

PSP0201

WEEK 5

WRITEUP

Group Name: Draco Malfoy

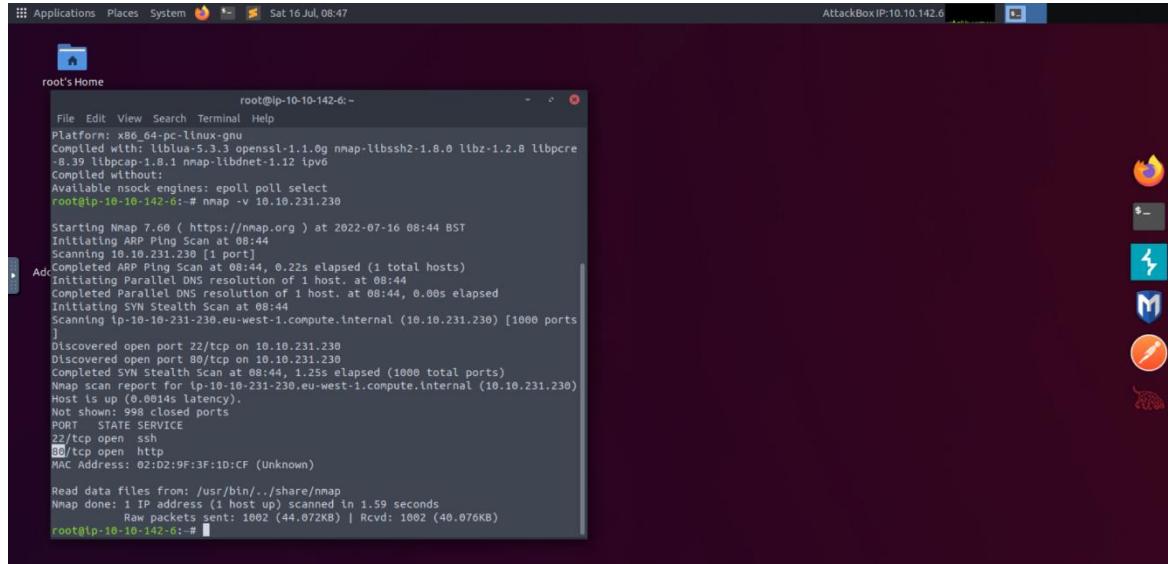
Aqra Alisa binti Rashidi	1211103093
Nurul Aqilah binti Mohd Shariff	1211103097
Nur Inqsyira binti Zamri	1211103098
Siti Nur Amirah binti Zuraihan	1211102093

Day 16: Help! Where is Santa?

Tools: firefox, nmap python3, requests, sublime text

Q1: What is the port number for the web server?

=80

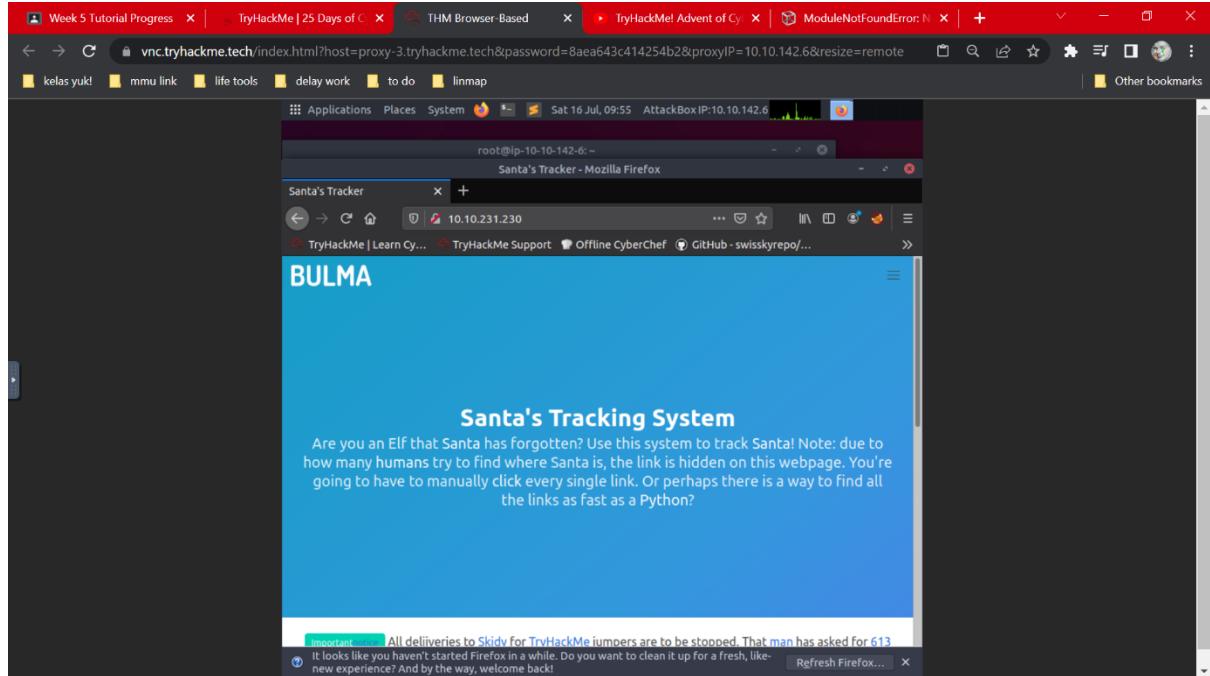


```
root@ip-10-10-142-6:~$ nmap -v -A 10.10.231.230
Starting Nmap 7.60 ( https://nmap.org ) at 2022-07-16 08:44 BST
Initiating ARP Ping Scan at 08:44
Scanning 10.10.231.230 [1 port]
Completed ARP Ping Scan at 08:44, 0.225 elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:44
Completed Parallel DNS resolution of 1 host. at 08:44, 0.005 elapsed
Initiating SYN Stealth Scan at 08:44
Scanning 10.10.231.230.eu-west-1.compute.internal (10.10.231.230) [1000 ports]
Discovered open port 22/tcp on 10.10.231.230
Discovered open port 80/tcp on 10.10.231.230
Completed SYN Stealth Scan at 08:44, 1.25s elapsed (1000 total ports)
Nmap scan report for 10.10.231.230.eu-west-1.compute.internal (10.10.231.230)
Host is up (0.014s latency).
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
MAC Address: 02:D2:9F:3F:D:CF (Unknown)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds
Raw packets sent: 1002 (44.072KB) | Rcvd: 1002 (40.076KB)
```

Q2: What templates are being used?

