

PSP0201

Week 5

Writeup

Group Name: 3 Ekor

Members

ID	Name	Role
1211103546	Muhammad Hafiz Haziq Bin Aminuddin	Leader
1211103298	Fahiman Danial Bin Harman Sham	Member
1211103527	Muhammad Irfan Haqief Bin Razak	Member

Day 16: Scripting - Help! Where is Santa?.

Tools used: Firefox, Linux Kali, BPython, Terminal, Text Editor

Solution/walkthrough:

Q1: What is the port number for the web server?

STEP 1 and ANSWER FOR Q1

Open Terminal and use nmap with the IP address provided to see the available port number. For http protocol, the port number 80 is available

```
(1211103527㉿kali)-[~]
$ nmap 10.10.220.26
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-04 11:29 EDT
Nmap scan report for 10.10.220.26
Host is up (0.20s 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 30.98 seconds
```

Q2: What templates are being used?

STEP 2 and ANSWER FOR Q2

Use the IP address and open it in Firefox. The website will open and show the templates used at the top left corner of the website

The screenshot shows a web page with a blue header containing the word "BULMA". Below the header, the main content area has a blue background. The title "Santa's Tracking System" is centered in white text. Below the title is a paragraph of text: "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?" At the bottom of the page, there is a footer with three columns of links under the heading "Important".

Important All deliveries to Skidy for TryHackMe jumpers are to be stopped. That man has asked for 613 on the premise that they are the softest jumper in the world. Please, we need to share them out.

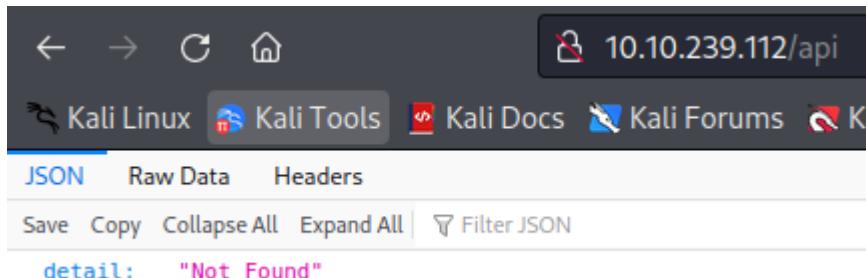
Category	Category	Category
Lore ipsum dolor sit amet	Labore et dolore magna aliqua	Objects in space
Vestibulum errato isse	Kanban airis sum eschelor	Playing cards with coyote
Lorem ipsum dolor sit amet	Modular modern free	Goodbye Yellow Brick Road
Asia caisia	The king of clubs	The Garden of Forking Paths
Murphy's law	The Discovery Dissipation	Future Shock
Flimsy Lavenrock	Course Correction	
Maven Mousie Lavender	Better Angels	

Bulma Templates MIT license

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

STEP 3 and ANSWER FOR Q3

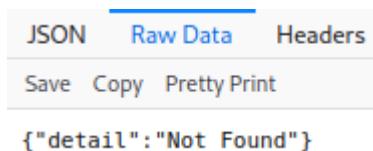
To open the website directory for API, just type in /api/ at the back of the IP address on Firefox search bar



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

ANSWER FOR Q4

Click on “Raw Data” and the answer will be provided



Q5: Where is Santa right now?

STEP 4

Open Text Editor and use Python language to find out the correct API key by using “for” so it can loop the codes until we got the true API key

```
1 import requests
2 import json
3
4 for i in range(1,101,2):
5     url = 'http://10.10.239.112/api/{}'.format(i)
6     response = requests.get(url)
7     response_content = json.loads(response.content)
8
9     print(response_content)
10
```

The screenshot shows a text editor window with the file name "santa.py" in the title bar. The code in the editor is a Python script that imports requests and json modules. It then uses a for loop to iterate through numbers 1 to 101 in steps of 2. For each iteration, it constructs a URL by concatenating "http://10.10.239.112/api/" with the current value of i (using string formatting). It makes a GET request to this URL using requests.get(). The response is converted to JSON using json.loads() and then printed to the console using print(). The code is numbered from 1 to 10.

STEP 5 and ANSWER FOR Q5

Copy every line in the Text Editor and open BPython which is already pre-installed in Kali. Run the code in BPython and wait for the process to finish. For the API key “57”, there is a result showing that santa is actually at Winter Wonderland, Hyde Park, London

```
bpython version 0.22.1 on top of Python 3.10.4 /usr/bin/python3
>>> import requests
>>> import json
Kali Tools  Kali Docs  Kali Forums  Kali NetHunter
>>>
>>> for i in range(1,101,2):
...     url = 'http://10.10.239.112/api/{}'.format(i)
...     response = requests.get(url)
...     response_content = json.loads(response.content)
...
...     print(response_content)
...
{'item_id': 1, 'q': 'Error. Key not valid!'}
{'item_id': 3, 'q': 'Error. Key not valid!'}
{'item_id': 5, 'q': 'Error. Key not valid!'}
{'item_id': 7, 'q': 'Error. Key not valid!'}
{'item_id': 9, 'q': 'Error. Key not valid!'}
{'item_id': 11, 'q': 'Error. Key not valid!'}
{'item_id': 13, 'q': 'Error. Key not valid!'}
{'item_id': 15, 'q': 'Error. Key not valid!'}
{'item_id': 17, 'q': 'Error. Key not valid!'}
{'item_id': 19, 'q': 'Error. Key not valid!'}
{'item_id': 21, 'q': 'Error. Key not valid!'}
{'item_id': 23, 'q': 'Error. Key not valid!'}
{'item_id': 25, 'q': 'Error. Key not valid!'}
{'item_id': 27, 'q': 'Error. Key not valid!'}
{'item_id': 29, 'q': 'Error. Key not valid!'}
{'item_id': 31, 'q': 'Error. Key not valid!'}
{'item_id': 33, 'q': 'Error. Key not valid!'}
{'item_id': 35, 'q': 'Error. Key not valid!'}
{'item_id': 37, 'q': 'Error. Key not valid!'}
{'item_id': 39, 'q': 'Error. Key not valid!'}
{'item_id': 41, 'q': 'Error. Key not valid!'}
{'item_id': 43, 'q': 'Error. Key not valid!'}
{'item_id': 45, 'q': 'Error. Key not valid!'}
{'item_id': 47, 'q': 'Error. Key not valid!'}
{'item_id': 49, 'q': 'Error. Key not valid!'}
{'item_id': 51, 'q': 'Error. Key not valid!'}
{'item_id': 53, 'q': 'Error. Key not valid!'}
{'item_id': 55, 'q': 'Error. Key not valid!'}
{'item_id': 57, 'q': 'Winter Wonderland, Hyde Park, London.'}
{'item_id': 59, 'q': 'Error. Key not valid!'}  

```

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 (10.10.94.92)

ANSWER FOR Q6

The correct API key is “57” as it shows santa’s current location

```
{'item_id': 57, 'q': 'Winter Wonderland, Hyde Park, London.'}
```

Thought Process/Methodology:

To find out what port number is available for our IP address, we must use nmap. So after using nmap, the available port number will show and we can see that there is port 80 for http files. To open the API website directory, just type in /api/ at the back of the IP address on Firefox search bar. Open TExt Editor and we have to use our recent Python knowledge to test out all correct API number combinations. We can use the code, “for” so we can loop and test different API numbers until we get it correct. Copy every line in the Text Editor and open BPython which is already pre-installed in Kali. Run the code in BPython and wait for the process to finish. For the API key “57”, there is a result showing that Santa is actually at Winter Wonderland, Hyde Park, London.

Day 17: Reverse Engineering - ReverseElfneering.

Tools used: SSH, Terminal

Solution/walkthrough:

Q1: Match the data type with the size in bytes

Q3: What is the command to set a breakpoint in radare2?

Q4: What is the command to execute a program until we hit a breakpoint?

STEP 1 / ANSWER FOR Q1, Q3, Q4

This can be answered by referring to the table in nothe notes such as given below. Q3 and Q4 can be answered by reading the notes which the answers are db and dc respectively.

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

STEP 2

We first need to establish a ssh connection with the target which in this case has the IP address of 10.10.17.45. The credentials are given in which the username is elfmceager with the password adventofcyber.

```
(1211103546㉿kali)-[~]
$ ssh elfmceager@10.10.17.45
elfmceager@10.10.17.45'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
In the 3rd line. The second line clears the
System information as of Tue Jul 12 01:22:13 UTC 2022
or less. The 5th and 6th lines are used to exit
System load: 0.0      Processes:         95
Usage of /: 39.4% of 11.75GB   Users logged in:  0
Memory usage: 8%           IP address for ens5: 10.10.17.45
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 yo
ur Internet connection or proxy settings

Last login: Tue Jul 12 00:56:03 2022 from 10.18.30.248
```

STEP 3

After accessing the machine, we then are tasked with analysing the challenge1 file located on the machine. We can access the file by running the command as shown below which will open the binary in debugging mode.

```
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1679 started ...
= attach 1679 1679
bin.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits 64
```

Q2: What is the command to analyse the program in radare2?

