PSP0201

Week 5 Writeup

Group Name : Ilomilo

Members:

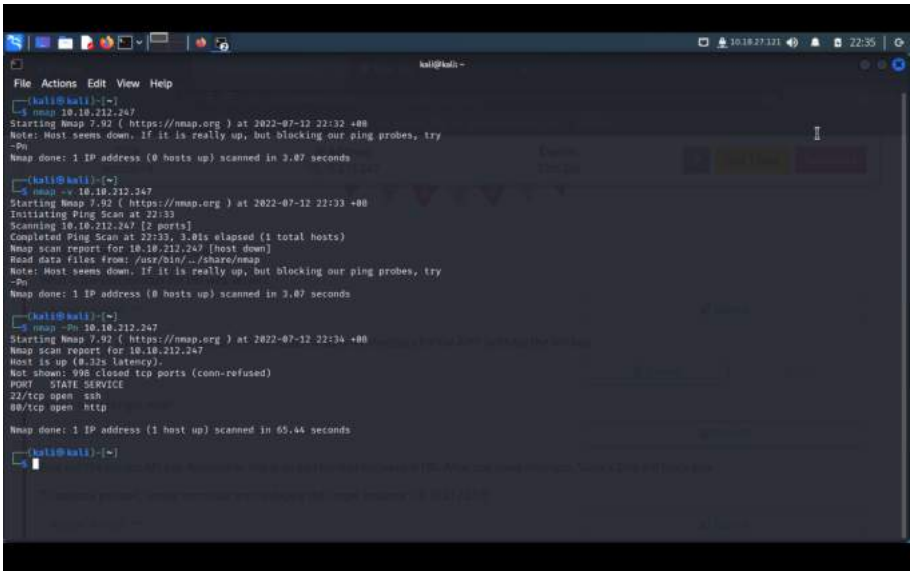
ID NUMBER	STUDENT NAME	Role
1211103196	Adriana Iman binti Noor Azrai	Leader
1211103282	Aida Maisarah binti Hisam	Member
1211103216	Sofea Hazreena binti Hasdi	Member
1211103227	Wan Alia Adlina binti Wan Azman	Member

Day 16 - Scripting Help! Where Is Santa?

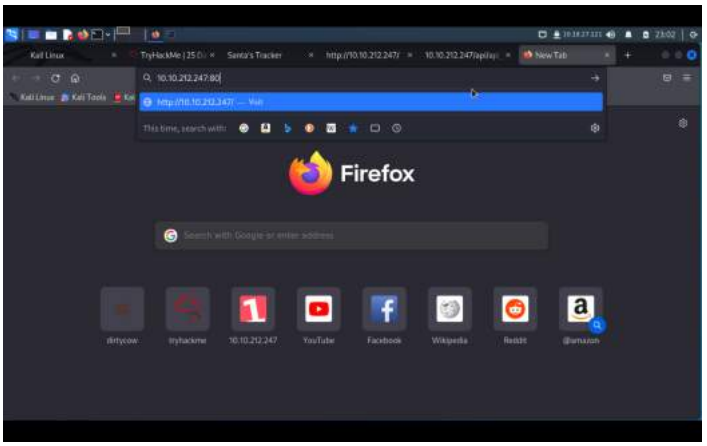
Tools Used : Kali Linux, Terminal, Firefox, Python

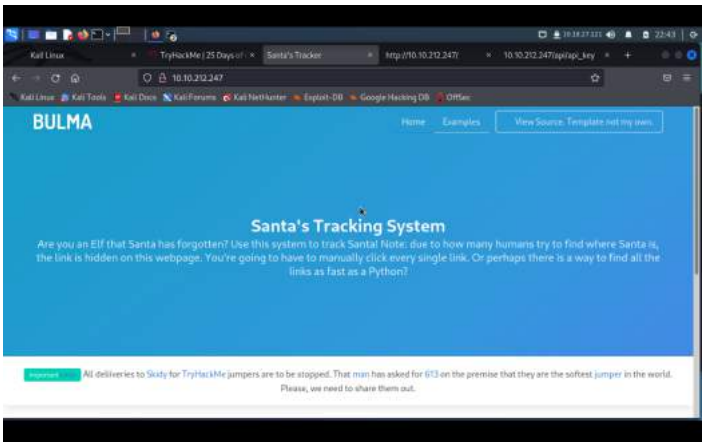
Solution/Walkthrough:

Q1: What is the port number for the web server?
Nmapping with the machine IP address, we were provided with 2 ports with ssh and http service.



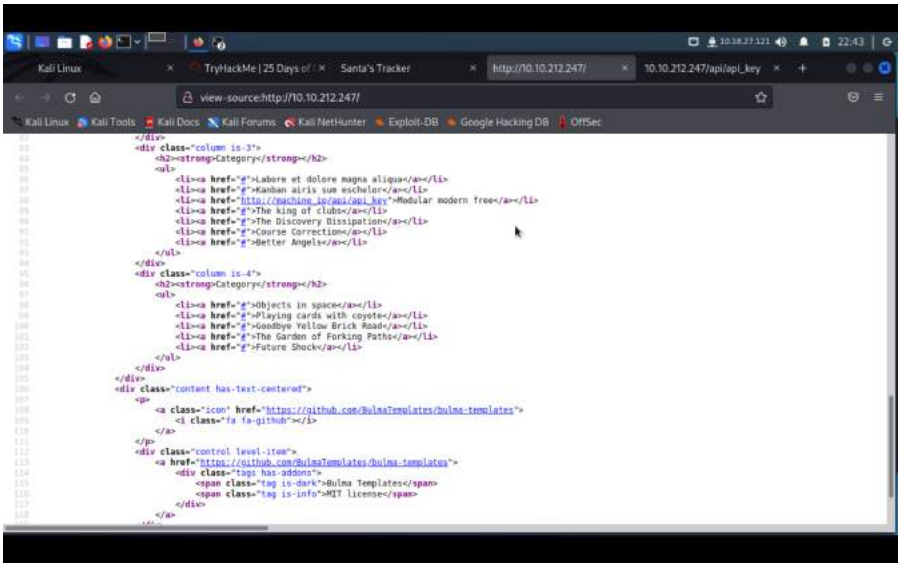
Q2: What templates are being used?
By putting the ip address along with the port, 80 we were navigated to a website called BULMA .





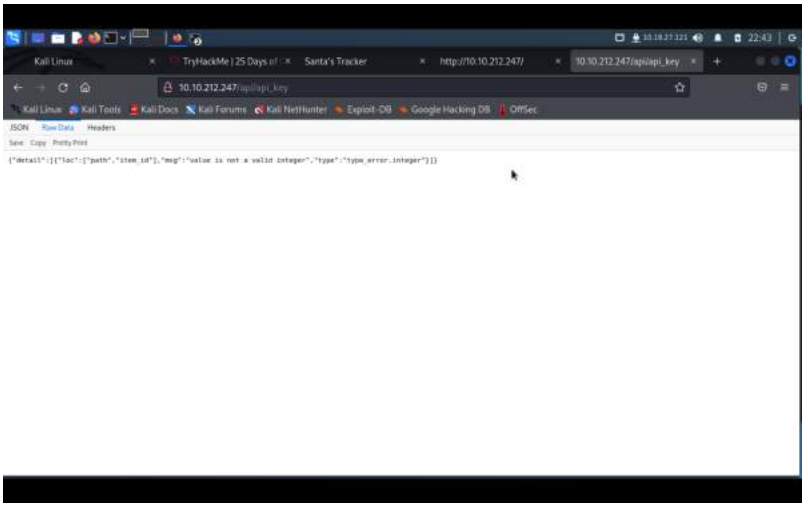
Q3: Without using enumerations tools such as Dirbuster, what is the directory for the API? (without the API key)

By clicking ‘view page source’, we were directed to the website codings where we can find the API’s directory.



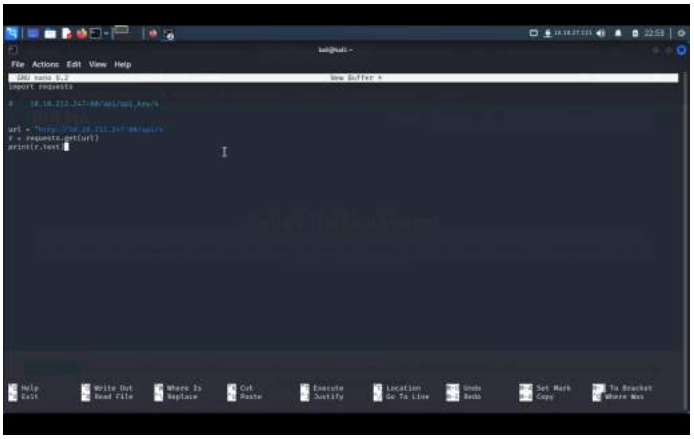
Q4: Go the API endpoint. What is the Raw Data returned if no parameters are entered?

