PSP0201

Week 5

Writeup

Group Name: GLM

Members

ID	Name	Role
1211102971	Leong Chun Kit	Leader
1211103023	Yap Weng Hong	Member
1211101232	Lim Kai Qian	Member
1211101407	Tan Fu Shun	Member

Day 16: Scripting - Help! Where is Santa?

Tools used: Firefox and Terminal

Solution/walkthrough:

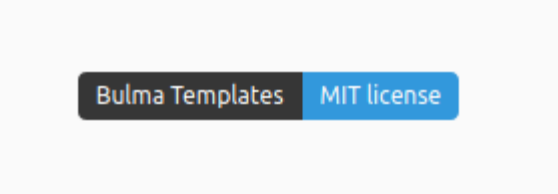
Question 1

We use nmap and type the machine IP then it shows the port number for us.

```
root@ip-10-10-73-242:~# nmap 10.10.143.111

Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-15 07:09 BST
Nmap scan report for ip-10-10-143-111.eu-west-1.compute.internal (10.10.143.111)
Host is up (0.034s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http
MAC Address: 02:AE:34:23:6C:39 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.99 seconds
```

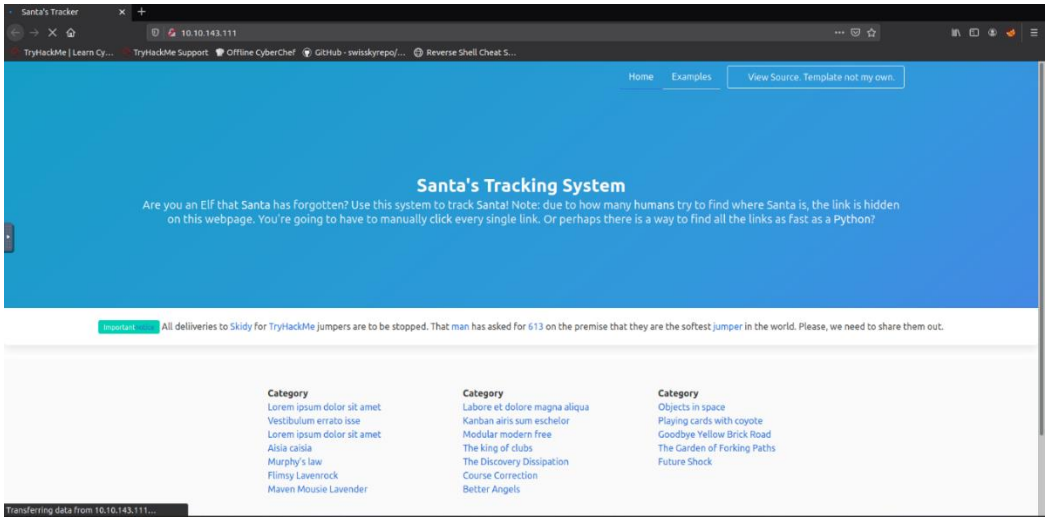
Question 2

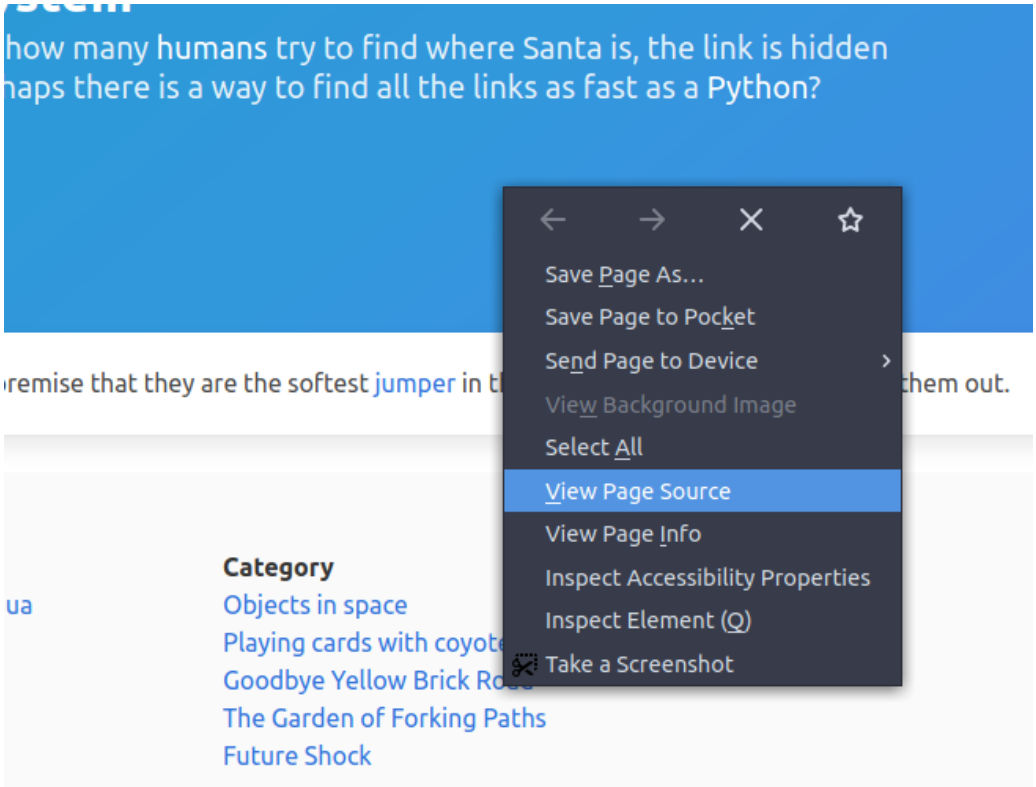
This is the template we used.



Question 3

First, we go Fire fox to search this IP. Then it will lead us to this website. After that, we should right click it and view the page source. Then we will found this link and this is the answer for question 3.

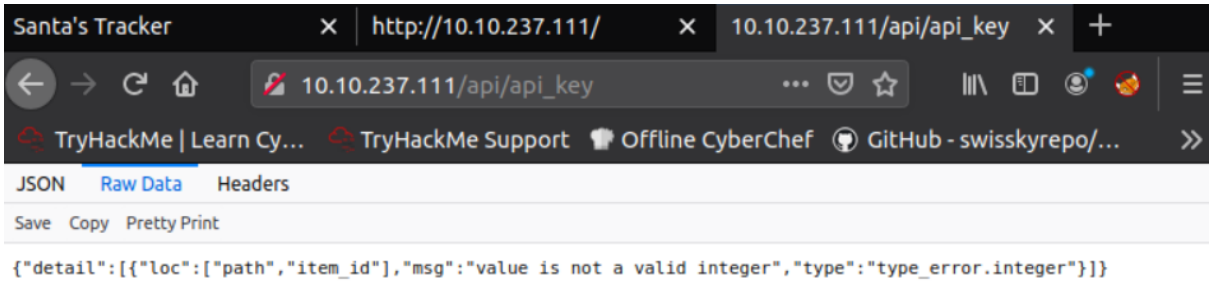

Santa's Tracker
10.10.143.111
TryHackMe | Learn Cy...
TryHackMe Support
Offline CyberChef
GitHub - swisskyrepo/...
Reverse Shell Cheat S...
Home
Examples
View Source. Template not my own.
Santa's Tracking System
Are you an Elf that Santa has forgotten? Use this system to track Santa! Note: due to how 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?
All deliveries to Skidy for TryHackMe jumpers are to be stopped. That man has asked for 613 on the premise that they are the softest jumper in the world. Please, we need to share them out.
Category
Lorem ipsum dolor sit amet
Vestibulum errato isse
Lorem ipsum dolor sit amet
Aisia caisia
Murphy's law
Flimsy Lavenrock
Maven Mousie Lavender
Category
Labore et dolore magna aliqua
Kanban airis sum eschelor
Modular modern free
The king of clubs
The Discovery Dissipation
Course Correction
Better Angels
Category
Objects in space
Playing cards with coyote
Goodbye Yellow Brick Road
The Garden of Forking Paths
Future Shock
Transferring data from 10.10.143.111...


how many humans try to find where Santa is, the link is hidden
haps there is a way to find all the links as fast as a Python?
remise that they are the softest jumper in t
them out.
Save Page As...
Save Page to Pocket
Send Page to Device
View Background Image
Select All
View Page Source
View Page Info
Inspect Accessibility Properties
Inspect Element (Q)
Take a Screenshot
Category
ua
Objects in space
Playing cards with coyot
Goodbye Yellow Brick Ro
The Garden of Forking Paths
Future Shock

```
<!DOCTYPE html>
<html>
    <head>
        <meta charset="utf-8">
        <meta http-equiv="X-UA-Compatible" content="IE=edge">
        <meta name="viewport" content="width=device-width, initial-scale=1">
        <title>Santa's Tracker</title>
        <link rel="shortcut icon" href="" type="image/x-icon">
        <link rel="stylesheet" type="text/css" href="../static/bulma.css">
        <!-- Bulma Version 0.9.0-->
        <link rel="stylesheet" type="text/css" href="../hero.css">
         <!-- <link rel="stylesheet" href="https://unpkg.com/bulma-modal-fx/dist/css/modal-fx.min.
    </head>
    <body>
        <section class="hero is-info is-medium is-bold">
            <div class="hero-head">
                <nav class="navbar">
                    <div class="container">
                        <div class="navbar-brand">
                            <a class="navbar-item" href="../">
                                <img src="http://bulma.io/images/bulma-type-white.png" alt="Logo">
                            </a>
                            <span class="navbar-burger burger" data-target="navbarMenu">
                                <span></span>
                                <span></span>
                                <span></span>
                            </span>
                        </div>
                        <div id="navbarMenu" class="navbar-menu">
                            <div class="navbar-end">
                                <div class="tabs is-right">
                                    <ul>
                                        <li class="is-active"><a>Home</a></li>
                                        <li><a href="">Examples</a></li>
                                    </ul>
                                    <span class="navbar-item">

    <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>
    </ul>
</div>
<div class="column is-4">
```

Question 4

We just open a new tab and follow the format link like Question 3, then it will show the RAW DATA returned and this is the answer.



Question 5 & 6

By using python, first we go import requests. Then, set the range for api_key from 1 to 100 and space twice. After that, we follow the photo and type the code and go terminal start running it.As you see that 57 is the correct key that we want. Question 6 also same with q5 and when we saw the api_key 57, we found that the places where Santa right now.

```python
#!/usr/bin/env python3

import requests

for api_key in range(1,100,2):
    print(f"api_key {api_key}")
    html = requests.get(f'http://10.10.48.42:8000/api/{api_key}')
    print(html.text)

```

```
kali@wsl:~/ctf/thm/aoc_day16$ python3 apibruter.py
{"item_id":1,"q":"Error. Key not valid!"}
kali@wsl:~/ctf/thm/aoc_day16$ python3 apibruter.py
api_key 1
{"item_id":1,"q":"Error. Key not valid!"}
api_key 3
{"item_id":3,"q":"Error. Key not valid!"}
api_key 5
{"item_id":5,"q":"Error. Key not valid!"}
api_key 7
```

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

Thought Process/Methodology:

First, we use nmap and type the machine IP then it shows the port number for us. Next, we go Fire fox to search this IP. Then it will lead us to this website. After that, we should right click it and view the page source. Then we will found this link and this is the answer for question 3. For question 4,we just open a new tab and follow the format link like Question 3, then it will show the RAW DATA returned and this is the answer. For question 5, by using python, we go import requests. Then, set the range for api_key from 1 to 100 and space twice. After that, we follow the photo and type the code and go terminal start running it. As you see that 57 is the correct key that we want. For question 6, it also same with q5 and when we saw the api_key 57, we found that the places where Santa right now.

Day 17: Reverse Engineering – ReverseELFneering

Tools used: Attack box

Solution/walkthrough:

Question 1

In 25 Days of Cyber Security in day 17 we can find out the notes had given the solution for Question 1

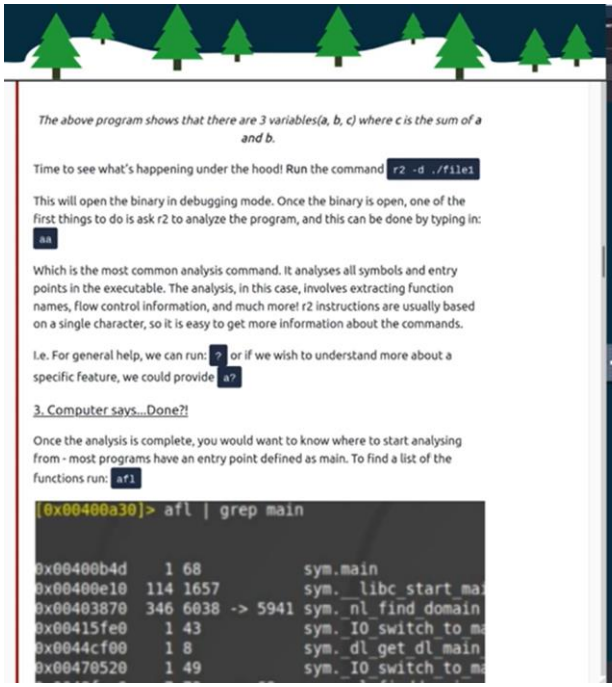
The core of assembly language involves using registers to do the following:

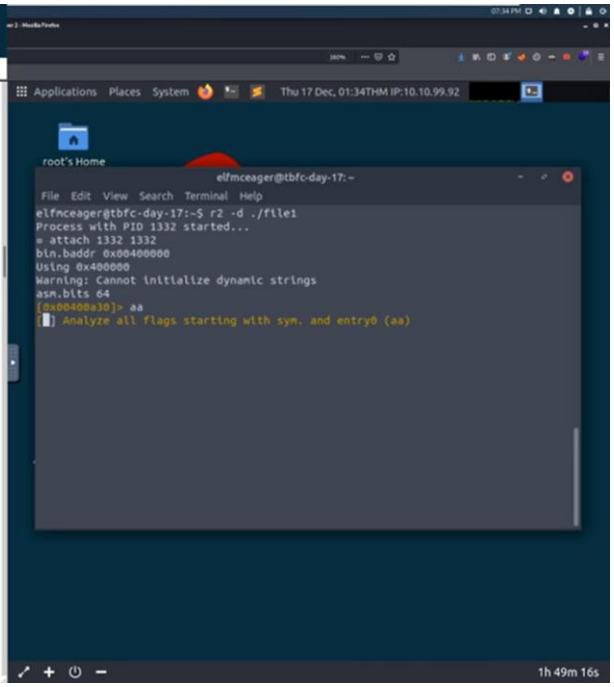
- Transfer data between memory and register, and vice versa
- Perform arithmetic operations on registers and data
- Transfer control to other parts of the program Since the architecture is x86-64, the registers are 64 bit and Intel has a list of 16 registers:

