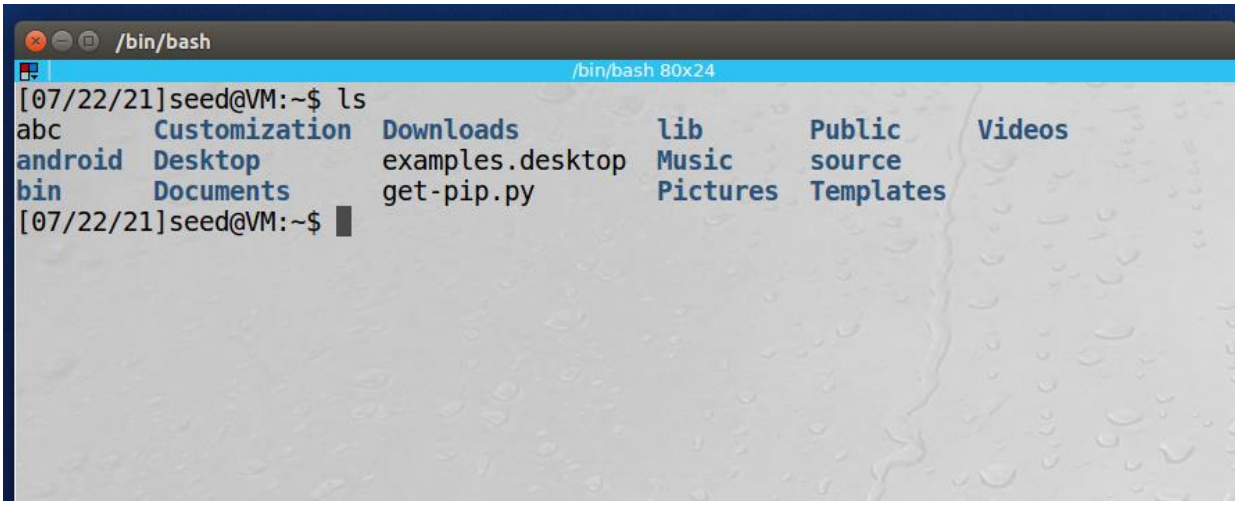
Roll : 1605043

ICMP Blind Connection–Reset + Blind throughput reduction attack against TCP

ICMP Blind Connection Reset Attack:

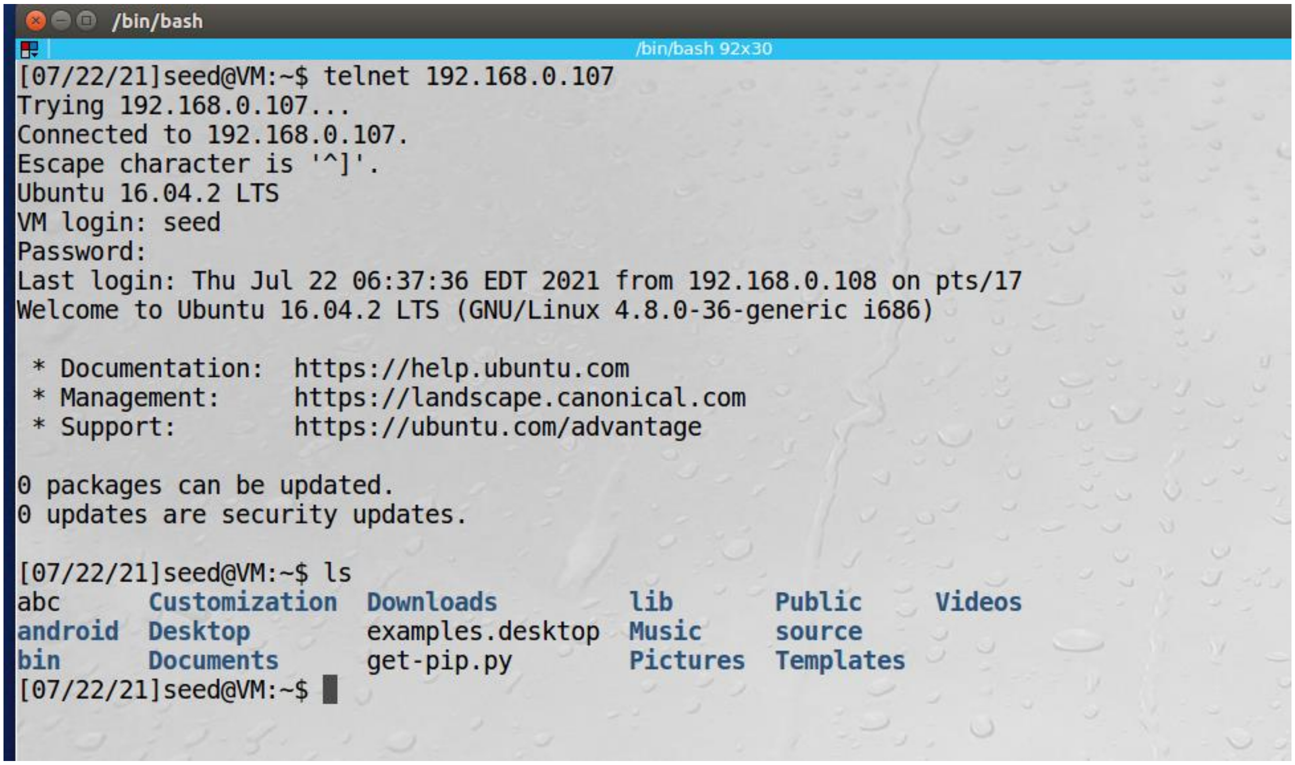
Step: 1- Establishing TCP connection between server and victim:

Firstly, a telnet connection was setup between the server and victim virtual machine. Telnet connection is based on TCP. The connection establishment is shown in the following screenshots.



```
[07/22/21]seed@VM:~$ ls
abc       Customization  Downloads         lib       Public     Videos
android   Desktop        examples.desktop  Music     source
bin       Documents      get-pip.py        Pictures  Templates
[07/22/21]seed@VM:~$ 
```

Screenshot: the server home directory



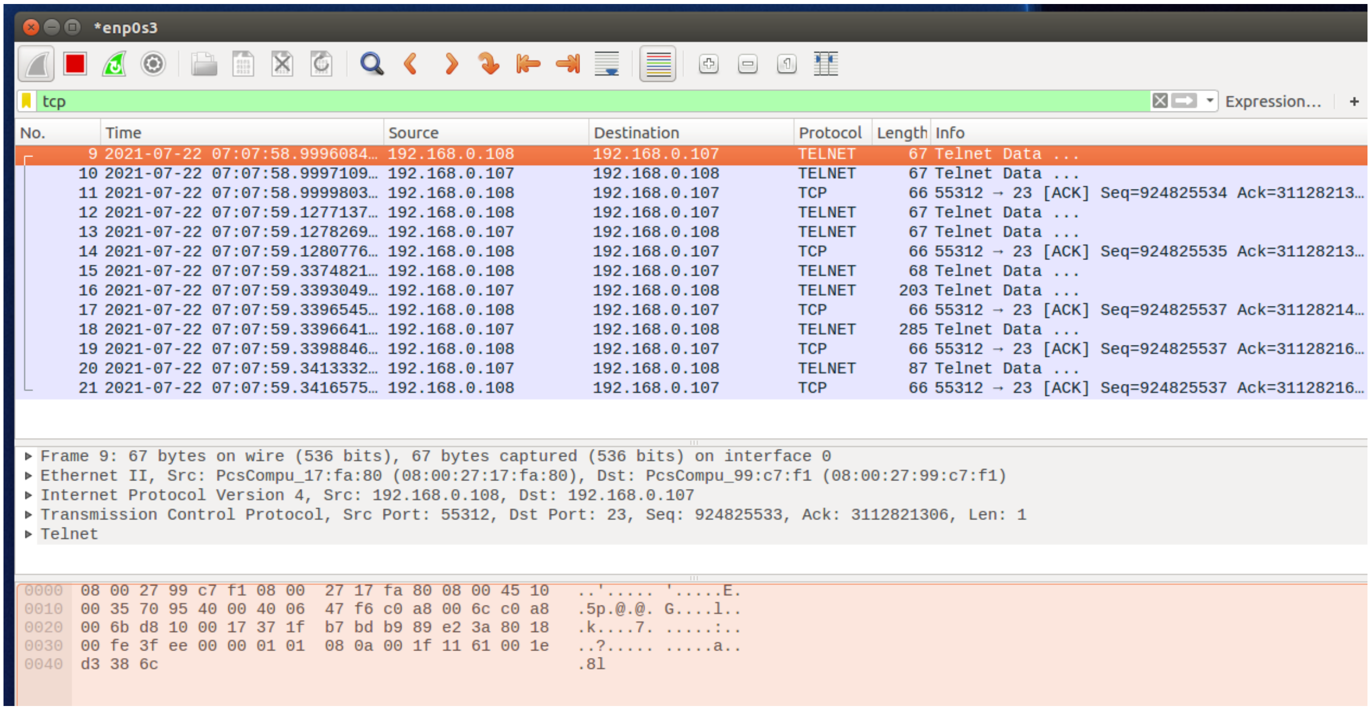
```
[07/22/21]seed@VM:~$ telnet 192.168.0.107
Trying 192.168.0.107...
Connected to 192.168.0.107.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Jul 22 06:37:36 EDT 2021 from 192.168.0.108 on pts/17
Welcome to Ubuntu 16.04.2 LTS (GNU/Linux 4.8.0-36-generic i686)

 * 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.

[07/22/21]seed@VM:~$ ls
abc      Customization  Downloads         lib       Public    Videos
android  Desktop        examples.desktop  Music     source
bin      Documents      get-pip.py        Pictures  Templates
[07/22/21]seed@VM:~$ 
```

