Assignment - 1 Passive and Active Recon

GroupID: 3

Member1: 212152:Muhammad Talha Attari

Member2: 211185:Ahmad Anwar

Course: CY243L - Penetration Testing - Lab

Date: 26/10/2023

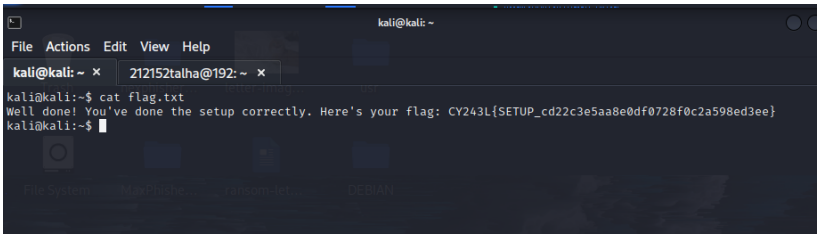
FlagsSubmitted: 5

Flag - 1 ~ (1 x `attacker`)

The first flag does not involve Enumeration and Exploitation as it was already given in the Assignment manual.

1. You just have to use the command `ls -l` and it will show three text files.
2. The file named as `flag.txt` contains the first flag.

```
ls -l
cat flag.txt
```



> `Flag # 1 :` `CY243L{SETUP_cd22c3e5aa8e0df0728f0c2a598ed3ee}`

Flag - 2 ~ (1 x `webapp.local`)

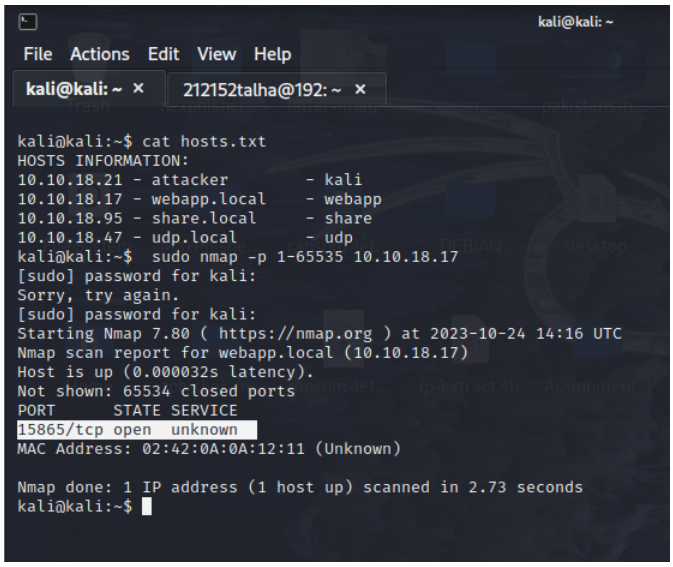
• **Enumeration** (How did I found the open ports)

1. First, we used `nmap` to scan for open ports in `webapp.local`. If we view the `hosts.txt` file, we get the IP addresses of all three hosts. In our case, the IP address of webapp.local is `10.10.18.17`.

2. To find open ports, we used the following command:

```
sudo nmap -p 1-65535 10.10.18.17
```

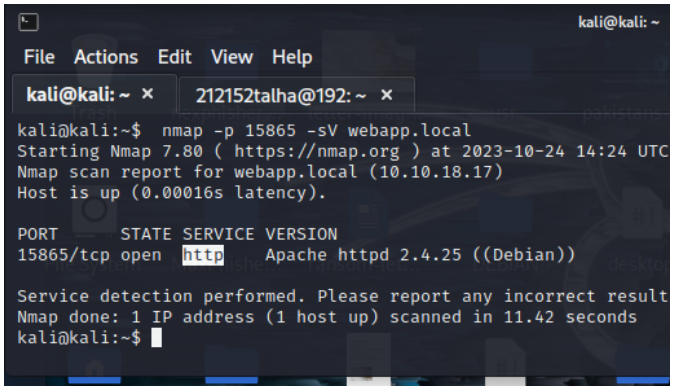
3. This gave us the following output which shows that port `15865` is open.



Screenshot

4. Now before connecting to the host, We don't know which service is being run on the open port. To check which service is run on `15865`, we used the following command:

```
nmap -p 15865 -sV webapp.local
```



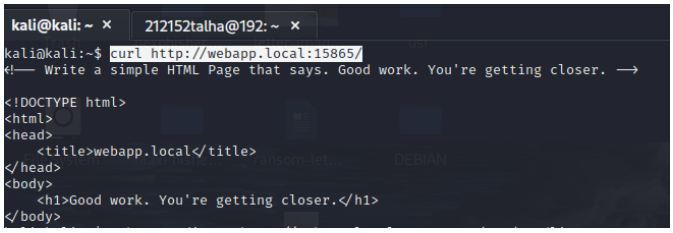
Screenshot of Service used in webapp.local

• **<u>Exploitation</u>** (Which tools did we used to exploit the service)

