PSP0201 Week 5 Writeup

GROUP NAME: Cyborgs

MEMBERS

ID NUMBER	NAME	ROLE
1211102066	Hemma Ravindran	Leader
1211100614	Tivaasheny Ananthan	Member
1211102168	Nicholas Cheok Jia Jie	Member
1211100986	Sarvesh Munusamy	Member

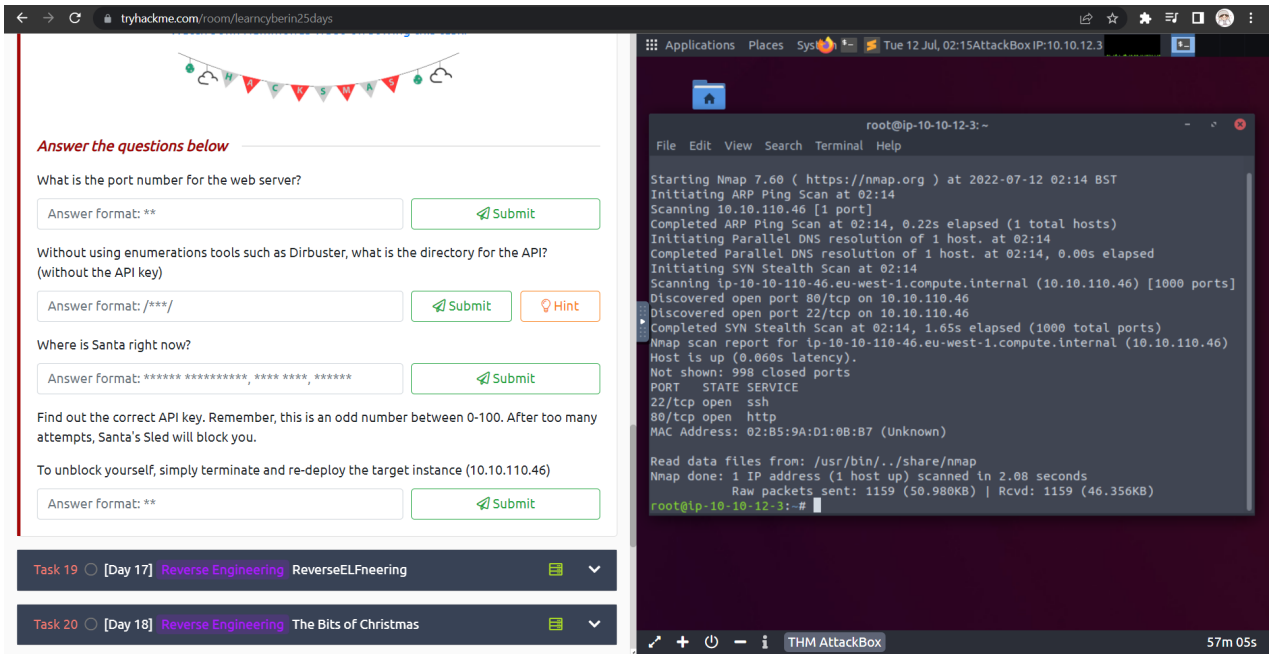
Day 16 - Help! Where is Santa?

Tool used: google and try hackme

Solution/walkthrough:

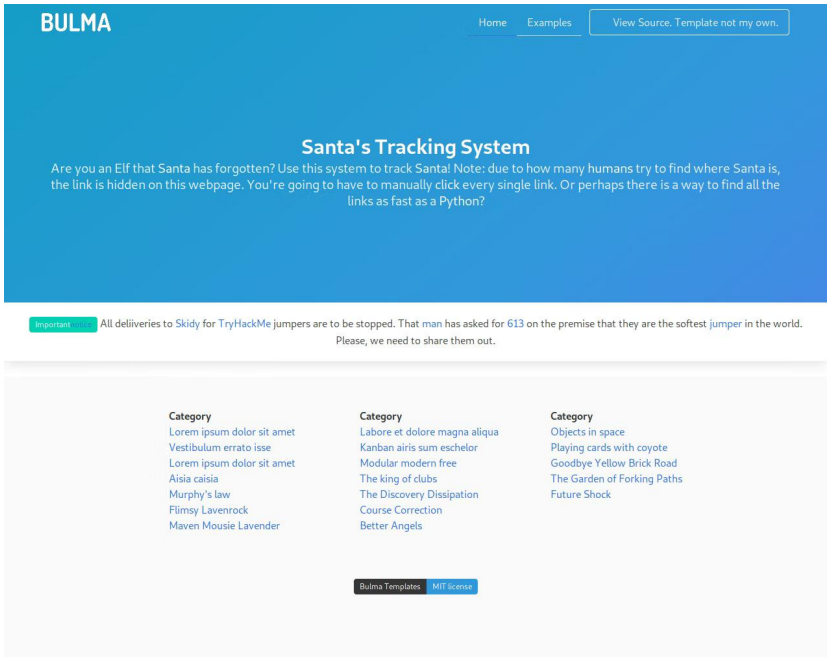
Question 1:

We are supposed to find the port number using the nmap.



