PSP0201

Week 6

Writeup

Group Name: F4urDeveloper

Members:

ID	NAME	ROLE
1211101242	RAJA FITRI HAZIQ BIN RAJA MOHD FUAD	LEADER
1211104237	ALIA MAISARA BINTI SHAHRIN	MEMBER
1211102287	TERRENCE CHENG	MEMBER
1211101153	MISCHELLE THANUSHA JULIUS	MEMBER

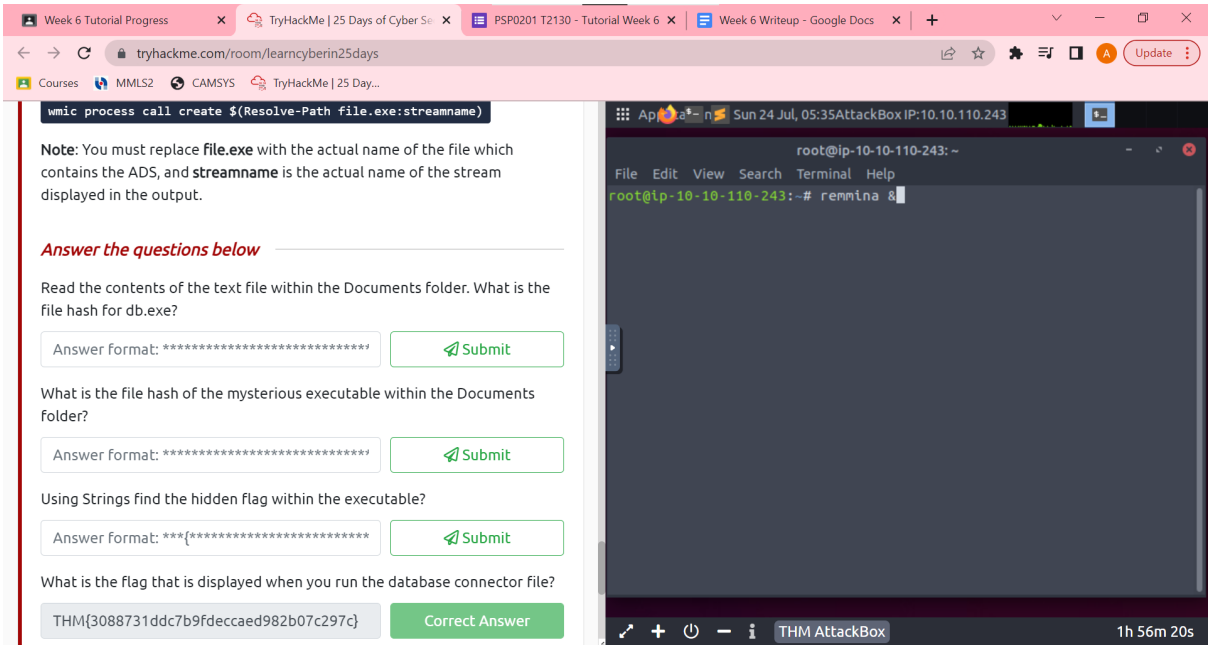
Day 21 - [Blue Teaming] Time for some ELForensics

Tools used: THM AttackBox, Chrome, Remmina

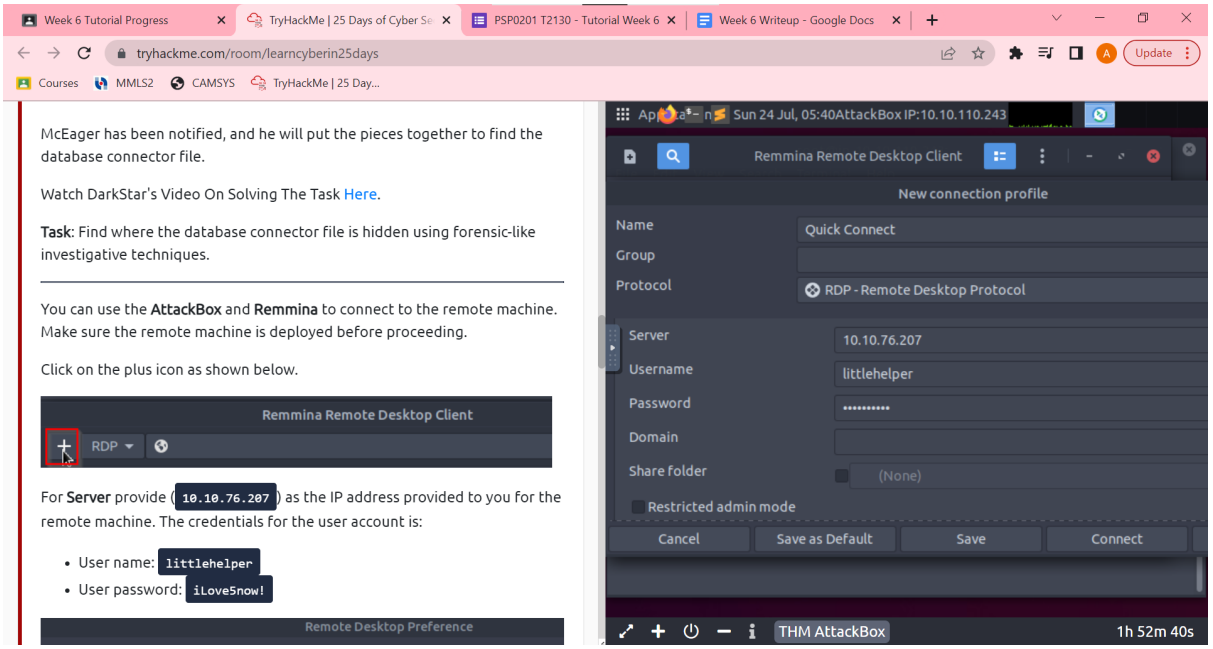
Solution/Walkthrough:

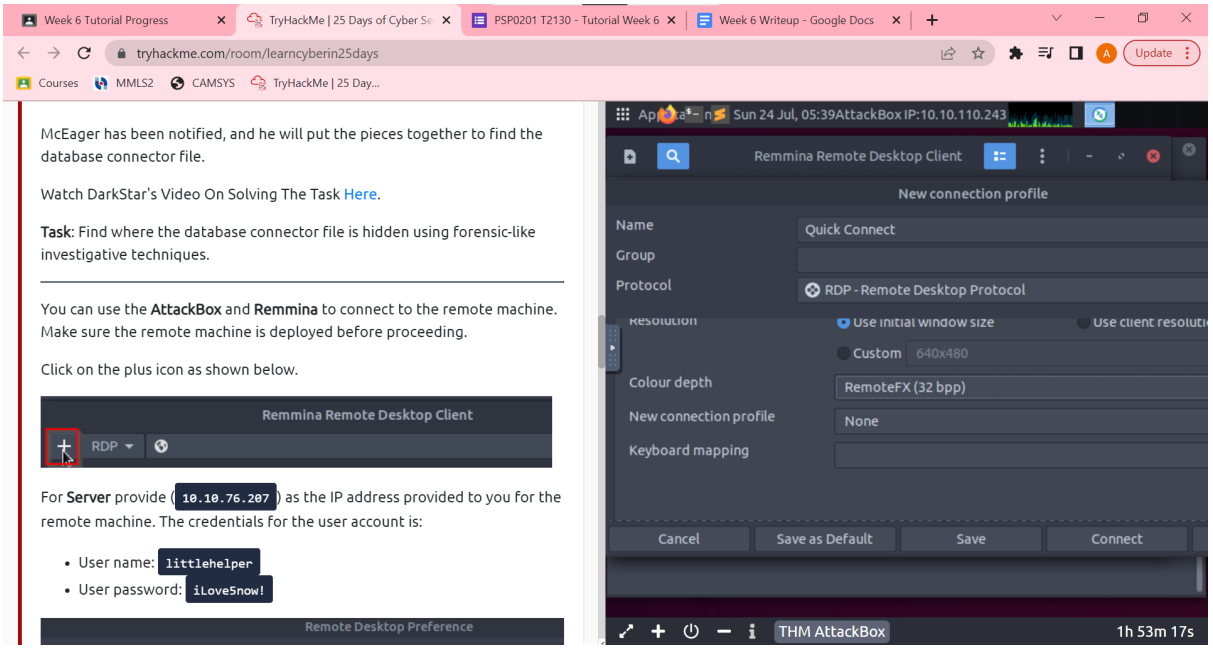
Q1: Read the contents of the text file within the Documents folder. What is the file hash for db.exe?

Open remmina

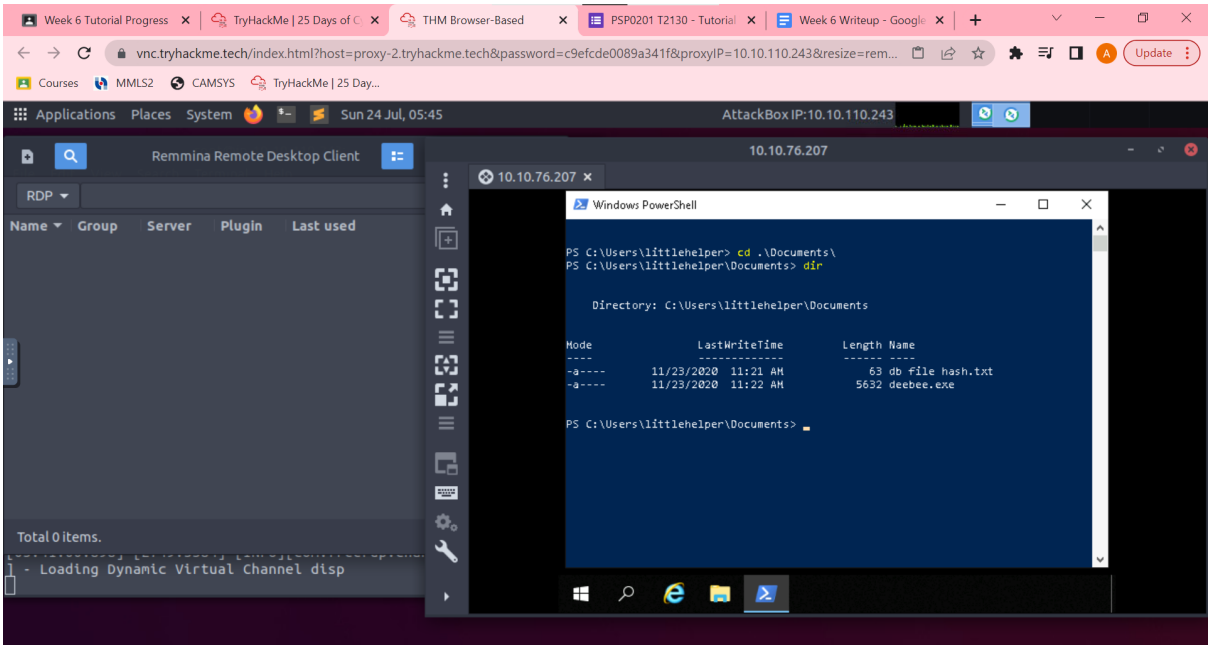


Fill in the server, username, and password and change the colour depth to RemoteFX(32 bpp). Save and connect.

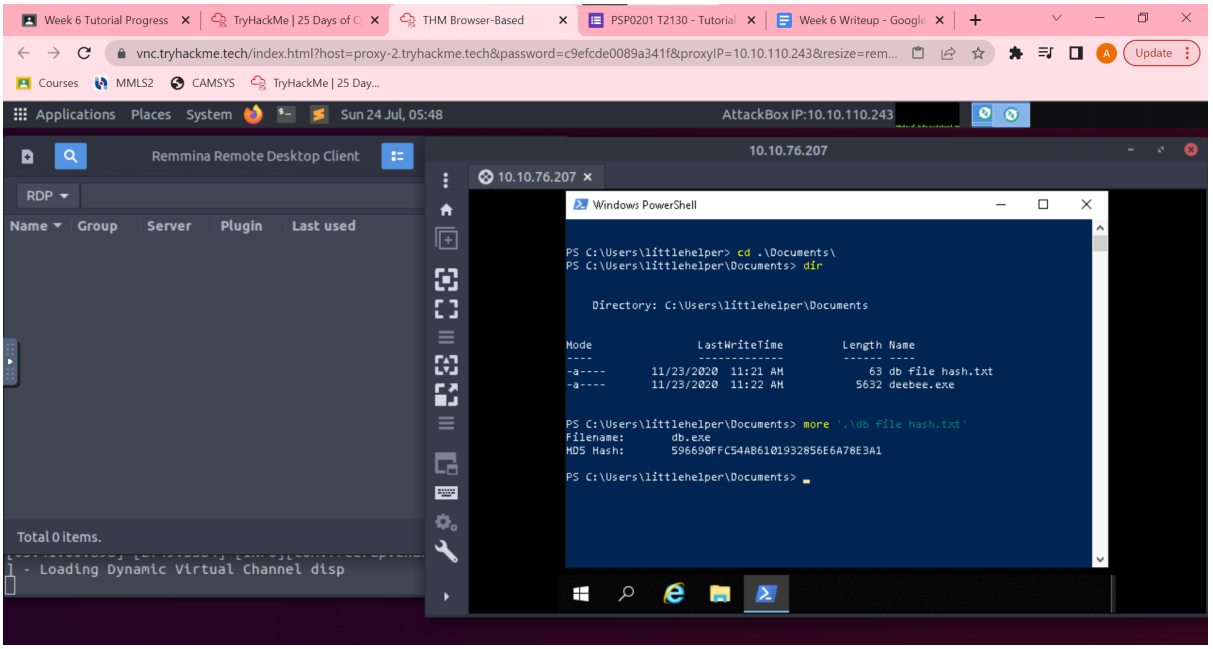




Open PowerShell and open Documents directory

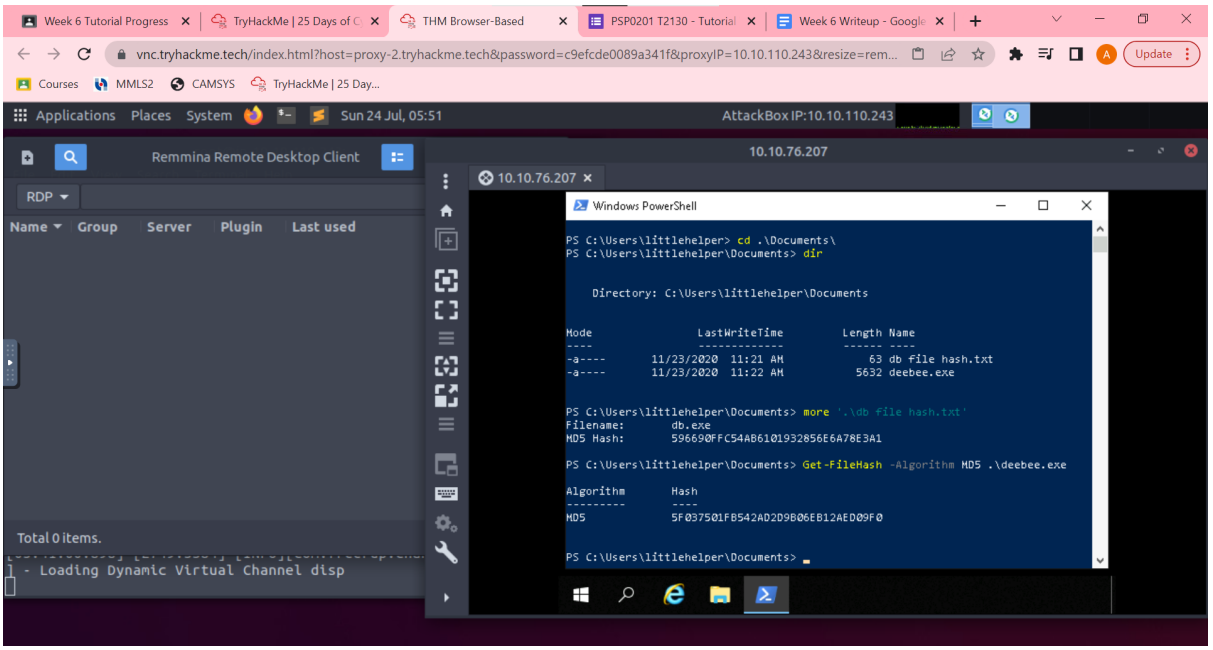


The file hash for db.exe is 596690FFC54AB6101932856E6A78E3A1



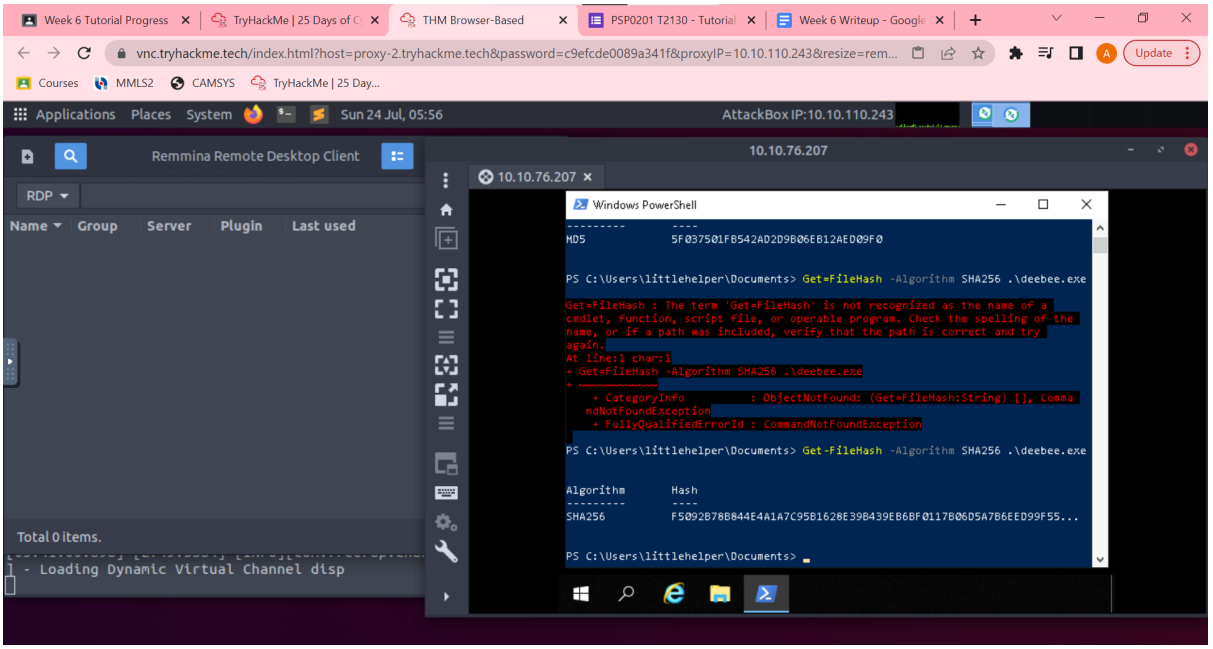
Q2: What is the MD5 file hash of the mysterious executable within the Documents folder?

Use Get-FileHash -Algorithm MD5 .\deebee.txt to get the file hash. The hash is 5F037501FB542AD2D9B06EB12AED09F0



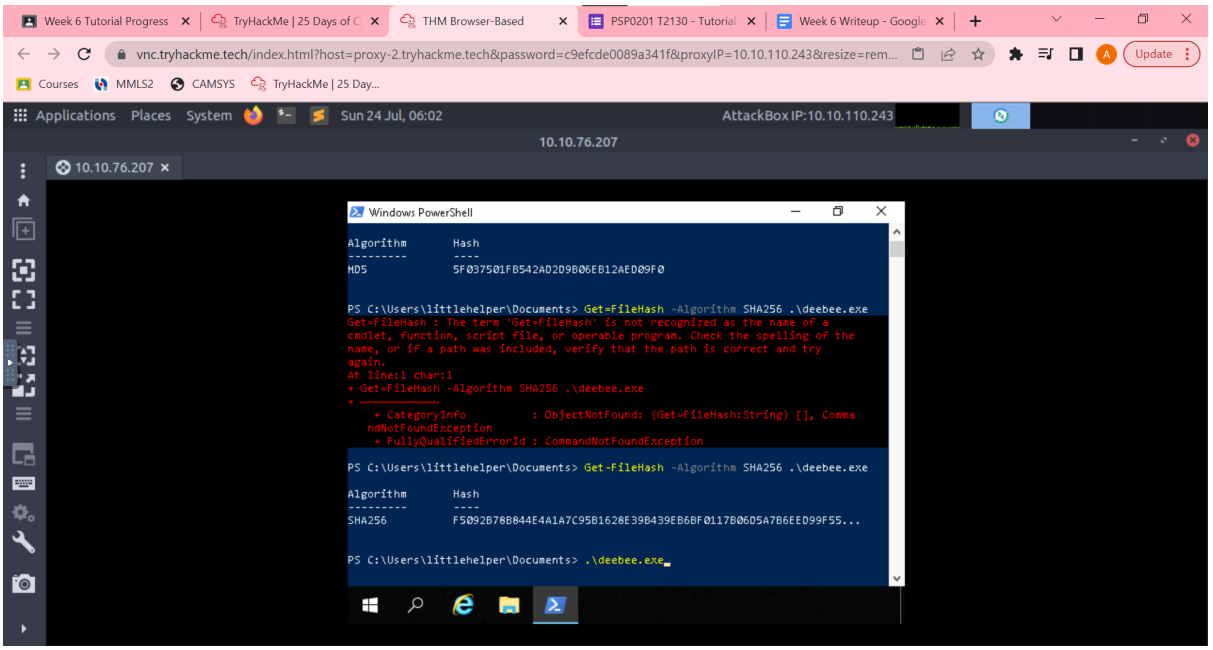
Q3: What is the SHA256 file hash of the mysterious executable within the Documents folder?

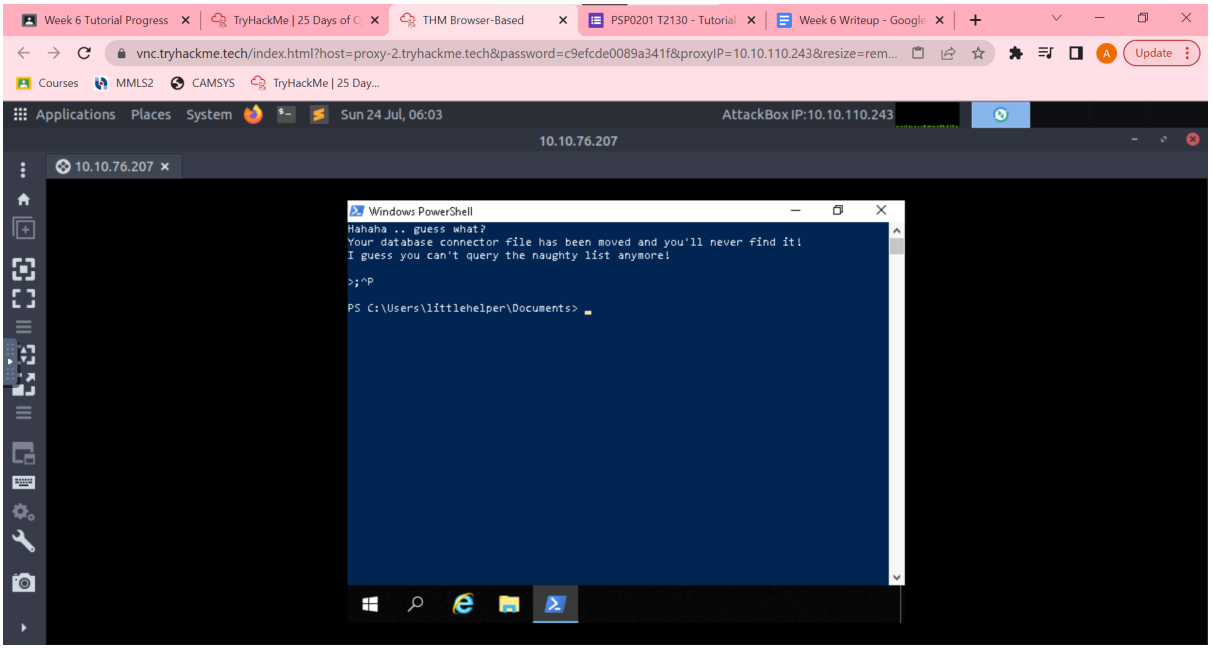
Use Get-FileHash -Algorithm SHA256 .\deebee.exe to get the file hash. The hash is F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F55...



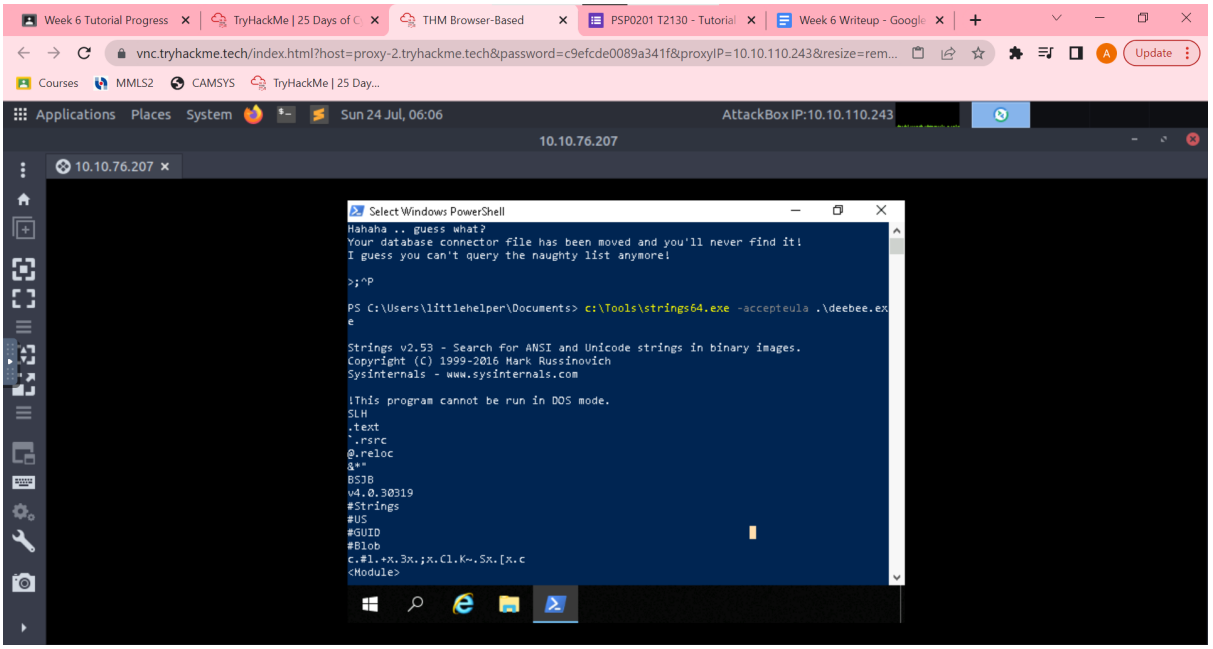
Q4: Using Strings find the hidden flag within the executable?

