PSP0201

Week 6 Writeup

Group name: SOLO

ID	NAME	ROLE
1211100574	Ivan Liew Qi Hong	leader

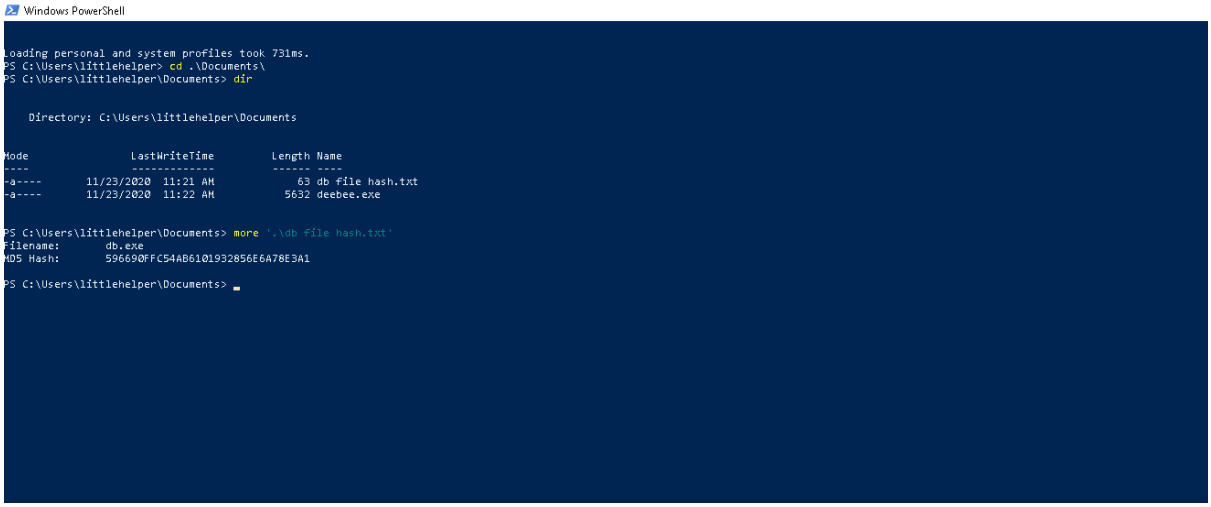
Day 21: [Blue Teaming] Time for some ELForensics

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

Login using rdp and open up powershell. Navigate to documents directory and read what's contained in text file



Question 2

Use get-FileHash to obtain md5 file hash

Question 3

Change the algorithm of the command from MD5 to SHA256

Question 4

Use string command to obtain the strings from the executable and look around for flag

```
PS C:\Users\littlehelper\Documents> c:\Tools\strings64.exe -accepteula .\deebee.exe

Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!This program cannot be run in DOS mode.
SLH
.text
`.rsrc
@.reloc
&*"
BSJB
```

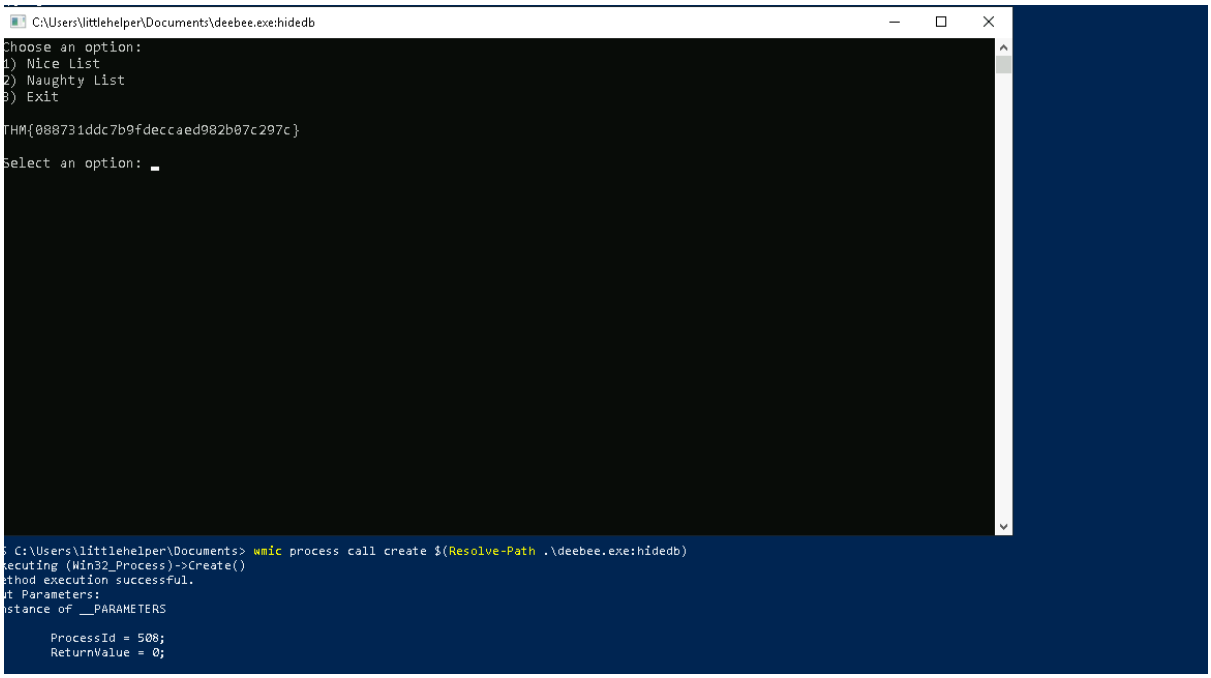
```
Accessing the Best Festival Company Databas
Done.
Using SSO to log in user...
Loading menu, standby...
THM{f6187e6cbeb1214139ef313e108cb6f9}
Set-Content -Path .\lists.exe -value $(Get-
Hahaha .. guess what?
Your database connector file has been moved
```