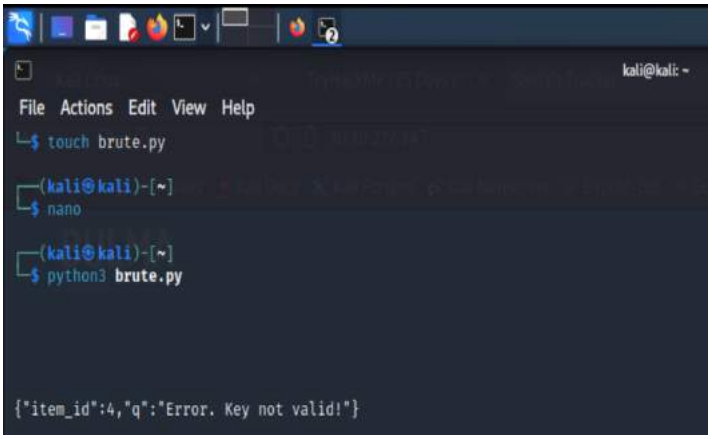
By using the link given, without parameters and using our machine IP address, we were directed to a page where it provides JSON, Raw Data and Headers of the link.

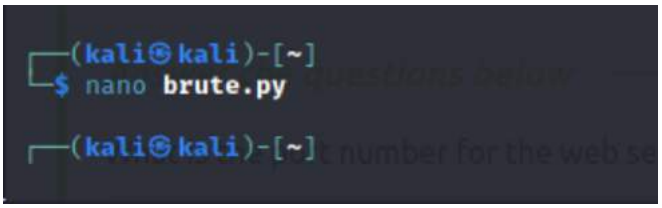


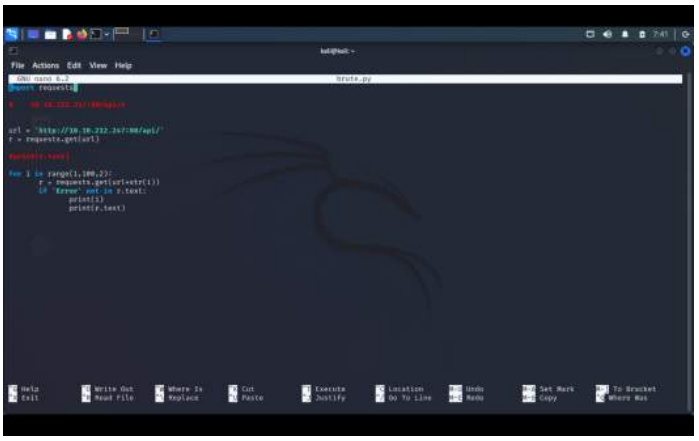
Q5: Where is Santa right now?

Opening a new file to make some coding for the python. By trying coding using url, resulting in printing out the same output as the url in Firefox. Thus, using the same way, we managed to print the place where Santa is. For the coding, by referring to TryHackMe day 15, we did our coding to get the data.



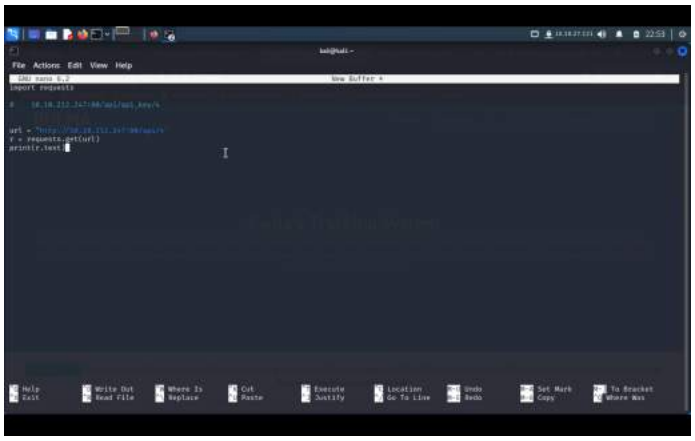


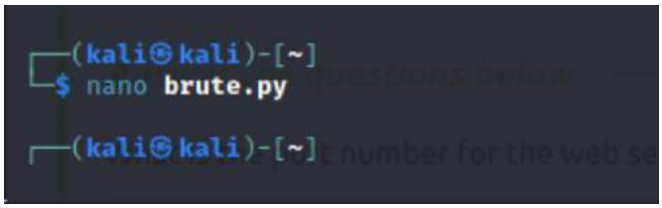


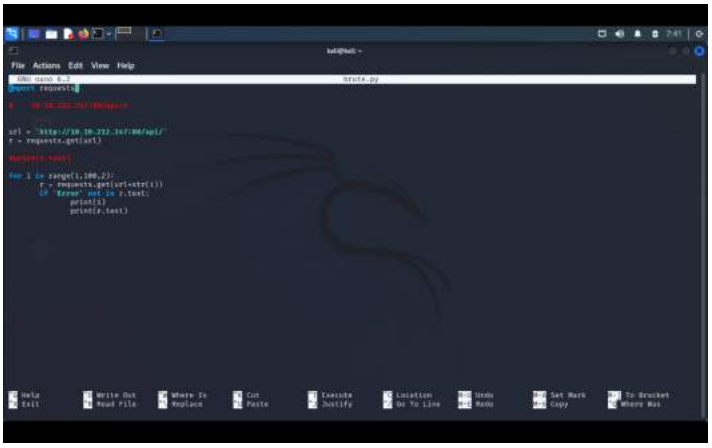


Q6: Find out the correct API key. Remember, this is an odd number between 0-100. After too many attempts, Santa's Sled will block you. To unblock yourself, simply terminate and re-deploy the target instance.

Using the same way as question 5, we managed to get the correct API key for it.







Throughout process/Methodology :

By logging in to Kali, we opened our terminal to nmap to the machine ip address. We were provided with 2 ports with ssh and http service. We choose the http so that we can use it for the website. By putting the ip address along with the port, 80 we were navigated to a website called BULMA. Then, we clicked 'view page source', and we were directed to the website coding where we can find the API's directory. By using the link given, without parameters and using our machine IP address, we were directed to a page where it provides JSON, Raw Data and Headers of the link. Then, we open a new file to make some coding for the python. By trying the coding, resulting in printing out the same output as the url in Firefox. If the output contains 'Error', they will not print the output resulting in only where Santa is as the output. Thus, using the same way, we managed to print the place where Santa is. For the coding, by referring to TryHackMe day 15, we did our coding to get the data. Lastly, using the same way as question 5, we managed to get the correct API key for it.

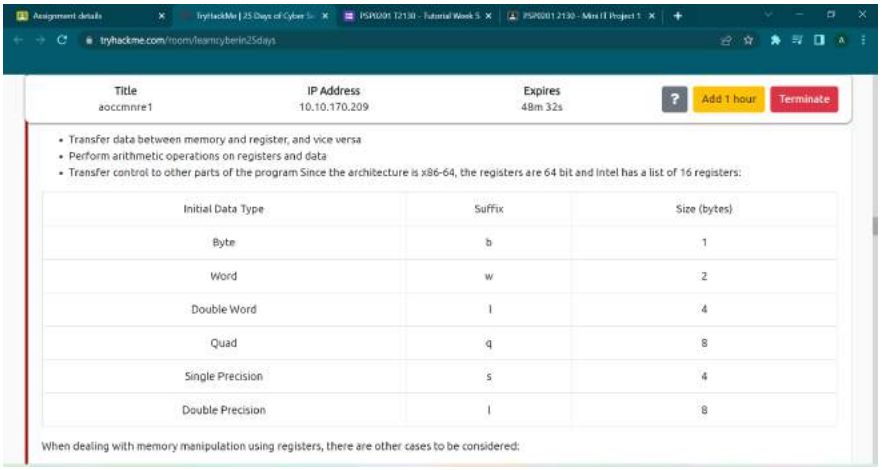
Day 17 - Reverse Engineering ReverseELFneering

Tools used: Kali Linux, Terminal, Radare2

Solution/Walkthrough:

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

This can be found in the table provided



Title	IP Address	Expires
aoccmnre1	10.10.170.209	48m 32s

Add 1 hour | Terminate

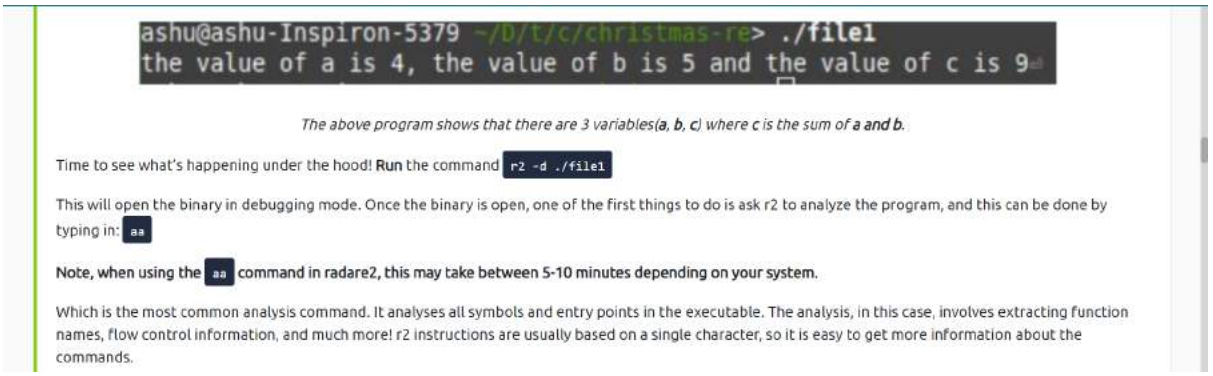
- Transfer data between memory and register, and vice versa
- Perform arithmetic operations on registers and data
- Transfer control to other parts of the program Since the architecture is x86-64, the registers are 64 bit and Intel has a list of 16 registers:

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

When dealing with memory manipulation using registers, there are other cases to be considered:

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

This also can be found in the instructions



```
ashu@ashu-Inspiron-5379 ~/D/t/c/christmas-re> ./file1
the value of a is 4, the value of b is 5 and the value of c is 9
```

The above program shows that there are 3 variables(a, b, c) where c is the sum of a and b.

