PSP0201 Week 5 Writeup

Group Name: Siuuu

Members

ID	Name	Role
1211103423	Muhammad Rino Frawidya bin Suheri	Leader
1211104232	Muhammad Amirul Haiqal Bin Zameri	Member
1211101924	Nur Ayu Farisha Binti Hamdan @ Hood	Member

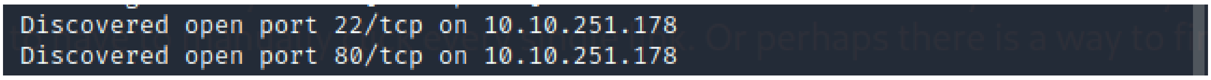
Day16: Scripting - Help! Where is Santa?

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

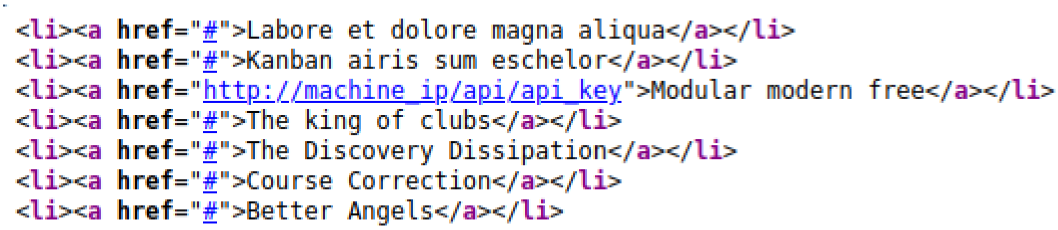
We scan the IP Address using nmap to get the port number



```
Discovered open port 22/tcp on 10.10.251.178
Discovered open port 80/tcp on 10.10.251.178
```

Question 2

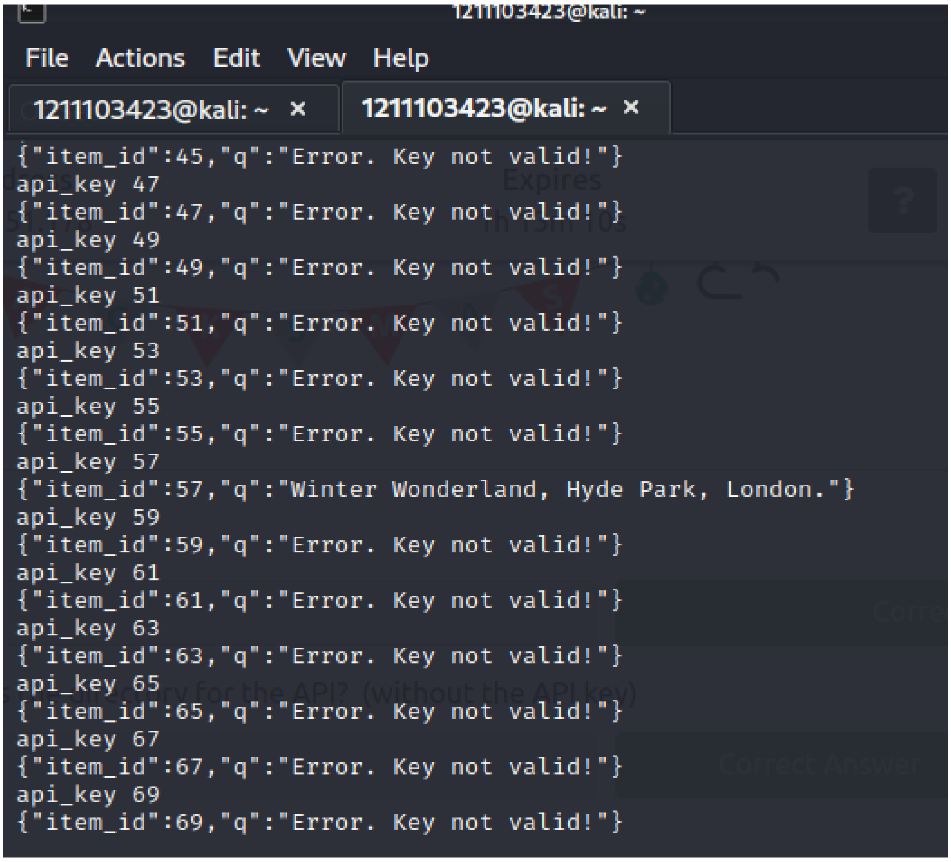
We view the page source of the web to find the directory of the api



```
<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>
```

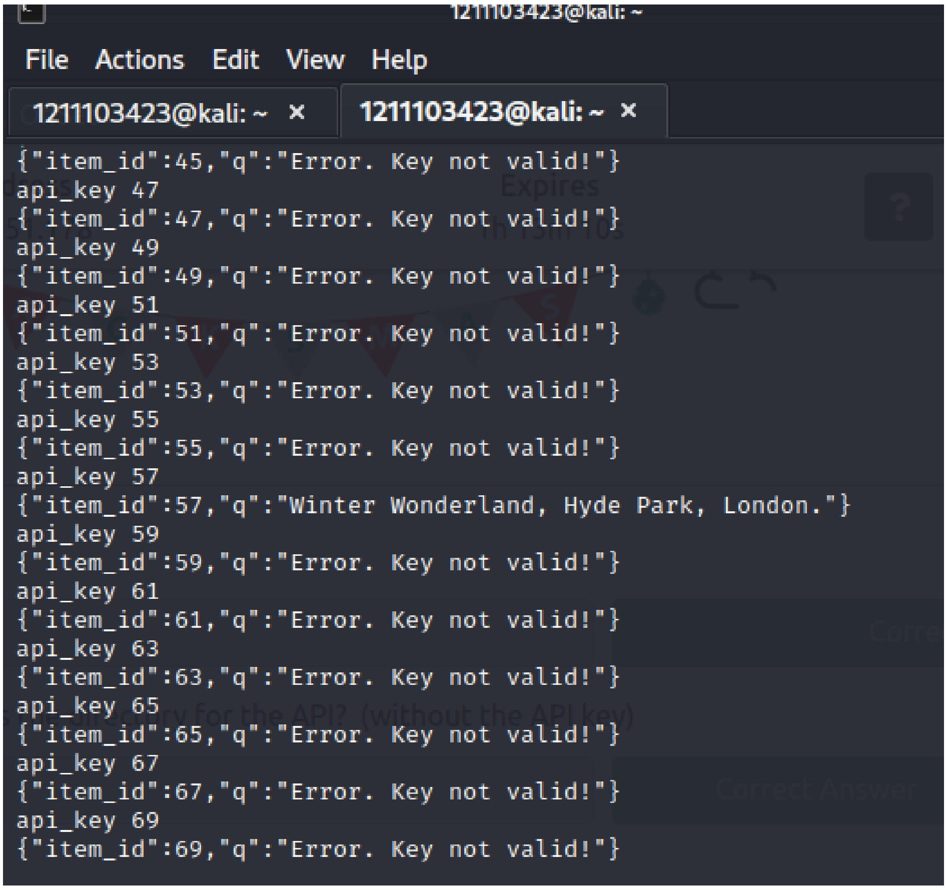
Question 3

We found the correct API key with using python



```
{"item_id":45,"q":"Error. Key not valid!"}
api_key 47
{"item_id":47,"q":"Error. Key not valid!"}
api_key 49
{"item_id":49,"q":"Error. Key not valid!"}
api_key 51
{"item_id":51,"q":"Error. Key not valid!"}
api_key 53
{"item_id":53,"q":"Error. Key not valid!"}
api_key 55
{"item_id":55,"q":"Error. Key not valid!"}
api_key 57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
api_key 59
{"item_id":59,"q":"Error. Key not valid!"}
api_key 61
{"item_id":61,"q":"Error. Key not valid!"}
api_key 63
{"item_id":63,"q":"Error. Key not valid!"}
api_key 65
{"item_id":65,"q":"Error. Key not valid!"}
api_key 67
{"item_id":67,"q":"Error. Key not valid!"}
api_key 69
{"item_id":69,"q":"Error. Key not valid!"}
```

Question 4



```
{"item_id":45,"q":"Error. Key not valid!"}
api_key 47
{"item_id":47,"q":"Error. Key not valid!"}
api_key 49
{"item_id":49,"q":"Error. Key not valid!"}
api_key 51
{"item_id":51,"q":"Error. Key not valid!"}
api_key 53
{"item_id":53,"q":"Error. Key not valid!"}
api_key 55
{"item_id":55,"q":"Error. Key not valid!"}
api_key 57
{"item_id":57,"q":"Winter Wonderland, Hyde Park, London."}
api_key 59
{"item_id":59,"q":"Error. Key not valid!"}
api_key 61
{"item_id":61,"q":"Error. Key not valid!"}
api_key 63
{"item_id":63,"q":"Error. Key not valid!"}
api_key 65
{"item_id":65,"q":"Error. Key not valid!"}
api_key 67
{"item_id":67,"q":"Error. Key not valid!"}
api_key 69
{"item_id":69,"q":"Error. Key not valid!"}
```

Thought Process/Methodology:

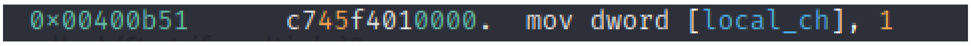
First thing first, we use nmap to scan the IP address and we get the port number of the IP Address. After that, we go to the web browser and search for “MACHINE_IP:port” using our IP address and the port number that we got before. Then we view the page source of the website to find the directory for the API. From what we learn on day 15, we use python to obtain the correct API key. Finally we are able to know the information about Santa.

