

PSP0201

Week 5

Writeup

Group Name : Mali Pape

Members:

ID	Name	Role
1211102895	Muhammad Irfan Bin Mohd Nazri	Leader
1211104288	Mohd Azriy Akmalhazim Bin Mohd Nazariee	Member
1211103634	Ho Tian Ming	Member
1211101035	Mohamad Zuhir Bin Mohamad Zailani	Member

Day 16 - (scripting) Help! Where's is santa

Tools used: Kali Linux, Firefox, Terminal, Nano, Python
Solution/walkthrough:

Question 1:

```
[1211100528@kali:~/home/1211100528] 
$ nmap -n -A 10.10.118.56
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-12 08:33 EDT
Initiating Ping Scan at 08:33
Scanning 1 host (1 target / 1 total ports)
Completed Ping Scan at 08:33
Initiating Parallel DNS resolution of 1 host at 08:33
Completed Parallel DNS resolution of 1 host at 08:33, 0.00s elapsed
Initiating Connect Scan at 08:33
Scanning 1 host (1 target / 1 total ports)
Completed Connect Scan at 08:33, 26.98s elapsed (1000 total ports)
Host 10.10.118.56 is up (0.26s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 27.22 seconds
[]

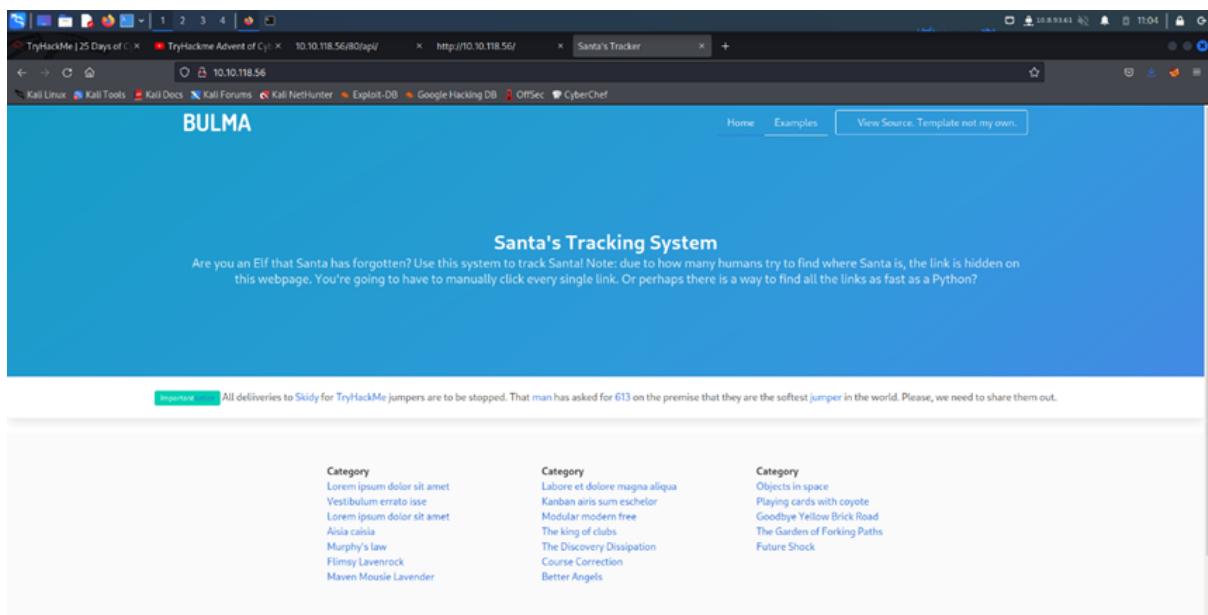
[1211100528@kali:~/home/1211100528]
$ ./nmap -n -A 10.10.118.56
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-12 08:42 EDT
Initiating Ping Scan at 08:42
Scanning 10.10.118.56 (2 ports)
Completed Ping Scan at 08:42, 0.28s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 08:42
Completed Parallel DNS resolution of 1 host at 08:42, 0.00s elapsed
Initiating Connect Scan at 08:42
Scanning 10.10.118.56 (1990 ports)
Completed Connect Scan at 08:42, 10.98s elapsed (1000 total ports)
Host 10.10.118.56 is up (0.26s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http

Category          Category
Lamest or easiest targets          Objects in space
Karma wins        Playing cards with nope
Masturbate        Naughty Princess
The King of Clubs   The Genius of Playing Paths
The Discovery Channel  Future Shock
The Game of Connect Four
Caveat Emptor
Dante's Inferno
Maven Mojang Lander
Bitter Angels

Santa's Tracking System
```

Utilise nmap with the address we just got. Obtaining the port number to launch the API is the next step.

Question 2:

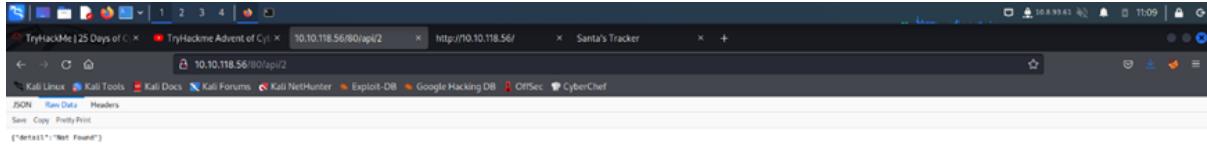


Get the template name by going to the URL page.

Question 3:

For this question, we can get the answer by putting “/api/” to the url and port number.

Question 4:



We must enter the url code along with the port number and api in order to visit this page. The RAW Data tab will then open.