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

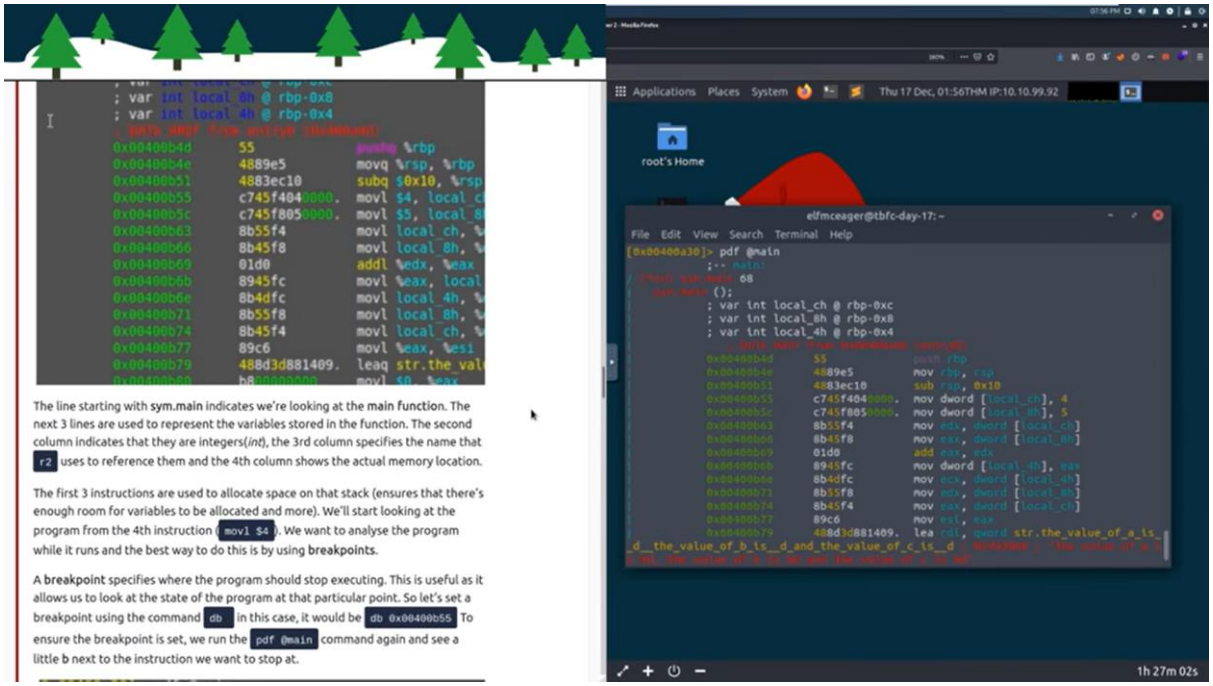
Run the command r2 -d ./file1 to opens the binary files in debugging mode. One of the first things to do is ask r2 to analyse the program, and this can be done by typing in: aa





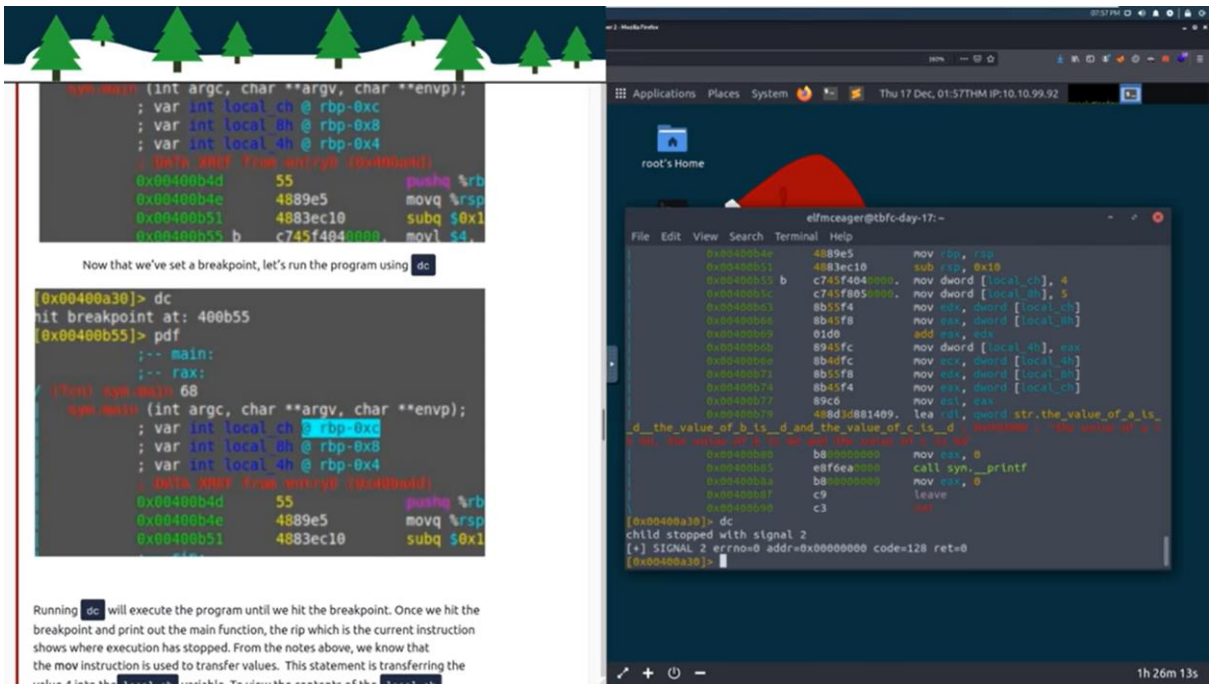
Question 3

After that start looking at the program from the 4th instruction and set it as a breakpoint by using db to analyse the program while it runs. So let's set a breakpoint using the command `db` in this case, it would be `db 0x00400b55`.



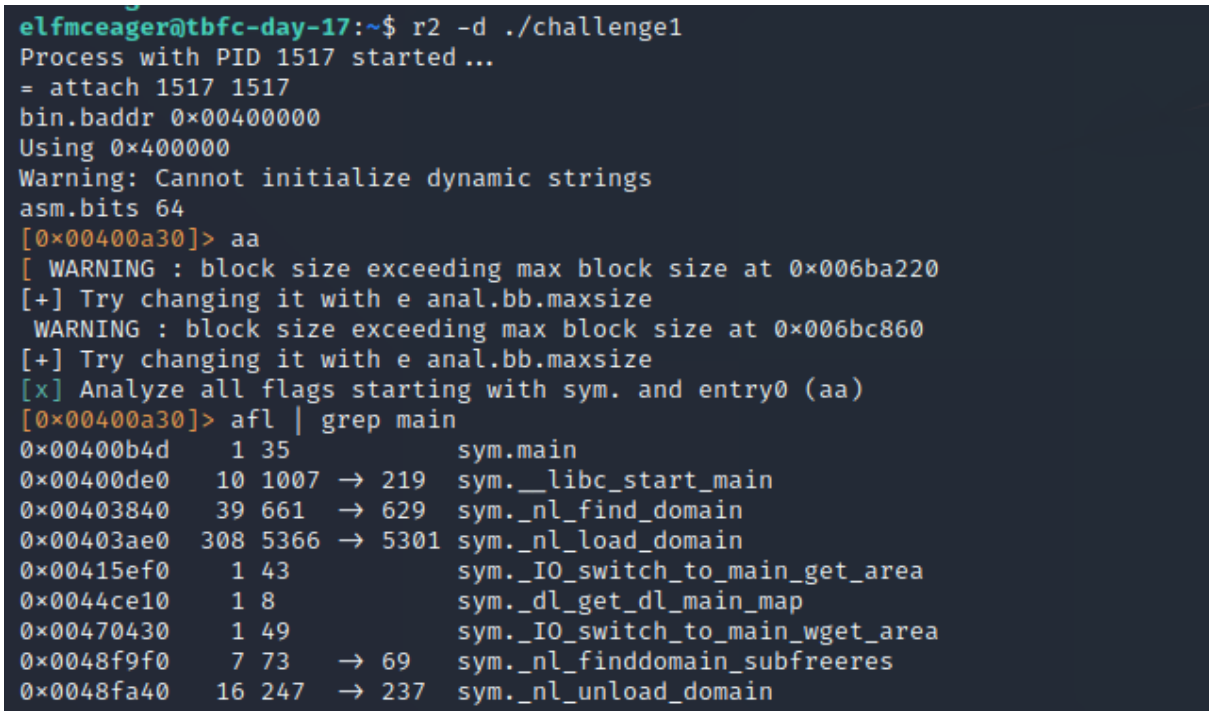
Question 4

Next we use the `dc` command to run the program until it hits the break point. Running `dc` will execute the program until we hit the breakpoint. Once we hit the breakpoint and print out the main function, the rip which is the current instruction shows where execution has stopped.



Question 5

We will start through with the challenge file with command r2 d ./challenge1.We follow the same initial steps. After that command pdf @main we can find out that mov dword [local_ch], 1. This means that the local_ch variable is being set to 1.



Question 6

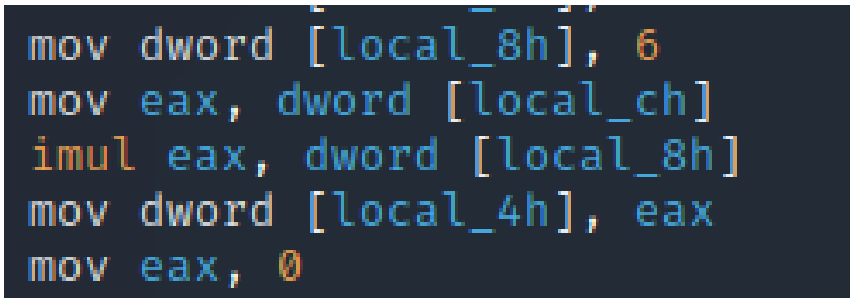
Using the instruction given by we can know that *imulq source, destination*: destination = destination * source. Then, `imul eax, dword [local_8h]` (destination * source or 6*1 = 6)

Some other important instructions are:

- *leaq source, destination*: this instruction sets destination to the address denoted by the expression in source
- *addq source, destination*: destination = destination + source
- *subq source, destination*: destination = destination - source
- *imulq source, destination*: destination = destination * source
- *salq source, destination*: destination = destination << source where << is the left bit shifting operator
- *sarq source, destination*: destination = destination >> source where >> is the right bit shifting operator
- *xorq source, destination*: destination = destination **XOR** source
- andq source, destination: destination = destination & source
- *orq source, destination*: destination = destination | source

Question 7

We confirmed that eax was set to 6. For this question we continue reading. After eax was set to 6, mov dword [local_4h], eax sets [local_4h] to the value of eax, which is 6.



Thought Process/Methodology:

In 25 Days of Cyber Security in day 17 we can find out the notes had given the solution for Question 1. Next, we run the command r2 -d ./file1 to opens the binary files in debugging mode. One of the first things to do is ask r2 to analyse the program, and this can be done by typing in: aa. After that start looking at the program from the 4th instruction and set it as a breakpoint by using db to analyse the program while it runs. So let's set a breakpoint using the command `db` in this case, it would be `db 0x00400b55`. Next,we use the `dc` command to run the program until it hits the break point. Running `dc` will execute the program until we hit the breakpoint. Once we hit the breakpoint and print out the main function, the rip which is the current instruction shows where execution has stopped. We will start through with the challenge file with command r2 d ./challenge1.We follow the same initial steps. After that command pdf @main we can find out that mov dword [local_ch], 1. This means that the local_ch variable is being set to 1. Using the instruction given by we can know that *imulq source, destination*: destination = destination * source. Then, `imul eax, dword [local_8h]` (destination * source or 6*1 = 6). We confirmed that eax was set to 6. For this question we continue reading. After eax was set to 6, mov dword [local_4h], eax sets [local_4h] to the value of eax, which is 6.

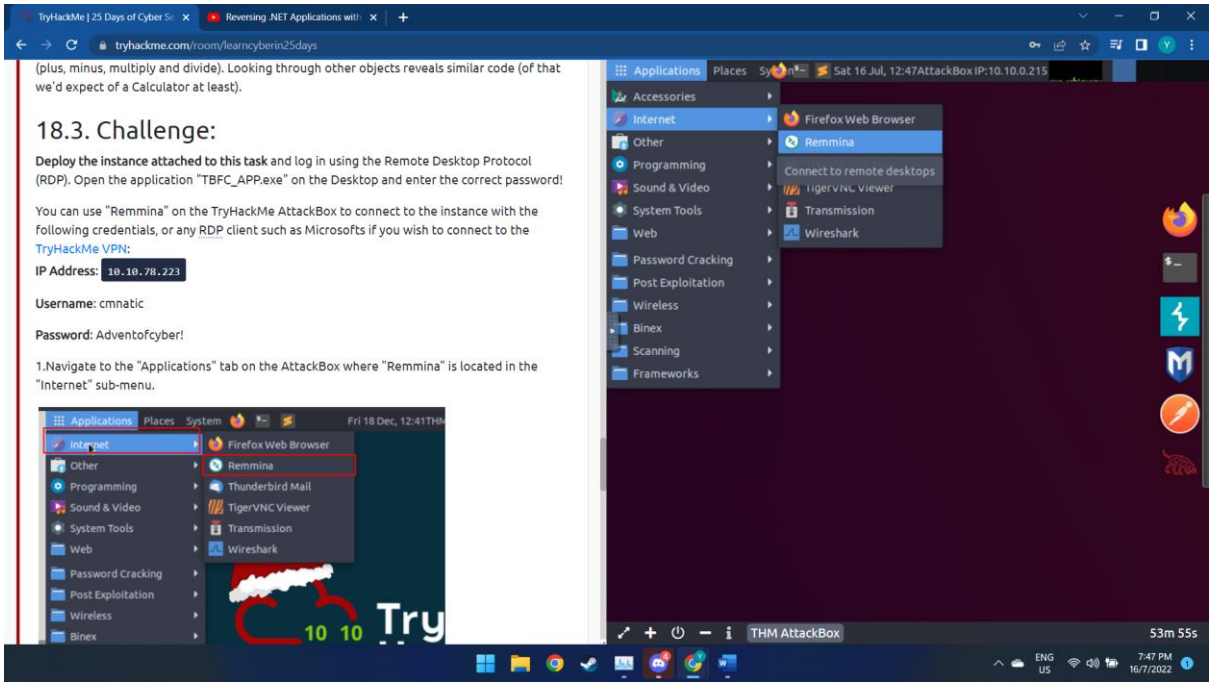
Day 18: Reverse Engineering - The Bits of Christmas

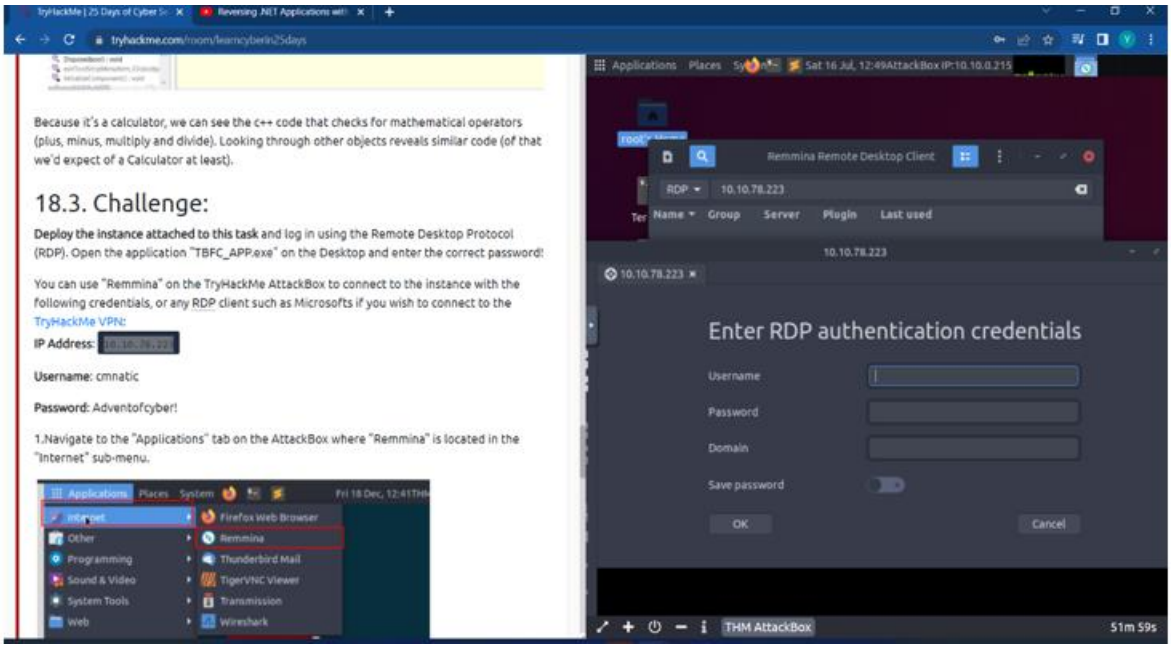
Tools used: IL SPY, Cyberchef, Remmina, TBFC and attack box

