PSP0201 WEEK 5 WRITE UP

Groupname: **CyberRivets**

Student ID	Name	Role
1211103426	Aminul Aiman Bin Abdullah	Leader
1211100965	Muhammad Izz Hakim Bin Mohd Zaki	Member
1211103429	Haifa Najieha Binti Hashim	Member
1211102576	‘Uzair Akhyar Bin Norazmi	Member

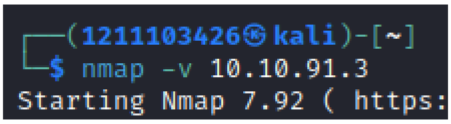
Day 16: Scripting - Help! Where is Santa?

Used Tools: Kali Linux, Firefox, Terminal, Python3

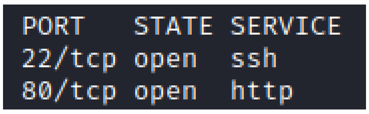
Solution:

Question 1

What is the port number for the web server?



```
┌──(1211103426㉿kali)-[~]
└─$ nmap -v 10.10.91.3
Starting Nmap 7.92 ( https:
```

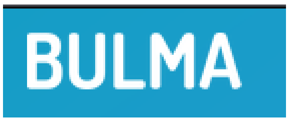


```
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
```

Use nmap to scan the IP address and find the open port. Our website will be using an HTTP service.

Question 2

What templates are being used?

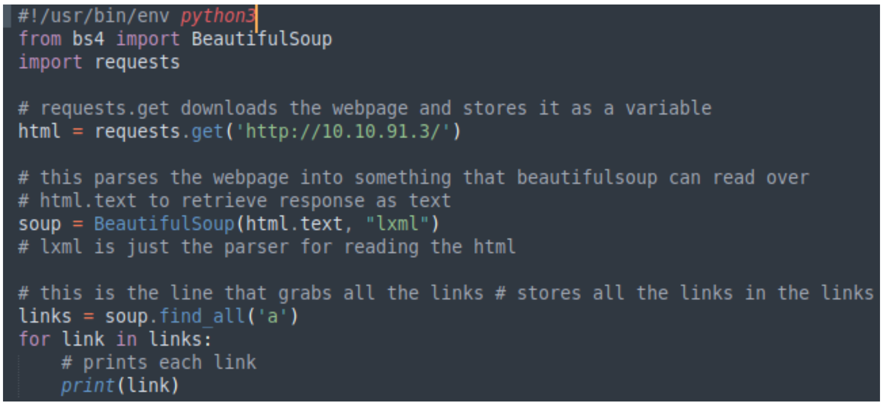


BULMA

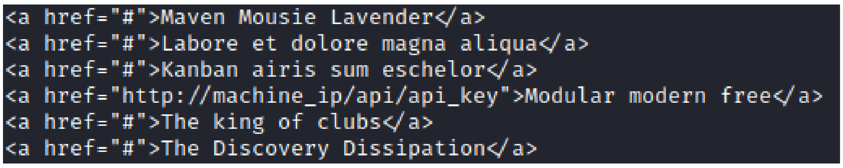
Look at the left upper corner to find the answer.

Question 3

Without using enumerations tools such as Dirbuster, what is the directory for the API? (without the API key)



```
#!/usr/bin/env python3
from bs4 import BeautifulSoup
import requests

# requests.get downloads the webpage and stores it as a variable
html = requests.get('http://10.10.91.3/')

# this parses the webpage into something that beautifulsoup can read over
# html.text to retrieve response as text
soup = BeautifulSoup(html.text, "lxml")
# lxml is just the parser for reading the html

# this is the line that grabs all the links # stores all the links in the links
links = soup.find_all('a')
for link in links:
    # prints each link
    print(link)
```

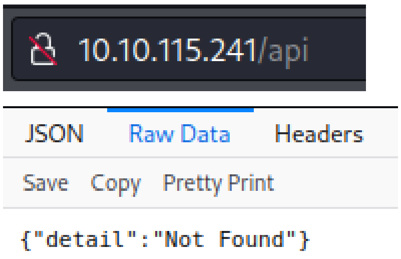


```
<a href="#">Maven Mousie Lavender</a>
<a href="#">Labore et dolore magna aliqua</a>
<a href="#">Kanban airis sum eschelor</a>
<a href="http://machine_ip/api/api_key">Modular modern free</a>
<a href="#">The king of clubs</a>
<a href="#">The Discovery Dissipation</a>
```

Use libraries like ‘BeautifulSoup’ to pull out data from the HTML and ‘requests’ to send HTTP requests. Make a useful tool out of them to filter out links/’a href’ tags from the website.

Question 4

Go the API endpoint. What is the Raw Data returned if no parameters are entered?



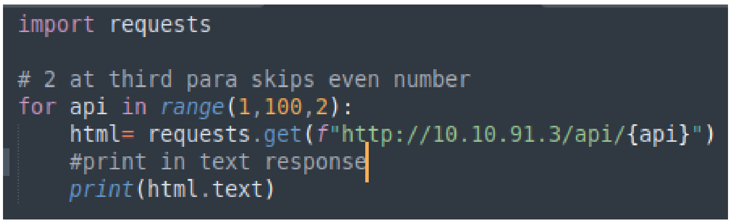
```
{"detail":"Not Found"}
```

Go into ‘API endpoint’ without any parameter. The answer can be found in the ‘Raw Data’ tab.

