PSP0201 Weekly Writeup

Week 5

Group Name: Metamorphosis

ID	Name	Role
1211101704	Aniq Danial Bin Mohd Adli	Leader
1211101790	Lee Heng Yep	Member
1211102806	Ong Kwang Zheng	Member
1211103063	Ng Weng Lam	Member

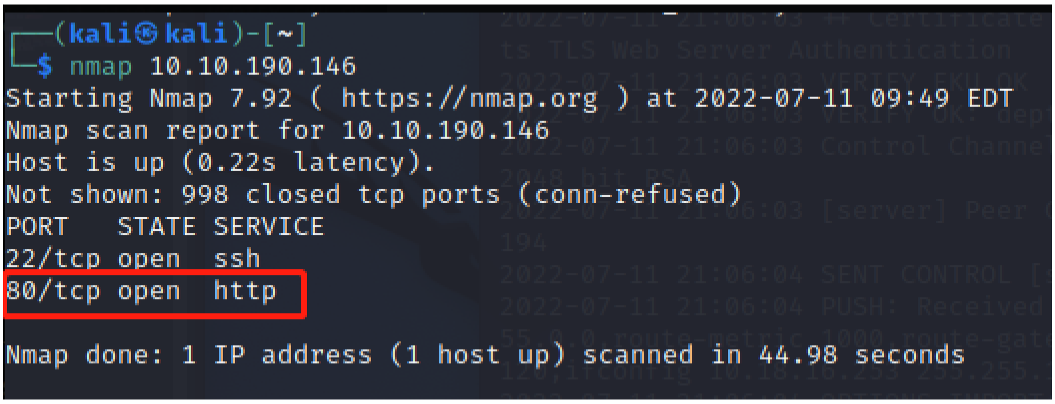
<u>Day 16: Help! Where is Santa? (Scripting)</u>

Tools used: Kali Linux, Python, Sublime Editor, Nmap

Solution/Walkthrough:

<u>Question 1:</u>

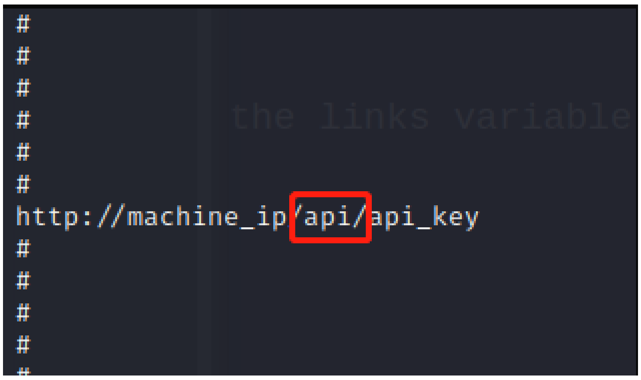
The port number for the web server is **80**



```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.190.146
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-11 09:49 EDT
Nmap scan report for 10.10.190.146
Host is up (0.22s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 44.98 seconds
```

<u>Question 2:</u>

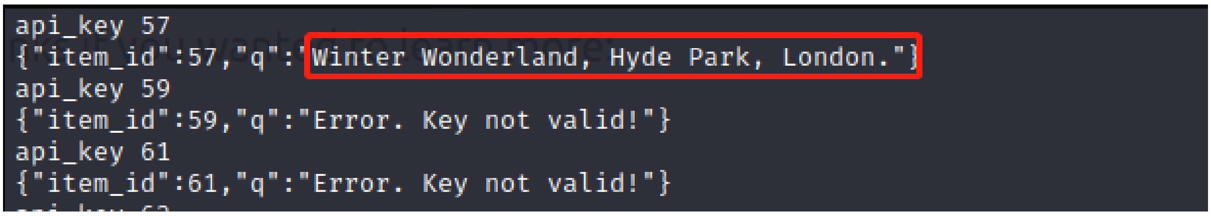
/api/



```
#
#
#
#
#
#
http://machine_ip/api/api_key
#
#
#
#
```

<u>Question 3:</u>

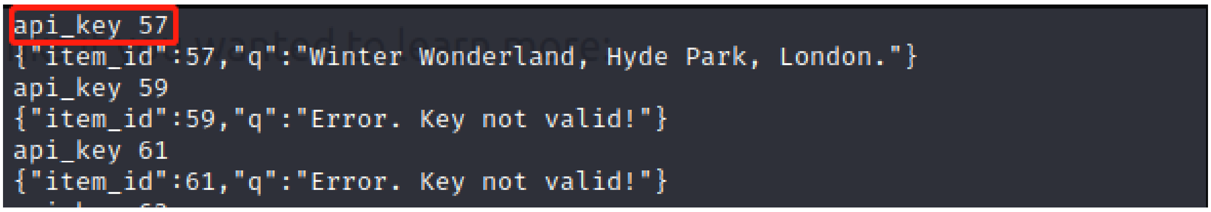
Winter Wonderland,Hyde Park,London



```
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!"}
```

Question 4:

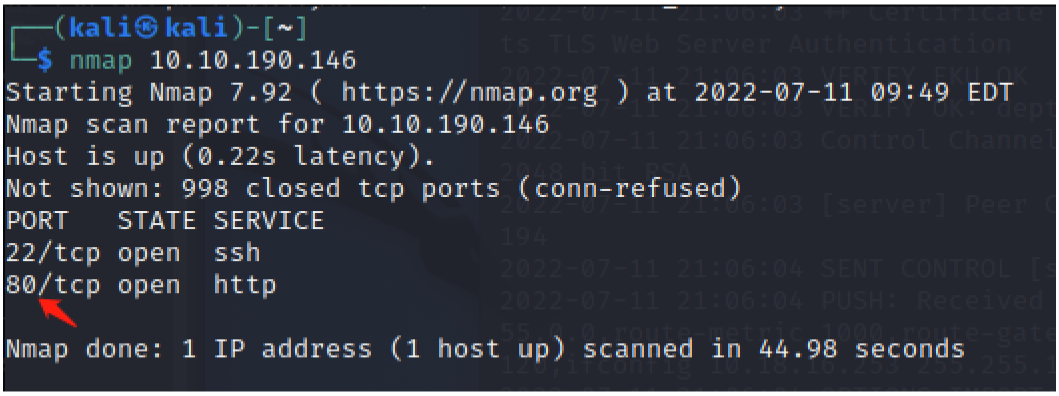
57



```
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!"}
```

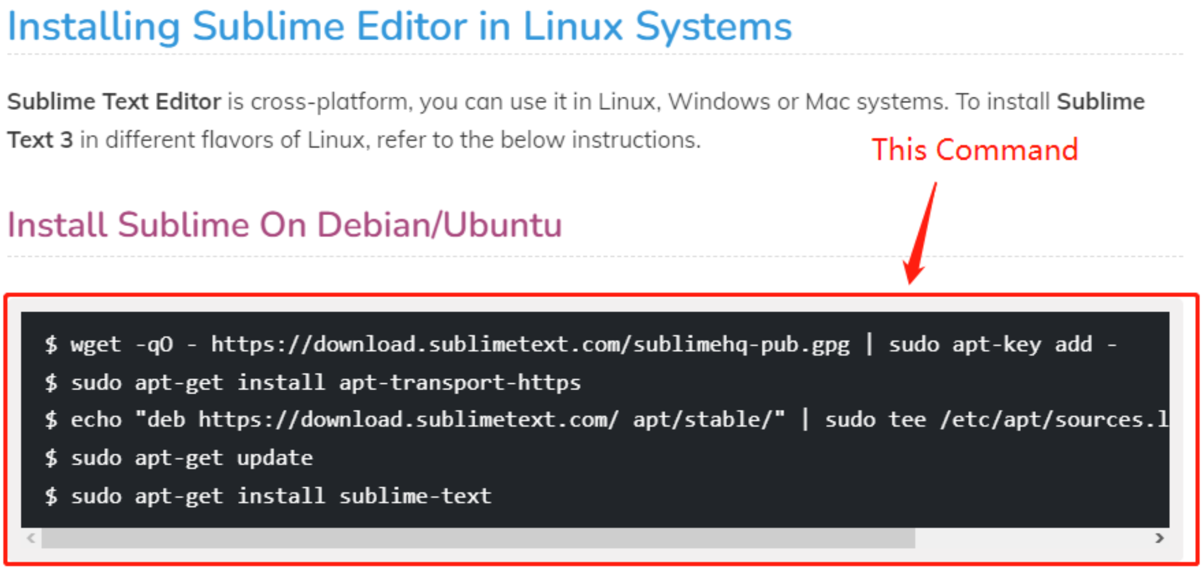
Thought Process/Methodology:

To solve the challenge we are facing, we start it by running the command nmap <MACHINE_IP> and this will appear.



```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.190.146
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-11 09:49 EDT
Nmap scan report for 10.10.190.146
Host is up (0.22s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 44.98 seconds
```

To proceed, we have to install something called **sublime editor** since we are using Kali Linux through the link https://www.tecmint.com/sublime-text-editor-for-linux/.



Installing Sublime Editor in Linux Systems

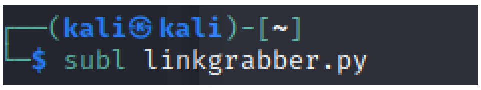
Sublime Text Editor is cross-platform, you can use it in Linux, Windows or Mac systems. To install **Sublime Text 3** in different flavors of Linux, refer to the below instructions.

This Command

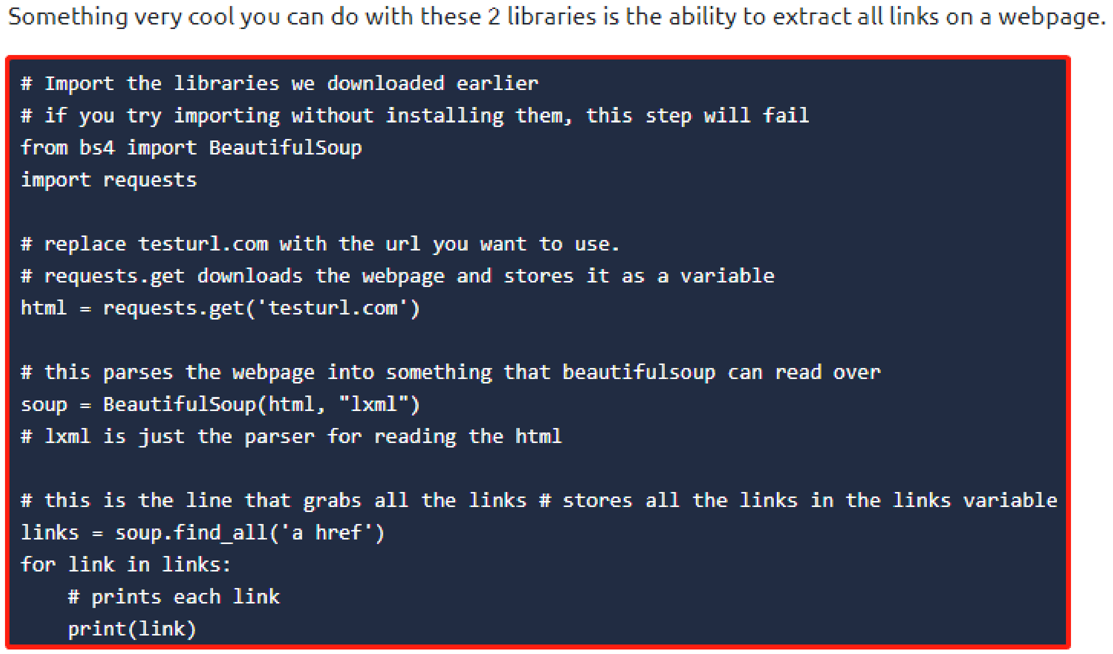
Install Sublime On Debian/Ubuntu

```
$ wget -qO - https://download.sublimetext.com/sublimehq-pub.gpg | sudo apt-key add -
$ sudo apt-get install apt-transport-https
$ echo "deb https://download.sublimetext.com/ apt/stable/" | sudo tee /etc/apt/sources.l
$ sudo apt-get update
$ sudo apt-get install sublime-text
```