Question 5

The command to view ADS is Get-Item -Path file.exe -Stream *

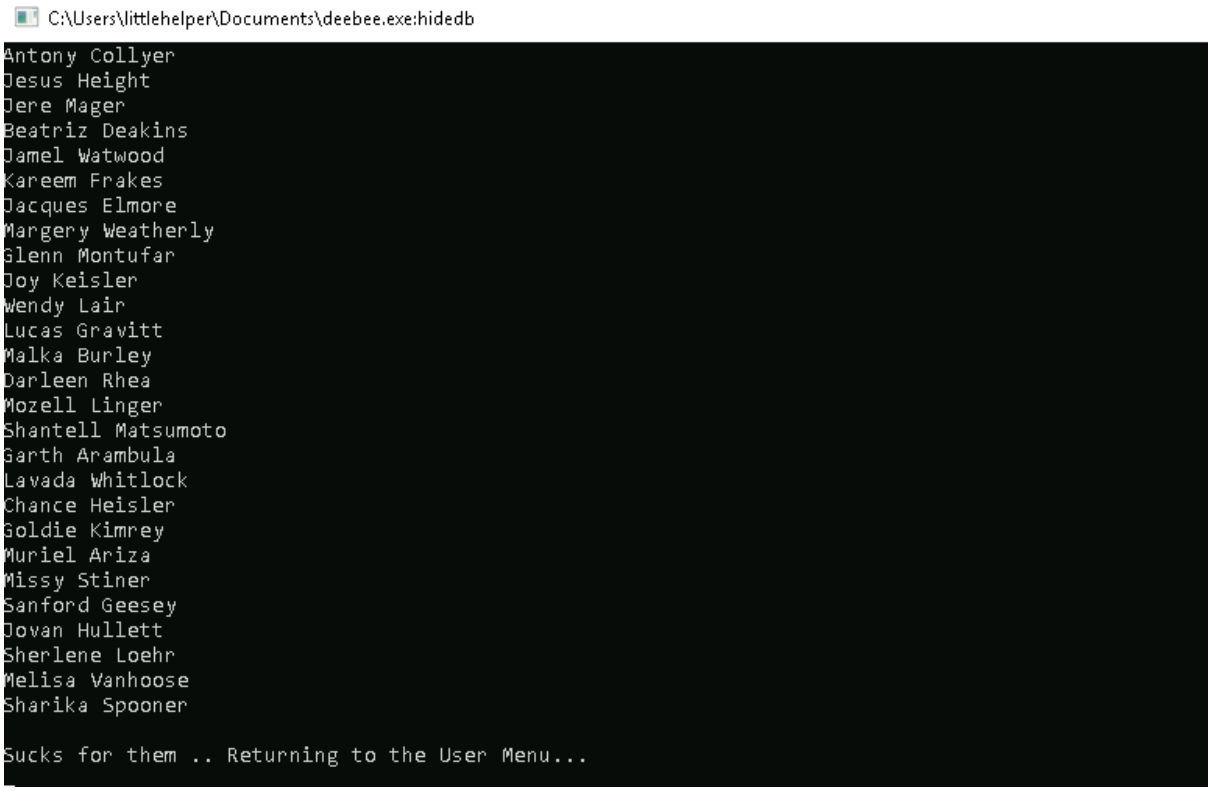
Question 6

Use command to run hidden executable and obtain flag



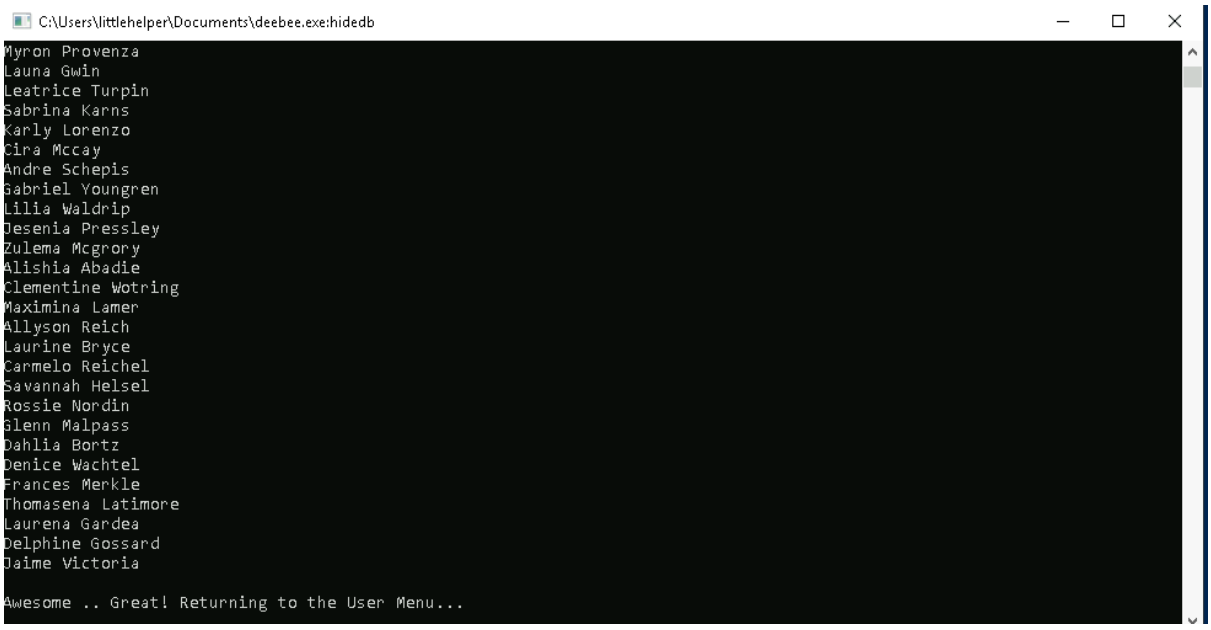
Question 7

Check naughty list for Shakira spooner



Question 8

Check nice list for Jaime Victoria



Thought Process/Methodology:

I logged in using rdp and the credentials given and then accessed powershell. I then