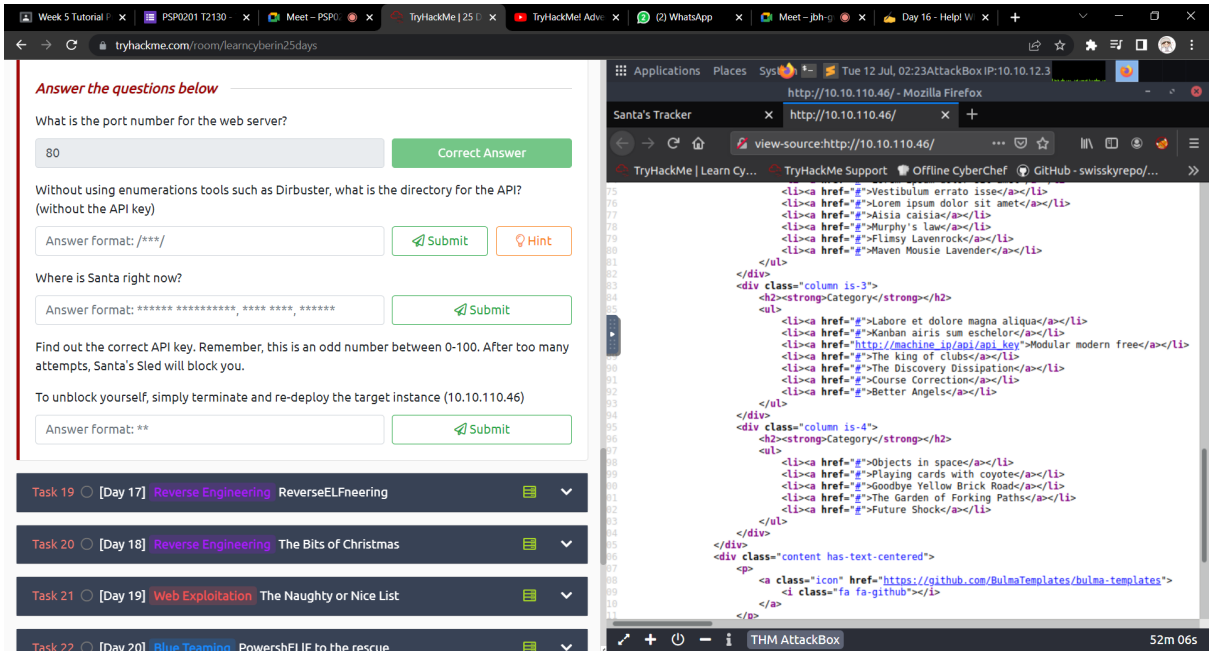
Question 2:

We got the answer from the hint given.



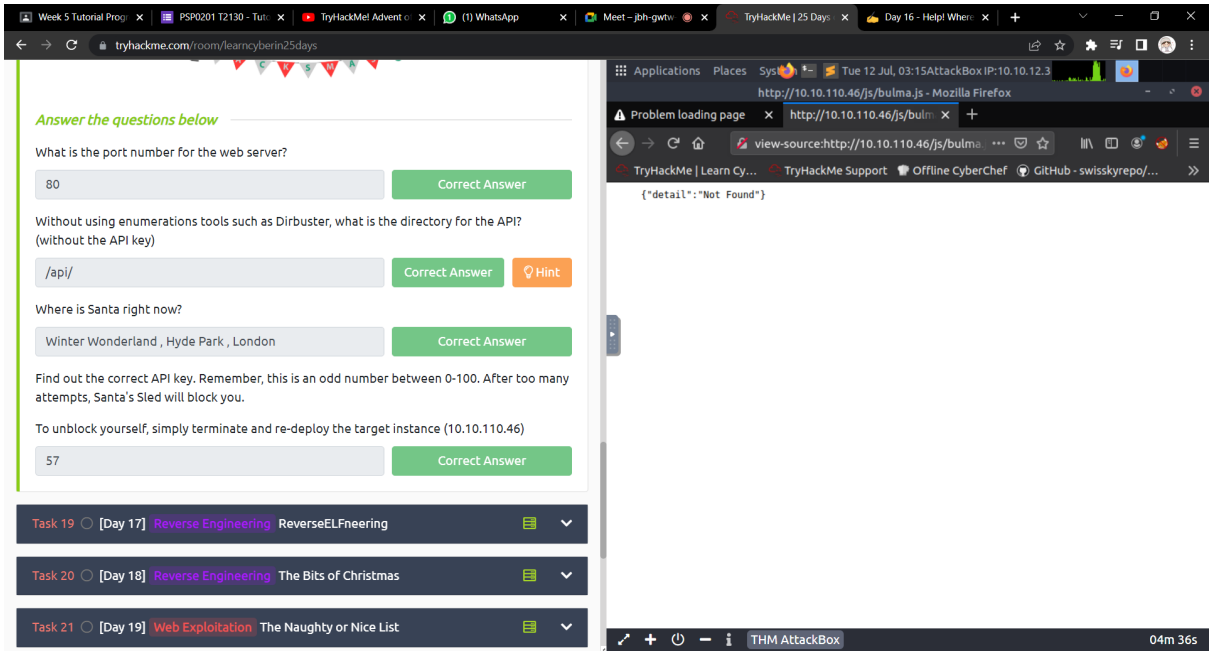
Question 3

We guessed it from the links given.



Question 4

We click the 'View Page Source' and then scroll to the bottom. Find the link, click it, then show up the answer.



Question 5 , 6

We can type out a simple code and put the range to make it more easier.

Thought Process/Methodology:

Firstly, find the port number using the nmap and then put the Ip address and the port number in mozilla firefox.We'll get a page.we must right click and go to the view page source. From there we can get the answer for the second and third question.For question number 4 we should go to the bottom of the view page source and then press the link. The answer will be displayed. Question 5,6 should be done using coding. We must type out a basic code and run it . We will get the answers .

