PSP0201 Week 6 Writeup

Group Name : Mali Pape

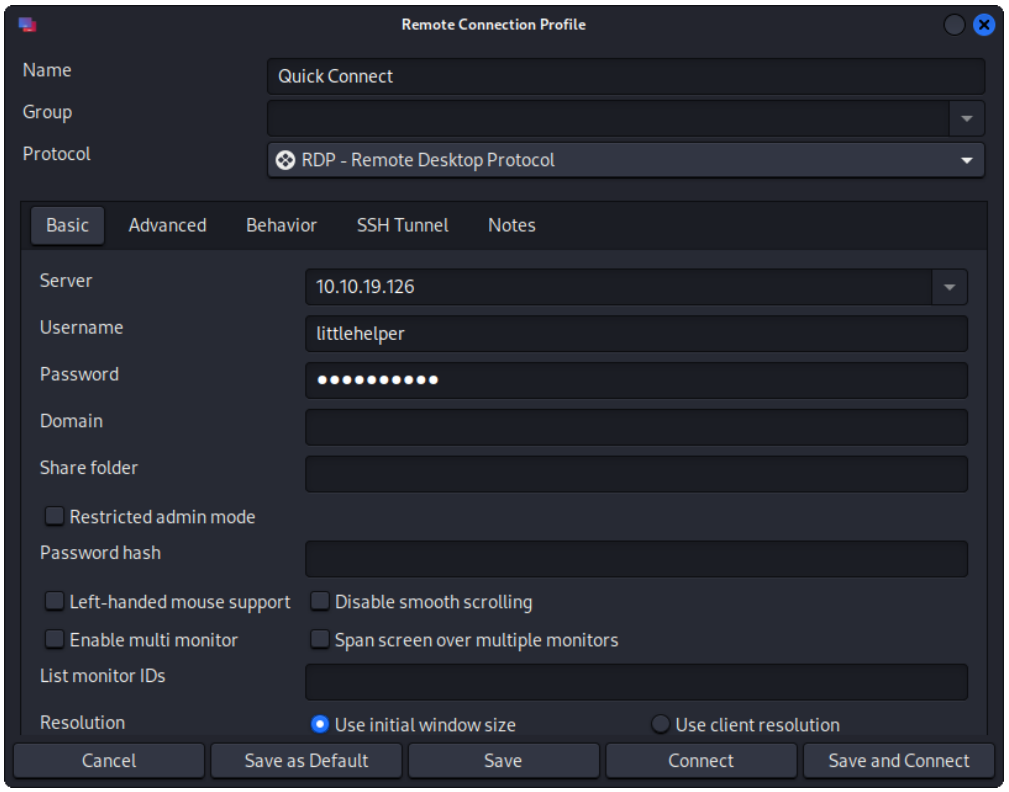
Members:

ID	Name	Role
1211102895	Muhammad Irfan Bin Mohd Nazri	Leader
1211104288	Mohd Azriy Akmalhazim Bin Mohd Nazariee	Member
1211103634	Ho Tian Ming	Member
1211101035	Mohamad Zuhir Bin Mohamad Zailani	Member

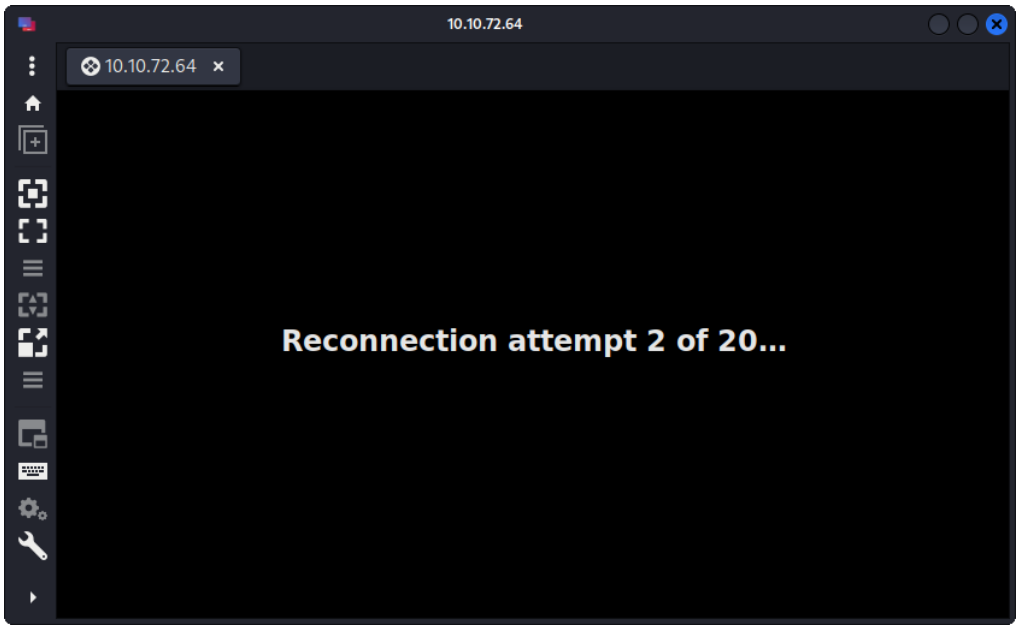
Day 21: Blue Teaming - Time for some ELForensics
Tools used: Kali Linux, Remmina
Solution/walkthrough:

Question 1:

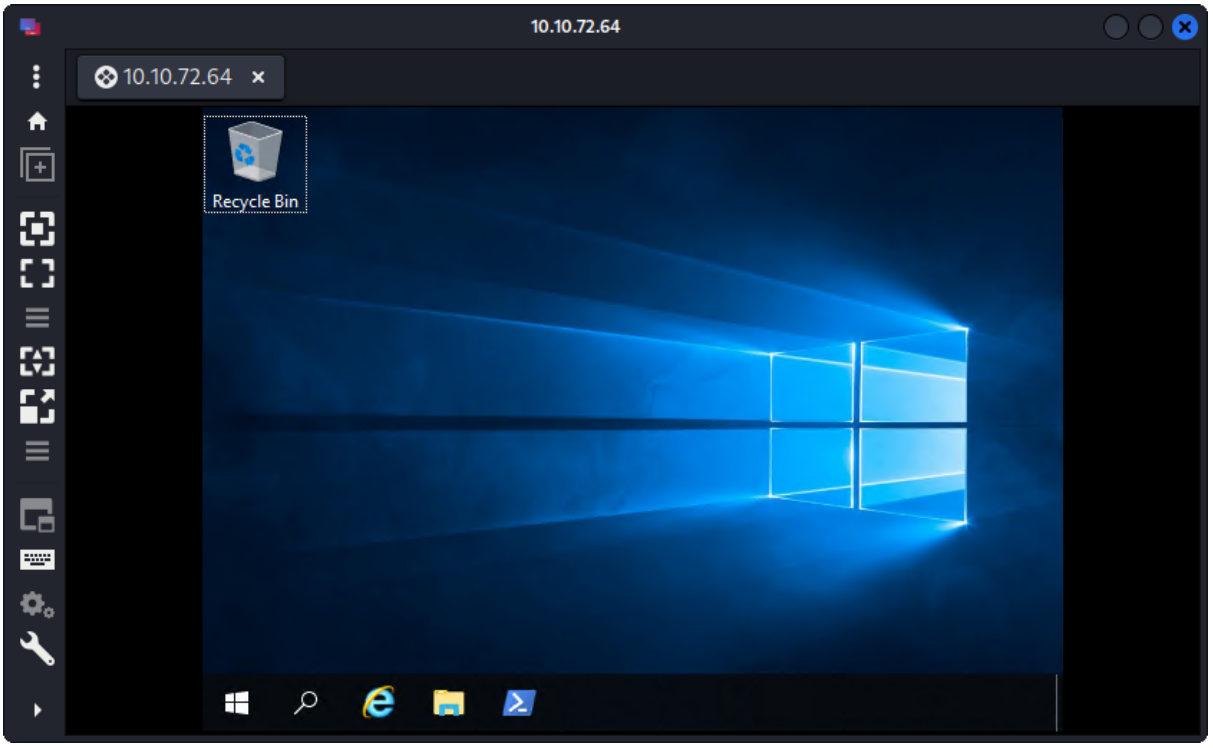
Setting up Remmina's Connection



Accept the certificate and log into the remote system

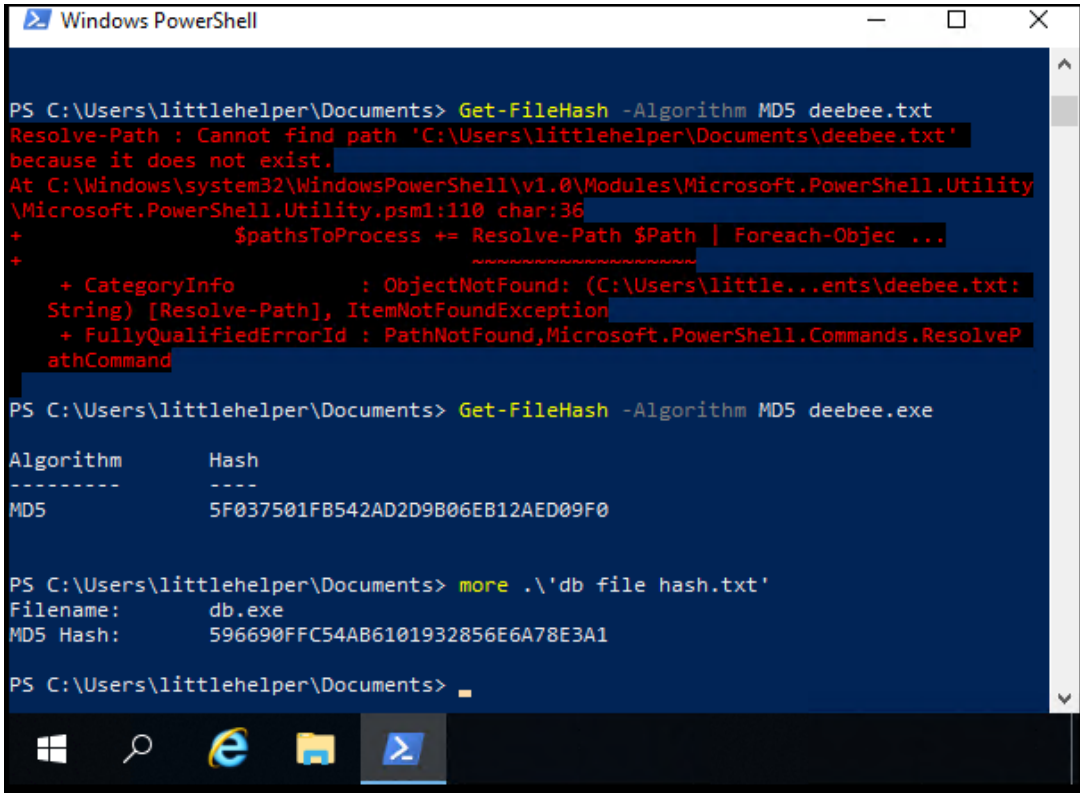


Log in to the remote system in Remmina



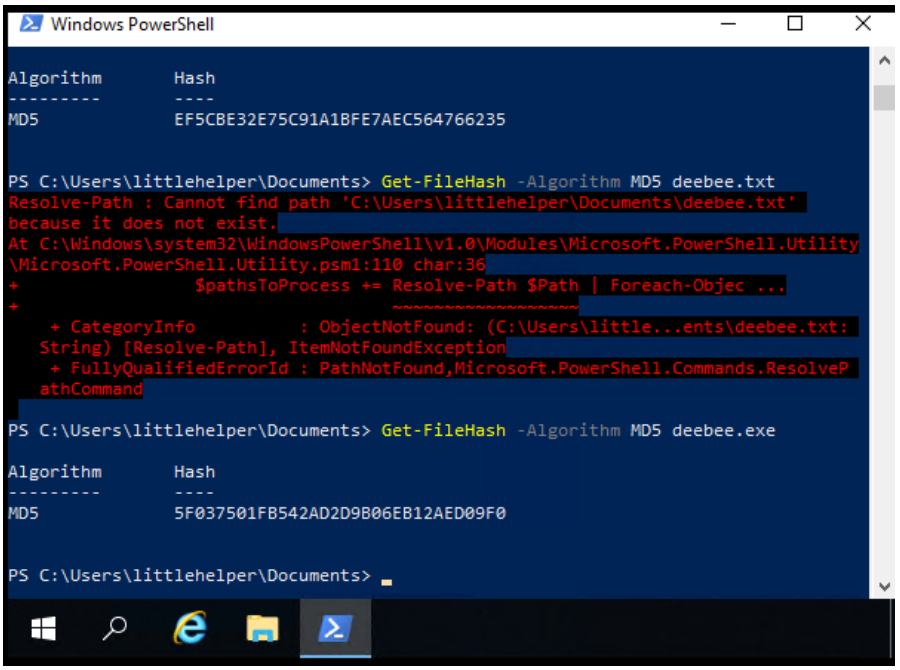
Open powershell, change directory and use dir command. Use more command to search for the file hash .

Answer : 596690FFC54AB6101932856E6A78E3A1



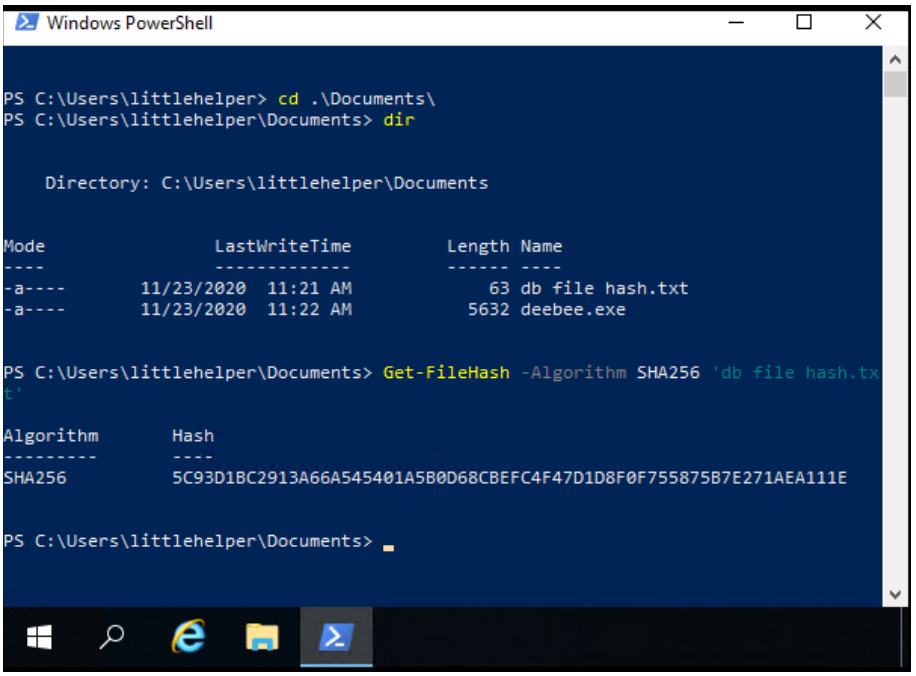
Question 2:

Use Get-FileHash -Algorithm MD5 deebee.txt to search for the file hash,
Answer : 5F037501FB542AD2D9B06EB12AED09F0



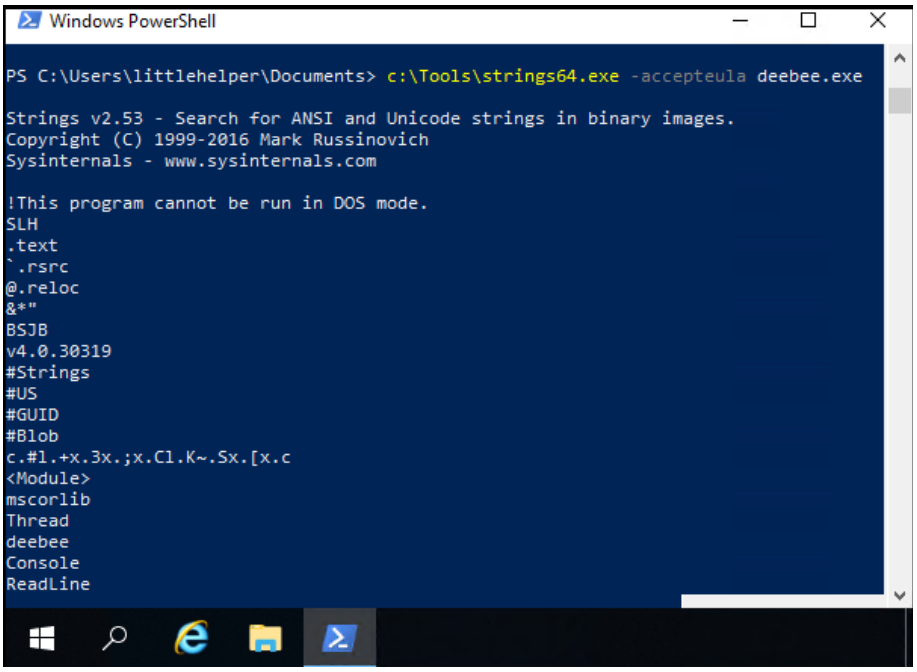
Question 3:

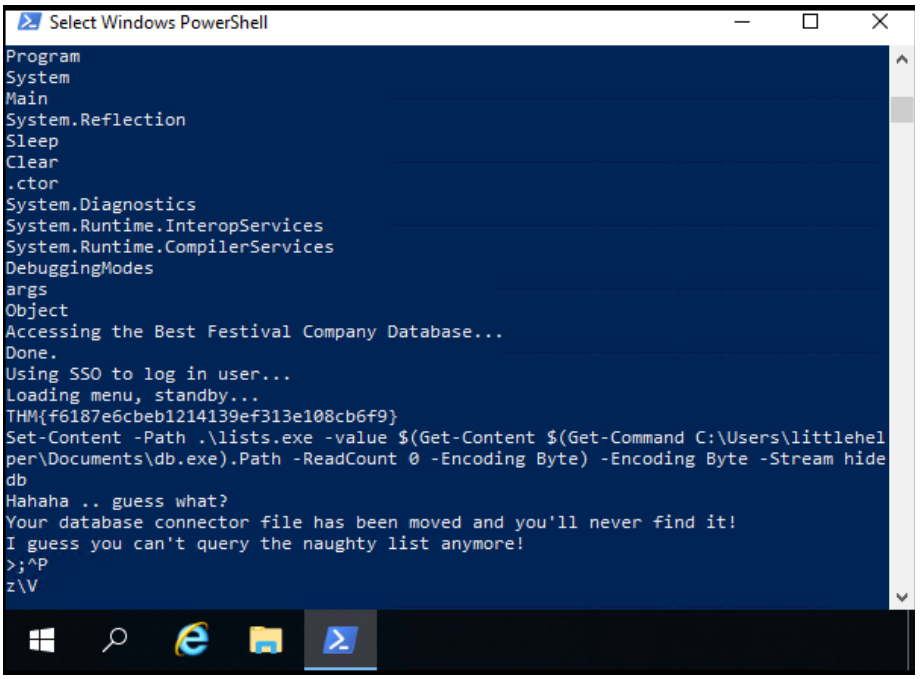
Use the same command with changes of MD5 to SHA256.
Answer :
5C93D1BC2913A66A545401A5B0D68CBEFC4F47D1D8F0F755875B7E271AEA111E



Question 4:

Use Strings command c:\Tools\strings64.exe -accepteula deebee.exe to search for the flag.
Answer: THM{f6187e6cbeb1214139ef313e108cb6f9}





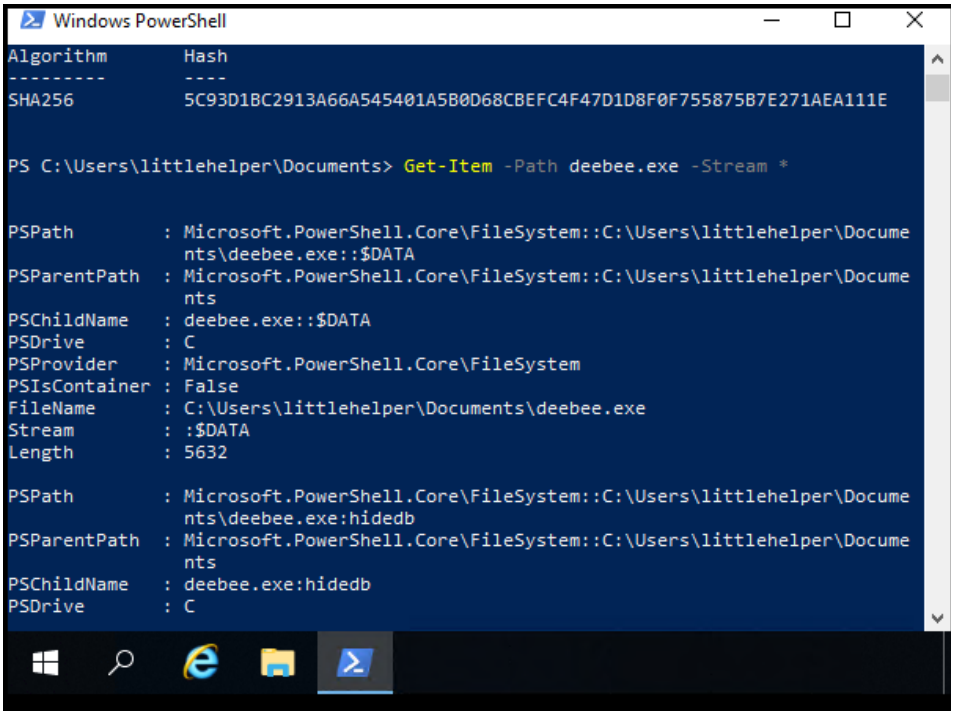
Question 5:

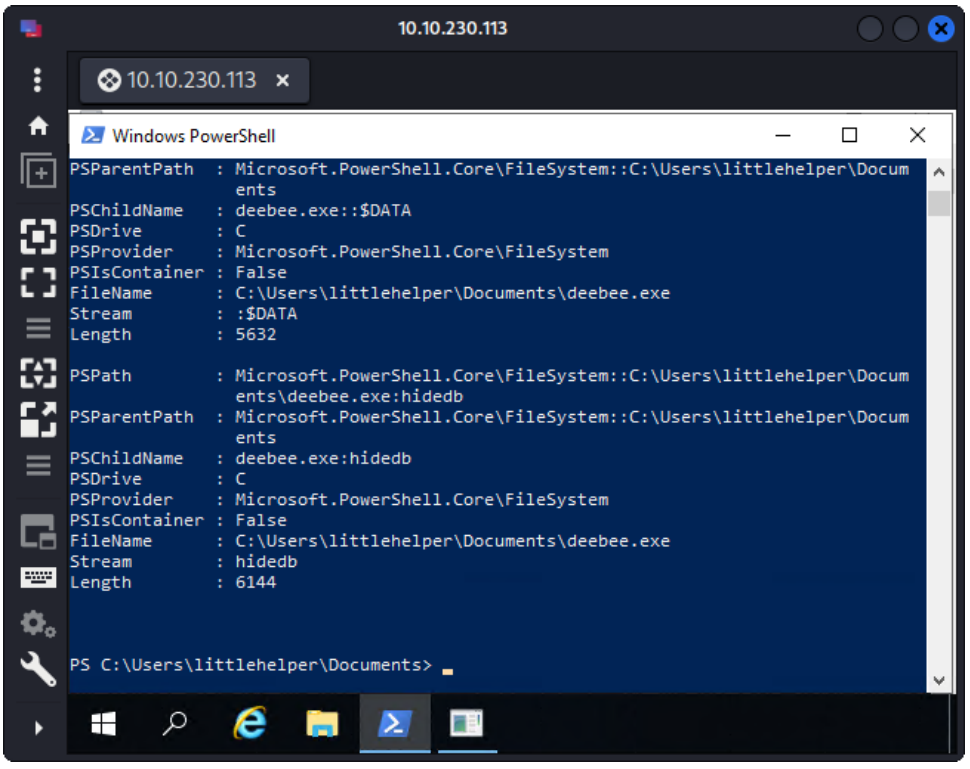
Answer : Get-Item -Path file.exe -Stream *

> The command to view ADS using Powershell: `Get-Item -Path file.exe -Stream *`

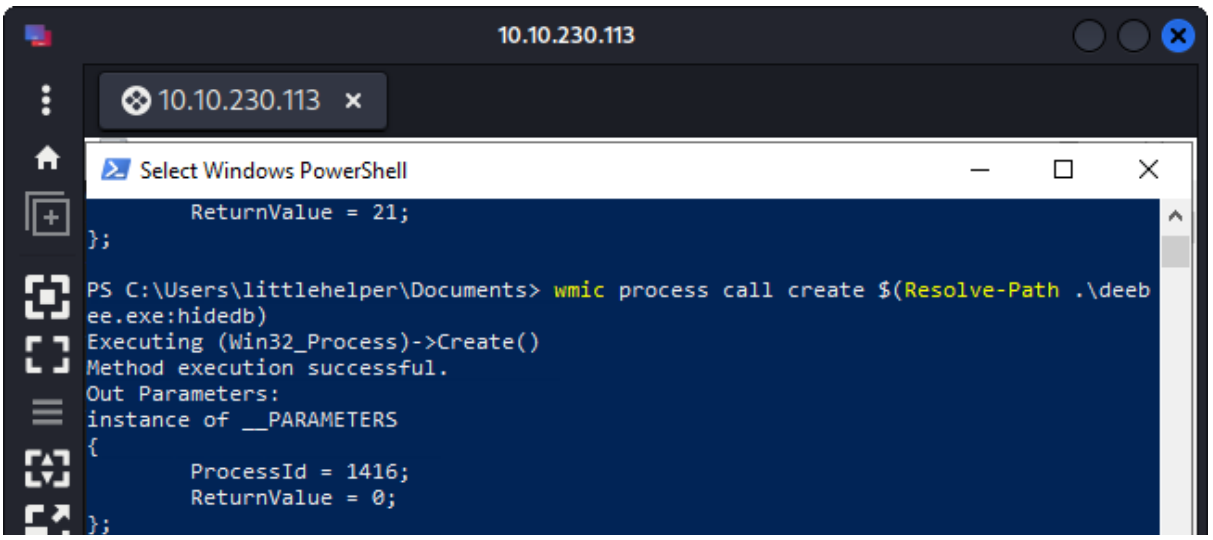
Question 6:

View ADS and search for the streamname

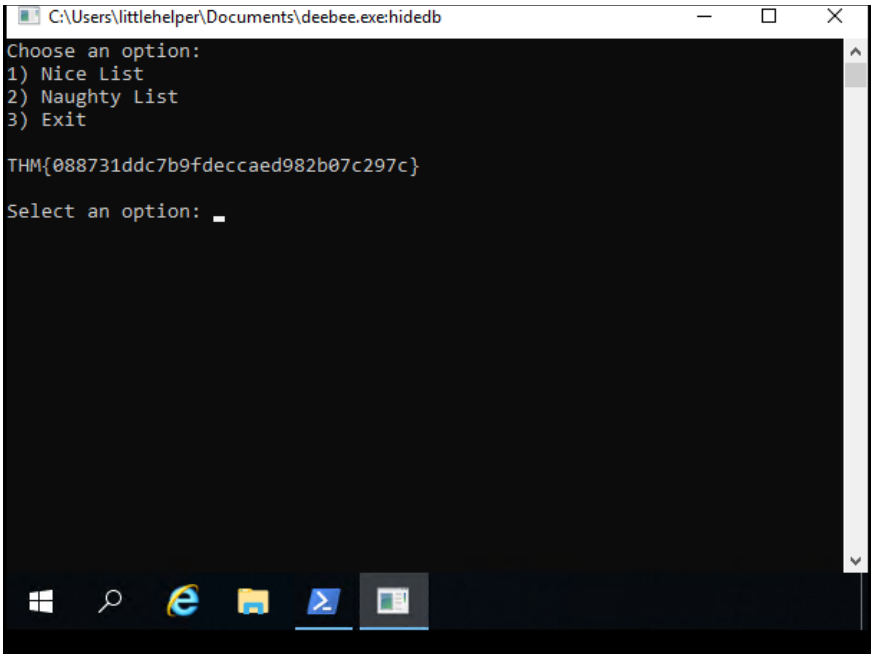




Launch the executable which is hidden in the ADS using command wmic process call create $(Resolve-Path deebee.exe:hidedb)

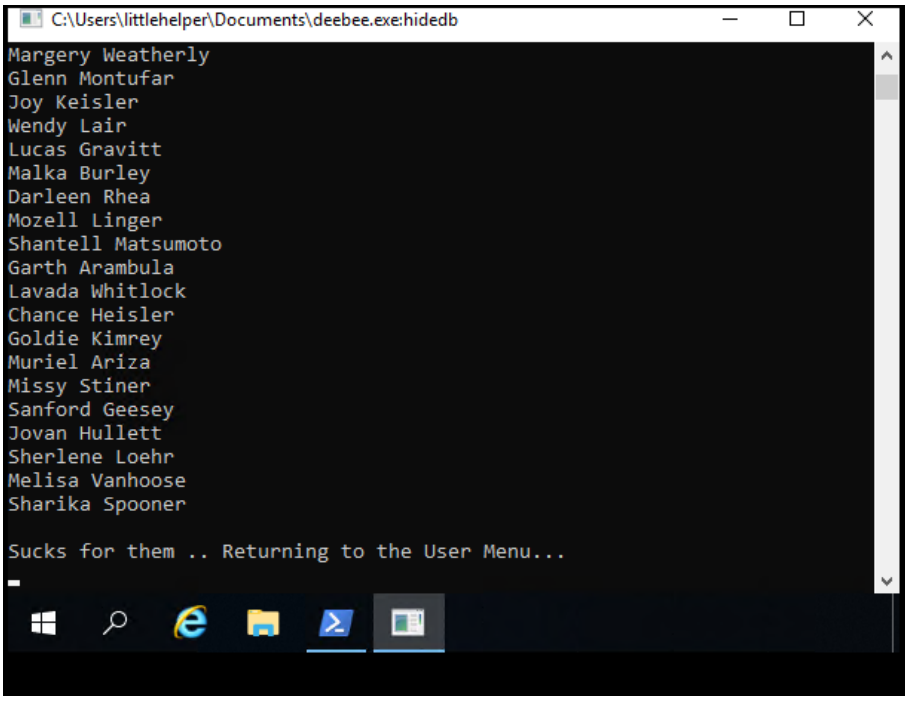


Answer: THM{088731ddc7b9fdeccaed982b07c297c}



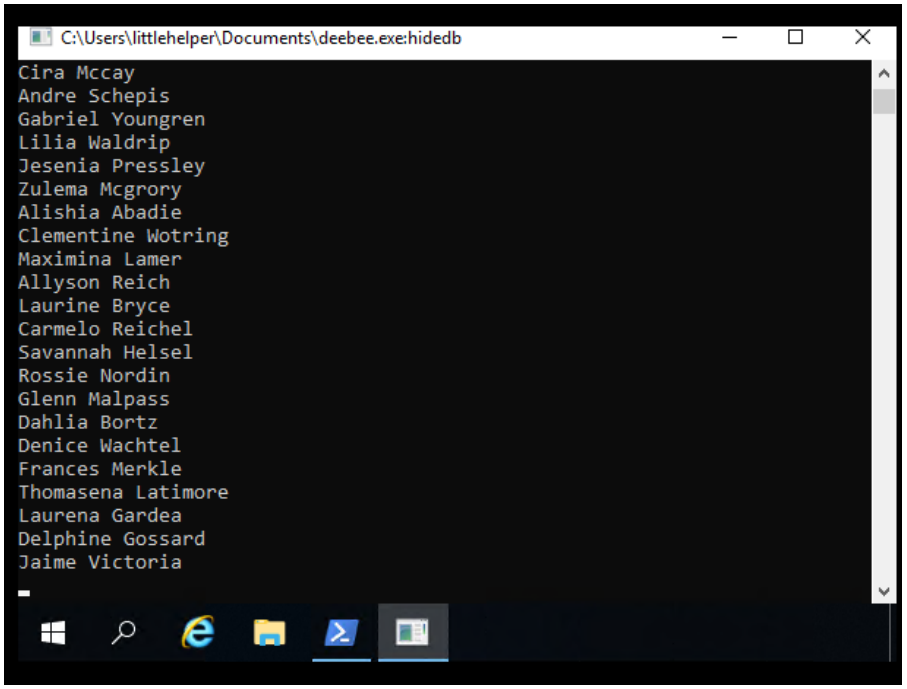
Question 7:

Run the program and search for the name.
Answer: Naughty List



Question 8:

Run the program and search for the name.
Answer: Nice List



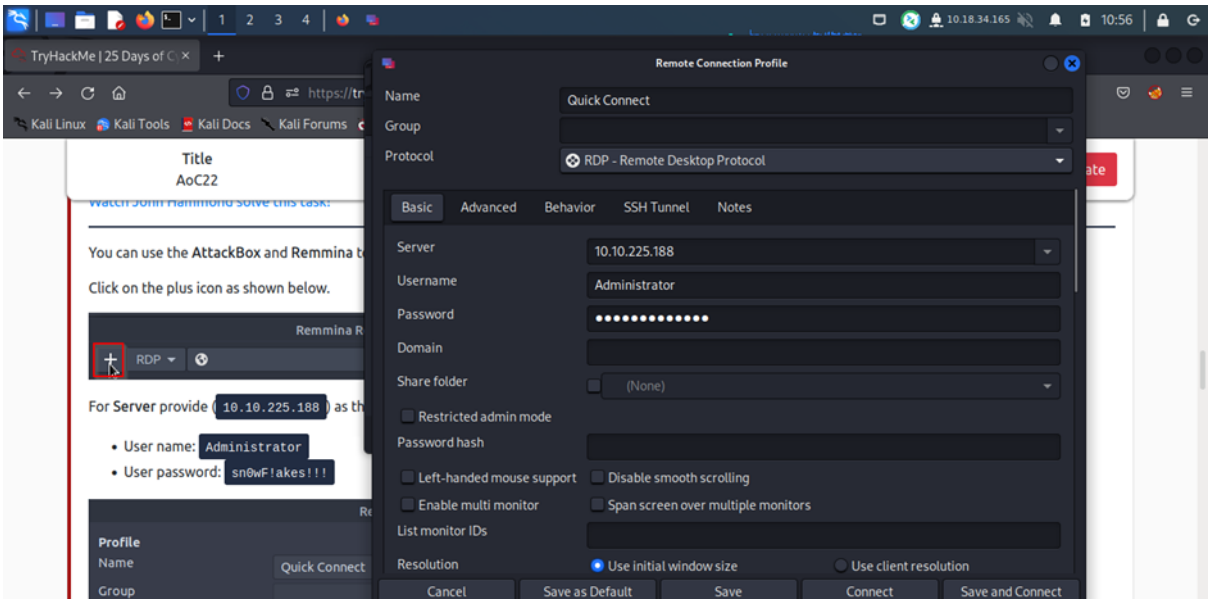
Thought Process/Methodology:

This challenge was started with the process of setting up a connection in Remmina to open up the remote machine using the ip address provided from the THM, username of `littlehelper` and password of `iLove5now!`. After the remote machine is successfully turned on, we can then navigate to the powershell and start the tasks. For the first question, I used the command of `cd .\Documents\` to change the current directory to Documents and use dir command to see the list of items located there. Then, I used `more` command to search for the file hash which then completed the question requirements. After that, for question 2, I used the command of `Get-FileHash -Algorithm MD5 deebee.txt` to search for the file hash of the mysterious file - deebee.exe. This then giving me the file hash of this file which is 5F037501FB542AD2D9B06EB12AED09F0. This step is repeated to look for the answer of Question 3 with a difference where I changed the `MD5` in the command with `SHA256`.To continue with question 4, I used the Strings command of c:\Tools\strings64.exe -accepteula deebee.exe to search for the flag indicated in question. Answer for question 5 can be found in the instruction from the THM website which is `Get-Item -Path file.exe -Stream *`. For question 6, I used the previous command to see the ADS and then launch the executable which is hidden in the ADS using the command `wmic process call create`

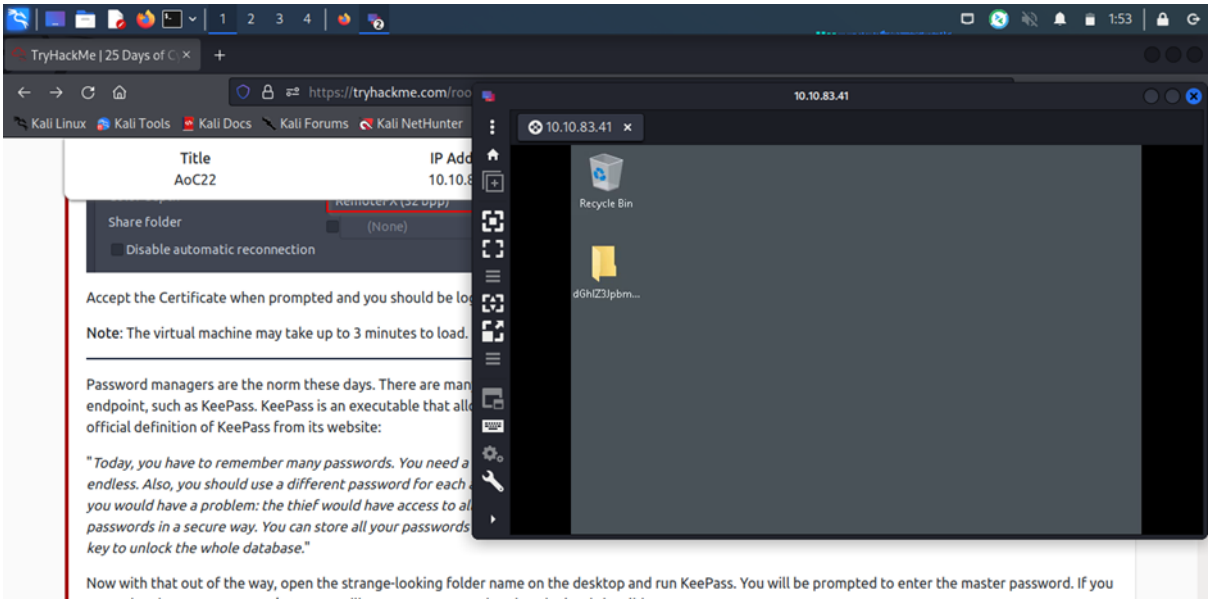
`$(Resolve-Path deebee.exe:hidedb)`. When the program is launched we obtain the flag required which is written on the program below the options given. The two last questions - question 7 and 8, shared the same steps where we needed to run the program and search for both people's names, Sharika Spooner and Jaime Victoria from the Nice and Naughty List.

Day 22: [Blue teaming]- Elf McEager Becomes CyberElf
Tools used: THM attackbox, remmina, keypass, cyberchef
Solution/walkthrough:

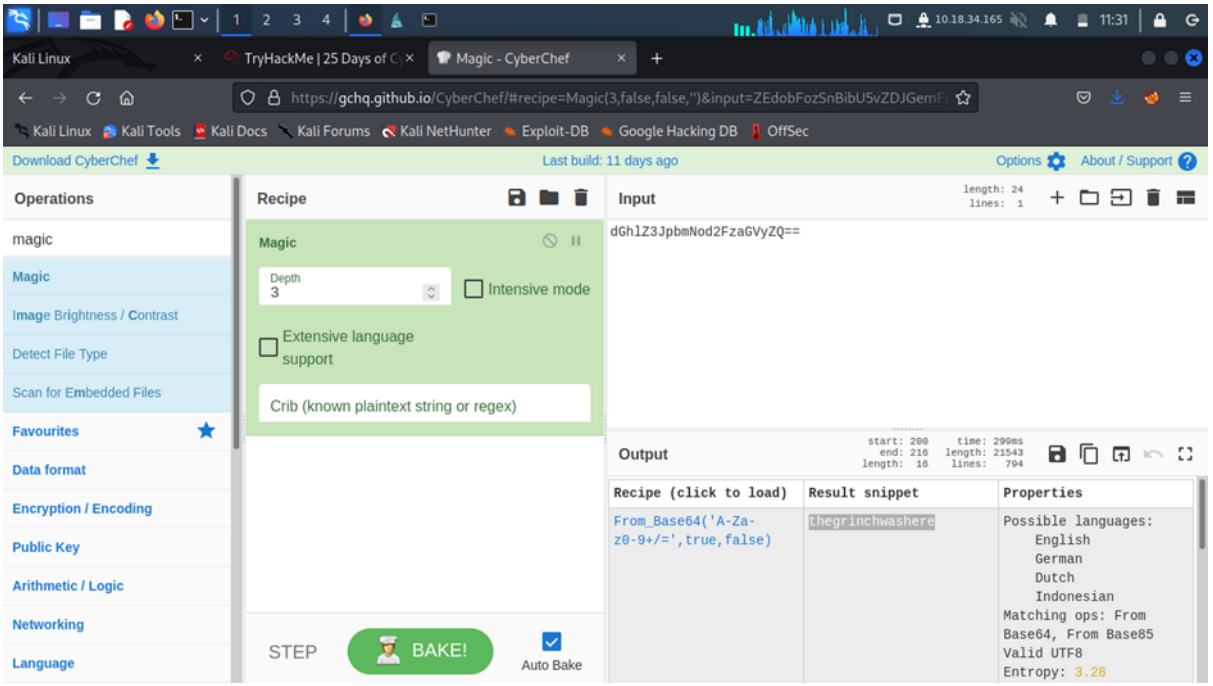
Question 1:



Open the remote connection profile, enter the server IP address, and then type the provided username and password.

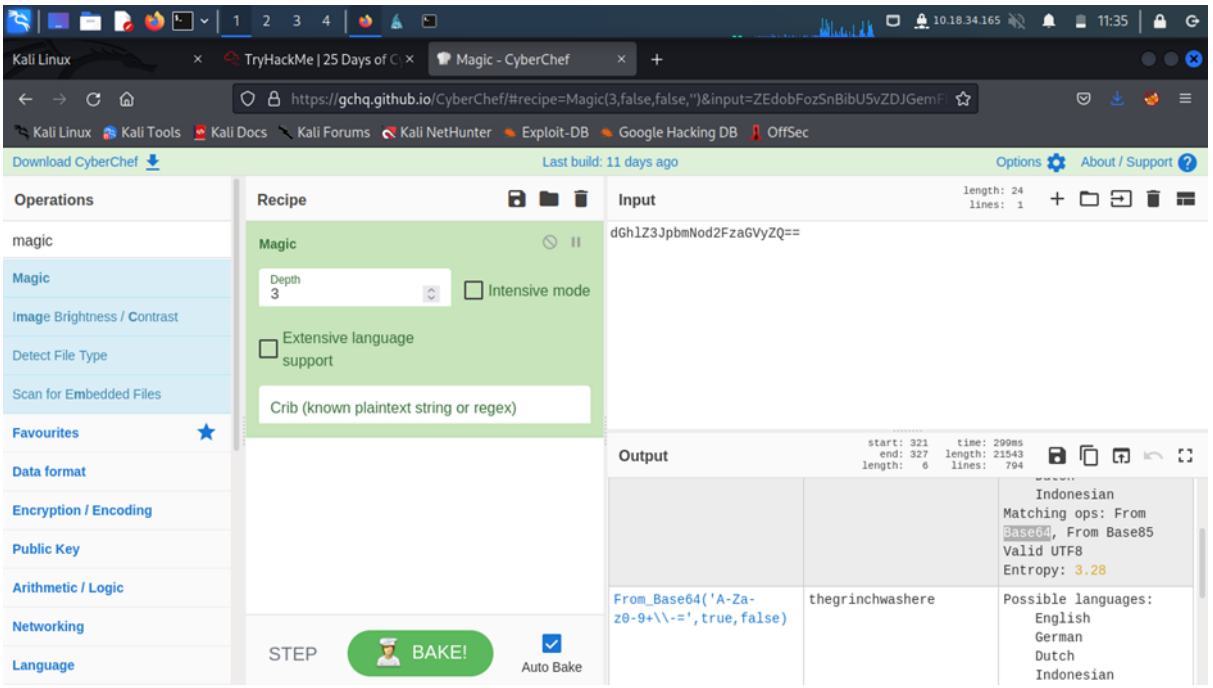


The encrypted file from the remmina will then be visible to you



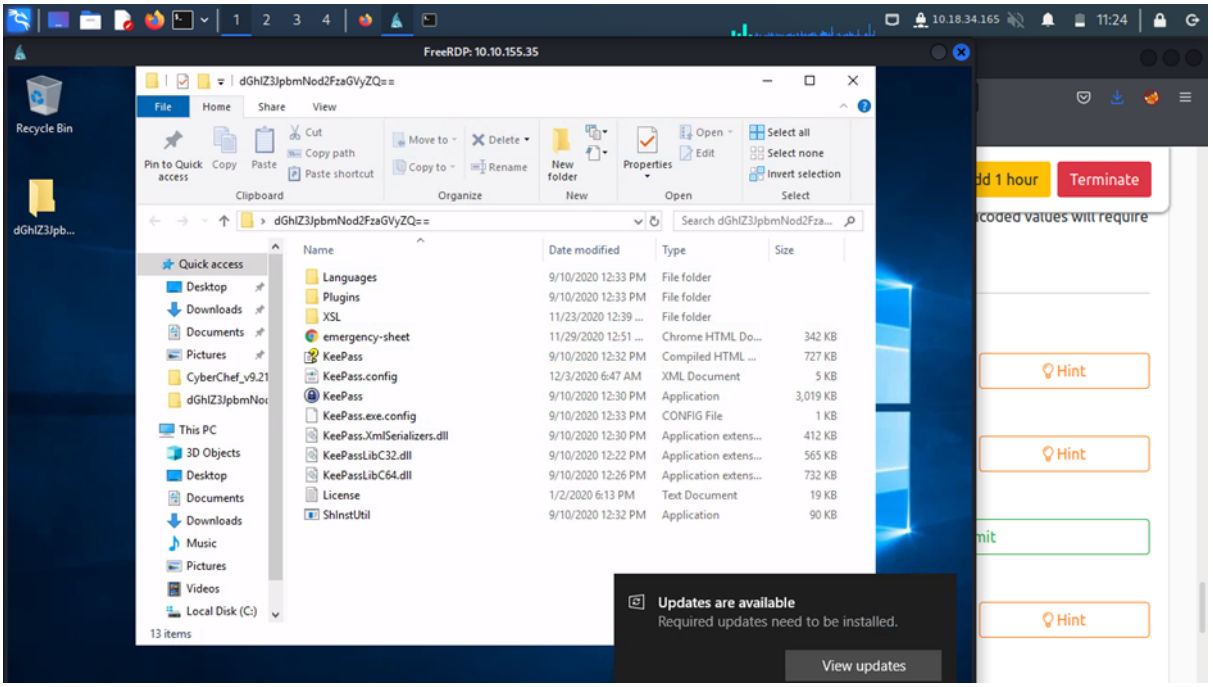
It is necessary to copy the encrypted file name. then use CyberChef to input the data. As a result, a snippet of the input code's outcome will be displayed.

Question 2:

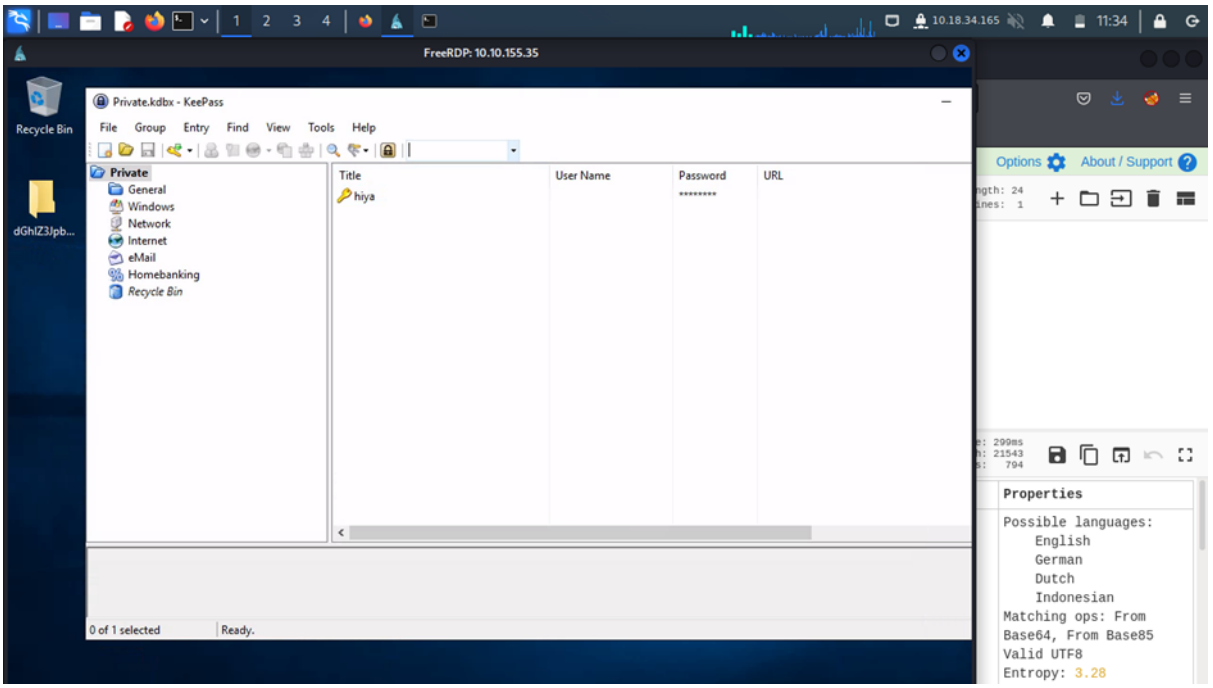


From the matching operators in the cyberchef online search, the list of encoding methods. It is in the output box on the right side.

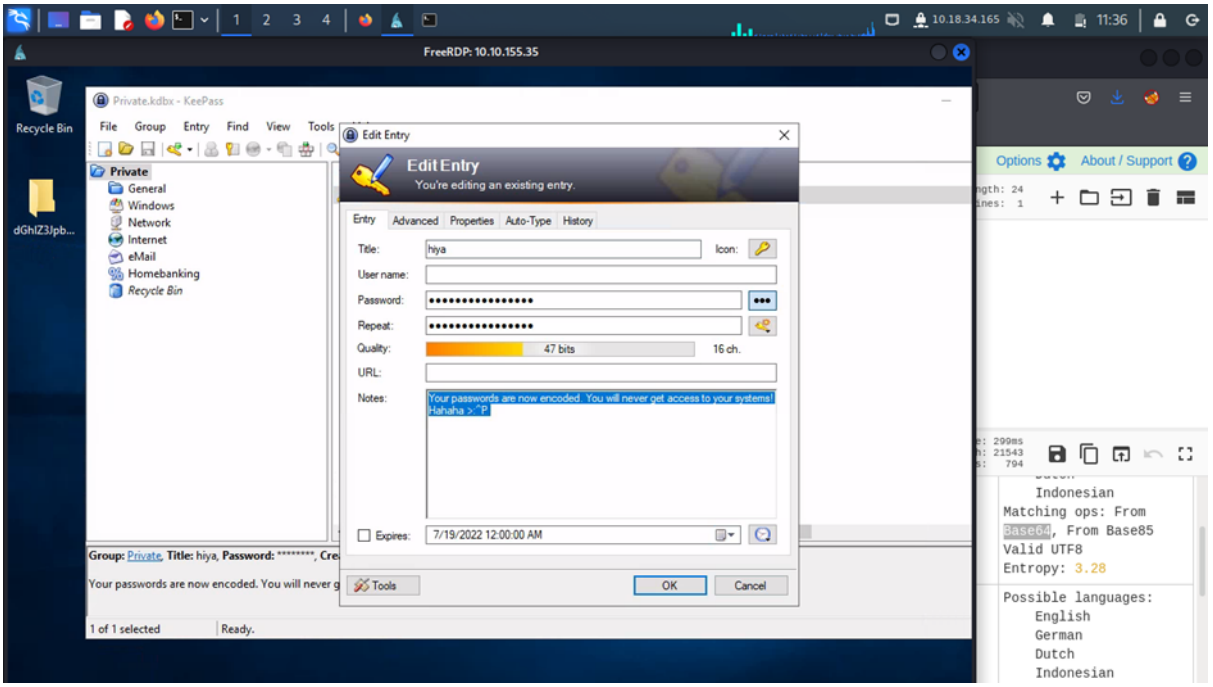
Question 3:



Open the document that was displayed inside the remina.

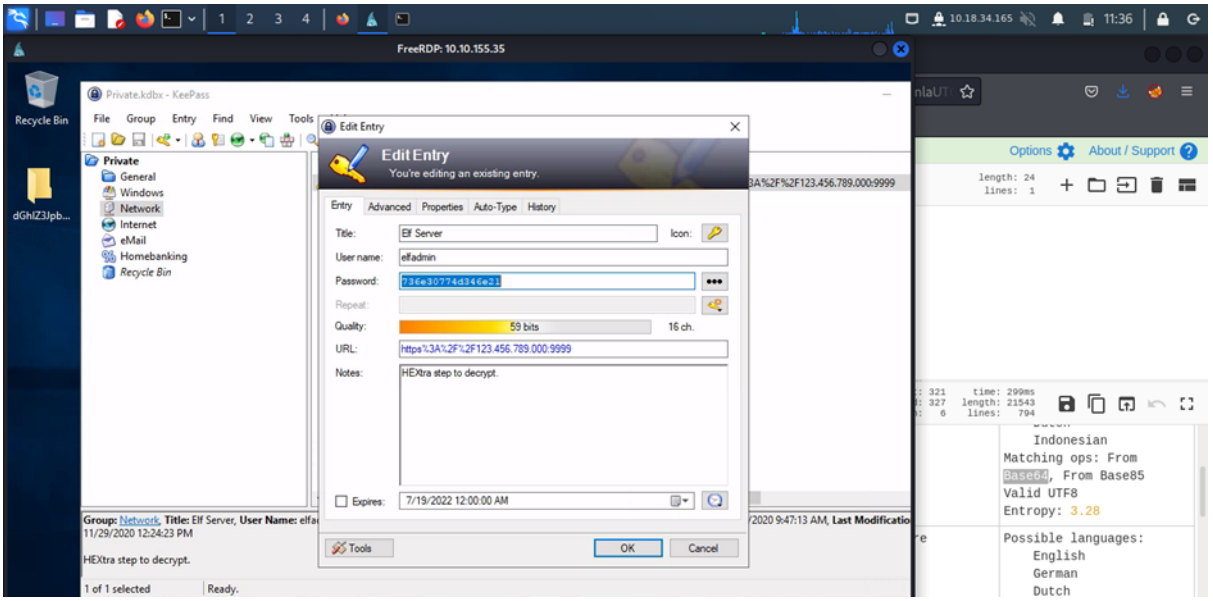


You may discover the password and hiya key by opening the KeePass programme.

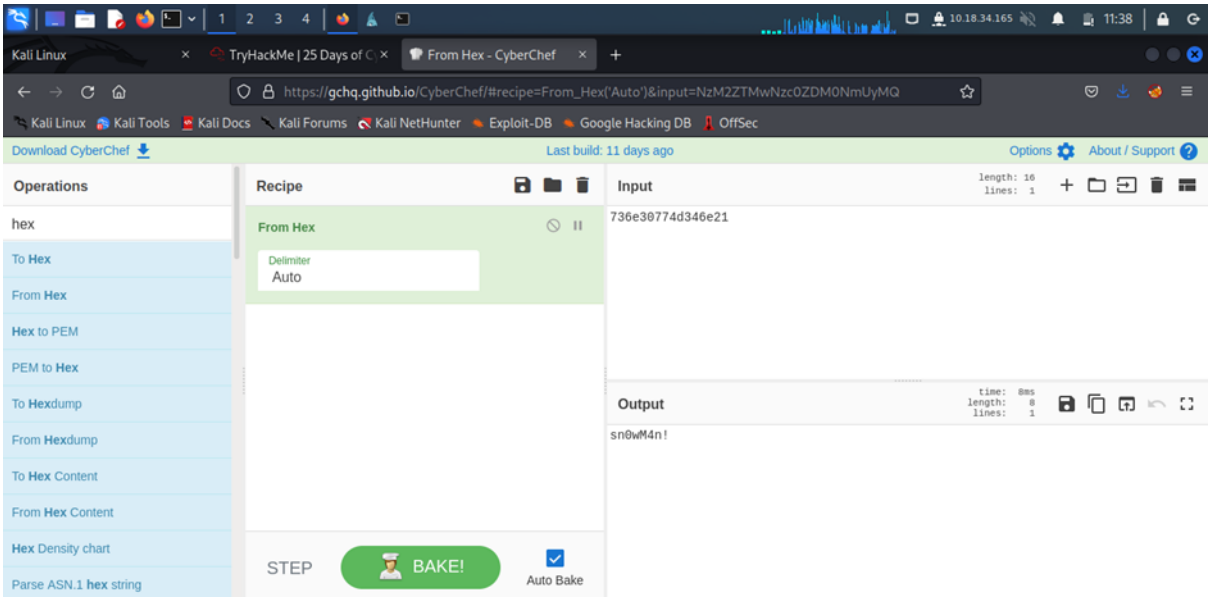


Including the question that was asked and the notes in the hiya key, are displayed when the hiya key is opened.

Question 4:

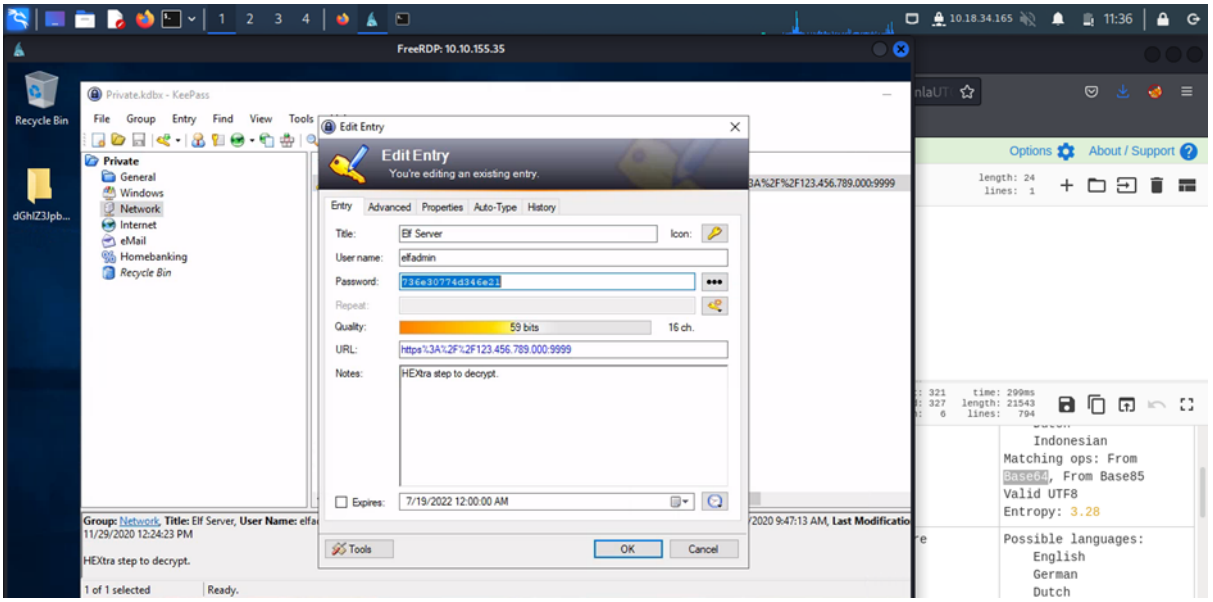


In the title of the edit entry, enter the value of the elf server. The message and the remainder of the edit entry information will therefore be displayed via the edit entry key. Copy the encrypted password.



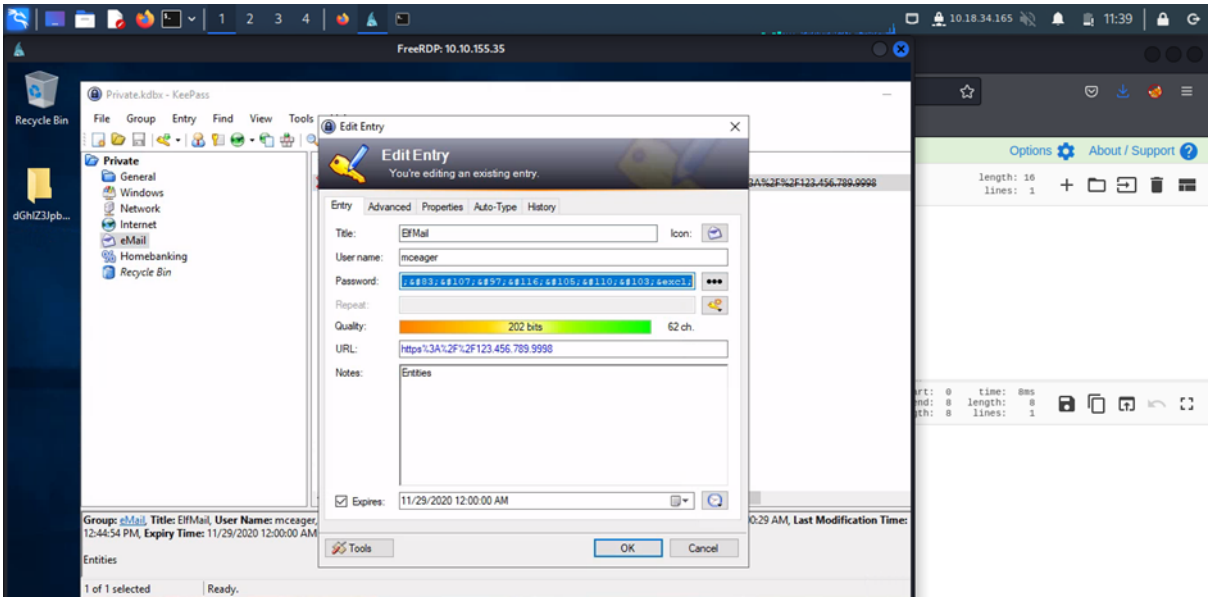
Enter the password that has been deciphered on the Cyberchef website. Consequently, it will display the results.

Question 5:

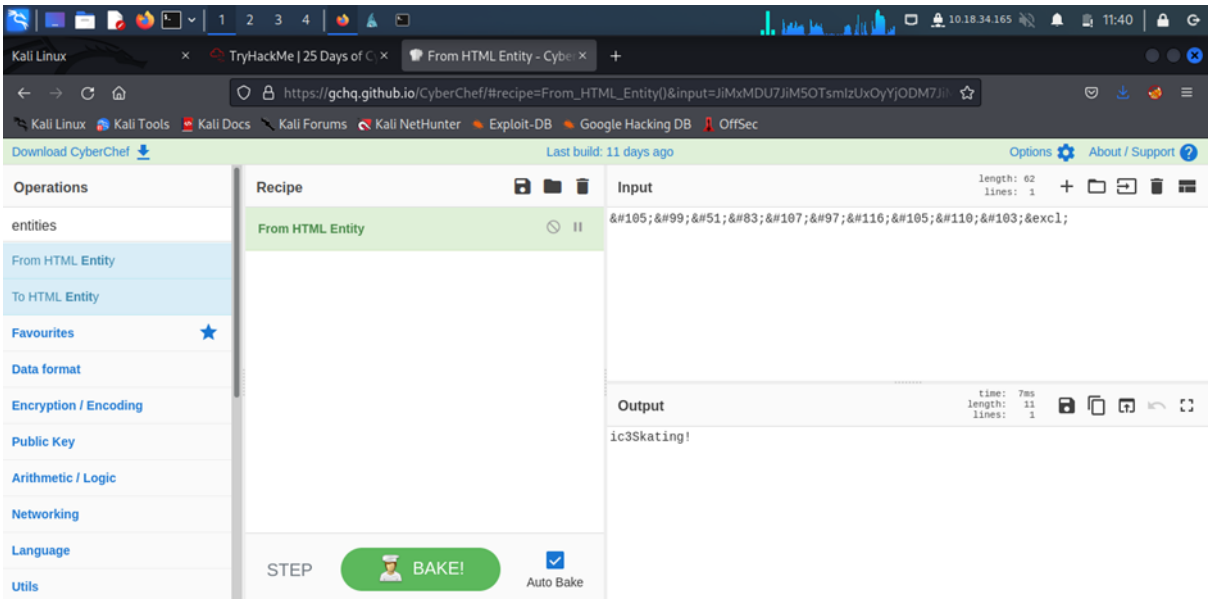


Reopen the edit entry programme and check the notes. It displays the password for the Elf Server's encoding.

Question 6:

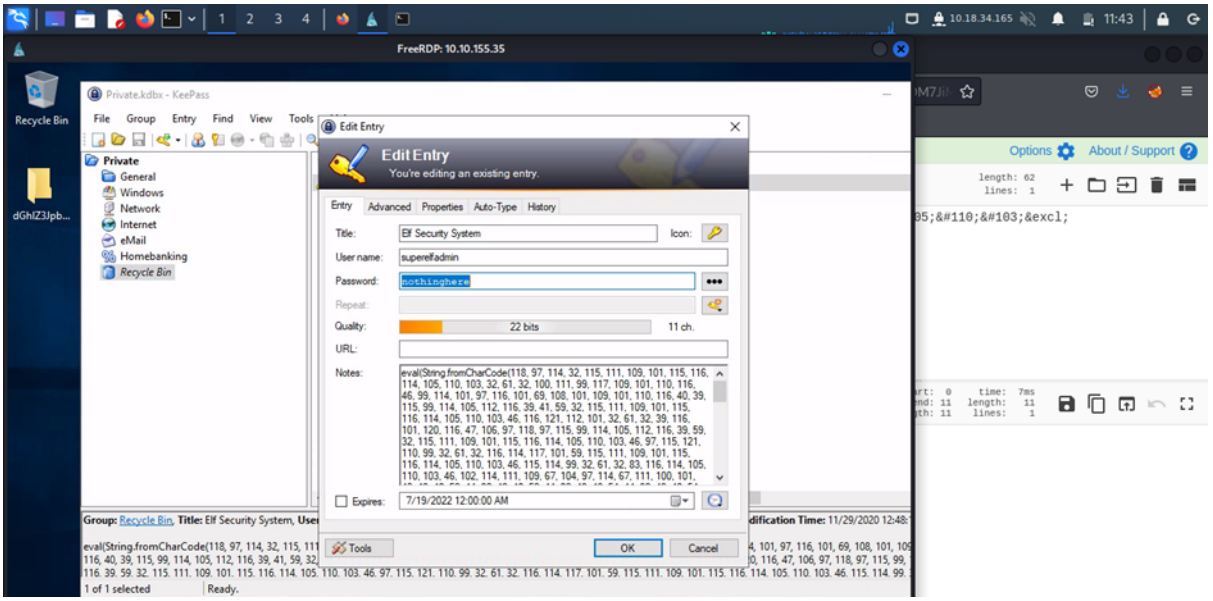


Enter the edit entry after opening the title ElfMail. It displays the edit entry title's details. Take note of the ElfMail password.



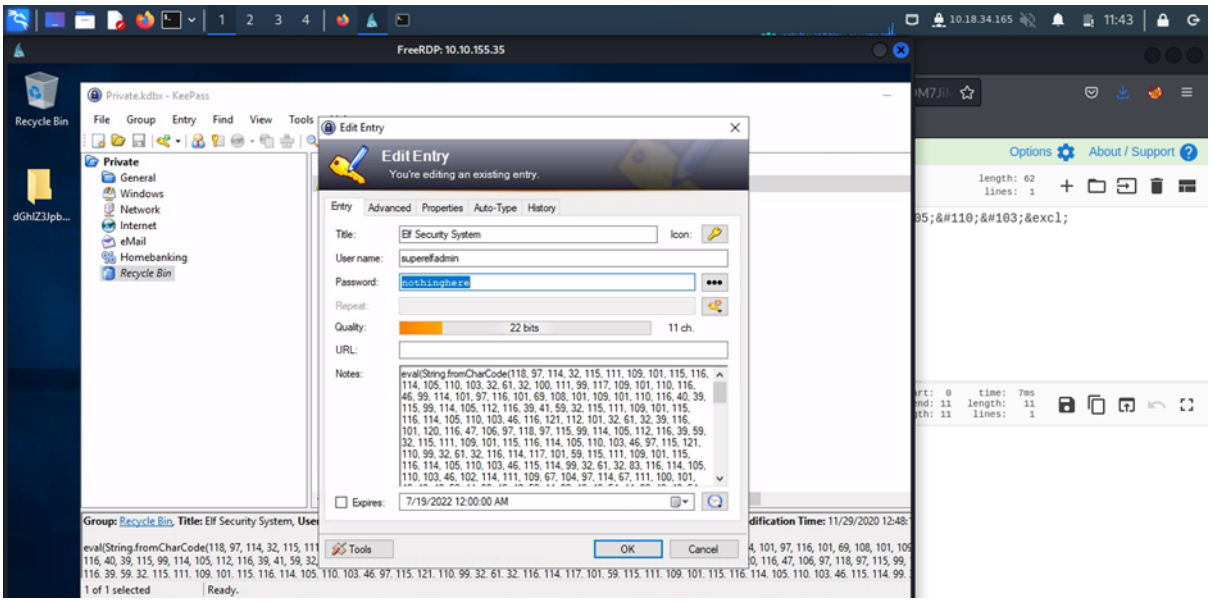
Use CyberChef to decode it and display the results.

Question 7:

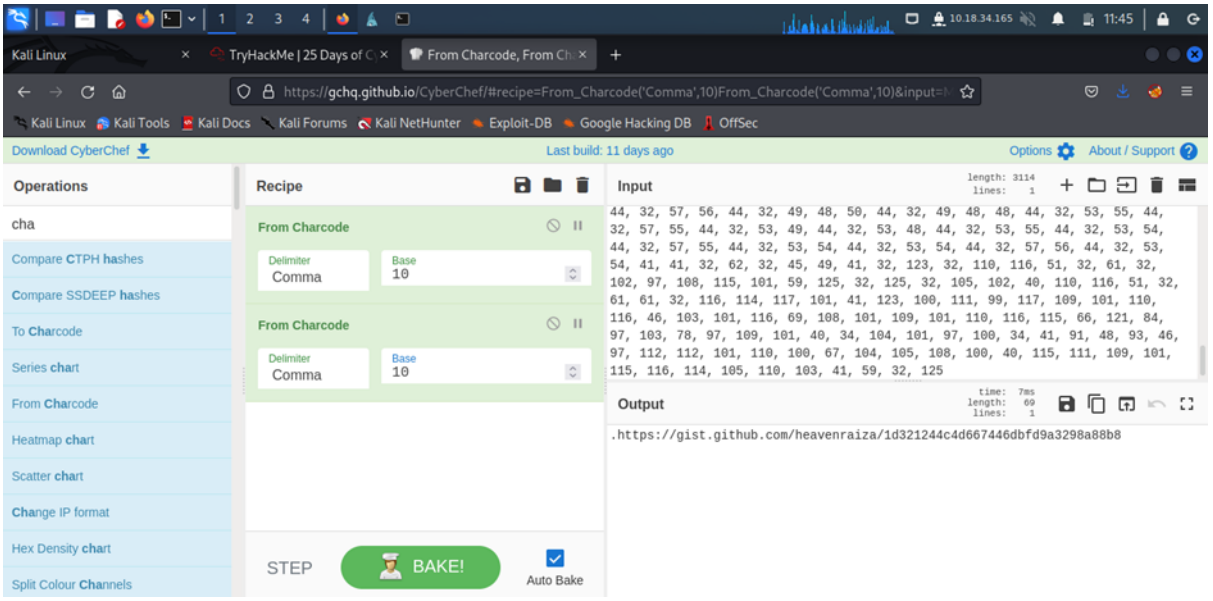


Elf Security System's username and password are displayed when you type in the title. Remember to provide your password.

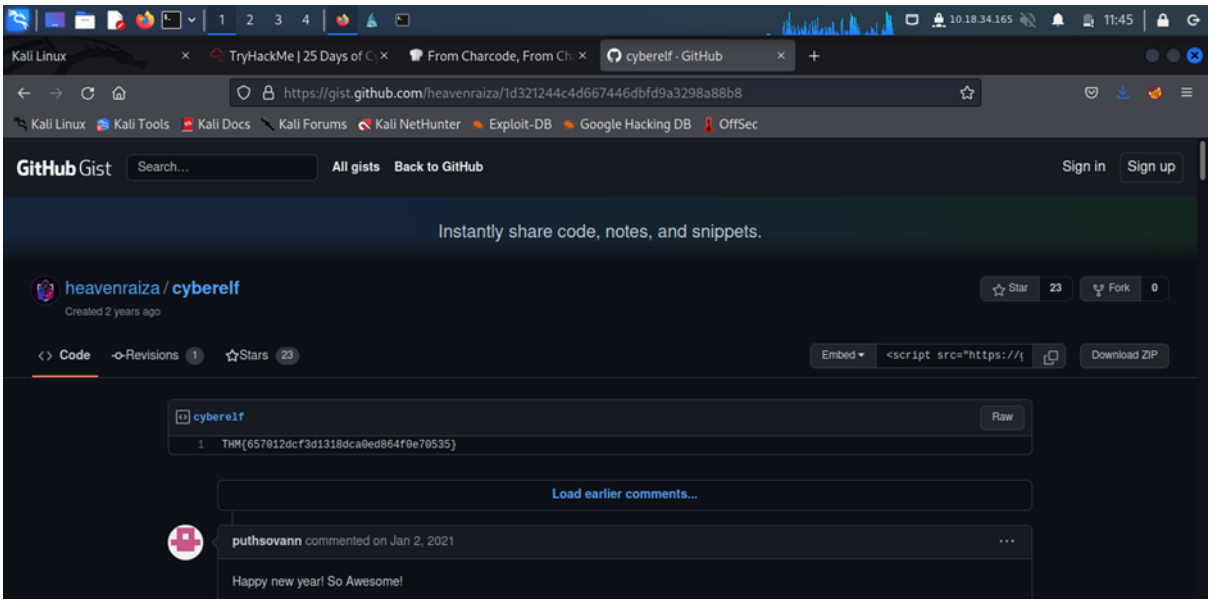
Question 8:



In the edit entry, copy the password.



When you paste the password into the input, the output on the CyberChef website is displayed.



There is a link to the github website. Copy the link, then paste it. It will display the appropriate question's flag.

Thought Process/Methodology:

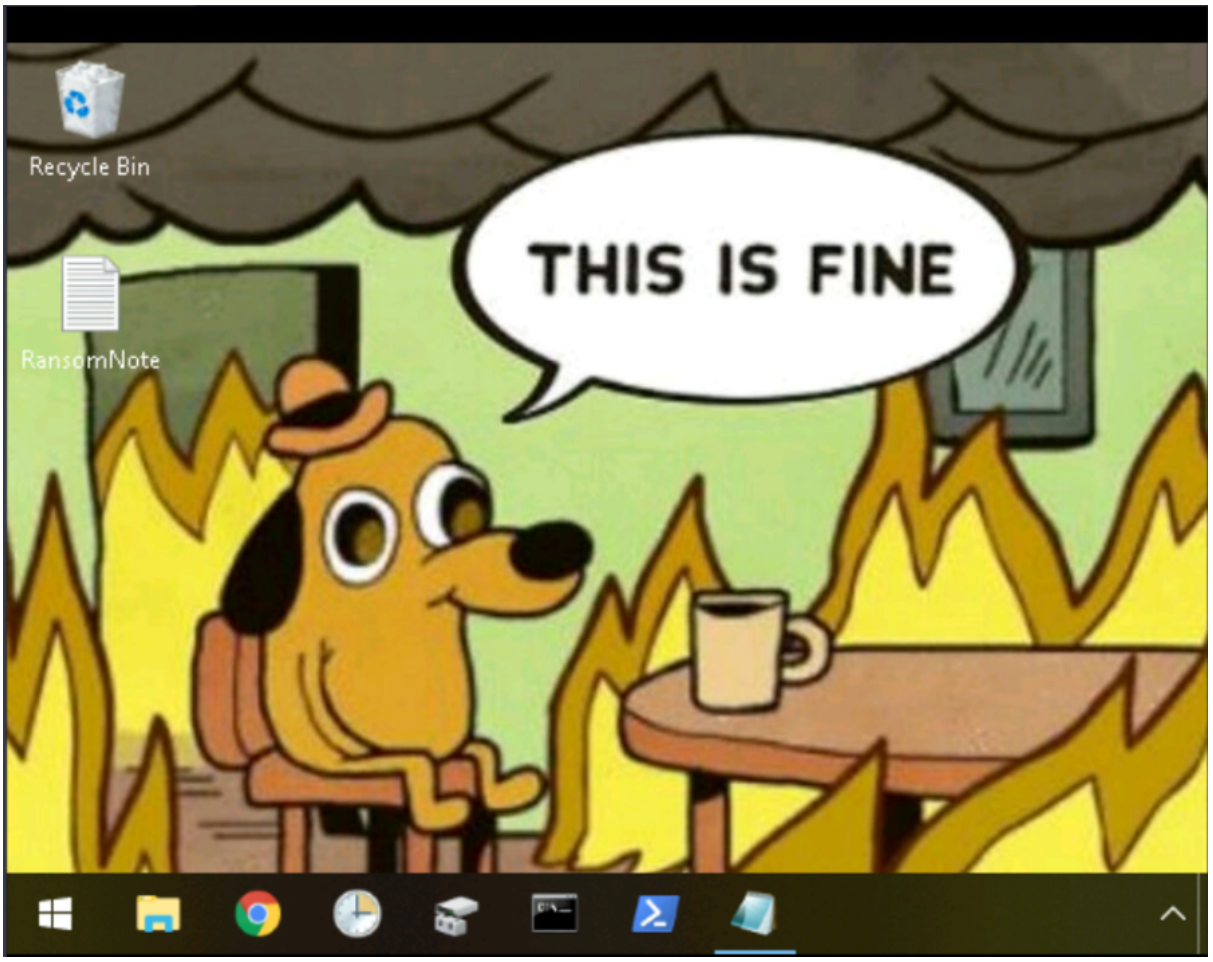
Remmina can be used to decode the file as requested, according to the day task above. To make the task more simpler, the file was provided. In addition, it has an application for editing entries that allows you to change the title of an entry. It displays the user name and password as well as any notes-provided data. Most often, we employ Cyberchef as a password decoder to obtain the required

information. Last but not least, the request for the flag was made in response to the last query. The flag was obtained via the Github link provided by the edit entry and was then decoded using Cyberchef. In the end, system titles make it simple to decrypt every password.

Day 23 : The Grinch strikes again!
Tools used: THM AttackBox, Remmina
Solution/walkthrough:

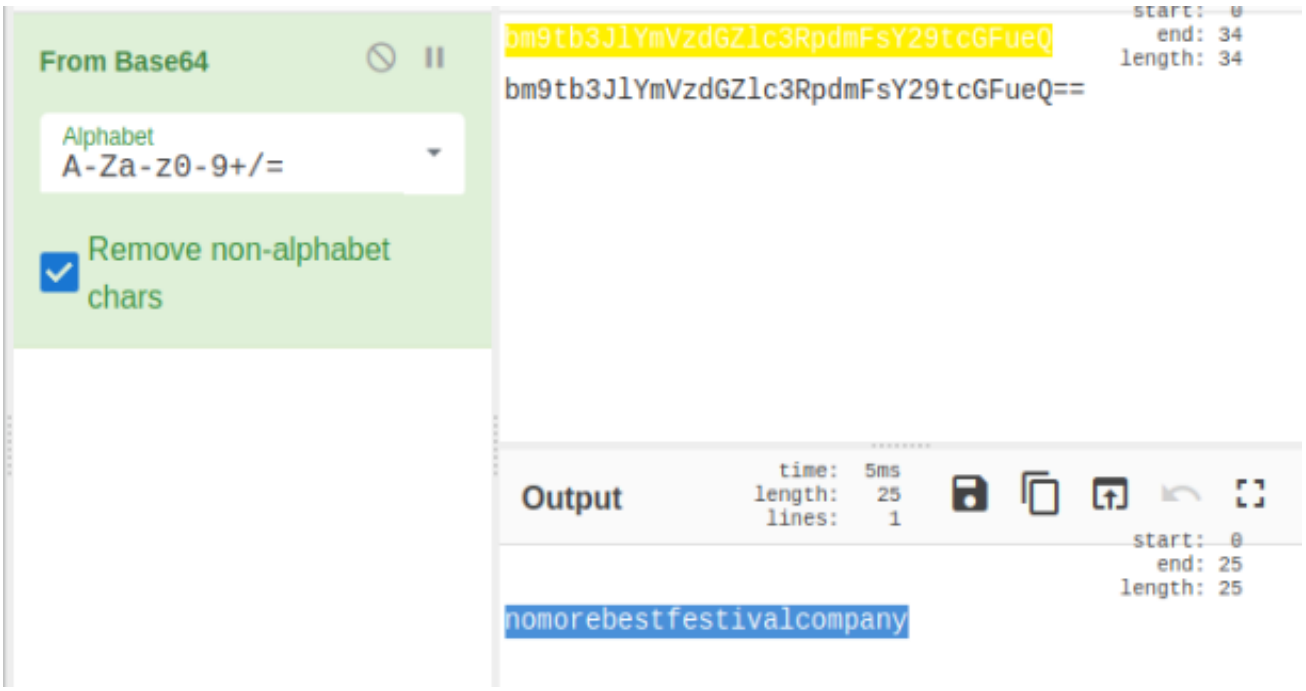
Question 1:

When we open up the RDP connection a wallpaper will appear that write “THIS IS FINE”



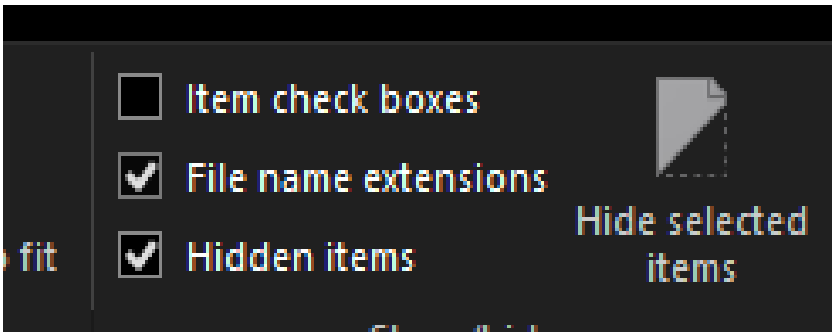
Question 2:

To decrypt the fake “bitcoin address” we can use the CyberChef tool to do it. We can copy paste the fake address onto CyberChef with the option “from Base64” and we’ll get the plain text value.

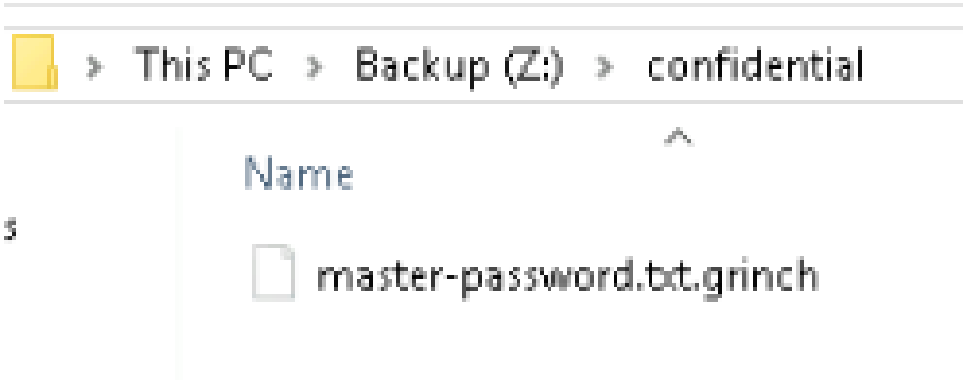


Question 3:

In the file explorer, we can go to the view section. Inside there we can tick the “hidden item” and ”File name extensions” box.

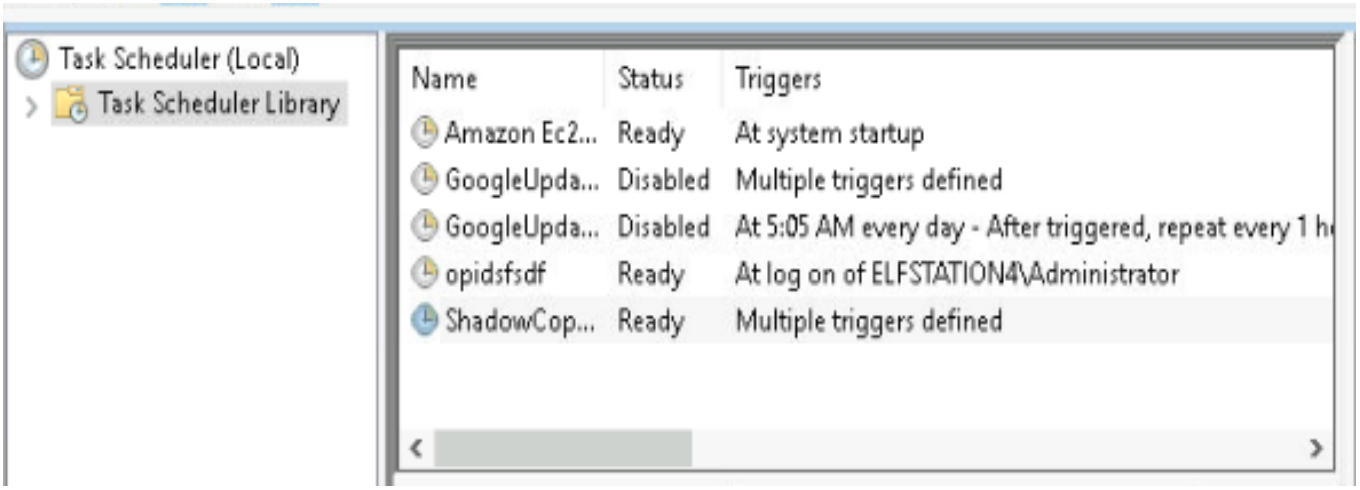


Now we can view a new file that was supposedly hidden called “confidential”. Inside there is a encrypted files and we are now able to identify the file extension.



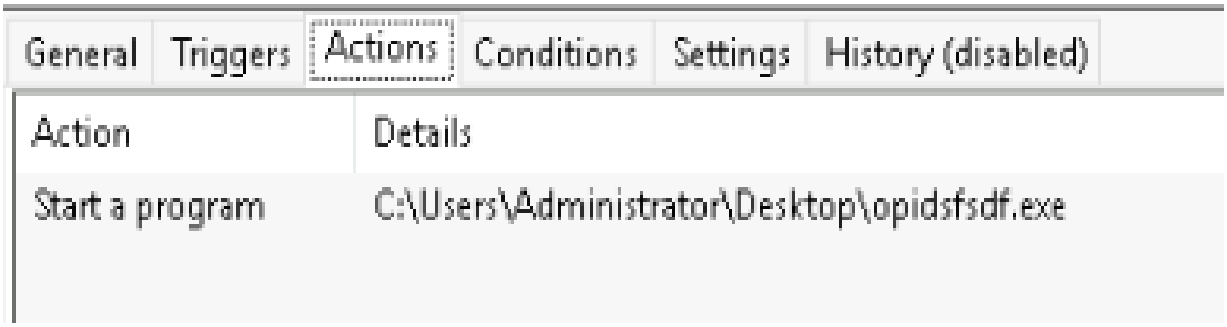
Question 4:

We can use the Task Scheduler to search for the suspicious scheduled task. After we open the Task Scheduler and click on the Task Scheduler Library one file stand out more than the other due to its odd name. That file is what we want.



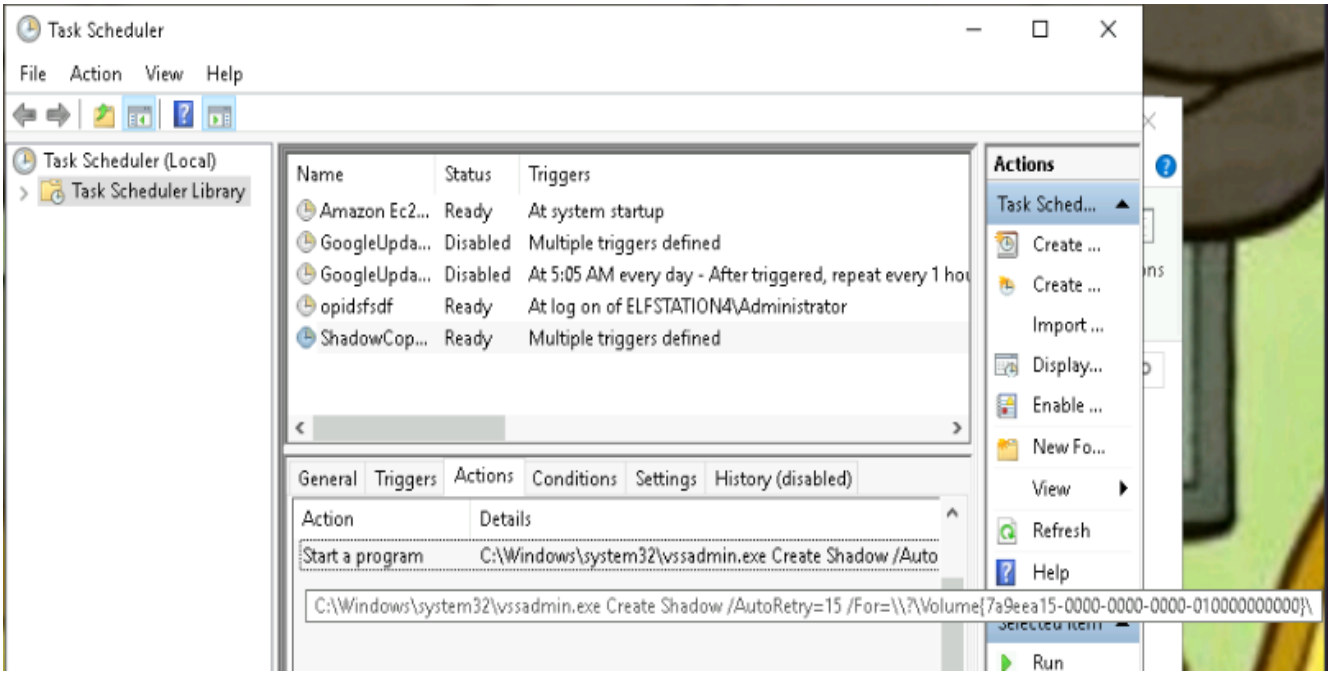
Question 5:

To inspect the properties of the scheduled task, we can click on the opidsfsdf task and below, there is an “ACtions” option. There, we can see the location of the executable

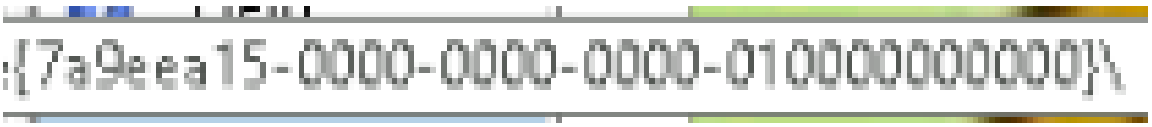


Question 6:

To find that ShadowCopyVolume ID we can repeat the same step from question 5 which is to first, open the task scheduler library and click on the ShadowCopyVolume task. Then, we click on the actions and we can see the location of executable

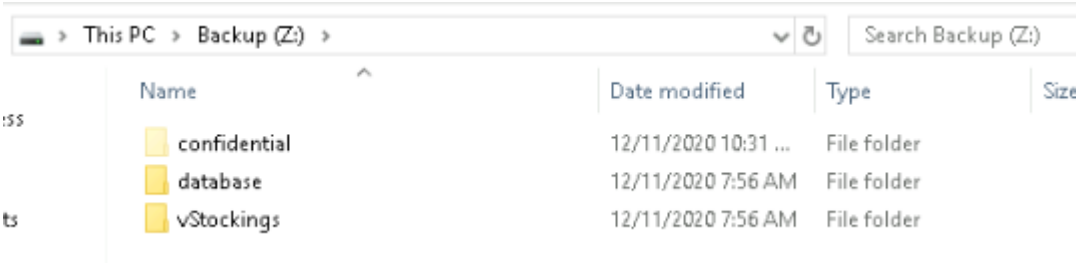


Then by hovering on the details of the program we can see the entire directory. At the end of the directory there's a weird combination of numbers and letters, that is the ID that we want.



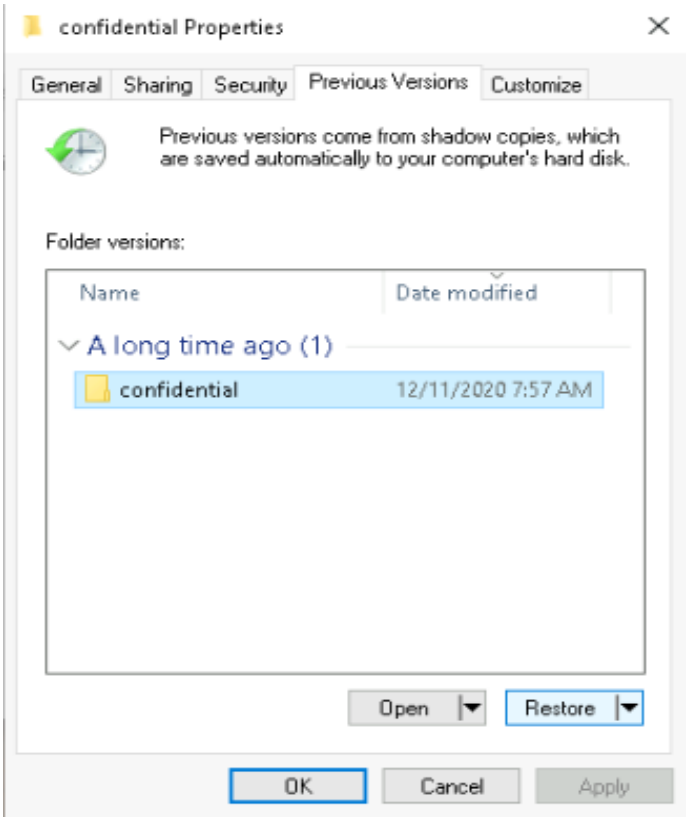
Question 7:

The name of the hidden file is “confidential” which we have already acquired from question 3.

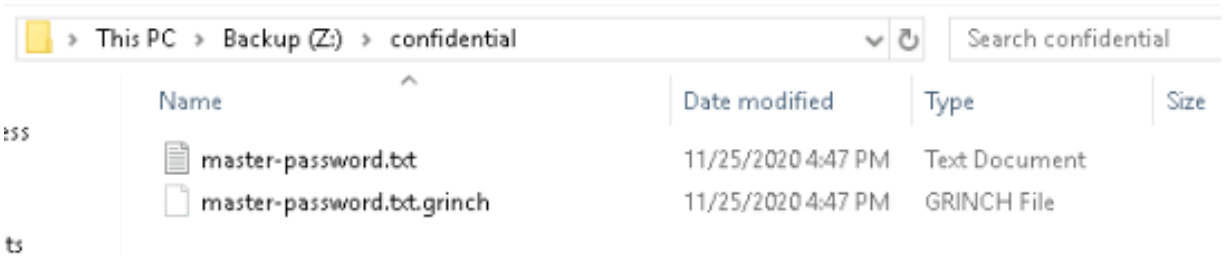


Question 8:

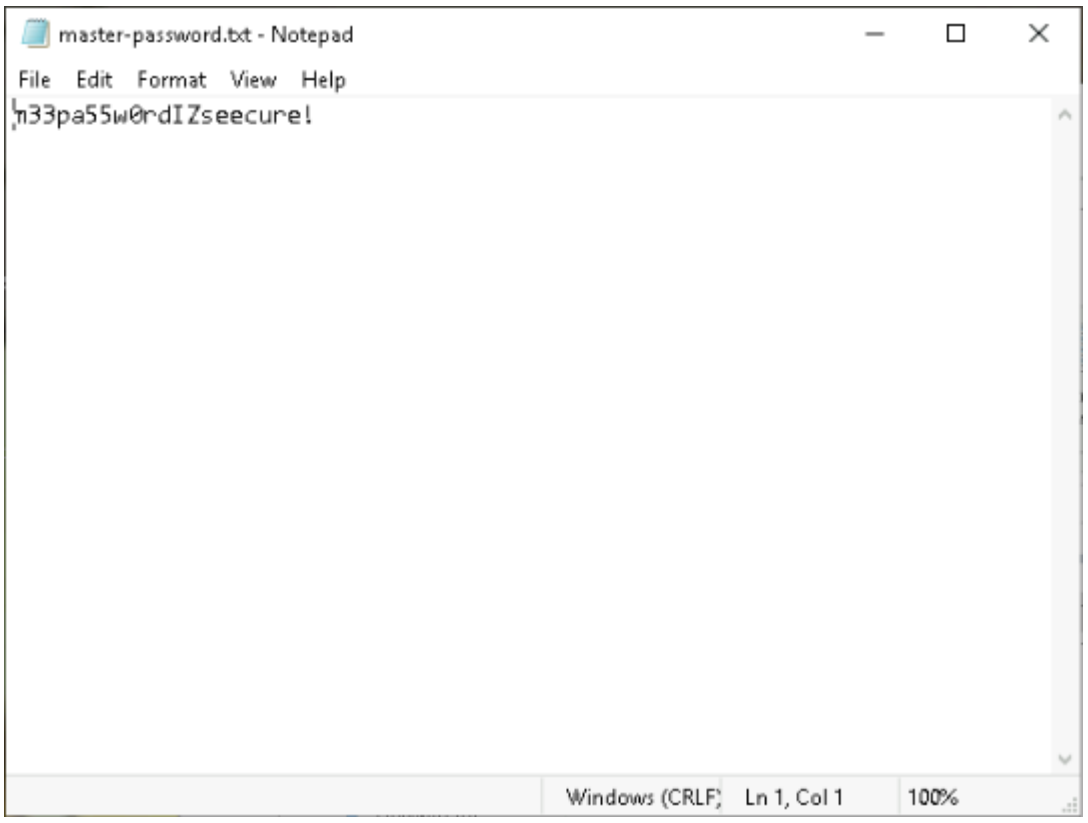
First we right-click and inspect the properties of the confidential folders and use the “Previous Versions” option.



We can click the “Restore” button to restore the previous file and now we have the master-password.txt file



Click the restored file and we will have the password

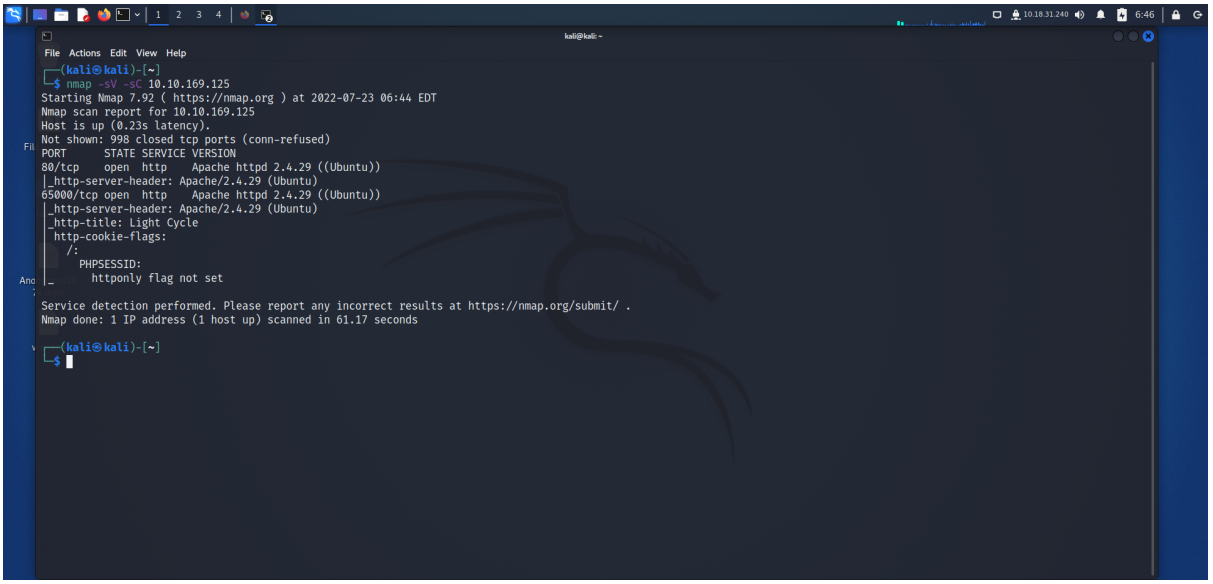


Thought Process/Methodology:

I use the TryHackMe AttackBox which already provides all the necessary tools to complete the task, life has been made easy. We can use the remmina to connect to the remote machine via RDP. After we finished connecting, it seems there's a ransom note inside the machine. To decrypt the fake bitcoin address inside the note, we can use CyberChef to decrypt it using the base64. Next we have to edit our File Explorer so that it can show the hidden files within and the file extension. To do that we can just change to the "view" option in the file explorer. Another fancy tool that we can use is the Task Scheduler. From there we can see a suspicious scheduled task which is the opidsfsdf.exe file. Using Task Scheduler we can also identify another scheduled task that is related to VSS which is the ShadowCopyVolume. Additionally we can also get its ID from Task Scheduler. For the final task we can restore the previous versions of the confidential folder to do that, we just have to inspect the properties of said folder and there's a "Restore Previous" section. After we restore the previous version, a new file will appear and inside we can get the password.

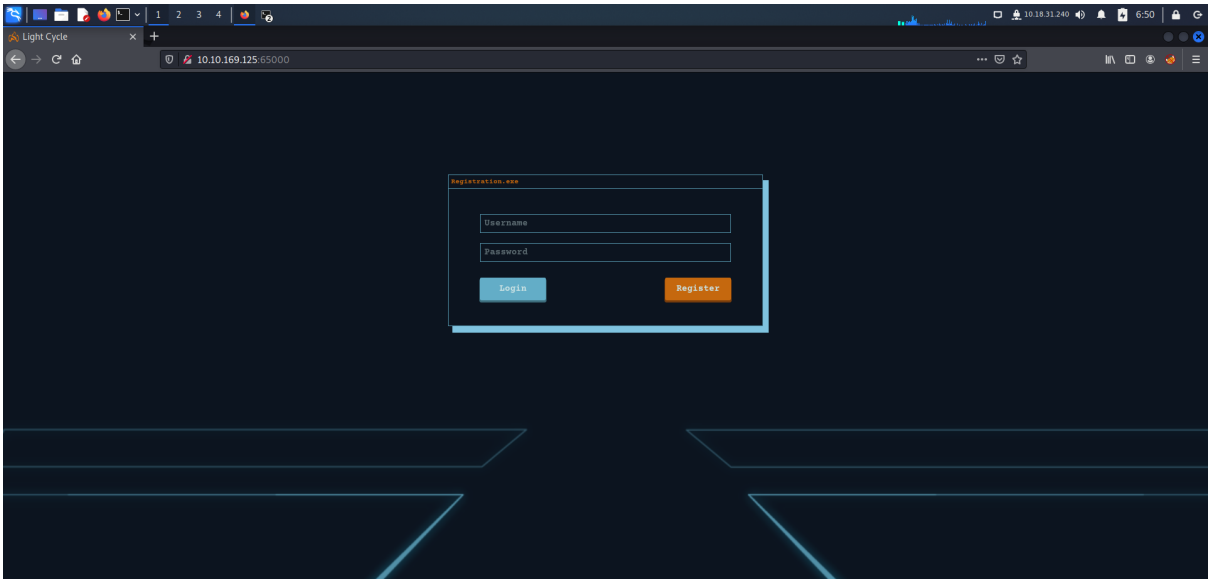
Day 24 - (Final Challenge) The Trial Before Christmas
Tools used: Kali Linux, Firefox, Terminal, Burp Suite
Solution/walkthrough:

Question 1: (Scan the machine. What ports are open)
Answer: 80 and 65000



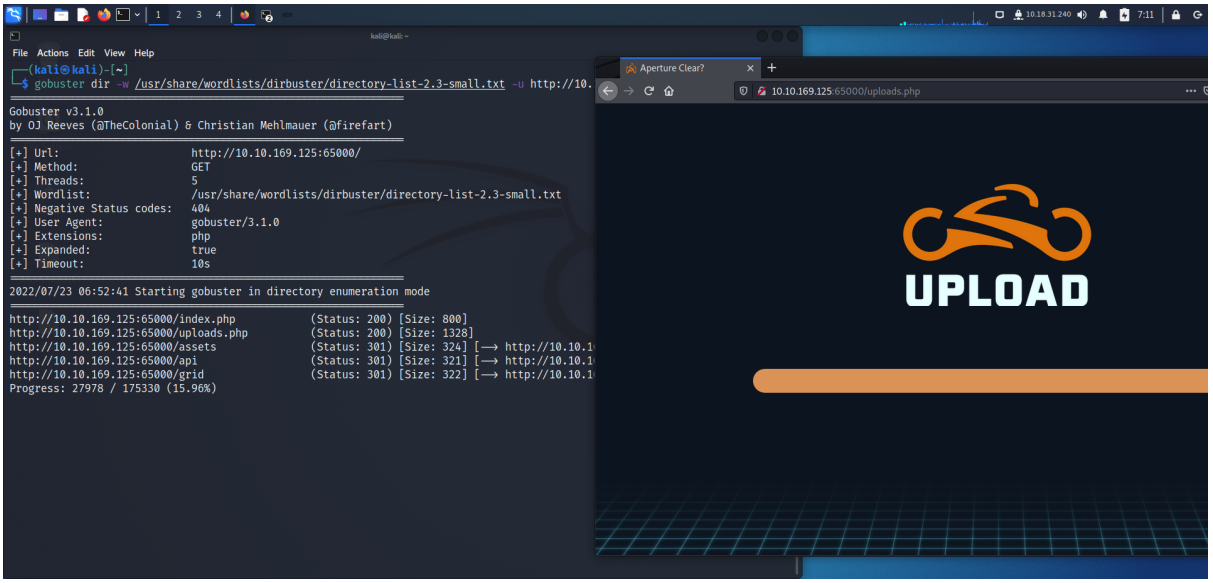
Run a nmap scap to find your answer.

Question 2:(What's the title of the hidden website?)
Answer: Light Cycle



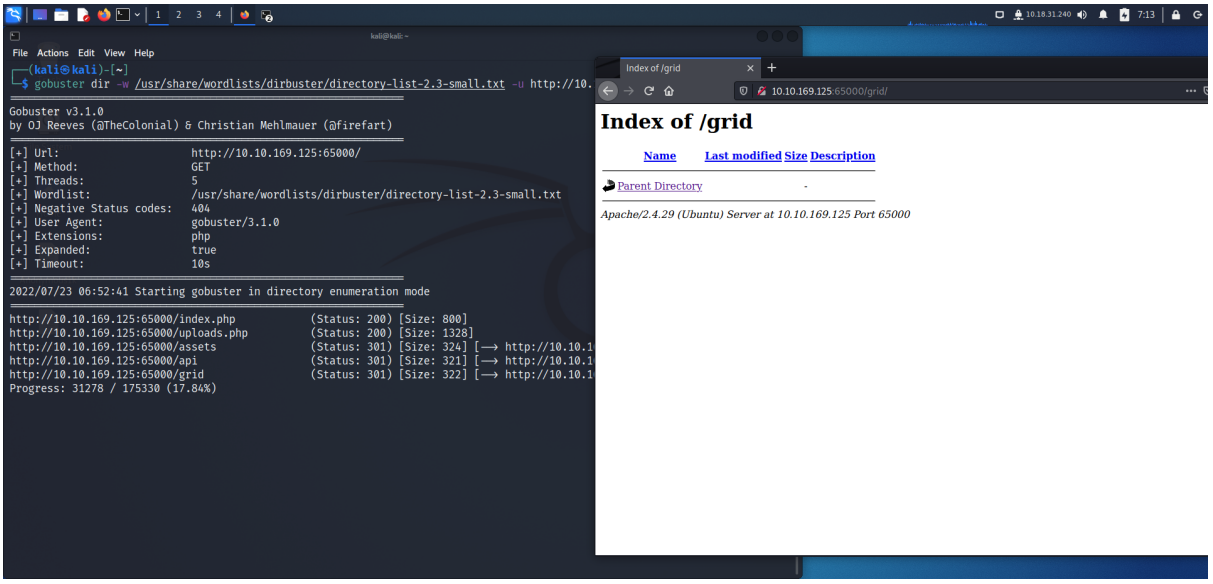
Go to the hidden website by using the ports that you had found

Question 3:(What is the name of the hidden php page?)
Answer: /uploads.php



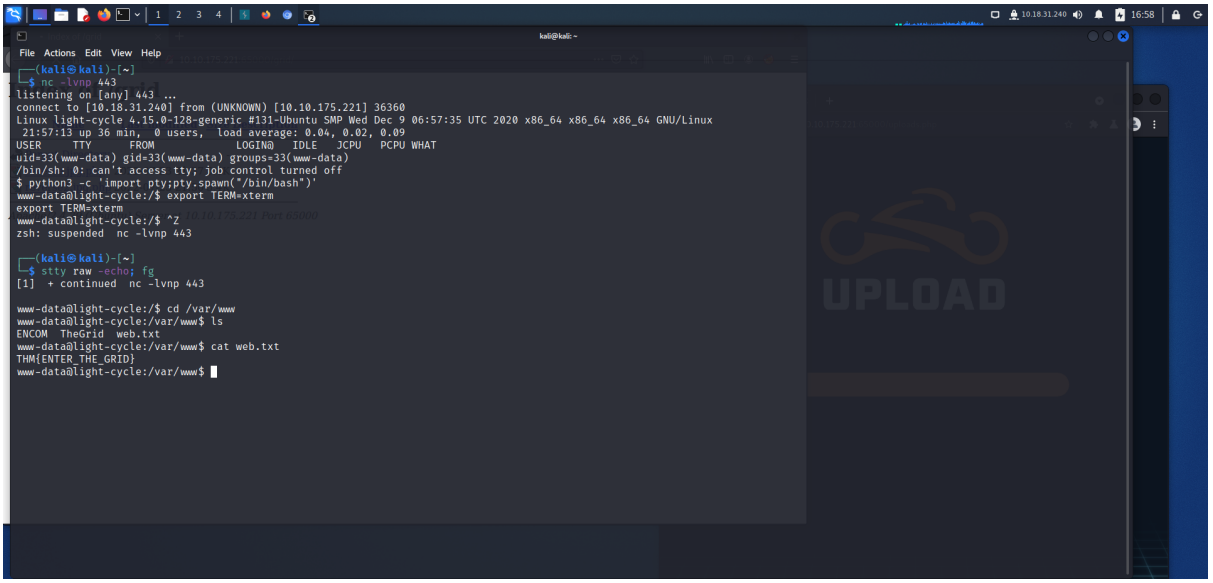
Use gobuster to find the directory

Question 4: (What is the name of the hidden directory where file uploads are saved?)
Answer: /grid



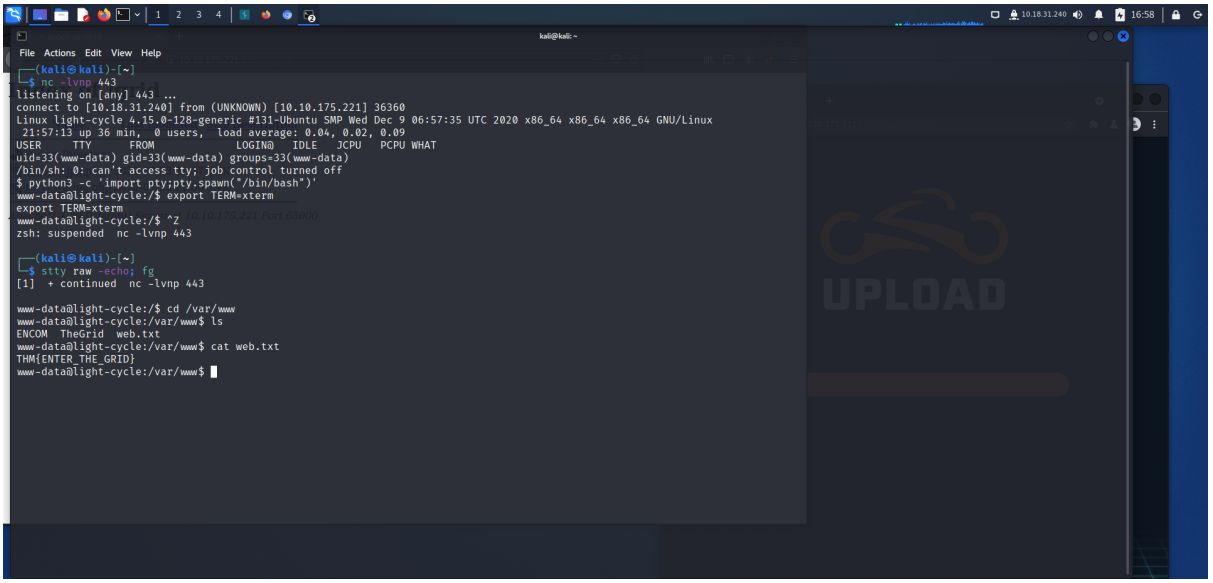
Same step with Question 3

Question 5: (What is the value of the web.txt flag?)
Answer: THM{ENTER_THE_GRID}



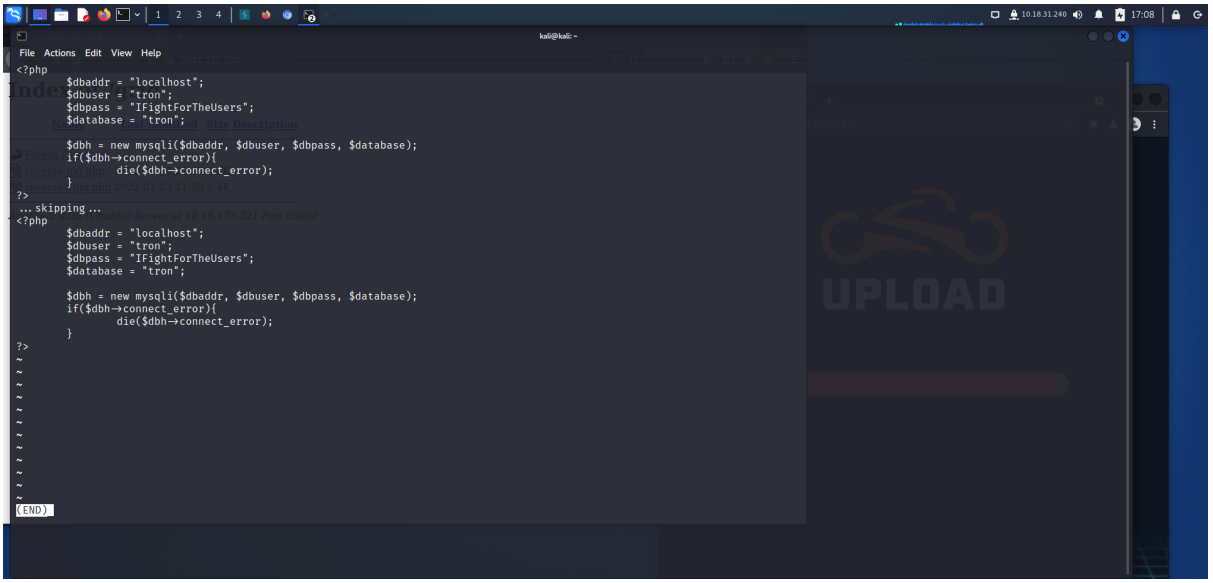
Bypass the upload page using burpsuite. Then use netcat to listen to the port to upgrade and stabilize the shell to find the answer.

Question 6: (What lines are used to upgrade and stabilize your shell?)
Answer: python3 -c 'import pty;pty.spawn("/bin/bash")' , export TERM=xterm, stty raw -echo; fg



Follow the instructions in Tryhackme.

Question 7: (What credentials do you find? username:password)
Answer: tron:IFightForTheUsers

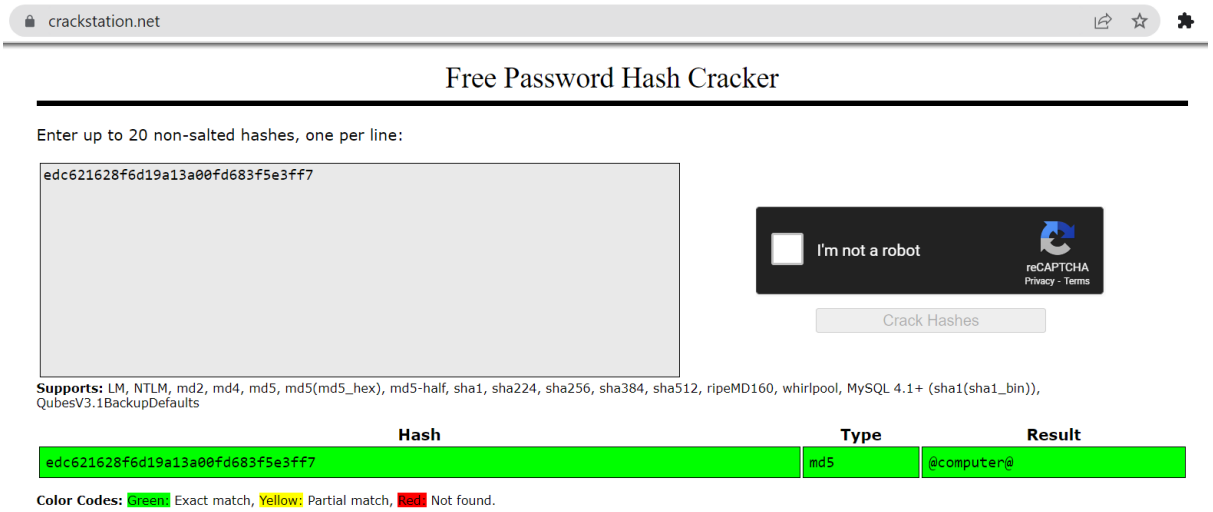


Find the files and cat it to find your answer.

Question 8: (What is the name of the database you find these in?)
Answer: tron

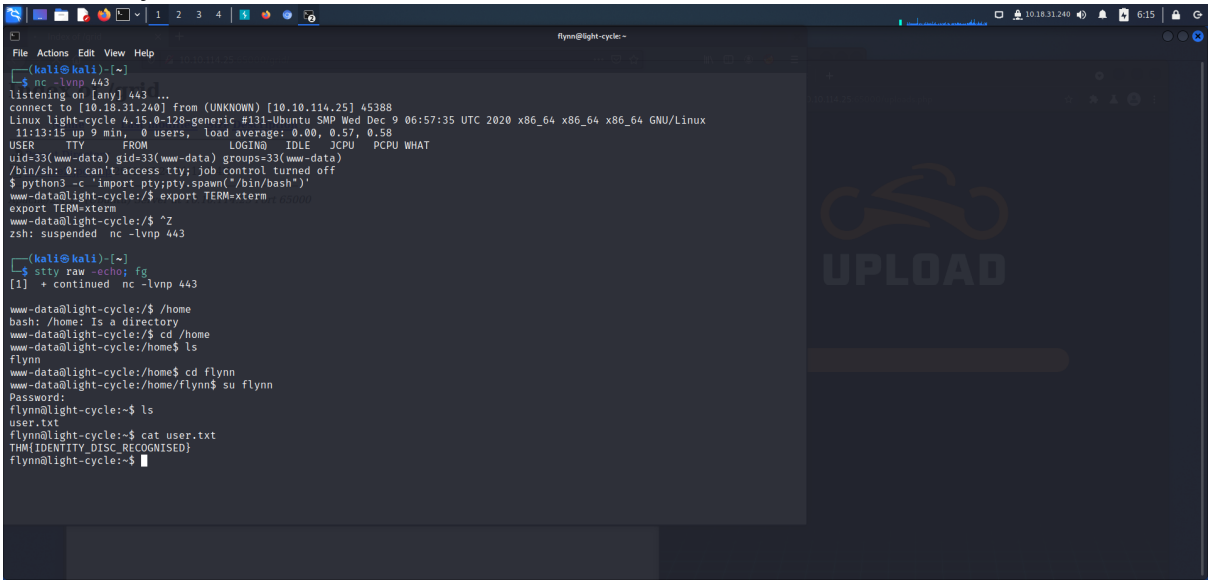
Find the answer by using mysql.

Question 9: (Crack the password. What is it?)
Answer: @computer@



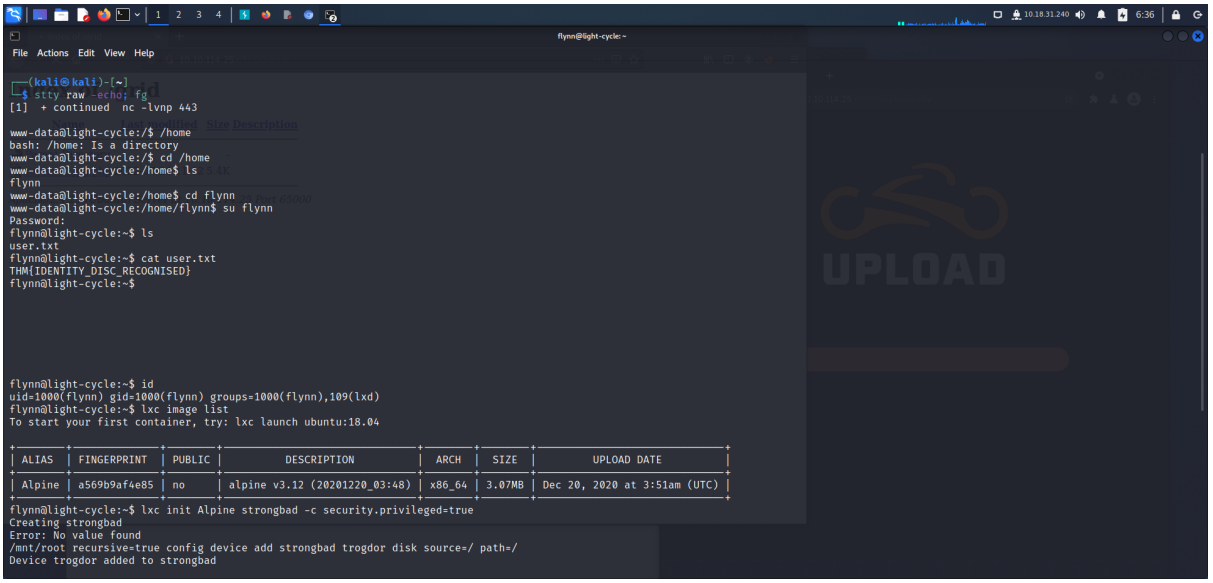
Find the answer by finding the tables from database and crack the encrypted password.

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



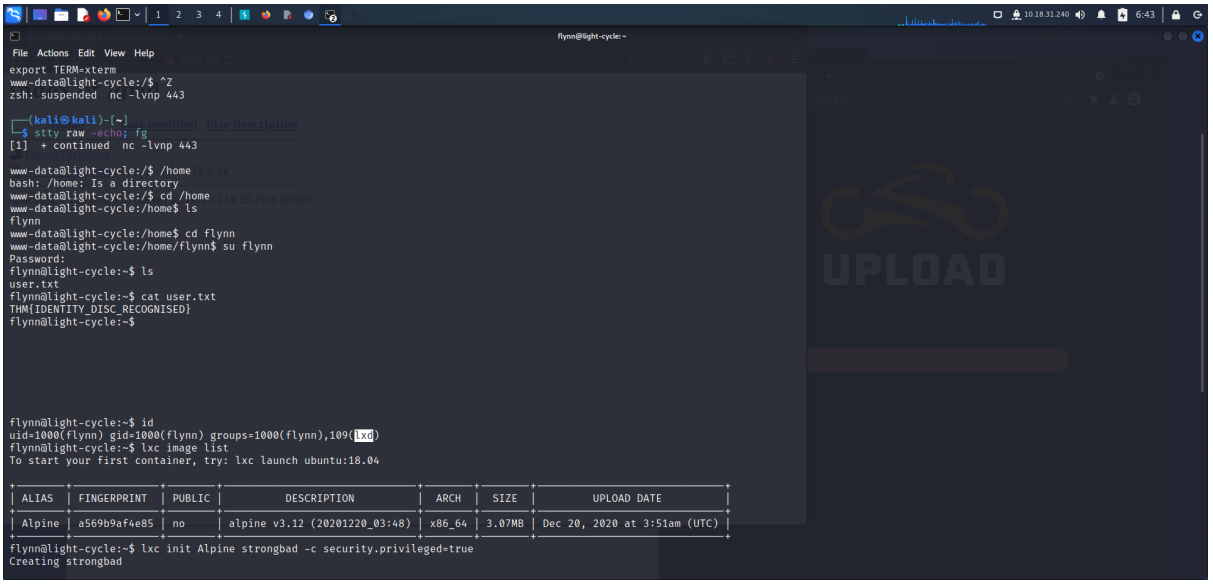
Login by using as flynn and insert the password that you had crack.

Question 11: (What is the value of the user.txt flag?)
Answer: THM{IDENTITY_DISC_RECOGNISED}



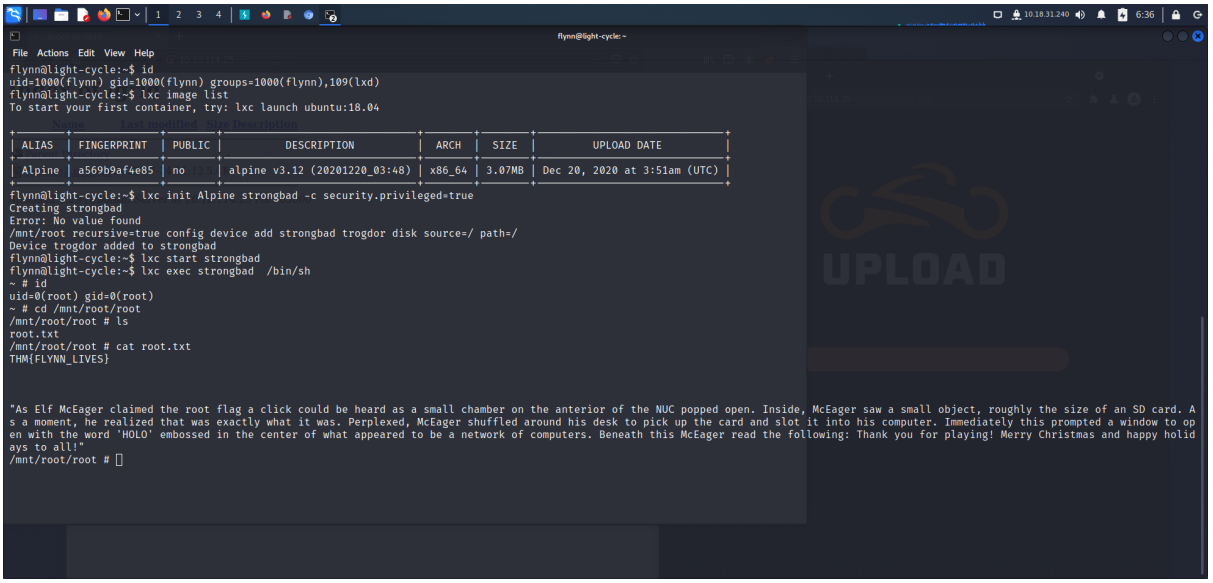
Search the directory after login as flynn and find the file and netcat it to find the answer.

Question 12: (Check the user's groups. Which group can be leveraged to escalate privileges?)
Answer: lxd



Find the answer by using command id.

Question 13: (What is the value of the root.txt flag?)
Answer: THM{FLYNN_LIVES}



Find the answer by using /root/

Thought process/Methodology:
For this day, it has 3 flags. First of all, run a nmap scan to find the ports. Next, open the firefox and go to the website with the ports that you have scanned. Next, find the directory by using gobuster. After finding the directory, you go to the pages which are /uploads.php and /grid. Bypass the filter by using Burp Suite. You also need to remove `|^js$` in the proxy options. After bypass it, run a netcat listener and then upload the file with reverse shell (remember to change the ip address and port)l and name it end with .jpg.php to upload it. Next, go to the /grid page and then click the file that you had upload just now and the netcat will show something. Then, you type `python3 -c 'import pty;pty.spawn("/bin/bash")'` and run it which uses Python to spawn a better-featured bash shell. Next, type `export TERM=xterm` . Then, press ctrl + z to background the shell, and type `stty raw -echo; fg` . After that, you will enter into www-data@light-cycle. To find the first flag, change the directory to /var/www/ and search the list of item inside the directory. Then, read the file (web.txt) by using cat. Then, you will found the first flag.

Next, to find the second flag, you need to access mysql. Firstly, go to /var/www/TheGrid/. See the list you will find 2 directory and 1 mp4. Go inside to /includes which are one of the directories that are listed, and then list all the files. Read the file which is named dbauth.php and you will find the username and password. Next, go back to home directory and find flynn. Change your directory to flynn and enter into mysql by typing mysql -utron -p. Enter the password that you had found just now. Inside the mysql, find the database and use it. Next, inside the database, find the tables and read it by commanding `SELECT * FROM users;` You will find the encrypted passwords. Encrypt the passwords by using some websites. Then, type su flynn and then enter the password that you had cracked just now. After entering it, find the files and read it. You will find the second flag.

To find the third flag, type id and you will find lxd. Next, type lxc image list. Next, type lxc init IMAGENAME CONTAINERNAME -c security.privileged=true which we name the IMAGENAME to Alpine and CONTAINERNAME to strongbad. Next, run lxc config device add CONTAINERNAME DEVICENAME disk source=/ path=/mnt/root

recursive=true which we name the DEVICENAME to trogdor. Next, type lxc start strongbad. Then run lxc exec strongbad /bin/sh. Next, type id to find whether we are escalated to root or not. Lastly, find the root.txt file and read it to find the flag. Congratulations, you had found all the flag!