PSP0201

Week 5

Writeup

Group Name: **Cyberteam**

Members

ID	Name	Role
1211101864	Julian Koh Chee Yong	Leader
1211103605	Danial Ierfan Bin Hazmi	Member
1211103281	Jievenesh Arvind Naidu A/L Uma Selvam	Member
1211103785	Brijhendhra A/L Saravanaraj	Member

Day 16 - Help! Where is Santa?

Tools used: Kali Linux, Firefox, Visual Studio Code

Solution/walkthrough:

Question 1: What is the port number for the web server?

Use Nmap to scan the IP addresses and ports in the network.

```
┌──(kali㉿kali)-[~]
└─$ nmap -v 10.10.174.122
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-16 04:03 EDT
Initiating Ping Scan at 04:03
Scanning 10.10.174.122 [2 ports]
Completed Ping Scan at 04:03, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:03
Completed Parallel DNS resolution of 1 host. at 04:03, 0.01s elapsed
Initiating Connect Scan at 04:03
Scanning 10.10.174.122 [1000 ports]
Discovered open port 22/tcp on 10.10.174.122
Discovered open port 80/tcp on 10.10.174.122
Increasing send delay for 10.10.174.122 from 0 to 5 due to max_successful_tryno increase to 4
Increasing send delay for 10.10.174.122 from 5 to 10 due to max_successful_tryno increase to 5
Completed Connect Scan at 04:03, 21.21s elapsed (1000 total ports)
Nmap scan report for 10.10.174.122
Host is up (0.20s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.47 seconds
```

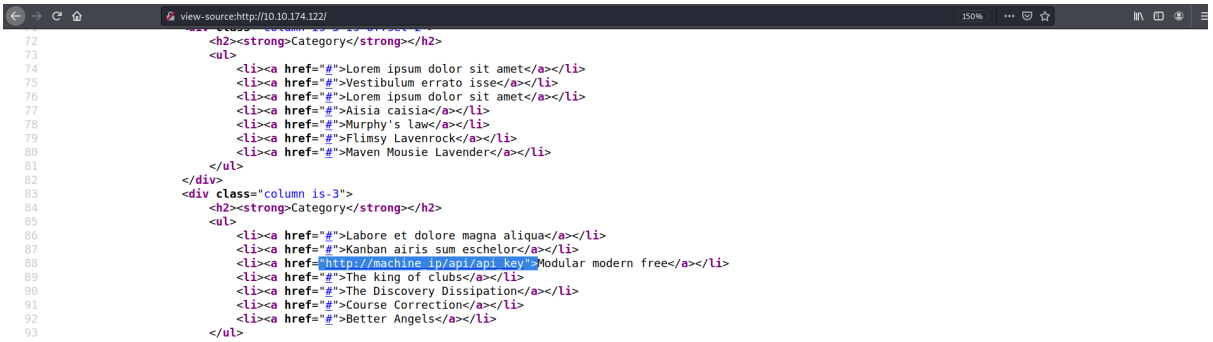
Answer: 80

Question 2: What templates are being used?

Answer: BULMA

Question 3: Without using enumerations tools such as Dirbuster, what is the directory for the API?

View the page source and find the odd link which includes the directory for the API.



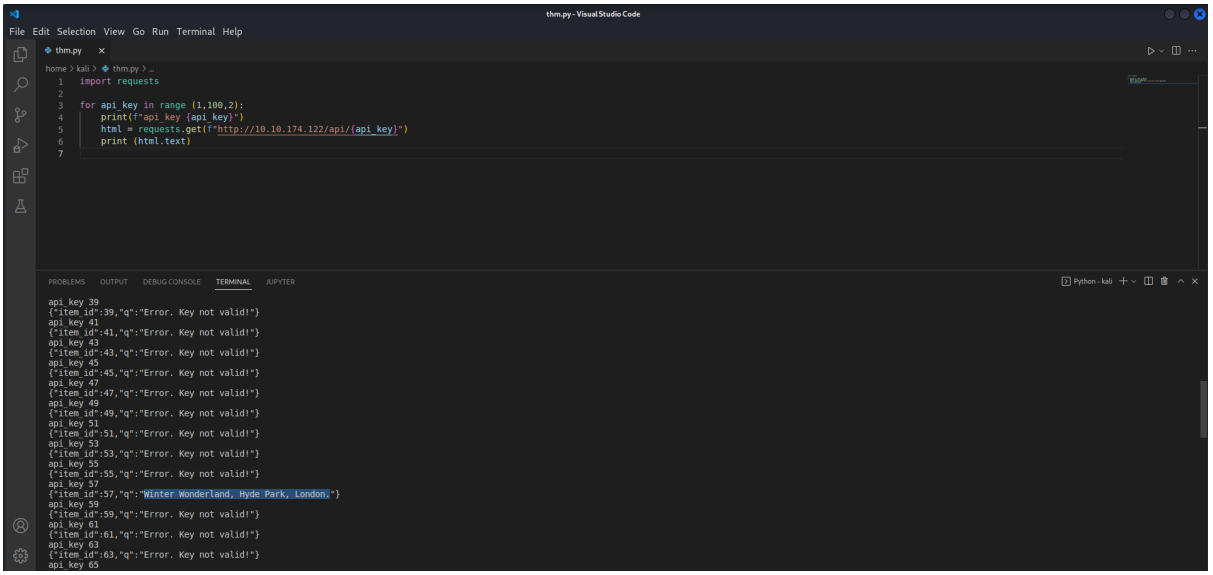
Answer: /api/

Question 4: Go the API endpoint. What is the Raw Data returned if no parameters are entered?

Answer: {"detail":[{"loc":["path","item_id"],"msg":"value is not a valid integer","type":"type_error.integer"}]}

Question 5: Where is Santa right now?

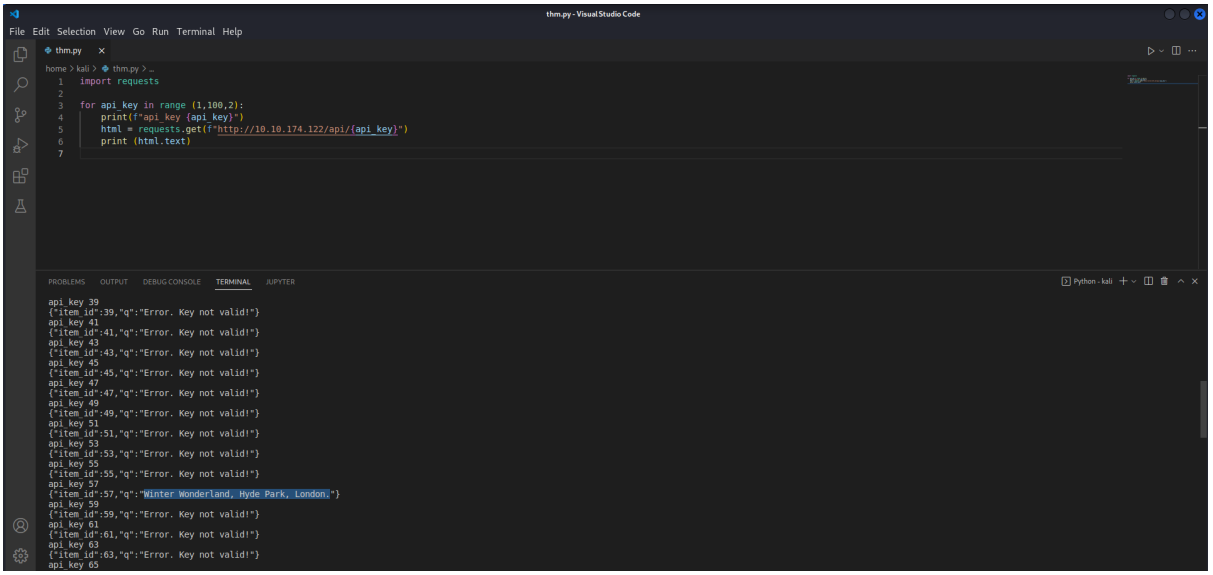
I used Visual Studio Code to program a loop.