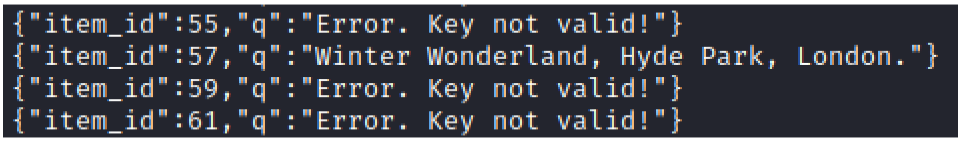
Questions 5 & 6

Where is Santa right now?

Find out the correct API key. Remember, this is an odd number between 0-100. After too many attempts, Santa's Sled will block you.



```
import requests

# 2 at third para skips even number
for api in range(1,100,2):
    html= requests.get(f"http://10.10.91.3/api/{api}")
    #print in text response
    print(html.text)
```



```
{"item_id":55,"q":"Error. Key not valid!"}
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
{"item_id":59,"q":"Error. Key not valid!"}
{"item_id":61,"q":"Error. Key not valid!"}
```

Make a looping tool from the ‘requests’ library to iterate every odd number finding the API key and Santa's location.

Methodology/Thought Process:

Scan the IP address that was given using NMAP to find the port used. We want to look for the HTTP service as the website is using HTTP. As there are many links on the website, we can either use look into it one by one, using tools like Dirbuster or create our own tool using Python3. By using two libraries: BeautifulSoup and requests, we can retrieve all data from the website and filter it out leaving out only link tags. Next, to find the correct API key, we can iterate through the odd number manually or automatically by sending tons of requests. Make a looping tool using the requests library to iterate through odd numbers. We will get both the API key and Santa’s location.

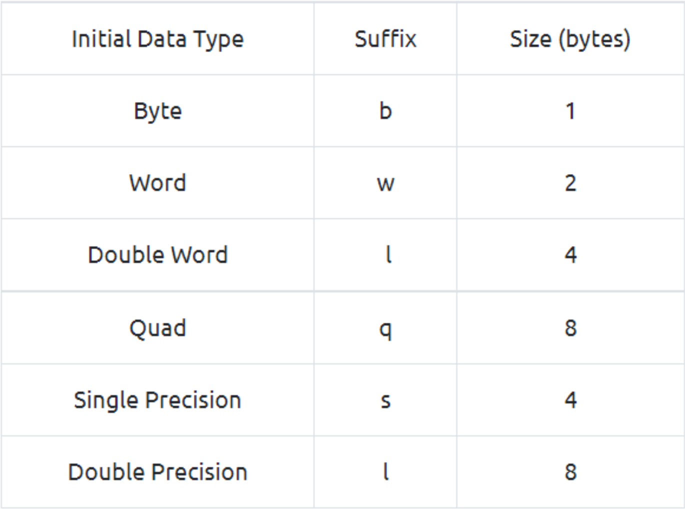
Day 17: Reverse Engineering - ReverseELFneering

Used Tools: Kali Linux, Terminal

Solution:

Question 1

Match the data type with the size in bytes:

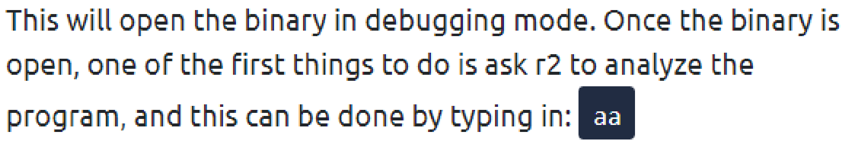


Initial Data Type	Suffix	Size (bytes)
Byte	b	1
Word	w	2
Double Word	l	4
Quad	q	8
Single Precision	s	4
Double Precision	l	8

Read through the notes in TryHackMe.

Question 2

What is the command to analyse the program in radare2?

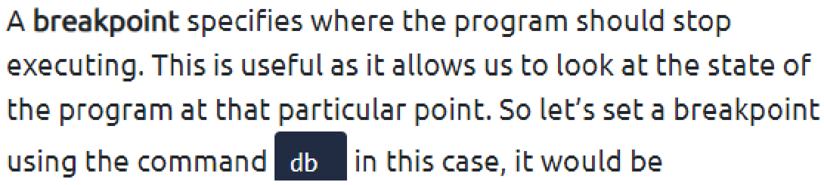


This will open the binary in debugging mode. Once the binary is open, one of the first things to do is ask r2 to analyze the program, and this can be done by typing in: `aa`

Read through the notes in TryHackMe. Command 'aa' used to analyse the program in radare2.

Question 3

What is the command to set a breakpoint in radare2?

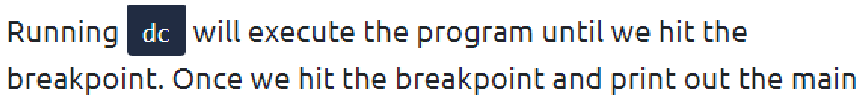


A **breakpoint** specifies where the program should stop executing. This is useful as it allows us to look at the state of the program at that particular point. So let's set a breakpoint using the command `db` in this case, it would be

Read through the notes in TryHackMe. Command 'db' used to set a breakpoint in radare2.

