# PSP0201
# WEEKLY WRITE UP
# WEEK 6
# GROUP 7

Group Name : Sang Haekeo ( The Hackers )

Sang
- Taken from a Malay word , sang , meaning ‘the’

Haekeo
- Taken from a Korean word , 해커 , meaning ‘hacker’

| ID | NAME | ROLE |
|---|---|---|
| 1211100930 | KU NAJWA SYAUQINA BINTI KU AZRIN | Member |
| 1211101693 | SAVITHA MURUGUMUNISEGARAN | Member |

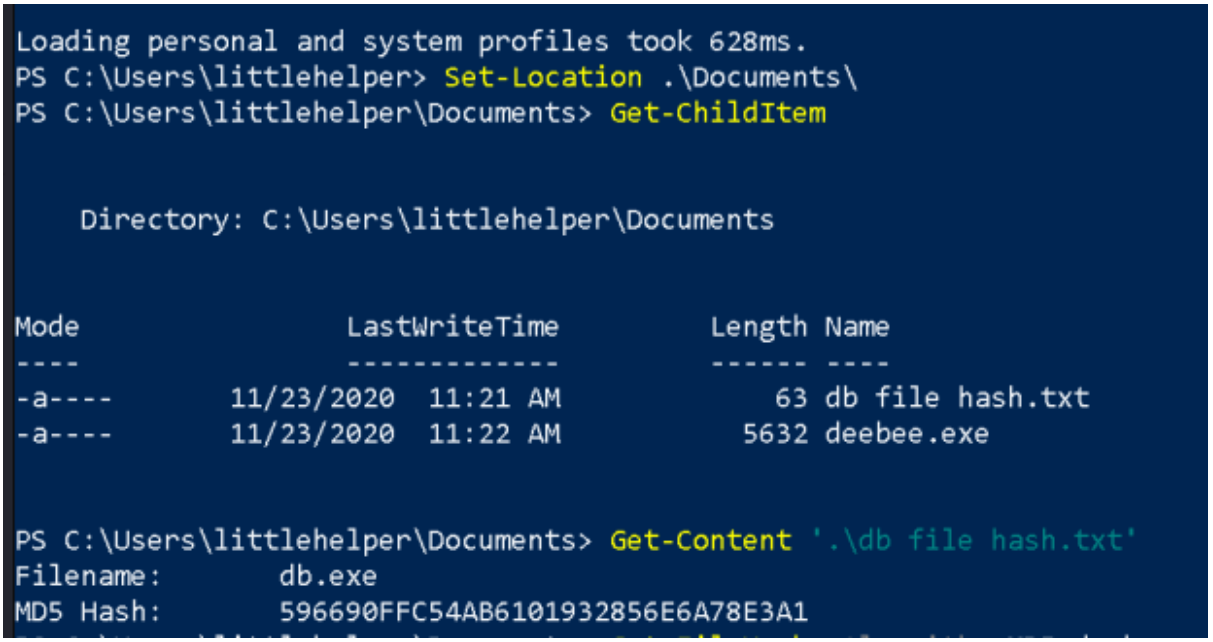
## Day 21: Time for some ELForensics

Question 1

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

Using the PowerShell commands, we can perform this process.

```
Set-Location c:\Users\littlehelper\Documents

Get-ChildItem

Get-Content 'db file hash.txt'
```




Question 2

What is the MD5 file hash of the mysterious executable within the Documents folder?

We can hash the file deebee.exe using Get-FileHash because we can see it in the Documents folder.

```
Get-FileHash -Algorithm MD5 'deebee.exe'
```

## Question 3

What is the SHA256 file hash of the mysterious executable within the Documents folder?

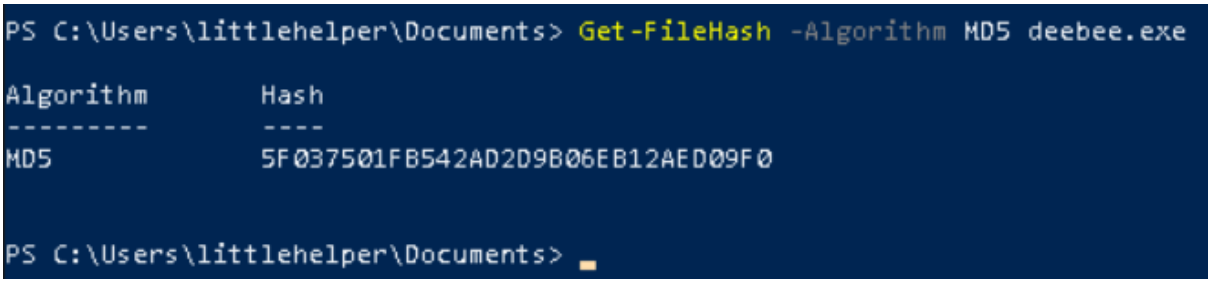
The executable file "deebee.exe" is the other one that is located in the "Documents" directory. We may use the command to create a hash value from a file in powershell.

Get-FileHash -Algorithm <alg> <path/filename>

For this question, the command will be

Get-FileHash -Algorithm MD5 deebee.exe

But keep in mind that SHA256 is the command's default algorithm. If we didn't provide the desired custom algorithm, the default value will be applied. Without the -Algorithm switch, We attempted to compute the hash, but the outcome was incorrect.




## Question 4

Using Strings find the hidden flag within the executable?

We first tried using the Select-String command to look for a Pattern containing "Red Ryder," but it was unsuccessful in doing so.

c:\Tools\strings64.exe -accepteula deebee.exe

Observe anything that appears out of the ordinary by scrolling back up to the top and then down through the file.

```
System
Main
System.Reflection
Sleep
Clear
.ctor
System.Diagnostics
System.Runtime.InteropServices
System.Runtime.CompilerServices
DebuggingModes
args
Object
Accessing the Best Festival Company Database...
Done.
Using SSO to log in user...
Loading menu, standby...
THM{f6187e6cbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -value $(Get-Content $(Get-Command C:\Users\littlehelper\Docume
nts\db.exe).Path -ReadCount 0 -Encoding Byte) -Encoding Byte -Stream hidedb
Hahaha .. guess what?
Your database connector file has been moved and you'll never find it!
I guess you can't query the naughty list anymore!
>;^P
z\V
WrapNonExceptionThrows
deebee
Copyright
```

Let's also note this fascinating discovery before moving on to the following topic.

```
THM{f6187e6cbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -value $(Get-Content $(Get-Command C:\Users\littlehelper\Docum
nts\db.exe).Path -ReadCount 0 -Encoding Byte) -Encoding Byte -Stream hidedb
Hahaha .. guess what?
Your database connector file has been moved and you'll never find it!
I guess you can't query the naughty list anymore!
>;^P
```

## Question 5

What is the powershell command used to view ADS?

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

## Question 6

What is the flag that is displayed when you run the database connector file?

We used the Get-Item command first. In the binary file, this makes it easier for us to find other data streams.

```
Get-Item -Path deebee.exe -Stream *
```

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


PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documen
                eebee.exe::$DATA
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documen
PSChildName   : deebee.exe::$DATA
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\littlehelper\Documents\deebee.exe
Stream        : :$DATA
Length        : 5632

PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documen
                eebee.exe:hidedb
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documen
PSChildName   : deebee.exe:hidedb
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\littlehelper\Documents\deebee.exe
Stream        : hidedb
Length        : 6144
```

Notice that we have two streams: the hidden ADS, "hidedb," and the default stream, "$DATA."

Let's use the following command to launch the hidden executable now that we know the ADS's name.

wmic process call create $(Resolve-Path c:\Users\littlehelper\Documents\deebee.exe:hidedb)

```
PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-Path c:\User
tlehelper\Documents\deebee.exe:hidedb)
Executing (Win32_Process)->Create()
```

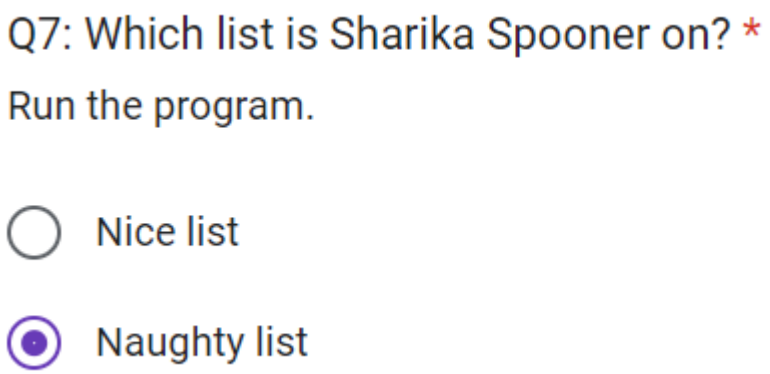
C:\Users\littlehelper\Documents\deebee.exe:hidedb

