

# PSP0201

## Week 5

# Writeup

Group Name: **CyberTeam**

Members

ID	Name	Role
121110186 4	Julian Koh Chee Yong	Leader
121110360 5	Danial Ierfan Bin Hazmi	Member
121110328 1	Jievenesh Arvind Naidu A/L Uma Selvam	Member
121110378 5	Brijhendhra A/L Saravanaraj	Member

## Day 16 - Help! Where is Santa?

### Tools used: Kali Linux, Firefox, Visual Studio Code

Solution/walkthrough:

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

Use Nmap to scan the IP addresses and ports in the network.

```
(kali㉿kali)-[~]
$ nmap -v 10.10.174.122
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-16 04:03 EDT
Initiating Ping Scan at 04:03
Scanning 10.10.174.122 [2 ports]
Completed Ping Scan at 04:03, 0.20s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:03
Completed Parallel DNS resolution of 1 host. at 04:03, 0.01s elapsed
Initiating Connect Scan at 04:03
Scanning 10.10.174.122 [1000 ports]
Discovered open port 22/tcp on 10.10.174.122
Discovered open port 80/tcp on 10.10.174.122
Increasing send delay for 10.10.174.122 from 0 to 5 due to max_successful_tryno increase to 4
Increasing send delay for 10.10.174.122 from 5 to 10 due to max_successful_tryno increase to 5
Completed Connect Scan at 04:03, 21.21s elapsed (1000 total ports)
Nmap scan report for 10.10.174.122
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

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 21.47 seconds
```

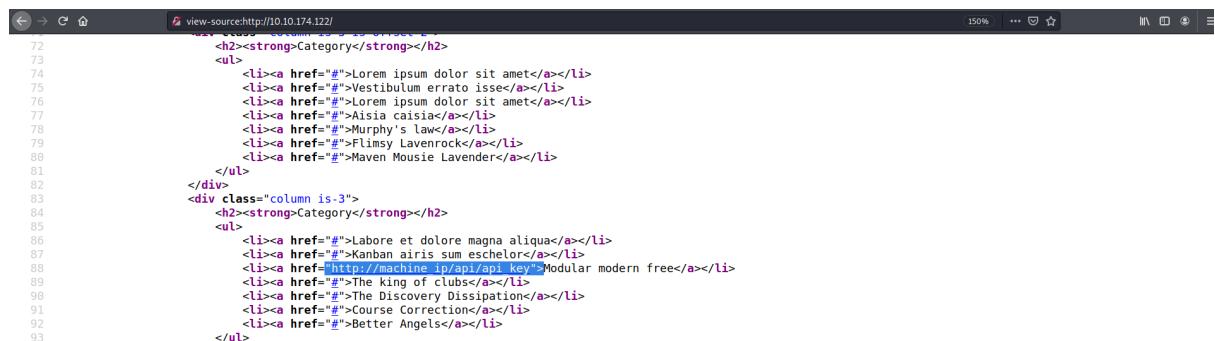
Answer: 80

### Question 2: What templates are being used?

Answer: BULMA

### Question 3: Without using enumerations tools such as Dirbuster, what is the directory for the API?

View the page source and find the odd link which includes the directory for the API.



```
view-source:http://10.10.174.122/
72      <h2><strong>Category</strong></h2>
73      <ul>
74        <li><a href="#">Lorem ipsum dolor sit amet</a></li>
75        <li><a href="#">Vestibulum errato isse</a></li>
76        <li><a href="#">Lorem ipsum dolor sit amet</a></li>
77        <li><a href="#">Asia Caisia</a></li>
78        <li><a href="#">Murphy's law</a></li>
79        <li><a href="#">Flimsy Lavenrock</a></li>
80        <li><a href="#">Raven 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 eschelorc</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>
```

Answer: /api/

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

Answer: {"detail":[{"loc":["path","item\_id"],"msg":"value is not a valid integer","type":"type\_error.integer"}]}

### Question 5: Where is Santa right now?

I used Visual Studio Code to program a loop.

```
File Edit Selection View Go Run Terminal Help
  thm.py x
home > kali > thm.py > ...
1 import requests
2
3 for api_key in range (1,100,2):
4     print(f'api key {api_key}')
5     html = requests.get(f'http://10.10.174.122/api/{api_key}')
6     print (html.text)
7

PROBLEMS OUTPUT DEBUG-CONSOLE TERMINAL JUPYTER
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!")

Python - kali + v □ ^ x
```

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)

I used Visual Studio Code to program a loop.

```
thm.py - Visual Studio Code
File Edit Selection View Go Run Terminal Help
thm.py x
home > kali > thm.py > ...
1 import requests
2
3 for api_key in range(39,63):
4     print(f"api key {api_key}")
5     html = requests.get(f"http://10.10.174.122/api/{api_key}")
6     print(html.text)
7

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL JUPYTER
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
```

Answer: 57

Thought/processes:

Firstly, we scan the URL's port using Nmap. Then, view the page source and find the link to gain the access to the system to track Santa. As we need to find the correct API key, we have programmed a loop to find it. Once we have found the correct API key, the location of Santa is shown.

## Day 17 - ReverseELFneering

### Tools used - Kali Linux, Firefox

Solution/Walkthrough:

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

The answer is available in THM script.

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

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 is searched from the link given in THM.

