Report PSP0201 T2130 Tutorial – Week 5

Group name: **Marceline**

ID	Name	Role
1211100899	Muhammad Shahril Aiman	Leader
1211101533	Muhammad Aniq Fahmi	Member
1211101303	Aiman Faris	Member
1211102759	Muhammad Zaquan	Member

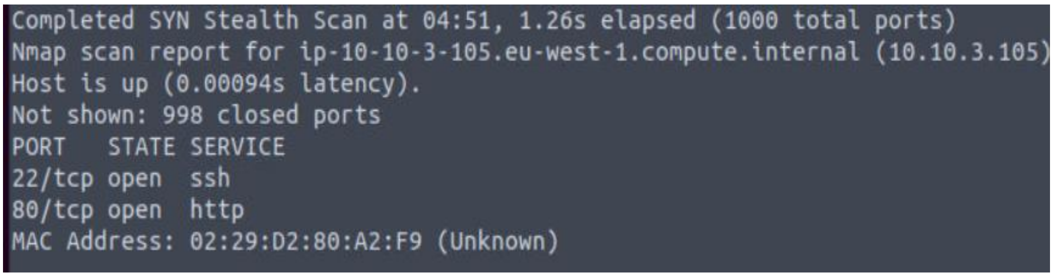
Day 16 - Help! Where is Santa?

Tools used: AttackBox, Firefox, Python3

Solution/Walkthrough:

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

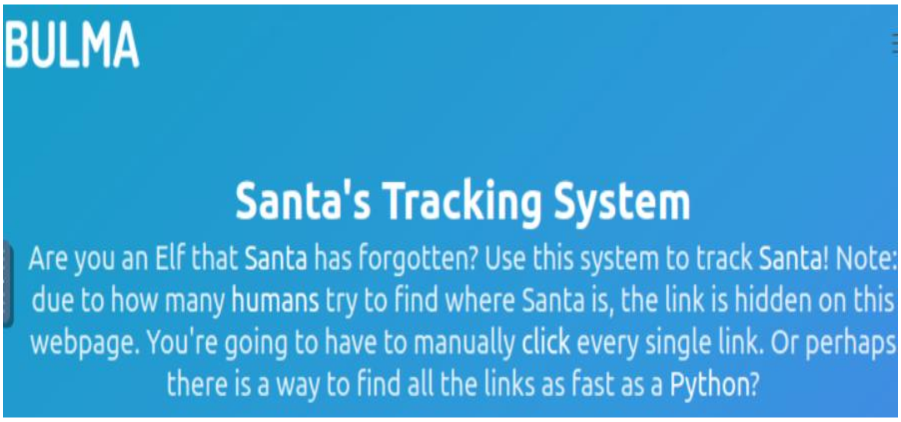
= 80



```
Completed SYN Stealth Scan at 04:51, 1.26s elapsed (1000 total ports)
Nmap scan report for ip-10-10-3-105.eu-west-1.compute.internal (10.10.3.105)
Host is up (0.00094s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:29:D2:80:A2:F9 (Unknown)
```

Question 2: What templates are being used?

= BULMA



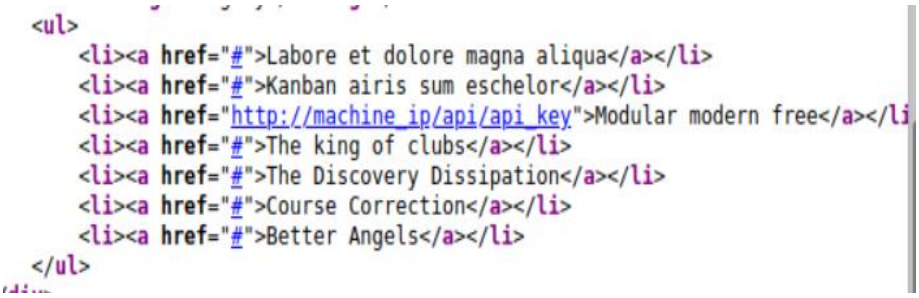
BULMA

Santa's Tracking System

Are you an Elf that Santa has forgotten? Use this system to track Santa! Note: due to how many humans try to find where Santa is, the link is hidden on this webpage. You're going to have to manually click every single link. Or perhaps there is a way to find all the links as fast as a Python?

