PSP0201

Week 5

Write Up

Group name: Code Blu

ID	Name	Role
1211103236	Tang Yu Xuan	Leader
1211102879	Koh Jia Jie	Member
1211101196	Tan Hui Jeen	Member
1211100571	Teh Yvonne	Member

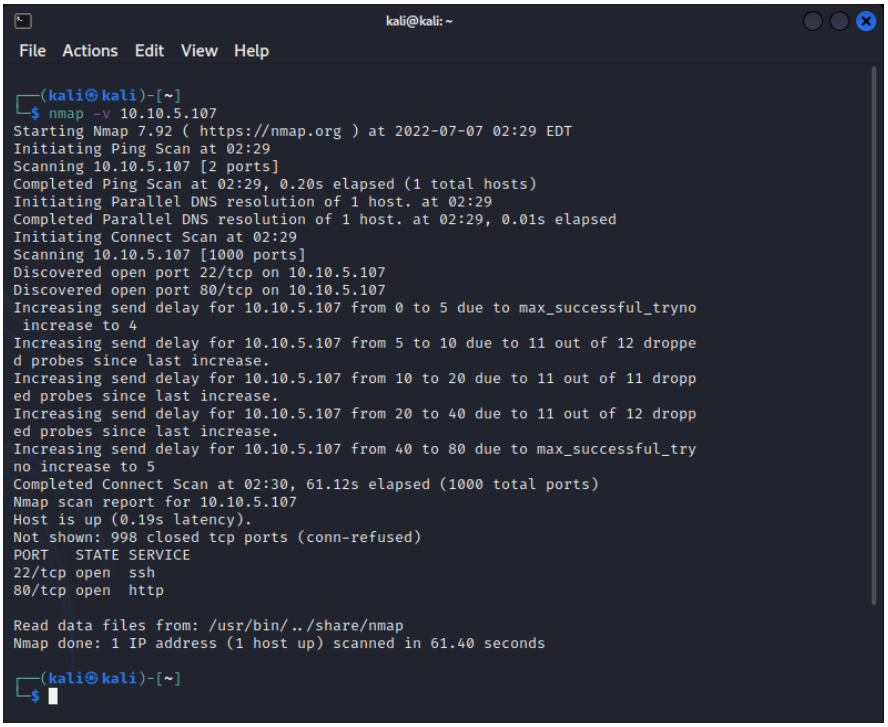
Day 16: Help! Where is Santa?

Tools Used: Kali Linux

Solution / Walkthrough:

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

In the terminal, we use nmap to scan the network with the '-v' tag (verbose mode) and the given ip address (10.10.5.107) to check for the port number. Here, we are able to find that the port number for the web server is **80**.



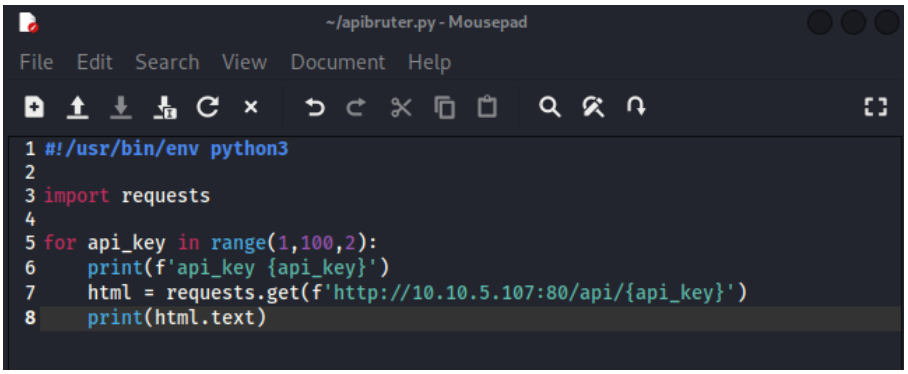
Question 2: Without using enumerations tools such as Dirbuster, what is the directory for the API? (without the API key)

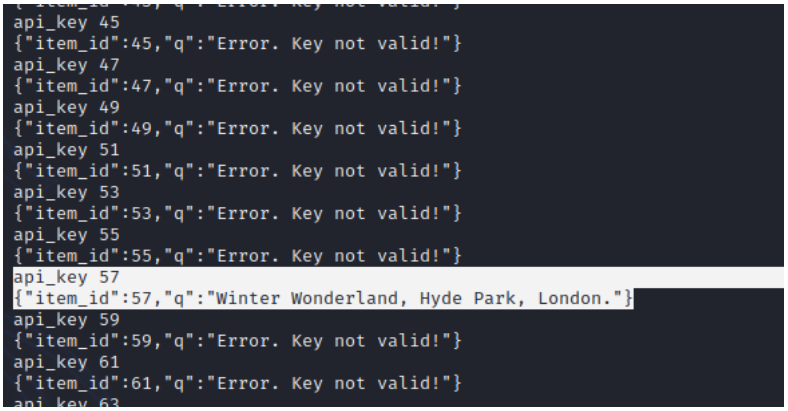
After entering the webpage: 10.10.5.107:80, we are able to view the source code and look for the directory for the API , which is **/api/** as seen below.

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

Question 3: Where is Santa right now?

After typing in the below codes in Python, specifying the range of API keys is between 1 to 100 and is an odd number, we are able to find the location of Santa: **Winter Wonderland, Hyde Park, London**.

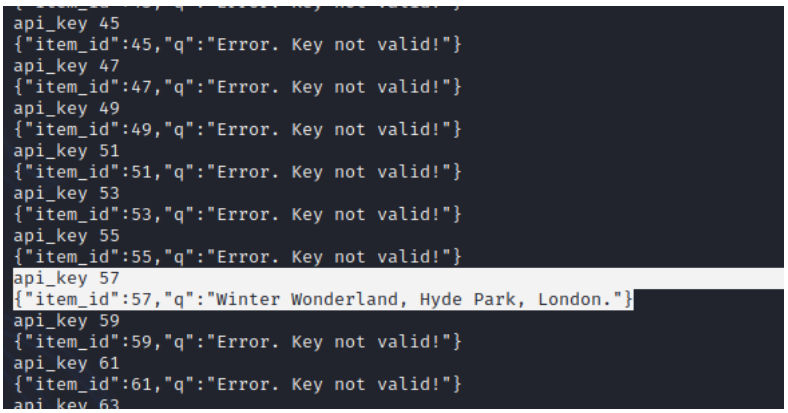




Question 4: Find out the correct API key. Remember, this is an odd number between 0-100. After too many attempts, Santa's Sled will block you.

