PSP0201

WEEK 6

WRITE-UP

GROUP NAME : PELITA

ID	Name	Role
1211102057	Muhammad Syahir Nazreen Bin Abdul Hamid	Leader
1211101935	Mohamed Imran Bin Mohamed Yunus	Member
1211103220	Muhammad Firzan Ruzain Bin Firdus	Member
1211102060	Farris Aiman Bin Mohd Harris	Member

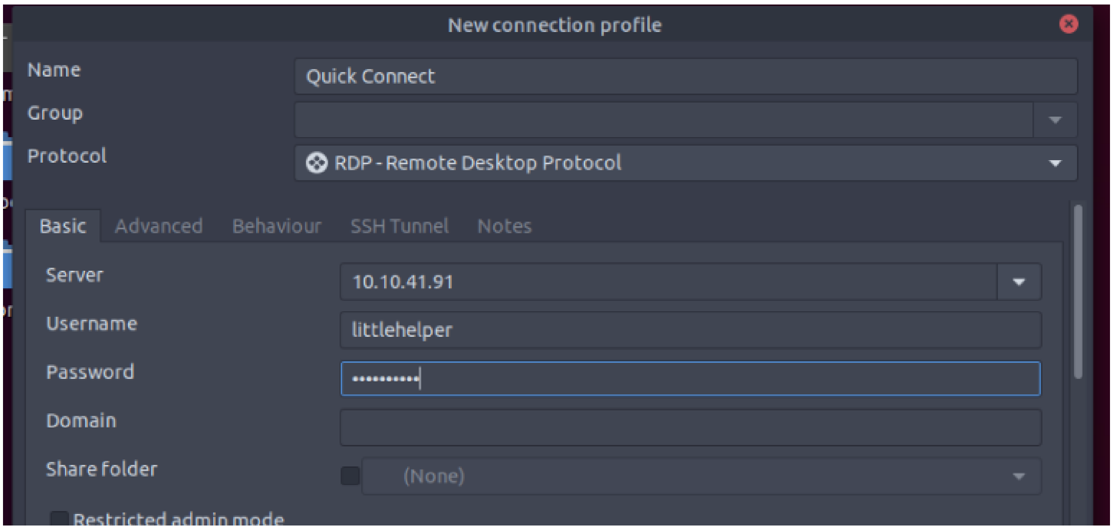
Day 21 - [Blue Teaming] Time for some ELForensics

Tools used: Kali, Remmina, Powershell

Solution/walkthrough:

<u>Question 1</u>

Created new profile for connection.



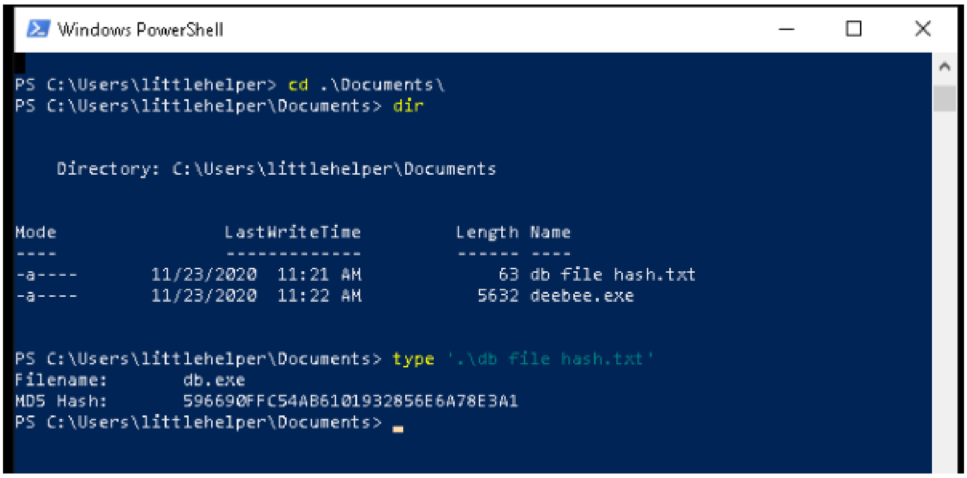
New connection profile

Name	Quick Connect
Group	
Protocol	RDP - Remote Desktop Protocol

Server	10.10.41.91
Username	littlehelper
Password	••••••••••
Domain	
Share folder	□ (None)

□ Restricted admin mode

Opened the windows powershell. Directed to the document folder and listed all files containing inside of it.



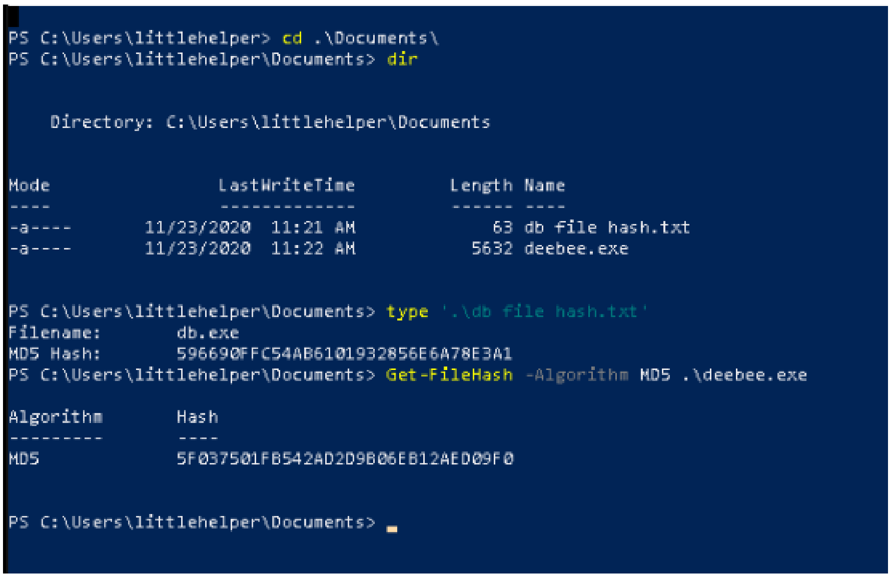
Windows PowerShell

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

Used command (type ’.\data file hash.txt’) to know the MD5 Hash. The hash is **596690FFC54AB6101932856E6A78E3A1**.

Question 2

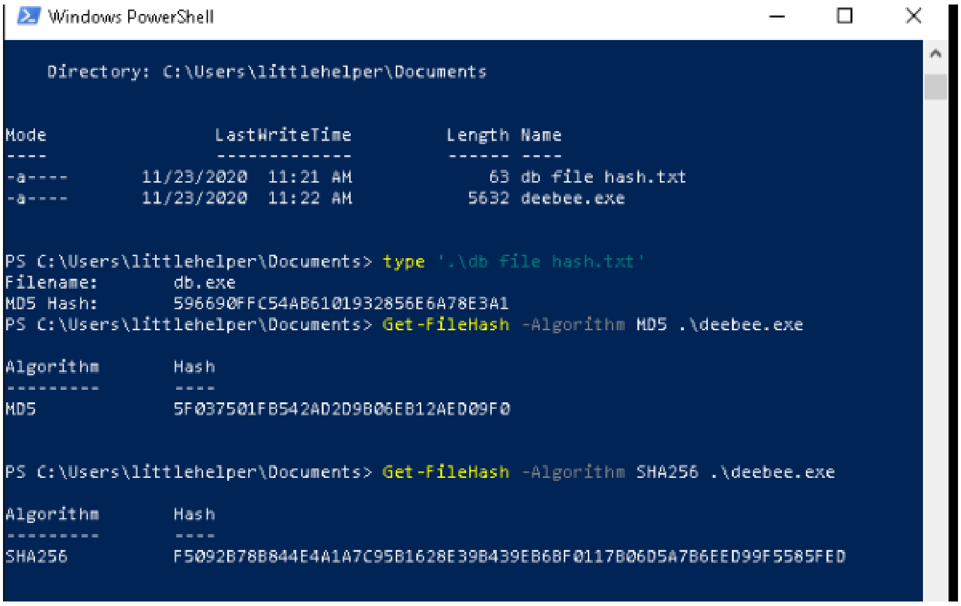
To get the MD5 file hash of the mysterious executable within the Documents folder, we used ‘Get-FileHash -Algorithm MD5 .\deebee.exe’ . It gets **5F037501FB542AD2D9B06EB12AED09F0** .



```
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> type '.\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>
```

Question 3

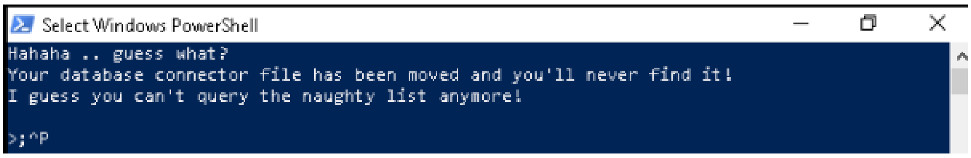
To get the SHA256 file hash of the mysterious executable within the Documents folder, we used ‘Get-FileHash -Algorithm SHA256 .\deebee.exe’ . It gets **F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED**.



```
    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> type '.\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
```

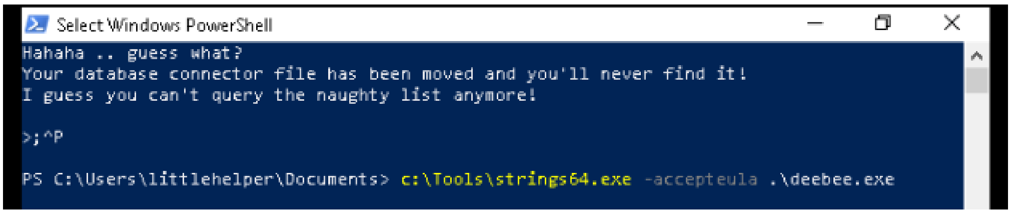
Question 4

Ran the deebee.exe . Notified that the file is moved elsewhere.