```
Choose an option:
1) Nice List
2) Naughty List
3) Exit

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option:
```

With the final flag in addition to the Nice and Naughty List, this opens the original Database file.

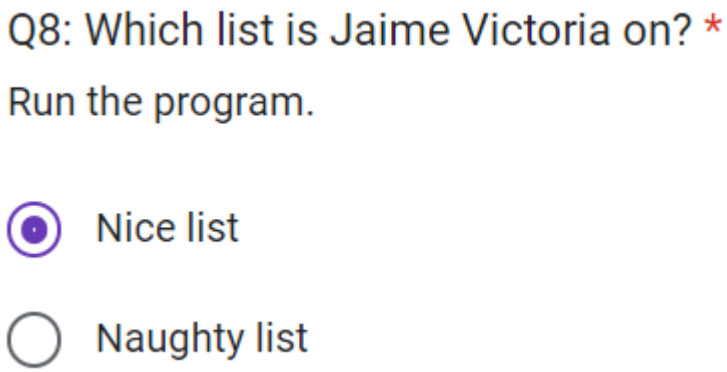
Question 7

`Which list is Sharika Spooner on?`




Question 8

`Which list is Jaime Victoria on?`

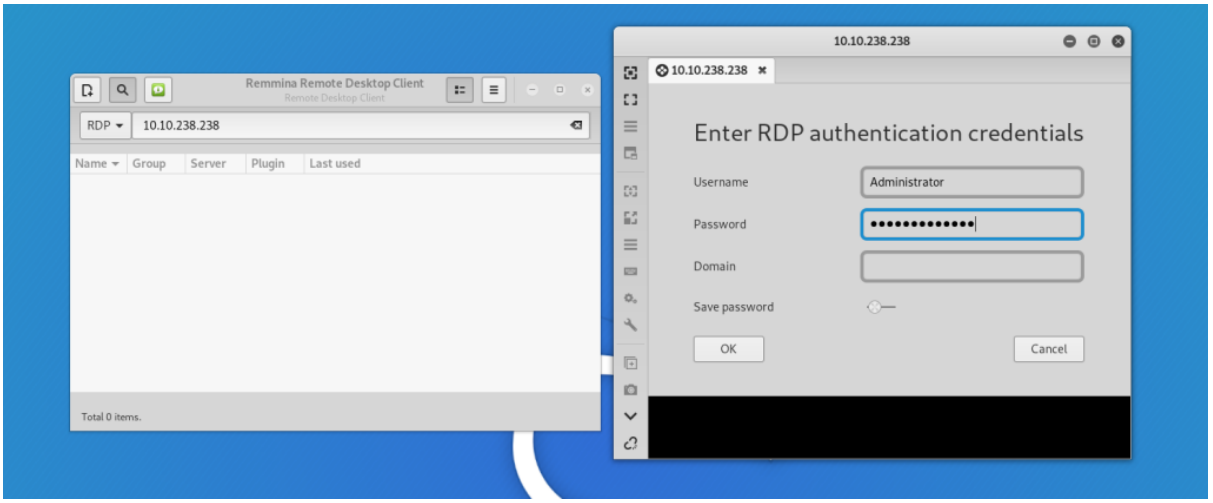


## Day 22: Elf McEager becomes CyberElf

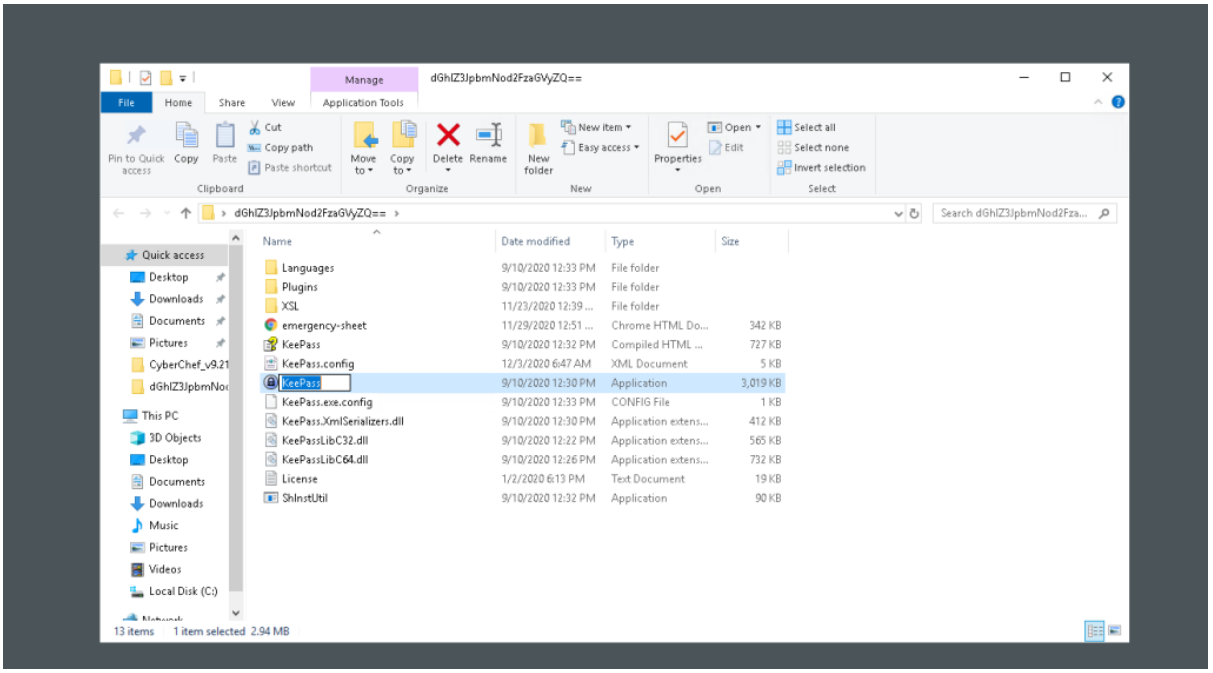
Question 1

What is the password to the KeePass database?

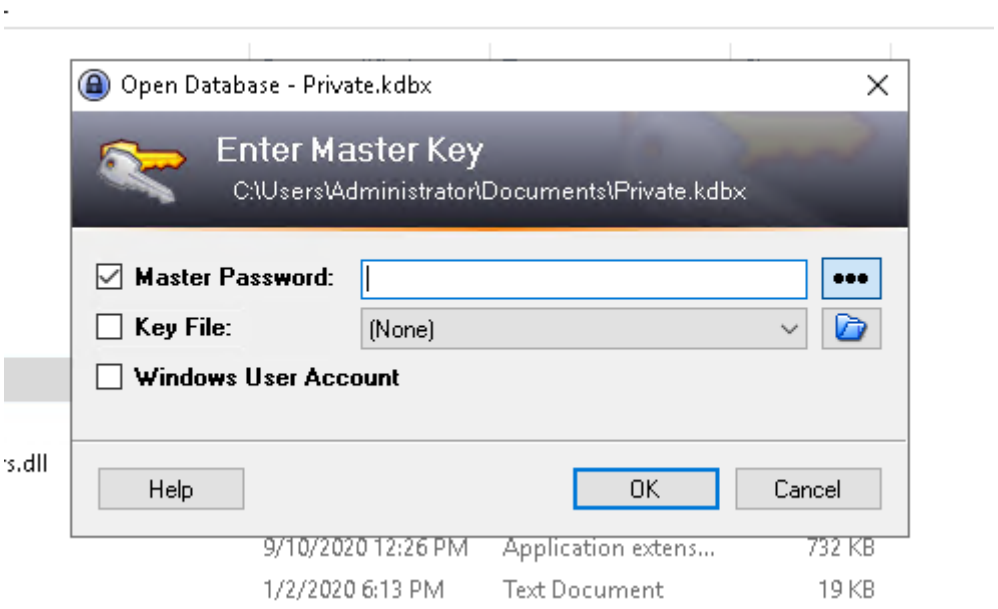
We will use Remmina to connect to our target computer after it has fully booted up. The login credentials are Administrator and sn0wF!akes!!!



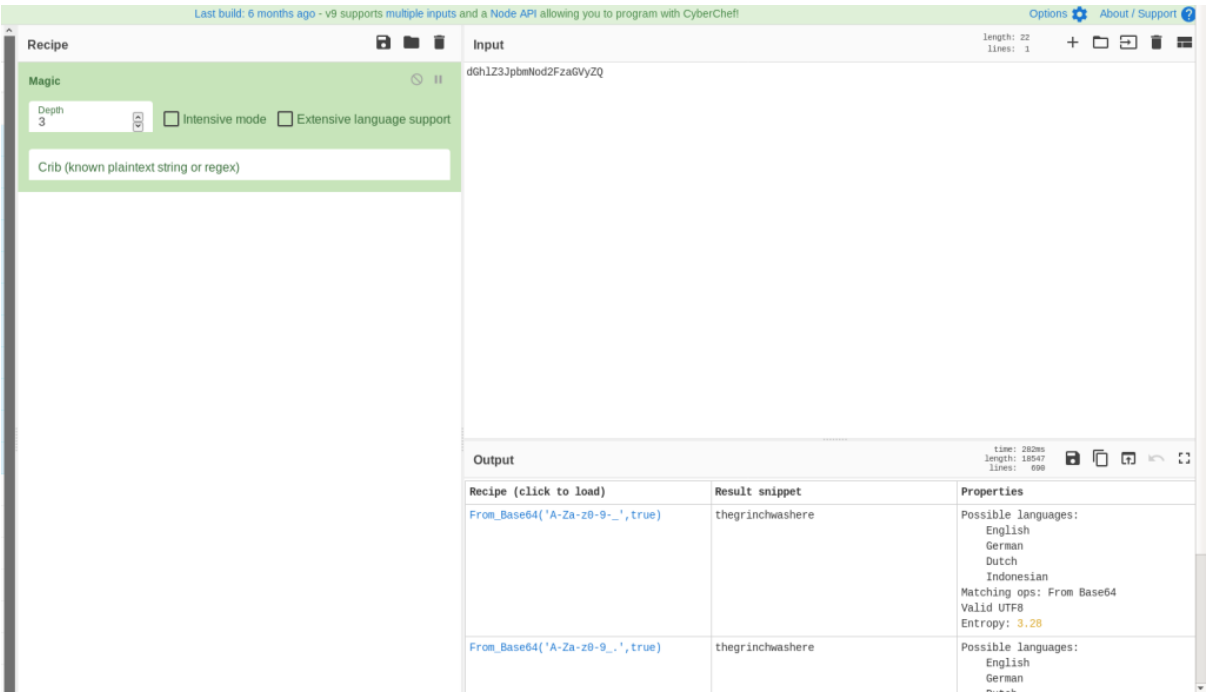

Let's open the oddly named folder on the Desktop when we have finished logging in. Run the KeePass programme after entering.



The master key is then required in order to enter. Sadly, we do not currently own the master key.




The name of the folder where KeePass is located appears dubious, almost as if it were encoded. Let's utilise the Magic recipe on CyberChef. When we type the folder's name, we can see that CyberChef was able to decode the Base64 encoding and that thegrinchwashere is the master key.




**Answer:** thegrinchwashere

## Question 2

What is the encoding method listed as the 'Matching ops'?

When we type the folder's name, we can see that CyberChef was able to decode the Base64 encoding.

**Answer:** base64

## Question 3

What is the note on the hiya key?

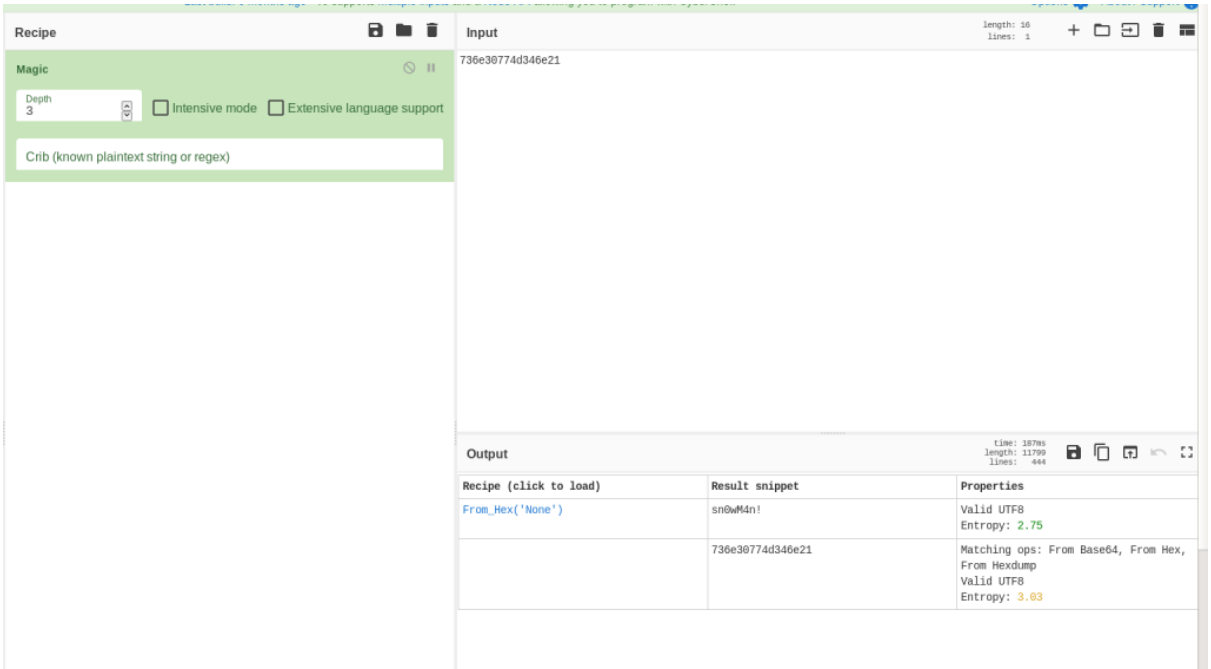
**Answer:** Your passwords are now encoded. You will never get access to your systems! Hahaha >:^P

## Question 4

What is the decoded password value of the Elf Server?