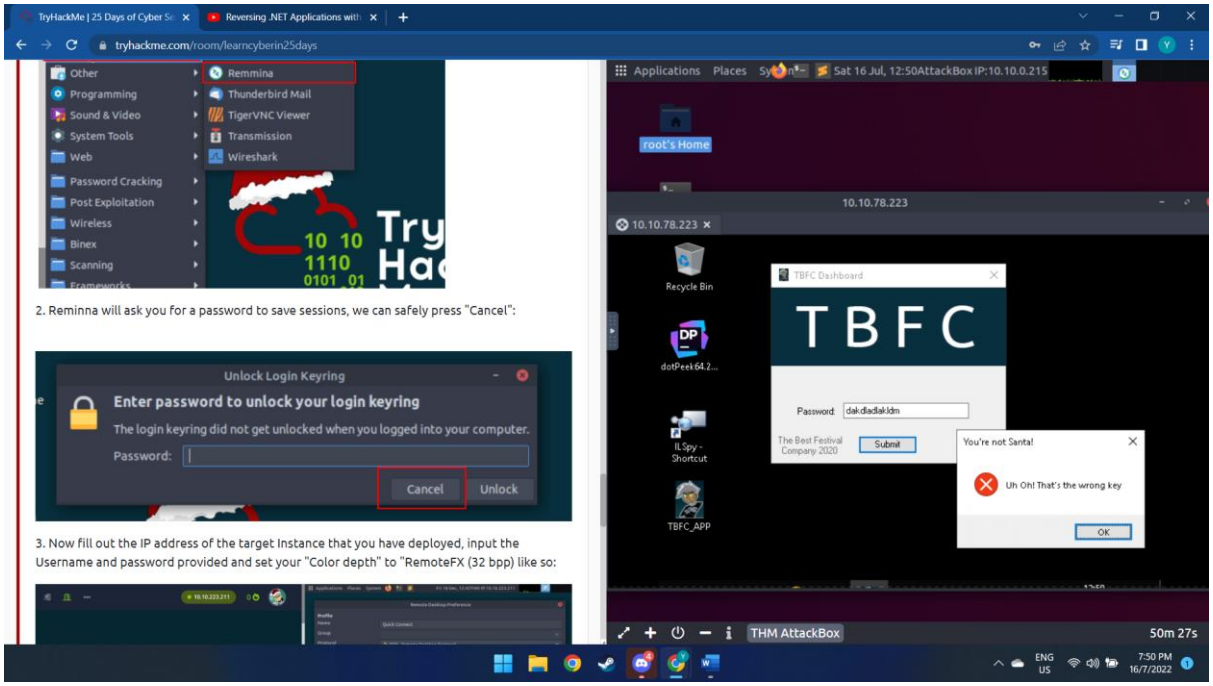
Solution/walkthrough:

Question 1

At start, we open Remmina like this. After that, we search the IP address which given in THM. Then, it will come out the page which inside 2nd photo and about username and password, we copy from THM also and it takes us to a new window. Then, we open the TBFC_APP and type any password because we don't know the password yet. At last, it shows a message which is "Uh Oh! That's the wrong key" which is the answer of question 1.

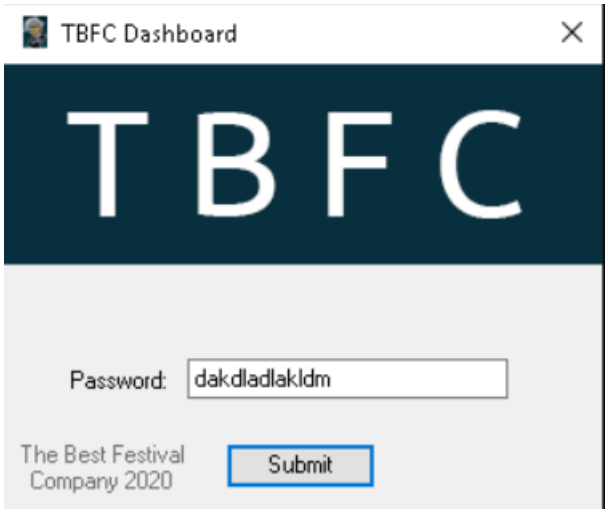






Question 2

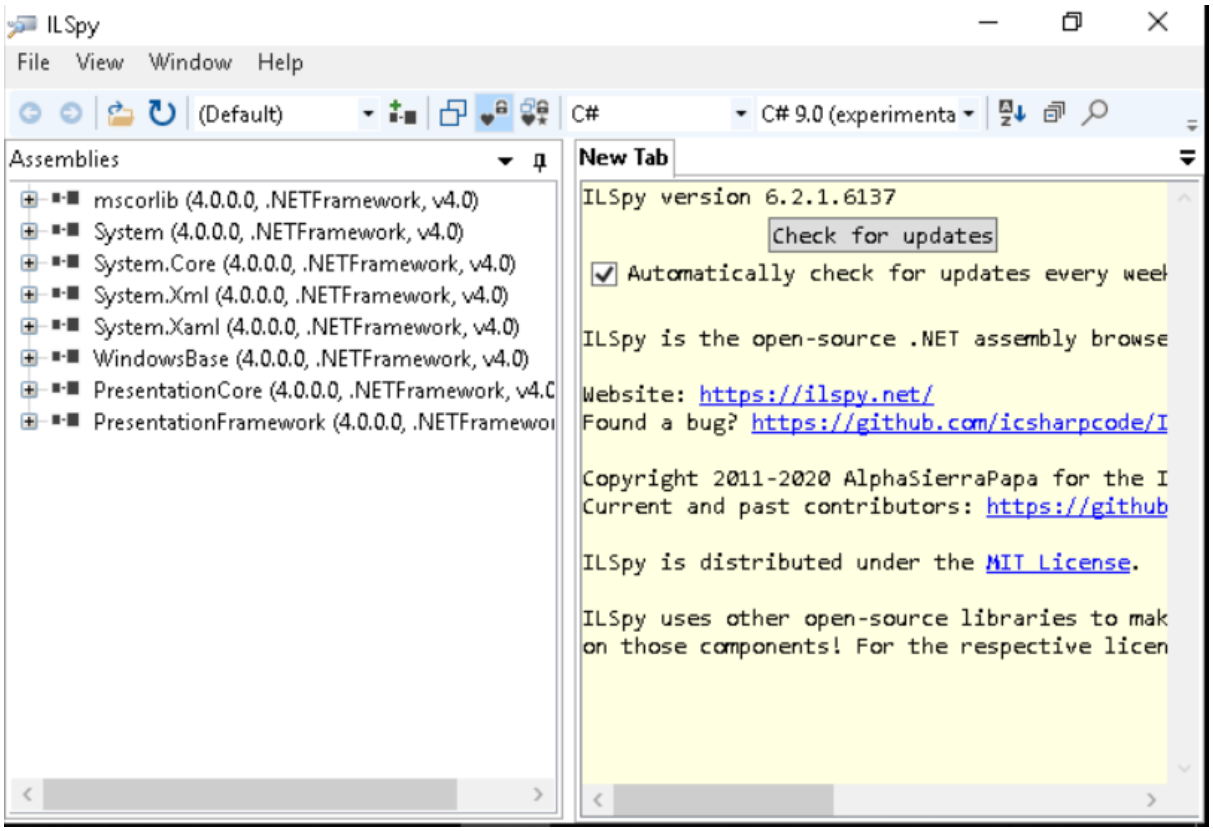
The name of TBFC is at the left bottom corner of the tab as you finish the question 1.

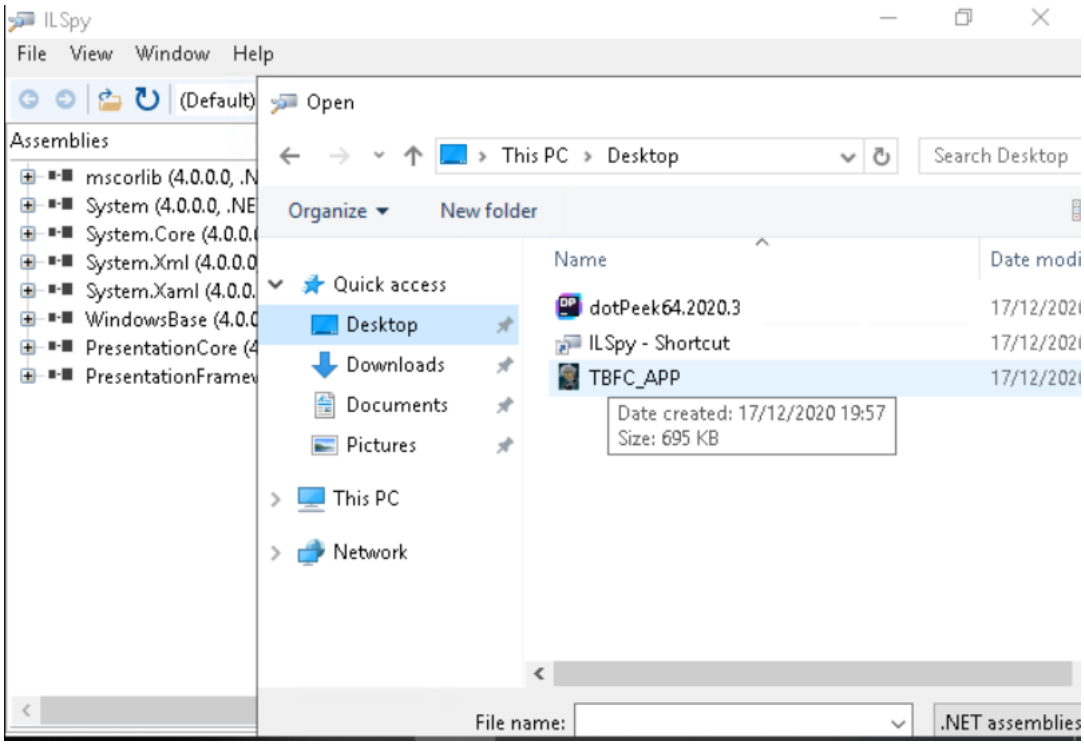


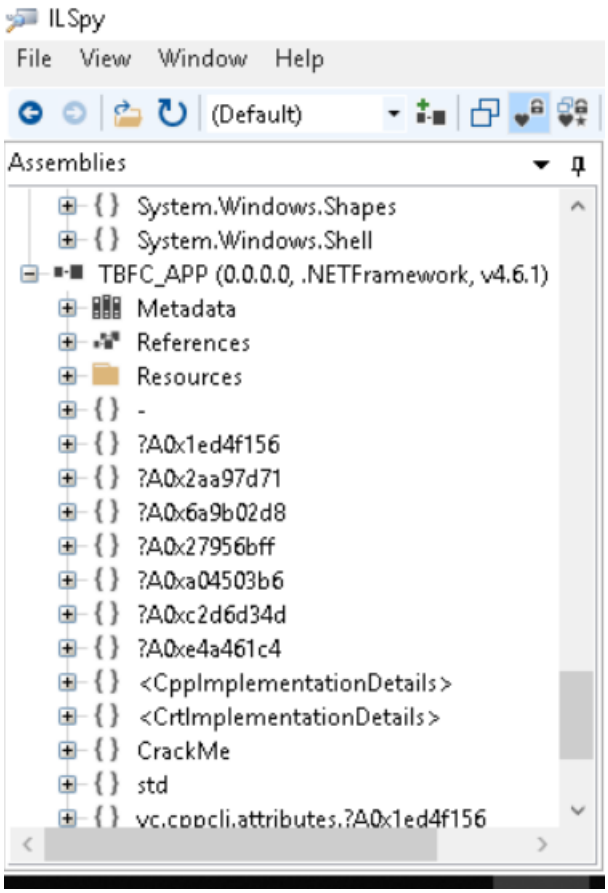
Question 3

We close the TBFC_APP and open another app which is IL Spy. Then, we open TBFC_APP inside IL Spy then it will comes out the new things in Assemblies. We open up the applications and there are many stuffs. Metadata, References and Resources are just not important but Crack Me is the module that catches our attentions and this module will lead us to solve following questions.


ILSpy -
Shortcut
Location: ILSpy

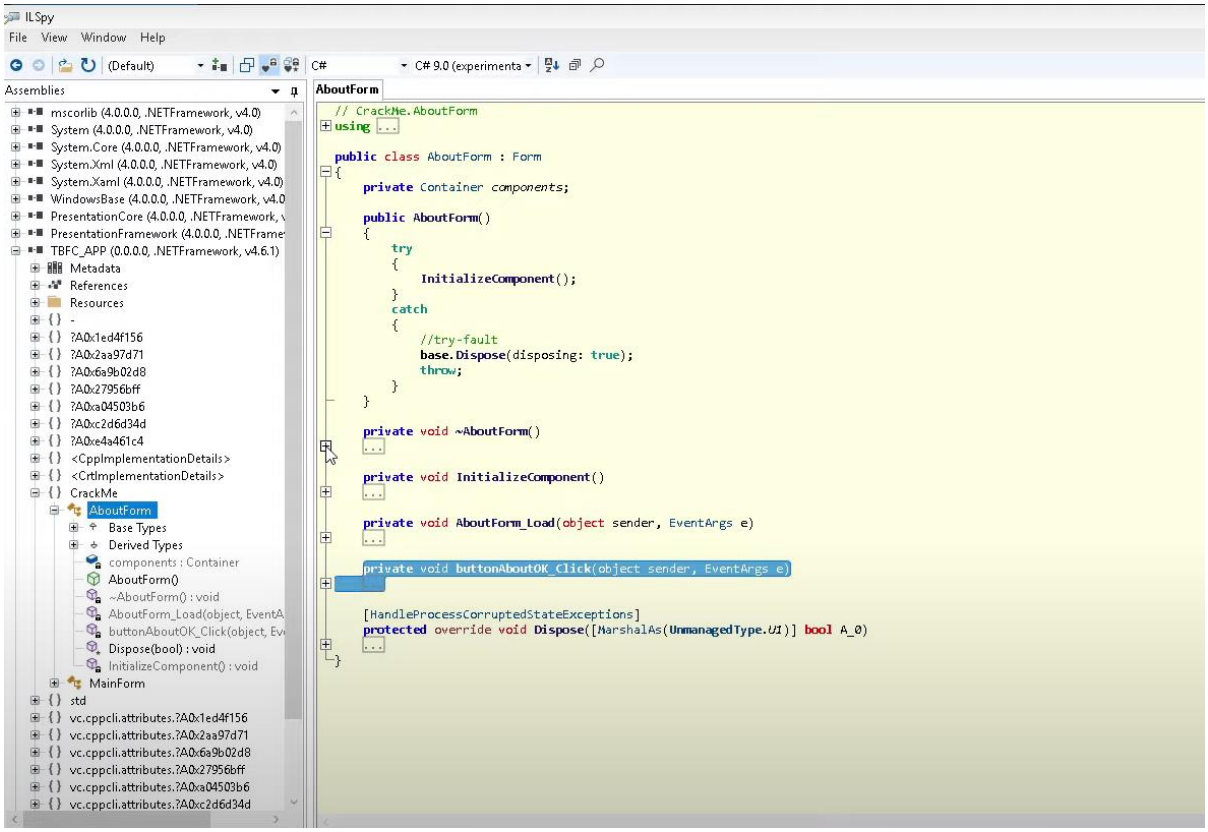

ILSpy
File View Window Help
(Default)
C#
C# 9.0 (experimenta
Assemblies
mscorlib (4.0.0.0, .NETFramework, v4.0)
System (4.0.0.0, .NETFramework, v4.0)
System.Core (4.0.0.0, .NETFramework, v4.0)
System.Xml (4.0.0.0, .NETFramework, v4.0)
System.Xaml (4.0.0.0, .NETFramework, v4.0)
WindowsBase (4.0.0.0, .NETFramework, v4.0)
PresentationCore (4.0.0.0, .NETFramework, v4.0
PresentationFramework (4.0.0.0, .NETFramewo
New Tab
ILSpy version 6.2.1.6137
Check for updates
Automatically check for updates every week
ILSpy is the open-source .NET assembly browse
Website: https://ilspy.net/
Found a bug? https://github.com/icsharpcode/I
Copyright 2011-2020 AlphaSierraPapa for the I
Current and past contributors: https://github
ILSpy is distributed under the MIT License.
ILSpy uses other open-source libraries to mak
on those components! For the respective licen

