PSP0201
Week 5
Writeup

Group Name: ikun no 1

Members

ID	Name	Role
1211102058	CHU LIANG CHERN	Leader
1211103095	SIDDIQ FERHAD BIN KHAIRIL ANUAL	Member
1211101401	CHONG JII HONG	Member
1211103206	NG KAI KEAT	Member

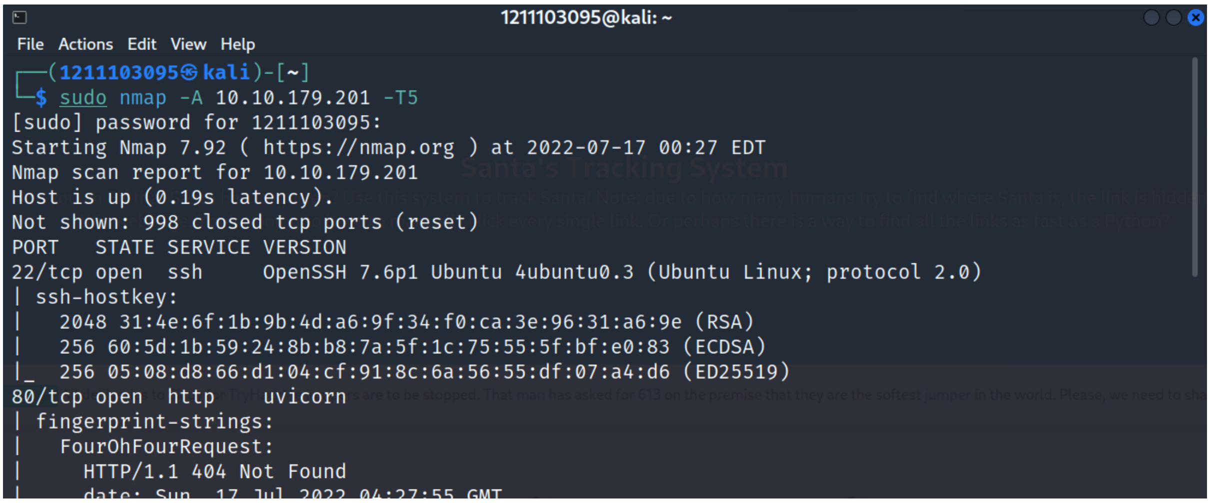
Day 16: Scripting – Help! Where is Santa?

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1

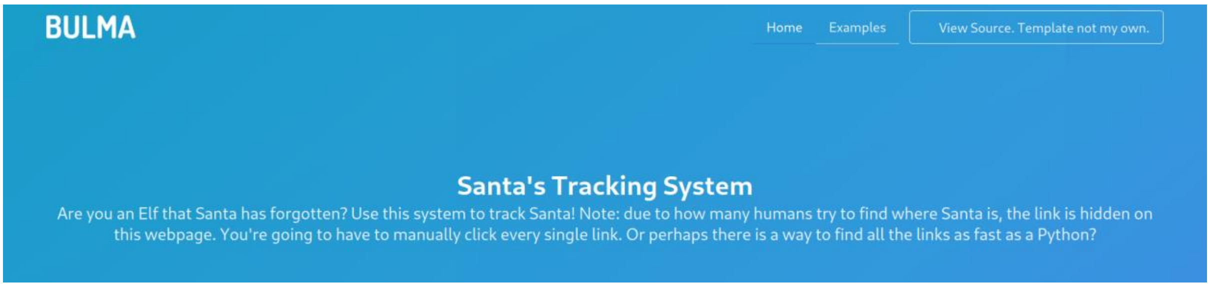
The port number for the web server is obtained by using nmap which is port 80.



```
┌──(1211103095㉿kali)-[~]
└─$ sudo nmap -A 10.10.179.201 -T5
[sudo] password for 1211103095:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-17 00:27 EDT
Nmap scan report for 10.10.179.201
Host is up (0.19s 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    uvicorn
| fingerprint-strings:
|   FourOhFourRequest:
|     HTTP/1.1 404 Not Found
|     date: Sun, 17 Jul 2022 04:27:55 GMT
```

Question 2

BULMA is the templates that are being used.

