PSP0201

Week 6

(DAY 21)

Writeup

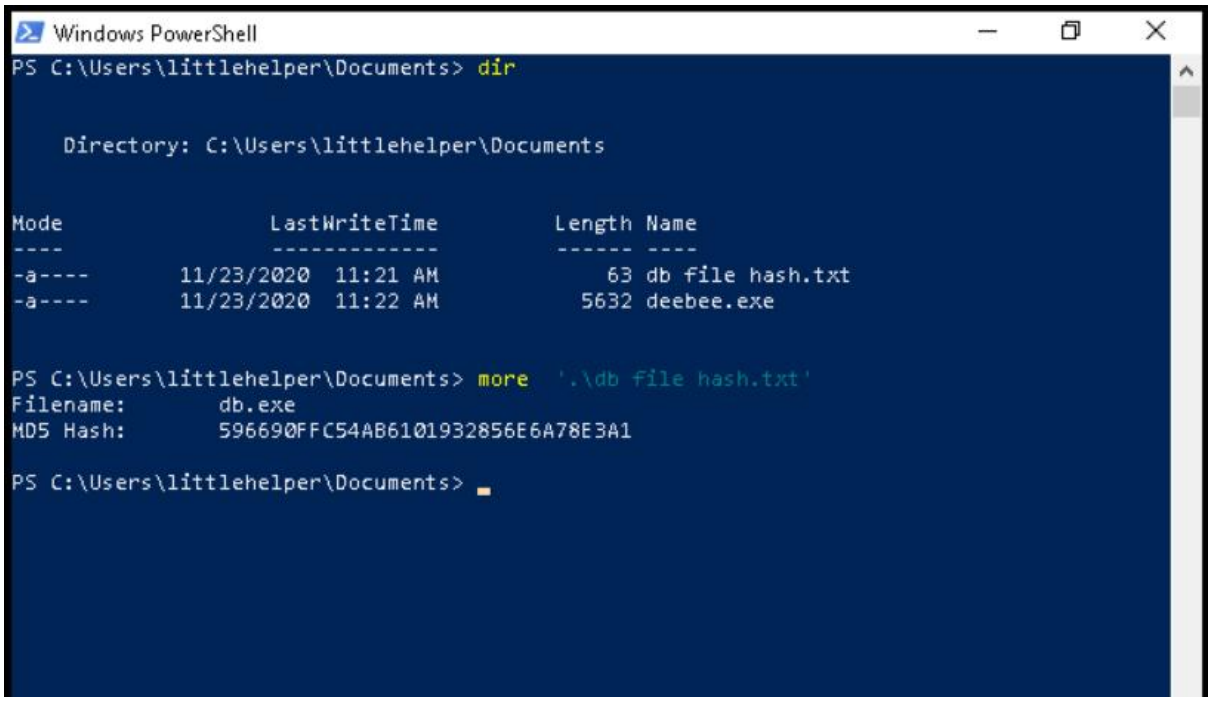
Group Name: Nvida

Members

ID	Name	Role
1211102656	Dennis Ng Chun Hung	Leader
1211101408	Ephrem Loo Ee Zhe	Member
1211102910	Khoo Jen-Au	Member
-	-	-

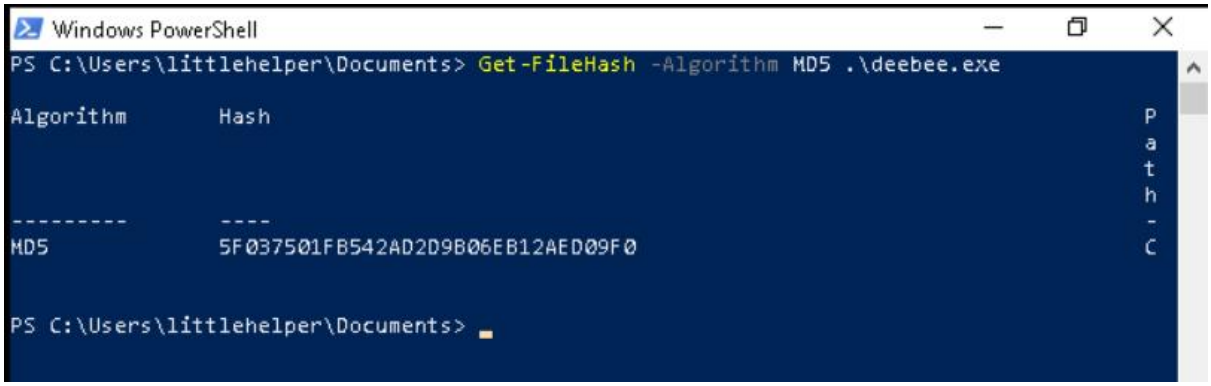
Tools Used:
Kali Linux, Remmina

Question 1
First connect to the remote machine by using remmina with the given server(MACHINE IP), username and password. Open powershell and change directory to “Documents”.
Read the file.



ANSWER: 596690FFC54AB6101932856E6A78E3A1

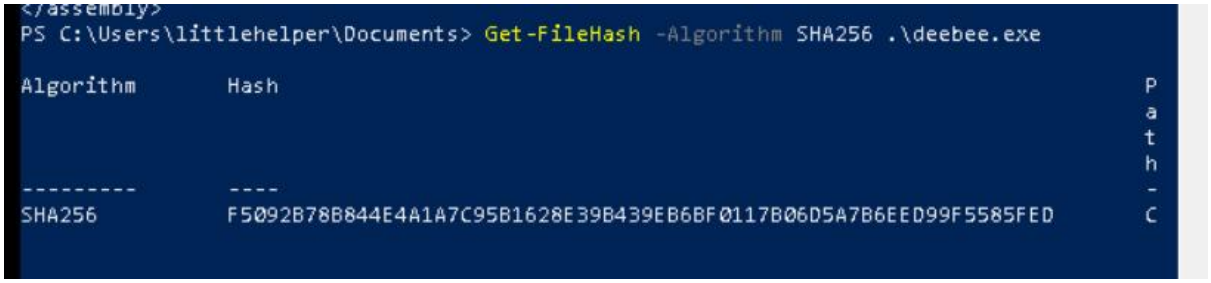
Question 2:
Execute the file and reveal its contents.



ANSWER: 5F037501FB542AD2D9B06EB12AED09F0

Question 3:

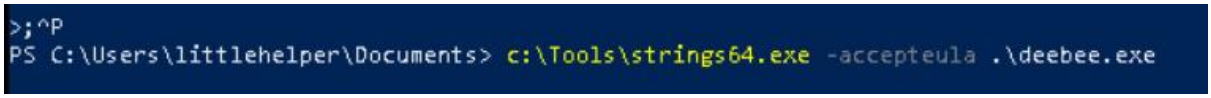
Execute the file with SHA256 file hash instead of MD5 file hash. Reveal its contents.



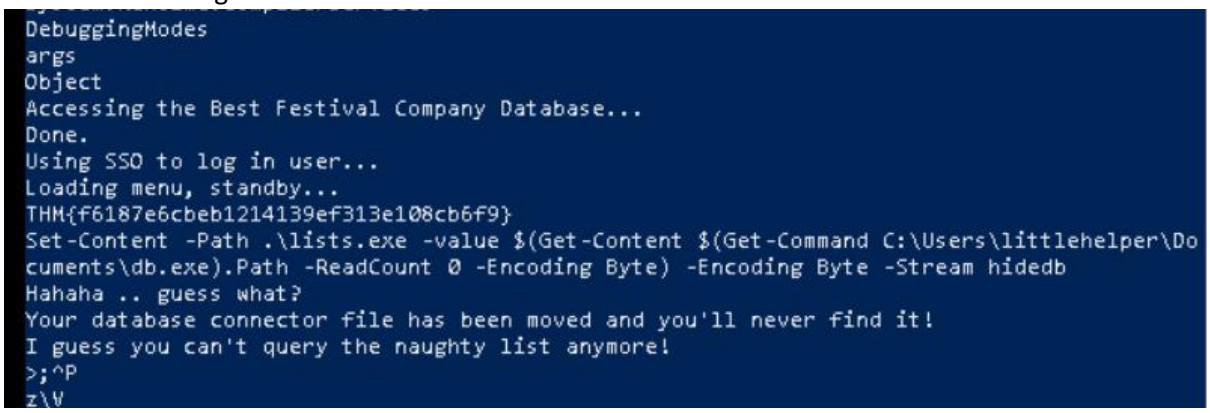
ANSWER: F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED

Question 4:

Using strings. Run the command



And locate the flag.



ANSWER: THM{f6187e6cbeb1214139ef313e108cb6f9}

Question 5:

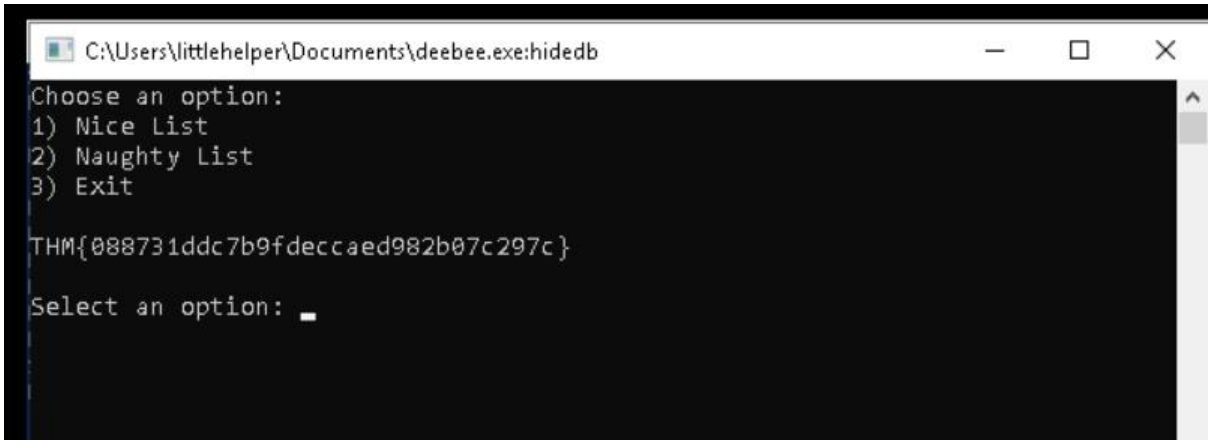
```
wmic process call create $(Resolve-Path file.exe:streamname)
```

By following and replacing the file.exe with correct filename and correct streamname.

ANSWER: wmic process call create $(Resolve-Path .\deebee,exe:hidedb)

Question 6:

BY running the command from the previous question we are able to reveal the flag.

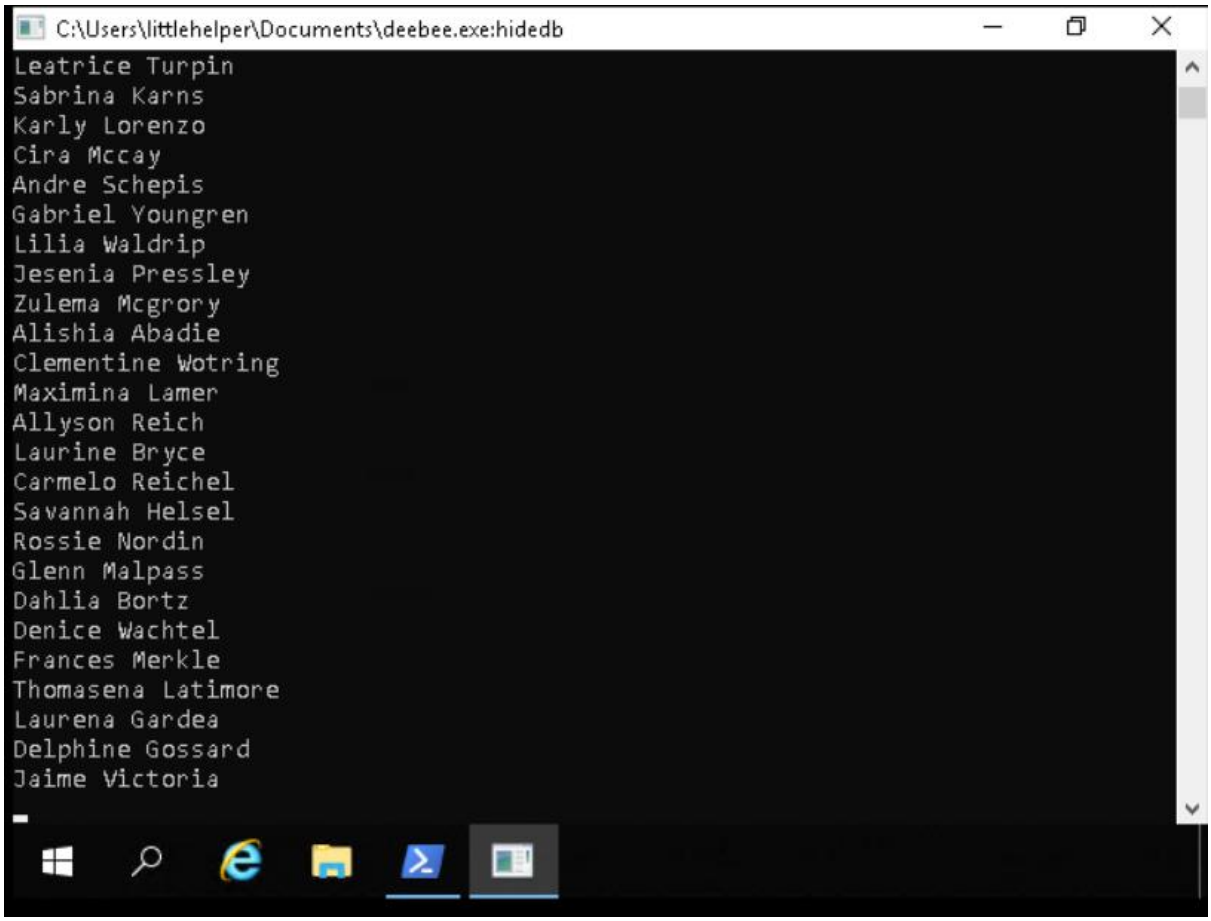


ANSWER: THM{088731ddc7b9fdeccaed982b07c297c}

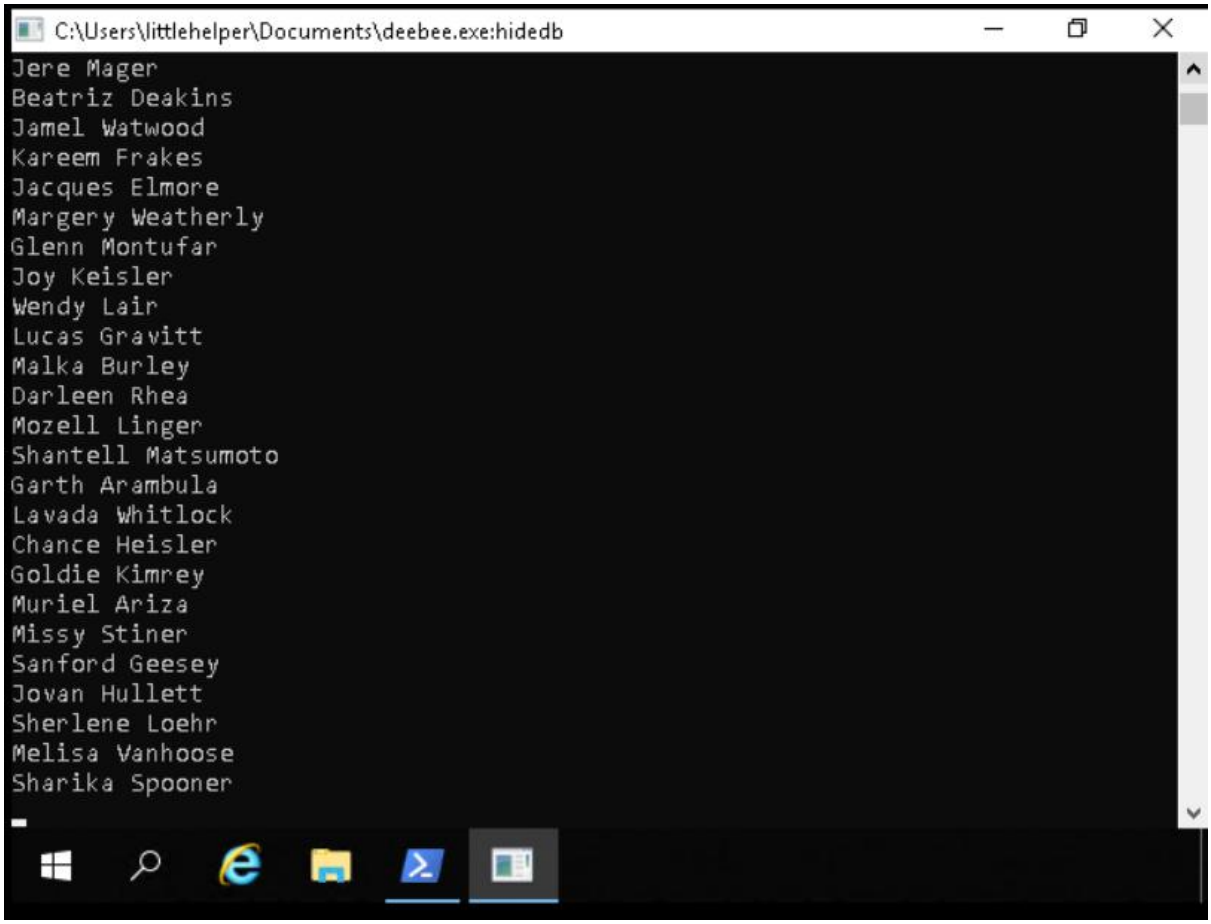
Question 7 & 8:

By selecting the option on 1(Nice List) or 2(Naughty List), we can reveal determine where Sharika Spooner and Jaime Victoria is on the list

NICE LIST



NAUGHTY LIST



ANSWERS:
Sharika Spooner is on Naughty list
Jaime Victoria is on Nice list

End of Day 21 report

PSP0201

Week 6

(DAY 22)

Writeup

Group Name: Nvida

Members

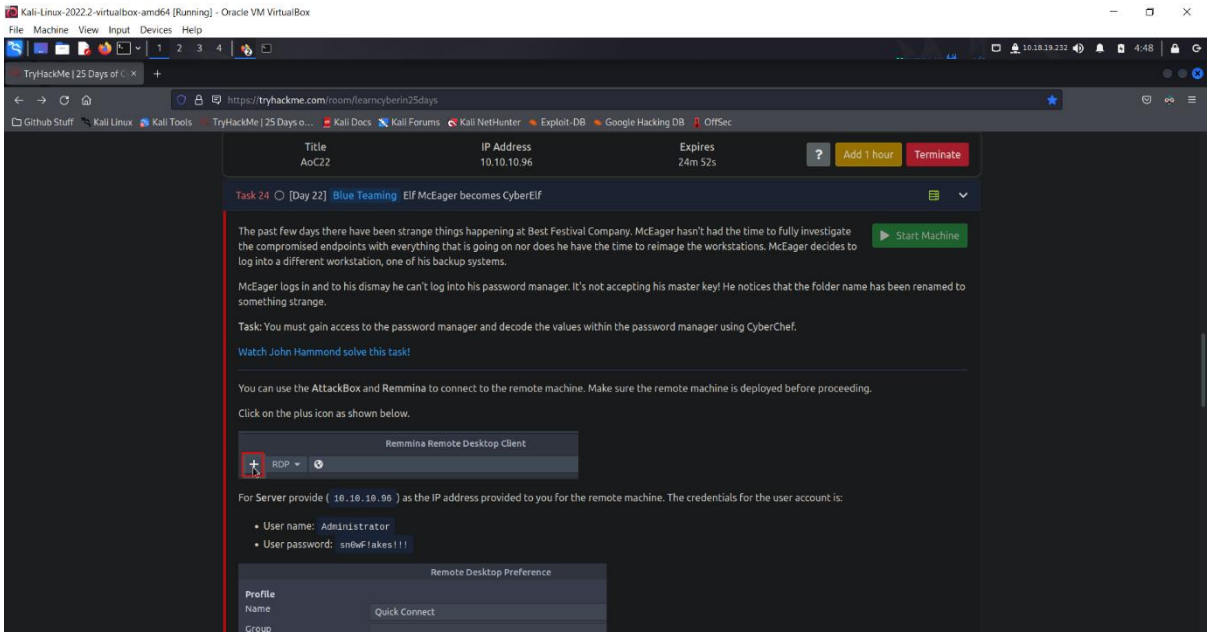
ID	Name	Role
1211102656	Dennis Ng Chun Hung	Leader
1211101408	Ephrem Loo Ee Zhe	Member
1211102910	Khoo Jen-Au	Member
-	-	-

Tools Used:

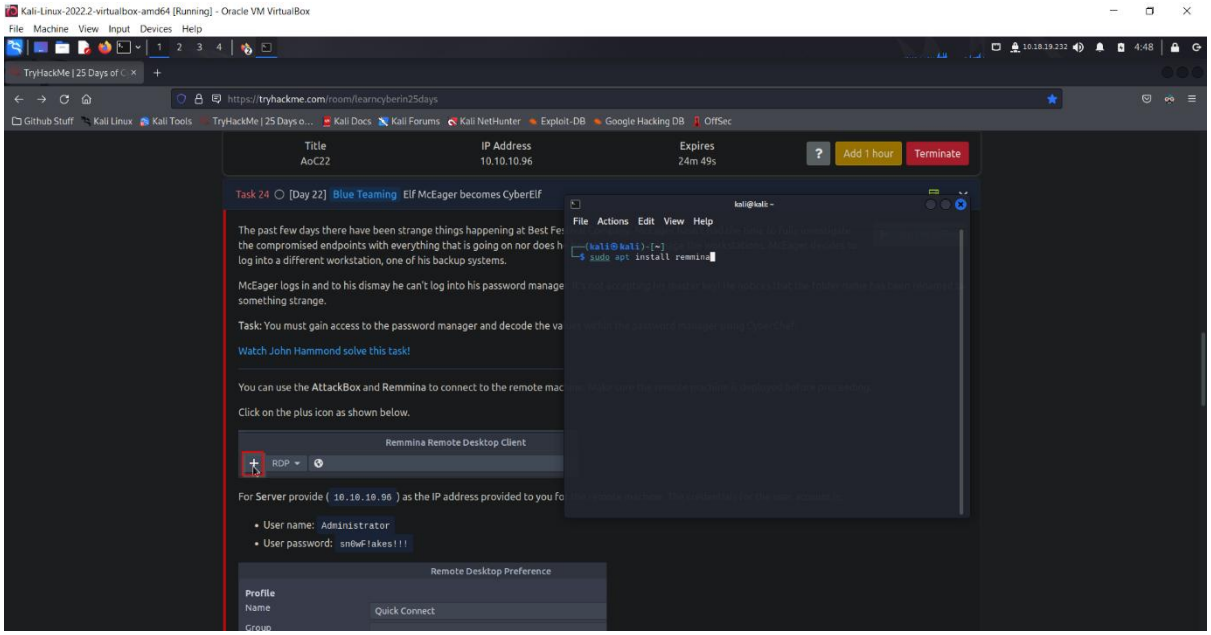
Kali, Firefox, Remmina, Cyberchef

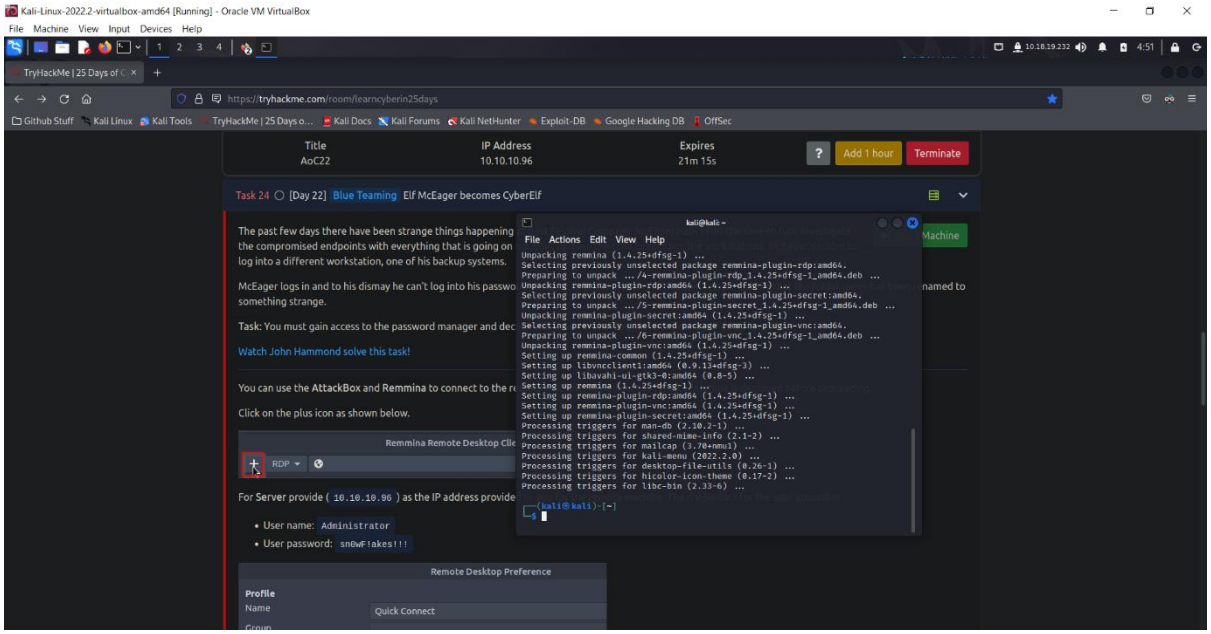
Step 1

Welcome to Day 22, let's start our Day by first deploying the machine.

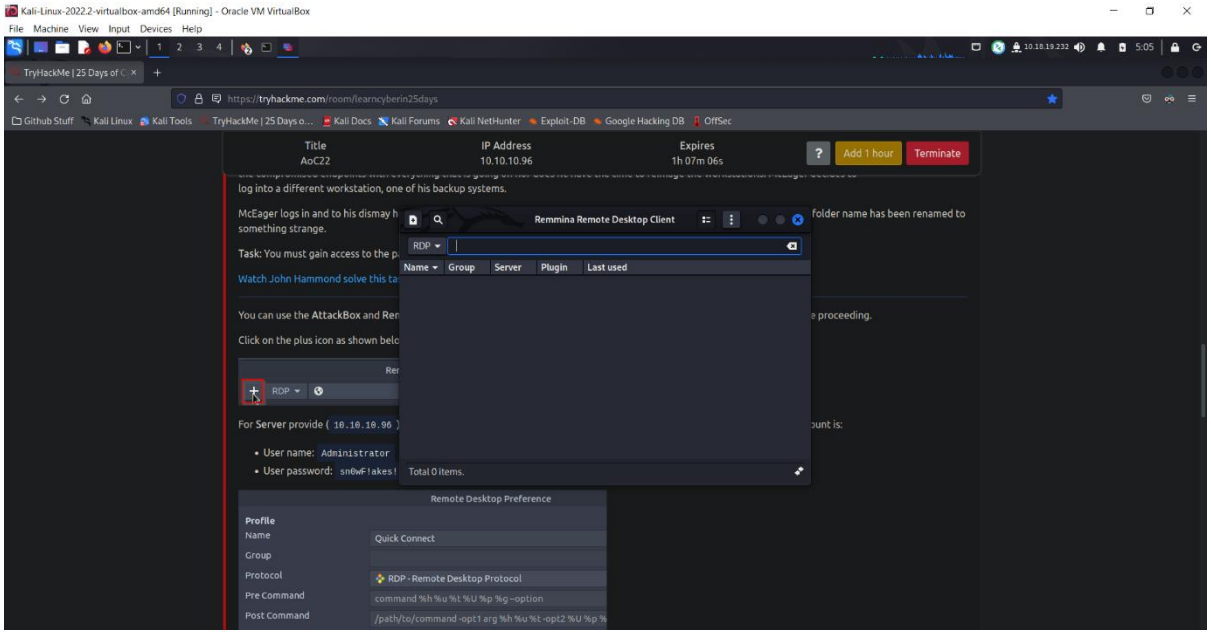


After deploying the machine, let's take a look at the instructions given by THM. So first of all, the tools we are going to use today would be Remmina, so let's go and install our Remmina.

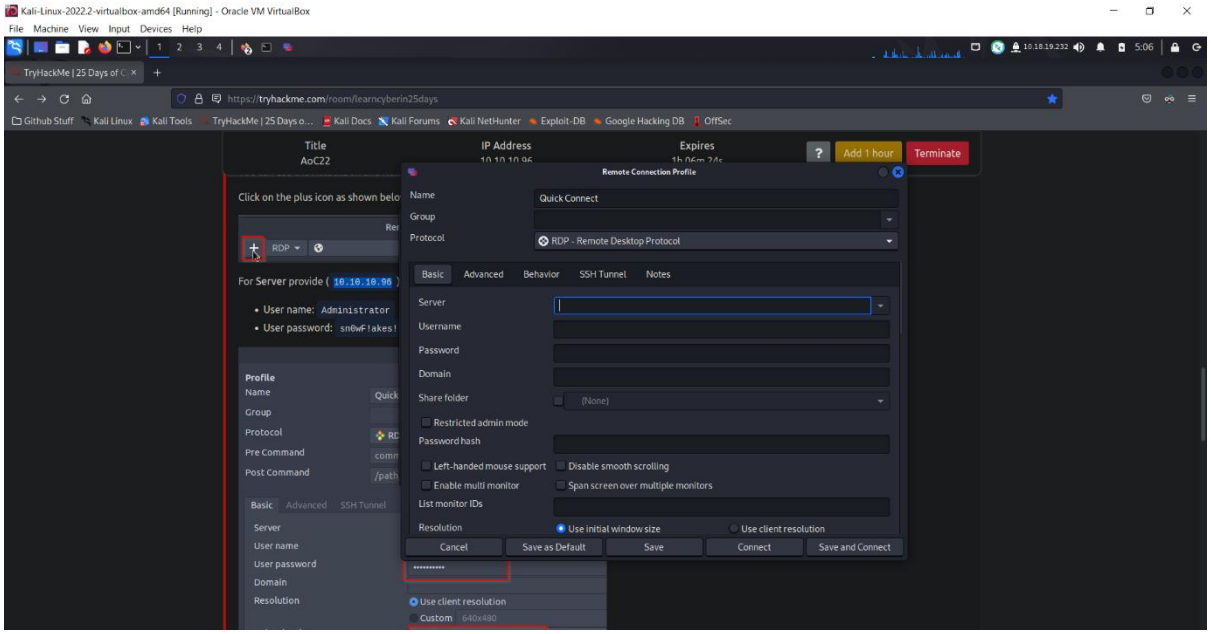




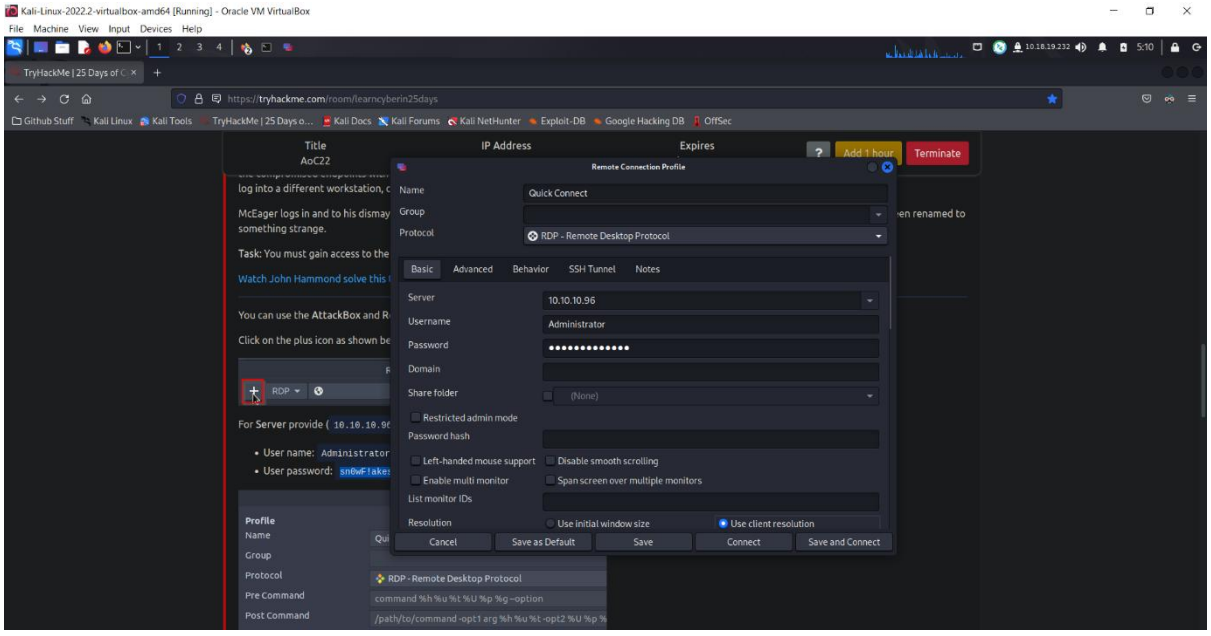
Great, Remmina is now installed in our Kali. Next, what we need to do would be opening up our Remmina.



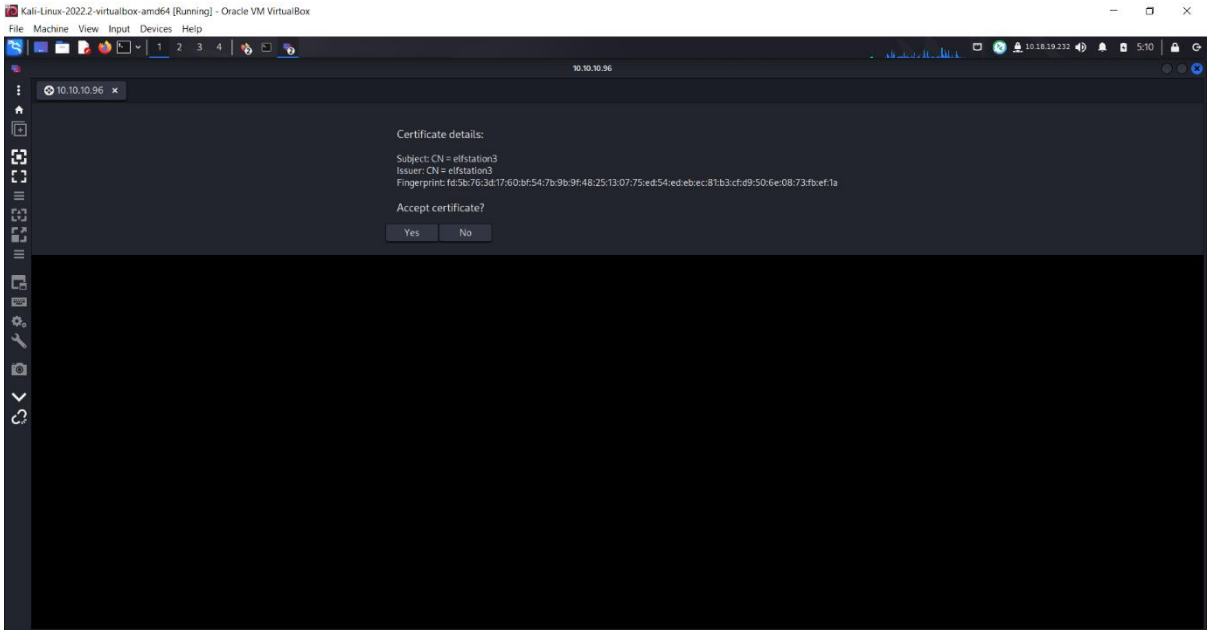
After Remmina is opened, we now need to head to the top left corner of the Pop up box and click on the symbol add file thingy.



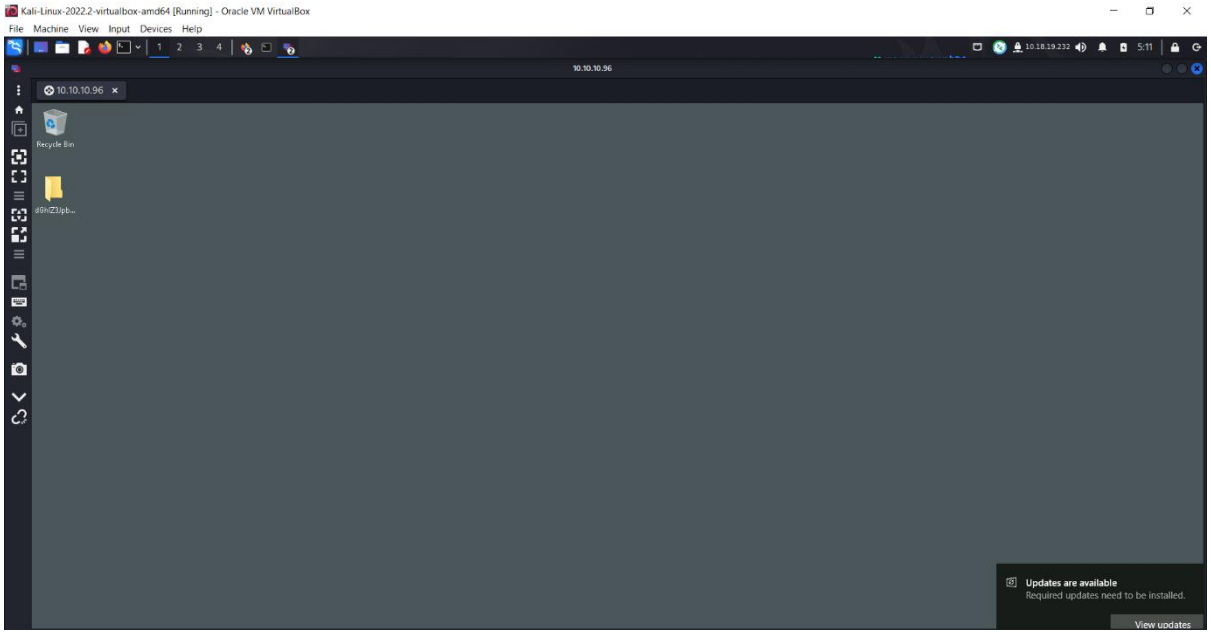
After clicking on that symbol, we are now shown with this page. In this page we just need to follow the instructions given in THM.



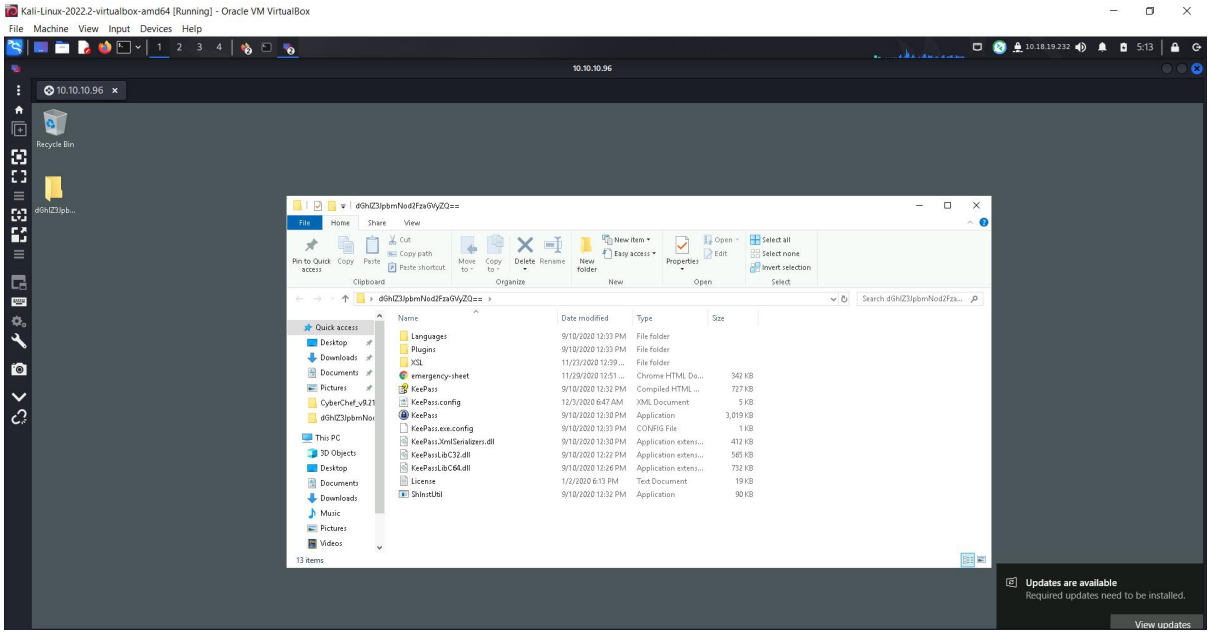
Like this. Once we're done, click on connect to continue on.



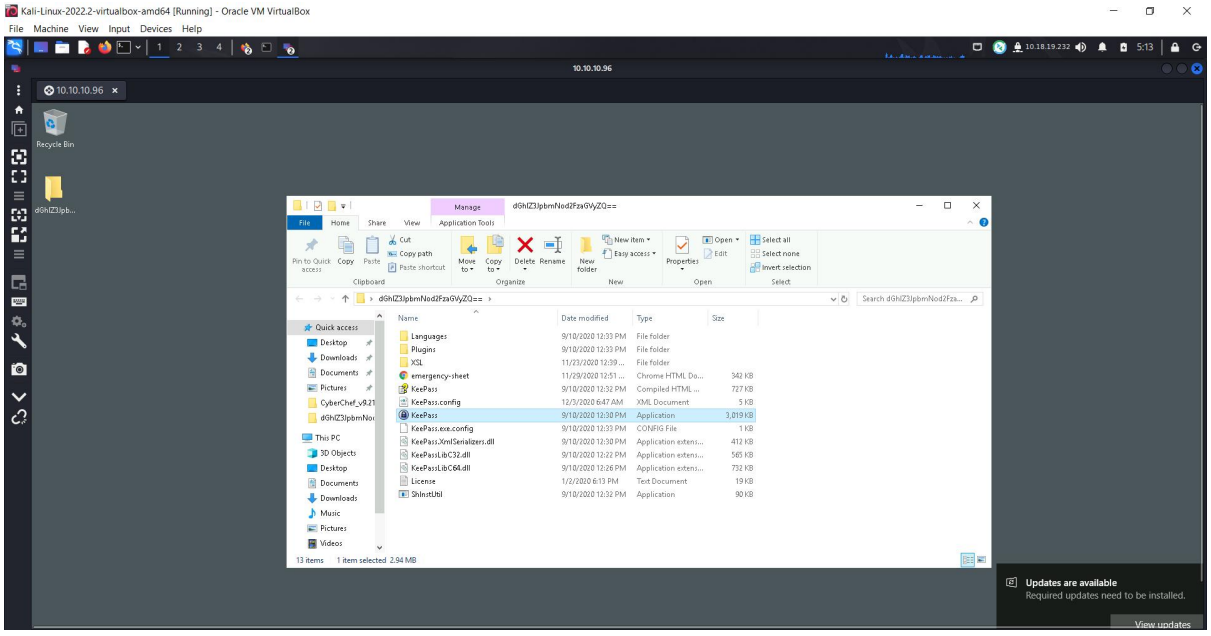
Click on Yes to proceed.



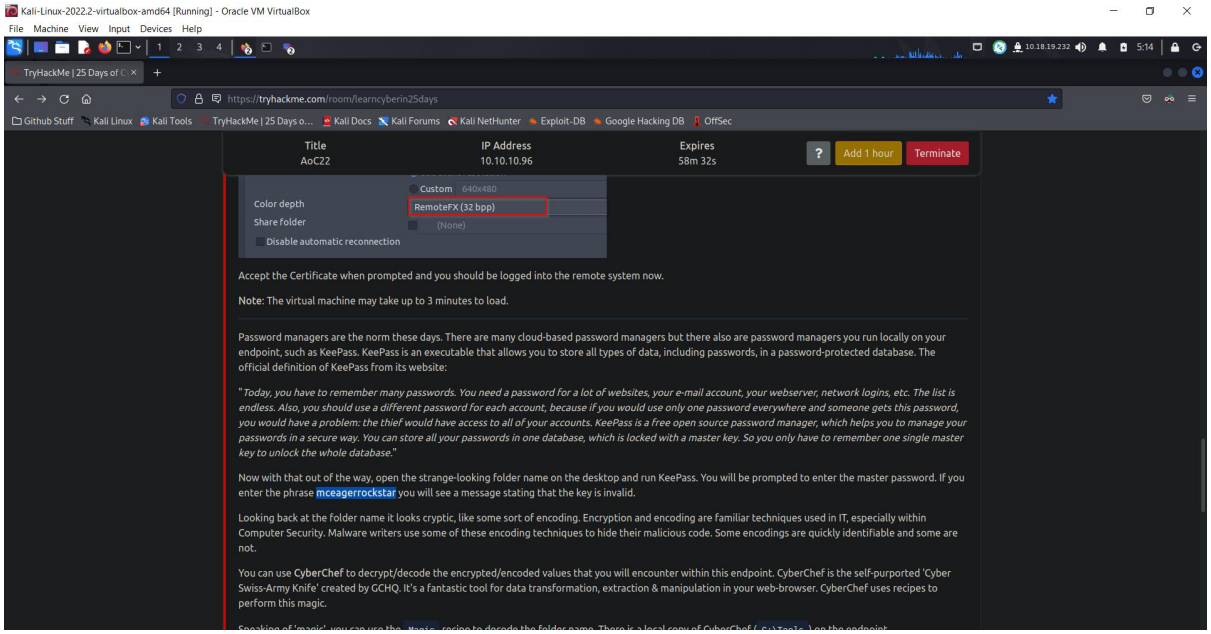
After everything is done, we are then shown with this.



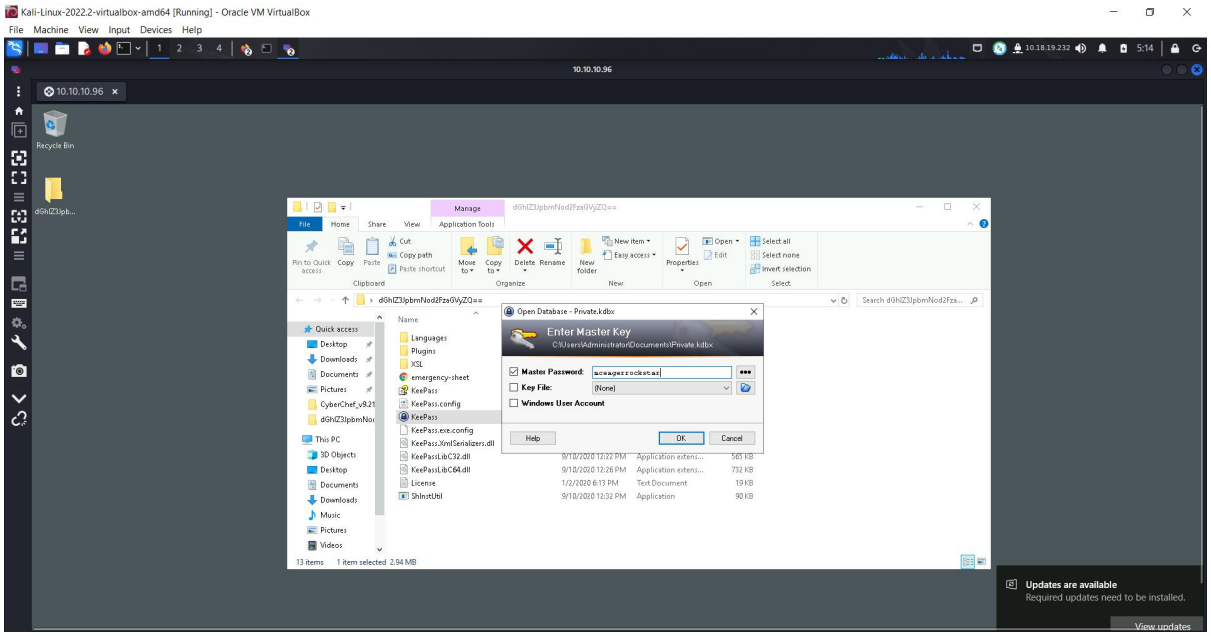
By reading the instructions given by THM, what we need to do next is to located the weird looking title folder and enter into it. Upon entering, we are shown with this page.

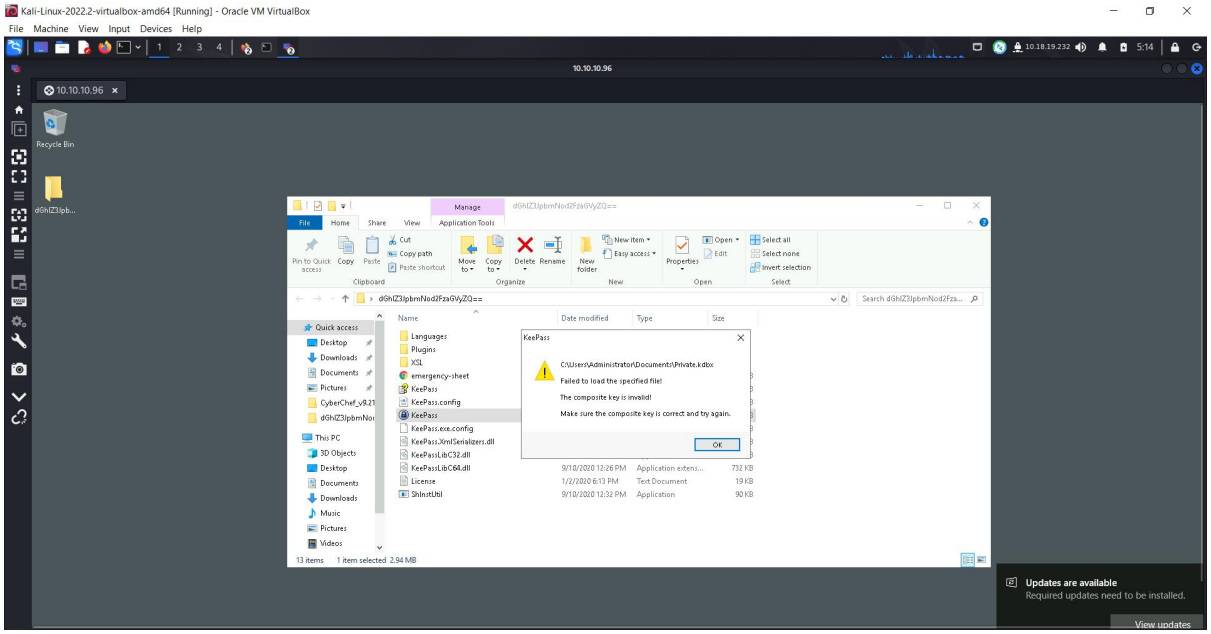


Next, click on KeePass as shown in the instructions. We will then be show a pop up where we need to key in the master key.

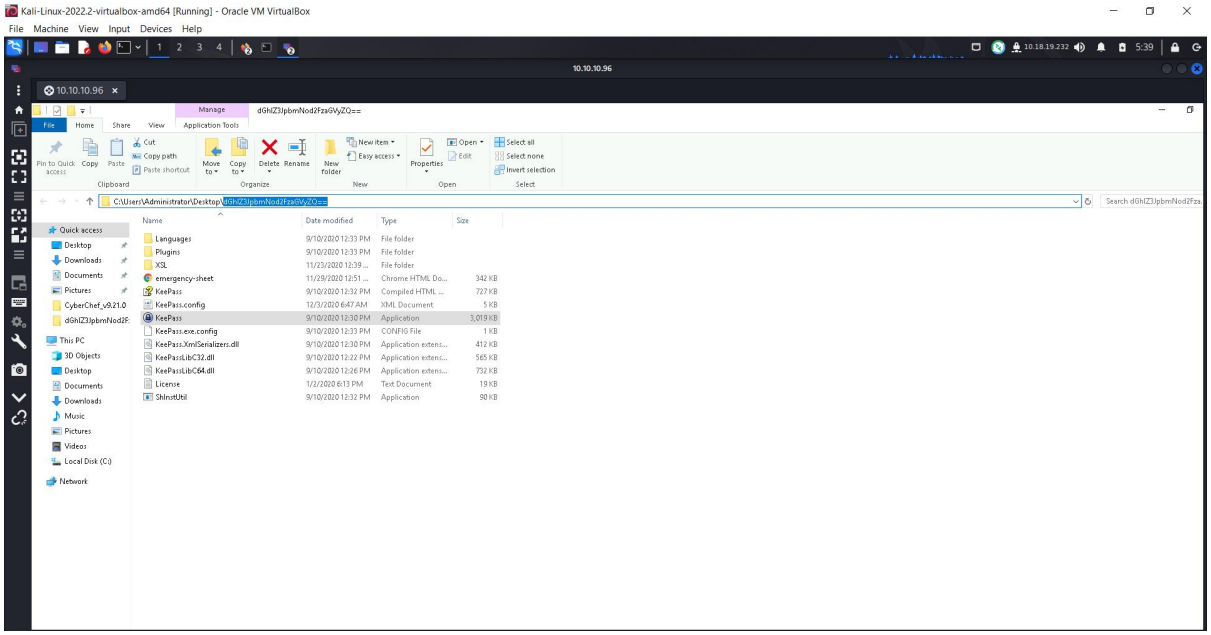


And in the instructions, we are to try out the password key **mceagerrockstar.** So let's go and give it a try.

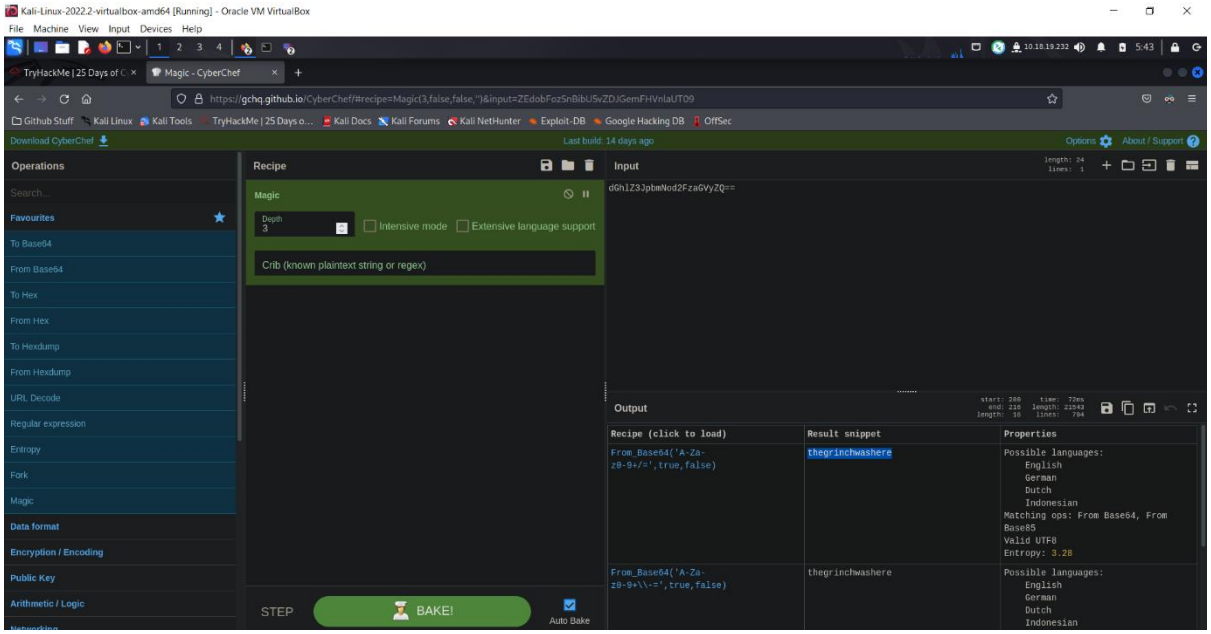




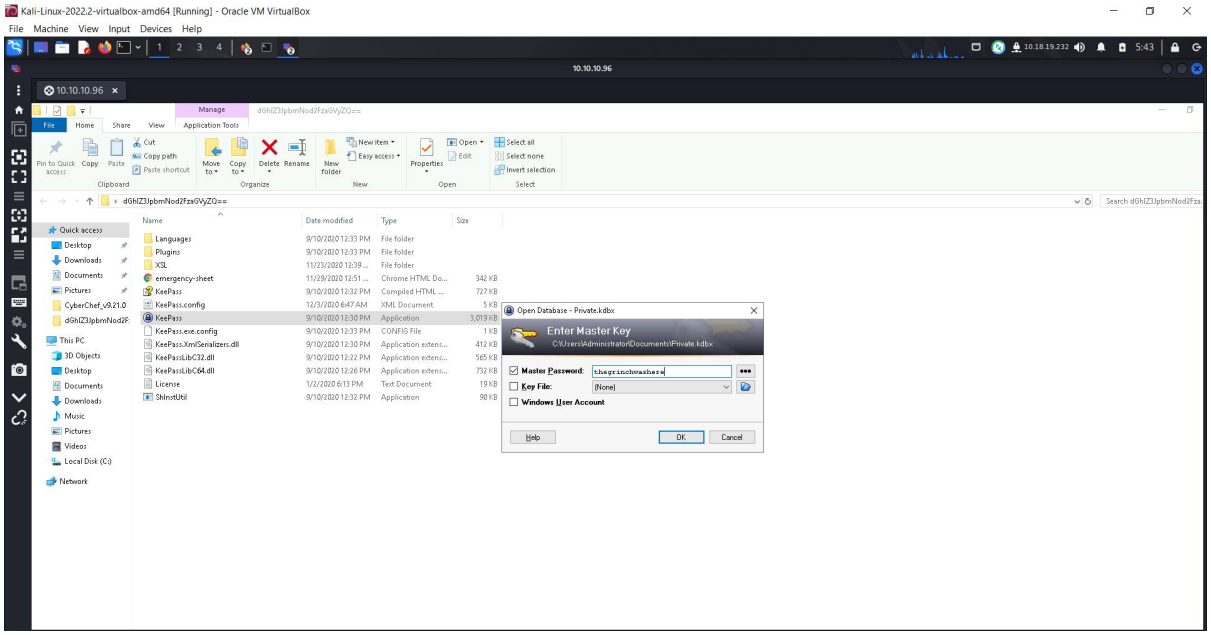
Oh no, it seems like the password given by THM is not the correct one. But wait, there's something that might be able to help us out. Noticed that the folder name is somewhat weird? We could take the name from the folder and decode it.



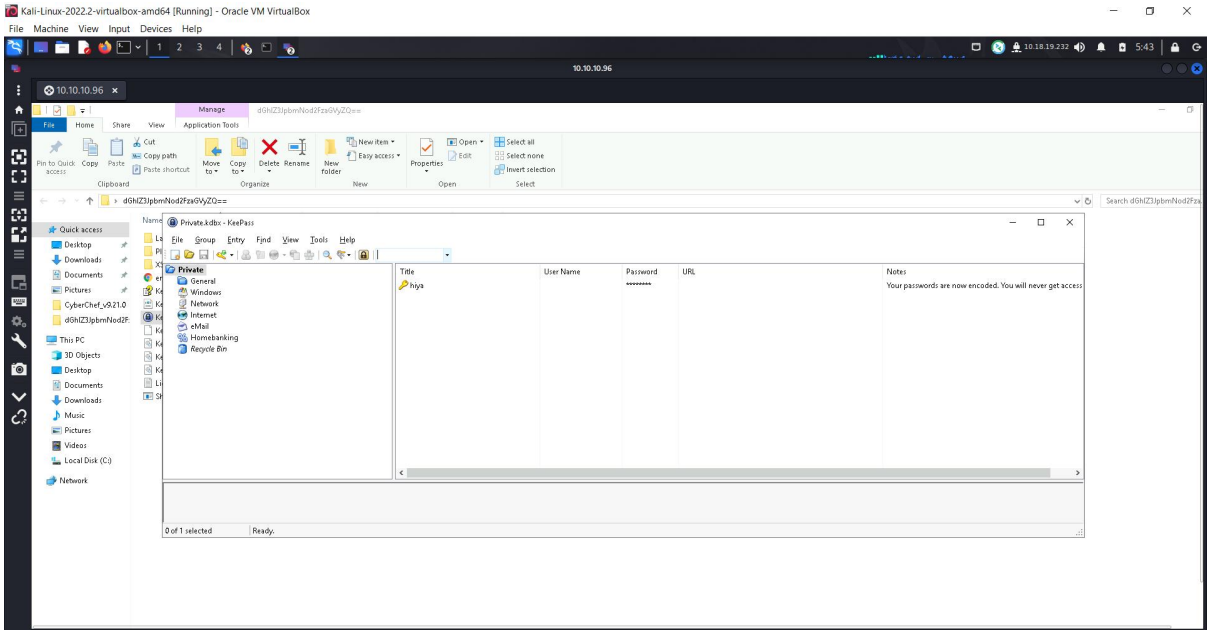
Let's select the name of the folder and copy paste it into our trusty Cyberchef.



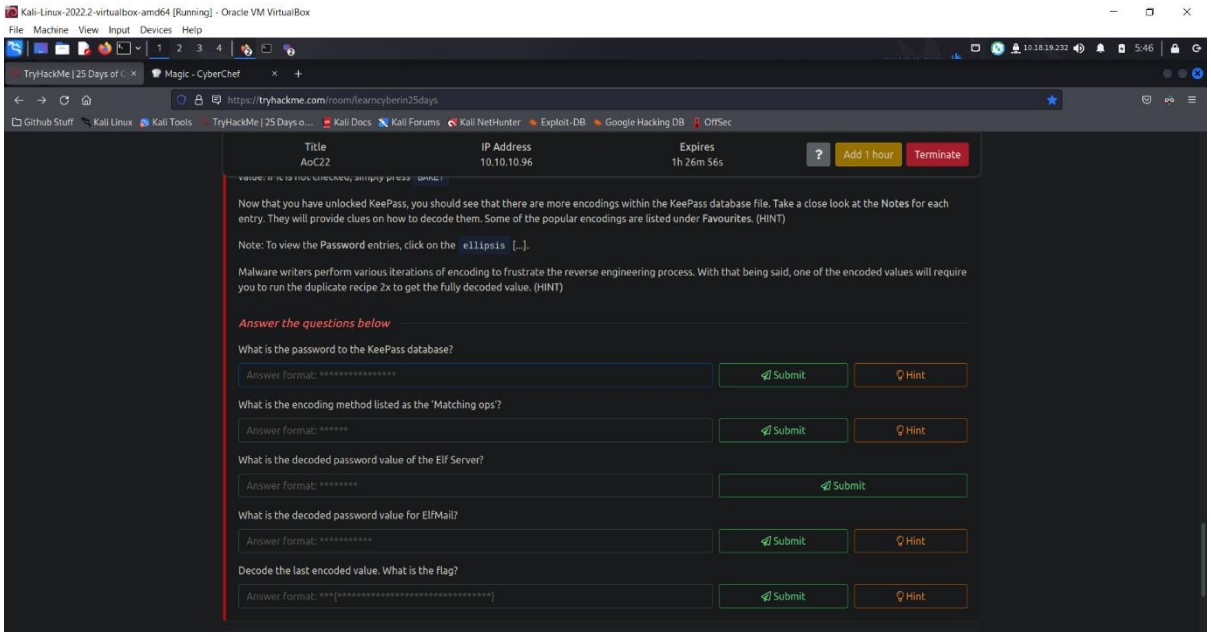
By following the instructions provided in THM, we can use the category Magic to help us decode with ease and efficient. After selecting Magic, we can now put the folder name in and start baking. And there we have it, the password for KeePass. Now let's select it and paste it into our KeePass.



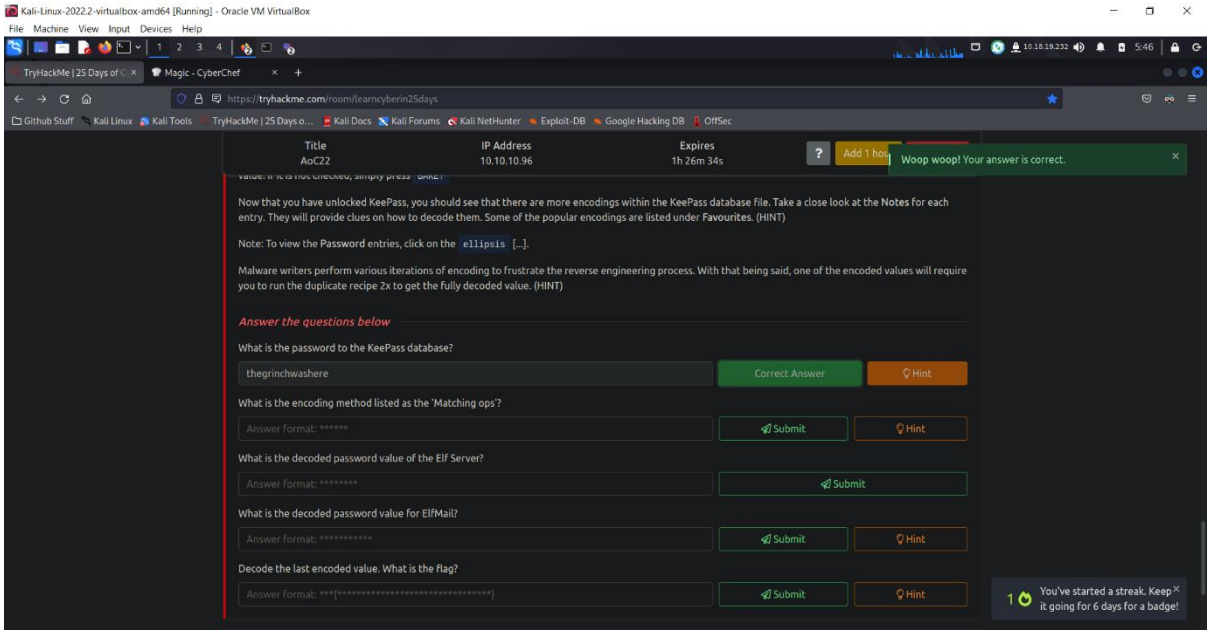
After the password is in, click ok.



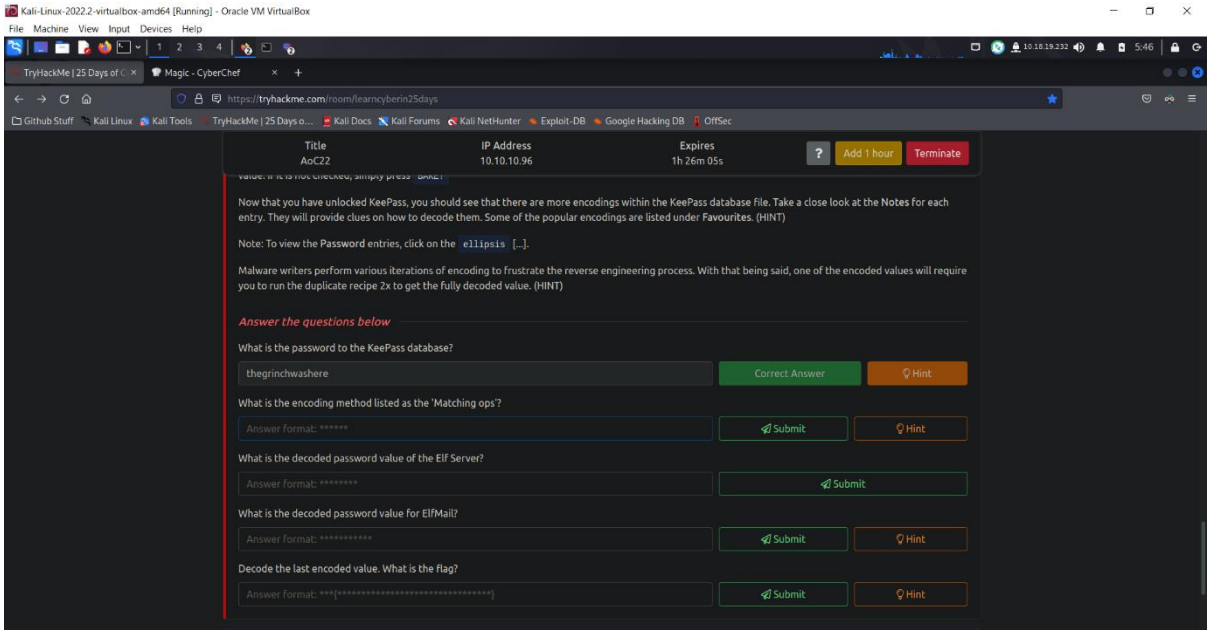
And there we go, we now have access into everything.



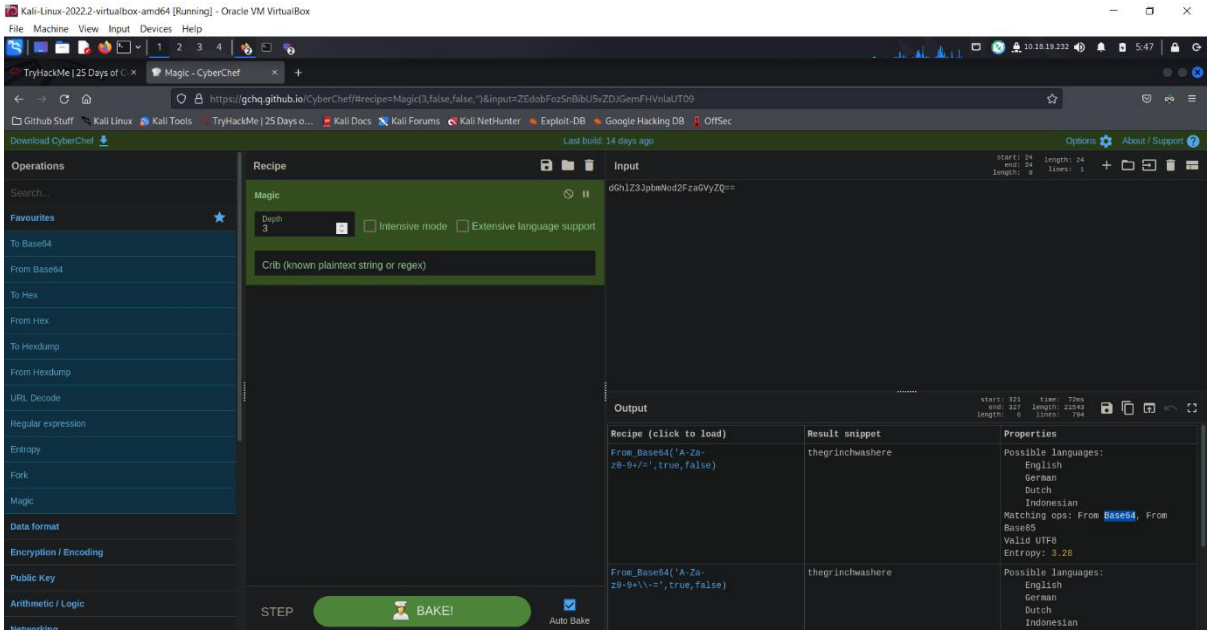
Now, let's take a look at our first question. It seems like we are asked to find the password to the KeePass database, which we already found it, and that would be thegrinchwashere.



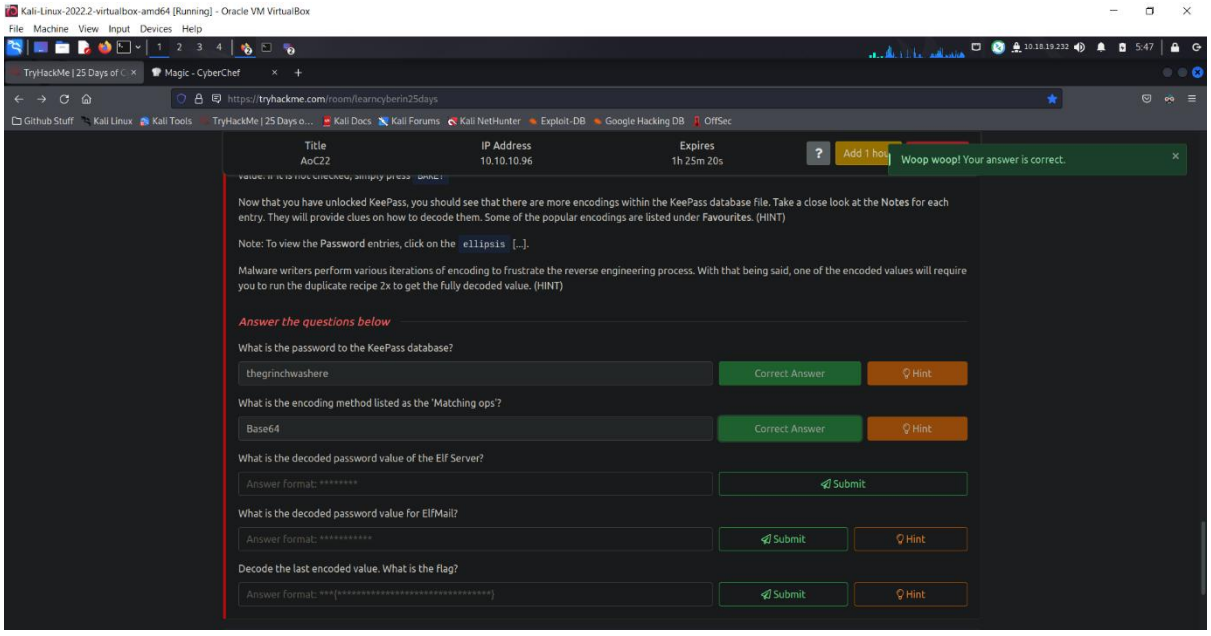
Great, now on to the next one.



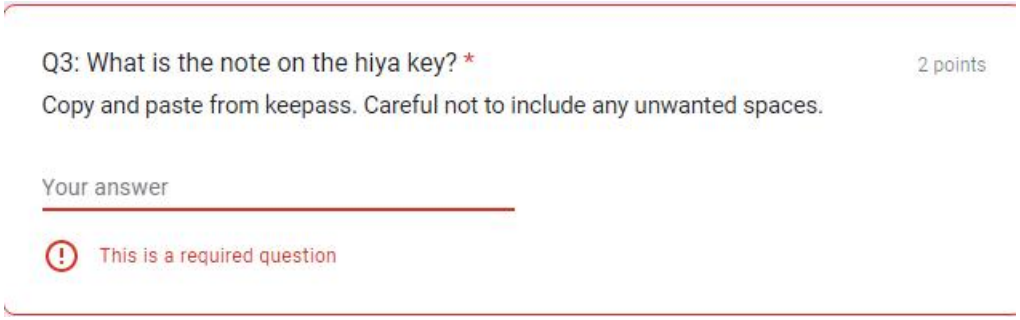
For question 2, we are asked what is the encoding method listed as the 'Matching ops'? Apparently we also already got the answer for this question, and it is found in one of the boxes in the previous decoding.



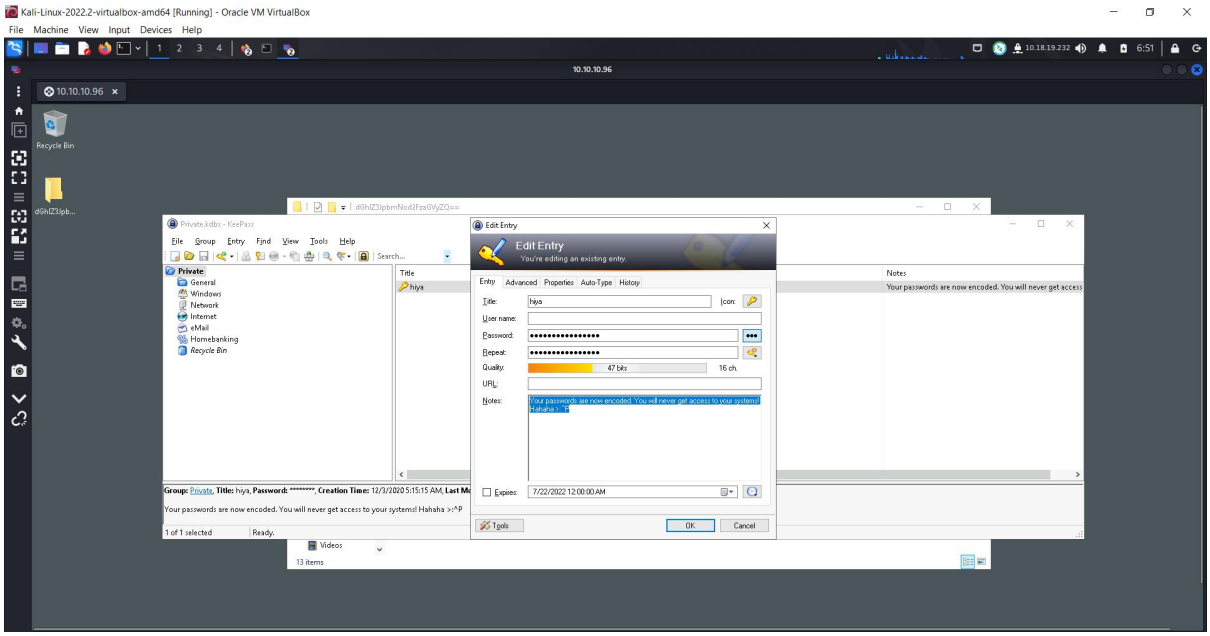
The answer lies in the properties box on the most right side of the box and we can see that the answer is Base64.



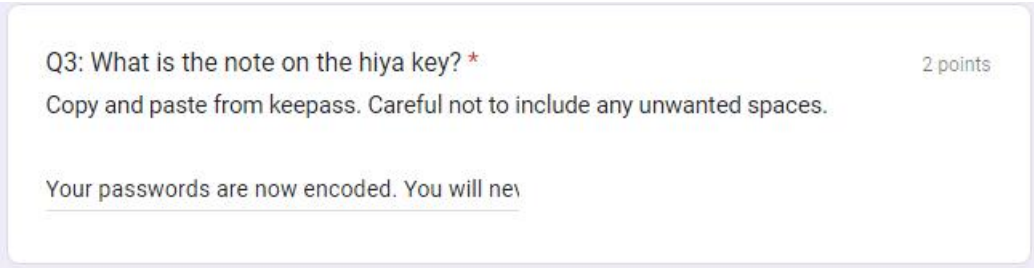
Nice, we got that right too. On to question 3.



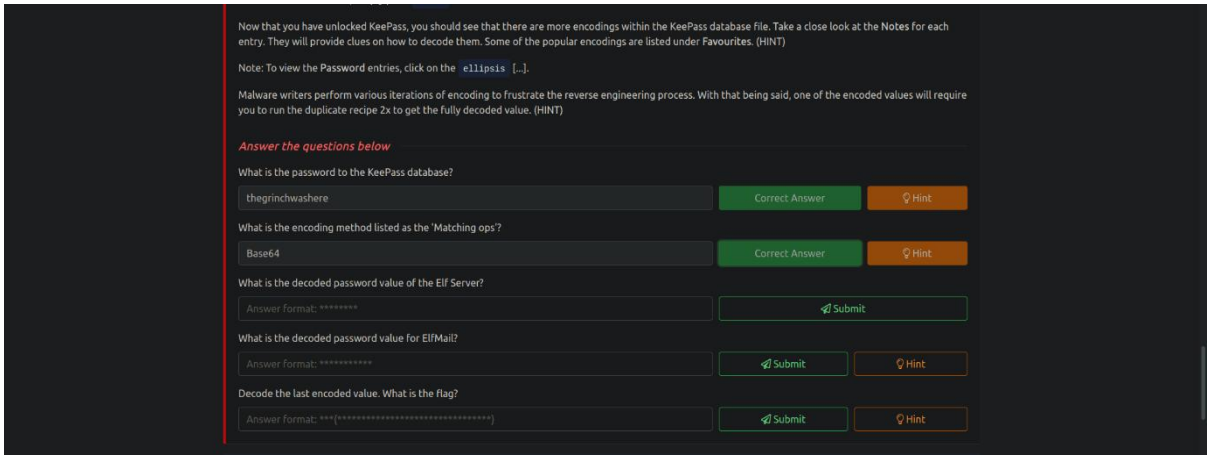
For question 3, it only can be found inside of the google form, so let's read it. It seems like we are to find what are the notes inside of hiya. So let's head to the folder hiya and click into it.



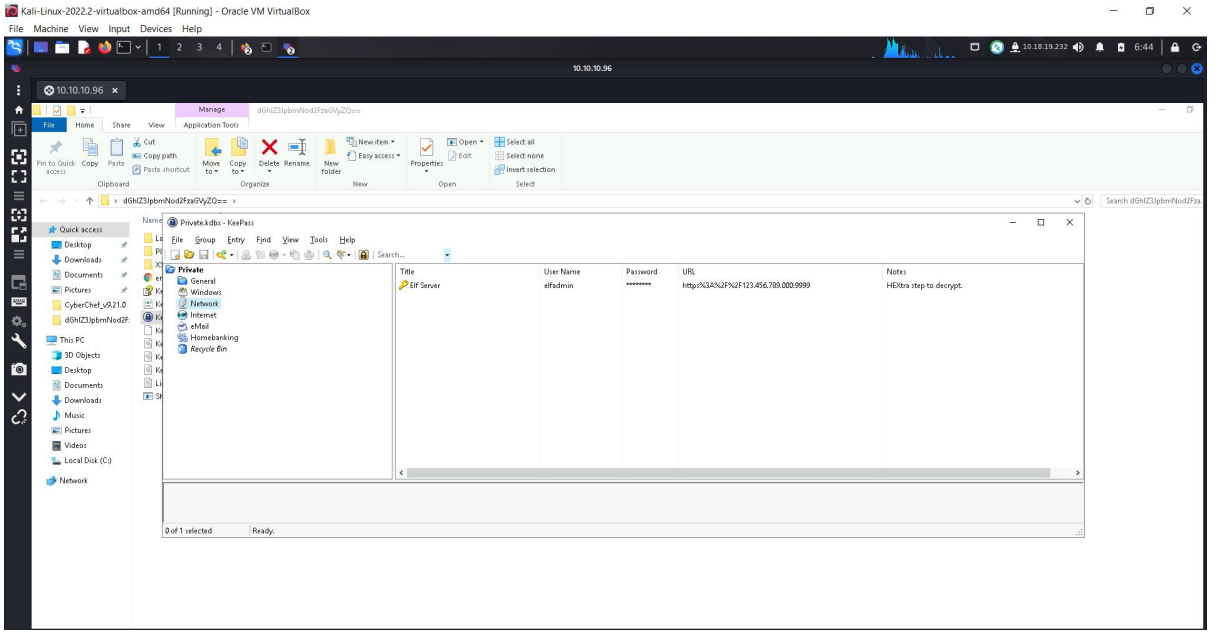
After clicking into it, we can find the notes at the most bottom of the pop up. Which is written as Your passwords are now encoded. You will never get access to your systems! Hahaha >:^P.



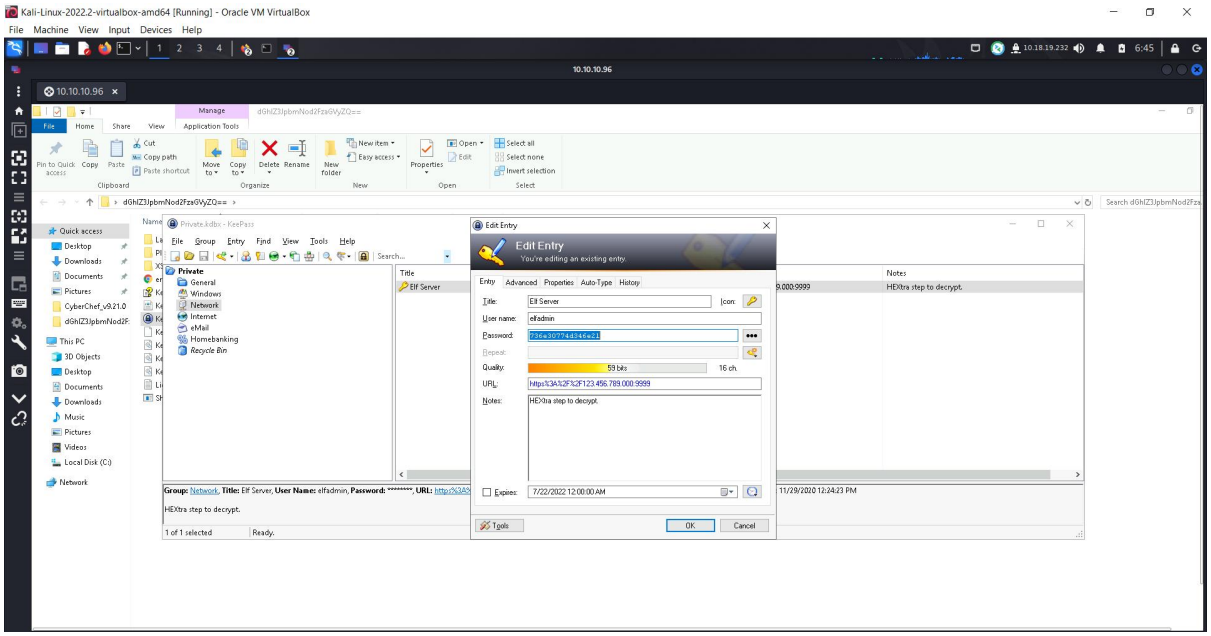
Alright we now have the answer, let's paste it into our google form question and let's move to the fourth question.



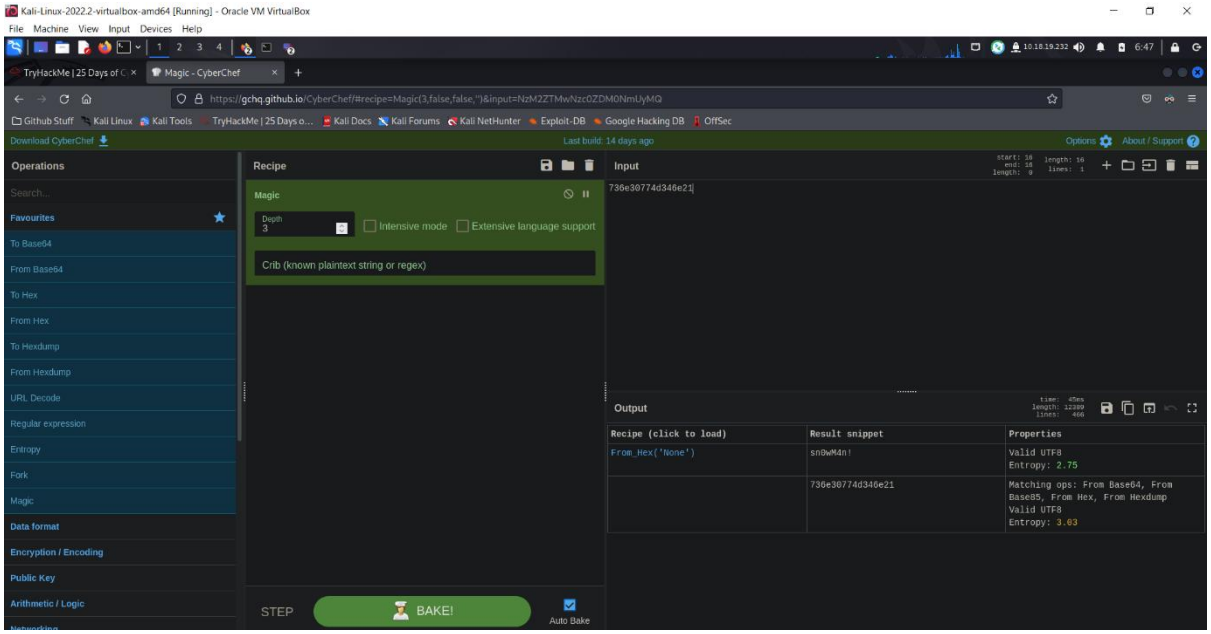
For the fourth question we are asked what is the decoded password value of the Elf Server? So let's go find this Elf Server in the file explorer.



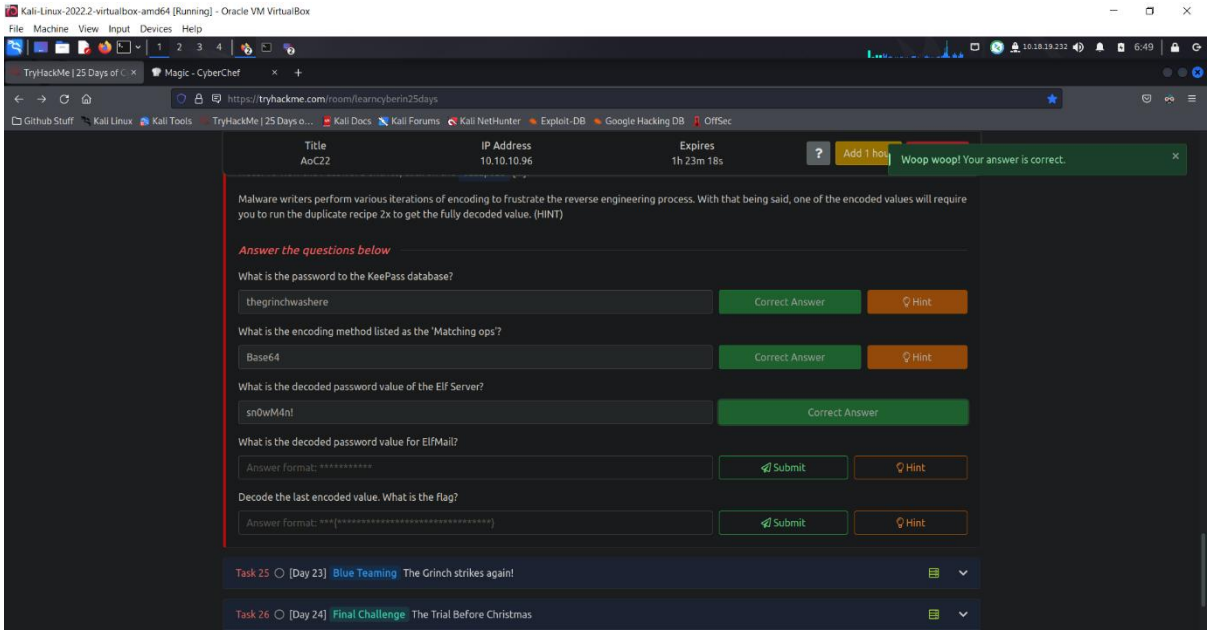
So it seems like the Elf Server is located at Network. So let's click into it and see what happens.



After clicking into it, we are now shown with the details of the Elf Server. Now let's go to the password section and copy it's value in there and paste it into Cyberchef to decode it.

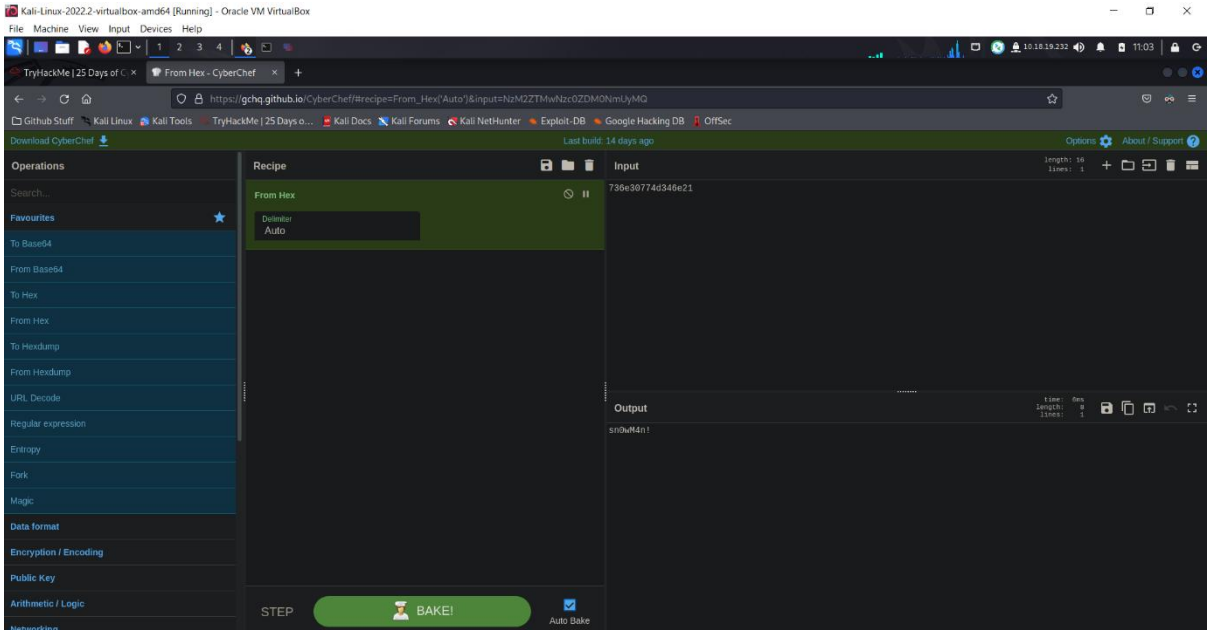


After we have paste it into the decoder, use the category Magic and start our baking. We will then get our answer which is sn0wM4n!. Now we got the answer for question 4, let's paste it in.

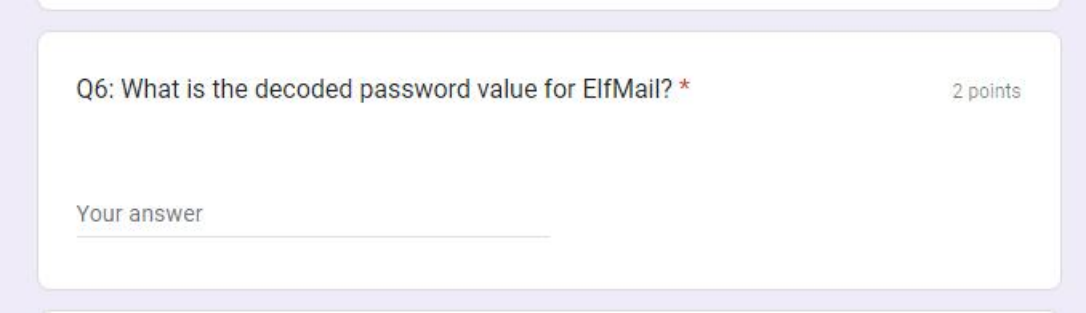


Amazing, we got it right. Now let's move on to question 5.

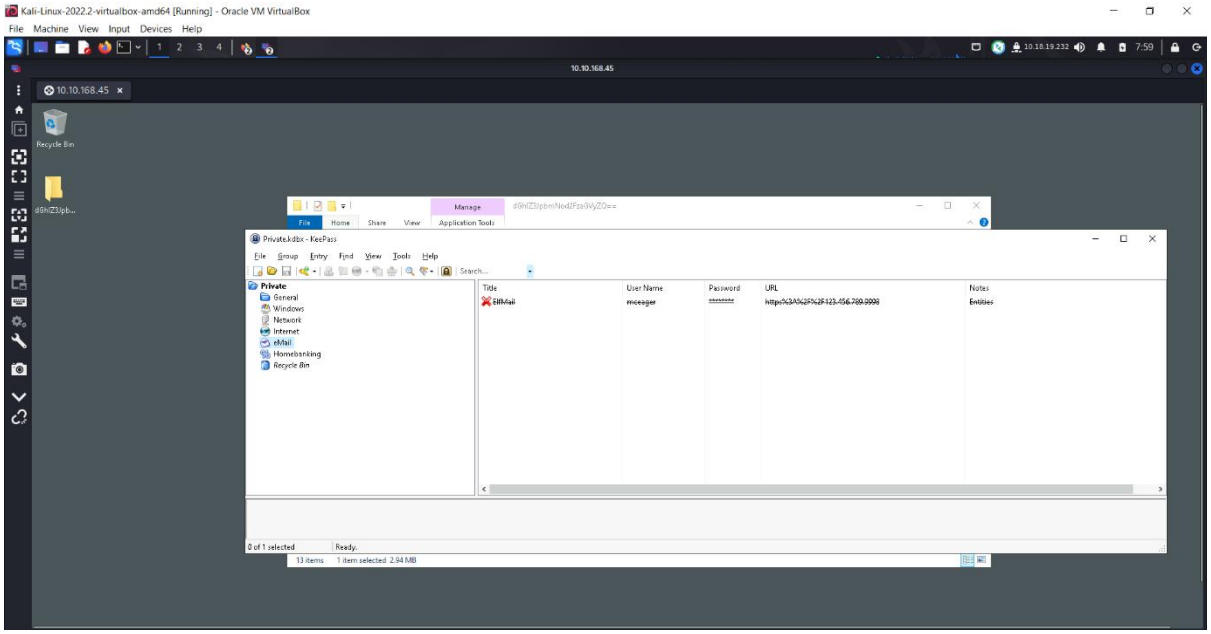
So for question 5 it's quite straight forward. We are asked what is the encoding used on the Elf Server password. So what we can do would be selecting the category in CyberChef and check it one by one.



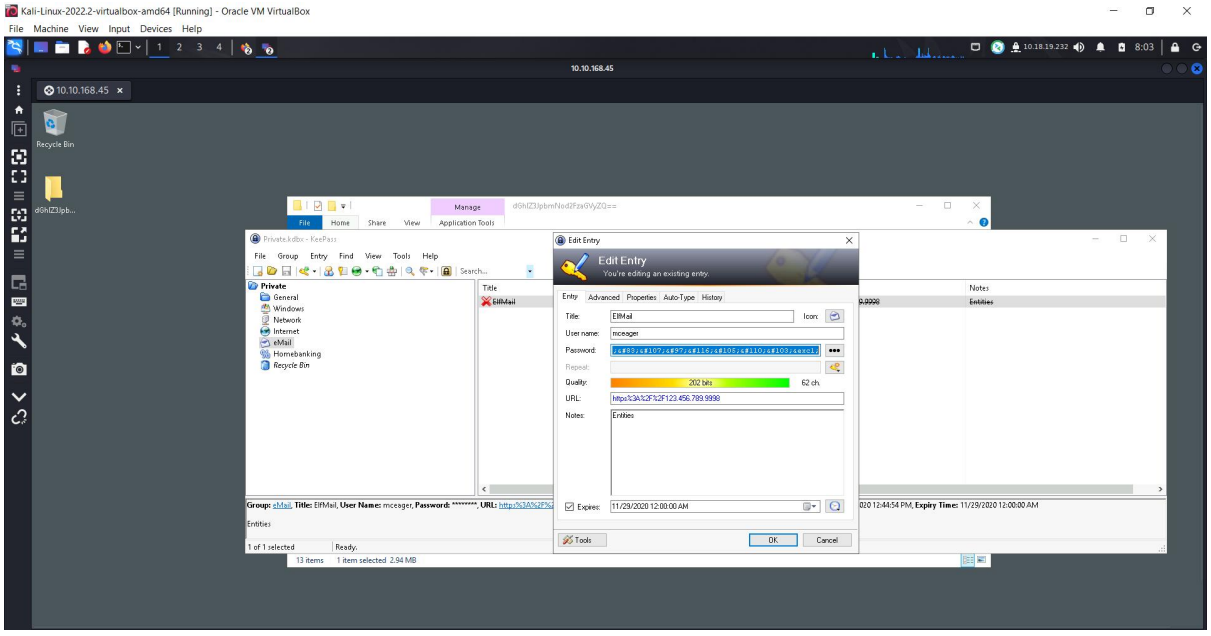
Aha, so we have found out that the answer would be Hex after trying all of them one by one. So the answer for question 5 would be Hex. Now to question number 6.



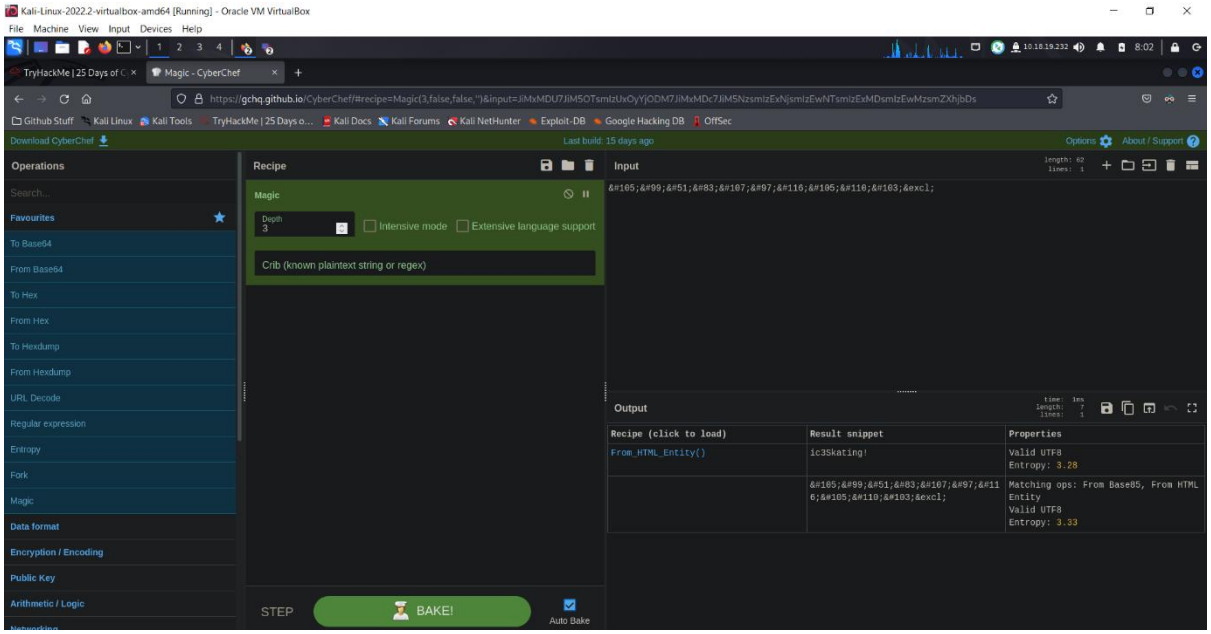
Question 6 ask us what is the decoded password value for ElfMail. So first, let's find where is this ElfMail is located at.



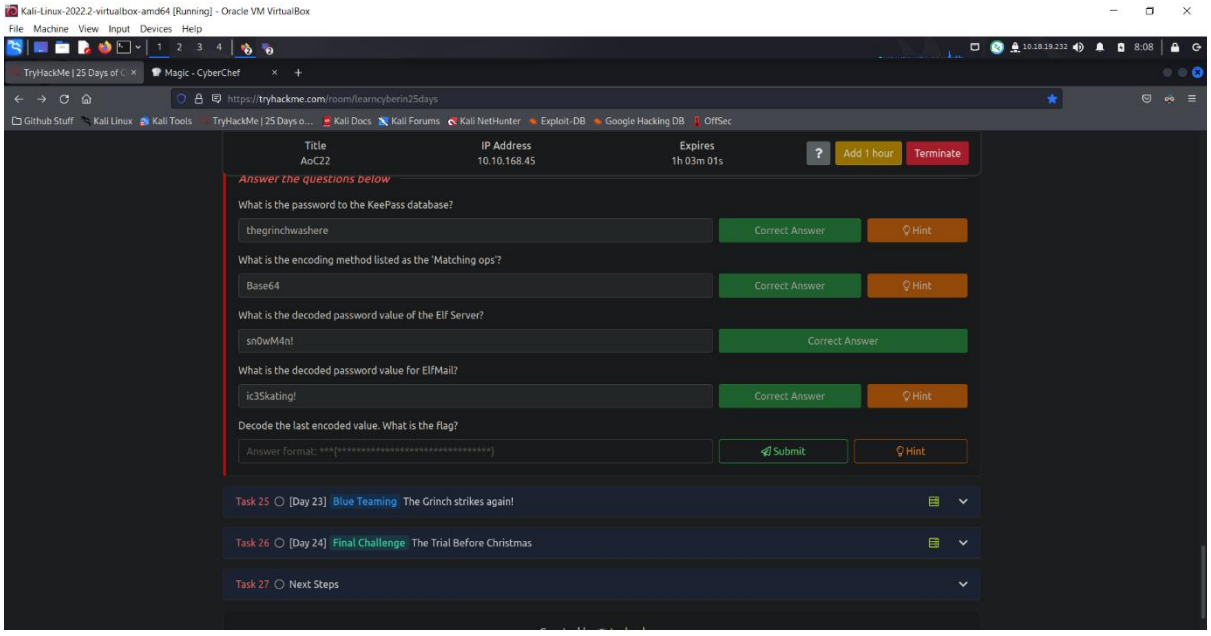
It seems like we have found it, and it's located under eMail. Now we have found it's location, let's go and check it's details.



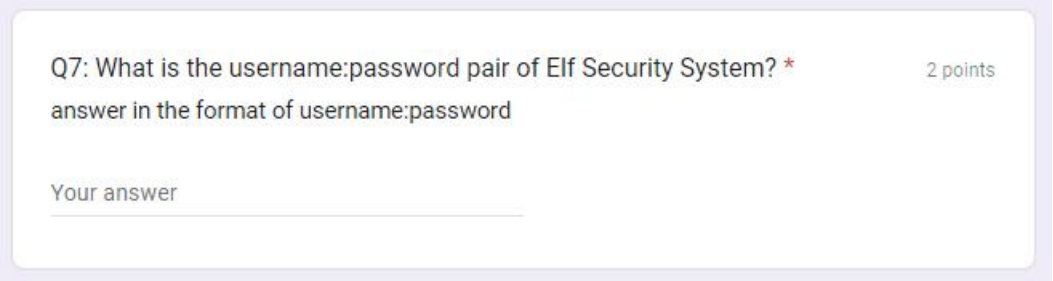
Great, now we got the password, let's head to CyberChef and decode it.



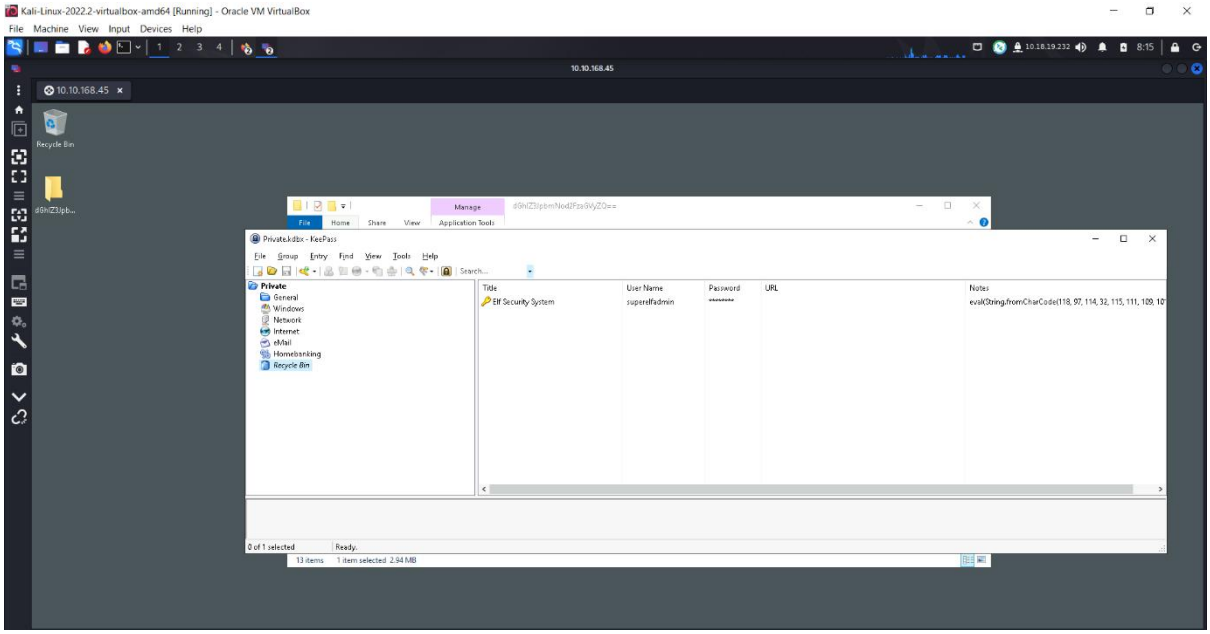
Now, let us insert the password from ElfMail and start the decoding. It seems like we got our answer for question 6, and it's ic3Skating!. Now, let's take the answer and paste it into THM.



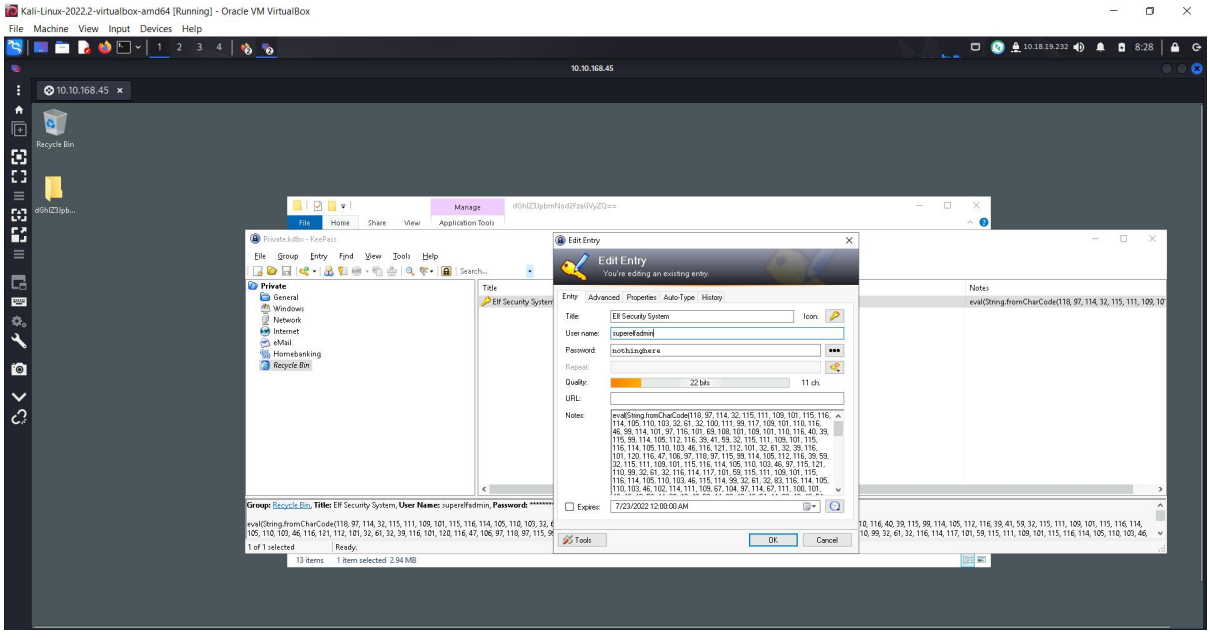
Nice! We got it correct! Now on to question 7.



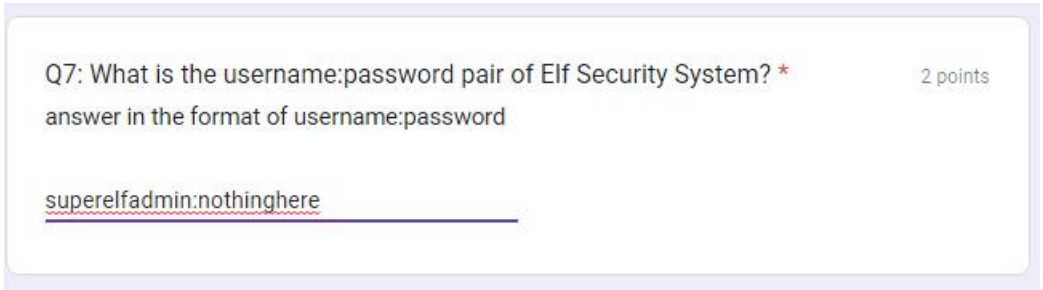
Question 7 wants us to find out the username and password for the Elf Security System. But first, let's find out where is the file located at.



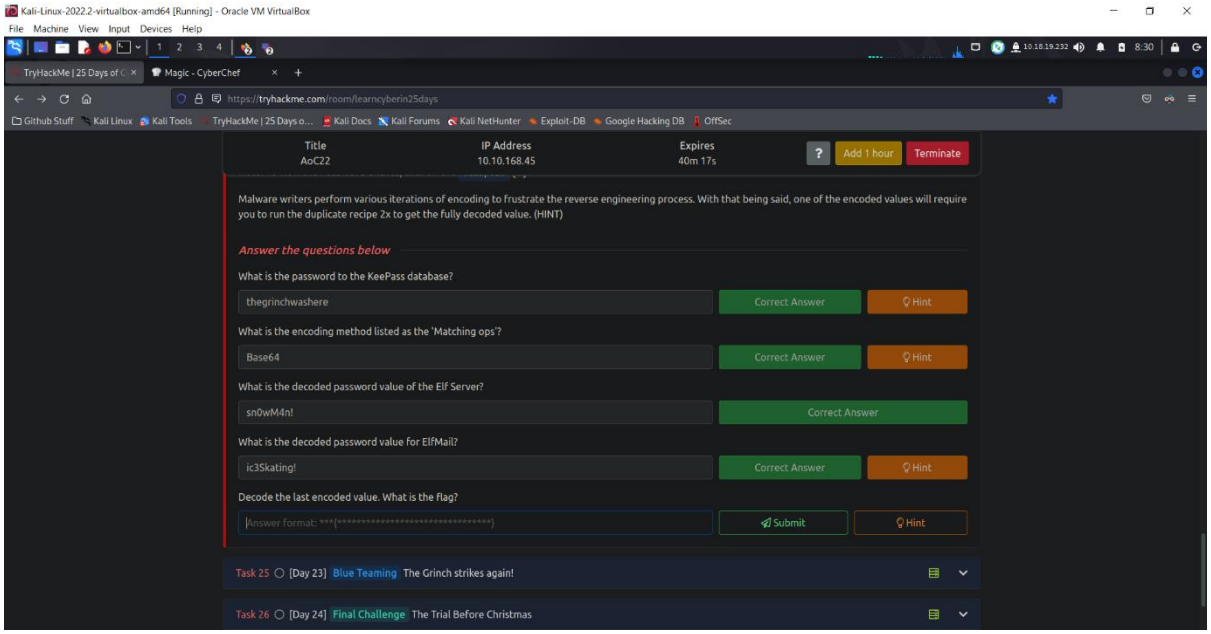
We have found it! It seems like it's located inside of recycle bin, which is funny. So let us continue on our work by first clicking into it and check the details inside.



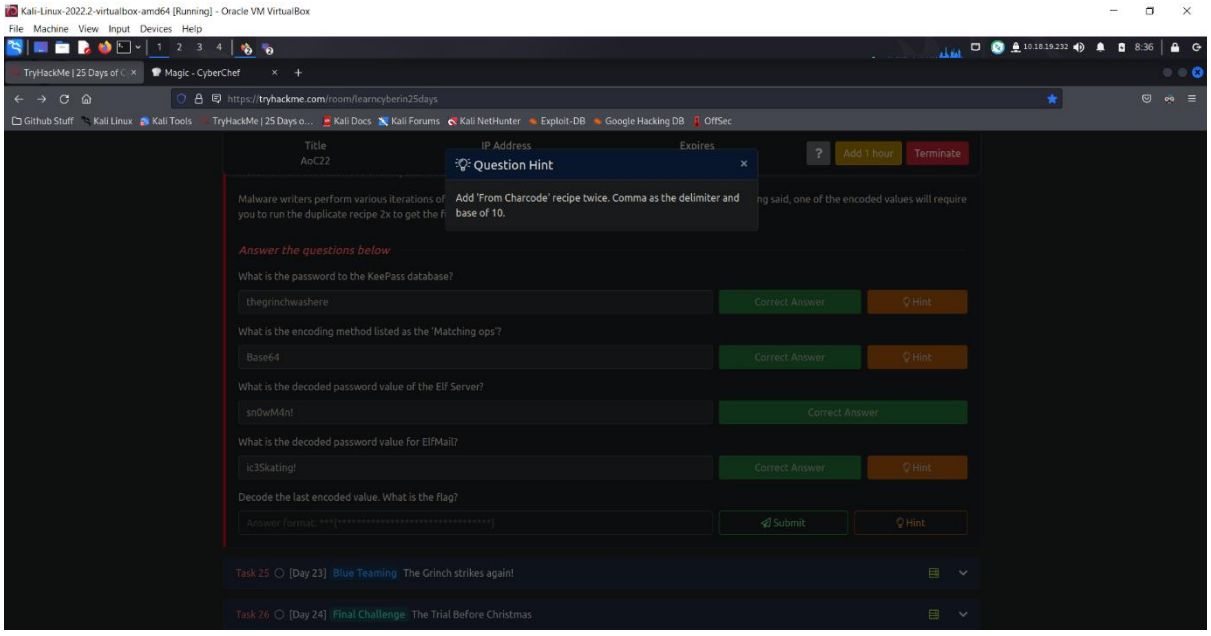
So we are tasked to find the username and the password, and it seems like we have hit the jackpot. So right now we just have to copy and paste it into our question 7 answer box.



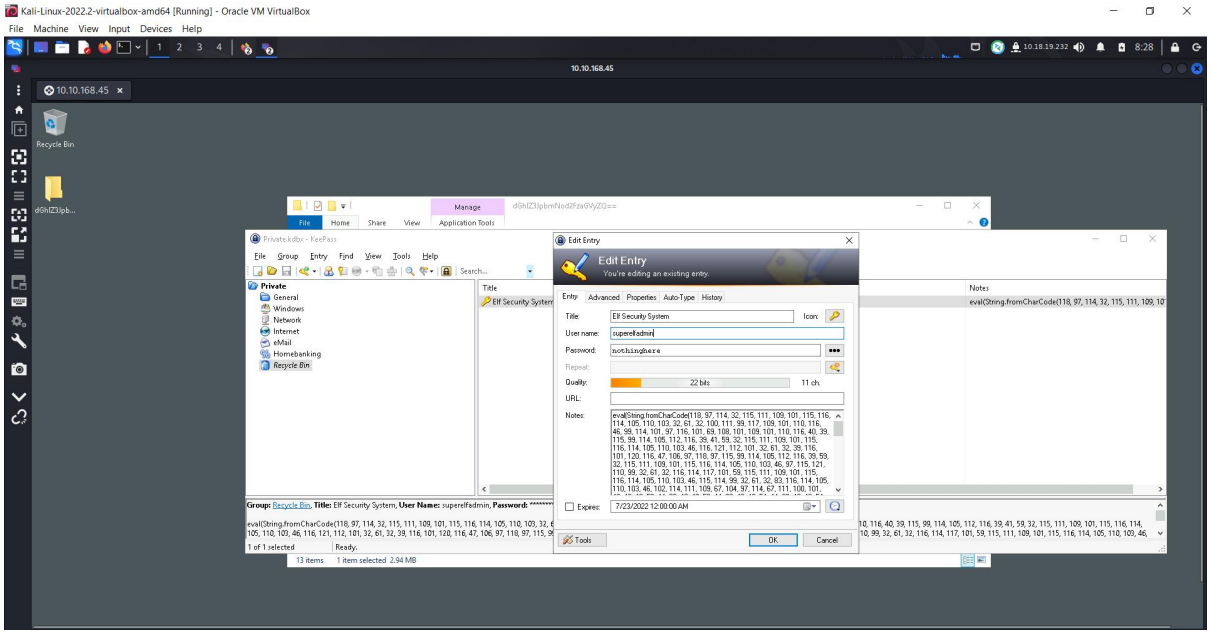
Anddd we're done with question 7!



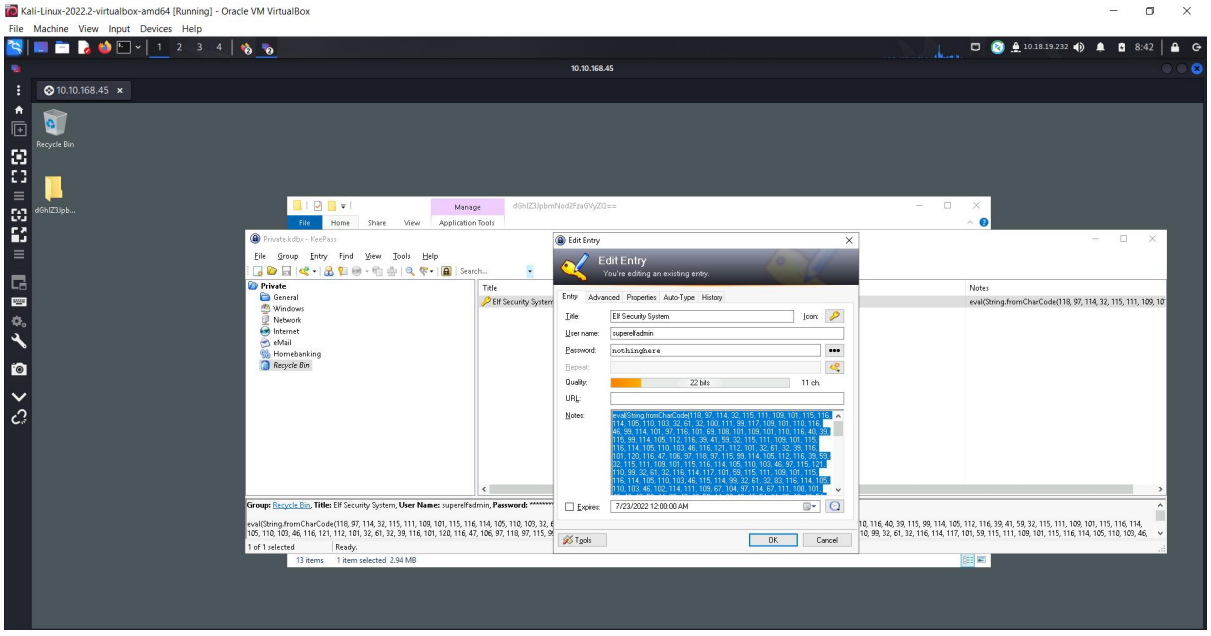
Now to our eighth and final question, we are to decode the last encoded value to find the flag for our final question.



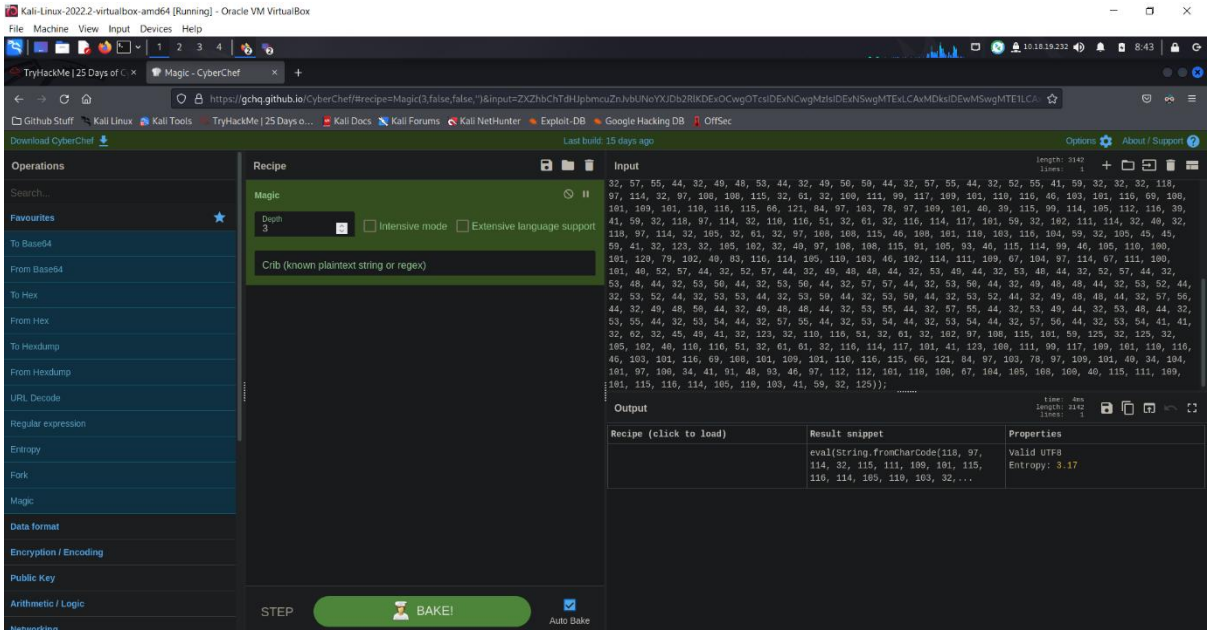
First, let's take a look at our hint. So the hint is hinting us this sentence : Add 'From Charcode' recipe twice. Comma as the delimiter and base of 10. For now we are not sure what does this mean so we shall move on ahead first and see if there's anything related to the hint.



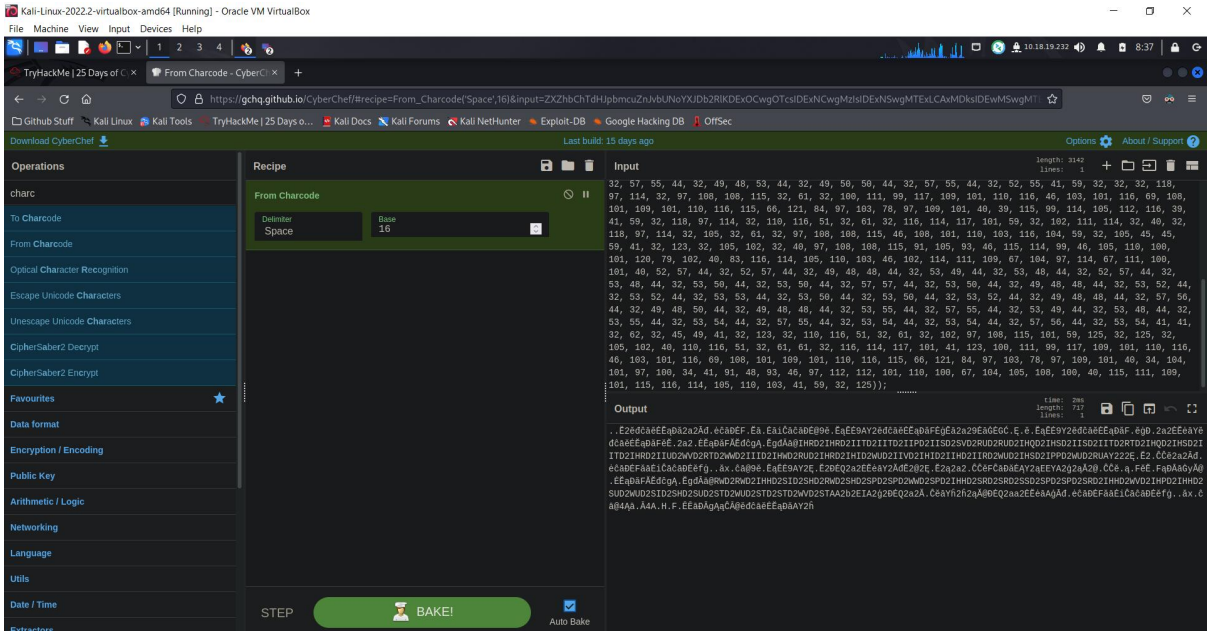
So after searching around for a while, we noticed that there's something in the notes of Elf Security System, let's take a look at it.



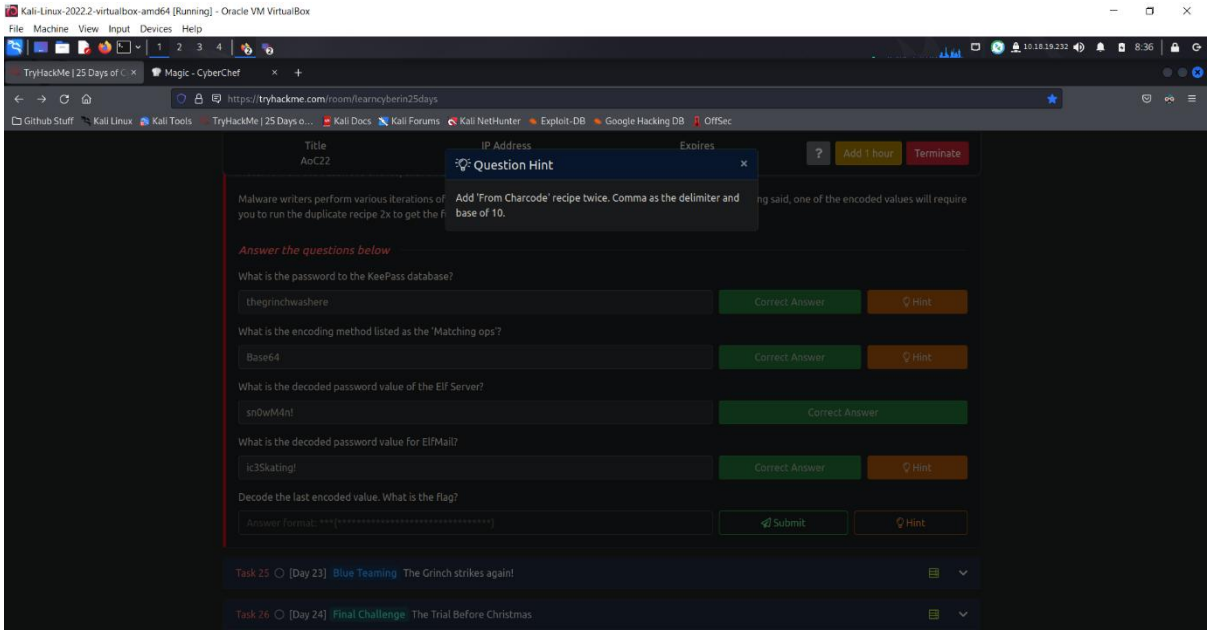
As we take a closer look, it seems like this might be something related to the hint we saw earlier, so let's copy all these and try decoding it.



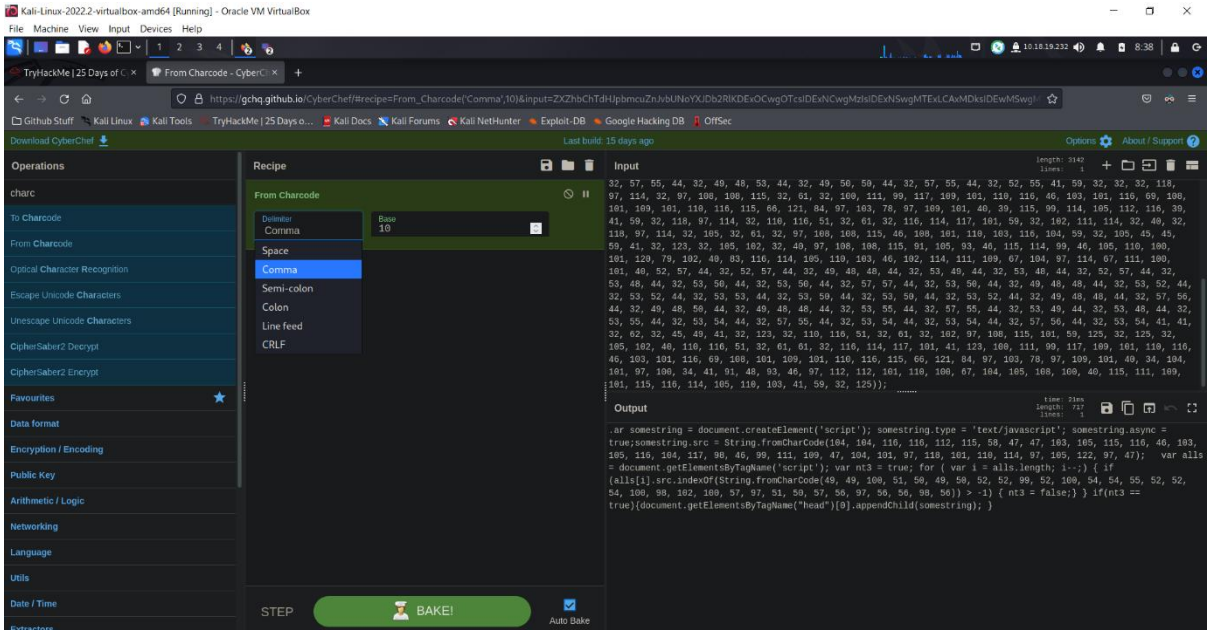
Huh, it seems like Magic isn't doing the trick. But in the output it says something about eval(String.fromCharCode). Maybe it's trying to tell us to use other method to decode it. So let's try and find the word CharCode in the receipt.

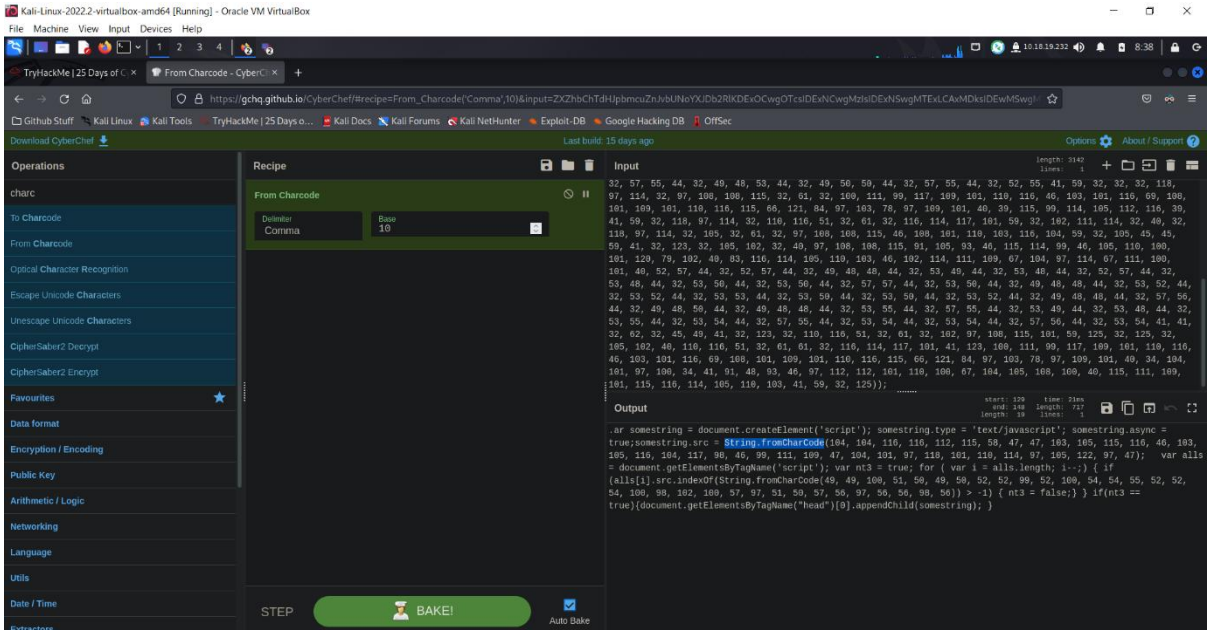


Apparently something changed, but it's still gibberish in the output, let's go back and take a look at the hint.

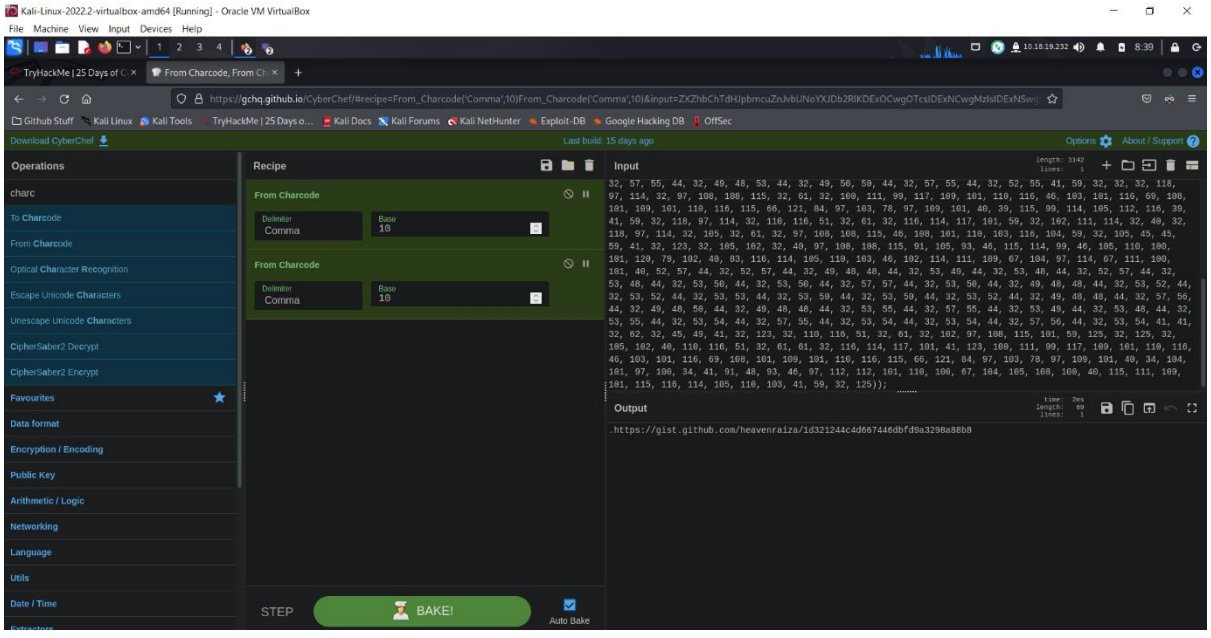


The hint from before is telling us add 'From Charcode' recipe twice. Comma as the delimiter and base of 10. Which means we just have to change the Delimiter and Base! Let's go and change it now.

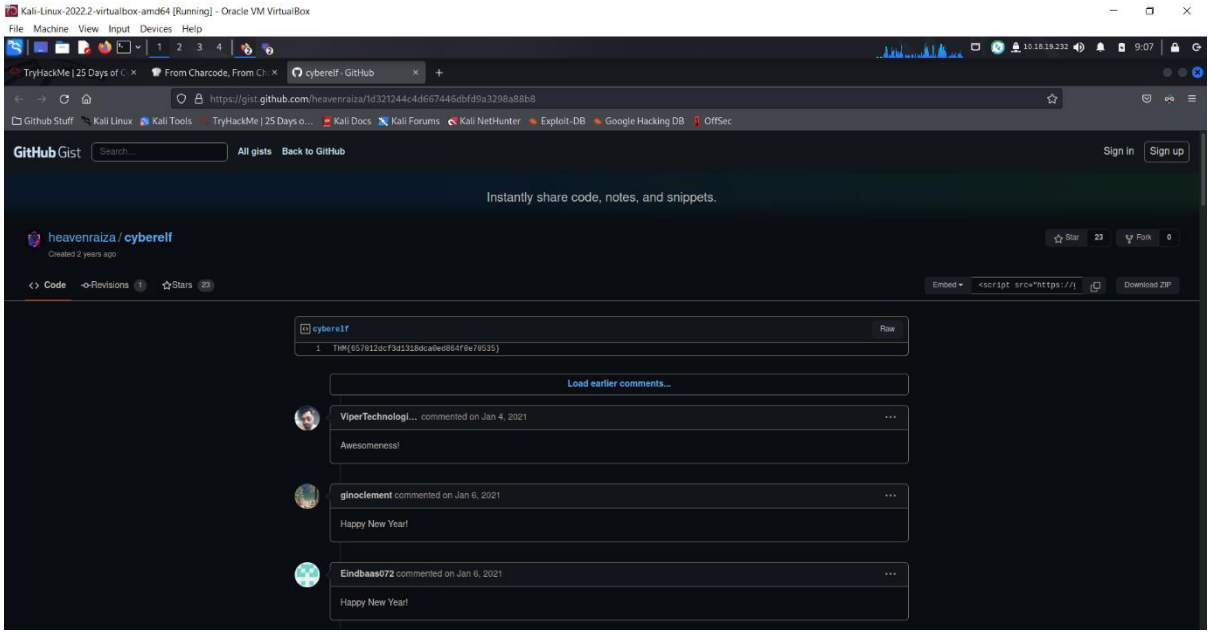




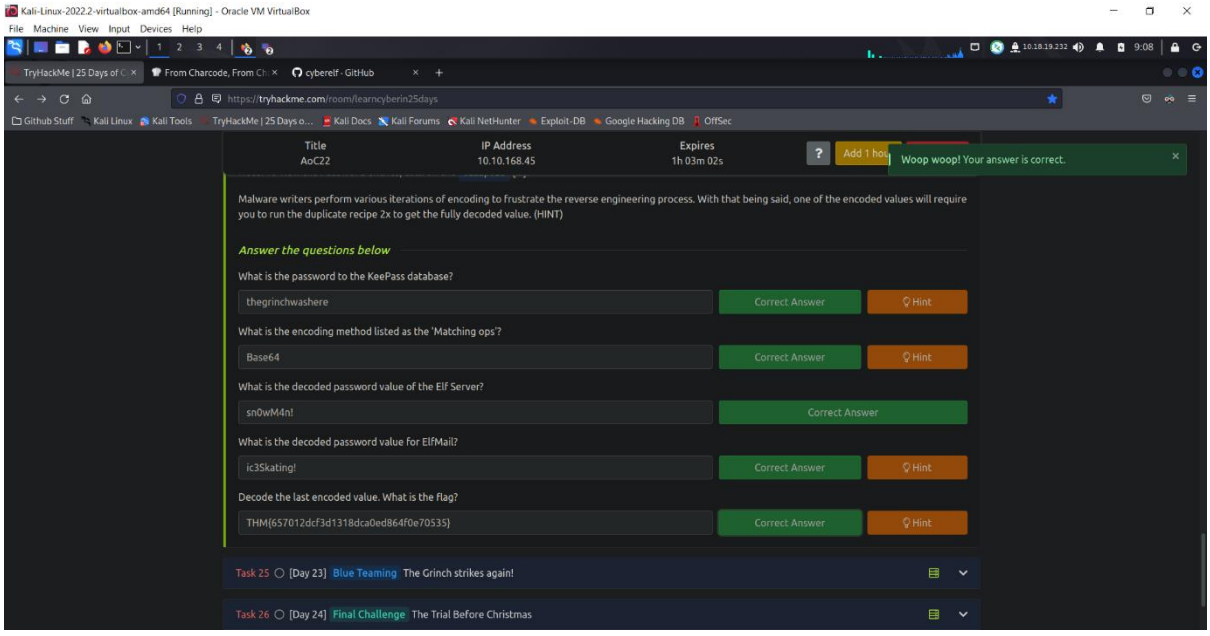
After we're done changing everything, we are shown with this output, apparently it's hinting us to insert one more receipt in order to fully decode it.



Ah, it seems like we are shown with a website link, let's copy it down and search for it.



Ah Ha, we have found the Flag for our final question. Let's copy it down and paste it in our answer box.



Yipee!! We are finally done with Day 22!!

End of Day 22 report

PSP0201

Week 6

(DAY 23)

Writeup

Group Name: Nvida

Members

ID	Name	Role
1211102656	Dennis Ng Chun Hung	Leader
1211101408	Ephrem Loo Ee Zhe	Member
1211102910	Khoo Jen-Au	Member
-	-	-

Tools Used:
Kali Linux , Firefox

[Day 23] The Grinch strikes again!

Question 1: What does the wallpaper say?

Log into the given server with the credentials using Remmina.

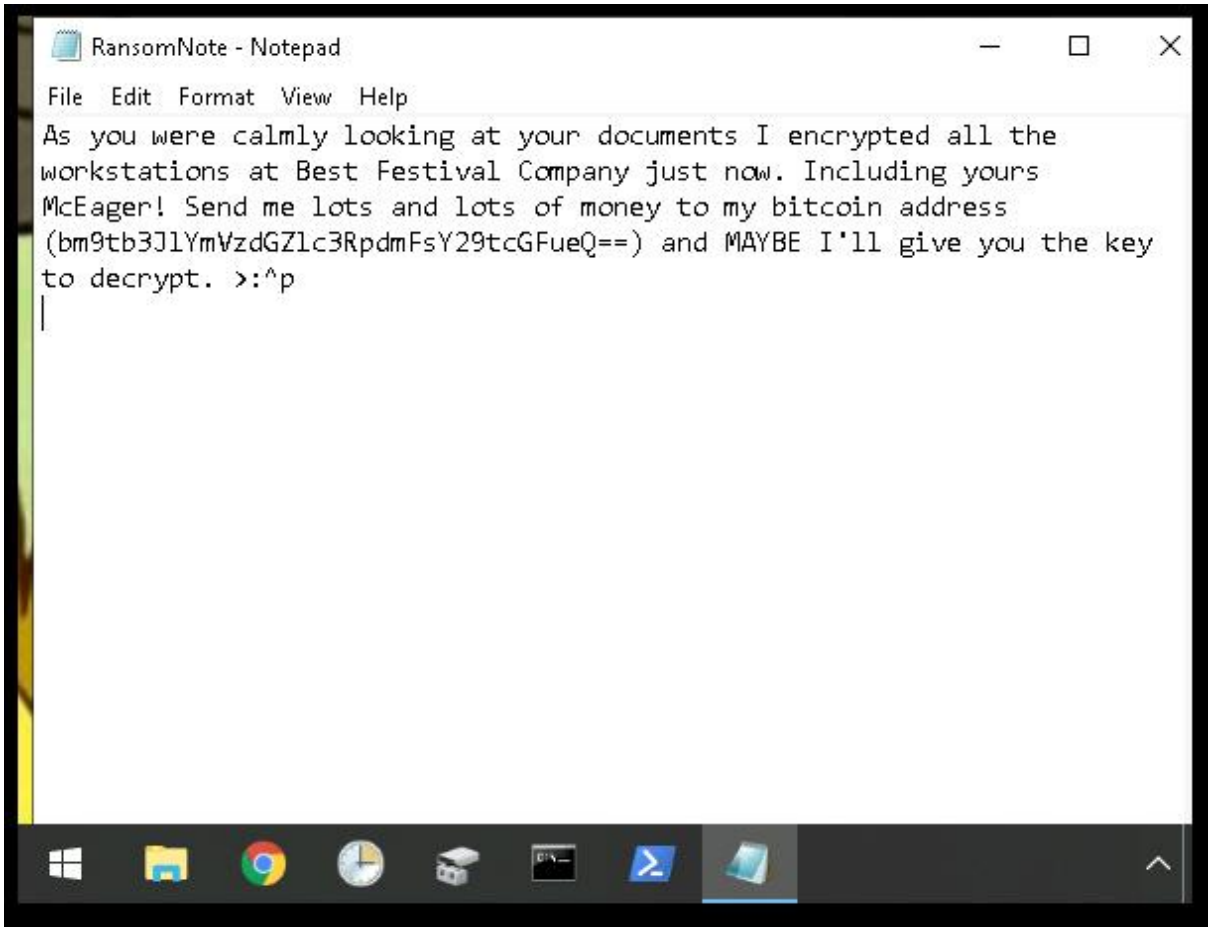
Click on connect.

Answer: THIS IS FINE

Question 2: Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?

Open the RansomNote.

Copy and paste the “bitcoin address” inside the note, and decrypt it.

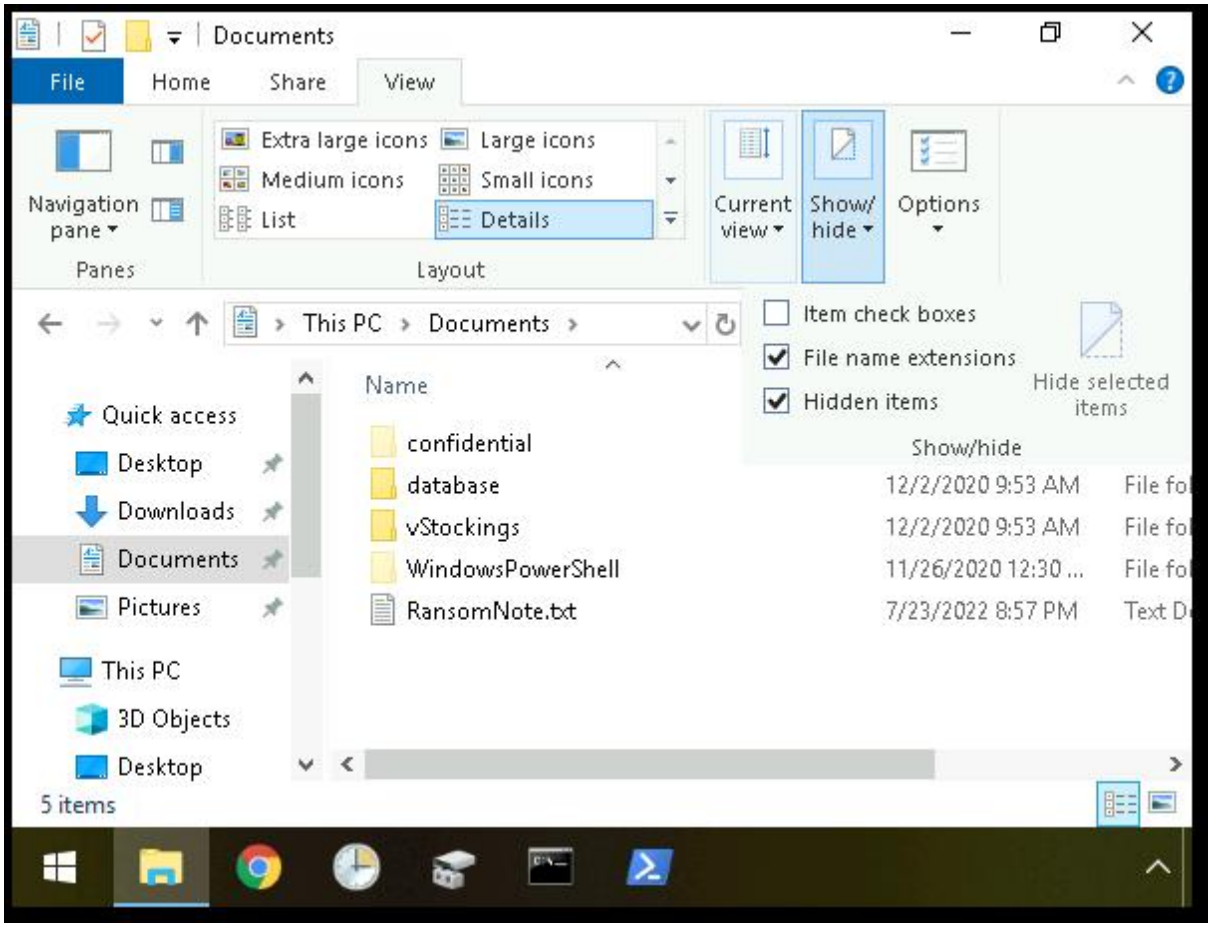



```
root@ip-10-10-58-61:~# echo "bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==" | base64 -d
nomorebestfestivalcompanyroot@ip-10-10-58-61:~#
```

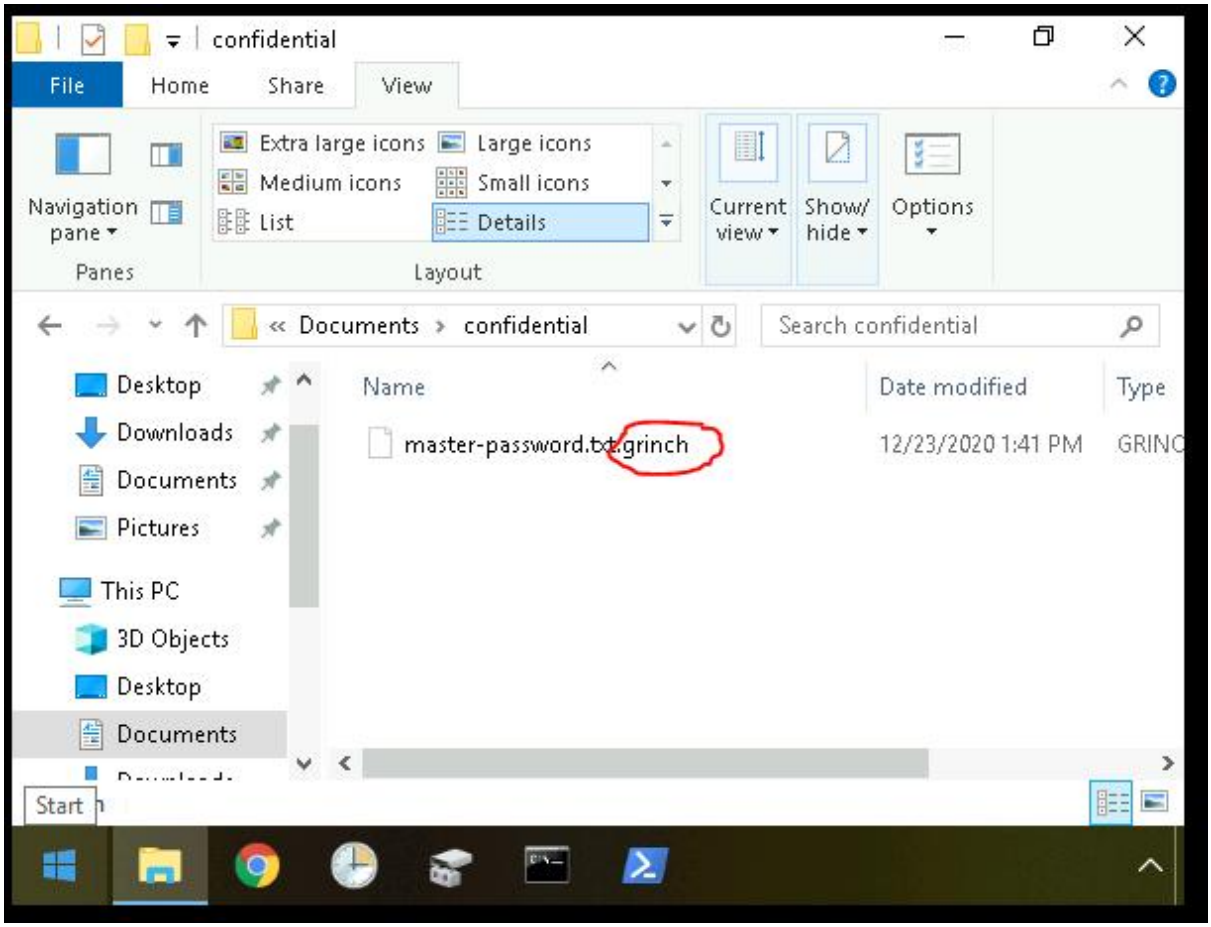
Answer: nomorethebestfestivalcompany

Question 3: At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files?

Remember to show hidden items and file name extensions so it's easier to locate the text file.



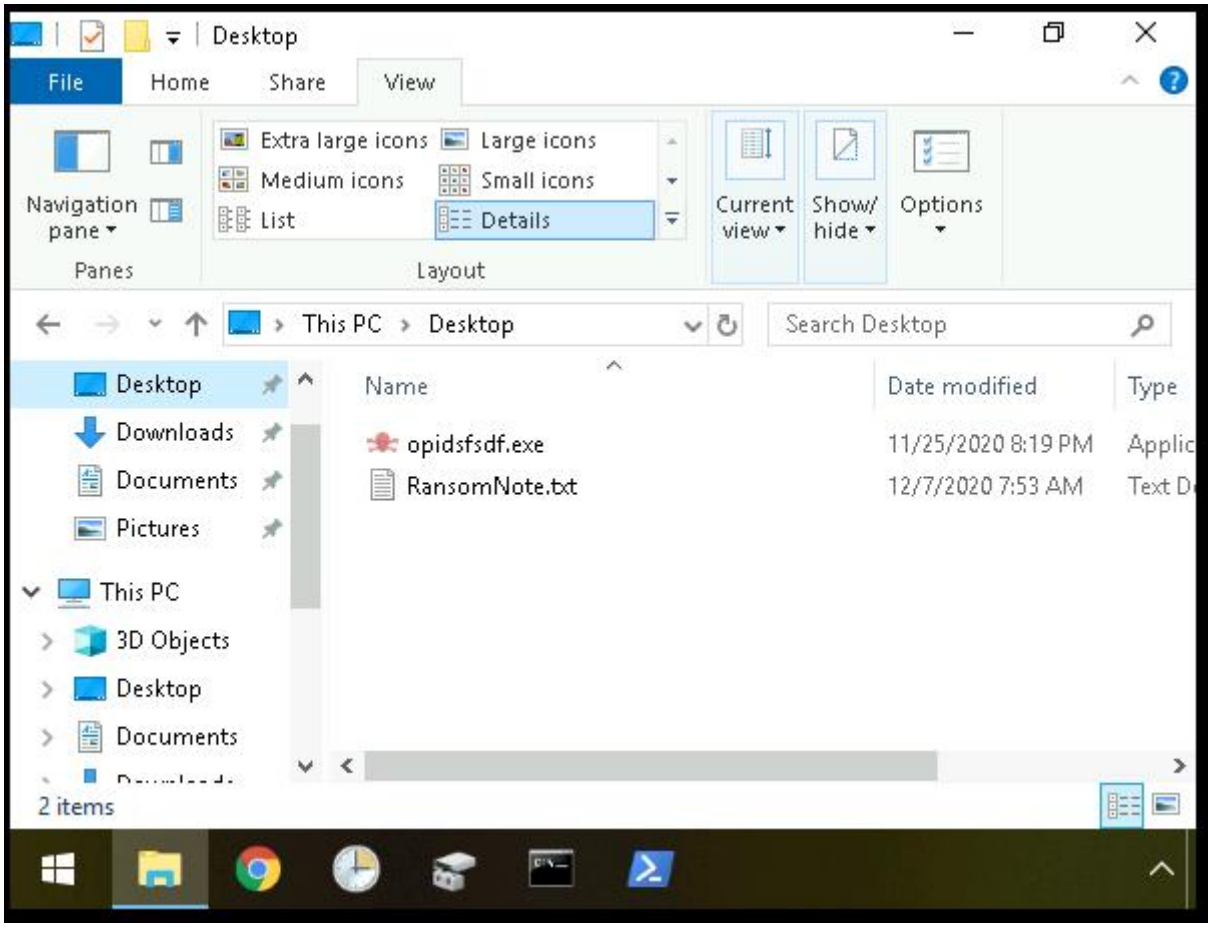
Look into the “confidential” file. There will be a text file in it.



Answer: .grinch

Question 4: What is the name of the suspicious scheduled task?

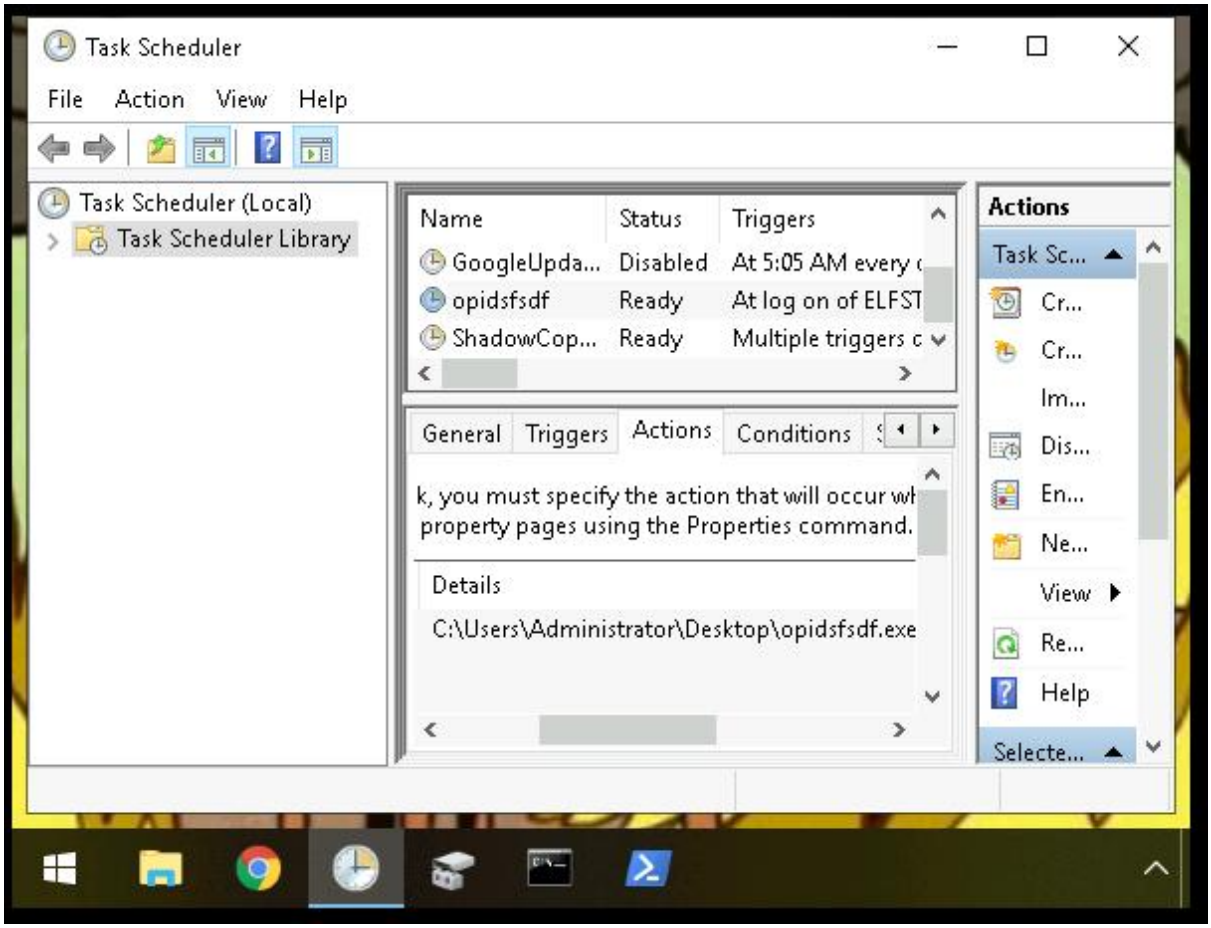
The scheduled task is the one on the desktop.



Answer: opidsfsdf

Question 5: Inspect the properties of the scheduled task. What is the location of the executable that is run at login?

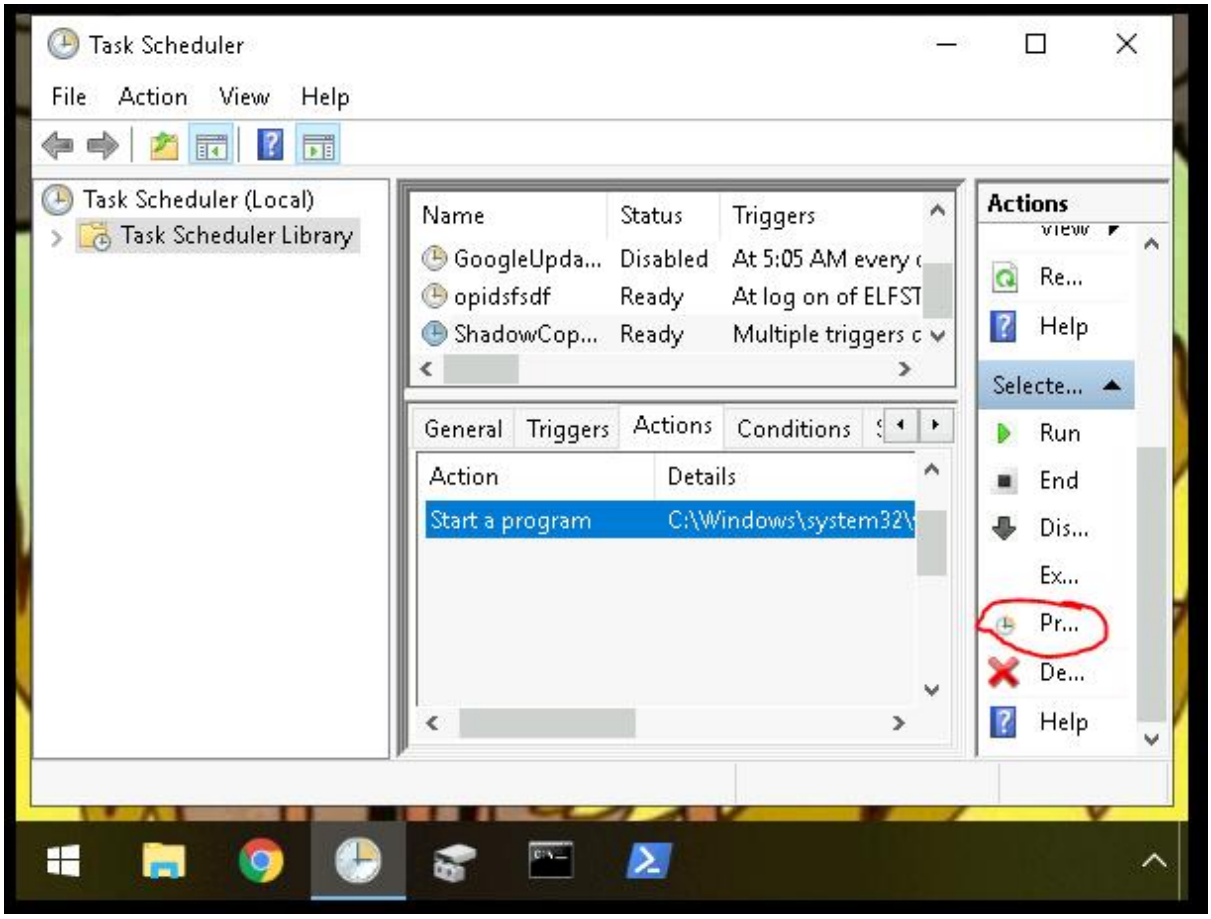
Click into the “Actions” tab



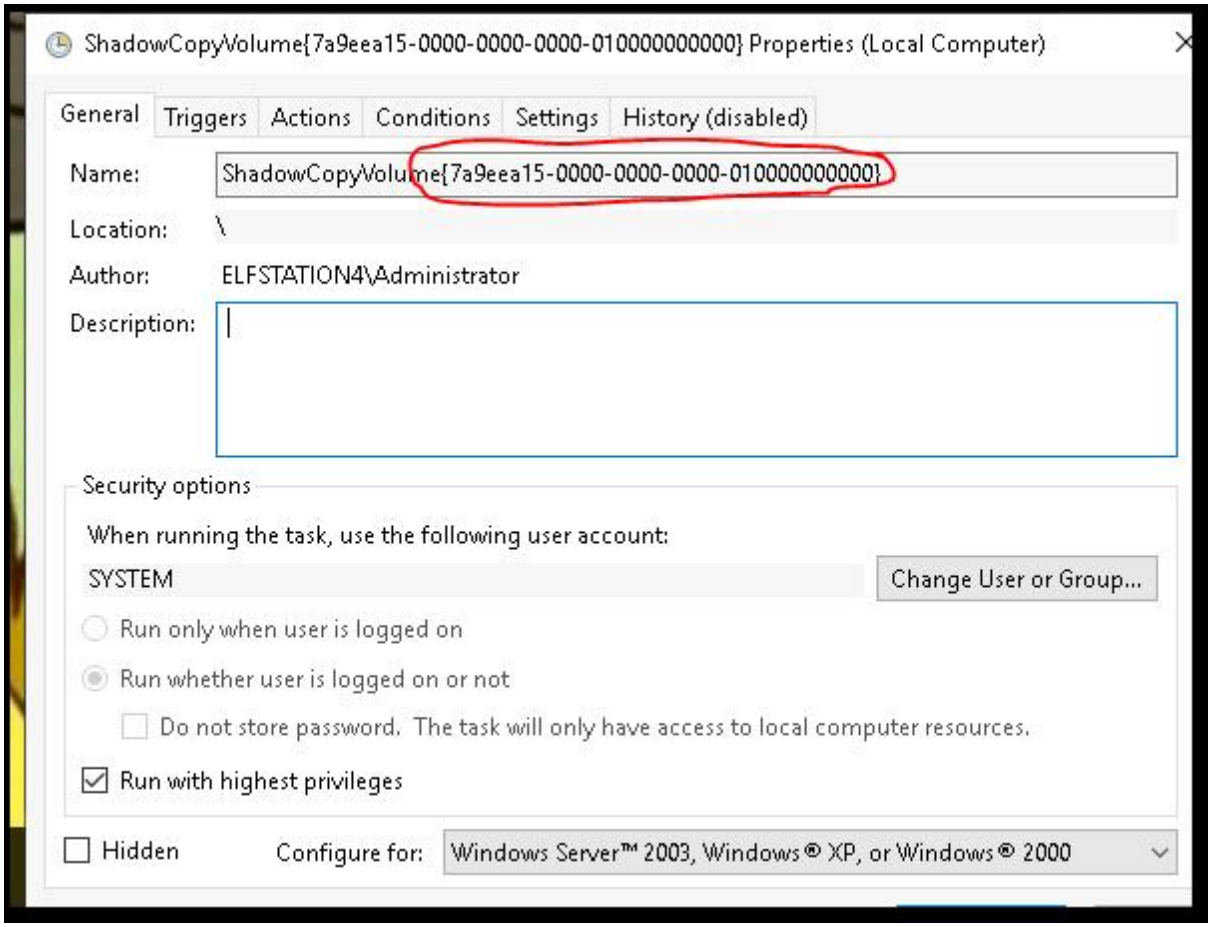
Answer: C:\Users\Administrator\Desktop\opidsfsdf.exe

Q6: There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?

Click on ShadowCopyVolume and then the Properties tab.



Here you can find the ID.



Answer: 7a9eea15-0000-0000-0000-0100000000000

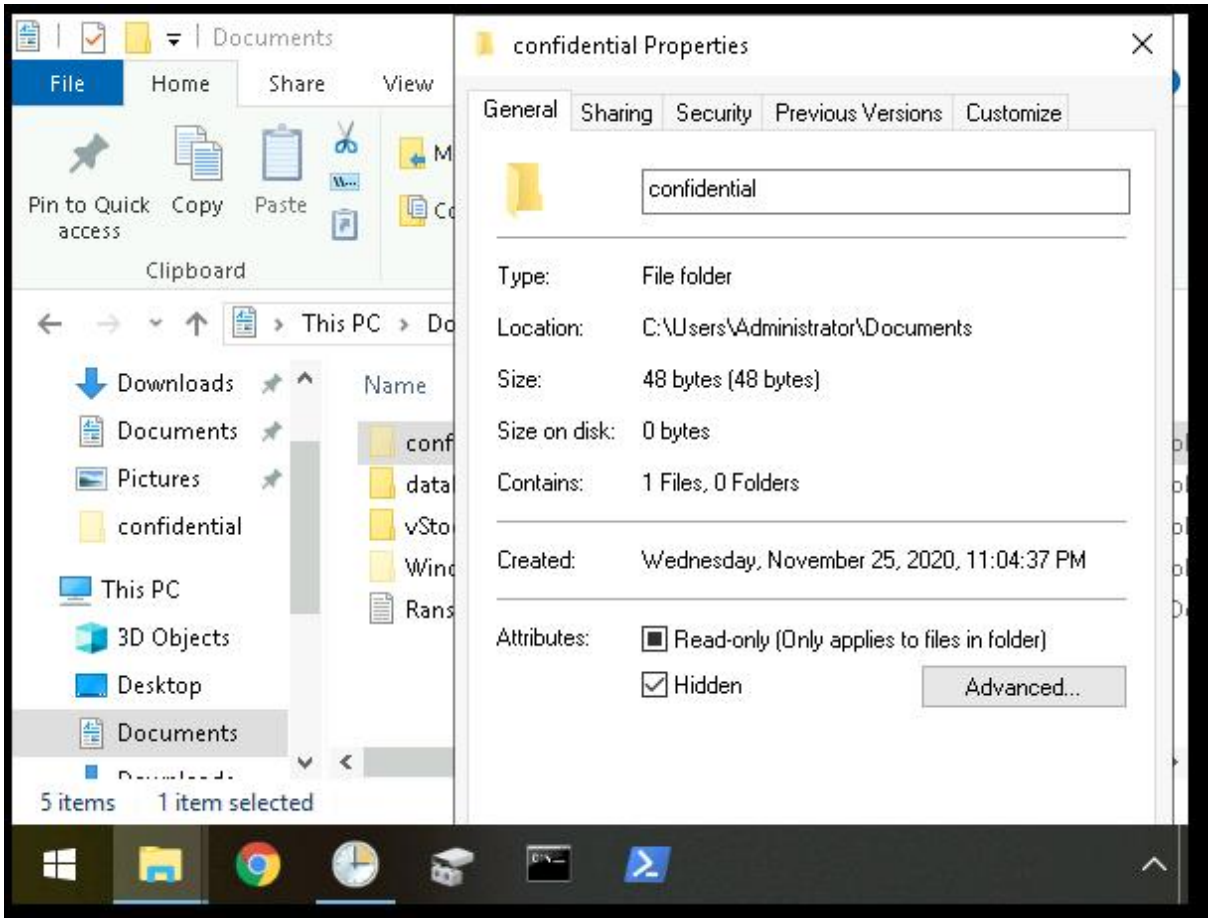
Question 7: Assign the hidden partition a letter. What is the name of the hidden folder?

We already found the hidden folder.

Answer: confidential

Question 8: Right-click and inspect the properties for the hidden folder. Use the 'Previous Versions' tab to restore the encrypted file that is within this hidden folder to the previous version. What is the password within the file?

Right click on the confidential file and click on “Properties”



Next, click on “Previous Versions” then restore the folder.
You will find a text file containing the master password.

Answer: m33pa55w0rdIZseecure!

End of Day 23 report

PSP0201 Week 6 (DAY 24) Writeup

Group Name: Nvida

Members

ID	Name	Role
1211102656	Dennis Ng Chun Hung	Leader
1211101408	Ephrem Loo Ee Zhe	Member
1211102910	Khoo Jen-Au	Member
-	-	-

Tools Used:
Kali Linux , Firefox , CrackStation

[Day 24] The Trial Before Christmas

Question 1: Scan the machine. What ports are open?

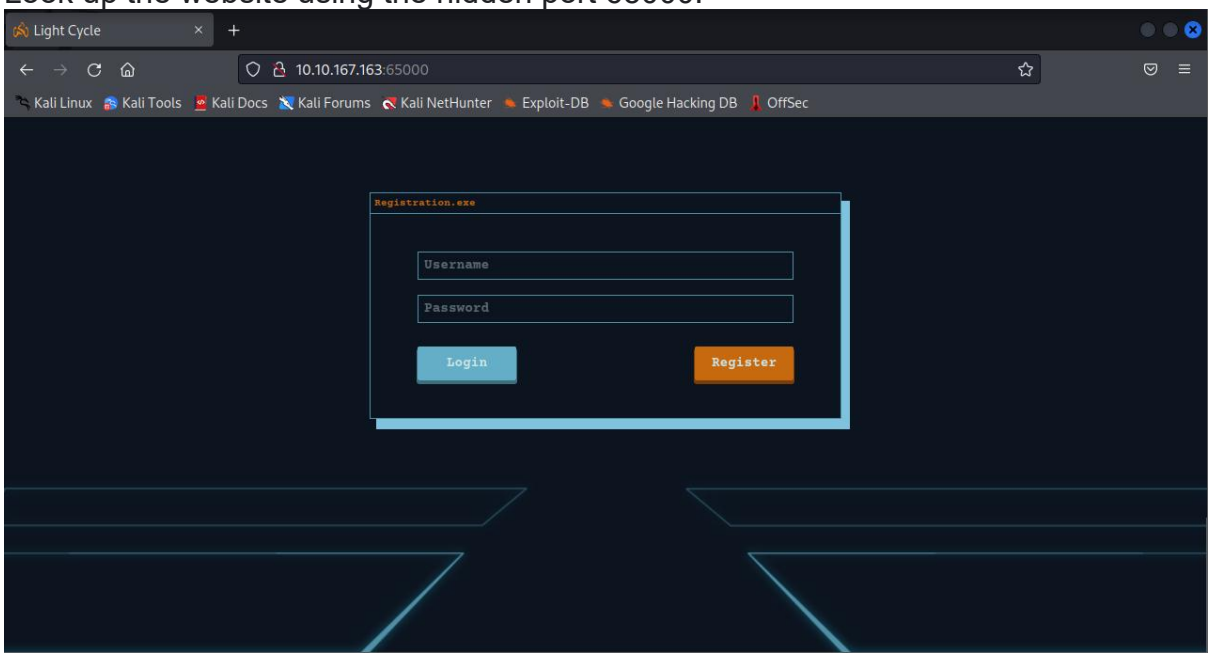
Scan the machine and wait for the response.

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- -T5 10.10.167.163
Nmap scan report for 10.10.167.163
Host is up (0.20s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
65000/tcp open  unknown
```

Answer: 80, 65000

Question 2: What's the title of the hidden website? It's worthwhile looking recursively at all websites on the box for this step.

Look up the website using the hidden port 65000.



Answer: Light Cycle

Question 3: What is the name of the hidden php page?

Use the command below to find the answer.
gobuster dir -u http://10.10.174.176:65000/ -x php -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40

```
2022/07/24 05:38:53 Starting gobuster in directory enumeration mode
/index.php            (Status: 200) [Size: 800]
/uploads.php          (Status: 200) [Size: 1328]
/assets               (Status: 301) [Size: 324] [--> http://10.10.174.176:650
00/assets/]
```

Answer: /uploads.php

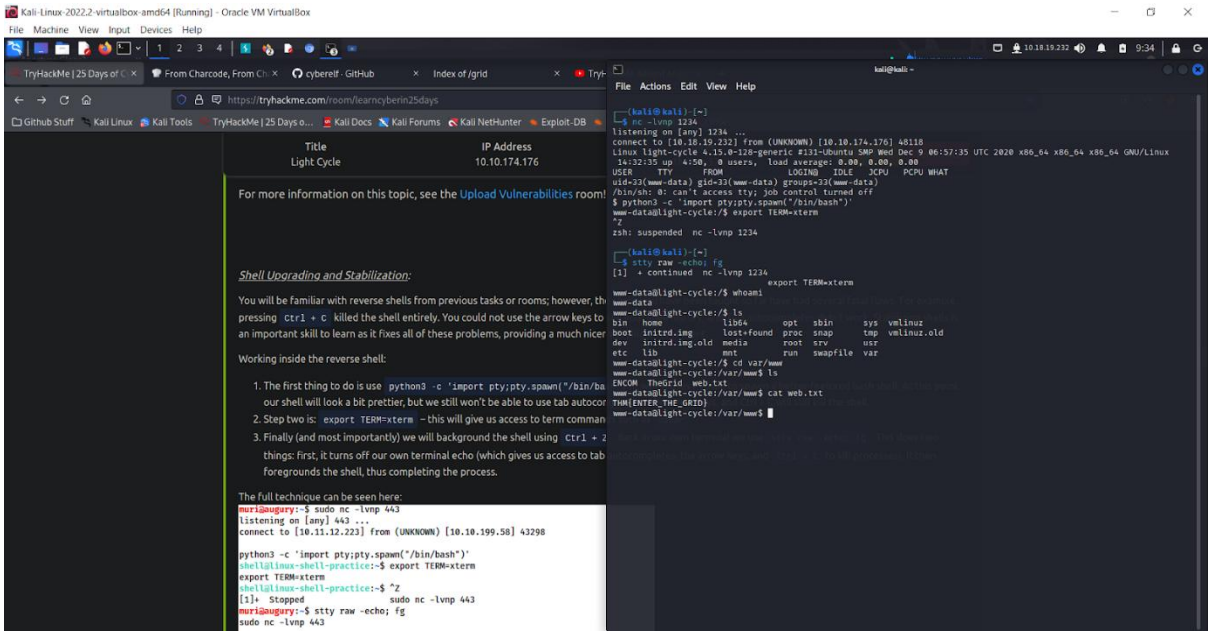
Question 4: What is the name of the hidden directory where file uploads are saved?

```
/grid                 (Status: 301) [Size: 322] [--> http://10.10.174.176:650
00/grid/]
Progress: 5150 / 441122 (1.17%)
```

After testing out the answers inside of THM, grid is the only correct answer.

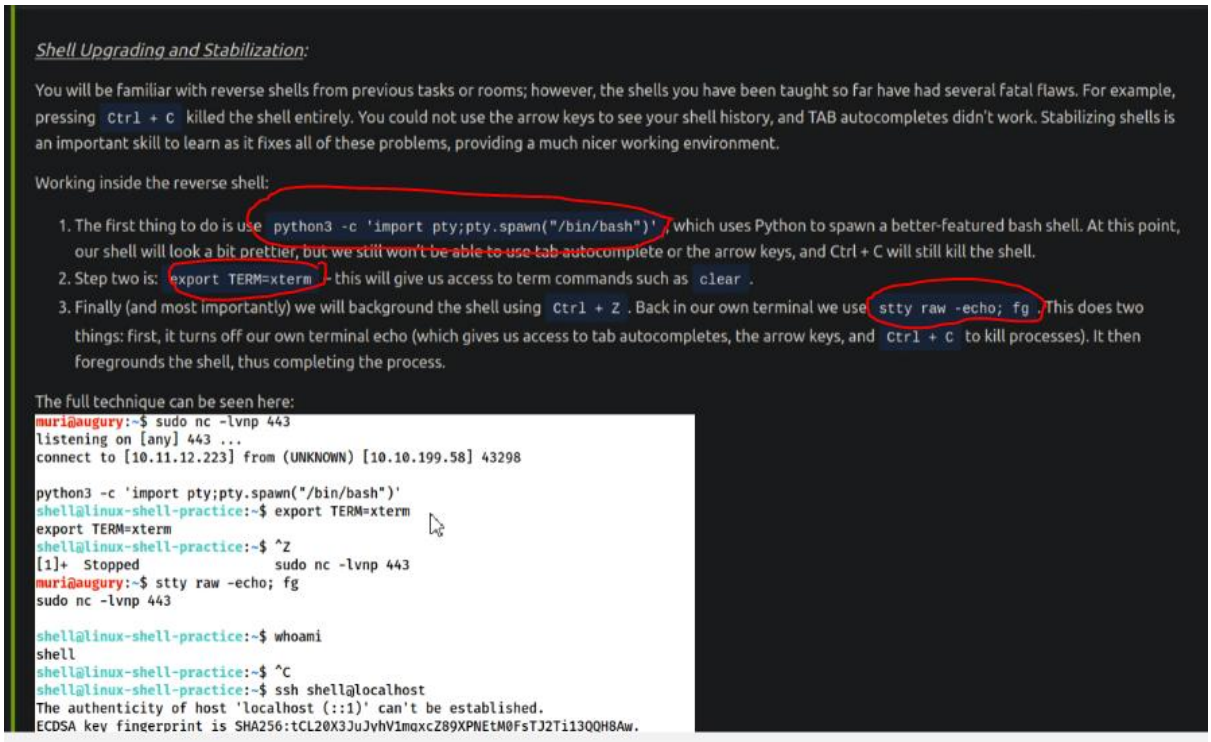
Answer: /grid

Question 5: What is the value of the web.txt flag?
Using the “cat” command and read the file.



Answer:THM{ENTER_THE_GRID}

Question 6: What lines are used to upgrade and stabilise your shell?



Answer:
export TERM=xterm
python3 -c 'import pty;pty.spawn("/bin/bash")'
stty raw -echo; fg

Question 7: Review the configuration files for the webserver to find some useful loot in the form of credentials. What credentials do you find?

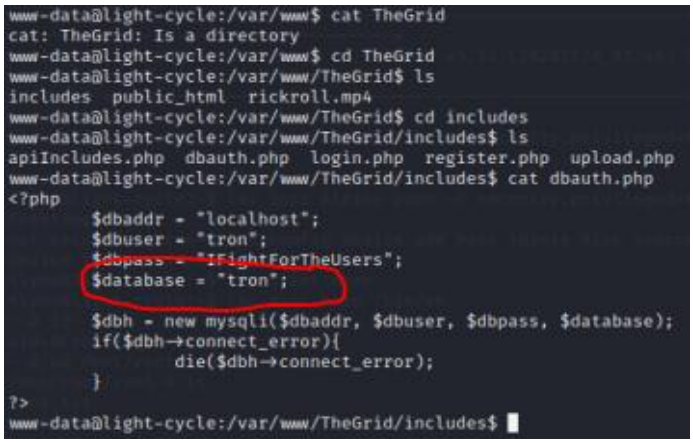
After we're done with TheGrid, use "cd TheGrid" and then "ls"
Then we will see the "includes" directory.
Repeat the same steps with "cd includes" and "ls", we will then get to see dbauth.php
Finally, cat that and we can see its details.

```
www-data@light-cycle:/var/www$ cat TheGrid
cat: TheGrid: Is a directory
www-data@light-cycle:/var/www$ cd TheGrid
www-data@light-cycle:/var/www/TheGrid$ ls
includes  public_html  rickroll.mp4
www-data@light-cycle:/var/www/TheGrid$ cd includes
www-data@light-cycle:/var/www/TheGrid/includes$ ls
apiIncludes.php  dbauth.php  login.php  register.php  upload.php
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbauth.php
<?php
        $dbaddr = "localhost";
        $dbuser = "tron";
        $dbpass = "IFightForTheUsers";
        $database = "tron";

        $dbh = new mysqli($dbaddr, $dbuser, $dbpass, $database);
        if($dbh->connect_error){
                die($dbh->connect_error);
        }
?>
www-data@light-cycle:/var/www/TheGrid/includes$
```

Answer: “IFightForTheUsers”

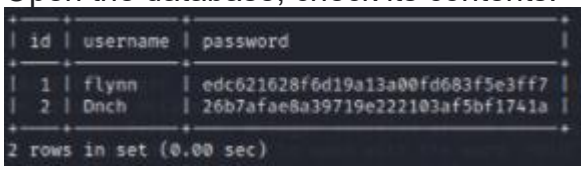
Question 8: Access the database and discover the encrypted credentials. What is the name of the database you find these in?



Answer: tron

Question 9: Crack the password. What is it?

Open the database, check its contents.



Copy the password from flynn and crack it using one of the provided 3 websites:

Online Password Cracking:

In the modern age of password cracking, weak passwords can often be cracked without any cracking at all! Many websites now exist with the sole goal of hosting rainbow tables - tables of previously cracked passwords. This allows us more than often to simply input a password hash and nearly instantly receive the cracked password. Some various sites that I find myself (Dark) commonly using, especially throughout the case of CTFs, include the following:

- https://crackstation.net/

- https://md5decrypt.net/en/

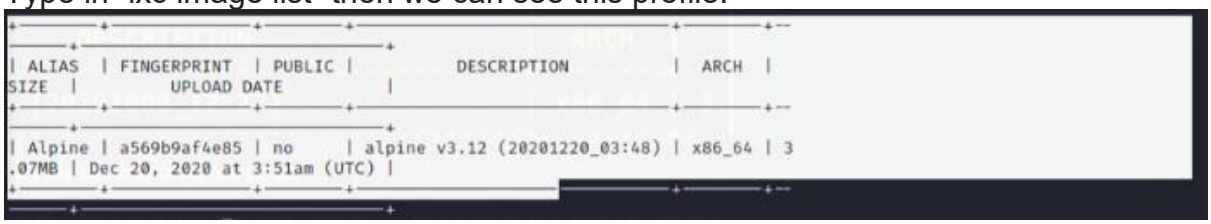
- https://hashes.com/en/decrypt/hash

Answer: @computer@

Question 10: Use su to login to the newly discovered user by exploiting password reuse. What is the user you are switching to?

We can use “lxc image” to determine the user profile.

Type in “lxc image list” then we can see this profile.



Answer: Alpine

Question 11: What is the value of the user.txt flag?

Type in “whoami”. Make sure you are under www-data

Type in: “su flynn” and enter the password.

```
www-data@light-cycle:/$ su flynn
Password:
```

Type in “ls”

```
flynn@light-cycle:/$ ls
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
```

Type in “cd home”, then repeat the same procedures, but this time with “cd flynn” instead of “cd home”.

```
flynn@light-cycle:/$ cd home
flynn@light-cycle:/home$ ls
flynn
flynn@light-cycle:/home$ cd flynn
flynn@light-cycle:~$ ls
user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
```

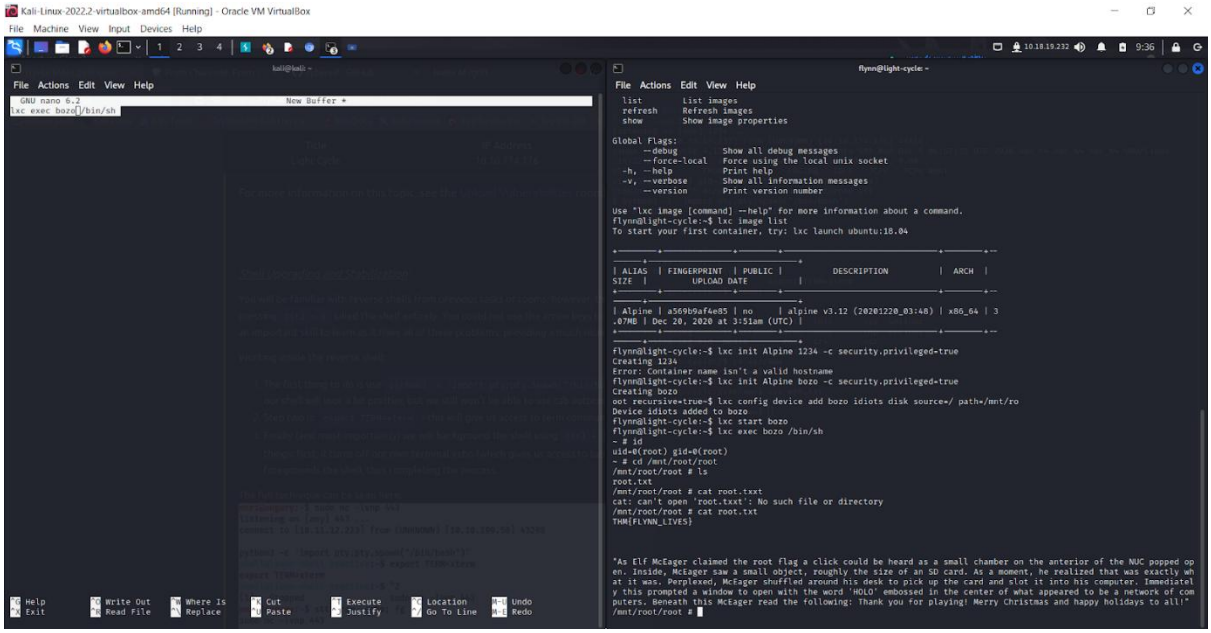
We will then see the user.txt and we can view its contents using “cat user.txt”

Answer: THM{IDENTITY_DISC_RECOGNISED}
Question 12: Check the user's groups. Which group can be leveraged to escalate privileges?

> *Privilege Escalation with LXD*:
>
> Among the more curious privilege escalation methods on Linux, lxd is certainly a mind-bender, to say the least. This technique involves leveraging a flaw in lxd, a program that we can use to spin up containers much akin to Docker. This exploit specifically involves abusing mount points to mount volumes from our victim machine (the machine we're attacking) within a container that we shouldn't be able to access/read. However, we have root powers on lxd containers - thus allowing us to bypass the read permission checks and escalate our privileges. We can perform this privesc method via the following steps:

Answer: LXD

Question 13: What is the value of the root.txt flag?
Read the root.txt with the “cat” command.



Answer: THM{FLYNN_LIVES}

End of Day 24 report