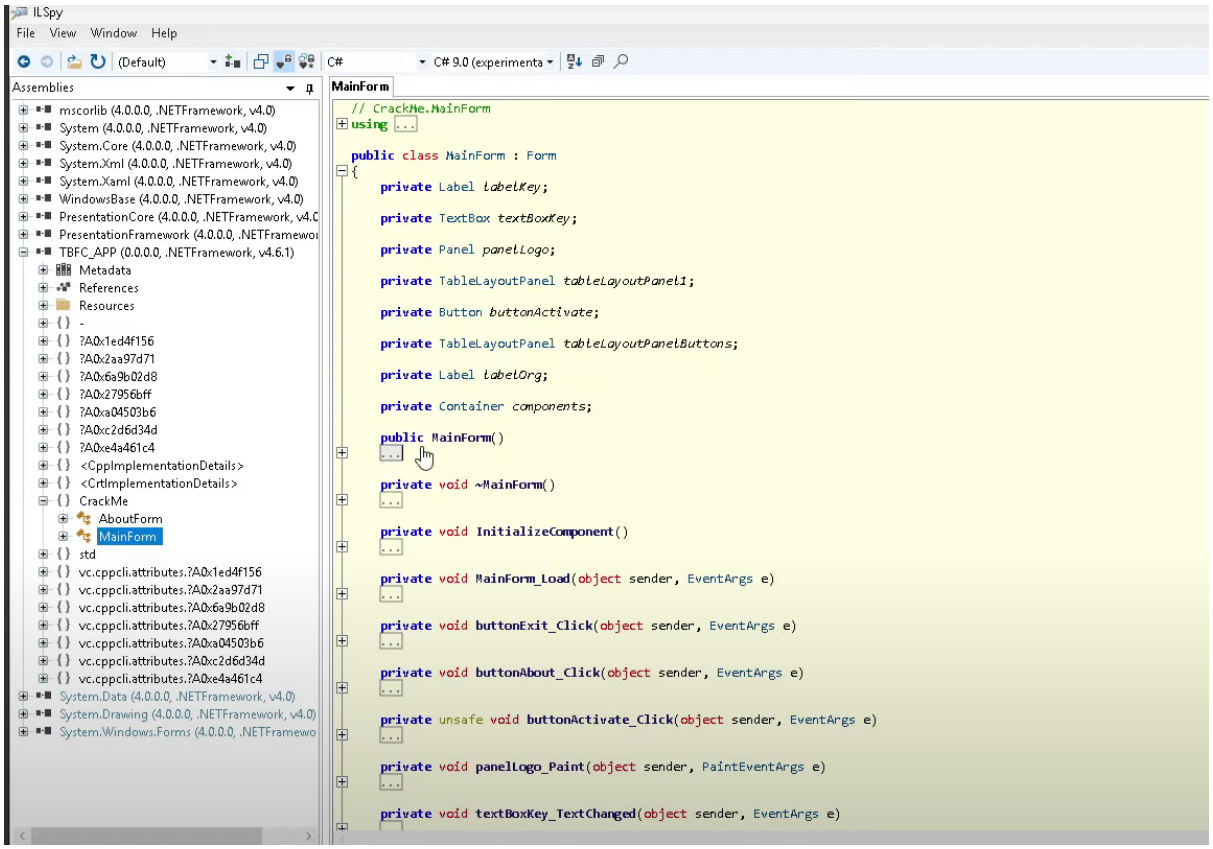

ILSpy
File View Window Help
(Default)
Assemblies
Open
This PC › Desktop
Search Desktop
Organize
New folder
Quick access
Desktop
Downloads
Documents
Pictures
This PC
Network
Name
Date modi
dotPeek64.2020.3
ILSpy - Shortcut
TBFC_APP
Date created: 17/12/2020 19:57
Size: 695 KB
File name:
.NET assemblies



Question 4

About CrackMe, it has 2 form which is AboutForm and MainForm. AboutForm just have a little bit information only and mainly MainForm is the forms that contains many information that we looking for.

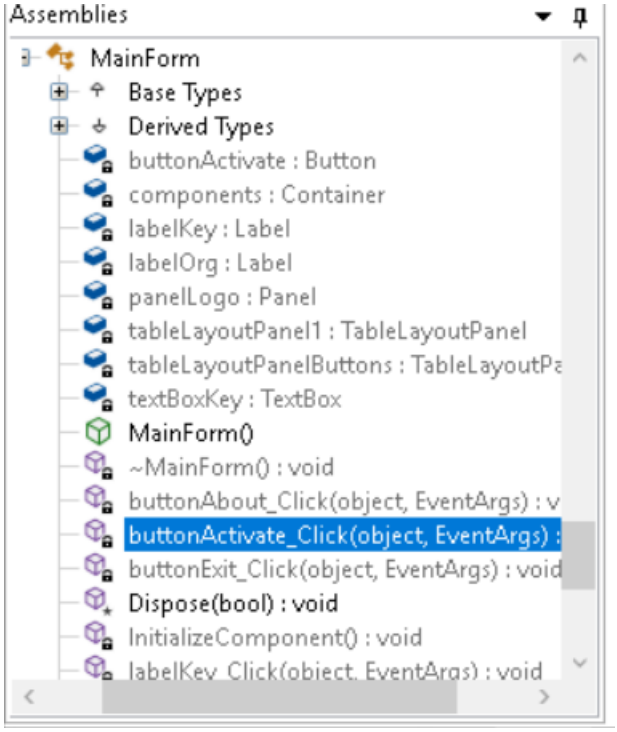

ILSpy
File View Window Help
(Default)
C#
C# 9.0 (experimenta
Assemblies
mscorlib (4.0.0.0, .NETFramework, v4.0)
System (4.0.0.0, .NETFramework, v4.0)
System.Core (4.0.0.0, .NETFramework, v4.0)
System.Xml (4.0.0.0, .NETFramework, v4.0)
System.Xaml (4.0.0.0, .NETFramework, v4.0)
WindowsBase (4.0.0.0, .NETFramework, v4.0)
PresentationCore (4.0.0.0, .NETFramework,
PresentationFramework (4.0.0.0, .NETFrame
TBFC_APP (0.0.0.0, .NETFramework, v4.6.1)
Metadata
References
Resources
-
?A0x1ed4f156
?A0x2aa97d71
?A0x6a9b02d8
?A0x27956bff
?A0xa04503b6
?A0xc2d6d34d
?A0xe4a461c4
<CppImplementationDetails>
<CrtImplementationDetails>
CrackMe
AboutForm
Base Types
Derived Types
components : Container
AboutForm()
~AboutForm() : void
AboutForm_Load(object, EventA
buttonAboutOK_Click(object, Ev
Dispose(bool) : void
InitializeComponent() : void
MainForm
std
vc.cppcli.attributes.?A0x1ed4f156
vc.cppcli.attributes.?A0x2aa97d71
vc.cppcli.attributes.?A0x6a9b02d8
vc.cppcli.attributes.?A0x27956bff
vc.cppcli.attributes.?A0xa04503b6
vc.cppcli.attributes.?A0xc2d6d34d
AboutForm
// CrackMe.AboutForm
using ...
public class AboutForm : Form
{
private Container components;
public AboutForm()
{
try
{
InitializeComponent();
}
catch
{
//try-fault
base.Dispose(disposing: true);
throw;
}
}
private void ~AboutForm()
...
private void InitializeComponent()
...
private void AboutForm_Load(object sender, EventArgs e)
...
private void buttonAboutOK_Click(object sender, EventArgs e)
...
[HandleProcessCorruptedStateExceptions]
protected override void Dispose([MarshalAs(UnmanagedType.U1)] bool A_0)
...
}


ILSpy
File View Window Help
(Default)
C#
C# 9.0 (experimenta
Assemblies
mscorlib (4.0.0.0, .NETFramework, v4.0)
System (4.0.0.0, .NETFramework, v4.0)
System.Core (4.0.0.0, .NETFramework, v4.0)
System.Xml (4.0.0.0, .NETFramework, v4.0)
System.Xaml (4.0.0.0, .NETFramework, v4.0)
WindowsBase (4.0.0.0, .NETFramework, v4.0)
PresentationCore (4.0.0.0, .NETFramework, v4.0
PresentationFramework (4.0.0.0, .NETFramewo
TBFC_APP (0.0.0.0, .NETFramework, v4.6.1)
Metadata
References
Resources
-
?A0x1ed4f156
?A0x2aa97d71
?A0x6a9b02d8
?A0x27956bff
?A0xa04503b6
?A0xc2d6d34d
?A0xe4a461c4
<CppImplementationDetails>
<CrtImplementationDetails>
CrackMe
AboutForm
MainForm
std
vc.cppcli.attributes.?A0x1ed4f156
vc.cppcli.attributes.?A0x2aa97d71
vc.cppcli.attributes.?A0x6a9b02d8
vc.cppcli.attributes.?A0x27956bff
vc.cppcli.attributes.?A0xa04503b6
vc.cppcli.attributes.?A0xc2d6d34d
vc.cppcli.attributes.?A0xe4a461c4
System.Data (4.0.0.0, .NETFramework, v4.0)
System.Drawing (4.0.0.0, .NETFramework, v4.0)
System.Windows.Forms (4.0.0.0, .NETFramewo
MainForm
// 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;
public MainForm()
...
private void ~MainForm()
...
private void InitializeComponent()
...
private void MainForm_Load(object sender, EventArgs e)
...
private void buttonExit_Click(object sender, EventArgs e)
...
private void buttonAbout_Click(object sender, EventArgs e)
...
private unsafe void buttonActivate_Click(object sender, EventArgs e)
...
private void panelLogo_Paint(object sender, PaintEventArgs e)
...
private void textBoxKey_TextChanged(object sender, EventArgs e)

```
private void InitializeComponent()
{
    System.ComponentModel.ComponentResourceManager resources = new System.ComponentModel.ComponentResourceManager(typeof(CrackMe.MainForm));
    labelKey = new System.Windows.Forms.Label();
    textBoxKey = new System.Windows.Forms.TextBox();
    panelLogo = new System.Windows.Forms.Panel();
    tableLayoutPanel1 = new System.Windows.Forms.TableLayoutPanel();
    buttonActivate = new System.Windows.Forms.Button();
    tableLayoutPanelButtons = new System.Windows.Forms.TableLayoutPanel();
    labelOrg = new System.Windows.Forms.Label();
    tableLayoutPanel1.SuspendLayout();
    tableLayoutPanelButtons.SuspendLayout();
    SuspendLayout();
    labelKey.Anchor = System.Windows.Forms.AnchorStyles.Right;
    labelKey.AutoSize = true;
    System.Drawing.Point location = new System.Drawing.Point(30, 14);
    labelKey.Location = location;
    labelKey.Name = "labelKey";
    System.Drawing.Size size = new System.Drawing.Size(56, 13);
    labelKey.Size = size;
    labelKey.TabIndex = 0;
    labelKey.Text = "Password:";
    labelKey.Click += new System.EventHandler(labelKey_Click);
    textBoxKey.Anchor = System.Windows.Forms.AnchorStyles.Left;
    System.Drawing.Point location2 = new System.Drawing.Point(92, 10);
    textBoxKey.Location = location2;
    textBoxKey.Name = "textBoxKey";
    System.Drawing.Size size2 = new System.Drawing.Size(160, 20);
    textBoxKey.Size = size2;
    textBoxKey.TabIndex = 1;
    textBoxKey.TextChanged += new System.EventHandler(textBoxKey_TextChanged);
    panelLogo.BackgroundImage = (System.Drawing.Image)resources.GetObject("panelLogo.BackgroundImage");
    panelLogo.BackgroundImageLayout = System.Windows.Forms.ImageLayout.Center;
    panelLogo.Dock = System.Windows.Forms.DockStyle.Top;
    System.Drawing.Point location3 = new System.Drawing.Point(0, 0);
    panelLogo.Location = location3;
    panelLogo.Name = "panelLogo";
    System.Drawing.Size size3 = new System.Drawing.Size(299, 100);
    panelLogo.Size = size3;
    panelLogo.TabIndex = 2;
    panelLogo.Paint += new System.Windows.Forms.PaintEventHandler(panelLogo_Paint);
    tableLayoutPanel1.ColumnCount = 2;
```

Question 5

We take a look at buttonActivate_Click and then we found that the code we looking for.