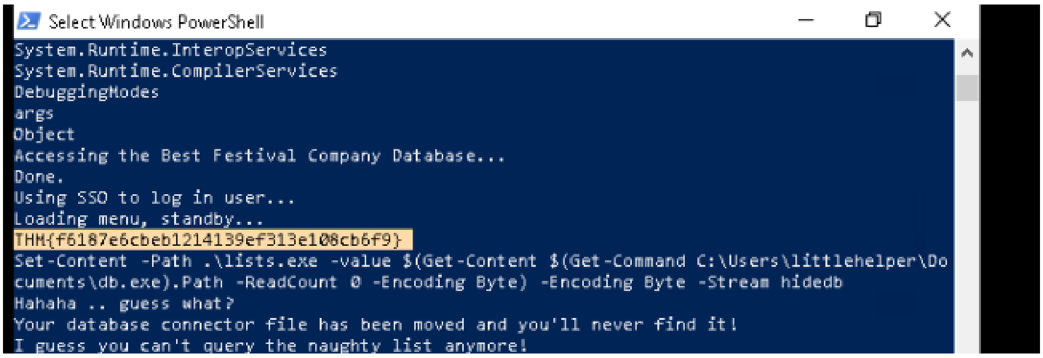


```
Hahaha .. guess what?
Your database connector file has been moved and you'll never find it!
I guess you can't query the naughty list anymore!

>;^P
```

Uesd a tool, String.exe to string scan the file. The flag were shown. **(THM{f6187e6cbeb1214139ef313e108cb6f9})**



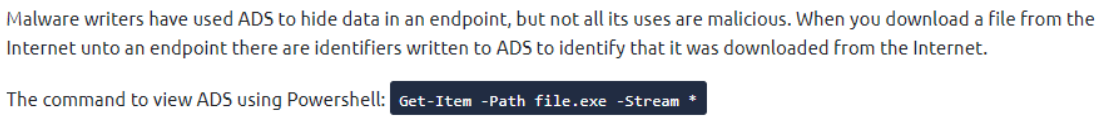
```
Hahaha .. guess what?
Your database connector file has been moved and you'll never find it!
I guess you can't query the naughty list anymore!

>;^P

PS C:\Users\littlehelper\Documents> c:\Tools\strings64.exe -accepteula .\deebee.exe
```



```
System.Runtime.InteropServices
System.Runtime.CompilerServices
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\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

The command to view ADS using Powershell: **Get-Item -Path file.exe -Stream ***

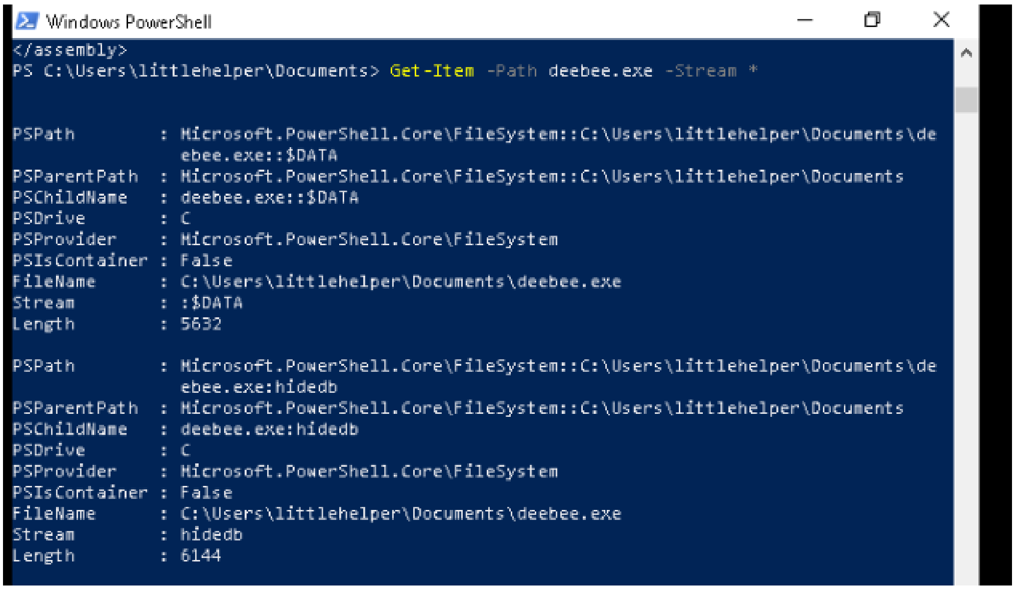


Malware writers have used ADS to hide data in an endpoint, but not all its uses are malicious. When you download a file from the Internet unto an endpoint there are identifiers written to ADS to identify that it was downloaded from the Internet.

The command to view ADS using Powershell: `Get-Item -Path file.exe -Stream *`

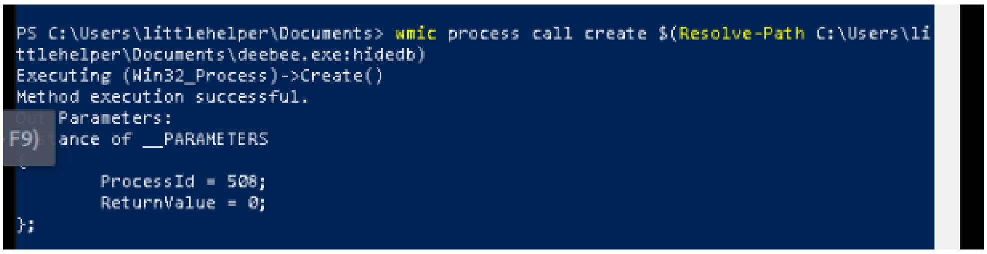
Question 6

Viewed ADS using powershell. Found 2 different Stream.



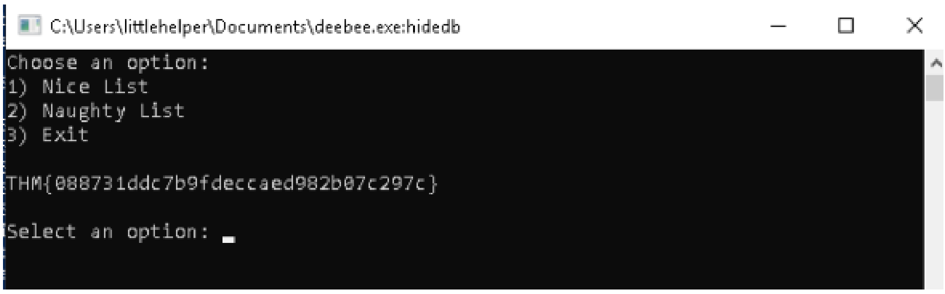
```
</assembly>
PS C:\Users\littlehelper\Documents> Get-Item -Path deebee.exe -Stream *


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
```

Ran the hidden executable hiding within ADS using the given command in hidedb stream.



```
PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-Path C:\Users\littlehelper\Documents\deebee.exe:hidedb)
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
F9) ance of __PARAMETERS
{
        ProcessId = 508;
        ReturnValue = 0;
};
```

Found the flag (**THM{088731ddc7b9fdeccaed982b07c297c}**).

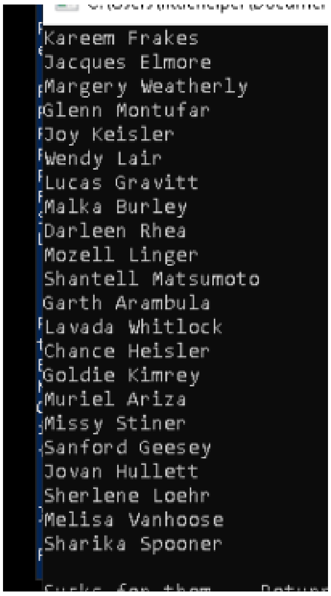


C:\Users\littlehelper\Documents\deebee.exe:hidedb

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

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option:
```

Question 7

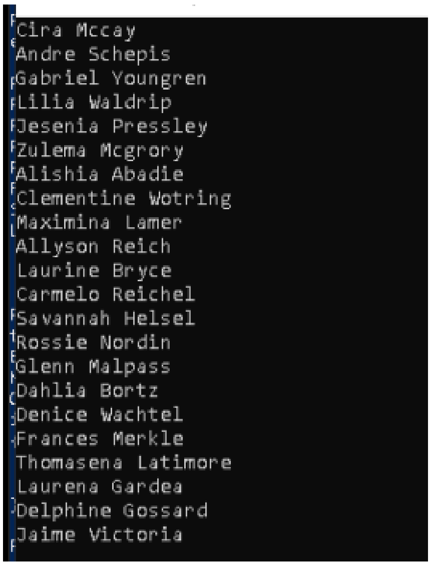
Sharika Spooner in on Naughty list.



```
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

Jaime Victoria in on Nice list .



```
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:

Created a new profile for the machine using the machine IP. Opened the windows powershell. Directed to the document folder and listed all files containing inside of it. Found 2 different file. Used the ‘type’ command to know the MD5 hash of the db file hash.txt. The hash is **596690FFC54AB6101932856E6A78E3A1**. To get the MD5 and SHA256 file hash of the mysterious executable within the Documents folder, we used ‘Get-FileHash -Algorithm MD5 .\deebee.exe’ for MD5 and ‘Get-FileHash -Algorithm SHA256 .\deebee.exe’ for SHA 256. Ran the deebee.exe . Notified that the file is moved elsewhere. String scanned it to show the flag. Viewed ADS using powershell. Found 2 different Stream. Ran the hidden executable hiding within ADS using the given command in hidedb stream. The flah , naughty list and nice list are shown.