Question 4

What is the command to execute the program until we hit a breakpoint?

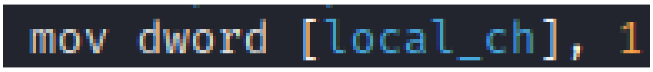


Running dc will execute the program until we hit the breakpoint. Once we hit the breakpoint and print out the main

Read through the notes in TryHackMe. Command 'dc' used to execute the program until it hit the breakpoint.

Question 5

What is the value of local_ch when its corresponding movl instruction is called (first if multiple)?

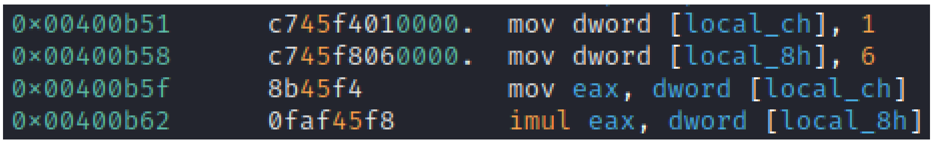


```
mov dword [local_ch], 1
```

Value 1 moved into [local_ch]. [local_ch] carries value 1.

Question 6

What is the value of eax when the imull instruction is called?

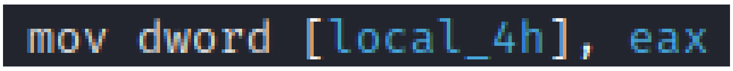


```
0x00400b51      c745f4010000.  mov dword [local_ch], 1
0x00400b58      c745f8060000.  mov dword [local_8h], 6
0x00400b5f      8b45f4         mov eax, dword [local_ch]
0x00400b62      0faf45f8       imul eax, dword [local_8h]
```

Value 6 moved into [local_8h]. [local_8h] carries value 6. Value 1 from [local_ch] moved into eax. ‘Imul’ functions multiply eax and [local_8h] values. 1 x 6 = 6.

Question 7

What is the value of local_4h before eax is set to 0?



```
mov dword [local_4h], eax
```

‘Eax’ value moved into [local_4h]. [local_4h] carries value 6.

Methodology/Thought Process:

Run ‘r2 -d ./challenge1’ to open the binary in debugging mode. Run ‘aa’ to analyze the file. After the process is complete, we want to check for the main functions. To call list of functions, we will use ‘afl’ command followed by ‘grep main’ to filter only main functions. Next, to look into the process in the main function, we need to observe and understand the assembly code. The code can be accessed by using ‘pdf @main’ command. We must understand the basics of assembly language. ‘Mov’ can be used to move the source into the destination. ‘Imul’ to multiply the source and the destination.

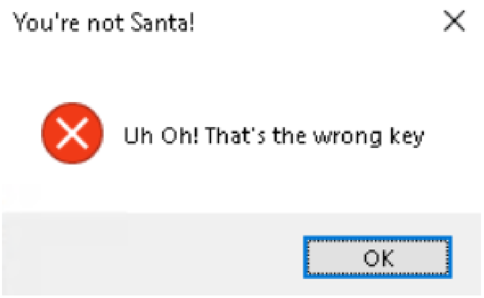
Day 18: Reverse Engineering - The Bits of Christmas

Used Tools: Kali Linux, Remmina, ILSpy

Solution:

Question 1

What is the message that shows up if you enter the wrong password for TBFC_APP?

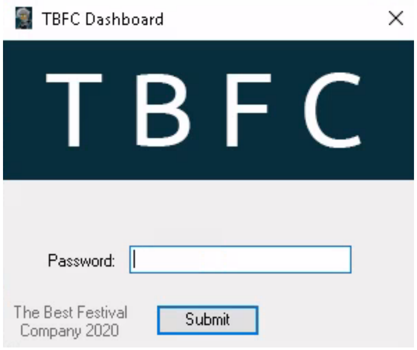


You're not Santa!

Uh Oh! That's the wrong key

Question 2

What does TBFC stand for?



TBFC Dashboard

TBFC

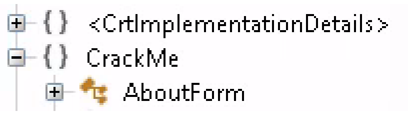
Password:

The Best Festival Company 2020

Look at the bottom left corner. ‘TBFC’ represents The Best Festival Company.

Question 3

Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?

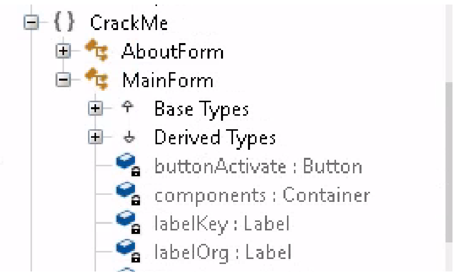


```
{ } <CrtImplementationDetails>
{ } CrackMe
    AboutForm
```

‘CrackMe’ module has an interesting name. We may want to see what contains inside it.