navigated to the documents directory to read what was in the text file and then used the get-filehash command to get the MD5 hash as well as the SHA256 hash. I then used the string command to find the flag. I then used the command to launch the hidden executable within the ADS to find the final flag as well as the people on the naughty and nice list.

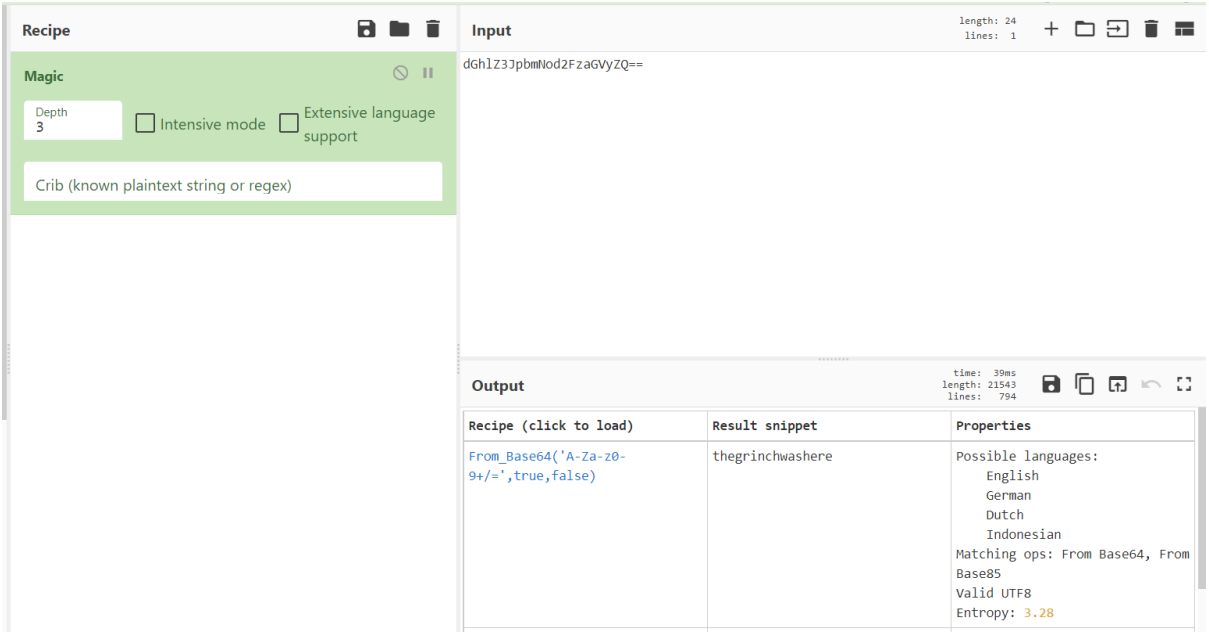
Day 22: [Blue Teaming] Elf McEager becomes CyberElf