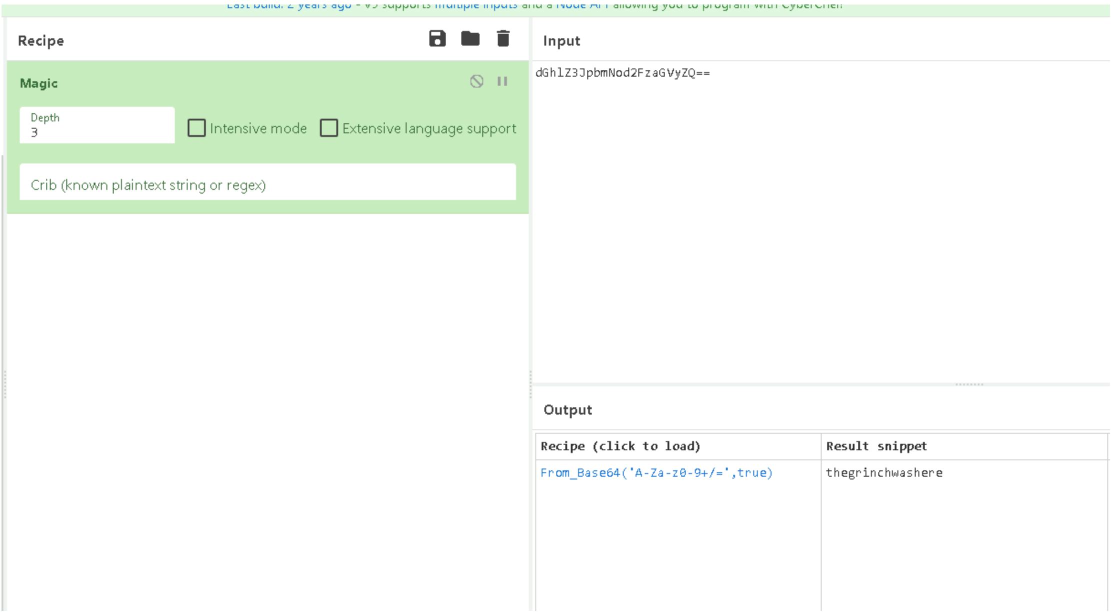
Day 22 - [Blue Teaming] Elf McEager becomes CyberElf

Tools used: Kali, Remmina, Cyberchef

Solution/walkthrough:

Question 1

What is the password to the KeePass database?



Last build: 2 years 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

```
dGhlZ3JpbmNod2FzaGVyZQ==
```

Output

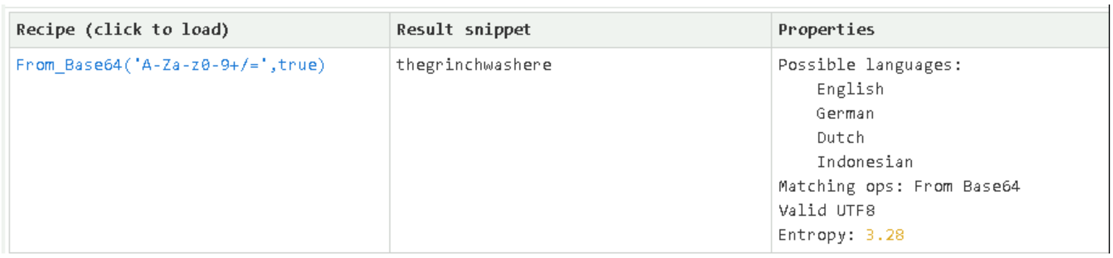
Recipe (click to load)	Result snippet
From_Base64('A-Za-z0-9+/=',true)	thegrinchwashere

The folder name can be decrypt by using CyberChef

Answer: **thegrinchwashere**

Question 2

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

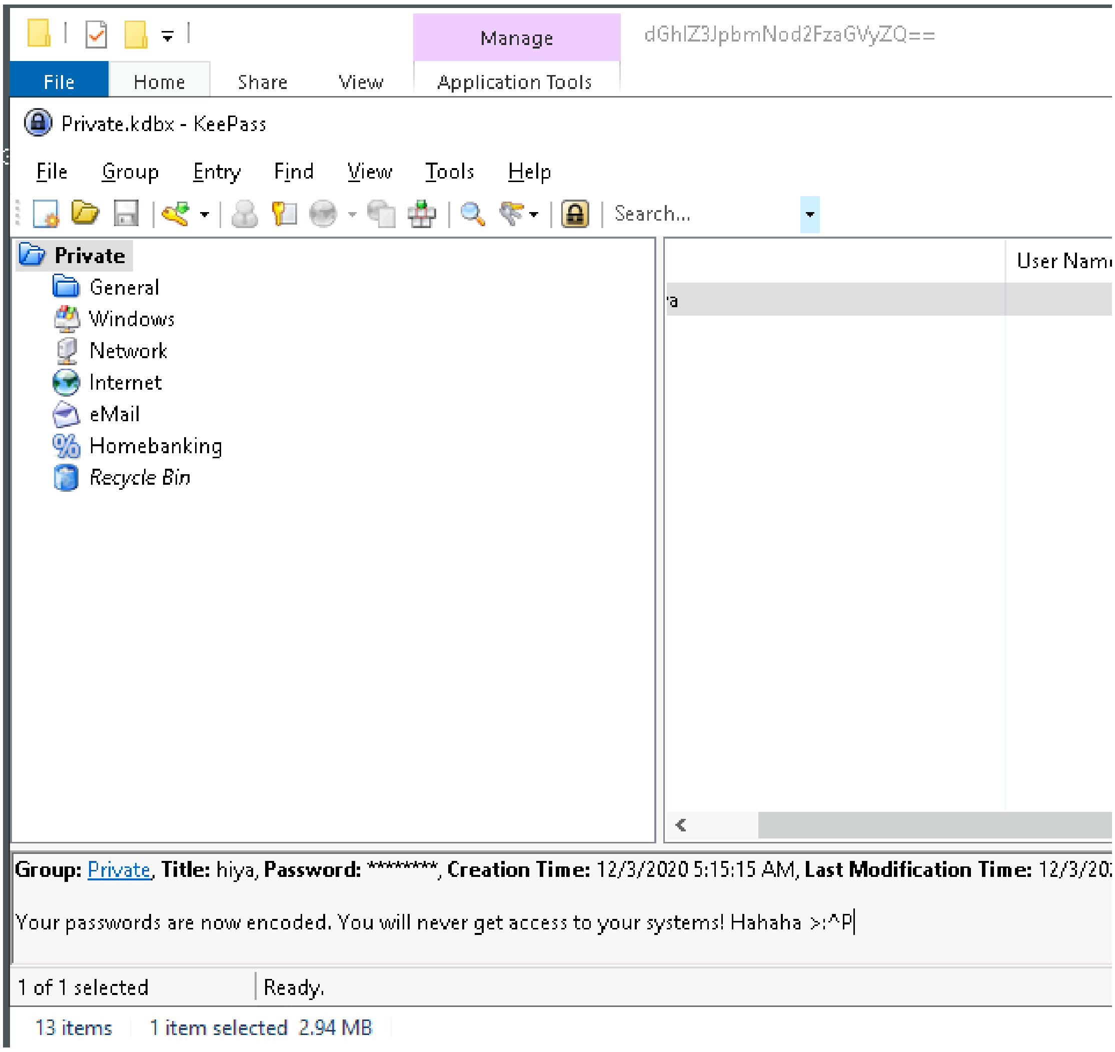


Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+/=',true)	thegrinchwashere	Possible languages: English German Dutch Indonesian Matching ops: From Base64 Valid UTF8 Entropy: 3.28

Answer: **Base64**

Question 3

What is the note on the hiya key?



Group: Private, **Title:** hiya, **Password:** ********, **Creation Time:** 12/3/2020 5:15:15 AM, **Last Modification Time:** 12/3/20

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

1 of 1 selected | Ready.