Time to see what's happening under the hood! **Run** the command `r2 -d ./file1`

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`

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

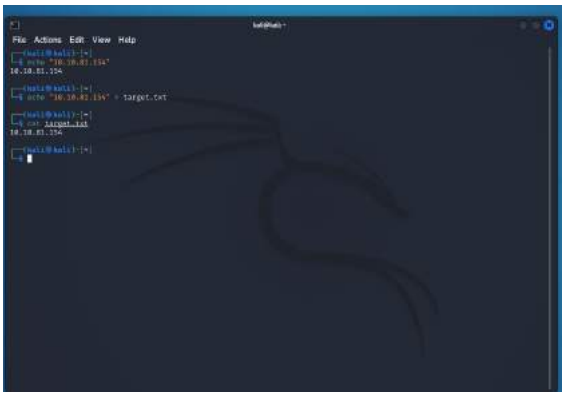
A **breakpoint** specifies where the program should stop executing. This is useful as it allows us to look at the state of the program at that particular point. So let's set a breakpoint using the command `db` in this case, it would be `db 0x00400b55` To ensure the breakpoint is set, we run the `pdf @main` command again and see a little **b** next to the instruction we want to stop at.

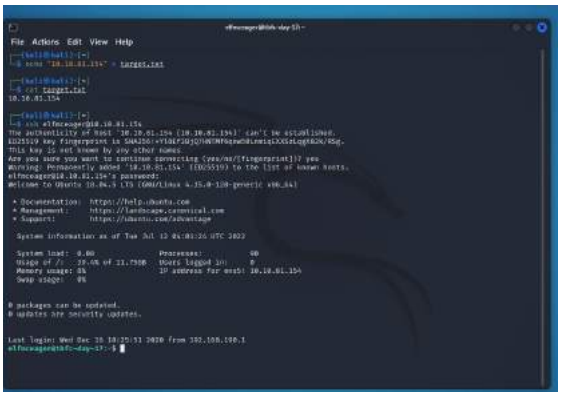
Question 4: What is the command to execute the program until we hit a breakpoint?

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-address` In this case, the corresponding memory address for `local_ch` will be `rbp-0xc` (from the first few lines of **@pdf main**) This instruction prints the values of memory in hex:

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

First, open terminal and type in echo “[ip address]” > target.txt to set our target. Then type in cat target.txt and if the output is the ip address that we have inserted just now, then we have successfully targeted our system. Then, type in ssh elfmceager@[ip address] to access that user and insert the password provided which is [adventofcyber]. Then, we have successfully logged into that user.





Then, type in the command ls and two files will show up which is challenge1 and file1

After that, type in the command r2 -d ./challenge1 to open up the binary in debugging mode.

```
elfmceager@tbfc-day-17:~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ echo "10.10.170.209" > target.txt

┌──(kali㉿kali)-[~]
└─$ cat target.txt
10.10.170.209

┌──(kali㉿kali)-[~]
└─$ ssh elfmceager@10.10.170.209
elfmceager@10.10.170.209'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 Tue Jul 12 04:57:52 UTC 2022

  System load:  0.0                Processes:           93
  Usage of /:   39.4% of 11.75GB   Users logged in:     0
  Memory usage: 8%                 IP address for ens5: 10.10.170.209
  Swap usage:   0%


0 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Tue Jul 12 04:26:22 2022 from 10.18.34.225
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1648 started...
= attach 1648 1648
bin.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits 64
[0x00400a30]>
```

Then, type in the command aa to analyse the program

```
elfmceager@tbfc-day-17:~
File  Actions  Edit  View  Help
0 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Tue Jul 12 04:26:22 2022 from 10.18.34.225
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1648 started...
= attach 1648 1648
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)
```

Type in pdf@main to examine the assembly code at main.

```
elfmceager@tbfc-day-17:~
File  Actions  Edit  View  Help
0 packages can be updated.
0 updates are security updates.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings


Last login: Tue Jul 12 04:26:22 2022 from 10.18.34.225
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1648 started...
= attach 1648 1648
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]> 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      8b05f4         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
[0x00400a30]>
```

From the output, we can see several [local_ch] so we take the first movl instruction which is the number beside the local_ch

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

Based on the output of pdf@main, the value of eax is obtained by multiplying 1 with 6 based on the values of local_ch

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

For this one, we just take the answer from before as it is set before eax is 0

Throughout process/Methodology :

First, open terminal and type in echo “[ip address]” > target.txt to set our target. Then type in cat target.txt and if the output is the ip address that we have inserted just now, then we have successfully targeted our system. Then, type in ssh elfmceager@[ip address] to access that user and insert the password provided which is [adventofcyber]. We have successfully logged into that user. Then, type in the command ls to check any files that is saved by that user and two files should show up which is challenge1 and file1. After that, type in the command r2 -d ./challenge1 to open up the binary in debugging mode. Then, type in the command aa to analyse the program. Type in pdf@main to examine the assembly code at main after analysing is done. From the output, we can see several [local_ch] so we take the first movl instruction which is the number beside the local_ch. Based on the output of pdf@main, the value of eax is obtained by multiplying 1 with 6 based on the values of local_ch. Finally, we just take the answer from before as it is set before eax is set to 0.

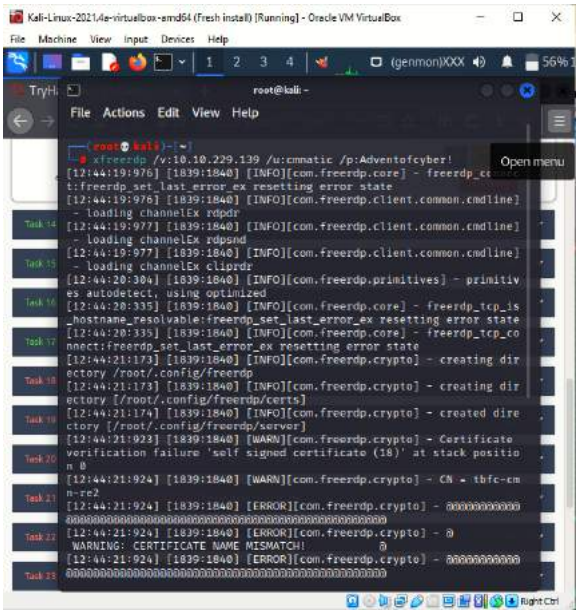
Day 18 - Reverse Engineering The Bits of Christmas

Tools used: Terminal, FireFox, ILSpy

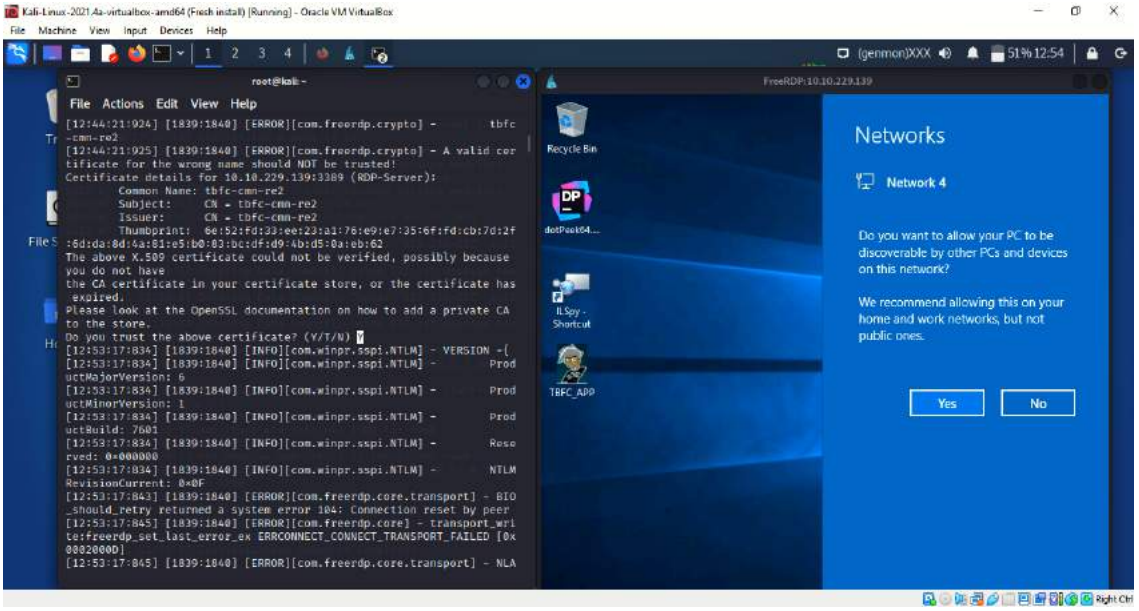
Solution/Walkthrough:

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

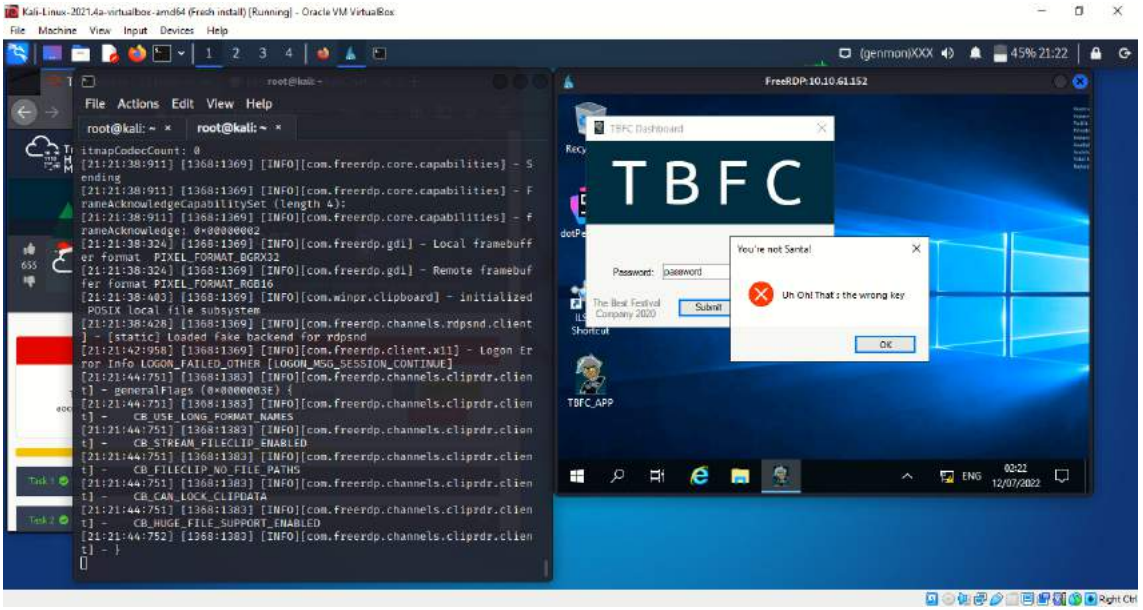
We connect the remote desktop by using xfreerdp, in the terminal we run the command in the form of xfreerdp, Ip address, Username and Password.



The problem with the certificate appears and we enter Y to agree to trust the certificate. Then, the remote desktop is connected via RDP and the window appears.

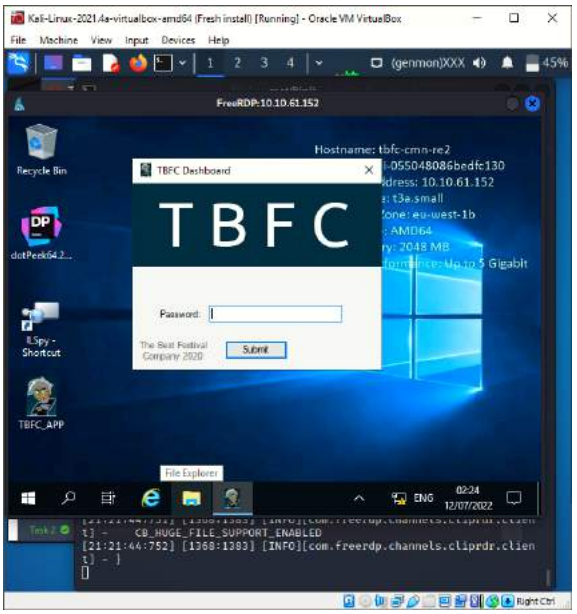


Double click at the TBFC_APP icon and TBFC Dashboard appears. Type in any word in the password box and click submit. The message shows up.



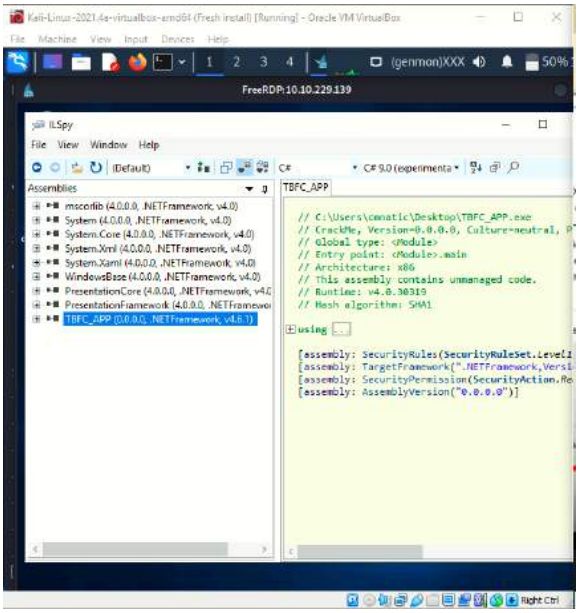
Question 2: What does TBFC stand for?

Using the same way as question 1. Beside the submit button, a long form of TBFC is shown there.



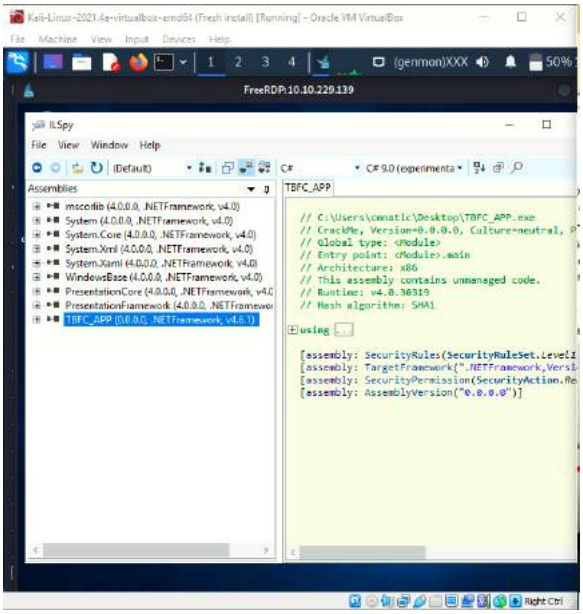
Question 3: Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?

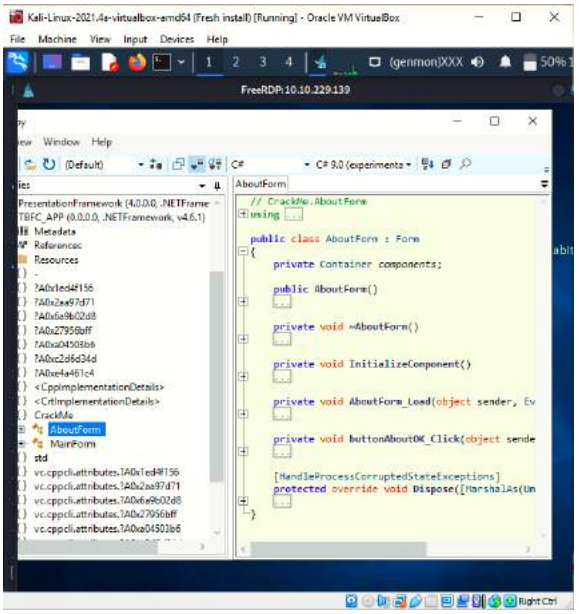
Double click on the ILSpy-Shortcut icon and we need to load TBFC_APP by clicking on the file and choose open. Click the desktop icon and select TBFC_APP. Then it loaded at the assemblies panel. The module is CrackMe, and it contains Metadata.



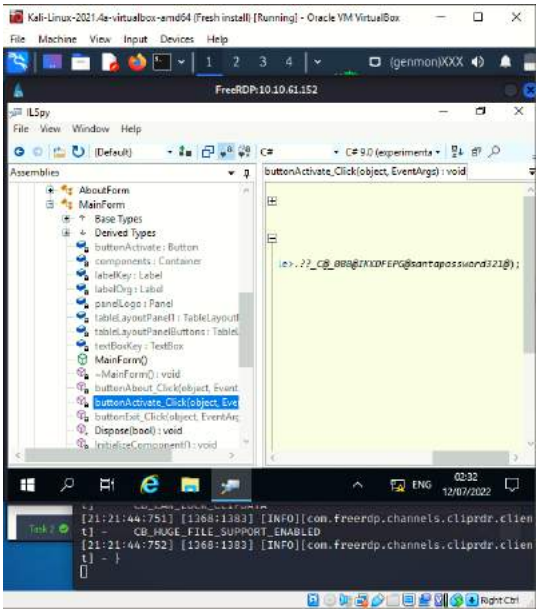
Question 4: Within the module, there are two forms. Which contains the information we are looking for?

In the assemblies panel, click on the '+' icon at TBFC_APP to expand. Then, we expand the Crackme by clicking the plus sign. It shows AboutForm and MainForm. When we click at the AboutForm it appears as a sort of function. Next, we click on the MainForm and it shows the source code behind the application.