6. As the service run on this port is `http` so the webpage is hosted as the name `webapp.local` also gives us a hint.

7. By using `curl` command, we verified that it was indeed a webpage, we used the following command:

```
curl http://webapp.local:15865/
```

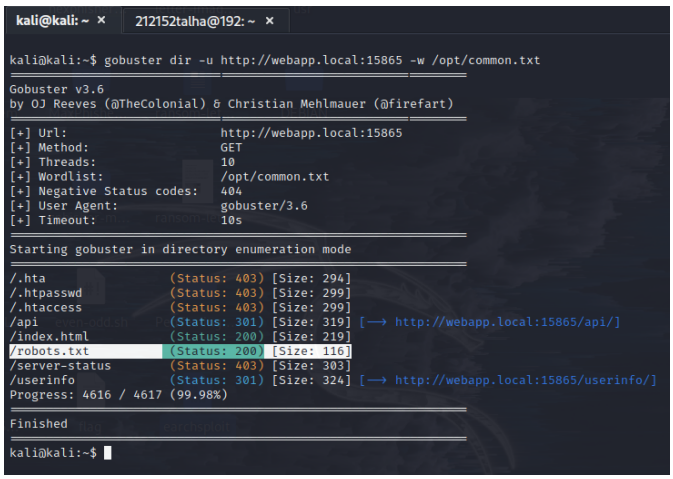


~ Screenshot

8. Now, in our assignment we have two wordlists provided, now we will scan for directories in the webpage by using `gobuster`. We will scan for directories using both `wordlist.txt` and `common.txt`,

9. First we used `common.txt`, we used the following command:

```
gobuster dir -u http://webapp.local:15865 -w /opt/common.txt
```



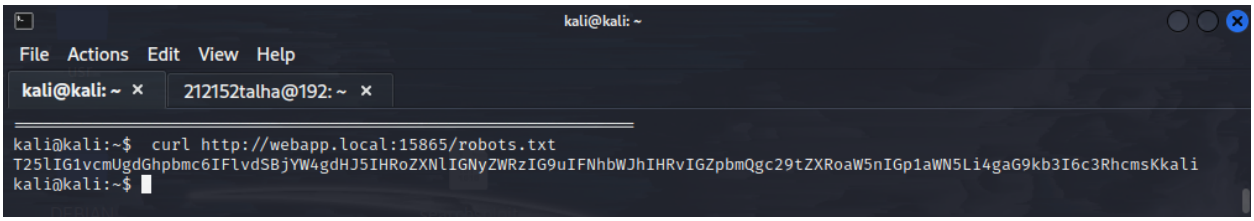
~ Screenshot

10. I found a couple of directories and a .txt file i.e., `robots.txt`. It has a Status: `200` means that we can directly access this file so we viewed this file using the following command:

```
curl http://webapp.local:15865/robots.txt
```

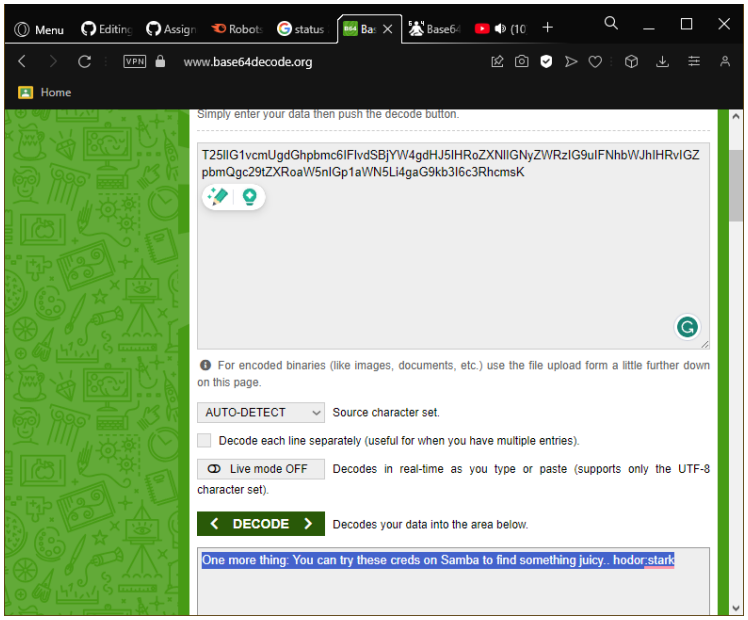
11. We got the following text:


```
T25lIG1vcmUgdGhpbmc6IFlvdSBjYW4gdHJ5IHRoZXNlIGNyZWRzIG9uIFNhbWJhIHRvIGZpbmQgc29tZXRoaW5nIGp1aWN5Li4gaG9kb3I6c3RhcmsKkali
```



~ Screenshot

12. We could not understand it, so we simply searched this on Google and found out that most texts are encrypted using Base64, ROT13 encryption method. So we went to base64decode.org and decrypted it and found this as shown in the following screenshot:



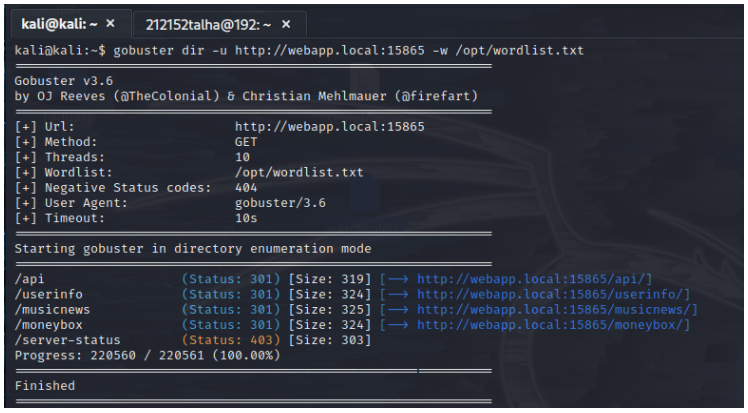
~ Screenshot

> This gave us credentials on Samba that we will use in Task 3 that is `share.local` to retrieve the next flag.

13. Now I scanned the web pp for more directories using `wordlist.txt` by using the following command:

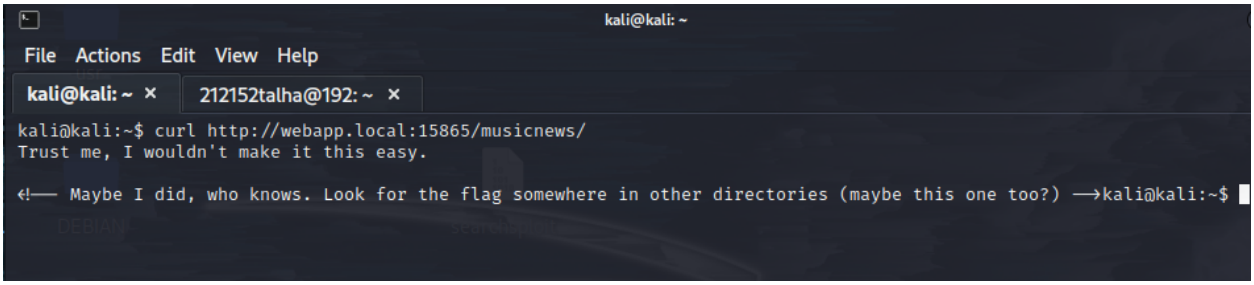
```
gobuster dir -u http://webapp.local:15865 -w /opt/wordlist.txt
```

and got the following directories:



~ Screenshot

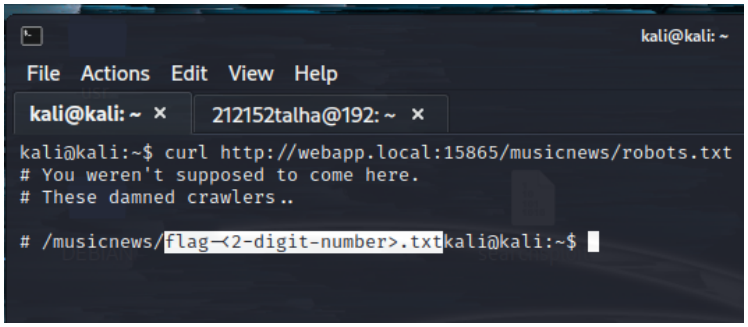
14. We went through every directory and got played xD but this one directory `musicnews` had some hint `"Maybe this one too?"` as shown in the screenshot below:



~ Screenshot

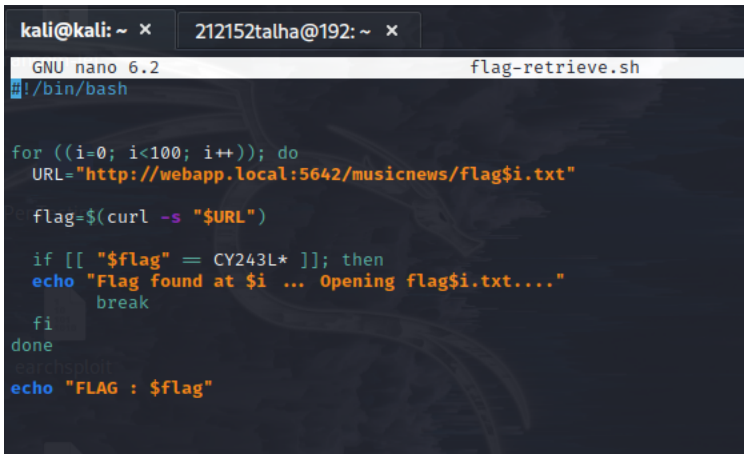
15. When we scanned using `common.txt`, we found `robots.txt`, now this .txt file is almost on every webpage but is not available for everyone to get access to. So I knew that there would be a text file hidden away from everyone. So I used the following command and got the following hint as shown in the screenshot below:

```
curl http://webapp.local:15865/musicnews/robots.txt
```



~ Screenshot

16. Now this hint is that there is a file in the directory `musicnews` that has the name `flag-<2-digit-number>.txt` but we don't know what this 2-digit-number is so we wrote a script that will put random numbers from 00 - 99 and will retrieve the flag if correct 2-digit-number is found:



~ Screenshot of my bash script. Also added this in Appendix at the end.

> **NOTE: We** wrote this script later therefore the `port used` in `this script` is changed therefore we got the flag when the open port was `5642` as seen the screenshot below!

Flag Found:

17. So here is the Flag that we got after running the above script with a screenshot attached:

> `FLAG # 2 : CY243L{WEB_fdd50565dbab8cda82fd79806ae20e16}` (1 x `webapp.local`)

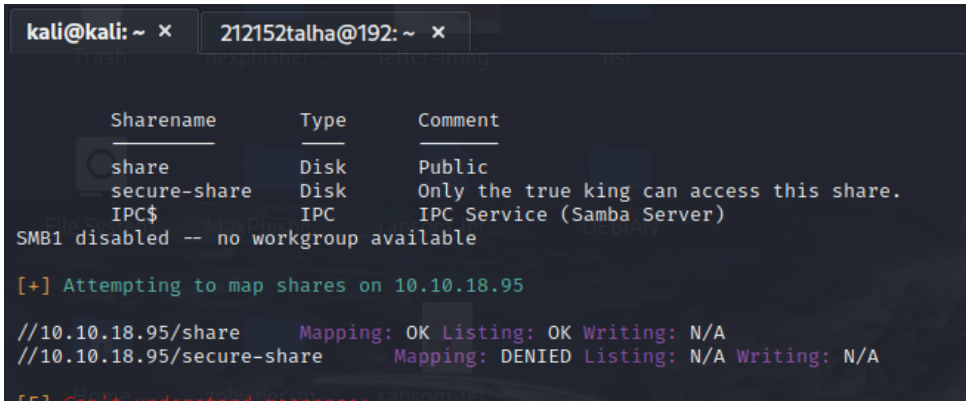
Flag - 3 & 4 ~ (2 x `share.local`)

- **First Flag of share.local:**
  - Enumeration:

1. First we used enum4linux to retrieve a list of users and groups from the samba share by using the following command:

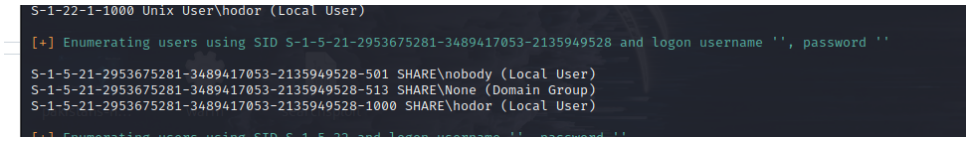
```
enum4linux 10.10.18.95
```

We found that it contained two shares:



~ Screenshot of Two Shares

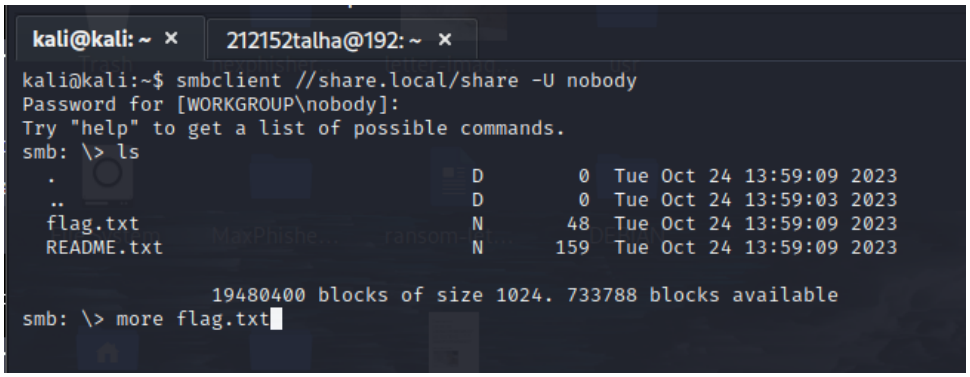
2. The first `share.local` contains these two users i.e., `nobody` and `hodor` :



~ Screenshot of users on share.local

3. Now we connected to the any of the above two-mentioned users by using the following command:

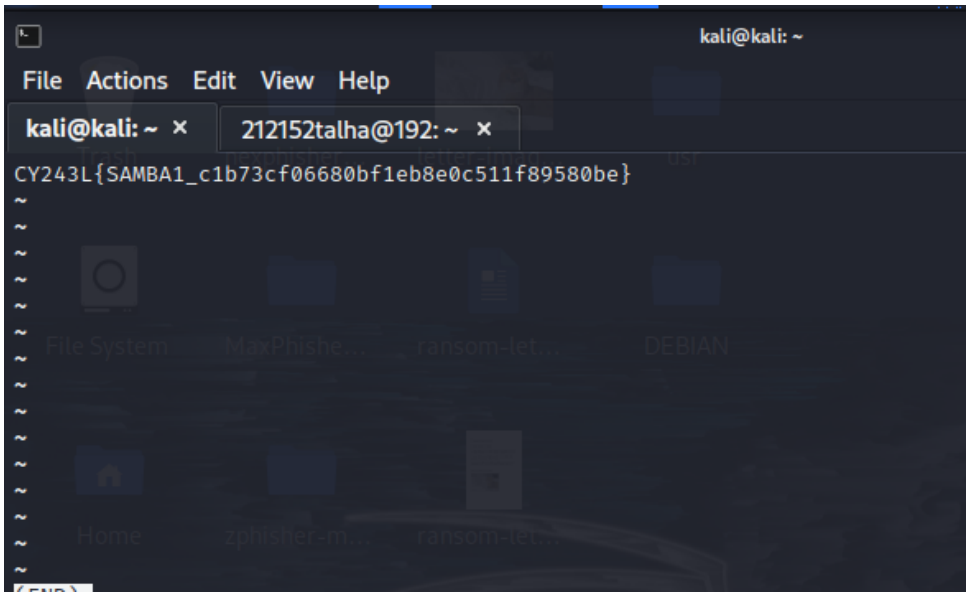
```
smbclient //share.local/share -U nobody          #Just leave the password field blank when ask for password
```



Flag Found:

4. By using the `ls` command to view files and reading the flag.txt by using the following command:

```
ls
more flag.txt
```



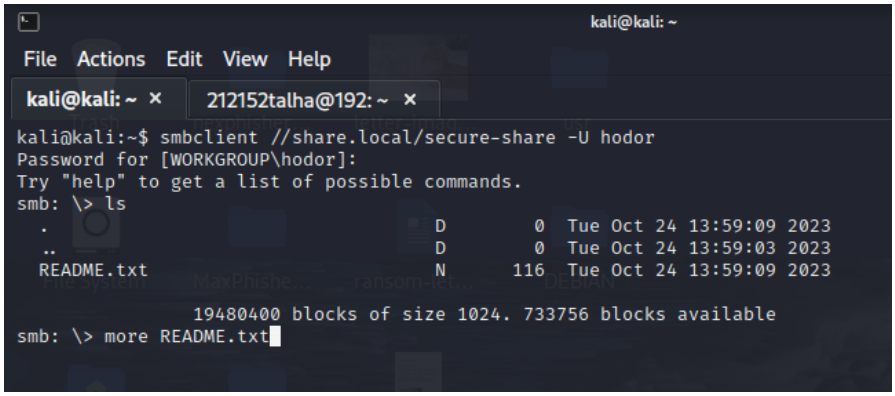
5. and got the flag:

> `FLAG # 3 :` `CY243L{SAMBA1_c1b73cf06680bf1eb8e0c511f89580be}` (1 x `share.local`)

- **<u>Second Flag of share.local</u>**
  - Enumeration:

1. After reading `README.txt`, it is now confirmed that the second flag is in second share i.e., `secure-share`. As we earlier found the credentials of secure-share.local in `webapp.local` i.e., Here in this screenshot .
2. Now I will connect to the `secure-share` using username `hodor` and password `stark` by using the following command:

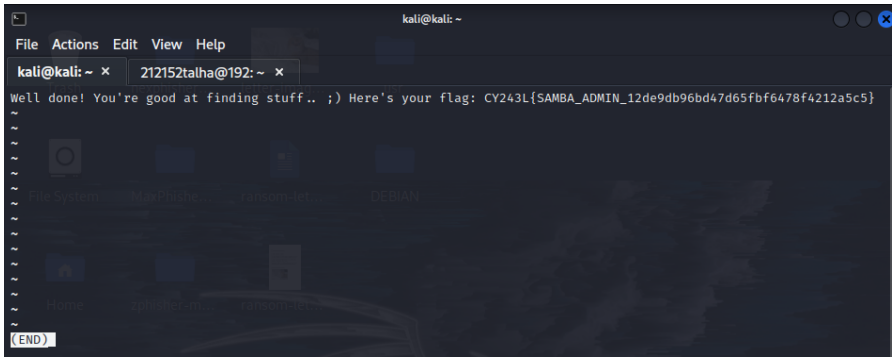
```
smbclient //share.local/secure-share -U hodor
```



Flag Found:

3. On viewing files, there is only one text file i.e., `README.txt.` On viewing this file by using the following command, we got the second flag:

```
ls
more README.txt
```



> **`FLAG # 4 :`** **`CY243L{SAMBA_ADMIN_12de9db96bd47d65fbf6478f4212a5c5}`** (1 x `share.local`)

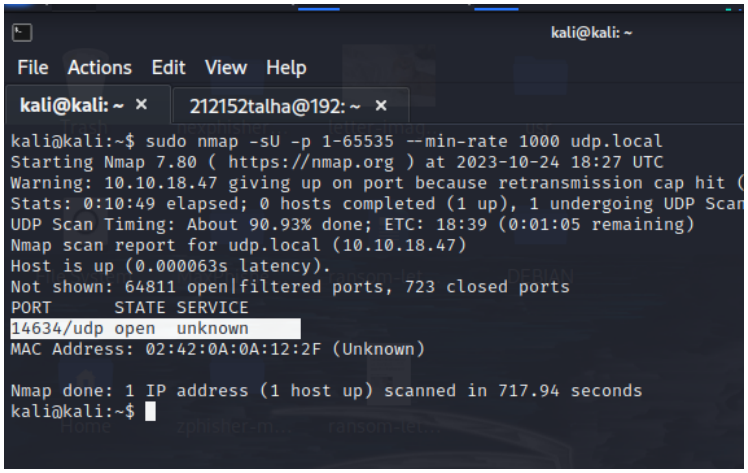
Flag - 5 ~ (1 x `udp.local`)

- **Enumeration:**

1. First I scanned for open ports on `udp.local` by using nmap:

Commands Used:

```
sudo nmap -sU -p 1-65535 --min-rate 1000 udp.local
```

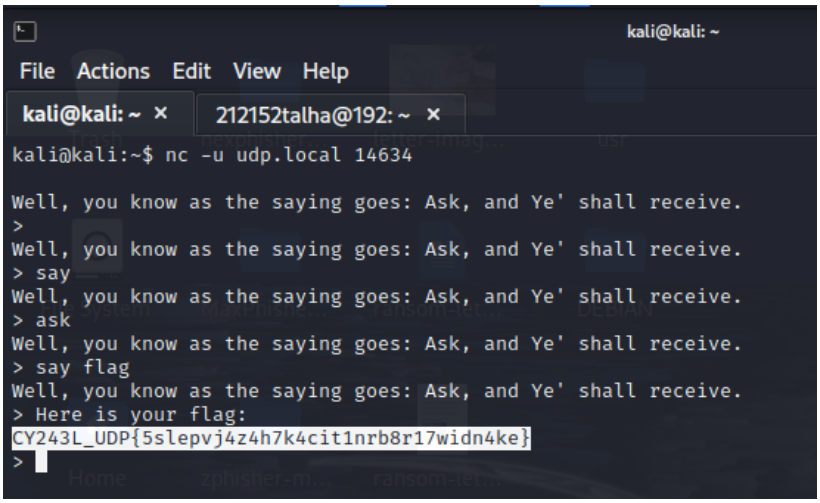


Flag Found:

2. As we can see that we have found an open port: `14634` now we connected on this port using `nc` and got the flag.

Command used:

```
nc -u udp.local 14634
```

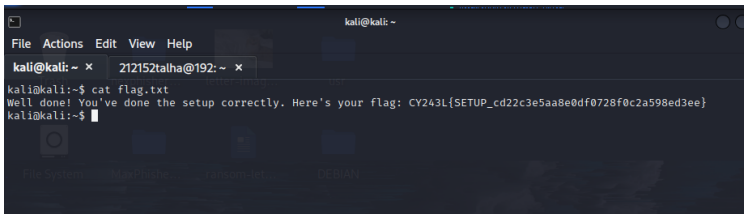


> **`FLAG # 5 :`** **`CY243L_UDP{5slepvj4z4h7k4cit1nrb8r17widn4ke}`** (1 x `share.local`)

Flag(s) Found:

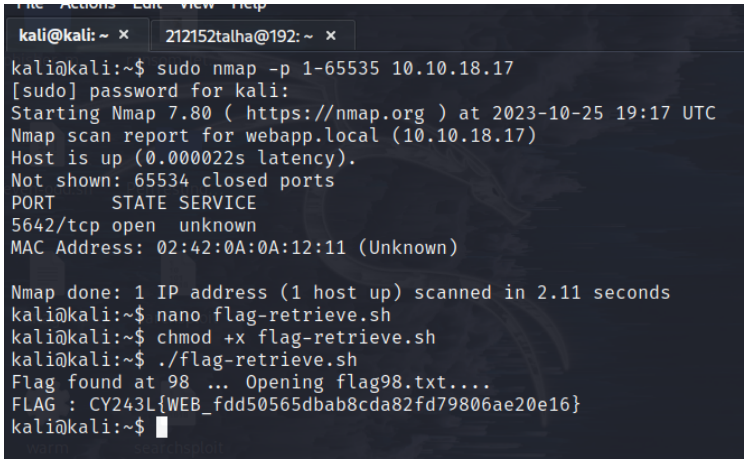
Flag 1:

> `Flag # 1 :` `CY243L{SETUP_cd22c3e5aa8e0df0728f0c2a598ed3ee}` (1 x `attacker`)



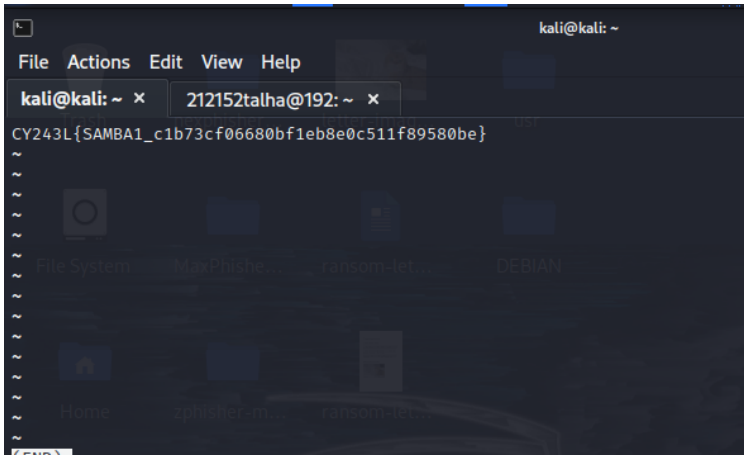
Flag 2:

> `FLAG # 2 :` `CY243L{WEB_fdd50565dbab8cda82fd79806ae20e16}` (1 x `webapp.local`)



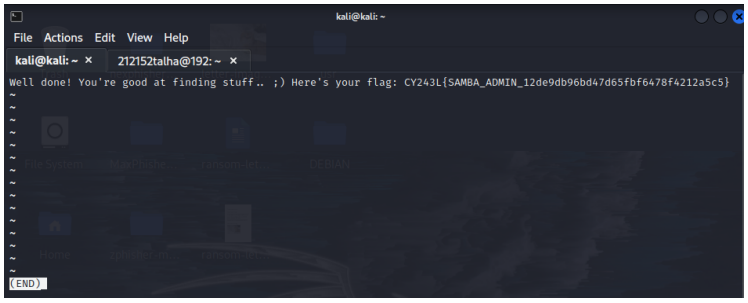
Flag 3:

> `FLAG # 3 :` `CY243L{SAMBA1_c1b73cf06680bf1eb8e0c511f89580be}` (1 x `share.local`)



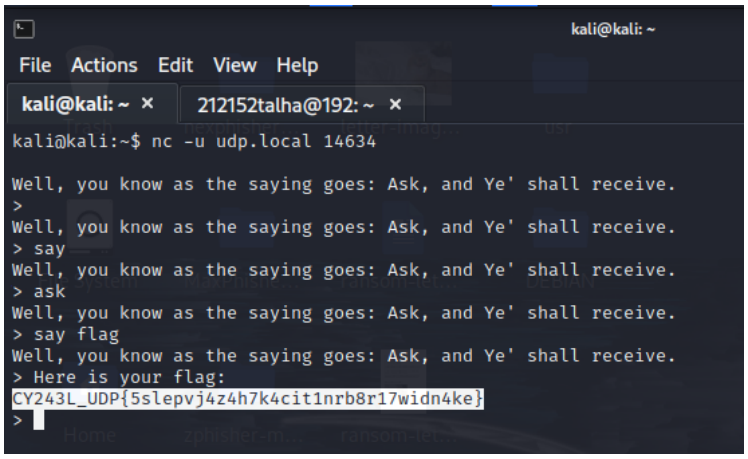
Flag 4:

> `FLAG # 4 :` `CY243L{SAMBA_ADMIN_12de9db96bd47d65fbf6478f4212a5c5}` (1 x `share.local`)



Flag 5:

> `FLAG # 5 :` `CY243L_UDP{5slepvj4z4h7k4cit1nrb8r17widn4ke}` (1 x `share.local`)



Additional Questions

> ### What service is running on `webapp.local` ?

1. `HTTP` service is running on webapp.local.
2. We found this earlier in webapp.local .i.e., Click on this -> to view screenshot with explanation.

> ### What users exists on `share.local` ?

1. The `share.local` contains these two users i.e., `nobody` and `hodor`.
2. We found this earlier in share.local using enum4linux i.e., Click on this -> to view screenshot with explanation.

> ### What is the password for the user is share.local? Add a screenshot of how you found it.

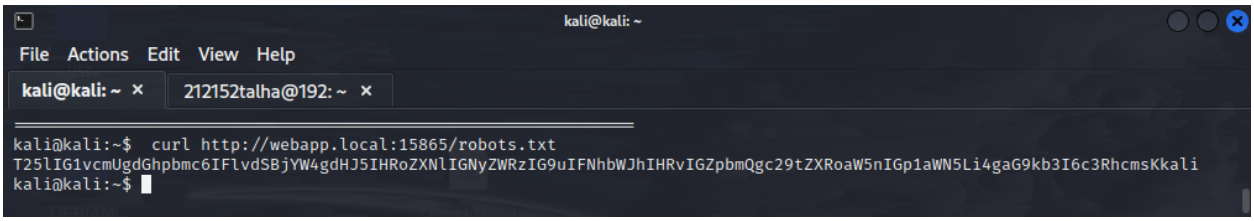
1. There was no password of users on share.local but found the password for users on `secure-share.local` which was `hodor:stark`.
2. This is how we found it earlier also during exploitation in `webapp.local`:

- I found a couple of directories and .txt file i.e., `robots.txt` in share.local. It has a Status: `200` means that we can directly access this file so we viewed this file using the following command:

```
curl http://webapp.local:15865/robots.txt
```

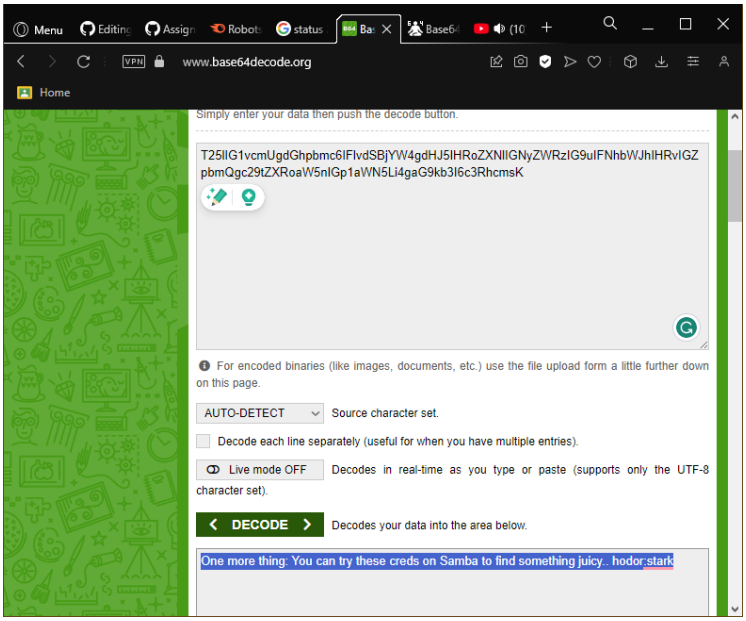
- We got the following text:

```
T25lIG1vcmUgdGhpbmc6IFlvdSBjYW4gdHJ5IHRoZXNlIGNyZWRzIG9uIFNhbWJhIHRvIGZpbmQgc29tZXRoaW5nIGp1aWN5Li4gaG9kb3I6c3RhcmsKkali
```



~ Screenshot

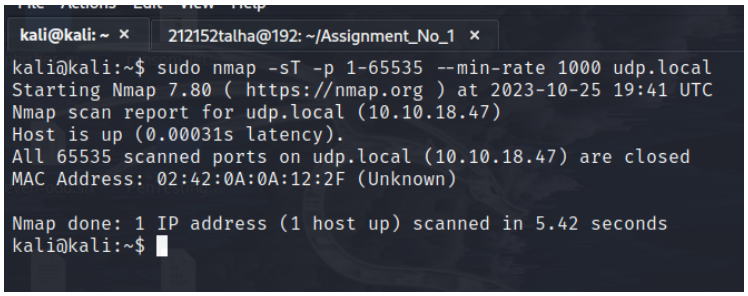
- We could not understand it, so we simply searched this on google and found out that most texts are encrypted using Base64, ROT13 encryption method. So we went to base64decode.org and decrypted it, found this as shown in the following screenshot:



~ Screenshot

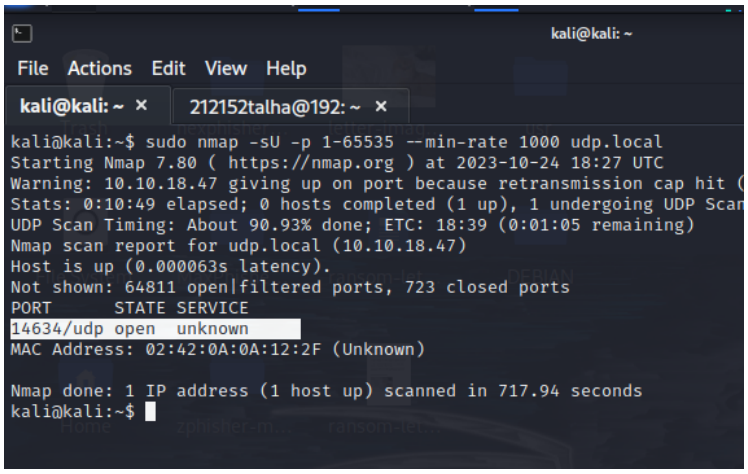
How many tcp ports are open on udp.local?

1. As the name suggests there is `no` tcp port open on udp.local.



How many udp ports are open on udp.local?

1. There is only `one` udp port open on udp.local.



Appendix

Script which we wrote to find the flag in `webapp.local` :

```
#!/bin/bash

search="CY243L"

for ((i=0; i<100; i++)); do
  URL="http://webapp.local:15865/musicnews/flag$i.txt"

  flag=$(curl -s "$URL")

  if [[ "$flag" == CY243L* ]]; then
  echo "Flag found at $i ... Opening flag$i.txt...."
```

```
        break
  fi
done

echo "FLAG : $flag"
```