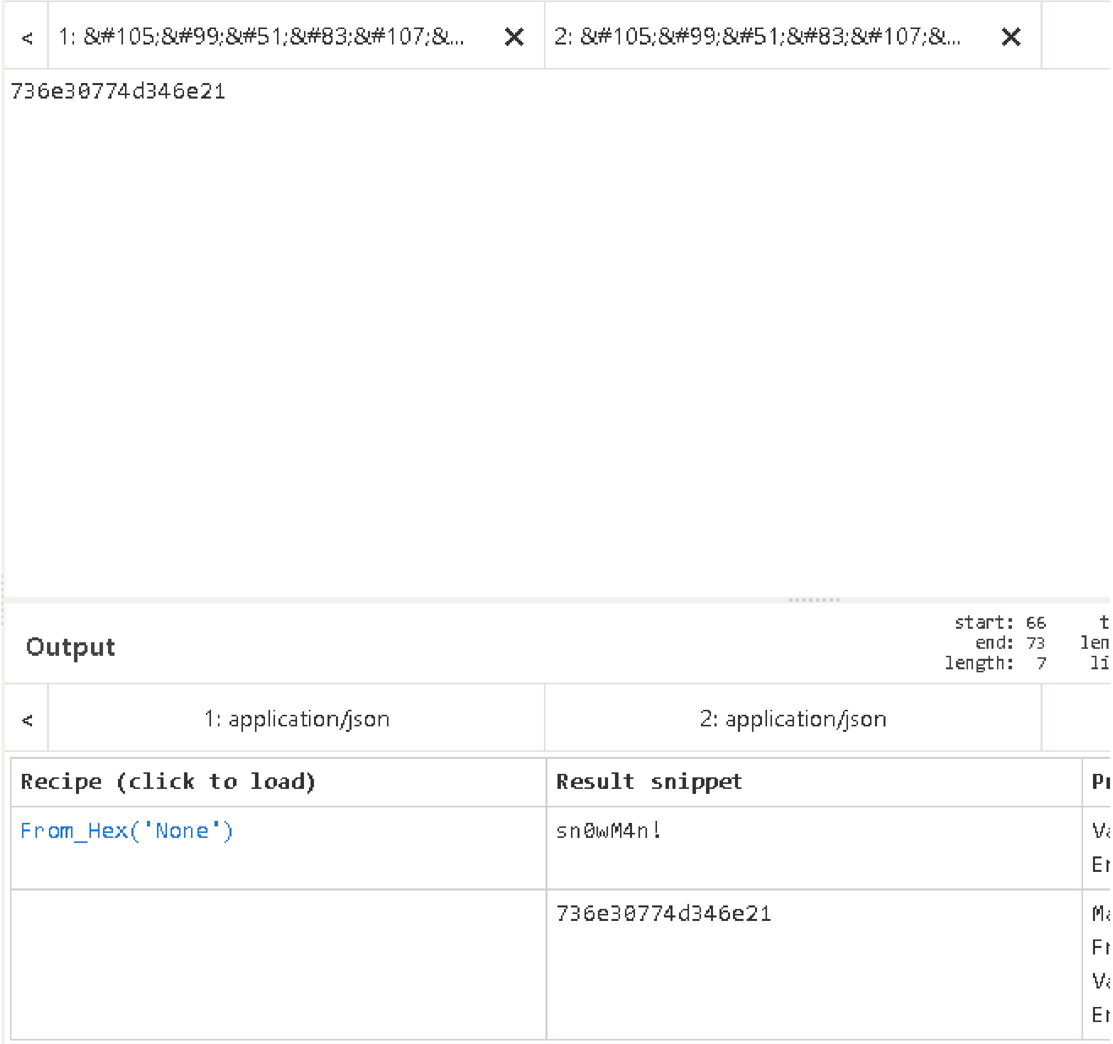
13 items | 1 item selected 2.94 MB

The note can be obtained from the entry

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

Question 4

What is the decoded password value of the Elf Server?



< 1: &#105;&#99;&#51;&#83;&#107;&... ✕ 2: &#105;&#99;&#51;&#83;&#107;&... ✕

```
736e30774d346e21
```

Output

```
 start: 66     t
   end: 73   len
length:  7    li
```

< 1: application/json 2: application/json

Recipe (click to load)	Result snippet	Pr
From_Hex('None')	sn0wM4n!	Va Er
	736e30774d346e21	Ma Fr Va Er

Answer: **sn0wm4n**!

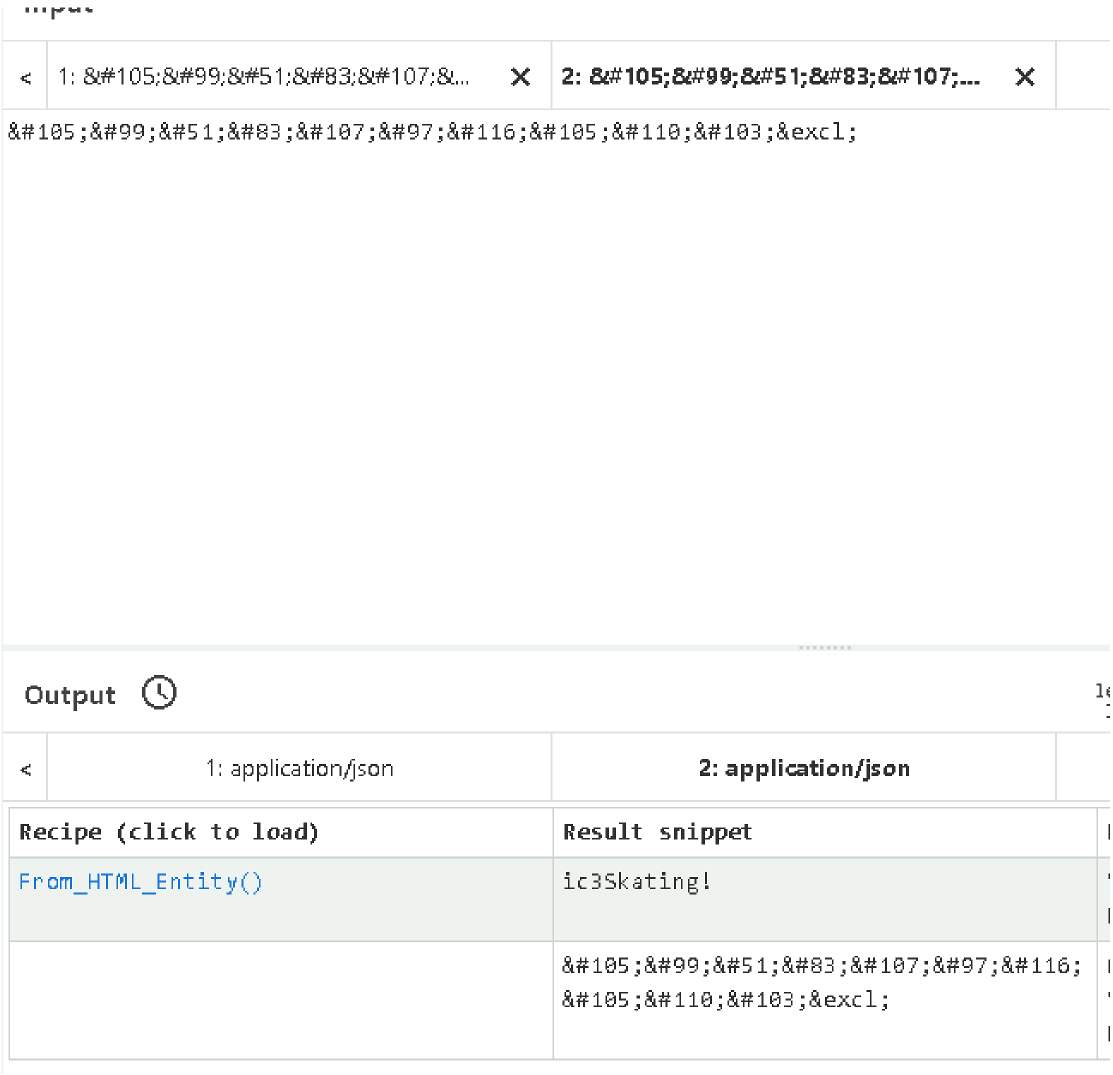
Question5

What was the encoding used on the Elf Server password?

Answer: **Hex**

Question 6

What is the decoded password value for ElfMail?



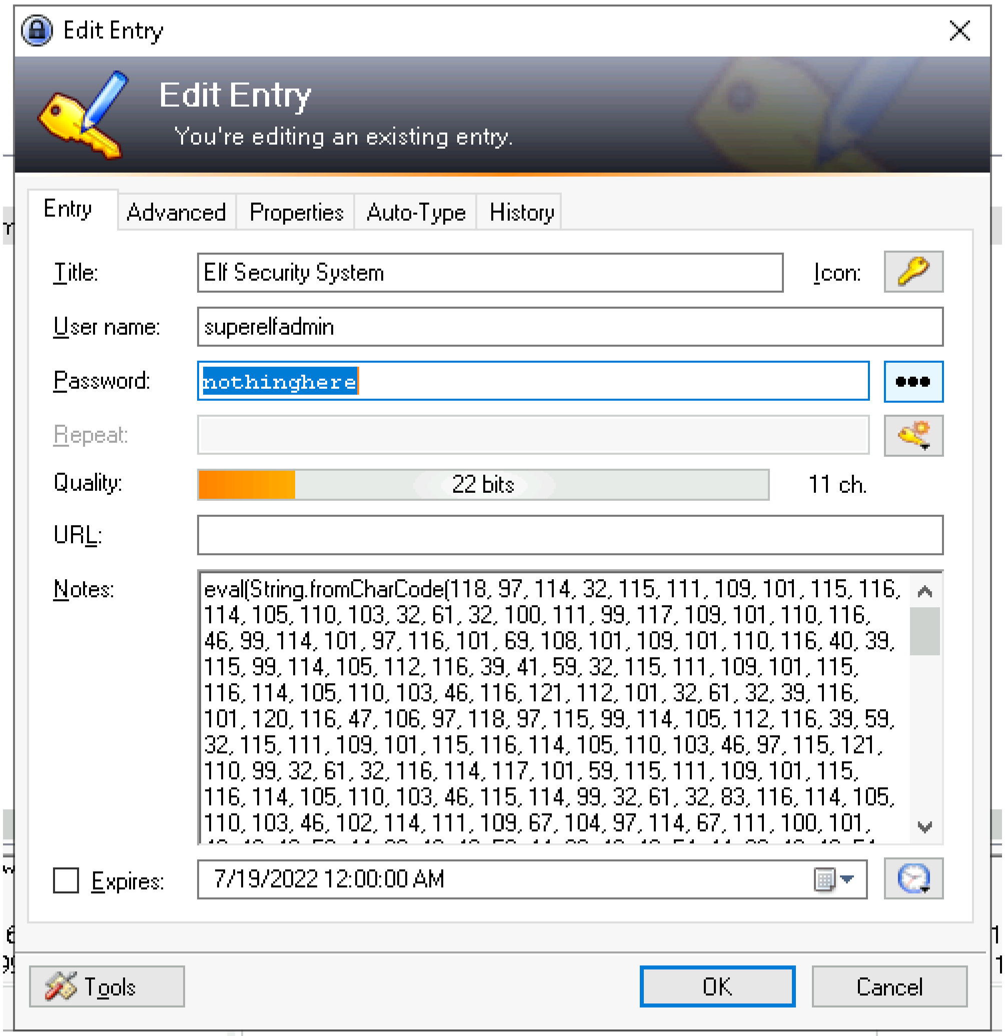
```
&#105;&#99;&#51;&#83;&#107;&#97;&#116;&#105;&#110;&#103;&excl;
```

Recipe (click to load)	Result snippet
From_HTML_Entity()	ic3Skating!
	ic3Skatin&#103;&excl;

Answer: **ic3Skating**

Question 7

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



Title: Elf Security System

User name: superelfadmin

Password: nothinghere

Quality: 22 bits 11 ch.