Let's explore KeePass after logging in to see if we can discover any other passwords. When we choose the Network tab, we can see that the Elf Server password has been stored. Let's try to decipher the password by copying it and pasting it into CyberChef.

Once more, the Magic formula is effective! It appears to have been successful in decoding the password from hex. The Elf Server password is sn0wm4n!




**Answer:** sn0wm4n!

## Question 5

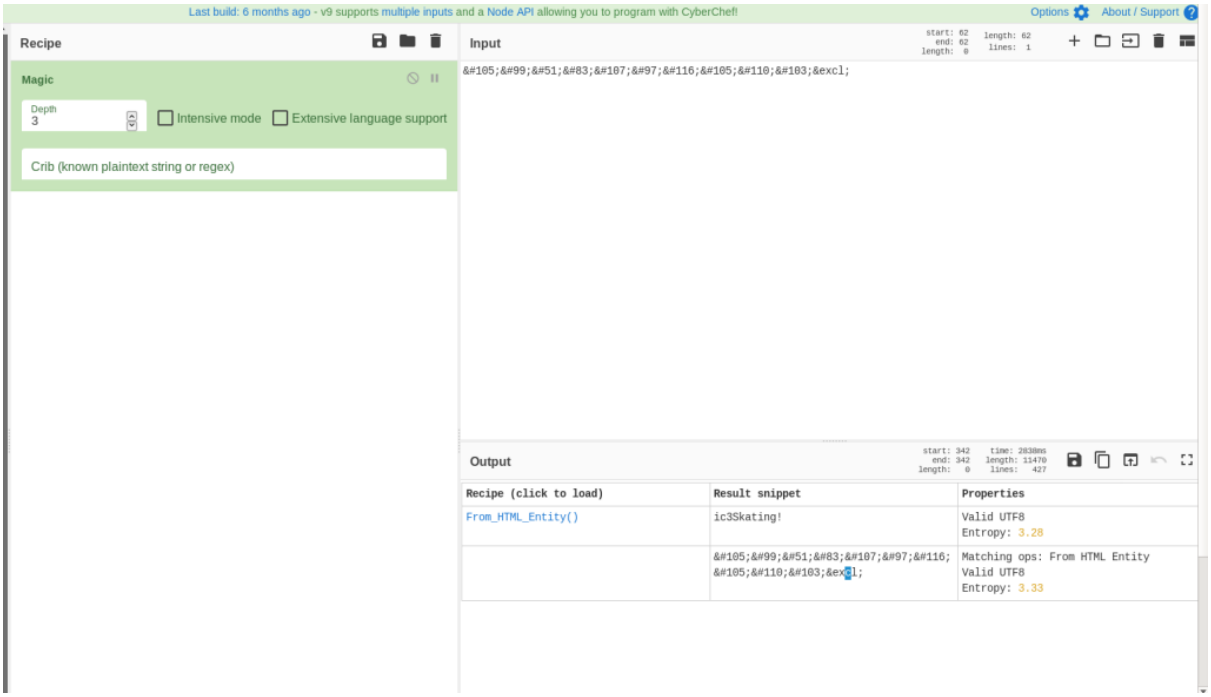
What was the encoding used on the Elf Server password?

**Answer:** hex

## Question 6

What is the decoded password value for ElfMail?

The password ic3Skating! decoded from an HTML entity can be found when we follow the same procedures for Elf Mail.




**Answer:** ic3Skating!

## Question 7

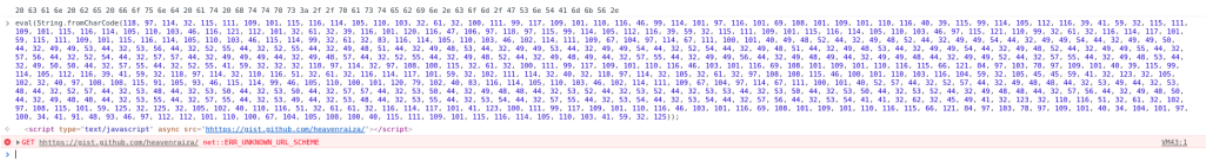
What is the username:password pair of Elf Security System?

**Answer:** superelfadmin:nothinghere

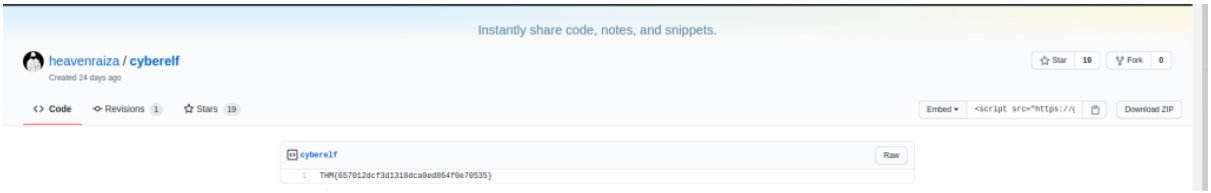
## Question 8

Decode the last encoded value. What is the flag?

To begin searching for the last flag, we clicked the Recycle Bin tab. We can make out what appears to be JavaScript code in the notes. So we can execute the code in the browser's console and observe that it will take us to a GitHub URL.



If we follow this link we see it leads to our flag THM{657012dcf3d1318dca0ed864f0e70535}.



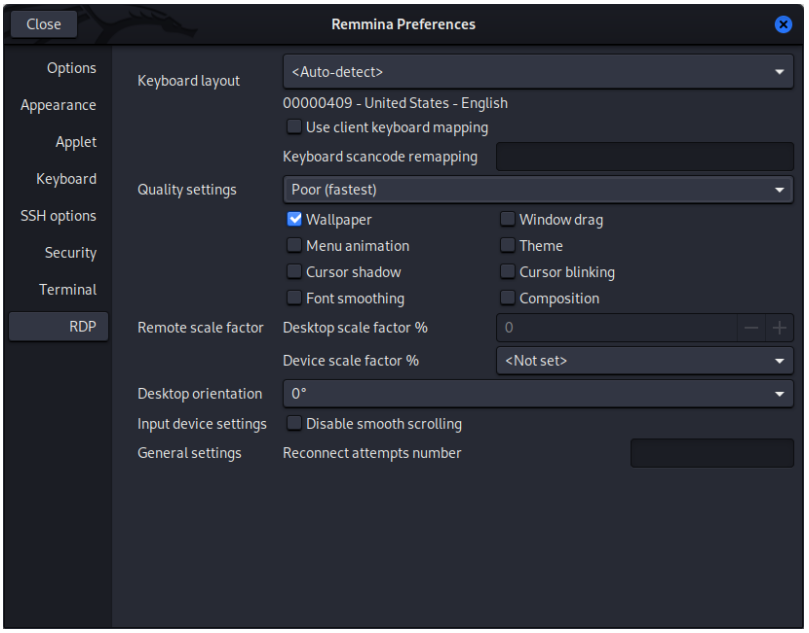

**Answer:** THM{657012dcf3d1318dca0ed864f0e70535}

## Day 23 – Blue Teaming: The Grinch Strikes Again!

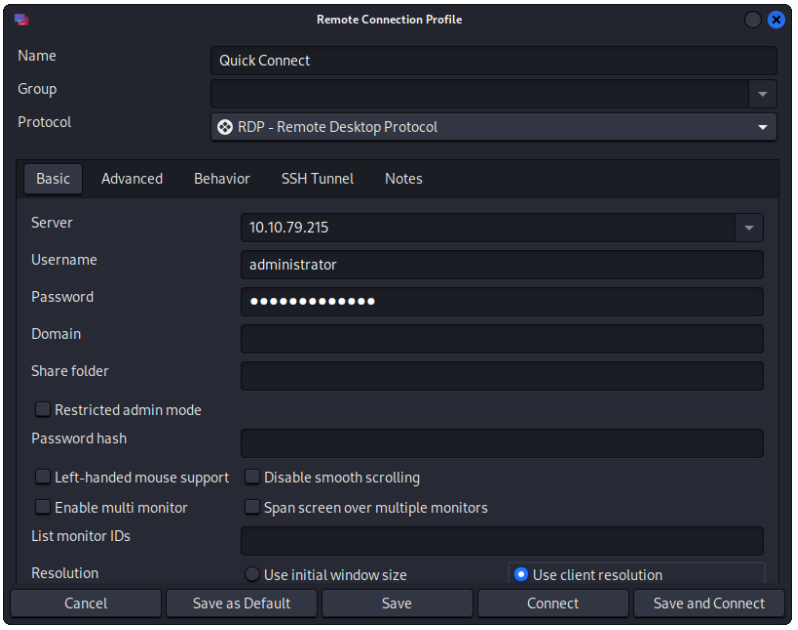
Q1: What does the wallpaper say?

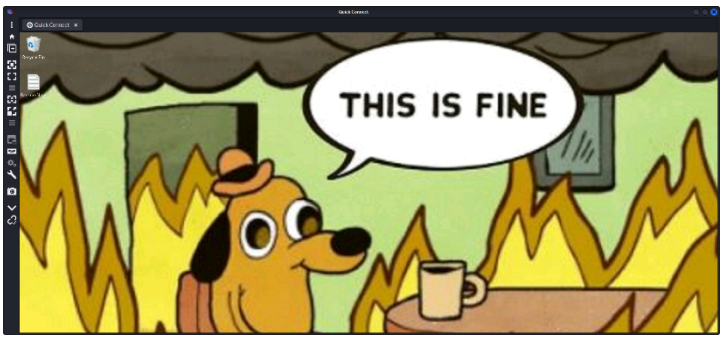
Ans : THIS IS FINE

use Remmina to connect to it. In Remmina, open Preferences -> RDP and make sure the wallpaper box is checked.




login with the username administrator and the password sn0wF!akes!!!

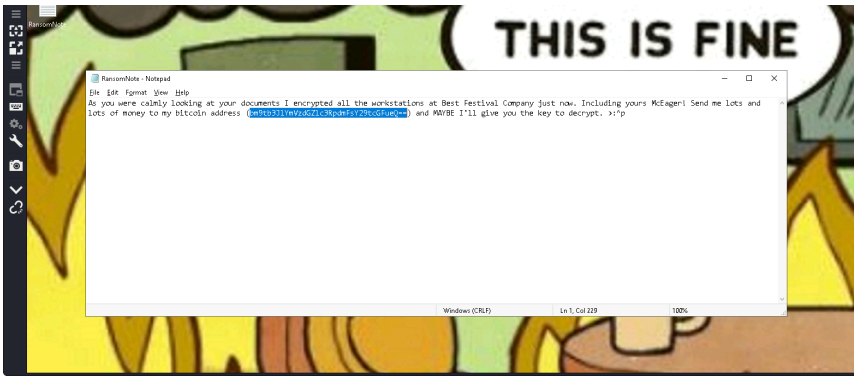