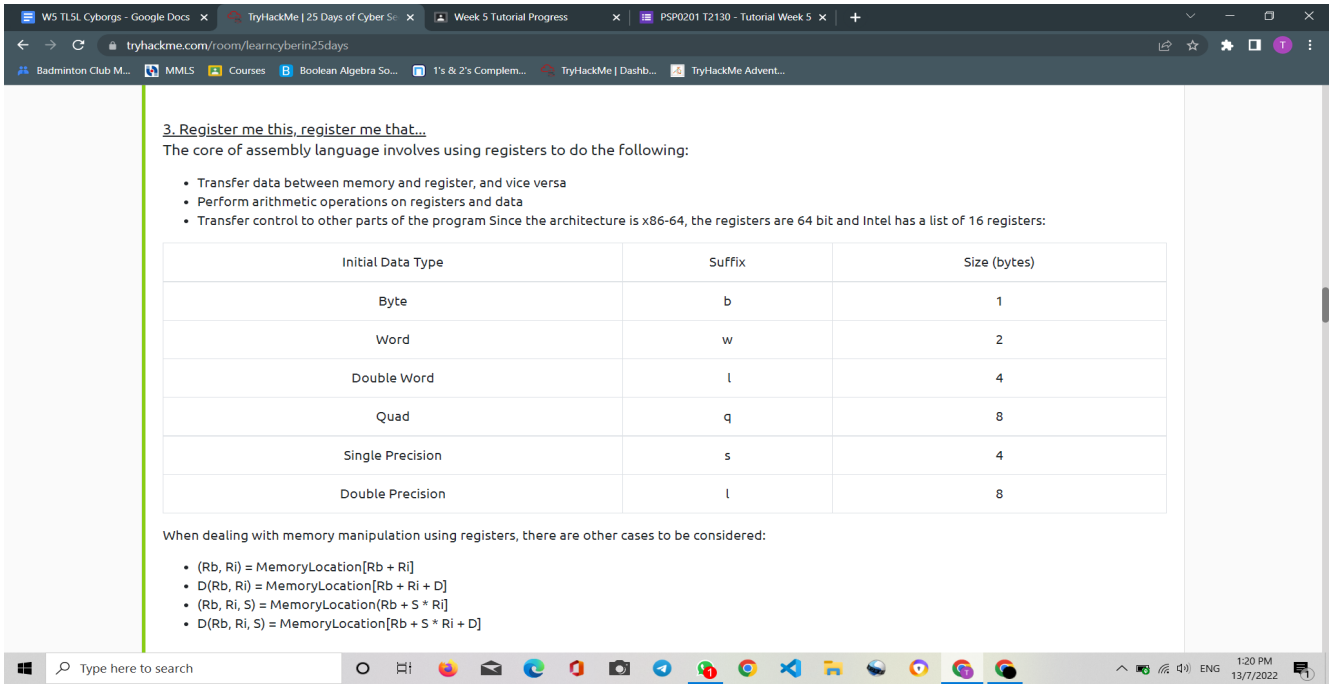
Day 17 - ReverseELFneering

Tool used: google and try hack me attack box

Solution/walkthrough:

Question 1:

We refer to this table that given in try hack me to get the answers.



3. Register me this, register me that...

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:

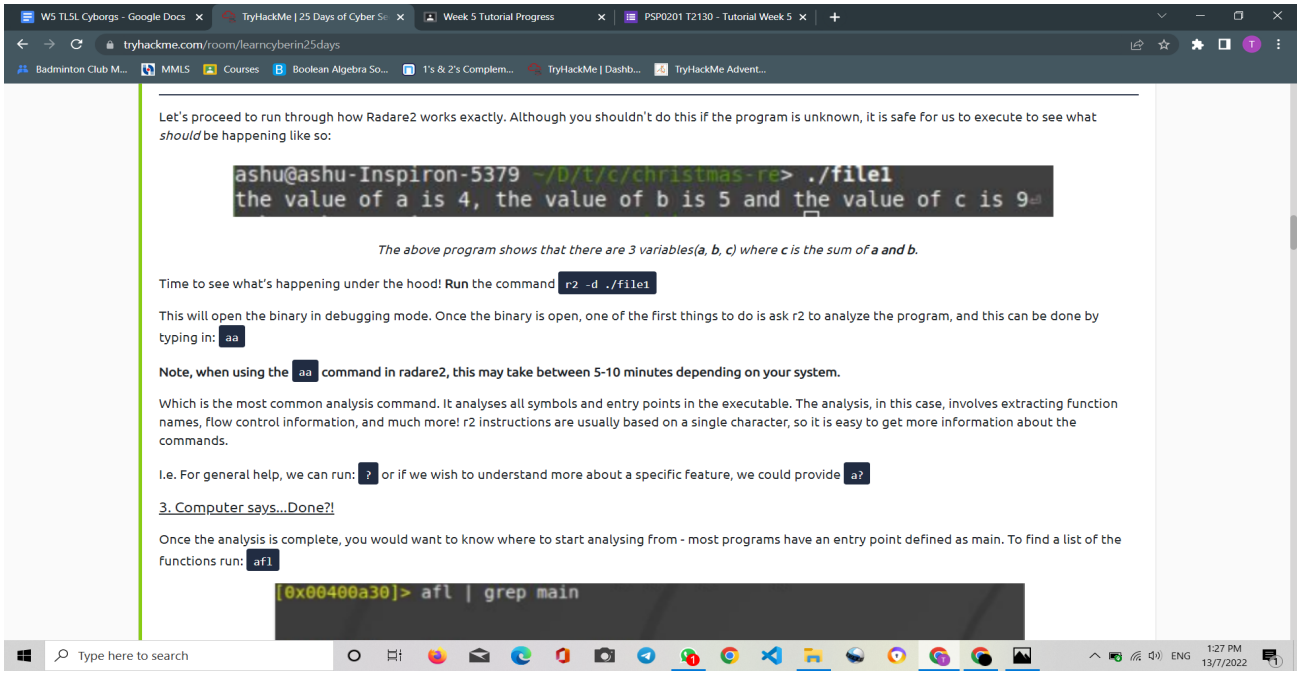
Initial Data Type	Suffix	Size (bytes)
Byte	b	1
Word	w	2
Double Word	l	4
Quad	q	8
Single Precision	s	4
Double Precision	l	8

When dealing with memory manipulation using registers, there are other cases to be considered:

- (Rb, Ri) = MemoryLocation[Rb + Ri]
- D(Rb, Ri) = MemoryLocation[Rb + Ri + D]
- (Rb, Ri, S) = MemoryLocation(Rb + S * Ri]
- D(Rb, Ri, S) = MemoryLocation[Rb + S * Ri + D]

Question 2:

We can get the answer from the try hack me and also we can do at the terminal to see it's function.