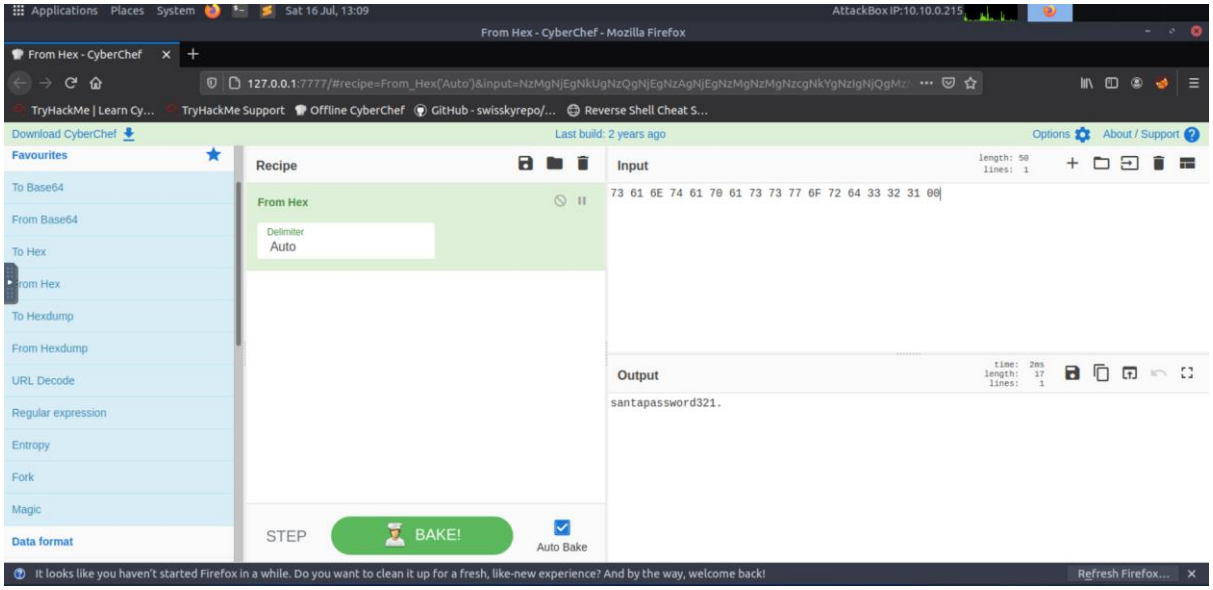


```
// CrackMe.MainForm
using ...

private unsafe void buttonActivate_Click(object sender, EventArgs e)
{
    IntPtr value = Marshal.StringToHGlobalAnsi(textBoxKey.Text);
    sbyte* ptr = (sbyte*)System.Runtime.CompilerServices.Unsafe.AsPointer(ref <Module>.??_C@_0BB@IKKDFEPG@santapassword321@);
    void* ptr2 = (void*)value;
    byte b = *(byte*)ptr2;
    byte b2 = 115;
    if ((uint)b >= 115u)
    {
        while ((uint)b <= (uint)b2)
        {
            if (b != 0)
            {
                ptr2 = (byte*)ptr2 + 1;
                ptr++;
                b = *(byte*)ptr2;
                b2 = (byte)(*ptr);
                if ((uint)b < (uint)b2)
                {
                    break;
                }
                continue;
            }
            MessageBox.Show("Welcome, Santa, here's your flag thm{046af}", "That's the right key!", MessageBoxButtons.OK, MessageBoxIcon.Asterisk);
            return;
        }
    }
    MessageBox.Show("Uh Oh! That's the wrong key", "You're not Santa!", MessageBoxButtons.OK, MessageBoxIcon.Hand);
}
```

Question 6

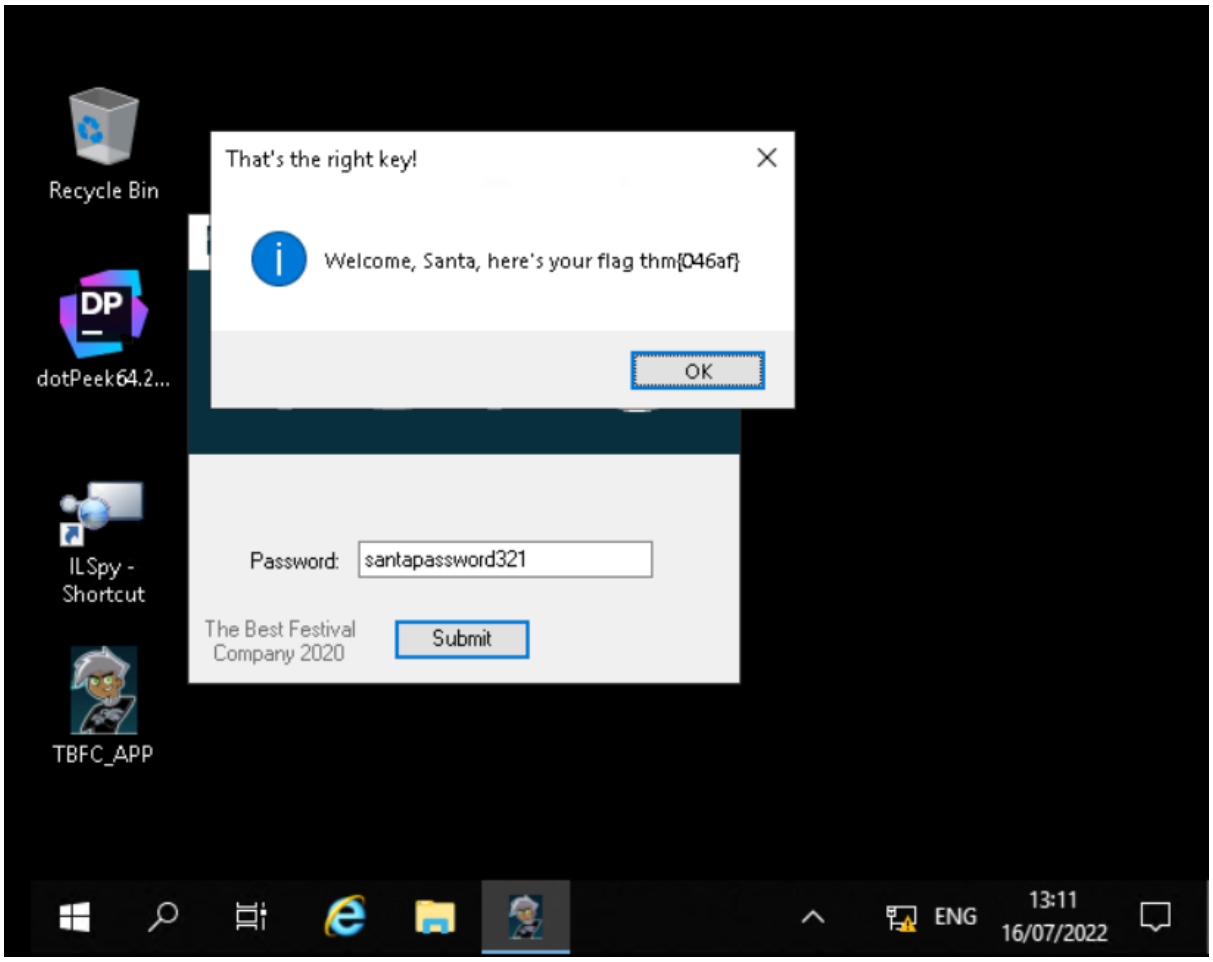
We doubleclick the code which under 1st photo and then it lead us to another code. We copy the number inside the bracket and use cyberchef to solve it. Then, we put inside the input and use the hexa recipe to convert it. Then we found the password.