URL:

Notes:

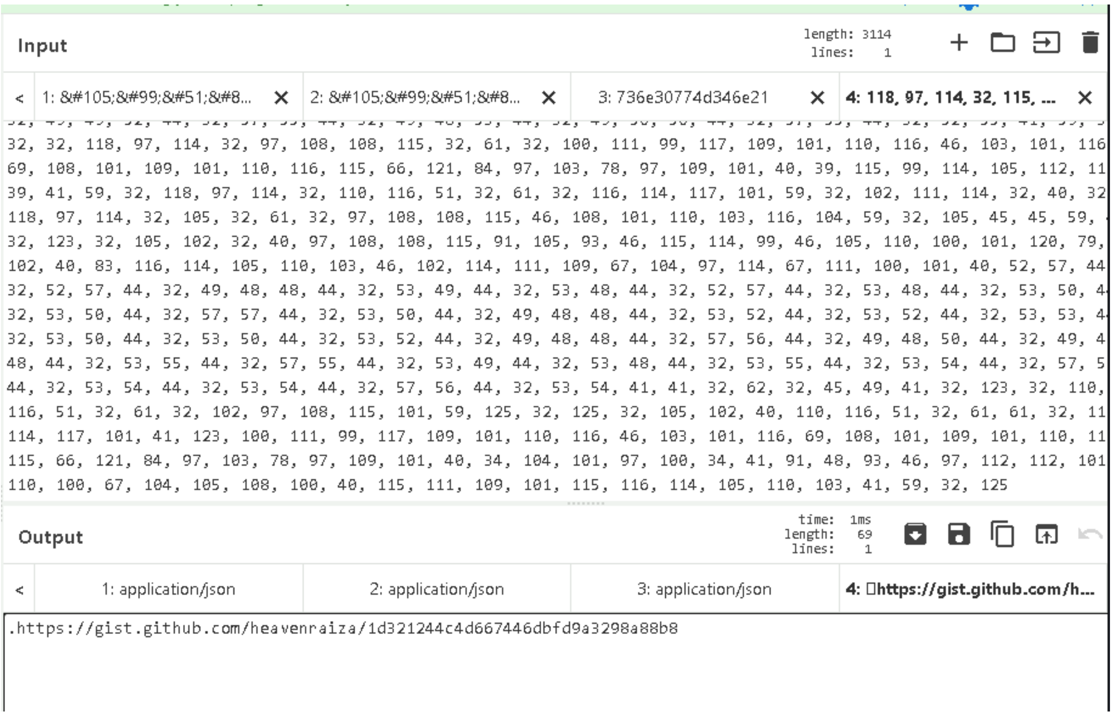
```
eval(String.fromCharCode(118, 97, 114, 32, 115, 111, 109, 101, 115, 116,
114, 105, 110, 103, 32, 61, 32, 100, 111, 99, 117, 109, 101, 110, 116,
46, 99, 114, 101, 97, 116, 101, 69, 108, 101, 109, 101, 110, 116, 40, 39,
115, 99, 114, 105, 112, 116, 39, 41, 59, 32, 115, 111, 109, 101, 115,
116, 114, 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,
```

□ Expires: 7/19/2022 12:00:00 AM

Answer: **superelfadmin:nothinghere**

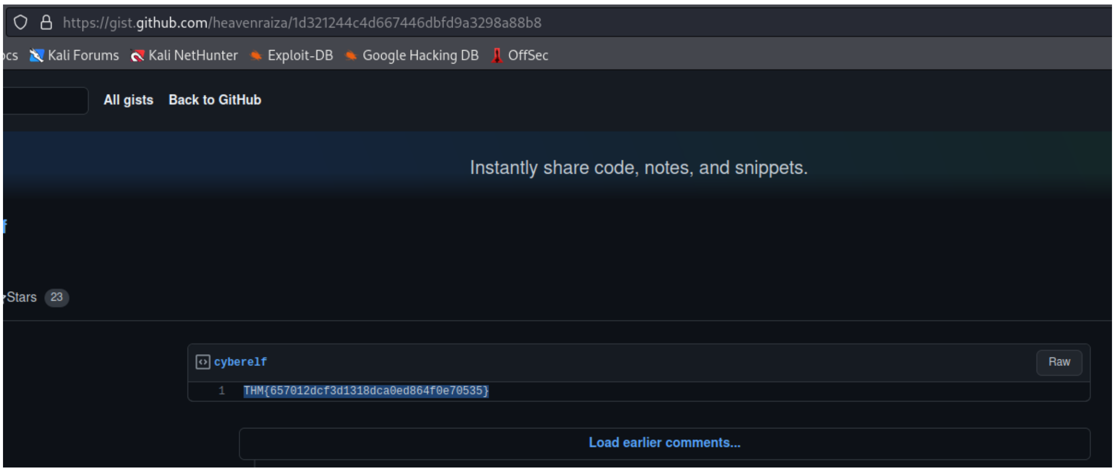
Question 8

Decode the last encoded value. What is the flag?



```
32, 32, 118, 97, 114, 32, 97, 108, 108, 115, 32, 61, 32, 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, 39, 115, 99, 114, 105, 112, 11
39, 41, 59, 32, 118, 97, 114, 32, 110, 116, 51, 32, 61, 32, 116, 114, 117, 101, 59, 32, 102, 111, 114, 32, 40, 32
118, 97, 114, 32, 105, 32, 61, 32, 97, 108, 108, 115, 46, 108, 101, 110, 103, 116, 104, 59, 32, 105, 45, 45, 59,
32, 123, 32, 105, 102, 32, 40, 97, 108, 108, 115, 91, 105, 93, 46, 115, 114, 99, 46, 105, 110, 100, 101, 120, 79,
102, 40, 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, 50, 4
32, 53, 50, 44, 32, 57, 57, 44, 32, 53, 50, 44, 32, 49, 48, 48, 44, 32, 53, 52, 44, 32, 53, 52, 44, 32, 53, 53, 4
32, 53, 50, 44, 32, 53, 50, 44, 32, 53, 52, 44, 32, 49, 48, 48, 44, 32, 57, 56, 44, 32, 49, 48, 50, 44, 32, 49, 4
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, 5
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, 11
114, 117, 101, 41, 123, 100, 111, 99, 117, 109, 101, 110, 116, 46, 103, 101, 116, 69, 108, 101, 109, 101, 110, 11
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
```

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



```
THM{657012dcf3d1318dca0ed864f0e70535}
```

The charcode will be decrypted into a github link, the flag is obtained from there.

Answer: **THM{657012dcf3d1318dca0ed864f0e70535}**

Thought Process/Methodology:

We can access the virtual machine by using remmina along with the username and password given. First of all the master key to the KeePass database can be obtained by decrypting the folder name in the desktop which is actually **thegrinchwashere**. The encoding method that was listed is **Base64**. After accessing the KeePass database we can see there is an entry saying all the passwords were decrypted. The note from the entry is "**Your passwords are now encoded. You will never get access to your systems! Hahaha >:^P"**. We then can proceed to decode one by one all the passwords. The Elf Server password can be decoded from **Hex** and we will get the password which is **sn0wm4n**!**.** For elfmail the password is decoded from html entity and we get **ic3Skating**. The username and password for Elf Security System is **superelfadmin** and **nothinghere** respectively. Lastly to get the flag we need to decode the notes from the Elf Security Team entry by using CyberChef. By using the charcode recipe twice we get a github link. From there we can get the flag which is **THM{657012dcf3d1318dca0ed864f0e70535}.**

DAY 23: The Grinch strikes again

Tools used: Kali, Remmina, cyberchef

Solution/walkthrough:

Question 1

Qs: What does the wallpaper say?