Run the command subl linkgrabber.py and a text file will be opened so we can paste the script that has been mentioned on the previous day into the text file.



```
┌──(kali㉿kali)-[~]
└─$ subl linkgrabber.py
```

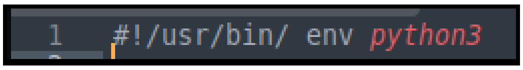


Something very cool you can do with these 2 libraries is the ability to extract all links on a webpage.

```
# Import the libraries we downloaded earlier
# if you try importing without installing them, this step will fail
from bs4 import BeautifulSoup
import requests

# replace testurl.com with the url you want to use.
# requests.get downloads the webpage and stores it as a variable
html = requests.get('testurl.com')

# this parses the webpage into something that beautifulsoup can read over
soup = BeautifulSoup(html, "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 variable
links = soup.find_all('a href')
for link in links:
    # prints each link
    print(link)
```

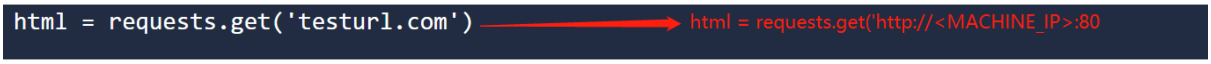
However, it requires us to do our own editing for some part of the script since it is just a script and obviously not suitable for the situation that we are facing at the moment.

1. **ADD !/usr/bin/ env python 3 in the first row**



```
#!/usr/bin/ env python3
```

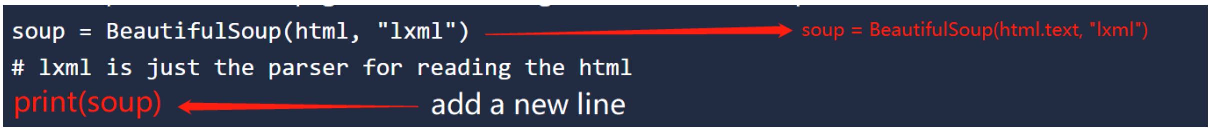
2.



```
html = requests.get('testurl.com')
```

html = requests.get('http://<MACHINE_IP>:80

3.



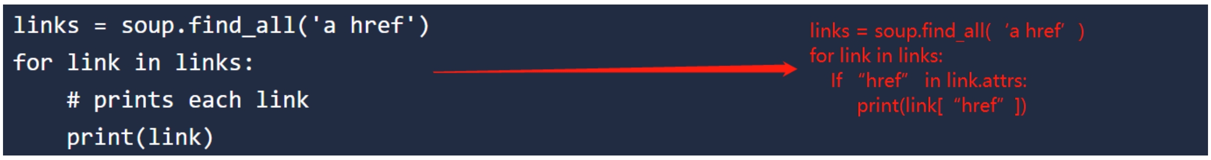
```
soup = BeautifulSoup(html, "lxml")
# lxml is just the parser for reading the html
```

soup = BeautifulSoup(html.text, "lxml")

print(soup)

add a new line

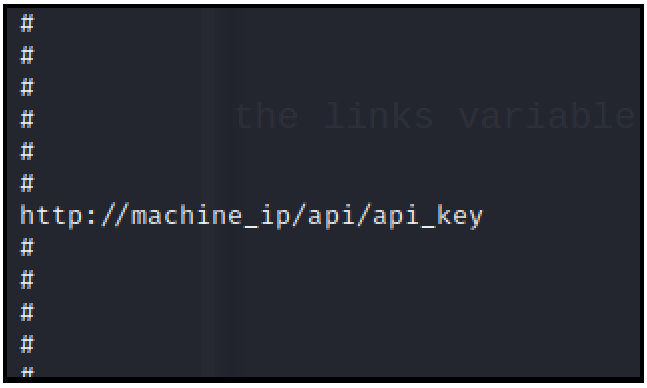
4.



```
links = soup.find_all('a href')
for link in links:
    # prints each link
    print(link)
```

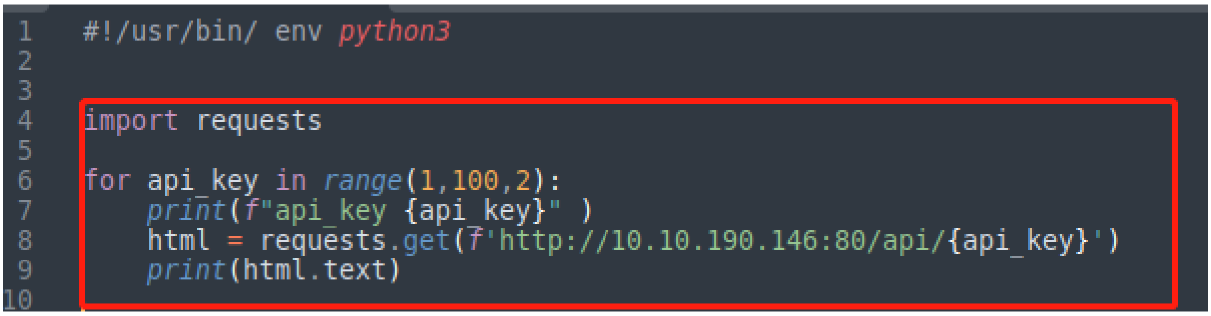
```
links = soup.find_all( ‘a href’ )
for link in links:
   If “href” in link.attrs:
     print(link[ “href” ])
```

After doing all the editing to the script, we may save the text file and run another command which is python3 linkgrabber.py and we can find the /api/ which is the answer for the question.



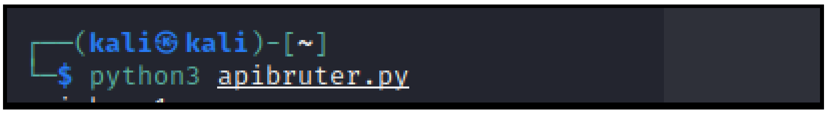
```
#
#
#
#
#
#
http://machine_ip/api/api_key
#
#
#
#
```

After that, we have to save the file as any name we like.For me, I saved the file as **apibruter**.After that we have to edit the file like this before saving.

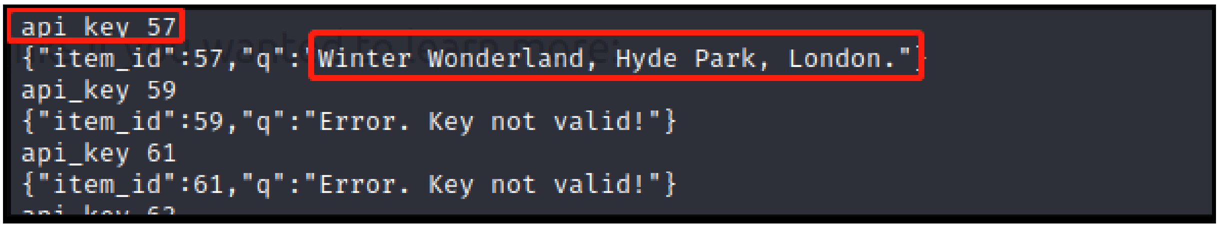


```
#!/usr/bin/ env python3


import requests

for api_key in range(1,100,2):
    print(f"api_key {api_key}" )
    html = requests.get(f'http://10.10.190.146:80/api/{api_key}')
    print(html.text)

```

After that, we run the command python3 <THELEASTFILENAME>.py.



```
┌──(kali㉿kali)-[~]
└─$ python3 apibruter.py
```



```
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!"}
```

<End of day 16>

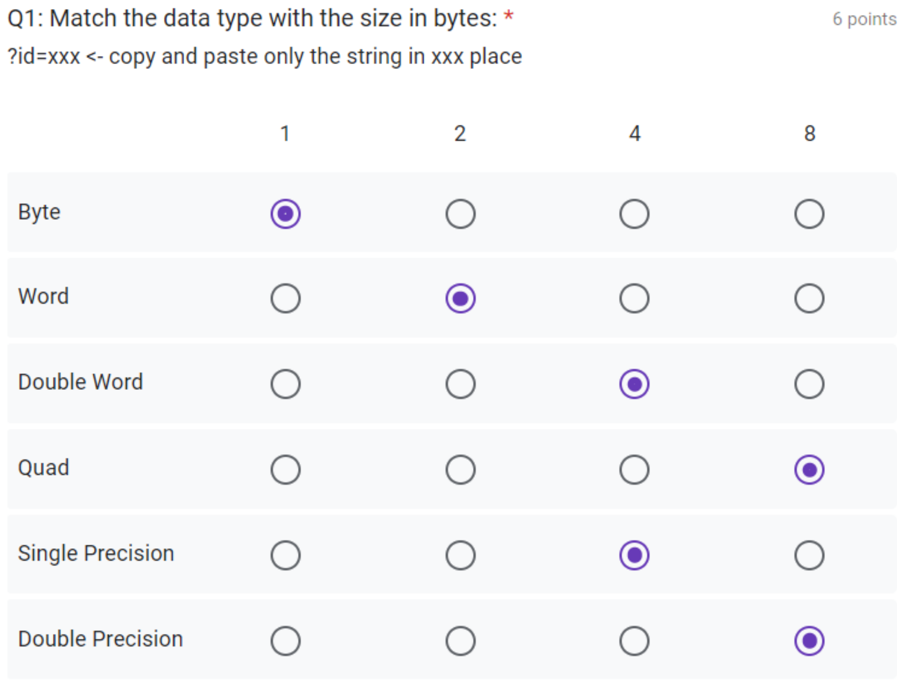
Day 17: ReverseELFneering (Reverse Engineering)

Tools used: Kali Linux, cmd

Solution/Walkthrough:

Question 1:

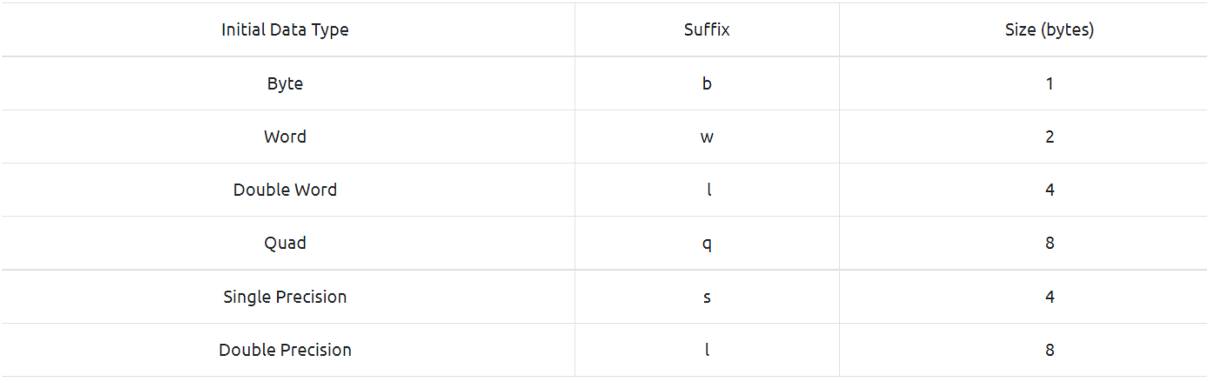
Answer:



Q1: Match the data type with the size in bytes: * 6 points

?id=xxx <- copy and paste only the string in xxx place

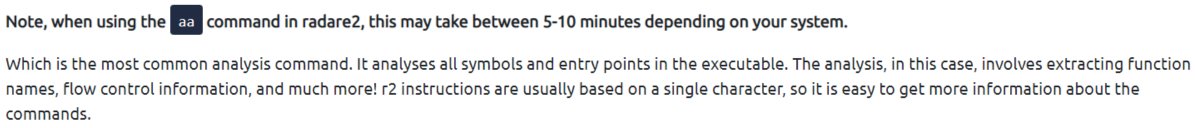
	1	2	4	8
Byte	●	○	○	○
Word	○	●	○	○
Double Word	○	○	●	○
Quad	○	○	○	●
Single Precision	○	○	●	○
Double Precision	○	○	○	●



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

Question 2

Answer: aa

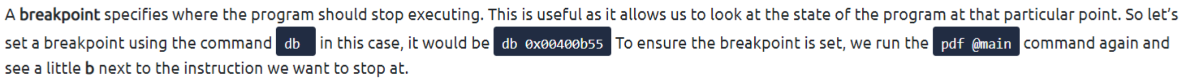


Note, when using the `aa` command in radare2, this may take between 5-10 minutes depending on your system.

Which is the most common analysis command. It analyses all symbols and entry points in the executable. The analysis, in this case, involves extracting function names, flow control information, and much more! r2 instructions are usually based on a single character, so it is easy to get more information about the commands.

Question 3

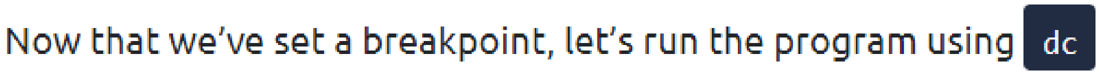
Answer: db



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 `db 0x00400b55` To ensure the breakpoint is set, we run the `pdf @main` command again and see a little **b** next to the instruction we want to stop at.

Question 4

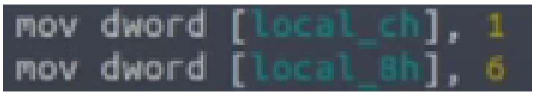
Answer: dc



Now that we've set a breakpoint, let's run the program using `dc`

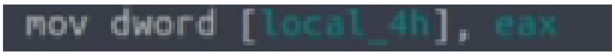
Question 5,6 and 7

Answer: 1, 6, 6



```
mov dword [local_ch], 1
mov dword [local_8h], 6
```

For Q5 and Q6

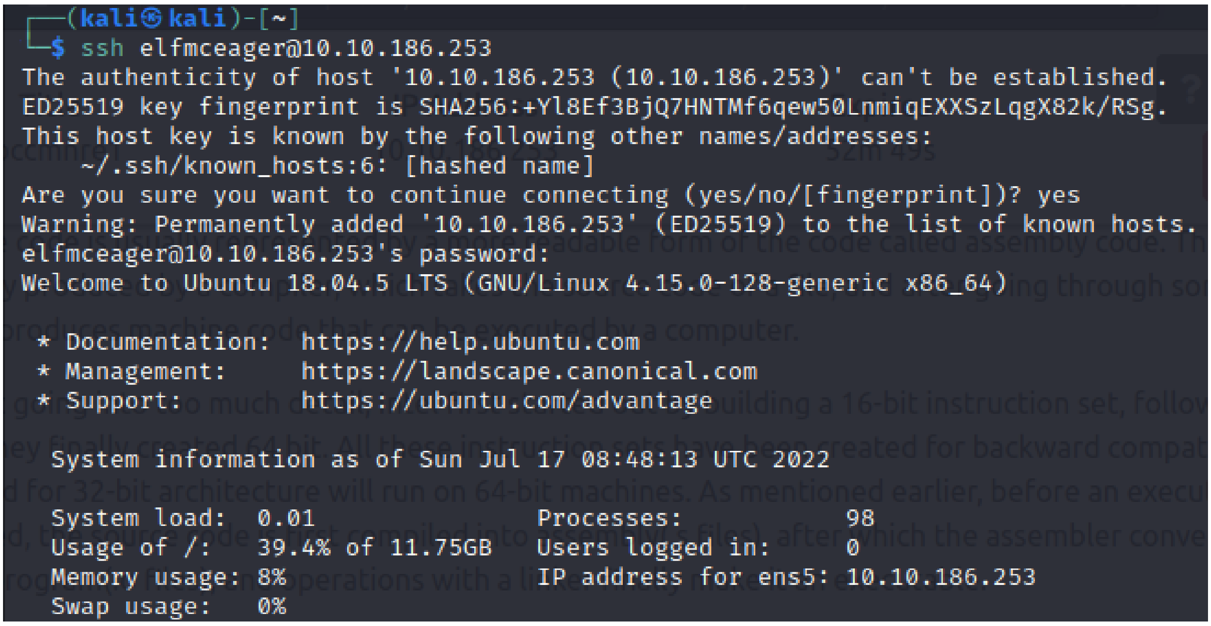


```
mov dword [local_4h], eax
```

For Q7 eax value is still 6 before it's set to 0

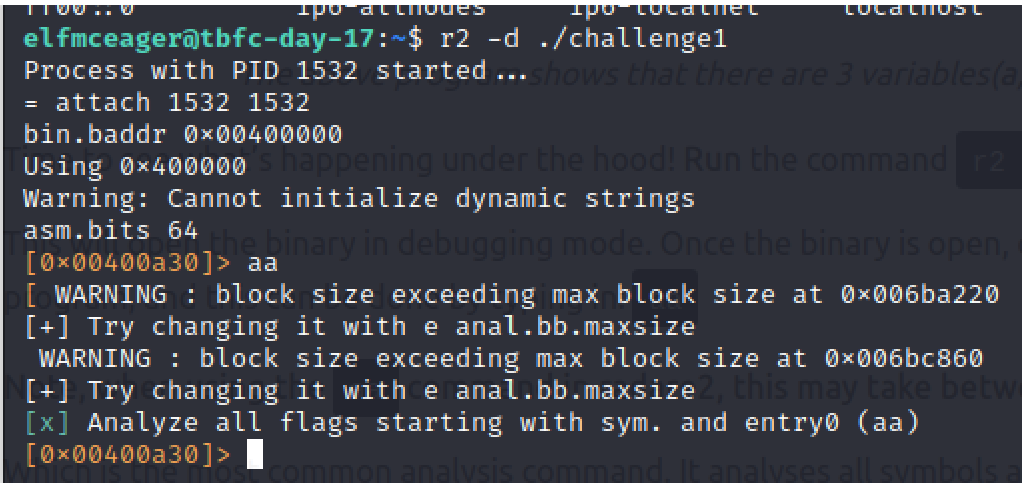
Thought Process/Methodology:

For the challenge, we first start up the machine and get the **<MACHINE_IP>,** then we run the command **SSH elfmceager@<MACHINE_IP>** and enter the password adventofcyber.



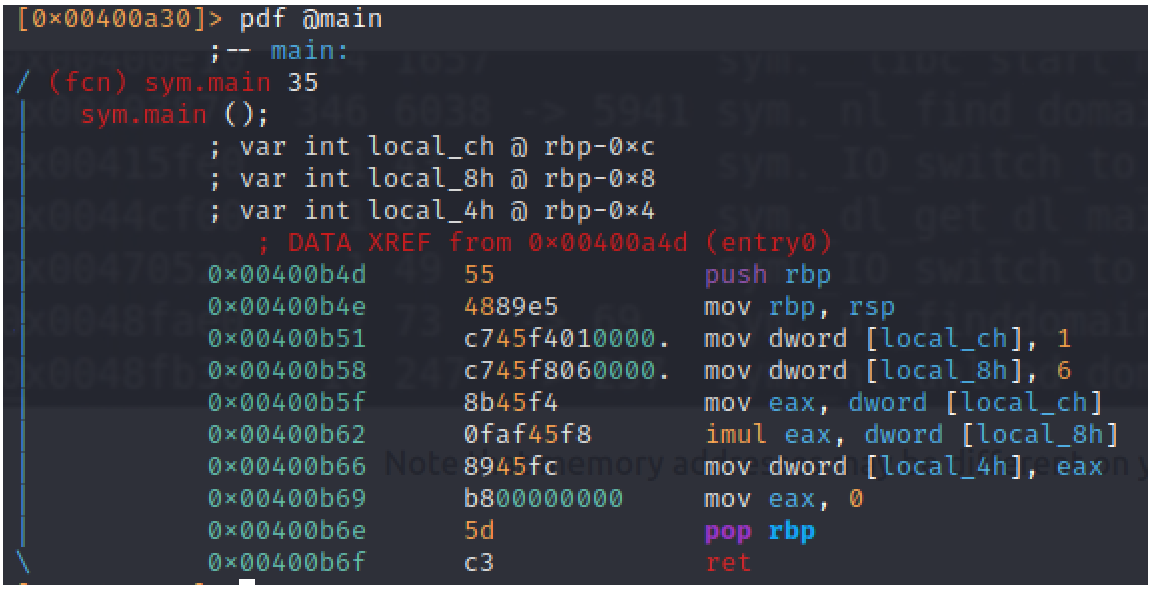
```
┌──(kali㉿kali)-[~]
└─$ ssh elfmceager@10.10.186.253
The authenticity of host '10.10.186.253 (10.10.186.253)' can't be established.
ED25519 key fingerprint is SHA256:+Yl8Ef3BjQ7HNTMf6qew50LnmiqEXXSzLqgX82k/RSg.
This host key is known by the following other names/addresses:
    ~/.ssh/known_hosts:6: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.186.253' (ED25519) to the list of known hosts.
elfmceager@10.10.186.253's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-128-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sun Jul 17 08:48:13 UTC 2022

  System load:  0.01              Processes:           98
  Usage of /:   39.4% of 11.75GB  Users logged in:     0
  Memory usage: 8%                IP address for ens5: 10.10.186.253
  Swap usage:   0%
```

After that we run the command r2 -d ./challenge1 to open the binary debugging mode. We ran aa to analyse the program.



```
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1532 started...
= attach 1532 1532
bin.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits 64
[0x00400a30]> aa
[ WARNING : block size exceeding max block size at 0x006ba220
[+] Try changing it with e anal.bb.maxsize
 WARNING : block size exceeding max block size at 0x006bc860
[+] Try changing it with e anal.bb.maxsize
[x] Analyze all flags starting with sym. and entry0 (aa)
[0x00400a30]> 
```