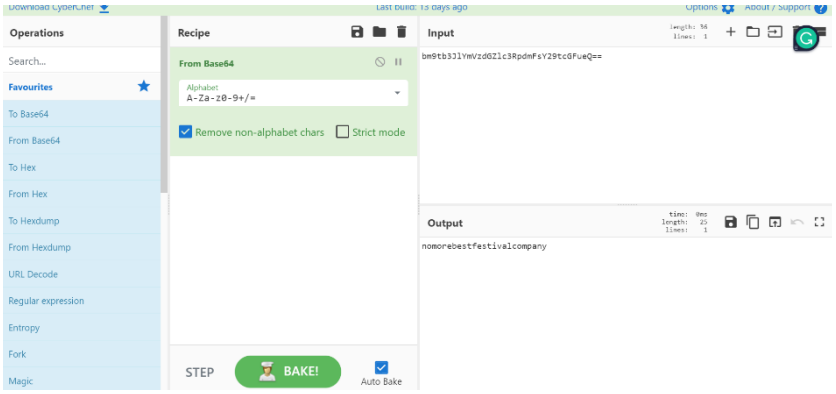



Q2: Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?

Ans : nomorebestfestivalcompany

Using CyberChef to decode the bitcoin address from Base 64 and we find that the address is nomorebestfestivalcompany.

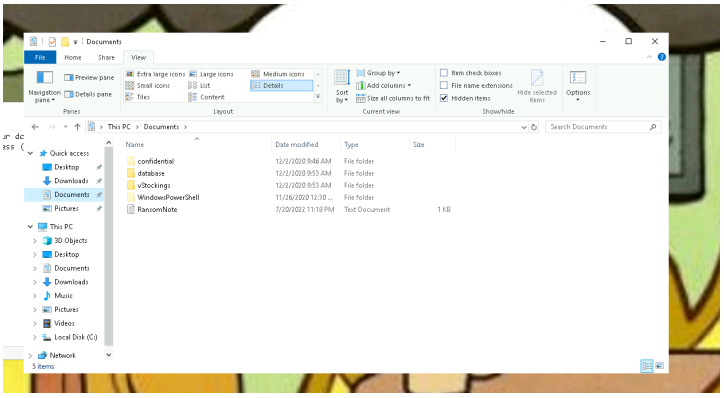


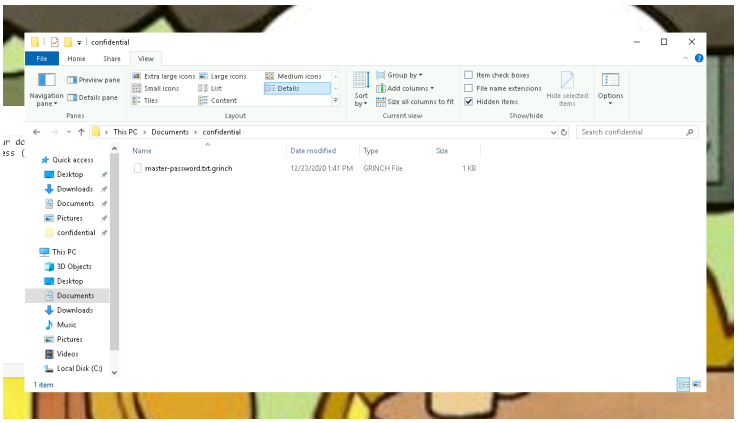



Q3:  At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files?

Ans : .grinch

open the file explorer and open document. Make sure that Hidden Items is selected under the view tab in your file explorer. Open confidential and we see that the extension is .grinch .

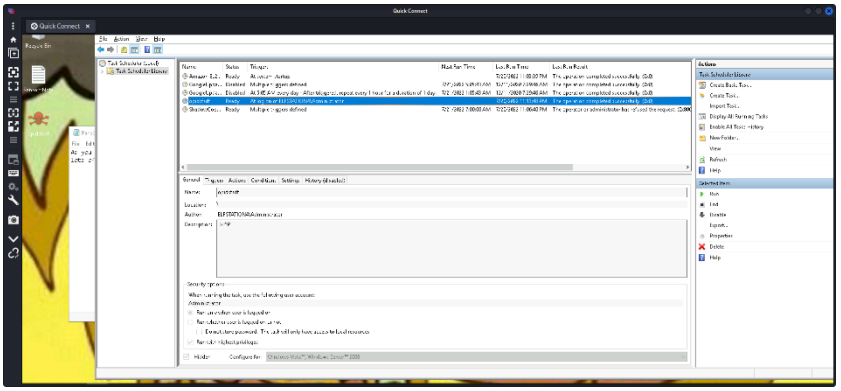




Q3:  What is the name of the suspicious scheduled task?

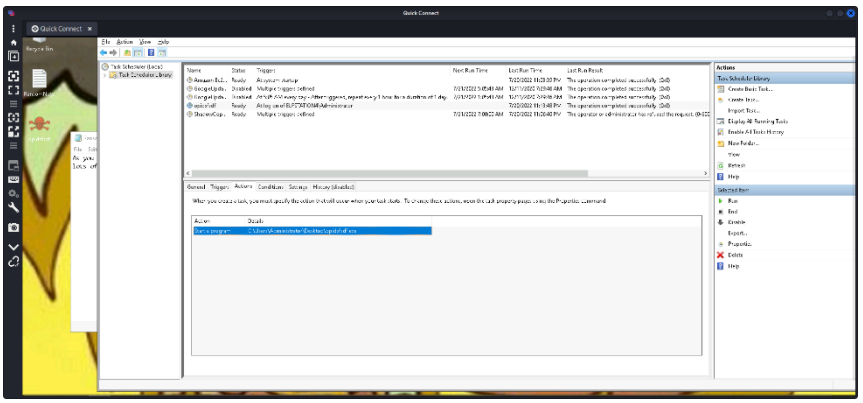
Ans : opidsfsdf

Open the Task Scheduler and click on the last scheduled task in the library. Look for a suspicious task named opidsfsdf. When we examine the properties we see this task runs a file located at C:\User\Administrator\Desktop\opidsfsdf.exe



Q4: Inspect the properties of the scheduled task. What is the location of the executable that is run at login?

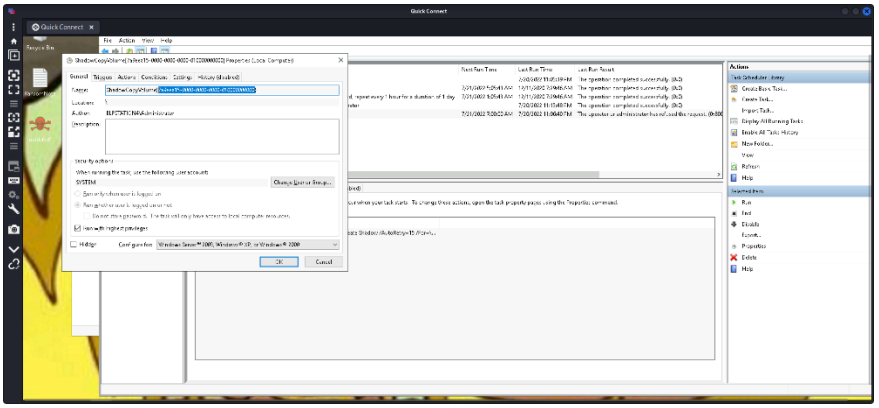
Ans : C:\User\Administrator\Desktop\opidsfsdf.exe



Q5 : There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?

Ans : 7a9eea15-0000-0000-0000-010000000000

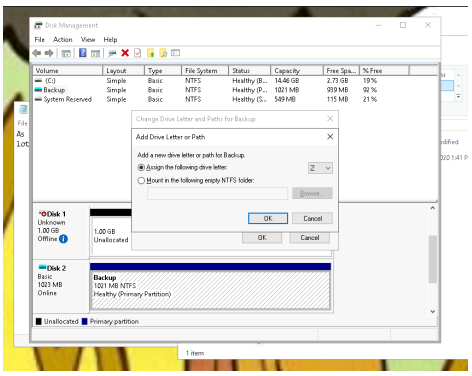
Click on shadowcopy and go to general.

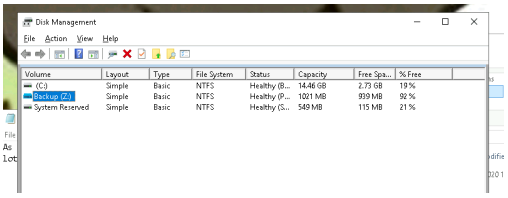


Q6: Assign the hidden partition a letter. What is the name of the hidden folder?

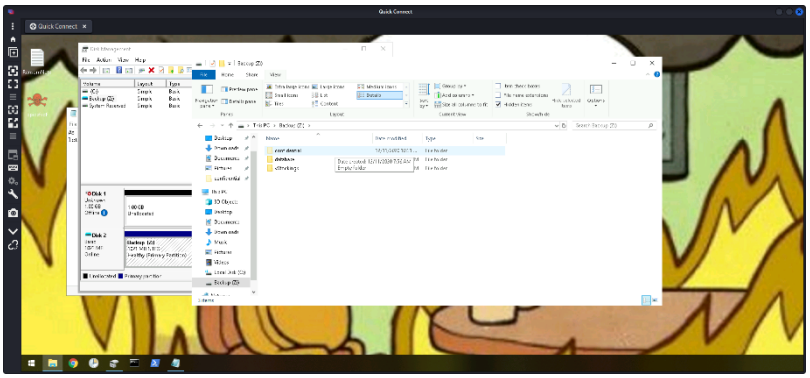
Ans : Confidential

Right click Backup and select Change Drive Letter and Paths. click Add and select any letter. We should now see Backup assigned to the letter Z.





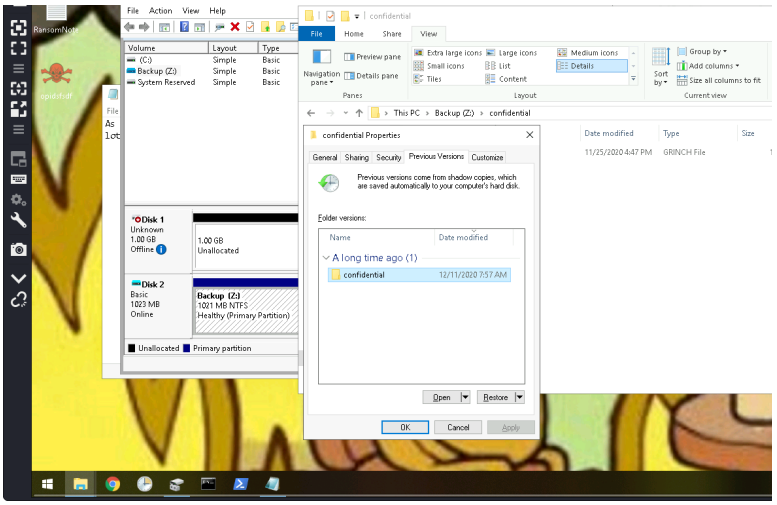