STEP 4 / ANSWER FOR Q2

We then need to enter the command aa to analyse it. This may take some time

```
[0x00400a30]> aa
[ ] Analyze all flags starting with sym. and entry0 (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)
```

STEP 5

After its done, we can find a list of functions by using the afl command. But to be more specific, we can run the command (afl | grep main), to specify the type of functions you want listed which in this case is the ones containing main.

```
[0x00400a30]> afl | grep main
0x00400b4d    1 35          sym.main
0x00400de0    10 1007 → 219  sym.__libc_start_main
0x00403840    39 661   → 629  sym._nl_find_domain
0x00403ae0    308 5366 → 5301 sym._nl_load_domain
0x00415ef0     1 43          sym._IO_switch_to_main_get_area
0x0044ce10     1 8           sym._dl_get_dl_main_map
0x00470430     1 49          sym._IO_switch_to_main_wget_area
0x0048f9f0    7 73   → 69  sym._nl_fnddomain_subfreeres
0x0048fa40    16 247  → 237 sym._nl_unload_domain
```

Q5: What is the value of local_ch when its corresponding movl instruction is called?

Q6: What is the value of eax when the imull instruction is called?

Q7: What is the value of local_4h before eax is set to 0

STEP 6 / ANSWER FOR Q5, Q6, Q7

As we can see that there is a function at main we can use the command pdf@main to examine the assembly code. In this we can use the results shown to answer the question 5, 6 and 7 in which the answer is 1, 6, 6 respectively.

```
[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
```

Thought Process/Methodology:

All we need to do is first establish a ssh connection with the ip address using the credentials already given. We then will be met with 2 files in which we are tasked with analysing the first one which is titled challenge1. By using the respective commands, we found that there is a file in sym.main which will be our target. We can then open this file with the pdf@main command and see the assembly language in it.

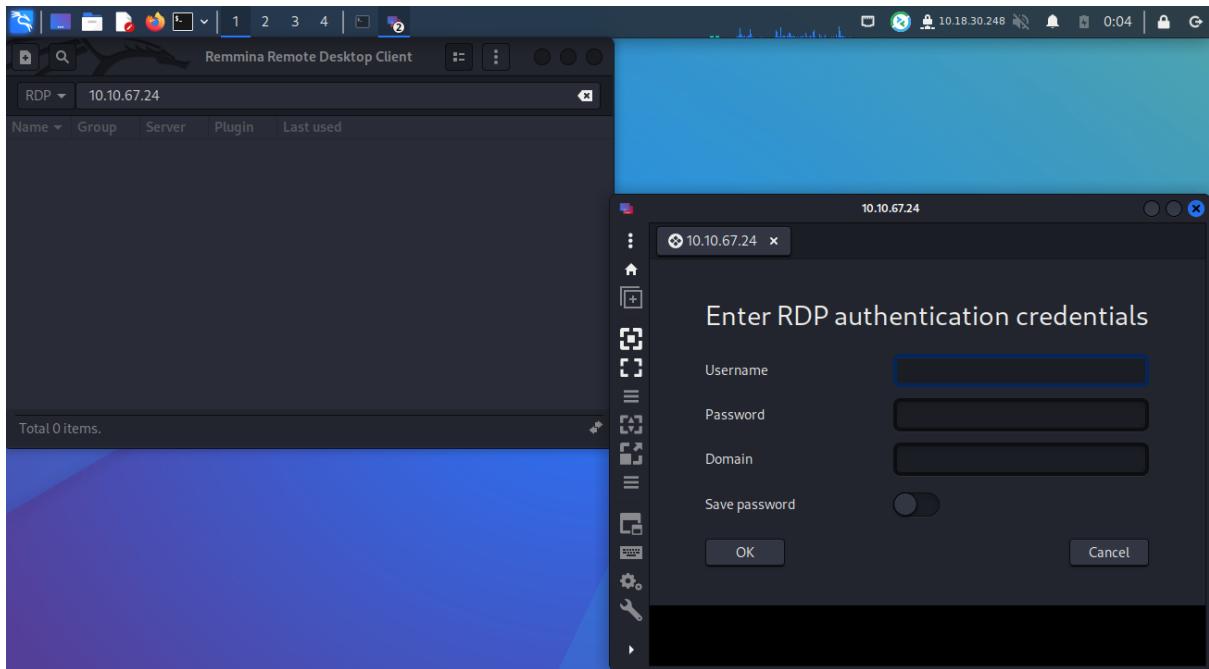
Day 18: Reverse Engineering - The Bits of Christmas.

Tools used: Remmina, ILspy

Solution/walkthrough:

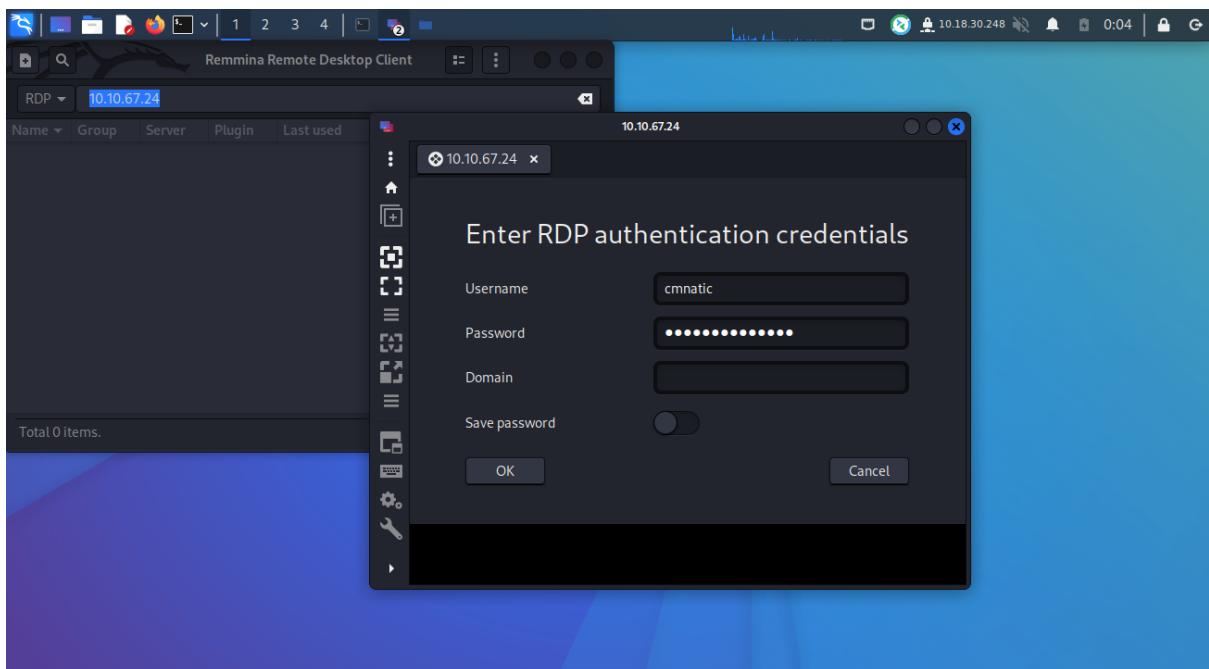
STEP 1

Use remmina to connect rdp with the ip address which will then show the below tab.



STEP 2

Use the credentials given to log in which the username is cmnatic with the password Adventofcyber!