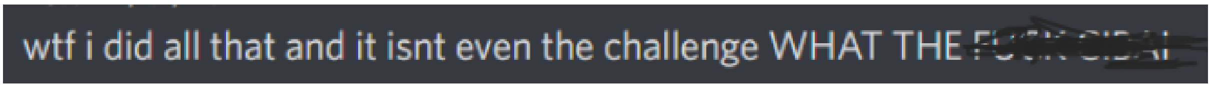
Then, we ran pdf @main that gives us the following values for the questions in THM



```
[0x00400a30]> pdf @main
            ;-- main:
/ (fcn) sym.main 35
|   sym.main ();
|           ; var int local_ch @ rbp-0xc
|           ; var int local_8h @ rbp-0x8
|           ; var int local_4h @ rbp-0x4
|              ; DATA XREF from 0x00400a4d (entry0)
|           0x00400b4d      55             push rbp
|           0x00400b4e      4889e5         mov rbp, rsp
|           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]
|           0x00400b66      8945fc         mov dword [local_4h], eax
|           0x00400b69      b800000000     mov eax, 0
|           0x00400b6e      5d             pop rbp
\           0x00400b6f      c3             ret
```

Wise words from our leader:

WHAT THE [redacted] IS THIS ASSEMBLY CODE [redacted]



wtf i did all that and it isnt even the challenge WHAT THE [redacted]

<End of Day 17>

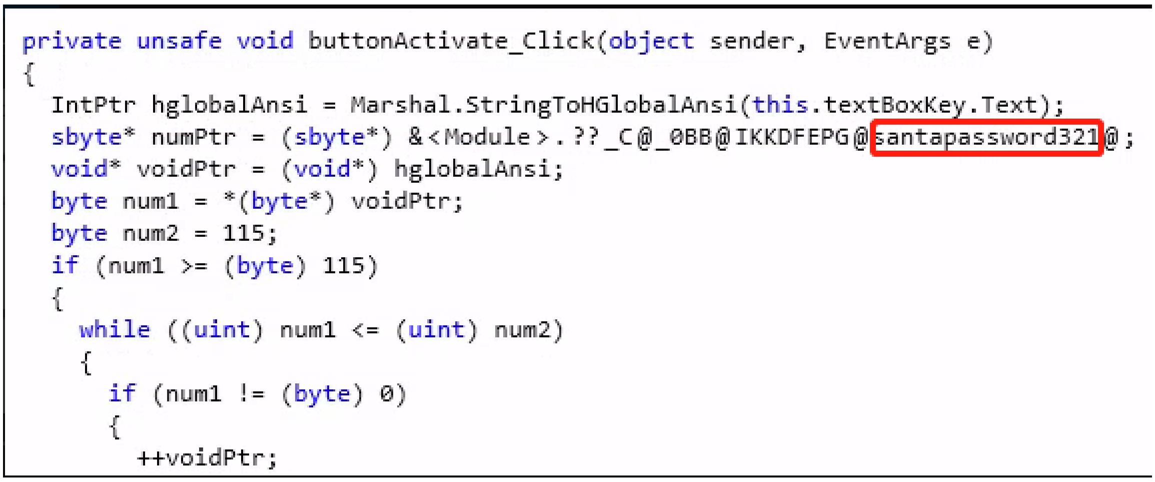
Day 18: The Bits of Christmas (Reverse Engineering)

Tools used: Kali Linux,Remmina,dotPeek,

Solution/Walkthrough:

Question 1:

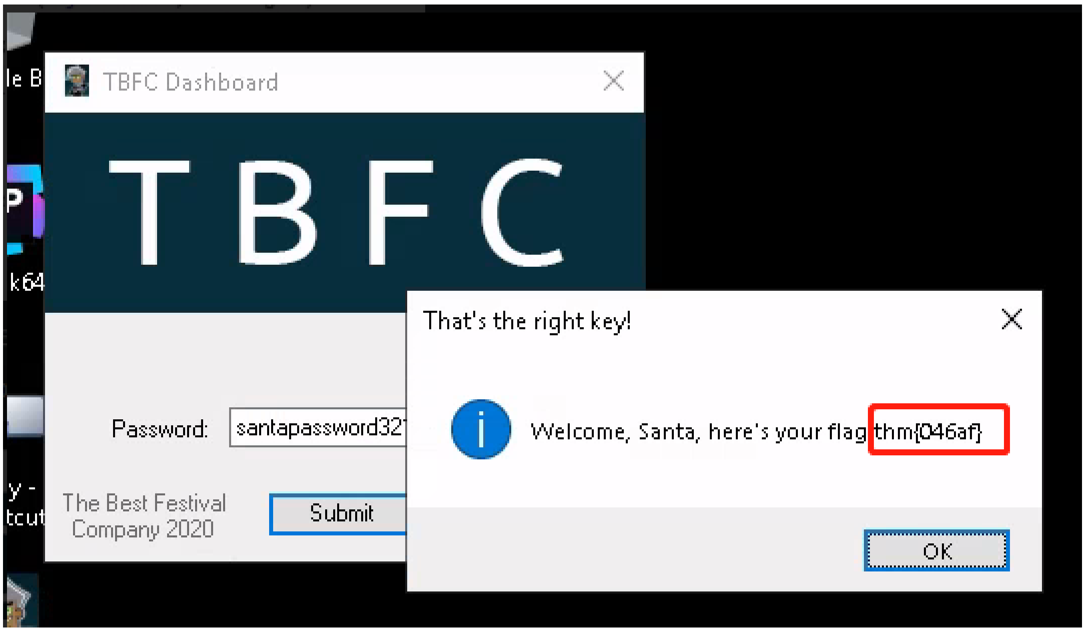
Answer:santapassword321



```
private unsafe void buttonActivate_Click(object sender, EventArgs e)
{
  IntPtr hglobalAnsi = Marshal.StringToHGlobalAnsi(this.textBoxKey.Text);
  sbyte* numPtr = (sbyte*) &<Module>.??_C@_0BB@IKKDFEPG@santapassword321@;
  void* voidPtr = (void*) hglobalAnsi;
  byte num1 = *(byte*) voidPtr;
  byte num2 = 115;
  if (num1 >= (byte) 115)
  {
    while ((uint) num1 <= (uint) num2)
    {
      if (num1 != (byte) 0)
      {
        ++voidPtr;
```

Question 2:

Answer:thm{046af}



Password: santapassword321

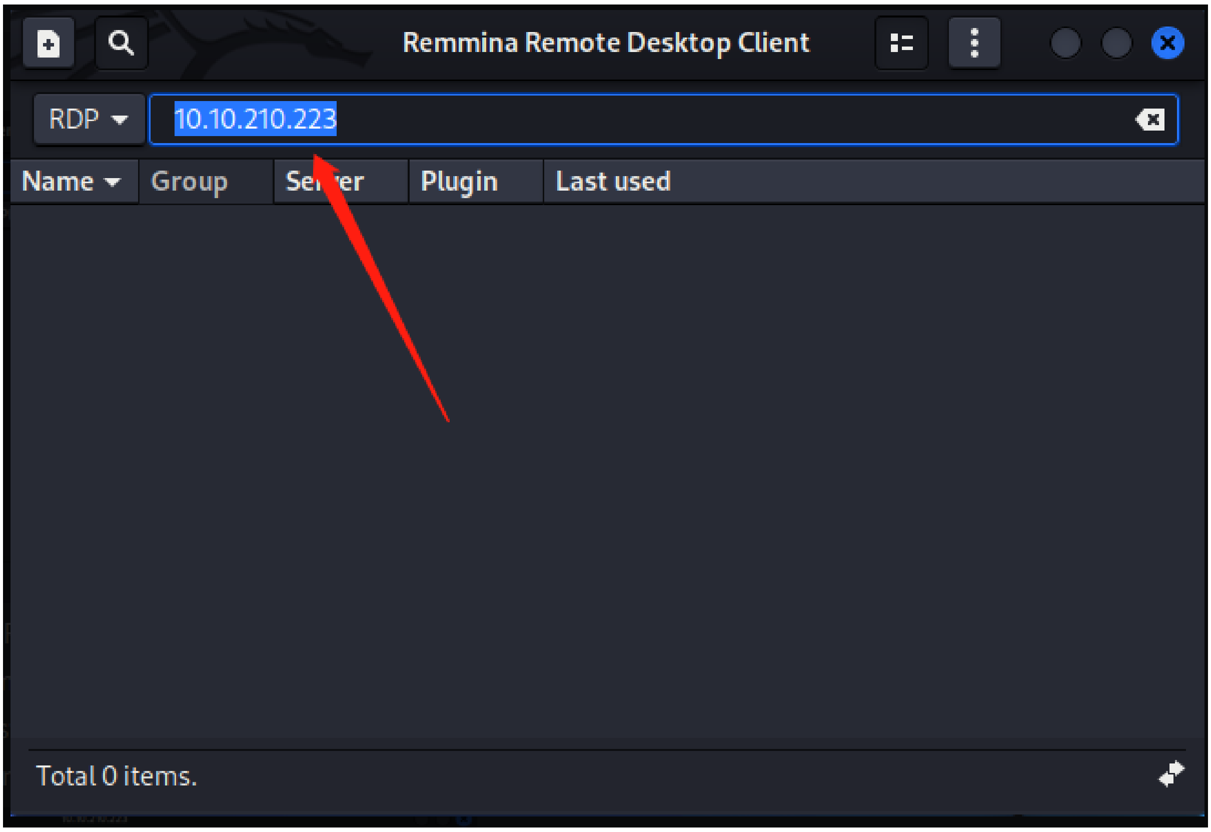
The Best Festival Company 2020

That's the right key!