Open deebee.exe file

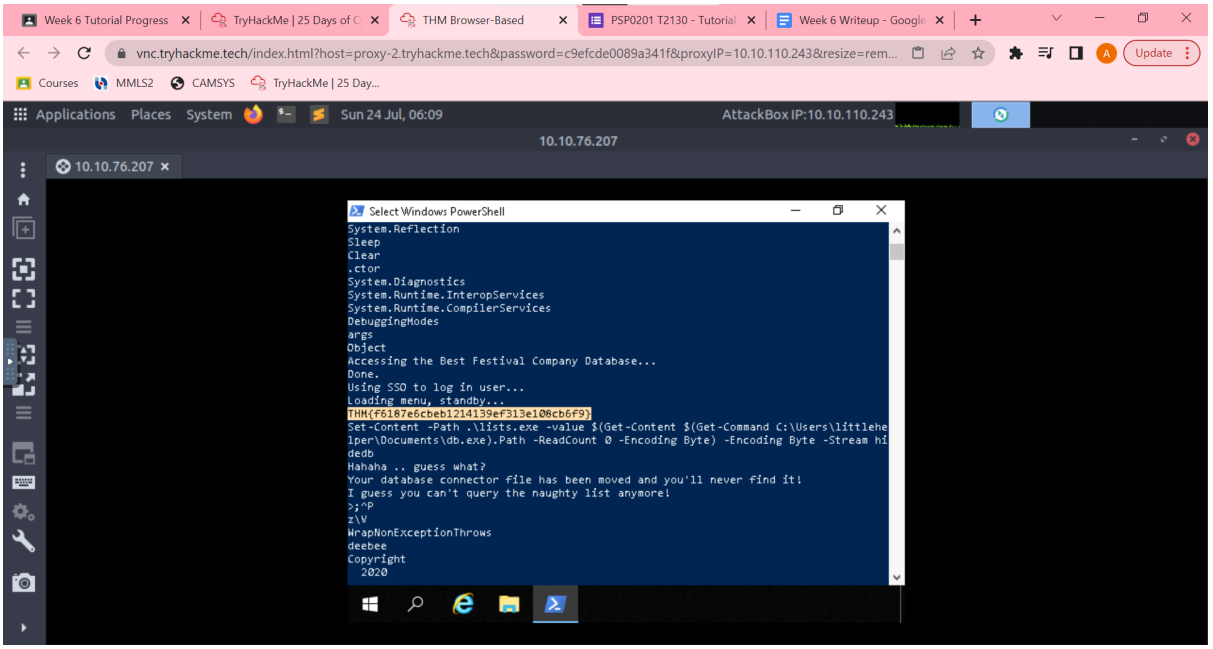




Use c:\Tools\strings64.exe -accepteula .\deebee.exe to scan the file

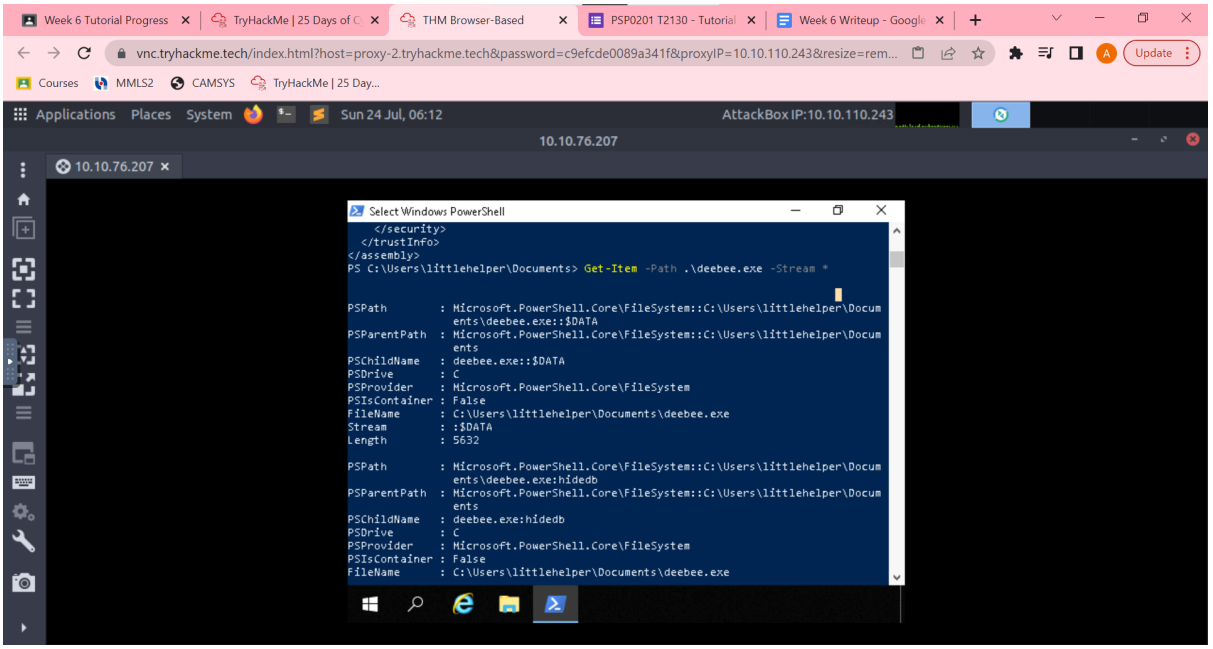


The flag is THM{f6187e6cbeb1214139ef313e108cb6f9}



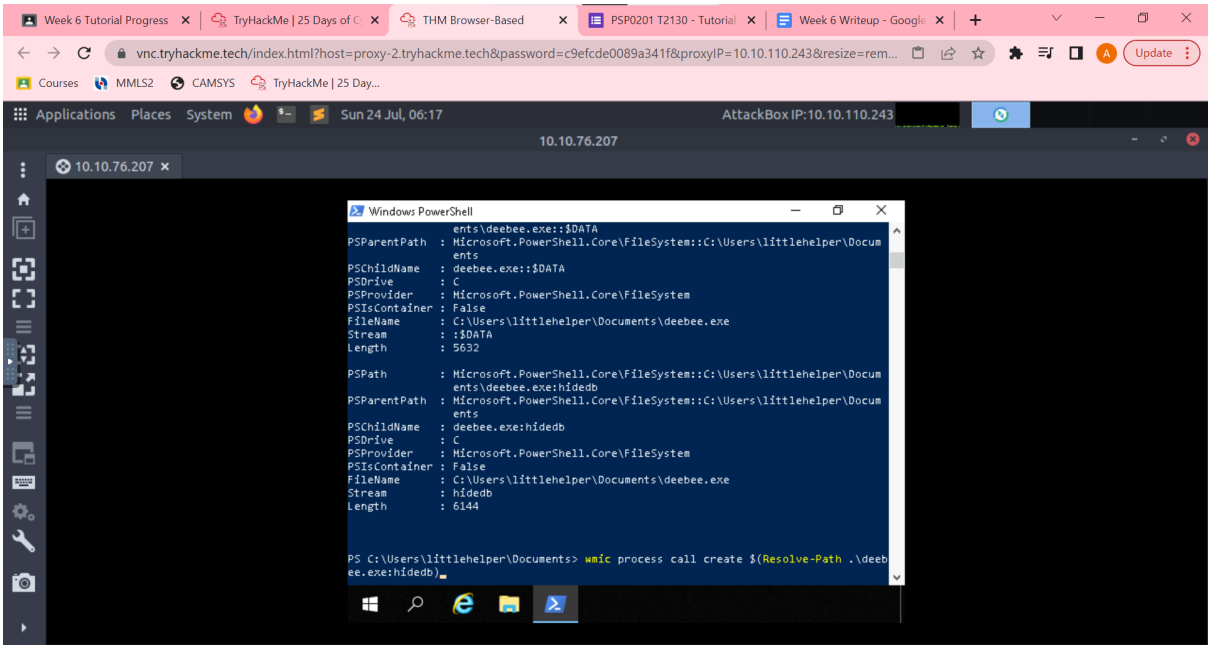
Q5: What is the powershell command used to view ADS?

The command is Get-Item -Path .\deebee.exe -Stream *

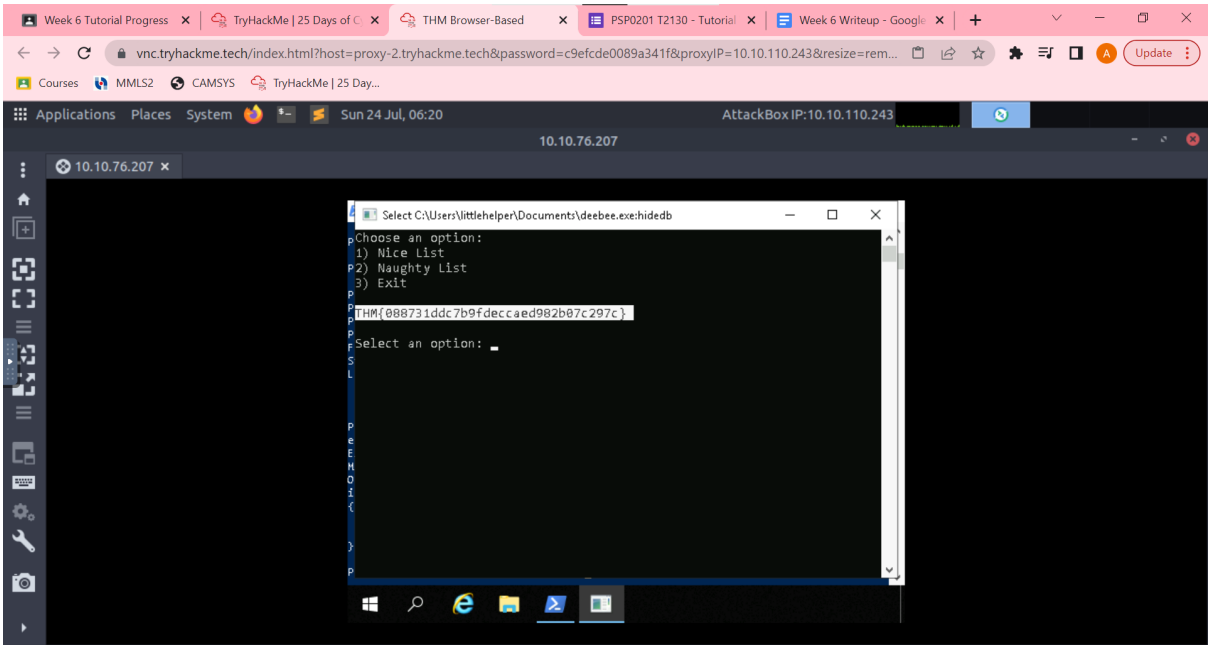


Q6: What is the flag that is displayed when you run the database connector file?

Launch the hidden executable hiding within ADS

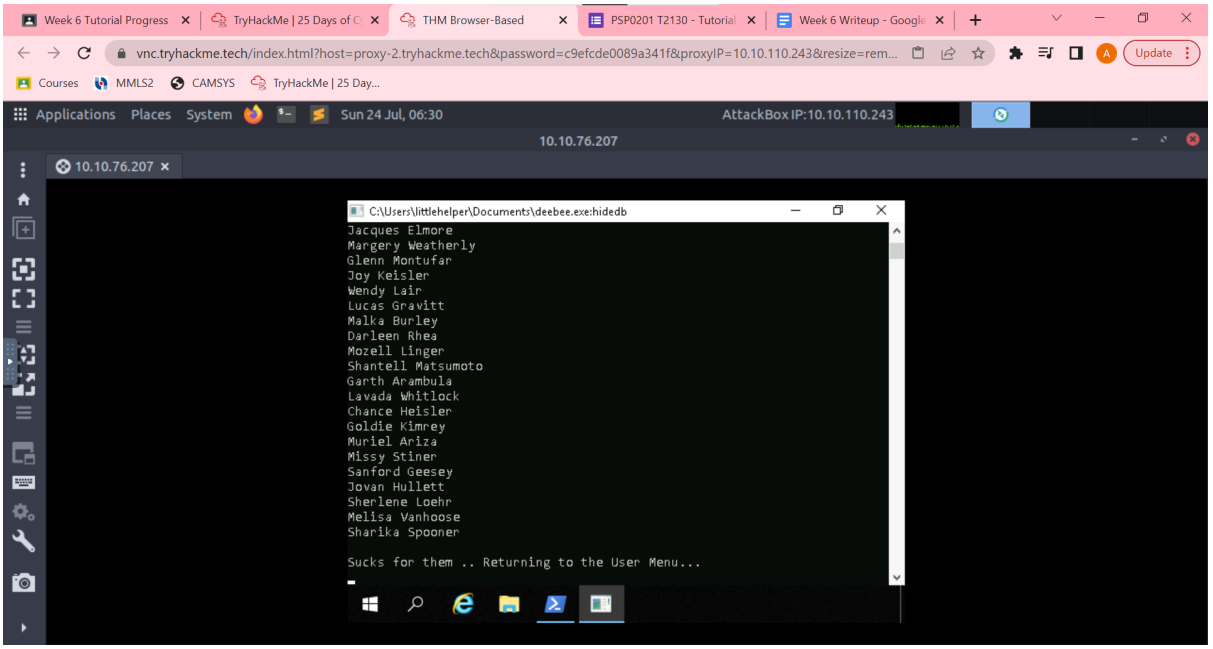


The flag is THM{088731ddc7b9fdeccaed982b07c297c}



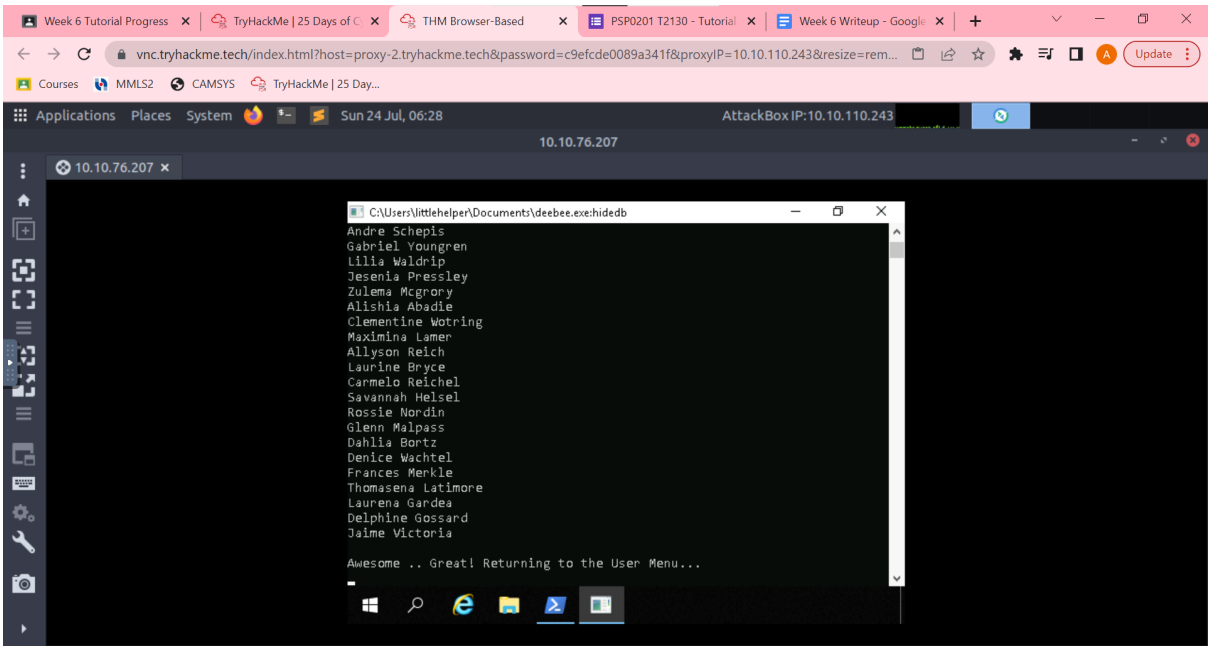
Q7: Which list is Sharika Spooner on?

Naughty list



Q8: Which list is Jaime Victoria on?

Nice list



Thought Process/Methodology:

Remmina can be used to connect to other servers as long as we have the IP Address, username and password. After connecting to the server, we opened Documents by using PowerShell. After we know the file name that exists in the directory, we can use the more command to read the file named db file hash.txt. By doing that, we can easily know the file that exists in the file which is db.exe and the MD5 hash. After that, we find the MD5 Hash for the other file in Documents directory which is deebee.exe. By comparing the two MD5 Hash,

we can know whether the file is authentic or not. After knowing that deebee.exe is not authentic, we opened the file only to find out that the file has been moved to somewhere else. To snoop around the file, we use the Strings tools to know where the file has been moved to. After that, we view Alternate Data Streams (ADS) and find the stream name to execute the hidden file. After we get the stream name and file name, we launch the hidden file and run the program.

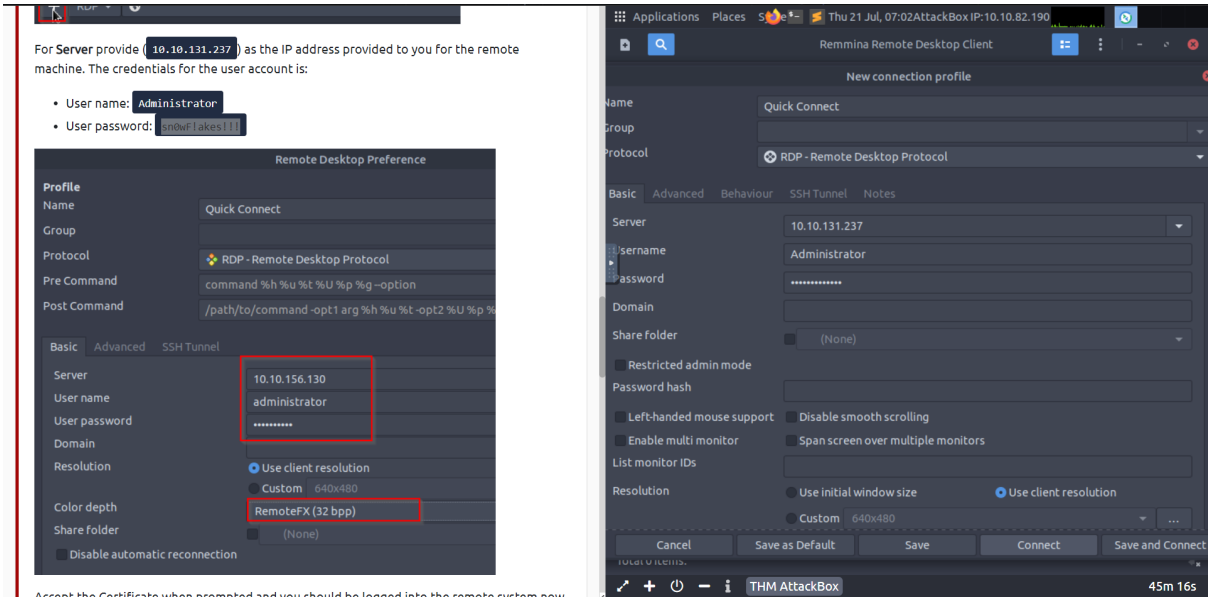
[Day 22] **Blue Teaming** Elf McEager becomes CyberElf

Tools used: THM AttackBox, Cyberchef, Remmina

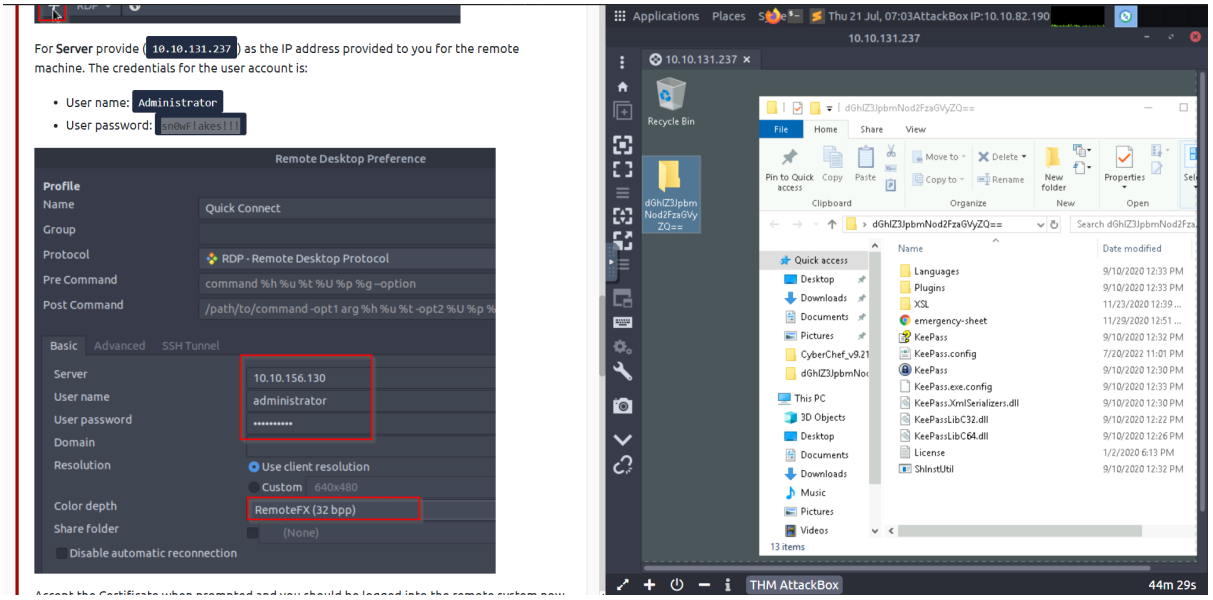
Solution/Walkthrough:

Q1: What is the password to the KeePass database?

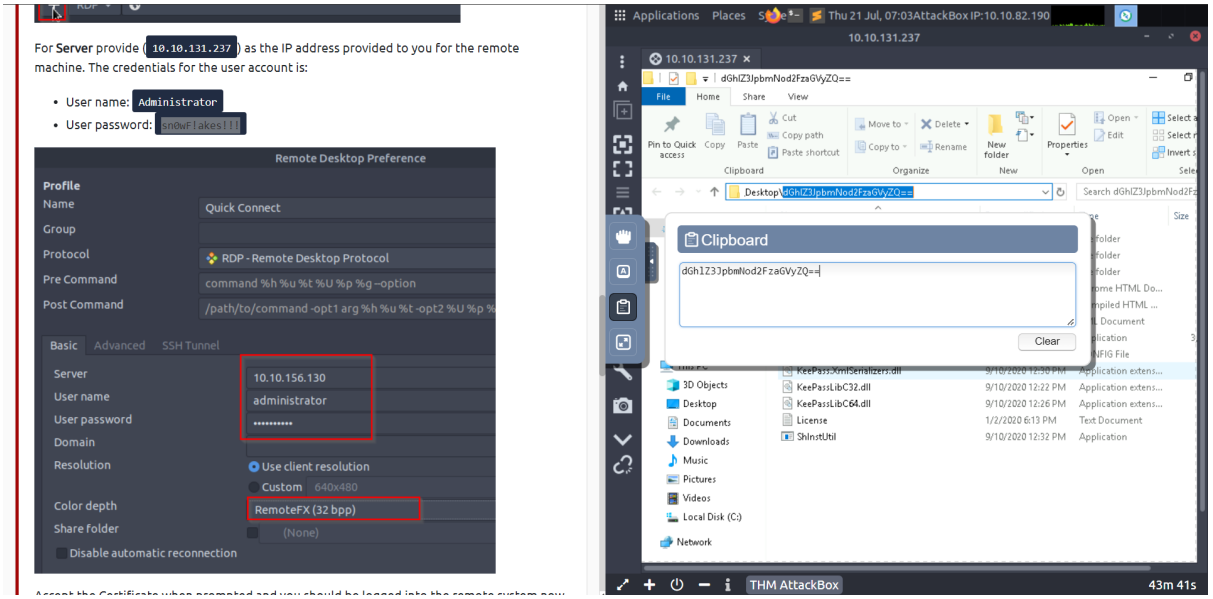
Insert the given IP address, username and password into Remmina on the Attackbox. Change the resolution to “use client resolution” and the colour depth to “RemoteFX (32 bpp)”.



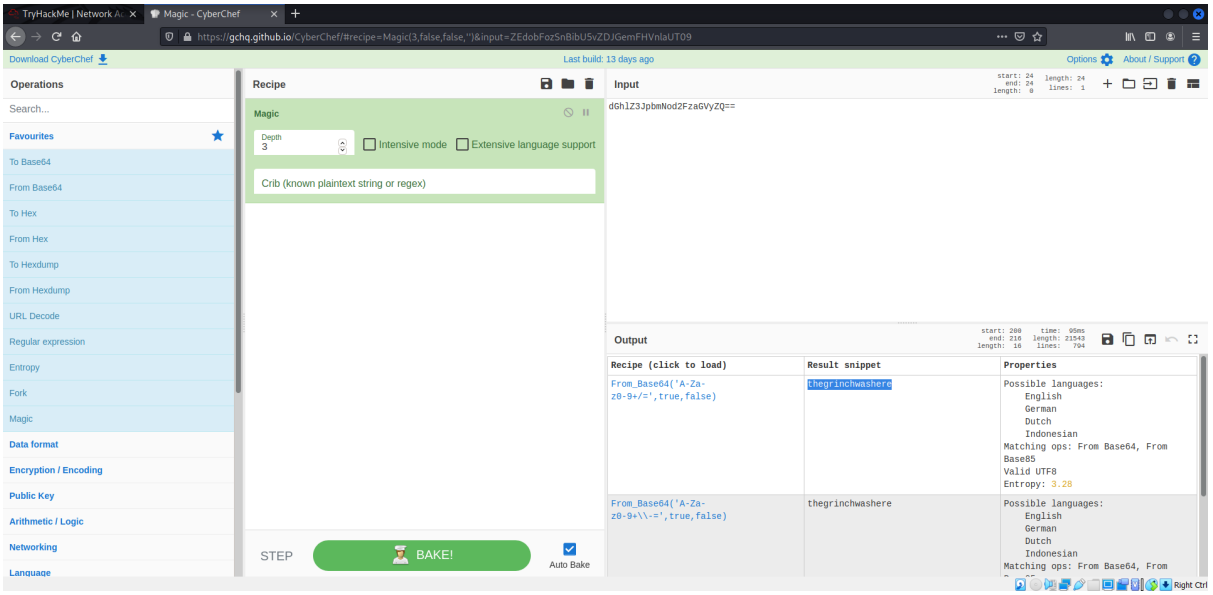
Double-click the yellow folder after accessing the server.



Copy the folder's name and paste it into the clipboard.



Open Cyberchef and paste in the copied folder's name. Use "Magic" as the recipe and the password should be "thegrinchwashere" as highlighted in the image below.



Q2; What is the encoding method listed as the 'Matching ops'?