Screenshot: Telnet(TCP) connection established from Victim to access Server home directory.



```
tcp
```

```
No.  Time                          Source          Destination     Protocol  Length Info
   9 2021-07-22 07:07:58.9996084…  192.168.0.108   192.168.0.107   TELNET       67 Telnet Data ...
  10 2021-07-22 07:07:58.9997109…  192.168.0.107   192.168.0.108   TELNET       67 Telnet Data ...
  11 2021-07-22 07:07:58.9999803…  192.168.0.108   192.168.0.107   TCP          66 55312 → 23 [ACK] Seq=924825534 Ack=31128213…
  12 2021-07-22 07:07:59.1277137…  192.168.0.108   192.168.0.107   TELNET       67 Telnet Data ...
  13 2021-07-22 07:07:59.1278269…  192.168.0.107   192.168.0.108   TELNET       67 Telnet Data ...
  14 2021-07-22 07:07:59.1280776…  192.168.0.108   192.168.0.107   TCP          66 55312 → 23 [ACK] Seq=924825535 Ack=31128213…
  15 2021-07-22 07:07:59.3374821…  192.168.0.108   192.168.0.107   TELNET       68 Telnet Data ...
  16 2021-07-22 07:07:59.3393049…  192.168.0.107   192.168.0.108   TELNET      203 Telnet Data ...
  17 2021-07-22 07:07:59.3396545…  192.168.0.108   192.168.0.107   TCP          66 55312 → 23 [ACK] Seq=924825537 Ack=31128214…
  18 2021-07-22 07:07:59.3396641…  192.168.0.107   192.168.0.108   TELNET      285 Telnet Data ...
  19 2021-07-22 07:07:59.3398846…  192.168.0.108   192.168.0.107   TCP          66 55312 → 23 [ACK] Seq=924825537 Ack=31128216…
  20 2021-07-22 07:07:59.3413332…  192.168.0.107   192.168.0.108   TELNET       87 Telnet Data ...
  21 2021-07-22 07:07:59.3416575…  192.168.0.108   192.168.0.107   TCP          66 55312 → 23 [ACK] Seq=924825537 Ack=31128216…
```

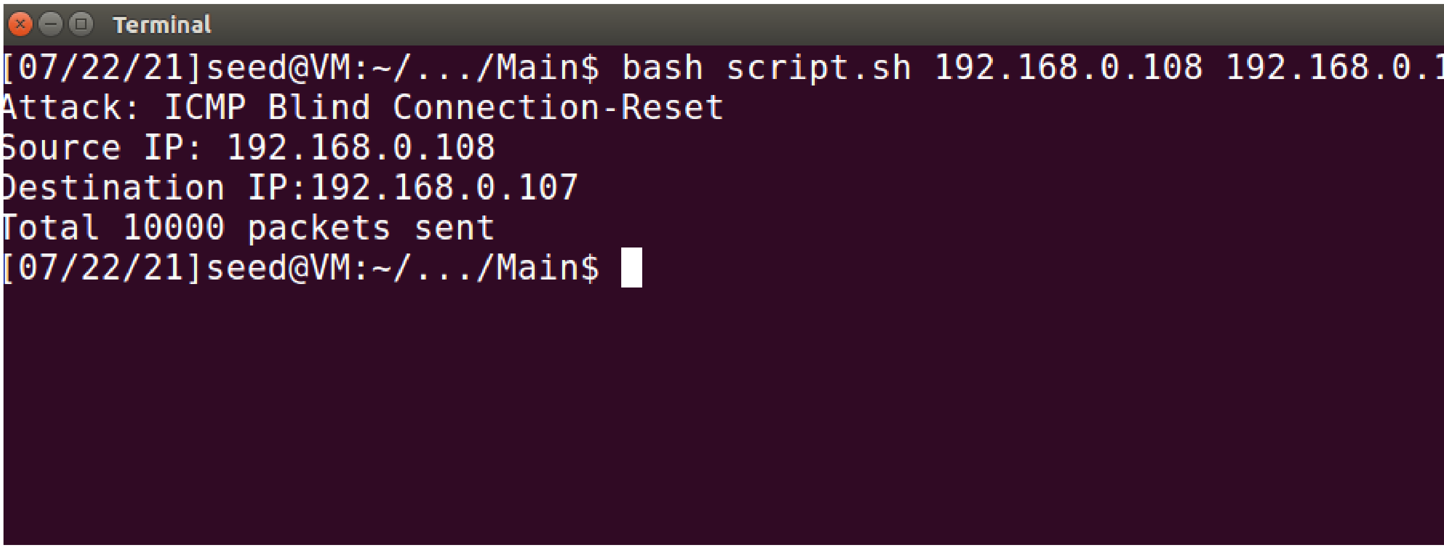
```
▸ Frame 9: 67 bytes on wire (536 bits), 67 bytes captured (536 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_17:fa:80 (08:00:27:17:fa:80), Dst: PcsCompu_99:c7:f1 (08:00:27:99:c7:f1)
▸ Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.107
▸ Transmission Control Protocol, Src Port: 55312, Dst Port: 23, Seq: 924825533, Ack: 3112821306, Len: 1
▸ Telnet
```

```
0000  08 00 27 99 c7 f1 08 00  27 17 fa 80 08 00 45 10   ..'..... '.....E.
0010  00 35 70 95 40 00 40 06  47 f6 c0 a8 00 6c c0 a8   .5p.@.@. G....l..
0020  00 6b d8 10 00 17 37 1f  b7 bd b9 89 e2 3a 80 18   .k....7. .....:..
0030  00 fe 3f ee 00 00 01 01  08 0a 00 1f 11 61 00 1e   ..?..... .....a..
0040  d3 38 6c                                           .8l
```

Screenshot: TCP packets received from victim to server.