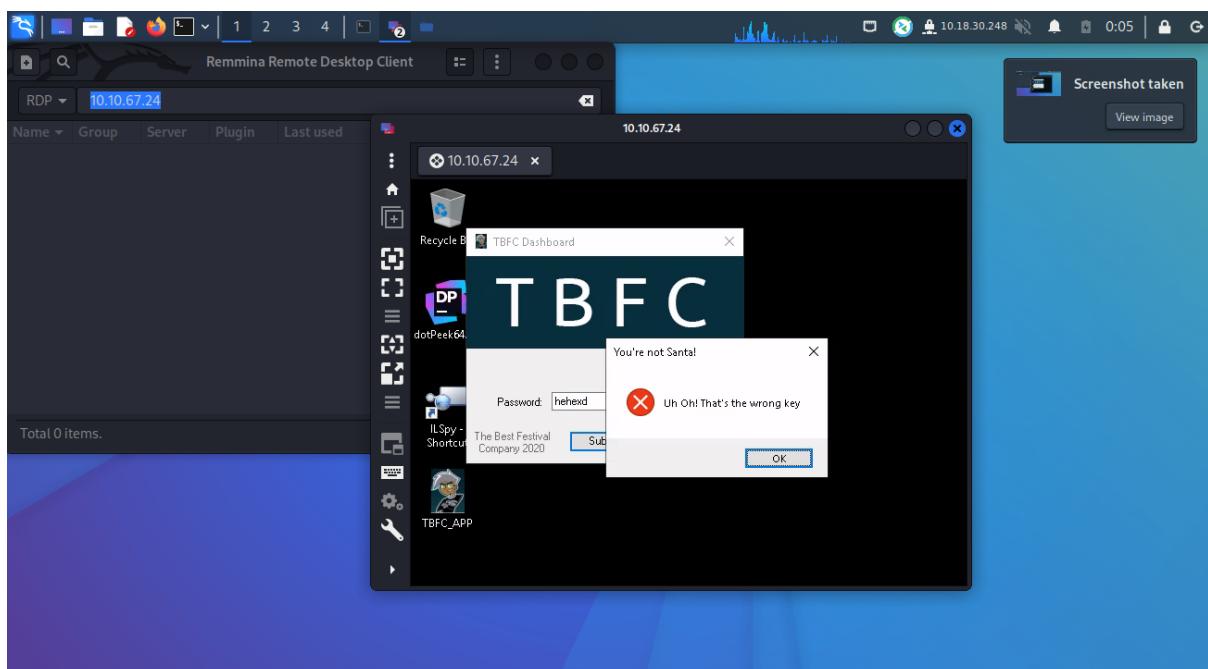
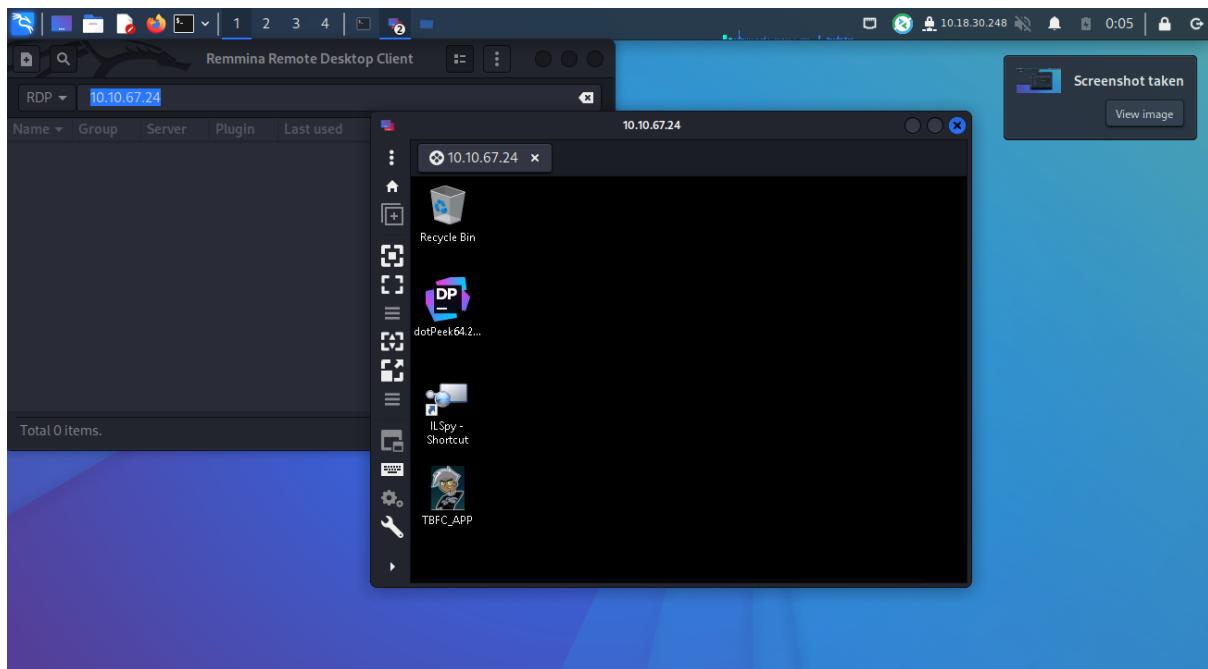


Q1: What is the message that shows up if you enter the wrong password for TBFC_APP?

Q2: What does TBFC stands for?

STEP 3 / ANSWER FOR Q1,Q2

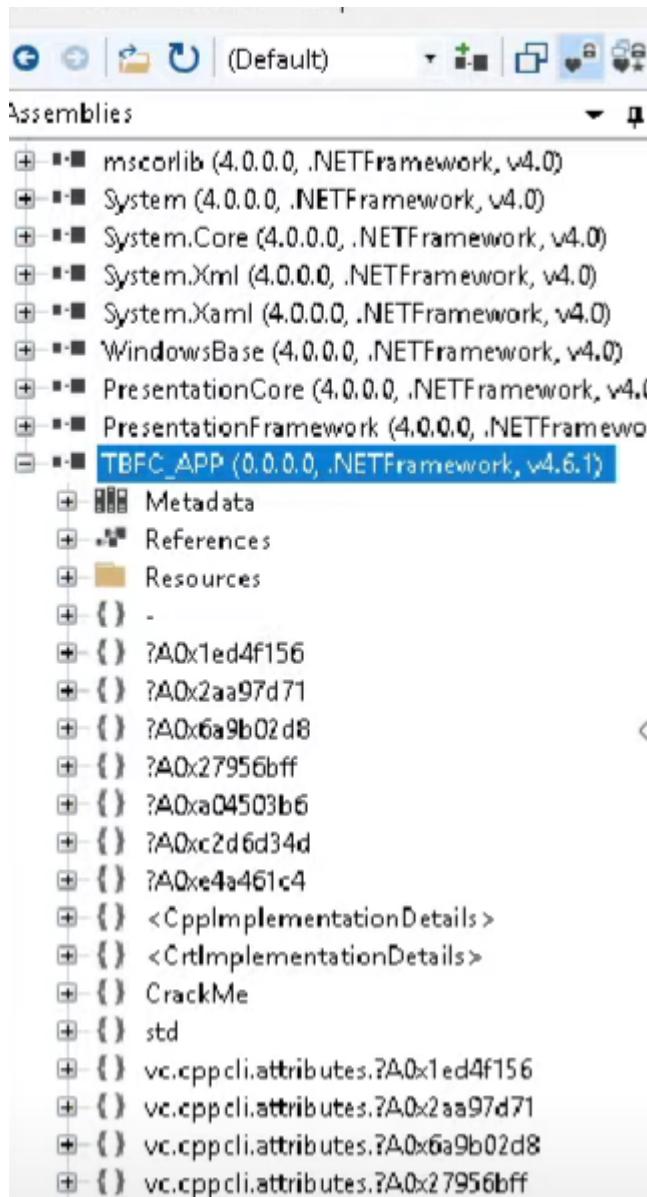
This will show you this tab which has both tbfc app and the ILspy. The second pic also shows the answers for Q1 and Q2 which is “Uh Oh! That's the wrong key” and “The Best Festival Company” respectively.



Q3: Decompile the TBFC_APP with ILspy. What is the module that catches your attention?

STEP 4 / ANSWER FOR Q3

We then need to open ILspy to analyse the app. Open the app in ILspy and analyze it. We can see that in the list, one sticks out which seems weird in the list. This is the one named crack me.



Q4: Within the module, there are two forms. Which contains the information we are looking for?

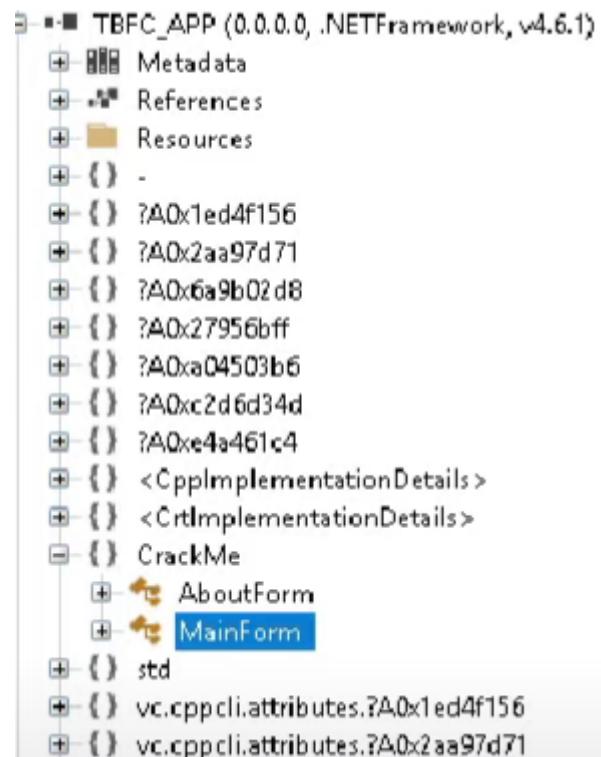
Q5: Which method within the form from Q4 will contain the information we are seeking?