Day17: Reverse Engineering - ReverseELFneering

Tools used: Kali Linux, Firefox

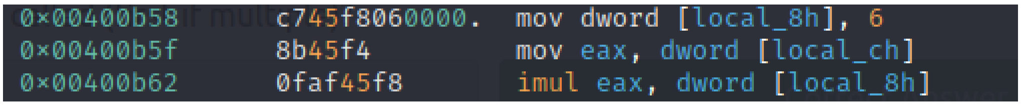
Solution/Walkthrough:

Question 1



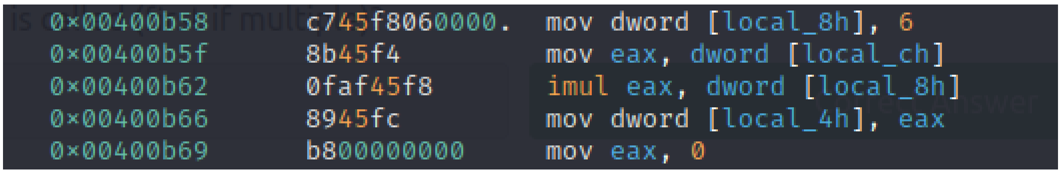
```
0x00400b51      c745f4010000.  mov dword [local_ch], 1
```

Question 2



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

Question 3



```
0x00400b58      c745f8060000.  mov dword [local_8h], 6
0x00400b5f      8b45f4         mov eax, dword [local_ch]
0x00400b62      0faf45f8       imul eax, dword [local_8h]
0x00400b66      8945fc         mov dword [local_4h], eax
0x00400b69      b800000000     mov eax, 0
```

Thought Process/Methodology:

In order to run the programme in debugging mode with radare2, we must SSH to the target IP address . Following that, we use the aa command to instruct radare2 to analyse the programme and the afl instruction to provide a list of functions. The next step is finding the main function in the list and using the command pdf @main to examine the assembly code inside the main function. A breakpoint was set before the instructions were carried out to enable us to see the program's state at a certain point. Run dc command to execute the program until breakpoint, and px @memory-address command to view the contents in the variables.After that, we run the ds command to carry out the instruction we are now on and go on to the next one. The ds command lets us insert a value into the specified variable for the Day 17 task. To see the register variable and ensure that the values are accurate, we may also use the dr command.

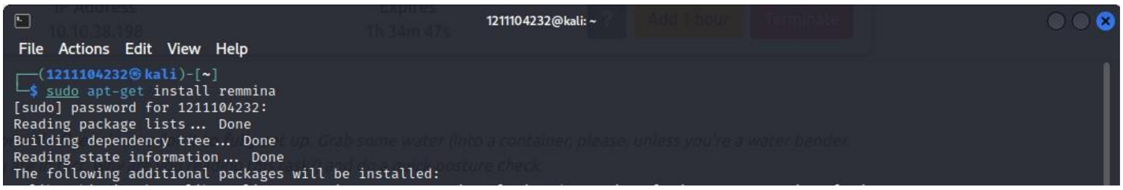
Day18: Reverse Engineering - The Bits of Christmas

Tools used: Kali Linux, Firefox, Remmina

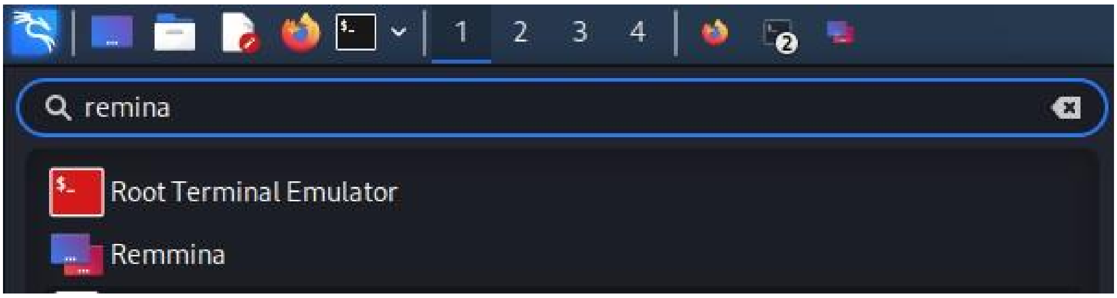
Solution/Walkthrough:

Question 1

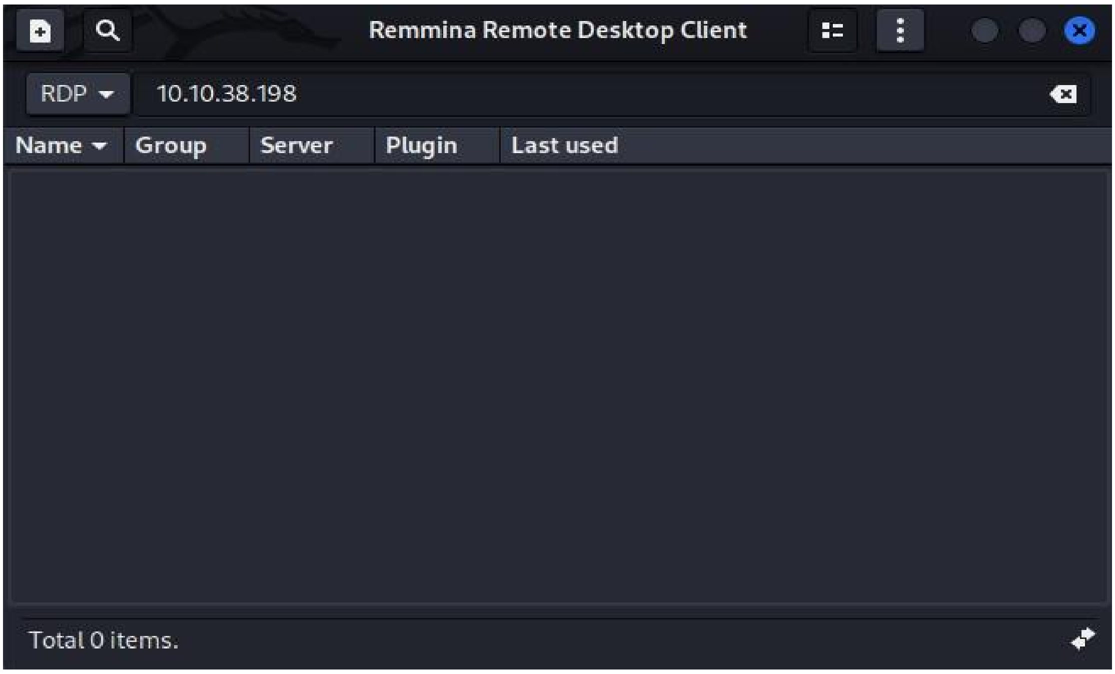
We installed Remmina by using this command: *sudo apt install remmina*



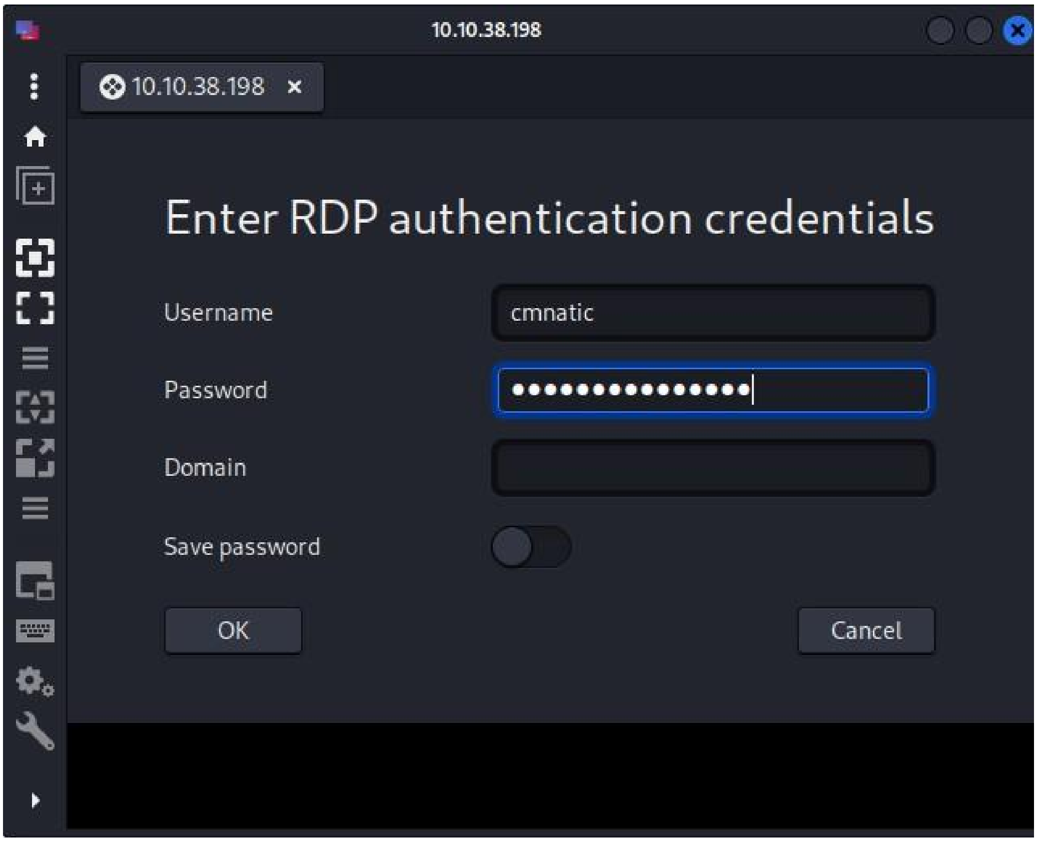
```
┌──(1211104232㉿kali)-[~]
└─$ sudo apt-get install remmina
[sudo] password for 1211104232:
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following additional packages will be installed:
```



We entered Remmina and inputted the following IP address and hit enter.