Question 5&6

The terminal session shows a user performing a brute-force attack on a service. The user has identified the service as 'Santa's Tracking System' and is attempting to find a valid API key. The user has already found several invalid keys (e.g., 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 63, 65, 67, 69, 71, 73, 75, 77, 79, 81, 83) and is currently testing key 85. The user notes that the service is down for maintenance.

```
File Actions Edit View Help
1211100528@kali: ~
api_key 37
("item_id":37,"q":"Error. Key not valid!")
api_key 39
("item_id":39,"q":"Error. Key not valid!")
api_key 41
("item_id":41,"q":"Error. Key not valid!")
api_key 43
("item_id":43,"q":"Error. Key not valid!")
api_key 45
("item_id":45,"q":"Error. Key not valid!")
api_key 47
("item_id":47,"q":"Error. Key not valid!")
api_key 49
("item_id":49,"q":"Error. Key not valid!")
api_key 51
("item_id":51,"q":"Error. Key not valid!")
api_key 53
("item_id":53,"q":"Error. Key not valid!")
api_key 55
("item_id":55,"q":"Error. Key not valid!")
api_key 57
("item_id":57,"q":"Winter Wonderland, Hyde Park, London.")
api_key 59
("item_id":59,"q":"Error. Key not valid!")
api_key 61
("item_id":61,"q":"Error. Key not valid!")
api_key 63
("item_id":63,"q":"Error. Key not valid!")
api_key 65
("item_id":65,"q":"Error. Key not valid!")
api_key 67
("item_id":67,"q":"Error. Key not valid!")
api_key 69
("item_id":69,"q":"Error. Key not valid!")
api_key 71
("item_id":71,"q":"Error. Key not valid!")
api_key 73
("item_id":73,"q":"Error. Key not valid!")
api_key 75
("item_id":75,"q":"Error. Key not valid!")
api_key 77
("item_id":77,"q":"Error. Key not valid!")
api_key 79
("item_id":79,"q":"Error. Key not valid!")
api_key 81
("item_id":81,"q":"Error. Key not valid!")
api_key 83
("item_id":83,"q":"Error. Key not valid!")
api_key 85
```

The brute.py method and the nano app should be used to locate the address, and python commands should then be used to obtain the location address and the appropriate api key in front of the address.

Thought process/Methodology:

In order to access the IP address, we must first launch the machine and open the webpage. Next, we must use the nmap method to open the terminal and obtain the port number. The website can then be accessed by utilising both the IP address and

the port number. After that, we can add "/api/" to the url to enter the api secret page and obtain a wealth of data, including raw data. Finally, we need to utilise the brute technique using the python language as a command to acquire the stuff we want, which includes Santa's location address and the api key.

Day 17- [reverse engineering] ReverseELFneering

Tools used: Kali Linux, Firefox, Terminal.

Solution/walkthrough:

Question 1:

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	I	8

We can find the answer in tryhackme.

Question 2:

The command "aa" must be entered in radare2 in order to analyse the programme.

Question 3:

The command "db" would be used to set a breakpoint in radare2.

Question 4:

The command "pdf @main" is what we'll need to run the programme until we reach a breakpoint.

Question 5:

The value of local ch when the movl instruction that corresponds to it is called "1" as in the digit.

Question 6:

when the imull instruction is referred to as "6" as in the numeral digit, the value of eax.

Question 7:

Before eax is set to 0, local 4h would have the value "6."

Thought process/Methodology:

Using the commands "nmap" and "cat target.txt" to target the web page, we must first connect the terminal to the website that we wish to view. To use Radare2 to enter the binary debugging mode, we only need to access the page using the username and password that were provided. The command "aa" can then be used to begin analysing the r2 programme. Once the analysis is finished, we must determine where to begin the analysis as a starting point, which is done by using the command

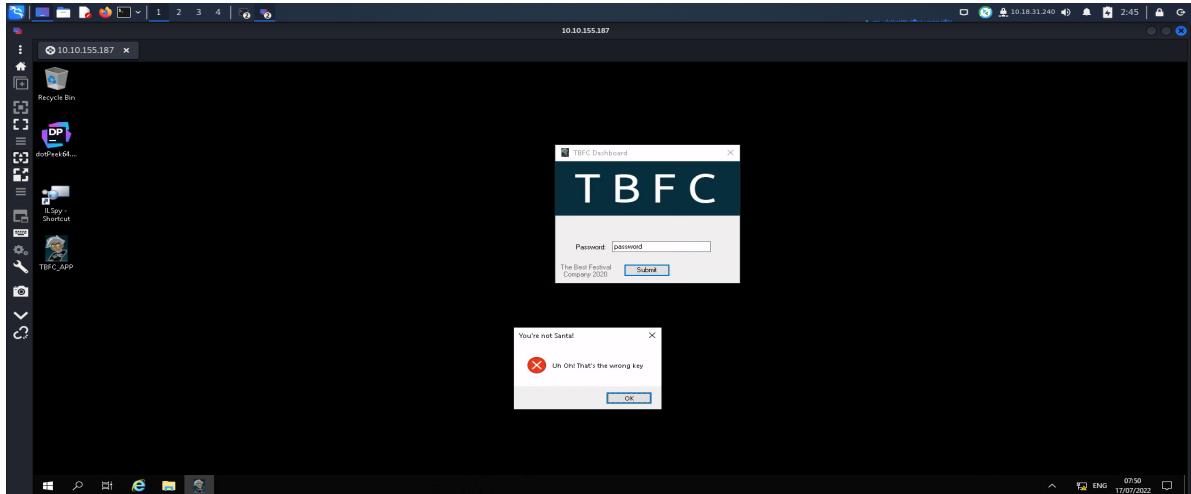
"afl." After determining the main function, we can use the command "pdf @main" to view the assembly code. Then

Day 18- [reverse engineering] The Bits of Christmas

Tool used: Kali Linux, Remmina

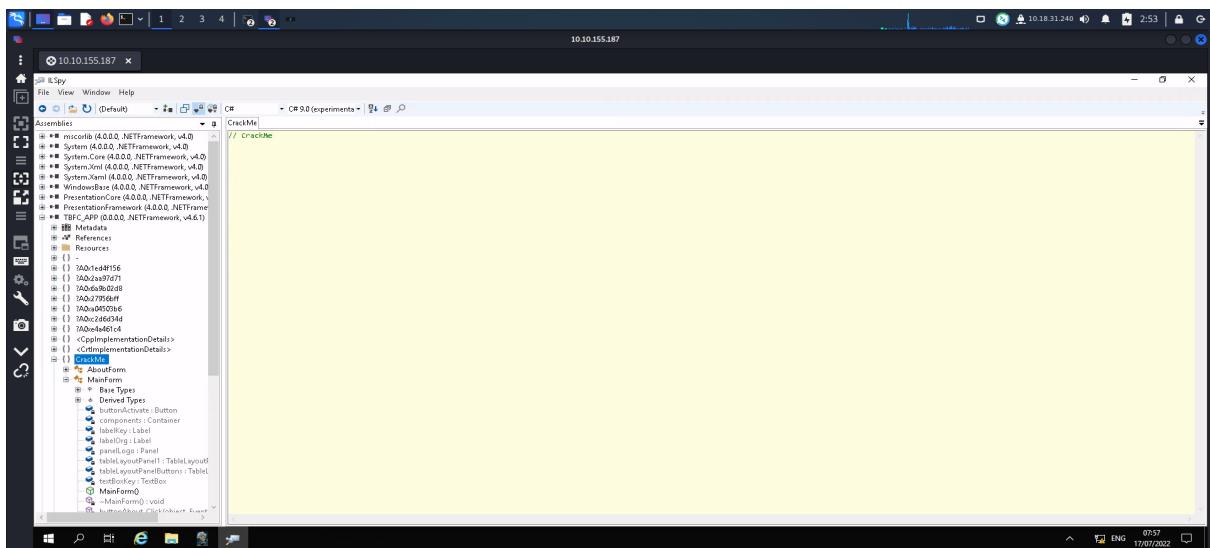
Solution/walkthrough:

Question 1&2:



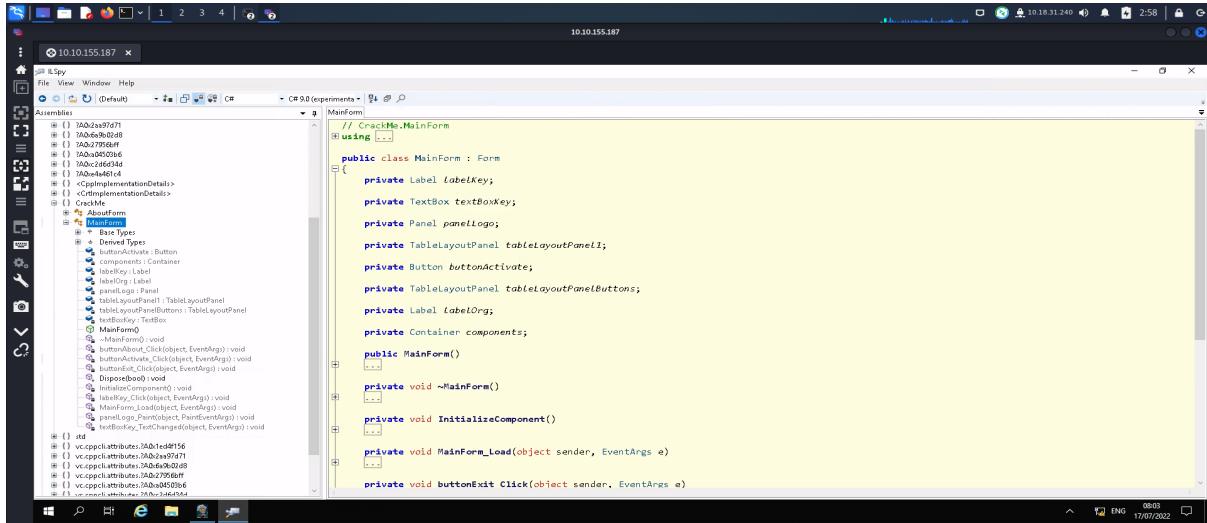
Open the remmina and open the TBFC and insert a random password. For question 2, The answer is beside the submit button.

Question 3:



Open the IL Spy and click file and open the TBFC_App. Then find the special one that is CrackMe.

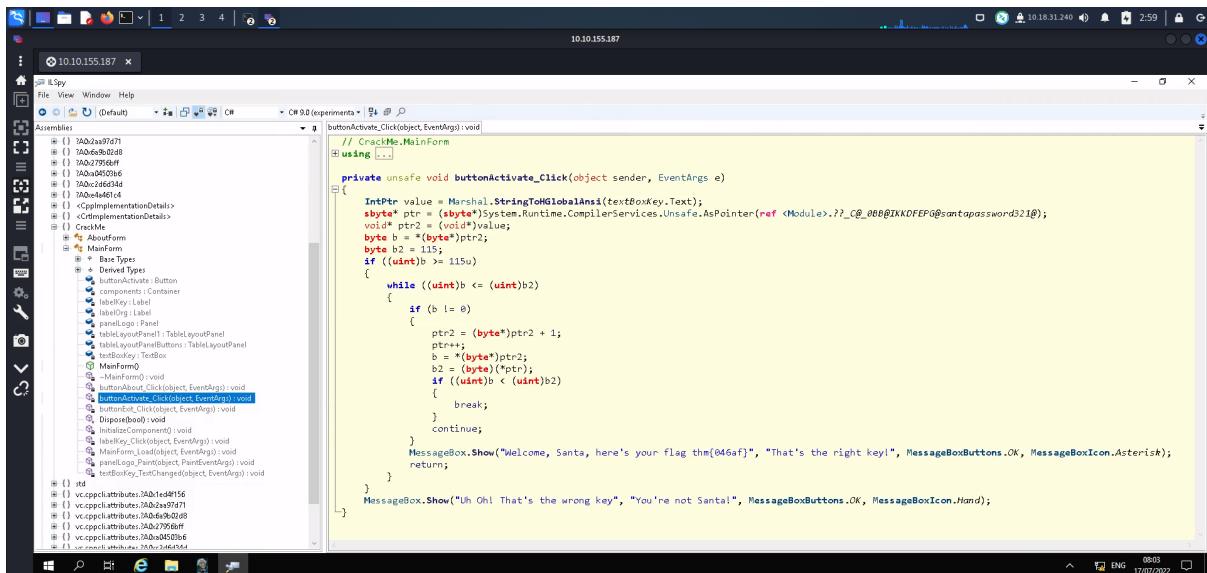
Question 4:



```
// CrackMe.MainForm
using ...
public class MainForm : Form
{
    private Label labelKey;
    private TextBox textBoxKey;
    private Panel panelLogo;
    private TableLayoutPanel tableLayoutPanelPanel;
    private Button buttonActivate;
    private TableLayoutPanel tableLayoutPanelButtons;
    private Label labelOrg;
    private Container components;
    public MainForm()
    {
        ...
    }
    protected void ~MainForm()
    {
        ...
    }
    protected void InitializeComponent()
    {
        ...
        Main();
        ...
    }
    private void MainForm_Load(object sender, EventArgs e)
    {
        ...
    }
    private void buttonExit_Click(object sender, EventArgs e)
    {
        ...
    }
}
```