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

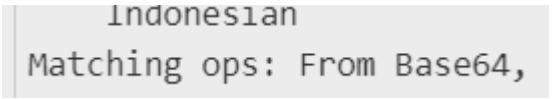
Question 1

Copy code string from folder name and decode it for password



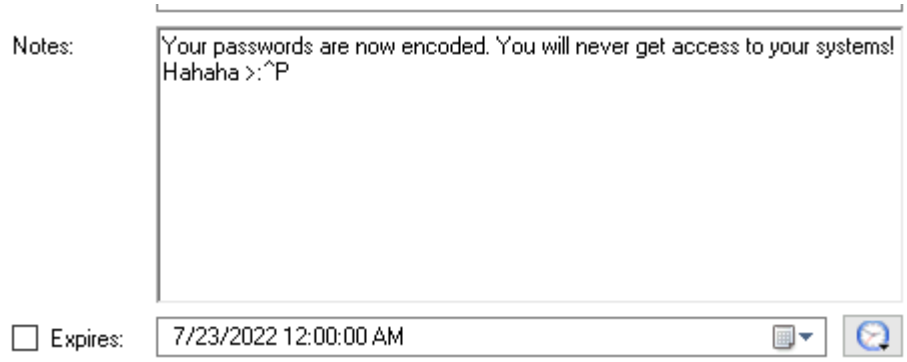
Question 2

Encoding method is base64



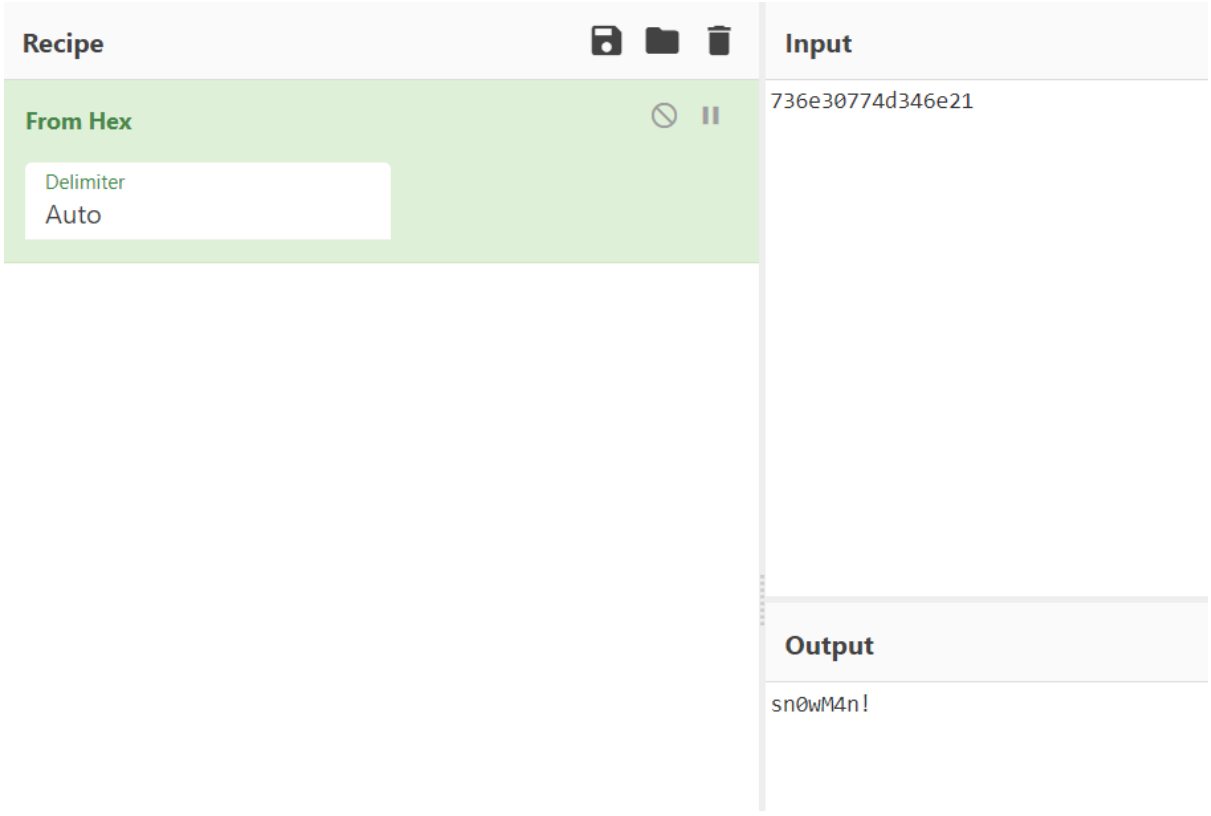
Question 3

Copy note from hiya key



Question 4

Decode code from hex for the password

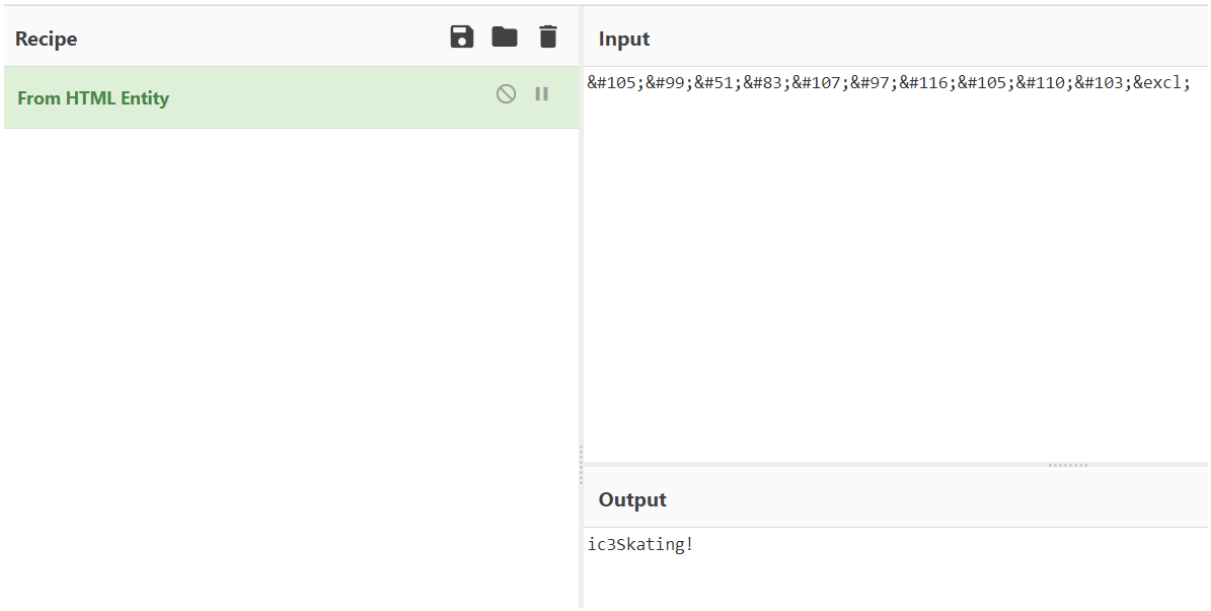


Question 5