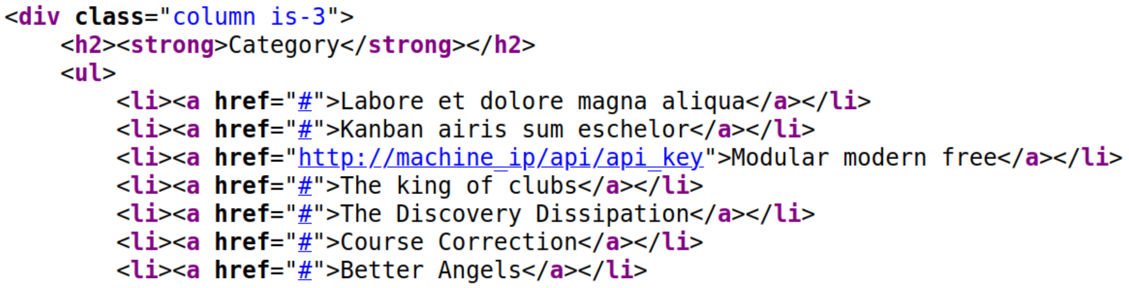


Santa's Tracking System

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

Question 3

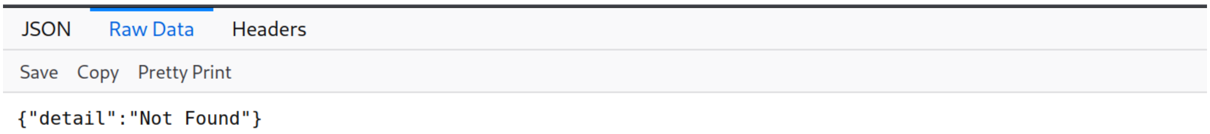
The directory for the API is /api/.



```
<div class="column is-3">
    <h2><strong>Category</strong></h2>
    <ul>
        <li><a href="#">Labore et dolore magna aliqua</a></li>
        <li><a href="#">Kanban airis sum eschelor</a></li>
        <li><a href="http://machine_ip/api/api_key">Modular modern free</a></li>
        <li><a href="#">The king of clubs</a></li>
        <li><a href="#">The Discovery Dissipation</a></li>
        <li><a href="#">Course Correction</a></li>
        <li><a href="#">Better Angels</a></li>
```

Question 4

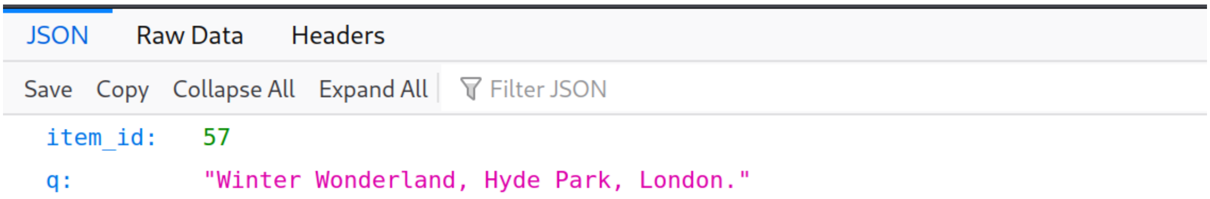
The Raw Data returned if no parameters are entered is as shown:



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

Question 5

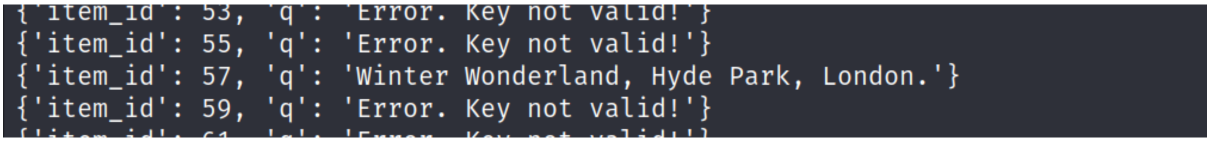
Santa is at:



```
item_id:    57
q:          "Winter Wonderland, Hyde Park, London."
```

Question 6

The correct API key is 57.



```
{'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!'}
```

Thought Process/Methodology:

Having accessed the target machine, we proceeded by using nmap to get the port number that is open. After that, we will be shown with a website. We proceeded by using 'View page source' to get the directory for the API. Then, we proceeded by using Python to get the correct API key. Once we get the API key, the location of Santa will be shown right beside the correct API key in the terminal.

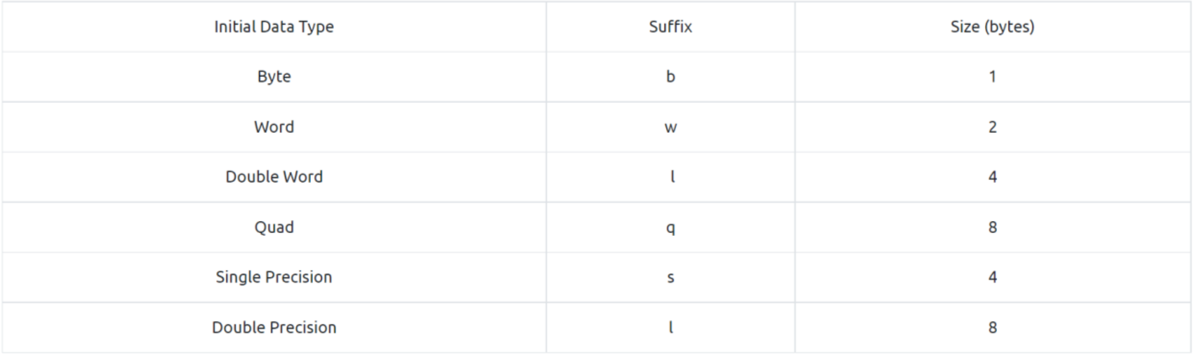
Day 17: Reverse Engineering – ReverseELFneering