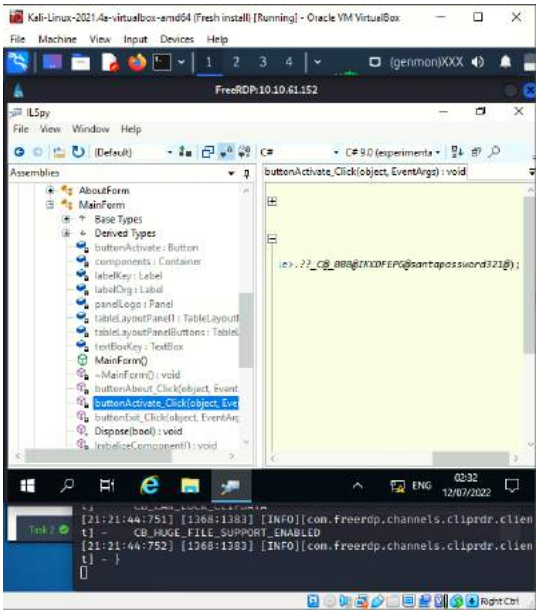


Next, we click on the MainForm and it shows the source code behind the application.



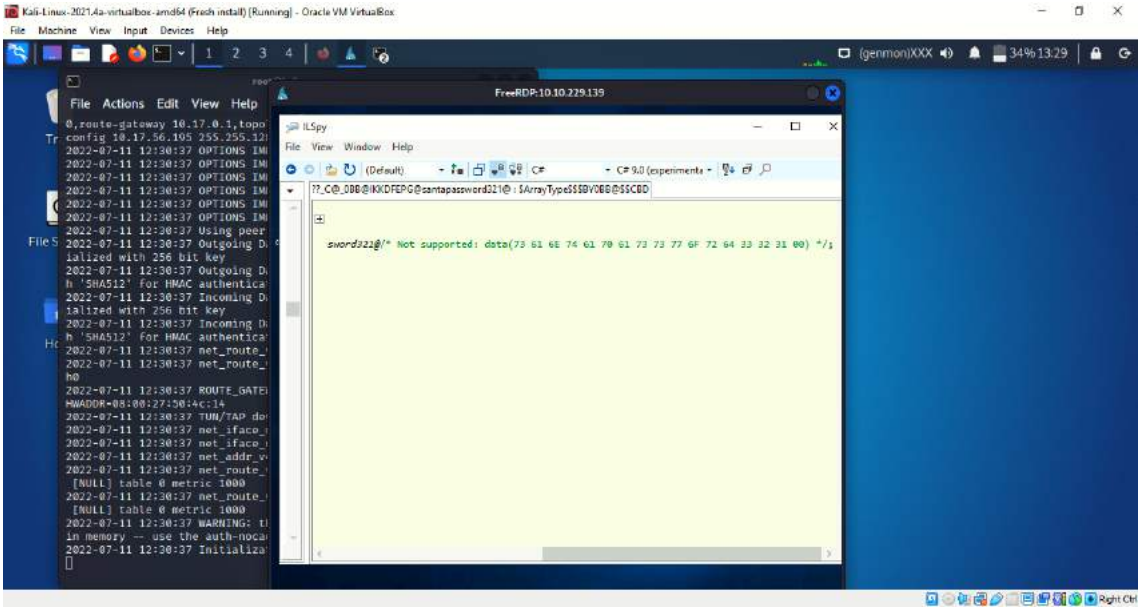
Question 5: Which method within the form from Q4 will contain the information we are seeking?

After we expand the MainForm, we go to the specific under the Derived Types. Click on the buttonActivate and it shows the function that executes after we click any button at the TBFC dashboard. All the message, flag and password is shown in the source code.

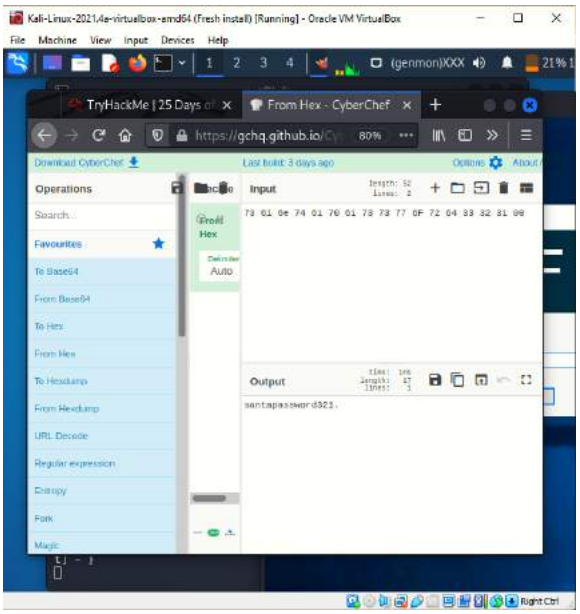


Question 6: What is Santa's password?

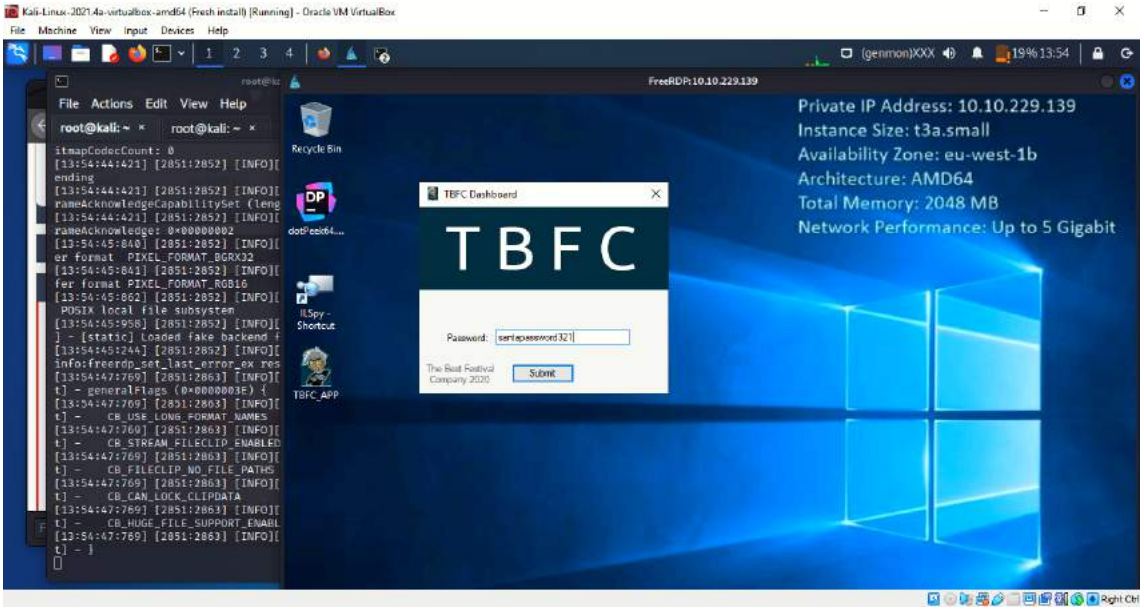
The solution is the same as question 6 and we continue by clicking at the password to make sure it is the information that we want and ILSpy will locate us to the data inside the hyphen icon. It is given a clue that it is hexadecimal and we need to convert it.



We select all and copy. Open Cyberchef in Firefox, paste it in the input section. Then, drag the 'From Hex' to the recipe. The output shows the password.

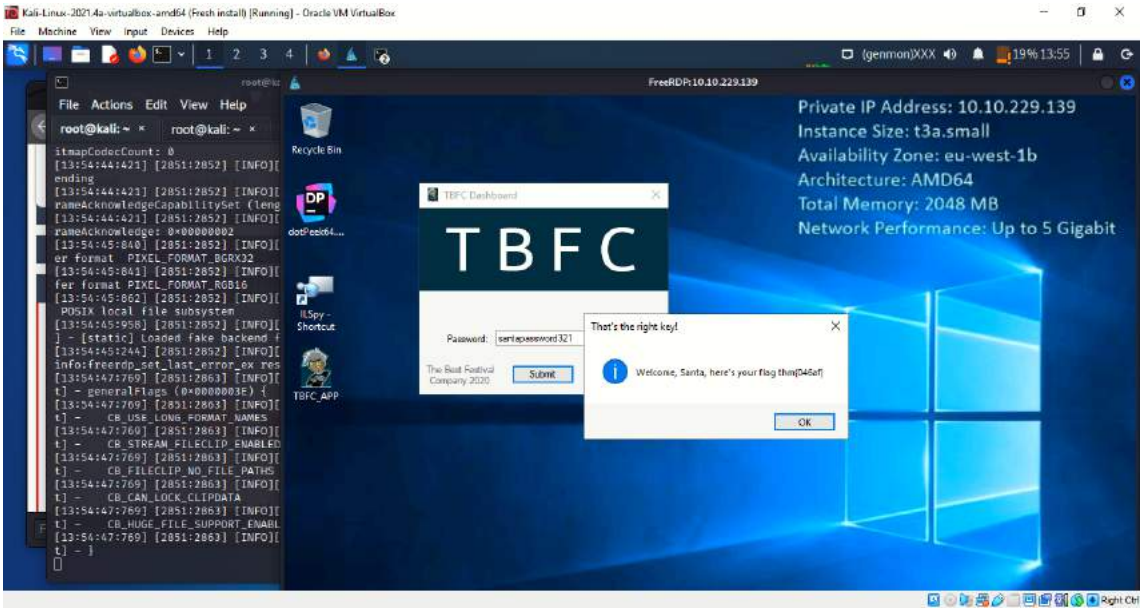


Double click the TBFC_APP icon and paste in the password.