Answer: THIS IS FINE

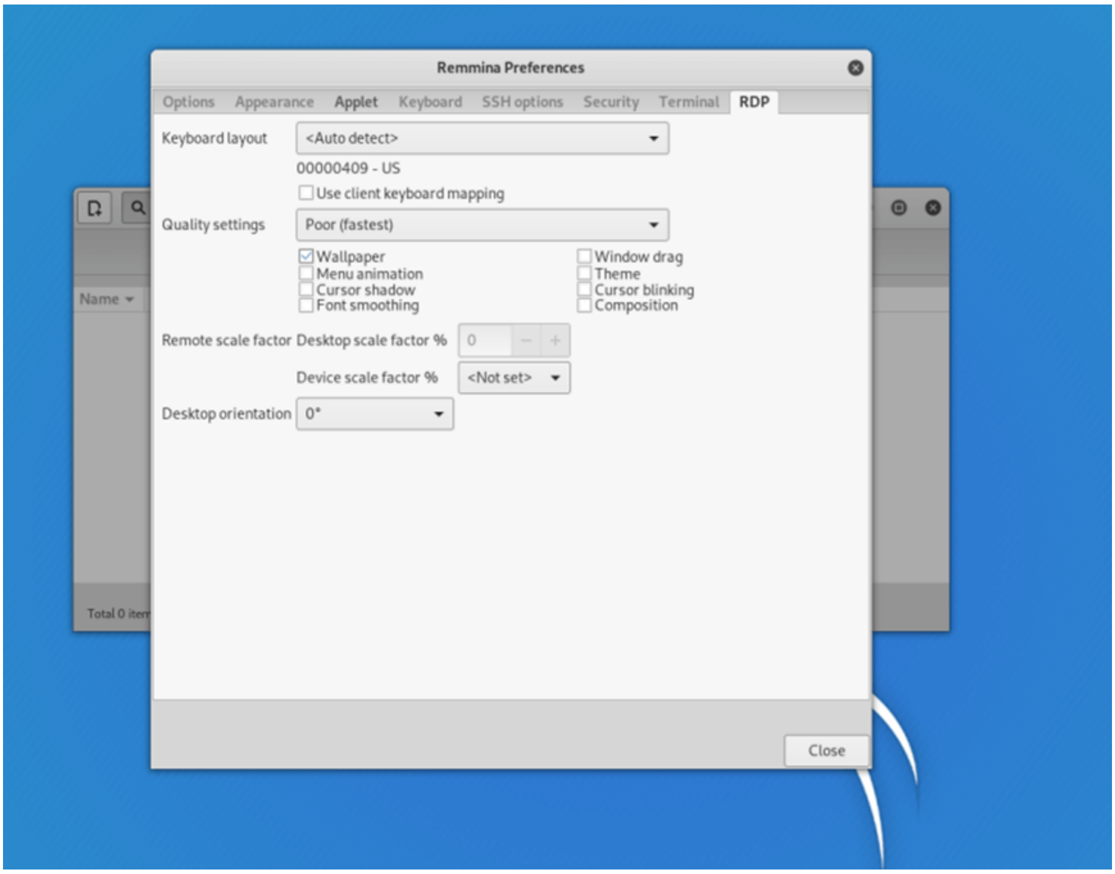
THIS IS FINE

Question 2

Qs:

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

Answer: nomorebestfestivalcompany



Keyboard layout <Auto detect>

00000409 - US

□ Use client keyboard mapping

Quality settings Poor (fastest)

☑ Wallpaper
□ Menu animation
□ Cursor shadow
□ Font smoothing
□ Window drag
□ Theme
□ Cursor blinking
□ Composition

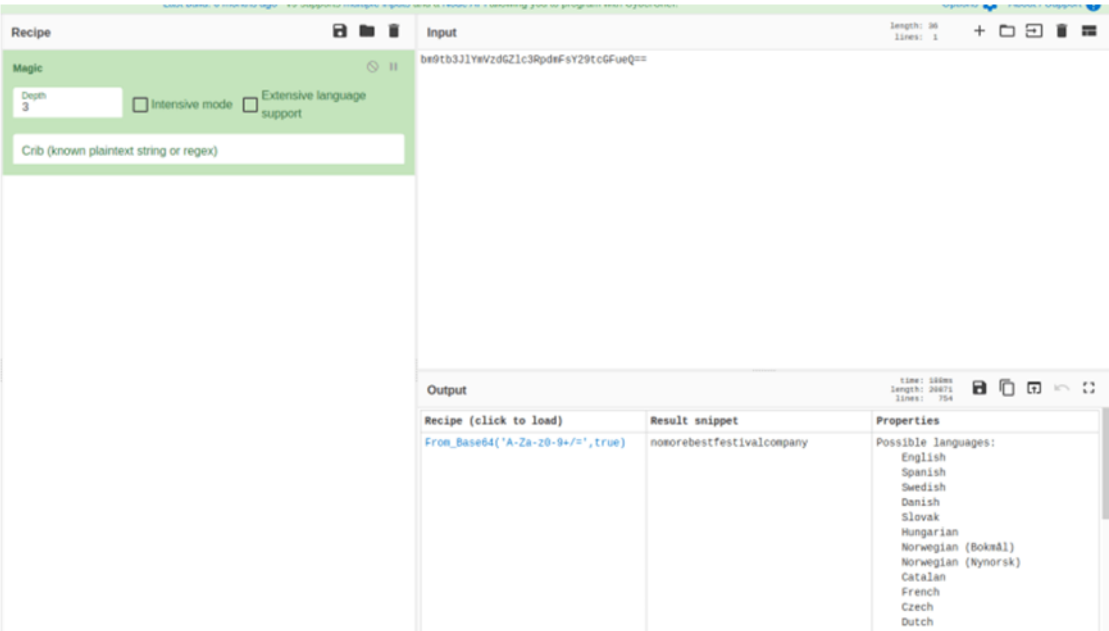
Remote scale factor Desktop scale factor % 0

Device scale factor % <Not set>

Desktop orientation 0°

Login as administrator and put sn0wF!akes!!! for the password.

We will find an encrypted bitcoin address.



Recipe

Magic

Depth
3

□ Intensive mode □ Extensive language support

Crib (known plaintext string or regex)

Input

length: 36
lines: 1

```
bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==
```

Output

time: 186ms
length: 20871
lines: 754

Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+/=',true)	nomorebestfestivalcompany	Possible languages: English Spanish Swedish Danish Slovak Hungarian Norwegian (Bokmål) Norwegian (Nynorsk) Catalan French Czech Dutch

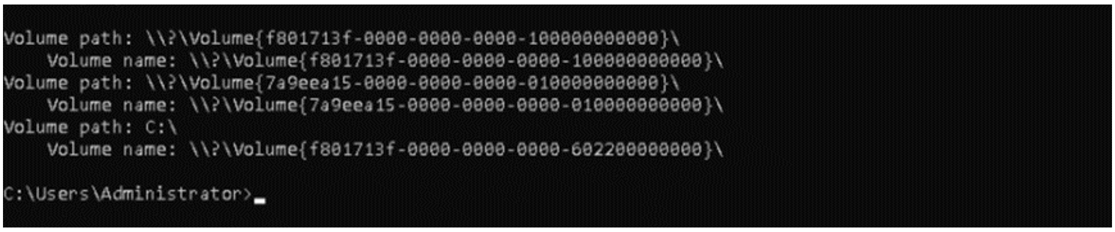
<u>So now we will use cyberchef to decode that address and we will get the answer</u>

Question 3

Qs:

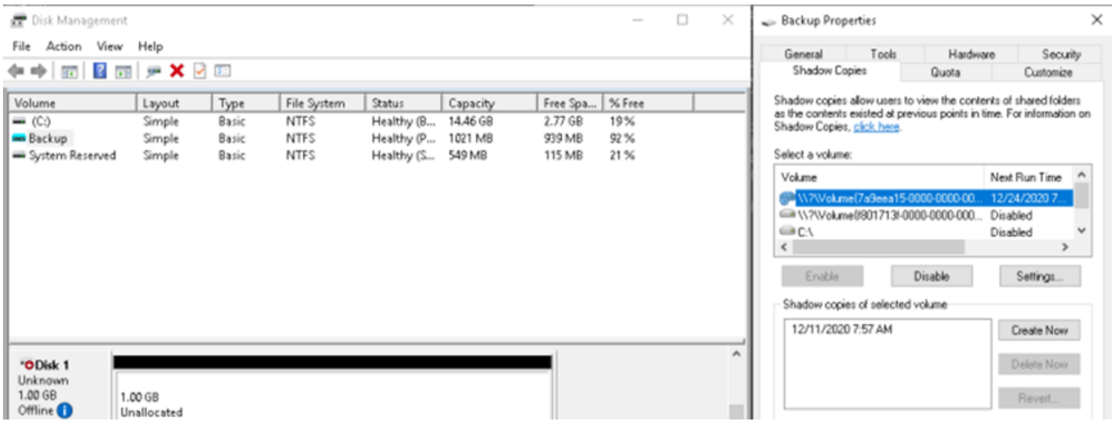
At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files?

Answer: .grinch



```
Volume path: \\?\Volume{f801713f-0000-0000-0000-100000000000}\
    Volume name: \\?\Volume{f801713f-0000-0000-0000-100000000000}\
Volume path: \\?\Volume{7a9eea15-0000-0000-0000-010000000000}\
    Volume name: \\?\Volume{7a9eea15-0000-0000-0000-010000000000}\
Volume path: C:\
    Volume name: \\?\Volume{f801713f-0000-0000-0000-602200000000}\

C:\Users\Administrator>_
```

First open Task Scheduler and pick the last schedule, we noticed that there is a VSS volume with a matching ID but unlike C it does not have a letter assigned



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(C:)	Simple	Basic	NTFS	Healthy (B...	14.46 GB	2.77 GB	19 %
Backup	Simple	Basic	NTFS	Healthy (P...	1021 MB	939 MB	92 %
System Reserved	Simple	Basic	NTFS	Healthy (S...	549 MB	115 MB	21 %

Disk 1
Unknown
1.00 GB
Offline

1.00 GB
Unallocated

Shadow copies allow users to view the contents of shared folders as the contents existed at previous points in time. For information on Shadow Copies, click here.