Tools used: Kali Linux

Solution/walkthrough:

Question 1

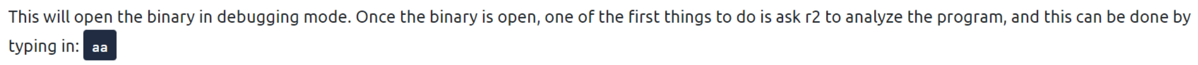
Data type with the size in bytes:



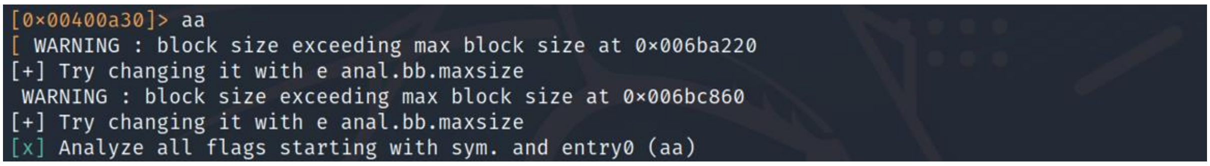
Initial Data Type	Suffix	Size (bytes)
Byte	b	1
Word	w	2
Double Word	l	4
Quad	q	8
Single Precision	s	4
Double Precision	l	8

Question 2

The command to analyse the program in radare2 is aa.



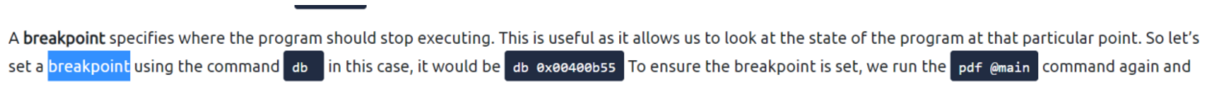
This will open the binary in debugging mode. Once the binary is open, one of the first things to do is ask r2 to analyze the program, and this can be done by typing in: `aa`



```
[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)
```

Question 3

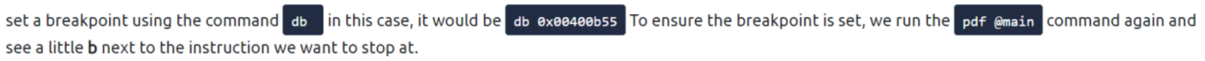
The command to set a breakpoint in radare2 is db.



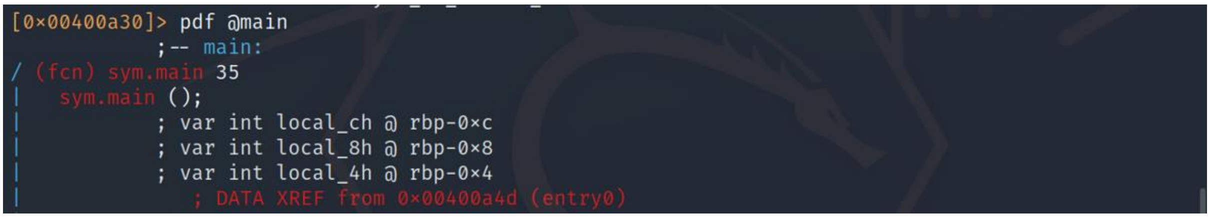
A **breakpoint** specifies where the program should stop executing. This is useful as it allows us to look at the state of the program at that particular point. So let's set a breakpoint using the command `db` in this case, it would be `db 0x00400b55` To ensure the breakpoint is set, we run the `pdf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

Question 4

The command to execute the program until we hit a breakpoint is pdf @main.