Answer: Winter Wonderland, Hyde Park, London

Question 6: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. To unblock yourself, simply terminate and re-deploy the target instance (10.10.94.92)

I used Visual Studio Code to program a loop.



Answer: 57

Thought/processes:

Firstly, we scan the URL's port using Nmap. Then, view the page source and find the link to gain the access to the system to track Santa. As we need to find the correct API key, we have programmed a loop to find it. Once we have found the correct API key, the location of Santa is shown.

Day 17 - ReverseELFneering

Tools used - Kali Linux, Firefox

Solution/Walkthrough:

Question 1 : Match the data type with the size in bytes.

The answer is available in THM script.

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

Answer :

	1	2	4	8
Byte	◉	○	○	○
Word	○	◉	○	○
Double Word	○	○	◉	○
Quad	○	○	○	◉
Single Precision	○	○	◉	○
Double Precision	○	○	○	◉

Question 2 : What is the command to analyse the program in radare2?

Answer is searched from the link given in THM.

Analysis [a]

Analyse all	aa[a[a]]
Analyse function calls	aac
Analyse consecutive function	aat
Graphviz output	ag <addr>
ASCII Graph	agf
Xrefs from	axf
Xrefs to	axt
Rename function	afn
Rename locals/args	afvn
List functions	afl

Answer :

aa

Question 3 : What is the command to set a breakpoint in radare2?

Answer is searched from the link given in THM.

Debugger [d]

Set breakpoint	`db [addr]`
Remove breakpoint	`db -[addr]`
Continue execution	`dc`
Show memory maps	`dm`
Show memory maps with bars	`dm=`
Start process	`do`
Attach to process	`dp`
Show register	`dr`
Step	`ds [num]`
Step over	`dso [num]`
Show heap graph	`dmhg`
List heap chunks	`dmh`
List heap chunks of arena	`dmh <arena`
List bins	`dmhb`
List fastbins	`dmhf`

Answer :

db

Question 4 : What is the command to execute the program until we hit a breakpoint?

Answer is searched from the link given in THM.

Debugger [d]

Set breakpoint	`db [addr]`
Remove breakpoint	`db -[addr]`
Continue execution	`dc`
Show memory maps	`dm`
Show memory maps with bars	`dm=`
Start process	`do`
Attach to process	`dp`
Show register	`dr`
Step	`ds [num]`
Step over	`dso [num]`
Show heap graph	`dmhg`
List heap chunks	`dmh`
List heap chunks of arena	`dmh <arena`
List bins	`dmhb`
List fastbins	`dmhf`

Answer :

dc

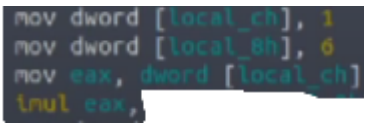
Question 5 : What is the value of local_ch when its corresponding movl instruction is called (first if multiple)?

Use pdf @main for a simpler program to read.

Answer :

1

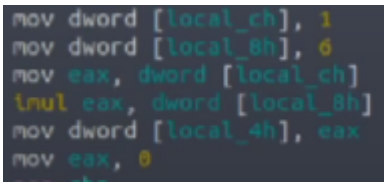
Question 6 : What is the value of eax when the imull instruction is called?



Answer :

6

Question 7 : What is the value of local_4h before eax is set to 0?



Answer :

6

Thought/Processes :

Firstly, look through the script in THM to match the Initial Type Data with the Size of Bit. Then, with the link given, search through the radare2 cheatsheet. After setting in all the commands, use pdf @main to get a simpler view of the data.

Day 18 - The Bits of Christmas

Tools used - Kali Linux, Firefox, Remmina

Solution/Walkthrough :

Question 1 : What is the message that shows up if you enter the wrong password for TBFC_APP?

Enter any random password in the box given.

Answer :

Uh Oh! That's the wrong key

Question 2 : What does TBFC stand for?

Answer :

The Best Festival Company

Question 3 : Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?

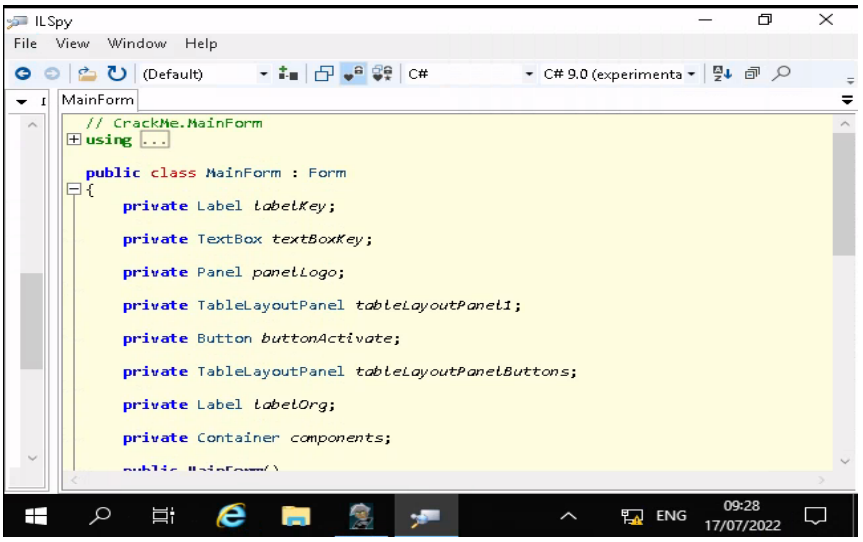
Go to File and click on Desktop. When you see TBFC App, click on it once and click on Open.

```
// C:\Users\cmnatic\Desktop\TBFC_APP.exe
// CrackMe, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null
// Global type: <Module>
// Entry point: <Module>.main
// Architecture: x86
// This assembly contains unmanaged code.
// Runtime: v4.0.30319
// Hash algorithm: SHA1
```

Answer :

CrackMe

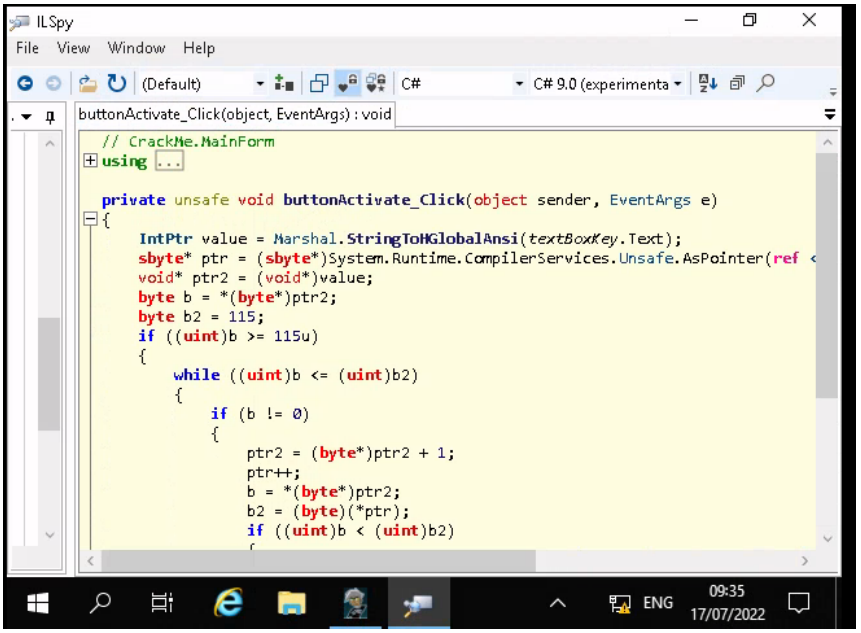
Question 4 : Within the module, there are two forms. Which contains the information we are looking for?