### Analysis [a]

Analyse all	<b>aa[a[a]]</b>
Analyse function calls	aac
Analyse consecutive function	aat
Graphviz output	ag <addr>
ASCII Graph	agf
Xrefs from	axf
Xrefs to	axt
Rename function	afn
Rename locals/args	afvn
List functions	afl

Answer :

**aa**

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

Answer is searched from the link given in THM.

### Debugger [d]

Set breakpoint	db [addr]
Remove breakpoint	db - [addr]
Continue execution	dc
Show memory maps	dm
Show memory maps with bars	dm=
Start process	do
Attach to process	dp
Show register	dr
Step	ds [num]
Step over	dso [num]
Show heap graph	dmhg
List heap chunks	dmh
List heap chunks of arena	dmh <arena
List bins	dmhb
List fastbins	dmhf

Answer :

**db**

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

Answer is searched from the link given in THM.

### Debugger [d]

Set breakpoint	db [addr]
Remove breakpoint	db - [addr]
Continue execution	dc
Show memory maps	dm
Show memory maps with bars	dm=
Start process	do
Attach to process	dp
Show register	dr
Step	ds [num]
Step over	dso [num]
Show heap graph	dmhg
List heap chunks	dmh
List heap chunks of arena	dmh <arena
List bins	dmhb
List fastbins	dmhf

Answer :

**dc**

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

Use pdf @main for a simpler program to read.

```
0x00400b51      c745f4810000.  mov dword [local_ch], 1
```

Answer :

1

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

```
mov dword [local_ch], 1
mov dword [local_8h], 6
mov eax, dword [local_ch]
imul eax,
```

Answer :

6

Question 7 : What is the value of local\_4h before eax is set to 0?

```
mov dword [local_ch], 1
mov dword [local_8h], 6
mov eax, dword [local_ch]
imul eax, dword [local_8h]
mov dword [local_4h], eax
mov eax, 0
...
```

Answer :

6

Thought/Processes :

Firstly, look through the script in THM to match the Initial Type Data with the Size of Bit. Then, with the link given, search through the radare2 cheatsheet. After setting in all the commands, use pdf @main to get a simpler view of the data.

## Day 18 - The Bits of Christmas

### Tools used - Kali Linux, Firefox, Remmina

Solution/Walkthrough :

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

Enter any random password in the box given.



Answer :

**Uh Oh! That's the wrong key**

Question 2 : What does TBFC stand for?



Answer :

**The Best Festival Company**

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

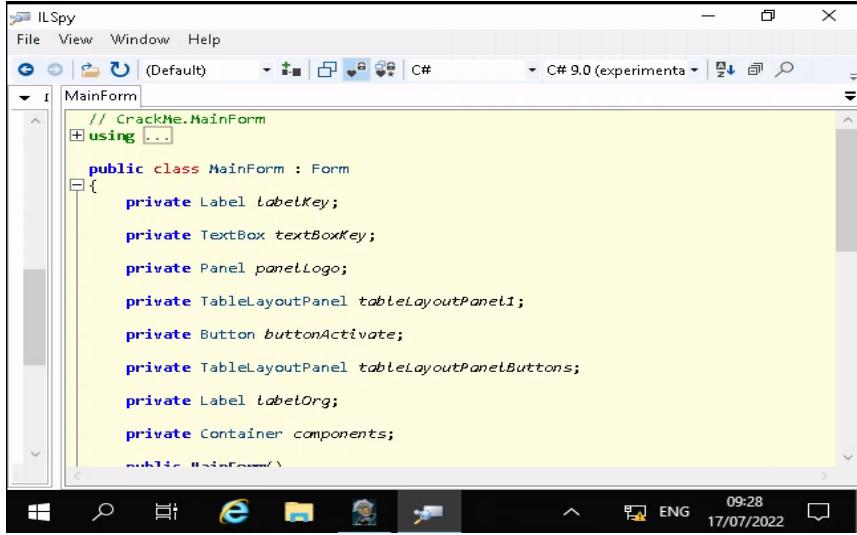
Go to File and click on Desktop. When you see TBFC App, click on it once and click on Open.

```
// C:\Users\cmnatic\Desktop\TBFC_APP.exe
// CrackMe, Version=0.0.0.0, Culture=neutral, PublicKeyToken=null
// Global type: <Module>
// Entry point: <Module>.main
// Architecture: x86
// This assembly contains unmanaged code.
// Runtime: v4.0.30319
// Hash algorithm: SHA1
```

Answer :