We can tell the drives that are hidden by the fact that they are slightly transparent which is confidential.

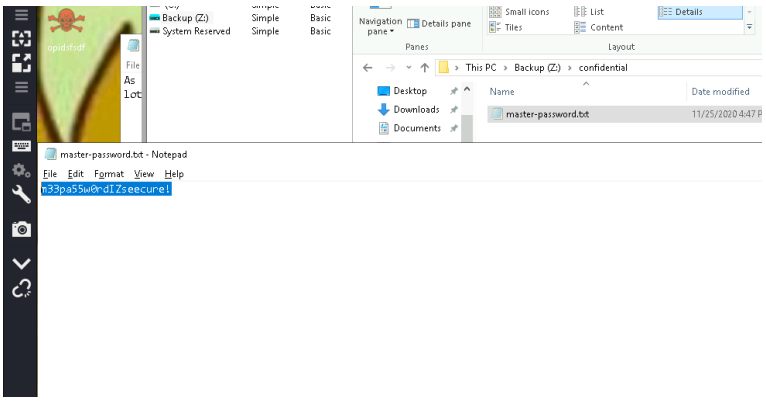


Q7: Right-click and inspect the properties for the hidden folder. Use the 'Previous Versions' tab to restore the encrypted file that is within this hidden folder to the previous version. What is the password within the file?

Ans : m33pa55w0rdIZseecure!

restore the previous version of the master-password.txt.grinch file by right-clicking and open the file properties. Go to Previous Versions tab and select OK. open the file with notepad to reveal the flag.



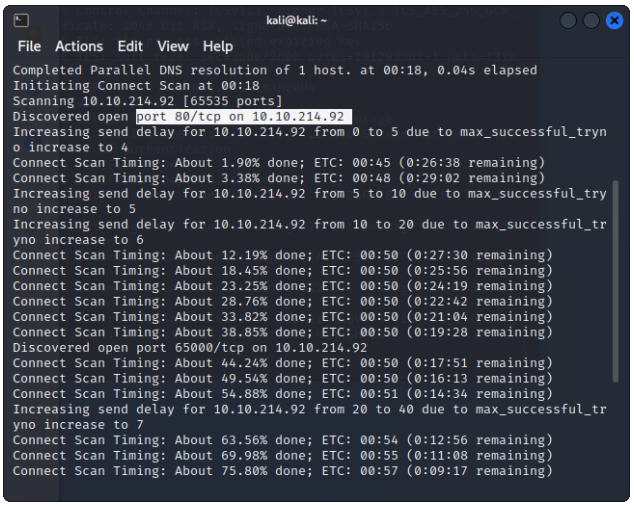

opidsfsdf
Backup (Z:) Simple Basic
System Reserved Simple Basic
Navigation pane
Details pane
Panes
Small icons
List
Details
Tiles
Content
Layout
This PC › Backup (Z:) › confidential
Desktop
Downloads
Documents
Name
Date modified
master-password.txt
11/25/2020 4:47 P
master-password.txt - Notepad
File Edit Format View Help
w33pa55w0rdIZseecure!

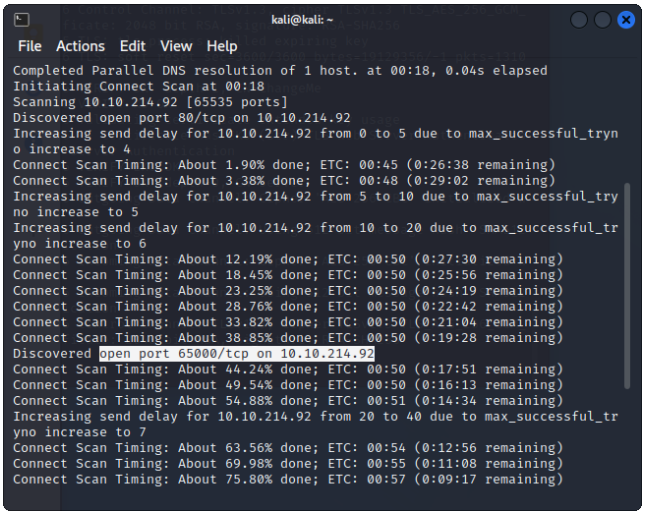
## Day 24 – The Final Challenge: The Trial Before Christmas

Q1:  Scan the machine. What ports are open?

Answer: 80, 65000

run a scan with nmap to see what ports are open.

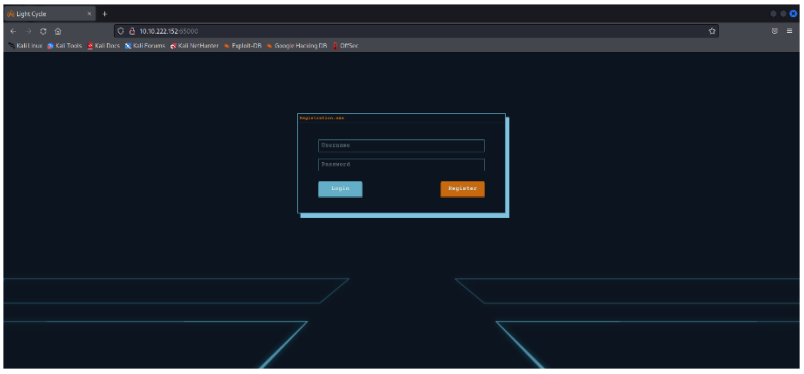



Q2: What's the title of the hidden website? It's worthwhile looking recursively at all websites on the box for this step.

Ans : Light Cycle

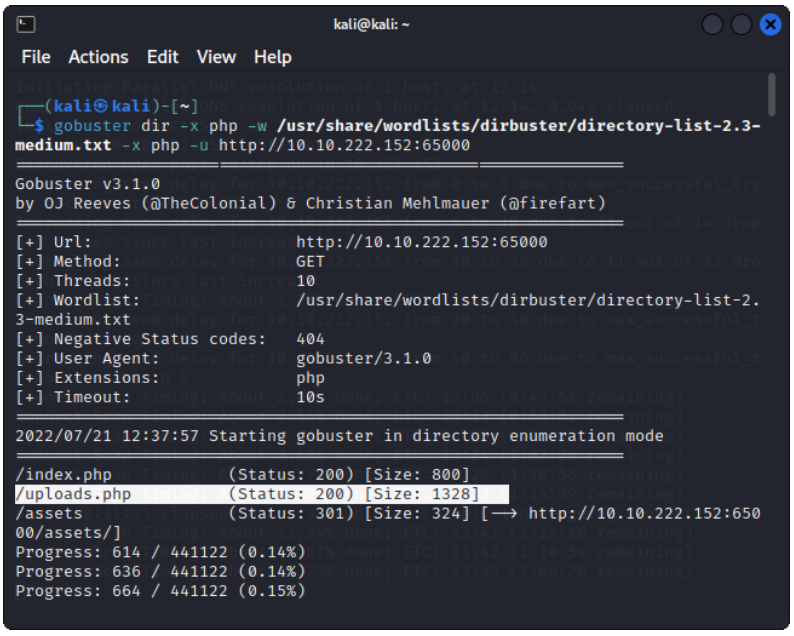
Go to webserver running on port 65000. we see a website with the title Light Cycle which gives us the option to register or login.



Q3: What is the name of the hidden php page?

Ans : uploads.php

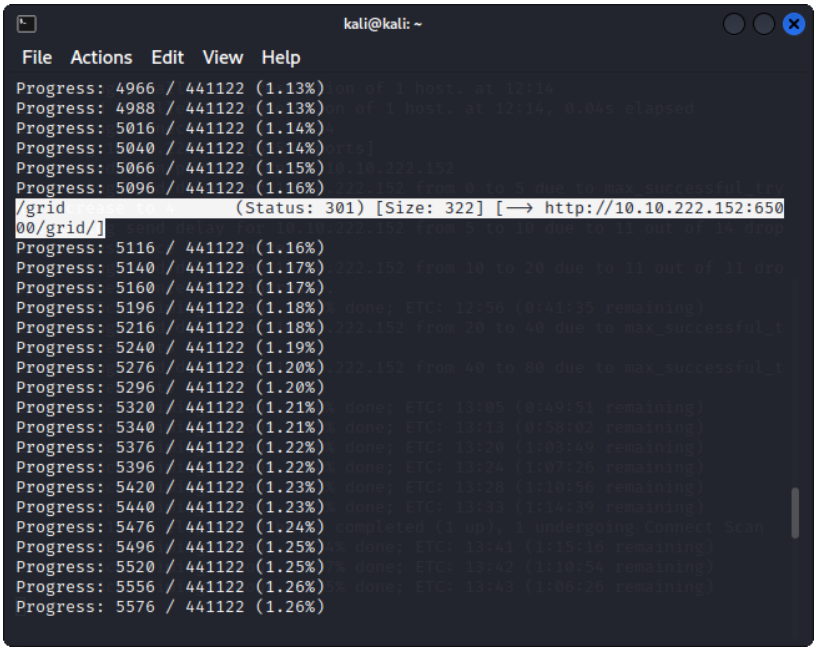
gobuster dir -x php -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php -u http://10.10.222.152:65000



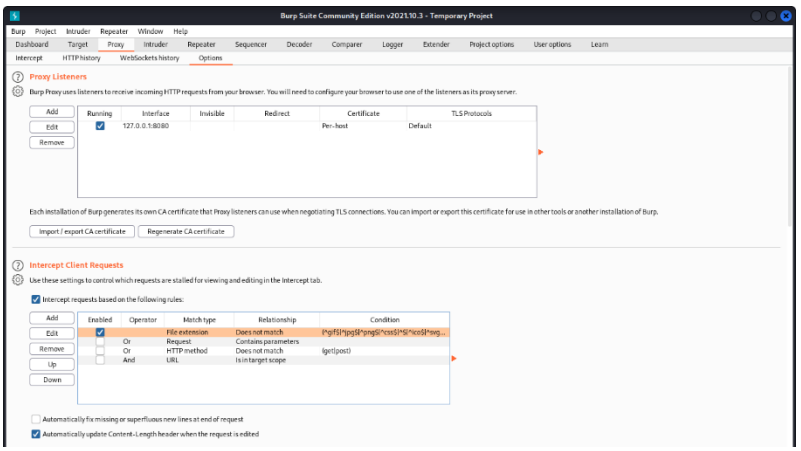