To unblock yourself, simply terminate and re-deploy the target instance (10.10.14.113)

We are also able to identify the API key is **57** after finding Santa's location.



Through process/ methodology:

Firstly, we typed in "nmap -v 10.10.5.107" to find the port number for the web server. After running it successfully, we are able to enter the webpage with the port number, "10.10.5.107:80". Here, we found the directory for the API by right clicking to view source code or by using Python with Libraries which was learnt on day 15. Next, we found Santa's

location using Python by specifying the range of API keys is from 1 to 100 and it is an odd number. Lastly, the API key was shown when we searched for Santa’s location.

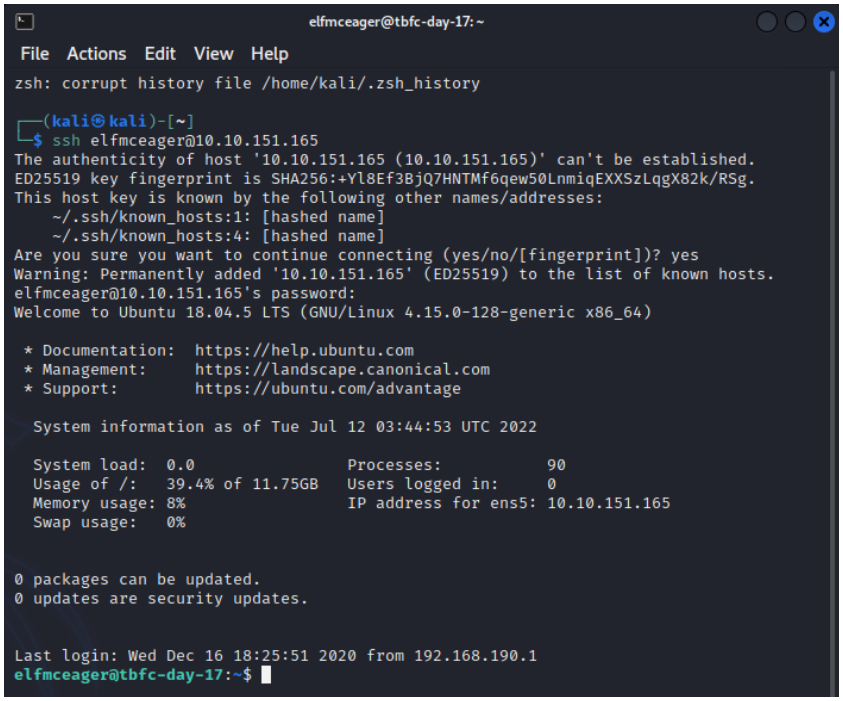
Day 17: ReverseELFneering

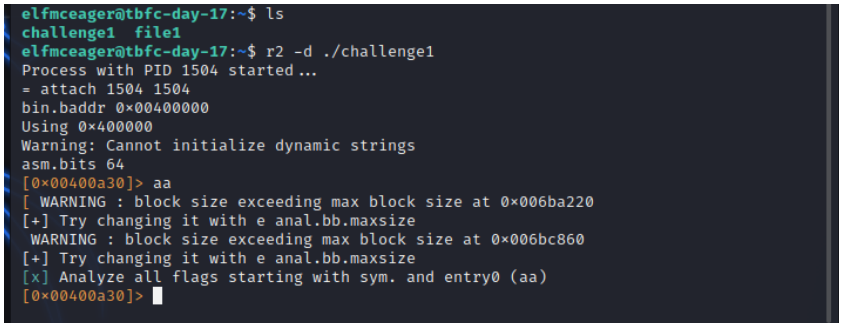
Tools Used: Kali Linux

Solution / Walkthrough:

Question 1: What is the value of local_ch when its corresponding movl instruction is called (first if multiple)?

Using ssh and the password given (adventofcyber), we logged in as elfmceager. We were able to see the folder "challenge1" and ran the following command to open the binary in debugging mode. After this, we used "aa" to analyse the program. To find a list of the functions, we ran the command "afl | grep main". Then, we examine the assembly code at main by running the command "pdf @main". From here, we are able to see that the value **1** is copied into local_ch.





Question 2: What is the value of eax when the imull instruction is called?

The value 6 is copied into local_8h. Next, the value in local_ch, 1 is copied into eax. We are able to obtain the value of eax by multiplying the value in local_8h with eax, which is 6 multiplied by 1, hence eax has the value **6** now.

Question 3: What is the value of local_4h before eax is set to 0?

The value in eax, **6** is copied to local_4h.

Through process/ methodology:

After logging in to elfmceager with the password given (adventofcyber), we can open the binary in debugging mode of the folder “challenge1” and analyse the program. After the analysis is done, we found the functions containing “main”. Lastly, by using “pdf @main” we are able to examine the assembly code.