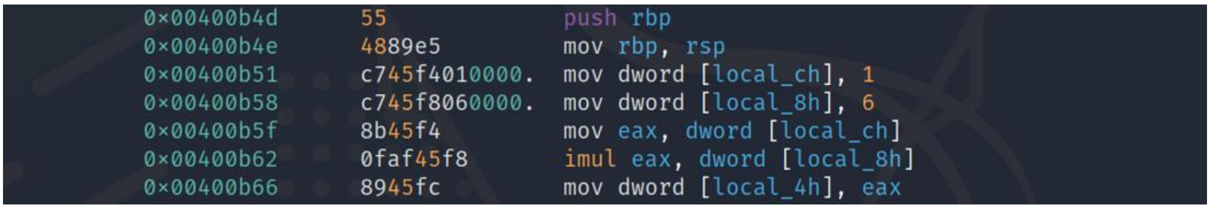
set a breakpoint using the command `db` in this case, it would be `db 0x00400b55` To ensure the breakpoint is set, we run the `pdf @main` command again and see a little **b** next to the instruction we want to stop at.



```
[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)
```

Question 5

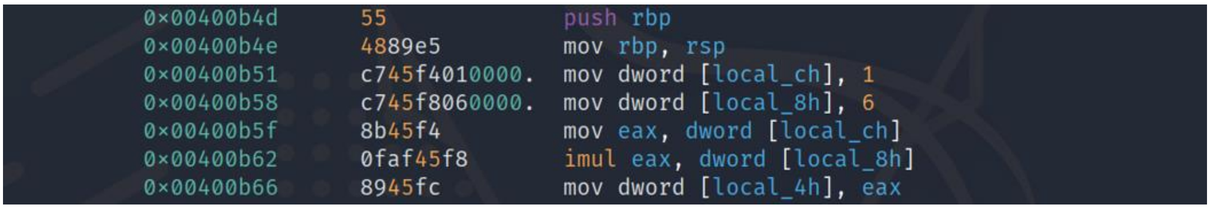
The value of local_ch when its corresponding movl instruction is called (first if multiple) is 1.



```
            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
```

Question 6

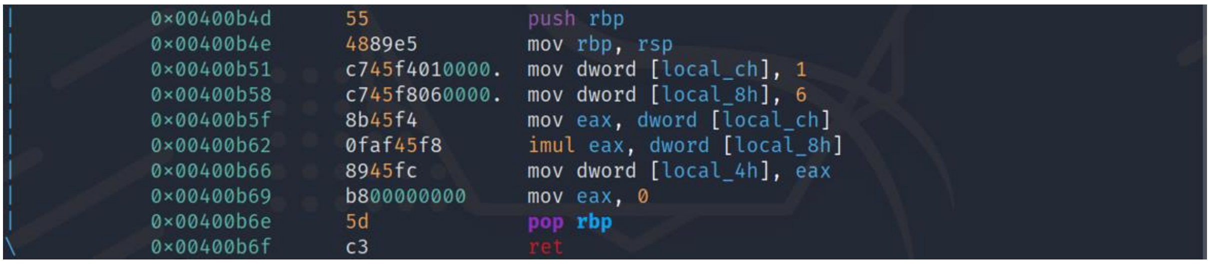
The value of eax when the imull instruction is called is 6. (The value of eax is 1, then multiply by 6 from local_8h).



```
            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
```