Click the CrackMe and then find MainForm

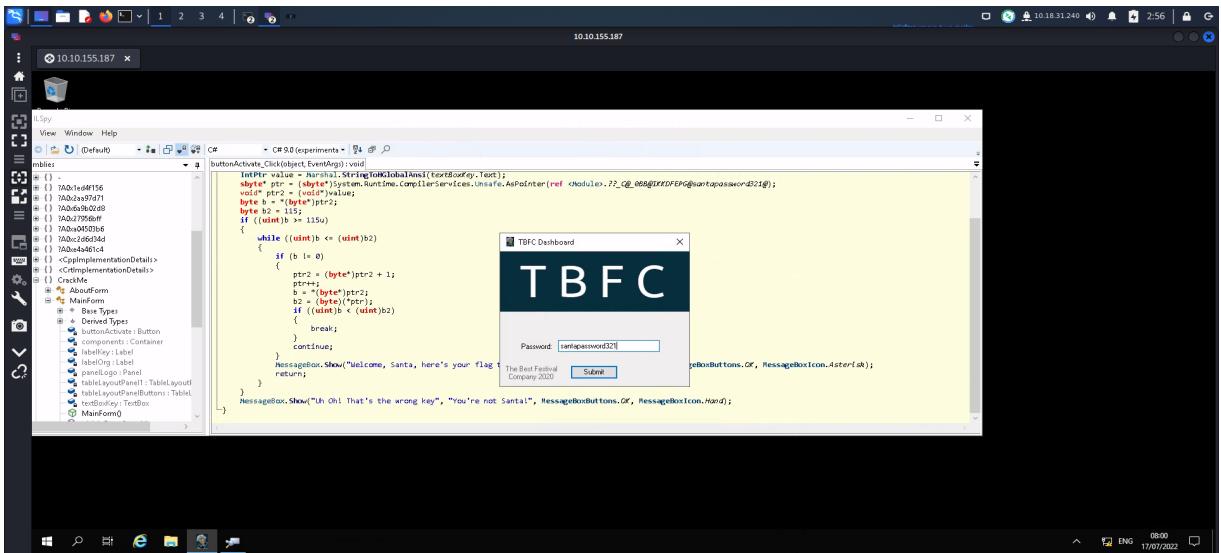
Question 5:



```
// CrackMe.MainForm
private unsafe void buttonActivate_Click(object sender, EventArgs e)
{
    IntPtr value = Marshal.StringToHGlobalAnsi(textBoxKey.Text);
    byte* ptr = (byte*)System.Runtime.CompilerServices.Unsafe.AsPointer(ref Module._?_C8_08B@IKDFEP@ santapassword3218);
    void* ptr2 = (void*)value;
    byte b = *(byte*)ptr2;
    byte b2 = 115;
    if ((uint)b >= 115)
    {
        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);
        }
    }
    MessageBox.Show("Uh Oh! That's the wrong key!", "You're not Santa!", MessageBoxButtons.OK, MessageBoxIcon.Hand);
}
```

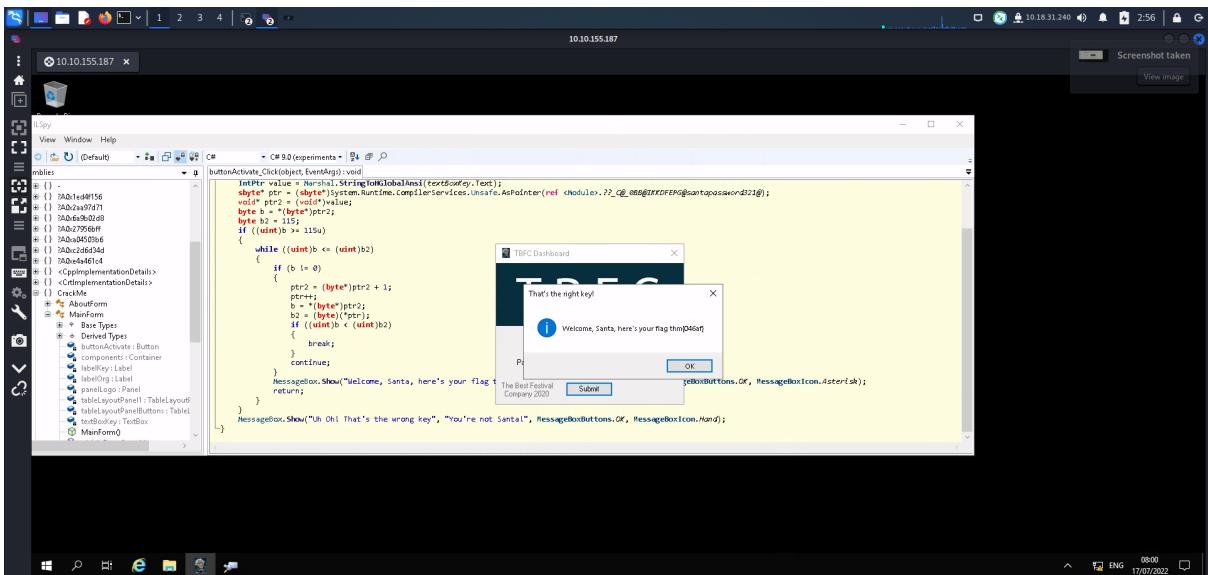
Find the buttonActivate_Click

Question 6:



Click the buttonActivate_Click and you will find the password on your right.

Question 7:



Enter the correct password and you will found the flag

Thought process/Methodology:

First of all, connect your vpn. Next, download remmina in your kali Linux. Then, open your remmina once it has downloaded completely. Enter your password when opening the remmina. Insert your ip address (website) in the RDP column. Then press enter. After that, it will appear a RDP authentication credentials. Now, Insert the username and password that are provided from the website. After filing the username and password, click ok. Wait for a while, the window machine will appear. Next, you will found out that there are recycle bin, dotPeek, IL Spy and TBFC_App on the desktop. Open the TBFC_App first. Next, insert a random password. Then it will tell you you're not a santa. To access the TBFC_App, you need to open IL Spy.

Next, you click file, click open, click desktop, click TBFC_App and lastly click open. The IL Spy will show a lot of line in the assemblies. Then, click the plus on CrackMe. It will show about form and main form. Click the plus on the main form, it will show more lines(reference to elements). Click the buttonActive_Click and see the source code (which are in the right with yellow page). You will found out the password in the line start with word sbyte*. Insert the password into the TBFC_App without the @ symbol. Lastly, press submit. Congratulations, you had found the flag.

Day 19- [Web exploitation] The Naughty or Nice List

Tool used: Kali Linux,

Solution/walkthrough:

Question 1:

After we connect to the web app, we can search up names in the search bar to look for who is in the naughty or nice list. For example Tib3rius is on the nice list



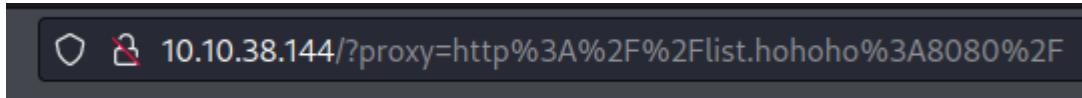
Name:

Tib3rius is on the Nice List.