Q4: What is the name of the hidden directory where file uploads are saved?

Ans : grid

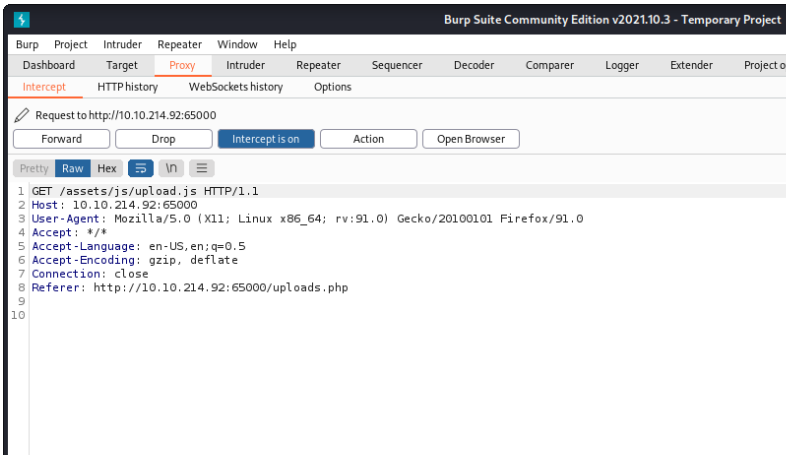
We also see a directory named /grid which is where the uploaded files are stored.



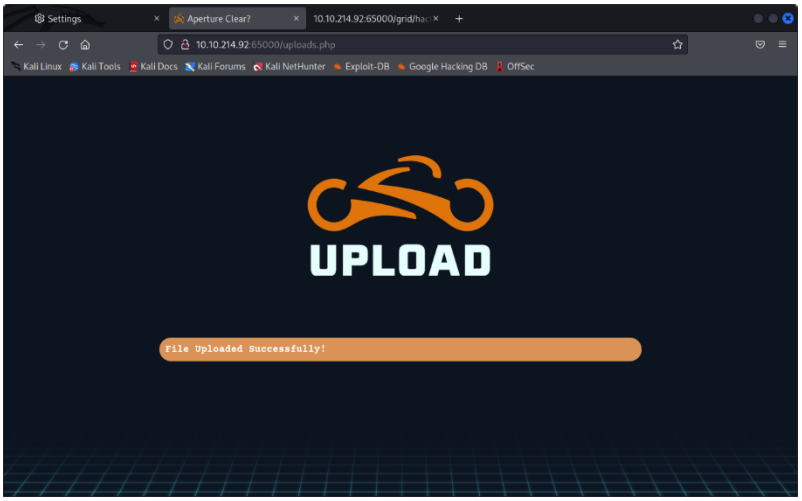

Open Burp Suite, then navigate to the Proxy -> Options tab. Click on the top line in Intercept Client Requests and then select Edit. Delete js from the match condition. ensure Intercept requests based on the following rules is checked.

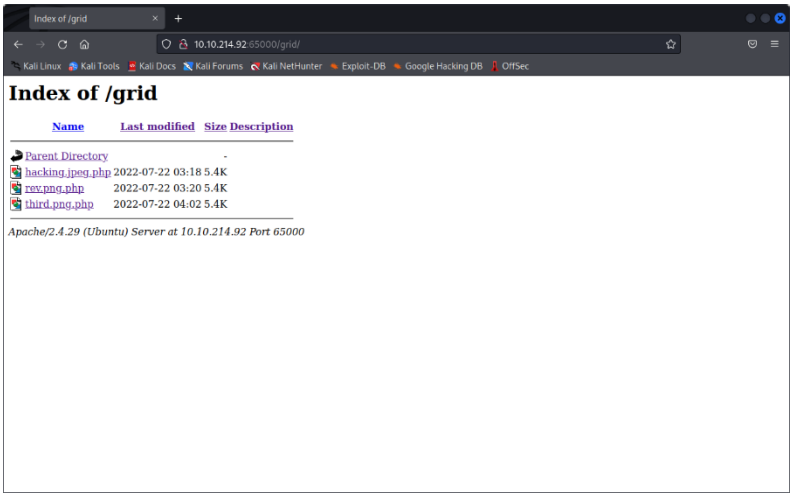


Go to the uploads page and burb suite will automatically intercept. forward requests until you come to one with the URL /assets/js/filter.js and drop it to allow files to be uploaded.

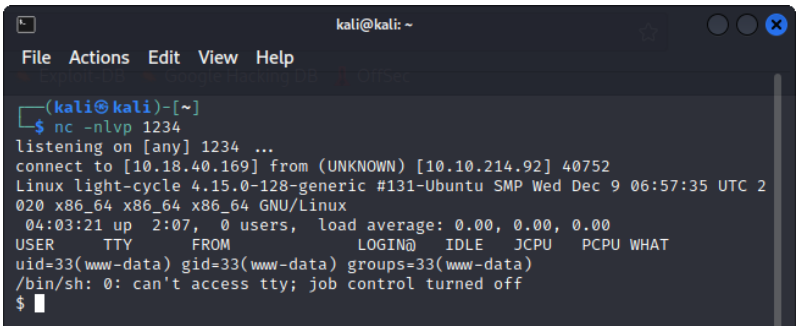



Now that we can upload files, make a php reveres shell and upload it. Once upload success, go to grid page and we will see our php file.



set up a netcat listener nc -nlvp 1234 and click and the file we uploaded on the grid page. Our terminal will be updated.



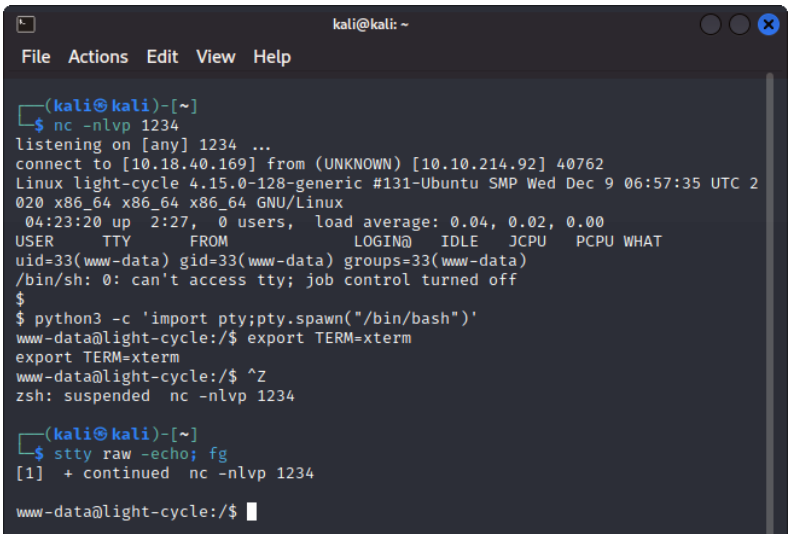

upgrade our shelling using python, and export command, and the stty raw command.

python3 -c 'import pty;pty.spawn("/bin/bash")'

export TERM=xterm

Hit Ctrl + Z

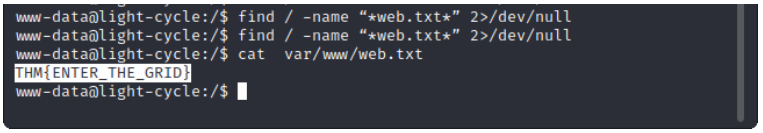
stty raw -echo; fg




Q5: What is the value of the web.txt flag?

Ans : THM{ENTER_THE_GRID}

Using command cat /var/www/web.txt to get the flag.




Q6: What lines are used to upgrade and stabilize your shell?

Ans : python3 -c 'import pty;pty.spawn("/bin/bash")'

Q7: Review the configuration files for the webserver to find some useful loot in the form of credentials. What credentials do you find? username:password

Ans : tron:IFightForTheUsers

Using command cd /var/www/TheGrid/includes and cat dbauth.php to get the password and username.