Question 7

The value of local_4h before eax is set to 0 is 6. (The value of eax from before which is 6, is copied to local_4h).



```
|           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:

Having accessed the target machine, we proceeded by using ssh. By using the command "ls", we found out that there are 2 files in the directory. We then proceeded by accessing the challenge1 file by using the command "r2 -d ./challenge1". Next, we proceeded by asking radare2 to analyze the program by using the command "aa" followed by the command "afl | grep main" to find the list of functions. We then found that there actually is a function at main. After that, we examined the assembly code at main by running the command "pdf @main". We will then be shown with several things like instructions, variables like local_ch and local_8h and also its values.

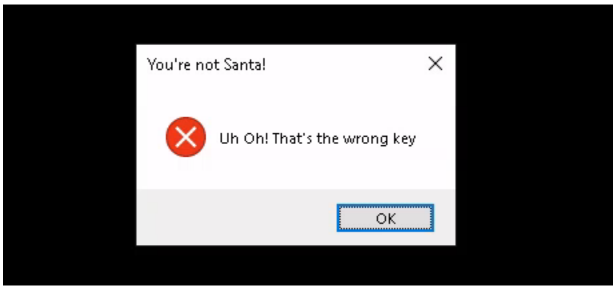
Day 18: Reverse Engineering – The Bits of Christmas

Tools used: Kali Linux, Remmina

Solution/walkthrough:

Question 1

"Uh Oh! That's the wrong key" shows up if we enter the wrong password for TBFC_APP.

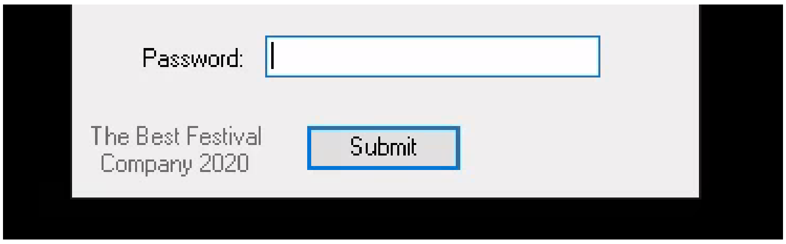


You're not Santa!

Uh Oh! That's the wrong key

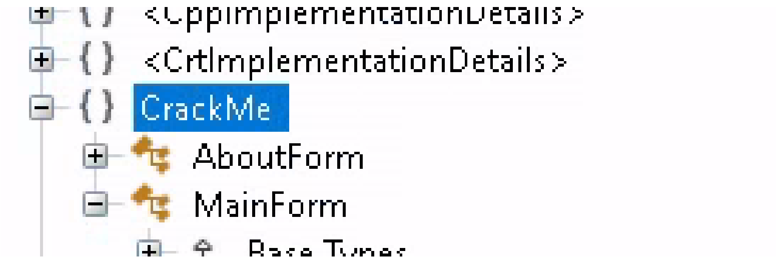
Question 2

TBFC stands for The Best Festival Company.



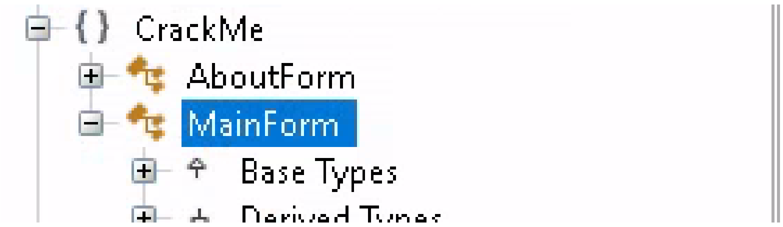
Question 3

After decompiling the TBFC_APP with ILSpy, the module that catches my attention is CrackMe.



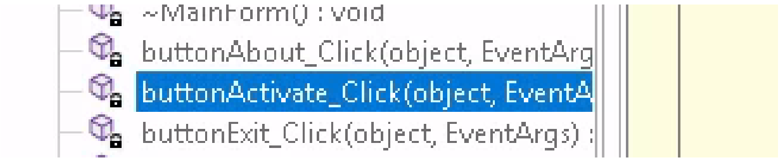
Question 4

MainForm contains the information we are looking for.



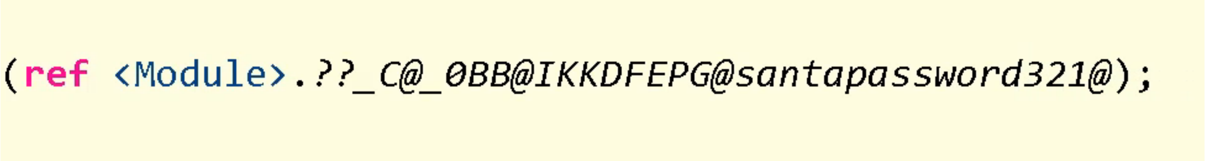
Question 5

buttonActivate_Click contain the information we are seeking.


~MainForm() : void
buttonAbout_Click(object, EventArg
buttonActivate_Click(object, EventA
buttonExit_Click(object, EventArgs) :

Question 6

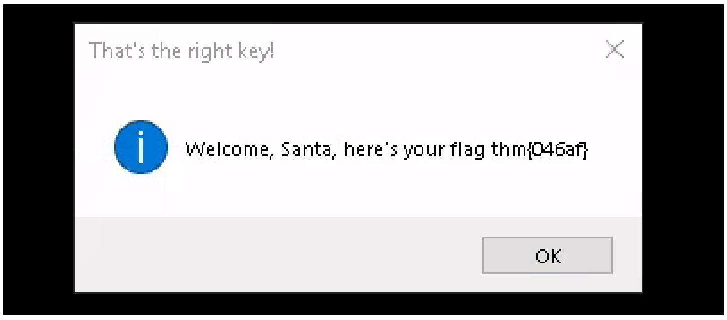
Santa's password is santapassword321.