After accepting the certificate,we entered the username of *cmnatic* and the password of *Adventofcyber!*



Enter RDP authentication credentials

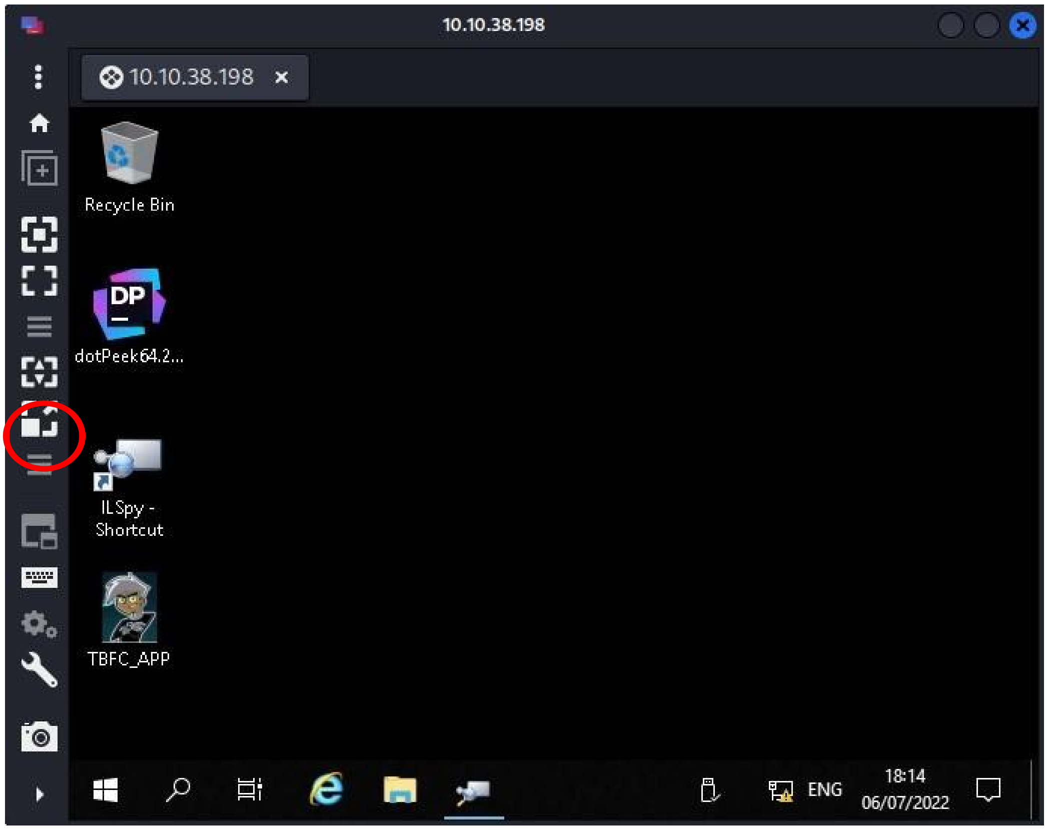
Username: cmnatic

Password: ●●●●●●●●●●●●●●●

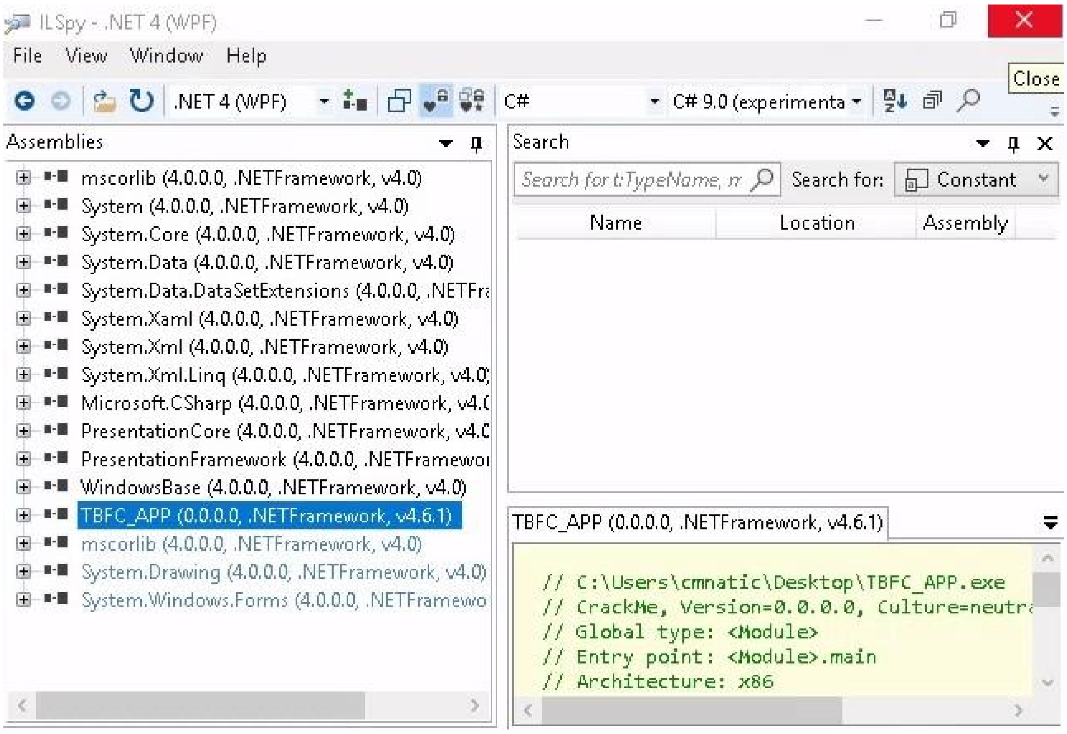
Domain:

Save password: ○

We toggled that following button on the left sidebar to make resolution better



We opened the TBFC_APP in ILSpy. Open the ILSpy – Shortcut and then drag the TBFC_APP into the ILSPY Window. Hence, we got this view below after we did that.



Search for t:TypeName, n

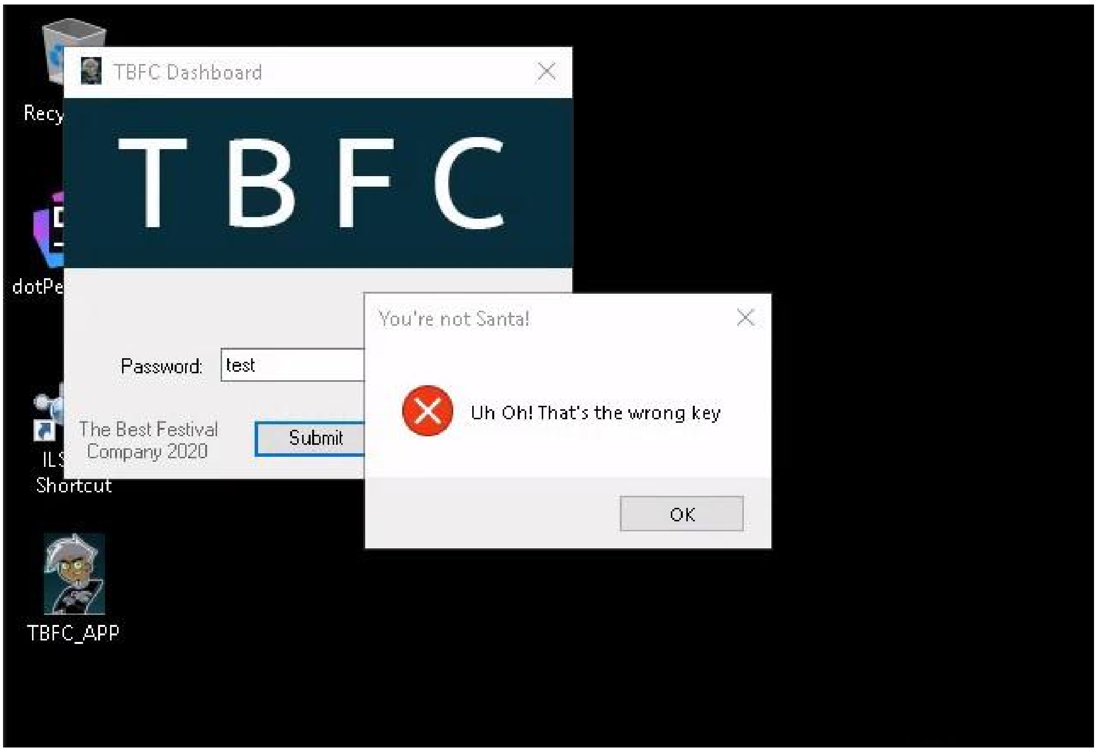
Search for: Constant

- 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.Data (4.0.0.0, .NETFramework, v4.0)
- System.Data.DataSetExtensions (4.0.0.0, .NETFr
- System.Xaml (4.0.0.0, .NETFramework, v4.0)
- System.Xml (4.0.0.0, .NETFramework, v4.0)
- System.Xml.Linq (4.0.0.0, .NETFramework, v4.0)
- Microsoft.CSharp (4.0.0.0, .NETFramework, v4.(
- PresentationCore (4.0.0.0, .NETFramework, v4.C
- PresentationFramework (4.0.0.0, .NETFramewo
- WindowsBase (4.0.0.0, .NETFramework, v4.0)
- TBFC_APP (0.0.0.0, .NETFramework, v4.6.1)
- mscorlib (4.0.0.0, .NETFramework, v4.0)
- System.Drawing (4.0.0.0, .NETFramework, v4.0)
- System.Windows.Forms (4.0.0.0, .NETFramewo

TBFC_APP (0.0.0.0, .NETFramework, v4.6.1)

```
// C:\Users\cmnatic\Desktop\TBFC_APP.exe
// CrackMe, Version=0.0.0.0, Culture=neutr
// Global type: <Module>
// Entry point: <Module>.main
// Architecture: x86
```

We opened the TBFC_APP and we tried entering the password as a test.



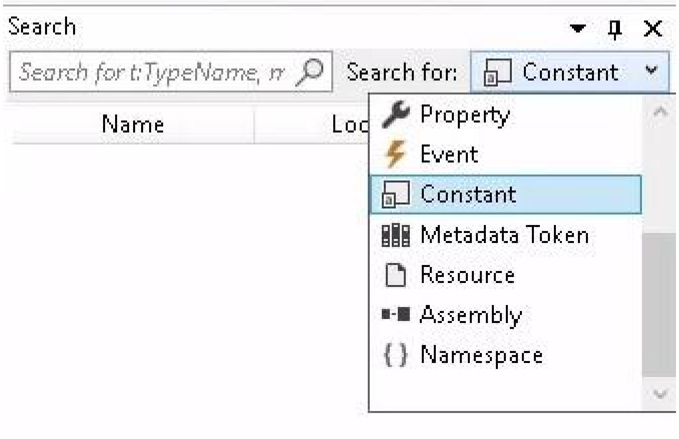
Password: test

The Best Festival Company 2020

You're not Santa!