=BULMA

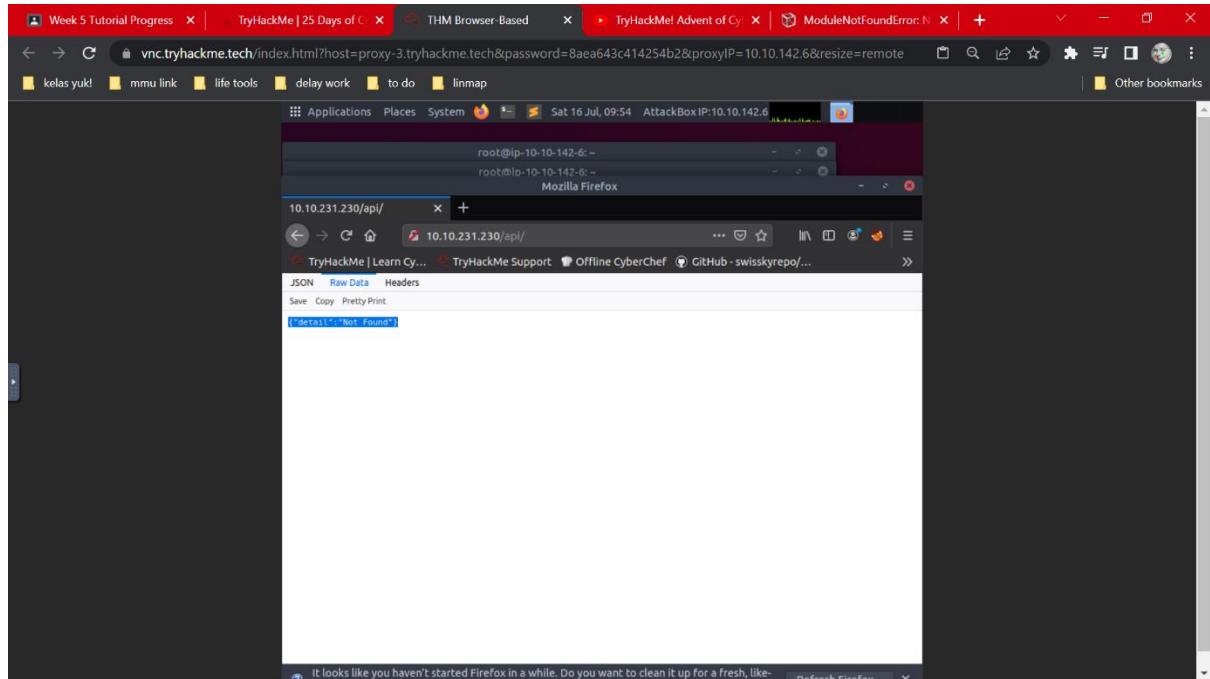


Q3: Without using enumerations tools such as Dirbuster, what is the directory for the API? (without the API key)

=/api/

Q4: Go the API endpoint. What is the Raw Data returned if no parameters are entered?

= {"detail": "Not Found"}



Q5: Where is Santa right now?

= { Winter Wonderland, Hyde Park, London }

Q6: Find out the correct API key. Remember, this is an odd number between 0-100

=57

```
root@ip-10-10-142-6:~\nroot@ip-10-10-142-6:~\n~/apibruter.py -- Sublime Text (UNREGISTERED)\nFile Edit Selection Find View Goto Tools Project Preferences Help\n< > untitled * | linkgrabber.py * | apibruter.py *\n1 #!/usr/bin/env python3\n2 # Import the libraries we downloaded earlier\n3 # If you try importing without installing them, this step will fail\n4\n5 import requests\n6\n7 for api_key in range(1,100,2):\n8     print(f"api key {api_key}\")\n9     htmlfile = requests.get(f"http://10.10.231.230:80/api/{api_key}\")\n10    print(htmlfile.text)\n\nLine 10; Column 25\nSpaces: 4 Python
```

```
root@ip-10-10-142-6:~\nroot@ip-10-10-142-6:~\nroot@ip-10-10-1... x root@ip-10-10-1... x root@ip-10-10-1... x root@ip-10-10-14...\napl_key 45\n  ("item_id":45,"q":"Error. Key not valid!")\napl_key 47\n  ("item_id":47,"q":"Error. Key not valid!")\napl_key 49\n  ("item_id":49,"q":"Error. Key not valid!")\napl_key 51\n  ("item_id":51,"q":"Error. Key not valid!")\napl_key 53\n  ("item_id":53,"q":"Error. Key not valid!")\napl_key 55\n  ("item_id":55,"q":"Error. Key not valid!")\napl_key 57\n  ("item_id":57,"q":"Winter Wonderland, Hyde Park, London.")\napl_key 59\n  ("item_id":59,"q":"Error. Key not valid!")\napl_key 61\n  ("item_id":61,"q":"Error. Key not valid!")\napl_key 63\n  ("item_id":63,"q":"Error. Key not valid!")\napl_key 65\n  ("item_id":65,"q":"Error. Key not valid!")\napl_key 67\n  ("item_id":67,"q":"Error. Key not valid!")\n\nLine 10; Column 25\nSpaces: 4 Python
```

Methodology (Day16):

To begin with, we scanned for available port using nmap. Turns out, it shows port: 80. We then continue browsing to the firefox and finds out BULMA as the template used. Next, we go to /api/ default and heads to raw tab to get the raw data. Moreover, we use python3 to find out the correct API key by creating apibruter.py file for the python code. Open the file using command “python3 our-file-name” and we now obtain the correct API key as well as the location of Santa.

Day 17: Reverse ELFneering

Tools: terminal, ssh radare2

Q1: Match the data type with the size in bytes

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

Q2: What is the command to analyse the program in radare2?

= aa

Q3: What is the command to set a breakpoint in radare2?

=db

Q4: What is the command to execute the program until we hit a breakpoint?

=dc

The screenshot shows a Linux desktop environment with a terminal window and a browser window.

Terminal Window:

```
root@ip-10-10-14-132:~# echo "10.10.221.103" > target.txt
root@ip-10-10-14-132:~# cat target.txt
10.10.221.103
root@ip-10-10-14-132:~# ssh elfmeager@10.10.221.103
The authenticity of host '10.10.221.103 (10.10.221.103)' can't be established.
ECDSA key fingerprint is SHA256:xrBux5o5owRkvvRdrSfE/9F5ccAZqlXahRhzB1dV7U.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.221.103' (EDSA) to the list of known hosts.
elfmeager@10.10.221.103's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-128-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

System information as of Tue Jul 5 01:47:44 UTC 2022

System load: 0.27      Processes:      99
Usage of /: 10.4% of 11.75GB   Users logged in: 0
Memory usage: 8%       IP address for ens5: 10.10.221.103
Swap usage: 0%         

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

Last login: Wed Dec 16 18:25:51 2020 from 192.168.190.1
elfmeager@tbfcc-day-17:~
```

Browser Window:

The browser window shows a TryHackMe challenge page for Day 17: Reverse ELFneering. The page content includes:

- Follow along with Darkstar747 and solve Day 17!
- 2. Introduction to x86-64 Assembly
- Computers execute machine code, which is encoded as bytes, to carry out tasks on a computer. Since different computers have different processors, the machine code executed on these computers is specific to the processor. In this case, we'll be looking at the Intel x86-64 instruction set architecture which is most commonly found today. Machine code is usually represented by a more readable form of the code called assembly code. This machine code is usually produced by a compiler, which takes the source code of a file, and after going through some intermediate stages, produces machine code that can be executed by a computer.
- Without going into too much detail, Intel first started out by building a 16-bit instruction set, followed by 32 bit, after which they finally created 64 bit. All these instruction sets have been created for backward compatibility, so code compiled for 32-bit machines will run on 64-bit machines. As mentioned earlier, before an executable file is produced, the source code is first compiled into assembly (.s files), after which the assembler converts it into an object program (.o files), and operations with a linker finally make it an executable.
- The best way to actually start explaining assembly is by diving in. We'll be using radare2 to do this - radare2 is a framework for reverse engineering and analysing binaries. It can be used to disassemble binaries/translate machine code to assembly, which is actually readable) and debug said binaries(by allowing a user to step through the execution and view the state of the program).
- Luckily for us, everything we need has been provided to you via an instance that you can deploy and log into:

 1. Press the "Deploy" button on the top-right of this task
 2. Wait for the IP address of the target instance to display
 3. Log into your instance using the following information:

IP Address: 10.10.221.103
Username: elfmeager
Password: adventofcyber

- Let's proceed to run through how Radare2 works exactly. Although you shouldn't do this if the program is unknown, it is safe for us to execute to see what should be happening like so:

```
ashu@ashu-Inspiron-5379 ~$ ./file1
the value of a is 4. the value of b is 5 and the value of c is 9.
```

The image shows a Windows desktop environment with three main windows:

- Top Left Browser Tab:** "TryHackMe | 25 Days of Cyber Security" - A challenge page for task r2_cupdf. It contains instructions and a form to enter IP address, username, and password. Below the form is a terminal window showing the output of running the binary with ./file1.
- Bottom Left Browser Tab:** "tryhackme.com/room/learnbyern35days" - A challenge page for task r2_cupdf. It contains instructions and a form to enter IP address, username, and password. Below the form is a terminal window showing the output of running the binary with ./file1.
- Right Terminal Window:** A Linux terminal session on an AttackBox (IP: 10.10.14.132) as root user. The terminal shows the user connecting to the target host (IP: 10.10.221.103) and performing various system checks and updates.