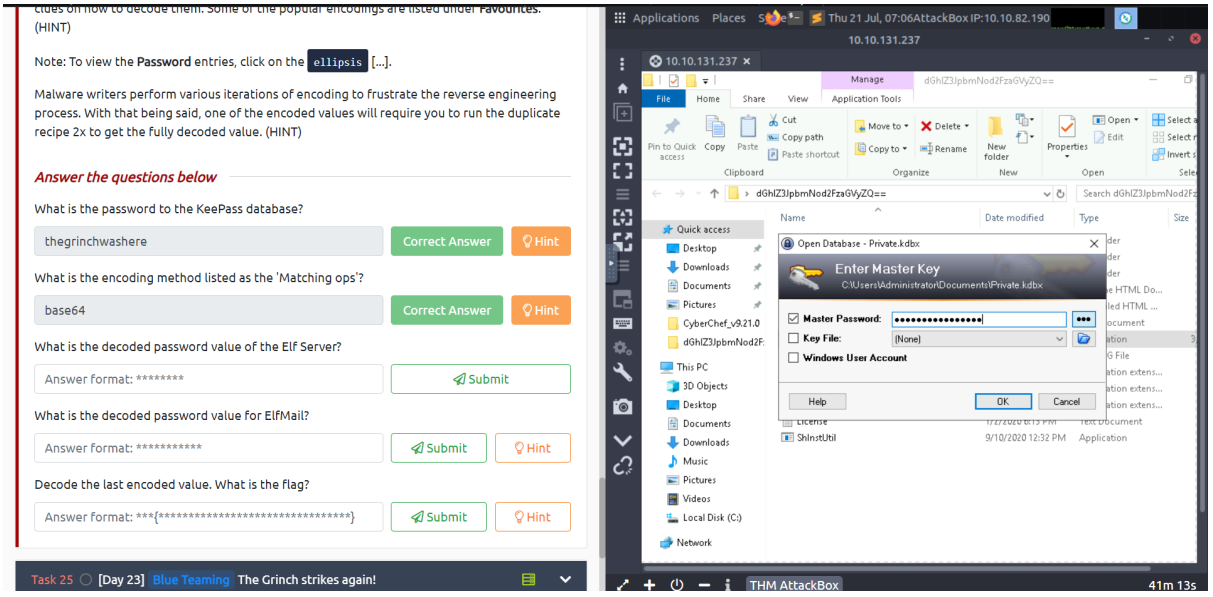
The encoding method listed is highlighted in the image below. The answer should be "**Base64**"

Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+/=',true,false)	thegrinchwashere	Possible languages: English German Dutch Indonesian Matching ops: From Base64, From Base85 Valid UTF8 Entropy: 3.28
From_Base64('A-Za-z0-9+\\-=',true,false)	thegrinchwashere	Possible languages: English German Dutch Indonesian Matching ops: From Base64, From

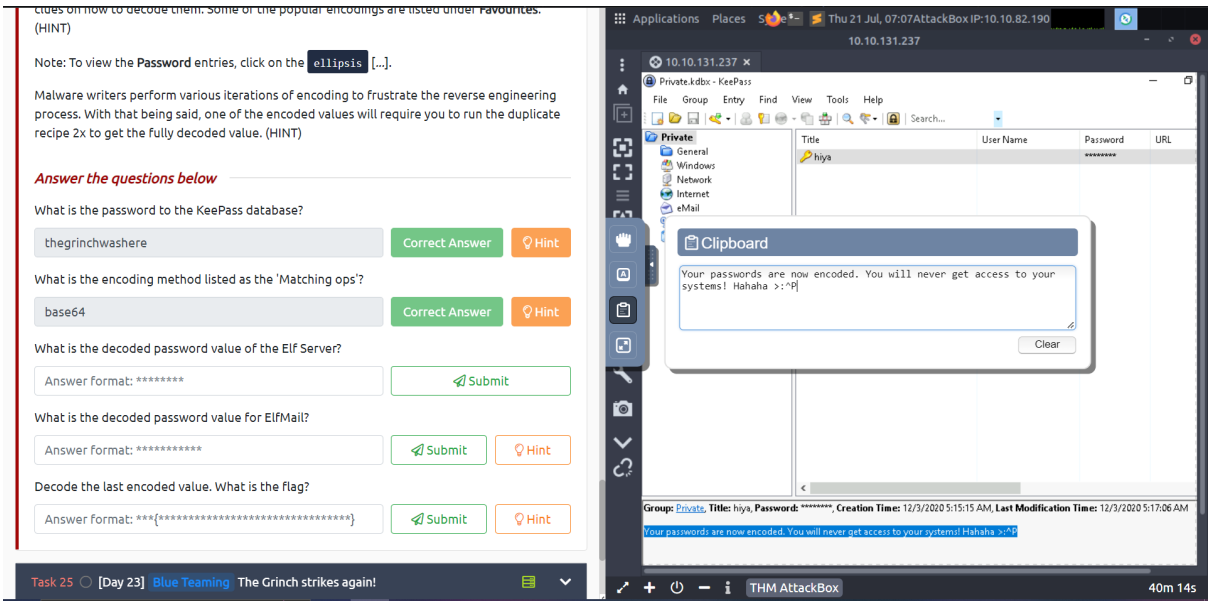
Right Ctrl

Q3: What is the note on the hiya key?

After obtaining “thegrinchwashere” as the password for Keypass. Type it in the “Master Password” section and press “OK”.

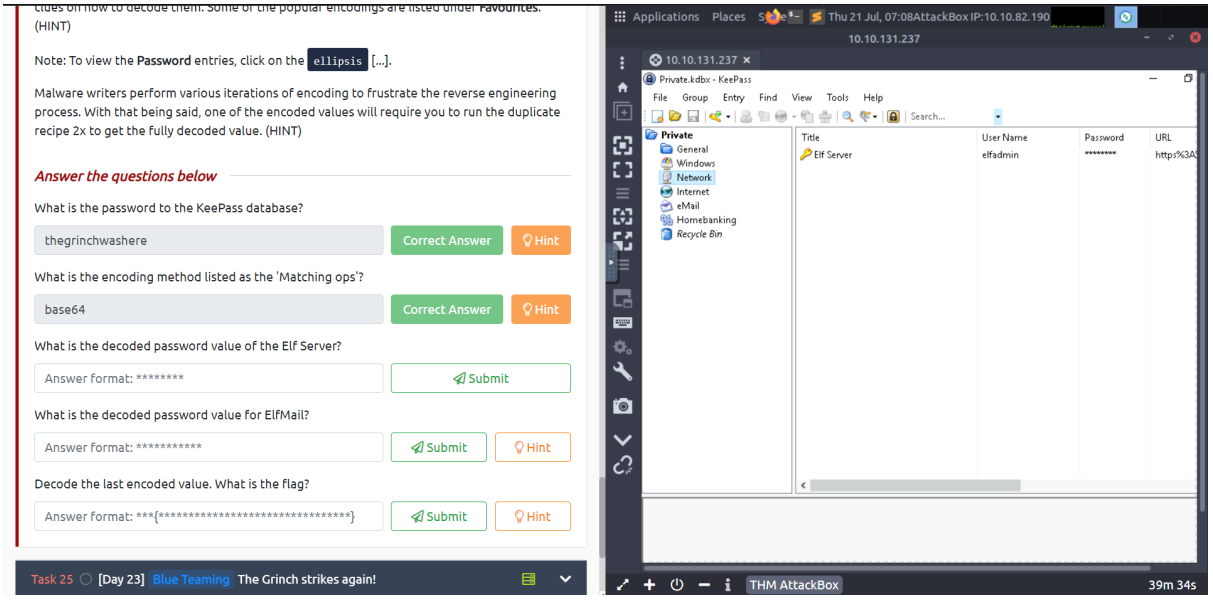


The first thing that should pop up is the Keypass for “hiya”. The note on the hiya key can be found at the bottom of the page as highlighted below. The answer should be “**Your passwords are now encoded. You will never get access to your systems! Hahaha >:^P**”

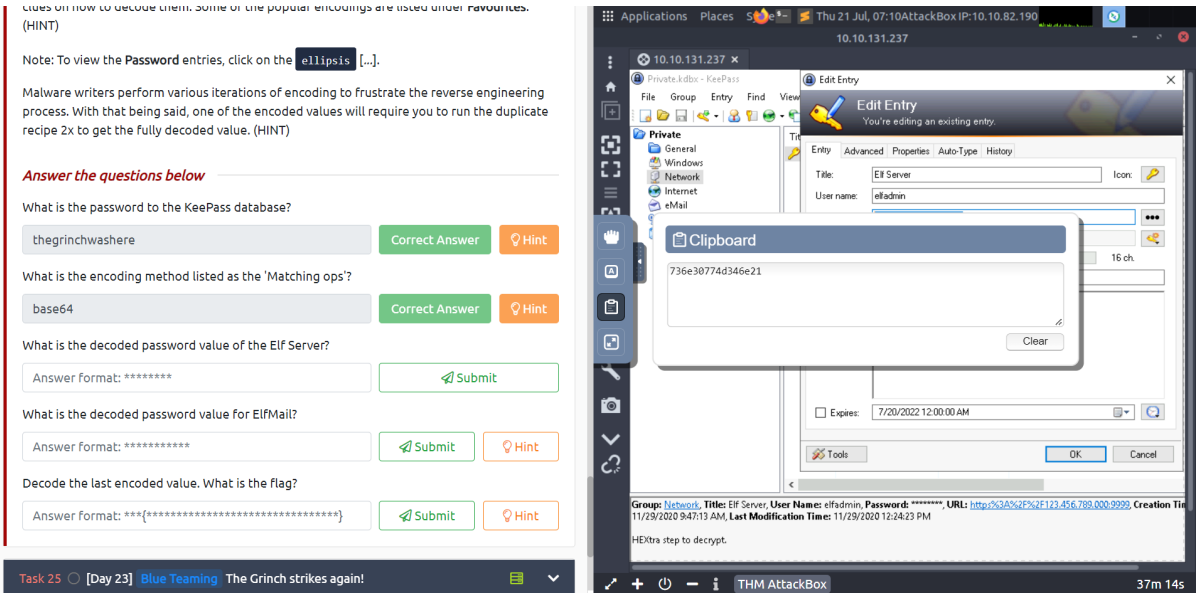


Q4: What is the decoded password value of the Elf Server?

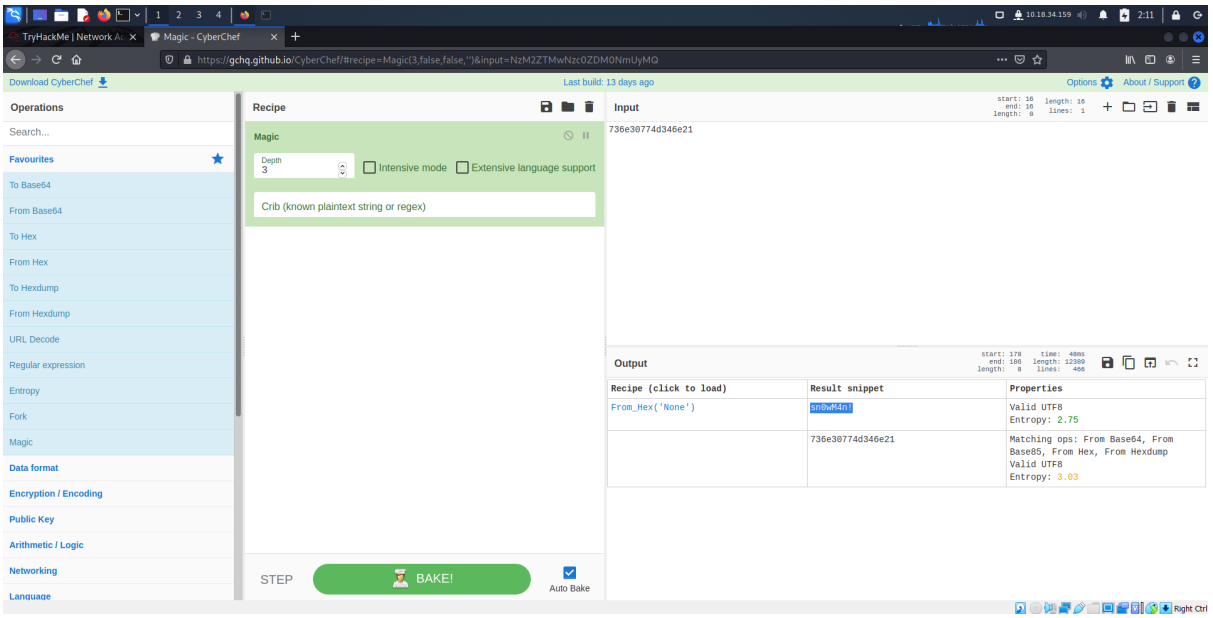
Click the “Network” option to find Elf Server.



Double-click the “Elf Server” option to obtain the encoded password. Click the “...” icon, copy the password and paste it into the clipboard.

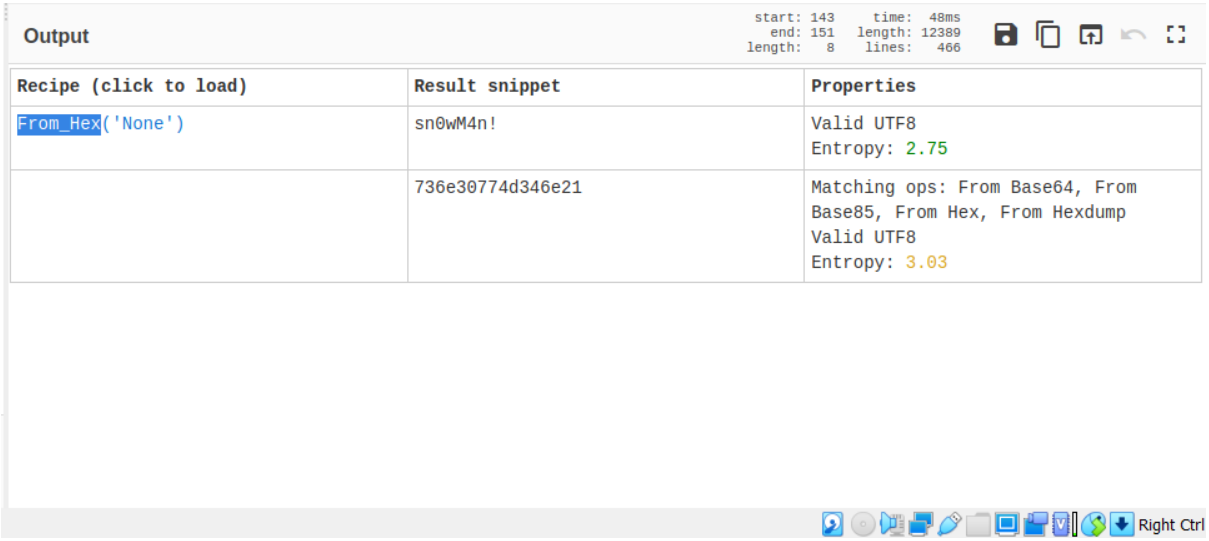


Go into Cyberchef and paste in the password. Using “Magic” for the recipe, the password should be decoded as shown in the image below. The answer should be “**sn0wM4n!**”



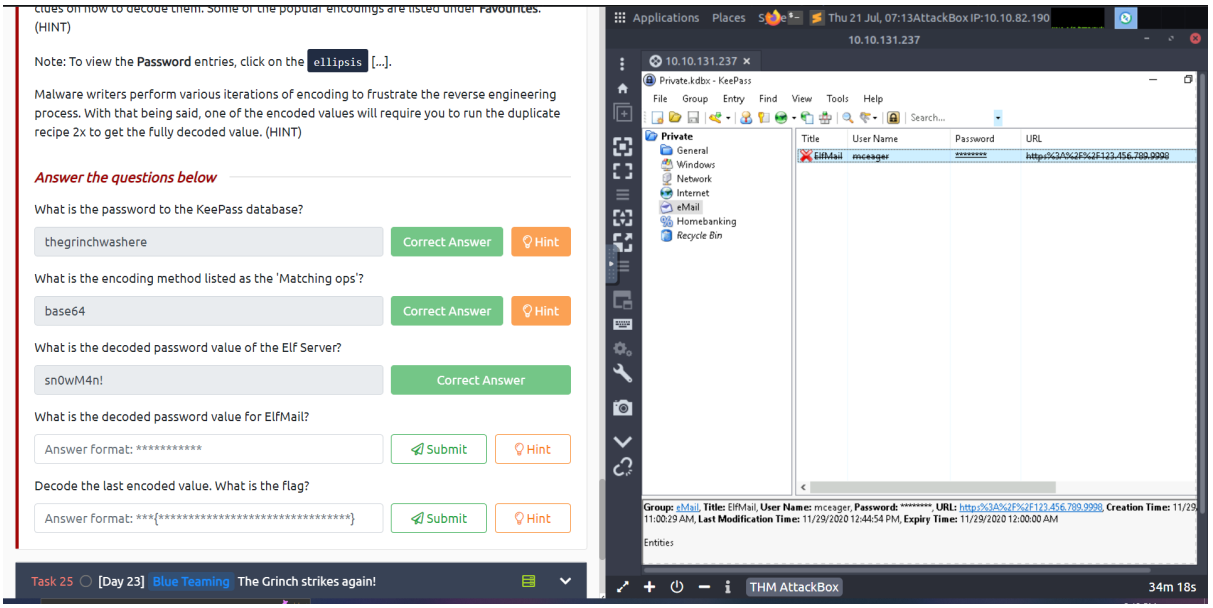
Q5: What was the encoding used on the Elf Server password?

The encoding used should be “**Hex**” as shown in the image below.

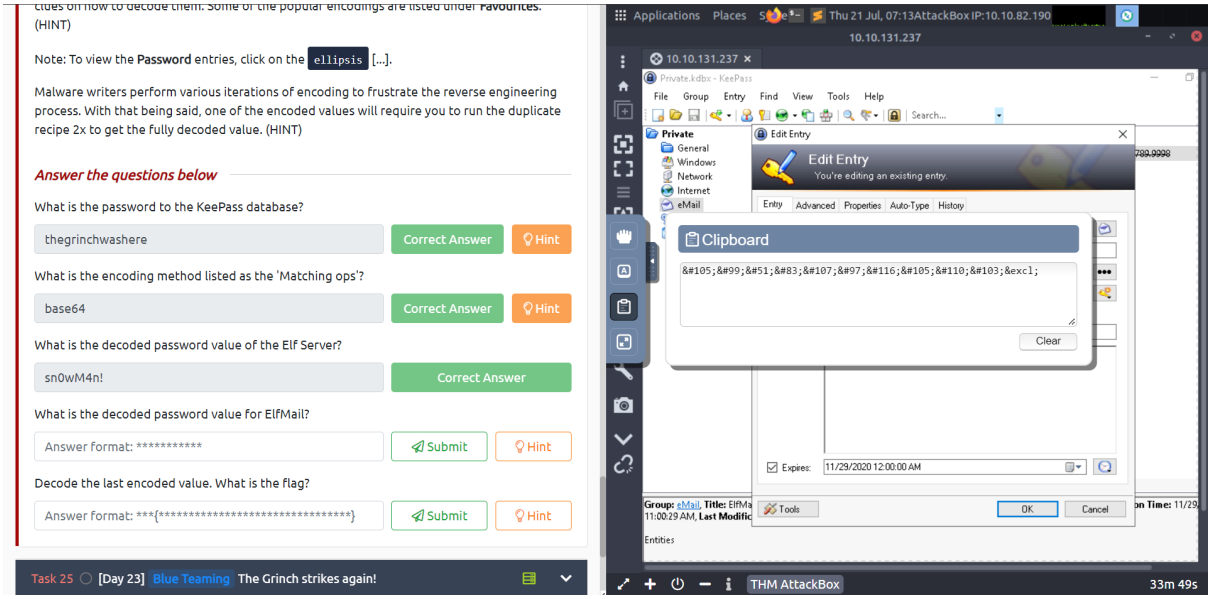


Q6: What is the decoded password value for ElfMail?

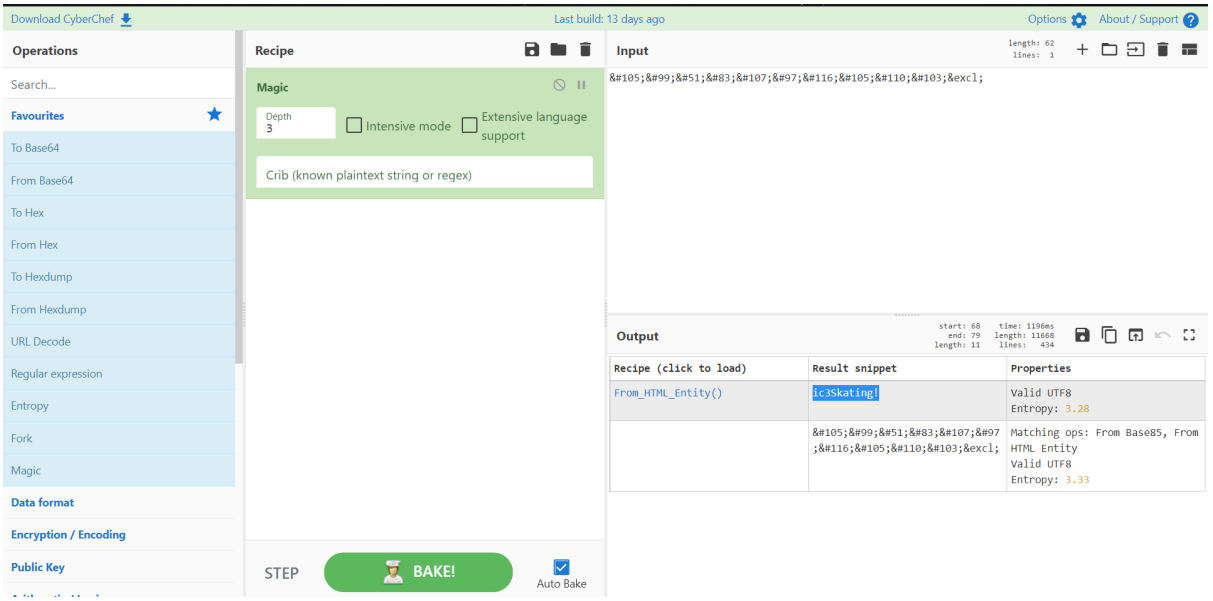
Click the “eMail” option to find Elfmail.



Double-click the “Elmail” option to obtain the encoded password. Click the “...” icon, copy the password and paste it into the clipboard.

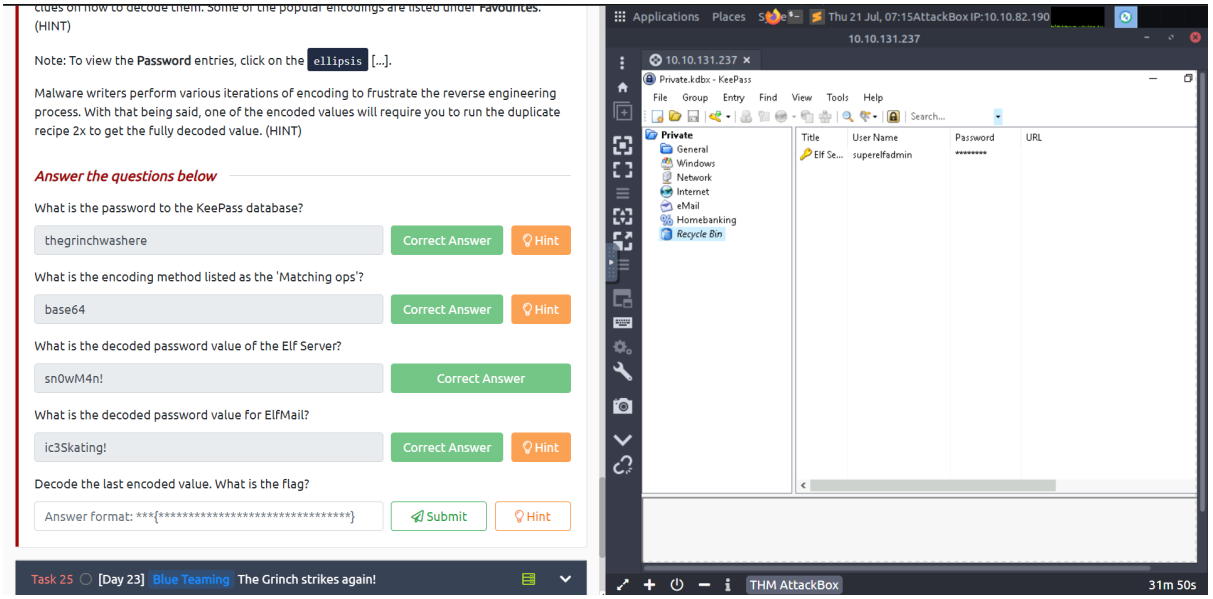


Go to Cyberchef and paste in the copied password. Using “Magic” for the recipe, the answer should be as shown in the image below. The answer should be “**ic3Skating!**”

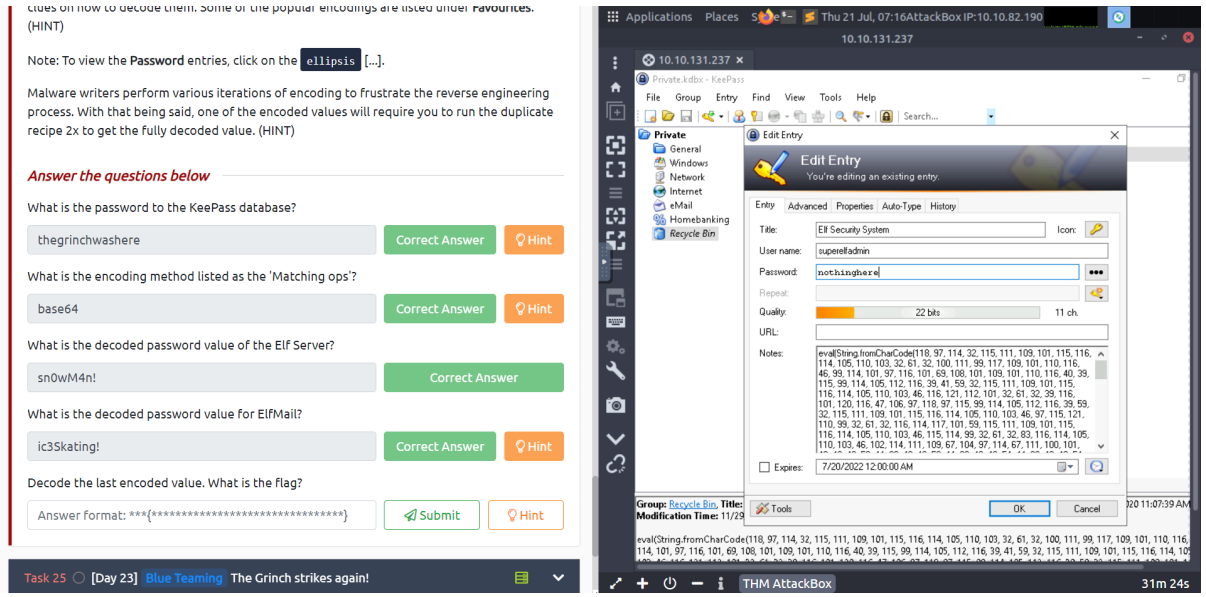


Q7: What is the username:password pair of Elf Security System?

Click the “Recycle Bin” option to find Elf Security System.