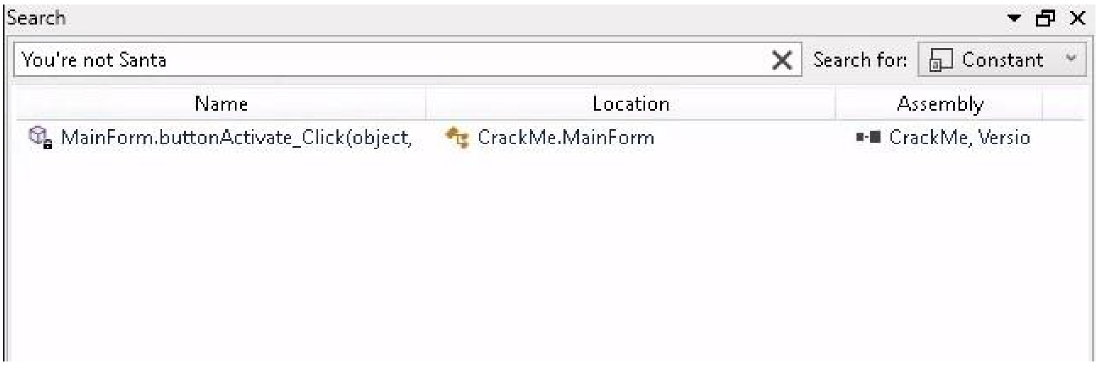
Uh Oh! That's the wrong key

Went to the ILSPY window again and changed what we were searching for as shown below, to constant.



Search for: Constant

We used this error message to search for the correct password. We used *You’re not Santa* which was at the top of the error message.

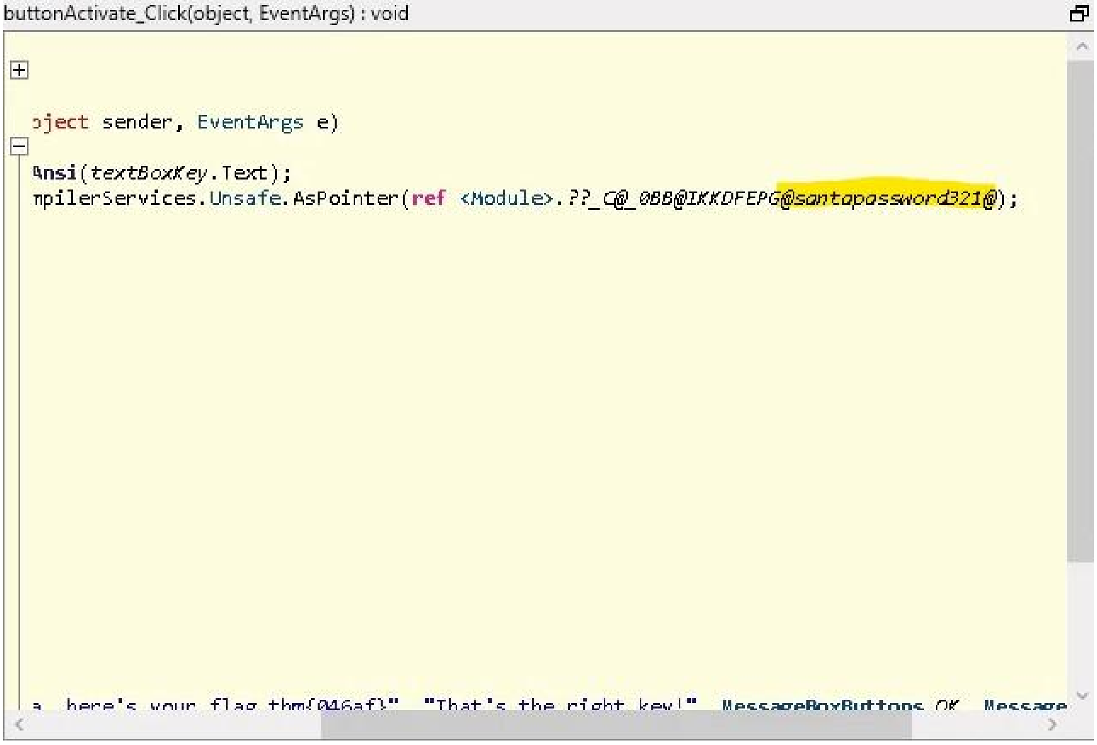


You're not Santa

Search for: Constant

Name	Location	Assembly
MainForm.buttonActivate_Click(object,	CrackMe.MainForm	CrackMe, Versio

We double clicked on the MainForm and look at the code and found the password; ***santapasword321***

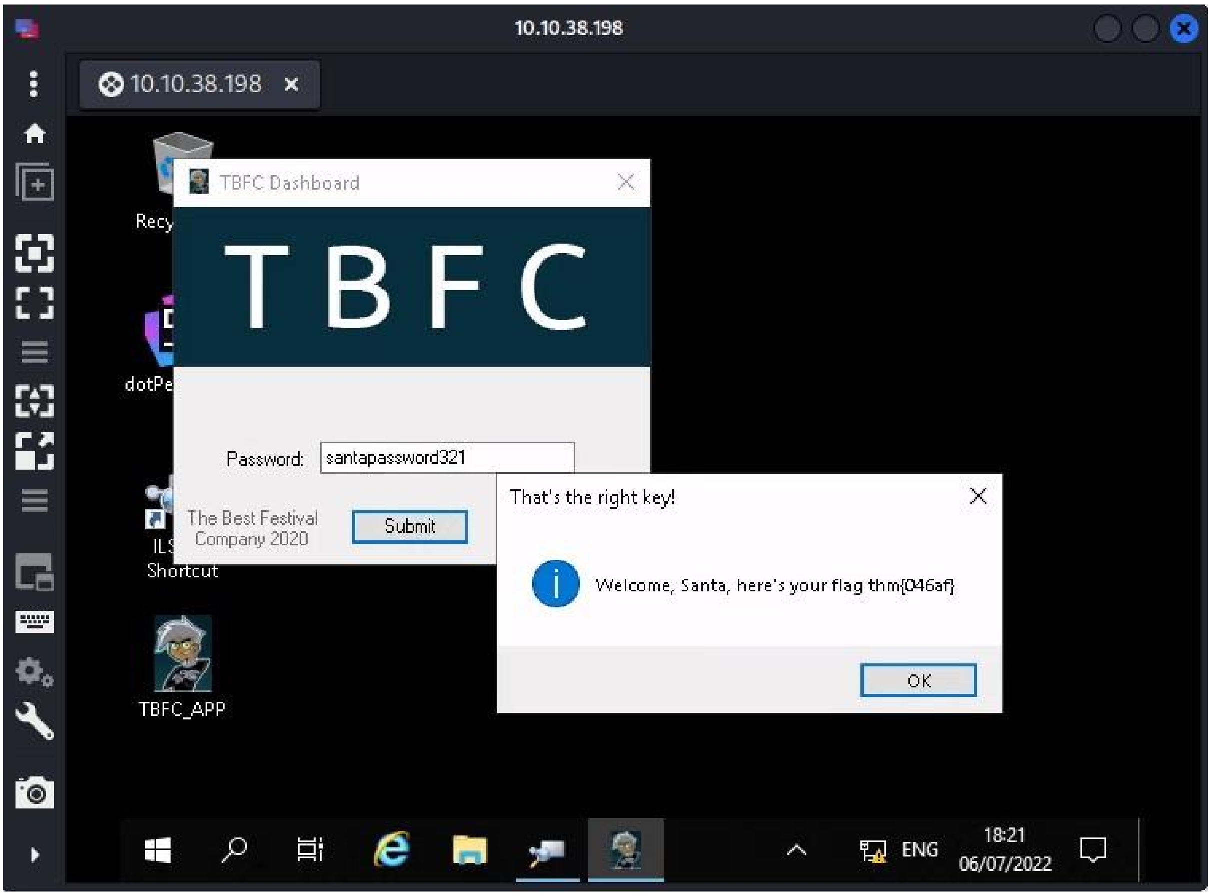


buttonActivate_Click(object, EventArgs) : void

```
ɔject sender, EventArgs e)

Ansi(textBoxKey.Text);
mpilerServices.Unsafe.AsPointer(ref <Module>.??_C@_0BB@IKKDFEPG@santapassword321@);

a, here's your flag thm{046af}", "That's the right key!", MessageBoxButtons.OK, Message
```

Question 2

After entering the password, we managed to get the flag too which was ***thm{046af}***



Password: santapassword321

That's the right key!

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

Thought Process/Methodology:

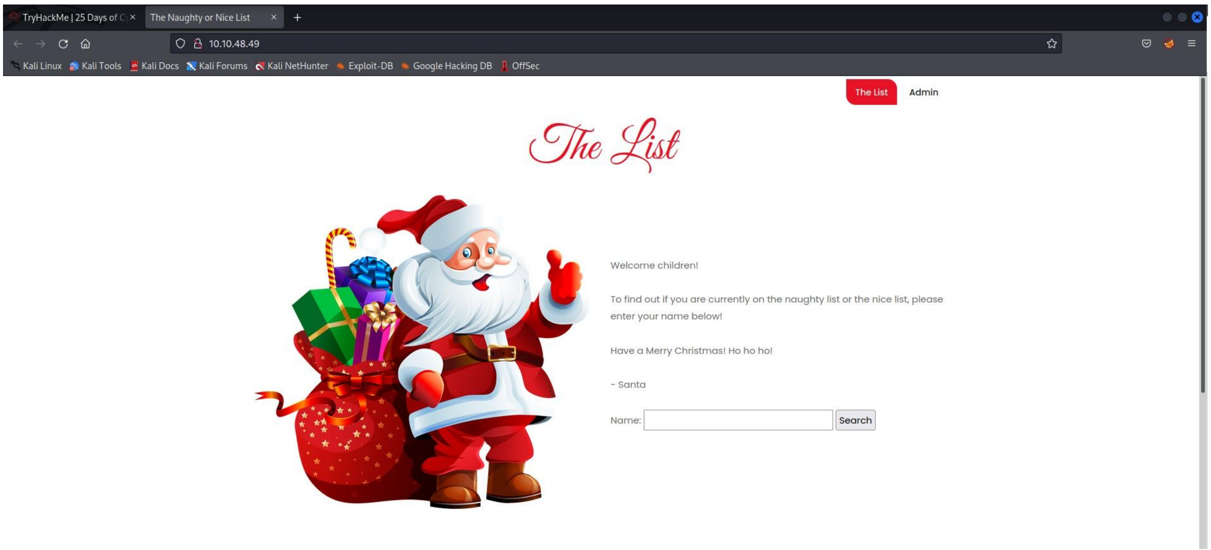
Firstly, we installed Remmina by using this command "*sudo apt install remmina".* We entered Remmina and inputted our IP address and hit enter. After accepting the certificate,we entered the username of *cmnatic* and the password of *Adventofcyber!* given. We toggled the *Toggle Dynamic Resolution Update* button on the left sidebar to make resolution better. We opened the TBFC_APP in ILSpy. We opened the ILSpy – Shortcut and then dragged the TBFC_APP into the ILSPY Window. We opened the TBFC_APP and we tried entering the password as a test. Went to the ILSPY window again and changed what we were searching for to "constant". We used this error message to search for the correct password. We used *You're not Santa* which was at the top of the error message. We double clicked on the MainForm and looked at the code and found the password "***santapasword321****".* After entering the password, we managed to get the flag too which was ***thm{046af}.***

<u>Day19: Web Exploitation - The Naughty or Nice List</u>

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

We navigated to its IP address in our address bar and it led us to this page below.