Note has given that the encoding used was hex

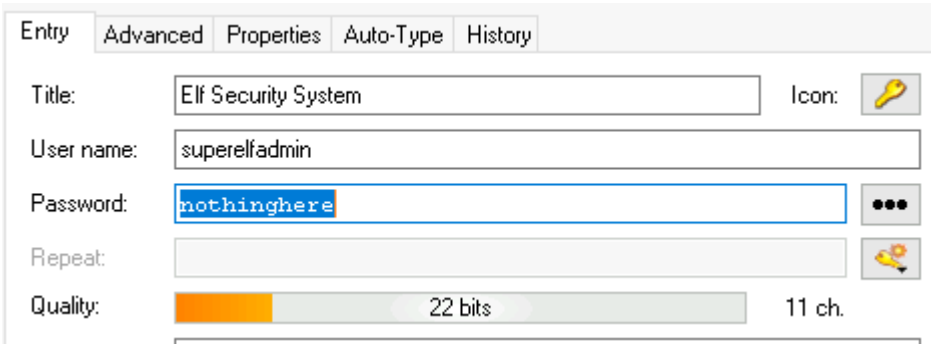
Question 6

Decode code from entity for the password



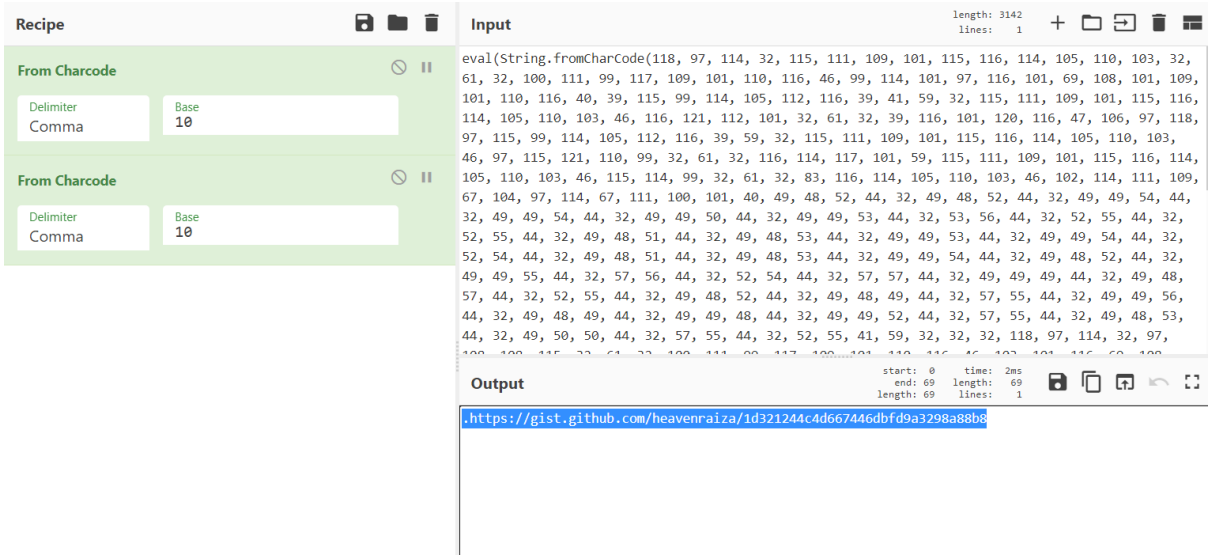
Question 7

Check properties of elf security system for username and password



Question 8

Obtain code from note in elf security system and decode it using charcode twice with the delimiter set to comma and the base of 10 to obtain the link with the flag