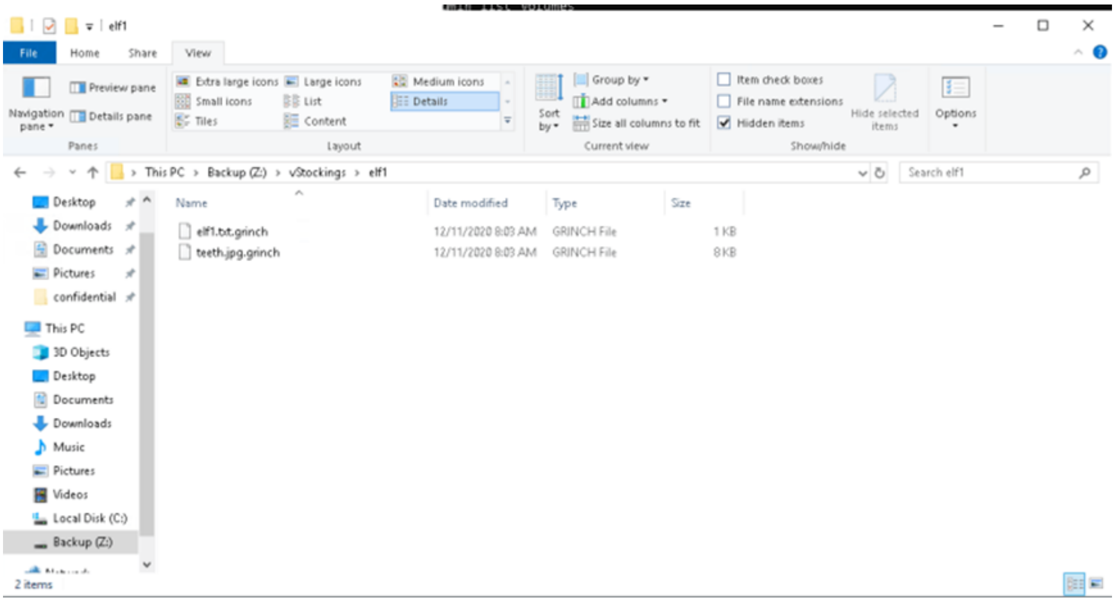
Select a volume:

Volume	Next Run Time
\\?\Volume{7a9eea15-0000-0000-00...	12/24/2020 7...
\\?\Volume{f801713f-0000-0000-000...	Disabled
C:\	Disabled

Shadow copies of selected volume

12/11/2020 7:57 AM

So we will use Disk Management and find the partial labeled backup,when we navigate to shadow copies tab we see there we see is a copy with a matching ID.



☐ Item check boxes
☐ File name extensions
☑ Hidden items

This PC › Backup (Z:) › vStockings › elf1

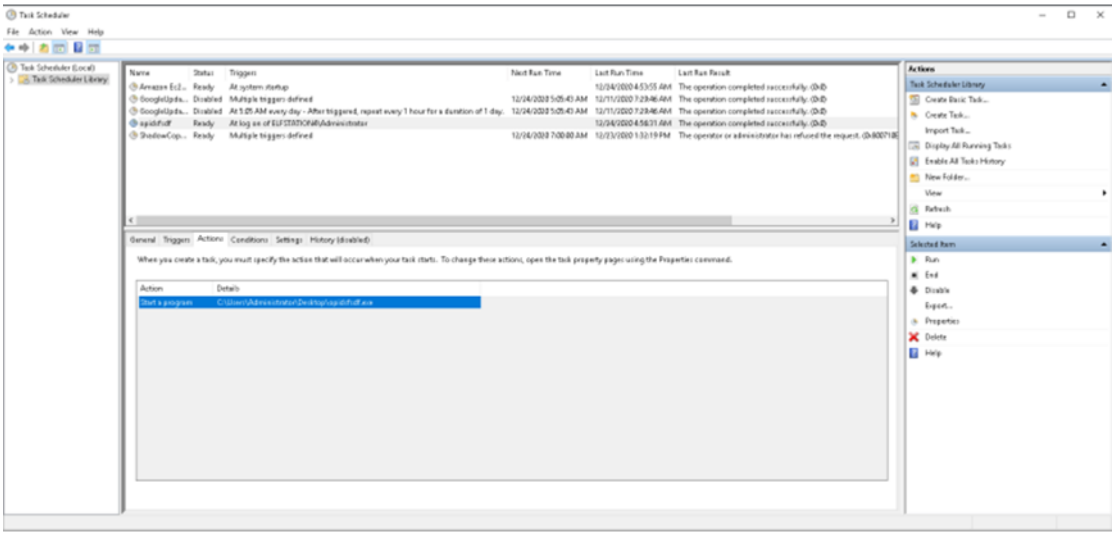
Name	Date modified	Type	Size
elf1.txt.grinch	12/11/2020 8:03 AM	GRINCH File	1 KB
teeth.jpg.grinch	12/11/2020 8:03 AM	GRINCH File	8 KB

Now after we done with all the backup we can go to file explorer.Go to Hidden Items and when we navigate to vStockings/elf1 in our drive we see the files have been change to the answer

Question 4

Qs: **What is the name of the suspicious scheduled task?**

Answer: opidsfsdf



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result
Amazon Ec2...	Ready	At system startup		12/24/2020 4:53:55 AM	The operation completed successfully. (0x0)
GoogleUpda...	Disabled	Multiple triggers defined	12/24/2020 5:05:43 AM	12/11/2020 7:29:46 AM	The operation completed successfully. (0x0)
GoogleUpda...	Disabled	At 5:05 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	12/24/2020 5:05:43 AM	12/11/2020 7:29:46 AM	The operation completed successfully. (0x0)
opidsfsdf	Ready	At log on of ELFSTATION\Administrator		12/24/2020 4:56:31 AM	The operation completed successfully. (0x0)
ShadowCop...	Ready	Multiple triggers defined	12/24/2020 7:00:00 AM	12/23/2020 1:32:19 PM	The operator or administrator has refused the request. (0x80071

When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

Action	Details
Start a program	C:\Users\Administrator\Desktop\opidsfsdf.exe

With Task Scheduler we will take at a suspicious file name opidsfsdf (our first answer). When we examine the properties we see this this file run a file located at

C:\User\Administrator\Desktop\opidsfsdf.exe.(our second answer)

Question 5

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

Answer: **C:\users\administrator\desktop\opidsfsdf.exe**

Question 6

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

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

At the same time, it also ask us the ShadowCopyVolume ID of the VSS task whichwe have already found earlier.

Which was *7a9eea15-0000-0000-0000-010000000000*

Question 7

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

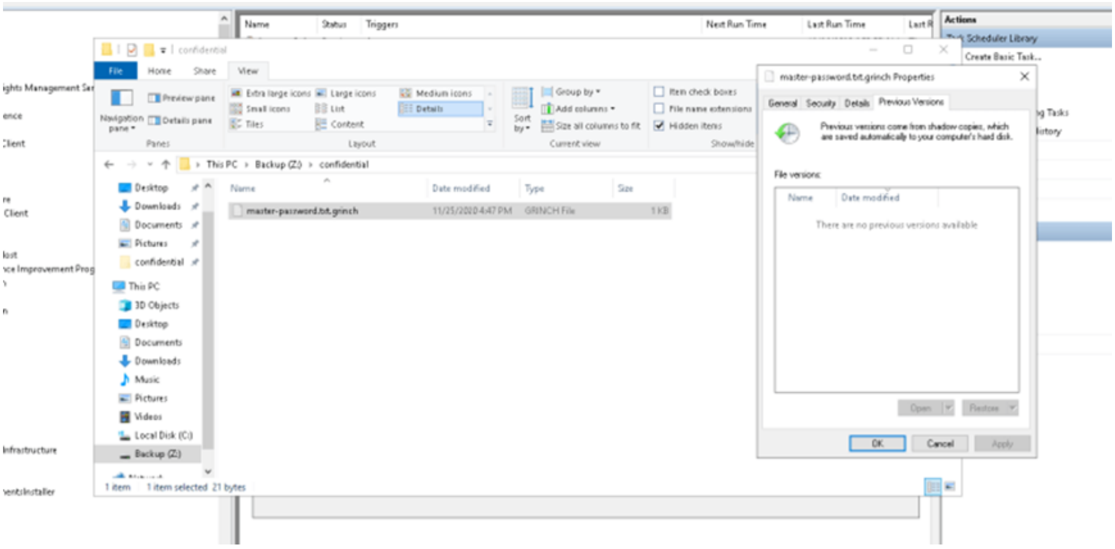
Answer: Confidential

The next ask us the name of the hidden folder on this drive.we can already tell by the fact that it is slightly transparent.But still we can see the name of the drive confidential which further show us the fact it is hidden.

Question 8

Qs: 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?

Answer: m33pa55w0rdIZseecure!



master-password.txt.grinch Properties

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

There are no previous versions available

This PC > Backup (Z:) > confidential
master-password.txt.grinch 11/25/2020 4:47 PM GRINCH File 1 KB
General
Security
Details
Previous Versions
File versions:
Open
Restore
OK
Cancel
Apply
1 item 1 item selected 21 bytes

Next, we want to restore the previous version of the master-password.txt.grinch file. We can do this by right-clicking and open the file properties. Then navigate to the Previous Versions tab and select OK.

Lastly open the file with notepad to reveal the flag

Thought Process/Methodology:

For getting the answer it was quite easy as we just need to enter all the necessary information that have already been given. Login as administrator and put the password to gain access and see the wallpaper. We will then find an encrypted bitcoin address for us that we will use at cyberchef to decode that address and we will get the second answer. First open Task Scheduler and pick the last schedule, we noticed that there is a VSS volume with a matching ID but unlike C it does not have a letter assigned so we will use Disk Management and find the partial labeled backup, when we navigate to shadow copies tab we see there we see is a copy with a matching ID. Now after we done with all the backup we can go to file explorer. Go to Hidden Items and when we navigate to vStockings/elf1 in our drive we see the files have been change to the answer. With Task Scheduler we will take at a suspicious file name opidsfsdf (our first answer). When we examine the properties we see this this file run a file located at C:\User\Administrator\Desktop\opidsfsdf.exe.(our second answer). At the same

time, it also ask us the ShadowCopyVolume ID of the VSS task which we have already found earlier.