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 ~/D/t/c/christmas-re> ./file1
the value of a is 4, the value of b is 5 and the value of c is 9
```

The above program shows that there are 3 variables(a, b, c) where c is the sum of a and b.

Time to see what's happening under the hood! **Run** the command `r2 -d ./file1`

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

Note, when using the `aa` command in radare2, this may take between 5-10 minutes depending on your system.

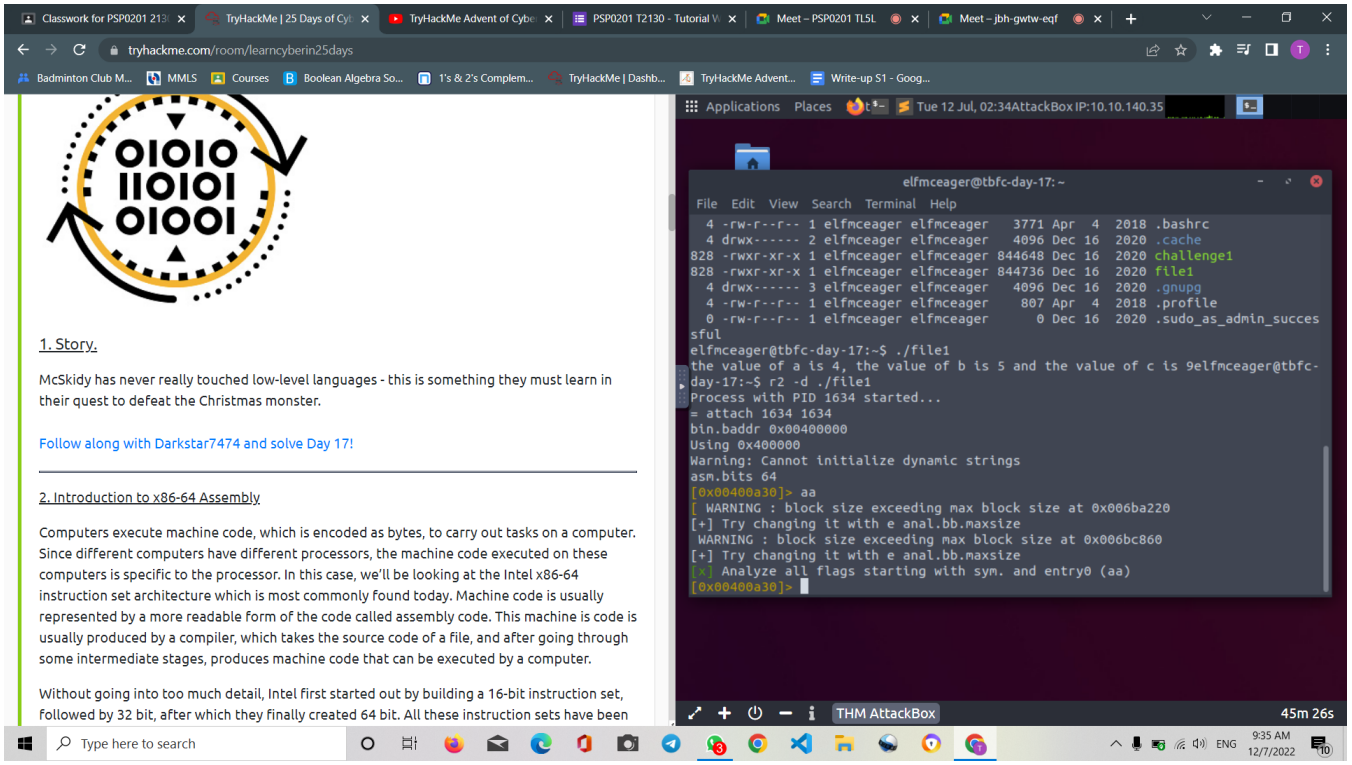
Which is the most common analysis command. It analyses all symbols and entry points in the