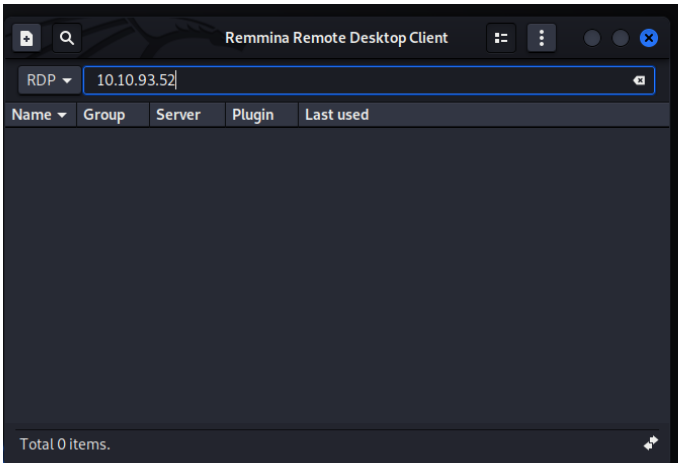
Day 18: The Bits of Christmas

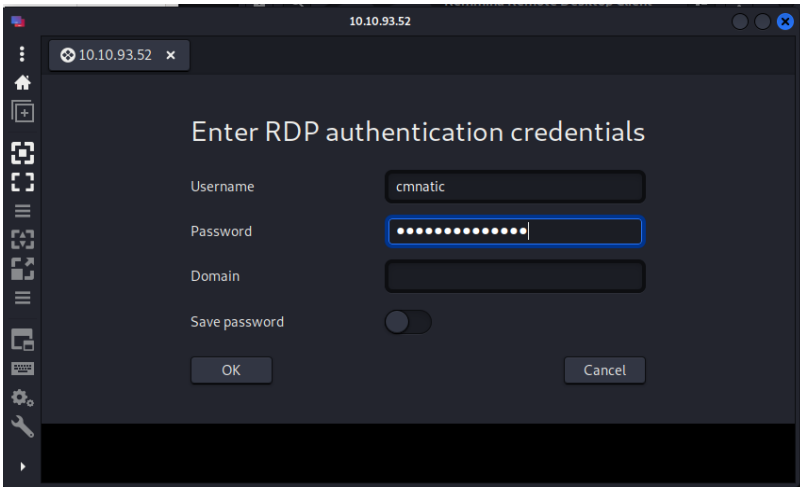
Tools Used: Kali Linux, Remmina, ILSpy

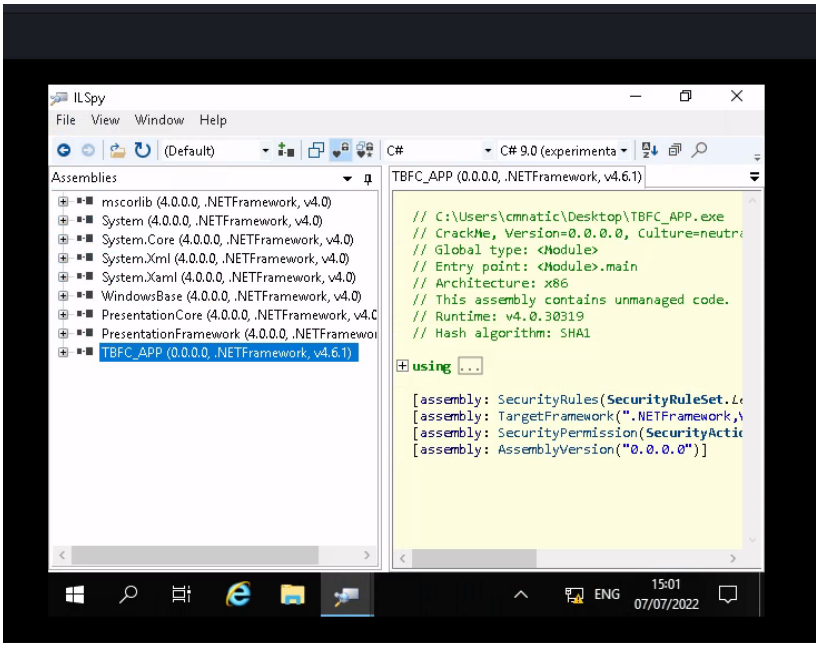
Solution / Walkthrough:

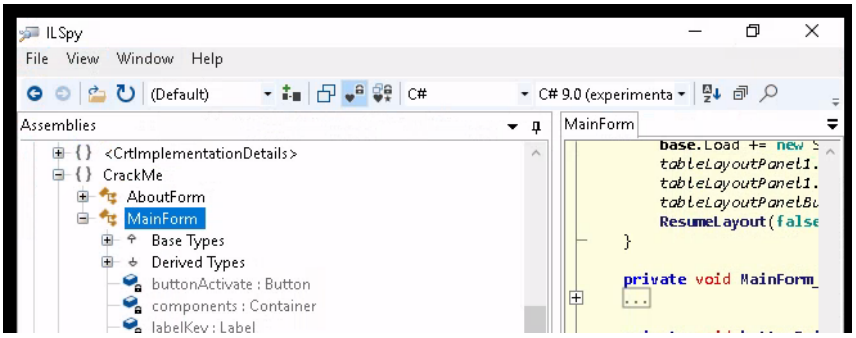
Question 1: What is Santa's password?

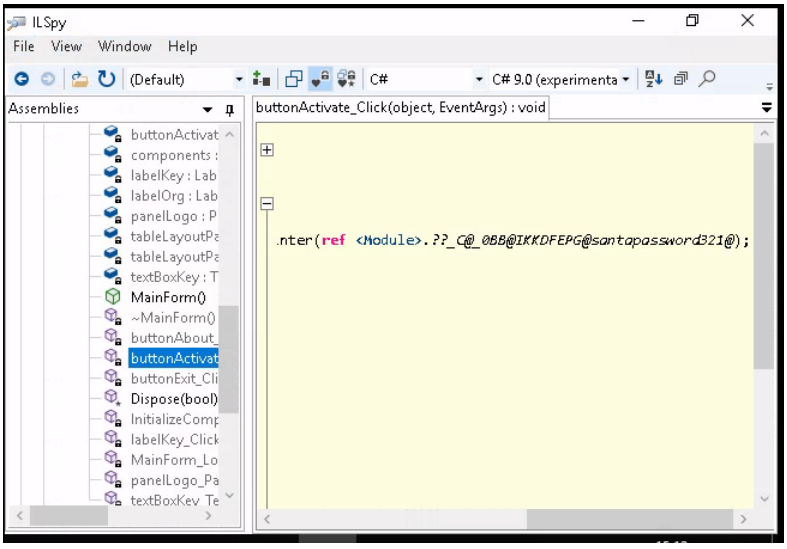
Using Remmina, we type in the IP address given into the RDP. A pop up screen will appear asking for the username: “cmnatic” and the password: “Adventofcyber!”. After clicking ILSpy, we opened TBFC_APP from the Desktop. From here, we clicked the “+” button to view more details. We are able to see “CrackMe” and under it, we can see the details of “MainForm”. In the “MainForm”, we clicked into “buttonActivate…” to view it and double clicked into the”santapassword321” and copied the values. We then used Cyberchef to convert the hexadecimal values, which indeed showed Santa’s password to be “**santapassword321**”.