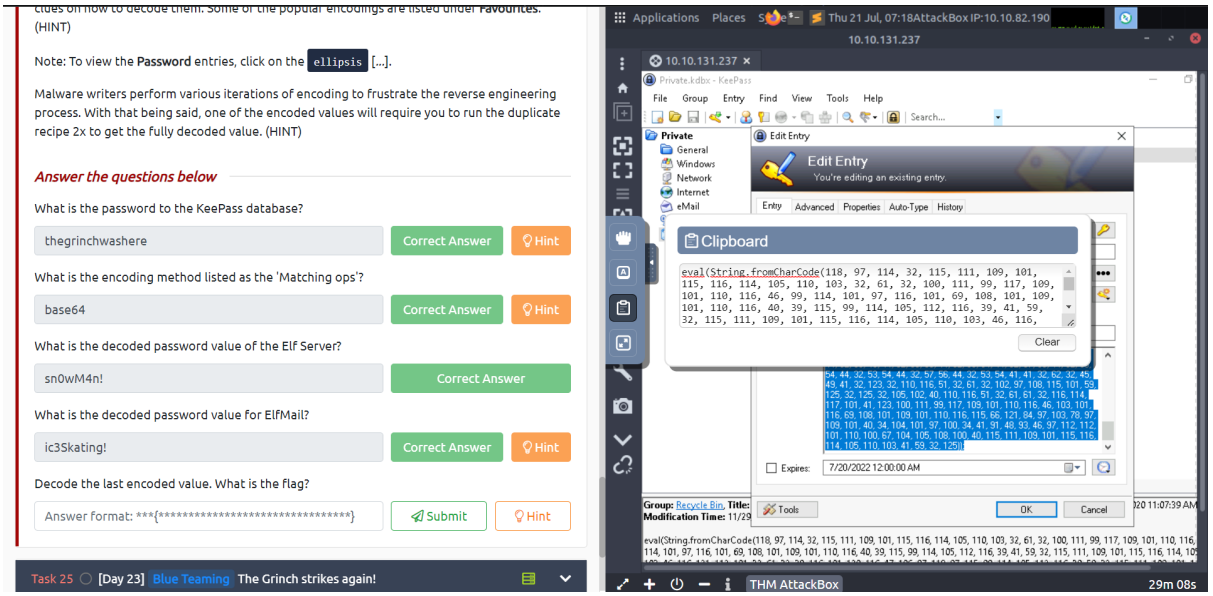


Double-click the “Elf Security System” option to obtain the username and the password. The answer should be as follows, “**superelfadmin:nothinghere**”

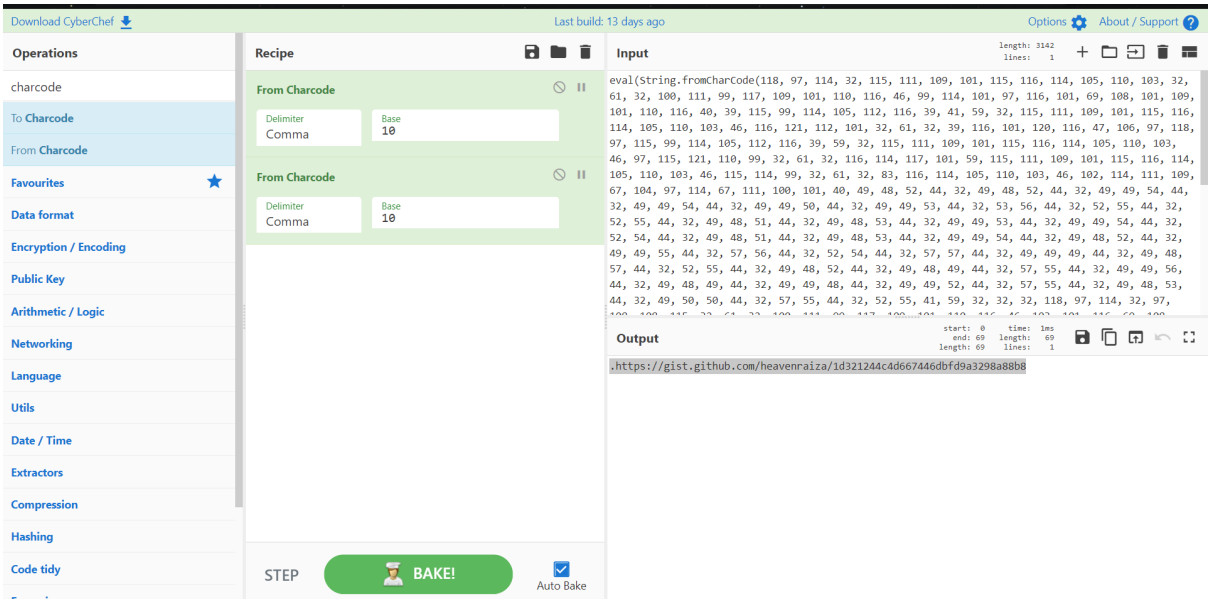


Q8: Decode the last encoded value. What is the flag?

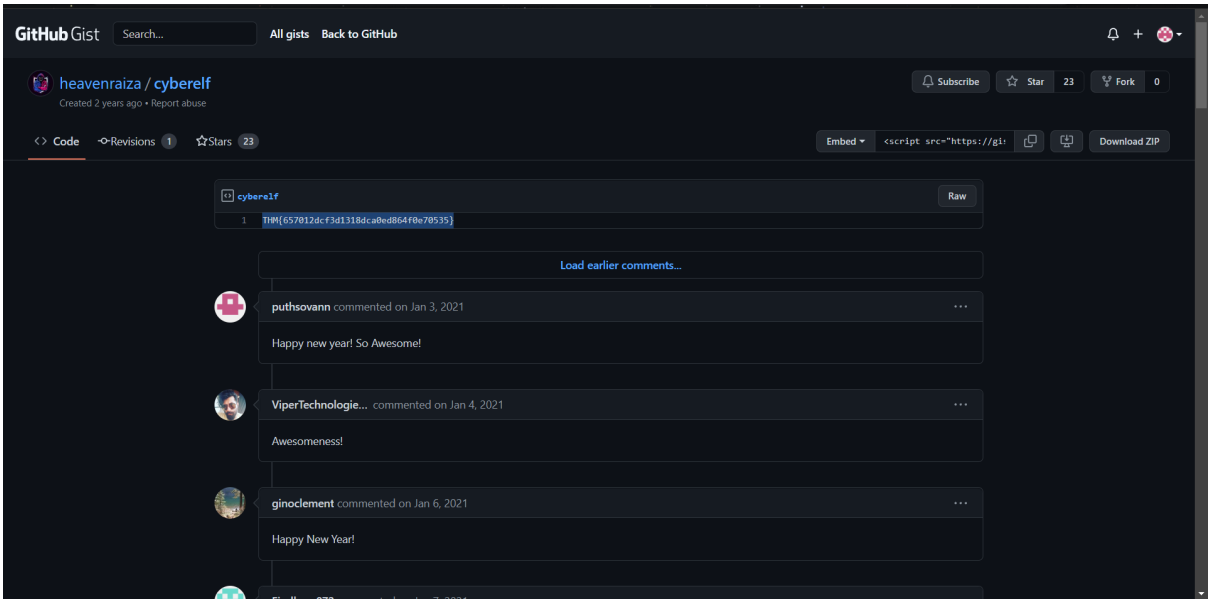
Continuing the work from the previous question, copy the encoded value as highlighted in the image below and paste in into the clipboard.



Go into Cyberchef to decode the value. Follow the hint given by THM to obtain the website which should show us the flag.



The website should show a github profile with the following flag "**THM{657012dcf3d1318dca0ed864f0e70535}**"



Thought Process/Methodology:

For Question 1, insert the given IP Address, username and password into Remmina on the Attackbox. Change the resolution to "use client resolution" and the colour depth to "RemoteFX (32 bpp)". After doing so, double click the yellow folder after accessing the server. Copy the folder's name and paste it into the clipboard. Continue your work by opening Cyberchef and paste in the copied folder's name. Use "Magic" as the recipe and the password should be "thegrinchwashere". For Question 2, the encoding method can be found at the same time after obtaining the password, it should be "Base64" as stated in the left side of the password. For Question 3, log into Keypass by using "thegrinchwashere" as the password. The first thing that should pop up is the keypass for ""hiya". The note on the hiya

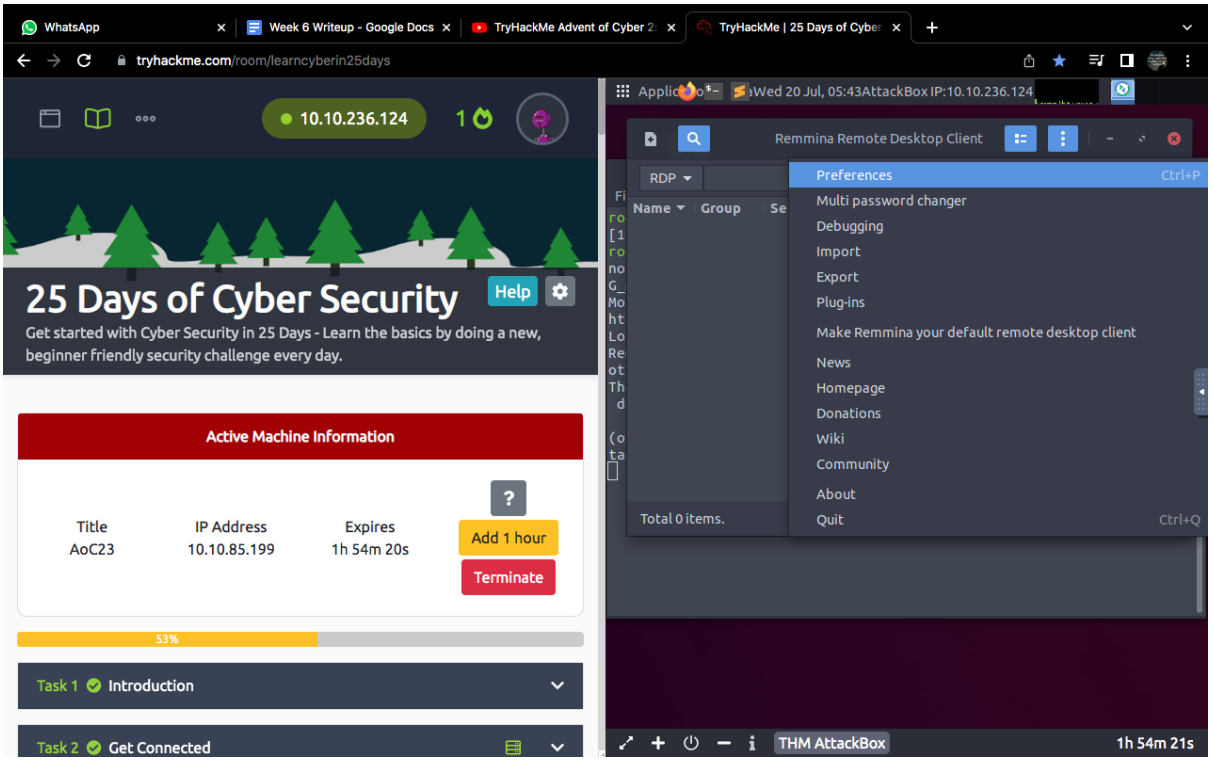
key can be found in the bottom of the page. For Question 4, find Elf Server on Network, double click it, click the “...” icon to reveal the password, go to Cyberchef to decode the password. For Question 5, the encoding used can be found at the left side of the password on Cyberchef. For Question 6, find Elfmail on Email, double click it, click the “...” icon to reveal the password, go to Cyberchef to decode the password. For Question 7, find Elf Security System on Recycle Bin, double click it to obtain both the username and the password. For Question 8, copy the highlighted encoded value, go to Cyberchef to decode the value and to obtain the flag.

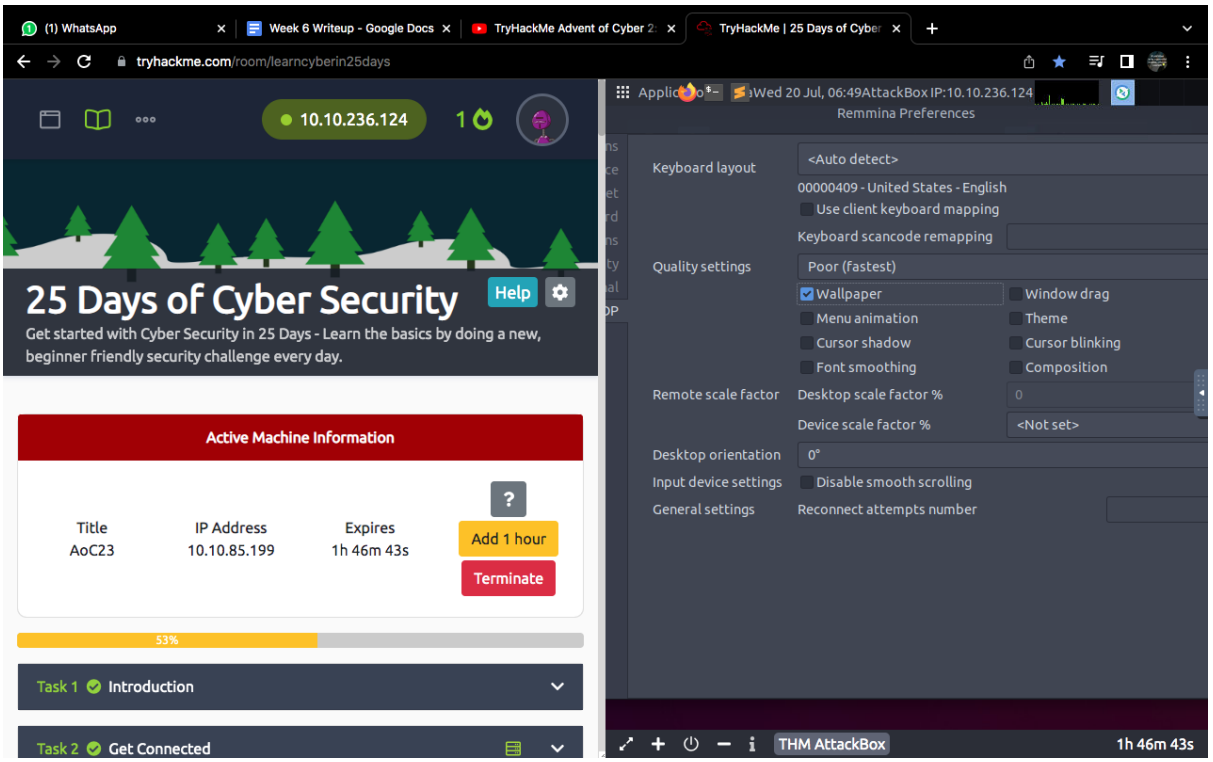
Day 23 - [Blue Teaming] The Grinch strikes again!

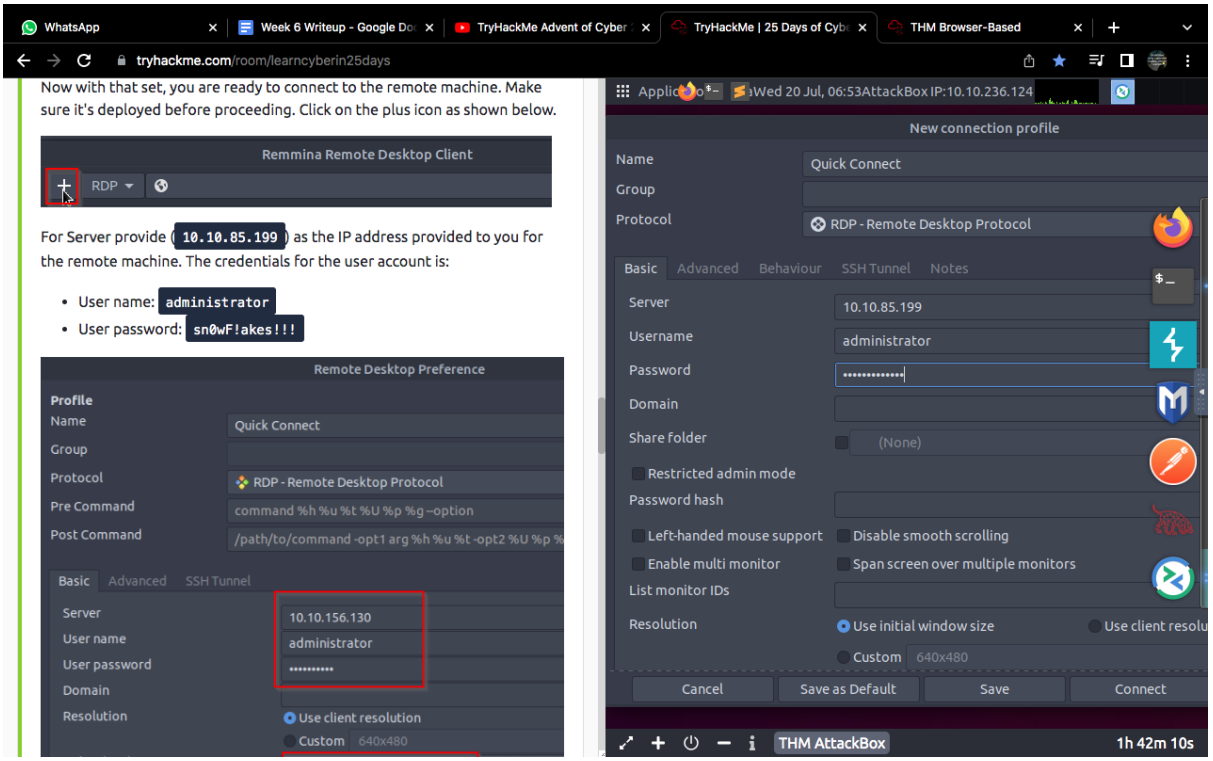
Tools used: Attackbox, Remmina

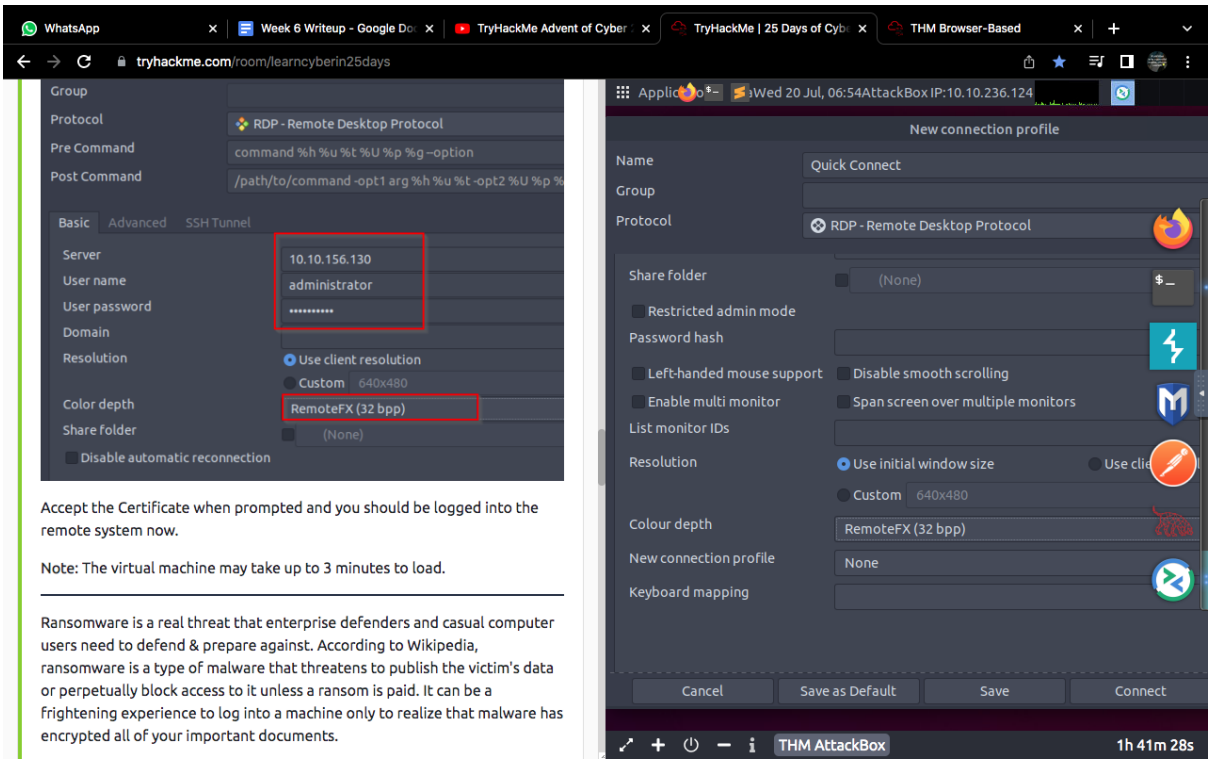
Solution/walkthrough:

Question 1
What does the wallpaper say?

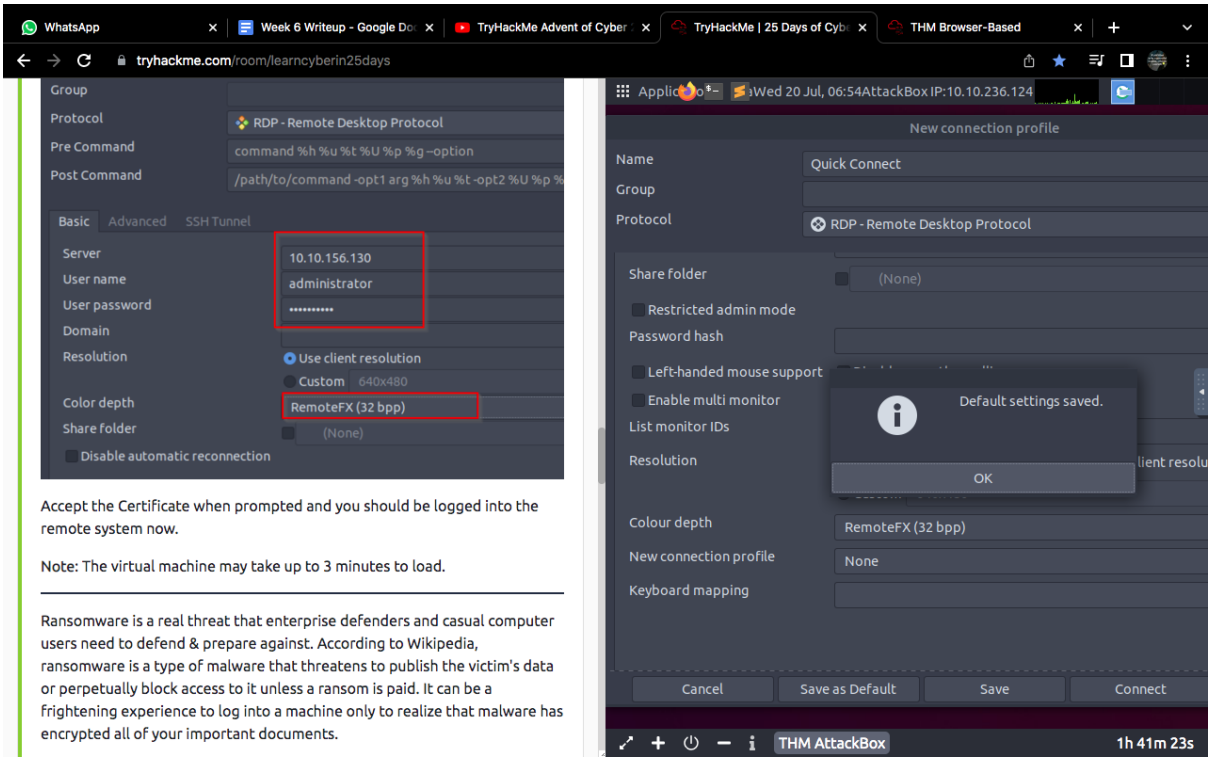


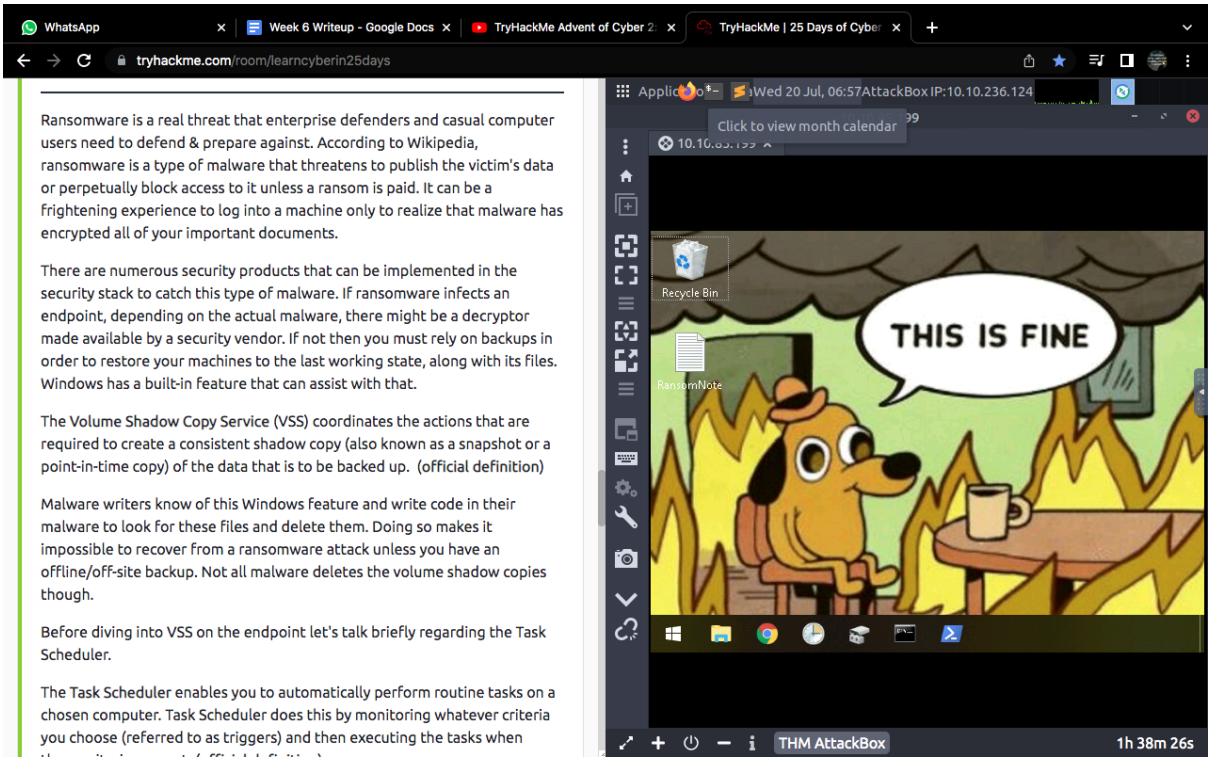






Fill in the information given in the RDP tab given.