```
www-data@light-cycle:/$ cd var/www
www-data@light-cycle:/var/www$ cd /var/www/TheGrid/includes/
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbough.php
cat: dbough.php: No such file or directory
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbouth.php
cat: dbouth.php: No such file or directory
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($dbh->connect_error);
        }
?>
www-data@light-cycle:/var/www/TheGrid/includes$
www-data@light-cycle:/var/www/TheGrid/includes$
www-data@light-cycle:/var/www/TheGrid/includes$
```

Q8: Access the database and discover the encrypted credentials. What is the name of the database you find these in?

Ans : tron

We can now access the MySQL client using this login information. We can enter the shell with the command mysql -utron -p and then enter the password when prompted.

```
kali@kali: ~
File  Actions  Edit  View  Help
www-data@light-cycle:/var/www/TheGrid/includes$ mysql -u tron -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 14
Server version: 5.7.32-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement
.

mysql>
```

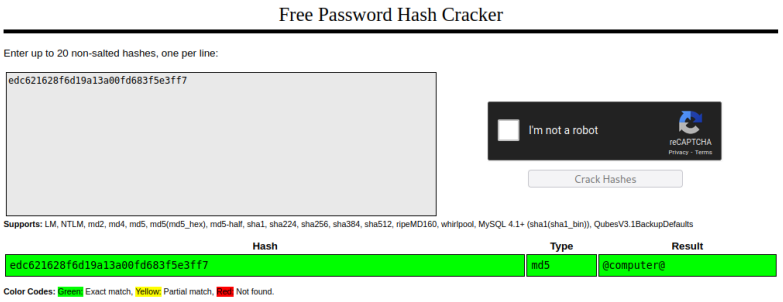
use command show databases; This shows database called tron, select the tron database by using the command use tron; and then list the contents of the users table with SELECT * FROM users;.