Question 7: Now that you've retrieved this password, try to login...What is the flag? *
Copy and paste from THM

The same way as the previous question. We type in the password and click submit. The flag is shown in the message box.



Throughout process/Methodology :

Using xfreerdp, we connect to the remote desktop by running the command xfreerdp, IP address, Username, and Password in the terminal. The issue with the certificate is displayed, and we type Y to accept the certificate. The remote desktop is then linked using RDP, and the window is displayed. We double-click the TBFC APP icon, the TBFC Dashboard displays. Enter any word in the password field and press the submit button. The message appears. In the same way as in question 1, a long form of TBFC is displayed next to the submit button. Double click on the ILSpy-Shortcut icon and we need to load TBFC_APP by clicking on the file and choose open. Select TBFC APP from the desktop icon. It was then loaded at the assembly panel. CrackMe is the module, and it contains Metadata. To expand TBFC APP in the assemblies panel, click the '+' symbol. The Crackme is then expanded by clicking the + sign. It displays the AboutForm and MainForm forms. When we click on the AboutForm button, it displays the function. When we click on the MainForm, the source code for the application is displayed. We proceed to the particular under the Derived Types when we expand the MainForm. When we click the buttonActivate, it displays the function that is executed when we click any button on the TBFC dashboard. The source code displays the entire message, flag, and password. We proceed by clicking on the password to ensure that it is the information we need, and ILSpy will direct us to the data contained within the hyphen icon. It is indicated that it is hexadecimal and that we must convert it. We choose everything and copy it. Open Cyberchef in Firefox and paste the code into the input field. After that, drag the 'From Hex' to the recipe. The password is displayed in the output. Copy and paste the password into the TBFC_APP icon. We enter the password and press the submit button. The flag can be seen in the message box.

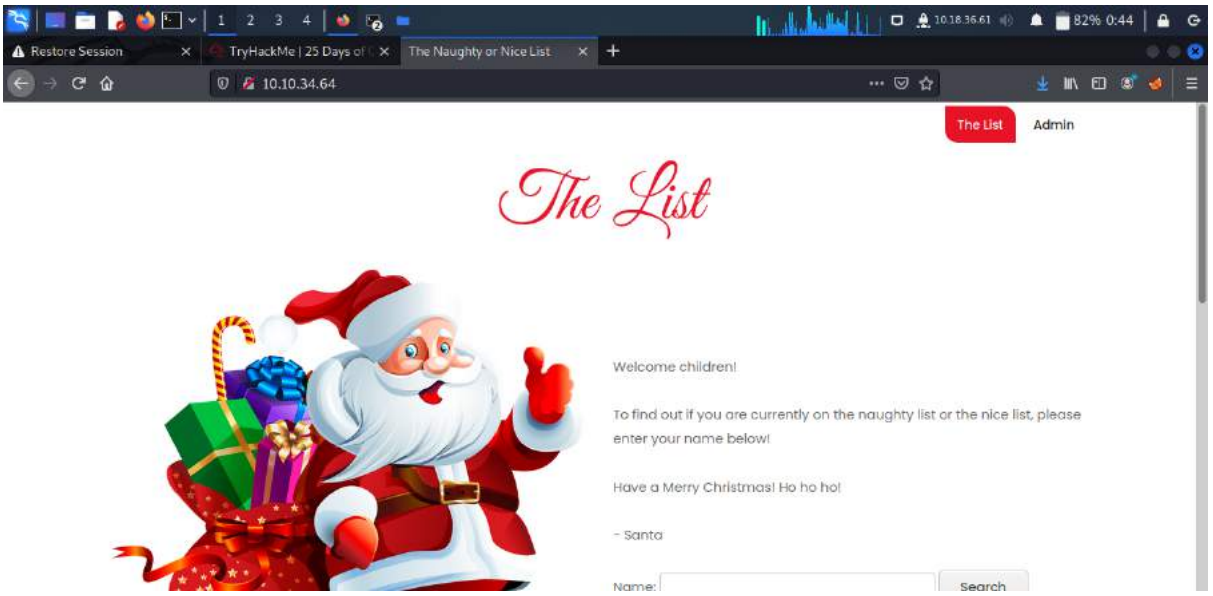
Day 19 - Web Exploitation The Naughty or Nice List

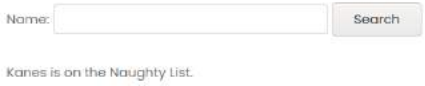
Tools used: kali, terminal, firefox

Solution/Walkthrough:

Question 1 : Which list is this person on? Select the proper words in the proper place of the command: [a] -c -z file,[b] http://[c].xyz/api.[d]?[e]=FUZZ

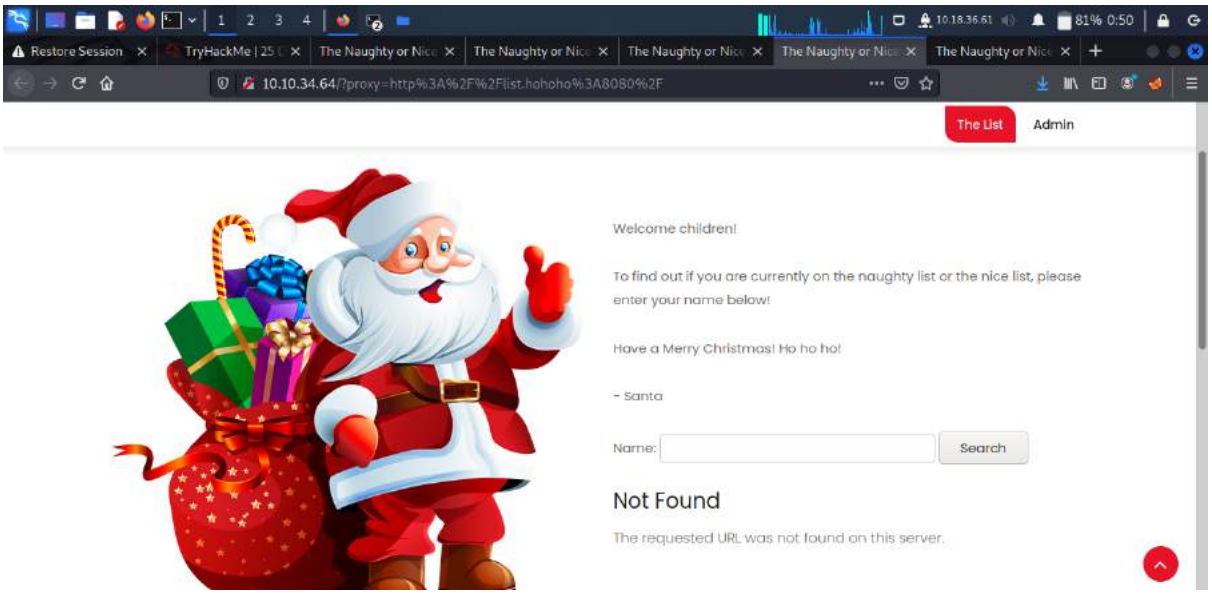
First we connect to the web app by entering the ip machine given. We then were directed to the Naughty or Nice List. we then entered the name in the name box below and got the result.





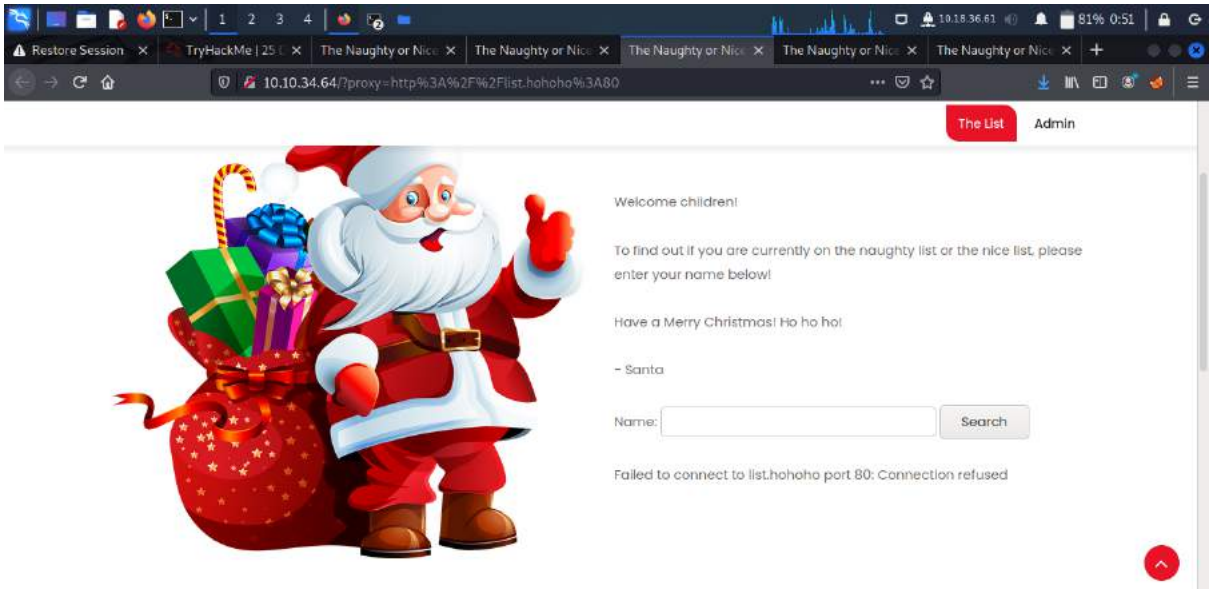
Question 2 : What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"? Copy and paste from THM

When we browsed to the URL, we were displayed that message.