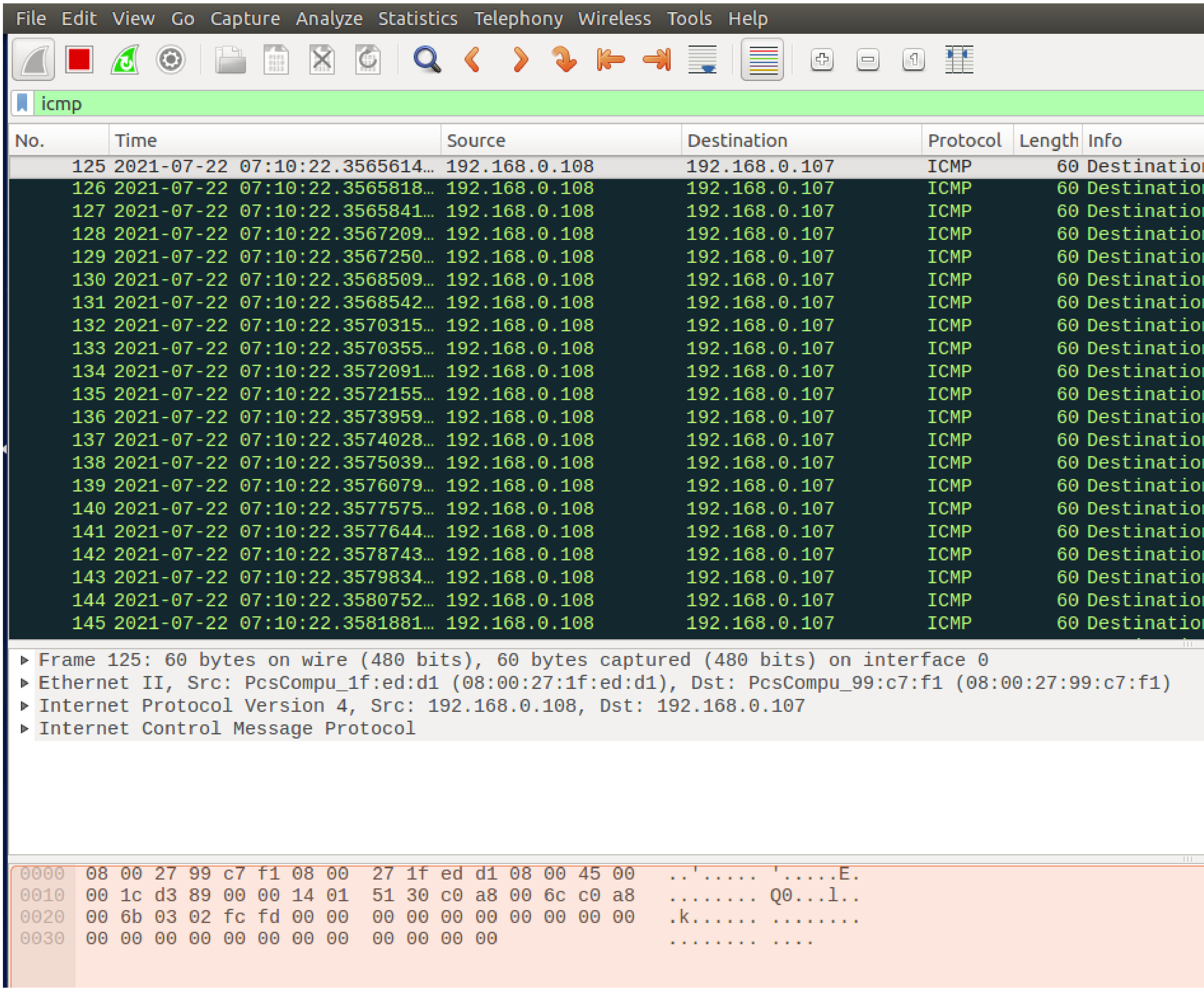
Step: 2-Perform the Blind Connection Reset attack from Attacker:

I used my C program to make modified ICMP packets as Hard error messages and send them to the Server, disguised as the Victim so that the TCP connection between them gets terminated. The program takes three command line arguments: 1. Source IP address, 2. Destination IP address, 3. Choice of attack. In the case of this attack the choice is 1. This following attack is performed as Type: 3, code: 2 ICMP message, which means “Protocol Unreachable”.



```
[07/22/21]seed@VM:~/.../Main$ bash script.sh 192.168.0.108 192.168.0.1
Attack: ICMP Blind Connection-Reset
Source IP: 192.168.0.108
Destination IP:192.168.0.107
Total 10000 packets sent
[07/22/21]seed@VM:~/.../Main$ 
```

Screenshot: Attacker performing attack 1.