Q5: What is the value of local_ch when its corresponding movl instruction is called (first if multiple)?

= 1

Q6: What is the value of eax when the imull instruction is called?

=6

Q7: What is the value of local_4h before eax is set to 0?

=6

The screenshot shows a Linux desktop environment with two terminal windows and a file browser. The terminal windows are running on an AttackBox IP: 10.10.14.132. The file browser shows a directory structure under 'root's Home'.

Terminal 1:

```
hit breakpoint at: 400b55
[0x00400b55]> pdf
... main:
... fax:
(gdb) sys main 68
$0x00400b54 int argc, char **argv, char **envp;
$0x00400b55 ; var int local_ch @ rbp-0xc
$0x00400b56 ; var int local_8h @ rbp-0x8
$0x00400b57 ; var int local_4h @ rbp-0x4
$0x00400b58 DATA WORD From encryp (0x410000)
$0x00400b59    55      pushq %rbp
$0x00400b5a    4889e5  movq %rsp, %rbp
$0x00400b5b    4883ec10 subq $0x10, %rsp
```

Terminal 2:

```
elfmeager@tbfc-day-17:~
```

File Browser:

- root's Home
- bin
- tmp
- var
- Tools
- Additional

The terminal windows show assembly code for the 'main' function, with specific instructions highlighted in blue. The assembly code includes pushes, moves, and loads from memory locations. The file browser shows a standard Linux file structure.

Methodology (Day17):

First, we login using ssh with the information provided. We then get the list of programme using ls command. Then, we analyse the programme (challenge1) using aa command. Next,

we are using pdf@main command to examine the assembly code at main. After that, we are supposed to get the answer for the rest of question by reading the current assembly code.

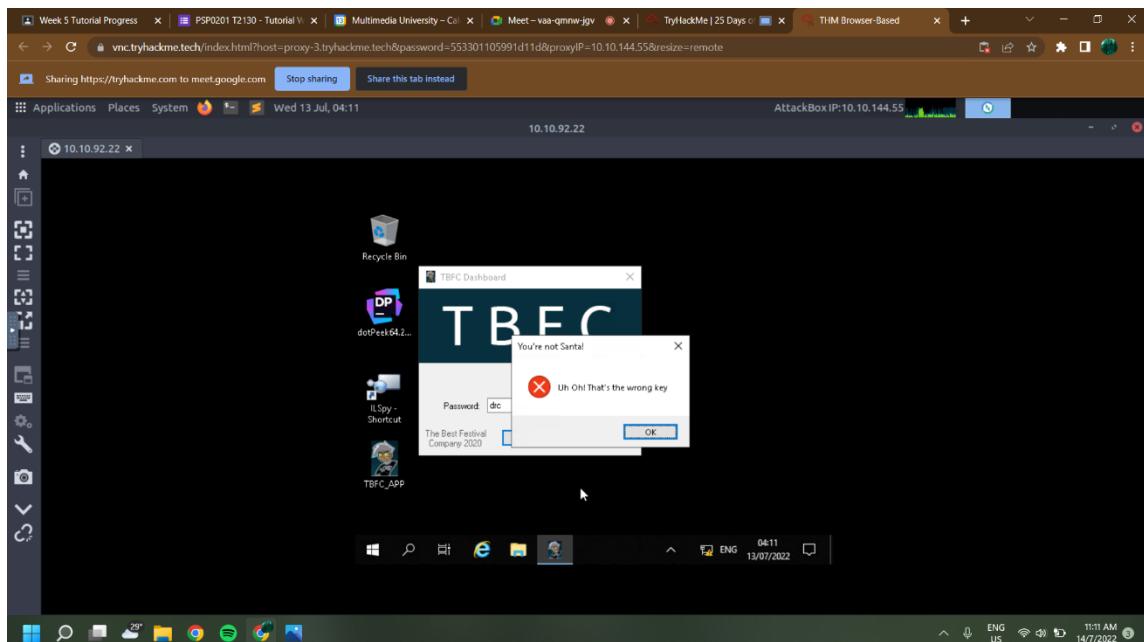
DAY 18: [Reverse Engineering] The Bits of Christmas

Tools: Attackbox

Question 1

Q1: What is the message that shows up if you enter the wrong password for TBFC_APP?

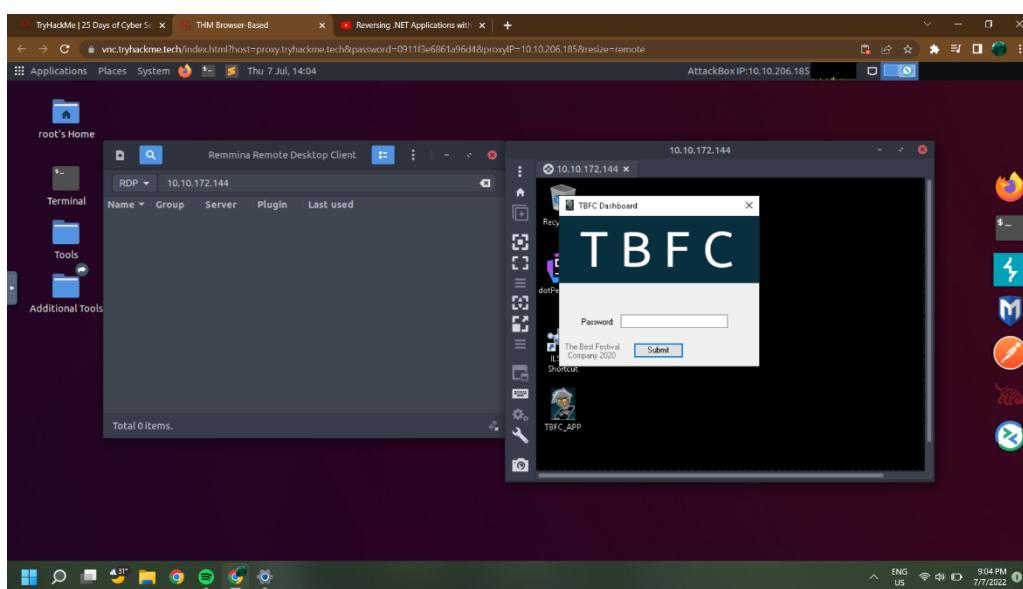
= Uh Oh! That's the wrong key



Question 2

Q2: What does TBFC stand for?

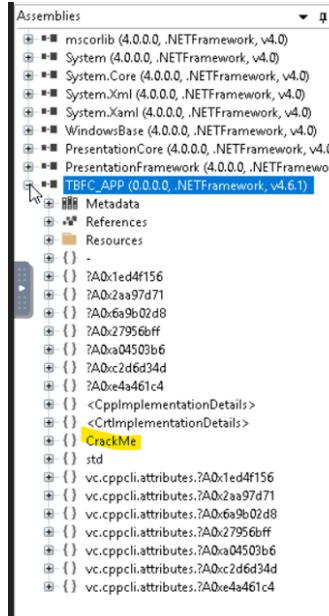
= The Best Festival Company



Question 3

Q3: Decompile the TBFC_APP with ILSpy. What is the module that catches your attention?