Question 4

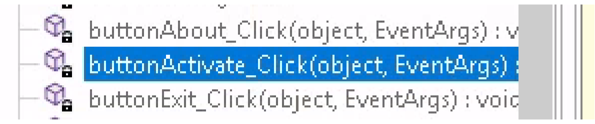
Within the module, there are two forms. Which contains the information we are looking for?



‘MainForm’ contains a lot of functions which possibly have the information we are looking for.

Question 5

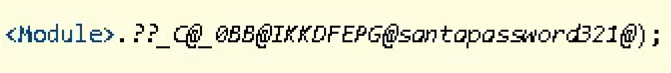
Which method within the form from Q4 will contain the information we are seeking?


buttonAbout_Click(object, EventArgs) : v
buttonActivate_Click(object, EventArgs) :
buttonExit_Click(object, EventArgs) : voic

‘buttonActivate_Click’ function is possibly related to the login authentication. Skim the code and find Santa’s password.

Question 6

What is Santa's password?

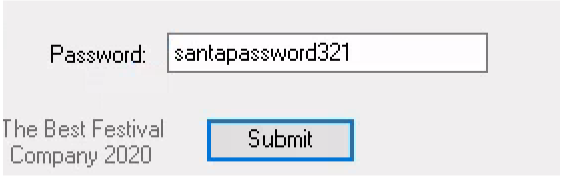


```
<Module>.??_C@_0BB@IKKDFEPG@santapassword321@);
```

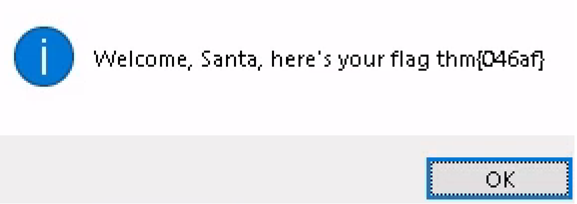
Find ‘buttonActivate_Click’ function, Santa’s password was left behind.

Question 7

Now that you've retrieved this password, try to login...What is the flag?



Password: santapassword321



Welcome, Santa, here's your flag thm{046af}

Login using Santa’s password to capture the flag.

Methodology/Thought Process:

Use Remmina to connect remotely to Windows using the IP address given. Login with the credentials given by TryHackMe. To find the Santa password, we might want to dissect what is inside the TBFC_APP. We can use ILSpy to look into the application source code. Open TBFC_APP in the ILSpy. Choose the '.NET assemblies' as the application is using '.NET Framework'. Now we want to look into anything that might be related to the password like 'login button'. There is also a hint like 'CrackMe'. Look into it and observe if there is anything useful. In the 'buttonActivate_Click' function, Santa's password was left behind. Open TBFC_APP and use the password we got earlier. After successful login, we captured the flag.

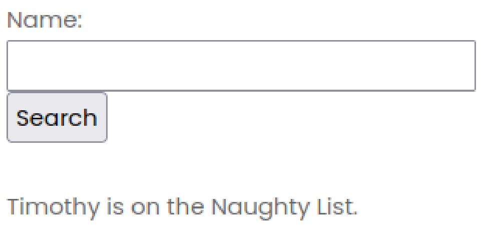
Day 19: Web Exploitation - The Naughty or Nice List

Used Tools: Kali Linux, Terminal, CyberChef, Firefox

Solution:

<u>Question 1</u>

Which list is this person on?

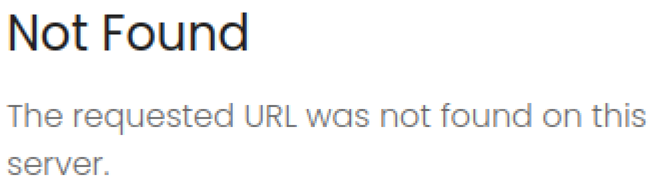


Timothy is on the Naughty List.

Type the name in the box and click on ‘Search’ to know whether it's on the nice or naughty list.

<u>Question 2</u>

What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"?



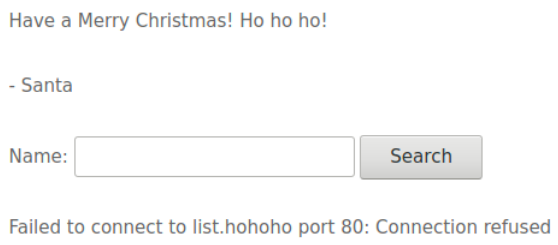
Not Found

The requested URL was not found on this server.

Replace the parameter in the link and observe the differences. Port 8080 does not return the output we looking for.

<u>Question 3</u>

What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A80"?



Have a Merry Christmas! Ho ho ho!

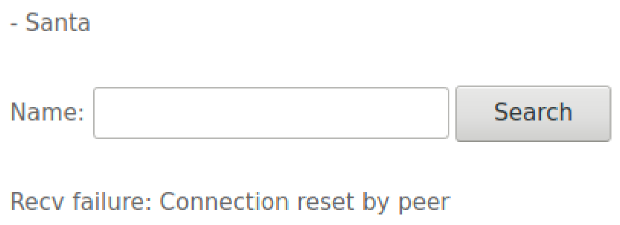
- Santa

Failed to connect to list.hohoho port 80: Connection refused

Replace the parameter in the link and observe the differences. Port 80 does not seem to be open on ‘list.hohoho’.