**CrackMe**

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



The screenshot shows the IL Spy interface with the MainForm.cs file open. The code defines a class named MainForm that extends the Form class. It contains several private fields: labelKey, textBoxKey, panelLogo, tableLayoutPanelPanel1, buttonActivate, tableLayoutPanelButtons, labelOrg, and components. The code is part of the CrackMe namespace.

```
// CrackMe.MainForm
using ...

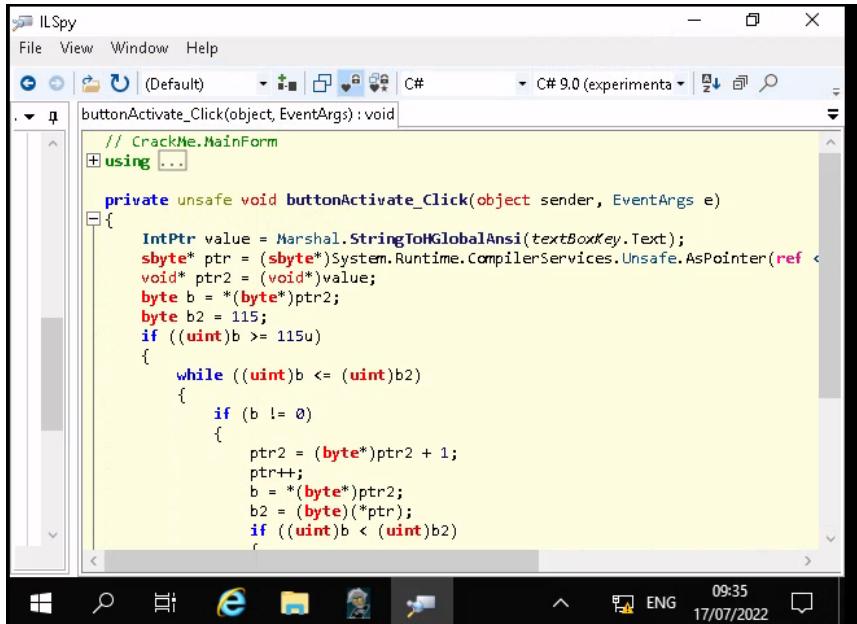
public class MainForm : Form
{
    private Label labelKey;
    private TextBox textBoxKey;
    private Panel panelLogo;
    private TableLayoutPanel tableLayoutPanel1;
    private Button buttonActivate;
    private TableLayoutPanel tableLayoutPanelButtons;
    private Label labelOrg;
    private Container components;
}

partial class MainForm
```

Answer :

**MainForm**

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



The screenshot shows the IL Spy interface with the buttonActivate\_Click method highlighted. This method is part of the MainForm class and takes an object and EventArgs as parameters. It uses unsafe code to manipulate memory pointers, specifically working with the textBoxKey.Text string. The method checks if a character's ASCII value is greater than or equal to 115 and then iterates through the string, incrementing a pointer and comparing characters until it finds one less than 115.

```
buttonActivate_Click(object sender, EventArgs e)
{
    IntPtr value = Marshal.StringToGlobalAnsi(textBoxKey.Text);
    sbyte* ptr = (sbyte*)System.Runtime.CompilerServices.Unsafe.AsPointer(ref value);
    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)
```

The screenshot shows the ILSpy decompiler interface. The title bar says "ILSpy". The menu bar includes "File", "View", "Window", and "Help". The toolbar has icons for file operations like Open, Save, and Build. The language dropdown is set to "C#". The assembly dropdown is set to "C# 9.0 (experimental)". The current method being viewed is "buttonActivate\_Click(object, EventArgs) : void". The code is as follows:

```
buttonActivate_Click(object, EventArgs) : void
{
    while ((uint)b <= (uint)b2)
    {
        if (b != 0)
        {
            ptr2 = (byte*)ptr2 + 1;
            ptr++;
            b = *(byte*)ptr;
            b2 = (byte)(*ptr);
            if ((uint)b < (uint)b2)
            {
                break;
            }
            continue;
        }
        MessageBox.Show("Welcome, Santa, here's your flag thm{046af}", "That's return");
    }
    MessageBox.Show("Uh Oh! That's the wrong key", "You're not Santa!", MessageBoxButtons.OK);
}
```

Answer :

**buttonActivate\_Click**

Question 6 : What is Santa's password?

Double click on the input saying santa password and copy the numbers displayed at the end.

The screenshot shows the ILSpy decompiler interface. The title bar says "ILSpy". The menu bar includes "File", "View", "Window", and "Help". The toolbar has icons for file operations like Open, Save, and Build. The language dropdown is set to "C#". The assembly dropdown is set to "C# 9.0 (experimental)". The current method being viewed is part of a module named "??.C@\_0BB@IKKDFEPG@santapassword321@ : \$ArrayType\$\$\$BY0BB@\$\$.CBD". The code is as follows:

```
// <Module>
+using ...

internal static $ArrayType$$$BY0BB@$$.CBD ??_C@_0BB@IKKDFEPG@santapassword321@/* N
```

Use CyberChef to debug the hexadecimal numbers.

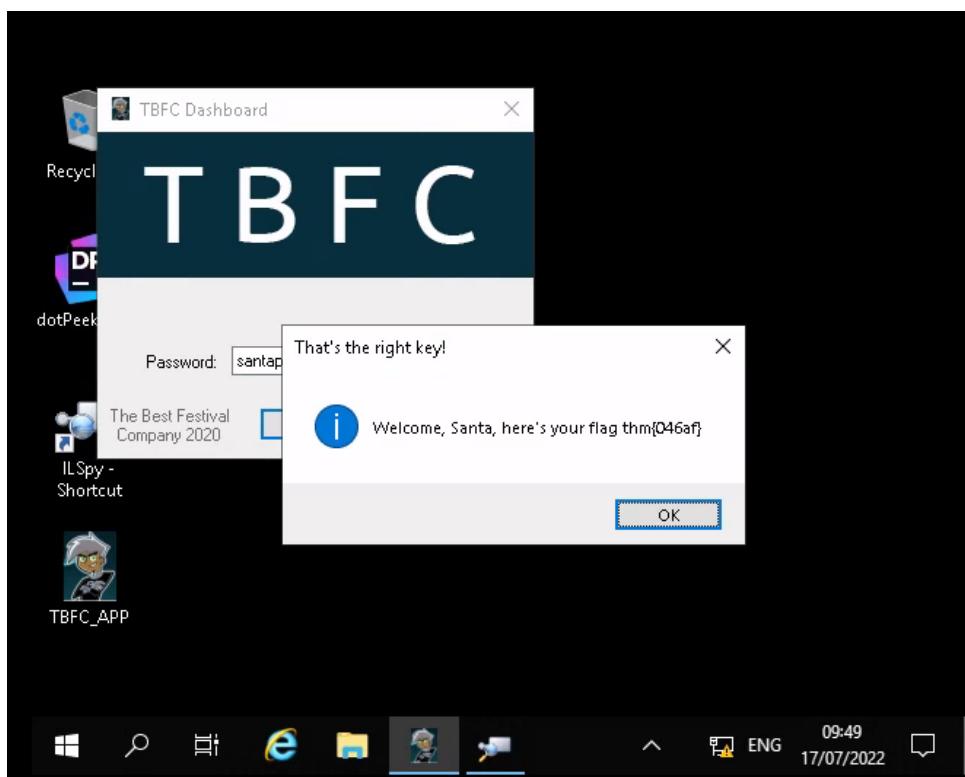
The screenshot shows the CyberChef interface. In the 'Input' section, there is a 'From Hex' field containing the hex bytes: 73 61 6E 74 61 70 61 73 73 77 6F 72 64 33 32 31. The 'Output' section shows the resulting ASCII text: santapassword321. The 'Recipe' section at the top has 'From Hex' selected.