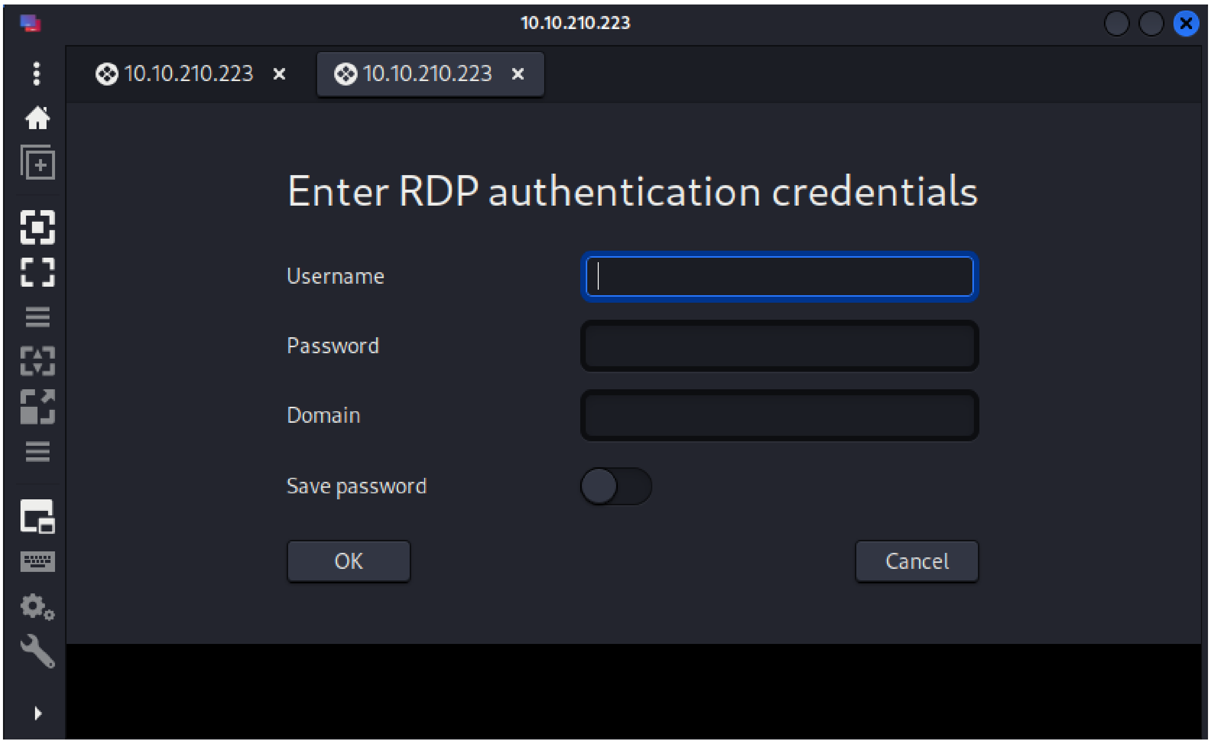
Welcome, Santa, here's your flag thm{046af}

Thought Process/Methodology:

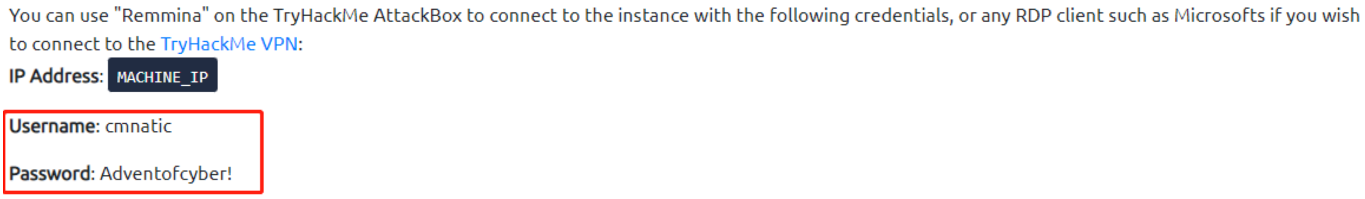
Firstly,we will need an RDP client for today's challenge.We are using Remmina today.To install Remmina on Kali Linux (https://installati.one/kalilinux/remmina/).After installing,we enter our <MACHINE_IP> in the searching field.



And then we will go to the page



Enter username and password which is provided in THM.



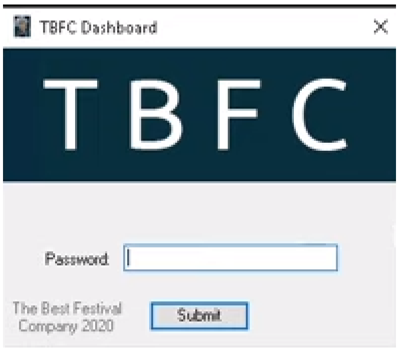
You can use "Remmina" on the TryHackMe AttackBox to connect to the instance with the following credentials, or any RDP client such as Microsofts if you wish to connect to the TryHackMe VPN:

IP Address: `MACHINE_IP`

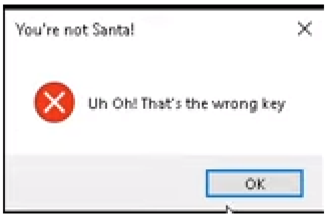
Username: cmnatic

Password: Adventofcyber!

Open TBFC_APP



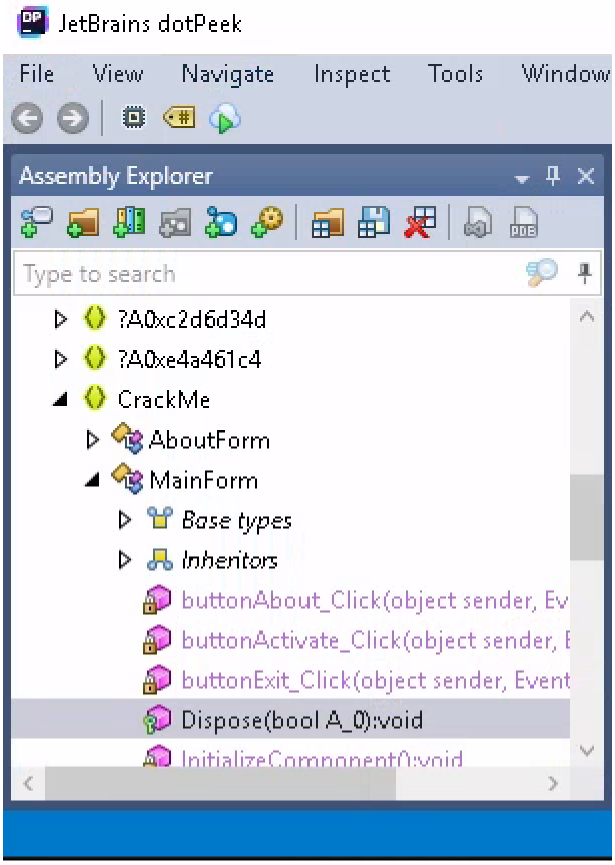
If we enter the wrong password, this will happen.



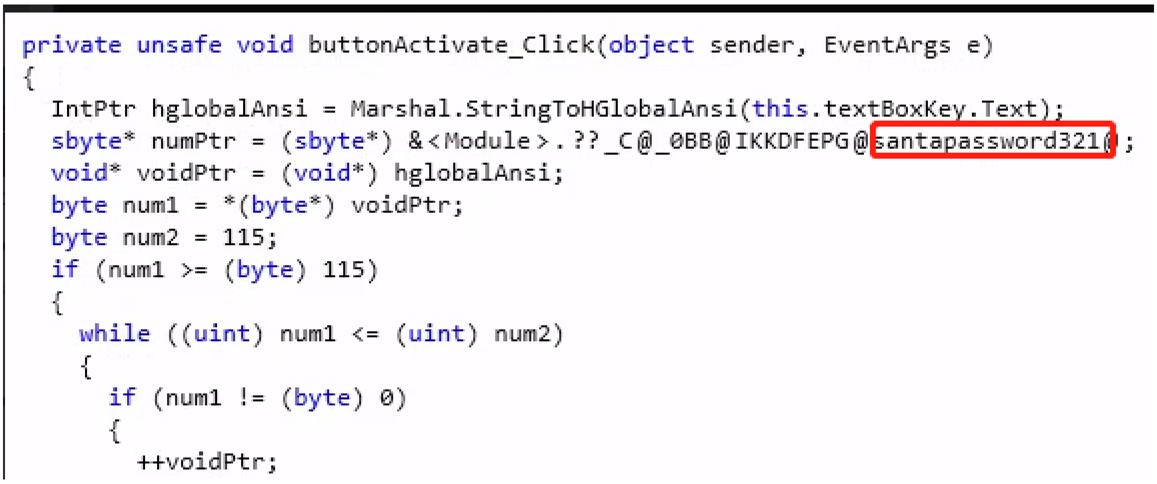
You're not Santa!

Uh Oh! That's the wrong key

So to find the correct password, we will be using dotPeek.Next, select the exe file by clicking on file > open > select and we open the Dispose under CrackMe>MainForm.

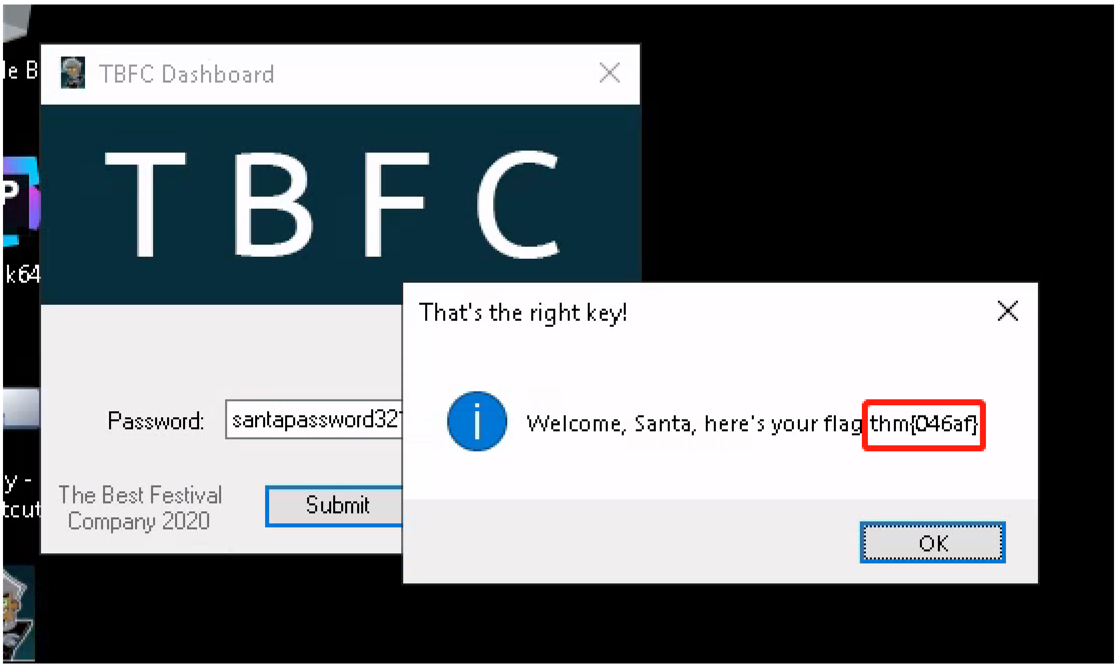


Go through the code and we will find out that there is an if else statement that shows ust he password which is **santapassword321**



```
private unsafe void buttonActivate_Click(object sender, EventArgs e)
{
  IntPtr hglobalAnsi = Marshal.StringToHGlobalAnsi(this.textBoxKey.Text);
  sbyte* numPtr = (sbyte*) &<Module>.??_C@_0BB@IKKDFEPG@santapassword321@;
  void* voidPtr = (void*) hglobalAnsi;
  byte num1 = *(byte*) voidPtr;
  byte num2 = 115;
  if (num1 >= (byte) 115)
  {
    while ((uint) num1 <= (uint) num2)
    {
      if (num1 != (byte) 0)
      {
        ++voidPtr;
```

After entering the correct password that we found in the TBFC Dashboard, we will get the flag which is the answer for the question in THM.



Password: santapassword32

The Best Festival Company 2020

That's the right key!

