

PSP0201

Week 5

Writeup

Group Name: **No Entry**

Members:

ID	Name	Role
1211102976	Lee Le Xuan	Leader
1211103182	Ester Ong Xiang Lin	Member
1211102020	Jackter Un Chia Te	Member
1211102575	Pang Ding Yuan	Member

Day 16: [Scripting] Help! Where is Santa?

Tools used: Kali Linux, terminal, nmap

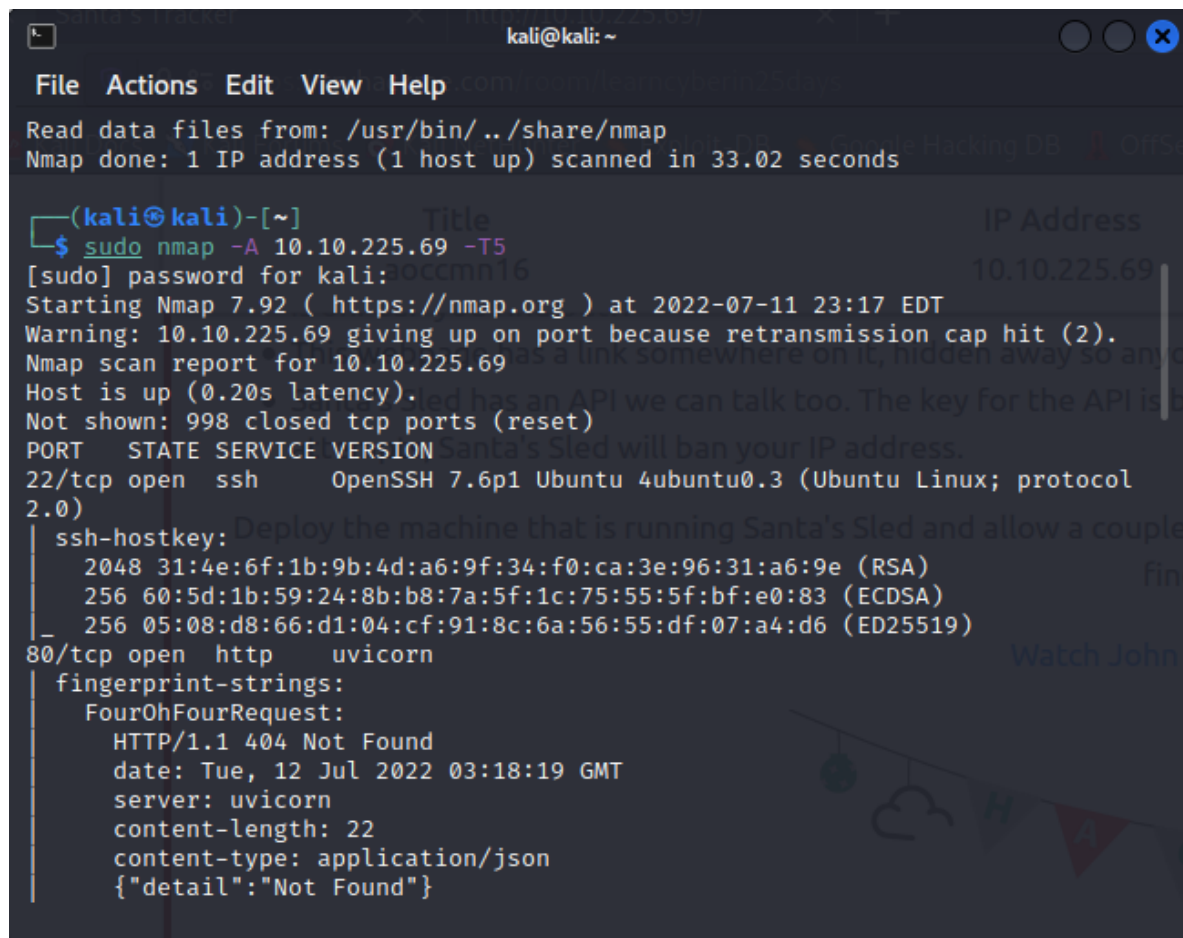
Walkthrough:

Step 1

Firstly, we type the command → `<sudo nmap -A 10.10.225.69 -T5>` to find the open port. We found that 80 is the port.

