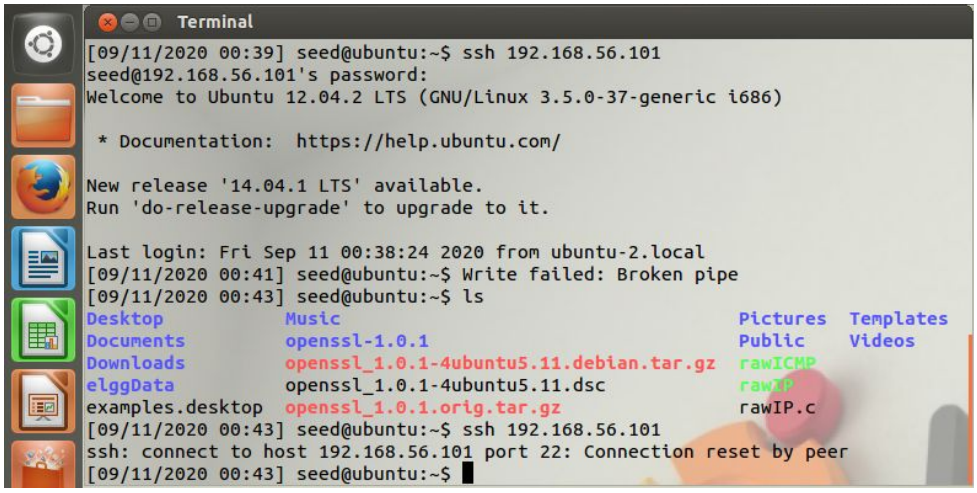
## VM2:

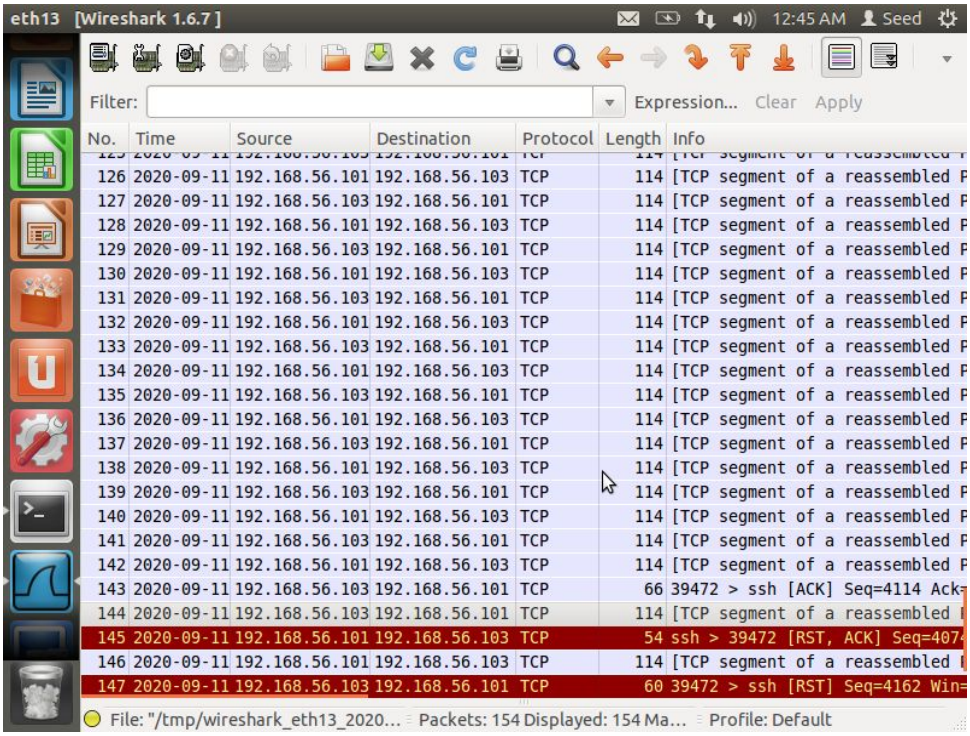

Terminal
[09/09/2020 19:16] seed@ubuntu:~$ telnet 192.168.56.101
Trying 192.168.56.101...
Connected to 192.168.56.101.
Escape character is '^]'.
Ubuntu 12.04.2 LTS
ubuntu login: seed
Password:
Last login: Wed Sep 9 19:16:04 PDT 2020 from ubuntu-2.local on pts/2
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)
* Documentation: https://help.ubuntu.com/
New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
[09/09/2020 19:17] seed@ubuntu:~$ Connection closed by foreign host.
[09/09/2020 19:18] seed@ubuntu:~$


eth13 [Wireshark 1.6.7]
7:19 PM
Seed
Filter:
Expression...
Clear
Apply
No. Time Source Destination Protocol Length Info
52 2020-09-09 19:17:10.32 192.168.56.101 192.168.56.103 TELNET 129 Telnet Data ...
53 2020-09-09 19:17:10.32 192.168.56.103 192.168.56.101 TCP 66 48316 > telnet [
54 2020-09-09 19:17:10.32 192.168.56.101 192.168.56.103 TELNET 68 Telnet Data ...
55 2020-09-09 19:17:10.32 192.168.56.103 192.168.56.101 TCP 66 48316 > telnet [
56 2020-09-09 19:17:10.32 192.168.56.101 192.168.56.103 TELNET 68 Telnet Data ...
57 2020-09-09 19:17:10.32 192.168.56.103 192.168.56.101 TCP 66 48316 > telnet [
58 2020-09-09 19:17:10.32 192.168.56.101 192.168.56.103 TELNET 113 Telnet Data ...
59 2020-09-09 19:17:10.32 192.168.56.103 192.168.56.101 TCP 66 48316 > telnet [
60 2020-09-09 19:17:10.32 192.168.56.101 192.168.56.103 TELNET 150 Telnet Data ...
61 2020-09-09 19:17:10.32 192.168.56.103 192.168.56.101 TCP 66 48316 > telnet [
62 2020-09-09 19:17:10.64 192.168.56.101 192.168.56.103 TELNET 100 Telnet Data ...
63 2020-09-09 19:17:10.64 192.168.56.103 192.168.56.101 TCP 66 48316 > telnet [
64 2020-09-09 19:17:20.14 192.168.56.101 192.168.56.100 DHCP 342 DHCP Request
65 2020-09-09 19:17:20.22 192.168.56.100 192.168.56.101 DHCP 590 DHCP ACK
66 2020-09-09 19:17:25.15 CadmusCo_eb:b0: CadmusCo_92:c8: ARP 42 Who has 192.168.
67 2020-09-09 19:17:25.15 CadmusCo_92:c8: CadmusCo_eb:b0: ARP 60 192.168.56.100 i
68 2020-09-09 19:18:02.64 192.168.56.103 192.168.56.101 TELNET 67 Telnet Data ...
69 2020-09-09 19:18:02.64 192.168.56.101 192.168.56.103 TCP 54 telnet > 48316 [
70 2020-09-09 19:18:02.64 192.168.56.101 192.168.56.103 TELNET 67 Telnet Data ...
71 2020-09-09 19:18:02.64 192.168.56.103 192.168.56.101 TCP 60 48316 > telnet [
72 2020-09-09 19:18:07.64 CadmusCo_a3:73: CadmusCo_eb:b0: ARP 60 Who has 192.168.
73 2020-09-09 19:18:07.64 CadmusCo_eb:b0: CadmusCo_a3:73: ARP 42 192.168.56.101 i
File: "/tmp/wireshark_eth13_2020... Packets: 73 Displayed: 73 Mark... Profile: Default