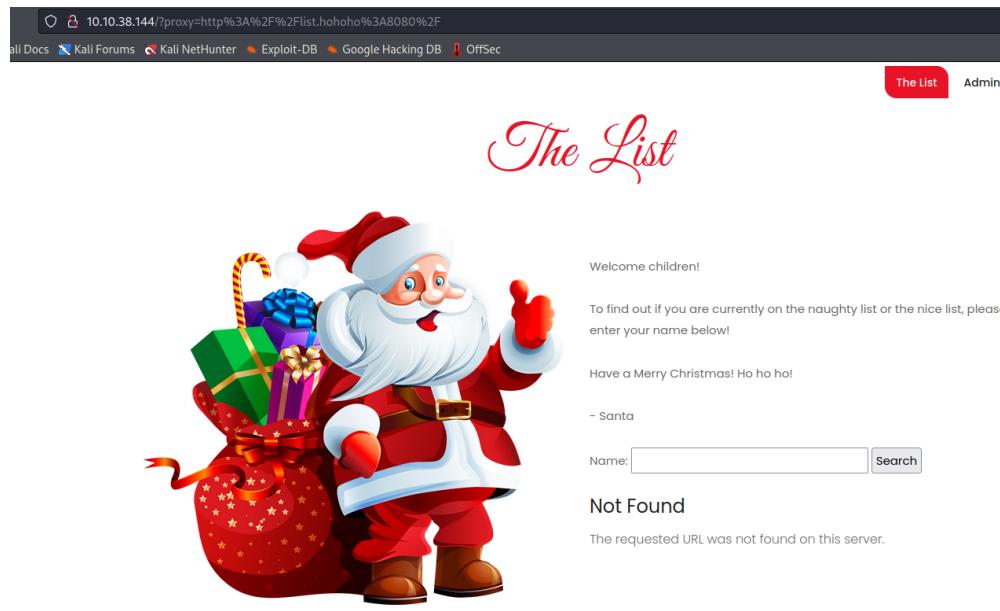
With this we can identify on which list Kanes, Timothy, YP, Ian Chai, and JJ are currently in

Question 2:

If we search up,



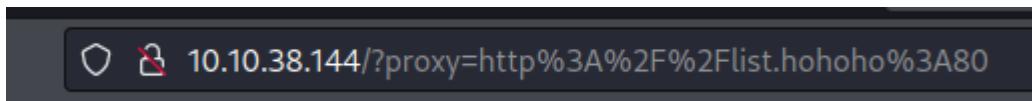
In the url, this page will appear



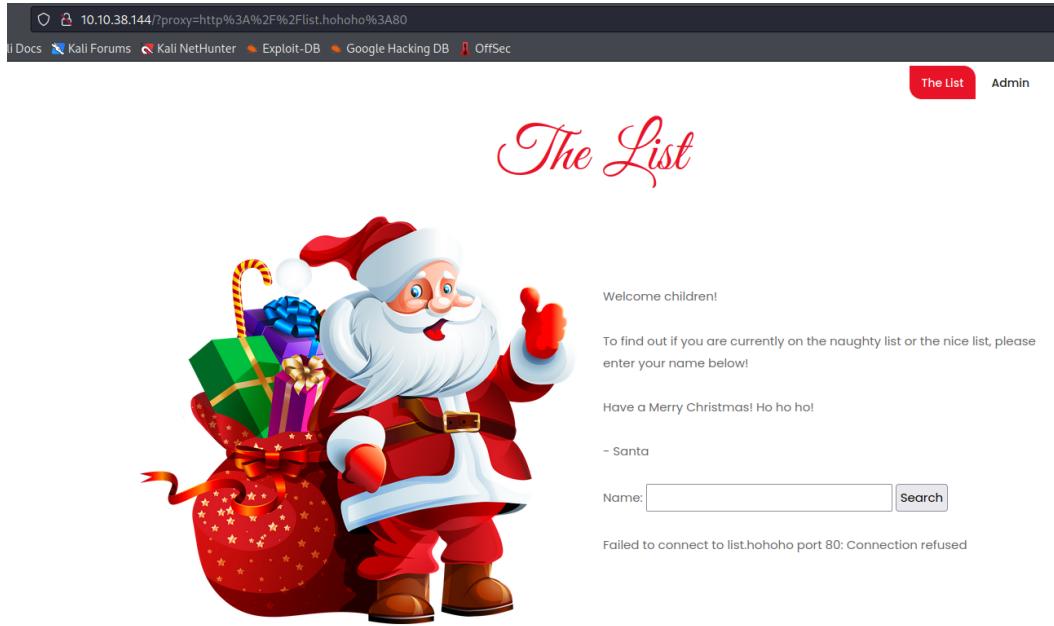
On the page, it displays the “Not Found” error.

Question 3

For this question, we can insert this url



To get the respective page,

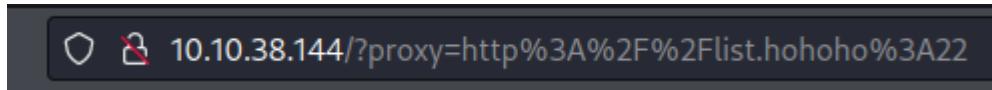


The screenshot shows a web application titled "The List". At the top, there's a navigation bar with links to "Docs", "Kali Forums", "Kali NetHunter", "Exploit-DB", "Google Hacking DB", and "OffSec". On the right side of the header are buttons for "The List" and "Admin". The main content features a cartoon illustration of Santa Claus carrying a large sack filled with wrapped gifts. To the right of the illustration, there's a message from Santa: "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". Below this message is a search form with a text input field labeled "Name:" and a "Search" button. A status message at the bottom indicates: "Failed to connect to list.hohoho port 80: Connection refused".

On the page it displays “Failed to connect to list.hohoho port 80: Connection refused

Question 4:

Next we can insert the url



The screenshot shows a browser's address bar with the URL "10.10.38.144/?proxy=http%3A%2F%2Flist.hohoho%3A22".