executable. The analysis, in this case, involves extracting function names, flow control information, and much more! r2 instructions are usually based on a single character, so it is easy to get more information about the commands.

I.e. For general help, we can run: `?` or if we wish to understand more about a specific feature, we could provide `a?`

3. Computer says...Done?!

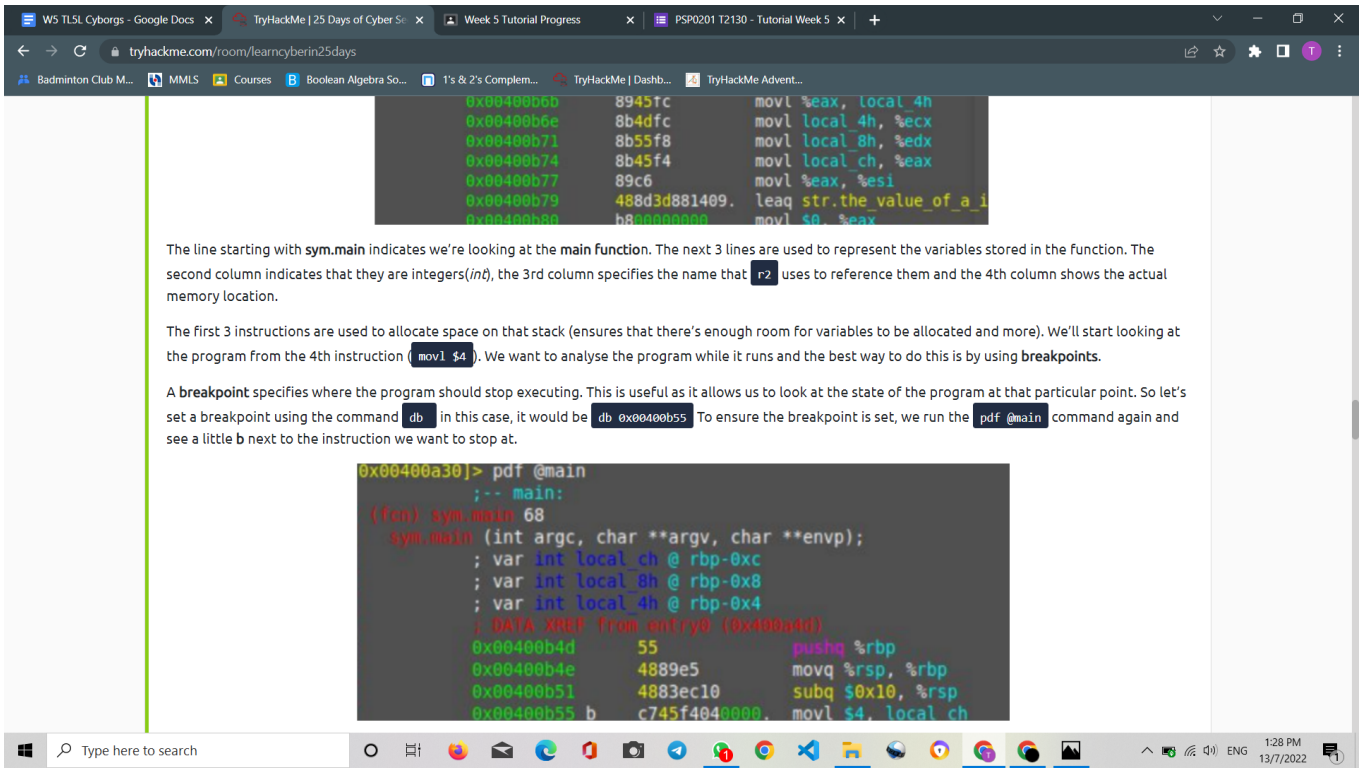
Once the analysis is complete, you would want to know where to start analysing from - most programs have an entry point defined as main. To find a list of the functions run: `afl`

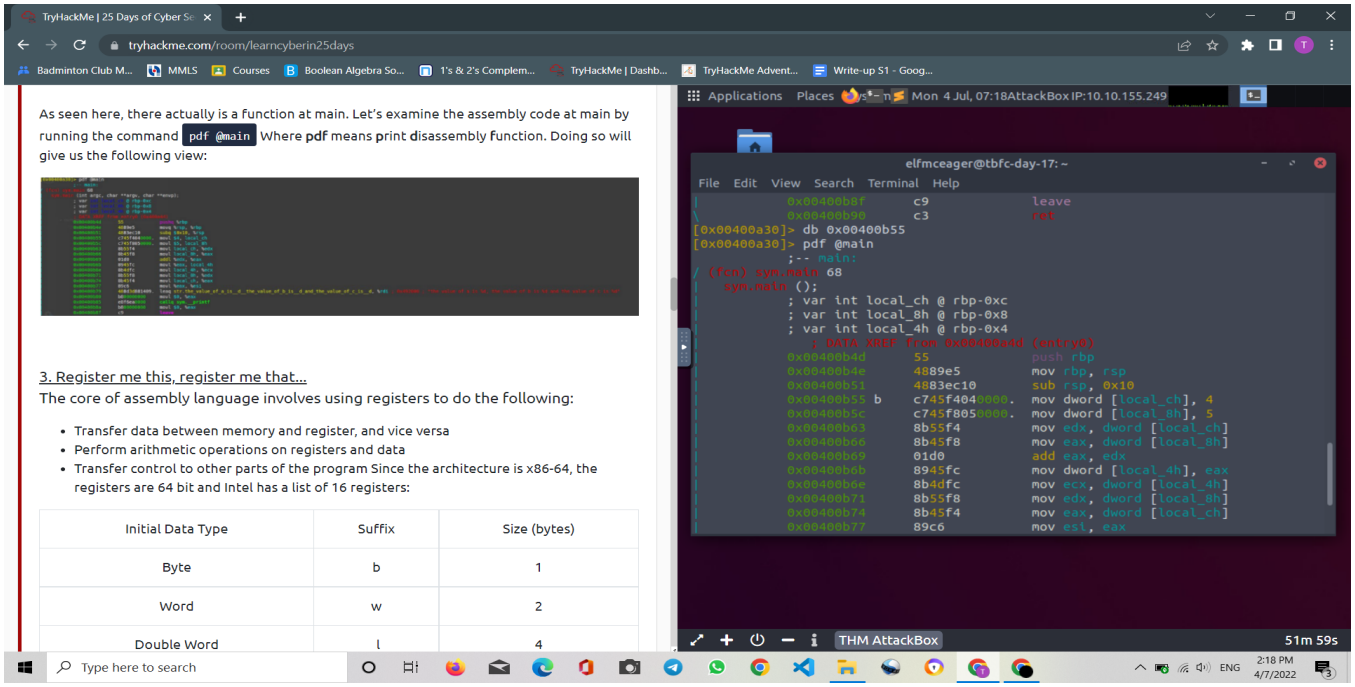