Question 4

What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A22"?



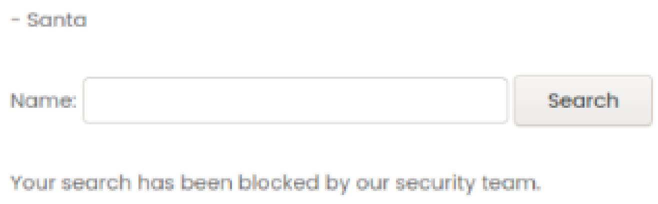
- Santa

Recv failure: Connection reset by peer

Changing to port 22 seems to have different output. Port 22 is open but it is for SSH. Thus, the HTML request is unreadable.

Question 5

What is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"?



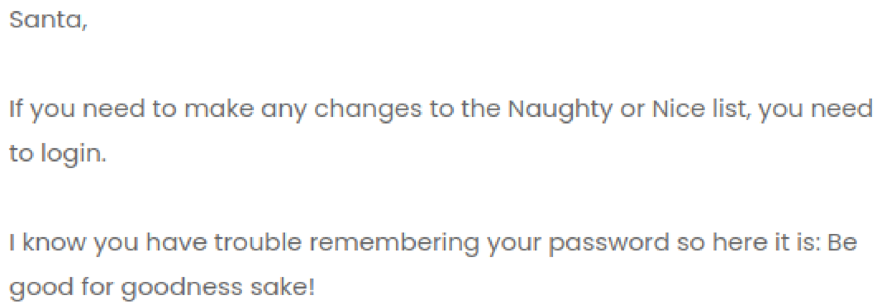
- Santa

Your search has been blocked by our security team.

Trying to access services locally using localhost is blocked by the security team.

Question 6

What is Santa's password?



Santa,

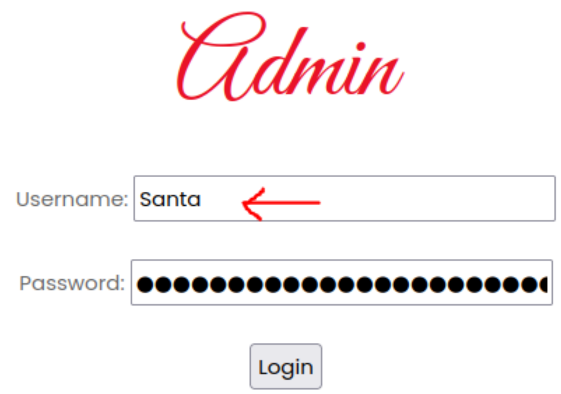
If you need to make any changes to the Naughty or Nice list, you need to login.

I know you have trouble remembering your password so here it is: Be good for goodness sake!

The password is ‘Be good for goodness sake!’

Question 7

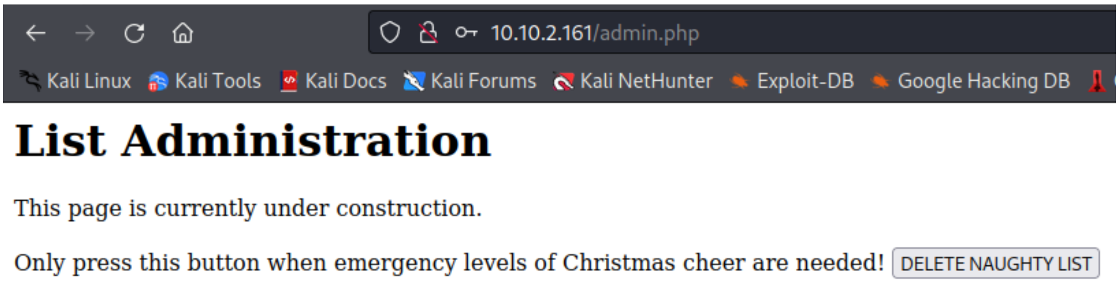
What is the challenge flag?



Admin

Username: Santa

Password: ●●●●●●●●●●●●●●●●●●●●●●●●

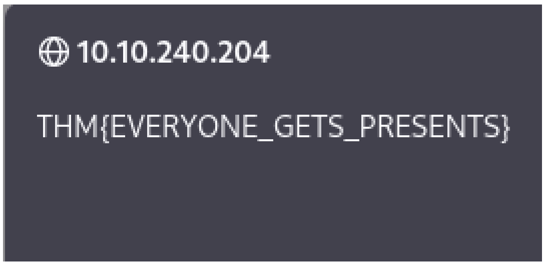


10.10.2.161/admin.php

List Administration

This page is currently under construction.

Only press this button when emergency levels of Christmas cheer are needed! DELETE NAUGHTY LIST



10.10.240.204

THM{EVERYONE_GETS_PRESENTS}

Put the username and password in the Admin login, then it will go to another page automatically and show ‘List Administration’ In that page have a button with the word ‘DELETE NAUGHTY LIST’. After clicking that button the flag will appear.