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

internal static $ArrayType$$$BY0BB@$$CBD ??_C@_0BB@IKKDFEPG@santapassword321@/* Not supported: data(73 61 6E 74 61 70 61 73 73 77 6F 72 64 33 32 31 00) */;
```



Question 7

As we type the correct password which given in Question 6 it will give the flag to us.



Thought Process/Methodology:

At start, we open Remmina like this. After that, we search the IP address which given in THM. Then, it will come out the page which inside 2nd photo and about username and password, we copy from THM also and it takes us to a new window. Then, we open the TBFC_APP and type any password because we don't know the password yet. At last, it shows a message which is "Uh Oh! That's the wrong key" which is the answer of question 1. The name of TBFC is at the left bottom corner of the tab as you finish the question 1. We close the TBFC_APP and open another app which is IL Spy. Then, we open TBFC_APP inside IL Spy then it will comes out the new things in Assemblies. We open up the applications and there are many stuffs. Metadata, References and Resources are just not important but Crack Me is the module that catches our attentions and this module will lead us to solve following questions. About CrackMe, it has 2 form which is AboutForm and MainForm. AboutForm just have a little bit information only and mainly MainForm is the forms that contains many information that we looking for. We take a look at buttonActivate_Click and then we found that the code we looking for. We doubleclick the code which under 1st photo and then it lead us to another code. We copy the number inside the bracket and use cyberchef to solve it. Then, we put inside the input and use the hexa recipe to convert it. Then we found the password. As we type the correct password which given in Question 6 it will give the flag to us.

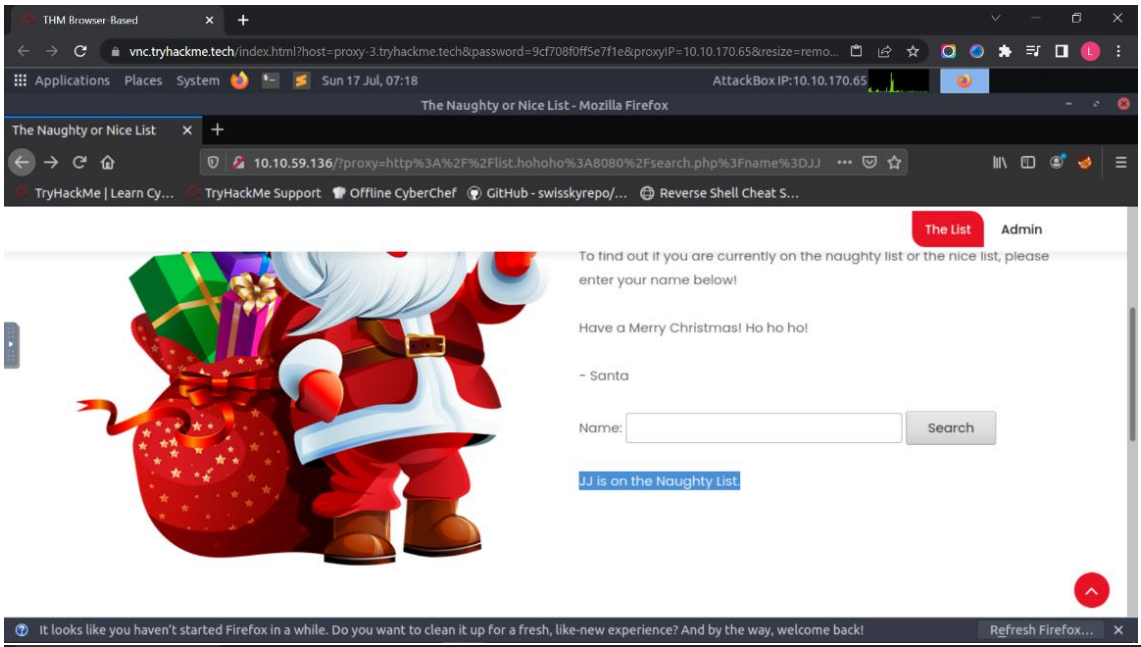
Day 19: Web Exploitation - The Naughty or Nice List

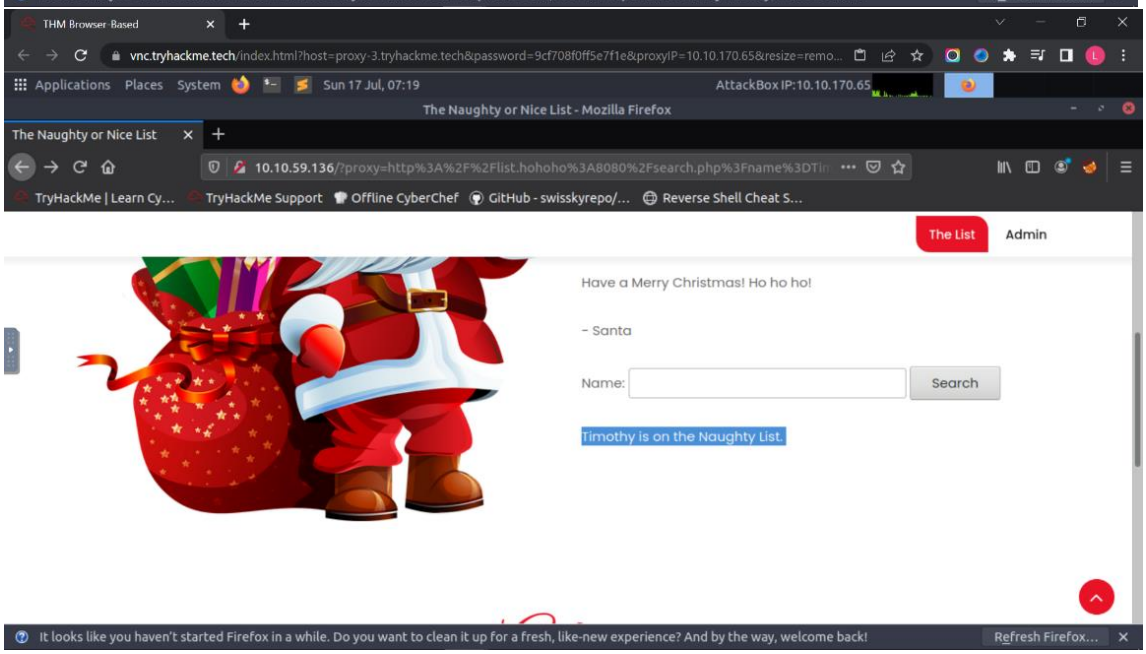
Tools used: Firefox and Terminal

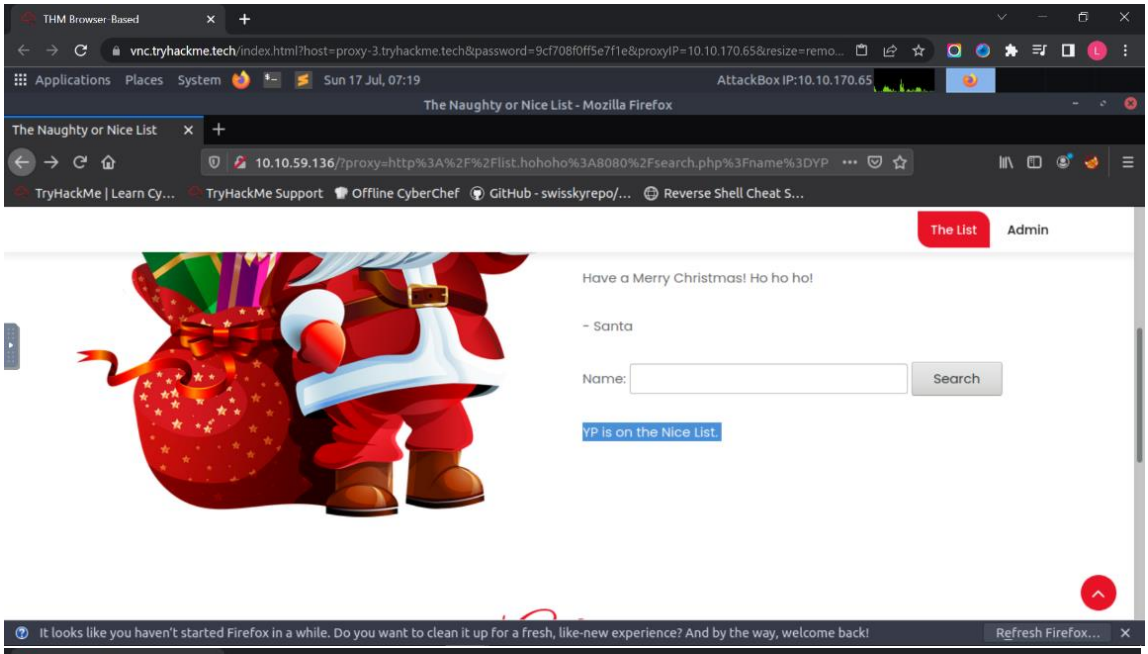
Solution/walkthrough:

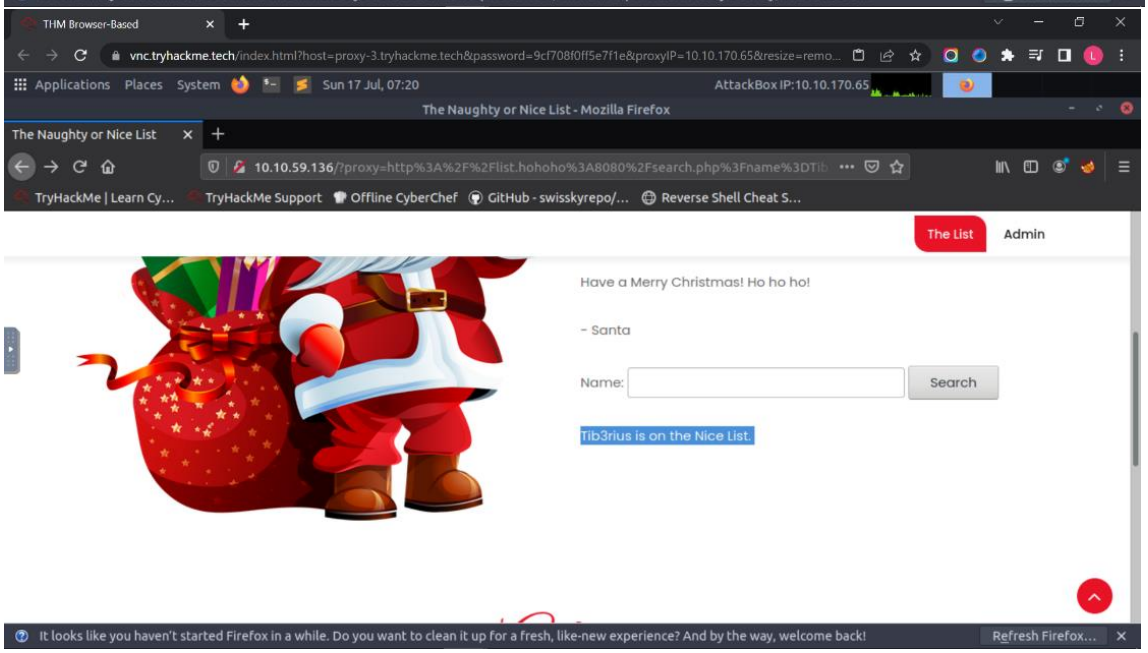
Question 1

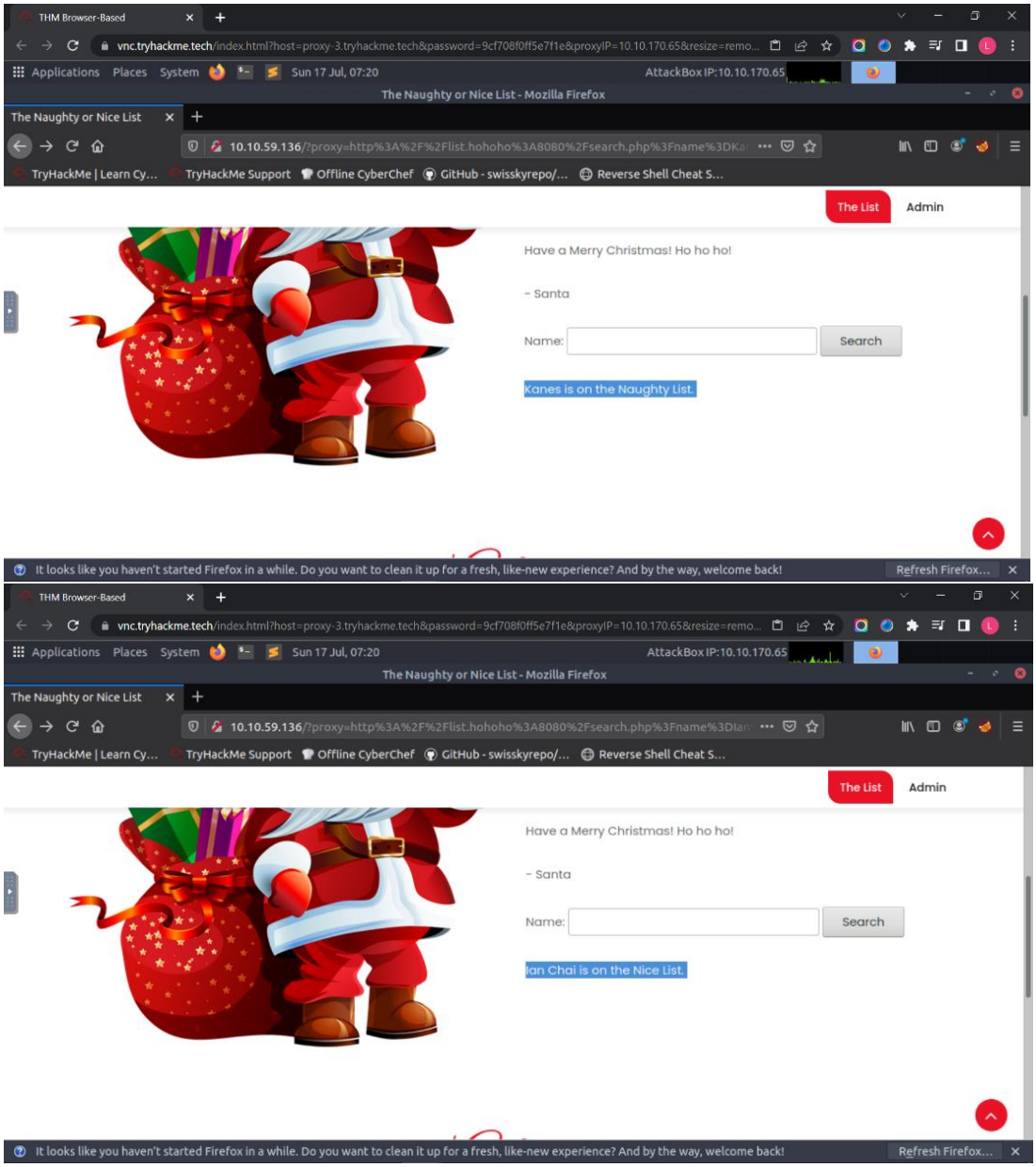
Access to URL “http://IP address” and type all the name one by one to see it is naughty or nice.





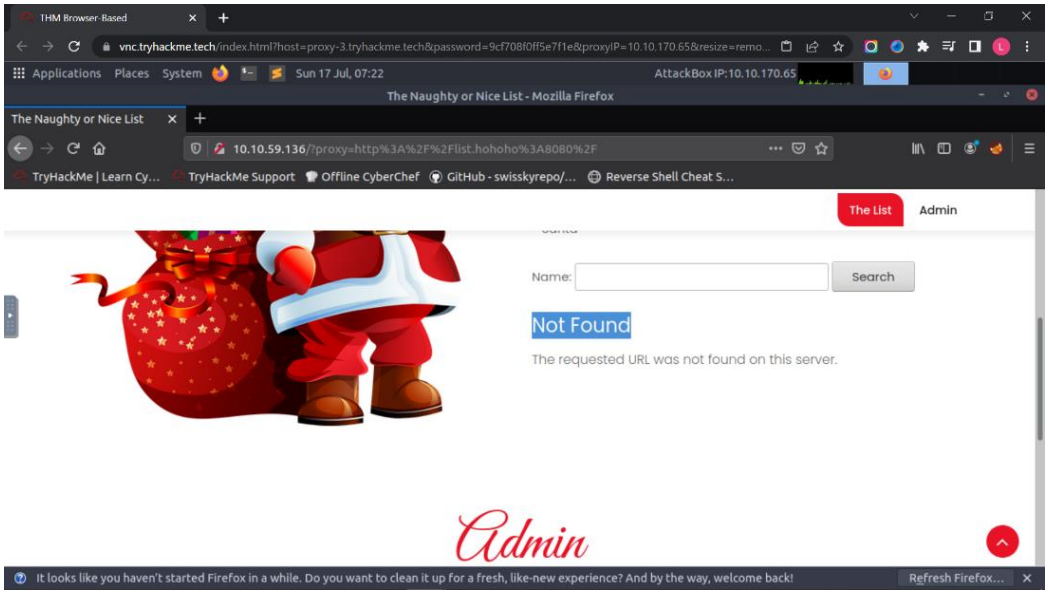

THM Browser-Based
vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=9cf708f0ff5e7f1e&proxyIP=10.10.170.65&resize=remo...
Applications Places System Sun 17 Jul, 07:19
AttackBox IP:10.10.170.65
The Naughty or Nice List - Mozilla Firefox
The Naughty or Nice List
10.10.59.136/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DYP
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...
The List
Admin
Have a Merry Christmas! Ho ho ho!
- Santa
Name:
Search
YP is on the Nice List.
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...


THM Browser-Based
vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=9cf708f0ff5e7f1e&proxyIP=10.10.170.65&resize=remo...
Applications Places System Sun 17 Jul, 07:20
AttackBox IP:10.10.170.65
The Naughty or Nice List - Mozilla Firefox
The Naughty or Nice List
10.10.59.136/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DTib
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...
The List
Admin
Have a Merry Christmas! Ho ho ho!
- Santa
Name:
Search
Tib3rius is on the Nice List.
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...



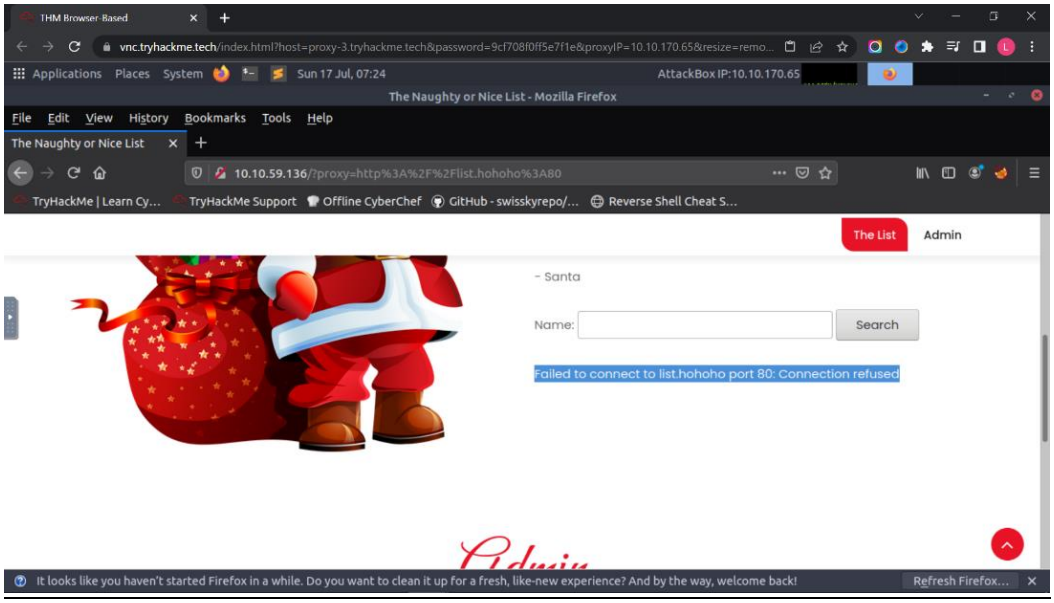
Question 2

Add "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F" behind the “http://IP address” and get the display of “Not Found. The requested URL was not found on this server.”



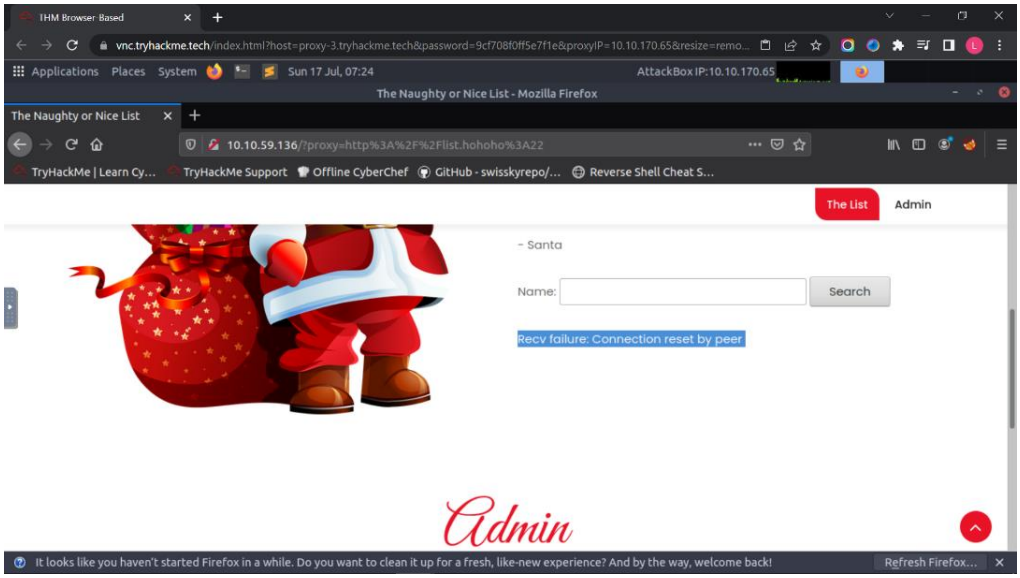
Question 3

Add "/?proxy=http%3A%2F%2Flist.hohoho%3A80" behind the "http://IP address" and get the display of "Failed to connect to list.hohoho port 80: Connection refused".