Q6: What is santa's password?

Q7: Now that you've retrieved this password, try to login... What is the flag?

STEP 5 / ANSWER FOR Q4, Q5, Q6, Q7

Under crack me, we can see 2 files which is aboutform and mainform. After tinkering around we can find that the one we are looking for is under mainform/buttonActivate_Click. This shows basically all the information we need. With this we can answer all questions from Q4 to Q7. The password is santapassword321 as seen on the line which has ptr=. To check on this more, we can double click on the text and we will be taken to a tab where ILspy shows more of the details. In this we can see the hexadecimal value which we can translate to normal text using the like of cyberchef. The bottom 2 lines also shows the message we will get when either we enter the right or even wrong password. This enables us to see the flag that will be given if we enter the right password. The answers for the questions are Mainform, buttonActivate_click, santapassword321 and thm{046af} respectively.



```
// IL SPY - .NET 4.0.0.0
[using ...]

private unsafe void buttonActivate_Click(object sender, EventArgs e)
{
    IntPtr value = Marshal.StringToGlobalAnsi(textBoxKey.Text);
    byte* ptr = (byte*)System.Runtime.CompilerServices.Unsafe.AsPointer(<ref >Module>.??_C@_0B@IKKDFEPG@santapassword321@);
    void* ptr2 = *(void**)value;
    byte b = *(byte*)ptr2;
    byte b2 = 115;
    if ((uint)b >= 115u)
    {
        while ((uint)b <= (uint)b2)
        {
            if (b != 0)
            {
                ptr2 = (byte*)ptr2 + 1;
                ptr++;
                b = *(byte*)ptr2;
                b2 = *(byte*)(ptr);
                if ((uint)b < (uint)b2)
                {
                    break;
                }
                continue;
            }
            MessageBox.Show("Welcome, Santa, here's your flag thm{046af}", "That's the right key!", MessageBoxButtons.OK, MessageBoxIcon.Asterisk);
            return;
        }
        MessageBox.Show("Uh Oh! That's the wrong key", "You're not Santa!", MessageBoxButtons.OK, MessageBoxIcon.Hand);
    }
}
```

Thought Process/Methodology:

In this, we would need to use remmina to connect to the ip address and then use the provided credentials to log in. After accessing it, we need to gain access to the TBFC app but we do not have the password to access it. This is where ILspy comes in handy. It allows us to see the building blocks of the app and the code on which it is constructed. In it we can see one odd looking file named crack me which we can see contains the part that handles the logging in part of the app. We can then find the very structure of the code that runs the login part which clearly shows the correct password which belongs to Santa and the message box it will display when we enter the correct password and even the wrong one.

Day 19: Web Exploitation - The Naughty or Nice List

Tools used: Web Browser

Solutions/Walkthrough:

Q1: Which list is this person on?

STEP 1 and ANSWER FOR Q1

Access the webpage and enter the names YP, JJ, Ian Chai, Timothy, Tib3rius and Kanes one by one into the search box. The answer for Q1:

The List

Welcome children!

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

Have a Merry Christmas! Ho ho ho!

- Santa

Name: Search

YP is on the Nice List.

The List

Welcome children!

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

Have a Merry Christmas! Ho ho ho!

- Santa

Name: Search

JJ is on the Naughty List.

The Naughty or Nice List

10.10.189.64/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3Dian%2520Chai

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

The List Admin

The List



Welcome children!

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

Have a Merry Christmas! Ho ho ho!

- Santa

Name: Search

Ian Chai is on the Nice List.

The Naughty or Nice List

10.10.189.64/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DTimothy

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

The List Admin

The List



Welcome children!

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

Have a Merry Christmas! Ho ho ho!

- Santa

Name: Search

Timothy is on the Naughty List.

The Naughty or Nice List

10.10.189.64/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DTib3rius

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

The List Admin

The List



Welcome children!

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

Have a Merry Christmas! Ho ho ho!

- Santa

Name: Search

Tib3rius is on the Nice List.

The Naughty or Nice List

10.10.189.64/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DKanes

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

The List Admin

The List



Welcome children!

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

Have a Merry Christmas! Ho ho ho!

- Santa

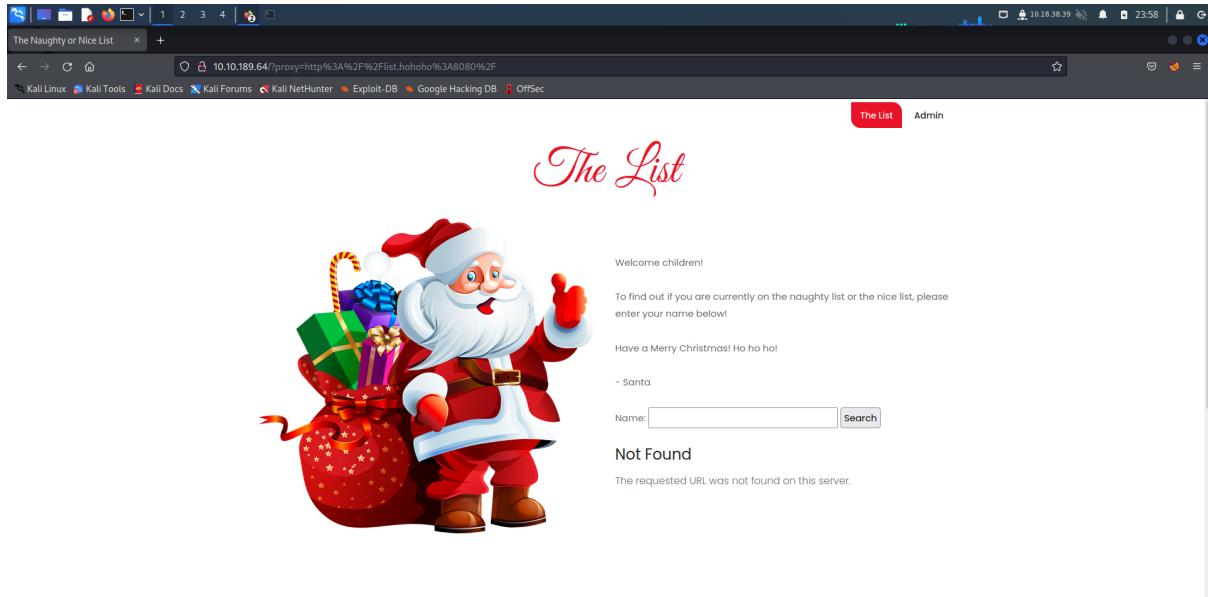
Name: Search

Kanes is on the Naughty List.

Q2: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"?

STEP 2 and ANSWER FOR Q2

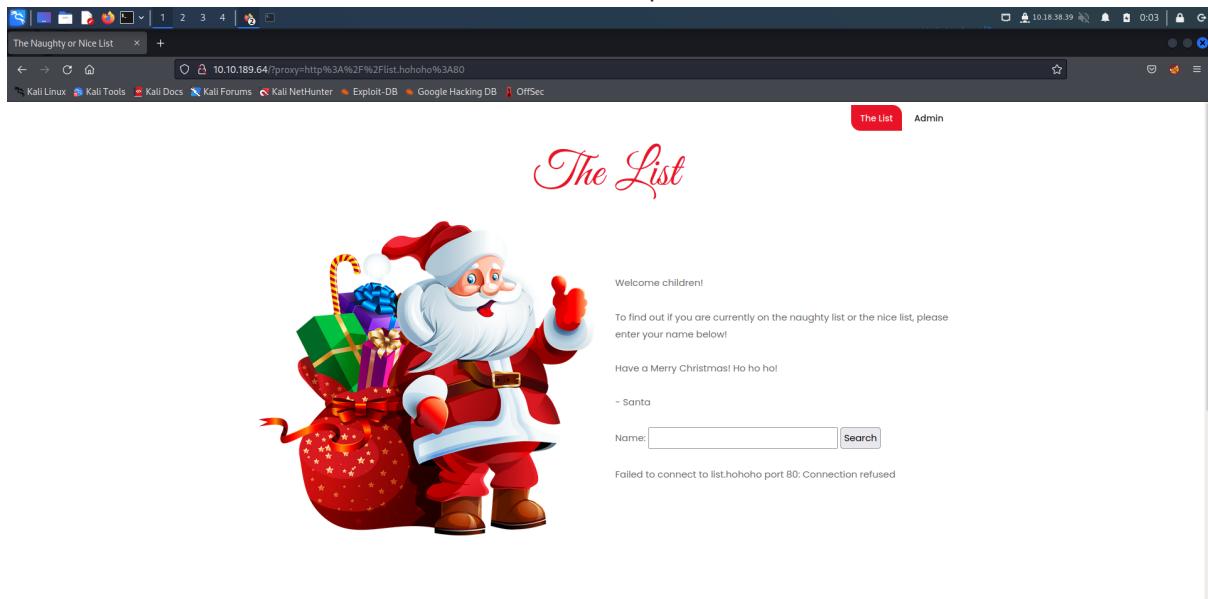
Add "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F" into the url behind the web server's original url. The answer for Q2 is "Not Found. The requested URL was not found on this server."