Methodology/Thought Process:

On Day 19, we want to try to find any useful information by using ‘server-side request forgery’. This can be done with some modifications to the URL. First, search any name in the search box to find any differences to the link. We see that the website use ‘list.hohoho’ as the hostname. Changing the port to 8080 and 22 (usually used by SSH server) is giving error messages. Changing the hostname to localhost also was blocked. At least, we know that ‘list.hohoho’ must be used. By converting the hostname into subdomain, we may get the output we want. This can be done by using ‘localtest.me’ as the domain which resolves every subdomain to localhost. Use the ‘/?proxy=http%3A%2F%%Flist.hohoho.localtest.me’ in the search bar, we will receive a short message with Santa’s password. Go to Admin and log in with Santa's credentials to enter the admin page. Once you entered, the page shows List Administrator with the button ‘DELETE NAUGHTY LIST’ below. Click it and the flag will be shown.

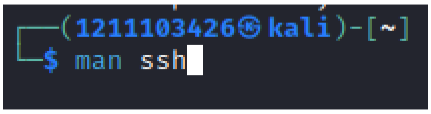
Day 20: Blue Teaming - PowershELIF to the rescue

Used Tools: Terminal, Kali Linux, PowerShell

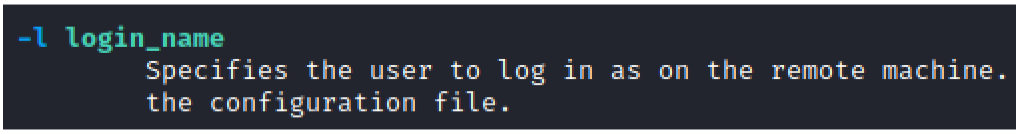
Solution:

Question 1

Check the ssh manual. What does the parameter -l do?



```
┌──(1211103426㉿kali)-[~]
└─$ man ssh
```

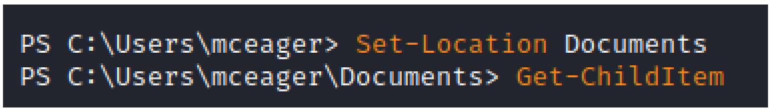


```
-l login_name
        Specifies the user to log in as on the remote machine.
        the configuration file.
```

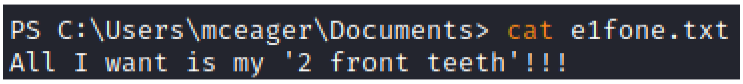
Go into SSH manual by using ‘man ssh’ command. Lookup for ‘-l’ tag and read the descriptions.

Question 2

Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?



```
PS C:\Users\mceager> Set-Location Documents
PS C:\Users\mceager\Documents> Get-ChildItem
```

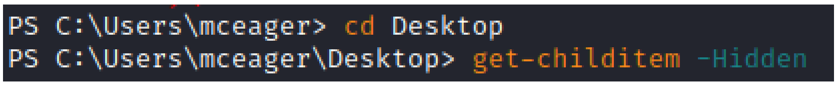


```
PS C:\Users\mceager\Documents> cat e1fone.txt
All I want is my '2 front teeth'!!!
```

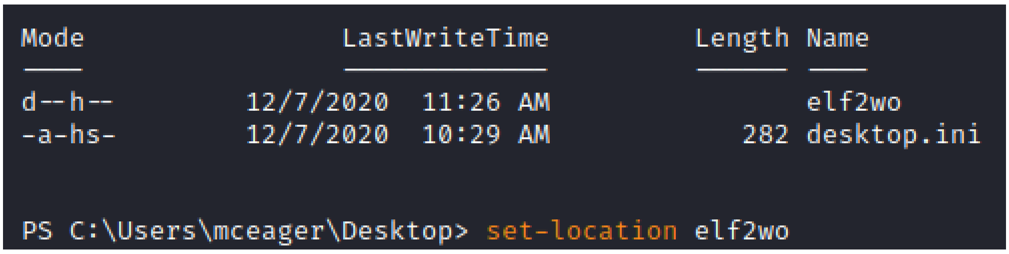
Using PowerShell to run the code. Type ‘Set Location Documents’ and after that use ‘Get-ChildItem’ code. Lastly, use ‘cat e1fone.txt’ to get the result.

Question 3

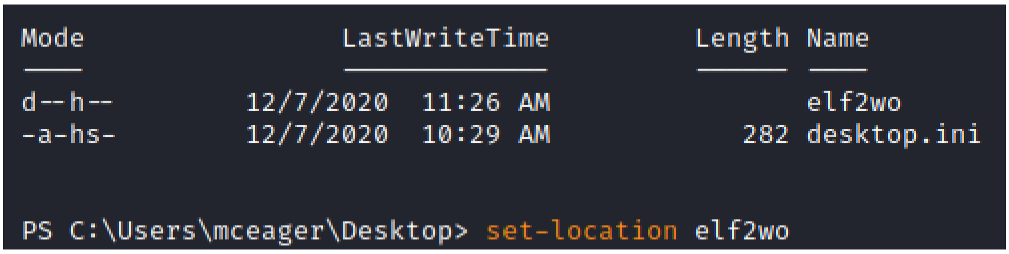
Search on the desktop for a hidden folder that contains the file for Elf 2. Read the contents of this file. What is the name of that movie that Elf 2 wants?



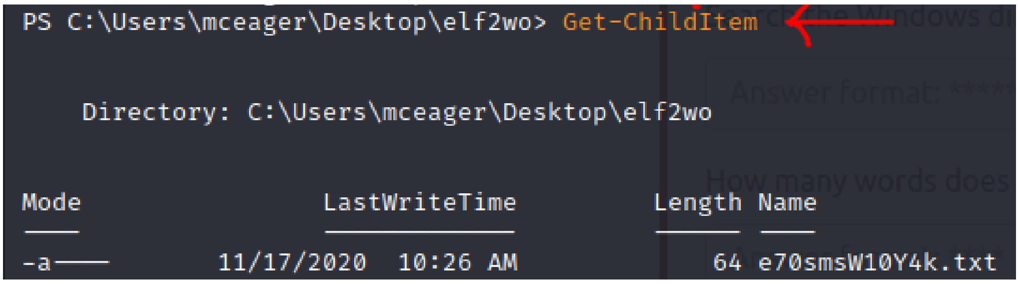
```
PS C:\Users\mceager> cd Desktop
PS C:\Users\mceager\Desktop> get-childitem -Hidden
```



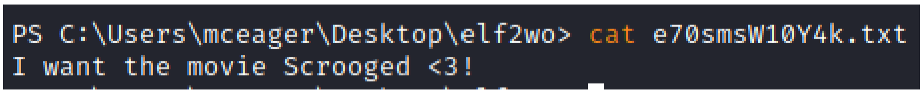
```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--         12/7/2020  11:26 AM                elf2wo
-a-hs-         12/7/2020  10:29 AM            282 desktop.ini


PS C:\Users\mceager\Desktop> set-location elf2wo
```



```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--         12/7/2020  11:26 AM                elf2wo
-a-hs-         12/7/2020  10:29 AM            282 desktop.ini


PS C:\Users\mceager\Desktop> set-location elf2wo
```



```
PS C:\Users\mceager\Desktop\elf2wo> Get-ChildItem


    Directory: C:\Users\mceager\Desktop\elf2wo


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/17/2020  10:26 AM             64 e70smsW10Y4k.txt
```

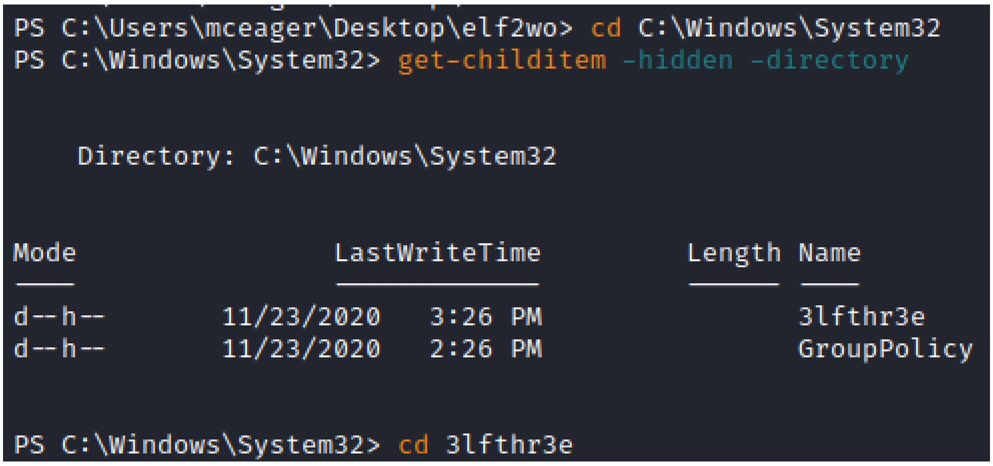


```
PS C:\Users\mceager\Desktop\elf2wo> cat e70smsW10Y4k.txt
I want the movie Scrooged <3!
```

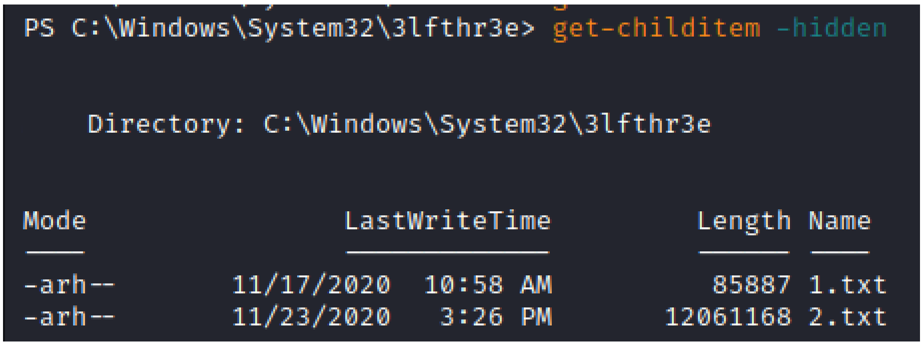
By using 'cd Desktop' and 'get-ChildItem' -Hidden in PowerShell, it will give 2 different files. Then use the first file with this command 'set-location elf2wo'. By command 'Get-ChildItem' to list the file back and it will show a different file. After that use 'cat e70smsW10Y4k.txt' to have the final result.