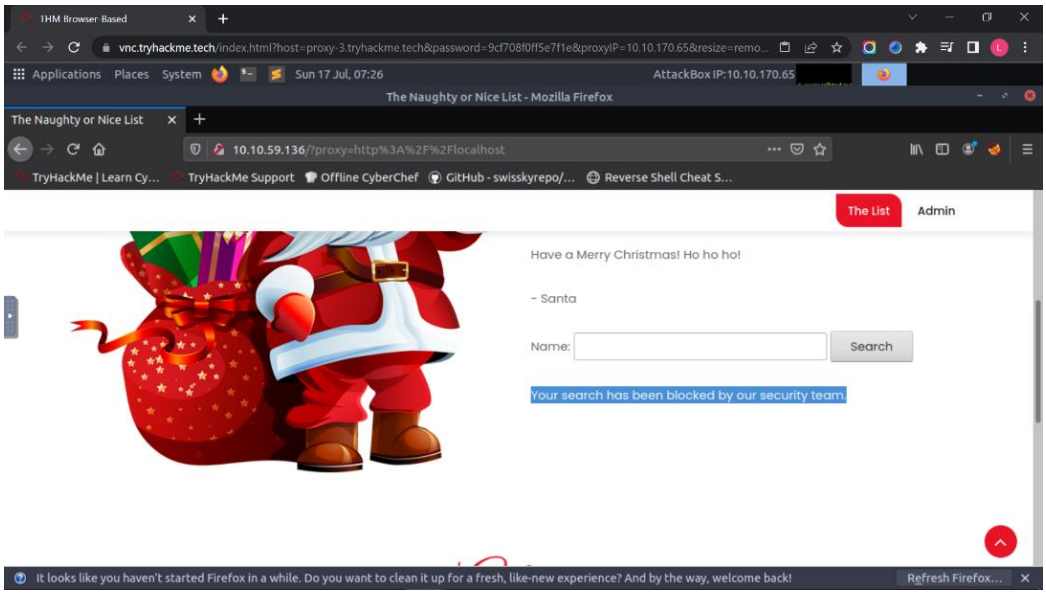
Question 4

Add "/?proxy=http%3A%2F%2Flist.hohoho%3A22" behind the "http://IP address" and get the display of "Recv failure: Connection reset by peer".



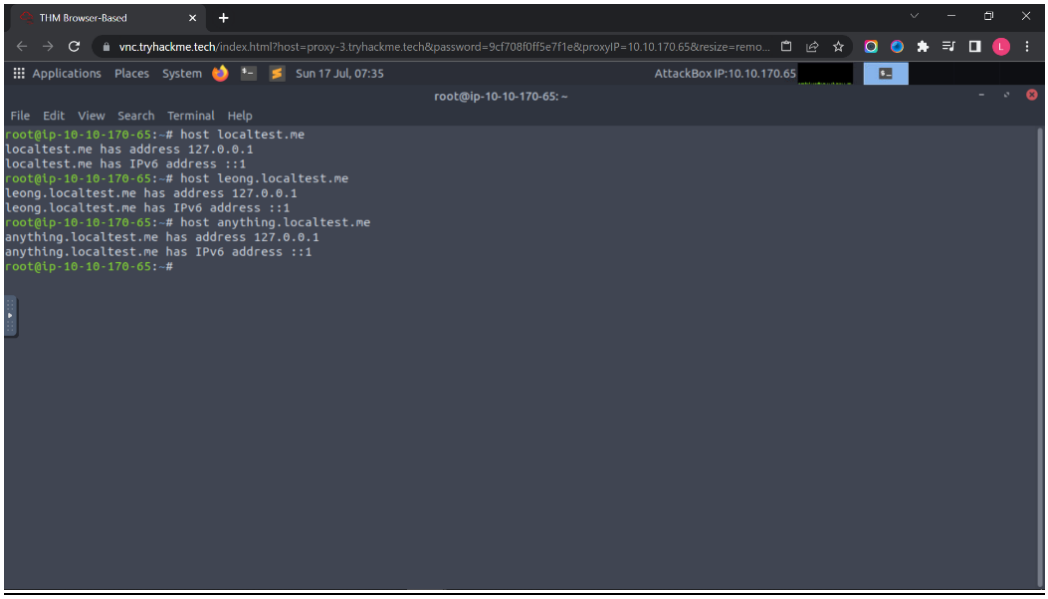
Question 5

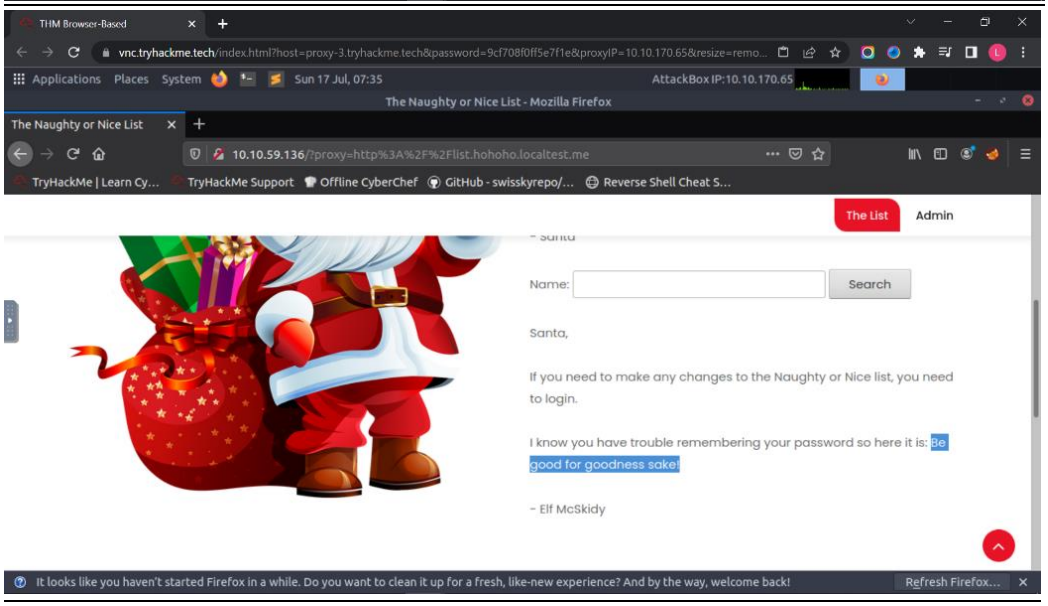
Add "/?proxy=http%3A%2F%2Flocalhost" behind the "http://IP address" and get the display of "Your search has been blocked by our security team.".



Question 6

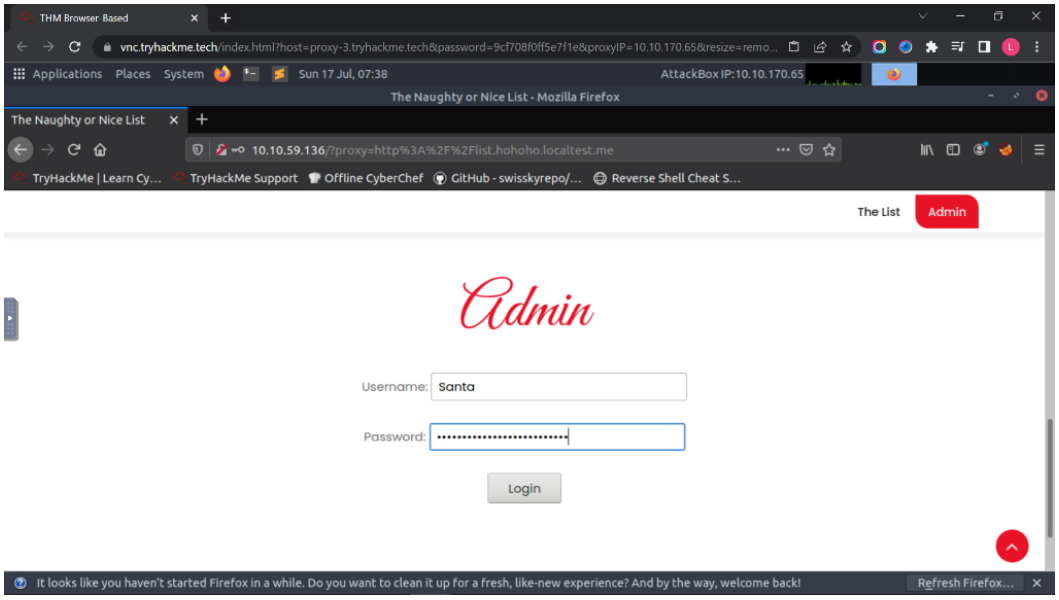
First, we need to prove that the address is the same 127.0.0.1 by using the terminal. We type "host localtest.me", "host leong.localtest.me" and "host anything.localtest.me" to make sure all of the output is the same address 127.0.0.1. Next, we add "/?proxy=http%3A%2F%2Flist.hohoho.localtest.me" behind the "http://IP address" and get the password of Santa.

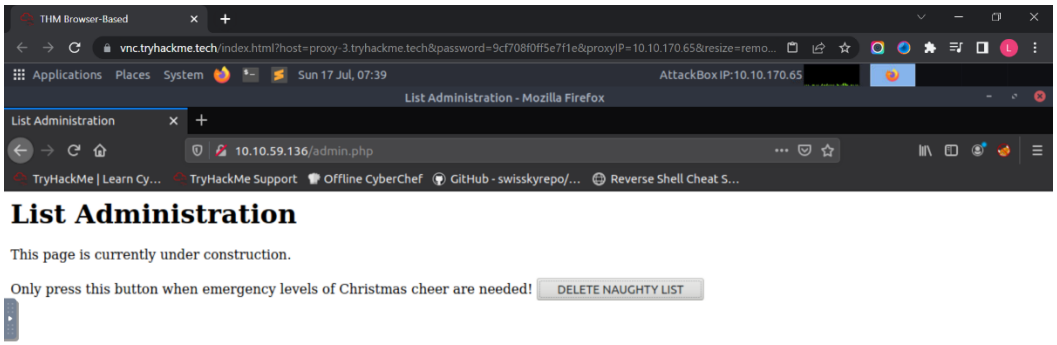


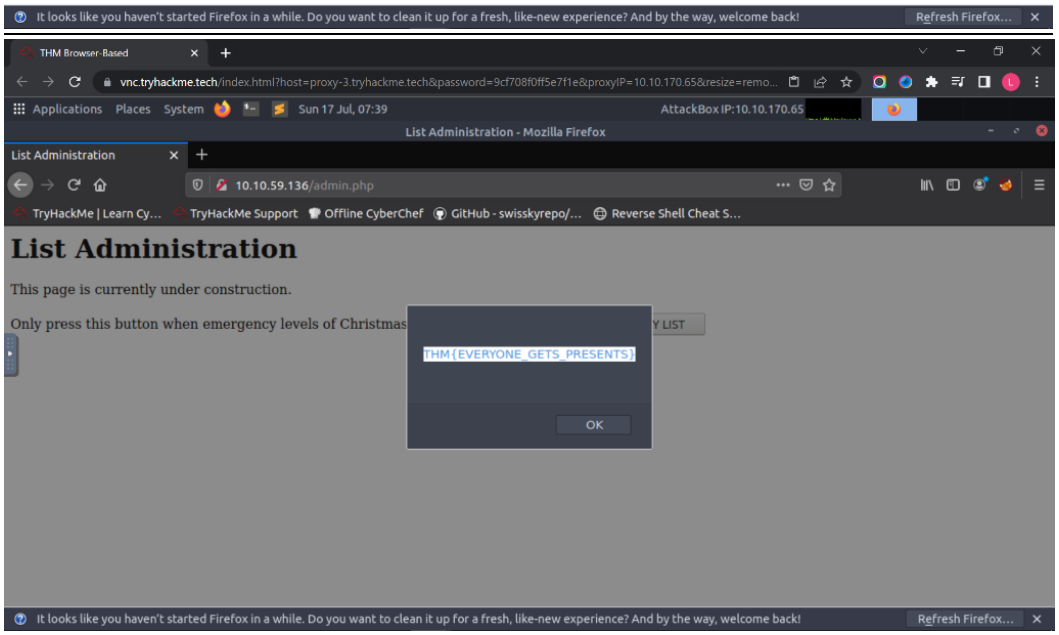


Question 7

First, we type the username “Santa” and the password “Be good for goodness sake!” to access to the next webpage. We will see the List Administration which mentions “This page is currently under construction.” . After that, we click on the button “DELETE NAUGHTY LIST” and get the flag.


THM Browser-Based
vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=9cf708f0ff5e7f1e&proxyIP=10.10.170.65&resize=remo...
Applications Places System Sun 17 Jul, 07:38
AttackBox IP:10.10.170.65
The Naughty or Nice List - Mozilla Firefox
The Naughty or Nice List
10.10.59.136/?proxy=http%3A%2F%2Flist.hohoho.localtest.me
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...
The List
Admin
Admin
Username: Santa
Password:
Login
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...


THM Browser-Based
vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=9cf708f0ff5e7f1e&proxyIP=10.10.170.65&resize=remo...
Applications Places System Sun 17 Jul, 07:39
AttackBox IP:10.10.170.65
List Administration - Mozilla Firefox
List Administration
10.10.59.136/admin.php
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...
List Administration
This page is currently under construction.
Only press this button when emergency levels of Christmas cheer are needed!
DELETE NAUGHTY LIST


It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...
THM Browser-Based
vnc.tryhackme.tech/index.html?host=proxy-3.tryhackme.tech&password=9cf708f0ff5e7f1e&proxyIP=10.10.170.65&resize=remo...
Applications Places System Sun 17 Jul, 07:39
AttackBox IP:10.10.170.65
List Administration - Mozilla Firefox
List Administration
10.10.59.136/admin.php
TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef GitHub - swisskyrepo/... Reverse Shell Cheat S...
List Administration
This page is currently under construction.
Only press this button when emergency levels of Christmas
Y LIST
THM{EVERYONE_GETS_PRESENTS}
OK
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!
Refresh Firefox...

Thought Process/Methodology:

Frist, we access to URL “http://IP address”. Next, we need to prove that the address is the same 127.0.0.1 by using the terminal. We type “host localtest.me”, “host leong.localtest.me” and “host anything.localtest.me” to make sure all of the output is the same address 127.0.0.1. Besides, we add “/?proxy=http%3A%2F%2Flist.hohoho.localtest.me" behind the “http://IP address” and get the password of Santa. First, we type the username “Santa” and the password “Be good for goodness sake!” to access to the next webpage. We will see the List Administration which mentions “This page is currently under construction.” . Lastly, we click on the button “DELETE NAUGHTY LIST” and get the flag.

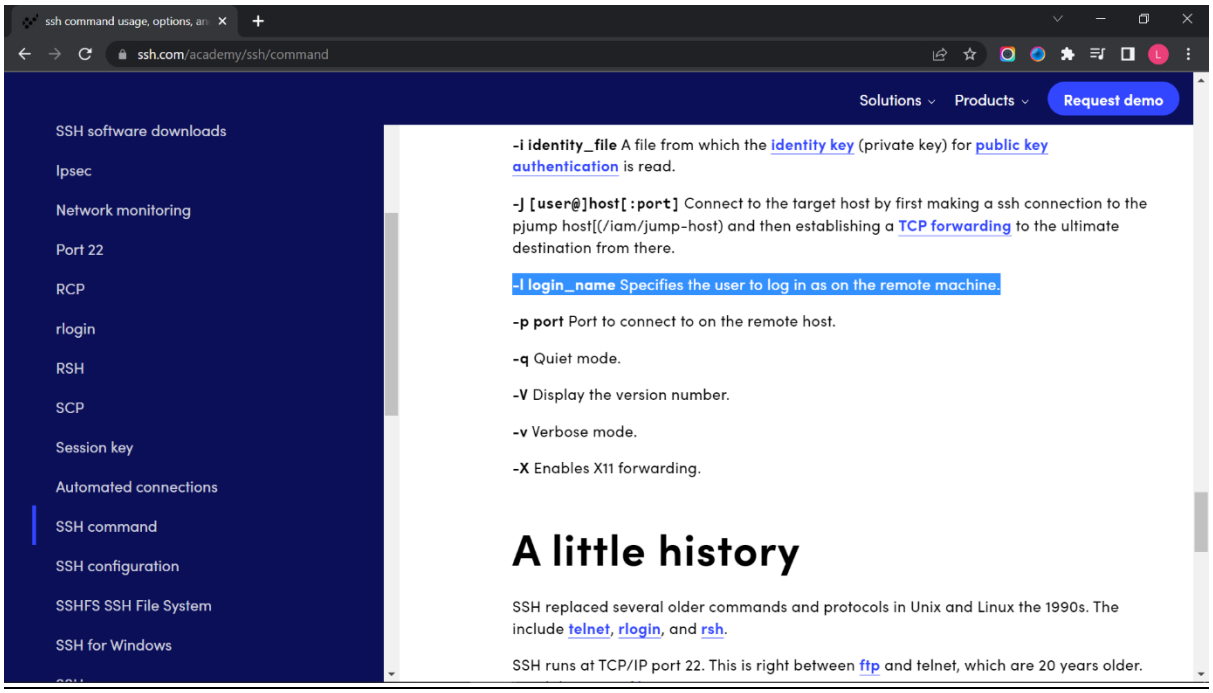
Day 20: Blue Teaming - PowershELlF to the rescue

Tools used: Terminal and PowerShell

Solution/walkthrough:

Question 1

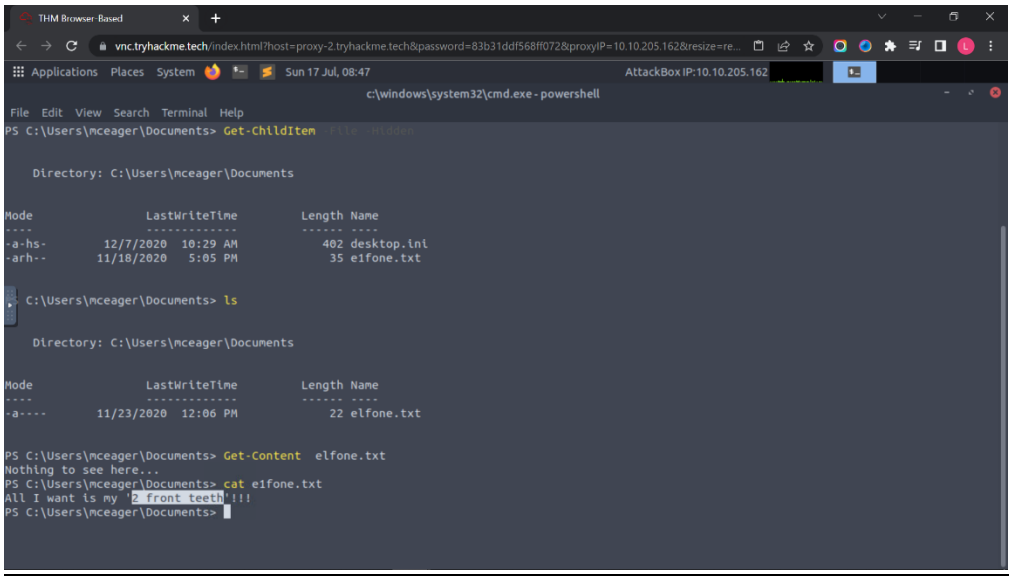
The parameter -l is used for the login name.