Q3: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A80"?

STEP 3 and ANSWER FOR Q3

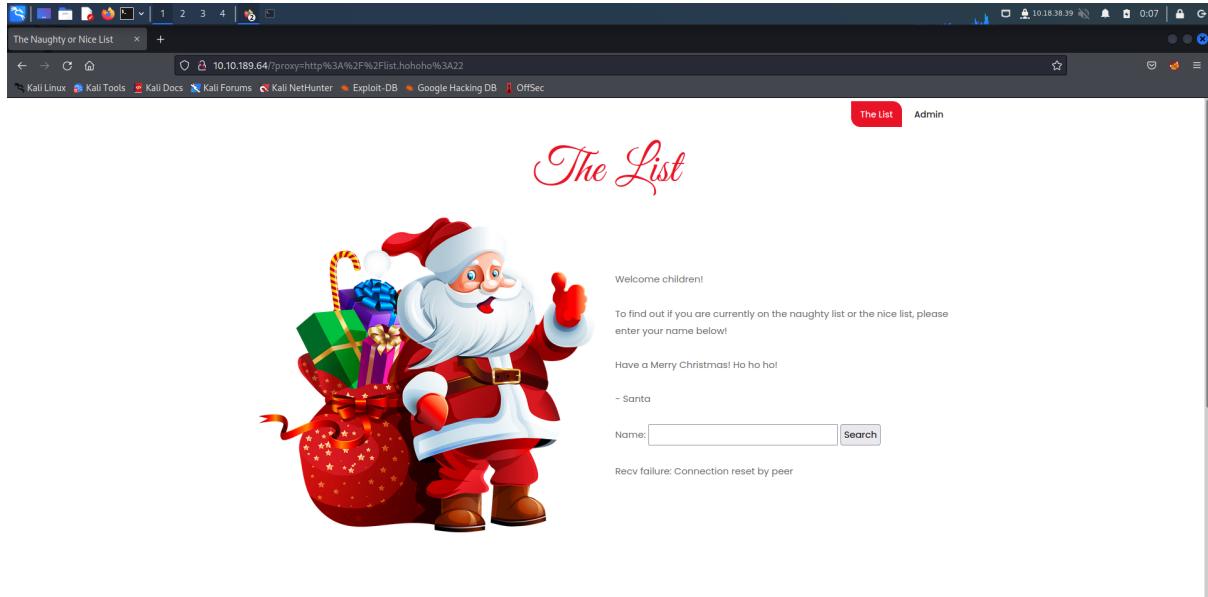
Add "/?proxy=http%3A%2F%2Flist.hohoho%3A80" into the url behind the webserver's original url. The answer for Q3 is "Failed to connect to list.hohoho port 80: Connection refused".



Q4: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A22"?

STEP 4 and ANSWER FOR Q4

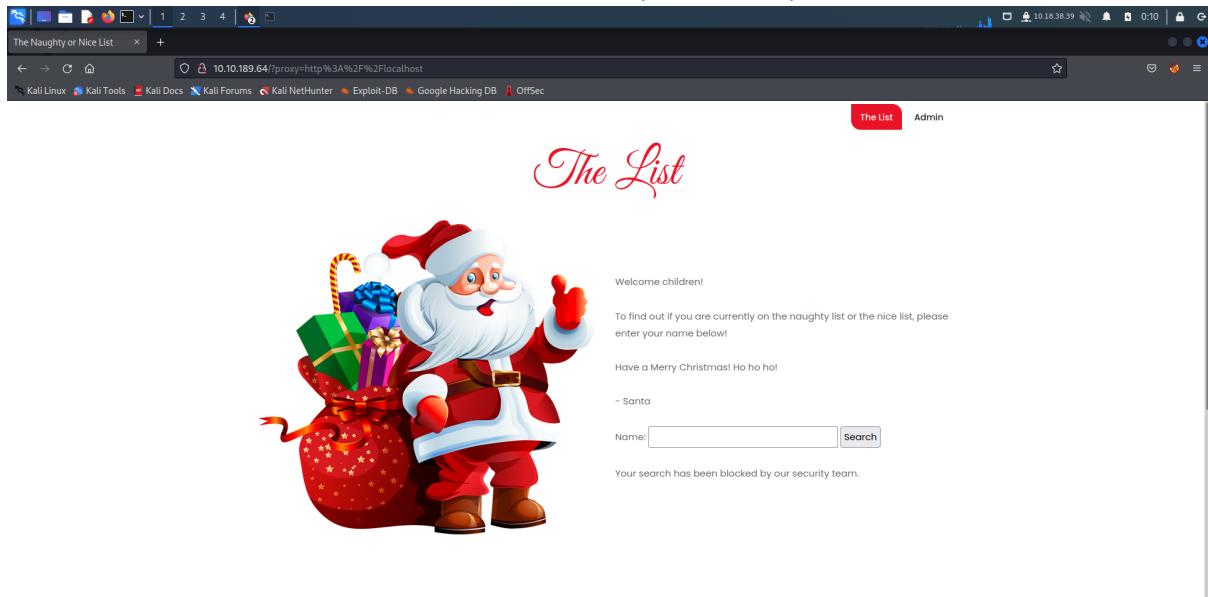
Add "/?proxy=http%3A%2F%2Flist.hohoho%3A22" into the url behind the webserver's original url.
The answer for Q4 is "Recv failure: Connection reset by peer".



Q5: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"?

STEP 5 and ANSWER FOR Q5

Add "/?proxy=http%3A%2F%2Flocalhost" into the url behind the webserver's original url.
The answer for Q5 is "Your search has been blocked by our security team."



Q6: What is Santa's password?

STEP 6 and ANSWER FOR Q6

Add “/?proxy=http%3A%2F%2Flist.hohoho.localtest.me” behind the original url and it will reveal a secret message left behind. The answer for Q6 is “Be good for goodness sake!”.

The List

Welcome children!

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

Have a Merry Christmas! Ho ho ho!

- Santa

Name:

Santa,

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

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

- Elf McSkidy

Q7: What is the challenge flag?

STEP 7 and ANSWER FOR Q7

Enter username Santa and password found in Q6 to login as Santa in the admin page and remove the naughty list. The answer for Q7 is THM{EVERYONE_GETS_PRESENTS}.

List Administration

This page is currently under construction.

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

OK

Thought Process/Methodology:

When we first enter the web server; testing the search box, a change in the url can be seen. After tinkering with the webserver, we discovered that we can exploit the url weakness since the request will pass through as long as the hostname has list.hohoho. Through this weakness, we discover a hidden message left behind for Santa in case he forgets his password. By using this discovered password and username Santa we were able to login, remove the naughty list and get the flag.

Day 20: Blue Teaming - PowershELf to the rescue

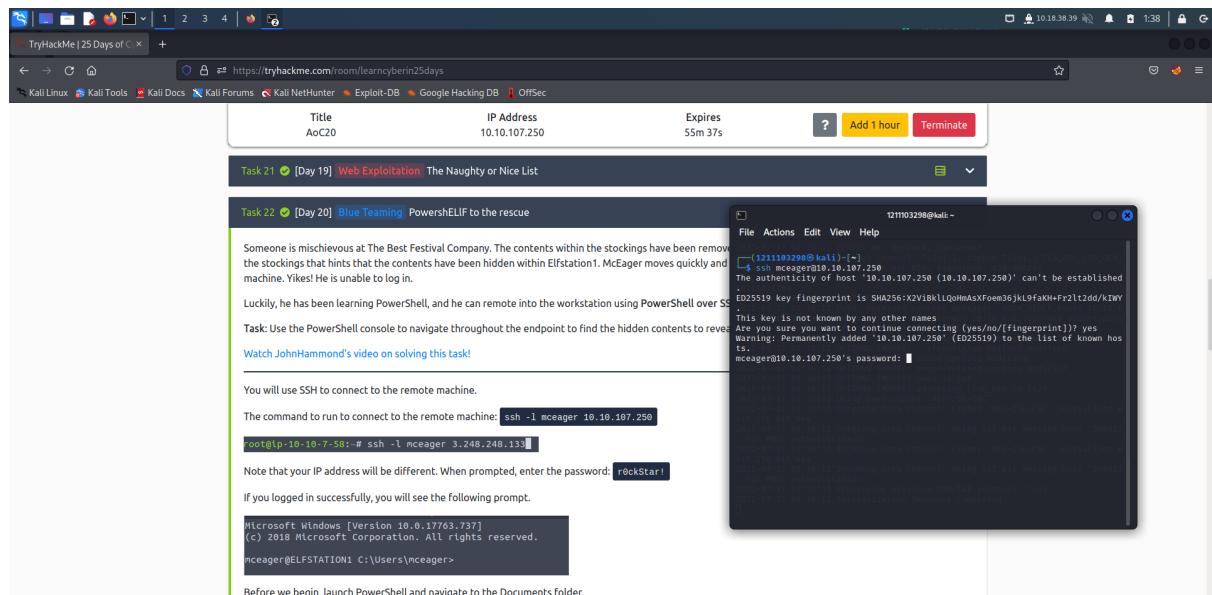
Tools used: Linux Terminal, PowerShell

Solutions/Walkthrough:

Q2: Search for the first hidden elf file within the Documents folder. Read the contents of this file.
What does Elf 1 want?