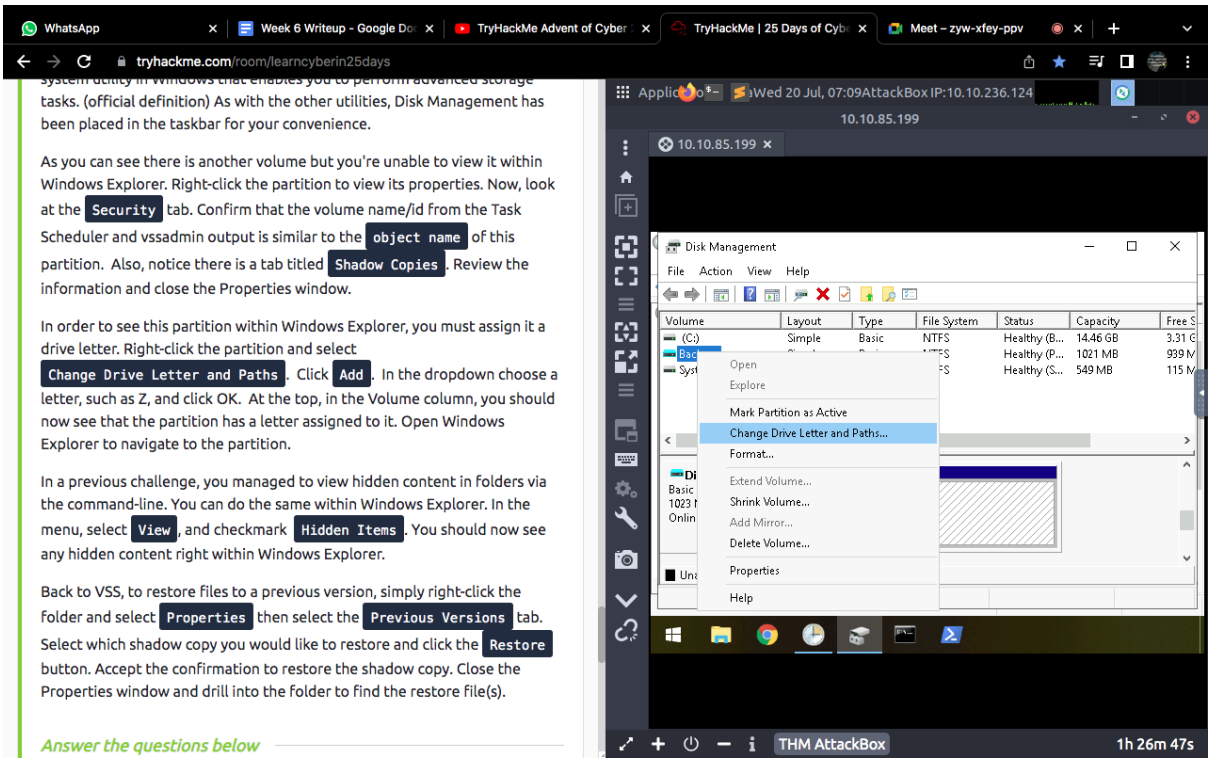


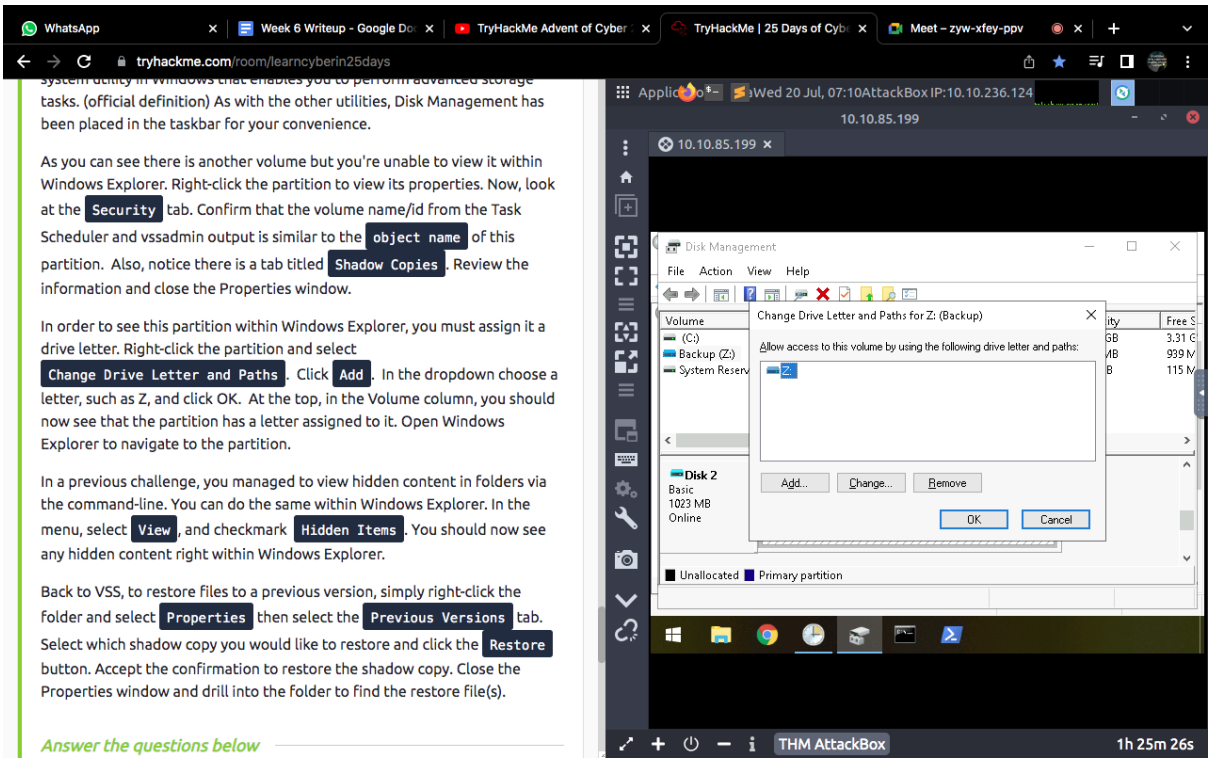


After filling in save and connect to see the wallpaper as above.

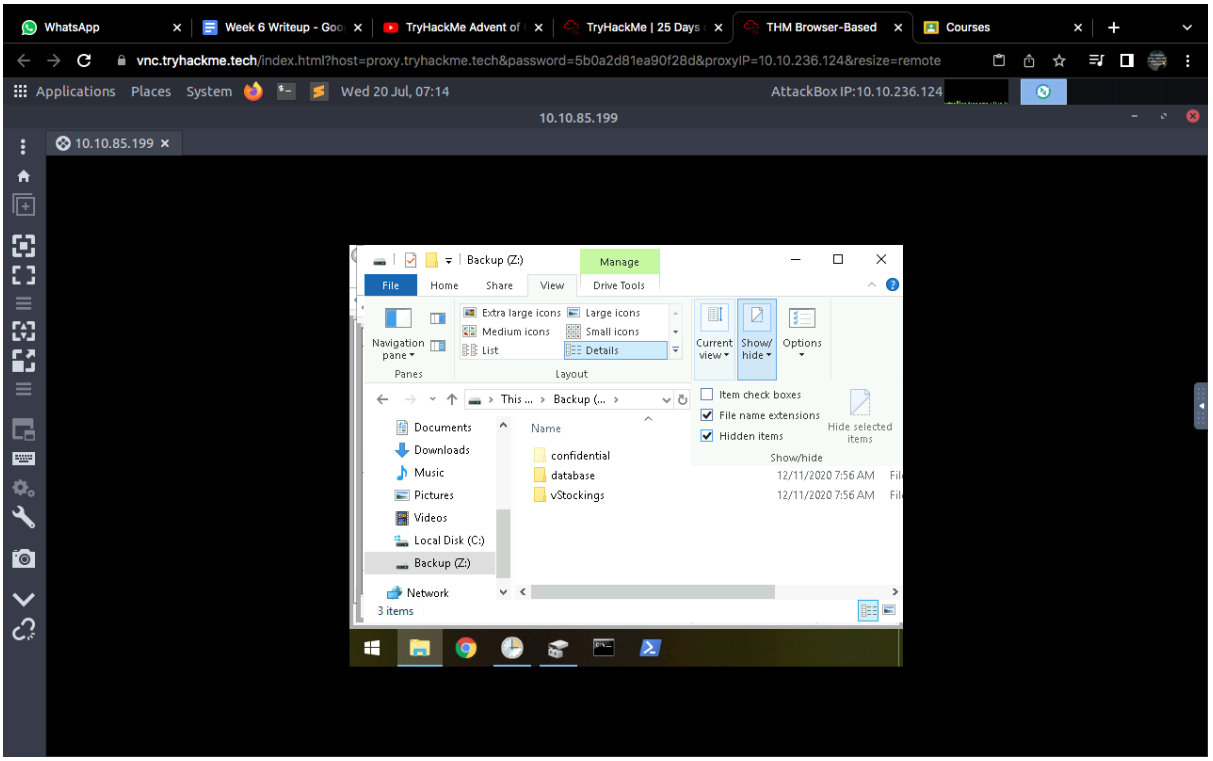
Question 2

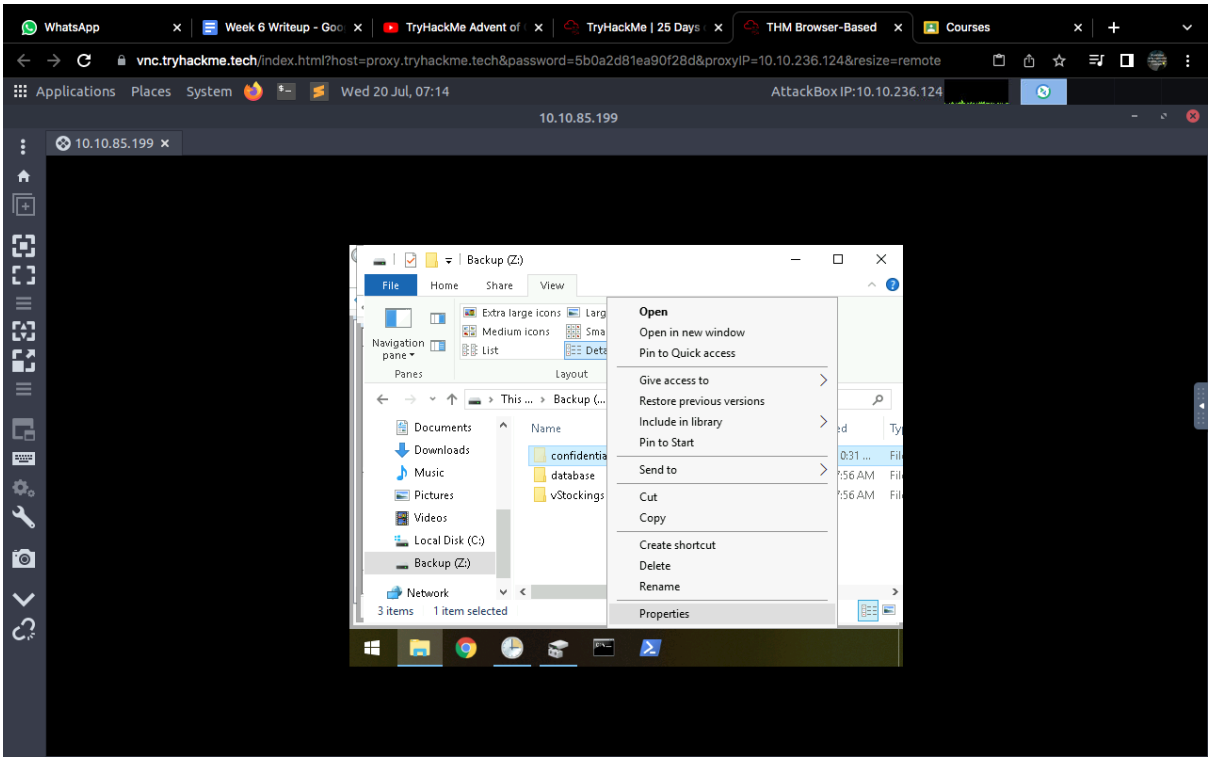
Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?



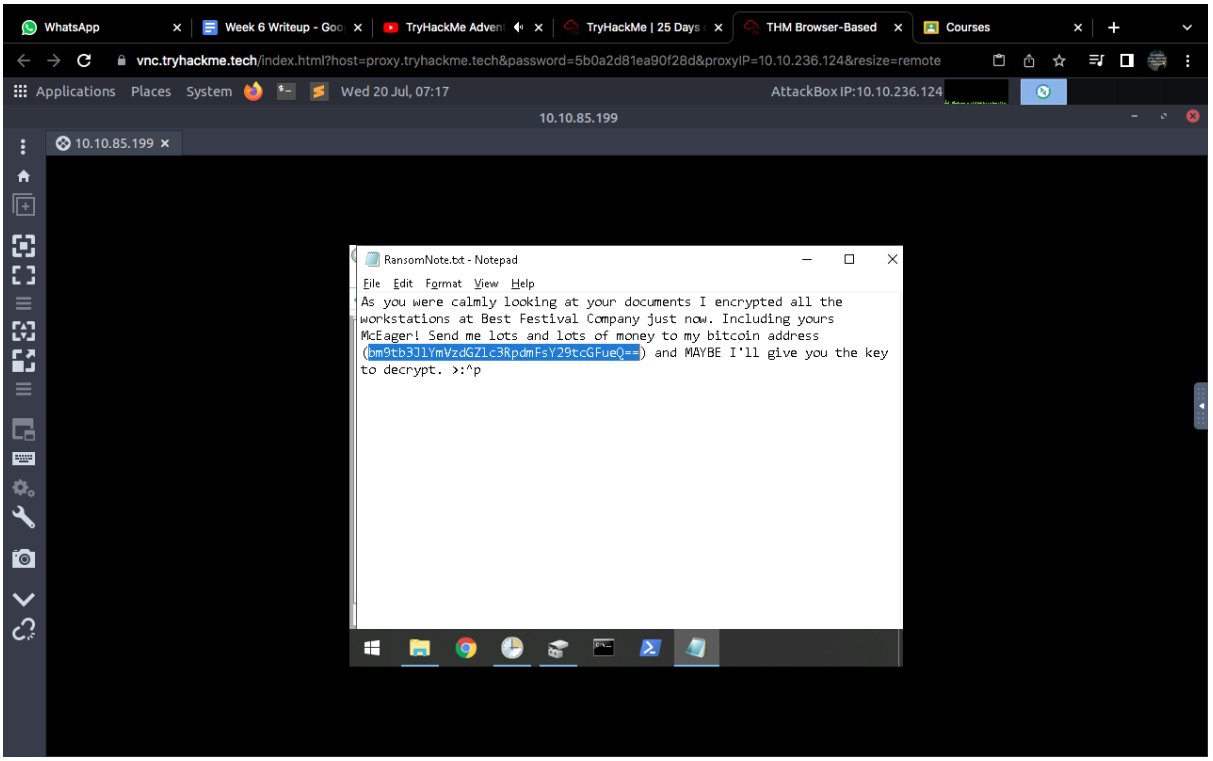


Change the backup to Backup-Z as above

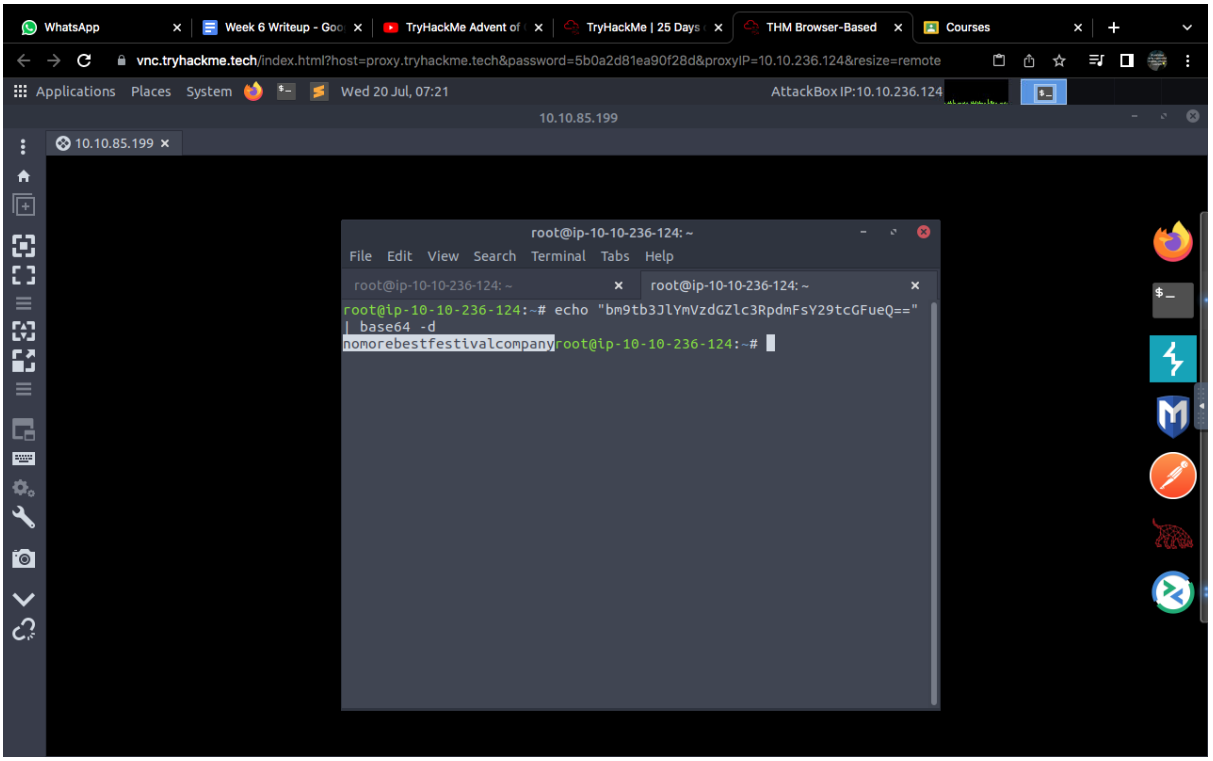




Go to folders and try to find Backup-Z and change the option to file name selection and hidden items by clicking the view tab.



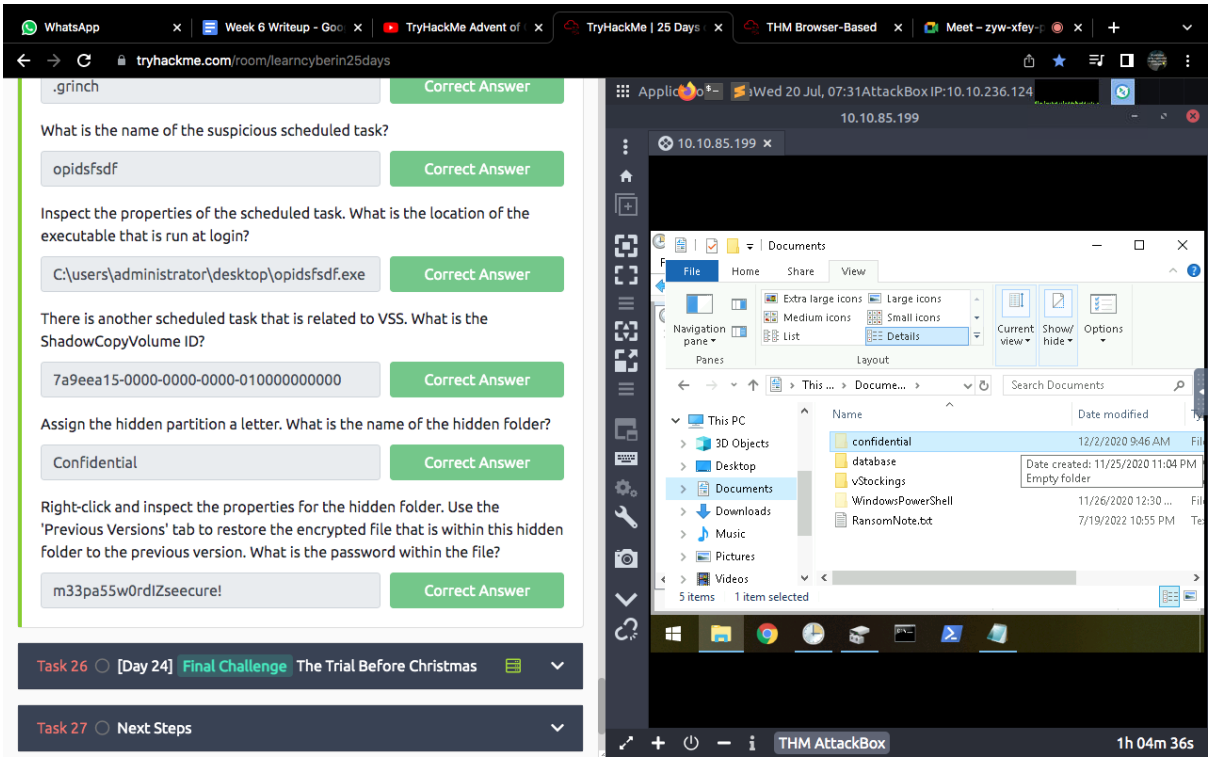
Then click the confidential folder to get the above sentence.

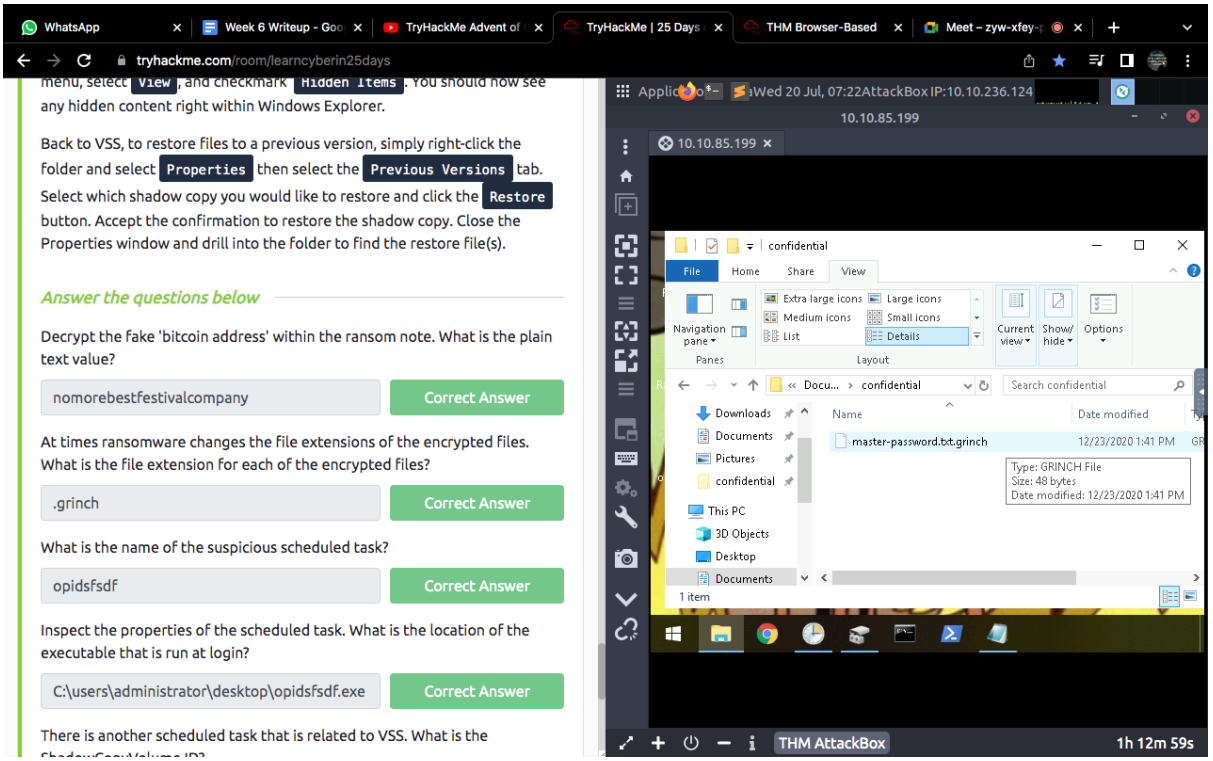


Transfer it to the terminal and do as above.

Question 3

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

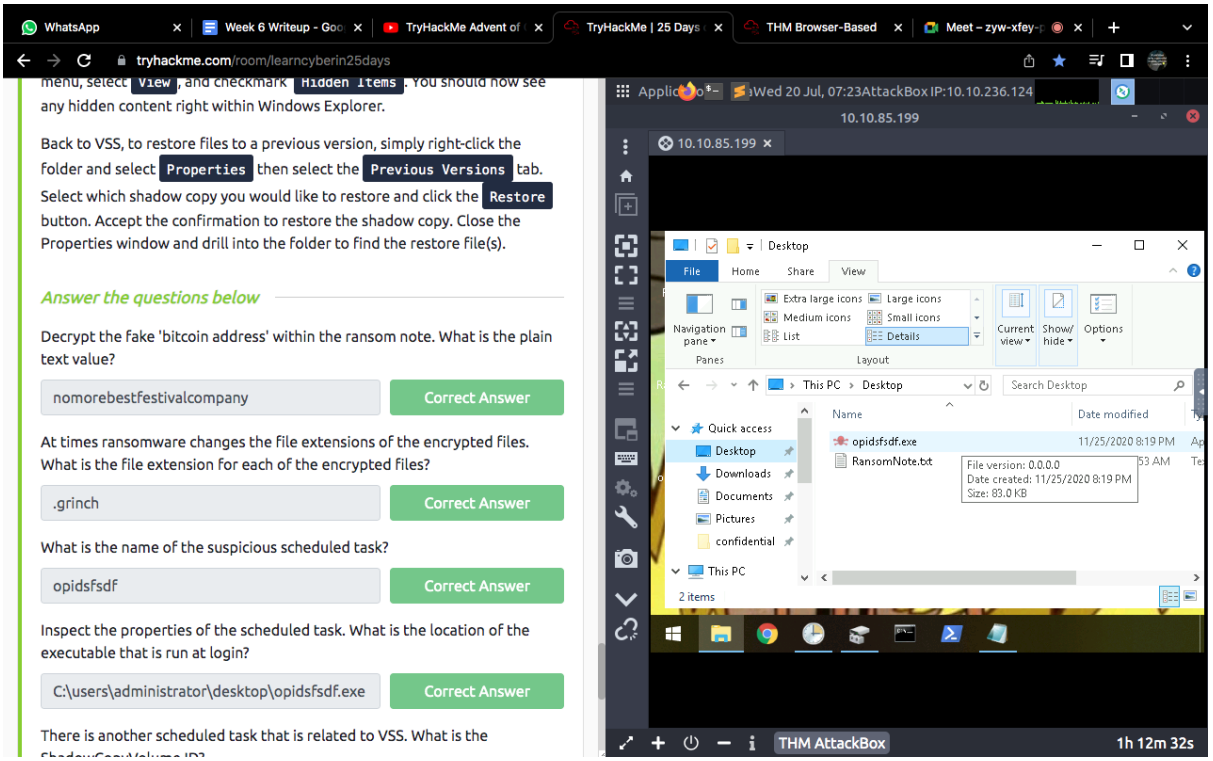




Go to the confidential folder in the documents file to find the answer.

Question 4

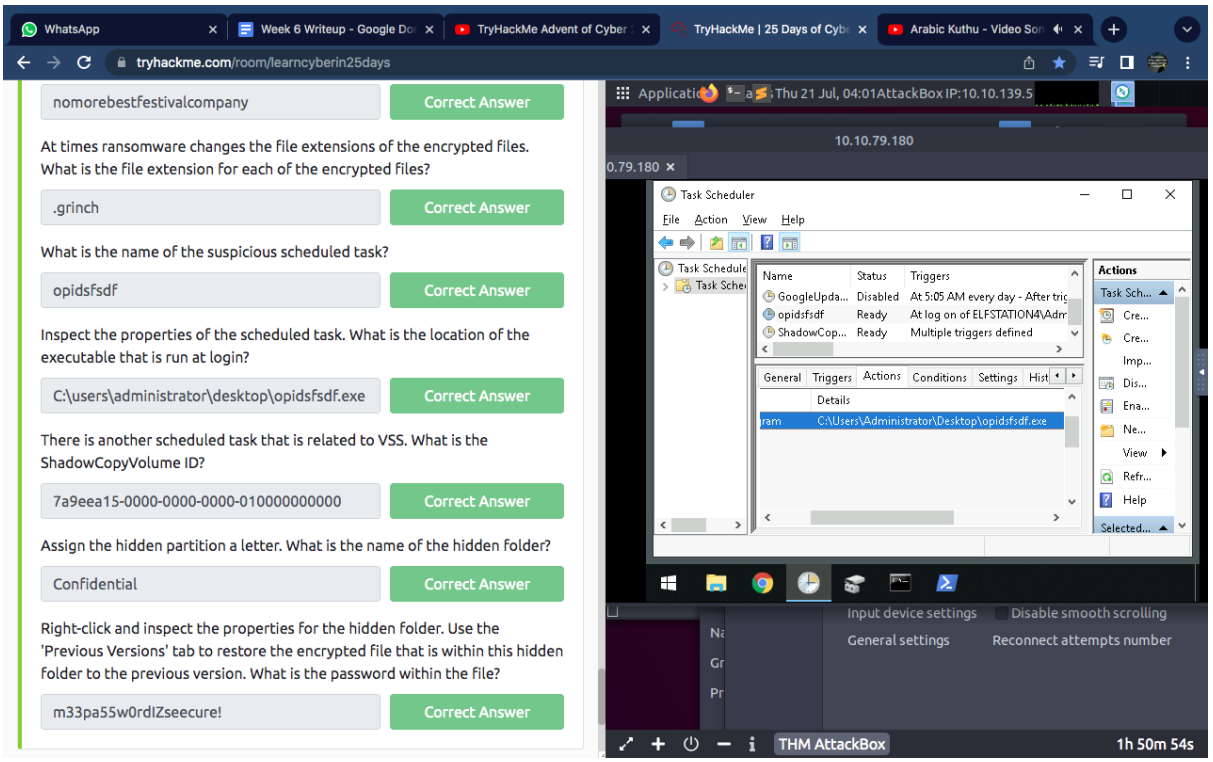
What is the name of the suspicious scheduled task?



The name can be find by clicking desktop in the folders.