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

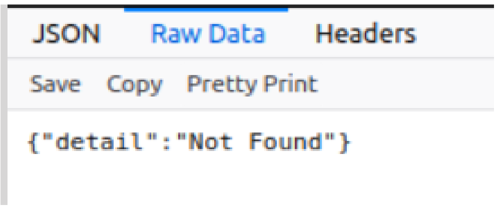
= /api/



```
<ul>
    <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>
</ul>
```

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

= {"detail":"Not Found"}



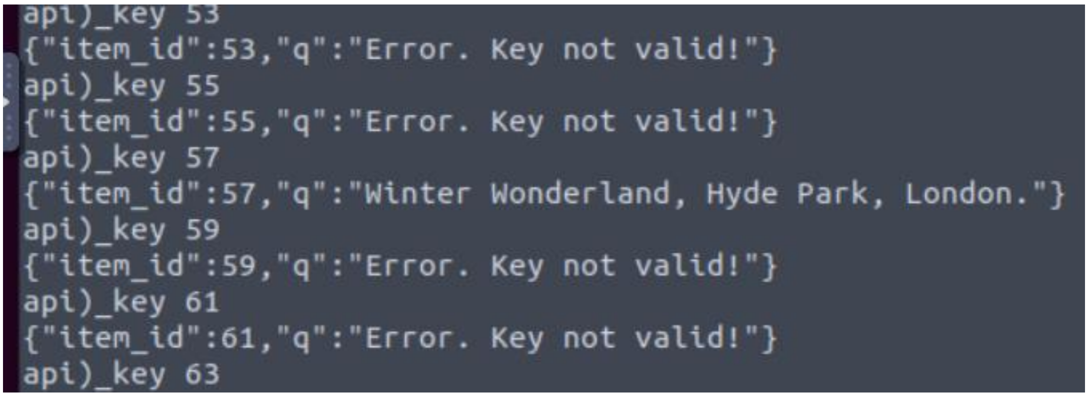
```
{"detail":"Not Found"}
```

Question 5: Where is Santa right now?

= 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)

= 57



```
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
```

METHODOLOGY:

We launch the AttackBox to gain the Ip address. First of all, we scan the Ip address using nmap with setting of (-v) to obtain the port number of the web server. After that, we use Firefox and open website by searching the Ip address with the port number. It brings us to BULMA website. We view the page source to survey and find the directory API. Next, we change the endpoint API by entered no parameters in it to solve question 4. Lastly, we use python3 in the AttackBox to figure out the correct API key and Santa current location.

Day 17 - Reverse Engineering: ReverseELFneering

Tools used: Kali Linux, Firefox.

Solution/Walkthrough

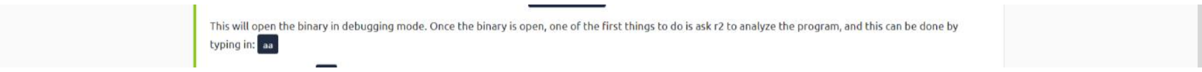
Question 1: Match the data type with the size in bytes

Answer:

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

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

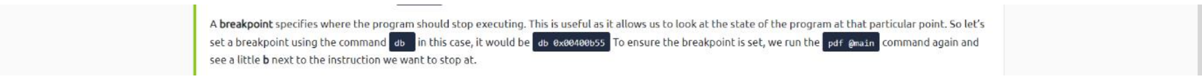
Answer: aa



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

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

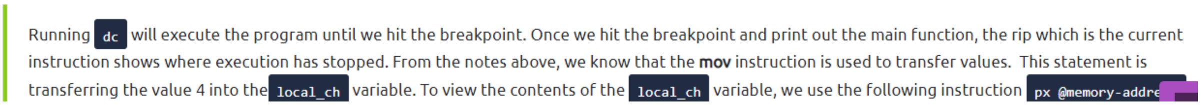
Answer: db



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

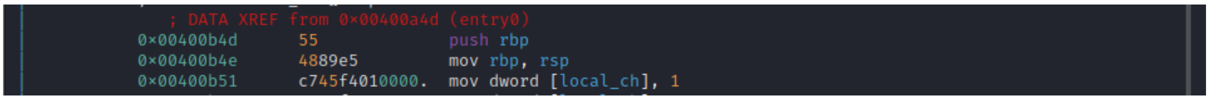
Answer: dc



Running `dc` will execute the program until we hit the breakpoint. Once we hit the breakpoint and print out the main function, the rip which is the current instruction shows where execution has stopped. From the notes above, we know that the **mov** instruction is used to transfer values. This statement is transferring the value 4 into the `local_ch` variable. To view the contents of the `local_ch` variable, we use the following instruction `px @memory-addre`

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

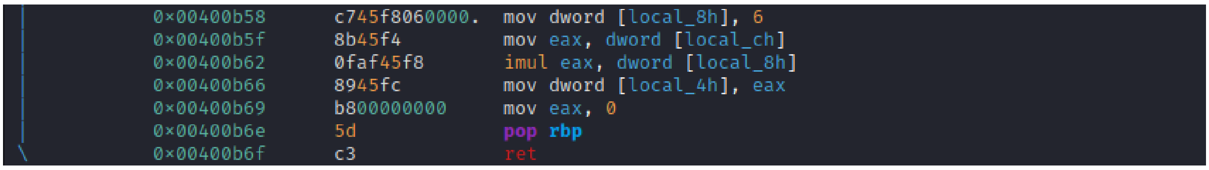
Answer: 1



```
        ; DATA XREF from 0x00400a4d (entry0)
      0x00400b4d      55             push rbp
      0x00400b4e      4889e5         mov rbp, rsp
      0x00400b51      c745f4010000.  mov dword [local_ch], 1
```

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

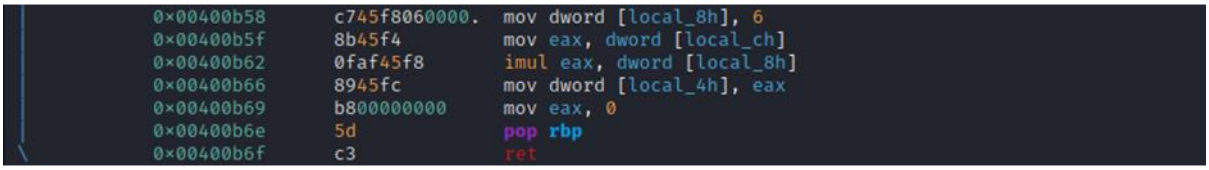
Answer: 6



```
|             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
```

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

Answer:6



```
|             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
```

METHODOLOGY

We deploy the Virtual Machine and the Kali Linux and directly open Firefox to access the website. I use the Ip address that given to me. I put the code at CMD at put the Ip address at the CMD. After that, it shows that the Ip address have two file which is ./file1 and ./challenge1. I type the code to open the file ./challenge1. After that it appear the security to login the file. We'll be using radare2 to do this - radare2 is a framework for reverse engineering and analysing binaries. We use the debugging mode for this task, so we have put the code and type "aa" So we type pdf @main and got into the data of file ./challenge1. Then, we can answer the question 5,6 and 7 using the data given to us at google form.