```
[0x00400a30]> afl | grep main
```



Question 3:

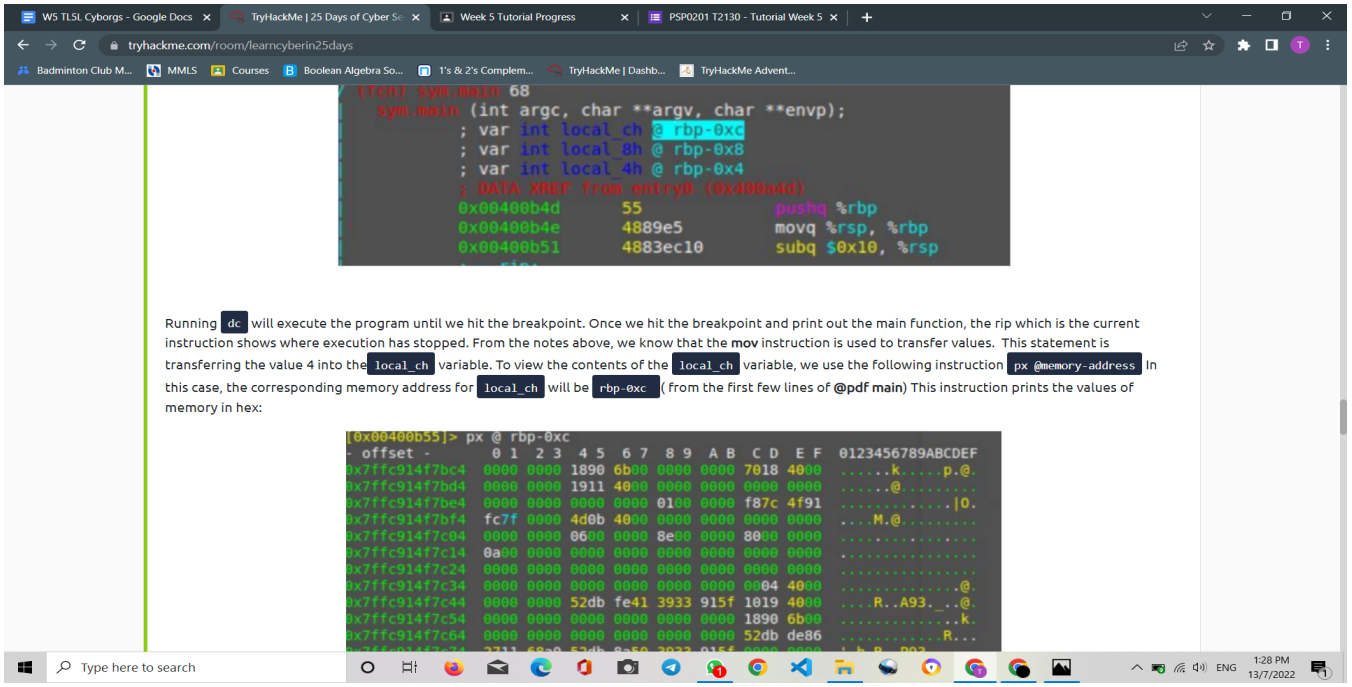
We can get the answer from the try hack me and also we can do at the terminal to see it's function.

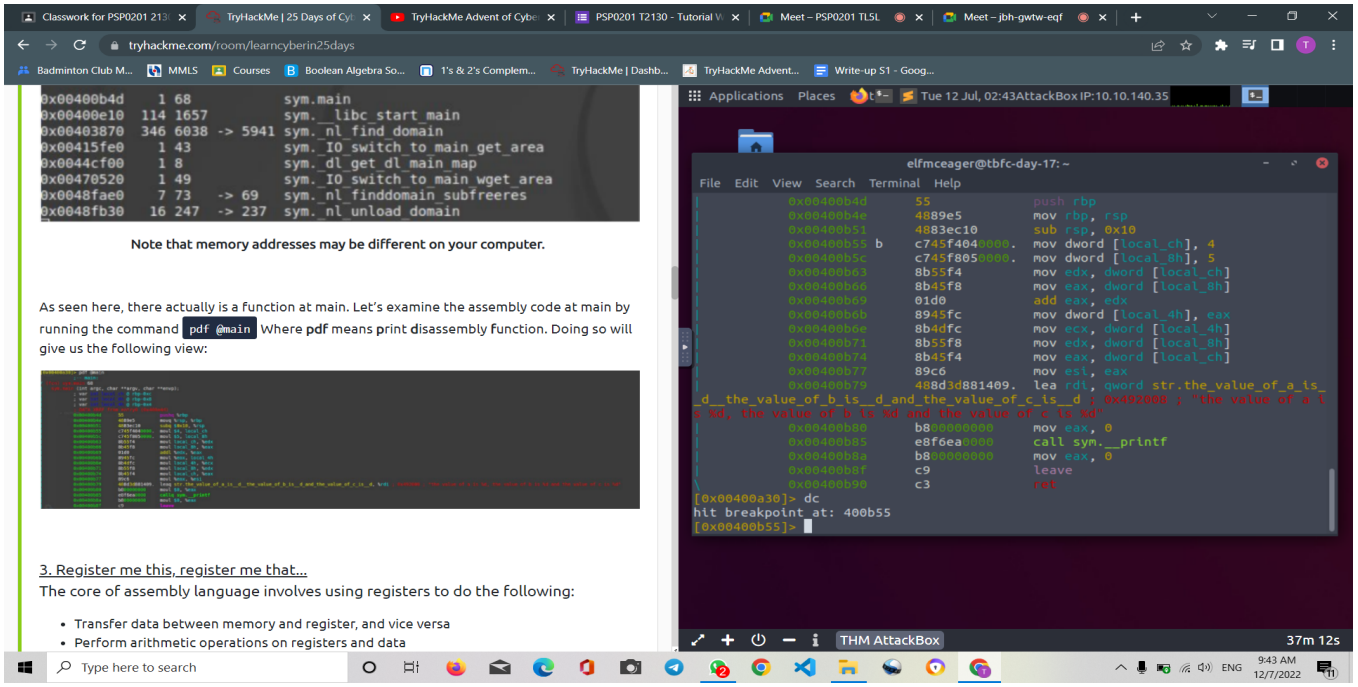




Question 4:

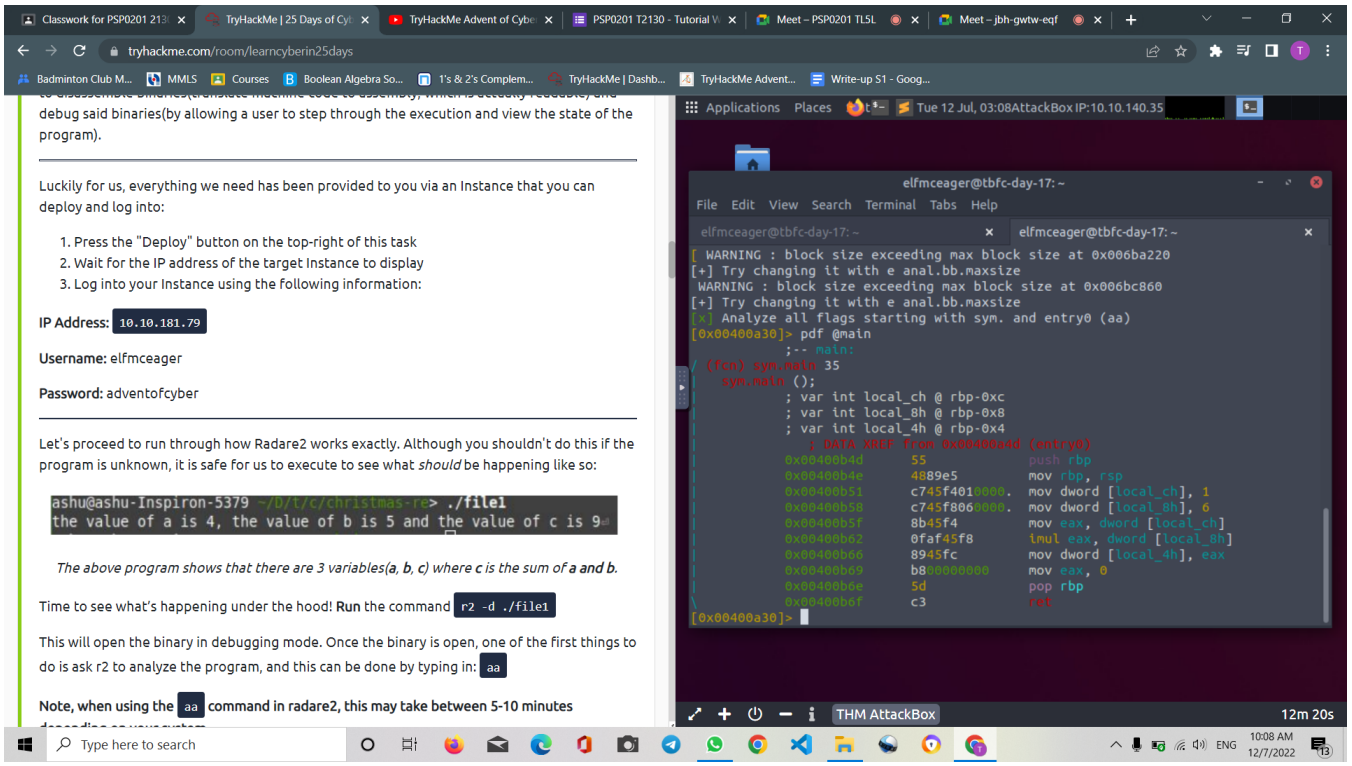
We can get the answer from the try hack me and also we can do at the terminal to see it's function.





Question 5, 6 and 7:

We need to do the challenge in terminal to get the answers.



Thought Process/Methodology:

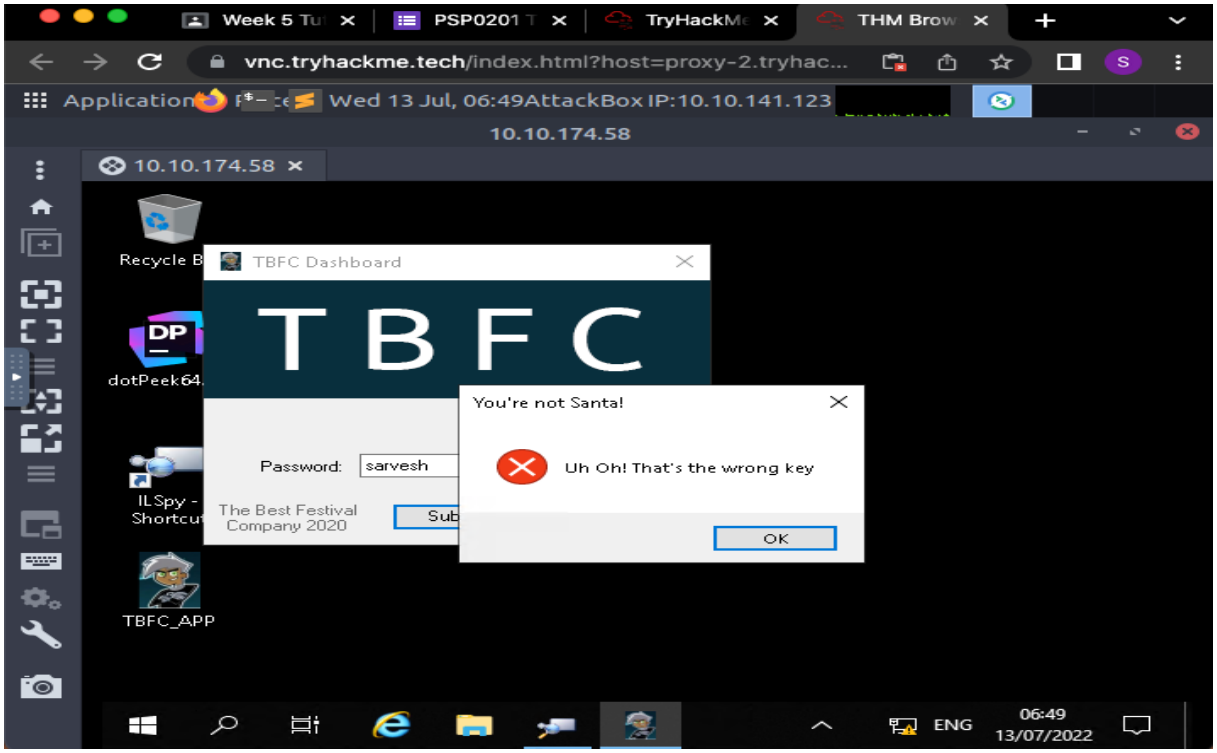