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
icmp
```

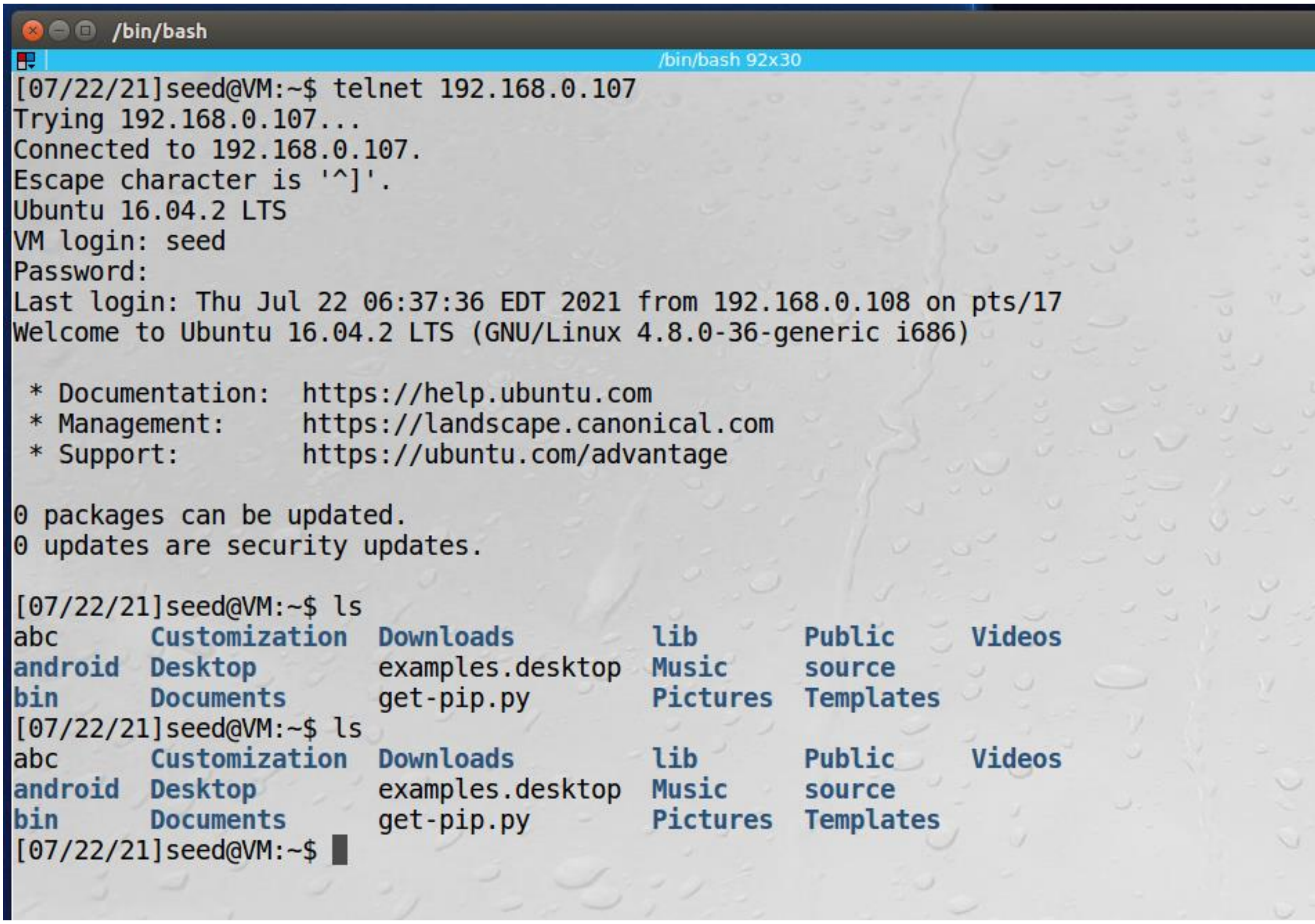
```
No.  Time                           Source          Destination     Protocol Length Info
 125 2021-07-22 07:10:22.3565614… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 126 2021-07-22 07:10:22.3565818… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 127 2021-07-22 07:10:22.3565841… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 128 2021-07-22 07:10:22.3567209… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 129 2021-07-22 07:10:22.3567250… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 130 2021-07-22 07:10:22.3568509… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 131 2021-07-22 07:10:22.3568542… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 132 2021-07-22 07:10:22.3570315… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 133 2021-07-22 07:10:22.3570355… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 134 2021-07-22 07:10:22.3572091… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 135 2021-07-22 07:10:22.3572155… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 136 2021-07-22 07:10:22.3573959… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 137 2021-07-22 07:10:22.3574028… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 138 2021-07-22 07:10:22.3575039… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 139 2021-07-22 07:10:22.3576079… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 140 2021-07-22 07:10:22.3577575… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 141 2021-07-22 07:10:22.3577644… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 142 2021-07-22 07:10:22.3578743… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 143 2021-07-22 07:10:22.3579834… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 144 2021-07-22 07:10:22.3580752… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
 145 2021-07-22 07:10:22.3581881… 192.168.0.108   192.168.0.107   ICMP       60 Destinatio
```

```
▸ Frame 125: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_1f:ed:d1 (08:00:27:1f:ed:d1), Dst: PcsCompu_99:c7:f1 (08:00:27:99:c7:f1)
▸ Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.107
▸ Internet Control Message Protocol
```

```
0000  08 00 27 99 c7 f1 08 00  27 1f ed d1 08 00 45 00   ..'..... '.....E.
0010  00 1c d3 89 00 00 14 01  51 30 c0 a8 00 6c c0 a8   ........ Q0...l..
0020  00 6b 03 02 fc fd 00 00  00 00 00 00 00 00 00 00   .k...... ........
0030  00 00 00 00 00 00 00 00  00 00 00 00               ........ ....
```

Screenshot: Wireshark on Server machince has captured the ICMP packets.

However, despite Server receiving the Hard Error ICMP messages, the TCP connection between Server and Victim was still ongoing.



```
[07/22/21]seed@VM:~$ telnet 192.168.0.107
Trying 192.168.0.107...
Connected to 192.168.0.107.
Escape character is '^]'.
Ubuntu 16.04.2 LTS
VM login: seed
Password:
Last login: Thu Jul 22 06:37:36 EDT 2021 from 192.168.0.108 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.