TryHackMe | 25 Days of C
The Naughty or Nice List
10.10.48.49
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

The List Admin

The List

Welcome children!

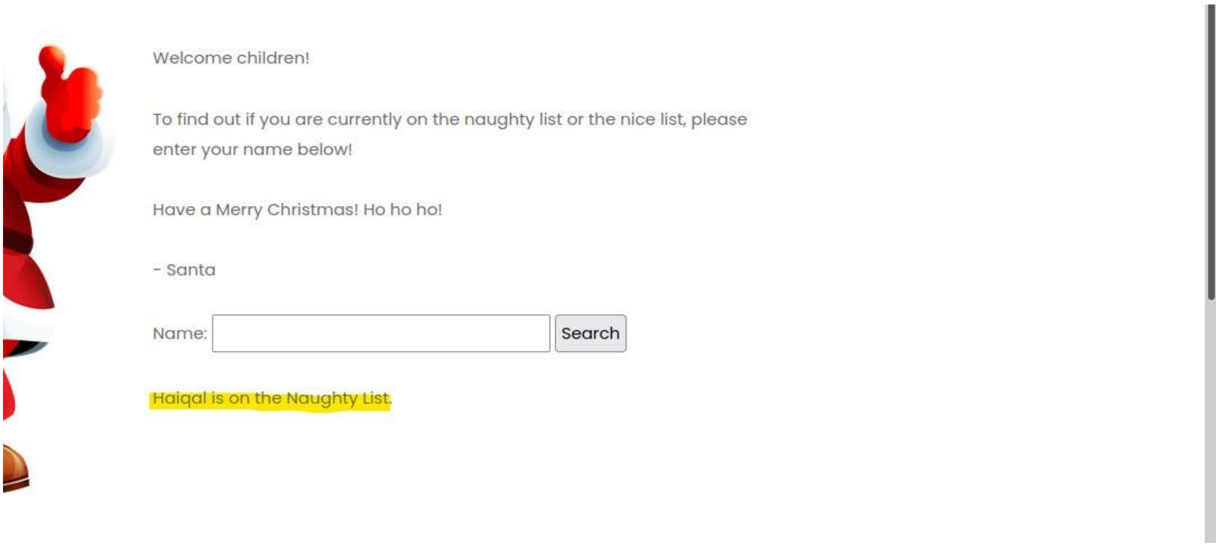
To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name: Search

I searched for a name and saw that Haiqal was on the naughty list.



Welcome children!

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

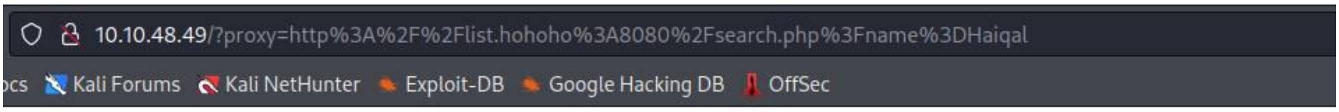
Have a Merry Christmas! Ho ho ho!

- Santa

Name: Search

Haiqal is on the Naughty List.

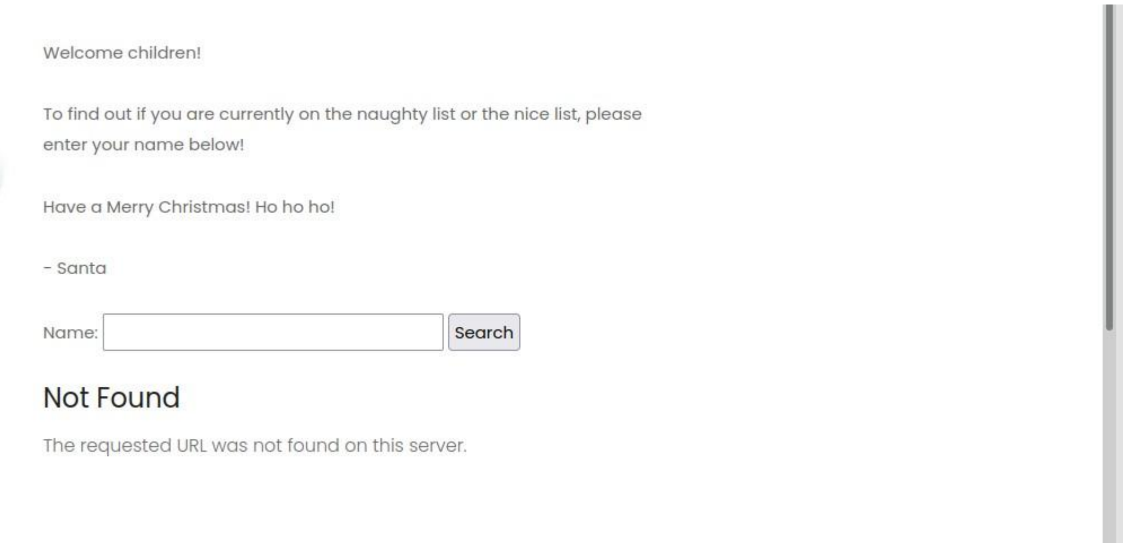
We see that there is a proxy parameter that shown below and can use to perform SRRF attack by changing it to localhost



```
10.10.48.49/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DHaiqal
```

ocs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Unfortunately, our request had been blocked



Welcome children!

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

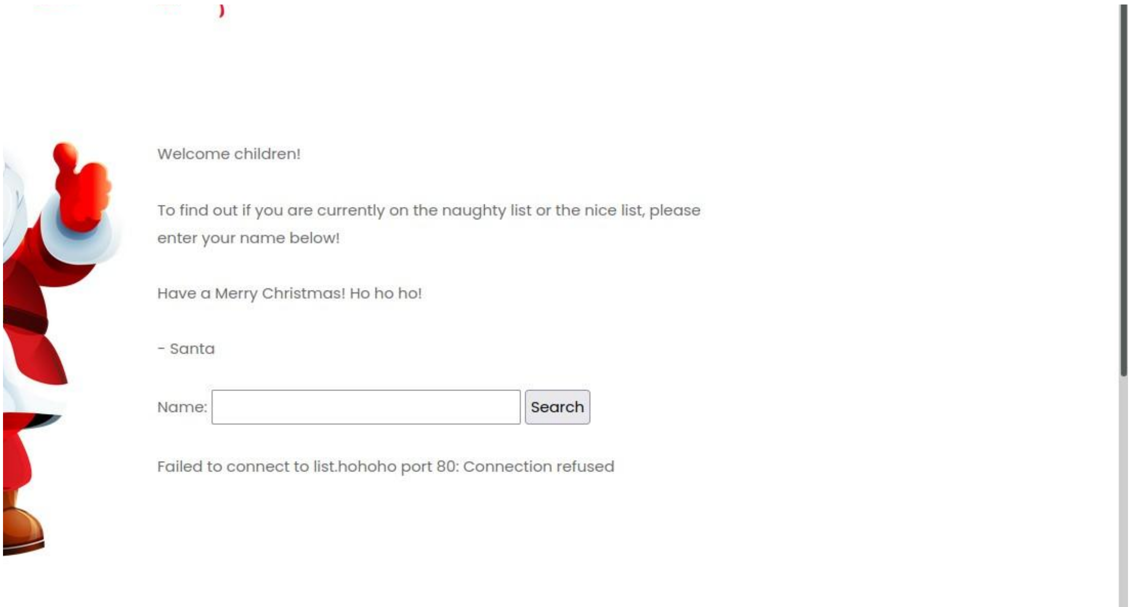
Have a Merry Christmas! Ho ho ho!

- Santa

Not Found

The requested URL was not found on this server.

After a few experiments, it seems that the only domain available is *list.hohoho*



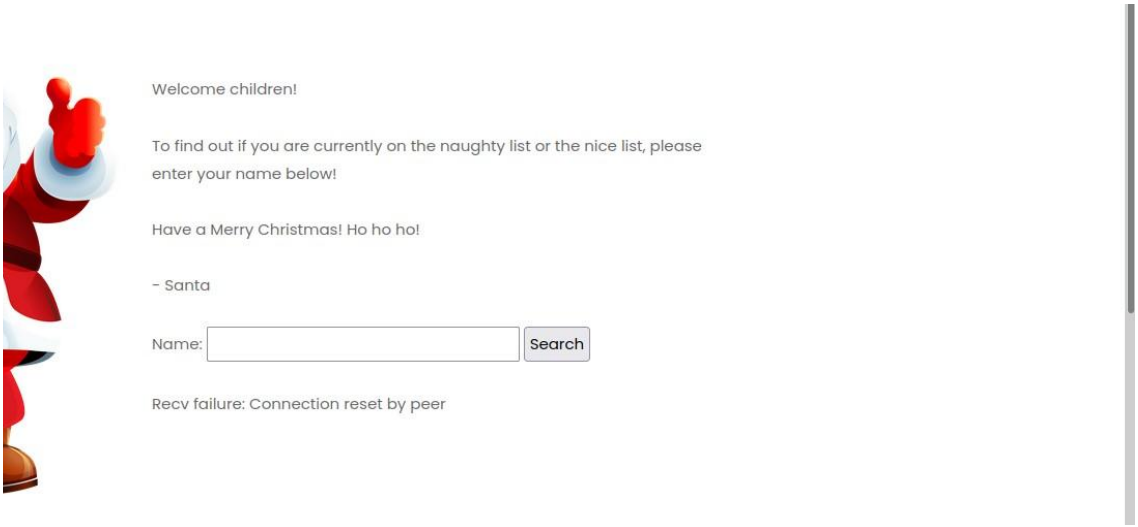
Welcome children!