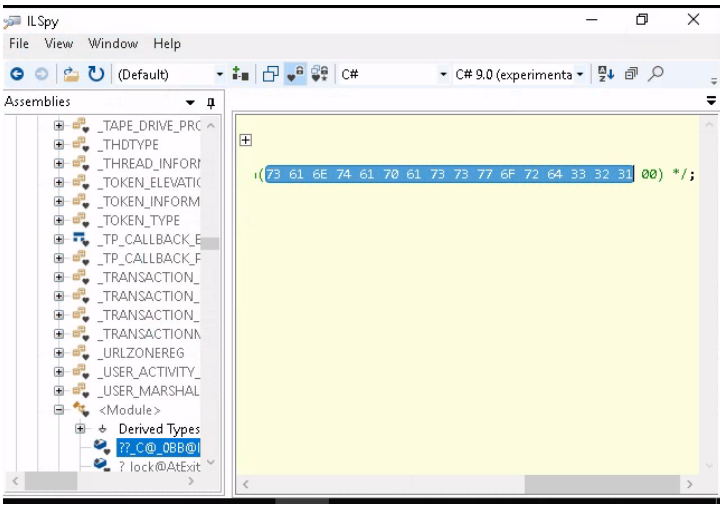


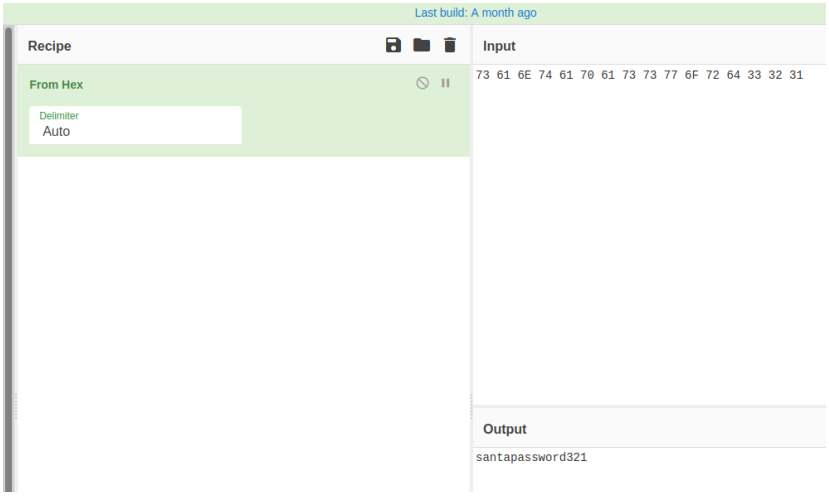



ILSpy
File View Window Help
(Default)
C#
C# 9.0 (experimenta
Assemblies
TBFC_APP (0.0.0.0, .NETFramework, v4.6.1)
mscorlib (4.0.0.0, .NETFramework, v4.0)
System (4.0.0.0, .NETFramework, v4.0)
System.Core (4.0.0.0, .NETFramework, v4.0)
System.Xml (4.0.0.0, .NETFramework, v4.0)
System.Xaml (4.0.0.0, .NETFramework, v4.0)
WindowsBase (4.0.0.0, .NETFramework, v4.0)
PresentationCore (4.0.0.0, .NETFramework, v4.0
PresentationFramework (4.0.0.0, .NETFramewor
TBFC_APP (0.0.0.0, .NETFramework, v4.6.1)
// C:\Users\cmnatic\Desktop\TBFC_APP.exe
// CrackMe, Version=0.0.0.0, Culture=neutra
// Global type: <Module>
// Entry point: <Module>.main
// Architecture: x86
// This assembly contains unmanaged code.
// Runtime: v4.0.30319
// Hash algorithm: SHA1
using ...
[assembly: SecurityRules(SecurityRuleSet.L
[assembly: TargetFramework(".NETFramework,
[assembly: SecurityPermission(SecurityActio
[assembly: AssemblyVersion("0.0.0.0")]
ENG
15:01
07/07/2022


ILSpy
File View Window Help
(Default)
C#
C# 9.0 (experimenta
Assemblies
MainForm
<CrtImplementationDetails>
CrackMe
AboutForm
MainForm
Base Types
Derived Types
buttonActivate : Button
components : Container
labelKey : Label
base.Load += new
tableLayoutPanel1.
tableLayoutPanel1.
tableLayoutPanelBu
ResumeLayout(false
}
private void MainForm_
...

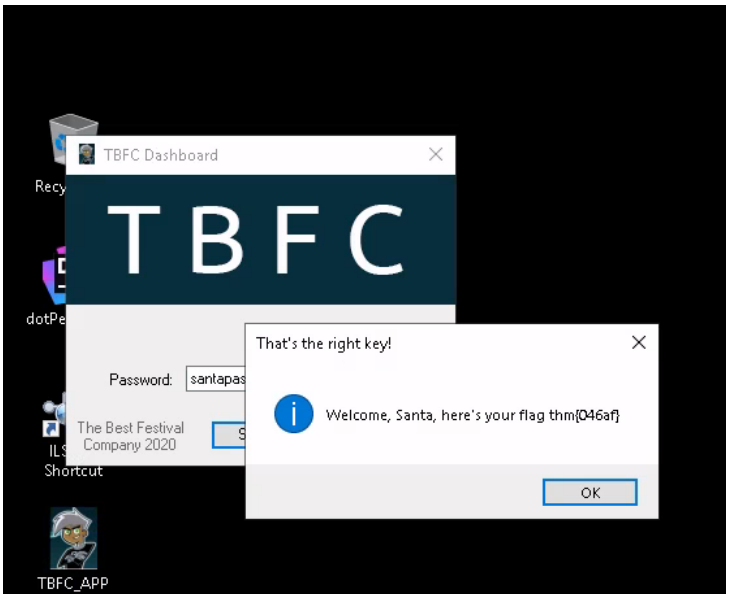

ILSpy
File View Window Help
(Default)
C#
C# 9.0 (experimenta
Assemblies
buttonActivate_Click(object, EventArgs) : void
buttonActivat
components :
labelKey : Lab
labelOrg : Lab
panelLogo : P
tableLayoutPa
tableLayoutPa
textBoxKey : T
MainForm()
~MainForm()
buttonAbout_
buttonActivat
buttonExit_Cli
Dispose(bool)
InitializeComp
labelKey_Click
MainForm_Lo
panelLogo_Pa
textBoxKey_Te
nter(ref <Module>.??_C@_0BB@IKKDFEPG@santapassword321@);





Question 2: Now that you've retrieved this password, try to login...What is the flag?