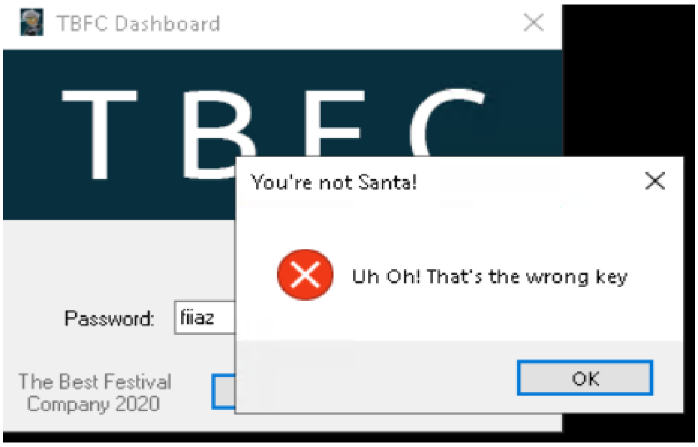
Day 18 - The Bits of Christmas

Tools used: AttackBox, Remina, ILSpy, CyberChef

Solution/Walkthrough:

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

= Uh oh! That's the wrong key



You're not Santa!

Uh Oh! That's the wrong key

Password: fiiaz

The Best Festival Company 2020

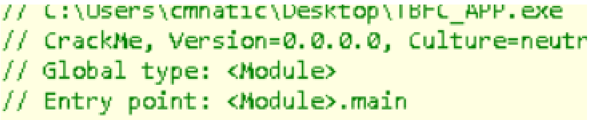
Question 2: What does TBFC stand for?

= The Best Festival Company

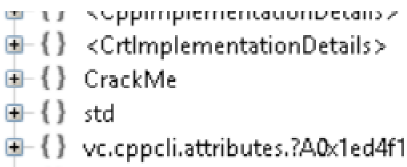
The Best Festival Company 2020

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

= CrackMe



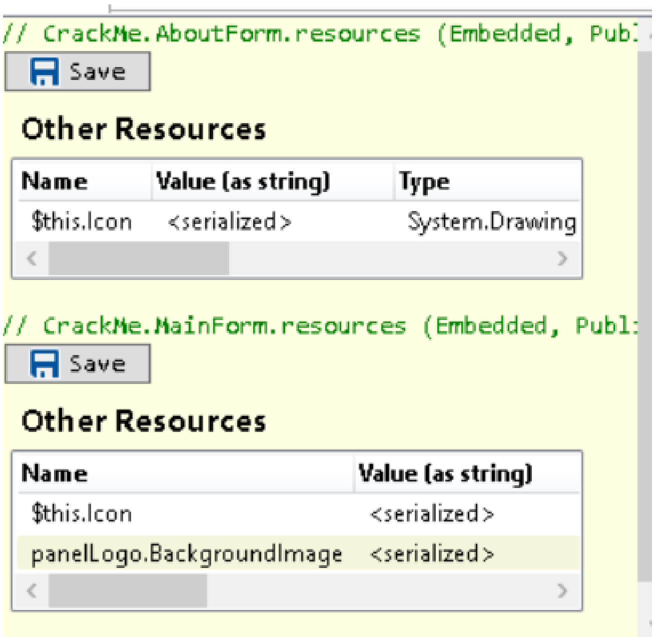
```
// C:\Users\cmnatic\Desktop\TBFC_APP.exe
// CrackMe, Version=0.0.0.0, Culture=neutr
// Global type: <Module>
// Entry point: <Module>.main
```



```
⊞ { } <CppImplementationDetails>
⊞ { } <CrtImplementationDetails>
⊞ { } CrackMe
⊞ { } std
⊞ { } vc.cppcli.attributes.?A0x1ed4f1
```

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

= MainForm



```
// CrackMe.AboutForm.resources (Embedded, Publ
```

Other Resources

Name	Value (as string)	Type
$this.Icon	<serialized>	System.Drawing

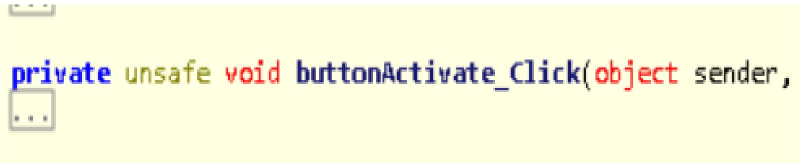
```
// CrackMe.MainForm.resources (Embedded, Publ:
```