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

Answer : 80



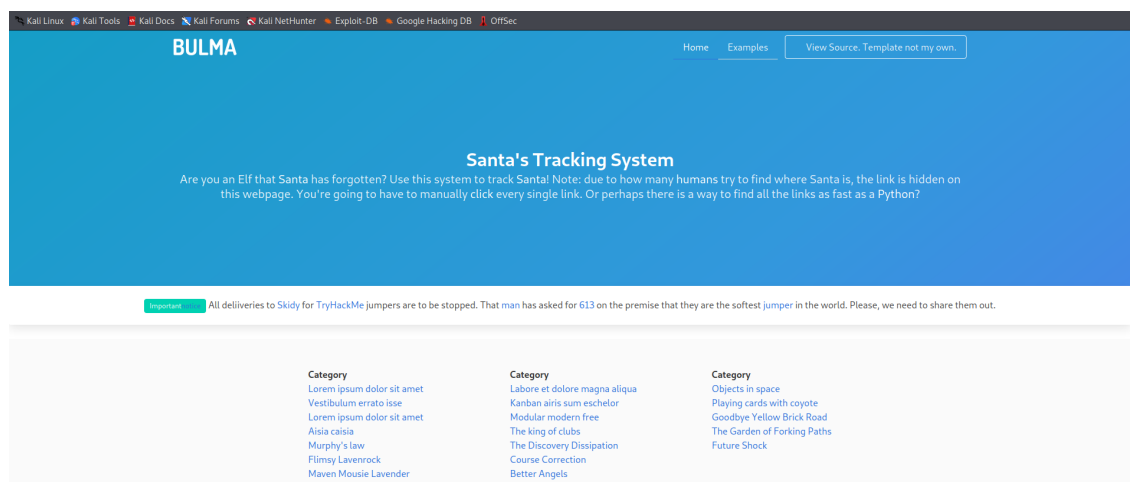
```
kali@kali: ~  
File Actions Edit View Help  
Read data files from: /usr/bin/../share/nmap  
Nmap done: 1 IP address (1 host up) scanned in 33.02 seconds  
  
(kali@kali)-[~]  
$ sudo nmap -A 10.10.225.69 -T5  
[sudo] password for kali:   
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-11 23:17 EDT  
Warning: 10.10.225.69 giving up on port because retransmission cap hit (2).  
Nmap scan report for 10.10.225.69  
Host is up (0.20s latency).  
Not shown: 998 closed tcp ports (reset)  
PORT      STATE SERVICE VERSION  
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)  
| ssh-hostkey:  
|   2048 31:4e:6f:1b:9b:4d:a6:9f:34:f0:ca:3e:96:31:a6:9e (RSA)  
|   256 60:5d:1b:59:24:8b:b8:7a:5f:1c:75:55:5f:bf:e0:83 (ECDSA)  
|_  256 05:08:d8:66:d1:04:cf:91:8c:6a:56:55:df:07:a4:d6 (ED25519)  
80/tcp    open  http      unicorn  
|_ fingerprint-strings:  
|_   FourOhFourRequest:  
|_     HTTP/1.1 404 Not Found  
|_     date: Tue, 12 Jul 2022 03:18:19 GMT  
|_     server: unicorn  
|_     content-length: 22  
|_     content-type: application/json  
|_     {"detail":"Not Found"}  
|_
```

Step 2

Add the port 80 behind the IP address and we get the page as below.

Question 2: What templates are being used?

Answer : BULMA



Step 3

Right click on the page and press view page source. Then, we will get the link which is the api.

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

Answer : /api/

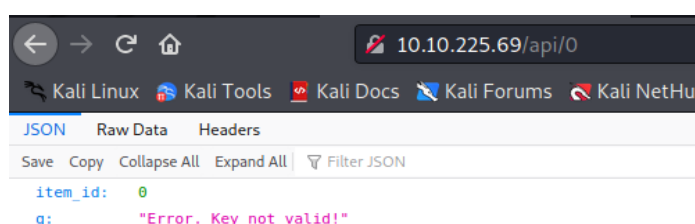
```

80      <li><a href="#">Maven Mousie Lavender</a></li>
81    </ul>
82  </div>
83  <div class="column is-3">
84    <h2><strong>Category</strong></h2>
85    <ul>
86      <li><a href="#">Labore et dolore magna aliqua</a></li>
87      <li><a href="#">Kanban airis sum eschelor</a></li>
88      <li><a href="http://machine_ip/api/api_key">Modular modern free</a></li>
89      <li><a href="#">The king of clubs</a></li>
90      <li><a href="#">The Discovery Dissipation</a></li>
91      <li><a href="#">Course Correction</a></li>
92      <li><a href="#">Better Angels</a></li>
93    </ul>

```

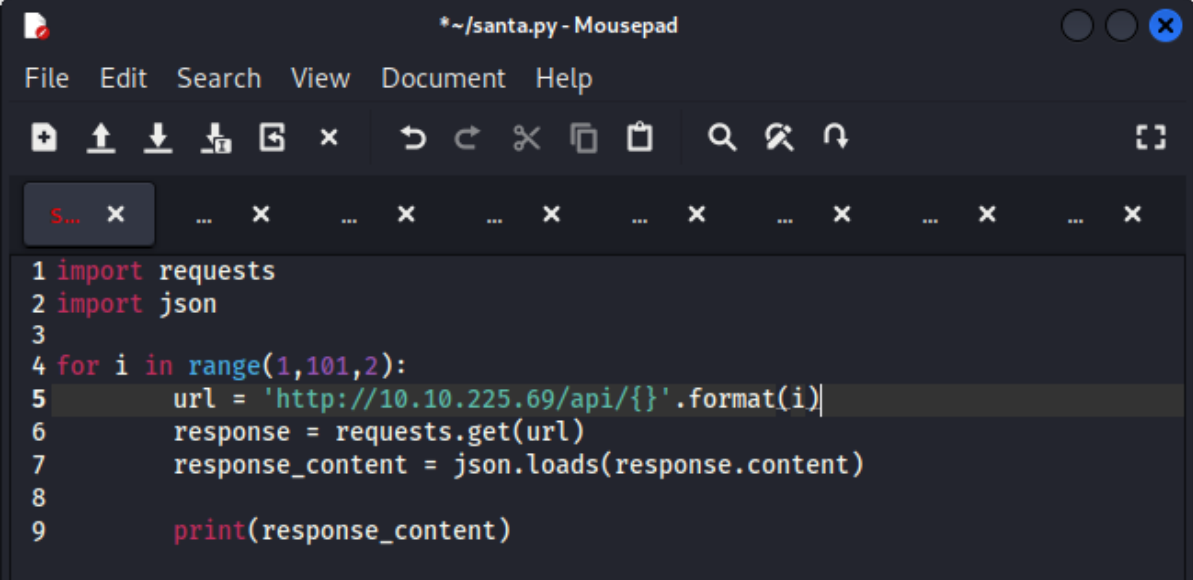
Step 4

We got the hint from tryhackme website that the key for the API is between 0 and 100. We must try out to know that what is the correct key. Starting from 0, we add the api key behind the IP address and search it in a new tab. The result showed 'Error. Key not valid' because it is not the correct key. However, it is time consuming and difficult to try it out one by one. So, we can use python to figure it out.