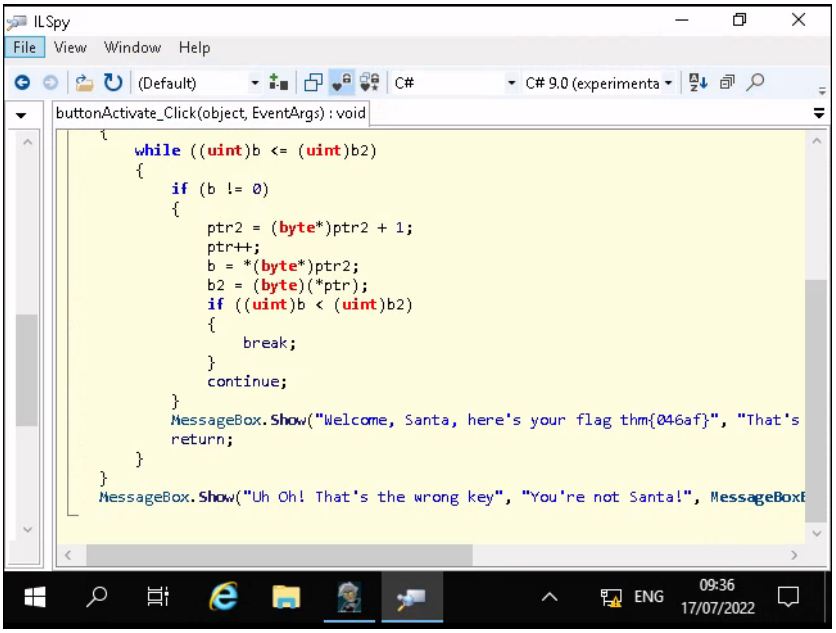


Answer :

MainForm

Question 5 : Which method within the form from Q4 will contain the information we are seeking?



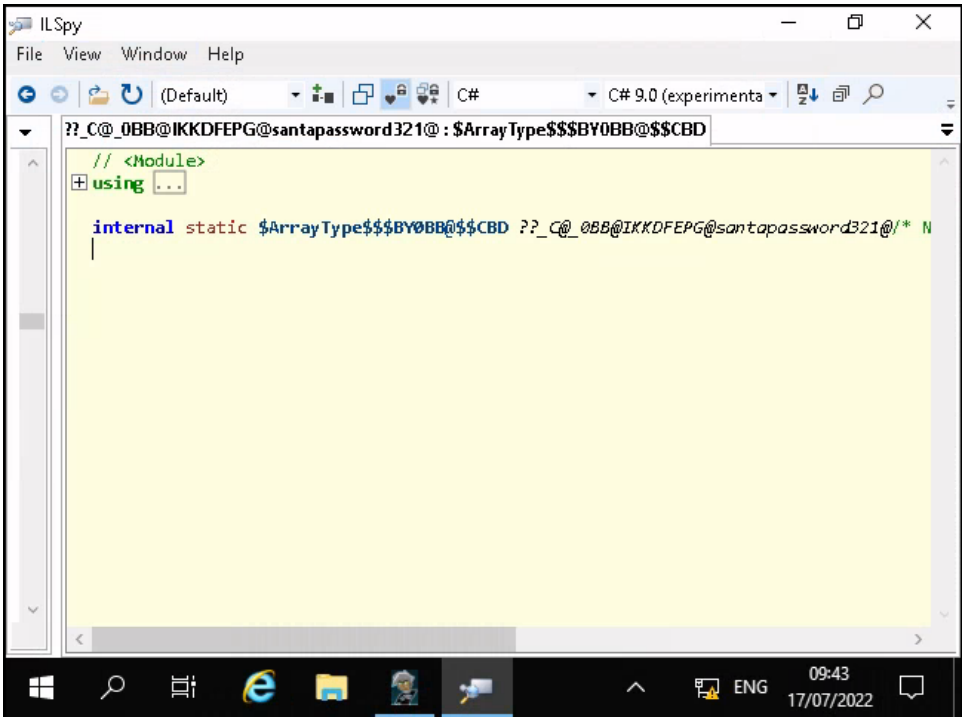


Answer :

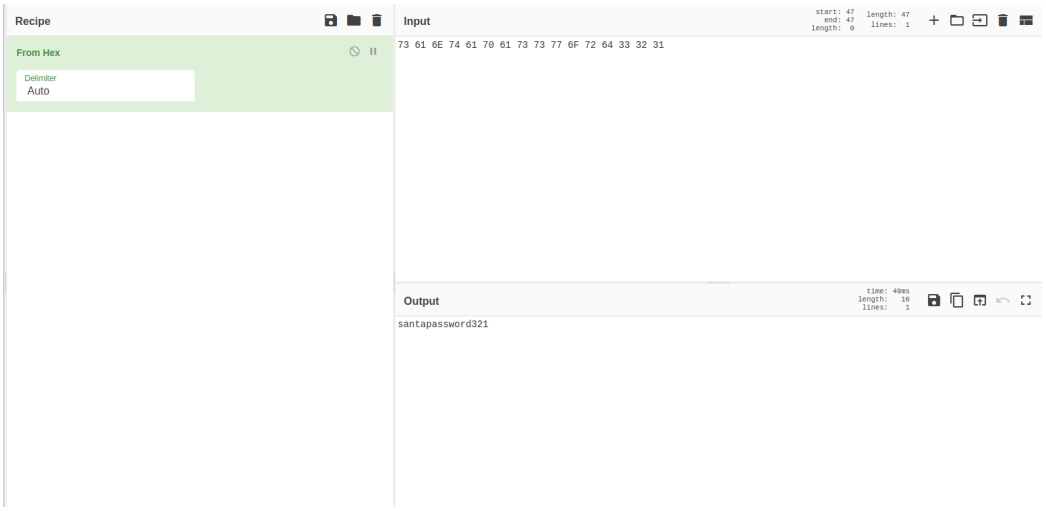
buttonActivate_Click

Question 6 : What is Santa's password?

Double click on the input saying santa password and copy the numbers displayed at the end.



Use CyberChef to debug the hexadecimal numbers.

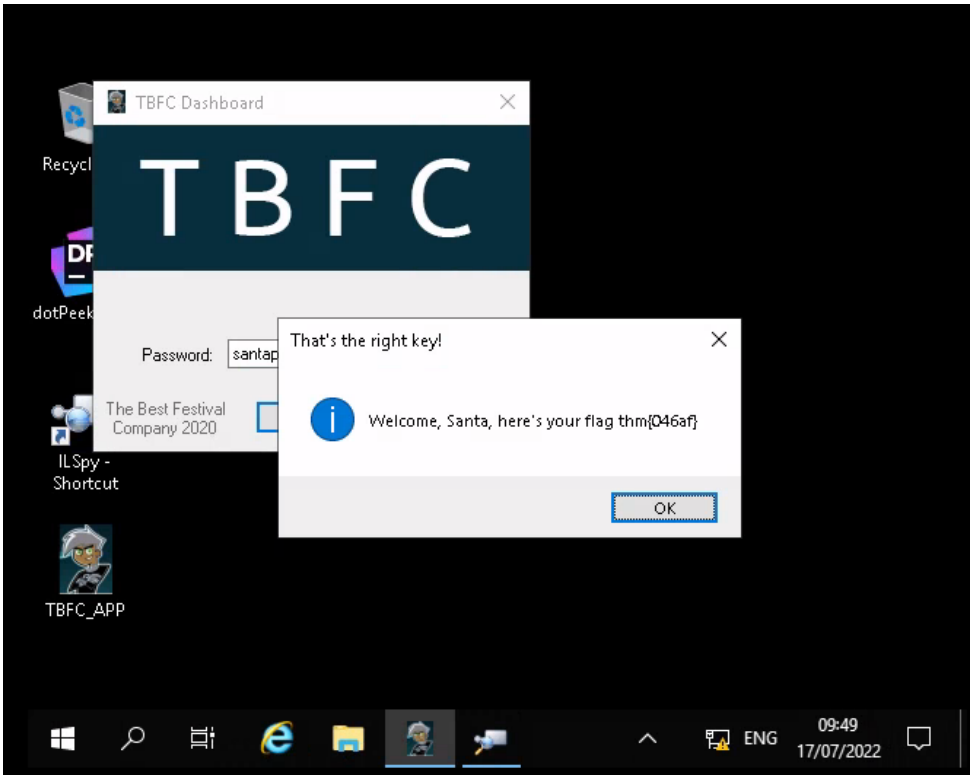


Answer :

santapassword321

Question 7 : Now that you've retrieved this password, try to login...What is the flag?