Answer :

**santapassword321**

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

Insert the password in TBFC dashboard.



Answer :

**thm{046af}**

Thought/Processes :

First, we went to Remmina and turned on the TBFC app. A password is needed to login. We went to ILSpy and navigated to MainForm. From there, we went to buttonActivate\_Click and clicked on [??\_C@\_0BB@IKKDFEPG@santapassword321@]. The data of hexadecimal numbers are copied and pasted into Cyberchef to debug the password. The password was then pasted back into TBFC app and the flag was posted.

**Day 19- [Web Exploitation], The Naughty or Nice list**

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Q1: Which list is this person on?

This can be checked by entering the name into the search box



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

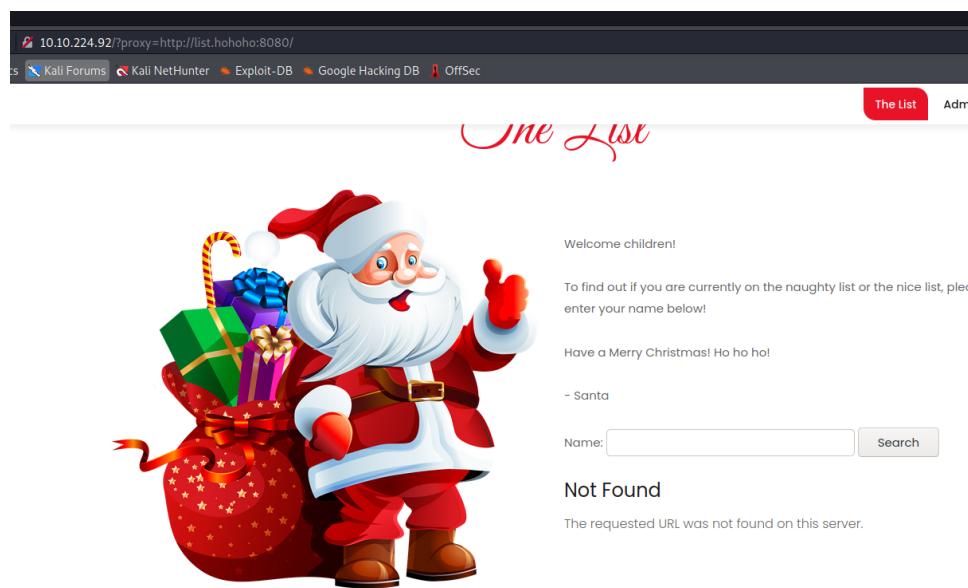
Name:

Ian Chai is on the Nice List.

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

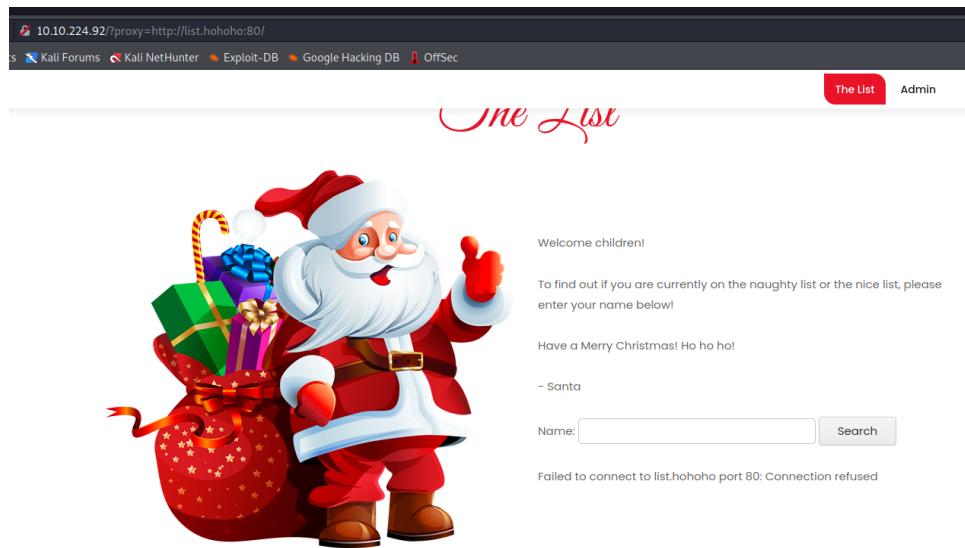
Q2: What is displayed on the page when you use  
["/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"](http://10.10.224.92/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F)?