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

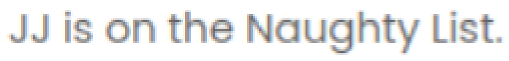
<End of day 18>

Day 19:The Naughty or Nice List (Web Exploitation)

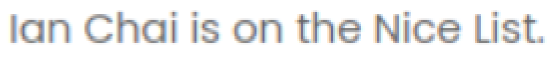
Tools used: Kali Linux, Firefox

Solution/Walkthrough:

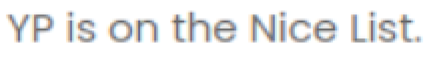
Question 1:



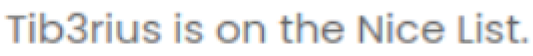
JJ is on the Naughty List.



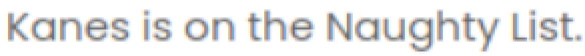
Ian Chai is on the Nice List.



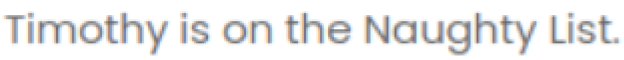
YP is on the Nice List.



Tib3rius is on the Nice List.



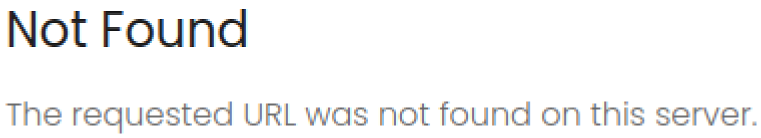
Kanes is on the Naughty List.



Timothy is on the Naughty List.

Question 2:

The requested URL was not found on this server.

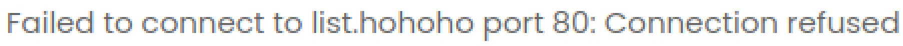


Not Found

The requested URL was not found on this server.

Question 3:

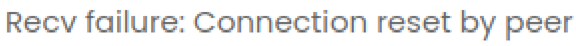
Failed to connect to list.hohoho port 80: Connection refused



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

Question 4:

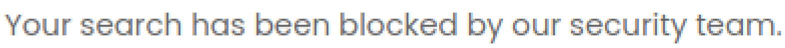
Recv failure: Connection reset by peer



Recv failure: Connection reset by peer

Question 5:

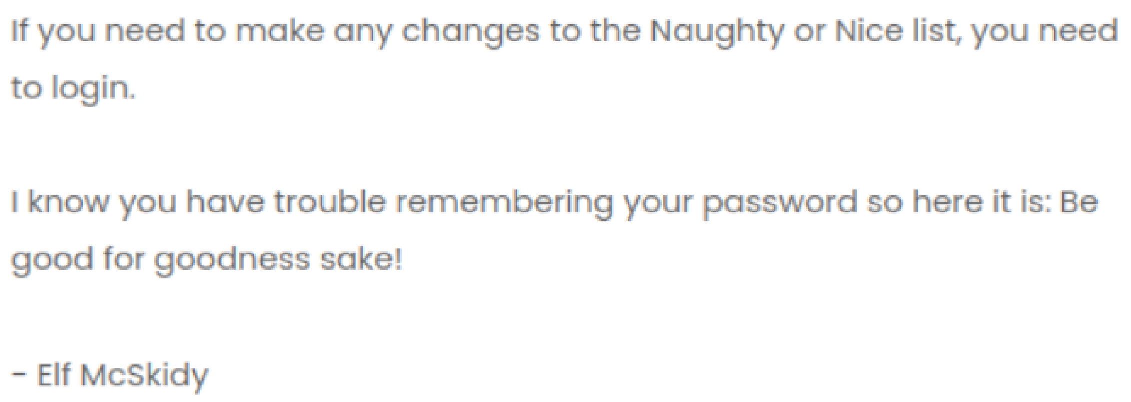
Your search has been blocked by our security team.



Your search has been blocked by our security team.

Question 6:

Be good for goodness sake!

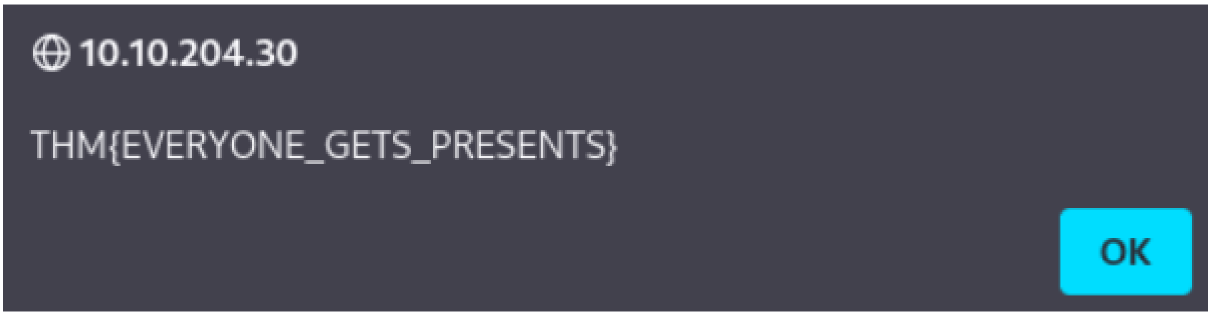


If you need to make any changes to the Naughty or Nice list, you need to login.

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

- Elf McSkidy

Question 7:
THM{EVERYONE_GETS_PRESENTS}

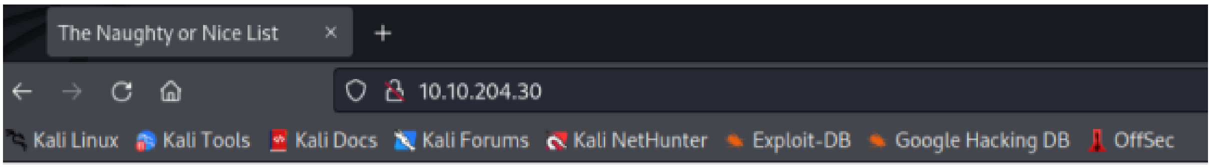


10.10.204.30

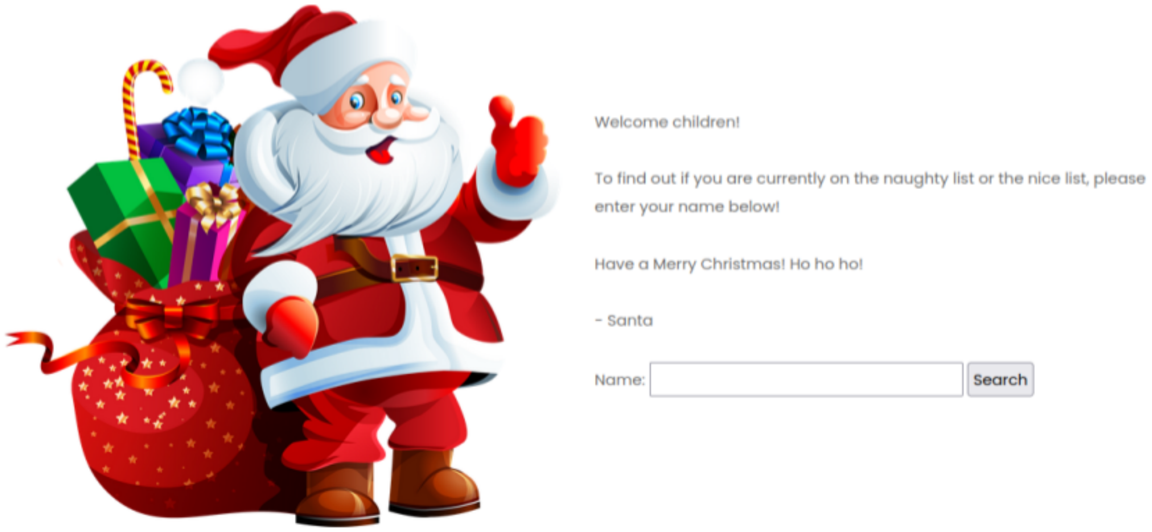
THM{EVERYONE_GETS_PRESENTS}

Thought Process/Methodology:

After the **<MACHINE_IP>** appeared, we opened up a browser window and entered the **<MACHINE_IP>** into Firefox.



Then we enter a name into the field, it would tell us whether that name is on the nice or naughty list.



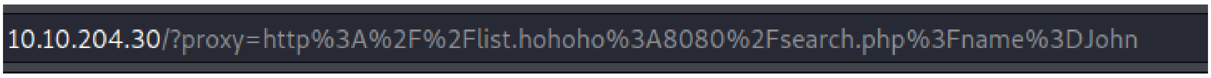
Welcome children!

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!

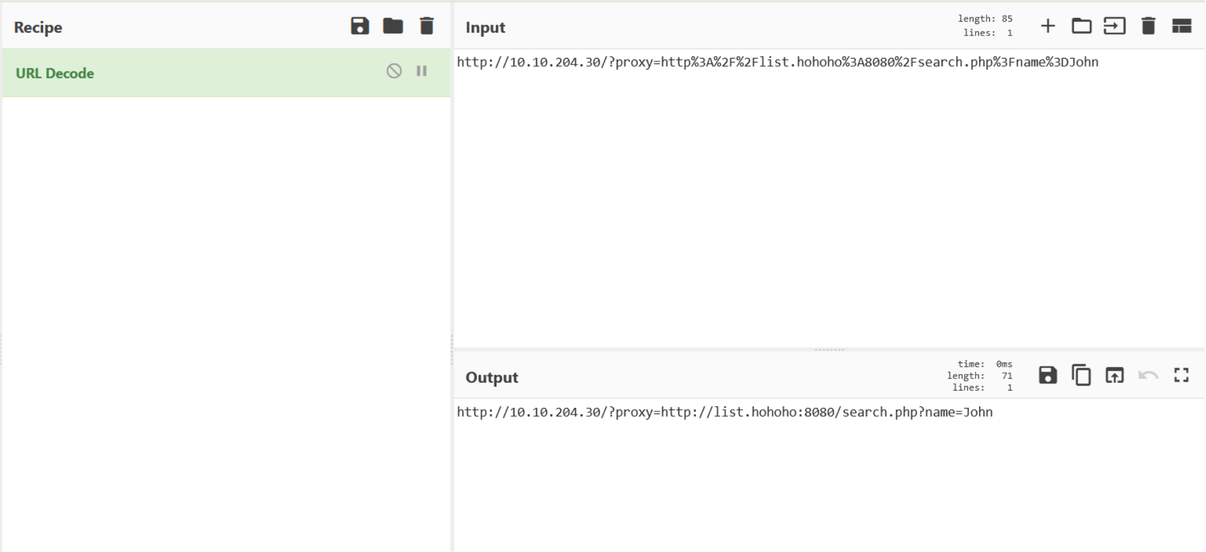
- Santa

For our group we key in **John** into the field and output a url that looks like http://10.10.204.30/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DJohn



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

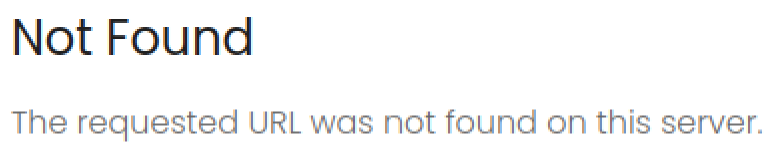
After that we use a url decoder on the value of the proxy parameter and we get http://list.hohoho:8080/search.php?name=John



```
http://10.10.204.30/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DJohn
```

```
http://10.10.204.30/?proxy=http://list.hohoho:8080/search.php?name=John
```

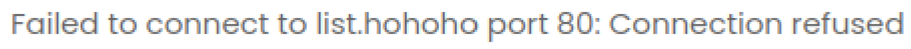
After we get url, we try to browse to the root of the site at http://10.10.204.30/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F and we get something like this



Not Found

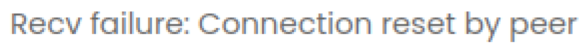
The requested URL was not found on this server.