Question 2

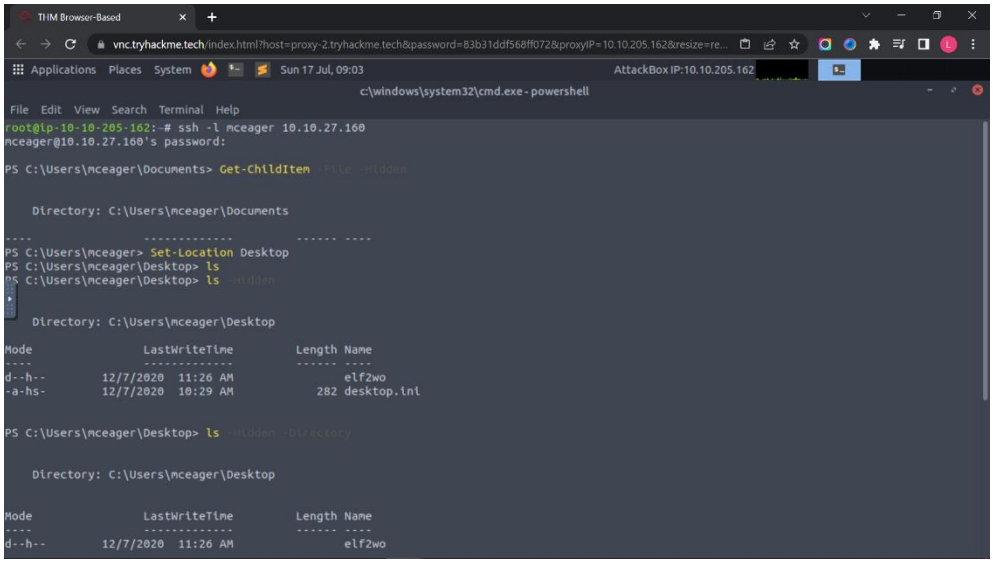
First, we type “ssh -l mceager IP address” and the password “r0ckStar!” in the terminal. Next, we type the command “cd Documents” and we are in the documents file. We type the command “Get-ChildItem -File -Hidden” to find all the files and hidden items and type the command “ls” to find out those files which are not hidden. We type the command “Get-Content elfone.txt” to check whatever

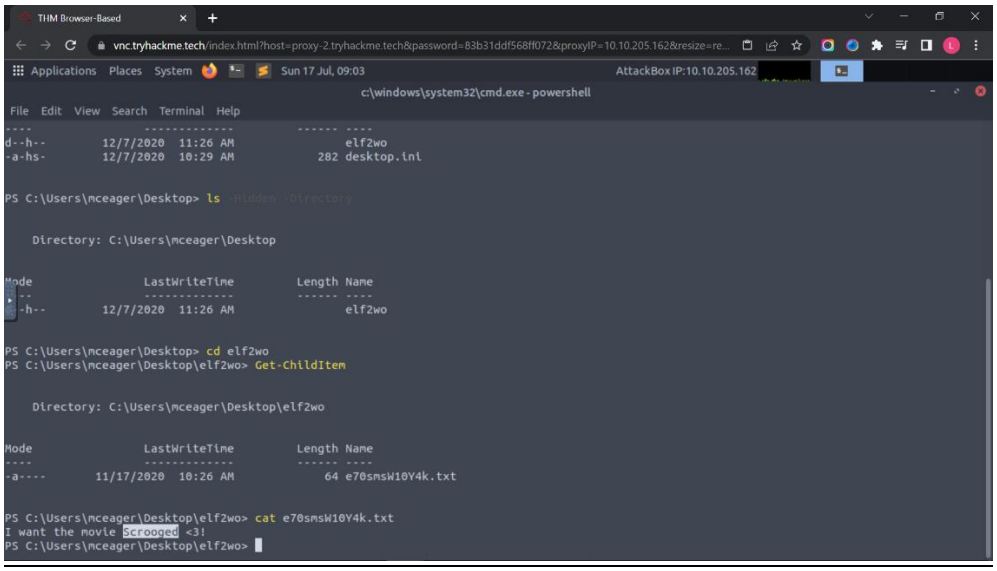
got anything inside “elfone.txt”. Lastly, we type the command “cat e1fone.txt” from the hidden file and we will get the content from Elf 1.



Question 3

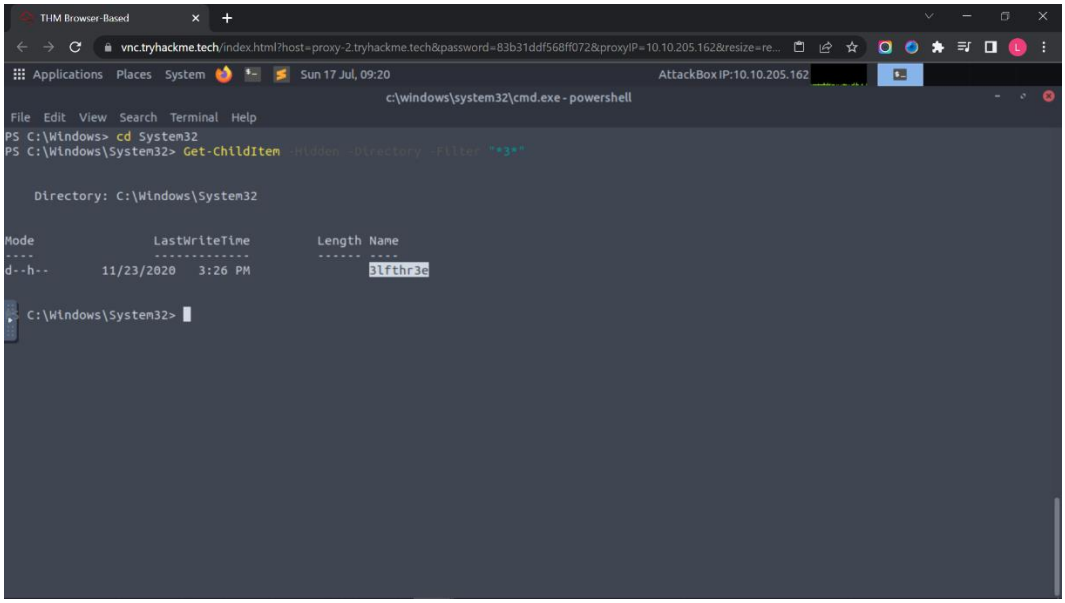
First, we need to change the file to Desktop by using the command “cd ..” and “Set-Location Desktop”. Next, we type the command “ls -Hidden -Directory” to find out the directory of the hidden items. We need to get in the file “elf2wo” by using the command “cd elf2wo” and use comment “Get-ChildItem” to list out the file inside “elf2wo” which is “e70smsW10Y4K.txt”. Lastly, we use the command “cat e70smsW10Y4K.txt” to get the content from this file.





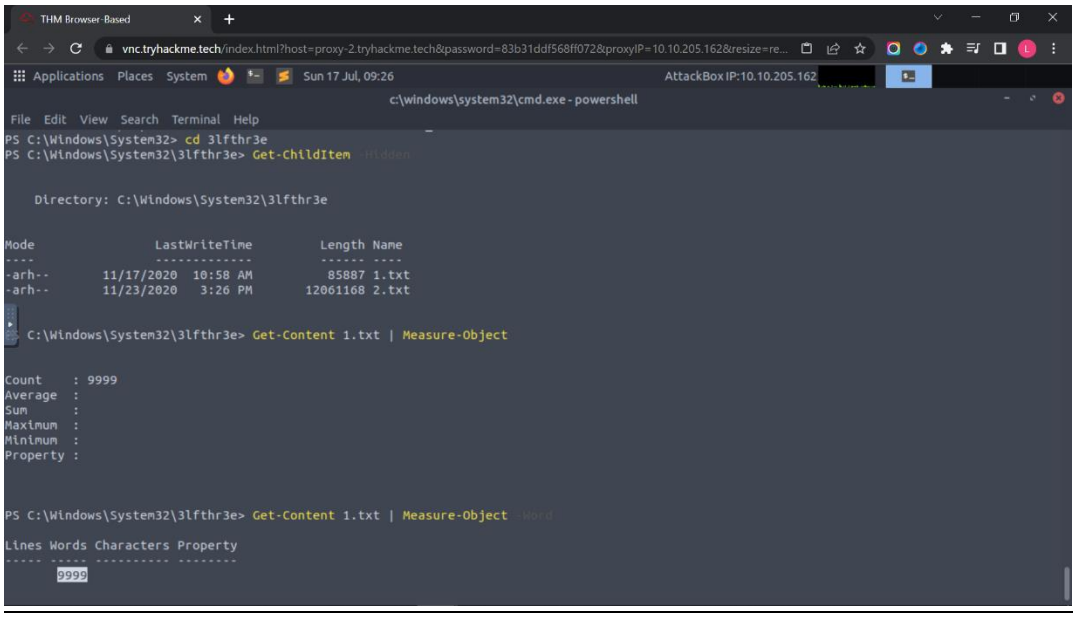
Question 4

First, we need to back to Windows and get to the files name “System32” by using the command “cd Windows” and “cd System32”. Lastly, we type the command “Get-ChildItem -Hidden -Directory -Filter “*3*”” to get the directory of the hidden item named with only the integer 3.



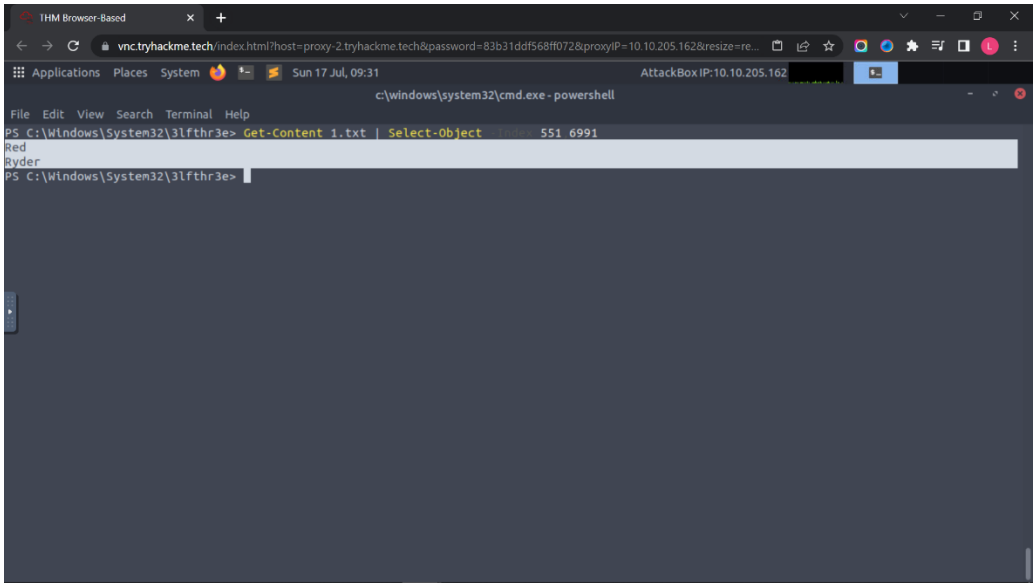
Question 5

First, we need to find the hidden item in “3lfthr3e” by using the command “Get-ChildItem -Hidden”. Next, we type the command “Get-Content 1.txt | Measure-Object” to know the words that the first file contain.



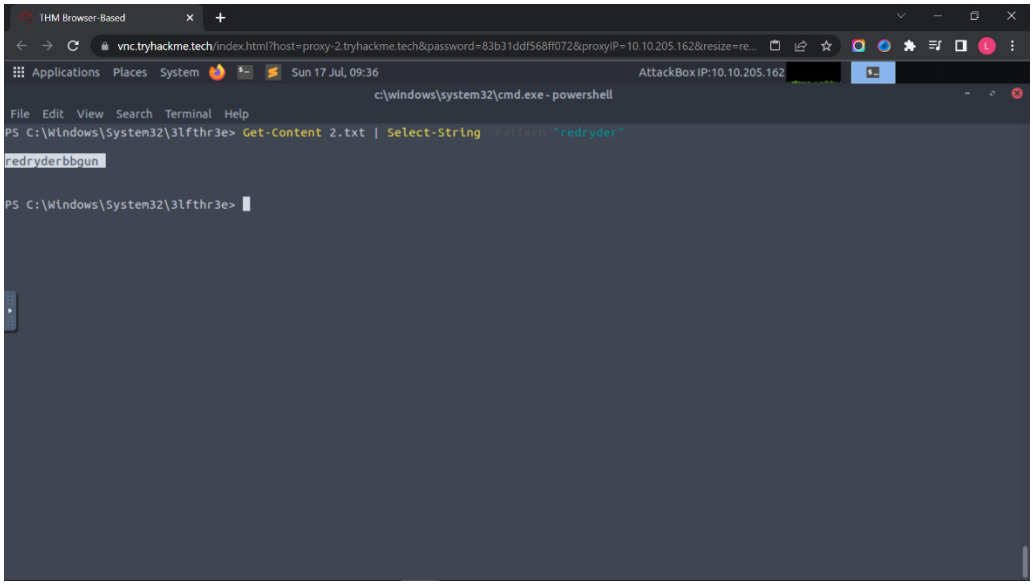
Question 6

We type the command “Get-Content 1.txt | Select-Object -Index 551,6991” to find out the two words in the index 551 and 6991 in the first file.



Question 7

We use the command “Get-Content 2.txt | Select-String -Pattern “redryder” to get the full answer in the second file.



Thought Process/Methodology:

Firstly, we type “ssh -l mceager IP address” and the password “r0ckStar!” in the terminal. Next, we type the command “cd Documents” and we are in the documents file. We type the command “Get-ChildItem -File -Hidden” to find all the files and hidden items and type the command “ls” to find out those files which are not hidden. We type the command “Get-Content elfone.txt” to check whatever got anything inside “elfone.txt”. To conclude, we type the command “cat e1fone.txt” from the hidden file and we will get the content from Elf 1. Secondly, we need to change the file to Desktop by using the command “cd ..” and “Set-Location Desktop”. Next, we type the command “ls -Hidden -Directory” to find out the directory of the hidden items. We need to get in the file “elf2wo” by using the command “cd elf2wo” and use comment “Get-ChildItem” to list out the file inside “elf2wo”

which is “e70smsW10Y4K.txt”. In a nutshell, we use the command “cat e70smsW10Y4K.txt” to get the content from this file. Thirdly, we need to back to Windows and get to the files name “System32” by using the command “cd Windows” and “cd System32”. Lastly, we type the command “Get-ChildItem -Hidden -Directory -Filter “*3*”” to get the directory of the hidden item named with only the integer 3. After that, we need to find the hidden item in “3lfthr3e” by using the command “Get-ChildItem -Hidden”. Next, we type the command “Get-Content 1.txt | Measure-Object” to know the words that the first file contain. We type the command “Get-Content 1.txt | Select-Object -Index 551,6991” to find out the two words in the index 551 and 6991 in the first file for question 6. We use the command “Get-Content 2.txt | Select-String -Pattern “redryder” to get the full answer in the second file for question 7.