Step 5

Below is the python code to find out the correct api key. We set the range from 1 to 101 with range of 2 because the hint stated that the key is an odd number. Save this code as a python file.



```
1 import requests
2 import json
3
4 for i in range(1,101,2):
5     url = 'http://10.10.225.69/api/{}'.format(i)
6     response = requests.get(url)
7     response_content = json.loads(response.content)
8
9     print(response_content)
```

Step 6

Open Terminal and run the python file. It will detect the key one by one. Once it is done, we can see that there is a valid key which is 57.

Question 5 : Where is Santa right now?

Answer : 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)

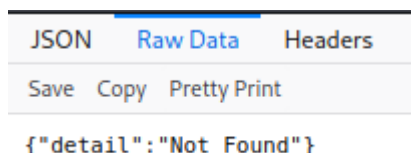
Answer : 57

```
(kali@kali)-[~]
$ sudo python3 santa.py
{'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!'}
{'item_id': 61, 'q': 'Error. Key not valid!'}
```

Solution:

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

Answer: {"detail":"Not Found"}



Thought Process/Methodology:

First and foremost, we used the nmap command to find the open port. Then, we found the port and we were able to access the page. We opened the page by adding the port number behind our IP address and we viewed the page source. We saw a link with api word. From the hint from tryhackme website, we know that the api key is in between 0-100. It is not encouraged for us to test it one by one by adding each port numbers behind the IP address. So, we wrote a python code and run it in Terminal instead. All the keys showed error except key 57. By that, we knew that 57 is the correct api key. Finally, we know where is Santa right now.

Day 17: [Reverse Engineering] ReverseELFneering

Tools used: Kali Linux,terminal

Walkthrough:

Step 1

To start with it, use the ssh tool to communicate with the computer of elfmceager as the username and password are provided in THM.

```
(kali㉿kali)-[~]
$ ssh elfmceager@10.10.199.137
The authenticity of host '10.10.199.137 (10.10.199.137)' can't be established.
ED25519 key fingerprint is SHA256:+Yl8Ef3BjQ7HNTMf6qew50LnmiqEXXSzLqgX82k/RSg.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:10: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.199.137' (ED25519) to the list of known hosts.
elfmceager@10.10.199.137'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 Thu Jul 14 09:00:53 UTC 2022

System load:  0.43                       Processes:    99
Usage of /:   39.4% of 11.75GB            Users logged in:  0
Memory usage: 8%                         IP address for ens5: 10.10.199.137
Swap usage:  0%

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

Last login: Wed Dec 16 18:25:51 2020 from 192.168.190.1
```

Step 2

Next, we start the radare2 in debugger mode and execute the file entitle **challenge1**.

```
elfmceager@tbfc-day-17:~$ ls
challenge1 file1
elfmceager@tbfc-day-17:~$ r2 -d ./challenge1
Process with PID 1539 started...
= attach 1539 1539
bin.baddr 0x00400000
Using 0x400000
Warning: Cannot initialize dynamic strings
asm.bits 64
[0x00400a30]>
```

Step 3

We analyse the program (all the symbols and entry-points) by using the command **aa**. Then, we list all the function which contain the “main” (most programs have an entry point defined as main).

```
[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]> afl | main
sh: 1: main: not found
[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_finddomain_subfreeres
0x0048fa40     16 247 → 237  sym._nl_unload_domain
```

Step 4

Lastly, we use the **pdf** command which stands for print disassembly function for all the function consists of “main”.

Based on the answer of question 5 which is one because the **local_ch** copy (using **mov**) the value of **1** from the source.

For question 6, the value of **eax** become 6 as it multiply (using **mov**) the value of **local_8h** which is 6. Before that, **eax** also obtain a value of **1** as it is copy from the **local_ch** file which has the value of 1. So it may becomes $1 \times 6 = 6$ solution.

In question 7, the value of **local_4h** is 6 as it copy (using **mov**) the value from **eax**.

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

Answer: 1

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

Answer: 6

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

Answer: 6

```

[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

```

Solution:

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

Answer:

	1	2	4	8
Byte	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Word	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Double Word	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Quad	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Single Precision	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>
Double Precision	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>

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

Answer: aa

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

Answer: db

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

Answer: dc

Thought Process/Methodology:

Firstly, we use the ssh tool to communicate with the computer of elfmceager as the username and password are provided in THM. Then we debug the program and analyse it. After using the PDF command to print all the disassembly functions, we can see the content and the value of each file inside it.