Thought Process/Methodology:

Fire up rdp and login, copy folder name and decode it with magic which determined it was from base64. Decode password from other keys by copying their password and decoding them with hex and entity. Decode character code from notes twice with comma delimiter and base 10 to obtain link which contain flag.

Day 23: [Blue Teaming] The Grinch Strikes again!

Tools used: Kali Linux, Firefox

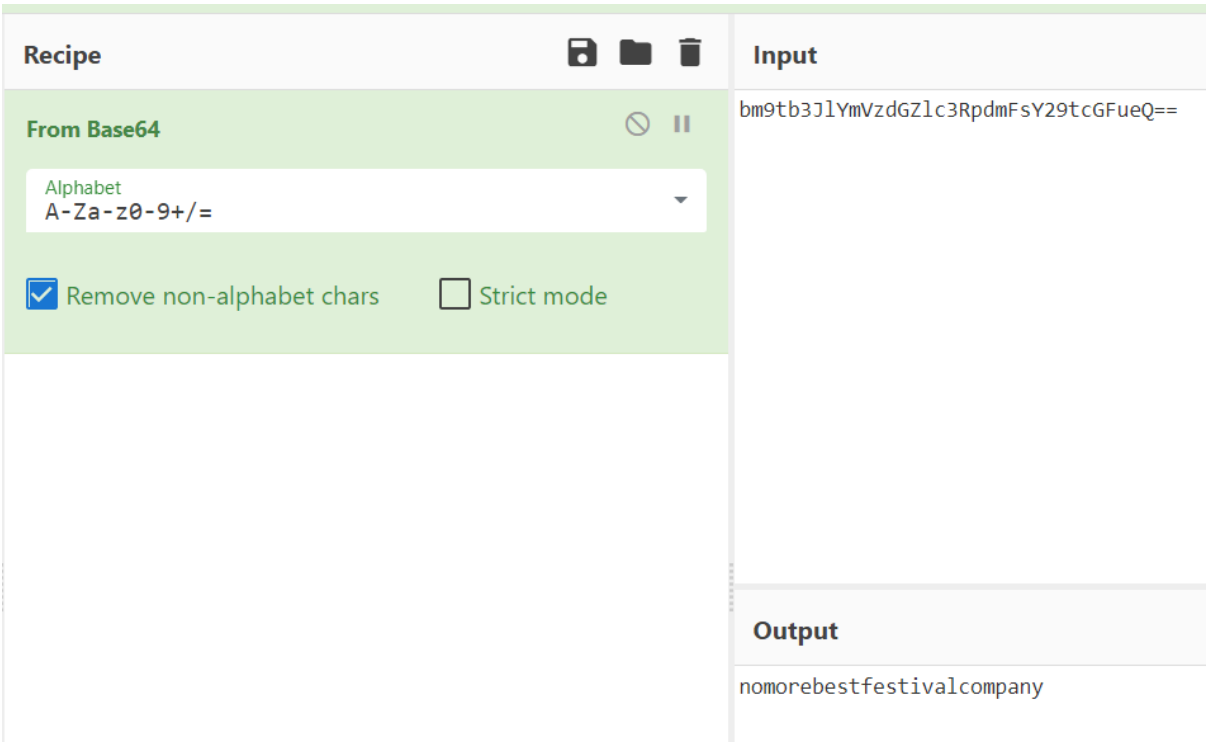
Solution/Walkthrough:

Question 1

Set quality in rdp preference to poor and turn on wallpapers and login to see text