Insert the password in TBFC dashboard.



Answer :

thm{046af}

Thought/Processes :

First, we went to Remmina and turned on the TBFC app. A password is needed to login. We went to ILSpy and navigated to MainForm. From there, we went to buttonActivate_Click and clicked on [??_C@_0BB@IKKDFEPG@santapassword321@]. The data of hexadecimal numbers are copied and pasted into Cyberchef to debug the password. The password was then pasted back into TBFC app and the flag was posted.

Day 19- [Web Exploitation], The Naughty or Nice list
Tools used: Kali Linux, Firefox

Solution/walkthrough:

Q1: Which list is this person on?

This can be checked by entering the name into the search box

Welcome children!

To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

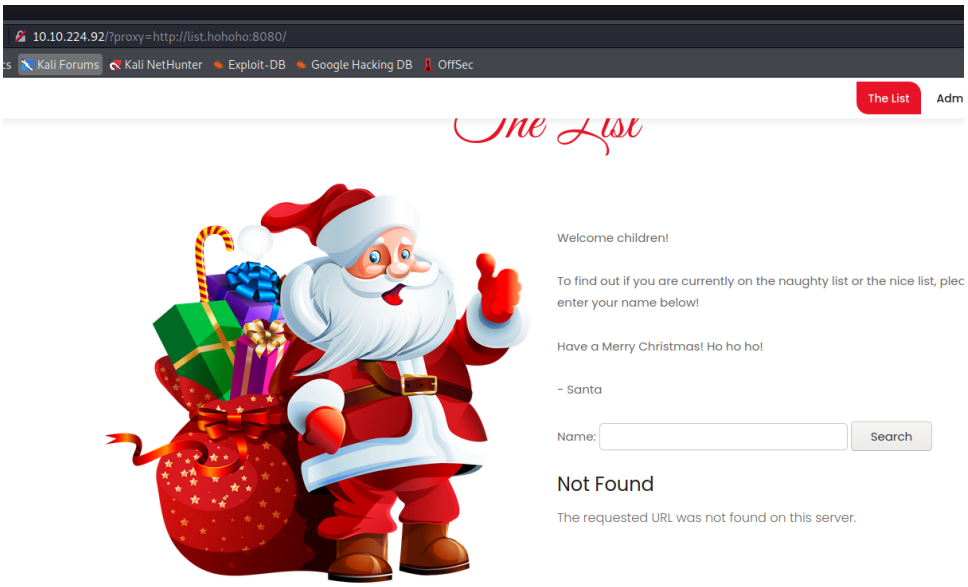
Name: Ian Chai Search

Ian Chai is on the Nice List.

	Naughty	Nice
YP	○	◉
Kanes	◉	○
Timothy	◉	○
JJ	◉	○
Ian Chai	○	◉
Tib3rius	○	◉

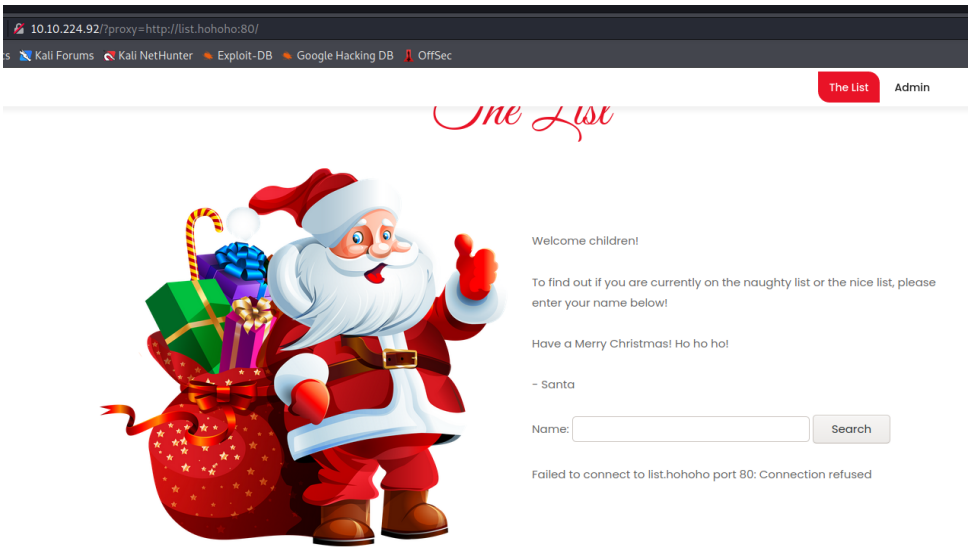
Q2: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"?

First, decode the code link to ASCII
/?proxy=http://list.hohoho:8080/



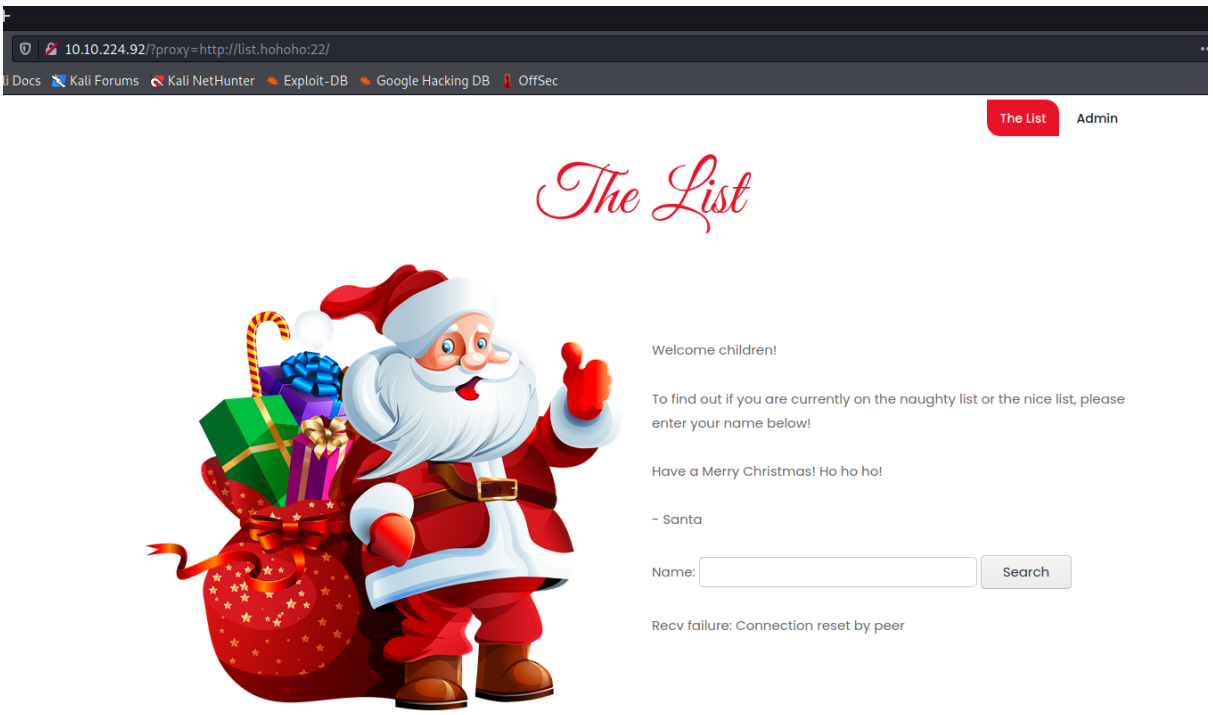
Answer: `Not Found. The requested URL was not found on this server.`

Q3: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A80"?