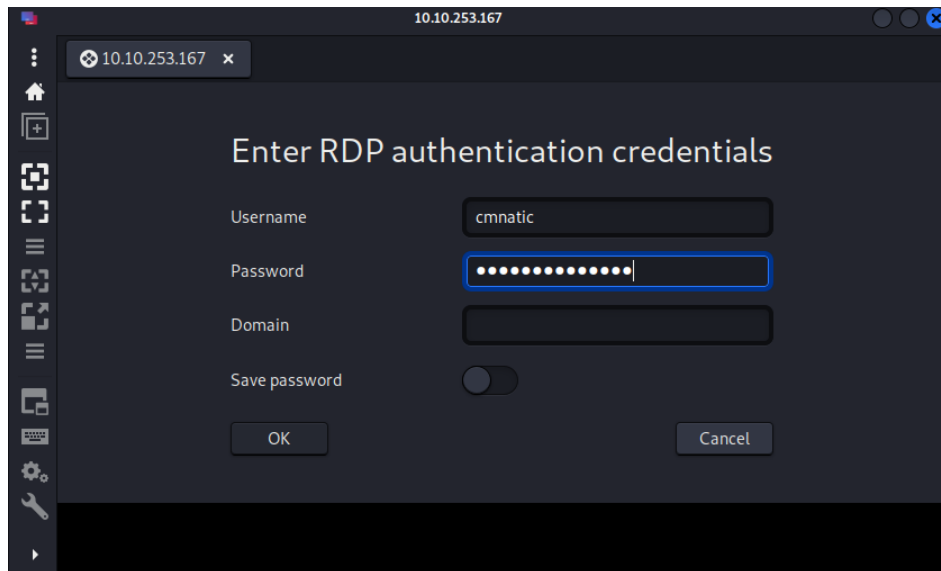
Day 18: [Reverse Engineering] The Bits of Christmas

Tools used: Kali Linux, Remmina

Walkthrough:

Step 1

We connect to the target instance provided with the given username and password in Remmina.



Step 2

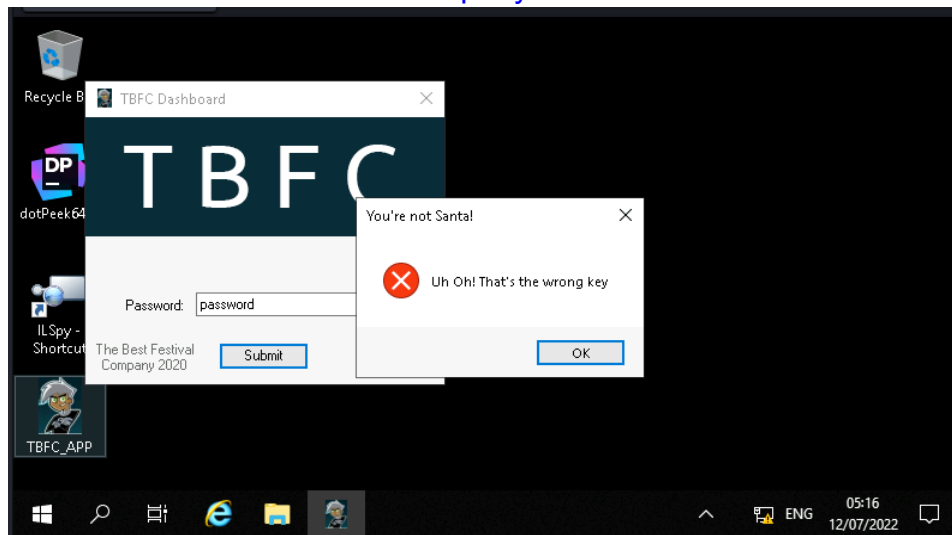
We open the TBFC_APP and try to enter something to get some clue of what to do.

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

Answer: Uh Oh! That's the wrong key

Question 2: What does TBFC stand for?

Answer: The Best Festival Company



Step 3

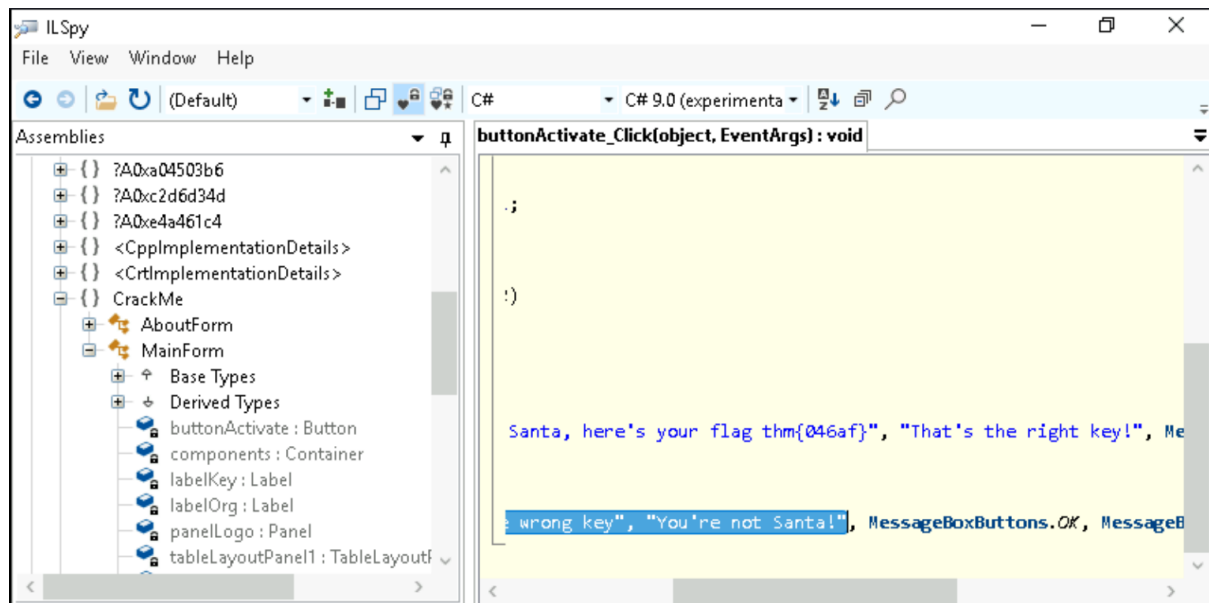
Load TBFC_APP into ILSpy and expand the resource to find the source code of the Submit button which can be useful.