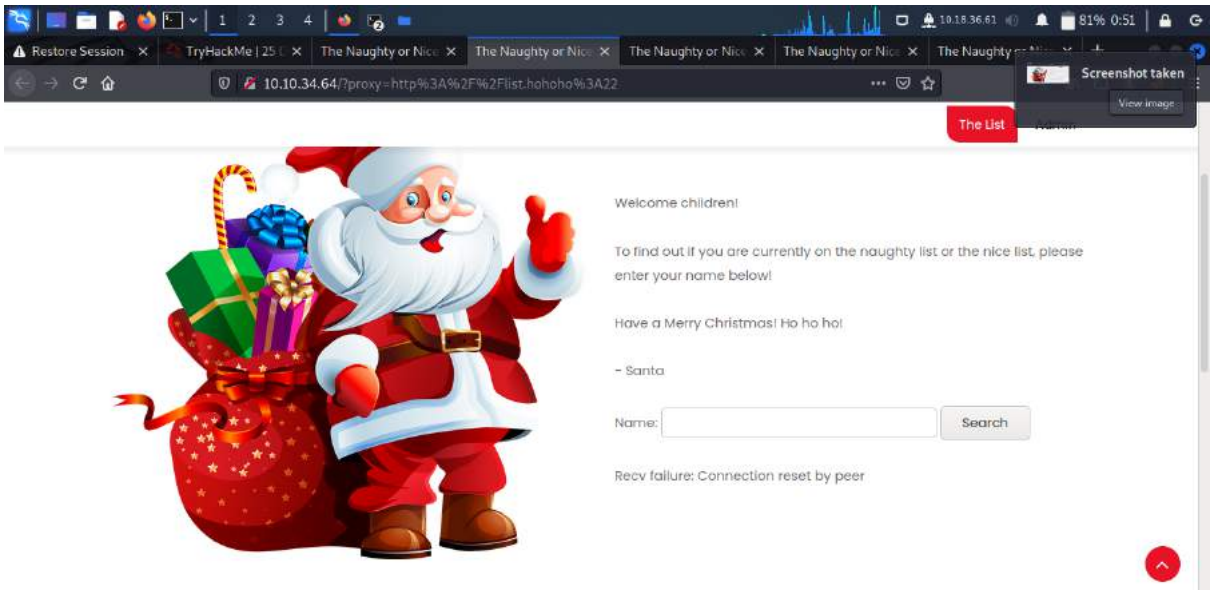
Question 3 : What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A80"? Copy and paste from THM

We then browsed to the URL given.



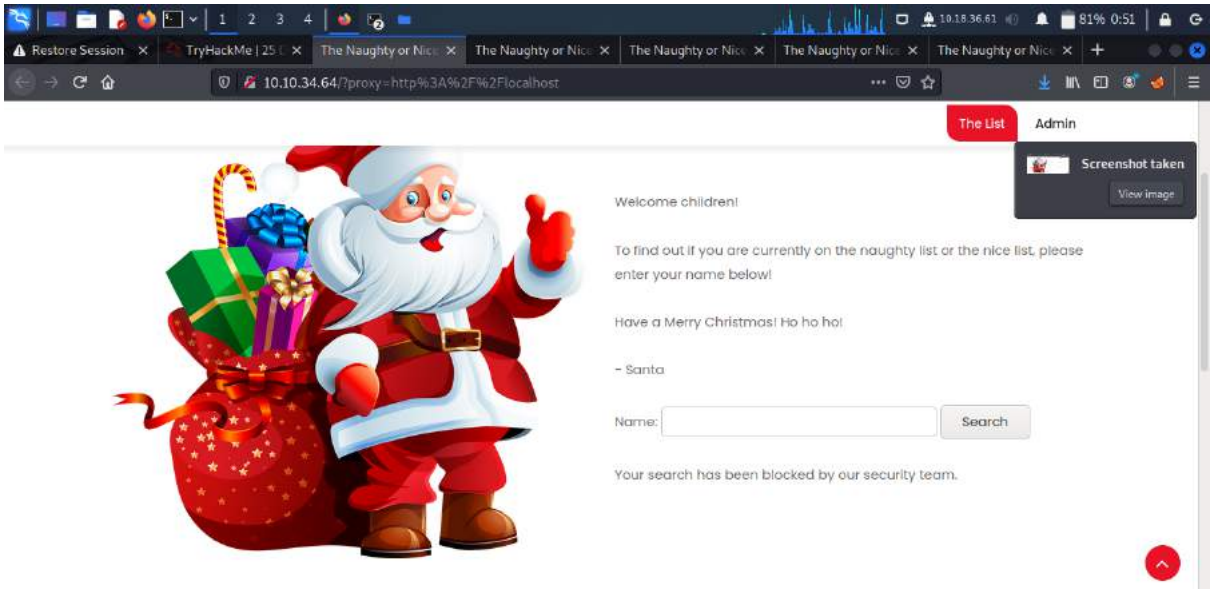
Question 4 : What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A22"? Copy and paste from THM

Then we browsed the given URL.



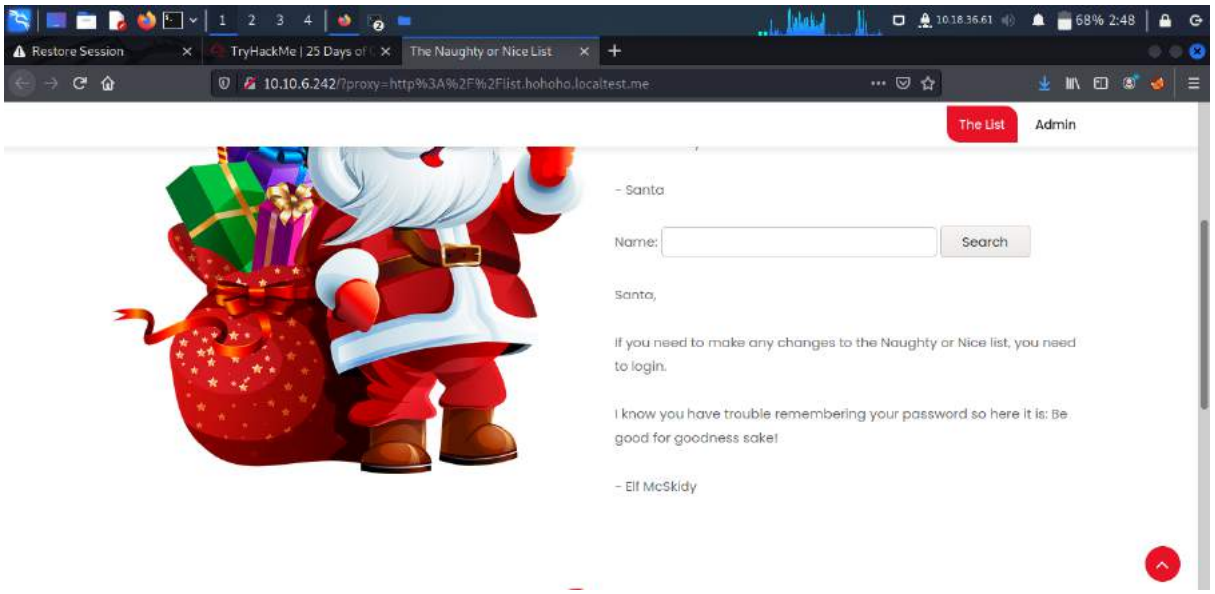
Question 5 : What is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"? Copy and paste from THM

Then we browsed the given URL.



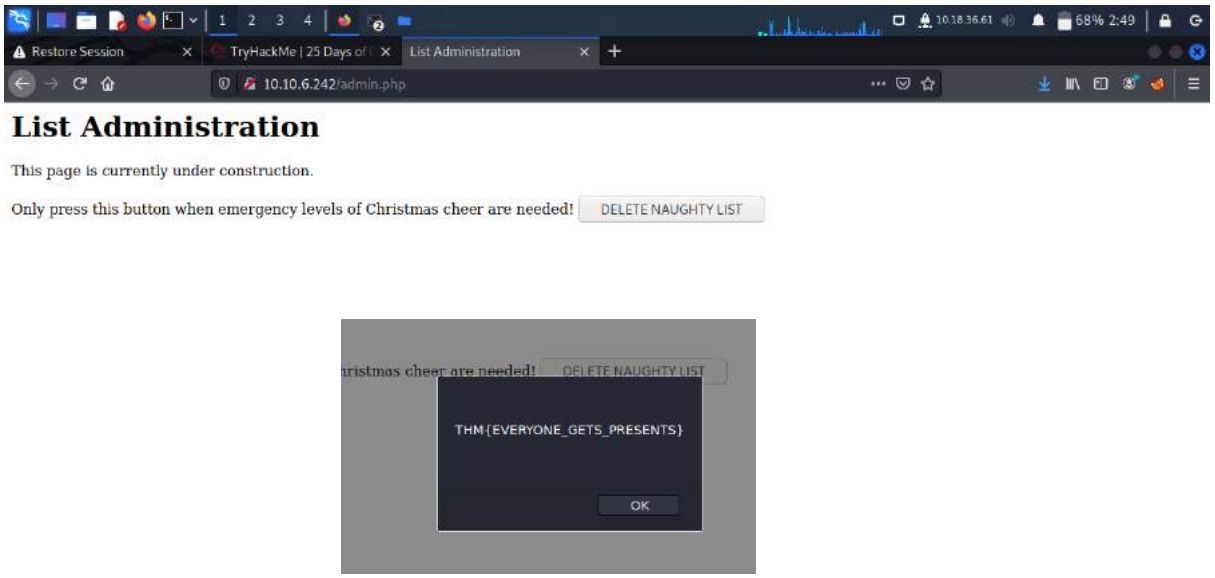
Question 6 : What is Santa's password?