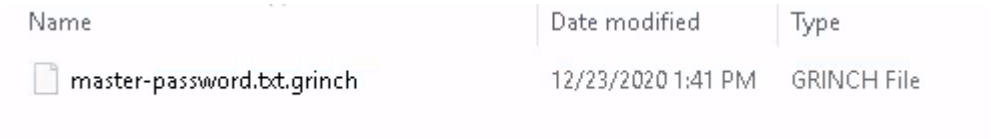
Question 2

Decrypt code from ransom text with base64



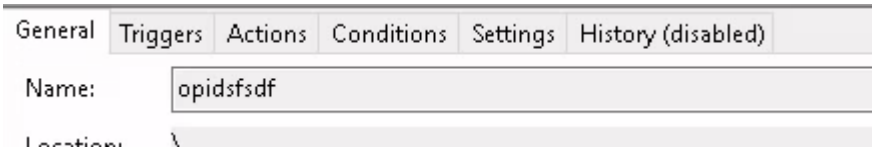
Question 3

File extension is .grinch



Question 4

Name can be found in task scheduler

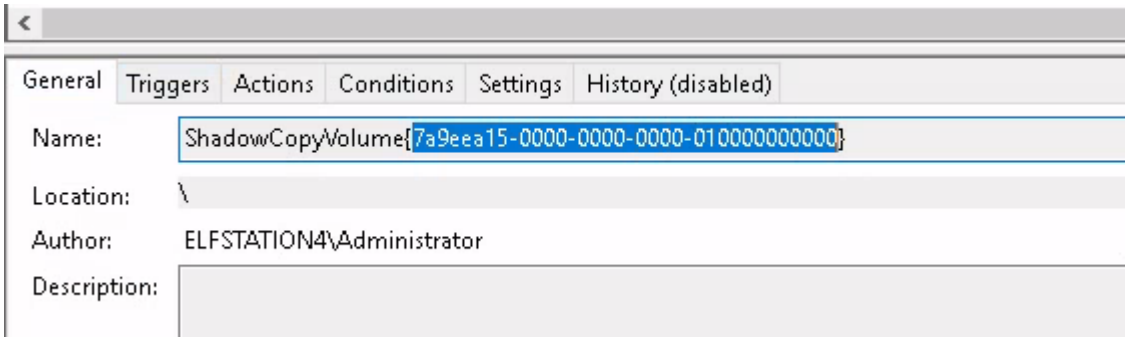


Question 5

Actions tab of the scheduled task

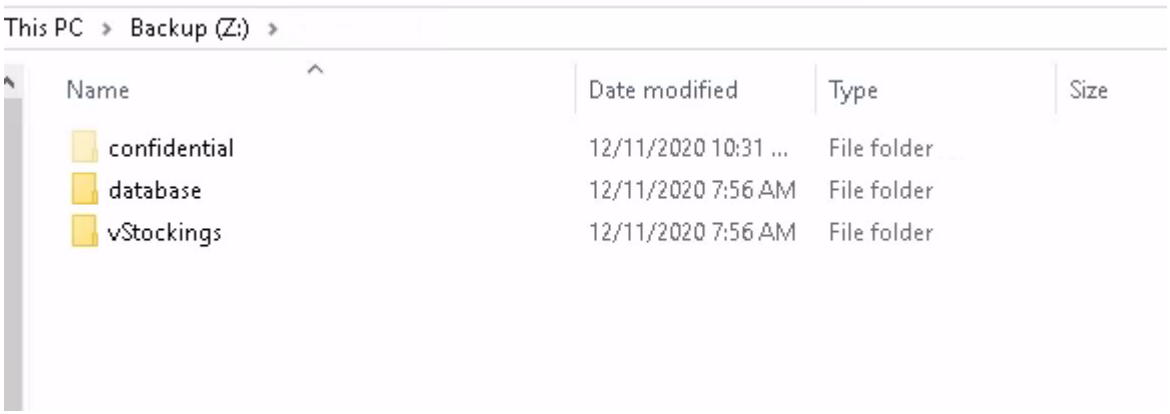
Question 6

Go to shadowcopy to get volume id



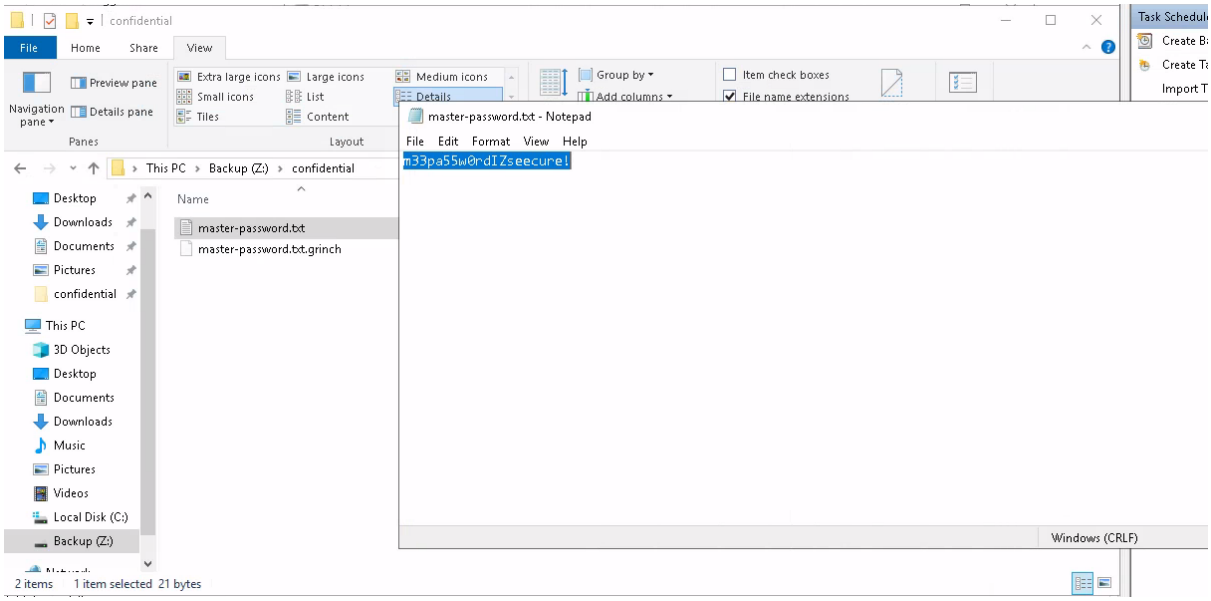
Question 7

Hidden folder name is confidential



Question 8

Restore confidential folder and obtain password



Thought Process/Methodology:

I changed the preferences on the rdp to allow the wallpaper to be seen. I then decoded the ransom text from base64. I then checked the file extension of the hidden folder. I then use the task scheduler to obtain the name of the scheduled task as well as finding out where it was going to execute itself. I also found the volume id of the shadowcopy in the task scheduler. I then restored the backup confidential folder to obtain the password.

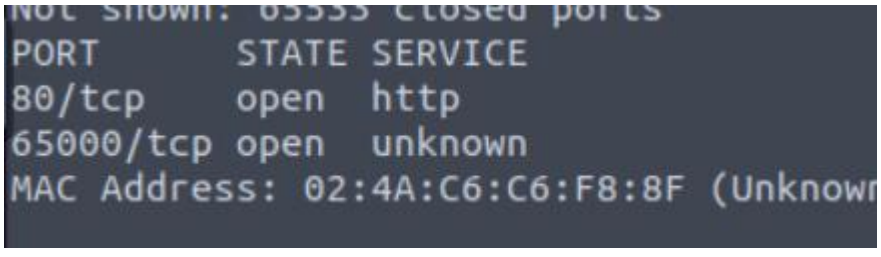
Day 24: [Final Challenge] The Trial Before Christmas

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

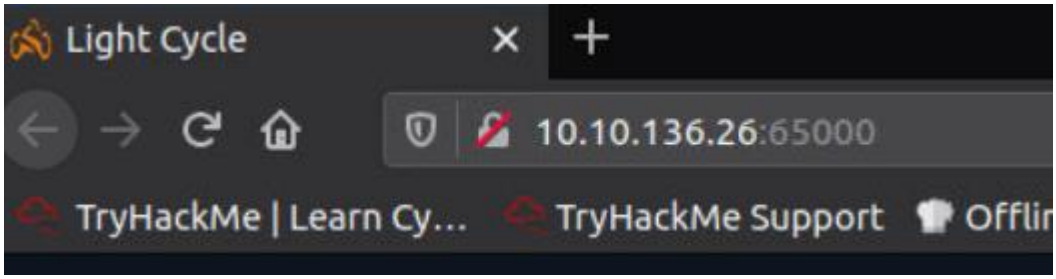
Question 1

Use nmap to see open ports



Question 2

Use port with ip address to locate website



Question 3 and 4

Use gobuster to determine name of hidden php page and hidden directory where files uploaded are saved

```
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: 28102 / 220561 (12.74%)
```

Question 5

Use burpsuite to intercept and enter /uploads.php. Create a reverse shell and upload it while also using netcat to listen to it. Navigate to var/www to obtain web.txt flag

Question 6

Lines used to stabilize shell are export TERM=xterm, stty raw -echo;fg and python3 -c 'import pty;pty.spawn("/bin/bash")'

Question 7

Navigate through the grid and find dbauth.php which contains the credentials

```
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";
```

Question 8

Use mysql to look at databases and find the encrypted credentials

```
mysql> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| tron               |
+--------------------+
2 rows in set (0.00 sec)
```

```
Database changed
mysql> show tables;
+----------------+
| Tables_in_tron |
+----------------+
| users          |
+----------------+
1 row in set (0.00 sec)

mysql> select * from users;
+----+----------+----------------------------------+
| id | username | password                         |
+----+----------+----------------------------------+
|  1 | flynn    | edc621628f6d19a13a00fd683f5e3ff7 |
+----+----------+----------------------------------+
1 row in set (0.00 sec)
```

Question 9

Use hash cracker to decode the password

Hash	Type	Result
edc621628f6d19a13a00fd683f5e3ff7	md5	@computer@

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found

Question 10

Login as Flynn with password

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

Question 11

Read user.txt to obtain flag

Question 12

The group is lxd

Question 13

Use commands to start container

Thought Process/Methodology:

I began by using nmap to determine to open ports of the address and then used the open ports to find the website. I then used gobuster to locate the hidden php page and file directory. Using burpsuite I intercepted the uploads page and bypassed it allowing me to upload a reverse shell created to listen to. This then allowed me to obtain the flag. I then found credentials in the grid directory. I followed that by using mysql to look at the databases in order to obtain the encrypted credentials which I took and decoded. I then logged using the decoded password and username given to obtain the user.txt flag. I tehn determined the group for elevating privileges was lxd and started a cointainer to obtain root.txt flag.