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

Answer: CrackMe

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

Answer: MainForm



Step 4

We found the password of santa in the source code of the button.

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

Answer: buttonActivate_Click

Question 6: What is Santa's password?

Answer: santapassword321

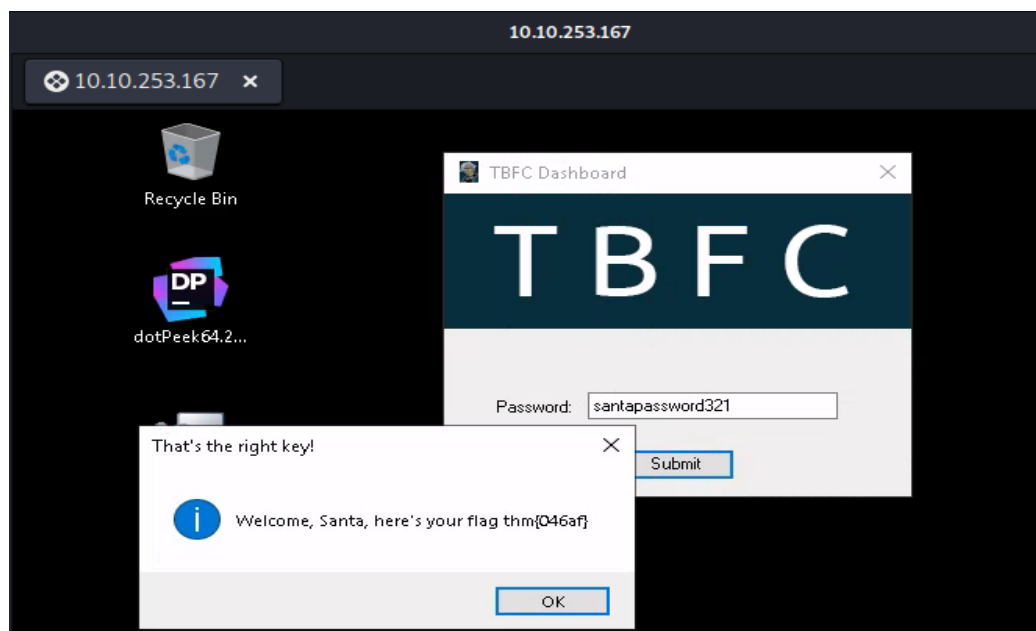
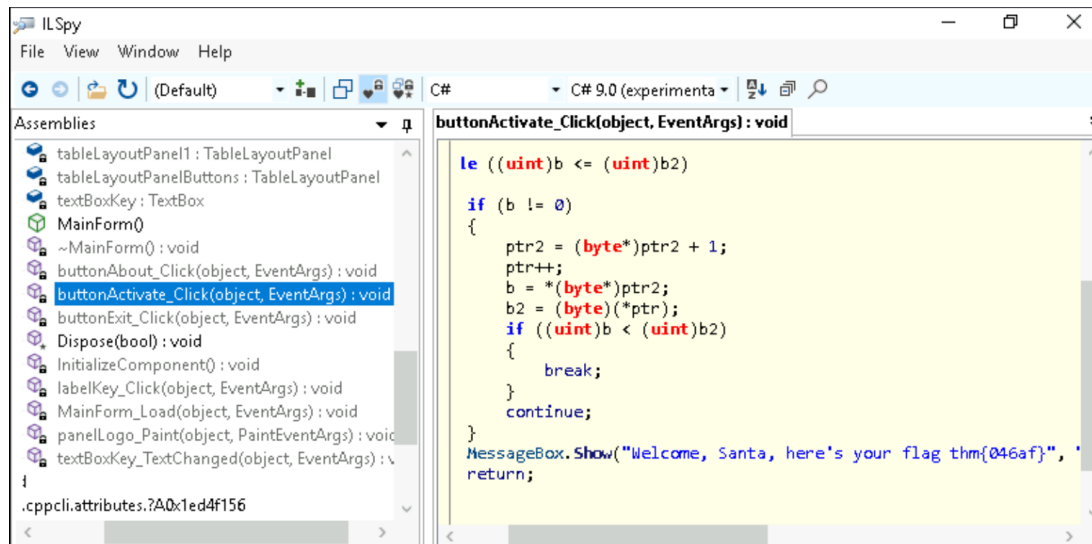


Step 5

We search in the source code or can also enter the password found into the TBFC dashboard to get the flag.

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

Answer: thm{046af}



Thought Process/Methodology:

Firstly, we connect to the provided instance in Remmina with the given credentials. We open the TBFC_APP and try to enter something to get some clue of what to do. After loading the TBFC_APP into ILSpy to verify that it is a .NET application, we look through the objects to find the helpful source code of the interactive "Submit" button. We can find the password in the source code of the button and use it in the app to get the flag. Not only that, we can also find the flag in the source code.