STEP 1

Connect to mceager machine through linux terminal with the password r0ckStar!.



The screenshot shows a web browser window with a terminal-like interface. The title bar says "TryHackMe | 25 Days of C" and the address bar shows "https://tryhackme.com/room/learnyberin25days". The terminal window has a header with "Title AoC20", "IP Address 10.10.107.250", and "Expires 55m 37s". A yellow button says "Add 1 hour" and a red button says "Terminate".

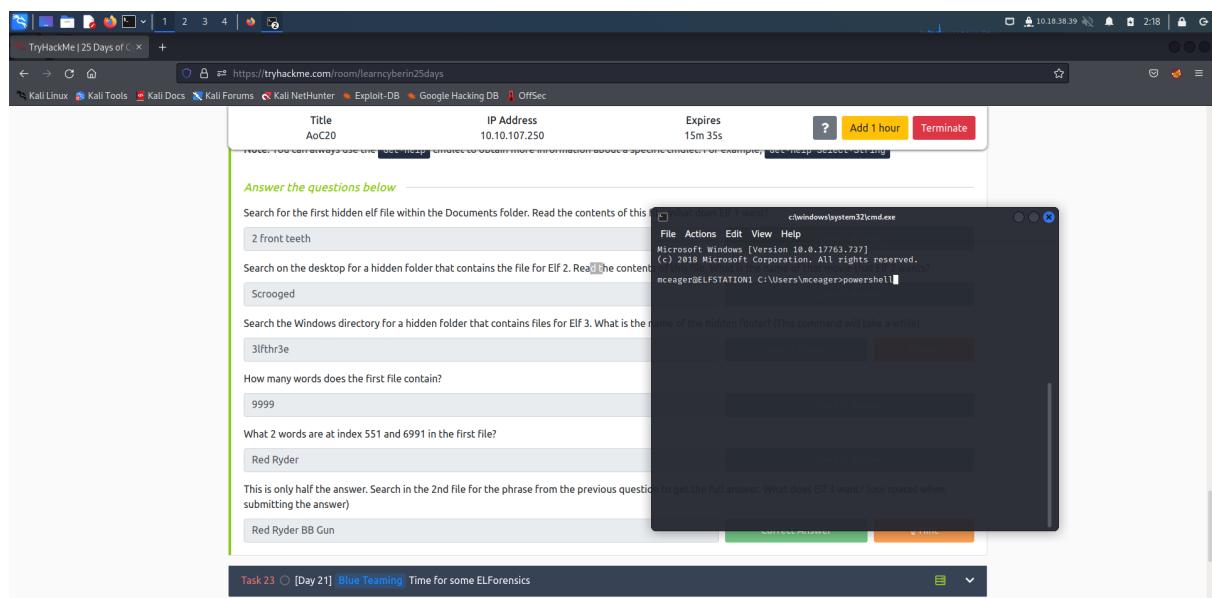
The main area contains a task description: "Task 21 [Day 19] Web Exploitation The Naughty or Nice List" and "Task 22 [Day 20] Blue Teamng PowershELF to the rescue". The terminal output shows:

```
[12110329@kali ~] $ ssh mceager@10.10.107.250
The authenticity of host '10.10.107.250 (10.10.107.250)' can't be established.
ED25519 key fingerprint is SHA256:X2Vi8KLQoHMsxFoem36jL9FaKH+Fz2lt2dd/k3WY.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.107.250' (ED25519) to the list of known hosts.
mceager@10.10.107.250's password: [REDACTED]
```

Below the terminal, there is a note: "You will use SSH to connect to the remote machine. The command to run to connect to the remote machine: ssh -l mceager 10.10.107.250". The terminal also shows a command being run: "root@lp:10-10-7-5B:~# ssh -l mceager 3.248.248.133". A note says: "Note that your IP address will be different. When prompted, enter the password: rockStar!". Another note says: "If you logged in successfully, you will see the following prompt." It shows a Microsoft Windows command prompt: "Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
mceager@ELFSTATION1 C:\Users\mceager>".

STEP 2

After connecting over to mceager machine through ssh, open powershell.



The screenshot shows a web browser window with a terminal-like interface. The title bar says "TryHackMe | 25 Days of C" and the address bar shows "https://tryhackme.com/room/learnyberin25days". The terminal window has a header with "Title AoC20", "IP Address 10.10.107.250", and "Expires 15m 35s". A yellow button says "Add 1 hour" and a red button says "Terminate".

The main area contains a task description: "Answer the questions below" and "Search for the first hidden elf file within the Documents folder. Read the contents of this file". The terminal output shows:

```
[12110329@kali ~] $ powershell
Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.17763.737]
(c) 2018 Microsoft Corporation. All rights reserved.
mceager@ELFSTATION1 C:\Users\mceager>powershell!
```

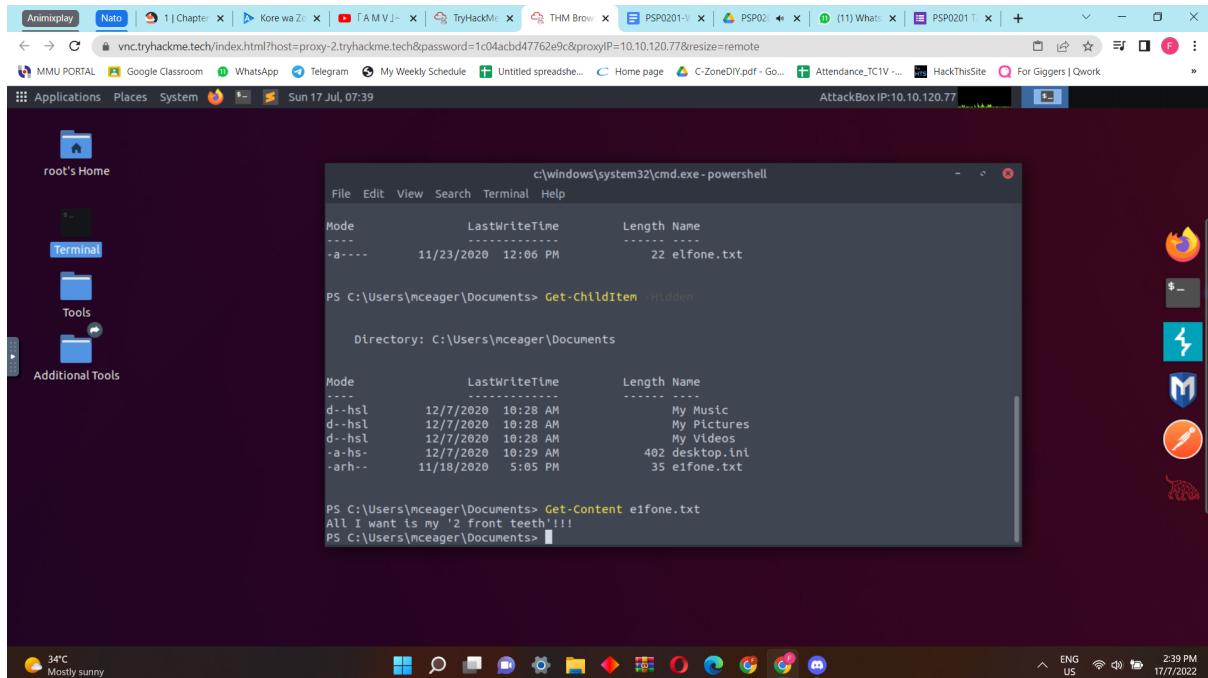
Below the terminal, there are several questions with answers:

- 2 front teeth
- Search on the desktop for a hidden folder that contains the file for Elf 2. Rea[REDACTED]the content
- Scrooged
- 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)
- 3ifthr3
- How many words does the first file contain?
- 9999
- What 2 words are at index 551 and 6991 in the first file?
- Red Ryder
- 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)
- Red Ryder BB Gun

At the bottom of the terminal window, there are two buttons: "CORRECT ANSWER" and "WRONG".