```
(ref <Module>.??_C@_0BB@IKKDFEPG@santapassword321@);
```

Question 7

After logging in, we will be shown with the flag as shown below:



That's the right key!

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

Thought Process/Methodology:

Having accessed the target machine, we proceeded by using Remmina to access the machine. After successfully logging in, we will be shown with a Windows GUI. We proceeded by running ILSpy and navigate to File > Open > TBFC_APP. After decompiling the app, we then navigate to CrackMe > MainForm > buttonActivate_Click. We will then be shown with Santa's password. We proceeded by using the password to login to TBFC_APP. Having doing this, we will be shown with the flag.

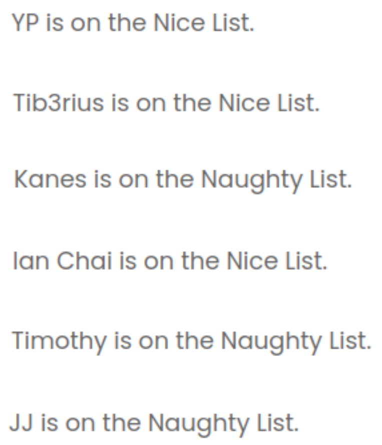
Day 19: Web Exploitation – The Naughty or Nice List

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1

The list this person is on:



YP is on the Nice List.

Tib3rius is on the Nice List.

Kanes is on the Naughty List.

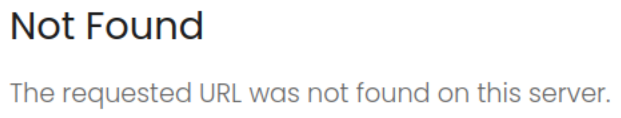
Ian Chai is on the Nice List.

Timothy is on the Naughty List.

JJ is on the Naughty List.

Question 2

"The requested URL was not found on this server." is displayed on the page.

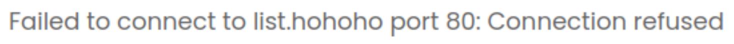


Not Found

The requested URL was not found on this server.

Question 3

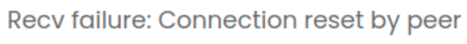
"Failed to connect to list.hohoho port 80: Connection refused" is displayed on the page.



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

Question 4

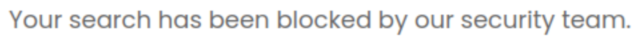
"Recv failure: Connection reset by peer" is displayed on the page.



Recv failure: Connection reset by peer

Question 5

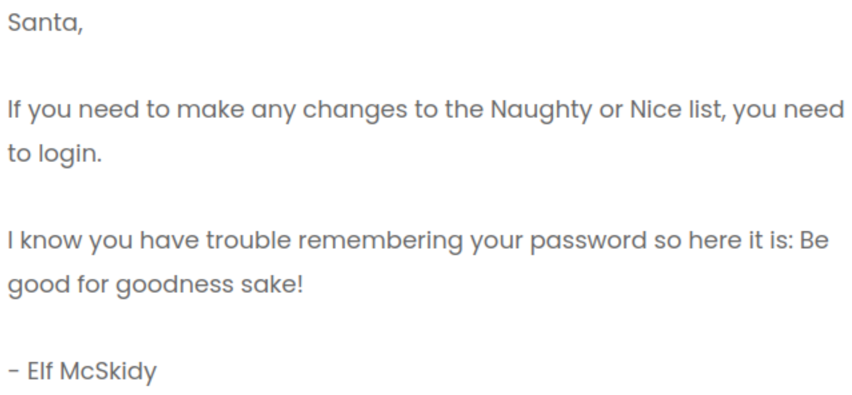
"Your search has been blocked by our security team." is displayed on the page.



Your search has been blocked by our security team.

Question 6

By setting the hostname in the URL to "list.hohoho.localtest.me", we obtained Santa's password as shown below:



Santa,

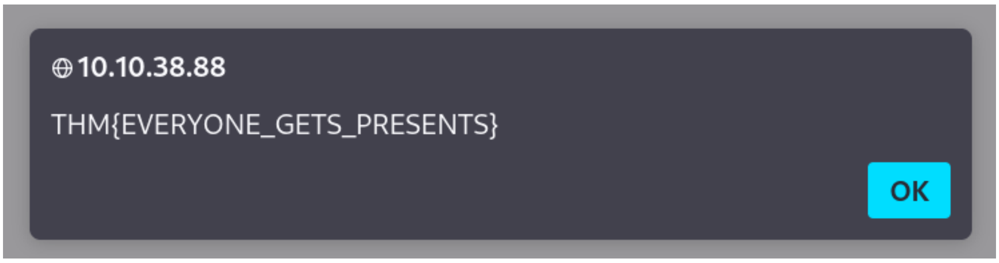
If you need to make any changes to the Naughty or Nice list, you need to login.

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

- Elf McSkidy

Question 7

After successfully logging in, the flag will be shown as below:



10.10.38.88

THM{EVERYONE_GETS_PRESENTS}

Thought Process/Methodology:

Having accessed the target machine, we will be shown with a website. We then proceeded by trying to fetch the root of the same site. We will be shown with a message “Not Found. The requested URL was not found on this server.". Next, we proceeded by changing the port number from 8080 to just 80. We will be shown with a message "Failed to connect to list.hohoho port 80: Connection refused" which shows that port 80 is not open on list.hohoho. Next, we proceeded by changing the port number to 22 (the default SSH port). We will be shown with a message "Recv failure: Connection reset by peer" which shows that port 22 is open but did not understand what was sent. Then, we proceeded by replacing the list.hohoho hostname with "localhost" or "127.0.0.1". We will be shown with a message "Your search has been blocked by our security team.". Finally, we can then set the hostname in the URL to "list.hohoho.localtest.me". We then successfully see a message from Elf McSkidy. We proceeded by using the password given to login as Santa. Having doing this, we will be shown with an option to delete naughty list, click on it and we will be shown with a flag.

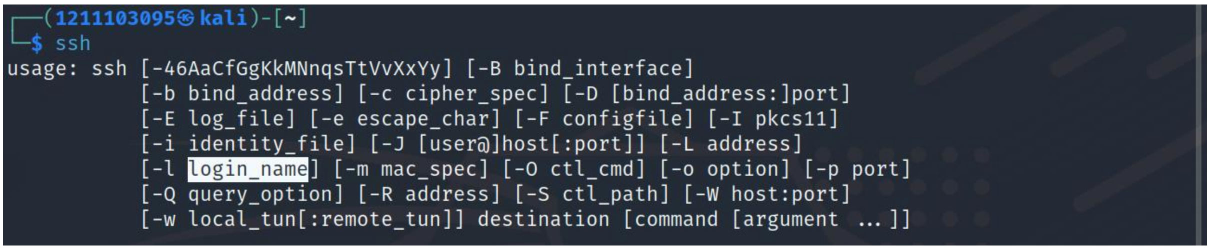
<u>Day 20: Blue Teaming – PowershELlF to the rescue</u>

Tools used: Kali Linux

Solution/walkthrough:

<u>Question 1</u>

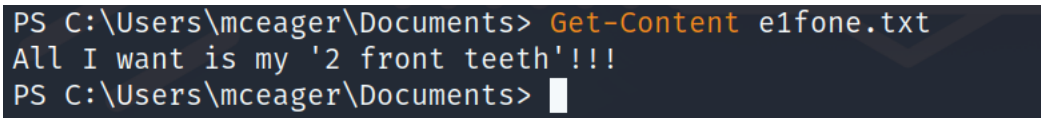
The parameter -l (login name).