First, decode the code link to ASCII  
[/?proxy=http://list.hohoho:8080/](http://list.hohoho:8080/)



**Answer:** 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"?**



**Answer:** 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"?**

The screenshot shows a web browser window with the URL `10.10.224.92/?proxy=http://list.hohoho:22/`. The page has a header with navigation links like 'Kali Docs', 'Kali Forums', 'Kali NetHunter', 'Exploit-DB', 'Google Hacking DB', and 'OffSec'. On the right, there are buttons for 'The List' and 'Admin'. The main content features a cartoon Santa Claus carrying a large sack of gifts. The text 'The List' is written in red cursive above the Santa image. Below Santa, there's a message: '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!', and '- Santa'. There's also a search form with a 'Name:' input field and a 'Search' button. A message at the bottom says 'Recv failure: Connection reset by peer'.

**Answer:** Recv failure: Connection reset by peer

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

This screenshot shows the same proxy page as the first one, but with a different URL: `10.10.224.92/?proxy=http://localhost`. The content is identical to the first screenshot, including the Santa illustration and the search form. However, the message at the bottom of the search form area now reads 'Your search has been blocked by our security team.'

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

**Q6: What is Santa's password?**

After setting the set the hostname in the URL to "list.hohoho.localtest.me" to bypass the check, I am able to access the local services



HAVE A MERRY CHRISTMAS! HO HO HO!

- Santa

Name:  Search

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

Answer: Be good for goodness sake!

#### Q7: What is the challenge flag?

Now that we have the password, we can log in and find the flag

Answer: THM{EVERYONE\_GETS\_PRESENTS}

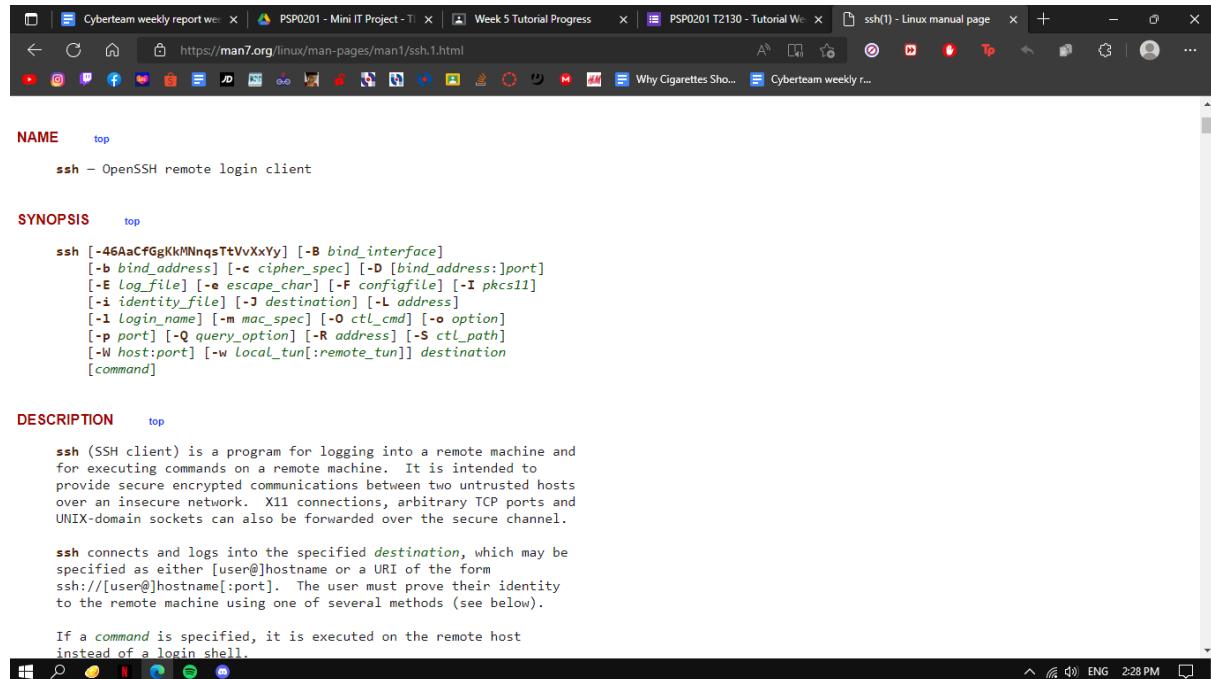
Thought/processes:

In order to not get blocked by the security, I need to have list.hohoho in the url, then use localtest.me, which will resolve the DNS entry to 127.0.0.1, adding it into the url, I was able to find the password.

#### Day 20 - PowershELIF to the rescue

## Tools used: Kali Linux, Firefox

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



**NAME** top  
**ssh** – OpenSSH remote login client

**SYNOPSIS** top

```
ssh [-46aCfGgKkMNnqsTtVvXxYy] [-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 destination] [-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] [-t local_tun[:remote_tun]] destination
     [command]
```

**DESCRIPTION** top

**ssh** (SSH client) is a program for logging into a remote machine and for executing commands on a remote machine. It is intended to provide secure encrypted communications between two untrusted hosts over an insecure network. X11 connections, arbitrary TCP ports and UNIX-domain sockets can also be forwarded over the secure channel.