Question 5

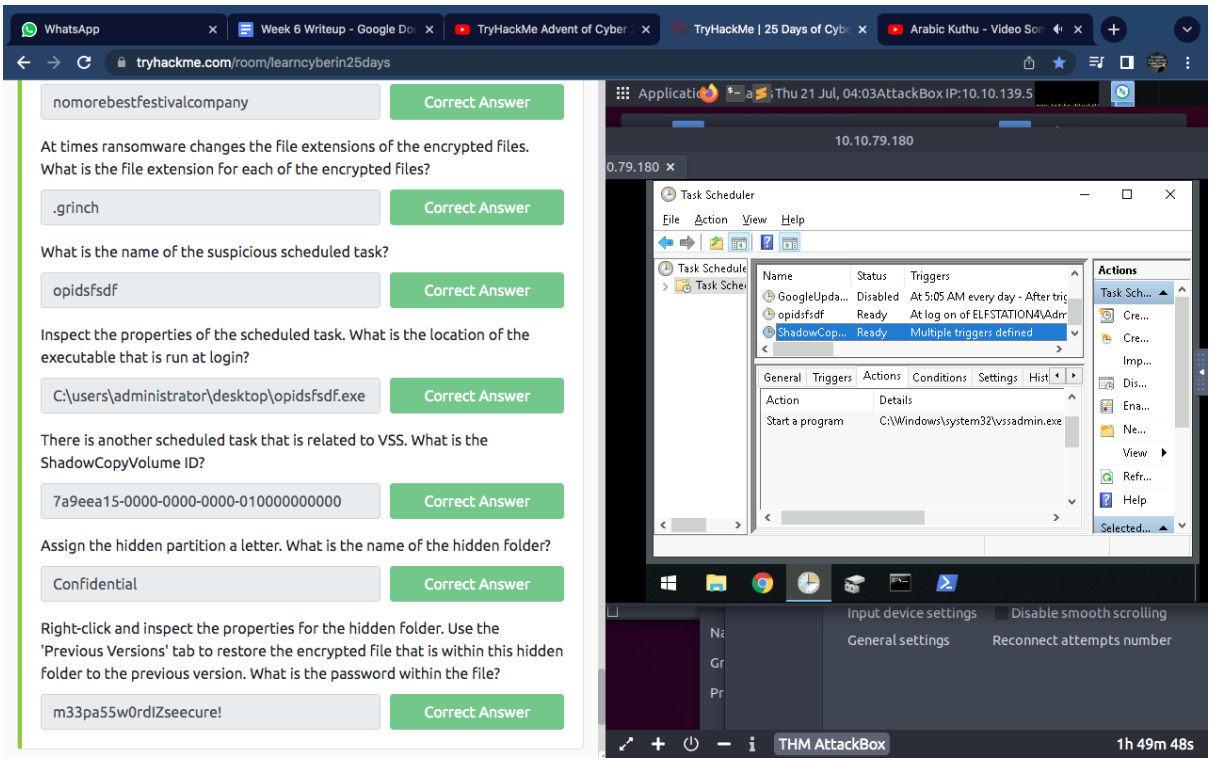
Inspect the properties of the scheduled task. What is the location of the executable that is run at login?

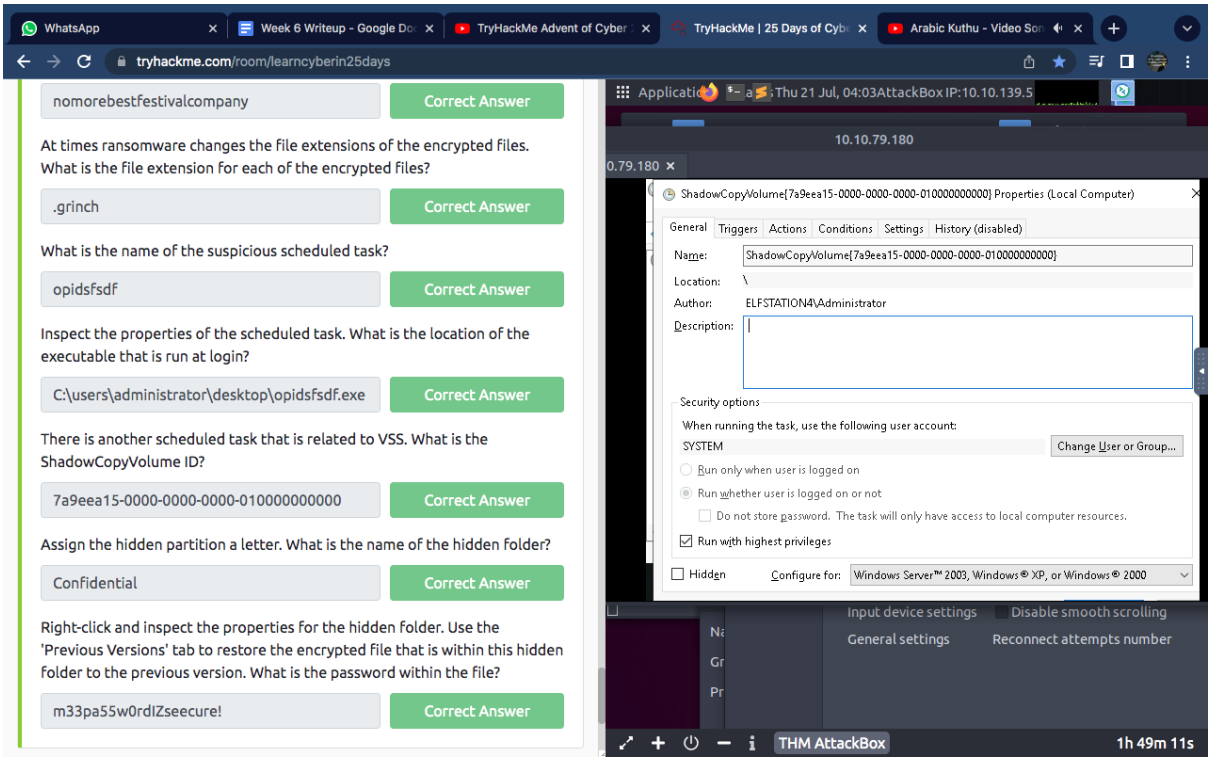


Click opidsnfdf and click actions to find the URL.

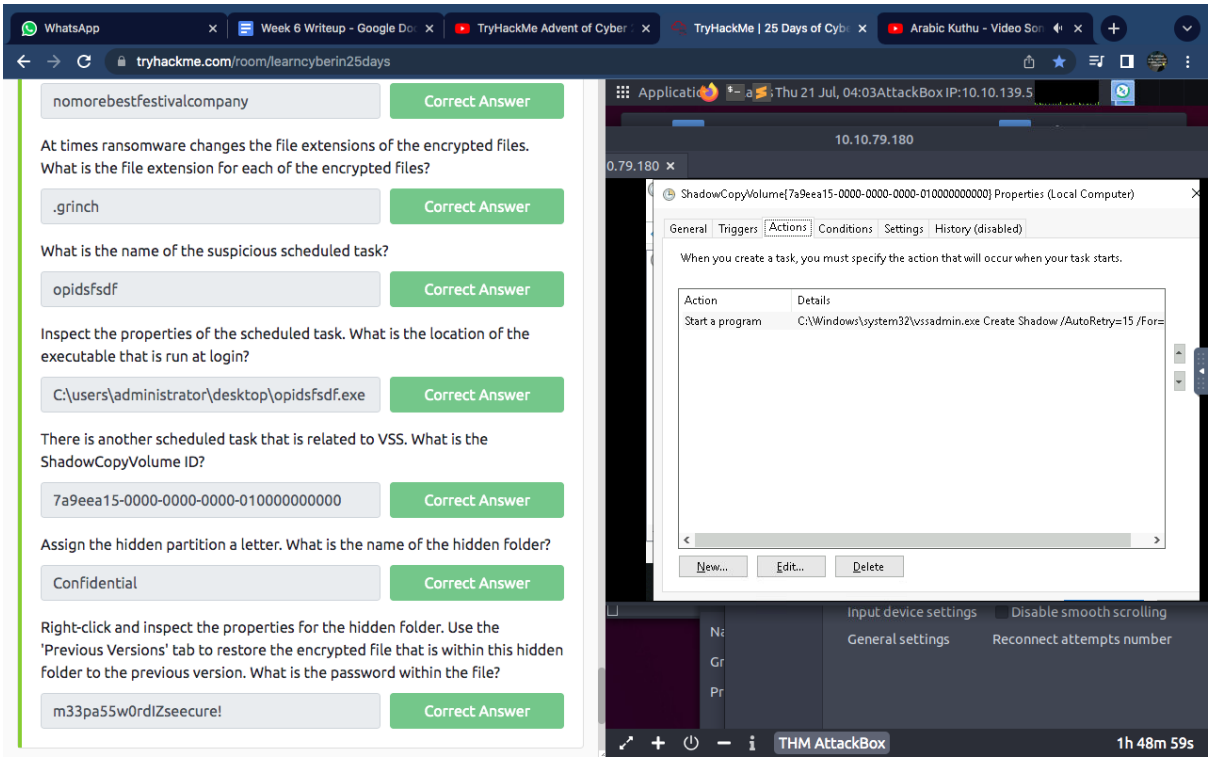
Question 6

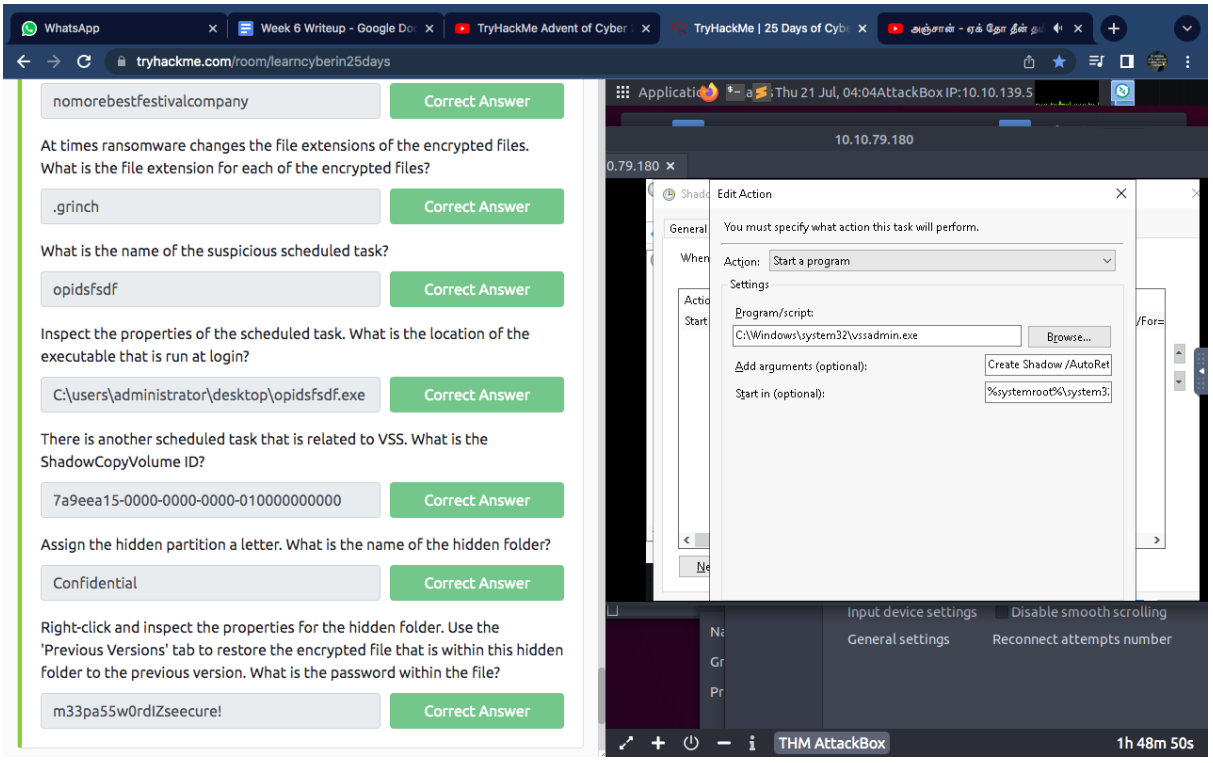
There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?



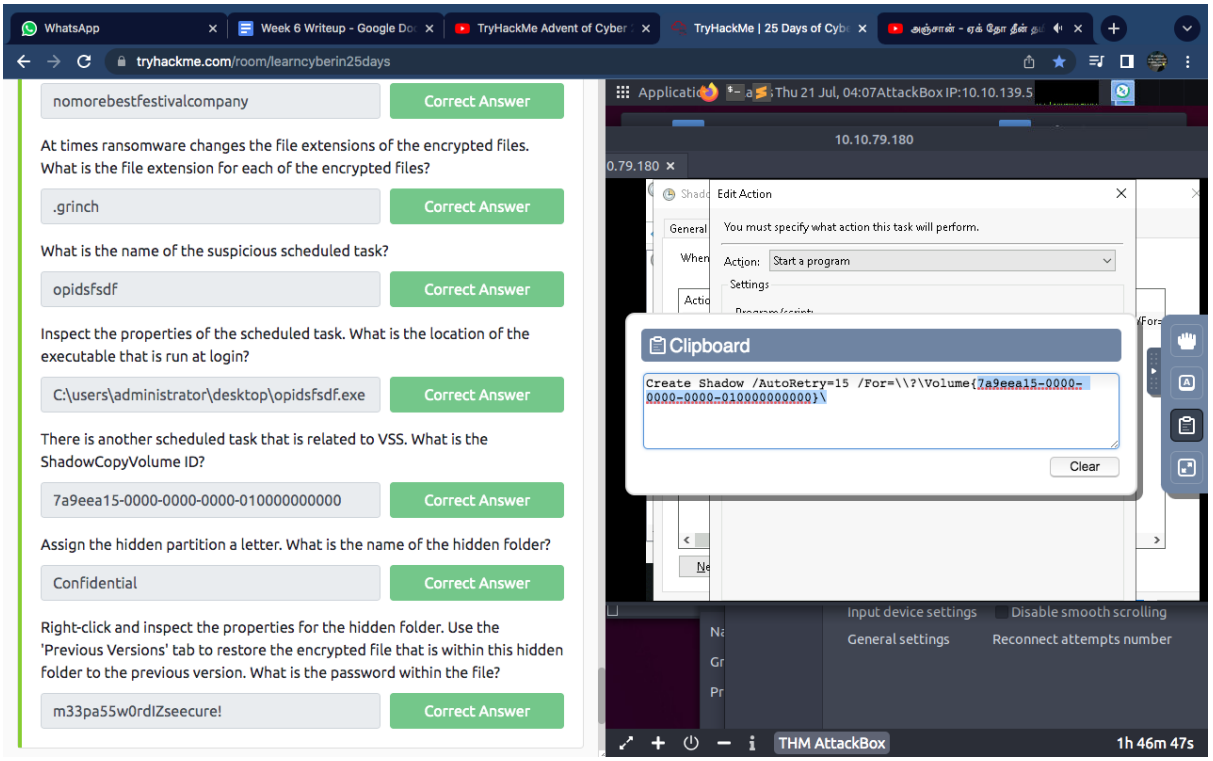


Click ShadowCopy in the task scheduled library then go to properties.





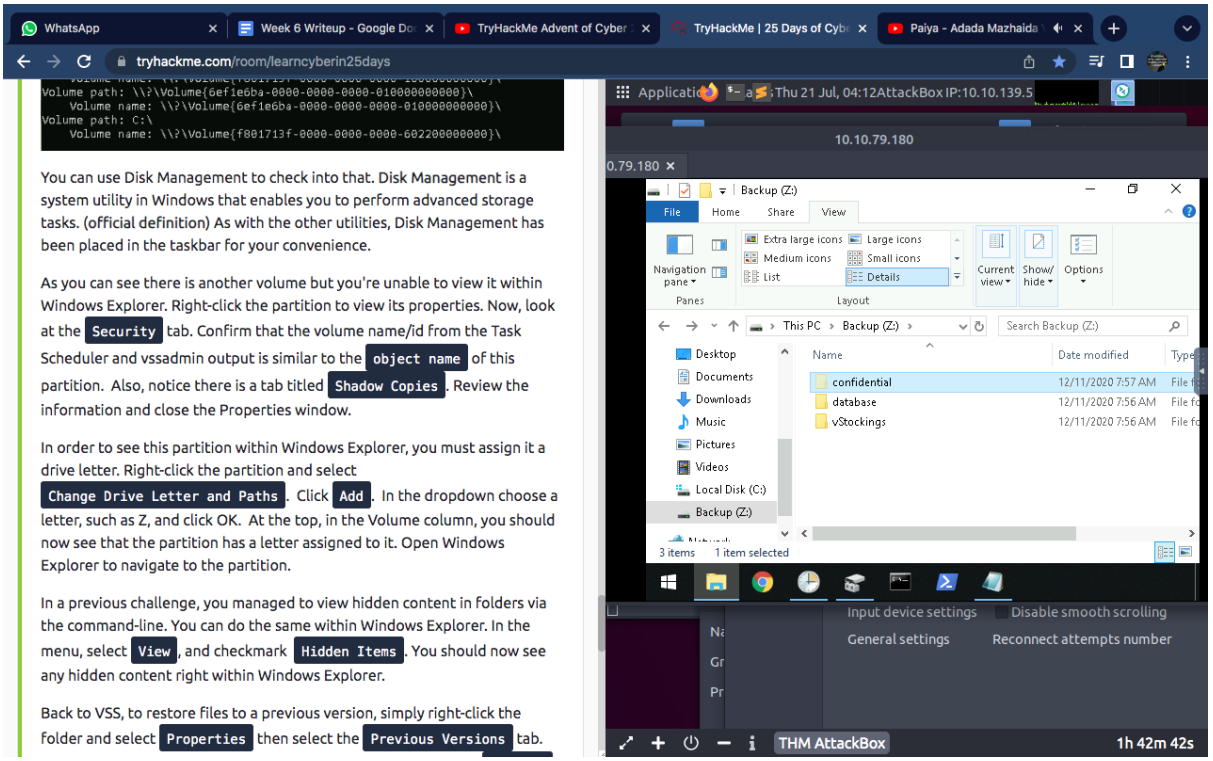
Choose actions and click the URL. Then click the add a argument(optional).



Copy the ShadowCopyVolume ID.

Question 7

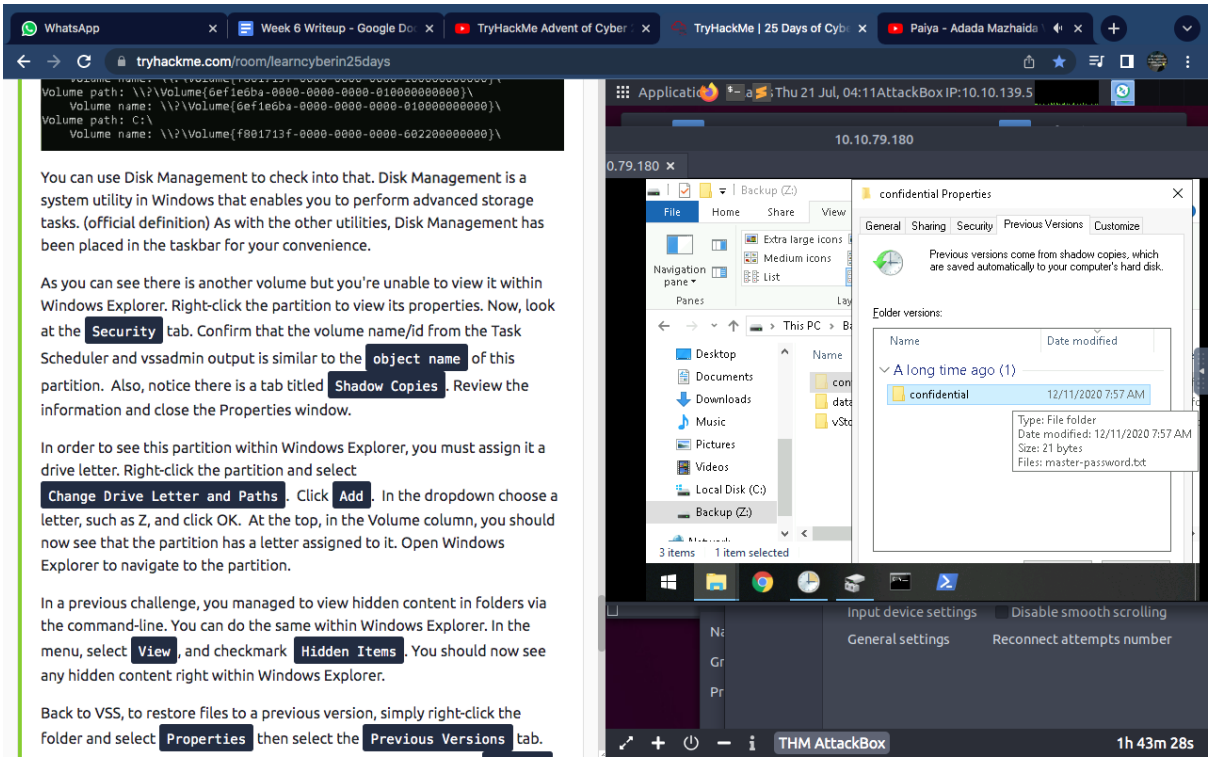
Assign the hidden partition a letter. What is the name of the hidden folder?

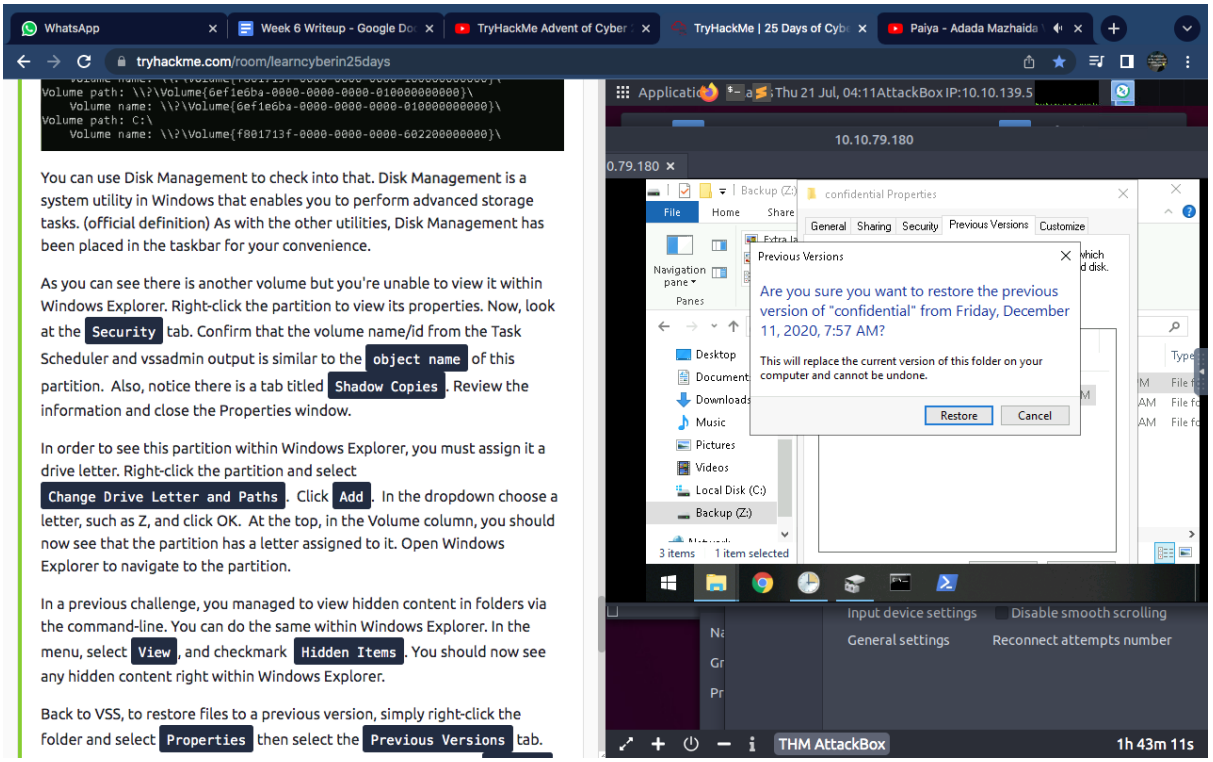


The folder will be confidential.

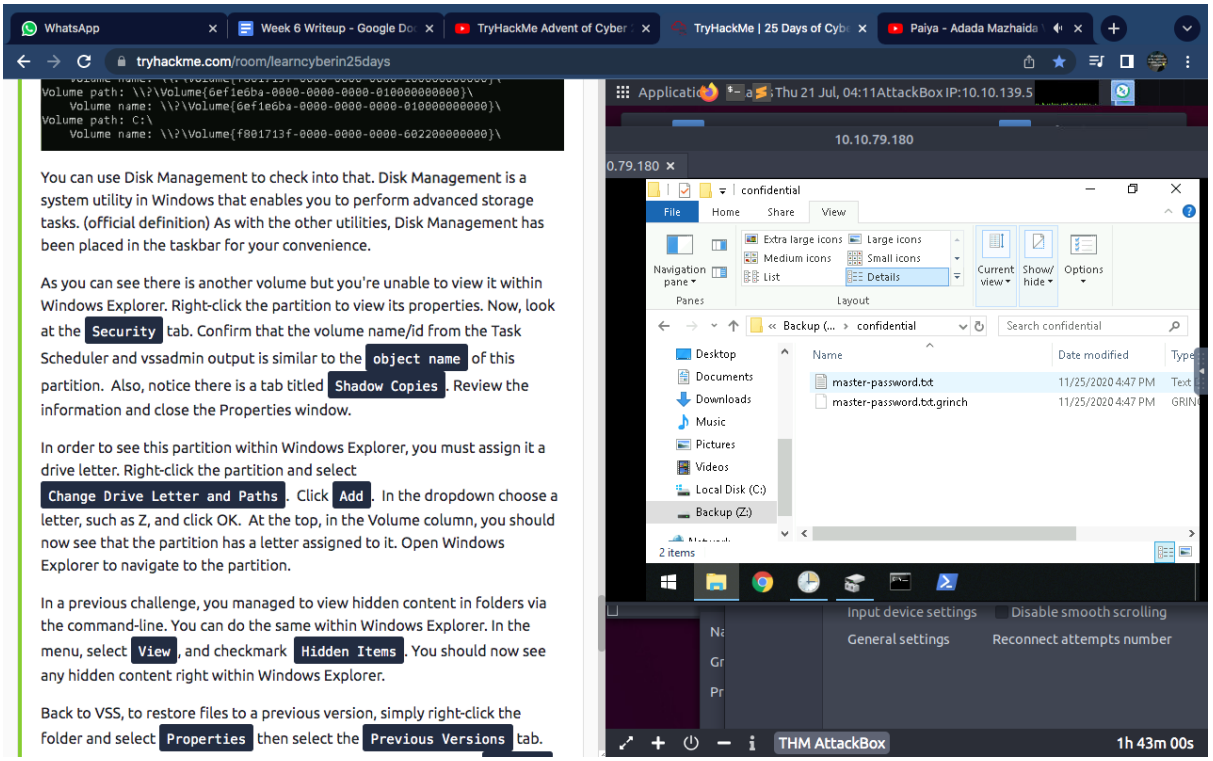
Question 8

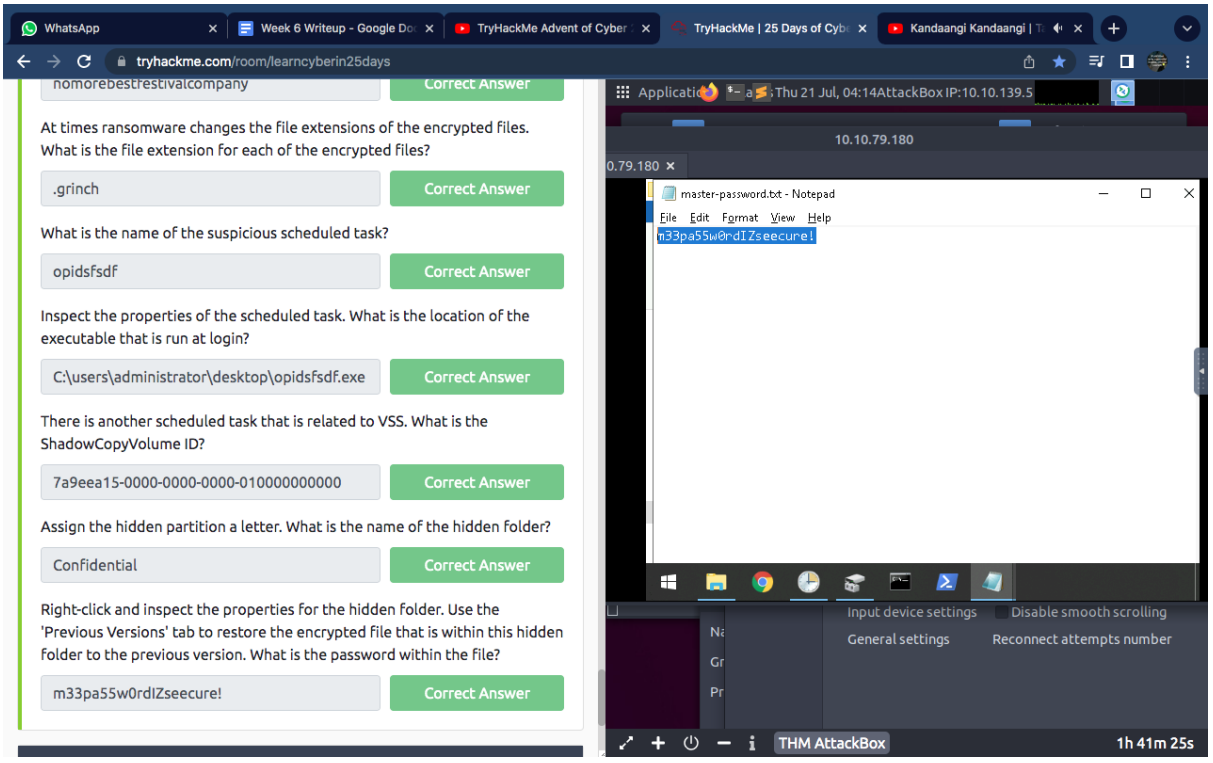
Right-click and inspect the properties for the hidden folder. Use the 'Previous Versions' tab to restore the encrypted file that is within this hidden folder to the previous version. What is the password within the file?