Other Resources

Name	Value (as string)
$this.Icon	<serialized>
panelLogo.BackgroundImage	<serialized>

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

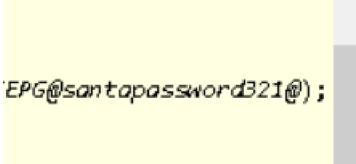
= buttonActivate_Click



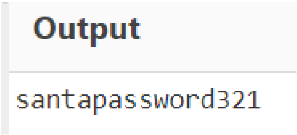
```
private unsafe void buttonActivate_Click(object sender,
...
```

Question 6: What is Santa's password?

= santapassword321



```
EPG@santapassword321@);
```

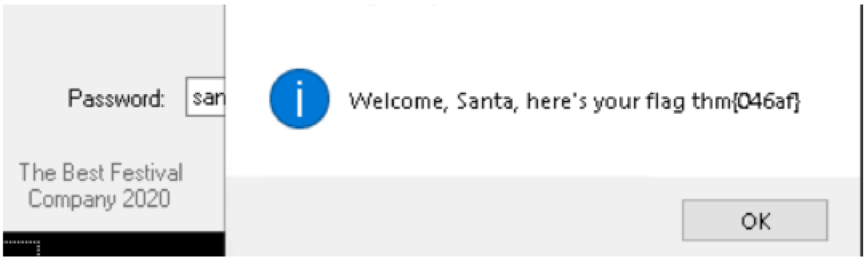


Output

```
santapassword321
```

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

= thm{046af}



Password: san

The Best Festival Company 2020

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

METHODOLOGY:

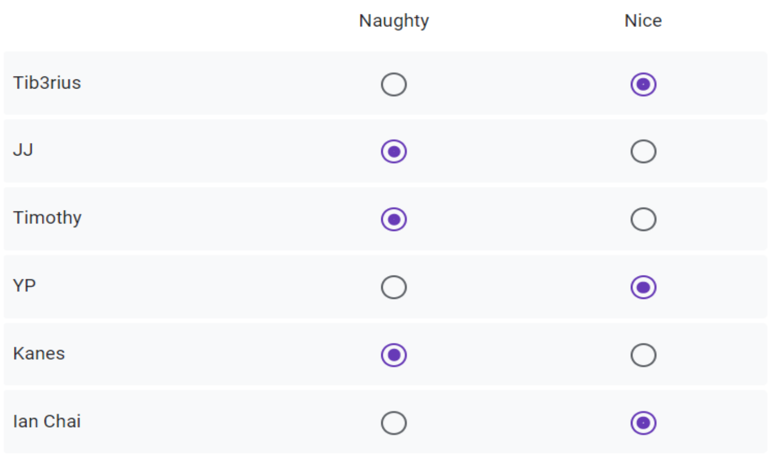
We deploy the AttackBox and VM to gain the Ip address. Then, we navigate to the "Applications" tab on the AttackBox where "Remmina" is located in the "Internet" sub-menu. Reminna will ask for a password to save sessions, we safely press "Cancel". After that, we filled out the IP address, input the Username (cmnatic) and password (Adventofcyber!) provided. Next, we open the TBFC_APP and purposedly enter the wrong password to see what message show up. We decompile the TBFC_APP with ILSpy and looking through resources in the ILSpy to answer the q3 until q7. We click the CrackMe file, went into MainForm file and reach to the buttonActivate_Click source code. We finally obtain Santa's password and the flag. To make sure the Santa's password is real, we go to the CyberChef website and put the bytes in the input, insert Hex recipe to get its output. So in the end, we try login the TBFC_APP by using the Santa's password (santapassword321) and receive the flag.