And we will get a new error message which is “Recv failure: Connection reset by peer ”

10.10.38.144/?proxy=http%3A%2F%2Flist.hohoho%3A22

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

Recv failure: Connection reset by peer

Question 5:

For the last url we need to search up,

10.10.38.144/?proxy=http%3A%2F%2Flocalhost

The page will display

10.10.38.144/?proxy=http%3A%2F%2Flocalhost

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

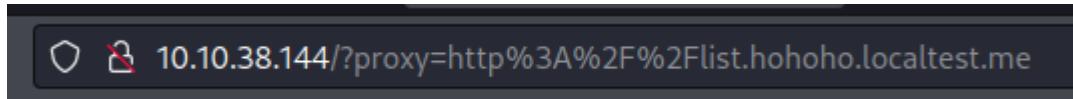
Name: Search

Your search has been blocked by our security team.

Where it says that our search has been blocked by our security team

Question 6:

To get Santa's password all we need to do is set the hostname in the URL to "list.hohoho.localtest.me"



After that, the page will display McSkidy's note to Santa

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

In the notes McSkidy, have reminded Santa of his password and thus we can use that to login with Santa's account

Santa,

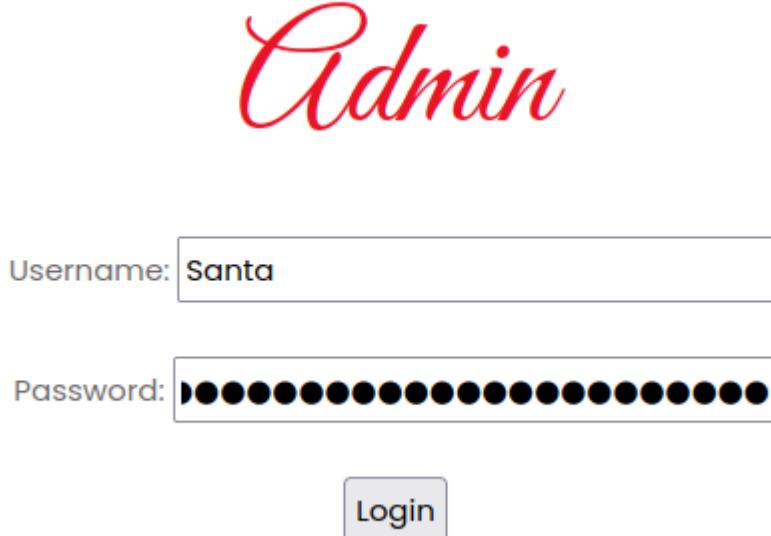
If you need to make any changes to the Naughty or Nice list, you need to login.

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

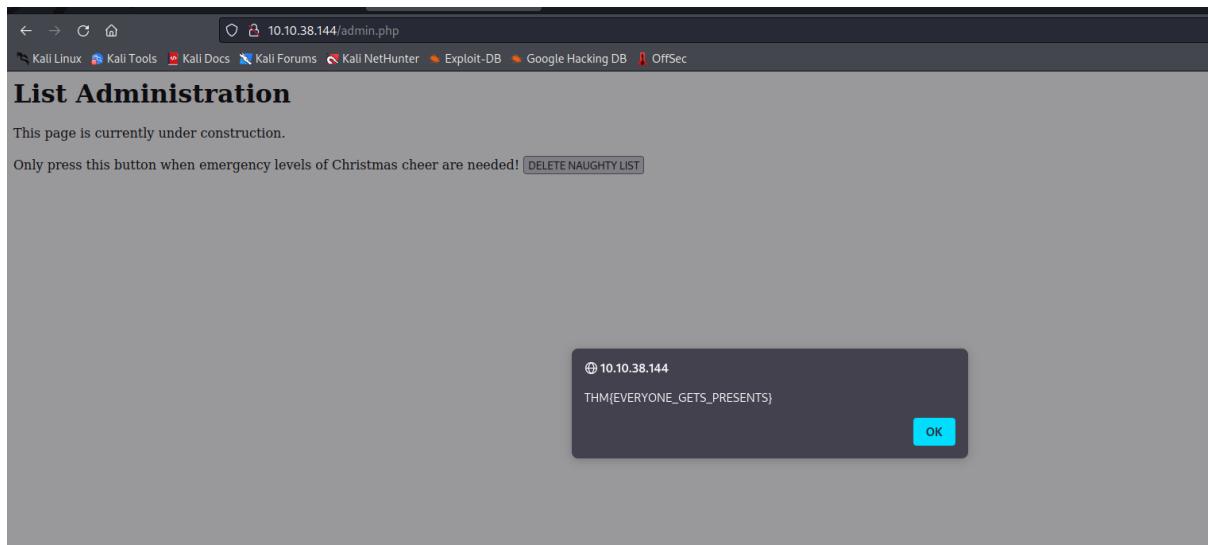
- Elf McSkidy

Question 7:

To get the challenge flag, we must first login in the admin section using santa's account



From there, we need to delete the naughty list and the flag will appear afterwards.



Thought Process / Methodology :

Once we open kali linux we can connect to the webapp. After that, in the website there's a search bar and inside we can search up a name. For example if we search up Tib3rius, it will tell us that the name is in the nice list. In the URL the hostname is