STEP 3 and ANSWER FOR Q2

Go into the documents folder by using set-location; to search for the hidden folder, use “Get-ChildItem -Hidden” therefore finding the file and can be retrieved through the cmdlet get-content. The answer for Q2 is ‘2 front teeth’.



```
c:\windows\system32\cmd.exe - powershell
File Edit View Search Terminal Help
Mode LastWriteTime Length Name
---- -----
-a--- 11/23/2020 12:06 PM 22 elfone.txt

PS C:\Users\mceager\Documents> Get-ChildItem -Hidden

Directory: C:\Users\mceager\Documents

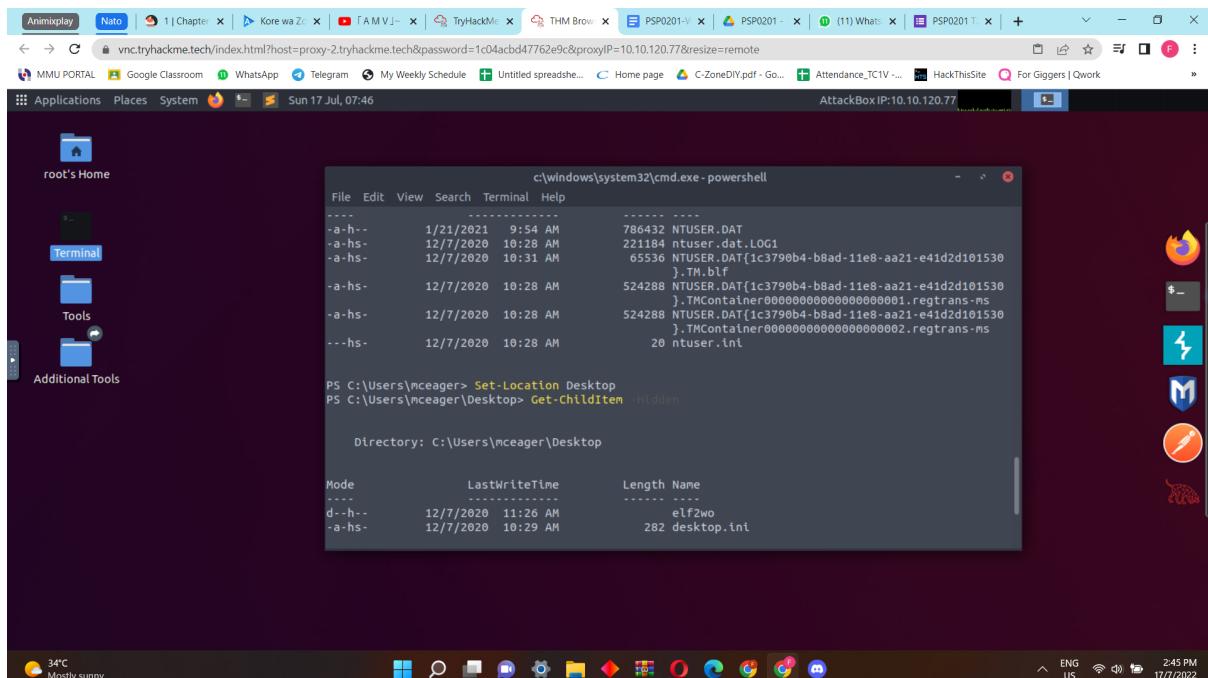
Mode LastWriteTime Length Name
---- -----
d--hsl 12/7/2020 10:28 AM My Music
d--hsl 12/7/2020 10:28 AM My Pictures
d--hsl 12/7/2020 10:28 AM My Videos
-a-hs- 12/7/2020 10:29 AM 402 desktop.lnk
-arh-- 11/18/2020 5:05 PM 35 elfone.txt

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

Q3: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?

STEP 4

By using cmdlet ‘Set-Location’ to go to Desktop, we then use cmdlet ‘Get-ChildItem -Directory -Hidden’ and find the dir elf2wo.



```
c:\windows\system32\cmd.exe - powershell
File Edit View Search Terminal Help
---- -----
-a-h-- 1/21/2021 9:54 AM 786432 NTUSER.DAT
-a-hs- 12/7/2020 10:28 AM 221184 ntuser.dat.LOG1
-a-hs- 12/7/2020 10:31 AM 65536 NTUSER.DAT[1c3790b4-b8ad-11e8-aa21-e41d2d101530].TM.blf
-a-hs- 12/7/2020 10:28 AM 524288 NTUSER.DAT[1c3790b4-b8ad-11e8-aa21-e41d2d101530].TMContainer00000000000000000000000000000001.regtrans-ms
-a-hs- 12/7/2020 10:28 AM 524288 NTUSER.DAT[1c3790b4-b8ad-11e8-aa21-e41d2d101530].TMContainer00000000000000000000000000000002.regtrans-ms
---hs- 12/7/2020 10:28 AM 28 ntuser.lnk

PS C:\Users\mceager> Set-Location Desktop
PS C:\Users\mceager\Desktop> Get-ChildItem -Hidden

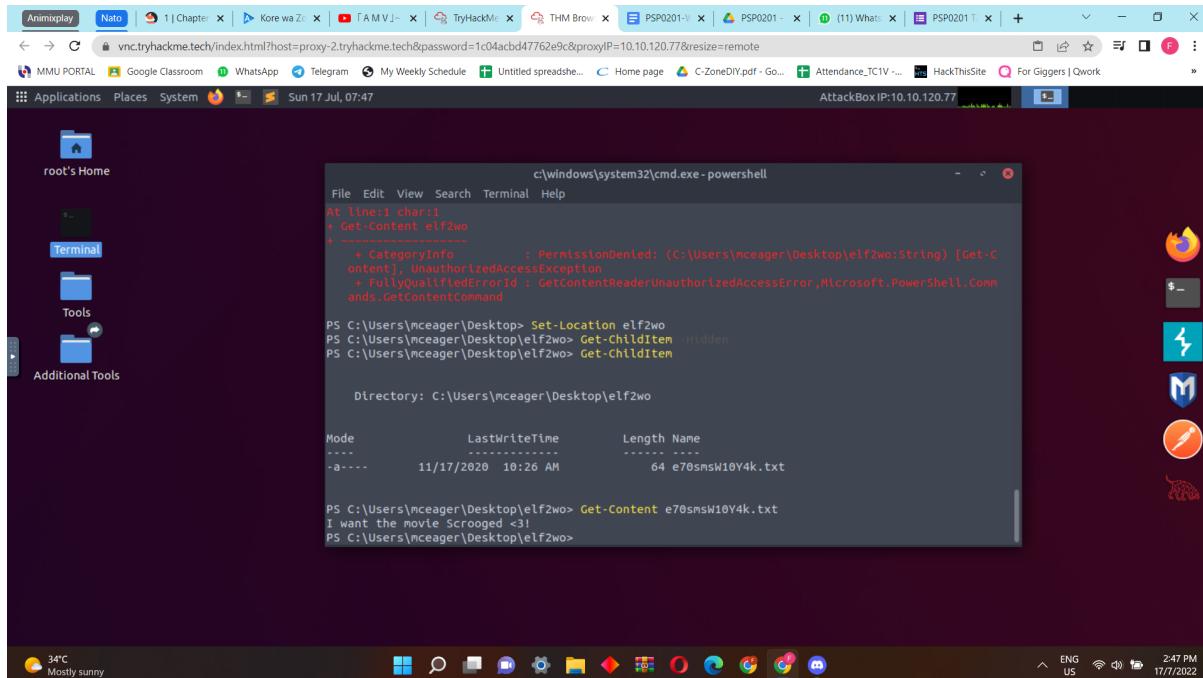
Directory: C:\Users\mceager\Desktop

Mode LastWriteTime Length Name
---- -----
d--h-- 12/7/2020 11:26 AM 168 elftwo
-a-hs- 12/7/2020 10:29 AM 282 desktop.lnk

ps C:\Users\mceager\Desktop> Get-Content elftwo
The Elf Returns!!!
PS C:\Users\mceager\Desktop>
```

STEP 5 and ANSWER FOR Q3

Enter into the directory elf2wo using cmdlet ‘Set-Location’ and use ‘Get-ChildItem -Hidden’ to find a file named “e70smsW10Y4K.txt” therefore using get-content cmdlet to get its content.The answer for Q3 is ‘Scrooged’.