```
┌──(1211103095㉿kali)-[~]
└─$ ssh
usage: ssh [-46AaCfGgKkMNnqsTtVvXxYy] [-B bind_interface]
           [-b bind_address] [-c cipher_spec] [-D [bind_address:]port]
           [-E log_file] [-e escape_char] [-F configfile] [-I pkcs11]
           [-i identity_file] [-J [user@]host[:port]] [-L address]
           [-l login_name] [-m mac_spec] [-O ctl_cmd] [-o option] [-p port]
           [-Q query_option] [-R address] [-S ctl_path] [-W host:port]
           [-w local_tun[:remote_tun]] destination [command [argument ...]]
```

Question 2

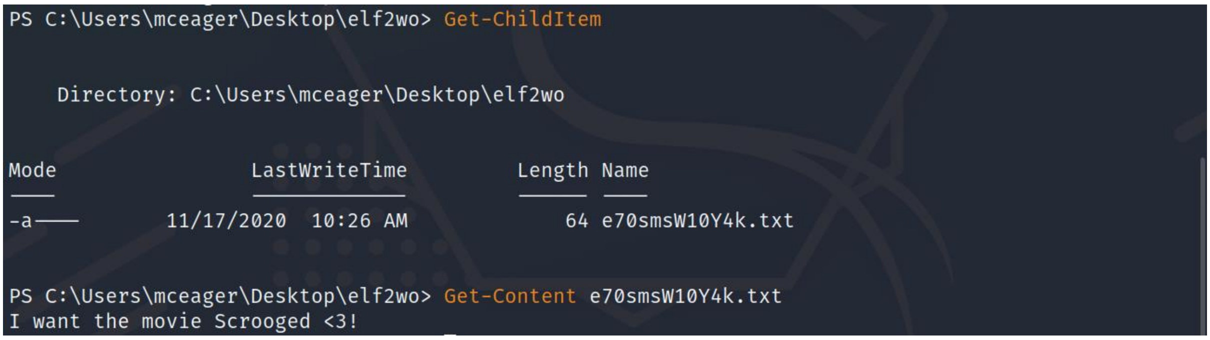
Elf 1 wants 2 front teeth.



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

Question 3

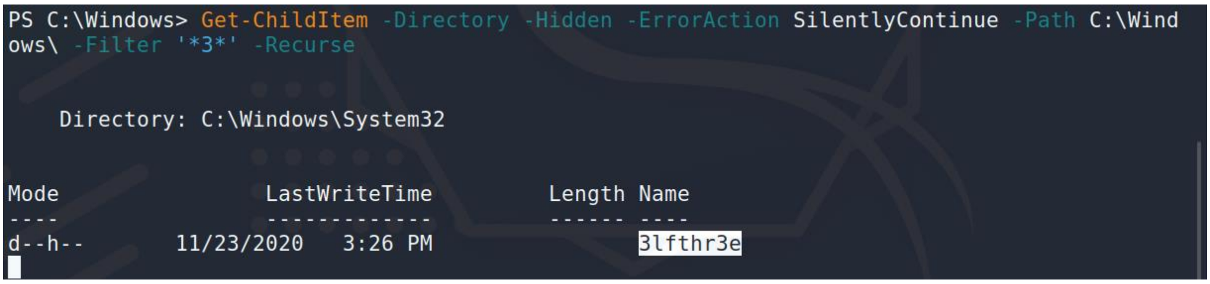
The name of the movie that Elf 2 wants is Scrooged.