Go to Backup-Z and right click in the confidential folder to restore it.





After that click again the confidential folder and choose the master-password.txt to find the password as above.

Solution/walkthrough:

As for question 1, type in remmina & in the terminal and as in the picture above, a tab will pop up with the name RDP. Now with that set, you are ready to connect to the remote machine. Make sure it's deployed before proceeding. Click on the plus icon as shown below.Type in the server, username, password and change the colour depth as RemoteFX(32 bpp).Right after doing that save as default and click connect to see the wallpaper. For question 2, go to disk management and change the backup to Backup Z then go to folders and click Backup Z at the bottom of the folder and click the view tab in the top of that and change the selection as file name selection and hidden items. Right after that we will be able to see a confidential folder.Right click on that folder and choose properties and we can see a ransom note tab appear and highlight the above sentence as above and go to terminal to do as in the picture above to get the answer.As for question 3 , go to documents and choose confidential folder to get the anwer. For question 4, click desktop to get the answer as above. Next, for question 5, go to task scheduler and click task library and click actions to see opidsfsdf to see the URL as above.As for question 6, click Shadow Copy and click the URL below and choose properties and choose actions. Right after that, click add argument(optional) and copy the ShadowCopyVolume ID. For question 7, the folder will be confidential. As for the last question, go to Backup Z right click confidential and choose properties to restore it. After completing that go into the confidential folder and click master-password.txt to find the password within the file.

Day 24: Final Challenge - The Trial Before Christmas

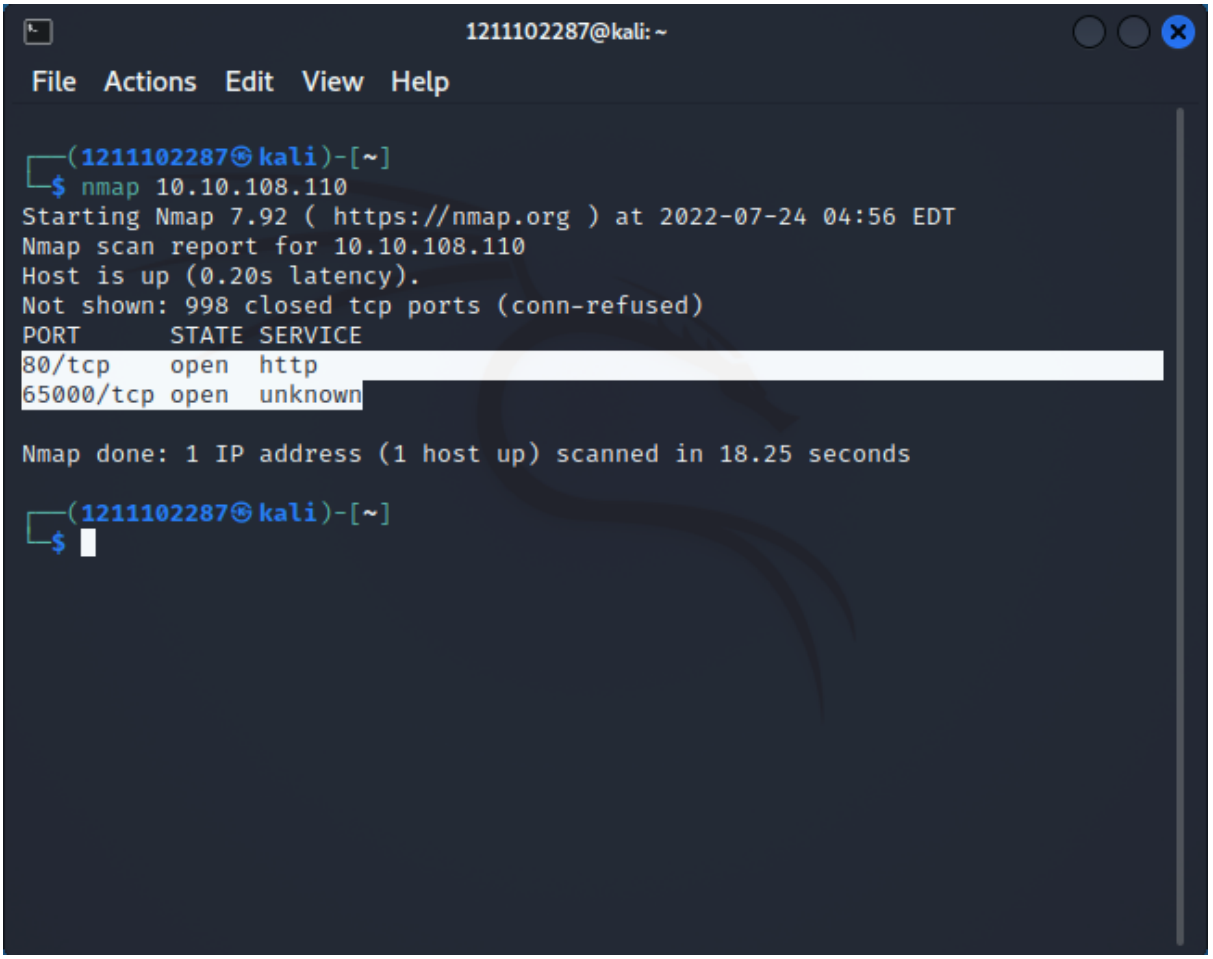
Tools used: THM Machine/Kali Linux/Mozilla Firefox/Gobuster/BurpSuite/Foxy Proxy/Nmap

Solution/Walkthrough:

Question 1

Scan the machine. What ports are open?

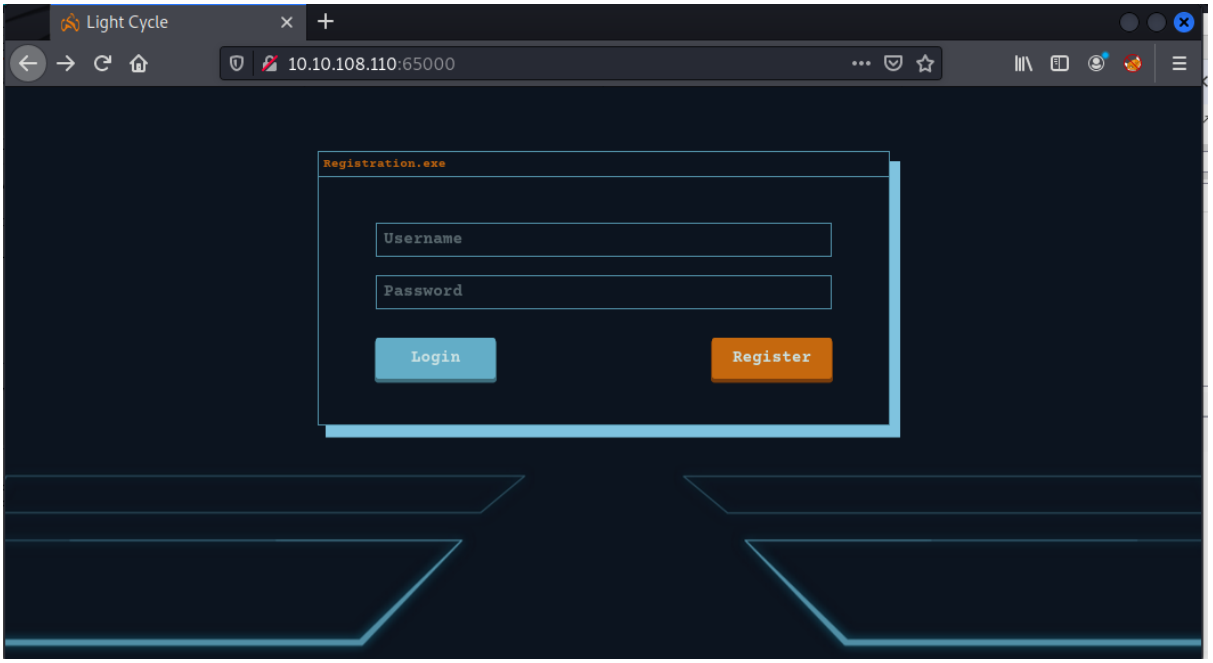
Use the **nmap** scan with the IP address to find the ports which are available. There are two ports which are opened (highlighted)



Question 2

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

We know that there are two ports which are open. By just adding the port **(65000)** after the IP address in the web browser, we could see there is a hidden website named **Light Cycle**.



Question 3

What is the name of the hidden php page?

With the help of **Gobuster**, we can check for the hidden pages and directories for the page. We can see there is a hidden file named **/uploads.php** file at the bottom of the terminal.

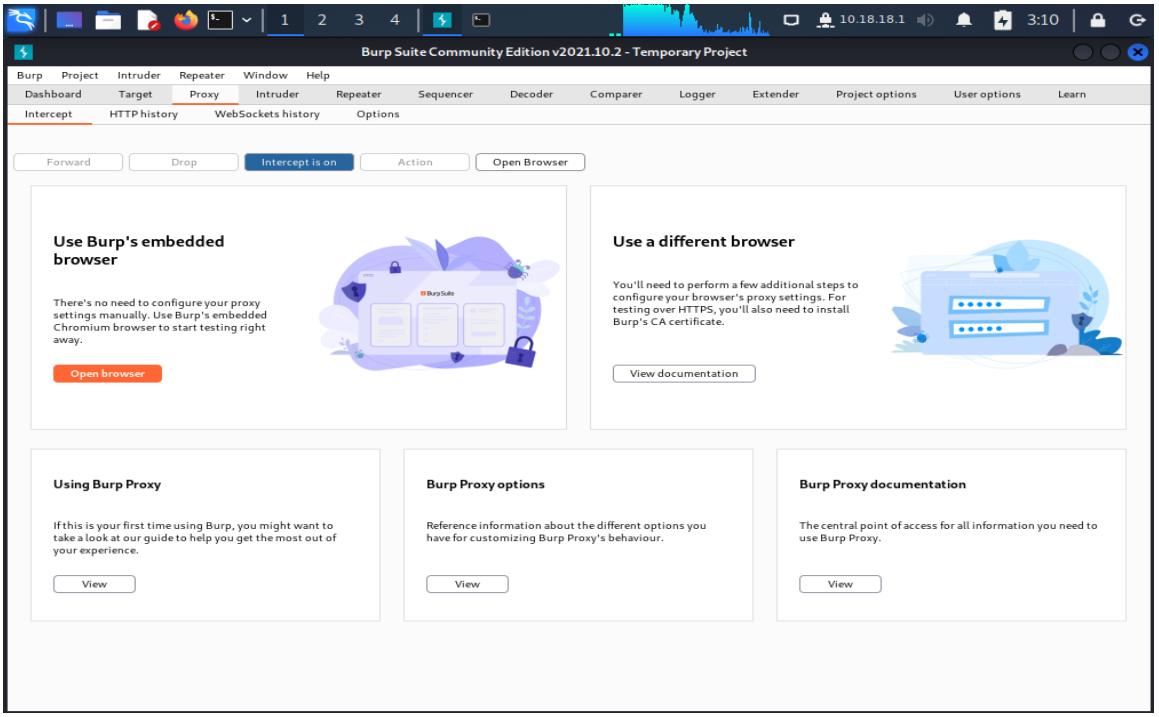
```
┌──(1211102287㉿kali)-[~]
└─$ gobuster dir -u http://10.10.108.110:65000 -w /usr/share/wordlists/big.tx
t -x php,txt,html
```

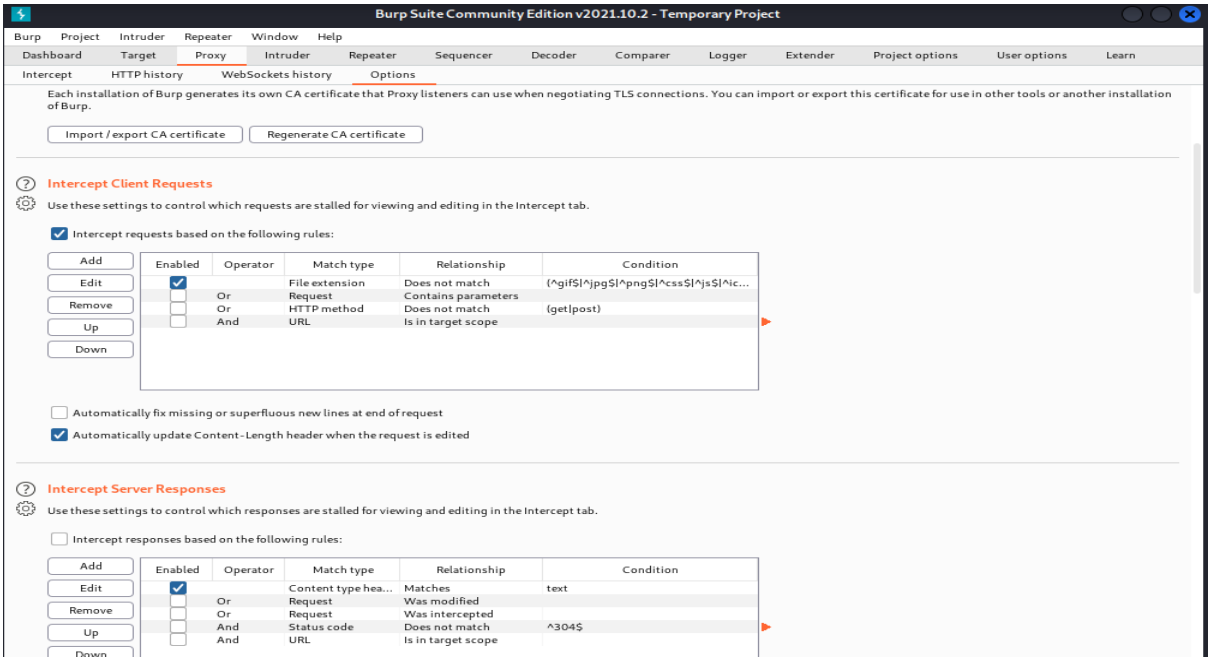
```
===============================================================
/.htaccess (Status: 403)
/.htaccess.html (Status: 403)
/.htaccess.php (Status: 403)
/.htaccess.txt (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.html (Status: 403)
/.htpasswd.php (Status: 403)
/.htpasswd.txt (Status: 403)
/api (Status: 301)
/assets (Status: 301)
/grid (Status: 301)
/index.php (Status: 200)
/server-status (Status: 403)
/uploads.php (Status: 200)
===============================================================
```

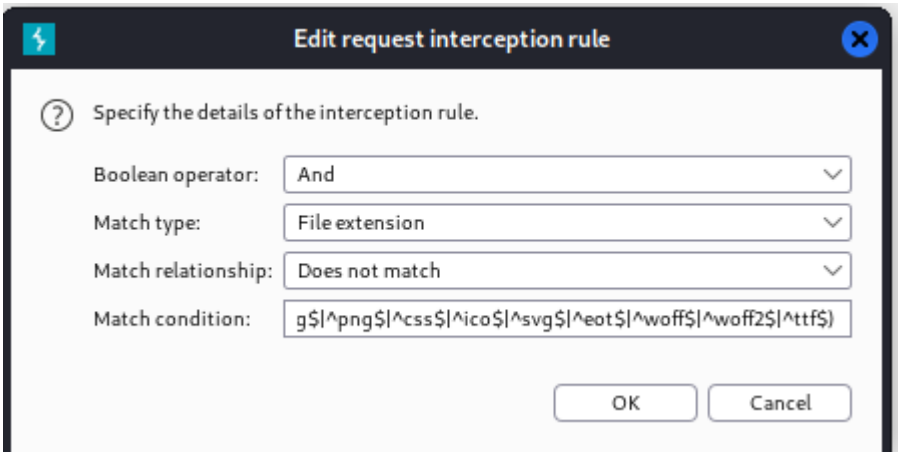
Question 4

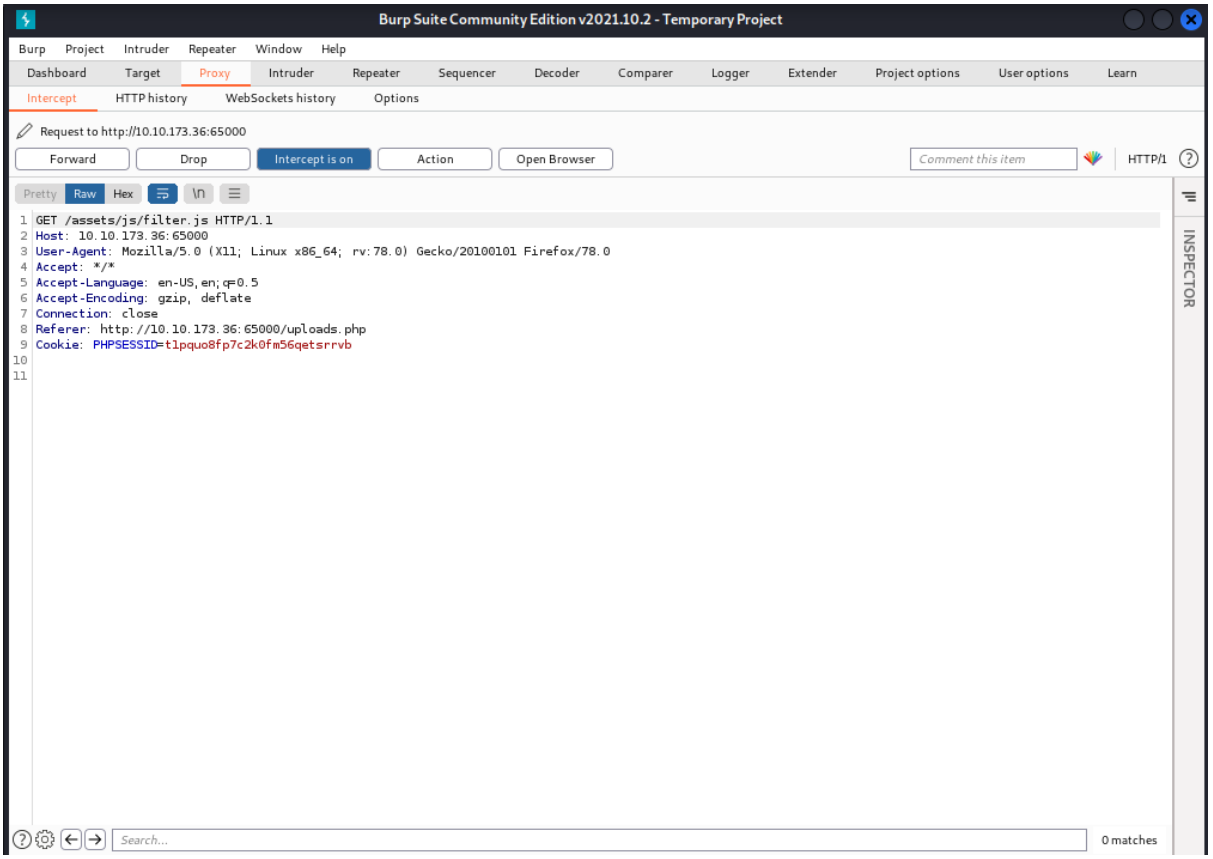
What is the name of the hidden directory where file uploads are saved?

Open Burp Suite and to bypass the client-side filter, we have to intercept the JavaScript code file containing the filter before it ever actually reaches our browser.

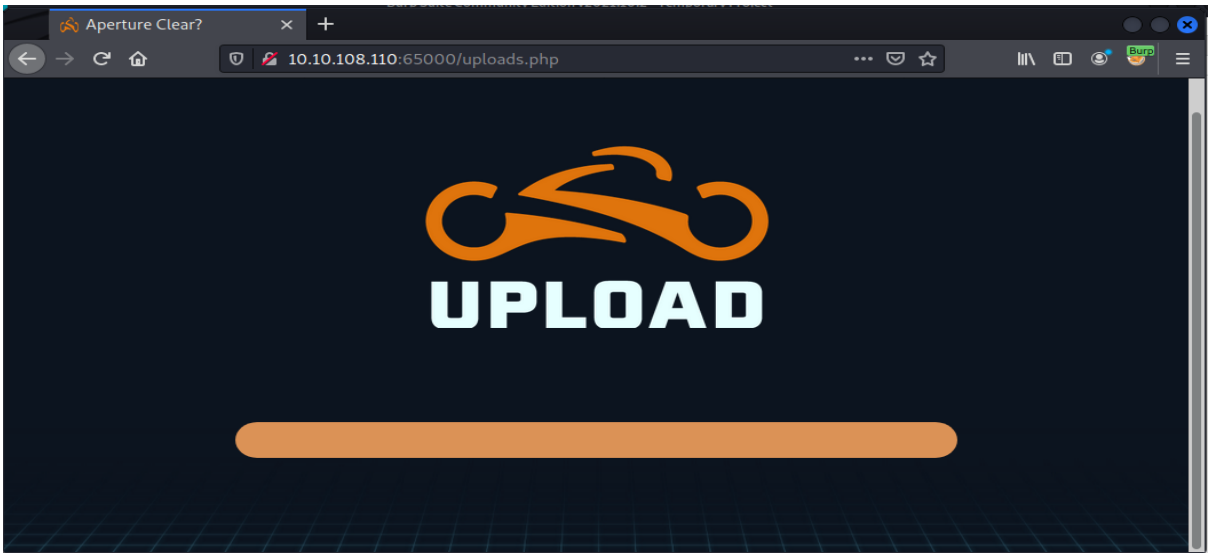



Burp Suite Community Edition v2021.10.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.
Import / export CA certificate
Regenerate CA certificate
Intercept Client Requests
Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.
Intercept requests based on the following rules:
Add
Edit
Remove
Up
Down
Enabled Operator Match type Relationship Condition
File extension Does not match (^gif$|^jpg$|^png$|^css$|^js$|^ic...
Or Request Contains parameters
Or HTTP method Does not match (get|post)
And URL Is in target scope
Automatically fix missing or superfluous new lines at end of request
Automatically update Content-Length header when the request is edited
Intercept Server Responses
Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.
Intercept responses based on the following rules:
Add
Edit
Remove
Up
Down
Enabled Operator Match type Relationship Condition
Content type hea... Matches text
Or Request Was modified
Or Request Was intercepted
And Status code Does not match ^304$
And URL Is in target scope

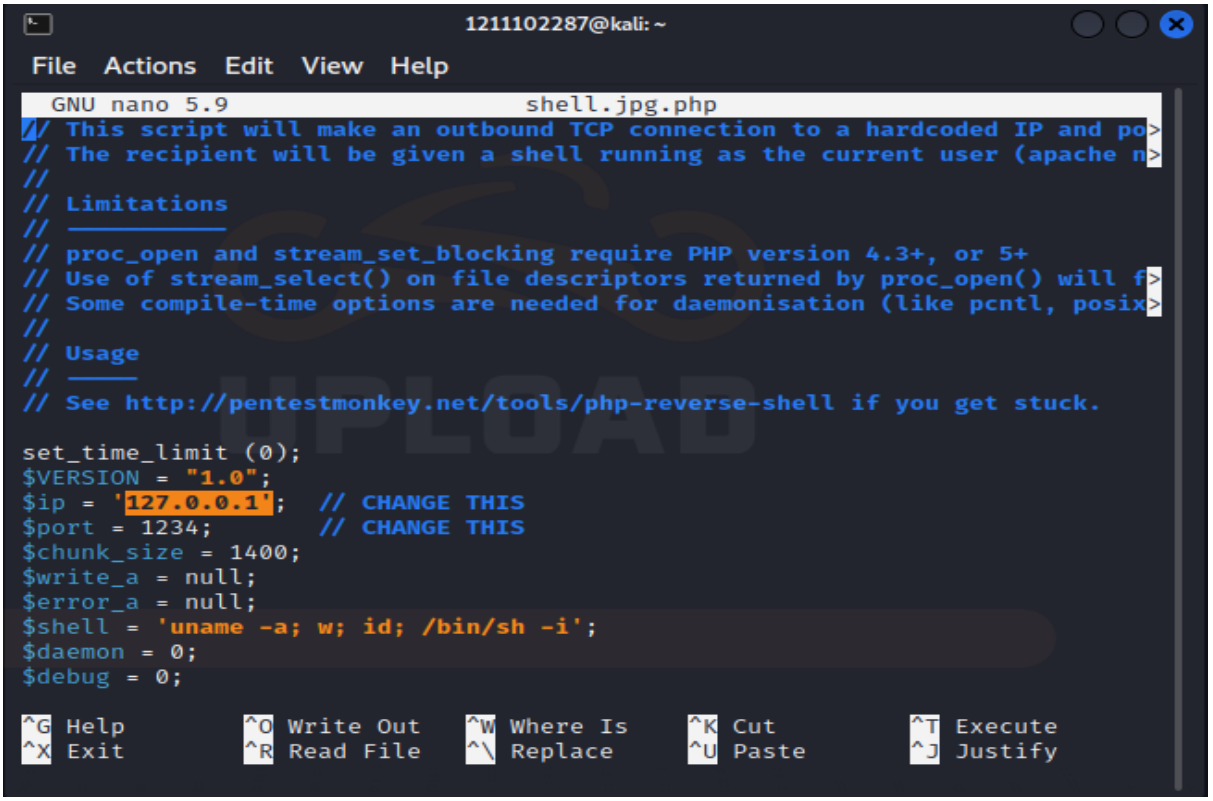

Edit request interception rule
Specify the details of the interception rule.
Boolean operator: And
Match type: File extension
Match relationship: Does not match
Match condition: g$|^png$|^css$|^ico$|^svg$|^eot$|^woff$|^woff2$|^ttf$)
OK
Cancel


