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.

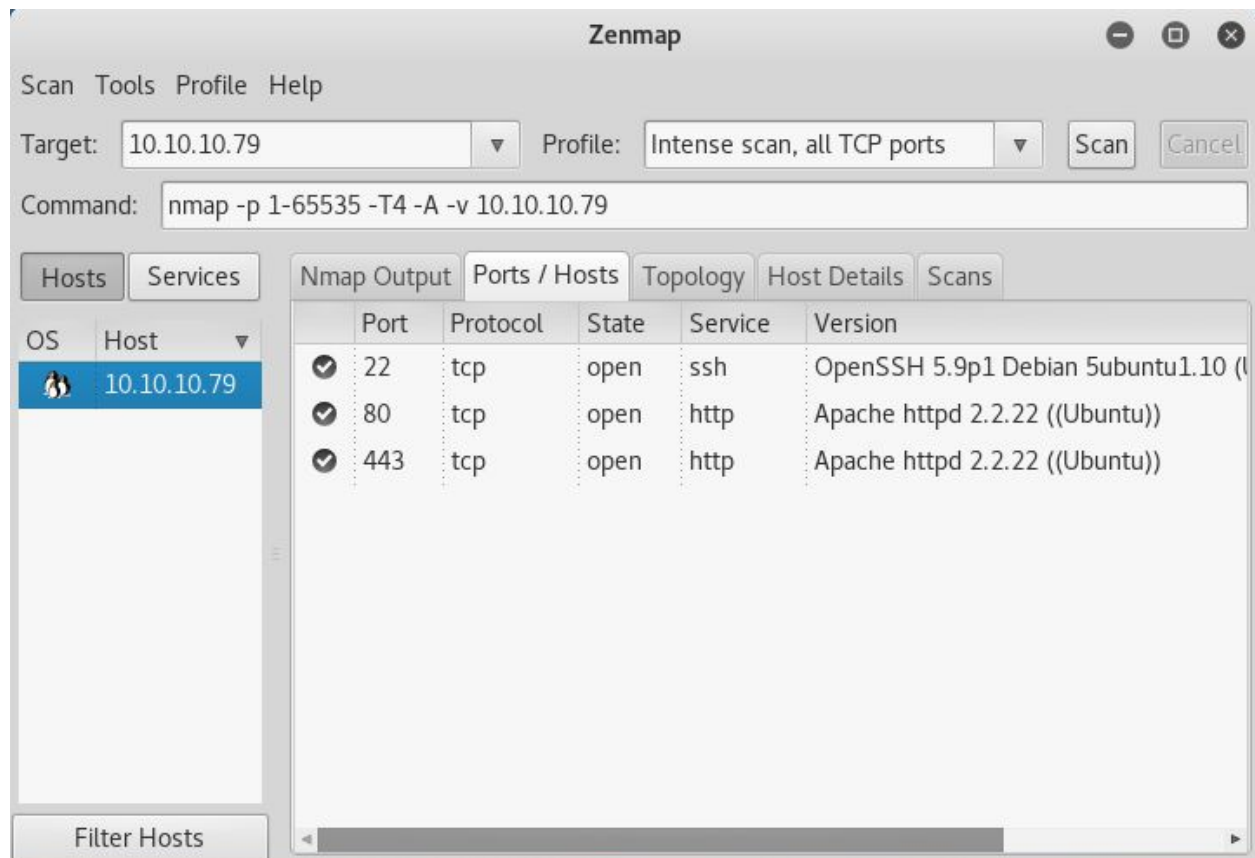### Skills Required

- 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

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

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.

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.

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.