[07/22/21]seed@VM:~$ ls
abc      Customization  Downloads         lib       Public     Videos
android  Desktop        examples.desktop  Music     source
bin      Documents      get-pip.py        Pictures  Templates
[07/22/21]seed@VM:~$ ls
abc      Customization  Downloads         lib       Public     Videos
android  Desktop        examples.desktop  Music     source
bin      Documents      get-pip.py        Pictures  Templates
[07/22/21]seed@VM:~$ 
```

Screenshot: Victim is still connected to the Server after the Blind reset attack. An “ls” command is performed to confirm that the telnet(TCP) connection is still alive between Server and Victim.

The same attack has been performed using other Hard error ICMP messages which are of Type: 3 Code: 3(Port Unreachable), Type: 3 Code: 4(fragmentation needed but don’t fragment bit set). In all cases, the attack has failed to terminate the connection between the server and victim.

Conclusion:

The attack was unsuccessful. As shown in the aforementioned demonstration, the TCP connection between Server and Victim was not terminated due to the attack. This is due to most popular TCP implementations treat all ICMP "hard errors" received for connections in any of the synchronized states (ESTABLISHED, FIN-WAIT-1, FIN-WAIT-2, CLOSE-WAIT, CLOSING, LAST-ACK, or TIME-WAIT) as "soft errors". Which means, they do not abort the corresponding connection upon receipt of these ICMP messages.

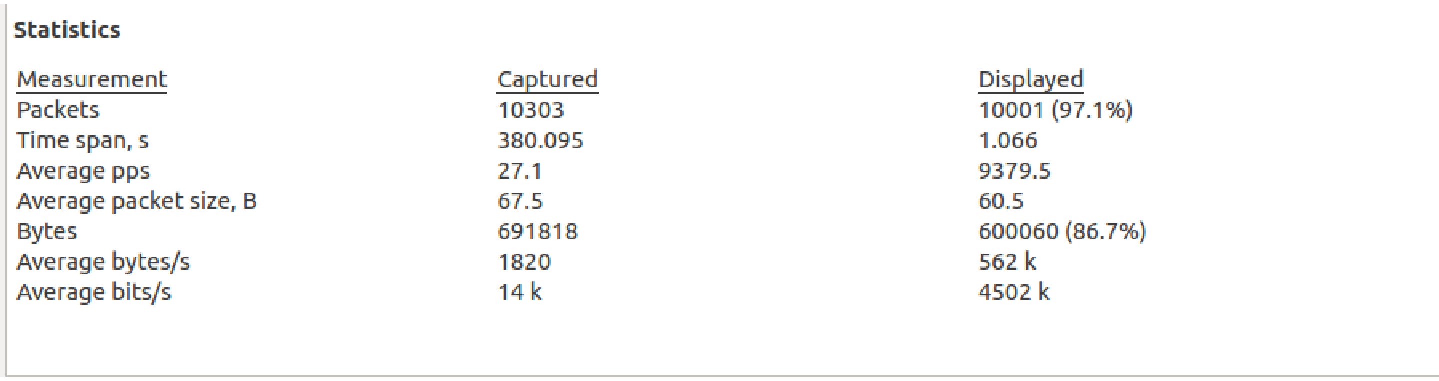
ICMP Blind throughput reduction attack:

Step: 1- Establishing TCP connection between server and victim:

Step 1 is the same as the previous attack.

Step: 2- Monitoring the Throughput of the Server via wireshark:

Using wireshark, I have noted the throughput of the Server before the ICMP source quench attack is performed.



Statistics

Measurement	Captured	Displayed
Packets	10303	10001 (97.1%)
Time span, s	380.095	1.066
Average pps	27.1	9379.5
Average packet size, B	67.5	60.5
Bytes	691818	600060 (86.7%)
Average bytes/s	1820	562 k
Average bits/s	14 k	4502 k

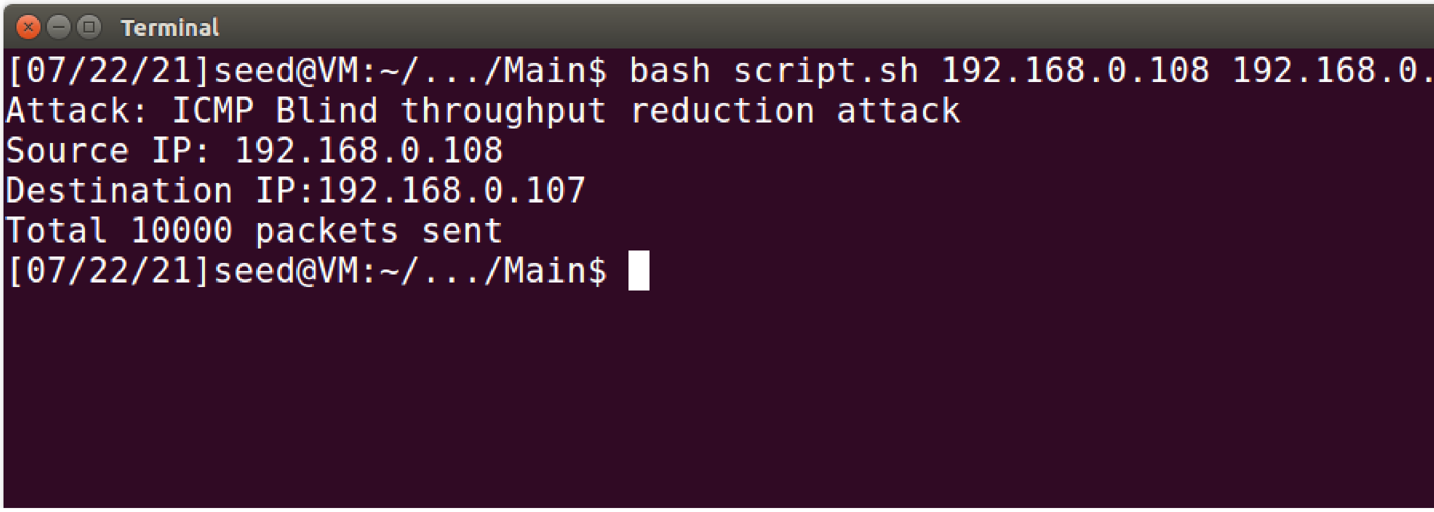
Here we can see that the average Packets per second(pps) is 27.1 before the attack is performed.

In case of a successful attack the throughput/pps is expected to be reduced significantly.

Step: 3- Performing the Blind Throughput reduction attack:

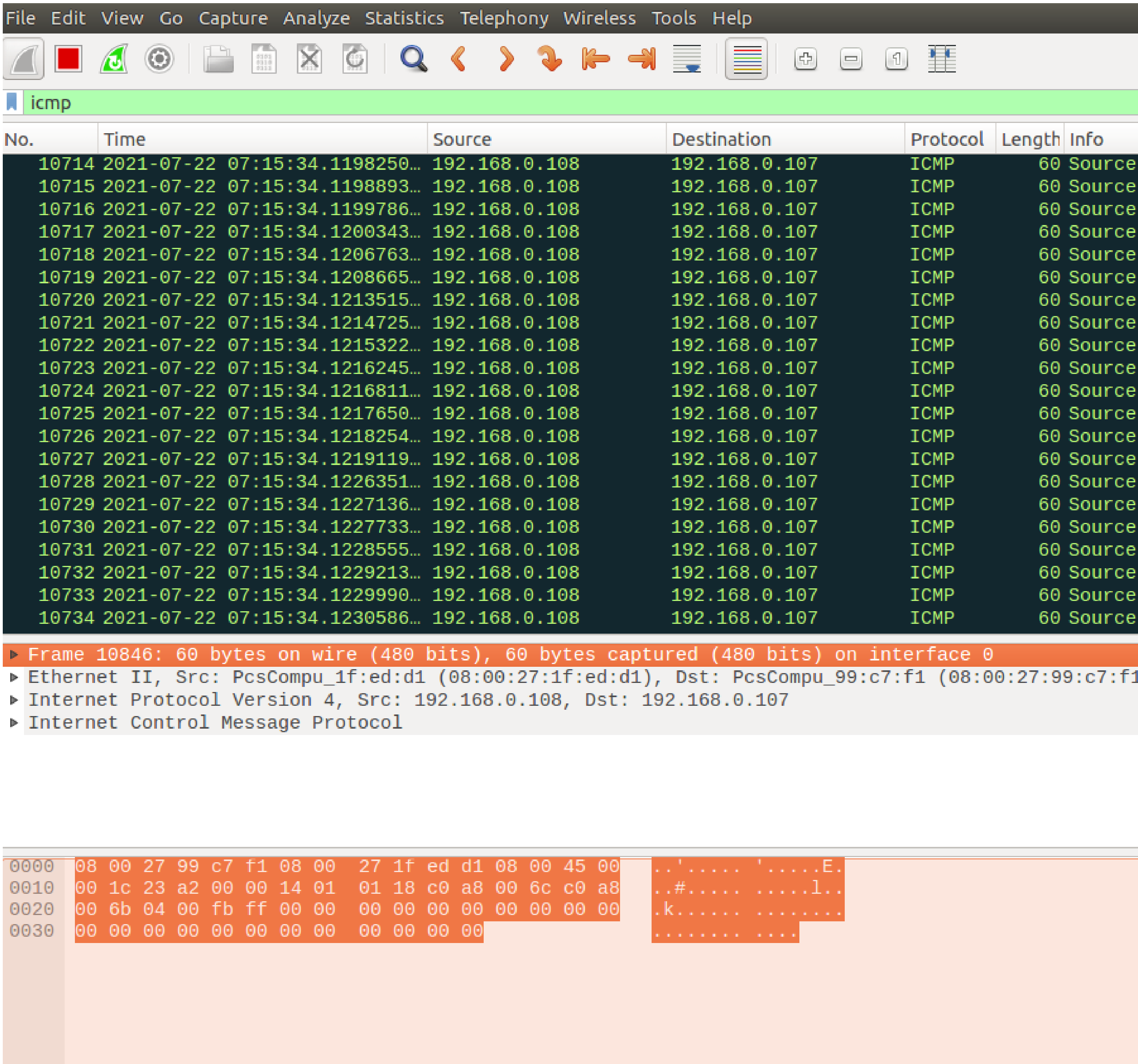
I have used my C program to generate Source quench ICMP messages(type: 4, code: 0) which I have sent from the Attacker to the Server, disguised as the Victim.

In case of this attack the program takes the third argument as 2.