=CrackMe



Question 4

Q4: Within the module, there are two forms. Which contains the information we are looking for?

=MainForm

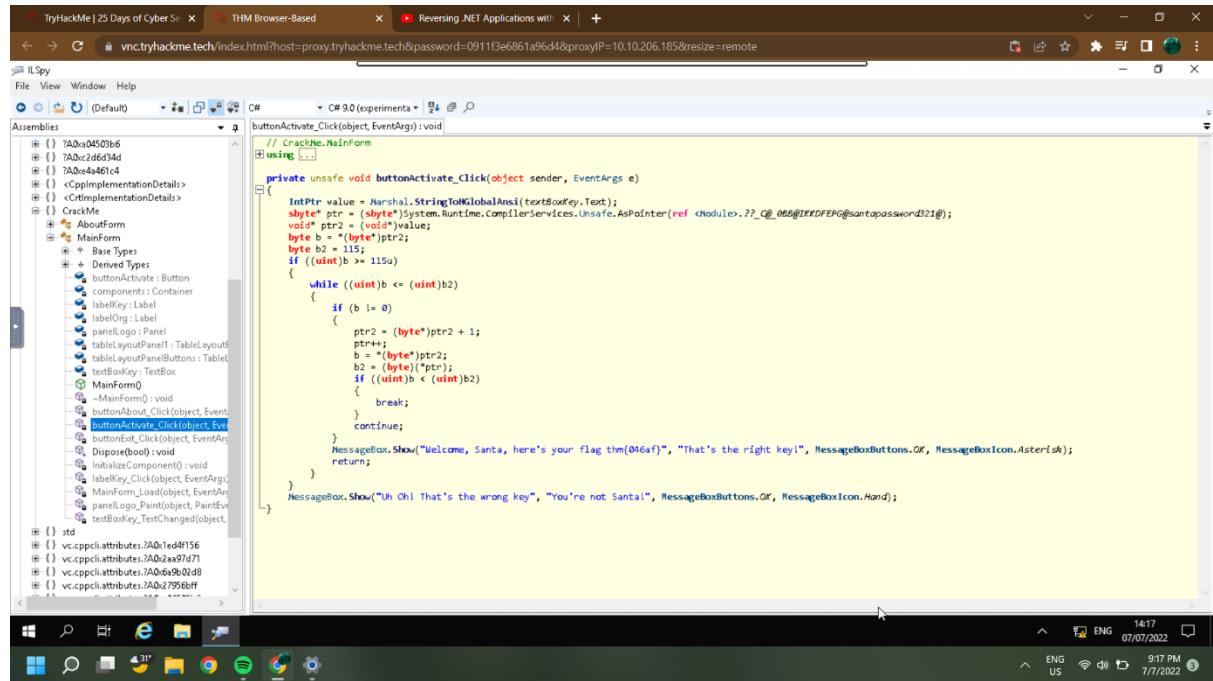
```
// CrackMe.MainForm
private unsafe void buttonActivate_Click(object sender, EventArgs e)
{
    IntPtr value = Marshal.StringToGlobalAnsi(textBoxKey.Text);
    byte* ptr = (byte*)System.Runtime.CompilerServices.Unsafe.AsPointer(ref Module.$__C@_0B@IKDFEP@ santapassword21@);
    byte b = *(byte*)ptr2;
    byte b2 = *(byte*)ptr;
    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 tlm(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);
    }
}
```

The screenshot shows the ILSpy interface with the decompiled code of the 'buttonActivate_Click' method in the 'MainForm' class. The code uses unsafe pointers to interact with a global variable and shows a MessageBox call. The assembly browser on the left shows the structure of the 'MainForm' class, which contains components like 'MainForm', 'MainForm0', and various UI controls.

Question 5

Q5: Which method within the form from Q4 will contain the information we are seeking?