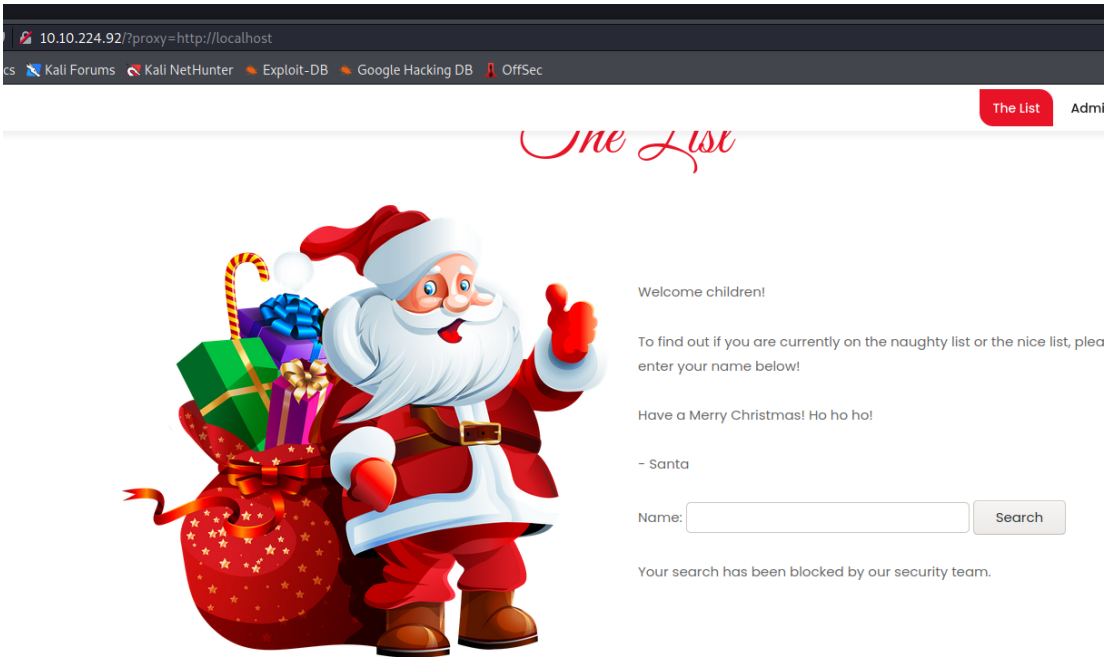
Answer: `Failed to connect to list.hohoho port 80: Connection refused`

Q4: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A22"?



Answer: `Recv failure: Connection reset by peer`

Q5: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"?



Answer: `Your search has been blocked by our security team.`

Q6: What is Santa's password?

After setting the set the hostname in the URL to "list.hohoho.localtest.me" to bypass the check, I am able to access the local services

Have a Merry Christmas! Ho Ho Ho!

- Santa

Name: Search

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!

- Elf McSkidy

Answer: Be good for goodness sake!

Q7: What is the challenge flag?

Now that we have the password, we can log in and find the flag

Answer: THM{EVERYONE_GETS_PRESENTS}

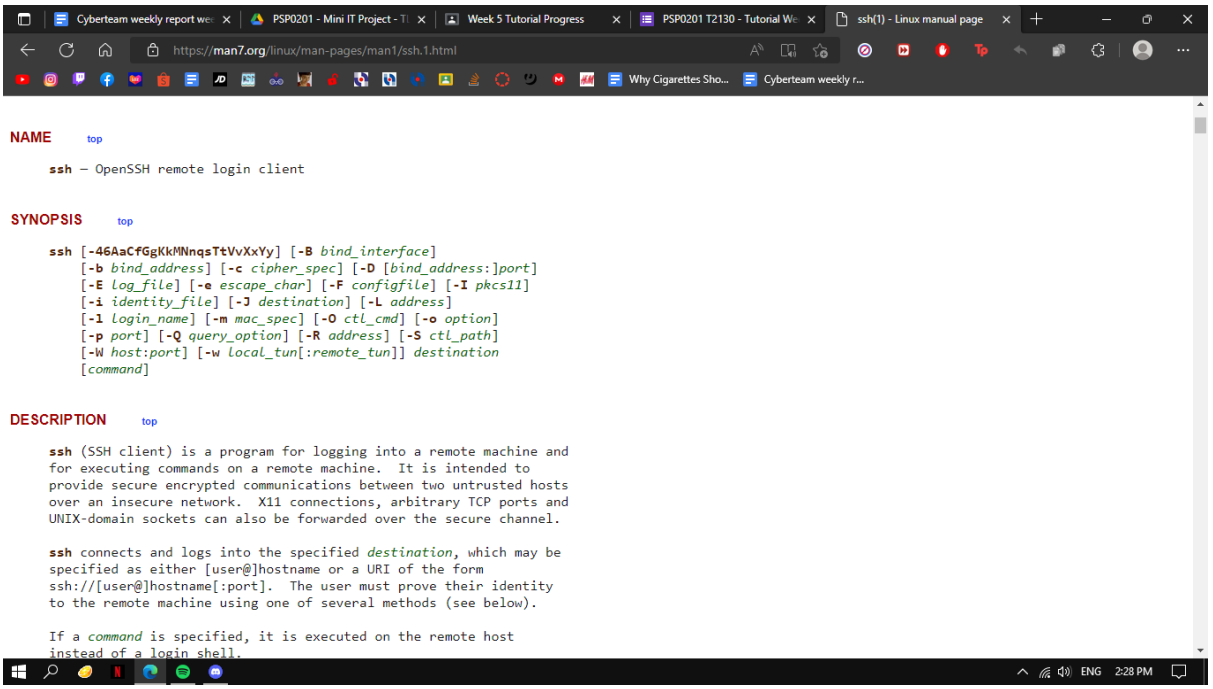
Thought/processes:

In order to not get blocked by the security, I need to have list.hohoho in the url, then use localtest.me, which will resolve the DNS entry to 127.0.0.1, adding it into the url, I was able to find the password.

Day 20 - PowershELIF to the rescue

Tools used: Kali Linux, Firefox

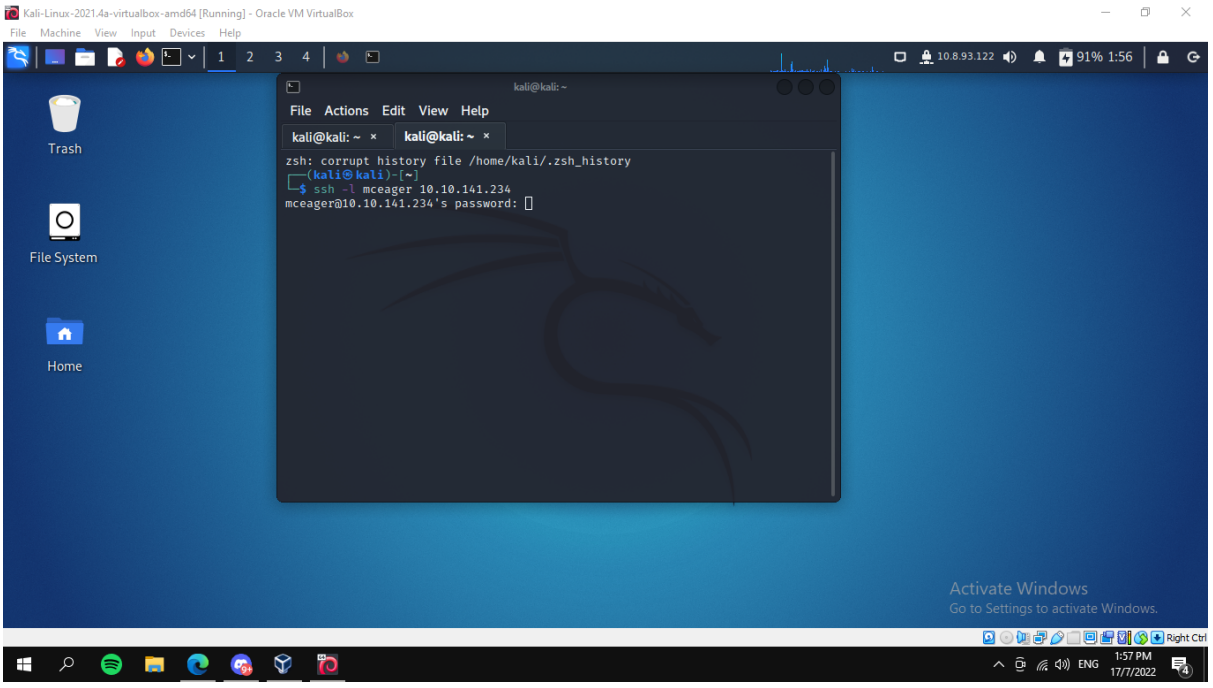
Q1: Check the ssh manual. What does the parameter -l do?