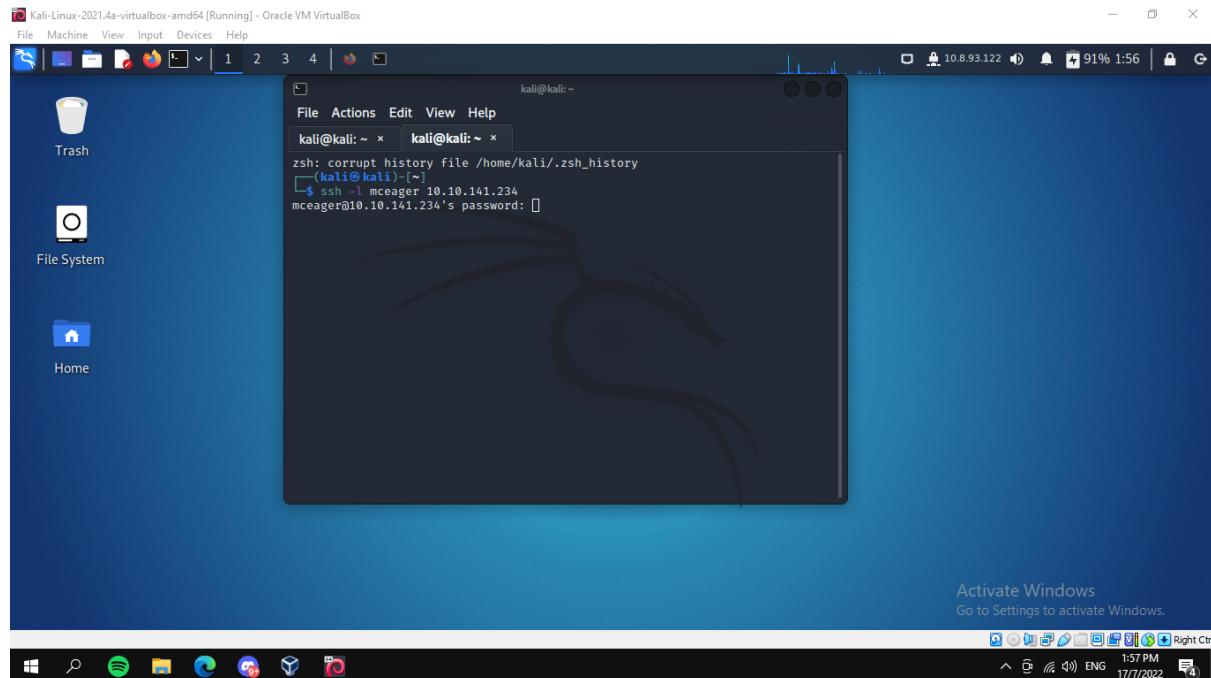
**ssh** connects and logs into the specified *destination*, which may be specified as either [user@]hostname or a URI of the form ssh://[user@]hostname[:port]. The user must prove their identity to the remote machine using one of several methods (see below).

If a *command* is specified, it is executed on the remote host instead of a login shell.