After knowing the password, we can login to TBFC_APP to get the flag, which is **thm{046af}**.



Through process/ methodology:

Having the password to open Remmina, we are able to open ILSpy from it. We then opened TBFC_APP in ILSpy. From here, we found “CrackMe”to be unique and clicked on the “+” button. We clicked on “MainForm” and then “buttonActivate…” to view the details in it. In this file, we can see the password was given but was unsure, hence, we double clicked into the password and found hexadecimal values. We then convert them using Cyberchef which shows the password in String. After knowing the password, we are able to successfully login to TBFC_APP using the password, which then shows us the flag.

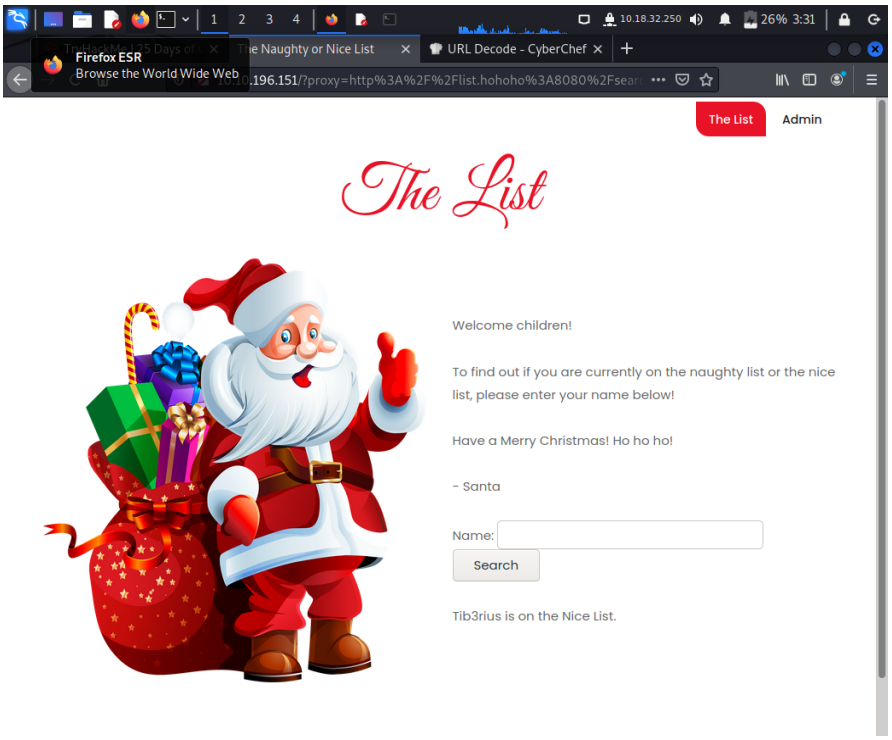
Day 19: The Naughty or Nice List

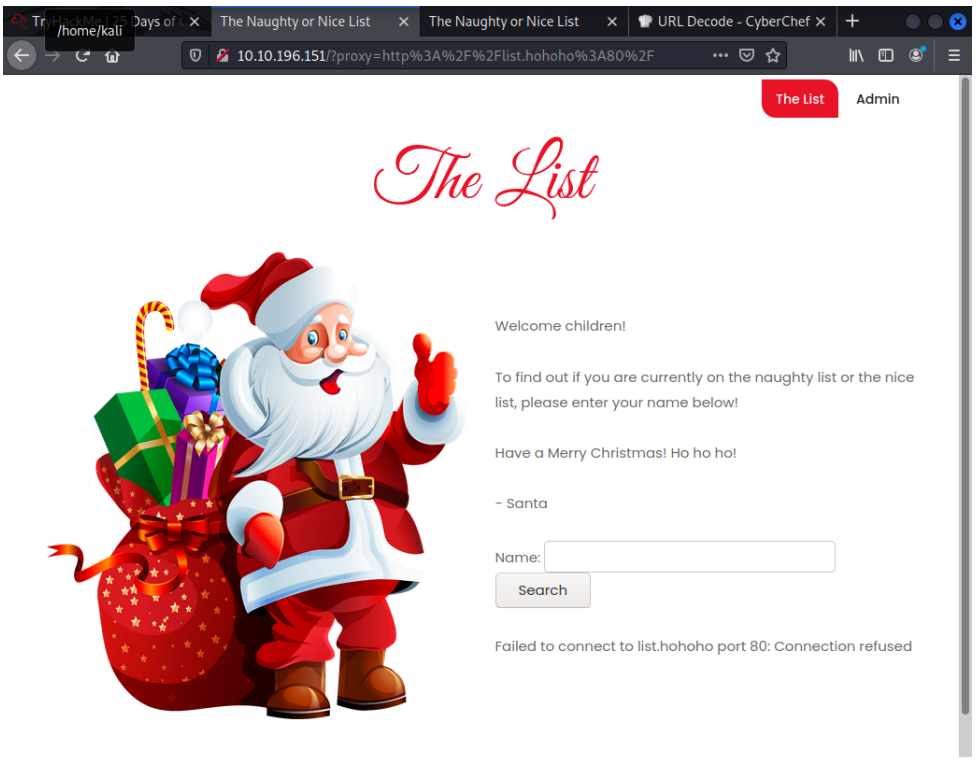
Tools Used: Kali Linux

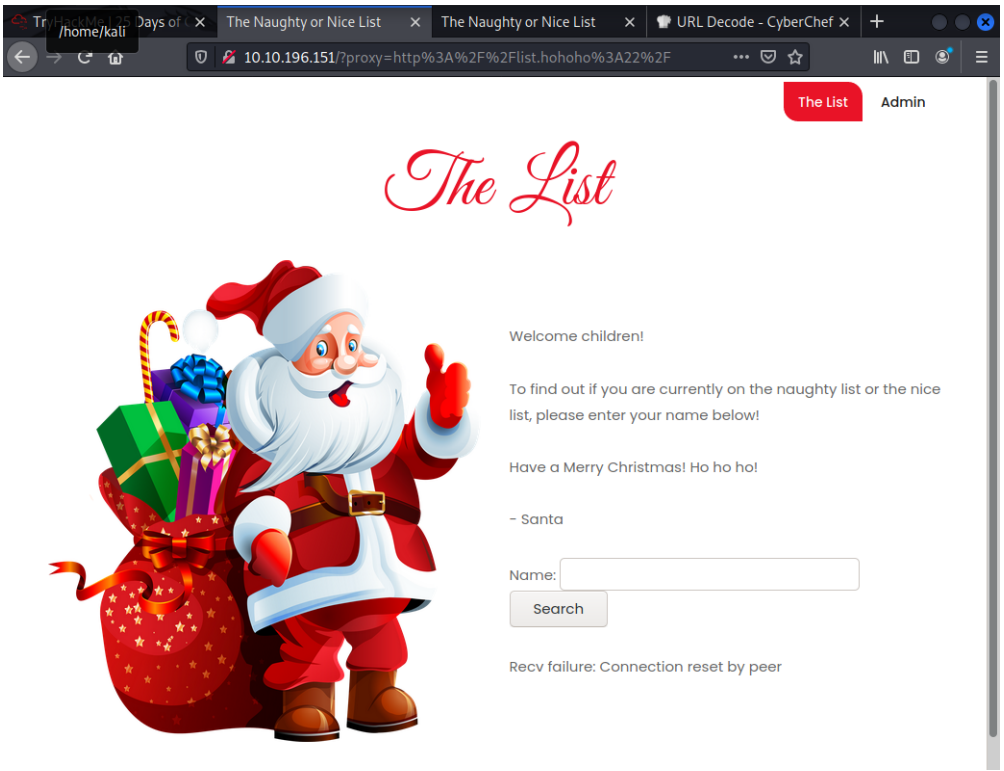
Solution / Walkthrough:

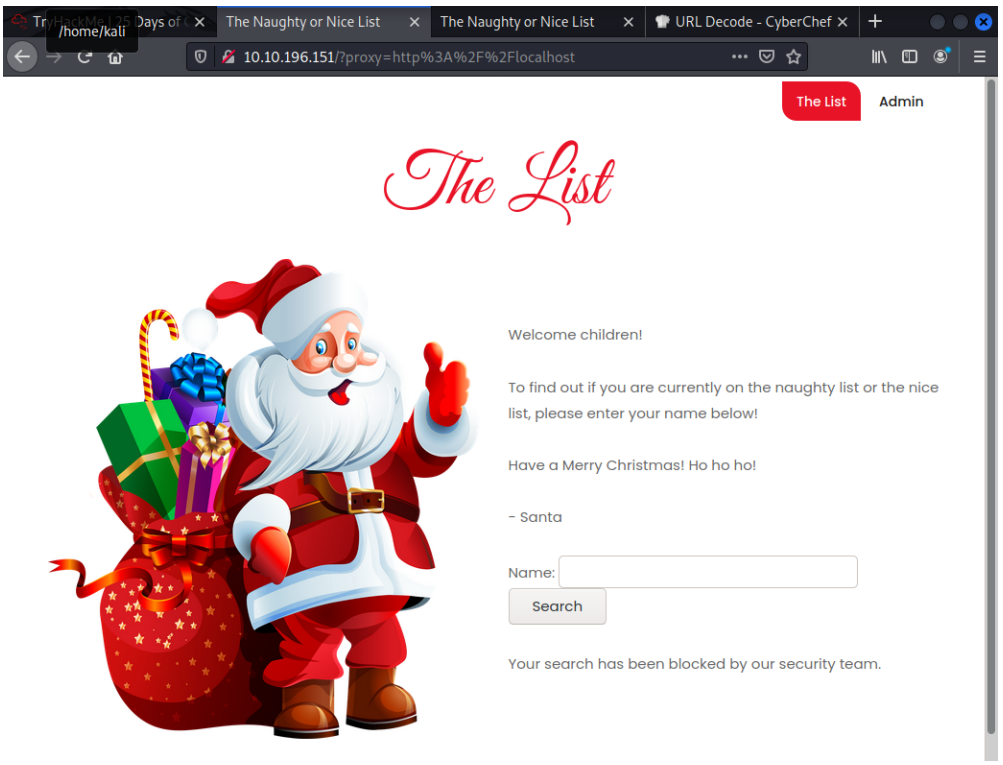
Question 1: What is Santa's password?

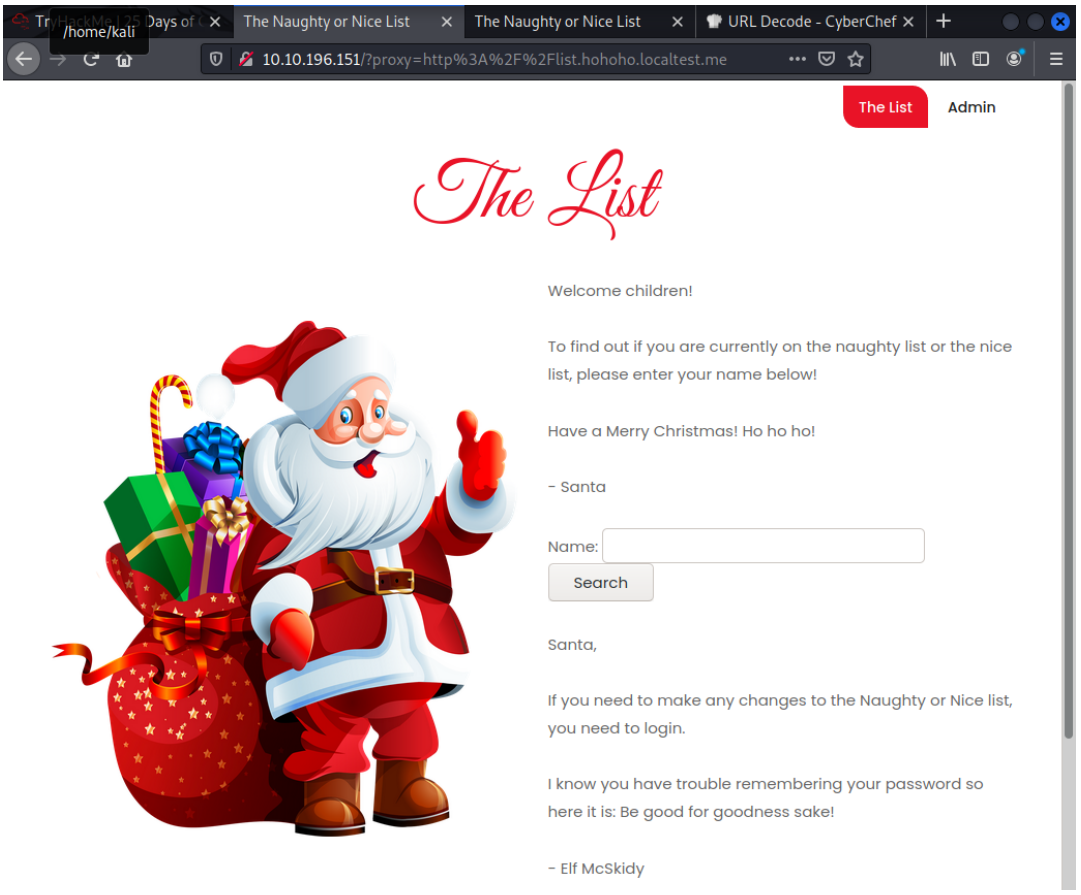
After entering the website (10.10.196.151), we checked for different ports in order to get Santa's password, such as port 80, 22 and localhost, however, these did not work out. We then tried with "localtest.me". It showed a message with Santa's password, which is "**Be good for goodness sake!**"