```
c:\windows\system32\cmd.exe - powershell
At line:1 char:1
+ Get-Content elf2wo
+ CategoryInfo          : PermissionDenied: (C:\Users\mceager\Desktop\elf2wo:String) [Get-Content], UnauthorizedAccessException
+ FullyQualifiedErrorId : GetContentReaderUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetContentCommand
PS C:\Users\mceager\Desktop> Set-Location elf2wo
PS C:\Users\mceager\Desktop\elf2wo> Get-ChildItem -Hidden
PS C:\Users\mceager\Desktop\elf2wo>

Directory: C:\Users\mceager\Desktop\elf2wo

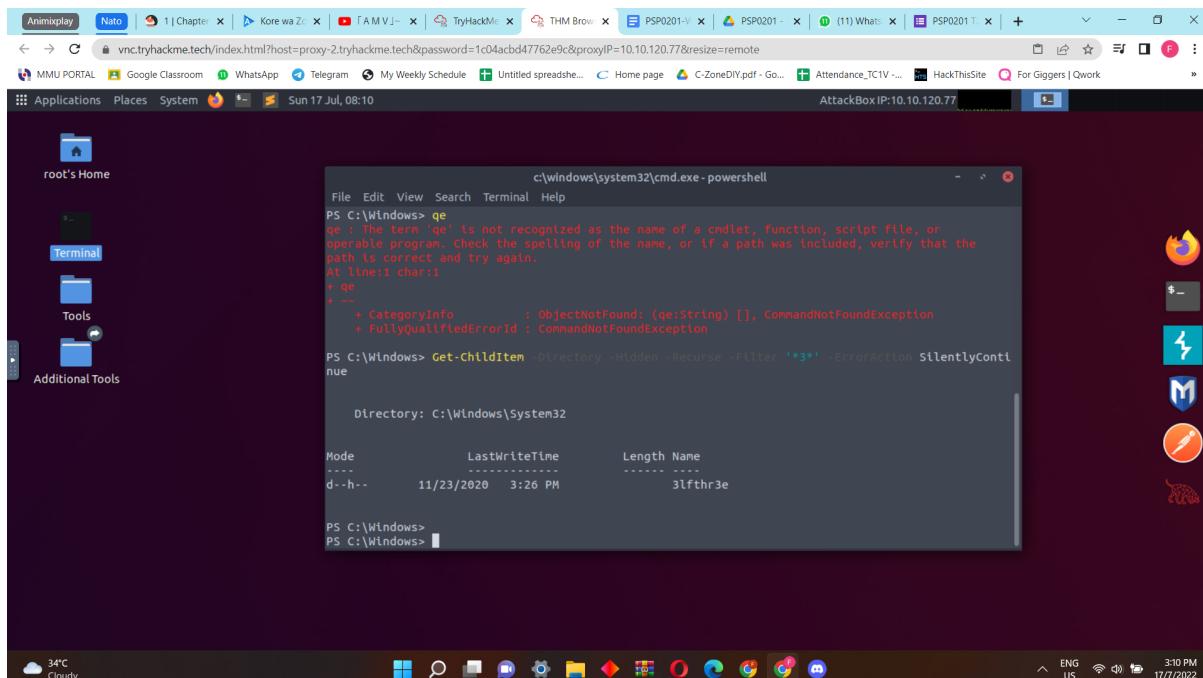
Mode                LastWriteTime         Length Name
----                -----          ----- 
-a----       11/17/2020 10:26 AM           64 e70smsW10Y4K.txt

PS C:\Users\mceager\Desktop\elf2wo> Get-Content e70smsW10Y4K.txt
I want the Movie Scrooged <3!
PS C:\Users\mceager\Desktop\elf2wo>
```

Q4: 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)

STEP 6 and ANSWER FOR Q4

Go to Windows dir using set-locations and use “Get-ChildItem -Directory -Hidden -Recurse -Filter “*3*” -ErrorAction SilentlyContinue” to find the hidden directory. The answer for Q4 is 3lfthr3e.



```
c:\windows\system32\cmd.exe - powershell
PS C:\Windows> qe
qe : The term 'qe' is not recognized as the name of a cmdlet, function, script file, or
operable program. Check the spelling of the name, or if a path was included, verify that the
path is correct and try again.
At line:1 char:1
+ qe
+ CategoryInfo          : ObjectNotFound: (qe:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException
PS C:\Windows> Get-ChildItem Directory -Hidden -Recurse -Filter "*3*" -ErrorAction SilentlyContinue

Directory: C:\Windows\System32

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

PS C:\Windows>
PS C:\Windows>
```

Q5: How many words does the first file contain?

STEP 7 and ANSWER FOR Q5

Enter into the directory in Q4 and we will discover 2 files by using cmdlet 'Get-ChildItem -Hidden'. Use "Get-Content -Path 1.txt | Measure-Object -Word".The answer for Q5 is 9999.

```
c:\windows\system32\cmd.exe - powershell
File Edit View Search Terminal Help
+ CategoryInfo          : InvalidArgument: () [Get-ChildItem], ParameterBindingException
+ FullyQualifiedErrorId : NamedParameterNotFound,Microsoft.PowerShell.Commands.GetChildItem
Command
PS C:\Windows\System32\3lfthr3e> Get-ChildItem -Hidden
Directory: C:\Windows\System32\3lfthr3e

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

PS C:\Windows\System32\3lfthr3e> Get-Content -Path 1.txt | Measure-Object -Word
Lines Words Characters Property
----- ----- -----
9999

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

Q6: What 2 words are at index 551 and 6991 in the first file?

STEP 8 and ANSWER FOR Q6

Still in the same directory, use cmdlet "(Get-Content -Path 1.txt)[index]" with indexes 551 and 6991 respectively. The content combine will be the answer for Q6 which is Red Ryder.

```
c:\windows\system32\cmd.exe - powershell
File Edit View Search Terminal Help
PS C:\Windows\System32\3lfthr3e> Get-ChildItem -Hidden
Directory: C:\Windows\System32\3lfthr3e

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

PS C:\Windows\System32\3lfthr3e> Get-Content -Path 1.txt | Measure-Object -Word
Lines Words Characters Property
----- ----- -----
9999

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

Q7: 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)

STEP 9 and ANSWER FOR Q7

Use cmdlet, Select-String -path 'C:\Windows\System32\3lfthr3e\2.txt' -pattern "redryder".
The answer for Q7 is 'redryderbbgun'.

c:\windows\system32\cmd.exe - powershell

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

```
PS C:\Windows\System32\3lfthr3e> Get-Content -Path 1.txt | Measure-Object -Word
Lines Words Characters Property
----- ----- -----
9999

PS C:\Windows\System32\3lfthr3e> (Get-Content -Path 1.txt)[551]
Red
PS C:\Windows\System32\3lfthr3e> (Get-Content -Path 1.txt)[6991]
Ryder
PS C:\Windows\System32\3lfthr3e> Select-String -path 'C:\Windows\System32\3lfthr3e\2.txt' -Pattern redryder
2.txt:558704:redryderbbgun

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

Q1: Check the ssh manual. What does the parameter -l do?

The answer is login_name.

```
-k' Disables forwarding (delegation) of GSSAPI credentials to the server.

-L
[

bind_address:]port:host:hostport
Specifies that the given port on the local (client) host is to be forwarded to the given host and port on the remote side. This works by allocating a socket to listen to port on the local side, optionally bound to the specified bind_address. Whenever a connection is made to this port, the connection is forwarded over the secure channel, and a connection is made to host port hostport from the remote machine. Port forwardings can also be specified in the configuration file. IPv6 addresses can be specified with an alternative syntax:
[bind_address/]port/host/hostport or by enclosing the address in square brackets. Only the superuser can forward privileged ports. By default, the local port is bound in accordance with the GatewayPorts setting. However, an explicit bind_address may be used to bind the connection to a specific address. The bind_address of "localhost" indicates that the listening port be bound for local use only, while an empty address or "*" indicates that the port should be available from all interfaces.

-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.

-M' Places the ssh client into "master" mode for connection sharing. Multiple -M options places ssh into "master" mode with confirmation required before slave connections are accepted. Refer to the description of ControlMaster in ssh_config(5) for details.

-m mac_spec
Additionally, for protocol version 2 a comma-separated list of MAC (message authentication code) algorithms can be specified in order of preference. See the MACs keyword for more information.

-N' Do not execute a remote command. This is useful for just forwarding ports (protocol version 2 only).
```

Thought Process/Methodology:

In this task, we were introduced to 3 cmdlet for usage in powershell “Get”, “Set” and “Select” with their own respective parameters. By using those provided cmdlet, we were able to scour through the elf mceager machine with ease using “set-location”, finding hidden files and directory and review its content using “Get” and selecting a specific string from a long text using “select-string”. Back to the start, since we can't use remmina, we were forced to connect to elf mceager windows using ssh since we were not provided with any other alternative in accordance to the task.