= buttonActivate_Click



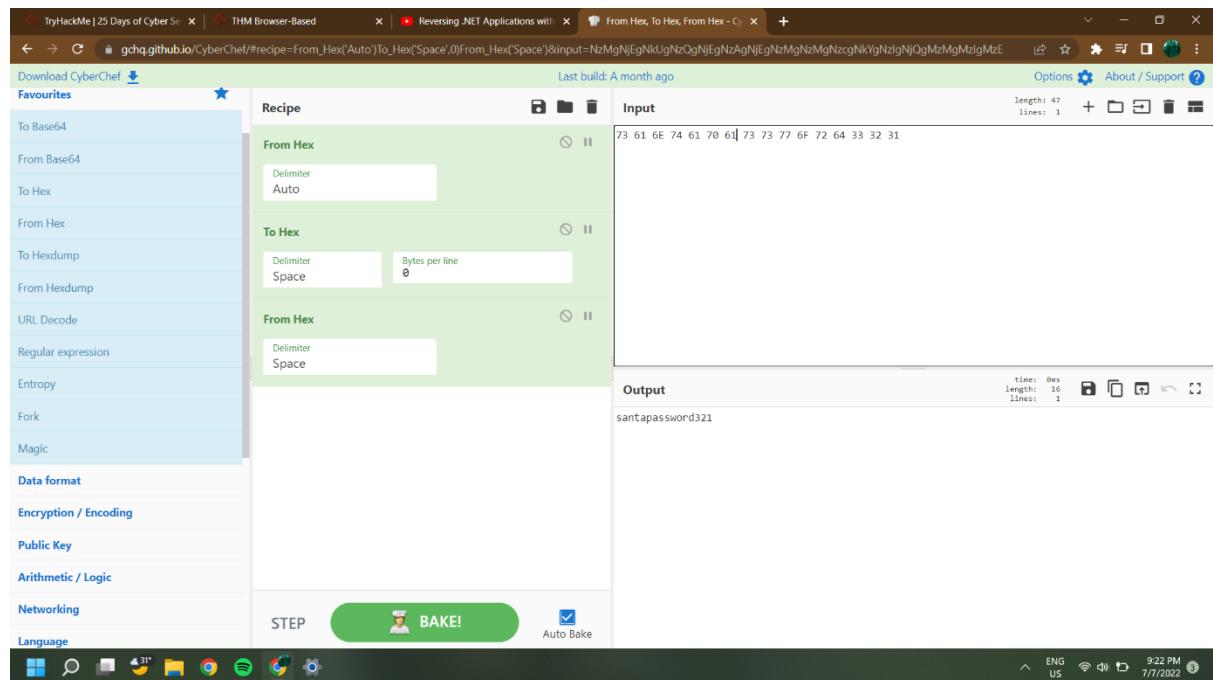
The screenshot shows the IL Spy interface with the assembly code for the buttonActivate_Click event handler. The code is written in C# and contains a unsafe block. It uses pointer arithmetic to manipulate memory at address 0x0000000000401000. The assembly code is as follows:

```
// CrackMe.MainForm
private unsafe void buttonActivate_Click(object sender, EventArgs e)
{
    IntPtr value = Marshal.StringToGlobalAnsi(textBoxKey.Text);
    byte* ptr = (byte*)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)
                {
                    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

Q6: What is Santa's password?

=santapassword321



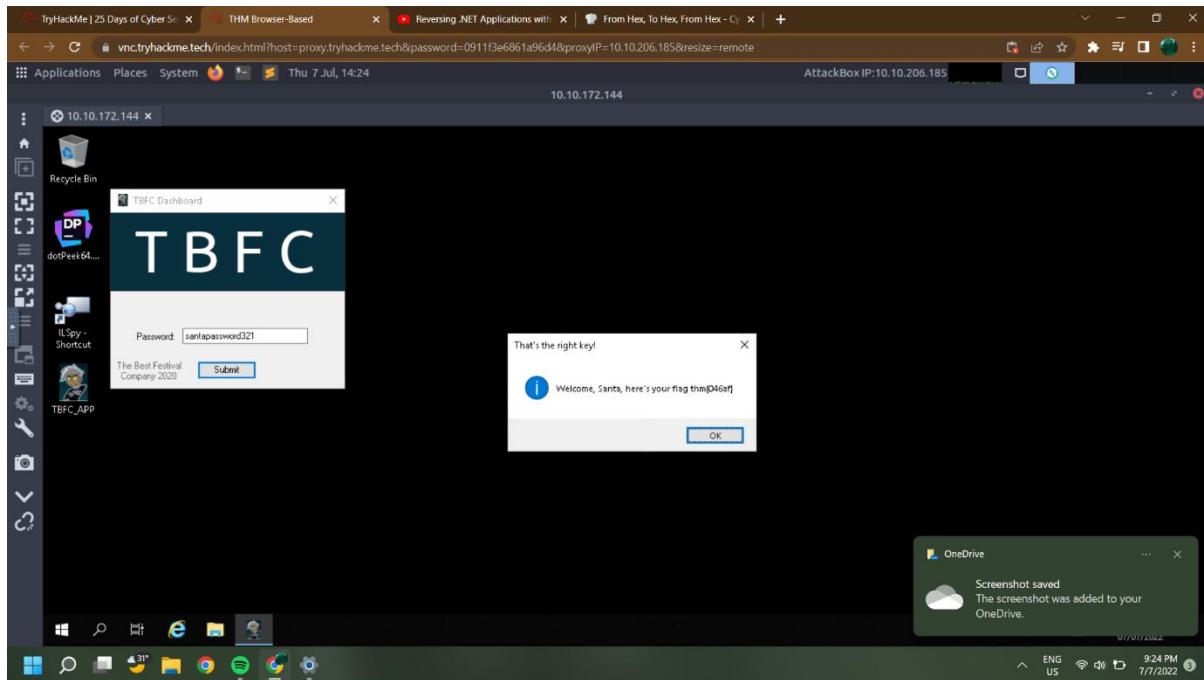
The screenshot shows the CyberChef interface with the following configuration:

- From Hex:** Delimiter: Auto, Input: 73 61 6E 74 61 70 61 73 73 77 6F 72 64 33 32 31
- To Hex:** Delimiter: Space, Bytes per line: 0
- From Hex:** Delimiter: Space
- Output:** santapassword321

Question 7

Q7: Now that you've retrieved this password, try to login...What is the flag?

= thm{046af}



Methodology (Day 18):

First and foremost, we deploy our machine and the respective AttackBox. Next, we navigate to the "Applications" tab on the AttackBox where "Remmina" is located in the "Internet" sub-menu. Remmina asked for a password to save sessions, we safely press "Cancel". Now we filled the IP address of the target Instance that we have deployed, input the Username and password provided and set the "Color depth" to "RemoteFX (32 bpp).

Username: cmnatic

Password: Adventofcyber!

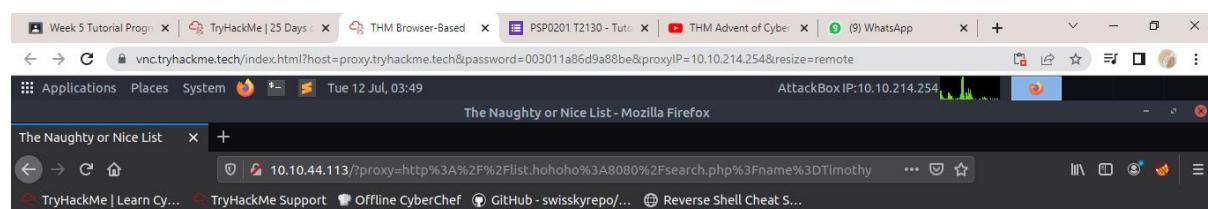
Subsequently, we open the TBFC App and tried to log in but failed. So we navigate to the ILSpy to do some hacking. We open the "TBFC_APP" application in ILspy and begin decompiling the code. In there, we successfully received the needed password and flag.

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

Tools : Firefox

Question 1:

Q1: Which list is this person on?



The Naughty or Nice List

Welcome children!

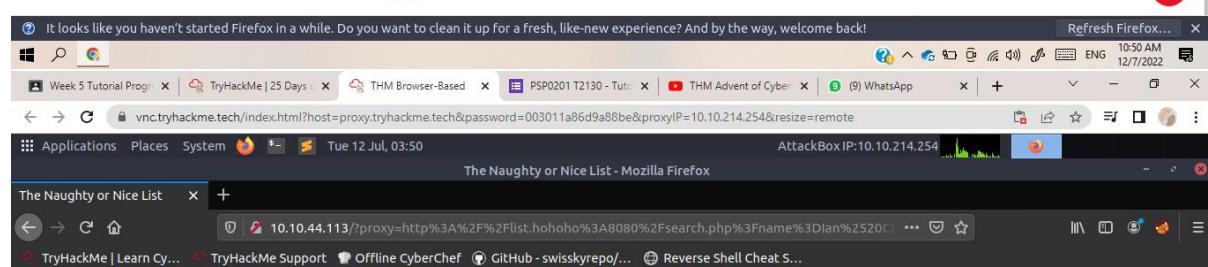
To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name: Search

Timothy is on the Naughty List.



The Naughty or Nice List

Welcome children!

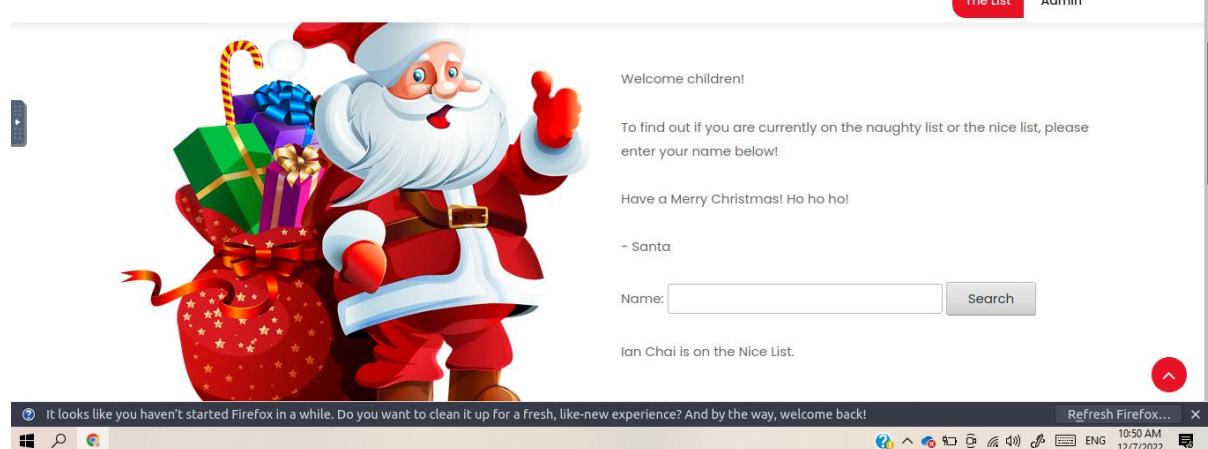
To find out if you are currently on the naughty list or the nice list, please enter your name below!

Have a Merry Christmas! Ho ho ho!

- Santa

Name: Search

Ian Chai is on the Nice List.



The Naughty or Nice 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

Ian Chai is on the Nice List.

The Naughty or Nice List - Mozilla Firefox

AttackBox IP:10.10.214.254

10.10.44.113/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DKanes

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