/home/kali
The Naughty or Nice List
The Naughty or Nice List
URL Decode - CyberChef
10.10.196.151/?proxy=http%3A%2F%2Flist.hohoho%3A80%2F
The List
Admin
The List
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:
Search
Failed to connect to list.hohoho port 80: Connection refused


/home/kali
The Naughty or Nice List
The Naughty or Nice List
URL Decode - CyberChef
10.10.196.151/?proxy=http%3A%2F%2Flist.hohoho%3A22%2F
The List
Admin
The List
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:
Search
Recv failure: Connection reset by peer

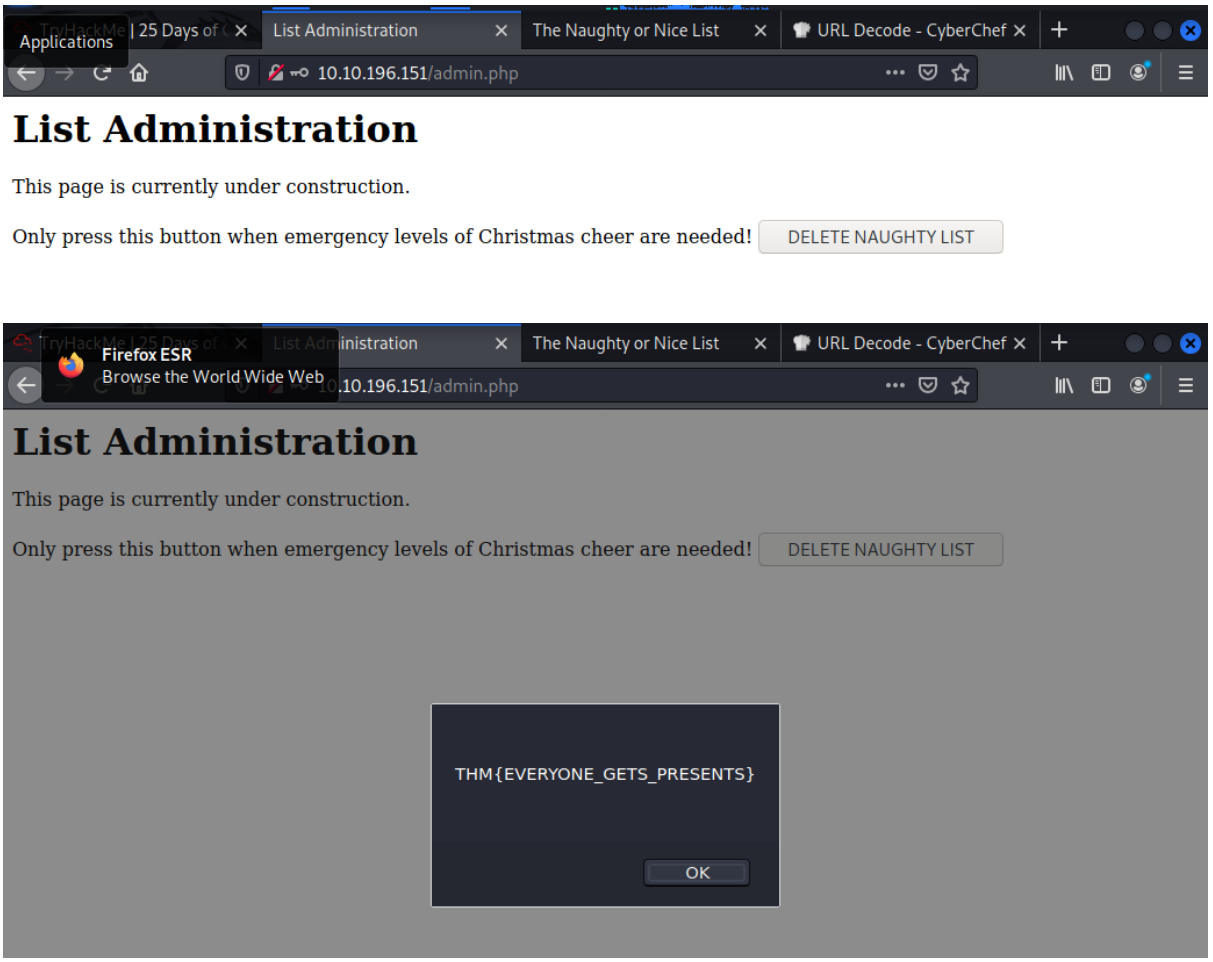

/home/kali
The Naughty or Nice List
The Naughty or Nice List
URL Decode - CyberChef
10.10.196.151/?proxy=http%3A%2F%2Flocalhost
The List
Admin
The List
Welcome children!
To find out if you are currently on the naughty list or the nice list, please enter your name below!
Have a Merry Christmas! Ho ho ho!
- Santa
Name:
Search
Your search has been blocked by our security team.


/home/kali
The Naughty or Nice List
The Naughty or Nice List
URL Decode - CyberChef
10.10.196.151/?proxy=http%3A%2F%2Flist.hohoho.localtest.me
The List
Admin
The List
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:
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

Question 2: What is the challenge flag?