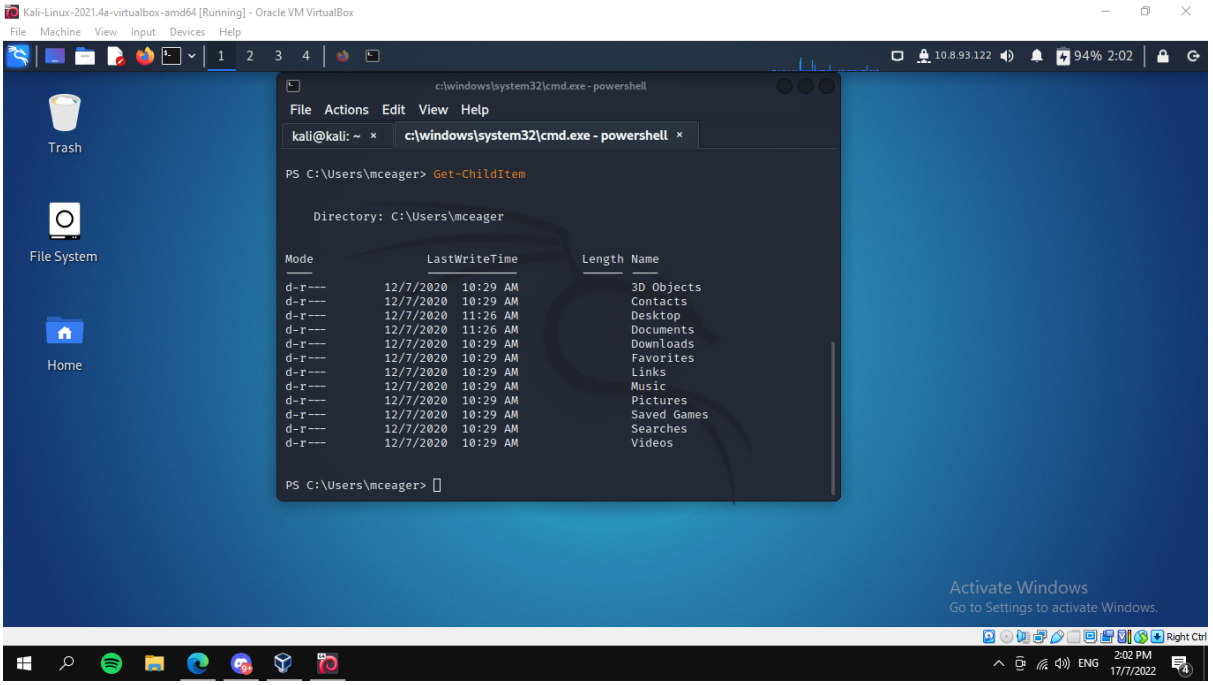
Answer: Login Name

Q2: Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

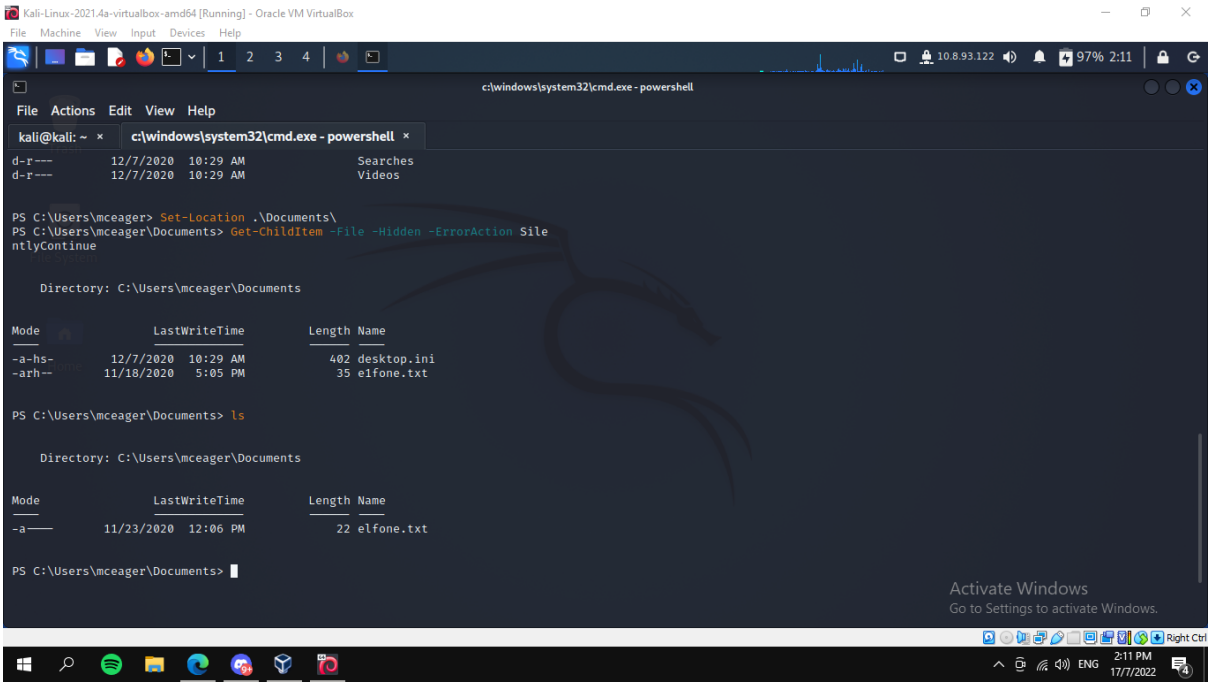
We first connect to the remote machine and input the password given



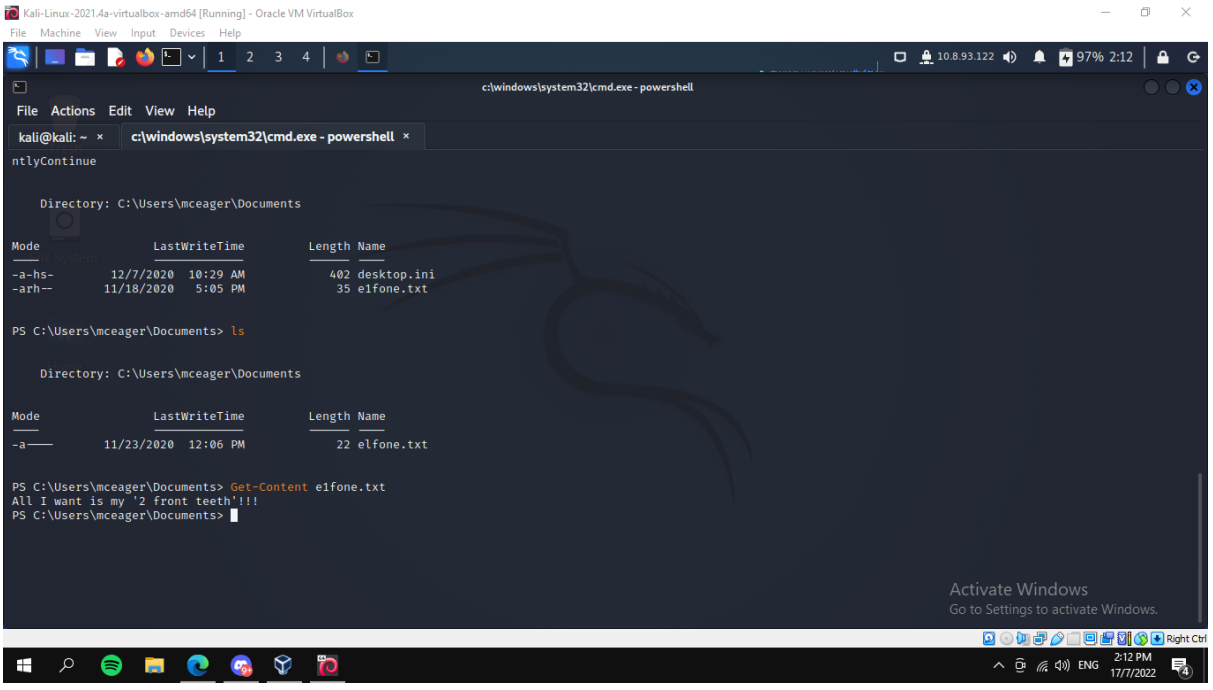
We then use the Get-ChildItem command to list down the contents of the current directory we are in



We then change the directory and view the hidden contents in the current directory. We then list files to view the text file



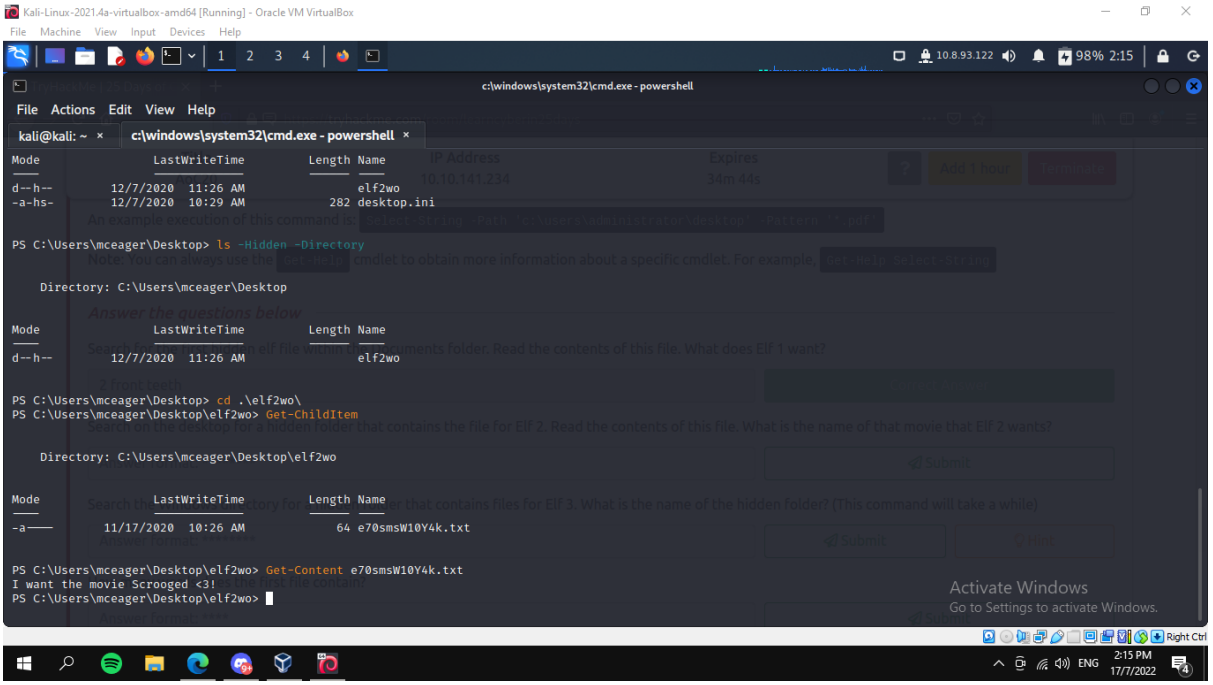
We then use Get-Content to read the contents of the file



Answer: 2 front teeth

Q3: 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?

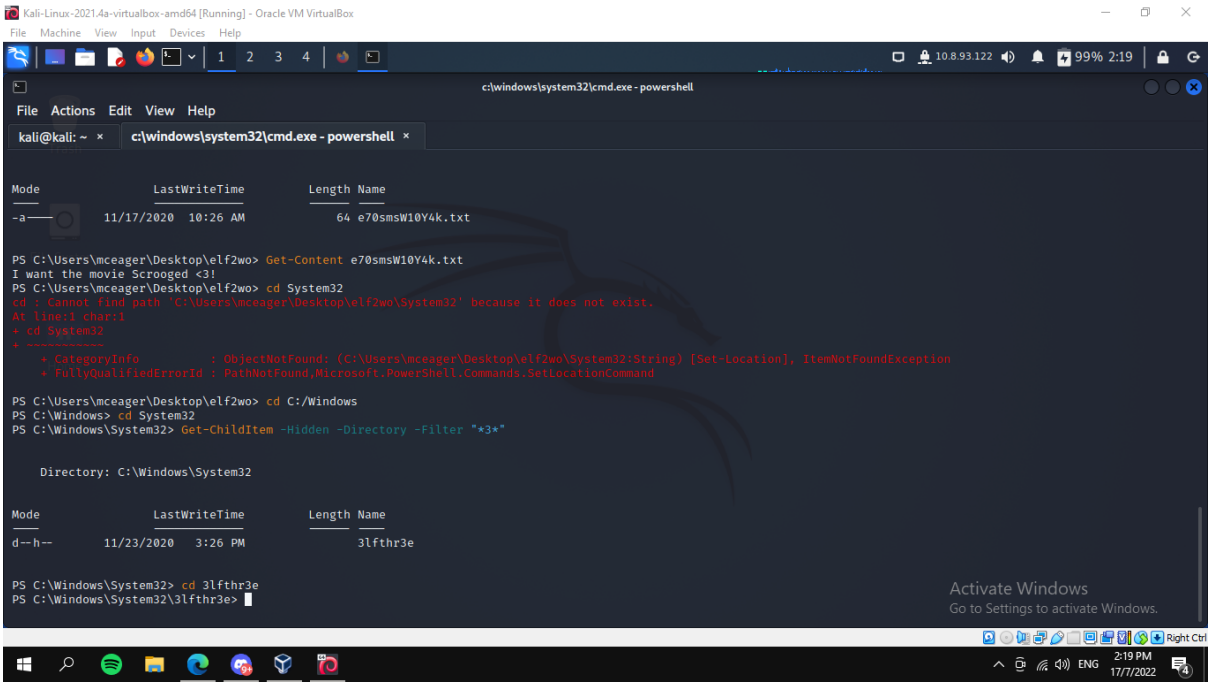
Once we changed directory to desktop, we list hidden files and list contents in them to get the text file. Then we can use Get-Content to read the contents of the text file.



Answer: Scrooged

Q4: 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)