The one we will be using is localtest.me, which resolves every subdomain to 127.0.0.1. We can therefore set the hostname in the URL to "list.hohoho.localtest.me", bypass the check, and access local services; ?proxy=http%3A%2F%2Flist.hohoho.localtest.me
Then we were directed to a page that had Elf Mcskidy's message which contained Santa's password.



Question 7 : What is the challenge flag?

We then log in as Santa. After that we were directed to the List Administration. Pressed the 'DELETE NAUGHTY LIST' button and we received the flag.



Throughout process/Methodology :

We first deploy the machine and after receiving the ip address, we browse the web page. Then we were directed to the “Naughty or Nice List”. There is a box where we can input names to see whether the name is in the naughty or the nice list. So we entered all the names given which are, YP, Tib3rius, Timothy, JJ, Kanes and Ian Chai and got to know whether they are in the naughty or the nice list. Next, we browse “/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F” URL and are displayed “Not Found. The requested URL was not found on this server.” Next we browse "/?proxy=http%3A%2F%2Flist.hohoho%3A80" and were displayed “Failed to connect to list.hohoho port 80: Connection refused”. Next we browse "/?proxy=http%3A%2F%2Flist.hohoho%3A22" and were displayed “Recv failure: Connection reset by peer”. Next we browse "/?proxy=http%3A%2F%2Flocalhost" and were displayed “Your search has been blocked by our security team.“ next we browse “?proxy=http%3A%2F%2Flist.hohoho.localtest.me” and were given a message from Elf Mcskidy with Santa’s password. We logged in as Santa in the admin site with the password given and were directed to a page where there is a button to delete the naughty list. Pressing that button, we then got the flag.

Day 20 - Blue Teaming PowershELlF To The Rescue

Tools used: kali, powershell

Solution/Walkthrough:

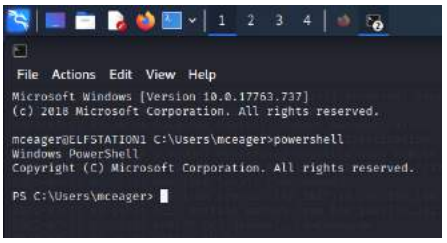
Question 1 : Check the ssh manual. What does the parameter -l do?

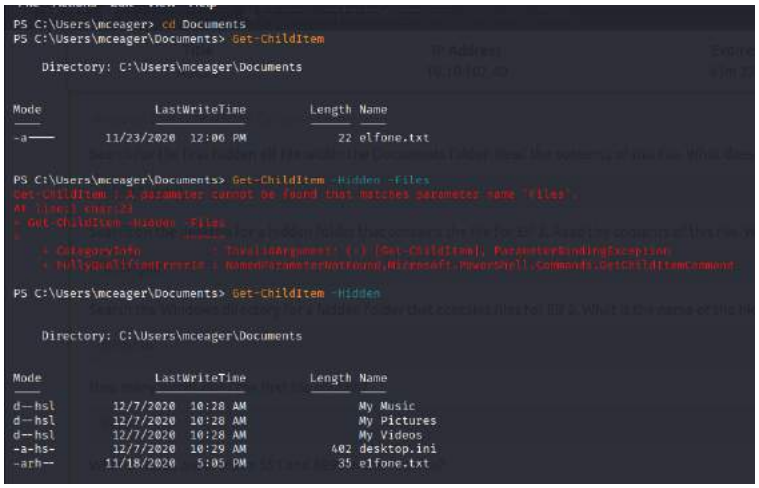
Checking the ssh manual, we can see the -l parameter function.

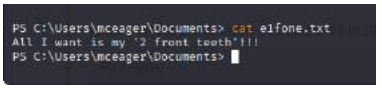
- -l — displays the details of the files, such as size, modified date and time, the owner, and the permissions.

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

We first deploy the machine and open the powershell. Logging in as mceager by using ssh, we activate powershell. We then use cd command to go to the Documents folder and use the Get-ChildItem command with -Hidden parameter to see what's hidden inside the folder. There we found a file of elf 1 named “e1fone.txt”. Using the cat command, we can open the content of the file.

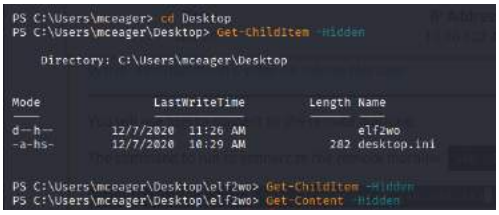


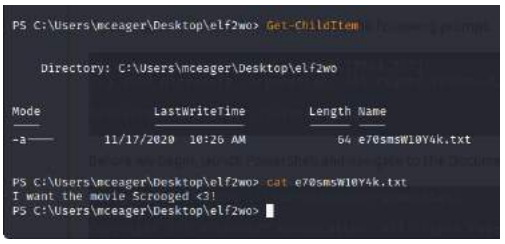




Question 3 : Search on the desktop for a hidden folder that contains the file for Elf 2. Read the contents of this file. What is the name of that movie that Elf 2 wants?

Next, we use the command cd to change the location to Desktop and then use the Get-ChildItem command with -Hidden parameter to find the hidden folder. We then find a folder named elf2wo so using the cd command again, we are in the elf2wo folder. Using the Get-ChildItem command, we then see a file named e70smsW10Y4k.txt so we open it using cat command and get to see the movie name that elf 2 wants.



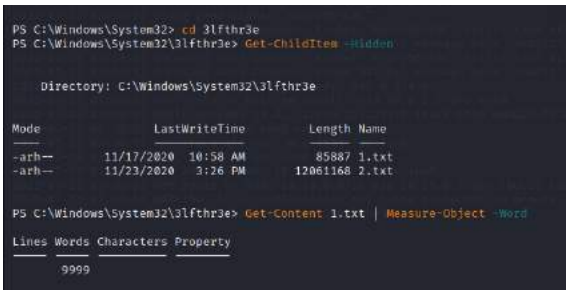


Question 4 : Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder? (This command will take a while)

After that, we change the directory to Windows by using the cd command and entering the system32 by using cd command again. We then use the Get-ChildItem command with -Hidden, -Directory and -Filter “*3*” parameter to find the hidden folder named 3lfthr3e.

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

Using the cd command, we go to the 3lfthr3e folder and then use the Get-ChildItem command with -Hidden parameter to see the files in the folder. Then we use the Get-Content command to see the contents of the first file and pipe the result by using Measure-Object with -Word parameter to see how many words does the first file contain.



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

To see the exact position in this file, we use the Get-Content parameter in a bracket to open the first file and using the square brackets to put the index.

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

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? (use spaces when submitting the answer)

Using the Get-Content command, we open the second file and pipe the result using Select-String with -Pattern “redryder” parameter to find what elf 3 wants.

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

redryderbbgun


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

Throughout process/Methodology :

We first deploy the machine to get the ip address and open the powershell. Logging in as mceager by using ssh, we activate the powershell. We then use cd command to go to the Documents folder and use the Get-ChildItem command with -Hidden parameter to see what's hidden inside the folder. There we found a file of elf 1 named “e1fone.txt”. Using the cat command, we can open the content of the file. Next we use the cd command to to change the location to Desktop and then use the Get-ChildItem command with -Hidden parameter to find the hidden folder. We then find a folder named elf2wo so using the cd command again, we are in the elf2wo folder. Using the Get-ChildItem command, we then see a file named e70smsW10Y4k.txt so we open it using cat command and get to see the movie name that elf 2 wants. After that, we change the directory to Windows by using the cd command and entering the system32 by using cd command again. We then use the Get-ChildItem command with -Hidden, -Directory and -Filter “*3*” parameter to find the hidden folder named 3lfthr3e. Next, we use the cd command to enter the 3lfthr3e folder and then use the Get-ChildItem command with -Hidden parameter to see the files in the folder. Then we use the Get-Content command to see the contents of the first file and pipe the result by using Measure-Object with -Word parameter to see how many words does the first file contain. To see the exact position in this file, we use the Get-Content parameter in

a bracket to open the first file and use the square brackets to put the index. After that, using the Get-Content command, we open the second file and pipe the result using Select-String with -Pattern “redryder” parameter to find what elf 3 wants.