```
[07/22/21]seed@VM:~/.../Main$ bash script.sh 192.168.0.108 192.168.0.
Attack: ICMP Blind throughput reduction attack
Source IP: 192.168.0.108
Destination IP:192.168.0.107
Total 10000 packets sent
[07/22/21]seed@VM:~/.../Main$ 
```

In the following photo we can see that the server has successfully received the Source Quench ICMP packets.



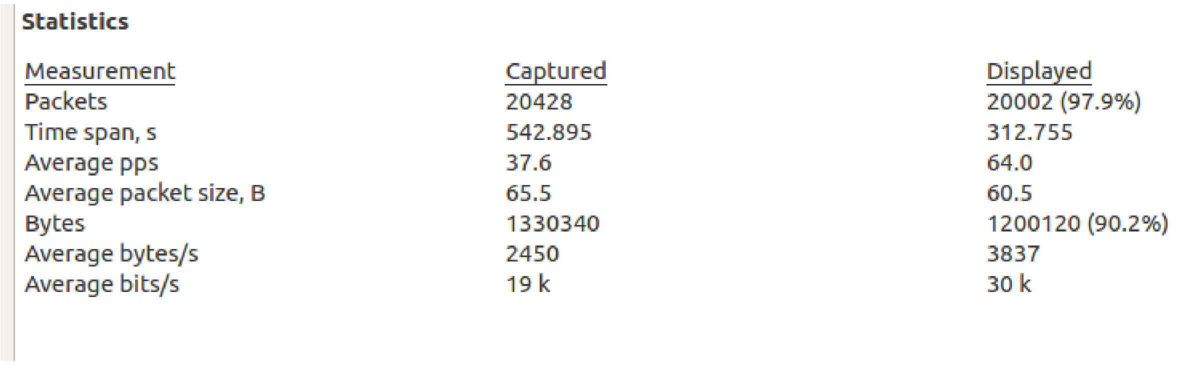
icmp