```
kali@kali: ~
File  Actions  Edit  View  Help

mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| tron               |
+--------------------+
2 rows in set (0.01 sec)

mysql> use tron;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

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

    →
```

Q9: Crack the password. What is it?

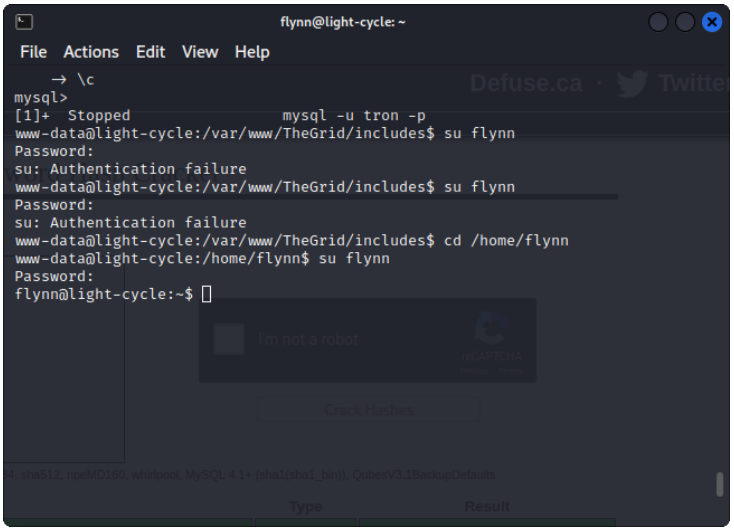
Ans : @computer@

Copy paste the password on https://crackstation.net/ to crack Flynn's password.


Q10: Use su to login to the newly discovered user by exploiting password reuse. What is the user you are switching to?

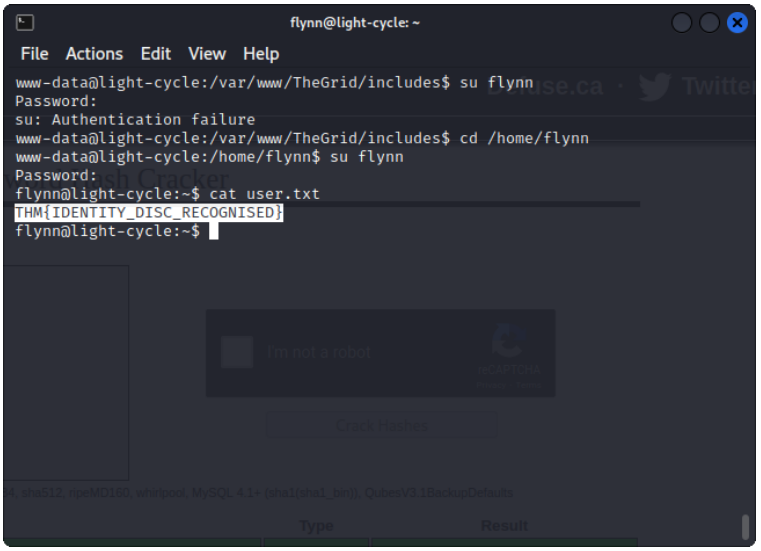
Ans : Flynn



Q11: What is the value of the user.txt flag?

Ans : THM{IDENTITY_DISC_RECOGNISED}

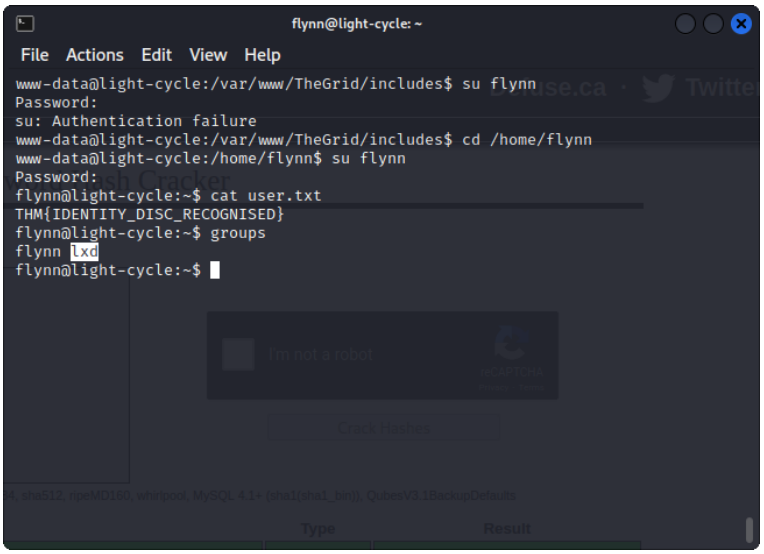
we can get the user flag by moving into the /home/flynn directory and running cat against user.txt




Q12: Check the user's groups. Which group can be leveraged to escalate privileges?

Ans : lxd

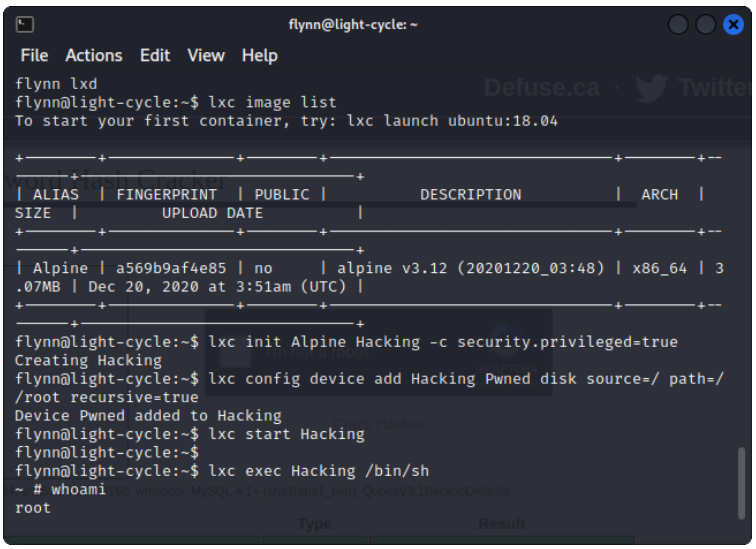
Run groups



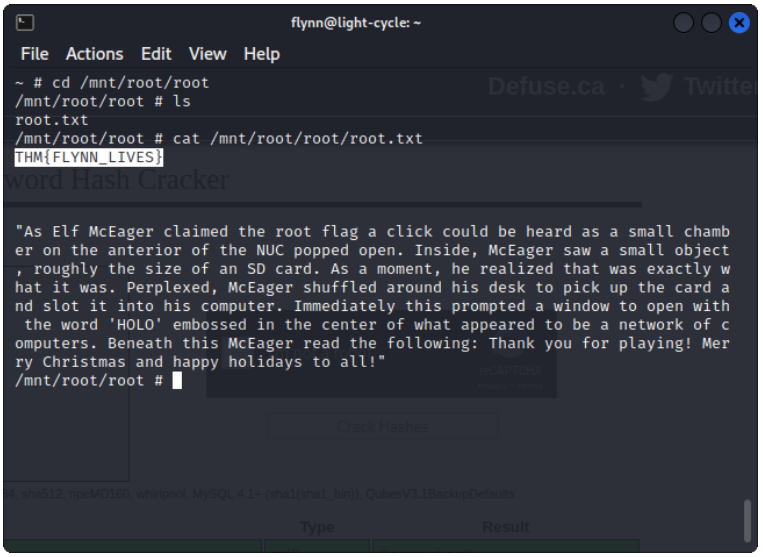
Q13: What is the value of the root.txt flag?

Ans : THM{FLYNN_LIVES}

list the image list by running lxc image list. create our own Image and Container from the template. start a shell within the container to gain root.




we need to cd into our /mnt directory.  We can find the flag at /mnt/root/root/root.txt



**Thought Process/Methodology:**

Day 21 - It's time to expand on our PowerShell talents with some ELForensics. Now, in addition to reading files and navigating the file system, we can also collect file hashes, look into executable files, examine their contents, and perhaps even look for other data streams.Day 22 - Elf McEager becomes CyberElf.  We may RDP into the computer first. We immediately notice this folder on the desktop, and at first inspection, it appears that the name has been Base64-encoded. The CyberChef will be loaded, and we will check it out.  It appears that the Grinch came to visit, and it was Base64. This also serves as the KeePass database's master password. Therefore, let's peek inside. For a security system, an email account, and an elf server, we have users and passwords. Despite being encoded, they were fortunate enough to give us indications in the database's remarks.Day 23- The Grinch makes another attack! In the Blue team tale, we are currently facing a new difficulty. After reading through, it appears that shadow copy HDD volumes and some type of malware are at play. This is nice wallpaper and a RansomeNote text document are displayed when we first open the RDP connection.Day 24 - The Trial Before Christmas.Last challenge/machine looks like it goes from nmap to enumeration, exploitation, privesc and full root access.There are Enumeration to answer question until 4. Then Bypassing Client-Side filter to upload files, we will use Burp Suite in order to bypass the front end filter which determines what files can be uploaded.  Finding the Web Flag in the Shell from question 5.Upgrading and Stabilizing Shell to make our shell more fully featured and resilient. Accessing MySQL Shell to look for a username and password combination from question 6,7 and 8.“In Like Flynn” to answer question 9. And lastly,LXD to Root Shell for question 10.