```
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!
```

Question 4

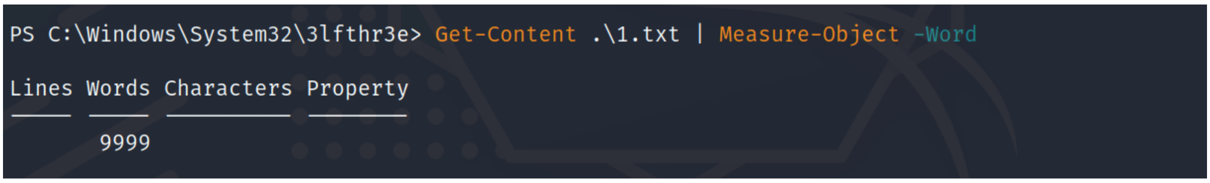
The name of the hidden folder is 3lfthr3e.



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


    Directory: C:\Windows\System32


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

Question 5

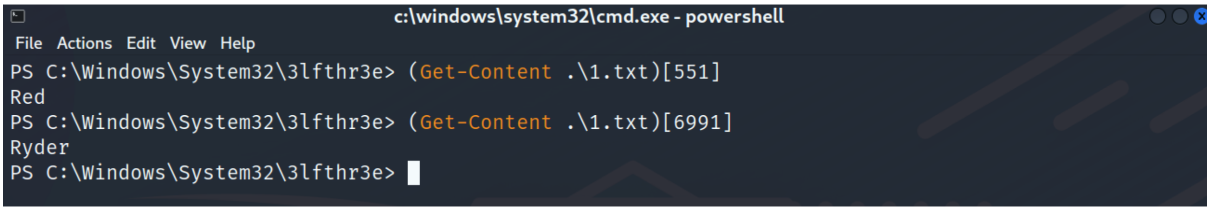
The first file contains 9999 words.



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

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

Question 6

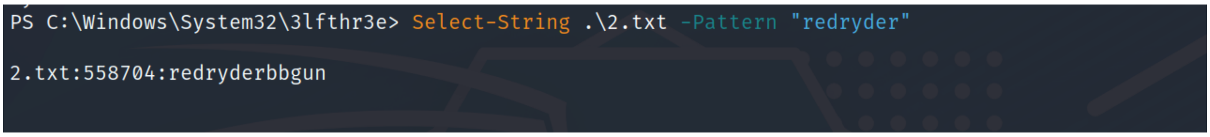
The 2 words at index 551 and 6991 in the first file are Red Ryder.


c:\windows\system32\cmd.exe - powershell
File Actions Edit View Help

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

Question 7

Elf 3 wants redryderbbgun.



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

2.txt:558704:redryderbbgun
```

Thought Process/Methodology:

Having accessed the target machine, we then proceeded by using ssh. We proceeded by using powershell command to access PowerShell. We then searched the Documents folder for a hidden file called e1fone.txt to look for what Elf 1 wanted. Next, we proceeded by searching the Desktop to look for a hidden folder called e70smsW10Y4k.txt. The name of the movie that Elf 2 wants can be found in it. Then, we proceeded by searching the Windows directory for a hidden folder called 3lfthr3e that contains files for Elf 3. After that, by using the Measure-Object cmdlet, we found that the first file contains 9999 words. We then later found the 2 words at index 551 and 6991 in the first file. Finally, by using the Select-String cmdlet, we found that Elf 3 wants redryderbbgun.