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

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



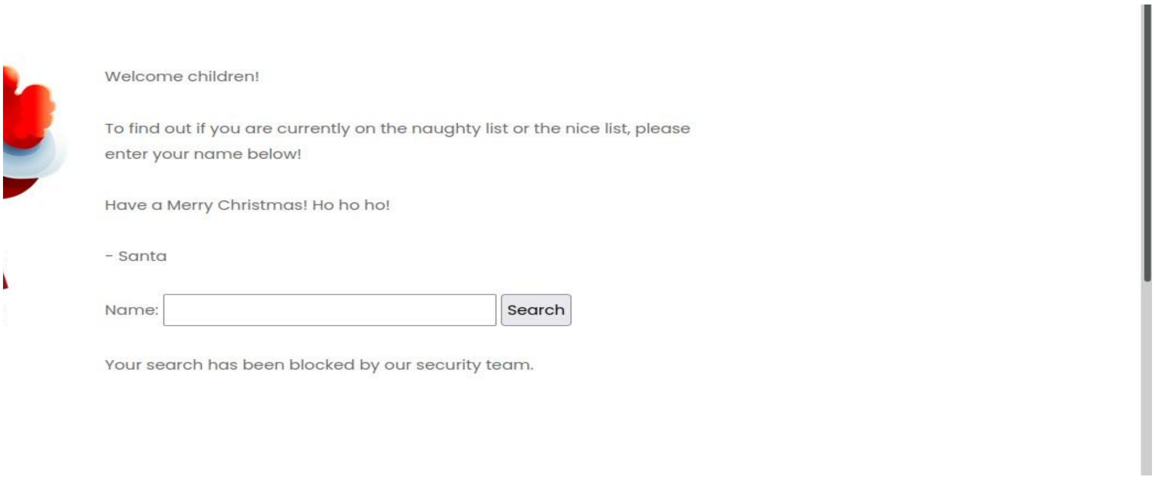
Welcome children!

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

Recv failure: Connection reset by peer



Welcome children!

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

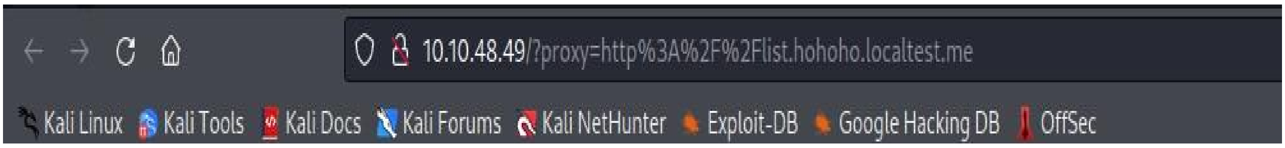
Have a Merry Christmas! Ho ho ho!

- Santa

Your search has been blocked by our security team.

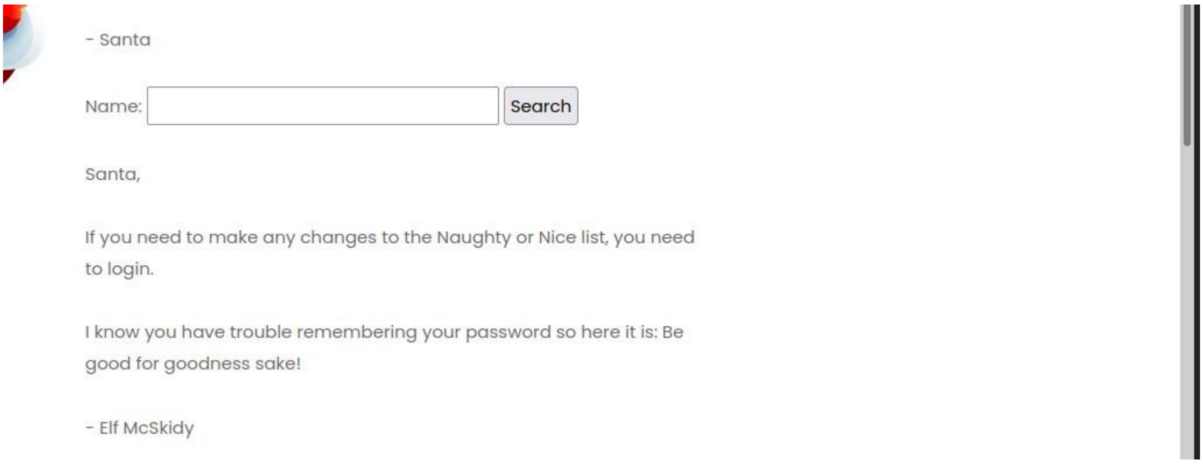
Question 1

We tried the subdomain called *localhost.me* in this challenge and added that to our request.



10.10.48.49/?proxy=http%3A%2F%2Flist.hohoho.localtest.me

We successfully obtained the message from Elf McSkidy from this URL which contained a password to log into the admin. The password was “**Be good for goodness sake!**”



- Santa

Santa,

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

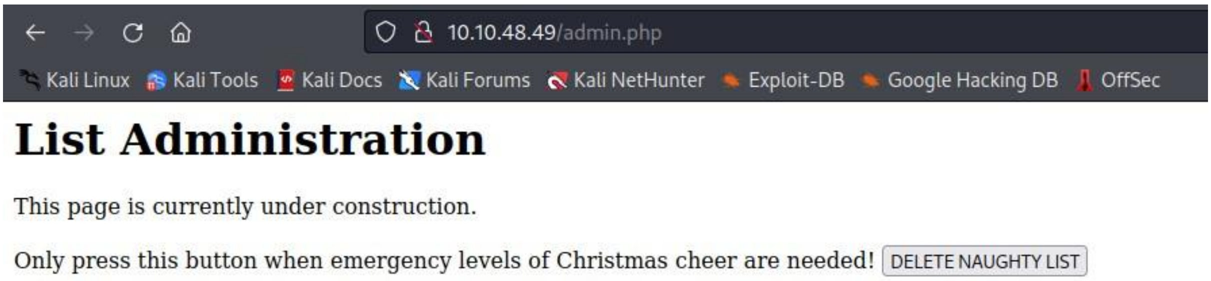
I know you have trouble remembering your password so here it is: Be good for goodness sake!

- Elf McSkidy

We logged into the admin by using Santa as a username and “Be good for goodness sake!” as the password.

Question 2

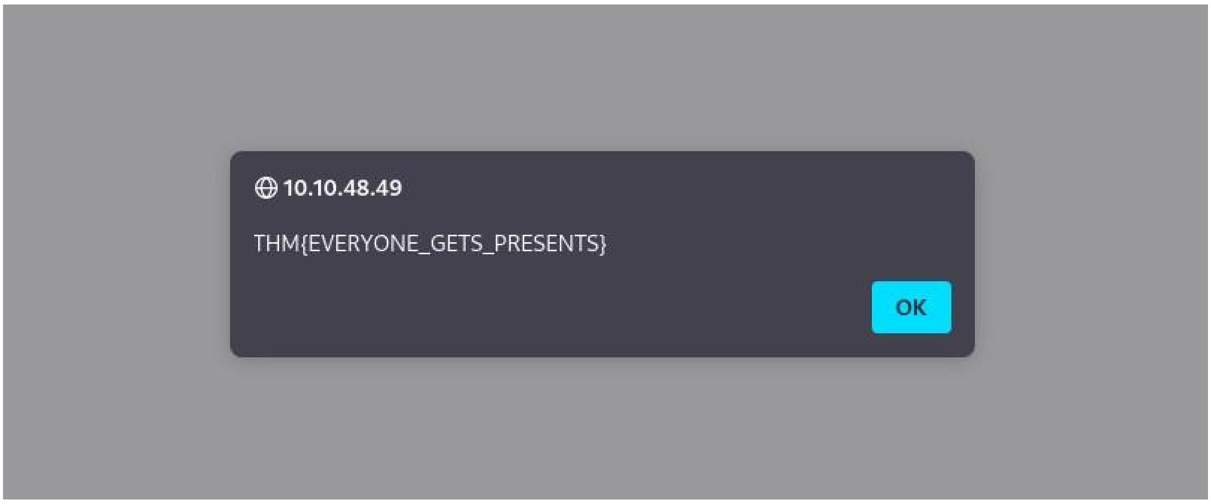
We deleted the naughty list and the flag appeared as **THM{EVERYONE_GETS_PRESENTS}**



List Administration

This page is currently under construction.

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



10.10.48.49

THM{EVERYONE_GETS_PRESENTS}

Thought Process/Methodology:

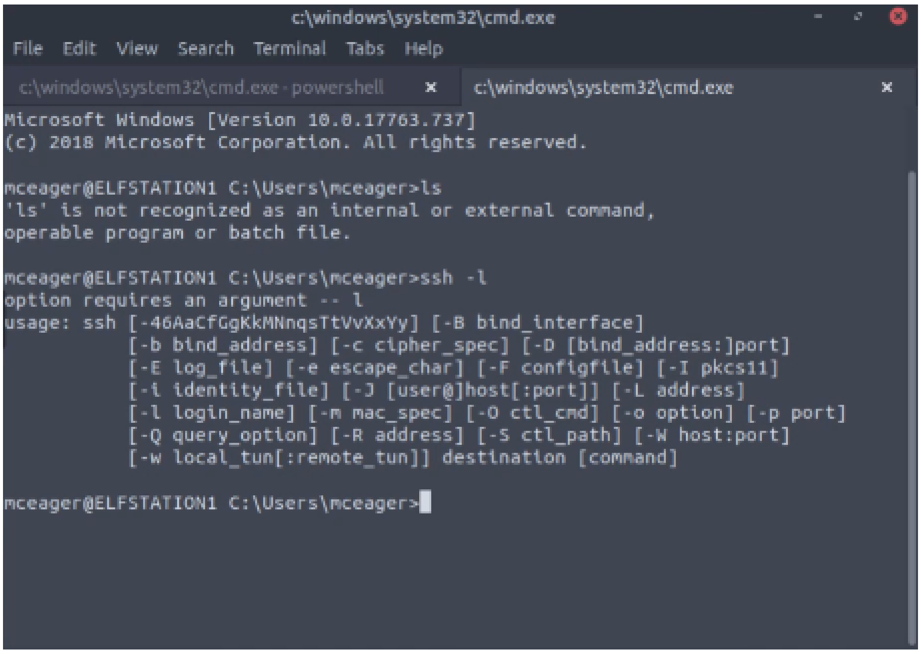
Firstly, We navigated to the IP address given in our address bar and it led us to the home page which let us enter a name and check if that person is on the Naughty or Nice list. We tried our names and we saw that there was a proxy parameter that can be used to perform an SRRF attack by changing it to *localhost*. Unfortunately, our request had been blocked when we used that. After a few experiments, it seems that the only domain available is *list.hohoho.* Then, we proceeded to try the subdomain called localhost.me in this challenge and added that to our request. We successfully obtained the message from Elf McSkidy from this URL which contained a password to log into the admin. The password was "**Be good for goodness sake!**". It took us a couple tries to guess the username, but we eventually were able to login using the username Santa and the password Be good for goodness sake! After that, we were on a page where we could delete the naughty list. We deleted the naughty list and found the flag **THM{EVERYONE_GETS_PRESENTS}** appeared.

Day20: Blue Teaming - PowershELIF to the rescue

Tools used: Kali Linux

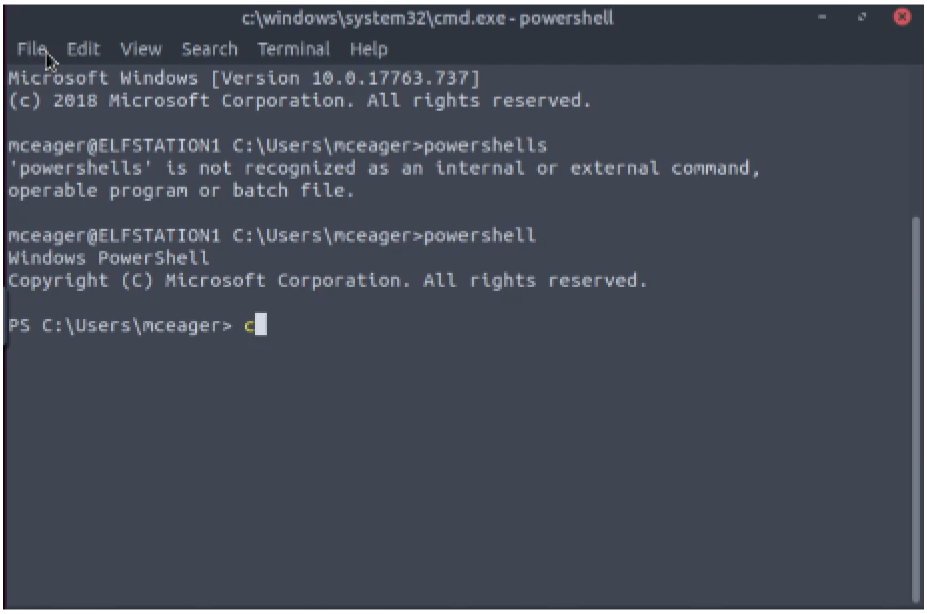
Solution/Walkthrough:

Question 1

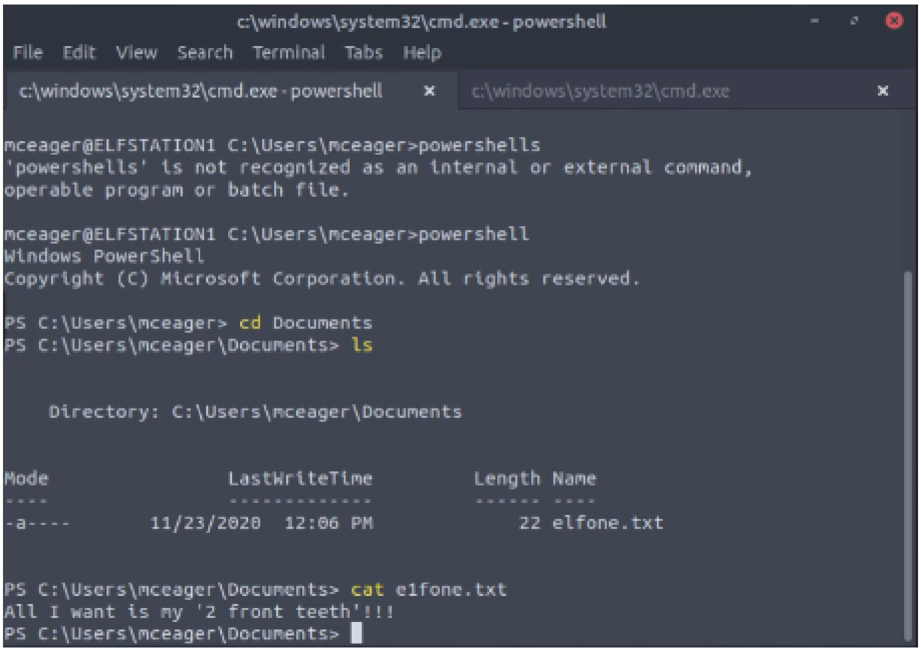

c:\windows\system32\cmd.exe
File Edit View Search Terminal Tabs Help
c:\windows\system32\cmd.exe - powershell
c:\windows\system32\cmd.exe

```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

mceager@ELFSTATION1 C:\Users\mceager>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

mceager@ELFSTATION1 C:\Users\mceager>ssh -l
option requires an argument -- l
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command]

mceager@ELFSTATION1 C:\Users\mceager>
```

Question 2

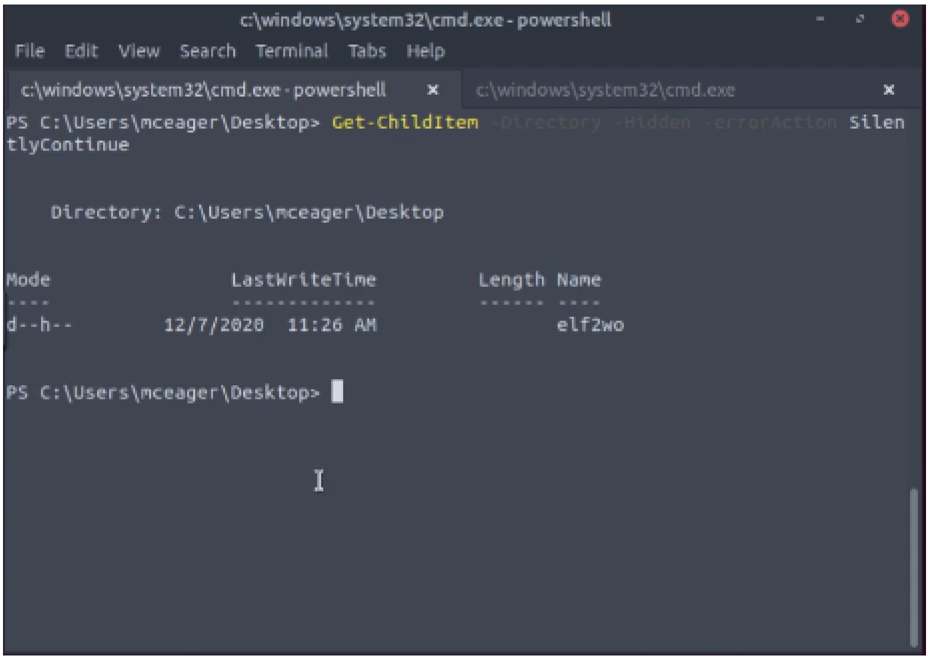


```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

mceager@ELFSTATION1 C:\Users\mceager>powershells
'powershells' is not recognized as an internal or external command,
operable program or batch file.

mceager@ELFSTATION1 C:\Users\mceager>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\mceager> c
```


c:\windows\system32\cmd.exe - powershell
File
Edit
View
Search
Terminal
Tabs
Help
c:\windows\system32\cmd.exe - powershell
c:\windows\system32\cmd.exe