Day 19 - The Naughty or Nice List

Tools used: AttackBox, Firefox

Solution/Walkthrough:

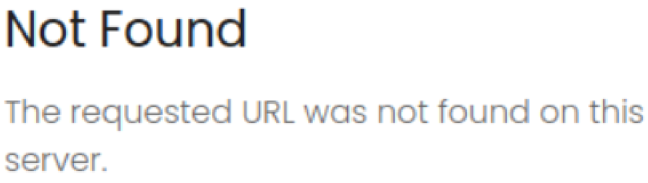
Question 1: Which list is this person on?



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

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

= Not Found. The requested URL was not found on this server.

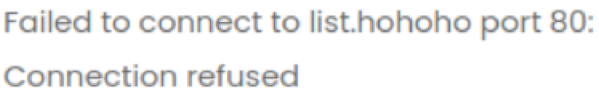


Not Found

The requested URL was not found on this server.

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

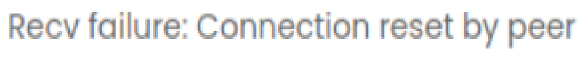
= Failed to connect to list.hohoho port 80: Connection refused



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

Question 4: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A22"?

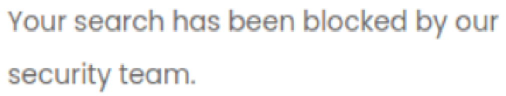
= Recv failure: Connection reset by peer



Recv failure: Connection reset by peer

<u>Question 5: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"?</u>

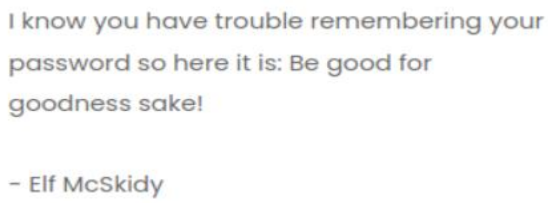
= Your search has been blocked by our security team.



Your search has been blocked by our security team.

<u>Question 6: What is Santa's password?</u>

= Be good for goodness sake!

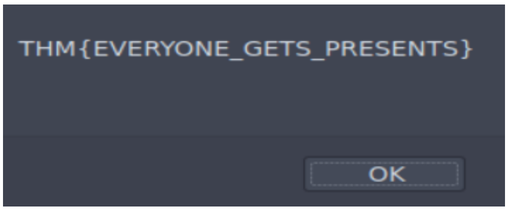


I know you have trouble remembering your password so here it is: Be good for goodness sake!

- Elf McSkidy

<u>Question 7: What is the challenge flag?</u>

= THM{EVERYONE_GETS_PRESENTS}



THM{EVERYONE_GETS_PRESENTS}

<u>METHODOLOGY:</u>

We deploy the Virtual Machine and the AttackBox and directly open Firefox to access the website The Naughty or Nice List by using the Ip address given by the VM. Next, we observe the website, enter a name in the form which is Santa and click the "Search" button then the page loads, and it tells us whether that name is on the Naughty List or the Nice List. We alternately test the name given in the google form to know which list is in the naughty or nice list. After that we tried to fetch the root of the same site by browsing to:(http://MACHINE_IP/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F) and the message shown was "Not Found. The requested URL was not found on this server." Beside that, we changed the port number from 8080 to just 80 and the message now changes to "Failed to connect to list.hohoho port 80: Connection refused". As well, we changed again the port number to 22 and now it displays "Recv failure: Connection reset by peer". Last but not least, we replaced the list.hohoho hostname with "localhost" the message returned says "Your search has been blocked by our security team." Finally, we access the local services by set the hostname in the URL to "list.hohoho.localtest.me" and quicken to finish the task by log in the admin use the Santa as the username and the password given by Elf McSkidy.