We logged in with the password given and typed in “Santa” as the username. After that, we deleted the naughty list which then displayed the flag:

THM{EVERYONE_GETS_PRESENTS}



Through process/ methodology:

In the webpage, we changed the port from 8080 to port 80, 22 and localhost. These ports did not work out, hence we tried it with “localtest.me”. This then displayed a message from Mc Skidy and Santa’s password. We logged into the admin page by using Santa as the username and the given password. From here, we were able to delete the naughty list, which then showed us the flag for this task.

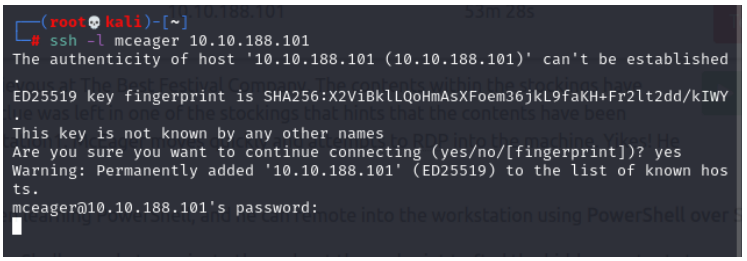
Day 20: PowershELlF to the rescue

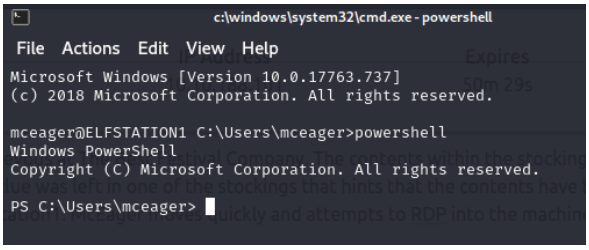
Tools Used: Kali Linux

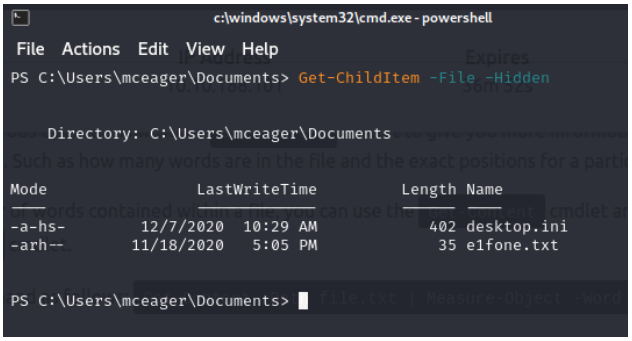
Solution / Walkthrough:

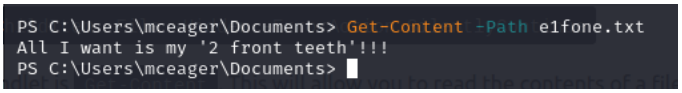
Question 1: Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

After typing in the following ssh command and password given (r0ckStar!), we typed in "powershell" and navigated to the Documents folder. Then, we used the commands below to find the hidden file. After finding the hidden file, we viewed the contents by using "Get-Content -Path e1fone.txt ", which displayed a message "All I want is my '**2 front teeth**'!!!".









Question 2: 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?

We redirected to the Desktop and searched for the hidden folder. In the hidden folder, we were able to find a file and view it, showing a message "I want the movie **Scrooged** <3!".

```
PS C:\Users\mceager\Documents> cd ..
PS C:\Users\mceager> Set-Location Desktop
PS C:\Users\mceager\Desktop> ls
PS C:\Users\mceager\Desktop> ls -Hidden

    Directory: C:\Users\mceager\Desktop


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> cd .\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!
PS C:\Users\mceager\Desktop\elf2wo>
```

Question 3: Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder?

We directed to Windows and searched for the hidden folder in System32 by filtering it. To make it easier, we included the "-Hidden -Directory" commands, which then showed "**3lfthr3e**".

```
PS C:\Users\mceager\Desktop\elf2wo> cd C:/Windows
PS C:\Windows> cd System32
PS C:\Windows\System32> Get-ChildItem -Filter "*3*"

    Directory: C:\Windows\System32

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         9/15/2018  12:12 AM         659720 advapi32.dll
-a----         9/15/2018  12:13 AM           2560 advapi32res.dll
-a----         9/15/2018  12:12 AM          79872 avicap32.dll
-a----         9/15/2018  12:12 AM         115712 avifil32.dll
-a----         9/15/2018  12:12 AM         293344 cfgmgr32.dll
-a----         9/15/2018  12:12 AM          73728 clfsw32.dll
-a----         9/15/2018  12:12 AM          37888 cmcfg32.dll
-a----         9/15/2018  12:12 AM         556032 cmdial32.dll
-a----         9/15/2018  12:12 AM          51712 cmdl32.exe
-a----         9/15/2018  12:12 AM          43008 cmmon32.exe
```

```
PS C:\Windows\System32> Get-ChildItem -Hidden -Directory -Filter "*3*"

    Directory: C:\Windows\System32

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

Question 4: How many words does the first file contain?

We viewed the folder and found two hidden files. We then typed in the following commands to get the words count for the first file, which is **9999**.

```
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

PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Measure-Object -Word

Lines Words Characters Property
----- ----- ---------- --------
        9999
```

Question 5: What 2 words are at index 551 and 6991 in the first file?

To get the words in the respective indexes, we typed in the commands below, which displayed "**Red**" at index 551 and "**Ryder**" at index 6991.

```
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[551]
Red
PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[6991]
Ryder
PS C:\Windows\System32\3lfthr3e>
```

Question 6: 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?

We used the command below to search for the particular file by including "redryder". It then displayed **red ryder bb gun**.

```
PS C:\Windows\System32\3lfthr3e> Get-Content 2.txt | Select-String -Pattern "
redryder"

redryderbbgun
```

Through process/ methodology:

We first typed in the ssh command and the password. After gaining access, we launched powershell and directed it to Documents. In the Documents, we searched for the hidden file and viewed the contents which displayed a message saying Elf 1 wants its 2 front teeth. Next, we directed to Desktop to search for the hidden folder and viewed the file in it, showing a message about Elf 2 wanting the movie Scrooged. Lastly, we directed to Windows, then to System32. We searched for the hidden folder by filtering it, including a string that contains "3". After finding the hidden folder, we got the words count for the first hidden file. In this file, we were able to know the words on index 551 and 6991. The next step was to find the phrase from the second hidden file. We simplified the searching process which then displayed the phrase.