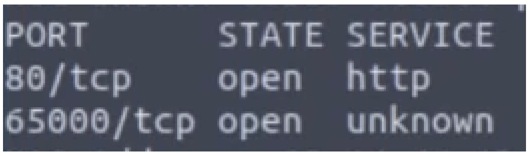
Then next ask us the name of the hidden folder on this drive.we can already tell by the fact that it is slightly transparent.But still we can see the name of the drive confidential which further show us the fact it is hidden.Last but least, we want to restore the previous version of the master-password.txt.grinch file. We can do this by right-clicking and open the file properties. Then navigate to the Previous Versions tab and select OK. At the end of it open the file with notepad to reveal the flag

Day 24 - The Trial Before Christmas

Tools used - Kali, MySQL, Burp Suite, Crack Station

Question 1

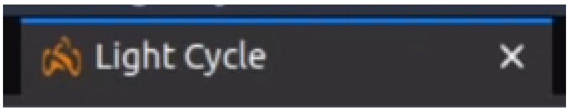
The ports that are open are **80, 65000**



```
PORT      STATE SERVICE
80/tcp    open  http
65000/tcp open  unknown
```

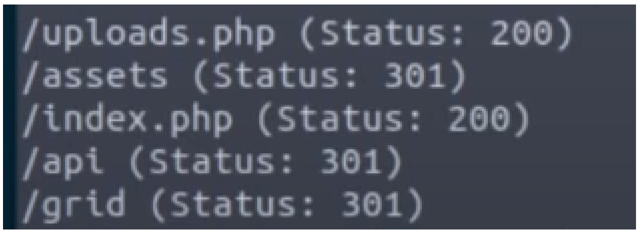
Question 2

The title of the hidden website is **Light Cycle**



Question 3

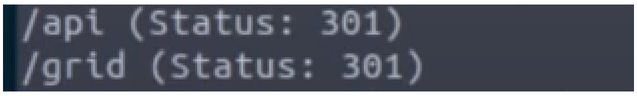
The name of the hidden php page is **/uploads.php**



```
/uploads.php (Status: 200)
/assets (Status: 301)
/index.php (Status: 200)
/api (Status: 301)
/grid (Status: 301)
```

Question 4

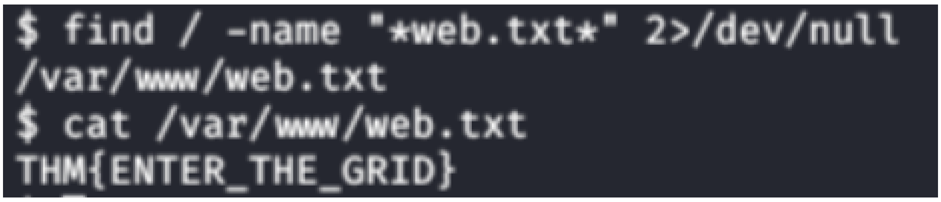
The name of the hidden directory where files uploads are saved is called **/grid**



```
/api (Status: 301)
/grid (Status: 301)
```

Question 5

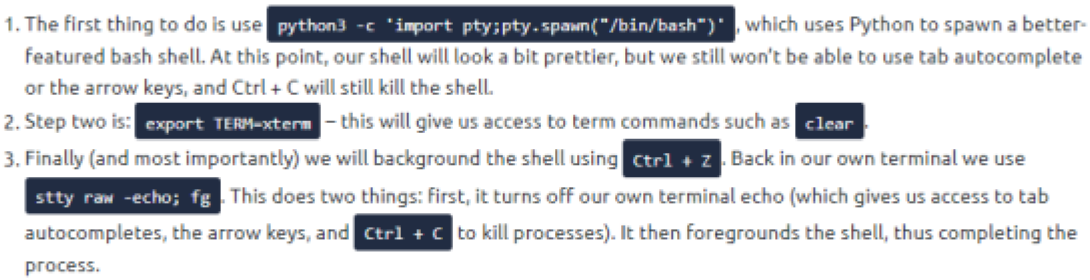
The value of the web.txt flag is **THM{ENTER_THE_GRID}**



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

Question 6

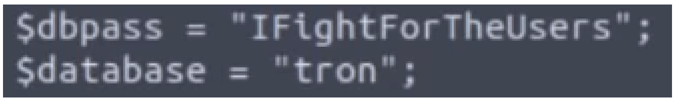
lines used to upgrade and stabilize your shell are **python3 -c 'import pty;pty.spawn("/bin/bash")' , export TERM=xterm , stty raw -echo; fg .**



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.

Question 7

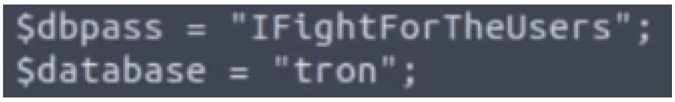
The credentials that I found was **tron:IFightForTheUsers**



```
$dbpass = "IFightForTheUsers";
$database = "tron";
```

Question 8

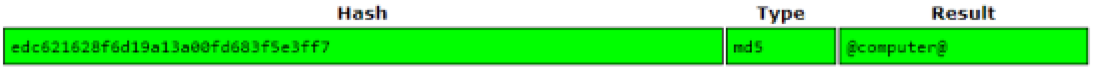
The name of the database is **tron**



```
$dbpass = "IFightForTheUsers";
$database = "tron";
```

Question 9

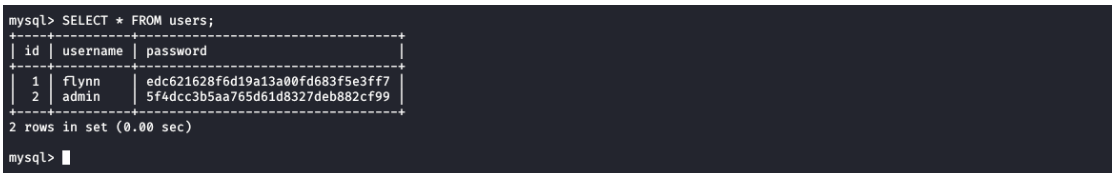
The password is **@computer@**



Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

Question 10

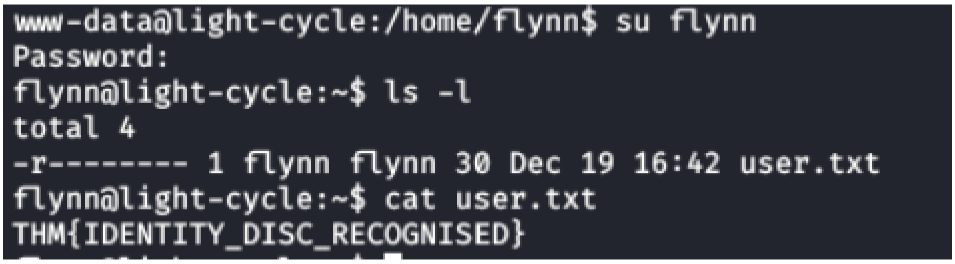
The user is switched to **Flynn**



```
mysql> SELECT * FROM users;
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
|  1 | flynn    | edc621628f6d19a13a00fd683f5e3ff7 |
|  2 | admin    | 5f4dcc3b5aa765d61d8327deb882cf99 |
+----+----------+----------------------------------+
2 rows in set (0.00 sec)

mysql> █
```

Question 11

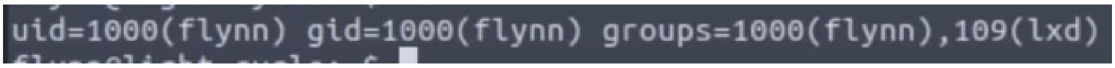
The value of the user.txt flag is **THM{IDENTITY_DISC_RECOGNISED}**



```
www-data@light-cycle:/home/flynn$ su flynn
Password:
flynn@light-cycle:~$ ls -l
total 4
-r-------- 1 flynn flynn 30 Dec 19 16:42 user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
```

Question 12

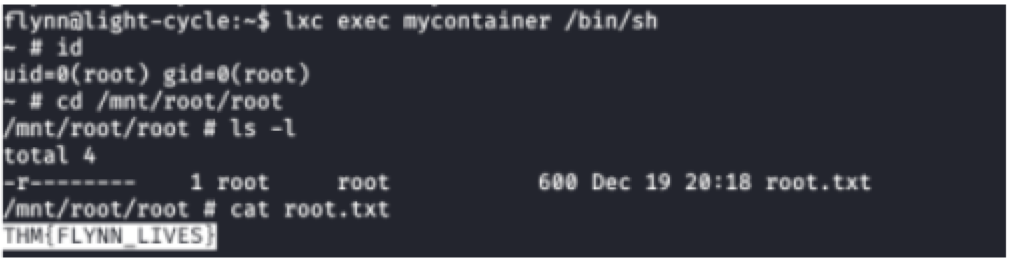
The group that can be leveraged to escalate privileges is **lxd**



```
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
```

Question 13

The value of root.txt flag is **THM{FLYNN_LIVES}**



```
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}
```

Methodology/Explanation:

Firstly I ran a scan using nmap to see what ports are open. From the scan i found that ports **80 and 65000** are open. I then opened the webserver on port 65000 to find the title of the hidden website, **Light Cycle.** By using the command " **gobuster dir -u http://<target_machine_ip>:65000 -x php -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40** " to find the hidden php page which is **/uploads.php.** From there we can also find the directory **/grid** which is where the files are stored. To get the web.txt flag which is found in **var/www/** the flag is **THM{ENTER_THE_GRID}.** There are three lines used to upgrade and stabilize the shell. **python3 -c 'import pty;pty.spawn("/bin/bash")' , export TERM=xterm and stty raw -echo; fg.** The username:password is found in **/var/www/TheGrid/includes/** and the username:password is **tron:IFightForTheUsers.** Next I entered the command mysql -utron -p and found the a database called **tron.** I then used Crack Station and entered the Hash and the result is **@computer@.** Now that the password is known I was able to locate the flag in the directory which is **THM{IDENTITY_DISC_RECOGNISED}.** I ran groups and found that Flynn is a part of a group called **lxd.** By following the steps in the Day 24 description i managed to find the root.txt file and from there i found the flag, **THM{FLYNN_LIVES}**