Day 20 - PowershELlF to the rescue

Tools used: AttackBox

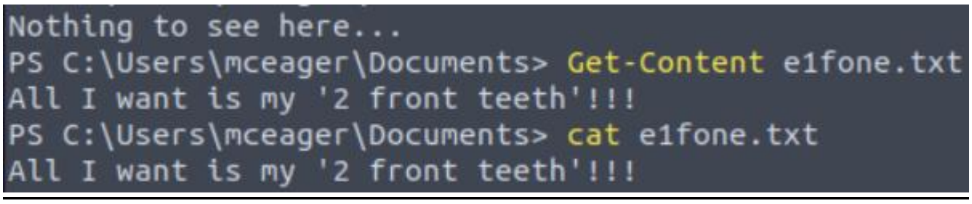
Solution/Walkthrough:

Question 1: Check the ssh manual. What does the parameter -l do?

= local host

Question 2: Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

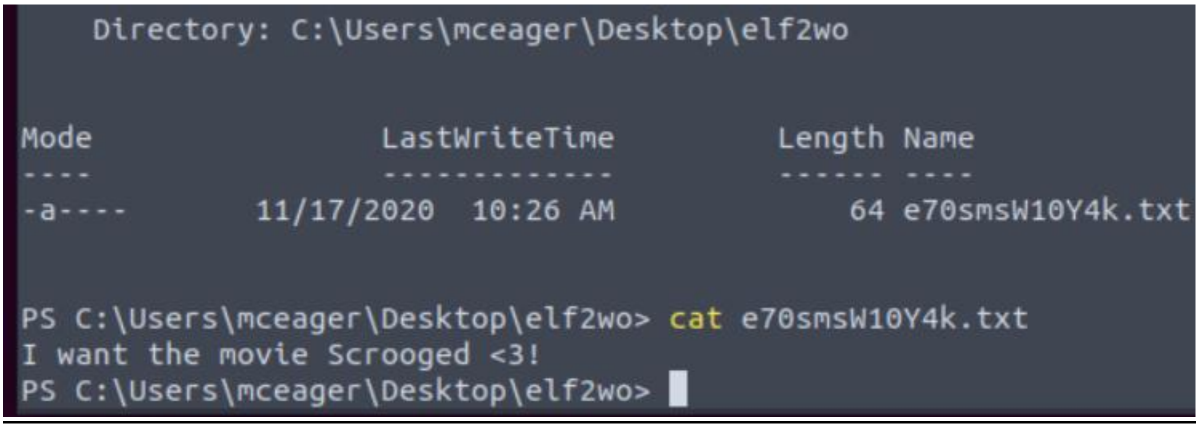
= 2 front teeth



```
Nothing to see here...
PS C:\Users\mceager\Documents> Get-Content e1fone.txt
All I want is my '2 front teeth'!!!
PS C:\Users\mceager\Documents> cat e1fone.txt
All I want is my '2 front teeth'!!!
```

Question 3: Search on the desktop for a hidden folder that contains the file for Elf 2. Read the contents of this file. What is the name of that movie that Elf 2 wants?