Kanes is on the 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!

The Naughty or Nice List - Mozilla Firefox

AttackBox IP:10.10.214.254

10.10.44.113/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DYP

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

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!

The Naughty or Nice List - Mozilla Firefox

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

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!

The Naughty or Nice List - Mozilla Firefox

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

JJ is on the 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!

The Naughty or Nice List - Mozilla Firefox

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

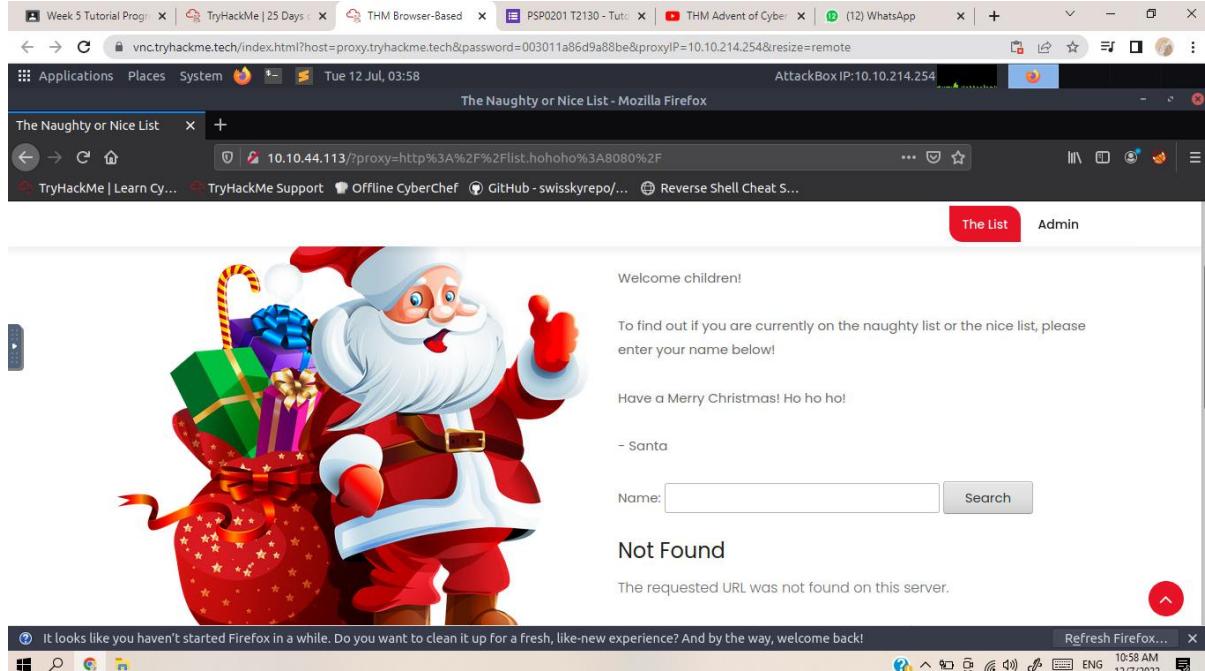
Name: Search

JJ is on the Naughty List.

Question 2:

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

= The requested URL was not found on this server.



The Naughty or Nice List - Mozilla Firefox

AttackBox IP:10.10.214.254

10.10.44.113/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F

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

Not Found

The requested URL was not found on this server.

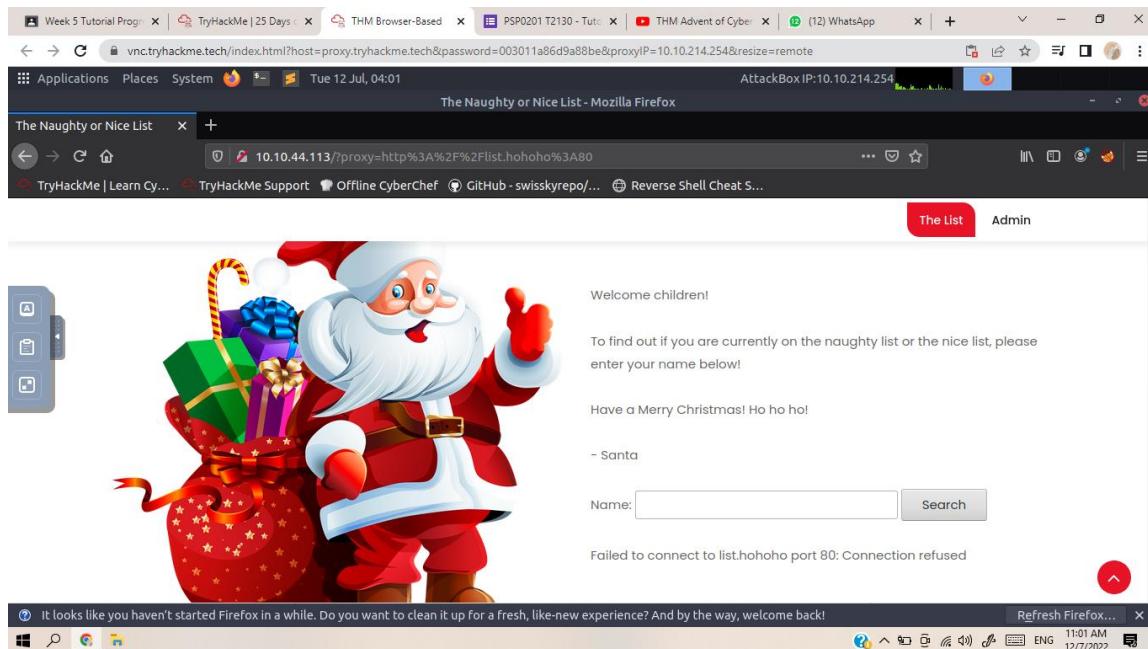
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox... 10:58 AM 12/7/2022

Question 3:

Q3: What is displayed on the page when you use
"/?proxy=http%3A%2F%2Flist.hohoho%3A80"?

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



The Naughty or Nice List - Mozilla Firefox

AttackBox IP:10.10.214.254

10.10.44.113/?proxy=http%3A%2F%2Flist.hohoho%3A80

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

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

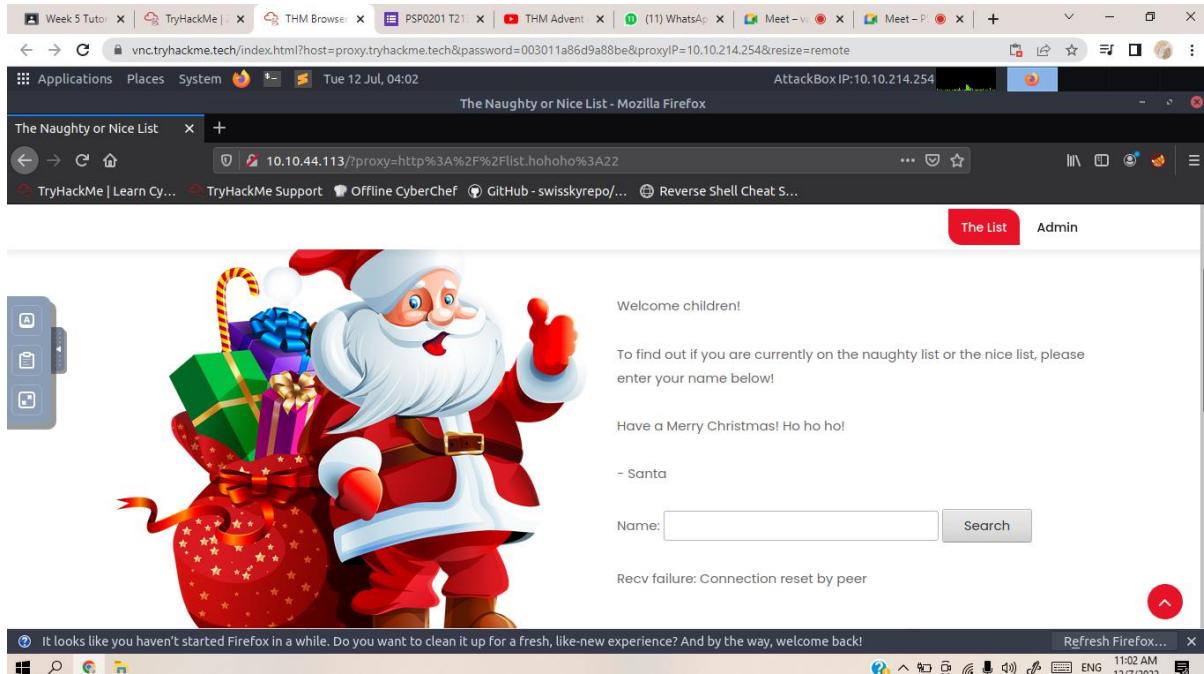
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox... 11:01 AM 12/7/2022

Question 4 :

Q4: What is displayed on the page when you use
"/?proxy=http%3A%2F%2Flist.hohoho%3A22"?

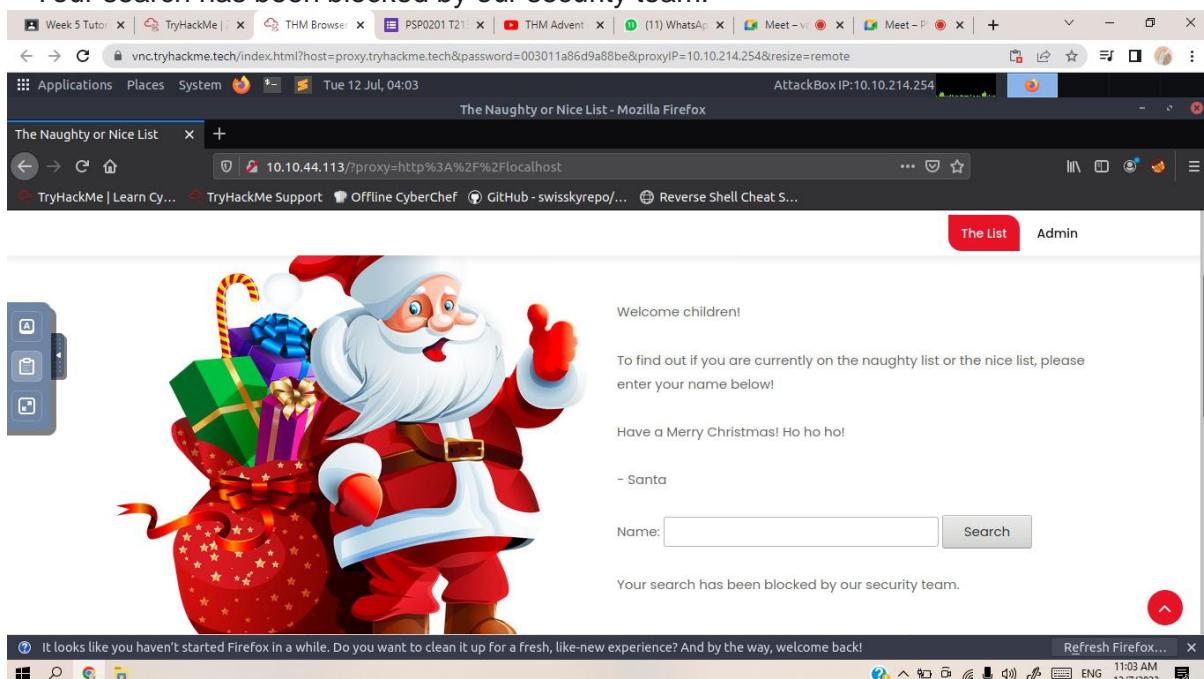
= Recv failure: Connection reset by peer



Question 5 :

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

= Your search has been blocked by our security team.



Question 6 : What is Santa's password?

Q6: Be good for goodness sake!

The Naughty or Nice List

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

AttackBox IP:10.10.214.254

Question 7 : What is the challenge flag?

Q7: THM{EVERYONE_GETS_PRESENTS}

List Administration

This page is currently under construction.

Only press this button when emergency levels of Christmas cheer

THM{EVERYONE_GETS_PRESENTS}

OK

AttackBox IP:10.10.214.254

Methodology: (Day 19)

First, we deploy our machine and attackbox. We started the progress by inserted IP address and we were shown The Naughty or Nice List page. We search which list is Timothy, Ian Chai, Kanes, YP, Tib3rius and JJ on. Then, we insert the URL given to look up what displayed on pages. After that, we try localtest.me to find out admin password and log in. We have to delete the naughty list to get the challenge flag.