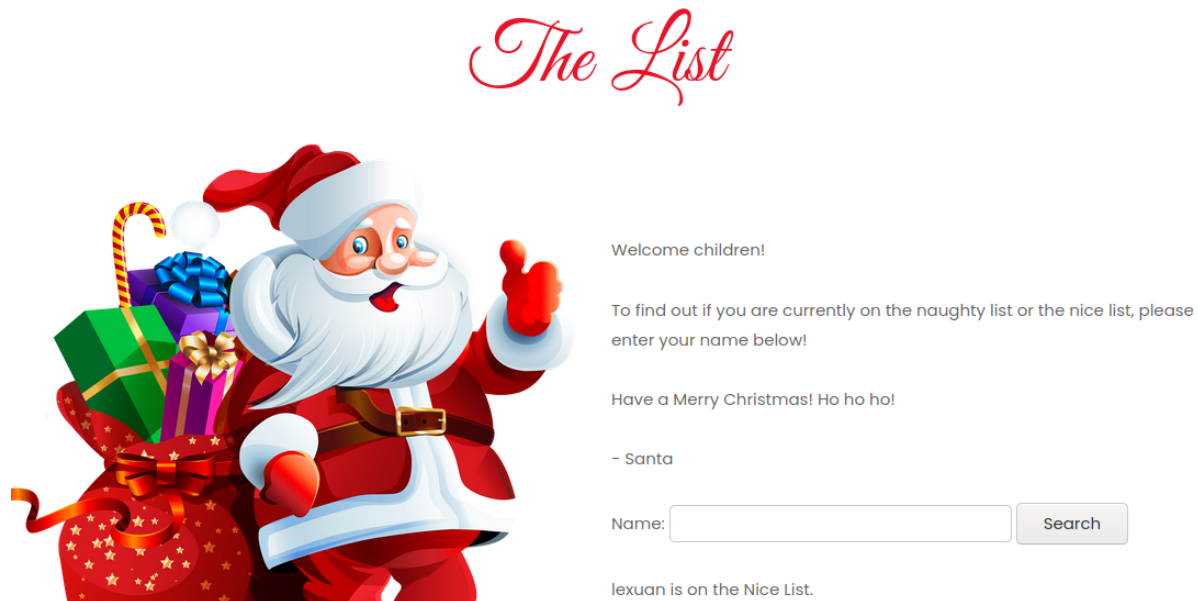
Day 19: [Web Exploitation] The Naughty or Nice List

Tools used: Kali Linux, terminal, fileformat.io

Walkthrough:

Step 1

Firstly, access to the IP address and a page as below will show up. Then, search by any names. If the name is not on the list, it will show the name is on Naughty List. If the name is on the list, it will show the name is on the Nice List.



Step 2

Compare the url and figure it out by using fileformat.io or search for the unicode in google.

File Edit Format View Help

```
http://10.10.77.185/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3Dlexuan
```

```
http://10.10.77.185/?proxy=http://list.hohoho:8080/search.php?name=lexuan
```

Step 3

Now we got the root and we can try whether it works. Use

<http://10.10.77.185/?proxy=http://list.hohoho:8080> to check. It shows "Not Found.

The requested URL was not found on this server." That means that it is not working.

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

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



Name:

Search

Not Found

The requested URL was not found on this server.

Step 4

Next, we can change to port 80(<http://10.10.77.185/?proxy=http://list.hohoho:80>). It shows “Failed to connect to list.hohoho port 80:Connection refused” That means this port is not opened.

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

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



Name:

Search

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

Step 5

Next, we can change to port 22(<http://10.10.77.185/?proxy=http://list.hohoho:22>). It shows “Recv failure: Connection reset by peer”. It means port 22 is actually opened but port 22 is for SSH. We are trying to access 22 through http which SSH could not understand. Thus, it does not work here.

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

Answer: Recv failure: Connection reset by peer



Name:

Search

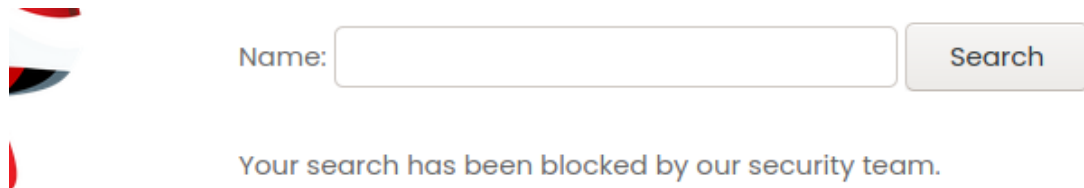
Recv failure: Connection reset by peer

Step 6

Next, we can replace the machine name and port with localhost (<http://10.10.77.185/?proxy=http://localhost>). It shows "Your search has been blocked by our security team." This means that the security team blocked it because they do not allow us to access it through localhost.

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

Answer: Your search has been blocked by our security team.