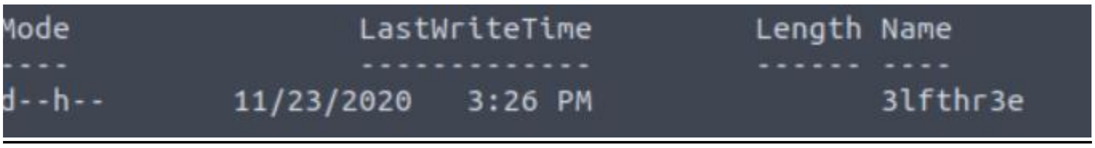
= Scrooged



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

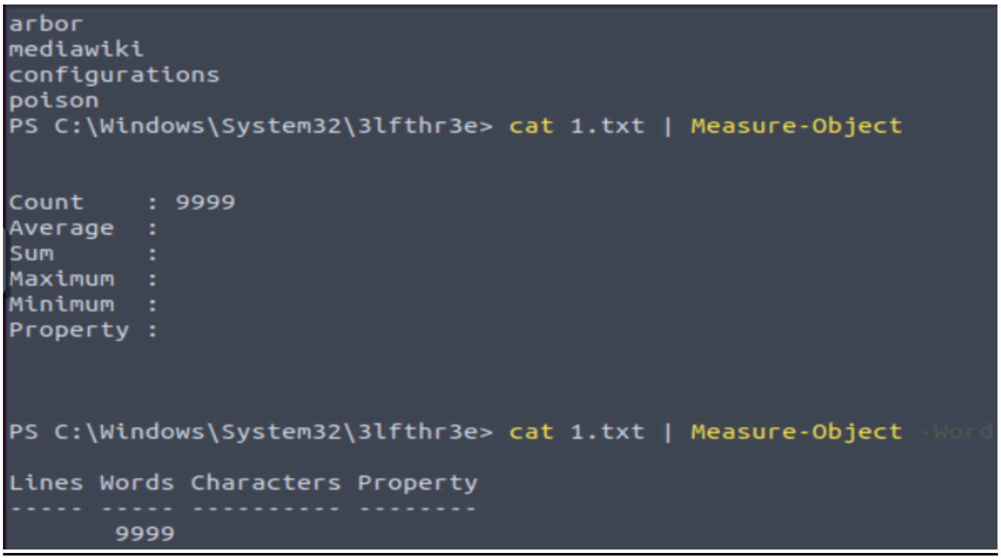
= 3lfthr3e



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

Question 5: How many words does the first file contain?

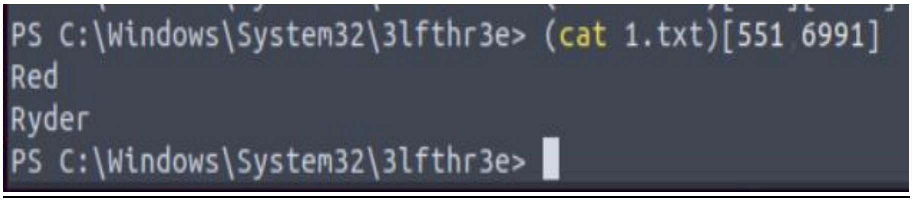
= 9999



```
arbor
mediawiki
configurations
poison
PS C:\Windows\System32\3lfthr3e> cat 1.txt | Measure-Object


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



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

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

Question 6: What 2 words are at index 551 and 6991 in the first file?

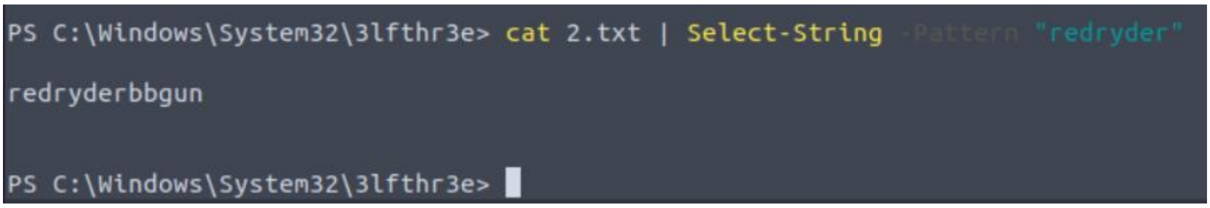
= Red Ryder



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

Question 7: This is only half the answer. Search in the 2nd file for the phrase from the previous question to get the full answer. What does Elf 3 want?

= redryderbbgun



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

redryderbbgun


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

METHODOLOGY:

We deploy the AttackBox as usual to receive the Ip address. We have been tasked to use SSH to connect to the remote machine by using command (ssh -l mceager MACHINE_IP) and then we enter the password given (r0ckStar!). We proceed to launch the PowerShell and navigate the documents folder. Furthermore, we use Get-ChildItem cmdlet to enhance its capabilities and list the contents of the current directory that we are in. Other than that, we also make use of another useful cmdlet which is Get-Content or cat to read the contents of a file and Set-Loaction cmdlet to change directories. In the end, we directly solved the task.