Burp Suite Community Edition v2021.10.2 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Logger Extender Project options User options Learn
Intercept HTTP history WebSockets history Options
Request to http://10.10.173.36:65000
Forward Drop Intercept is on Action Open Browser
Comment this item
HTTP/1
Pretty Raw Hex \n
1 GET /assets/js/filter.js HTTP/1.1
2 Host: 10.10.173.36:65000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.173.36:65000/uploads.php
9 Cookie: PHPSESSID=tlpquo8fp7c2k0fm56qetsrrvb
10
11
INSPECTOR
Search...
0 matches

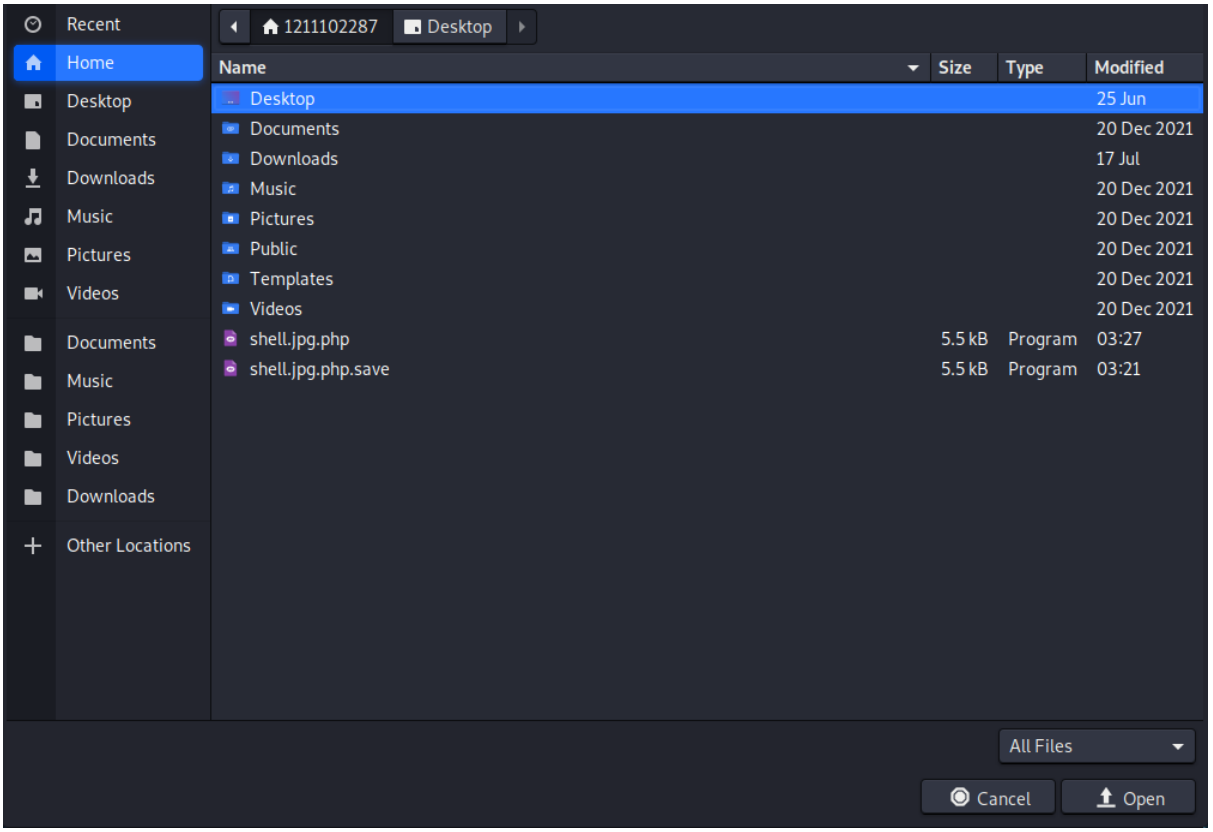
The page for uploading files could be seen after.



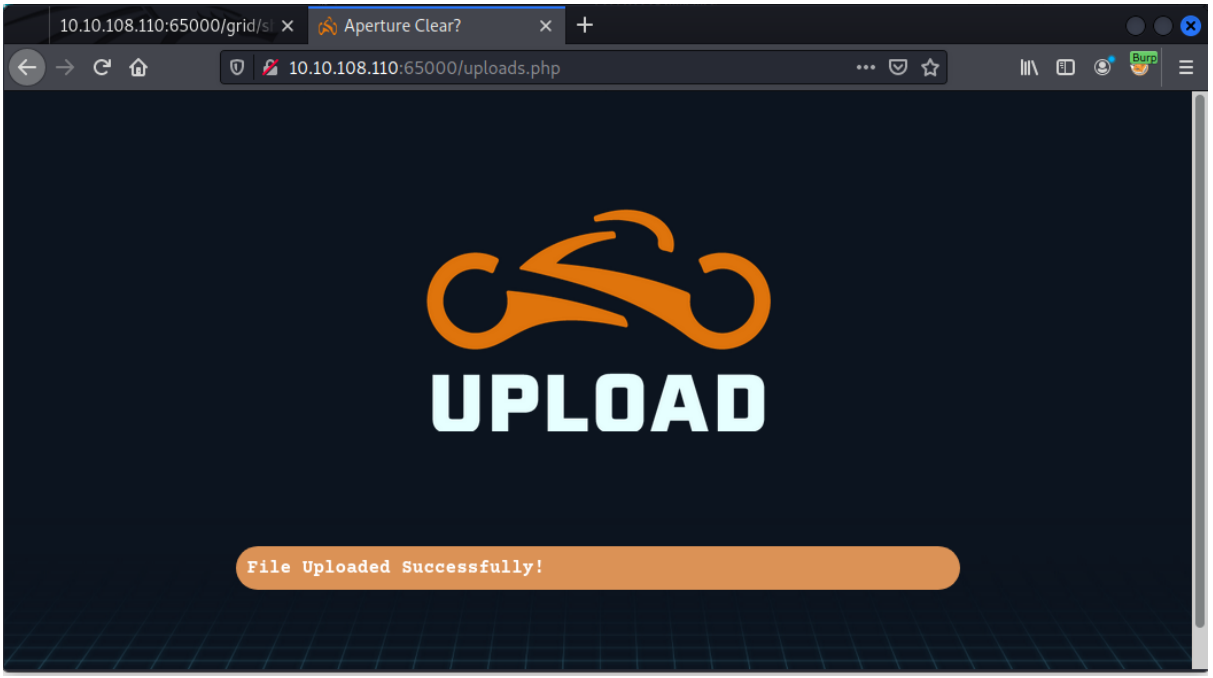
We have to upload and execute a reverse shell. Name our php file as **shell.jpg.php.** Change the IP to our linux machine and the port to 443.



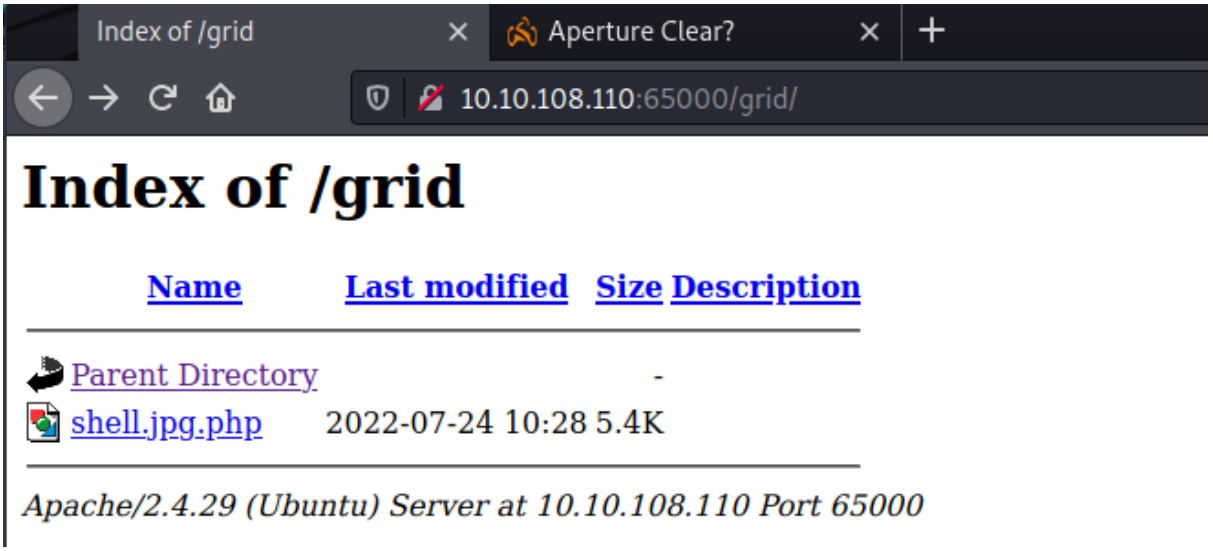
Upload the file in the upload page.



We can now see that the file is being uploaded successfully.



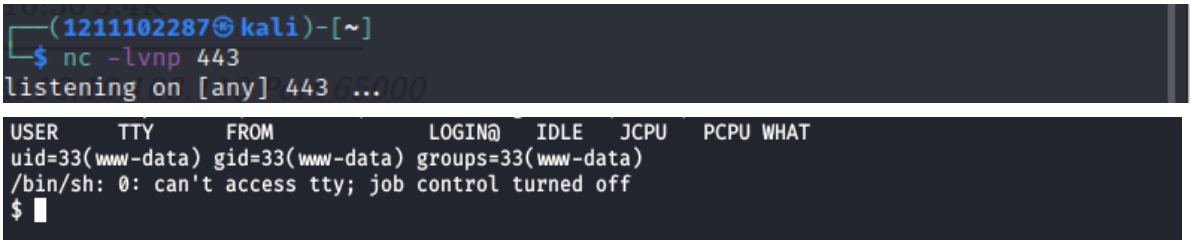
The directory **/grid** could be seen as a storage where files are uploaded and saved.



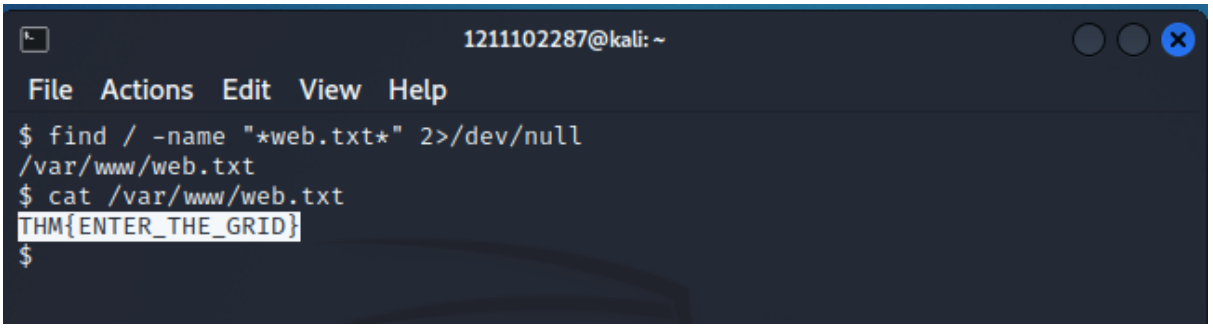
Question 5

What is the value of the web.txt flag?

Use netcat command to listen for our shell session.



By using the quick search command, we could know that the web.txt file we want to find is in the **/var/www/ directory.** Open the content in the directory by using the **cat** command. The flag inside the file could be seen (highlighted)



Question 6

What lines are used to upgrade and stabilize your shell?

From the hint given by THM, we know that the command **(python3 -c 'import pty;pty.spawn("/bin/bash")')** and the command **(export TERM=xterm)** are used to upgrade and stabilize the shell.

1. The first thing to do is use `python3 -c 'import pty;pty.spawn("/bin/bash")'`, which uses Python to spawn a better-featured bash shell. At this point, our shell will look a bit prettier, but we still won't be able to use tab autocomplete or the arrow keys, and Ctrl + C will still kill the shell.
2. Step two is: `export TERM=xterm` – this will give us access to term commands such as `clear`.

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

Question 7

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

Use the **ls** command to show the list for all files in the current directory. To show the content in the dbauth.php file, the cat command is used. In the file, the password and user is being shown (highlighted)

```
www-data@light-cycle:/var/www/TheGird/includes$ ls
aplincludes.php  dbauth.php  login.php  register.php  upload.php
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbauth.php
<?php

        $dbaddr = "localhost";
        $dbuser = "tron";
        $dbpass = "IFightForTheUsers";
        $database = "tron";
```

Question 8

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

Access and Log into our database using the credentials found. We can see that **“tron”** was being used in the database.

```
www-data@light-cycle:/var/www/TheGrid/includes$ mysql -utron -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
```

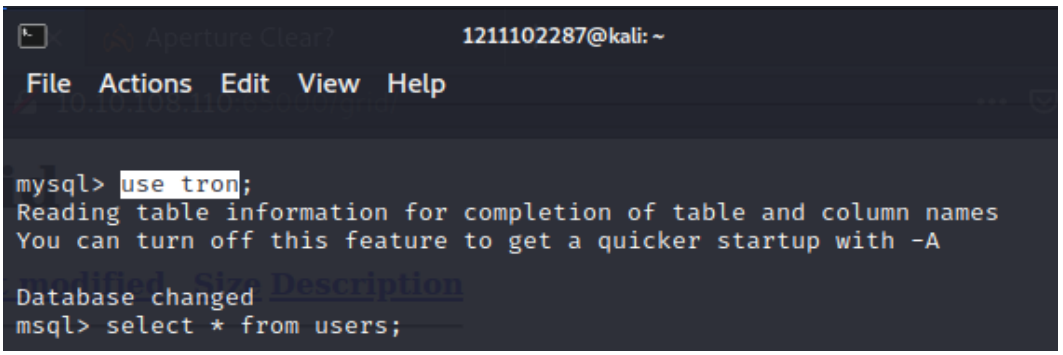
```
mysql> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| tron               |
+--------------------+
2 rows in set (0.00 sec)

mysql>
```

Question 9

Crack the password. What is it?

Select the tron database by typing the “use tron”command. Now we are in the tron database. Use the “select * from users;” command to see the content inside.

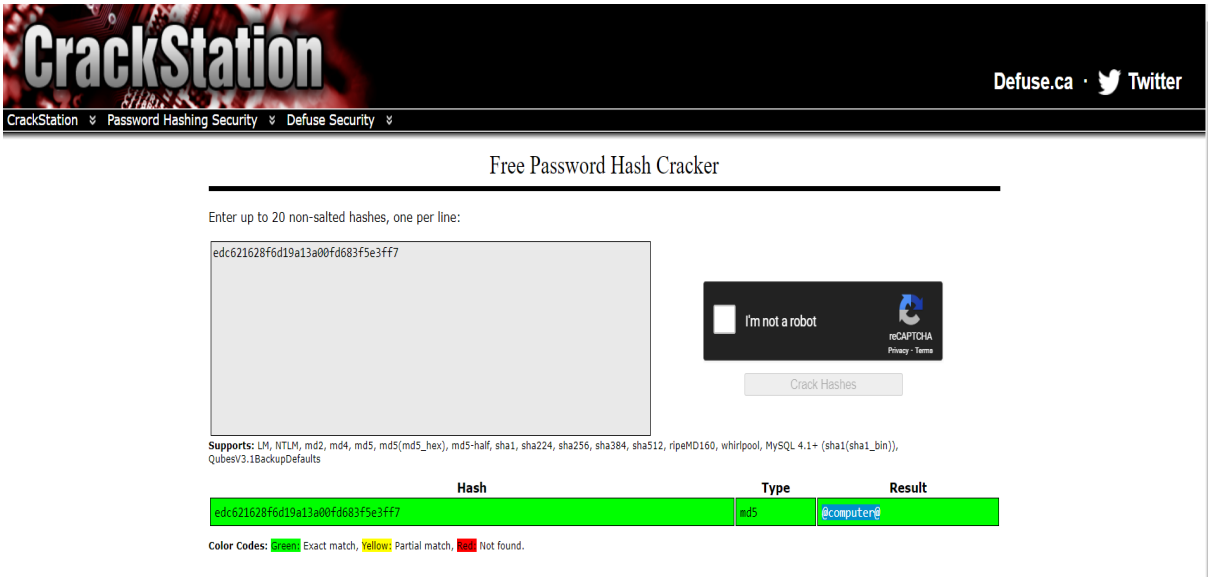


The encrypted password of the two users are being shown in the list.

```
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
|  1 | flynn    | edc621628f6d19a13a00fd683f5e3ff7 |
|  2 | admin    | 5f4dcc3b5aa765d61d8327deb882cf99 |
+----+----------+----------------------------------+
2 rows in set (0.00 sec)

mysql>
```

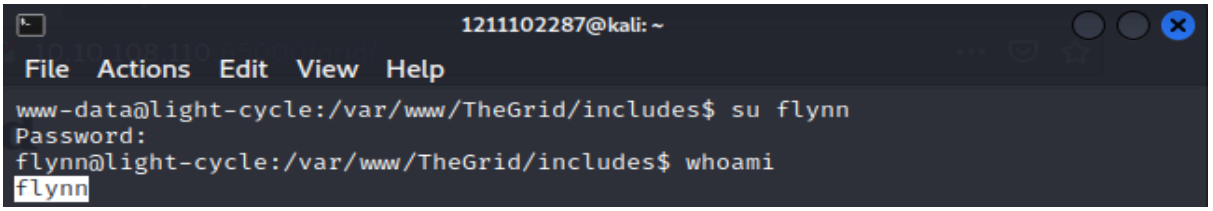
Copy Flynn's encrypted password and paste it at https://crackstation.net/ for password cracking. We can see that the result of the password in the **Result section** (highlighted)



Question 10

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

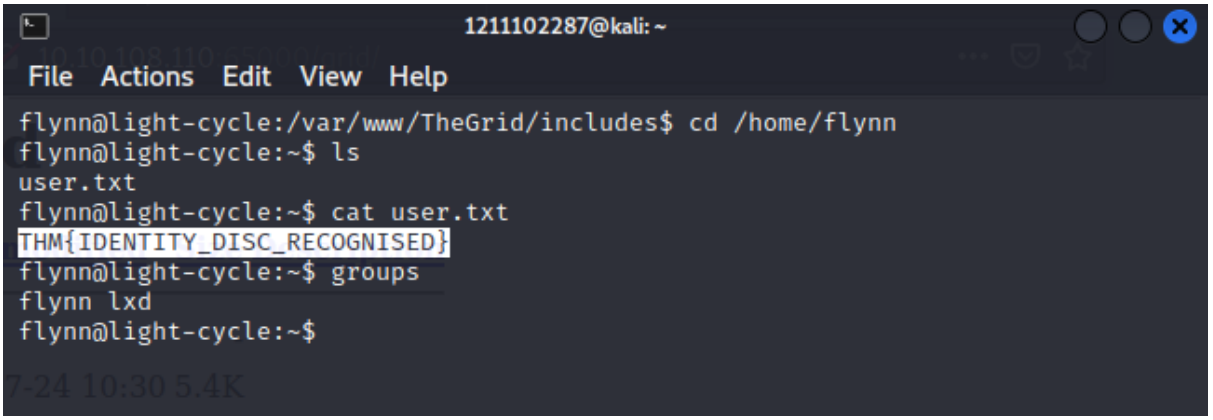
By using the username and password, we can change our user by using the su command. The new user could be made sure by using **"whoami"** (highlighted)



Question 11

What is the value of the user.txt flag?

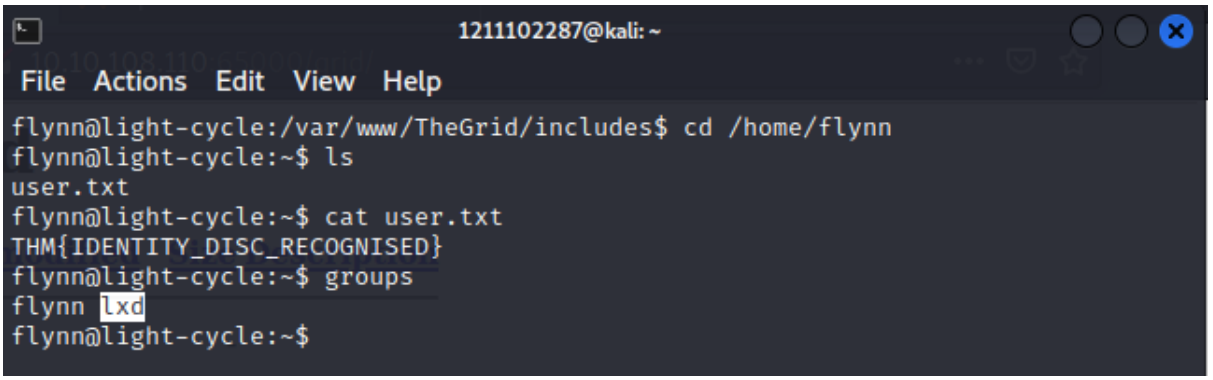
We have to find the root of Flynn's user. To find the text file inside the directory, **ls** is being used. We can see that there is a user.txt file. By using the **cat** command, we can read and see the contents in Flynn's directory. The flag could be seen in the Directory (highlighted)



Question 12

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

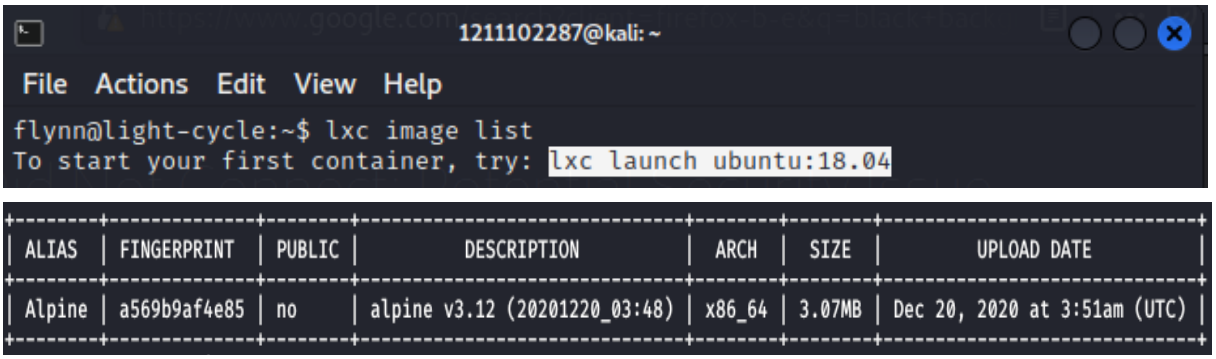
We can look for the group for the user by just inserting **"groups"**. The group of the user is shown in the line (highlighted)



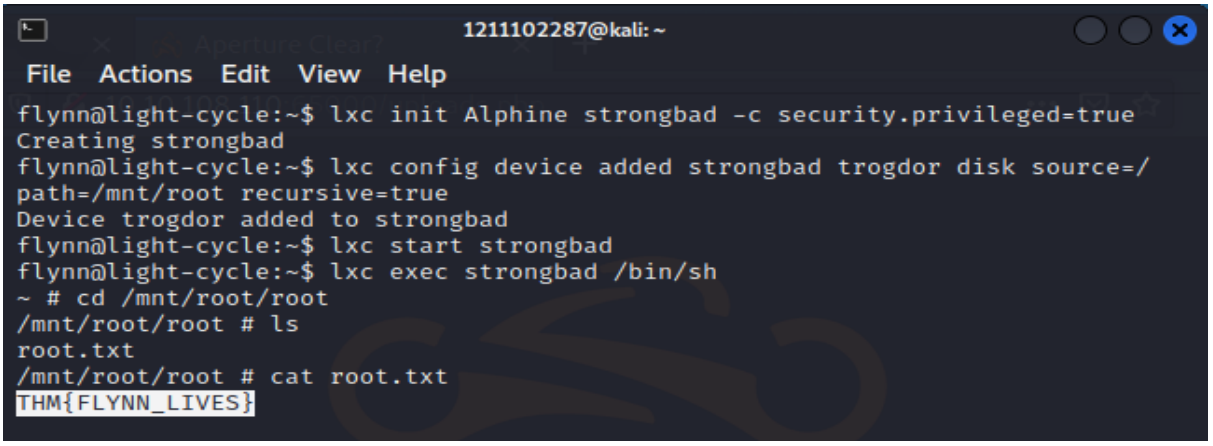
Question 13

What is the value of the root.txt flag?

Check the images which are available on the machine by using the command **lxc image list**. The list should pop up showing the details of the image.



After that, we have to initialize, configure the disks, and start the container. We named our container as **strongbad** and the device **trogdor**. Next, the commands are used to mount the storage. We can use the **ls** command to see the files in our directory. There is a file named **"root.txt"**. Cat the file and we can see a flag appeared there (highlighted).



Thought Process/Methodology:

Deploy the machine**,** use the **nmap** scan with the IP address to find the ports which are available. We can see that there are two ports which are open. We know that there are two ports which are open. By just adding the port **(65000)** after the IP address in the web browser, we could see there is a hidden website named **Light Cycle**. We can check for the hidden pages and directories for the page with Gobuster. A hidden file named **/uploads.php** file appears at the bottom of the terminal. Open Burp Suite and to bypass the client-side filter, we have to intercept the JavaScript code file containing the filter before it ever actually reaches our browser. The page for uploading files could be seen after the process. We have to upload and execute a reverse shell. Create our php file as **shell.jpg.php.** Change the IP to our linux machine and the port to 443. Upload the file in the upload page. After that, we can now see that the file is being uploaded successfully. The directory **/grid** could be seen as a storage where files are uploaded and saved. Use netcat command to listen for our shell session. By using the quick search command, we could know that the web.txt file we want to find is in the **/var/www/ directory.** Open the content in the directory by using the **cat** command. The flag inside the file could be seen. From the hint given by THM, we know that the command **(python3 -c 'import pty;pty.spawn("/bin/bash")')** and the command **(export TERM=xterm)** are used to upgrade and stabilize the shell. Use the **ls** command to show the list for all files in the current directory. To show the content in the dbauth.php file, the cat command is used. In the file, the password and user is being shown. Access and Log into our database using the credentials found. We can see that **"tron"** was being used in the database. Select the tron database by typing the "use tron"command. Now we are in the tron database. Use the "select * from users;" command to see the content inside. The encrypted password of the two users are being shown in the list. Copy Flynn's encrypted password and paste it at https://crackstation.net/ for password cracking. We can see that the result of the password in

the **Result section** By using the username and password, we can change our user by using the su command. The new user could be made sure by using **“whoami”.** We have to find the root of Flynn's user. To find the text file inside the directory, **ls** is being used. We can see that there is a user.txt file. By using the **cat** command, we can read and see the contents in Flynn's directory. The flag could be seen in the Directory. We can look for the group for the user by just inserting **“groups”**. The group of the user is shown in the line Check the images which are available on the machine by using the command **lxc image list**. The list should pop up showing the details of the image. After that, we have to initialize, configure the disks, and start the container. We named our container as **strongbad** and the device **trogdor**. Next, the commands are used to mount the storage. We can use the **ls** command to see the files in our directory. There is a file named **“root.txt”**. Cat the file and we can see a flag appeared there