Question 4

Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder? (This command will take a while)



```
PS C:\Users\mceager\Desktop\elf2wo> cd C:\Windows\System32
PS C:\Windows\System32> get-childitem -hidden -directory


    Directory: C:\Windows\System32


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d--h--        11/23/2020   3:26 PM                3lfthr3e
d--h--        11/23/2020   2:26 PM                GroupPolicy


PS C:\Windows\System32> cd 3lfthr3e
```

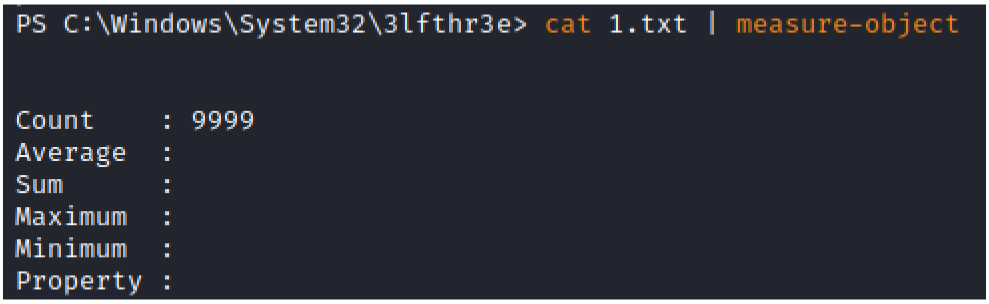


```
PS C:\Windows\System32\3lfthr3e> get-childitem -hidden


    Directory: C:\Windows\System32\3lfthr3e


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-arh--        11/17/2020  10:58 AM          85887 1.txt
-arh--        11/23/2020   3:26 PM       12061168 2.txt
```

‘cd C:\Windows\System32’ and then ‘get-childitem -hidden -directory’. Then, use ‘cd 3lfthr3e’ and ‘get-childitem -hidden’.

Question 5

How many words does the first file contain?

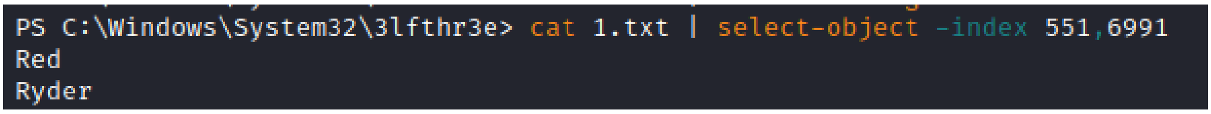


```
PS C:\Windows\System32\3lfthr3e> cat 1.txt | measure-object


Count    : 9999
Average  :
Sum      :
Maximum  :
Minimum  :
Property :
```

By using ‘cat 1.txt | measure-object’ will get how many counts.

Question 6

What 2 words are at index 551 and 6991 in the first file?

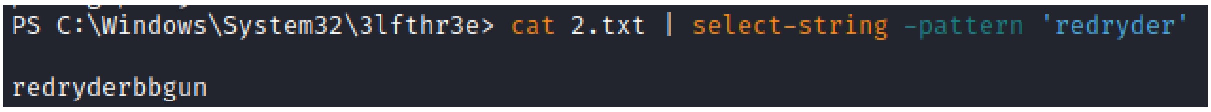


```
PS C:\Windows\System32\3lfthr3e> cat 1.txt | select-object -index 551,6991
Red
Ryder
```

Command ‘cat 1.txt | select-object -index 551, 6991’ will show the answer.

Question 7

This is only half the answer. Search in the 2nd file for the phrase from the previous question to get the full answer. What does Elf 3 want? (use spaces when submitting the answer)



```
PS C:\Windows\System32\3lfthr3e> cat 2.txt | select-string -pattern 'redryder'

redryderbbgun
```

‘ cat 2.txt | select-string -pattern ‘reyryder’ ‘ in the PowerShell.

Methodology/Thought Process:

After opening the terminal, put this ‘ssh -l mceager IP Address’ and the password just copy in the website. The terminal will change to PowerShell. By using ‘Set-Location Documents’ and press enter on your keyboard, and then command the ‘Get-ChildItem’ to see the list of files. ‘cat e1fone.txt’ will give the answer in the first file. Second, try using ‘cd Desktop’ and ‘get-childitem -Hidden’ so that the user can see what is hidden in the desktop. Using ‘set-location elf2wo’ and try to put this command ‘Get-ChildItem’ and the name of the file would show the alphabets and the number combined like ‘e70smsW10Y4k.txt’. Use this ‘cat e70smsW10Y4k.txt’ to get the result in that file. With ‘cd C:\Windows\System32’ and ‘get-childitem -hidden -directory’ can show two files with different names, ‘ 3lfthr3e’ and ‘GroupPolicy’ and then command ‘cd 3lfthr3e’. Use this code ‘get-childitem -hidden’ after using this code ‘cd 3lfthr3e’ to see the hidden file. Use first file ‘1.txt’ with this command ‘cat file_name | measure-object’ like this ‘cat 1.txt | measure-object’ and it will show how many counts the number. To find the name use ‘cat 1.txt | select-object -index 551,6991’ to see the name by the number given. Lastly, ‘cat 2.txt | select-string -pattern ‘redryder’’ to have the answer in the second file ‘2.txt’.