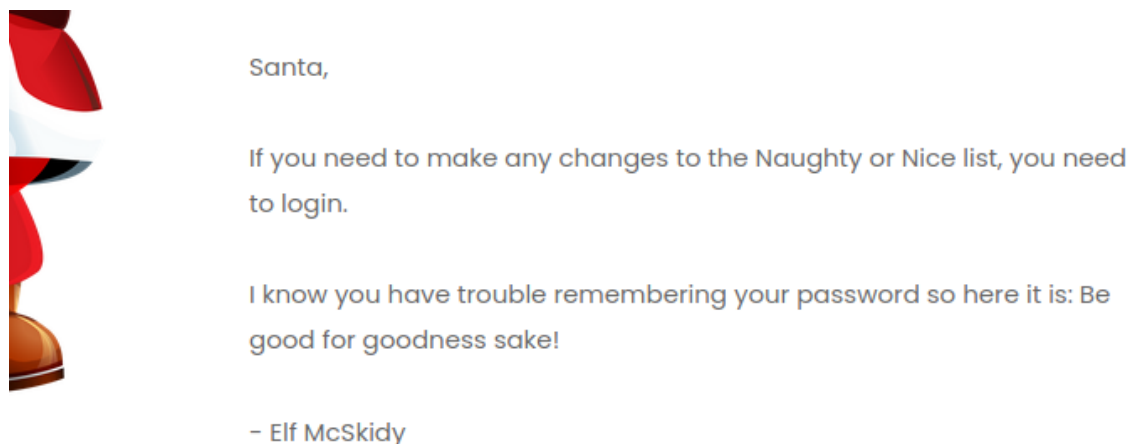


Step 7

The host name needs to start with 'list.hohoho', we need to access it by (<http://10.10.77.185/?proxy=http://list.hohoho.localtest.me>) The system accept 'list.hohoho', at the same time we add the 'localtest.me' behind it, the system will also accept it. We have already set 'localtest' to localhost. Then, the page shows the Santa's password.

Question 6: What is Santa's password?

Answer: Be good for goodness sake!



Step 8

Once we got the password, we can login to the system. Then the page as below shows up. We press the DELETE NAUGHTY LIST, and a flag will appear.

Question 7: What is the challenge flag?

Answer: THM{EVERYONE_GETS_PRESENTS}

List Administration

This page is currently under construction.

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



Solution:

Question 1: Which list is this person on?

Answer:

	Naughty	Nice
YP	<input type="radio"/>	<input checked="" type="radio"/>
Ian Chai	<input type="radio"/>	<input checked="" type="radio"/>
Timothy	<input checked="" type="radio"/>	<input type="radio"/>
JJ	<input checked="" type="radio"/>	<input type="radio"/>
Tib3rius	<input type="radio"/>	<input checked="" type="radio"/>
Kanes	<input checked="" type="radio"/>	<input type="radio"/>

Thought Process/Methodology:

First and foremost, we accessed the IP address and searched for several names to check whether they are on the list. Then, we were able to figure out the unicode of the URL by using fileformat.io or google. We used different ports such as 8080, 80 and 22 for the URL to see what is displayed on the page. We tried replacing the machine name and port to check what is displayed and it showed that the security team blocked it. Next, we know that the host name needs to be list.hohoho, then we added localtest.me behind it ,then the system accepted it and we got the Santa's password. We login to the system with the password and we pressed the DELETE NAUGHTY LIST. Lastly, a flag appeared.

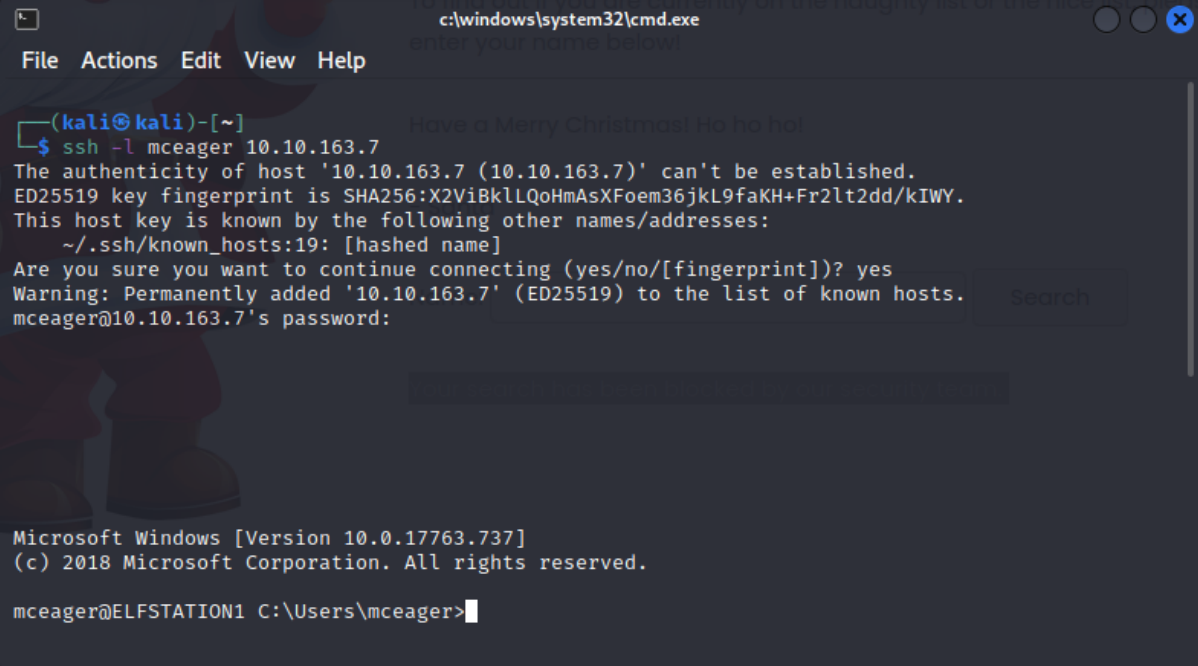
Day 20: [Blue Teaming] Powershell to the rescue