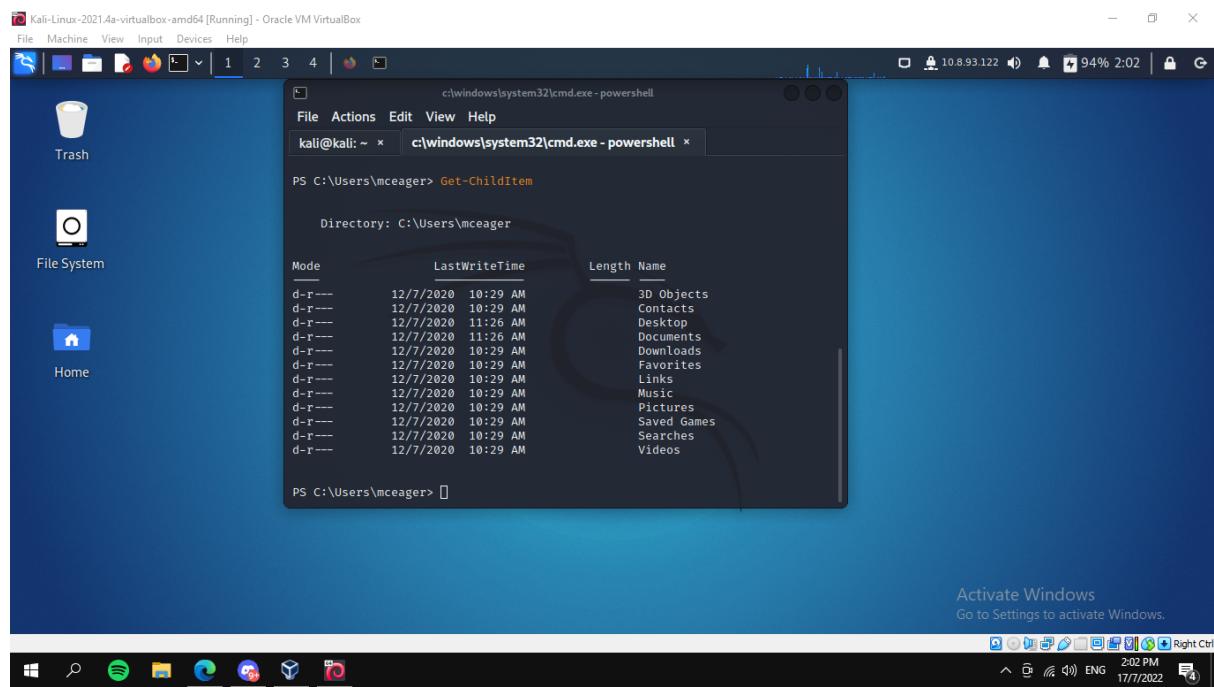
Answer: Login Name

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

We first connect to the remote machine and input the password given



We then use the Get-ChildItem command to list down the contents of the current directory we are in



```
c:\windows\system32\cmd.exe - powershell
File Actions Edit View Help
kali@kali: ~ x c:\windows\system32\cmd.exe - powershell x
PS C:\Users\mceager> Get-ChildItem

Directory: C:\Users\mceager

Mode LastWriteTime Length Name
-- -- -- -- --
d-r--- 12/7/2020 10:29 AM 3D Objects
d-r--- 12/7/2020 10:29 AM Contacts
d-r--- 12/7/2020 11:26 AM Desktop
d-r--- 12/7/2020 11:26 AM Documents
d-r--- 12/7/2020 10:29 AM Downloads
d-r--- 12/7/2020 10:29 AM Favorites
d-r--- 12/7/2020 10:29 AM Links
d-r--- 12/7/2020 10:29 AM Music
d-r--- 12/7/2020 10:29 AM Pictures
d-r--- 12/7/2020 10:29 AM Saved Games
d-r--- 12/7/2020 10:29 AM Searches
d-r--- 12/7/2020 10:29 AM Videos
PS C:\Users\mceager>
```

We then change the directory and view the hidden contents in the current directory. We then list files to view the text file

```

Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~ x c:\windows\system32\cmd.exe - powershell x
d-r-- 12/7/2020 10:29 AM Searches
d-r-- 12/7/2020 10:29 AM Videos

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

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> ls

Directory: C:\Users\mceager\Documents

Mode LastWriteTime Length Name
-a--- 11/23/2020 12:06 PM 22 elfone.txt

PS C:\Users\mceager\Documents>

```

Activate Windows  
Go to Settings to activate Windows.

Windows Start | Search | Spotify | File Explorer | Edge | File Manager | Task View | Taskbar Icons | System Tray | Right Ctrl

^ ⌘ ⌘ ENG 2:11 PM 17/7/2022

We then use Get-Content to read the contents of the file

```

Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~ x c:\windows\system32\cmd.exe - powershell x
nlyContinue

File System

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> ls

Directory: C:\Users\mceager\Documents

Mode LastWriteTime Length Name
-a--- 11/23/2020 12:06 PM 22 elfone.txt

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

```

Activate Windows  
Go to Settings to activate Windows.

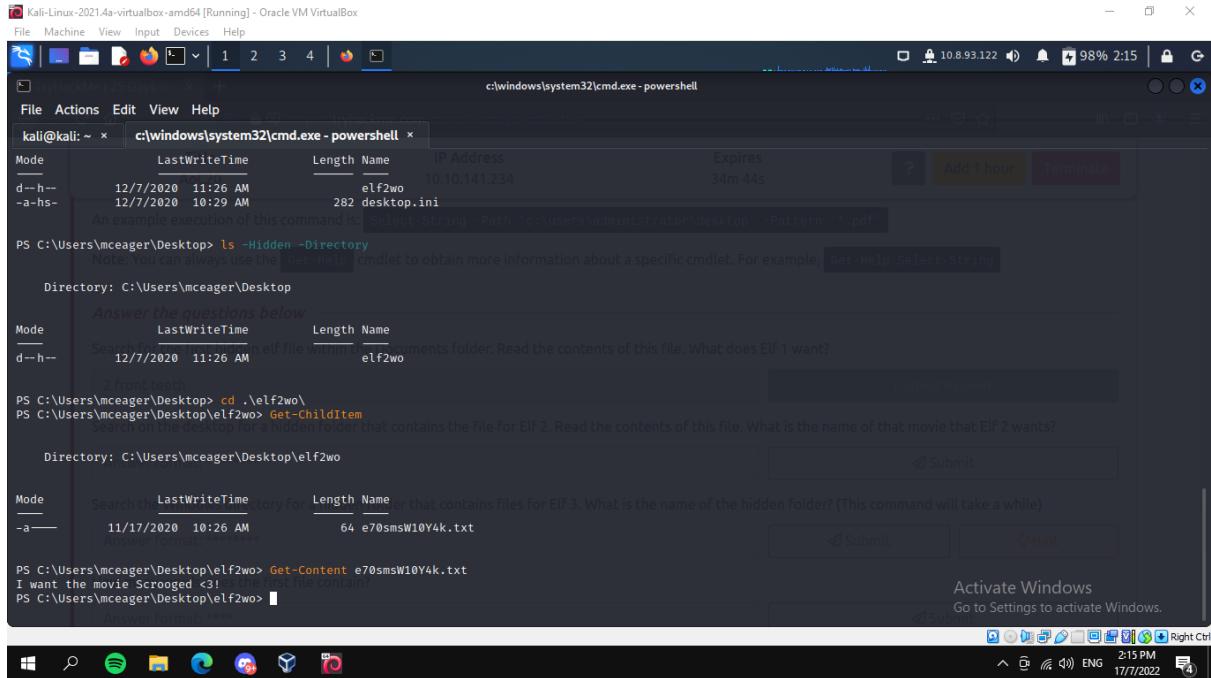
Windows Start | Search | Spotify | File Explorer | Edge | File Manager | Task View | Taskbar Icons | System Tray | Right Ctrl

^ ⌘ ⌘ ENG 2:12 PM 17/7/2022

Answer: 2 front teeth

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?