Day 20: Powershell to rescue

Tools: terminal, ssh

Question 1

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

= login name

Question 2

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

= 2 front teeth

The screenshot shows a Windows desktop environment. On the left, there is a browser window titled 'TryHackMe | 25 Days of Cyber S...' displaying the URL 'tryHackMe.com/room/learnCyberIn25Days'. On the right, there is a terminal window titled 'c:\windows\system32\cmd.exe - powershell'. The terminal session shows the following commands and output:

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

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

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

Below the terminal window, the taskbar shows the file 'r2.pdf' and the system tray indicates the date and time as '05/07/2022 11:18 AM'.

The original explanation of PowerShell is: "PowerShell is a cross-platform task automation and configuration management framework, consisting of a command-line shell and scripting language. Unlike most shells, which accept and return text, PowerShell is built on top of the .NET Common Language Runtime (CLR), and accepts and returns .NET objects. This fundamental change brings entirely new tools and methods for automation."

PowerShell has grown in popularity in the last few years among defenders and especially attackers. Knowing PowerShell is a necessary skill. If you have only heard of PowerShell but never dabbled with it, fret not, today you will.

Recall from the definition above that PowerShell is a command-line shell. We must enter commands into the command prompt to instruct PowerShell on what we want it to do for us. PowerShell commands are known as cmdlets.

To list the contents of the current directory we are in, we can use the `Get-ChildItem` cmdlet. There are various other options we can use with this cmdlet to enhance its capabilities further.

- `-Path` Specifies a path to one or more locations. Wildcards are accepted.
- `-File / -Directory` To get a list of files, use the File parameter. To get a list of directories, use the Directory parameter. You can use the Recurse parameter with File and/or Directory parameters.
- `-Filter` Specifies a filter to qualify the Path parameter.
- `-Recurse` Gets the items in the specified locations and in all child items of the locations.
- `-Hidden` To get only hidden items, use the Hidden parameter.
- `-ErrorAction SilentlyContinue` Specifies what action to take if the command encounters an error.

For example, if you want to view all of the hidden files in the current directory you are in, you can issue the following command:

```
Get-ChildItem -File -Hidden -ErrorAction SilentlyContinue
```

Another useful cmdlet is `Get-Content`. This will allow you to read the contents of a file.

You can run this command as follows:

```
Get-Content -Path file.txt
```

You can run numerous operations with the `Get-Content` cmdlet to give you more information about the particular file you are inspecting. Such as how many words are in the file and the exact positions for a particular string within a file.

To get the number of words contained within a file, you can use the `Get-Content` cmdlet and pipe the results to the `Measure-Object` cmdlet.

```
You run this command as follows: Get-Content -Path file.txt | Measure-Object -Word
```

To get the exact position of a string within a file, you can use the following command:

```
PS C:\Users\ncearer> Get-Content -Path file.txt | Select-String -Pattern "front teeth"
```

The screenshot shows a Windows terminal window titled "THM AttackBox" running on "Tue 5 Jul, 04:20". It displays the output of several PowerShell commands. The first command is `c:\windows\system32\cmd.exe -powershell`, followed by `Set-Location .\Documents` and `Get-ChildItem` with parameters `-File -Hidden -ErrorAction SilentlyContinue`. The output shows a list of files in the `\Documents` folder. The second part of the screenshot shows the output of `Get-Content efone.txt`, which contains the text "I want to see my front teeth!!!". The third part shows the directory listing for `C:\Users\ncearer`, which includes standard system folders like Desktop, Downloads, Pictures, and Videos.

Question 3

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?

=Scrooged

The official expansion of PowerShell is: PowerShell is a cross-platform task automation and configuration management framework, consisting of a command-line shell and scripting language. Unlike most shells, which accept and return text, PowerShell is built on top of the .NET Common Language Runtime (CLR), and accepts and returns .NET objects. This fundamental change brings entirely new tools and methods for automation.

PowerShell has grown in popularity in the last few years among defenders and especially attackers. Knowing PowerShell is a necessary skill. If you have only heard of PowerShell but never dabbled with it, fret not, today you will.

Recall from the definition above that PowerShell is a command-line shell. We must enter commands into the command prompt to instruct PowerShell on what we want it to do for us. PowerShell commands are known as cmdlets.

To list the contents of the current directory we are in, we can use the `Get-ChildItem` cmdlet. There are various other options we can use with this cmdlet to enhance its capabilities further:

- `-Path` Specifies a path to one or more locations. Wildcards are accepted.
- `-File -Directory` To get a list of files, use the File parameter. To get a list of directories, use the Directory parameter. You can use the Recurse parameter with File and/or Directory parameters.
- `-Filter` Specifies a filter to qualify the Path parameter.
- `-Recurse` Gets the items in the specified locations and in all child items of the locations.
- `-Hidden` To get only hidden items, use the Hidden parameter.
- `-ErrorAction SilentlyContinue` Specifies what action to take if the command encounters an error.

For example, if you want to view all of the hidden files in the current directory you are in, you can issue the following command: `Get-ChildItem -File -Hidden -ErrorAction SilentlyContinue`

Another useful cmdlet is `Get-Content`. This will allow you to read the contents of a file.

You can run this command as follows: `Get-Content -Path file.txt`

You can run numerous operations with the `Get-Content` cmdlet to give you more information about the particular file you are inspecting. Such as how many words are in the file and the exact positions for a particular string within a file.

To get the number of words contained within a file, you can use the `Get-Content` cmdlet and pipe the results to the `Measure-Object` cmdlet.

You run this command as follows: `Get-Content -Path file.txt | Measure-Object -Word`

To get the exact position of a string within the file, you can use the following command:

```

PS C:\Users\mceager> Get-Content e705msw10Y4k.txt
I want the movie Scrooged <3>
PS C:\Users\mceager>

```

THM AttackBox

Question 4

Q4: Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder?

=3lfthr3e

The screenshot shows a web browser window on the left and a terminal window on the right.

Web Browser (tryHackMe | 25 Days of Cyber Security - r2_cspdf):

- Index: The index is the numerical value that is the location of the string within the file. Since indexes start at zero, you typically need to subtract one from the original value to extract the string at the correct position. **This is not necessary for this exercise.**
- To change directories, you can use the `Set-Location` cmdlet.
- For example, `Set-Location -Path c:\users\administrator\Desktop` will change your location to the Administrator's desktop.
- The last cmdlet that is needed to solve this room is `Select-String`. This cmdlet will search a particular file for a pattern you define within the command to run.
- An example execution of this command is `Select-String -Path "c:\users\administrator\Desktop" -Pattern "*.pdf"`.
- Note: You can always use the `Get-Help` cmdlet to obtain more information about a specific cmdlet. For example, `Get-Help Select-String`.
- Answer the questions below:**
- Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?
- Front teeth Correct Answer
- 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?
- Scrooged Correct Answer
- Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder? (This command will take a while)
- Answer format: ***** Submit Hint
- How many words does the first file contain?
- Answer format: *** Submit
- What 2 words are at index 551 and 6991 in the first file?
- Answer format: *** * Submit

Terminal (c:\Windows\System32\cmd.exe - powershell):

```
PS C:\Windows\System32> Get-ChildItem -Hidden -Directory -Filter "*3*"
Directory: C:\Windows\System32

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

PS C:\Windows\System32>
```

Question 5

Q5: How many words does the first file contain?

=9999

The screenshot shows a web browser window on the left and a terminal window on the right.

Web Browser (tryHackMe | 25 Days of Cyber Security - r2_cspdf):

- Hidden To get only hidden items, use the Hidden parameter.
- ErrorAction SilentlyContinue Specifies what action to take if the command encounters an error.
- For example, if you want to view all of the hidden files in the current directory you are in, you can issue the following command: `Get-ChildItem -File -Hidden -ErrorAction SilentlyContinue`
- Another useful cmdlet is `Get-Content`. This will allow you to read the contents of a file.
- You can run this command as follows: `Get-Content -Path file.txt`
- You can run numerous operations with the `Get-Content` cmdlet to give you more information about the particular file you are inspecting. Such as how many words are in the file and the exact positions for a particular string within a file.
- To get the number of words contained within a file, you can use the `Get-Content` cmdlet and pipe the results to the `Measure-Object` cmdlet.
- You run this command as follows: `Get-Content -Path file.txt | Measure-Object -Word`
- To get the exact position of a string within the file, you can use the following command: `(Get-Content -Path file.txt)[index]`
- The index is the numerical value that is the location of the string within the file. Since indexes start at zero, you typically need to subtract one from the original value to extract the string at the correct position. **This is not necessary for this exercise.**
- To change directories, you can use the `Set-Location` cmdlet.
- For example, `Set-Location -Path c:\users\administrator\Desktop` will change your location to the Administrator's desktop.
- The last cmdlet that is needed to solve this room is `Select-String`. This cmdlet will search a particular file for a pattern you define within the command to run.
- An example execution of this command is `Select-String -Path "c:\users\administrator\Desktop" -Pattern "*.pdf"`.
- Note: You can always use the `Get-Help` cmdlet to obtain more information about a specific cmdlet. For example, `Get-Help Select-String`.
- Answer the questions below:**

Terminal (c:\Windows\System32\cmd.exe - powershell):

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

PS C:\Windows\System32>
```

Question 6

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

=Red Ryder

The screenshot shows the TryHackMe interface with the question details and a terminal window. In the terminal, the user has run the command `Get-Content -Path 1.txt | Measure-Object`. The output shows the total number of lines and characters, which the user has highlighted. Then, the user runs `Get-Content -Path 1.txt | Select-String -Pattern 'red ryder'`, and the terminal highlights the words "Red" and "Ryder" at indices 551 and 6991 respectively.

Question 7

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?

=redryderbbgun

The screenshot shows the TryHackMe interface with the question details and a terminal window. In the terminal, the user has run the command `Get-Content -Path 2.txt | Select-String -Pattern 'red ryder'`. The terminal highlights the string "redryderbbgun".

Methodology (Day20):

To begin with, we use SSH to connect to the remote machine using respective command. Then, continue by inserting the password as provided. First, we navigate to the Documents folder and using “Get-ChildItem -File -Hidden -ErrorAction SilentlyContinue” command to see the list of hidden folder. Next we use “Get-Content -Path e1fone.txt” command to access the contents of the file. Moving to the next task, we navigate to the Desktop folder. Using the same steps, we access the contents of the file that has been stored there. After that, we navigate to the Windows directory, “C:\Windows\System32”. To see the name of hidden folder, we use Get-ChildItem -Hidden -Directory -Filter “*3*” command. Then, proceeds with “Get-Content -Path 1.txt | Measure-Object -Word” command to get the number of words contained in that file. We also use “(Get-Content -Path 1.txt)[index] ” command to get exact position of a word within the file. Last, we use “Get-Content -Path 1.txt | Select-String -Pattern “redryder” ” command to get the full answer.