```
No.   Time                           Source          Destination     Protocol  Length Info
 10714 2021-07-22 07:15:34.1198250… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10715 2021-07-22 07:15:34.1198893… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10716 2021-07-22 07:15:34.1199786… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10717 2021-07-22 07:15:34.1200343… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10718 2021-07-22 07:15:34.1206763… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10719 2021-07-22 07:15:34.1208665… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10720 2021-07-22 07:15:34.1213515… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10721 2021-07-22 07:15:34.1214725… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10722 2021-07-22 07:15:34.1215322… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10723 2021-07-22 07:15:34.1216245… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10724 2021-07-22 07:15:34.1216811… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10725 2021-07-22 07:15:34.1217650… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10726 2021-07-22 07:15:34.1218254… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10727 2021-07-22 07:15:34.1219119… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10728 2021-07-22 07:15:34.1226351… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10729 2021-07-22 07:15:34.1227136… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10730 2021-07-22 07:15:34.1227733… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10731 2021-07-22 07:15:34.1228555… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10732 2021-07-22 07:15:34.1229213… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10733 2021-07-22 07:15:34.1229990… 192.168.0.108   192.168.0.107   ICMP         60 Source
 10734 2021-07-22 07:15:34.1230586… 192.168.0.108   192.168.0.107   ICMP         60 Source
```

```
▸ Frame 10846: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: PcsCompu_1f:ed:d1 (08:00:27:1f:ed:d1), Dst: PcsCompu_99:c7:f1 (08:00:27:99:c7:f1
▸ Internet Protocol Version 4, Src: 192.168.0.108, Dst: 192.168.0.107
▸ Internet Control Message Protocol
```

```
0000  08 00 27 99 c7 f1 08 00  27 1f ed d1 08 00 45 00    ..'..... '.....E.
0010  00 1c 23 a2 00 00 14 01  01 18 c0 a8 00 6c c0 a8    ..#..... .....l..
0020  00 6b 04 00 fb ff 00 00  00 00 00 00 00 00 00 00    .k...... ........
0030  00 00 00 00 00 00 00 00  00 00 00 00                ........ ....
```

<u>Step: 4- Monitoring the thourghput of the Server after the attack:</u>



Statistics

Measurement	Captured	Displayed
Packets	20428	20002 (97.9%)
Time span, s	542.895	312.755
Average pps	37.6	64.0
Average packet size, B	65.5	60.5
Bytes	1330340	1200120 (90.2%)
Average bytes/s	2450	3837
Average bits/s	19 k	30 k

Here we can see that the throughput/Packets per second(pps) of the server has rather increased(previously it was 27.1). The increase in Thoughput can be attributed to the numberous ICMP source quench messages sent to the server as a part of the attack(10000 in this case).

However, in case of a successful attack, the throughput was expected to decrease by a significant margin. We can safely consider the attack unsuccessful.

Conclusion:

The attack was unsuccessful as the ICMP source quench messages failed to reduce the throughput of the server. This is because ICMPv4 Source Quench messages are seen as an ineffective antidote for congestion. Thus, TCP implements its own congestion control mechanisms that do not depend on ICMPv4 Source Quench messages. Based on this reasoning, a large number of implementations completely ignore ICMPv4 Source Quench messages meant for TCP connections. This behavior has been implemented in, Linux since 2004. Therefore the attack is ineffective for up-to-date systems.

Refereces: [RFC] [RFC1122] [RFC5681] [RFC3168]