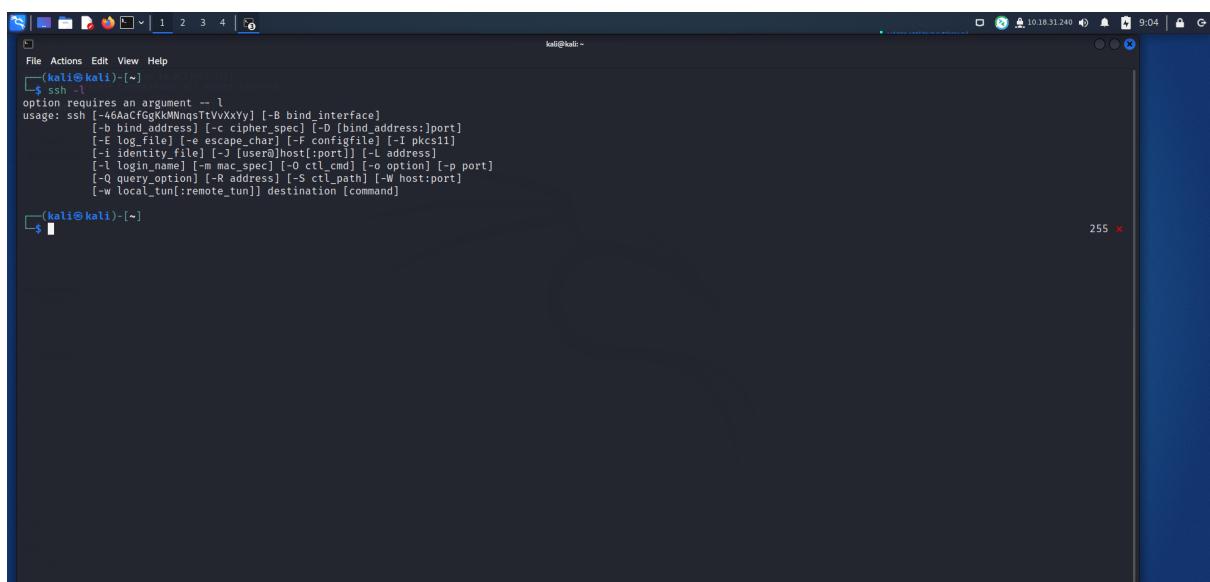
“list.hohoho” which is not a valid hostname. First we can browse “<http://10.10.38.144/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F>” to get the root of the same site. In the place where it originally says “Tib3rius is on the nice list” it instead said “Not Found. The requested URL was not found on this server.”. This seems like an error so we can try other methods like changing the port number from 8080 to just 80, or changing the port number to 22 which is the default SSH port, or even access services running locally on the server by replacing the “list.hohoho” with “localhost”. Unfortunately, each of them comes up with a different error every time. The last thing that we could do is by creating our own domain. We can set the hostname in the URL to “list.hohoho.localtest.me”. Afterwards, we could access a message from Elf McSkidy that contained Santa’s passwords. With this, we can now log in as admin using santa’s account and delete the naughty list to get the challenge flag.

Day 20- [Blue Teaming] PowershELIF to the rescue

Tool used: Kali Linux

Solution/walkthrough:

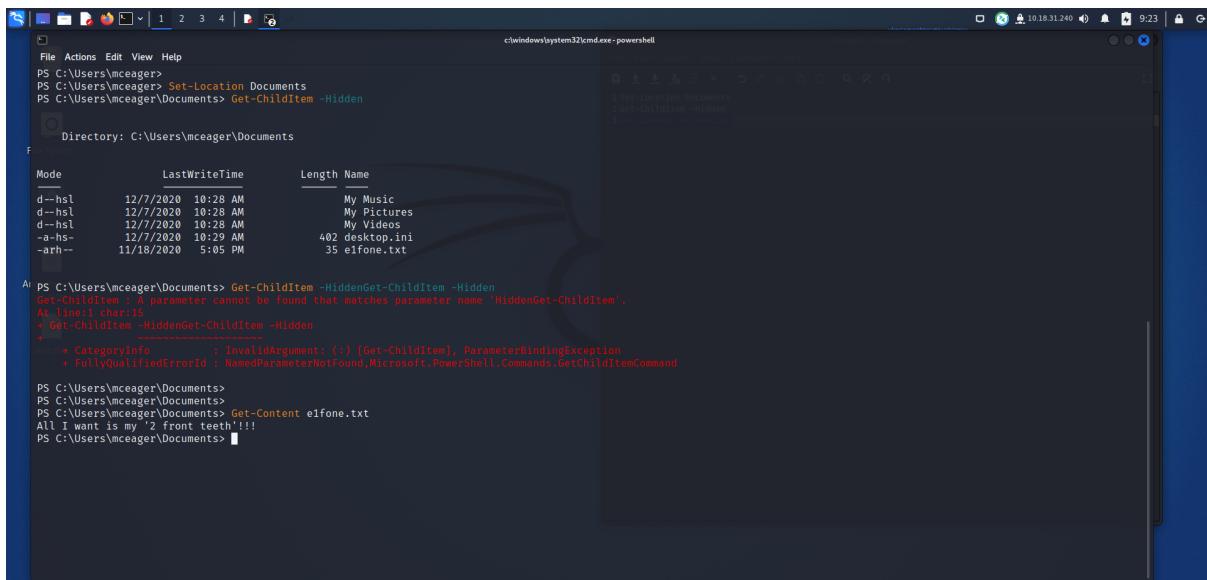
Question 1:



```
(kali㉿kali)-[~] $ ssh -l
option requires an argument -- l
usage: ssh [-46AaCfGgkMNnqsTtVxXxy] [-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]
```

Open the terminal Type ssh -l and you search for it

Question 2:



```
File Actions Edit View Help
PS C:\Users\mceager>
PS C:\Users\mceager> Set-Location Documents
PS C:\Users\mceager\Documents> Get-ChildItem -Hidden

    Directory: C:\Users\mceager\Documents

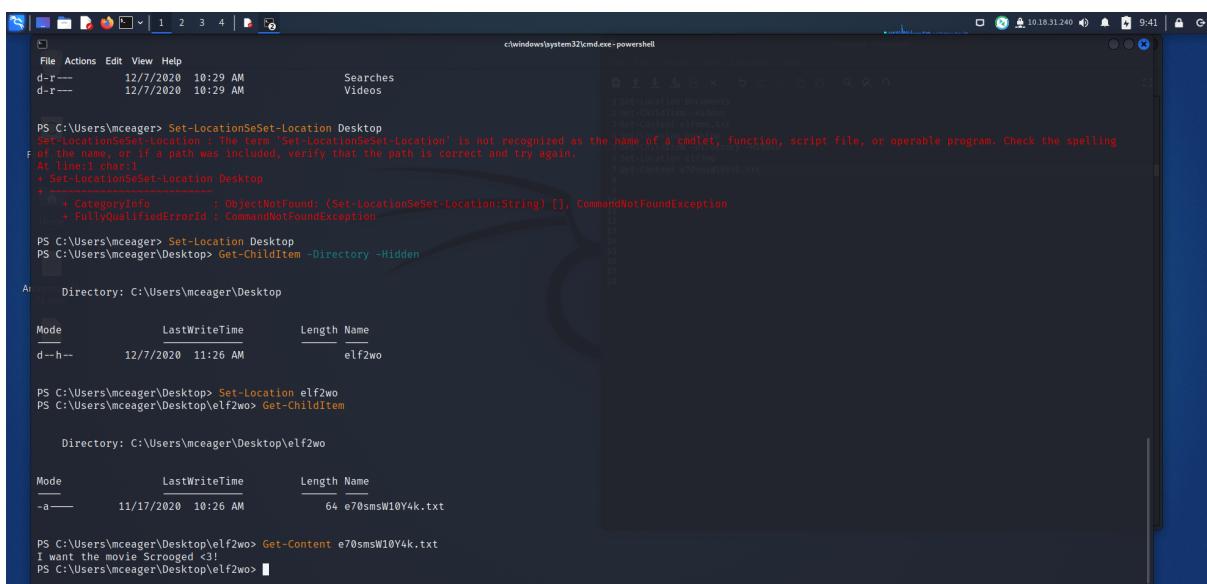
Mode LastWriteTime Length Name
d-hsl 12/7/2020 10:28 AM   My Music
d-hsl 12/7/2020 10:28 AM   My Pictures
d-hsl 12/7/2020 10:28 AM   My Videos
-a-hs- 12/7/2020 10:29 AM  402 desktop.ini
-arh-- 11/18/2020 5:05 PM   35 elfone.txt

At PS C:\Users\mceager\Documents> Get-ChildItem -HiddenGet-ChildItem -Hidden
Get-ChildItem : A parameter cannot be found that matches parameter name 'HiddenGet-ChildItem'.
At line:1 char:15
+ Get-ChildItem -HiddenGet-ChildItem -Hidden
+               ~~~~~
+ CategoryInfo          : InvalidArgument: () [Get-ChildItem], ParameterBindingException
+ FullyQualifiedErrorId : NamedParameterNotFound,Microsoft.PowerShell.Commands.GetChildItemCommand