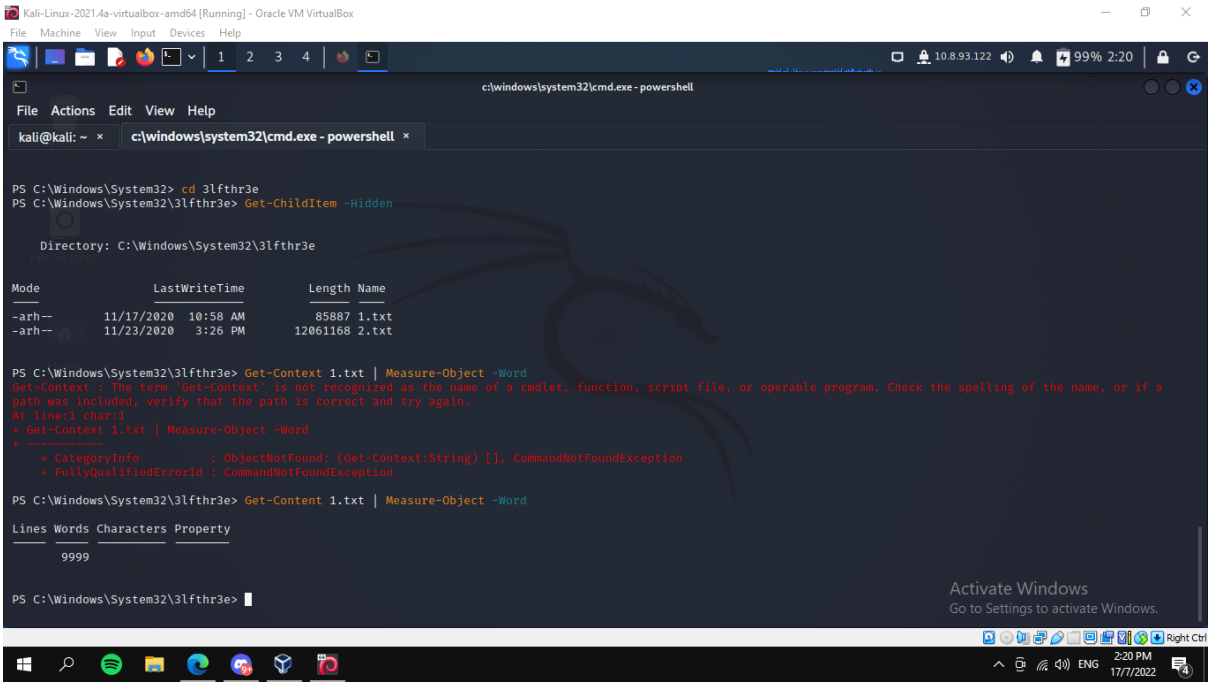
We change directory to Windows and then to System32, then we get the contents of the current directory with the help of filter command to filter out the file we want from the unnecessary files.



Answer: 3lfthr3e

Q5: How many words does the first file contain?

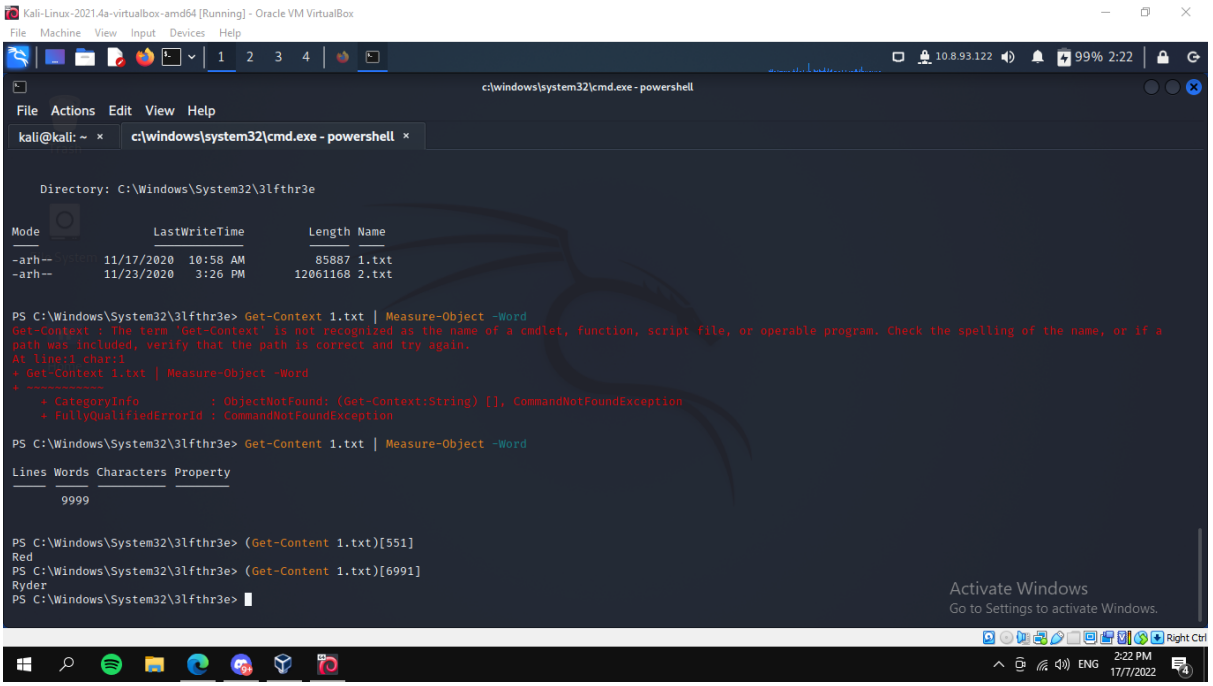
After reading the current directory and receiving the text file, we measure the words of the specific file with the help of the command given.



Answer: 9999

Q6: What 2 words are at index 551 and 6991 in the first file?

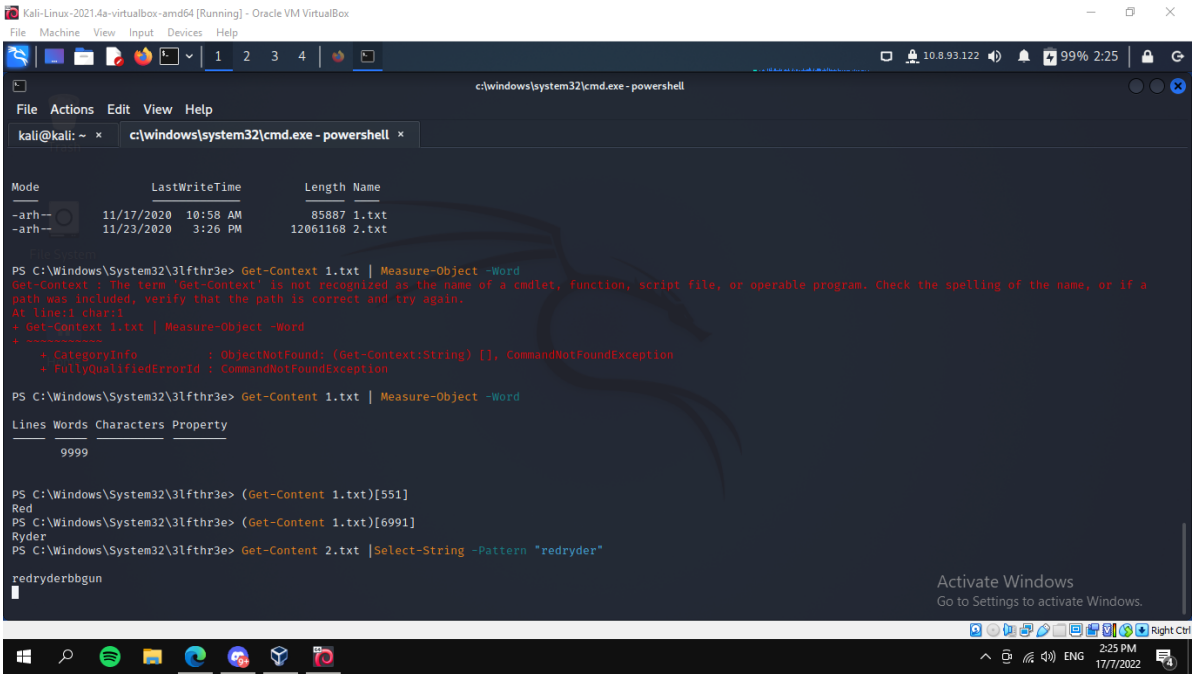
We can read the specific words in the list with Get-Content command along with the number of the line we want to read



Answer: Red Ryder

Q7: 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)

We can use the Select-String command along with the word we want which was redryder to get the phrase we want.



Answer: red ryder bb gun

Thought process/Methodology:

Having accessed the target machine, we are able to change the directory of the hidden file we want and list files to view the text files available. We also use commands such as Get-Content to read the contents of the file we want. This step is repeated for different directories. After reading the specific directory and receiving the text file, we measure the words of the specific file with the help of the command such as Measure-Object -Word. In a long list in the text file, we can use commands such as Select-String and with the help of filter, instantly get the result we want without looking for it which would be time consuming.