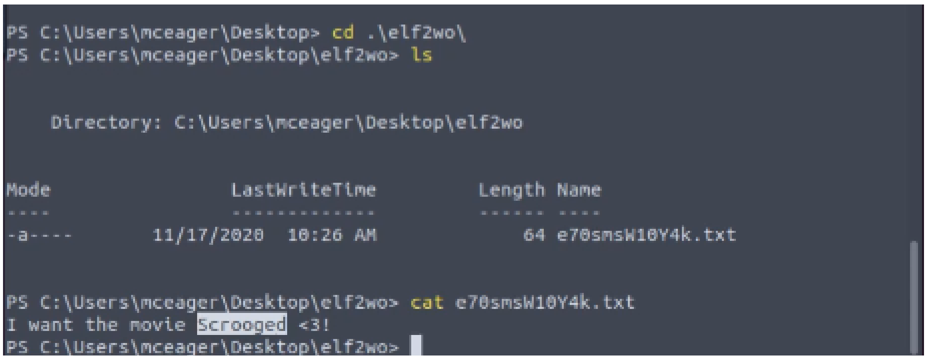
```
mceager@ELFSTATION1 C:\Users\mceager>powershells
'powershells' is not recognized as an internal or external command,
operable program or batch file.

mceager@ELFSTATION1 C:\Users\mceager>powershell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\mceager> cd Documents
PS C:\Users\mceager\Documents> ls


    Directory: C:\Users\mceager\Documents


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----       11/23/2020  12:06 PM             22 elfone.txt


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

Question 3



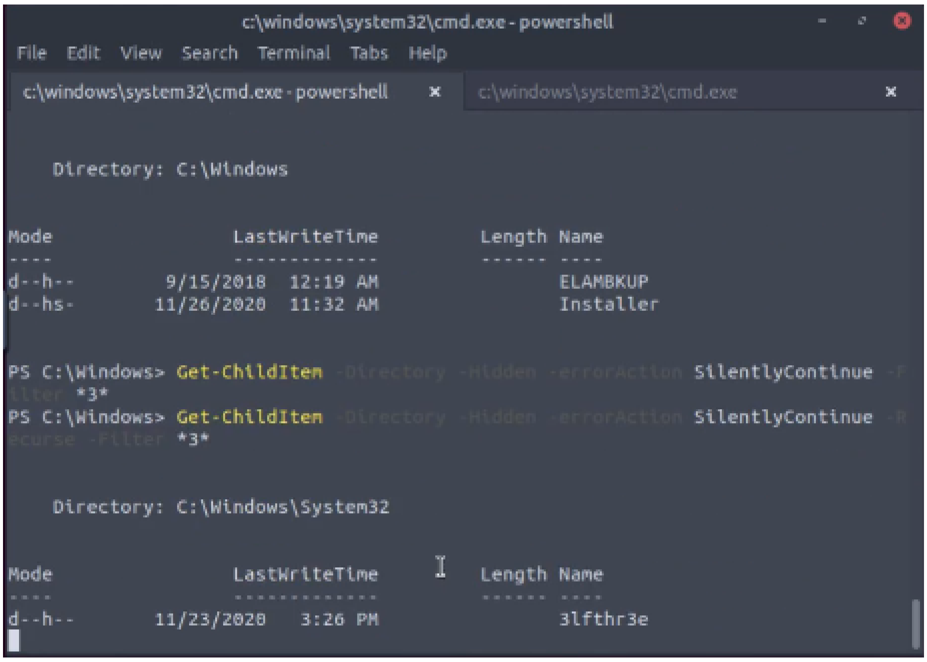
c:\windows\system32\cmd.exe - powershell
File Edit View Search Terminal Tabs Help
c:\windows\system32\cmd.exe - powershell
c:\windows\system32\cmd.exe

```
PS C:\Users\mceager\Desktop> Get-ChildItem -Directory -Hidden -errorAction Silen
tlyContinue


    Directory: C:\Users\mceager\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d--h--        12/7/2020  11:26 AM                elf2wo


PS C:\Users\mceager\Desktop>
```



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


    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>
```

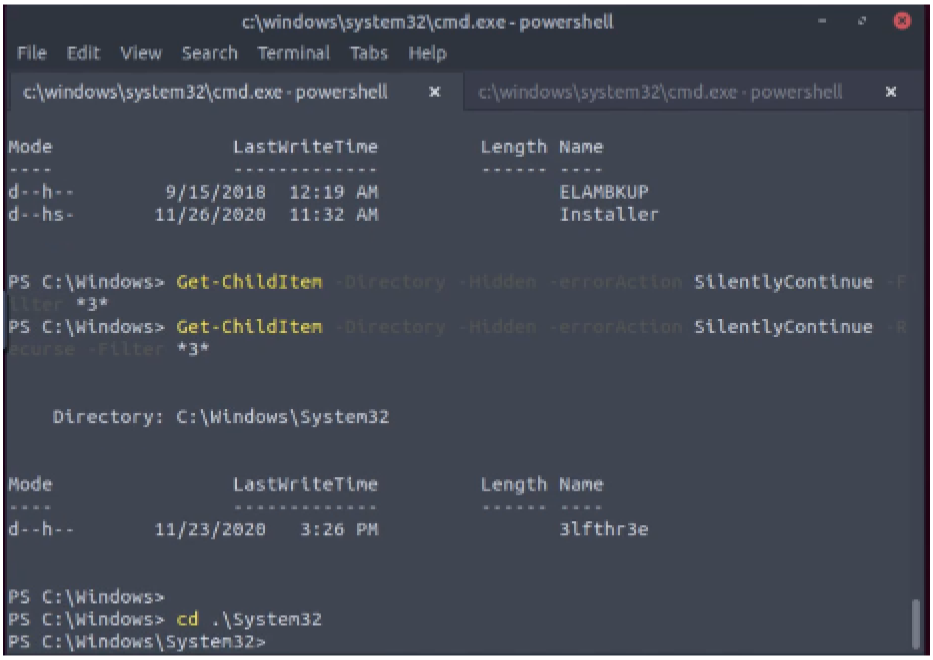
Question 4



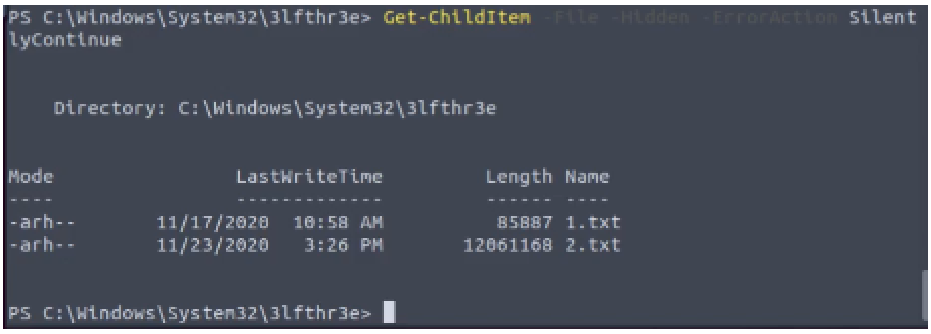
c:\windows\system32\cmd.exe - powershell
File Edit View Search Terminal Tabs Help
c:\windows\system32\cmd.exe - powershell
c:\windows\system32\cmd.exe

```
    Directory: C:\Windows


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d--h--        9/15/2018  12:19 AM                ELAMBKUP
d--hs-       11/26/2020  11:32 AM                Installer


PS C:\Windows> Get-ChildItem -Directory -Hidden -errorAction SilentlyContinue -F
ilter *3*
PS C:\Windows> Get-ChildItem -Directory -Hidden -errorAction SilentlyContinue -R
ecurse -Filter *3*


    Directory: C:\Windows\System32


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

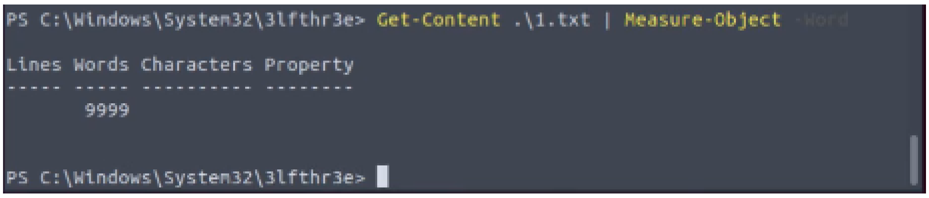
Question 5


c:\windows\system32\cmd.exe - powershell
File Edit View Search Terminal Tabs Help
c:\windows\system32\cmd.exe - powershell
c:\windows\system32\cmd.exe - powershell

```
Mode                LastWriteTime         Length Name
----                -------------         ------ ----
d--h--         9/15/2018  12:19 AM               ELAMBKUP
d--hs-        11/26/2020  11:32 AM               Installer


PS C:\Windows> Get-ChildItem -Directory -Hidden -errorAction SilentlyContinue -F
ilter *3*
PS C:\Windows> Get-ChildItem -Directory -Hidden -errorAction SilentlyContinue -R
ecurse -Filter *3*


    Directory: C:\Windows\System32


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


PS C:\Windows>
PS C:\Windows> cd .\System32
PS C:\Windows\System32>
```

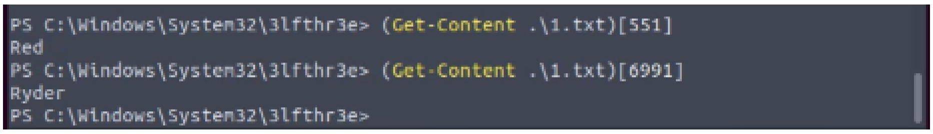


```
PS C:\Windows\System32\3lfthr3e> Get-ChildItem -File -Hidden -ErrorAction Silent
lyContinue


    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>
```



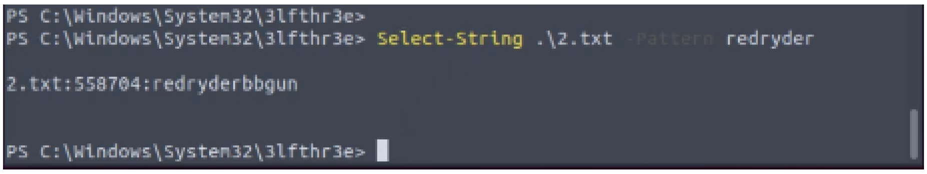
```
PS C:\Windows\System32\3lfthr3e> Get-Content .\1.txt | Measure-Object -Word

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


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

Question 6



```
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 7



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

2.txt:558704:redryderbbgun


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

Thought Process/Methodology:

First, we launch a terminal and enter our IP address to connect to the host. To start it, we navigate to PowerShell. We go to the Documents directory. Following that, we enter the directory to view all contents. One of the files listed there is called "e1fone.txt." We use the cat command to read the file and display the results. Next, we use the "Get-ChildItem -Directory -Hidden -ErrorAction SilentlyContinue" command to search 'elf2wo. Enter the "elf2wo" directory and list the directories there. It has a file named "e70smsW10Y4k.txt." To display the output, we use the cat command. Next, we go to Windows and run the "Get-ChildItem -Directory -Hidden -ErrorAction SilentlyContinue -Filter *3*" command, which lists "3lfthr3e". We enter the directory "3lfthr3e" and list the file there. It contains two files. Using the 'Measure-Object -Word' command, which displayed the words in the first file. Then we use the '(Get-Content.1.txt)[551]' and '(Get-Content.1.txt)[6991]' commands to see the words. Next, we use the 'Select-String -Pattern redryder' command to display the output.