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

In the powershell, Type Set-Location Documents, then type Get-ChildItem -Hidden. You will set the list. Type Get-Content elfone.txt and you will get the answer.

Question 3:



```
File Actions Edit View Help
PS C:\Users\mceager>
PS C:\Users\mceager> Set-Location Desktop
Set-LocationSet-Location : The term 'Set-LocationSet-Location' is not recognized as the name of a cmdlet, function, script file, or operable program. Check the spelling.
At line:1 char:1
+ Set-LocationSet-Location Desktop
+               ~~~~~
+ CategoryInfo          : ObjectNotFound: (Set-LocationSet-Location:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

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

    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 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!
PS C:\Users\mceager\Desktop\elf2wo>
```

Set your directory to desktop, and find the hidden folder for elf 2. Read the content of the file by using Get-Content.

Question 4:

```

File Actions Edit View Help
PS C:\Users\mceager> Set-Location Desktop
PS C:\Users\mceager\Desktop> Get-ChildItem -Directory -Hidden

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 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!
PS C:\Users\mceager\Desktop\elf2wo> Set-Location \ 
PS C:\> Set-Location Windows
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>

```

Set your directory to Window, then and find the hidden folder for Elf 3 by typing
Get-ChildItem -Directory -Hidden -Recurse -Filter '*3*' -ErrorAction SilentlyContinue

Question 5:

```

File Actions Edit View Help
PS C:\Windows> Set-Location System32
PS C:\Windows\System32> Get-ChildItem -Hidden

Directory: C:\Windows\System32

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

PS C:\Windows> Set-Location System32\3lfthr3e
PS C:\Windows\System32\3lfthr3e> Set-Location System32\3lfthr3e\System32\3lfthr3e
Set-Location : Cannot find path 'C:\Windows\System32\3lfthr3e\System32\3lfthr3e' because it does not exist.
At line:1 char:1
+ Set-Location System32\3lfthr3e
+ ~~~~~
CategoryInfo : ObjectNotFound: (C:\Windows\System32\3lfthr3e:String) [Set-Location], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

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 1.txt | Measure-Object -word
Lines Words Characters Property
----- -----
9999

PS C:\Windows\System32\3lfthr3e>

```

After found out the folder, Set you directory to the hidden folder, and get the number of words by typing Get-Content 1.txt | Measure-Object -word

Question 6:

```

File Actions Edt View Help
PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Measure-Object -word
Lines Words Characters Property
9999

PS C:\Windows\System32\3lfthr3e> Get-Content -Path 1.txt[551][6991]
Get-Content : An object at the specified path 1.txt[551][6991] does not exist, or has been filtered by the -Include or -Exclude parameter.
At Line:1 char:1
+ Get-Content -Path 1.txt[551][6991]
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (System.String[]:String[]) [Get-Content], Exception
+ FullyQualifiedErrorId : ItemNotFound,Microsoft.PowerShell.Commands.GetContentCommand

PS C:\Windows\System32\3lfthr3e> (Get-Content 1.txt)[551]
At Line:1 char:18
+ Get-Content 1.txt)[551]
+ ~~~~~
Unexpected token ')' in expression or statement.
At Line:1 char:20
+ Get-Content 1.txt)[551]
+ ~~~~~
Missing type name after '['.
+ CategoryInfo          : ParserError: () [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : UnexpectedToken

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

```

To find the word, type (Get-Content 1.txt)[551] and (Get-Content 1.txt)[6991]

Question 7:

```

File Actions Edt View Help
PS C:\Windows\System32\3lfthr3e> Get-Content 1.txt | Measure-Object -word
Lines Words Characters Property
9999

PS C:\Windows\System32\3lfthr3e> Get-Content -Path 1.txt[551][6991]
Get-Content : An object at the specified path 1.txt[551][6991] does not exist, or has been filtered by the -Include or -Exclude parameter.
At Line:1 char:1
+ Get-Content -Path 1.txt[551][6991]
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (System.String[]:String[]) [Get-Content], Exception
+ FullyQualifiedErrorId : ItemNotFound,Microsoft.PowerShell.Commands.GetContentCommand

PS C:\Windows\System32\3lfthr3e> (Get-Content -Path 1.txt)[551]
At Line:1 char:18
+ Get-Content -Path 1.txt)[551]
+ ~~~~~
Unexpected token ')' in expression or statement.
At Line:1 char:20
+ Get-Content -Path 1.txt)[551]
+ ~~~~~
Missing type name after '['.
+ CategoryInfo          : ParserError: () [], ParentContainsErrorRecordException
+ FullyQualifiedErrorId : UnexpectedToken

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

PS C:\Windows\System32\3lfthr3e>

```

To find the answer, type Select-String 2.txt -Pattern "redryder"

Thought Process / Methodology :

Use PowerShell to first reveal the majority of files within documents, including hidden files. To complete this work, we were required to locate the concealed content in the subject file, Elf. We can locate the file's location and specific contents using the command directory list. As a result, there are several hidden folder names that can be accessed by various command directories. The last two words, which were from the index numbers 551 and 6991, are displayed in the first and second files respectively. Finally, utilising PowerShell inside the Concealed Files module, we

were able to complete the entire file directory and any content that was hidden therein.