We try to connect to the site via port **80** instead of **8080** we get the following error



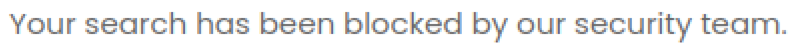
Failed to connect to list.hohoho port 80: Connection refused

Then we try to connect via port **22(SSH)** and we get the following error. However, it does indicate that the port is open.



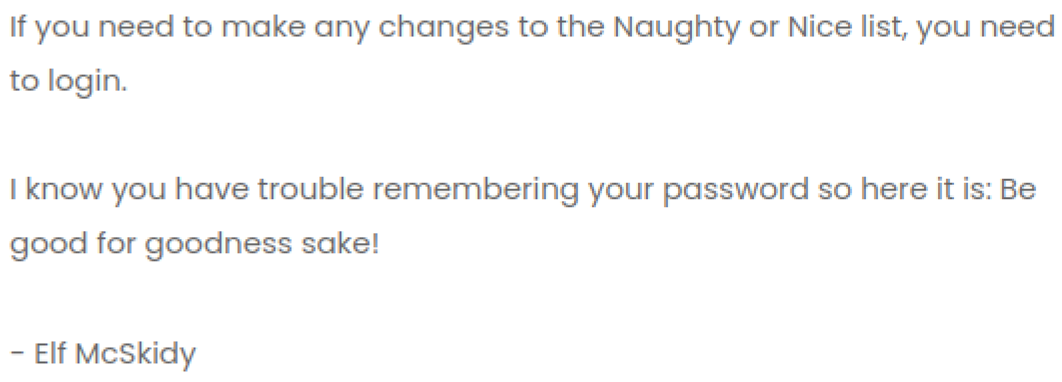
Recv failure: Connection reset by peer

We tried to access services running locally but it seems like they were one step ahead.



Your search has been blocked by our security team.

We can bypass the checks by using DNS subdomains
http://10.10.204.30/?proxy=http%3A%2F%2Flist.hohoho.localtest.me
this resolves the subdomain to 127.0.0.1 and we get the password which is **Be good for goodness sake!**

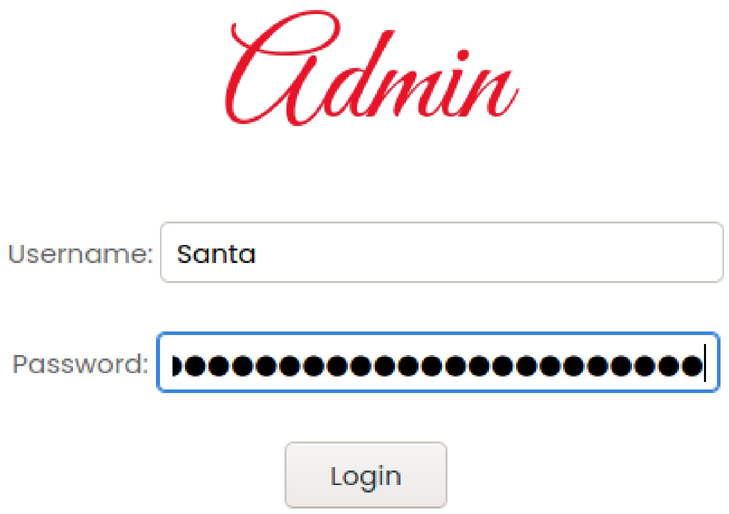


If you need to make any changes to the Naughty or Nice list, you need to login.

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

- Elf McSkidy

After we get the password, we can then login to the admin panel with the password we found. The username is **Santa**.

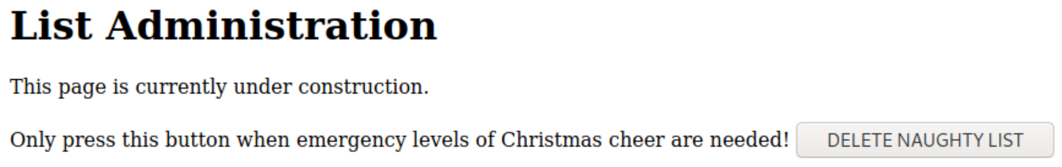


Admin

Username: Santa

Password: ●●●●●●●●●●●●●●●●●●●●●●●●

Once we are in **List Administration**

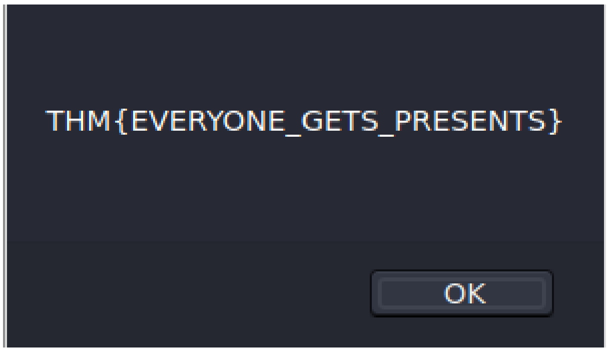


List Administration

This page is currently under construction.

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

We delete the naught list and we will get the flag which is **THM{EVERYONE_GETS_PRESENTS}**



THM{EVERYONE_GETS_PRESENTS}

<End of day 19>

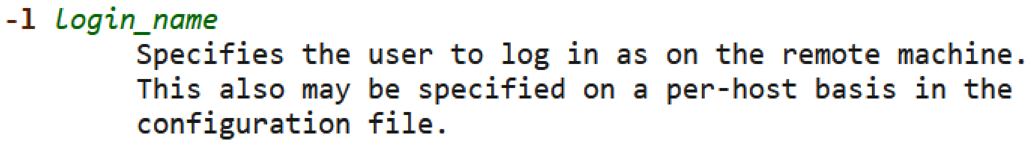
Day 20:PowershELlF to the rescue (Blue Teaming)

Tools used: Kali Linux, SSH, Powershell

Solution/Walkthrough:

Question 1:

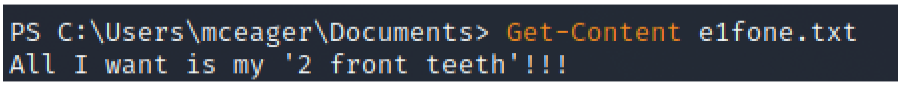
Login name



```
   -l login_name
           Specifies the user to log in as on the remote machine.
           This also may be specified on a per-host basis in the
           configuration file.
```

Question 2:

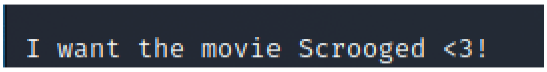
2 front teeth



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

Question 3:

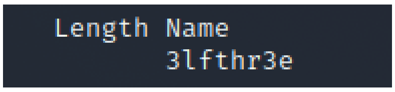
Scrooged



```
 I want the movie Scrooged <3!
```

Question 4:

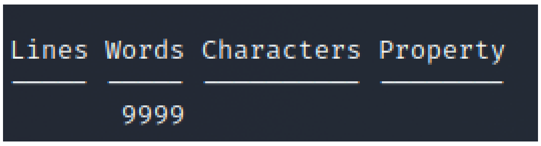
The filename is **3lfthr3e**



```
   Length Name
          3lfthr3e
```

Question 5:

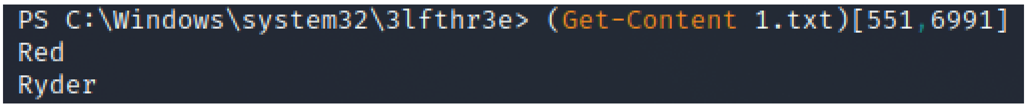
9999 words.



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

Question 6:

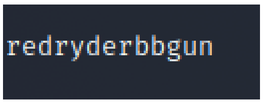
The 2 words are **Red** and **Ryder**.



```
PS C:\Windows\system32\3lfthr3e> (Get-Content 1.txt)[551,6991]
Red
Ryder
```

Question 7:

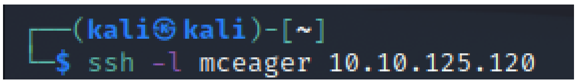
redryderbbgun



```
redryderbbgun
```

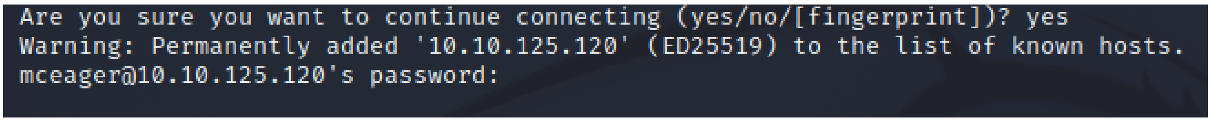
Thought Process/Methodology:

After the **<MACHINE_IP>** is ready, we ssh to the remote machine with command ssh -l mceager <MACHINE_IP> .



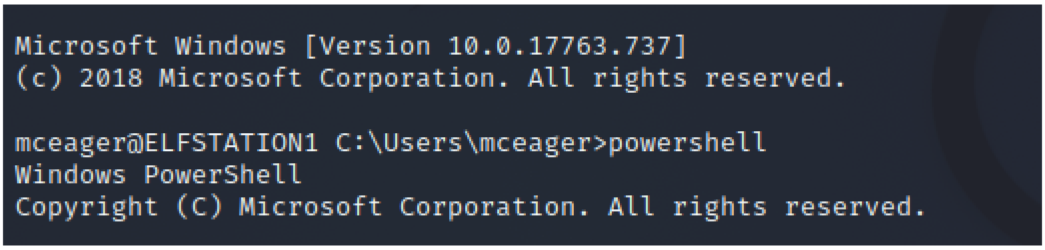
```
┌──(kali㉿kali)-[~]
└─$ ssh -l mceager 10.10.125.120
```

When prompted, enter the password that was provided from TryHackMe, **r0ckStar!**



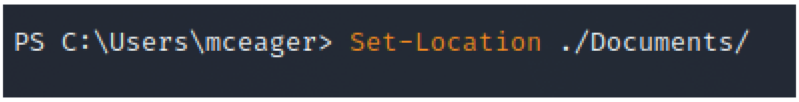
```
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.125.120' (ED25519) to the list of known hosts.
mceager@10.10.125.120's password:
```