## SSH:

### VM2:


Terminal
[09/11/2020 00:39] seed@ubuntu:~$ ssh 192.168.56.101
seed@192.168.56.101's password:
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic i686)
* Documentation: https://help.ubuntu.com/
New release '14.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
Last login: Fri Sep 11 00:38:24 2020 from ubuntu-2.local
[09/11/2020 00:41] seed@ubuntu:~$ Write failed: Broken pipe
[09/11/2020 00:43] seed@ubuntu:~$ ls
Desktop Music Pictures Templates
Documents openssl-1.0.1 Public Videos
Downloads openssl_1.0.1-4ubuntu5.11.debian.tar.gz rawICMP
elggData openssl_1.0.1-4ubuntu5.11.dsc rawIP
examples.desktop openssl_1.0.1.orig.tar.gz rawIP.c
[09/11/2020 00:43] seed@ubuntu:~$ ssh 192.168.56.101
ssh: connect to host 192.168.56.101 port 22: Connection reset by peer
[09/11/2020 00:43] seed@ubuntu:~$


eth13 [Wireshark 1.6.7]
12:45 AM Seed
Filter:
Expression... Clear Apply
No. Time Source Destination Protocol Length Info
126 2020-09-11 192.168.56.101 192.168.56.103 TCP 114 [TCP segment of a reassembled P
127 2020-09-11 192.168.56.103 192.168.56.101 TCP 114 [TCP segment of a reassembled P
128 2020-09-11 192.168.56.101 192.168.56.103 TCP 114 [TCP segment of a reassembled P
129 2020-09-11 192.168.56.103 192.168.56.101 TCP 114 [TCP segment of a reassembled P
130 2020-09-11 192.168.56.101 192.168.56.103 TCP 114 [TCP segment of a reassembled P
131 2020-09-11 192.168.56.103 192.168.56.101 TCP 114 [TCP segment of a reassembled P
132 2020-09-11 192.168.56.101 192.168.56.103 TCP 114 [TCP segment of a reassembled P
133 2020-09-11 192.168.56.103 192.168.56.101 TCP 114 [TCP segment of a reassembled P
134 2020-09-11 192.168.56.101 192.168.56.103 TCP 114 [TCP segment of a reassembled P
135 2020-09-11 192.168.56.103 192.168.56.101 TCP 114 [TCP segment of a reassembled P
136 2020-09-11 192.168.56.101 192.168.56.103 TCP 114 [TCP segment of a reassembled P
137 2020-09-11 192.168.56.103 192.168.56.101 TCP 114 [TCP segment of a reassembled P
138 2020-09-11 192.168.56.101 192.168.56.103 TCP 114 [TCP segment of a reassembled P
139 2020-09-11 192.168.56.103 192.168.56.101 TCP 114 [TCP segment of a reassembled P
140 2020-09-11 192.168.56.101 192.168.56.103 TCP 114 [TCP segment of a reassembled P
141 2020-09-11 192.168.56.103 192.168.56.101 TCP 114 [TCP segment of a reassembled P
142 2020-09-11 192.168.56.101 192.168.56.103 TCP 114 [TCP segment of a reassembled P
143 2020-09-11 192.168.56.103 192.168.56.101 TCP 66 39472 > ssh [ACK] Seq=4114 Ack=
144 2020-09-11 192.168.56.103 192.168.56.101 TCP 114 [TCP segment of a reassembled
145 2020-09-11 192.168.56.101 192.168.56.103 TCP 54 ssh > 39472 [RST, ACK] Seq=407
146 2020-09-11 192.168.56.101 192.168.56.103 TCP 114 [TCP segment of a reassembled
147 2020-09-11 192.168.56.103 192.168.56.101 TCP 60 39472 > ssh [RST] Seq=4162 Win=
File: "/tmp/wireshark_eth13_2020... Packets: 154 Displayed: 154 Ma... Profile: Default

# Task (5): TCP RST Attacks on Video Streaming Applications

In this task, netwox command was run in VM1 for breaking the TCP connection established during a video streaming application. I executed this task in my Kali Linux machine. The screenshot of the wireshark can be observed below: