PSP0201

WEEK 6

WRITEUP

Group name: Lion Force
Members:

ID	Name	Role
1211103128	Muhammad Ajwad bin Mohamad A’sim	Leader
1211102001	Muhammad Naqiuddin bin Edy Azhar	Member
1211103183	Nurul Nabilah binti Mohd Noor Hakim	Member
1211103165	Izzati Alia binti Incik Ghazali	Member

Table of contents

Day 21 - Blue Teaming - Time for some ELForensics 3

Day 22 - Blue Teaming - Elf McEager becomes CyberElf 10

Day 23 - Blue Teaming - The Grinch strikes again! 16

Day 24 - Final Challenge - The Trial Before Christmas 20

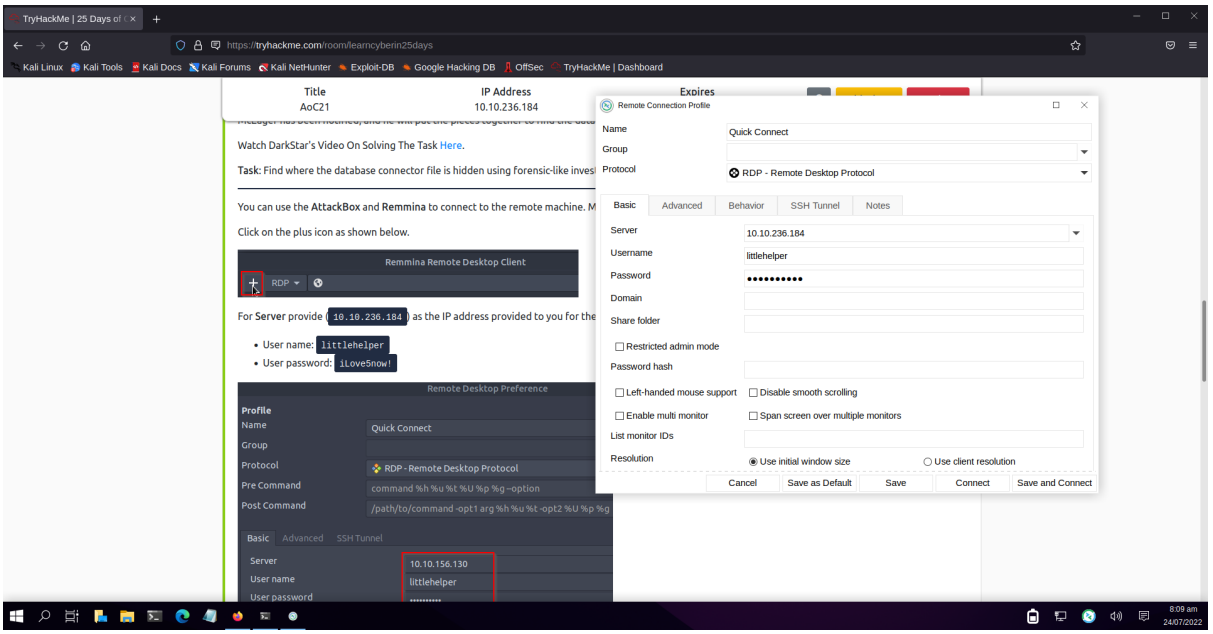
Day 21 - Blue Teaming - Time for some ELForensics

Tools used: Remmina, Terminal, Kali Linux

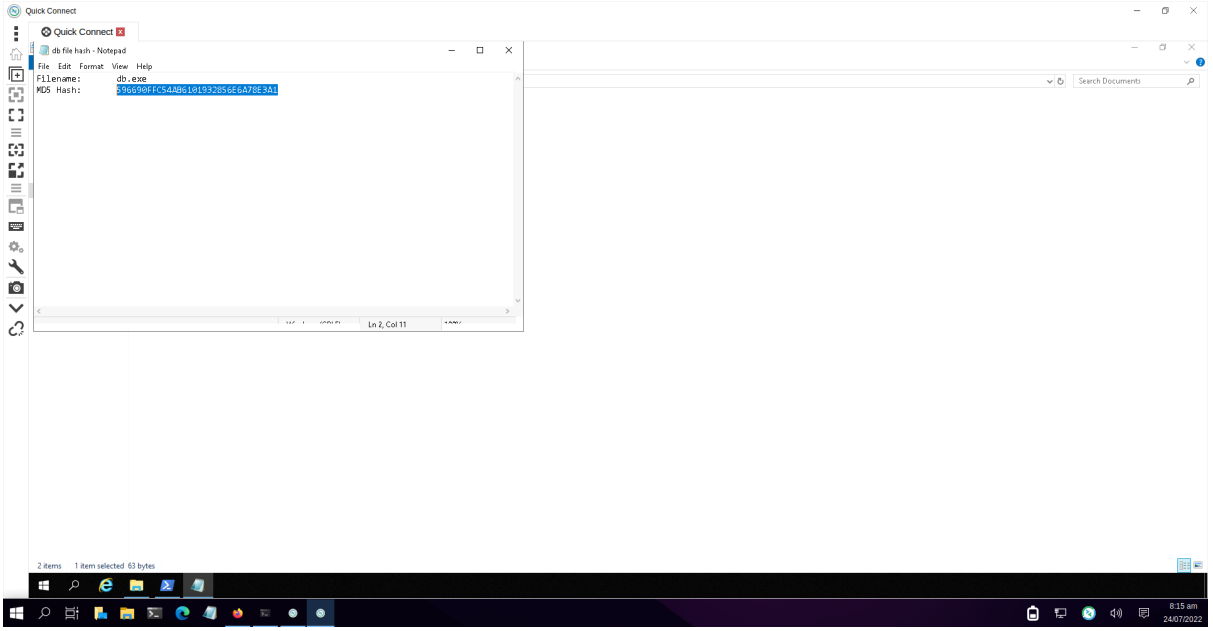
Solutions/Walktrough

<u>Question 1</u>

Connecting to remote desktop via Remmina

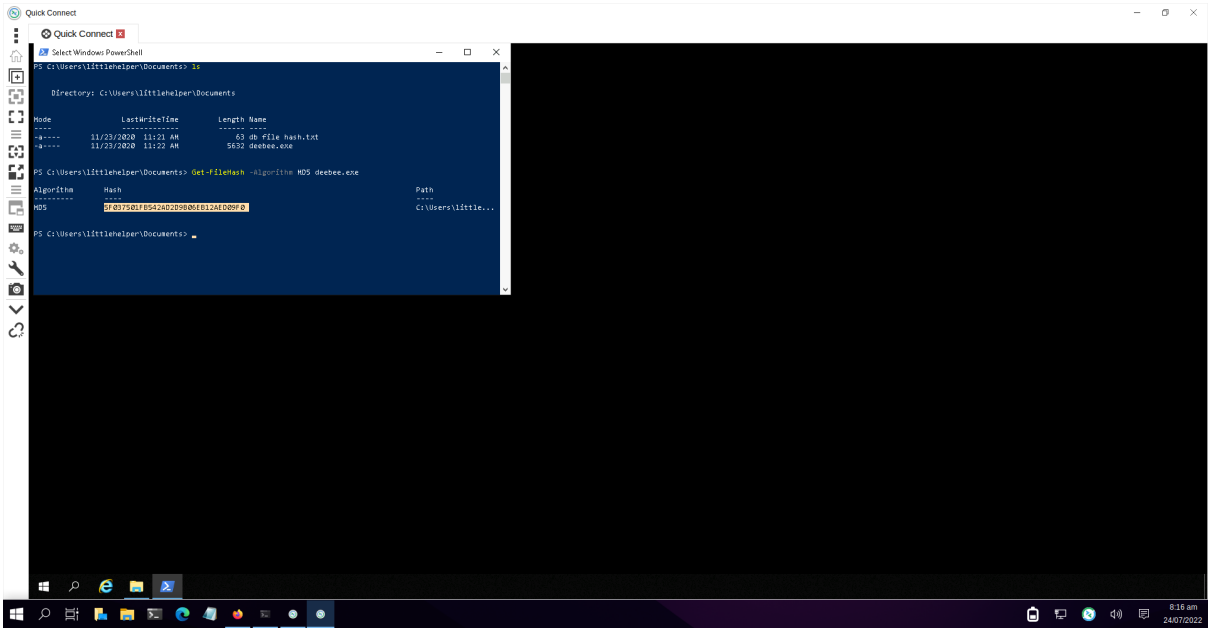


Finding the file hash for db.exe in Documents folder



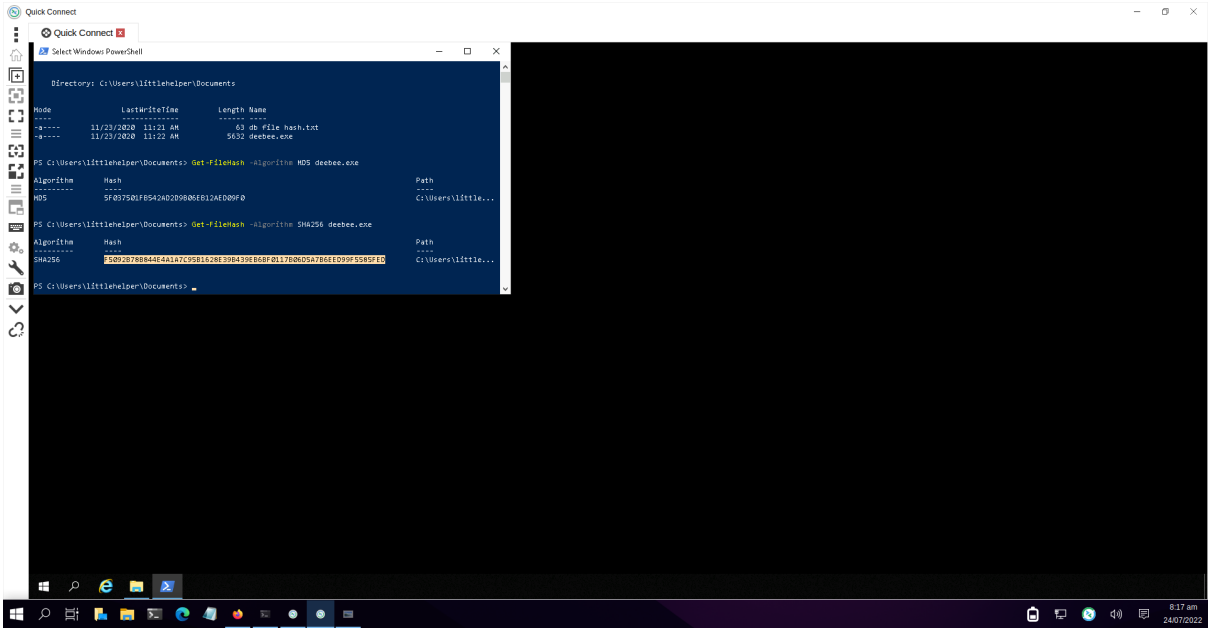
Question 2

Getting the MD5 file hash of deebee.exe using *Get-FileHash -Algorithm MD5 deebee.exe*



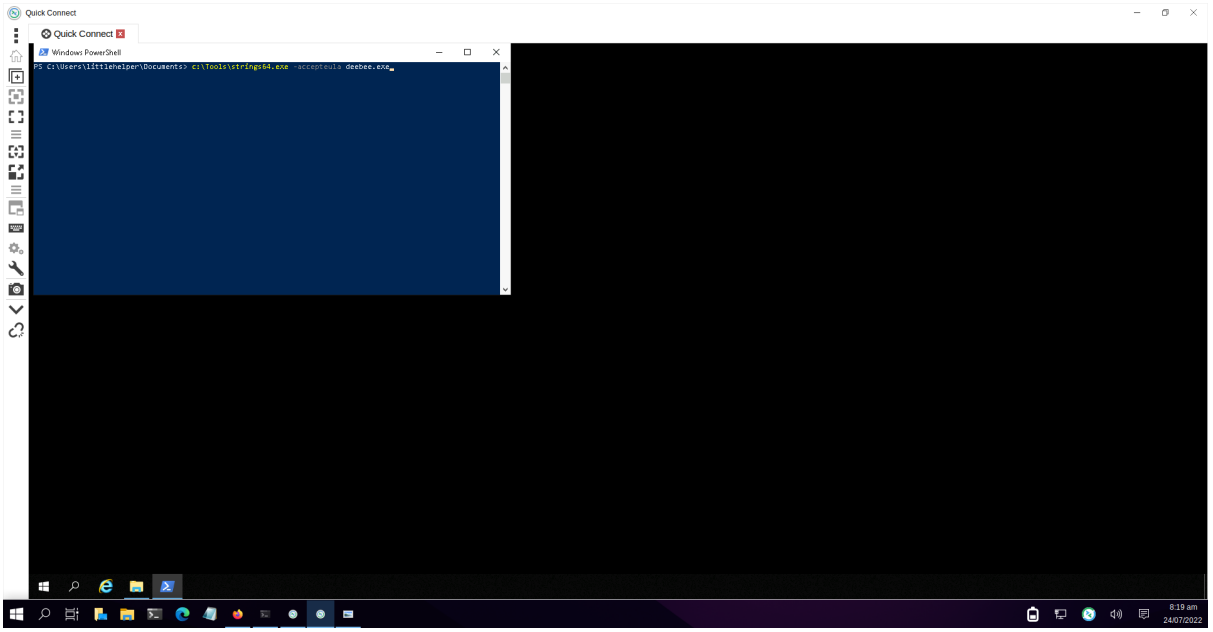
Question 3

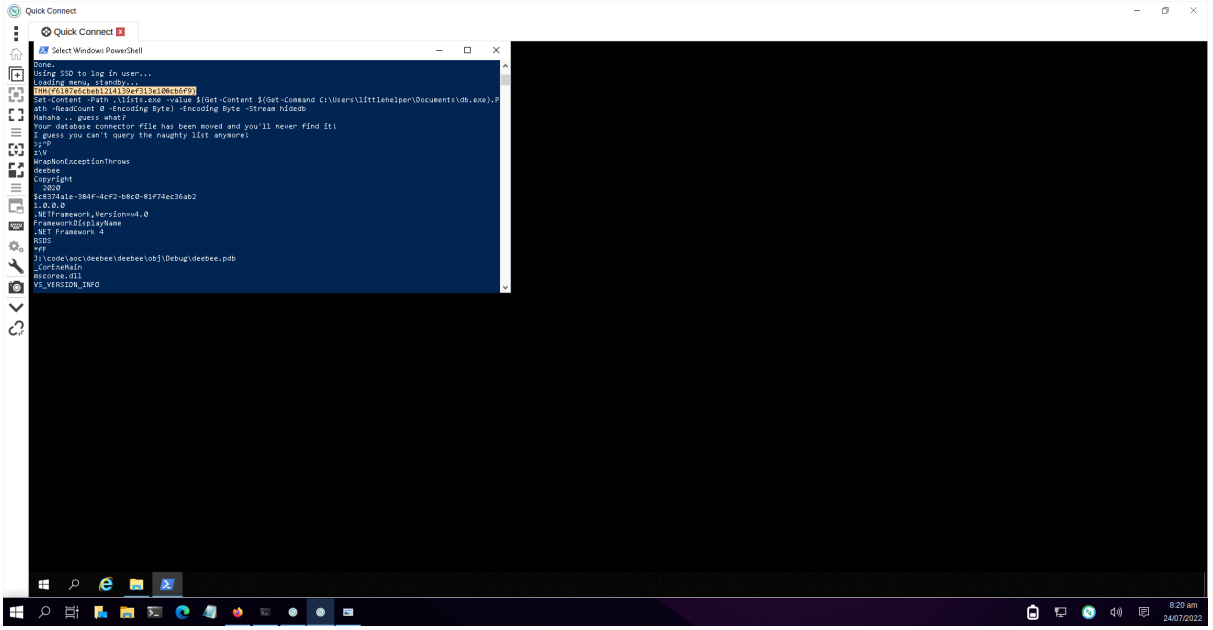
Getting the SHA256 file hash of deebee.exe by using command *Get-FileHash -Algorithm SHA256 deebee.exe*



Question 4

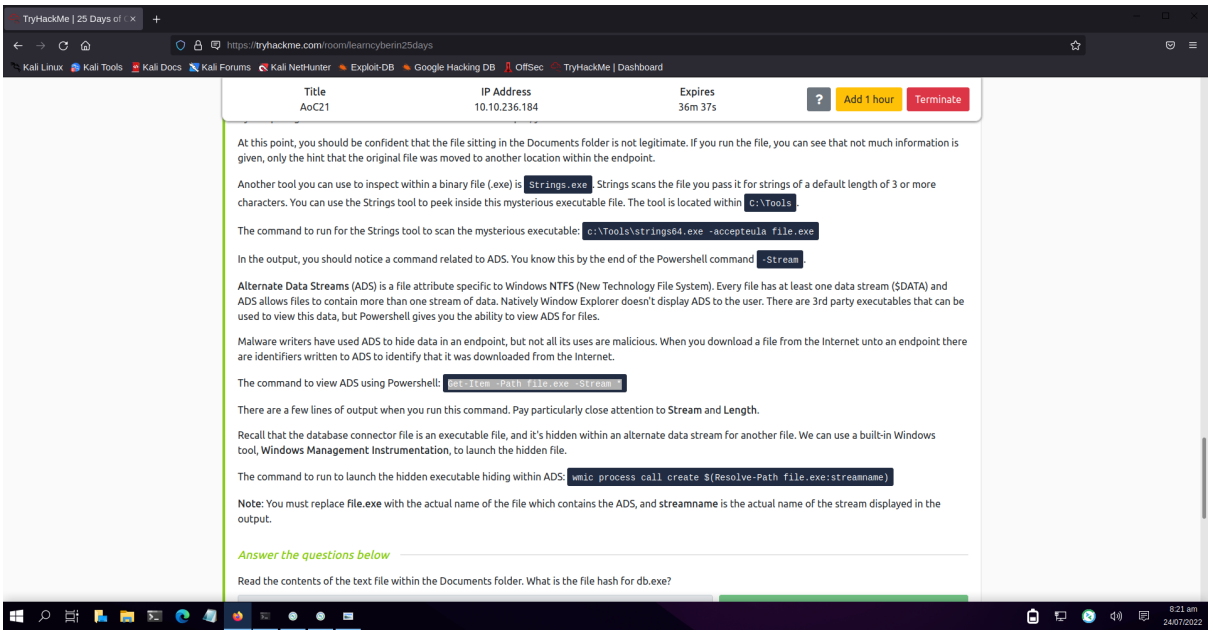
Finding the flag in deebee.exe using Strings





Question 5

Getting the powershell command to view ADS



TryHackMe | 25 Days of

https://tryhackme.com/room/learncyberin25days

Kali Linux | Kali Tools | Kali Docs | Kali Forums | Kali NetHunter | Exploit-DB | Google Hacking DB | OffSec | TryHackMe | Dashboard

Title	IP Address	Expires
AoC21	10.10.236.184	36m 37s

? Add 1 hour Terminate

At this point, you should be confident that the file sitting in the Documents folder is not legitimate. If you run the file, you can see that not much information is given, only the hint that the original file was moved to another location within the endpoint.

Another tool you can use to inspect within a binary file (.exe) is `Strings.exe`. Strings scans the file you pass it for strings of a default length of 3 or more characters. You can use the Strings tool to peek inside this mysterious executable file. The tool is located within `C:\Tools`.

The command to run for the Strings tool to scan the mysterious executable: `c:\Tools\strings64.exe -accepteula file.exe`

In the output, you should notice a command related to ADS. You know this by the end of the Powershell command `-Stream`.

Alternate Data Streams (ADS) is a file attribute specific to Windows **NTFS** (New Technology File System). Every file has at least one data stream ($DATA) and ADS allows files to contain more than one stream of data. Natively Window Explorer doesn't display ADS to the user. There are 3rd party executables that can be used to view this data, but Powershell gives you the ability to view ADS for files.

Malware writers have used ADS to hide data in an endpoint, but not all its uses are malicious. When you download a file from the Internet unto an endpoint there are identifiers written to ADS to identify that it was downloaded from the Internet.

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

There are a few lines of output when you run this command. Pay particularly close attention to **Stream** and **Length**.

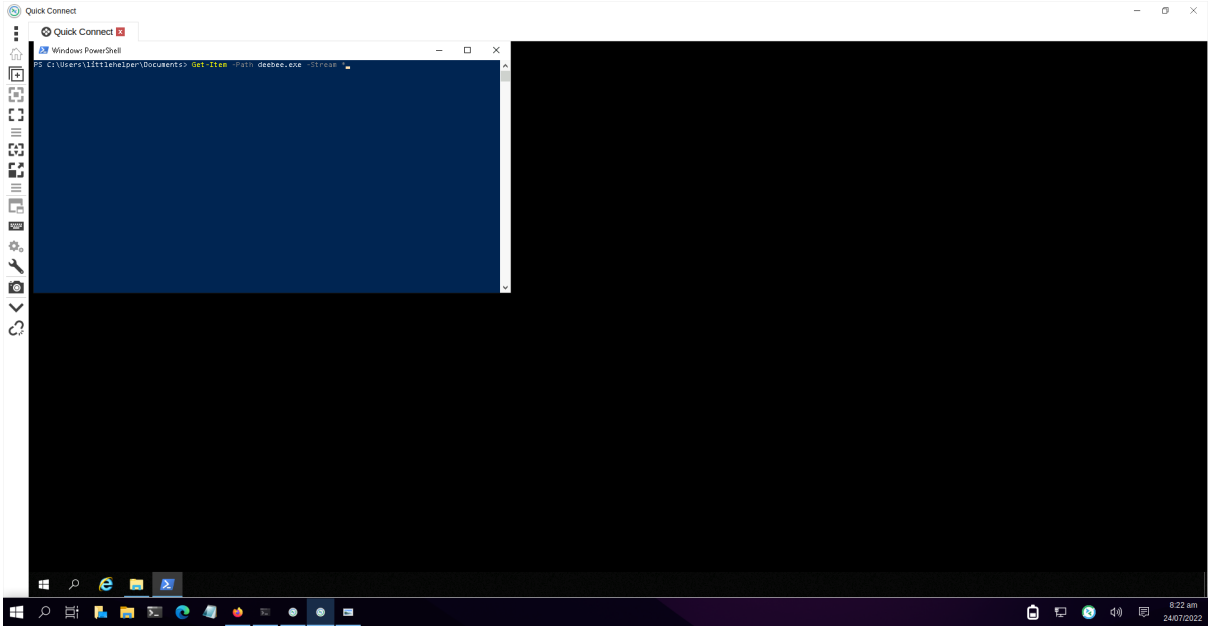
Recall that the database connector file is an executable file, and it's hidden within an alternate data stream for another file. We can use a built-in Windows tool, **Windows Management Instrumentation**, to launch the hidden file.

The command to run to launch the hidden executable hiding within ADS: `wmic process call create $(Resolve-Path file.exe:streamname)`

Note: You must replace **file.exe** with the actual name of the file which contains the ADS, and **streamname** is the actual name of the stream displayed in the output.

Answer the questions below

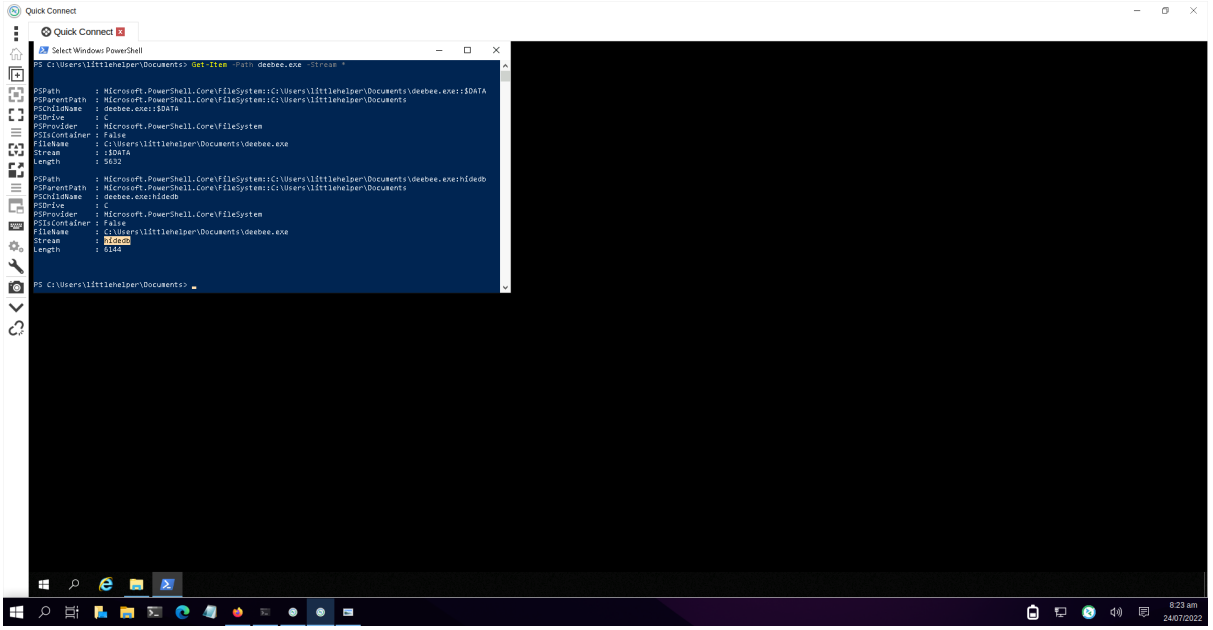
Read the contents of the text file within the Documents folder. What is the file hash for db.exe?



Quick Connect

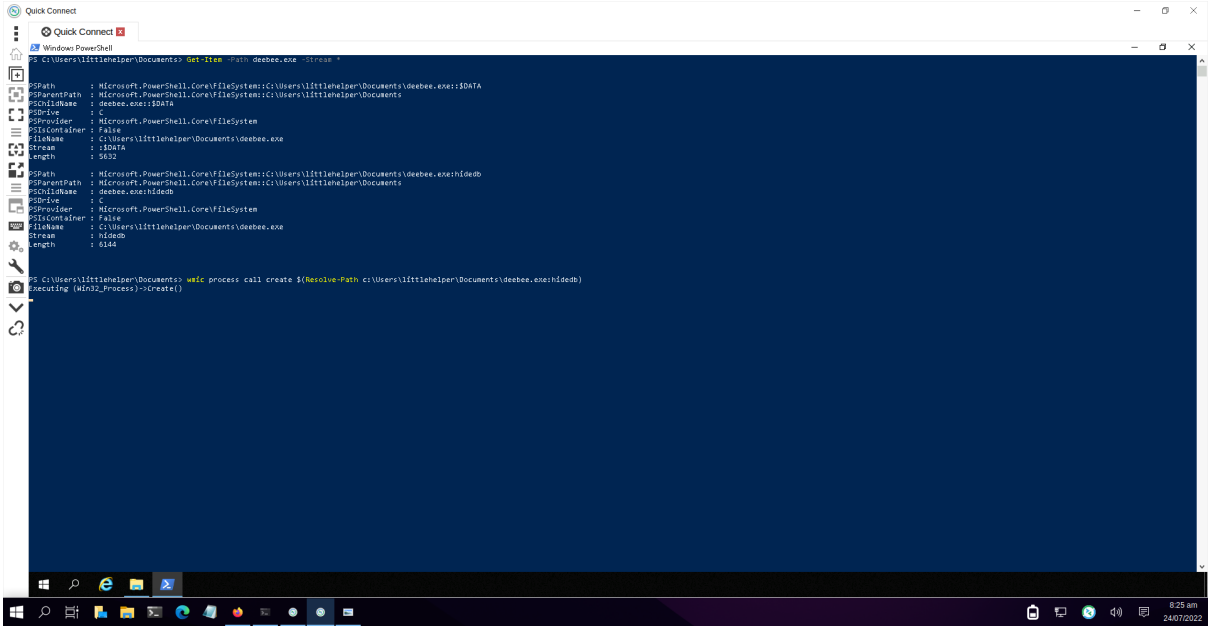
Windows PowerShell

```
PS C:\Users\littlehelper\Documents> Get-Item -Path deebee.exe -Stream *
```

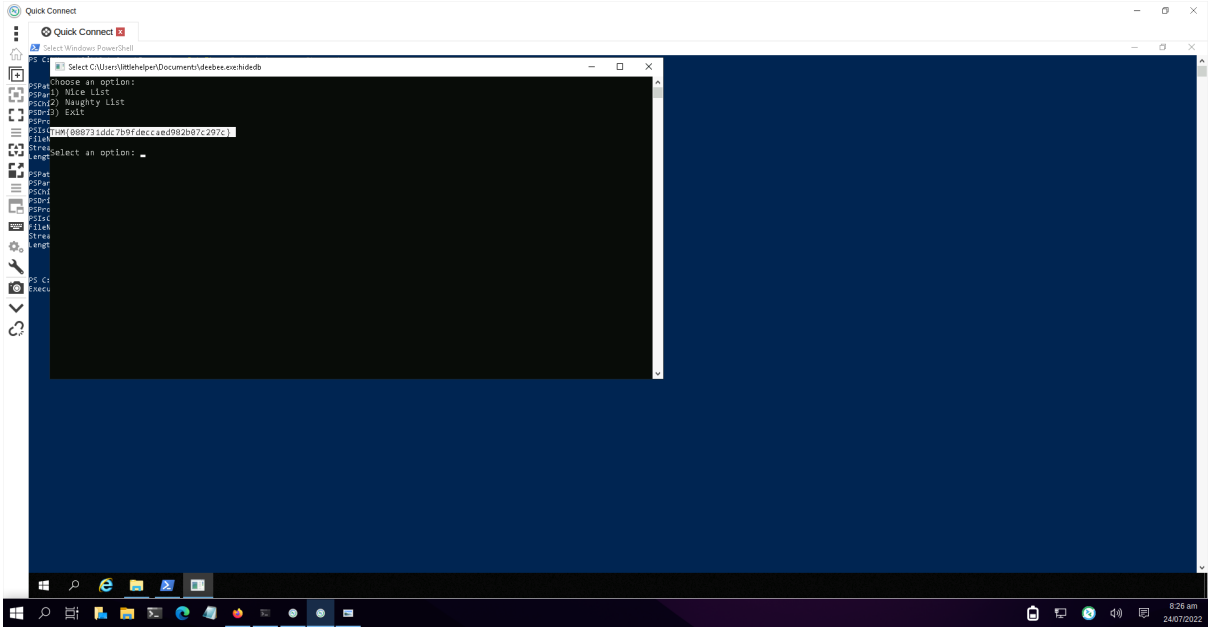


Question 6

Launching the hidden executable hiding within ADS

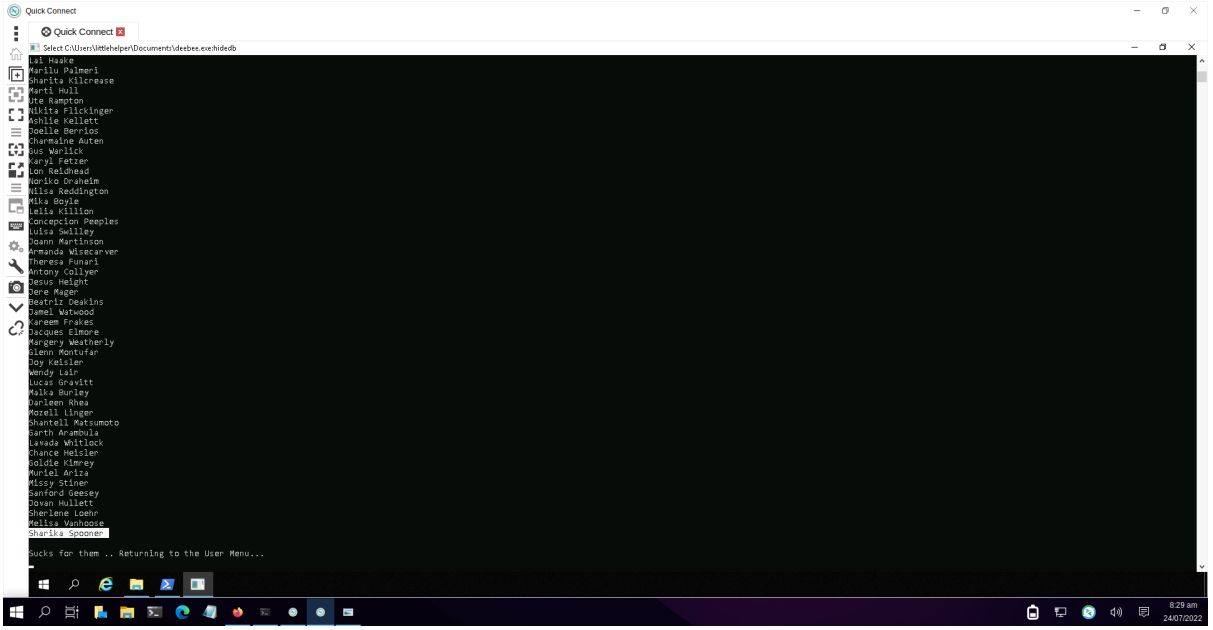


Finding the flag when database connector file is executed



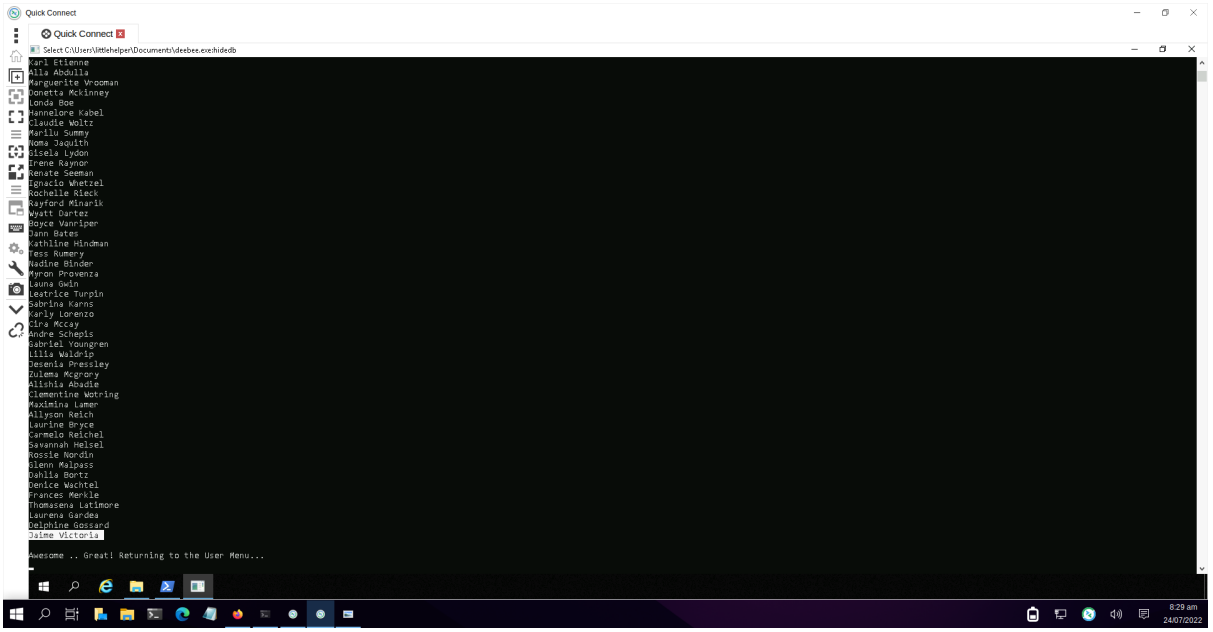
Question 7

Finding Sharika Spooner in naughty list



Question 8

Finding Jaime Victoria in nice list



Thought process/Methodology

Firstly, we run the remmina remote desktop using the credentials provided in the dossier. After that, we open the .txt file in the Documents folder to obtain the file hash of db.exe. Then, we run *Get-FileHash -Algorithm MD5 deebee.exe* command to obtain the MD5 file hash of deebee.exe. We also run *Get-FileHash -Algorithm SHA256 deebee.exe* to obtain the SHA256 file hash of deebee.exe. Then, we use *strings64.exe* in C:/Tools to inspect deebee.exe so that we can find the flag in it. We then use command *Get-Item -Path deebee.exe -Stream ** to view the ADS using powershell. After that, we found the flag when the database connector file is loaded. Lastly, we find out whether Sharika Spooner and Jaime Victoria in naughty list or nice list.

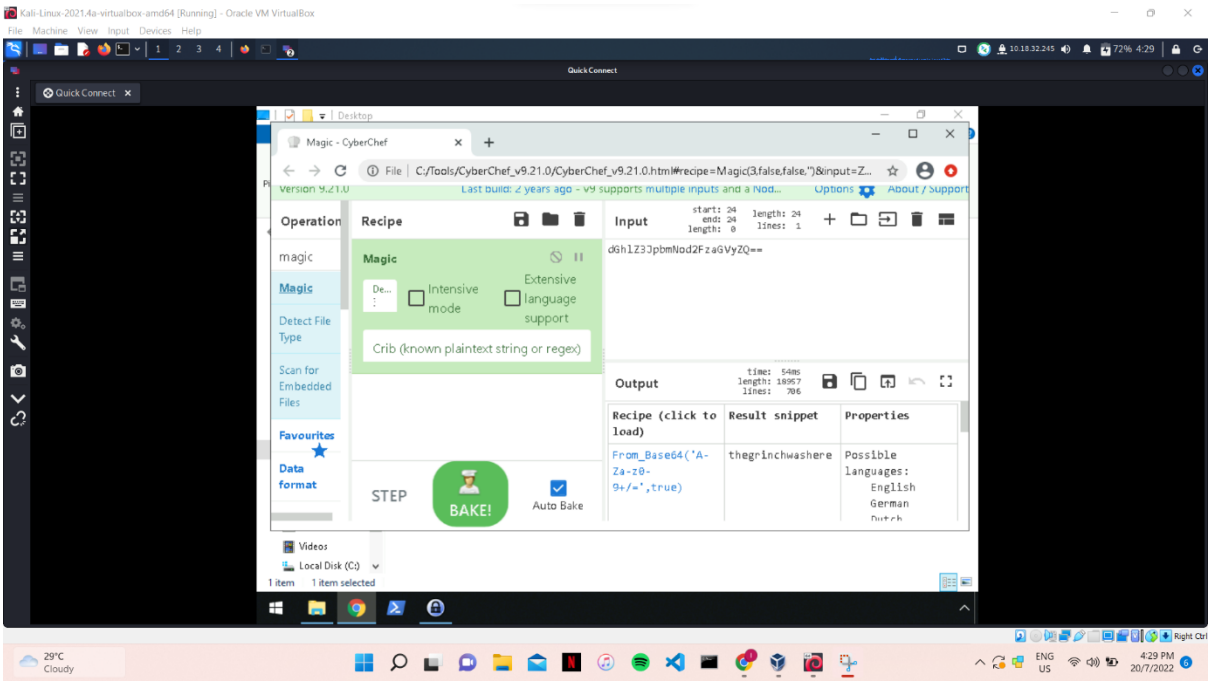
Day 22 - Blue Teaming - Elf McEager becomes CyberElf

Tools used: Kali Linux, Firefox, Remmina, CyberChef

Solution:

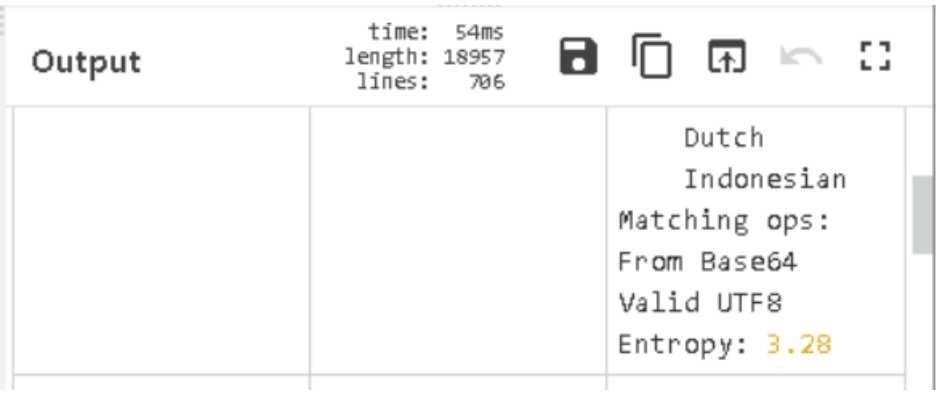
Question 1

Connect to the remote machine. Copy the name of the folder and paste it in cyberchef's input box. Use **'magic'** recipe to decode the folder name and gain the password.



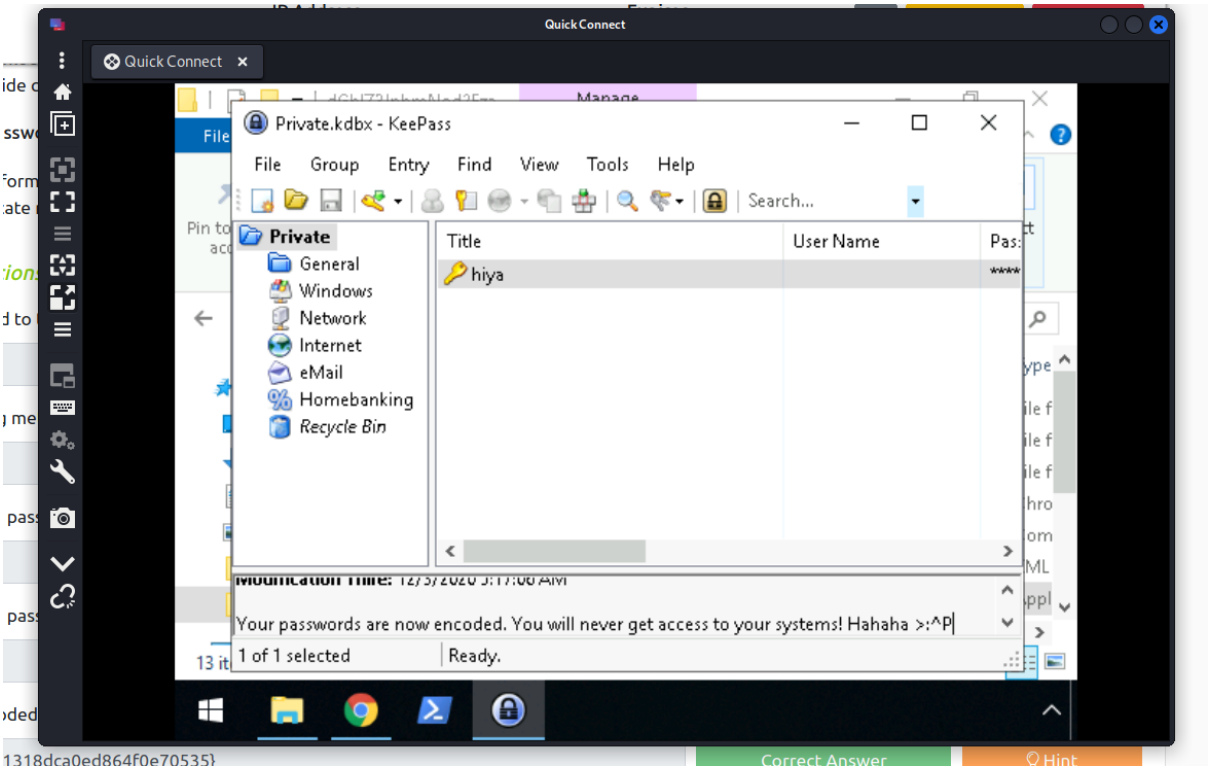
Question 2

Look under 'properties' section in the output box and find 'matching ops' to obtain the answer.



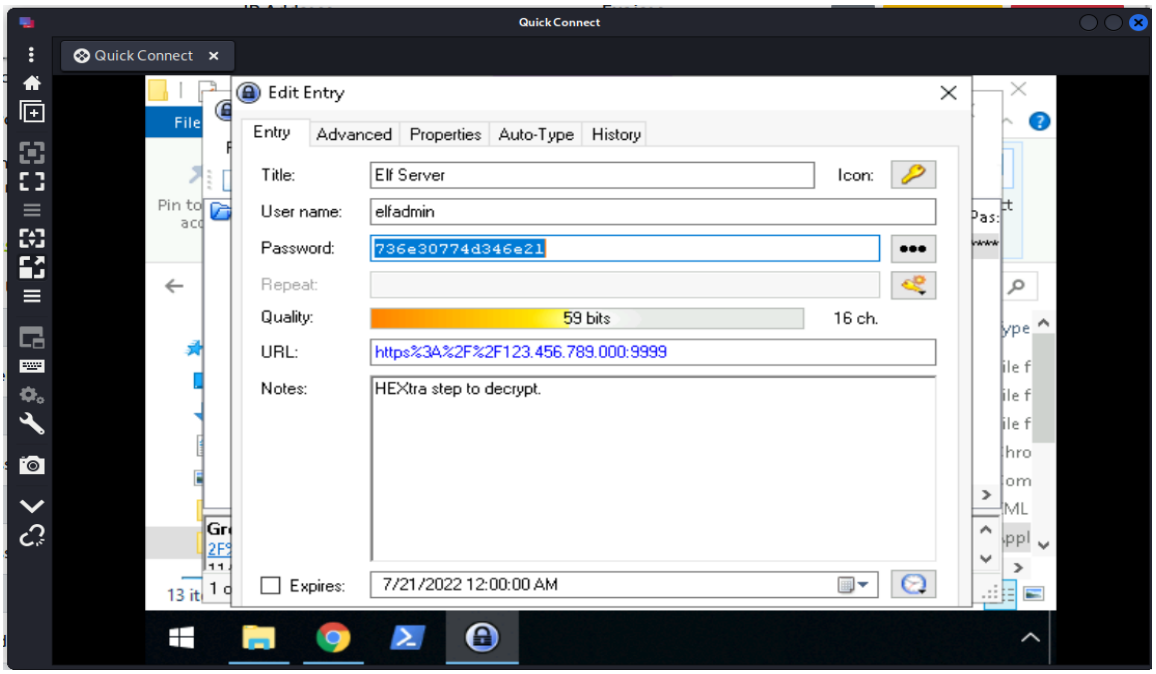
Question 3

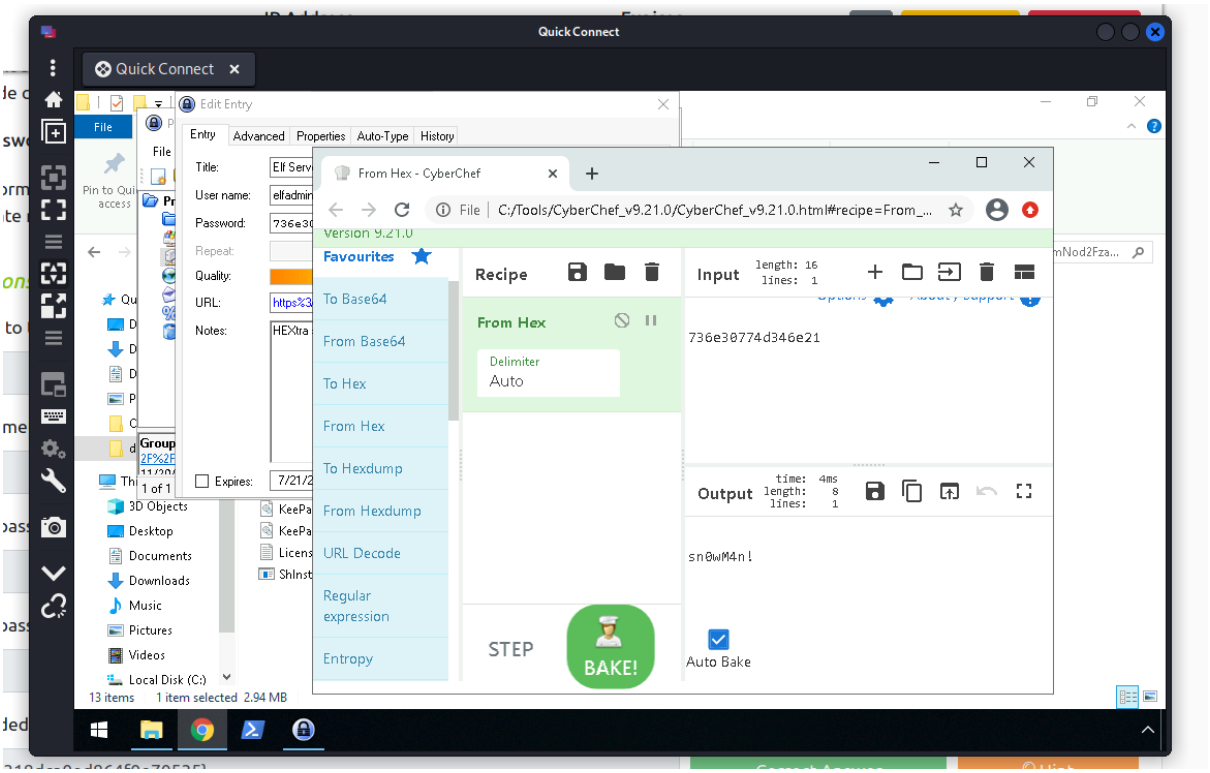
Log into the KeePass database using the obtained password. Click once on ‘hiya’ to view the notes.



Question 4

Search for the Elf Server. Click twice to view and edit the entry. Copy the password and paste it in the cyberchef. Use **‘from hex’** recipe to decode the value.



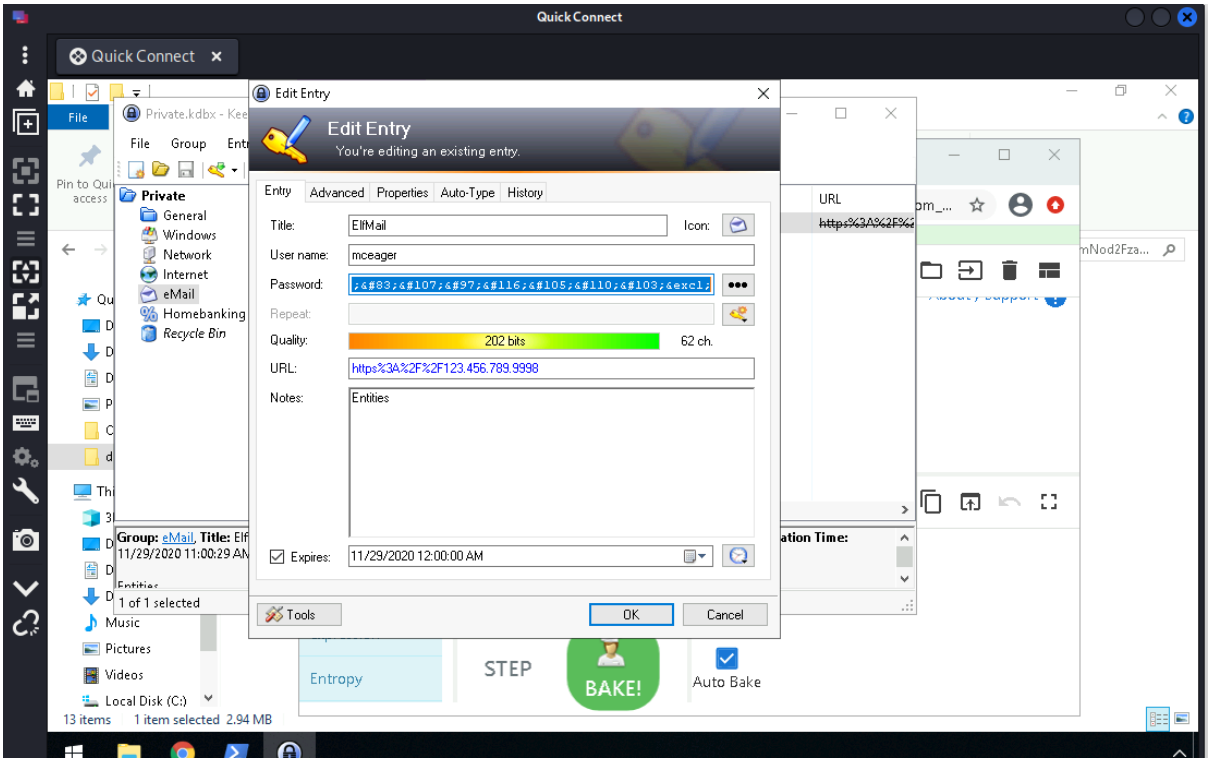

Quick Connect
Edit Entry
Entry
Advanced
Properties
Auto-Type
History
Title:
User name:
Password:
Repeat:
Quality:
URL:
Notes:
Expires:
From Hex - CyberChef
File | C:/Tools/CyberChef_v9.21.0/CyberChef_v9.21.0.html#recipe=From_...
Version 9.21.0
Favourites
To Base64
From Base64
To Hex
From Hex
To Hexdump
From Hexdump
URL Decode
Regular expression
Entropy
Recipe
From Hex
Delimiter
Auto
STEP
BAKE!
Input
length: 16
lines: 1
736e30774d346e21
Output
time: 4ms
length: 8
lines: 1
sn0wM4n!
Auto Bake

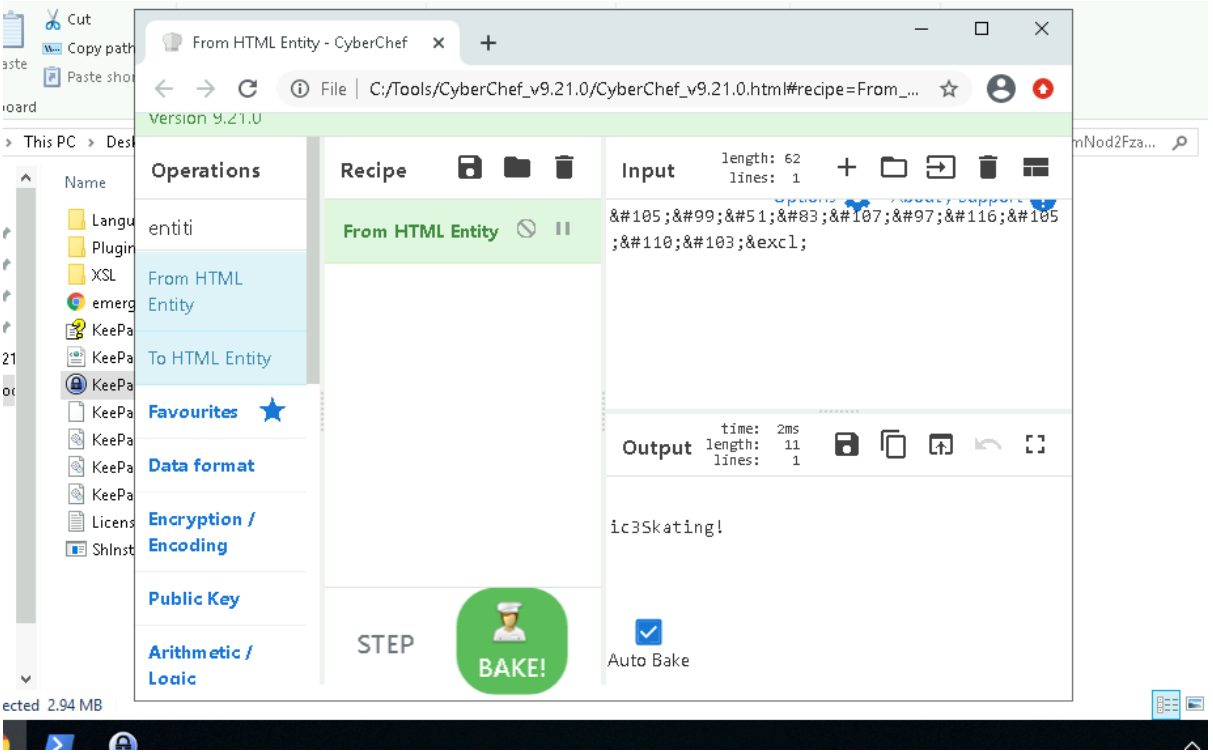
Question 5

Favourites
To Base64
From Base64
To Hex
From Hex
Recipe
From Hex
Delimiter
Auto
Input
length: 16
lines: 1
736e30774d346e21

Question 6

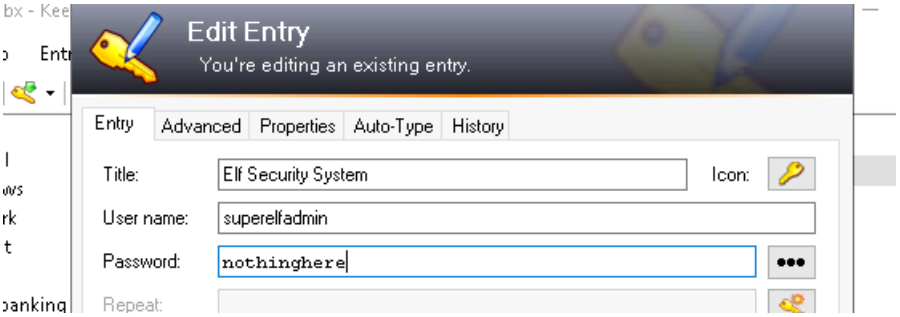
Look for the ElfMail. Click twice to view and edit the entry. Copy the password and paste it in the cyberchef. Use **'from HTML entity'** recipe to decode the value.





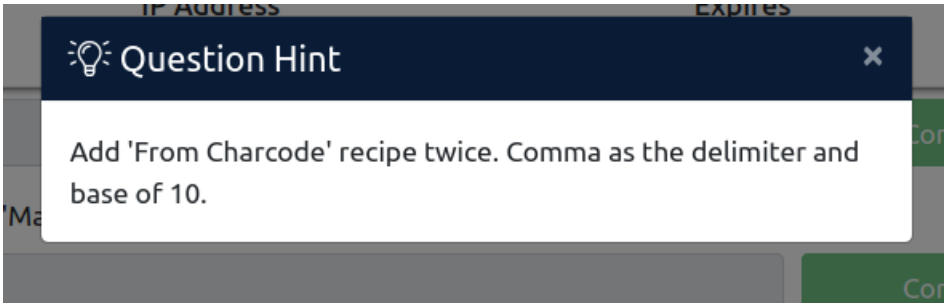
Question 7

Search for the Elf Security System. Click twice to view and edit the entry.

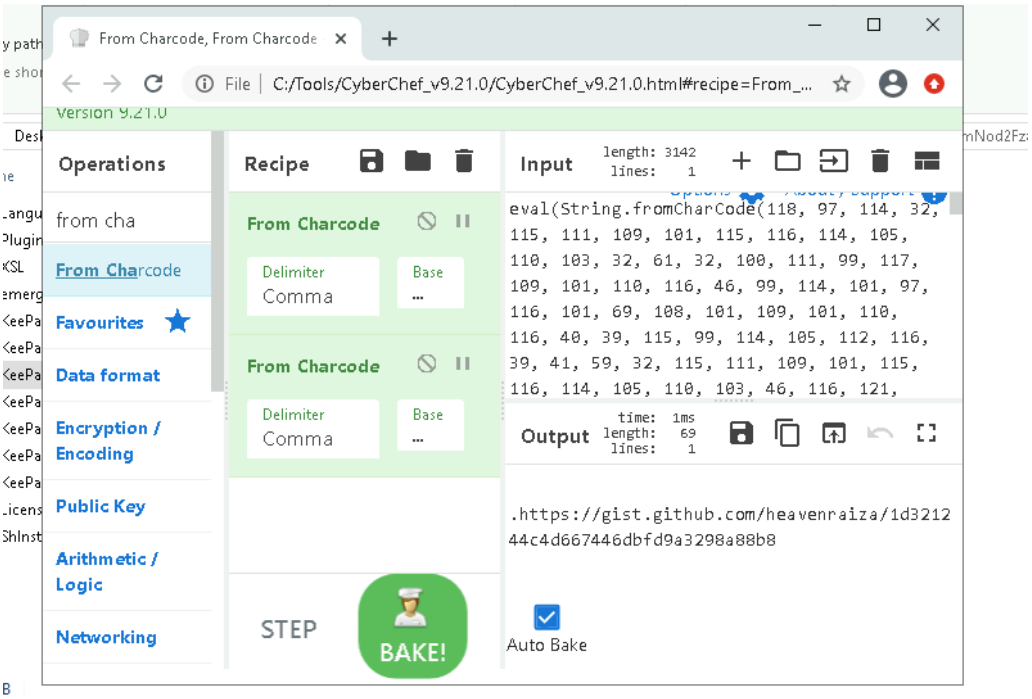


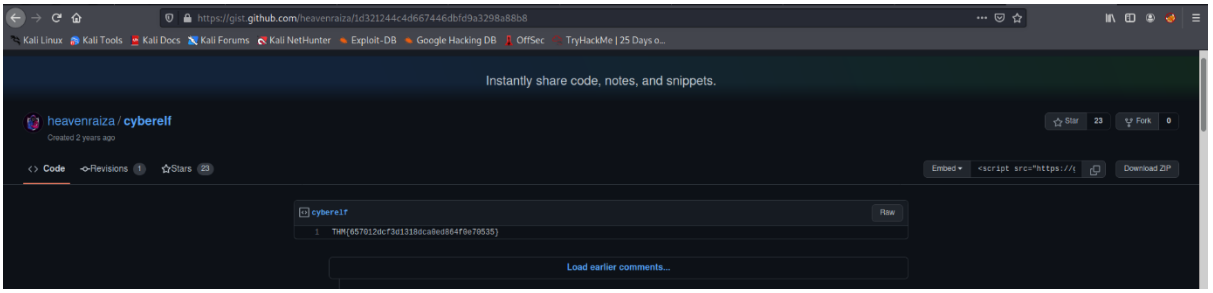
Question 8

Copy the value from Elf Security System notes and paste it in cyberchef. Use the hint given to decode the value.



Once decoded, browse to the url obtained to get the flag.





Thought process/methodology:

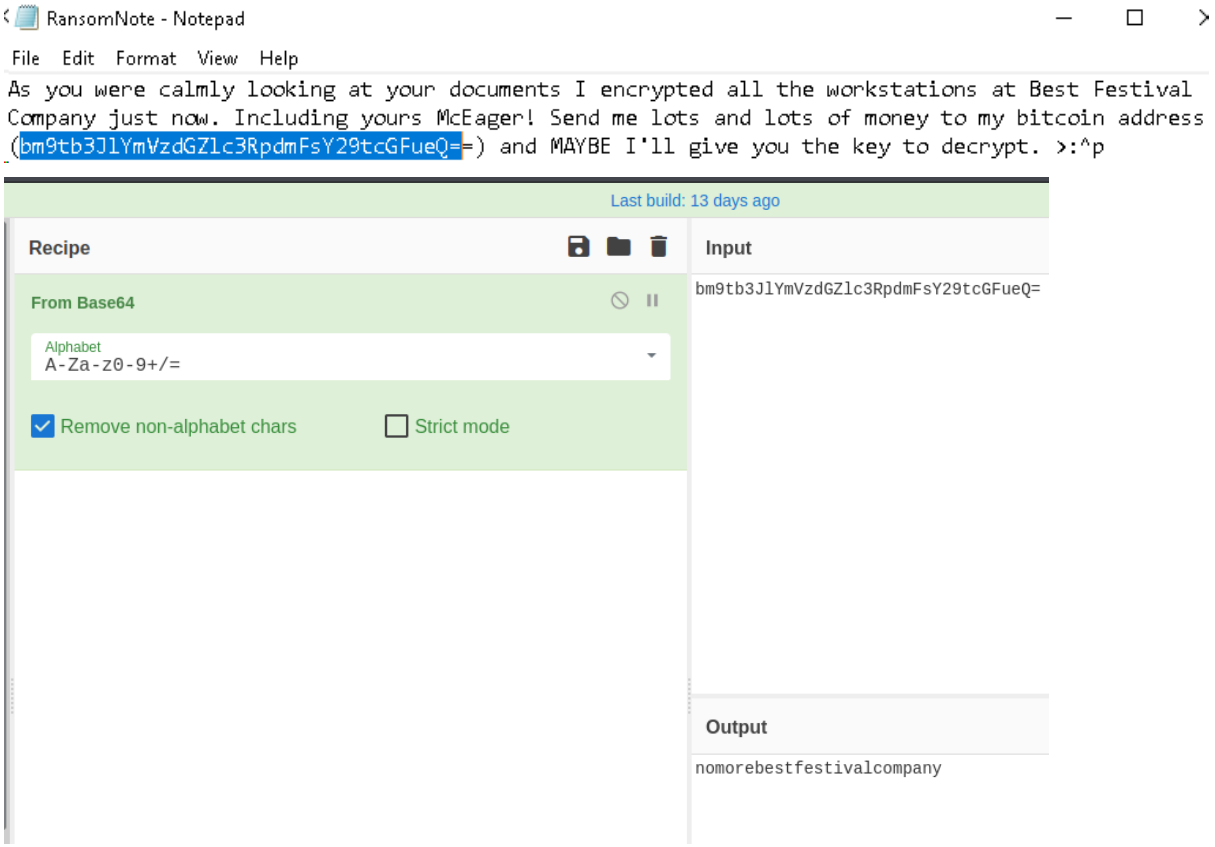
Once the machine deployed, we connect to the remote machine by using Remmina. Logging in as administrator, we found a strange-looking folder on the desktop. We then copied its name and paste it in the CyberChef's input box before decoding it using **'magic'** recipe. Once decoded, it displayed an output in the output box. Under 'result snippet' column, we successfully obtained the password to the KeePass database. After logging in, we found an entry named 'hiya'. We then clicked on it to view the notes written. Next, we searched for 'Elf Server' and found it in the network menu. By clicking on it twice, we managed to view its 'edit entry' and gained the encoded password. Once again, we copied it and paste in CyberChef's input box. Following the notes written, we used **'From Hex'** recipe to decode the value and yes! We managed to get the password. After that, we continued to search for the next entry which was ElfMail. We did the same as for Elf Server, but with different recipe. This time, we used **'from HTML entity'** recipe. Next, for the last entry which was Elf Security System, we also did the same; clicking twice to view its entry and obtained the username and password to answer question 7. Lastly, for question 8, we needed to decode the value from the notes box of Elf Security System. Repeating the same action, we copied and paste it in the input section. By using the hint given, we started to decode the value. We used **'from charcode'** recipe twice to decode it. Once it finished, we were given a URL. We then browsed to the URL, and successfully getting a flag.

Day 23 - Blue Teaming - The Grinch strikes again!

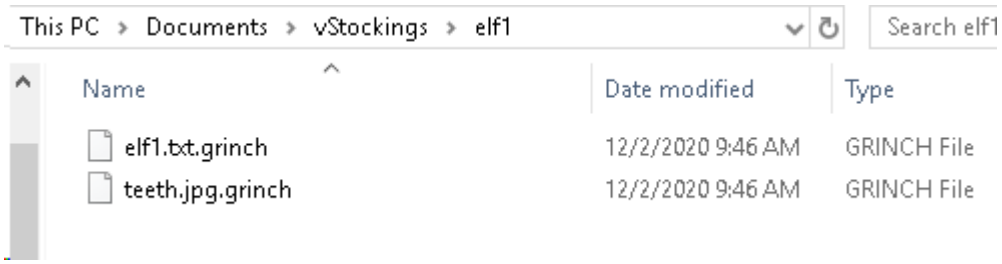
Tools Used: *Remmina, File Explorer, Task Scheduler, Disk Management, Command Prompt, Volume Shadow Copy Service(VSS)*

Walkthrough:

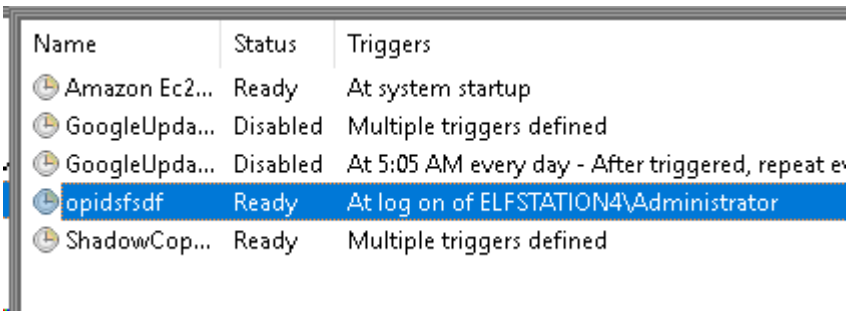
Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?



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

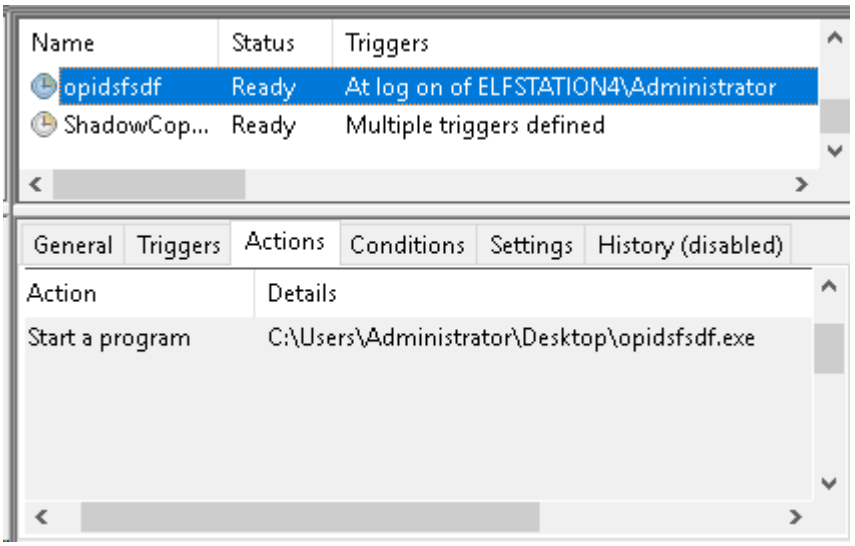


What is the name of the suspicious scheduled task?



Name	Status	Triggers
Amazon Ec2...	Ready	At system startup
GoogleUpda...	Disabled	Multiple triggers defined
GoogleUpda...	Disabled	At 5:05 AM every day - After triggered, repeat e
opidsfsdf	Ready	At log on of ELFSTATION4\Administrator
ShadowCop...	Ready	Multiple triggers defined

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

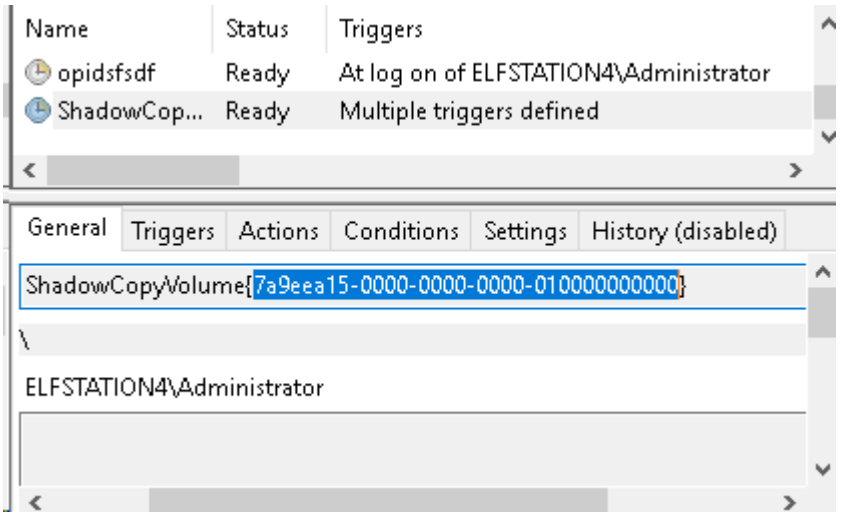


Name	Status	Triggers
opidsfsdf	Ready	At log on of ELFSTATION4\Administrator
ShadowCop...	Ready	Multiple triggers defined

General | Triggers | Actions | Conditions | Settings | History (disabled)

Action	Details
Start a program	C:\Users\Administrator\Desktop\opidsfsdf.exe

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



Name	Status	Triggers
opidsfsdf	Ready	At log on of ELFSTATION4\Administrator
ShadowCop...	Ready	Multiple triggers defined

General | Triggers | Actions | Conditions | Settings | History (disabled)

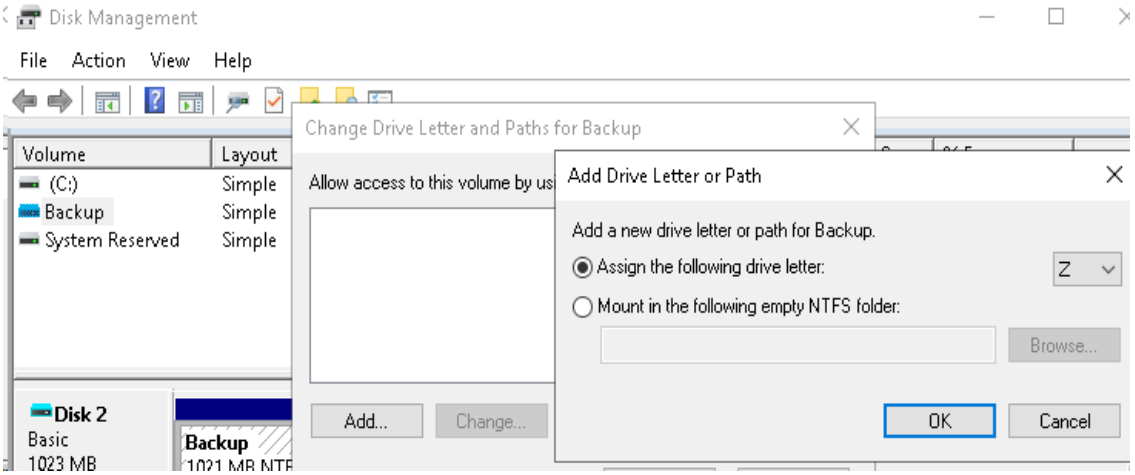
ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000}

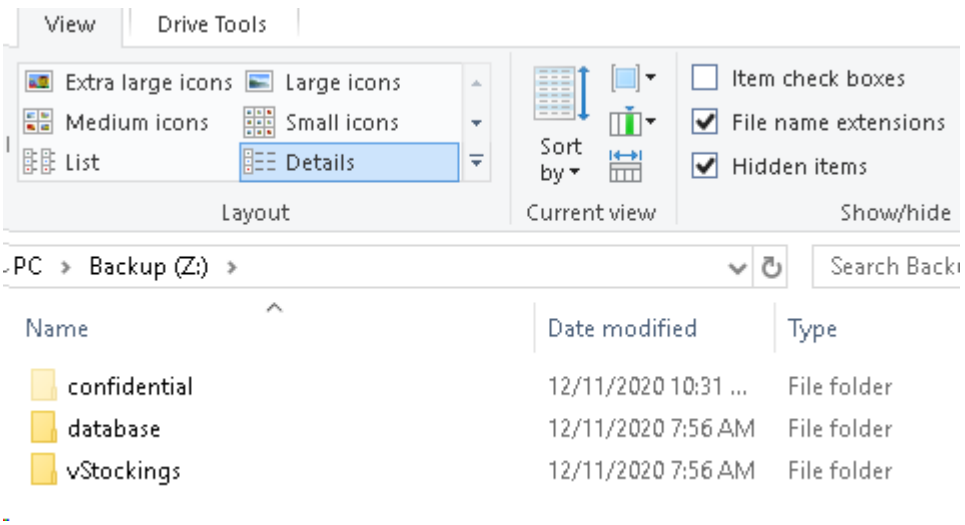
\

ELFSTATION4\Administrator

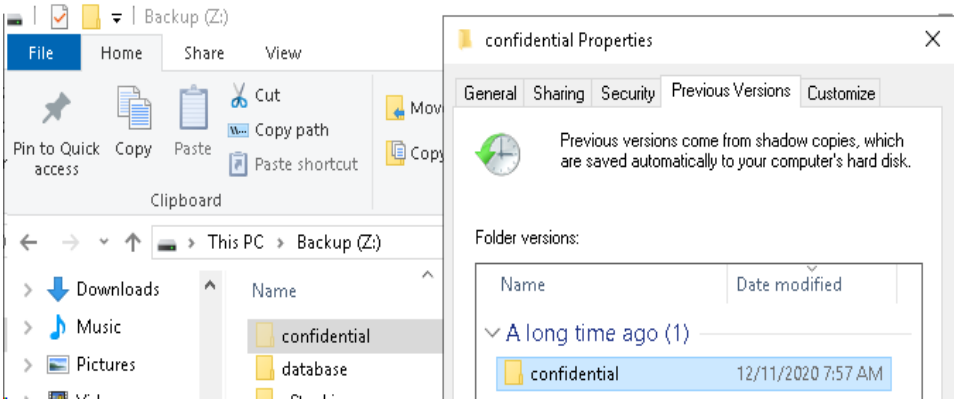
```
C:\Users\Administrator>vssadmin list volumes
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line too
(C) Copyright 2001-2013 Microsoft Corp.

Volume path: \\?\Volume{f801713f-0000-0000-0000-100000000000}\
    Volume name: \\?\Volume{f801713f-0000-0000-0000-100000000000}\
Volume path: \\?\Volume{7a9eea15-0000-0000-0000-010000000000}\
    Volume name: \\?\Volume{7a9eea15-0000-0000-0000-010000000000}\
Volume path: C:\
    Volume name: \\?\Volume{f801713f-0000-0000-0000-602200000000}\
```

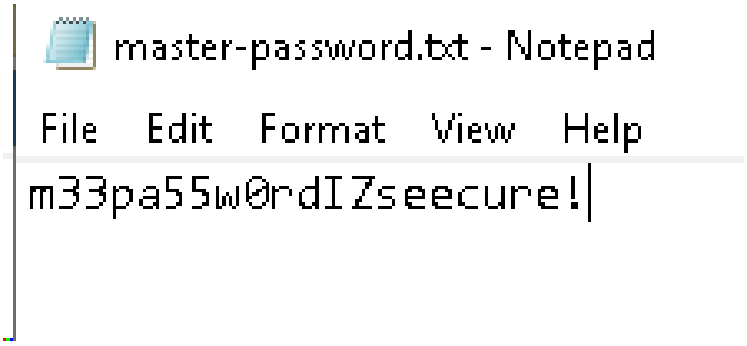
Assign the hidden partition a letter. What is the name of the hidden folder?





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?





<u>Thought Process/Methodology</u>:

When we first connect to the machine's RDP, we open the note/text file on the desktop. Where we find a note from the grinch and an Encrypted text on the note then went to cyberchef to decrypt the text from Base64. We then went to inspect the other files in File Explorer, in the Documents tab we find multiple files and in the vStocking file, we found that the .grinch extensions were in each elves folder. Then we went to open the Task Scheduler app, where we found multiple tasks and found a suspiciously named task where we inspect its properties in the actions tab and file path. In the command prompt, we list out all volumes and get the ShadowCopy volume ID. Then in Disk Management, we assigned a letter to the Backup drive and went back to File Explorer and enabled it to show Hidden Items where we find the hidden folder name. We then inspect the properties of the hidden folder and head over to the Previous Versions tab and open the older version of the folder and see a note/text file where when we open it we find the master password.

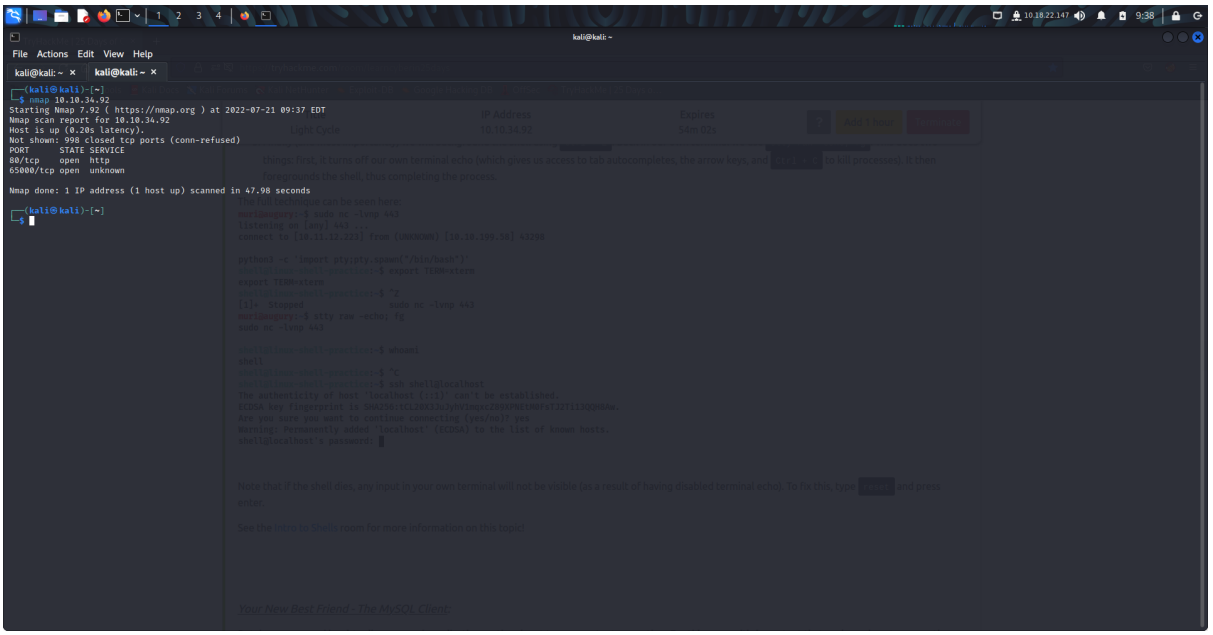
Day 24 - Final Challenge - The Trial Before Christmas

Tools used: terminal, mozilla firefox, nmap, kali linux, gobuster, burpsuite, netcat, mysql, crackstation.net, lxd

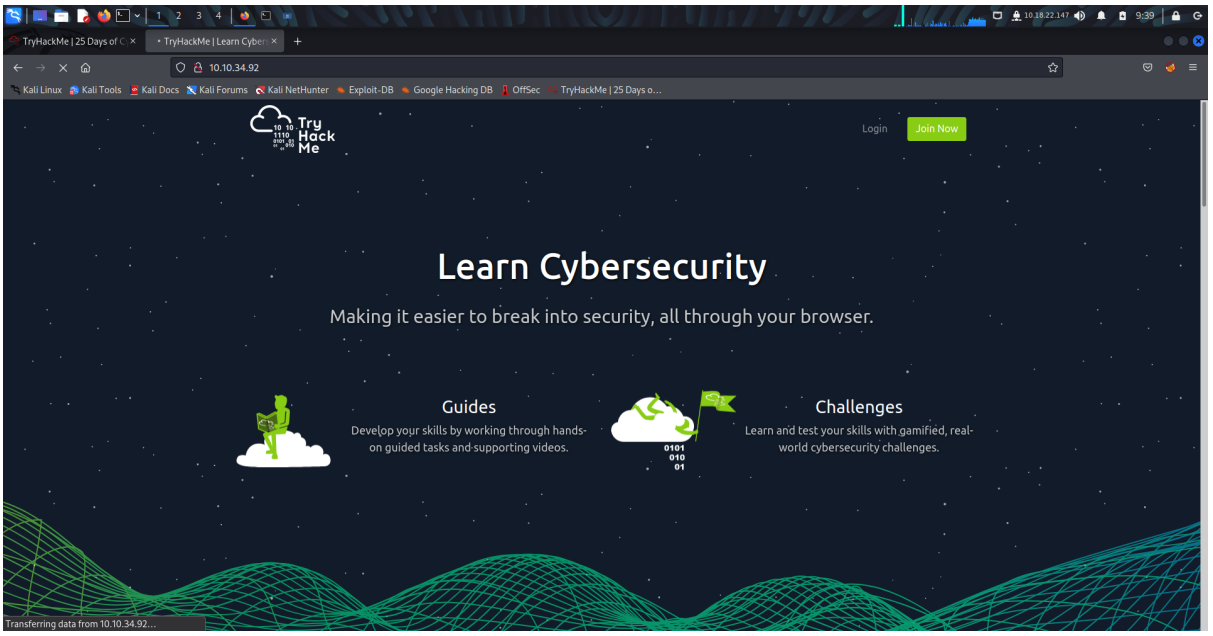
Solutions/Walkthrough

<u>Question 1</u>

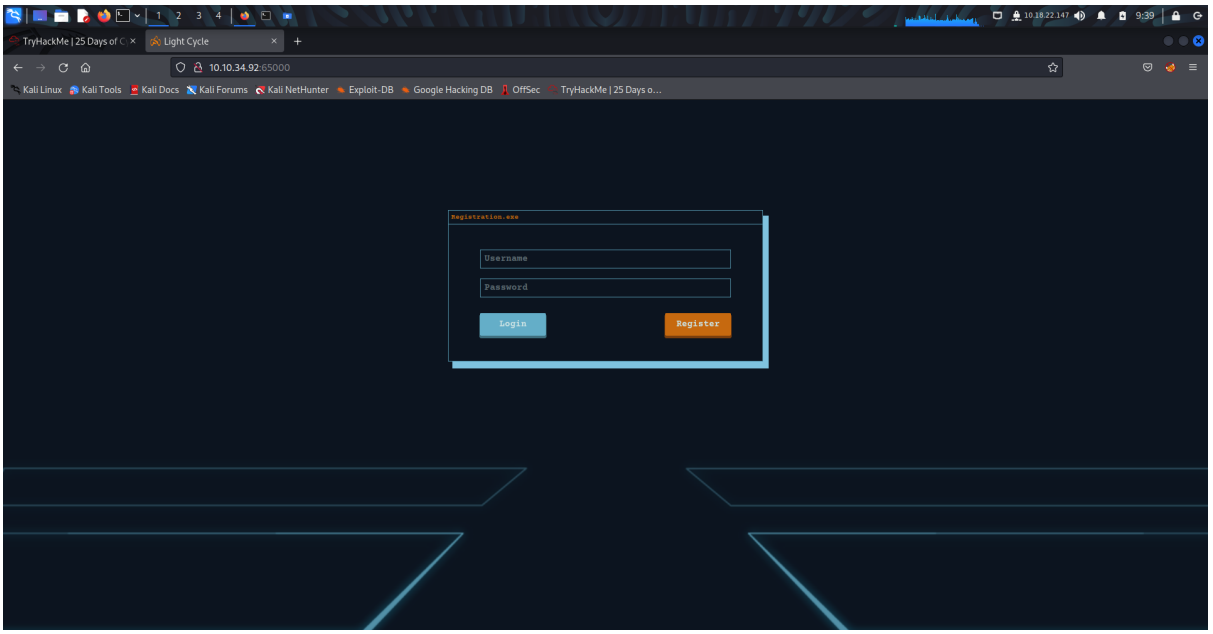
Using nmap to scan the open port of the website



The website when port 80 is used

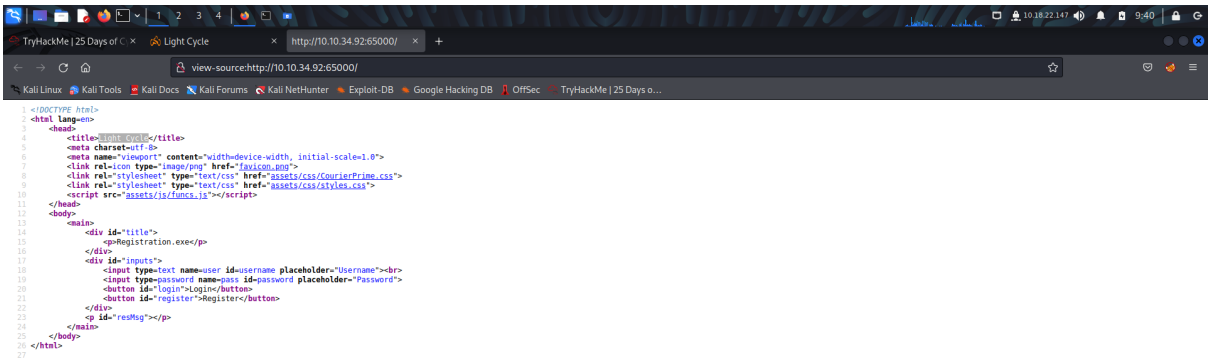


The website when port 65000 is used



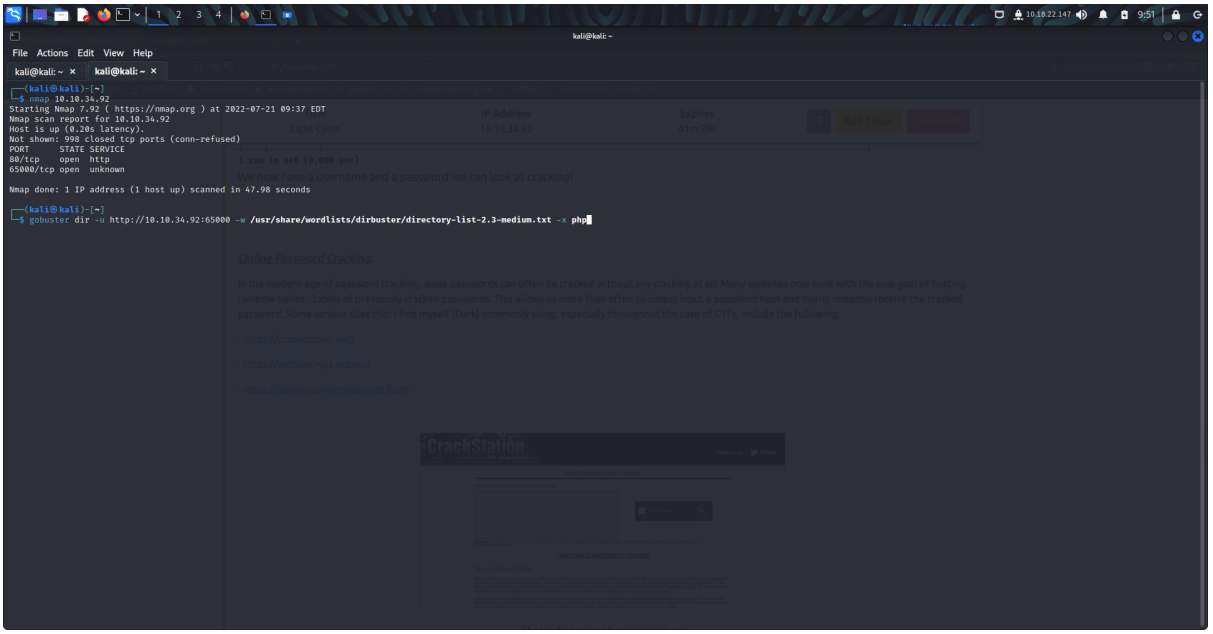
Question 2

Viewing page source of the website to retrieve the website title



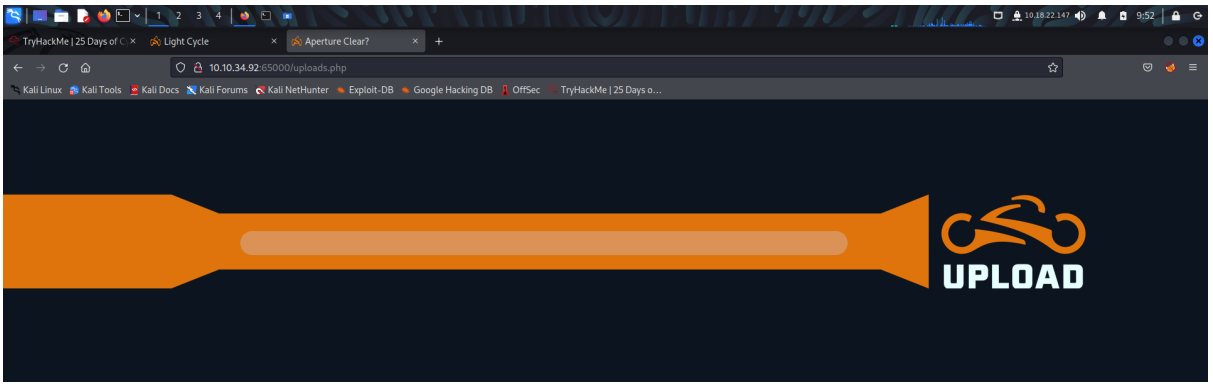
Question 3

Running gobuster to search the php filetype and to search for the directory to store the uploaded files



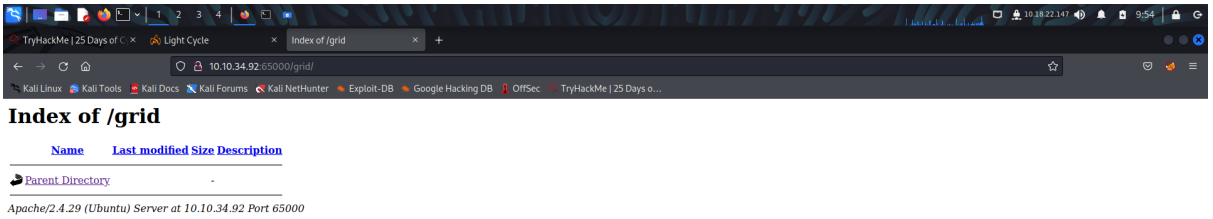
The result of the gobuster scan

The name of the php file is uploads.php



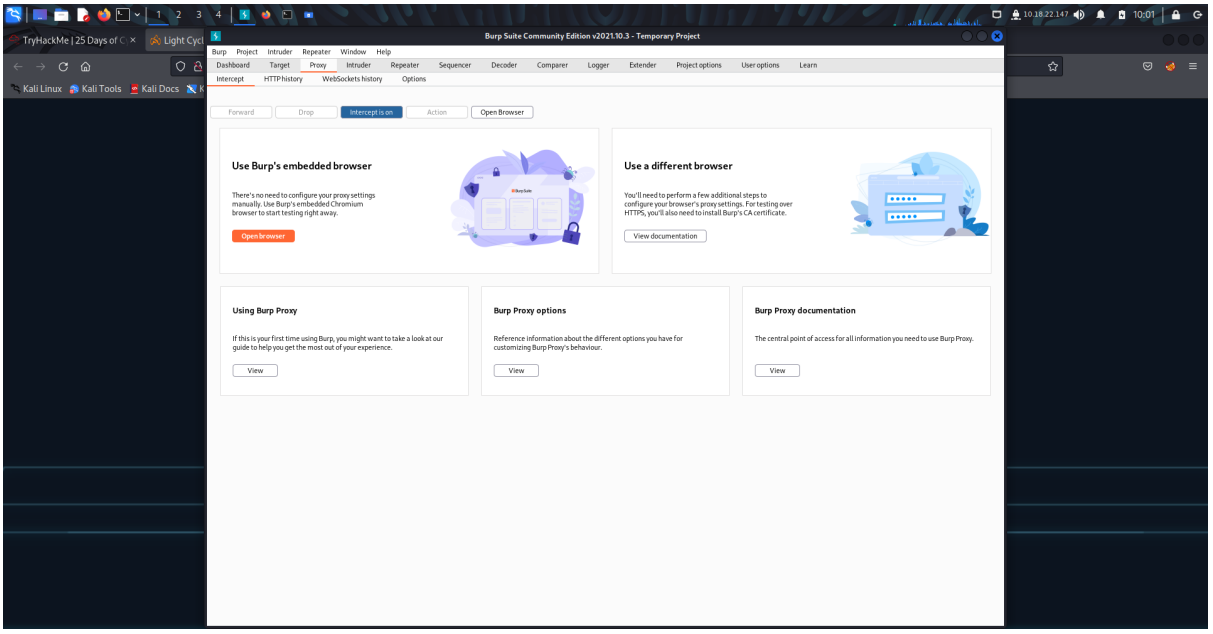
Question 4

The name of dir to store file uploads is /grid

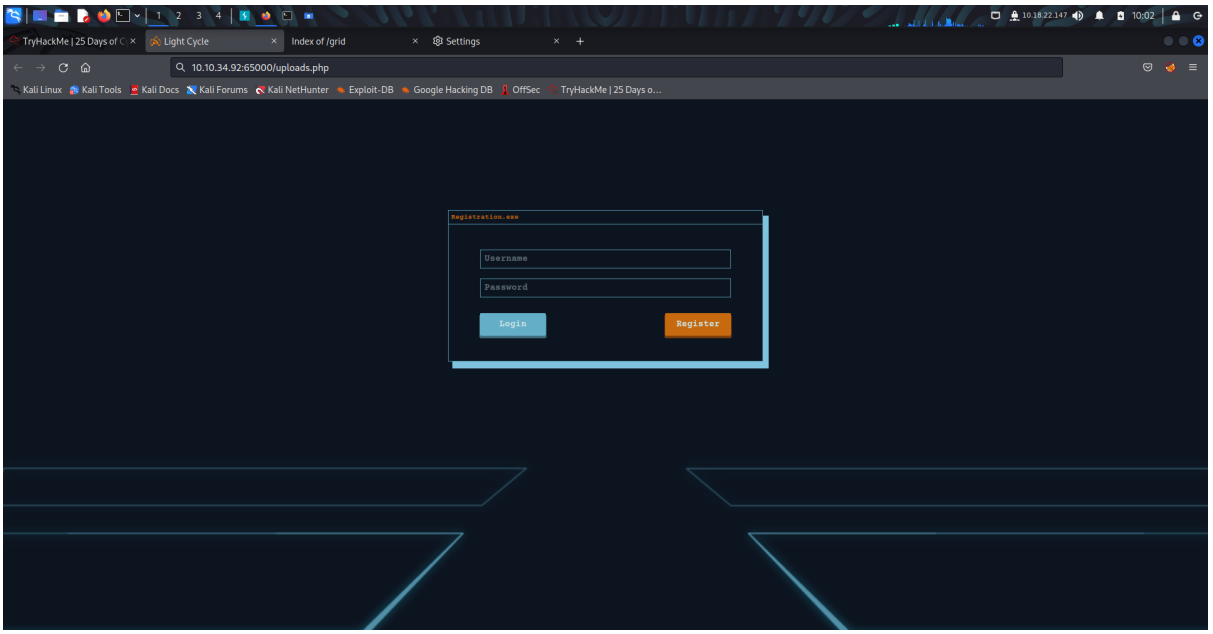


Question 5

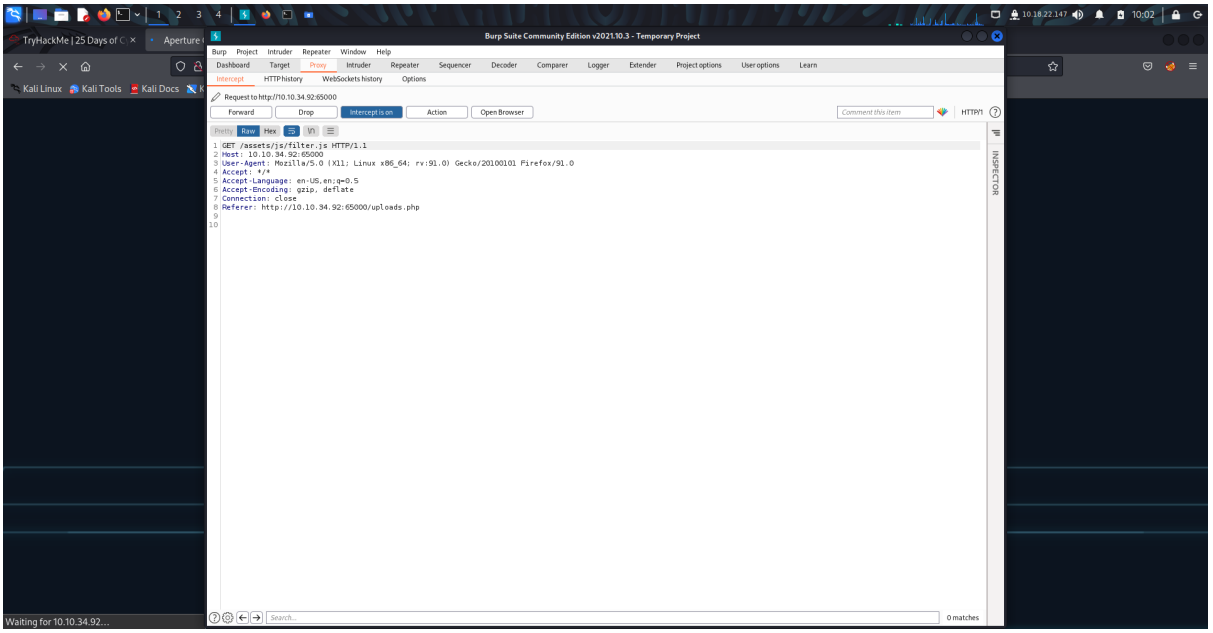
Setting up burpsuite to intercept the traffic of the website.



Redirecting to *10.10.34.92:65000/uploads.php*

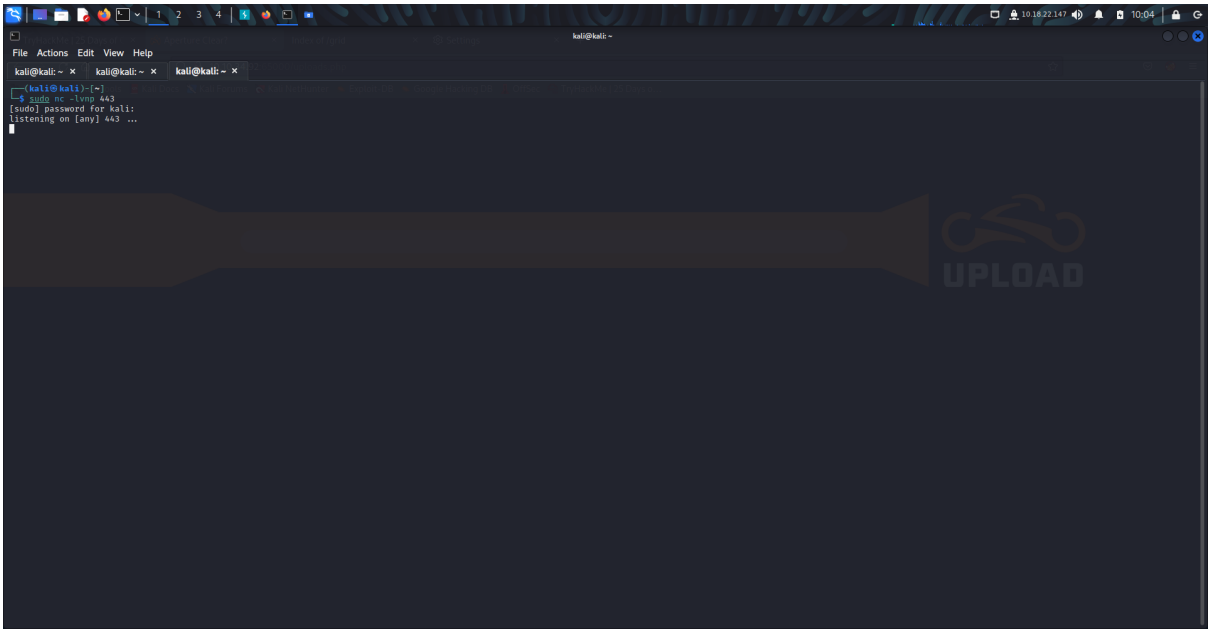


Dropping filter.js

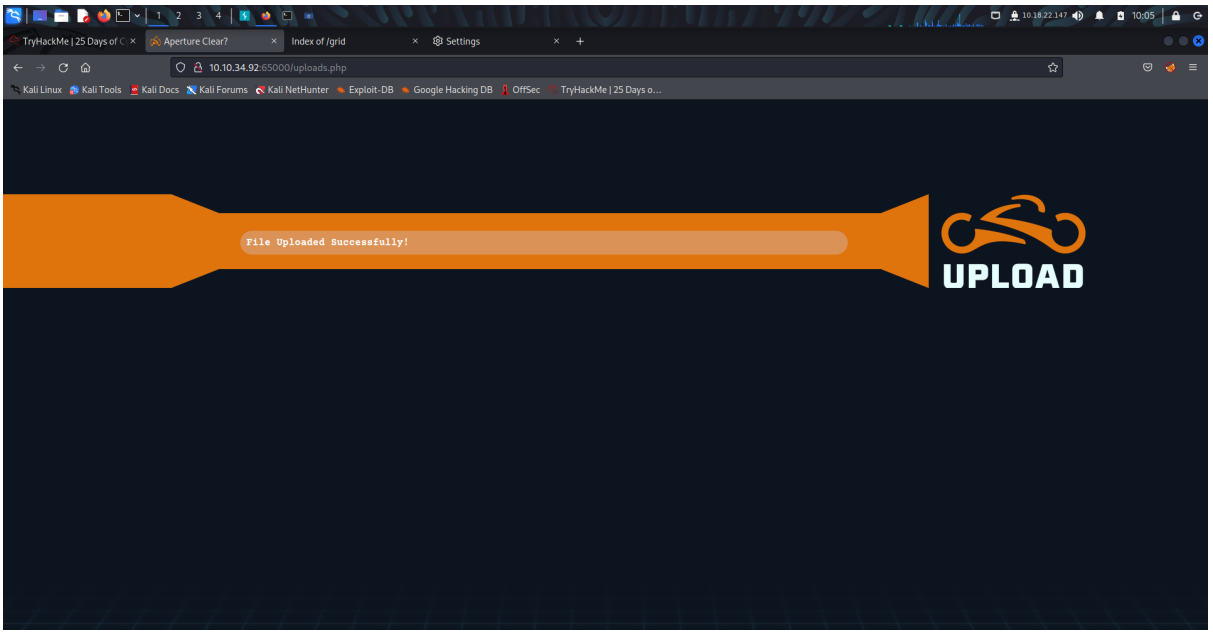


Editing the IP address and port number in reverse shell.php file

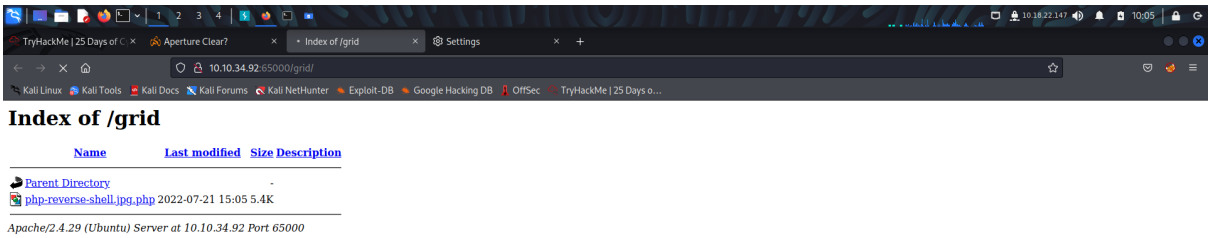
Activating netcat listener on port *443*



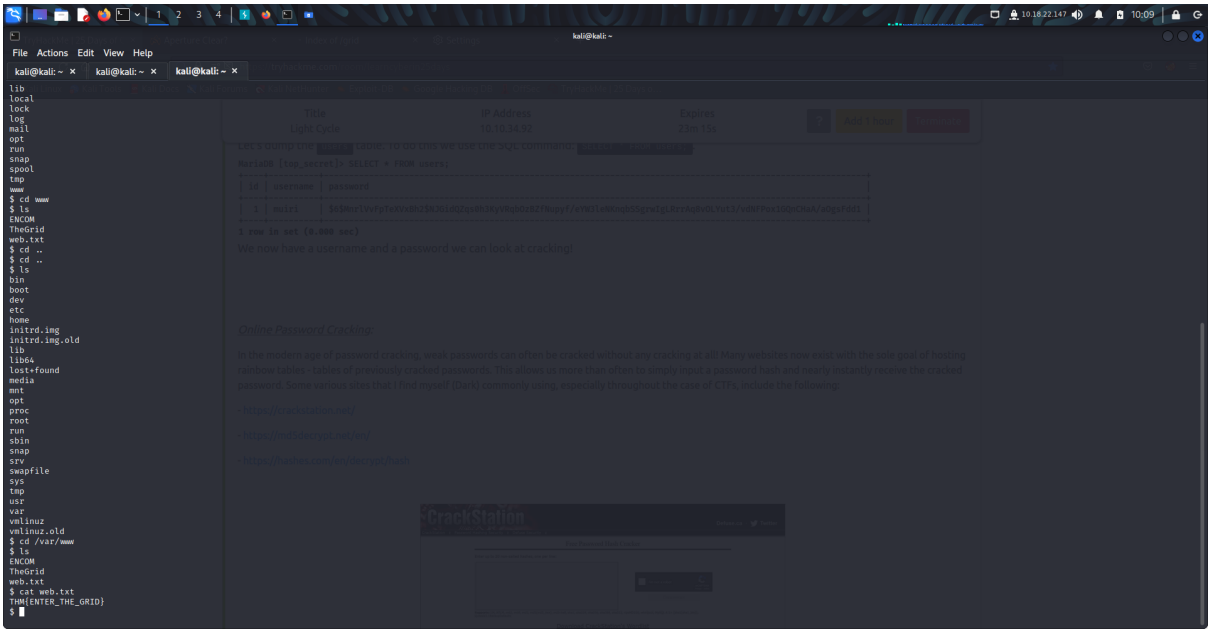
Redirected to *10.10.34.92:65000/uploads.php*



Uploaded the reverse shell into the website

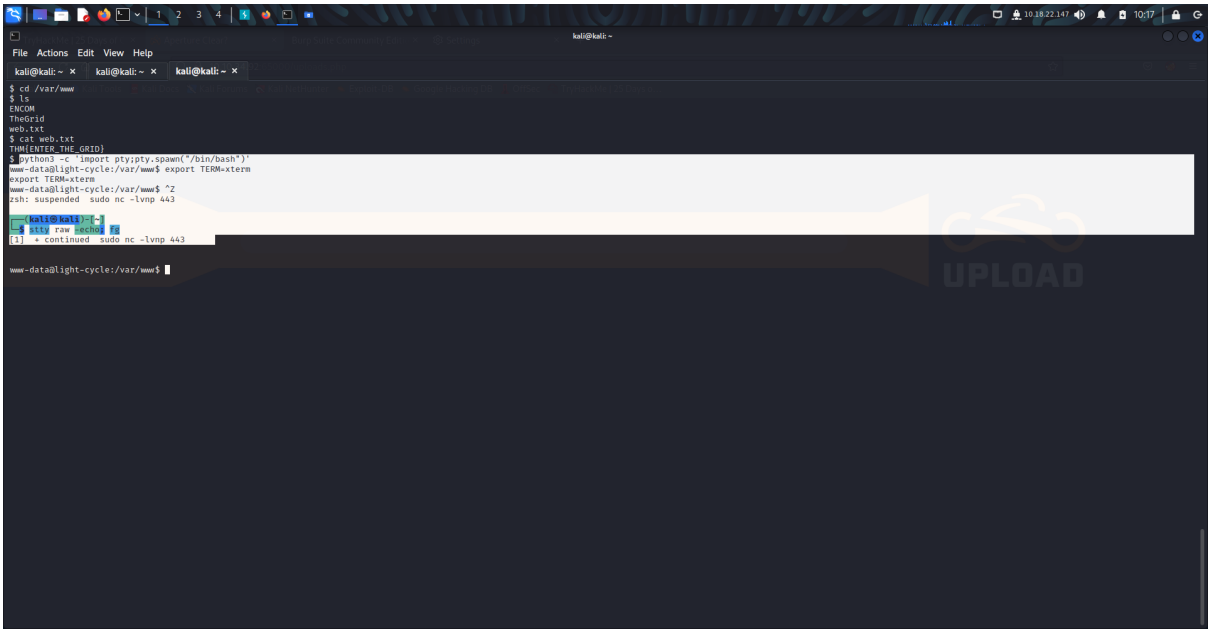


Discovering the value of web.txt flag



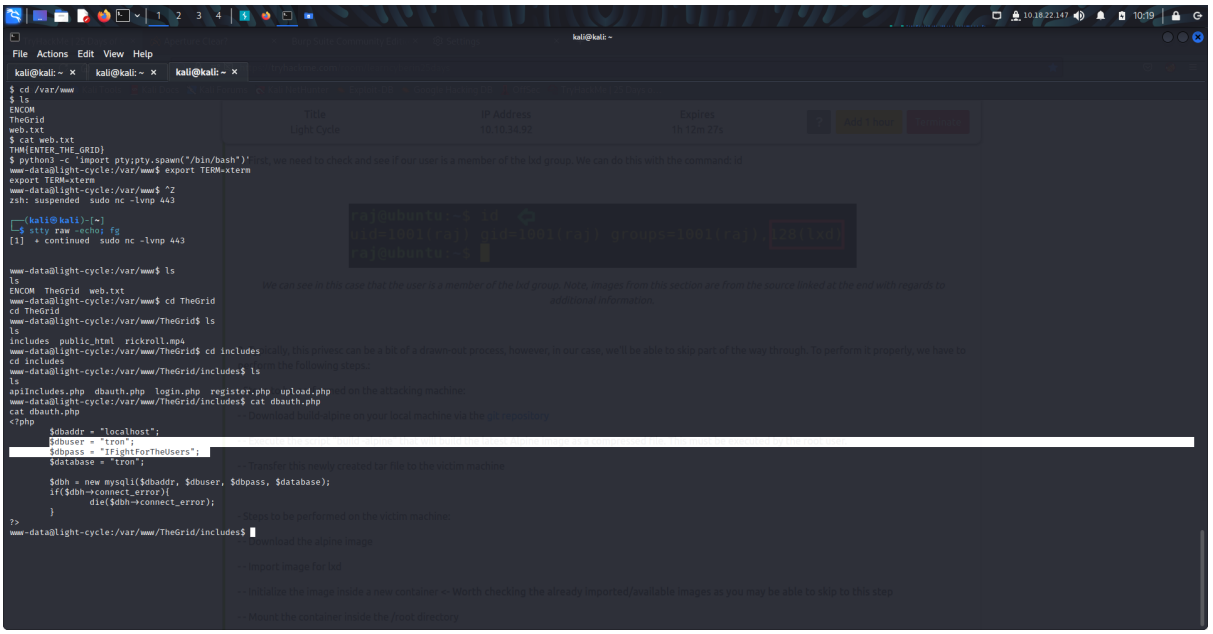
Question 6

Stabilising the shell



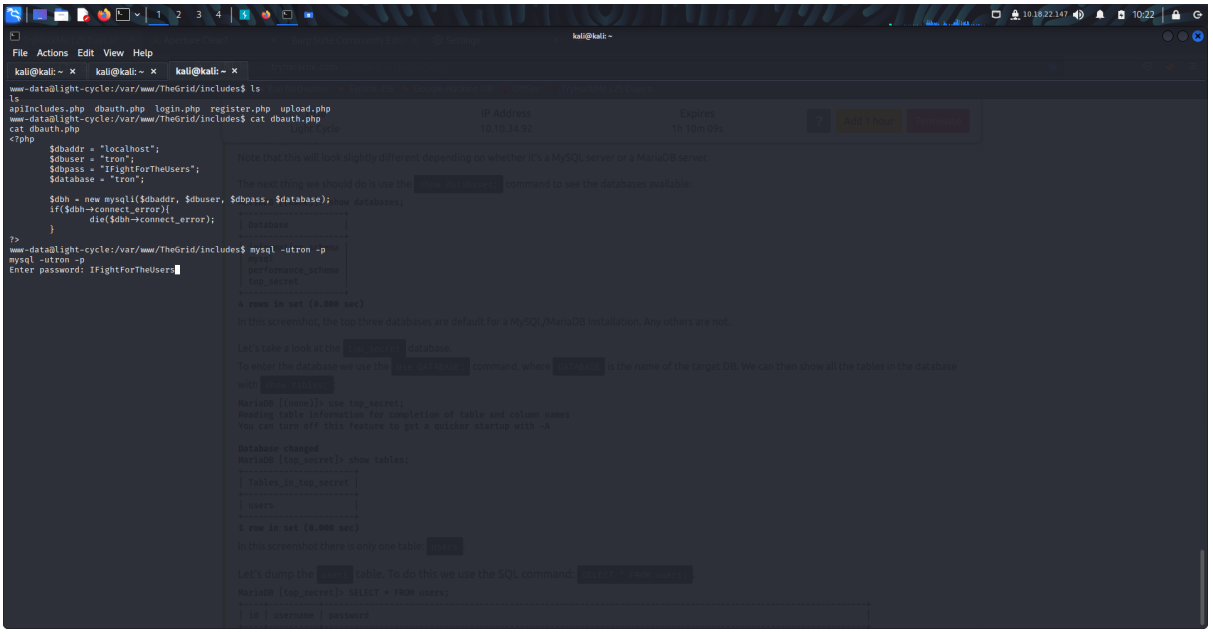
Question 7

Exploring /var/www/TheGrid/includes to find the username and password for the database

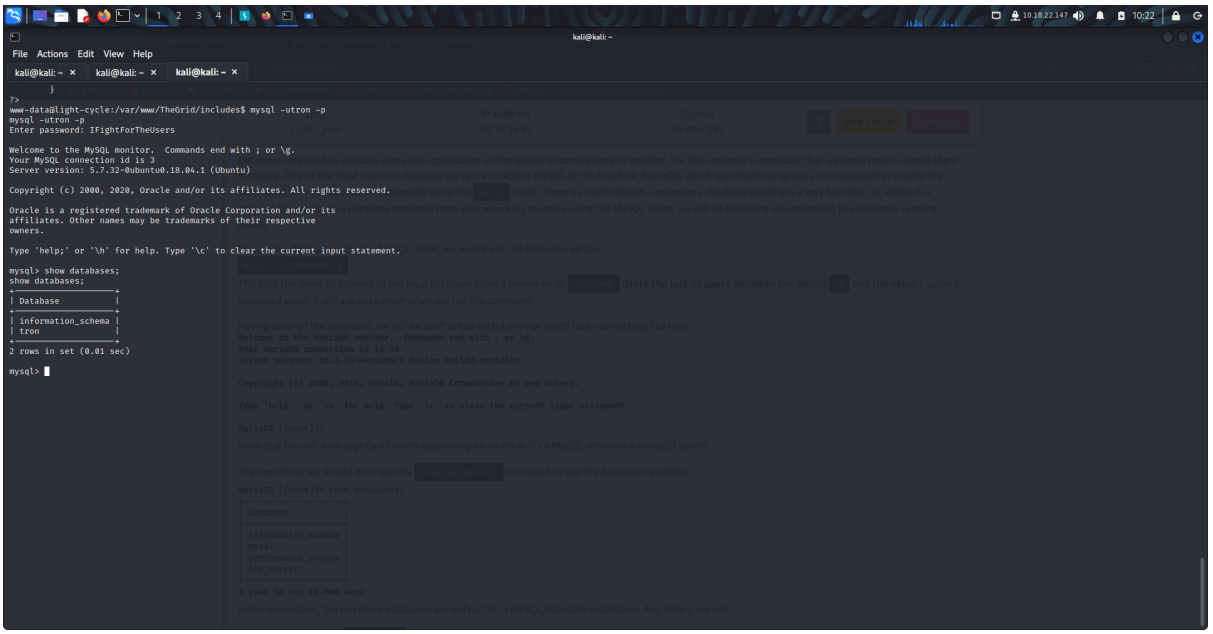


Question 8

Entering the credentials obtained from dbauth.php into mysql

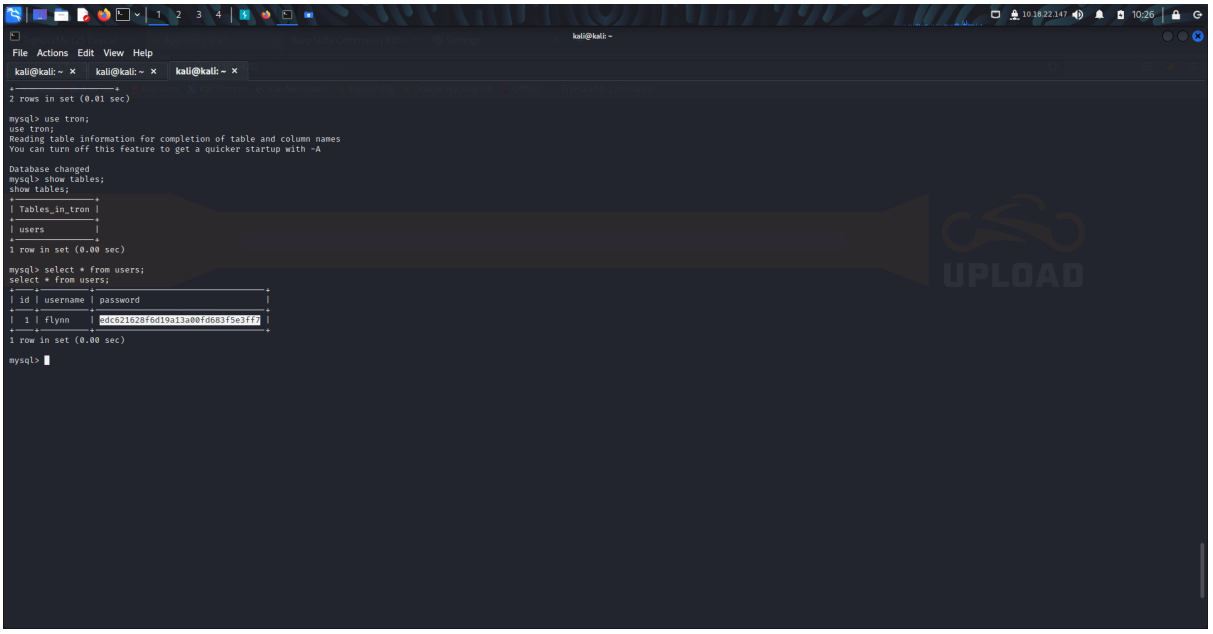


Showing the databases in the mysql

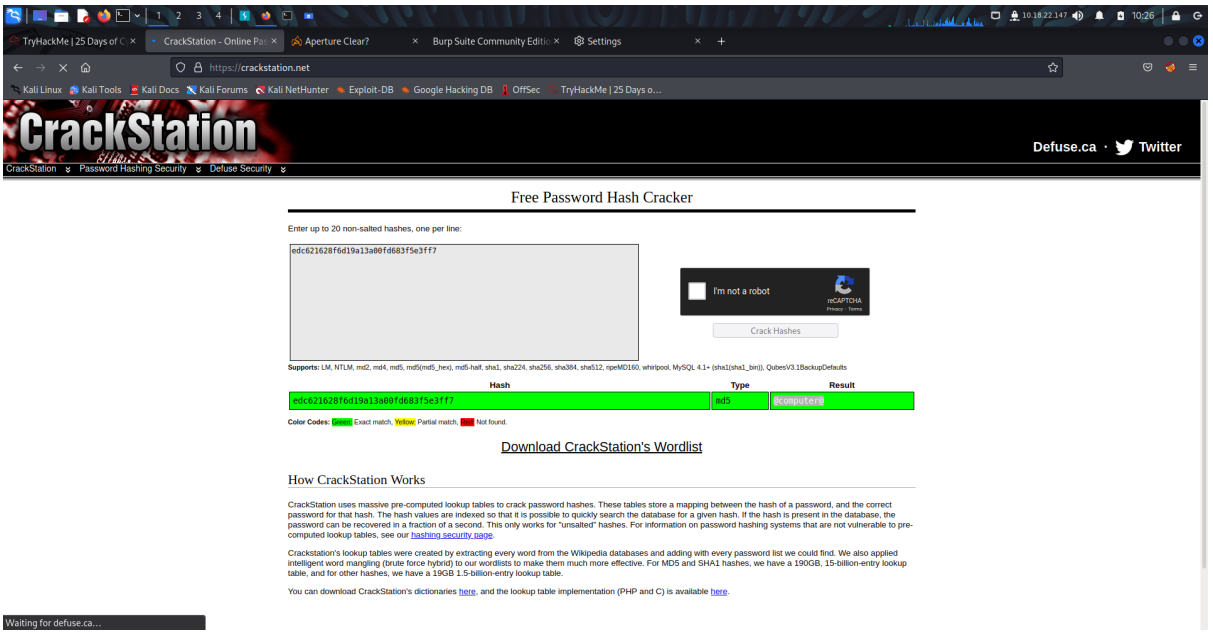


Question 9

Getting the encoded password by selecting all data in the users table

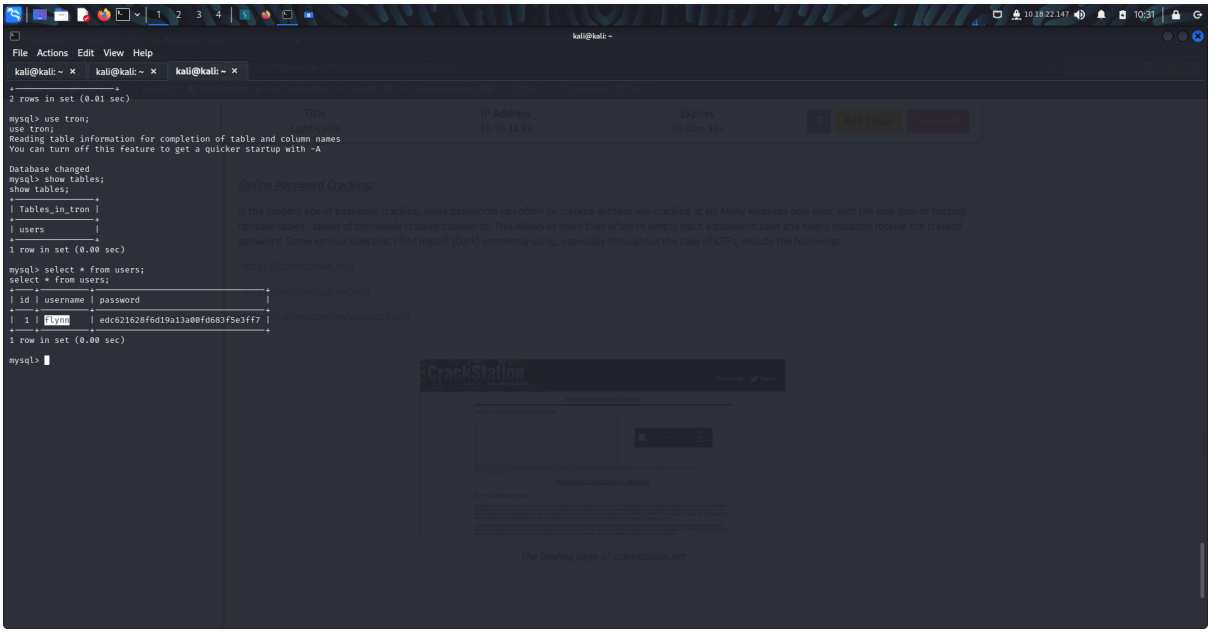


Decoding the password using *https://crackstation.net/*



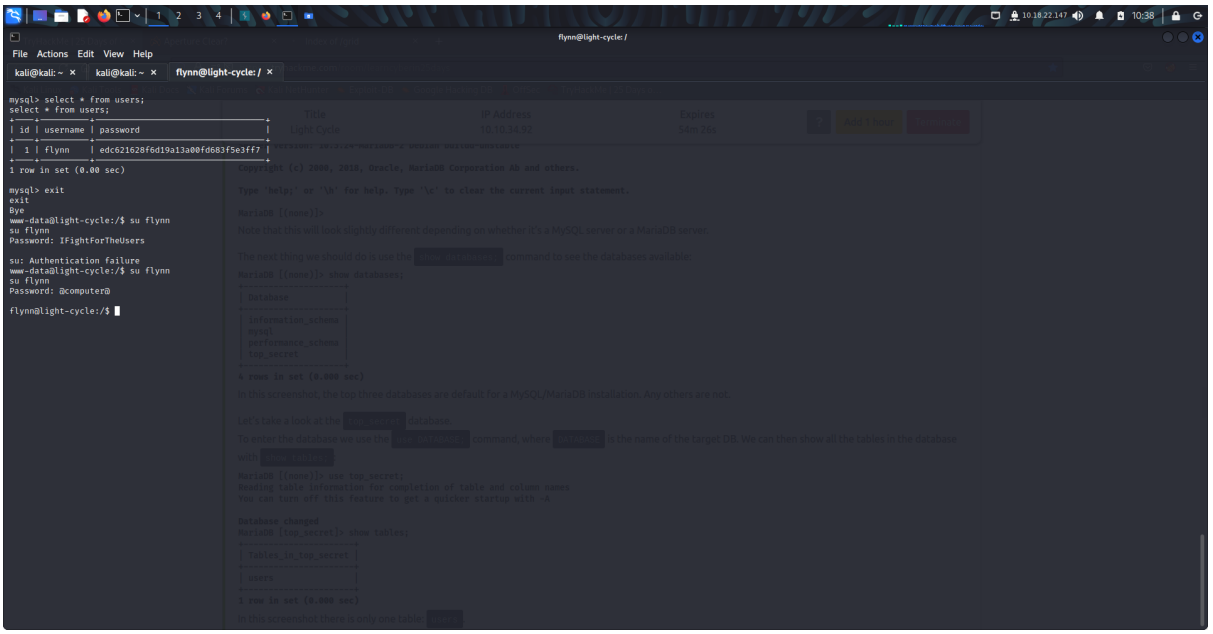
Question 10

The name of the user we are going to switch to

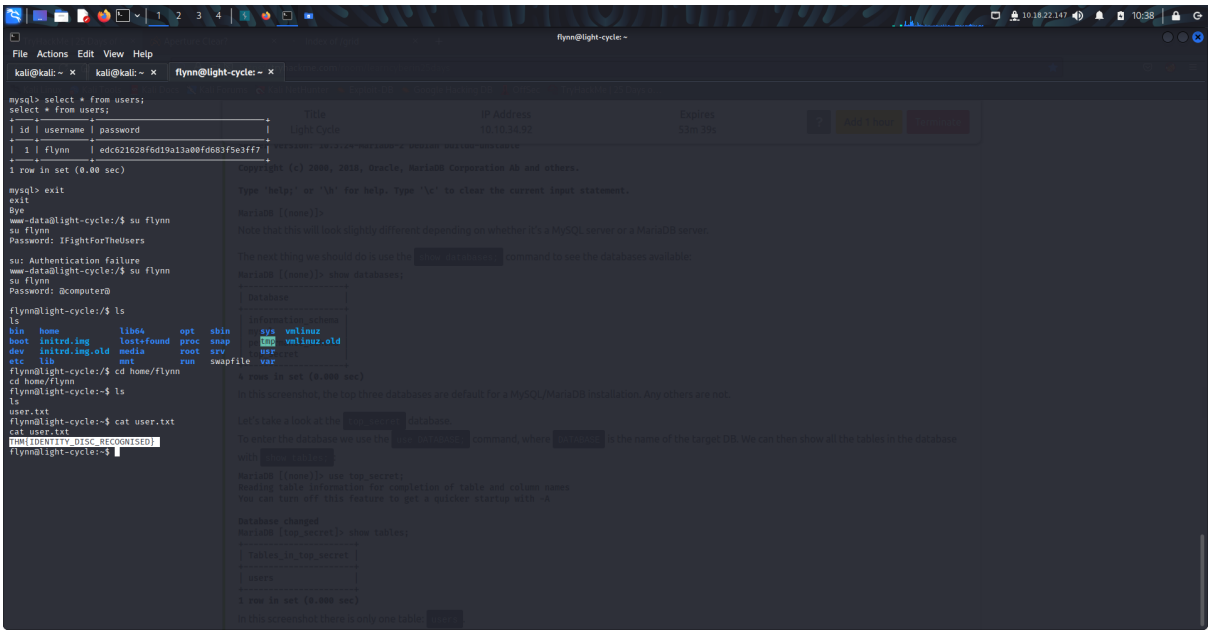


Question 11

Entering the credentials obtained from the users table in the database

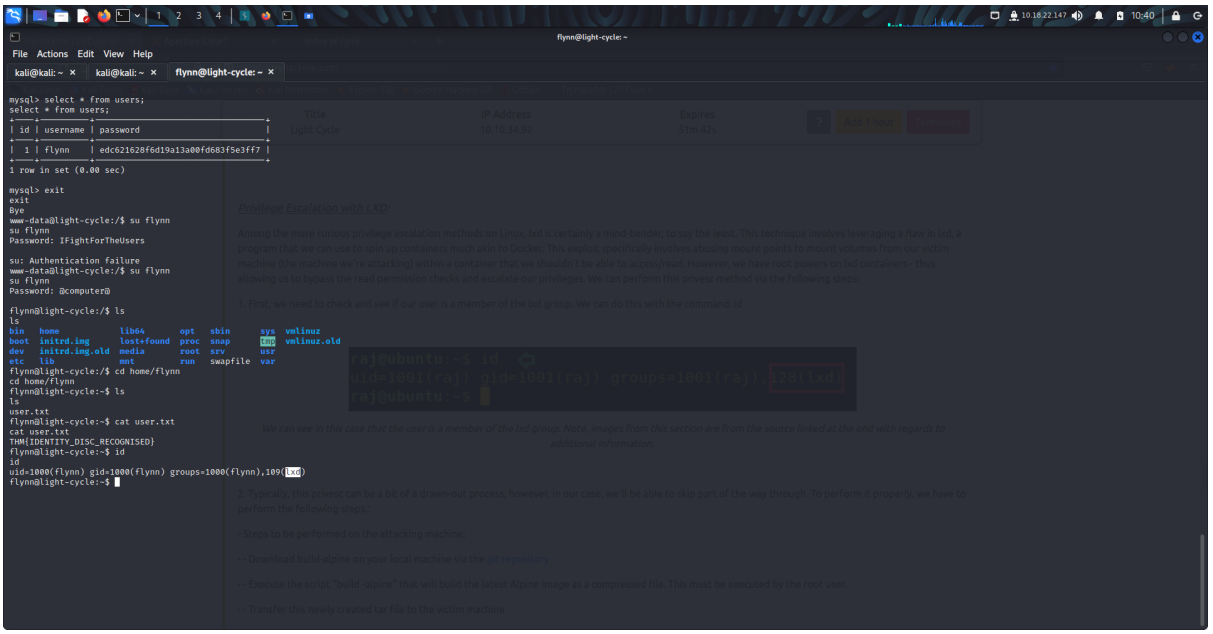


Exploring /home/flynn to get user.txt



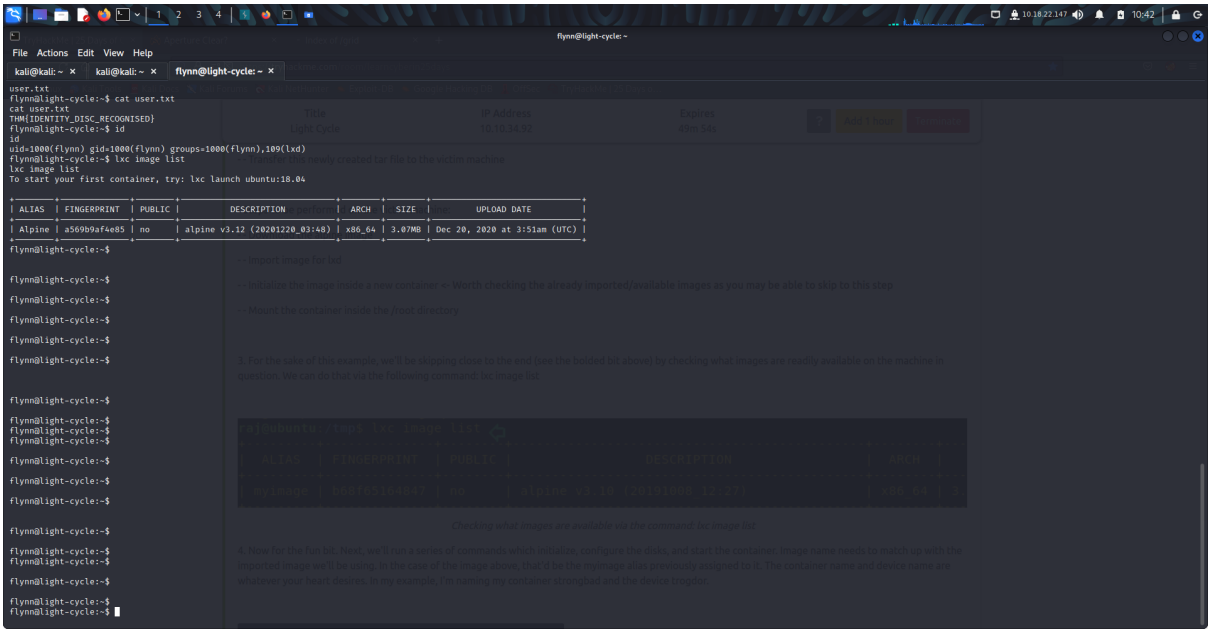
Question 12

Getting the group that will help to escalate the privilege

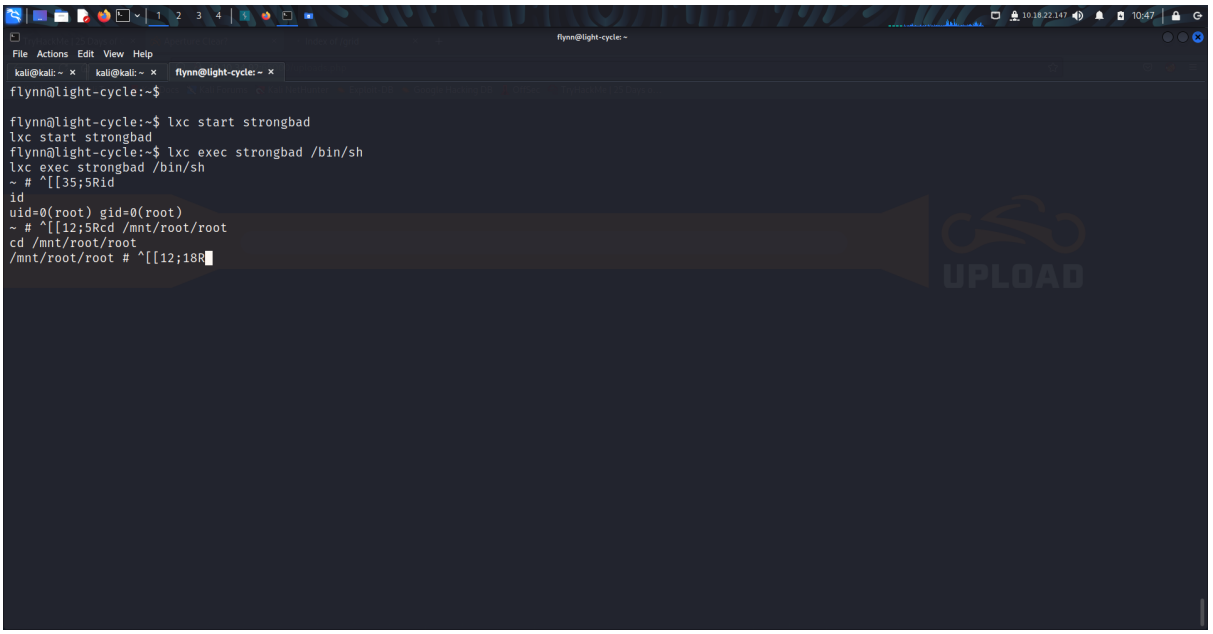


Question 13

Checking whether the image exist or not



Escalated the privilege to root level



Obtained the flag in the root.txt

```
flynn@light-cycle:~$

flynn@light-cycle:~$ lxc start strongbad
lxc start strongbad
flynn@light-cycle:~$ lxc exec strongbad /bin/sh
lxc exec strongbad /bin/sh
~ # ^[[35;5Rid
id
uid=0(root) gid=0(root)
~ # ^[[12;5Rcd /mnt/root/root
cd /mnt/root/root
/mnt/root/root # ^[[12;18Rls
ls
root.txt
/mnt/root/root # ^[[15;18Rcat root.txt
cat root.txt
THM{FLYNN_LIVES}


"As Elf McEager claimed the root flag a click could be heard as a small chamber on the anterior of the NUC popped open. Inside, McEager saw a small object, r
oughly the size of an SD card. As a moment, he realized that was exactly what it was. Perplexed, McEager shuffled around his desk to pick up the card and slo
t it into his computer. Immediately this prompted a window to open with the word 'HOLO' embossed in the center of what appeared to be a network of computers.
 Beneath this McEager read the following: Thank you for playing! Merry Christmas and happy holidays to all!"
/mnt/root/root # ^[[25;18R
```

Thought process/Methodology

Firstly, we use nmap to scan the website to search for the open port and found that port 80 and 65000 are open. Then, we try both port to see which one leads to the secret website and port 65000 is the one.

We find the title of the website by viewing the page source of the secret website and found that the title is Light Cycle.

After that, we use gobuster to find the hidden php page on the website and we also use gobuster to search the hidden directory where file uploads are saved.

After that, we copied the reverse shell.php file from /usr/share/webshells/php into our home directory and edited the name to bypass the server-side filter and we changed the IP address and the port number in the file and saved it. After that, we set up a netcat listener in port 443. Then, we upload the reverse shell to the website and open the reverse shell from the hidden directory where file uploads are saved.

As soon as we open the reverse shell, we have access to the reverse shell in the terminal where we set up the netcat listener. We change the directory into /var/www to get the web.txt flag. After that, we stabilise our shell by using the method provided in the dossier.
Then, we change directory into /var/www/TheGrid/includes to get the dbauth.php, which contains the username and password to unlock the database.

We then use mysql to log into the database and found out that there are 2 database and we decide to use database named tron. We found the username and the password which is encoded. We decode the password using crackstation.net.

By using the username *flynn* and password @*computer*@, we are able to switch user. After that, we change directory to home/flynn to obtain the user.txt flag. We check the group that will help us escalate our privilege by using command *id* and found that lxd is the group. Then, we check what image are readily available in the machine. After that, we run a series of commands which initialize, configure the disks, and start the container. Then, we escalated our privilege to root. We list the item in the directory and found the root.txt flag.