Tools used: Kali Linux, Terminal, Powershell

Walkthrough:

Step 1

Type the command `ssh -l mceager 10.10.163.7` to connect to the remote machine via SSH. (note that 10.10.163.7 is the remote machine's IP address given)



The screenshot shows a terminal window titled 'c:\windows\system32\cmd.exe' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(kali㉿kali)-[~]'. The user enters the command 'ssh -l mceager 10.10.163.7'. The terminal displays the SSH connection process, including a warning about the host's authenticity and a confirmation to add it to the known hosts list. The user enters 'yes' to confirm. The terminal then shows the Windows login screen for 'mceager@ELFSTATION1' with the password prompt. The user enters the password, and the terminal shows the Windows version and copyright information.

```
(kali㉿kali)-[~]  
$ ssh -l mceager 10.10.163.7  
The authenticity of host '10.10.163.7 (10.10.163.7)' can't be established.  
ED25519 key fingerprint is SHA256:X2ViBkLLQoHmAsXFoem36jkL9faKH+Fr2lt2dd/kIWY.  
This host key is known by the following other names/addresses:  
  ~/.ssh/known_hosts:19: [hashed name]  
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes  
Warning: Permanently added '10.10.163.7' (ED25519) to the list of known hosts.  
mceager@10.10.163.7's password:  
  
Microsoft Windows [Version 10.0.17763.737]  
(c) 2018 Microsoft Corporation. All rights reserved.  
  
mceager@ELFSTATION1 C:\Users\mceager>
```

Step 2

After connected successfully, launch PowerShell.

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

Step 3

Navigate to the Documents folder and list out the content of the directory. Read the content of elfone.txt.

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

Answer: 2 front teeth

```

PS C:\Users\mceager> Set-Location .\Documents\
PS C:\Users\mceager\Documents> Get-ChildItem -File -Hidden -ErrorAction SilentlyContinue

Directory: C:\Users\mceager\Documents

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

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

```

Step 4

Navigate to desktop and list out the hidden directory. Then, navigate to the hidden directory and read the file in the hidden directory.

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?

Answer: Scrooged

```

PS C:\Users\mceager\desktop> Get-ChildItem -Directory -Hidden -ErrorAction SilentlyContinue

Directory: C:\Users\mceager\desktop

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

PS C:\Users\mceager\desktop> Set-Location -Path C:\Users\mceager\desktop\elf2wo
PS C:\Users\mceager\desktop\elf2wo> Get-ChildItem

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!

```

Step 5

Navigate to the C directory and list out the contents of the directory. We'll see the Windows folder there. Navigate to the Windows folder. Find out the hidden directory in the Windows folder using the given filter.

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)

Answer: 3lfthr3e

```
PS C:\> Get-ChildItem
```

Directory: C:\

Mode	LastWriteTime	Length	Name
d-----	9/15/2018 12:19 AM		PerfLogs
d-r----	11/26/2020 11:24 AM		Program Files
d-----	11/23/2020 1:43 PM		Program Files (x86)
d-r----	12/7/2020 10:28 AM		Users
d-----	12/3/2020 1:15 PM		Windows

```
PS C:\> Set-Location .\Windows\
```

```
PS C:\Windows> Get-ChildItem -Directory -Hidden -ErrorAction SilentlyContinue -Filter '*3*' -Recurse
```

Directory: C:\Windows\System32

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

Step 6

Since the directory path is C:\Windows\System32\3lfthr3e, we navigate to the path and list out the hidden files in the directory. To get word count of the first file, enter the command `Get-Content -Path 1.txt | Measure-Object -Word`. While to get the string of an exact position in the first file, enter the command `(Get-Content -Path 1.txt)[551]&((Get-Content -Path 1.txt)[6991])`

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

Answer: 9999

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

Answer: Red Ryder

```
PS C:\Windows> Set-Location .\System32\3lfthr3e
PS C:\Windows\System32\3lfthr3e> Get-ChildItem -Hidden
```

Directory: C:\Windows\System32\3lfthr3e

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

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

Step 7

To figure out what exactly Elf3 wants, we search it from the second file using the command `Select-String .\2.txt -Pattern 'redryder'`

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)

Answer: redryderbbgun

```
PS C:\Windows\System32\3lfthr3e> Select-String .\2.txt -Pattern 'redryder'  
2.txt:558704:redryderbbgun
```

Solution:

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

Answer: login name

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

Thought Process/Methodology:

Firstly, we got connected to the remote machine via SSH. We then launched powershell in the terminal. As guided, we searched for the hidden file by navigating to the Documents folder and listing out the contents in it. We found a file named elfone.txt. We read the file and found out that the Elf 1 wants 2 front teeth. Next, we were required to search for a hidden directory in desktop. We first navigated to desktop and listed out the hidden directories in it. A folder named elf2wo was shown. We navigated into the folder and listed out its content. A file was shown and we read the file. We got to know that the movie that Elf 2 wants is Scrooged. Next, we were required to look for a hidden directory in the Windows folder. Hence, we navigated to the Windows folder to find out the hidden directory in it using the given filter. The hidden folder and its respective path was then shown. We navigated to the given path of the folder and listed out its content. Two text files were shown. As required, we first figured out the word count and the string of the given position of the first file using the given command in TryHackMe. Lastly, we found out what exactly Elf 3 wants by using the phrase we had gotten in the previous step for the pattern parameter in the command.