Then we launched powershell with command powershell



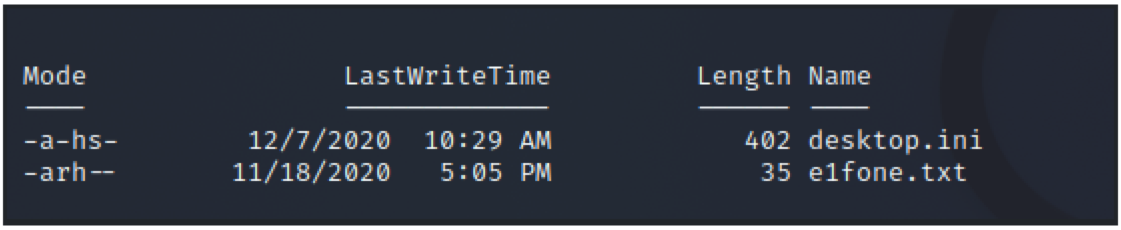
```
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.

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

After that, we navigate to the documents folder with command Set-Location ./Documents/



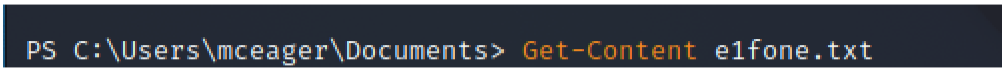
```
PS C:\Users\mceager> Set-Location ./Documents/
```

For finding the first hidden file we can run `Get-ChildItem -File -Hidden -ErrorAction SilentlyContinue` and the file is called **e1fone.txt**



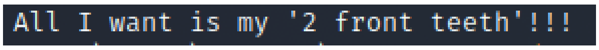
```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a-hs-          12/7/2020  10:29 AM            402 desktop.ini
-arh--         11/18/2020   5:05 PM             35 e1fone.txt
```

For further to see the contents of this file we run command `Get-Content e1fone.txt`



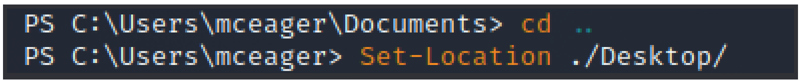
```
PS C:\Users\mceager\Documents> Get-Content e1fone.txt
```

We will get the answer which is **2 front teeth**



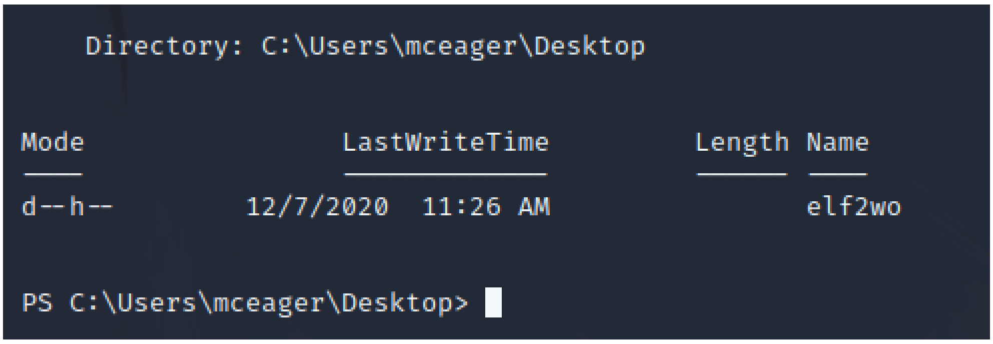
```
All I want is my '2 front teeth'!!!
```

Then we run the command `cd ..` to change the current directory to the parent directory. We navigate to the desktop by using command `Set-Location ./Desktop/`



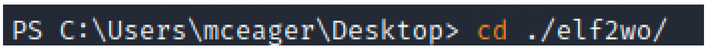
```
PS C:\Users\mceager\Documents> cd ..
PS C:\Users\mceager> Set-Location ./Desktop/
```

We search for the hidden folder with command `Get-ChildItem -Directory -Hidden -ErrorAction SilentlyContinue` and the directory is called **elf2wo**

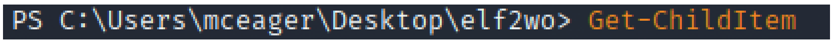


```
    Directory: C:\Users\mceager\Desktop


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


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

We run the command `cd ./elf2wo/` to enter the directory. Once we are in the directory we can run `Get-ChildItem` to find the text file.

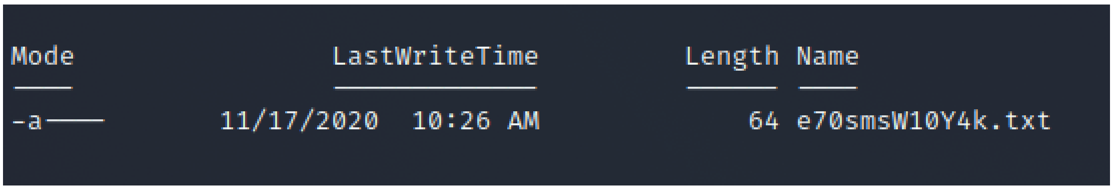


```
PS C:\Users\mceager\Desktop> cd ./elf2wo/
```



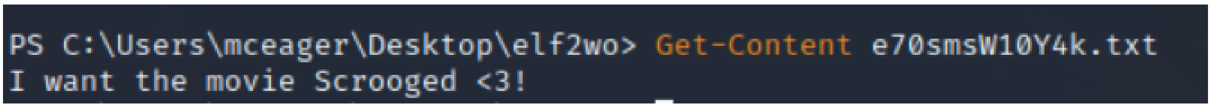
```
PS C:\Users\mceager\Desktop\elf2wo> Get-ChildItem
```

We will get this



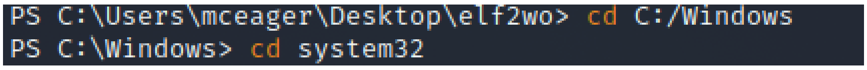
```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----        11/17/2020  10:26 AM             64 e70smsW10Y4k.txt
```

We read the contents of the file by running Get-Content e70smsW10Y4k.txt and we will get the answer which is **Scrooged**.



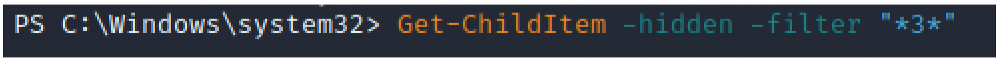
```
PS C:\Users\mceager\Desktop\elf2wo> Get-Content e70smsW10Y4k.txt
I want the movie Scrooged <3!
```

After that, to find the answer for question 3 we first have to change our directory by using command cd C:/Windows and cd system32



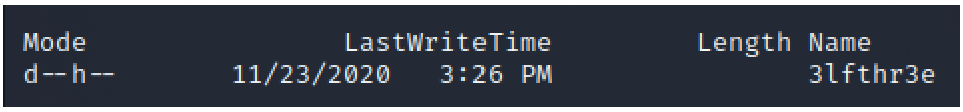
```
PS C:\Users\mceager\Desktop\elf2wo> cd C:/Windows
PS C:\Windows> cd system32
```

After we were in the directory, we key in command Get-ChildItem -Hidden -Directory -Filter '*3*' and we will find the folder.



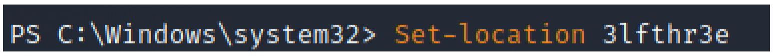
```
PS C:\Windows\system32> Get-ChildItem -hidden -filter "*3*"
```

The folder is called **3lfthr3e**



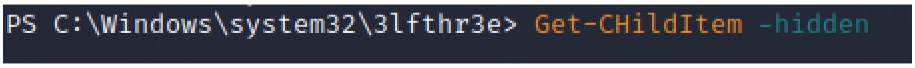
```
Mode                 LastWriteTime         Length Name
d--h--        11/23/2020   3:26 PM                3lfthr3e
```

We change directory by using command Set-Location3lfthr3e



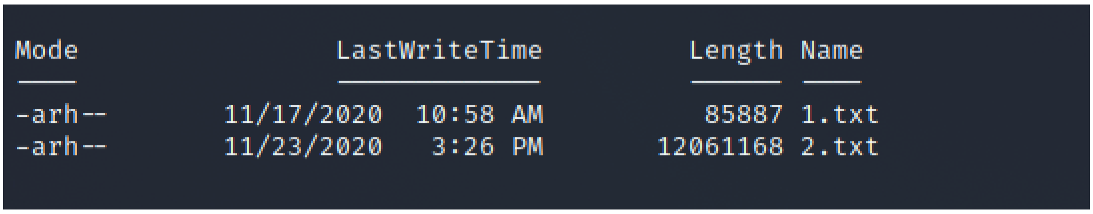
```
PS C:\Windows\system32> Set-location 3lfthr3e
```

Once we are in the folder we can run Get-ChildItem -hidden to find the files



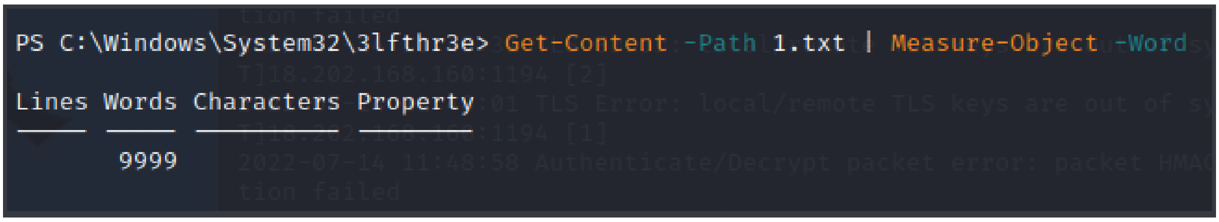
```
PS C:\Windows\system32\3lfthr3e> Get-CHildItem -hidden
```

Here’s the files.



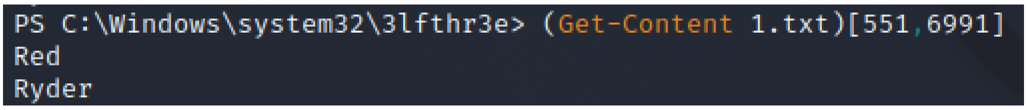
```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-arh--        11/17/2020  10:58 AM          85887 1.txt
-arh--        11/23/2020   3:26 PM       12061168 2.txt
```

To find out how many words are in the first file we can run Get-Content -Path 1.txt | Measure-Object -Word . After we run the command, we know that there are **9999** words in the first file.



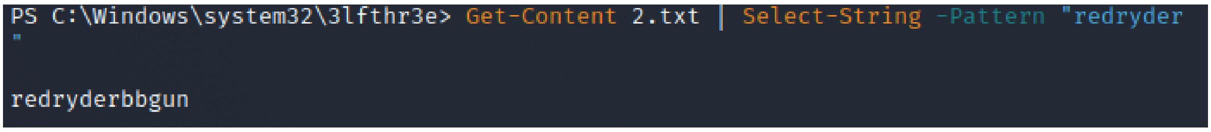
```
PS C:\Windows\System32\3lfthr3e> Get-Content -Path 1.txt | Measure-Object -Word

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

Then we find out the words by running (Get-Content 1.txt)[551,6991] and the words are **Red Ryder**



```
PS C:\Windows\system32\3lfthr3e> (Get-Content 1.txt)[551,6991]
Red
Ryder
```

Last but not least, to find the full phrase we can run Get-Content 2.txt | Select-String -Pattern "redryder" and we will get the phrase which is **redryderbbgun**



```
PS C:\Windows\system32\3lfthr3e> Get-Content 2.txt | Select-String -Pattern "redryder
"

redryderbbgun
```

<End of day 20>