Once we changed directory to desktop, we list hidden files and list contents in them to get the text file. Then we can use Get-Content to read the contents of the text file.



```
Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~ | c:\windows\system32\cmd.exe - powershell
Mode LastWriteTime Length Name IP Address Expires
d--h-- 12/7/2020 11:26 AM 10.10.141.234 34m 44s
-a-hs- 12/7/2020 10:29 AM 282 desktop.ini
An example execution of this command is: Select-String -Path 'C:\Users\Administrator\Desktop\' -Pattern 'Elf.pdf'
PS C:\Users\mceager\Desktop> ls -Hidden -Directory
Note: You can always use the Get-Help cmdlet to obtain more information about a specific cmdlet. For example, Get-Help Select-String
Directory: C:\Users\mceager\Desktop
Answer the questions below
Mode LastWriteTime Length Name
d--h-- 12/7/2020 11:26 AM 1 elf file within C:\Users\mceager\Desktop\elf2wo\ directory. Read the contents of this file. What does Elf 1 want?
2 front teeth
PS C:\Users\mceager\Desktop> cd .\elf2wo
PS C:\Users\mceager\Desktop\elf2wo> Get-ChildItem
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?
Directory: C:\Users\mceager\Desktop\elf2wo
Submit
Correct Answer
Mode Search Time 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>
Activate Windows
Go to Settings to activate Windows.
Windows Start Task View File Home Network People Mail Control Panel
2:15 PM 17/7/2022
```

Answer: Scrooged

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)

We change directory to Windows and then to System32, then we get the contents of the current directory with the help of filter command to filter out the file we want from the unnecessary files.

```

Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~ x c:\windows\system32\cmd.exe - powershell x

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> cd System32
cd : Cannot find path 'C:\Users\mceager\Desktop\elf2wo\System32' because it does not exist.
At line:1 char:1
+ cd System32
+ CategoryInfo          : ObjectNotFound: (C:\Users\mceager\Desktop\elf2wo\System32:String) [Set-Location], ItemNotFoundException
+ FullyQualifiedErrorId : PathNotFound,Microsoft.PowerShell.Commands.SetLocationCommand

PS C:\Users\mceager\Desktop\elf2wo> cd C:/Windows
PS C:\Windows> cd System32
PS C:\Windows\System32> Get-ChildItem -Hidden -Directory -Filter "*3*"

Directory: C:\Windows\System32

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

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

```

Activate Windows  
Go to Settings to activate Windows.

Answer: 3lfthr3e

Q5: How many words does the first file contain?

After reading the current directory and receiving the text file, we measure the words of the specific file with the help of the command given.

```

Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
kali@kali: ~ x c:\windows\system32\cmd.exe - powershell x

PS C:\Windows\System32> cd 3lfthr3e
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
Get-Content: The term 'Get-Content' 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
+ Get-Content 1.txt | Measure-Object -Word
+ CategoryInfo          : ObjectNotFound: (Get-Content:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

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

Lines Words Characters Property
-----
9999

PS C:\Windows\System32\3lfthr3e>

```

Activate Windows  
Go to Settings to activate Windows.

Answer: 9999

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

We can read the specific words in the list with Get-Content command along with the number of the line we want to read

Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

1 2 3 4

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

10.8.93.122 99% 2:22

File Actions Edit View Help

kali@kali: ~ x c:\windows\system32\cmd.exe - powershell x

Directory: C:\Windows\System32\3lfthr3e

Mode	LastWriteTime	Length	Name
-arh--	System 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 1.txt | Measure-Object -Word  
Get-Context : The term 'Get-Context' 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  
+ Get-Content 1.txt | Measure-Object -Word  
+ ~~~~~  
+ CategoryInfo : ObjectNotFound: (Get-Content:String) [], CommandNotFoundException  
+ FullyQualifiedErrorId : CommandNotFoundArgumentException

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

Lines	Words	Characters	Property
9999			

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>

Activate Windows  
Go to Settings to activate Windows.

2:22 PM 17/7/2022 ENG

Right Click

Answer: Red Ryder

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)

We can use the `Select-String` command along with the word we want which was redryder to get the phrase we want.

Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

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

File Actions Edit View Help

kali@kali: ~ x c:\windows\system32\cmd.exe - powershell x

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

File System

```
PS C:\Windows\System32\3lfthr3e> Get-Context 1.txt | Measure-Object -Word
Get-Context : The term 'Get-Context' 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
+ Get-Context 1.txt | Measure-Object -Word
+ ~~~~~
+ CategoryInfo          : ObjectNotFound: (Get-Context:String) [], CommandNotFoundException
+ FullyQualifiedErrorId : CommandNotFoundException

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

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> Get-Content 2.txt |Select-String -Pattern "redryder"

redryderbbgun
```

Activate Windows  
Go to Settings to activate Windows.

2:25 PM 17/07/2022

File Explorer Task View Start Taskbar

Answer: red ryder bb gun

### Thought process/Methodology:

Having accessed the target machine, we are able to change the directory of the hidden file we want and list files to view the text files available. We also use commands such as Get-Content to read the contents of the file we want. This step is repeated for different directories. After reading the specific directory and receiving the text file, we measure the words of the specific file with the help of the command such as Measure-Object -Word. In a long list in the text file, we can use commands such as Select-String and with the help of filter, instantly get the result we want without looking for it which would be time consuming.