We need to open the attack box in kali.Then if we follow the youtube video we manage to file1. We did it to learn the function dc db dr aa and more. But the main thing is we need to do the challenge to get the answers. Firstly, we need to type echo “our IP address” > target.txt enter cat target.txt enter ssh elfmceager@IP address enter. Then we need to type yes and the password. Later we need type ls enter ls -lsa enter then r2 -d ./challange1. Then we have to type aa and wait for awile. Finally we need to type pdf @main in order to get the answers.

Day 18 - The bits of christmas

Tools used : attackbox, TBFC APP, ILspy

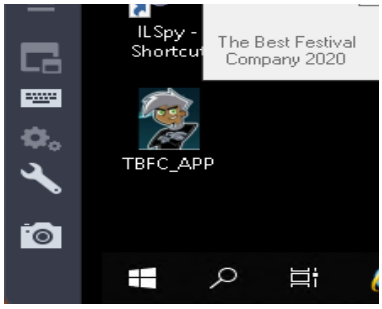
Question 1:

If we enter the wrong password in the TBFC APP, the message that pops up is “You’re not Santa”.



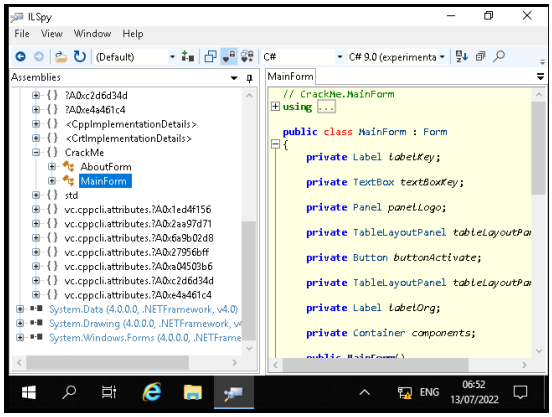
Question 2:

TBFC stands for The Best Festival Company.



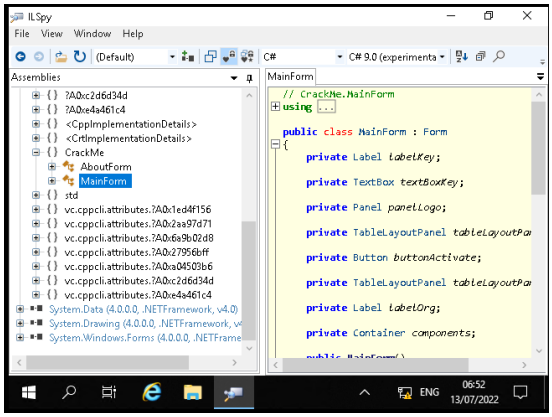
Question 3:

After decompiling the TBFC_APP with ILspy. The module that catches my attention is CrackMe.



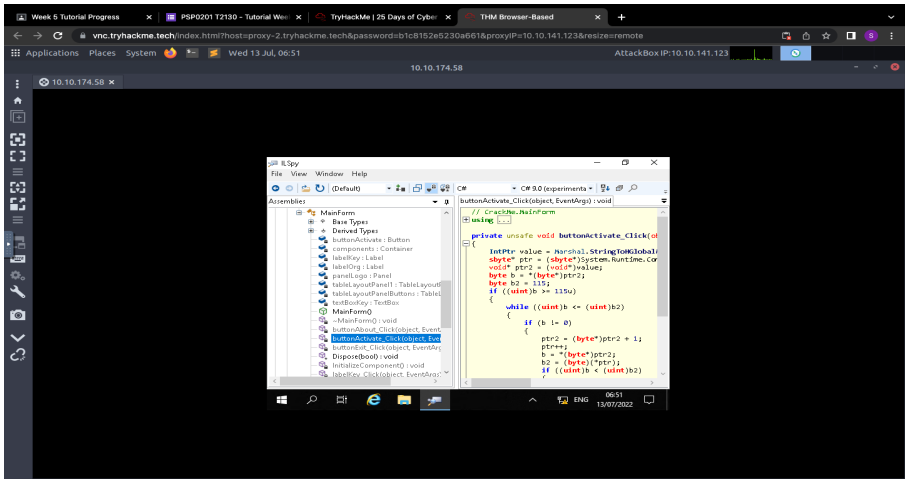
Question 4:

Within the module Crack me, “Main Form” is the form that contains the information we need.



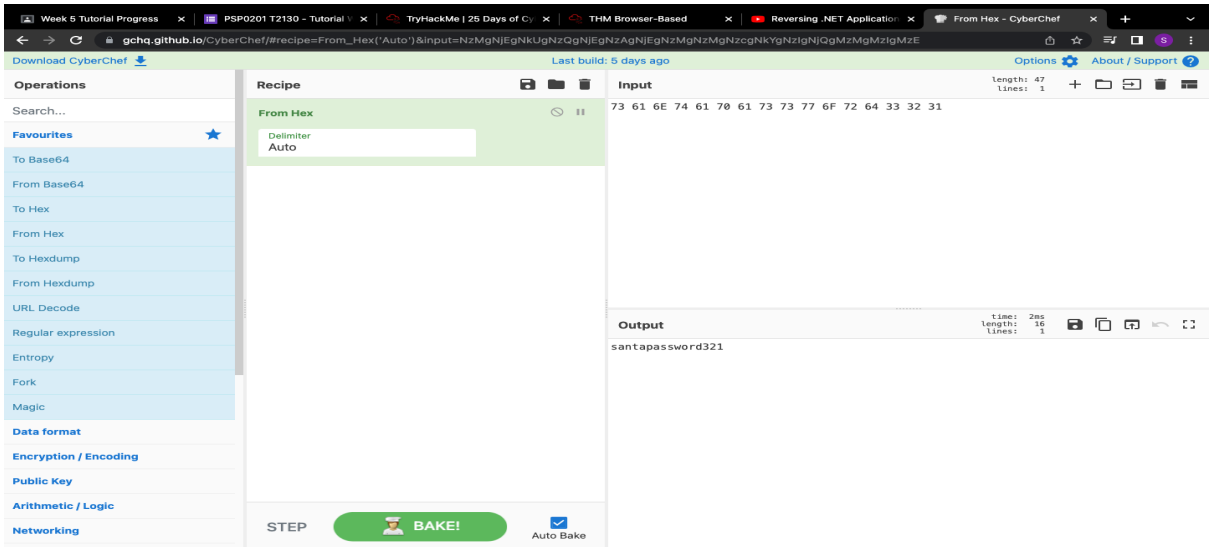
Question 5:

“buttonActivate_Click” is the method that we can use to contain the information that we need.



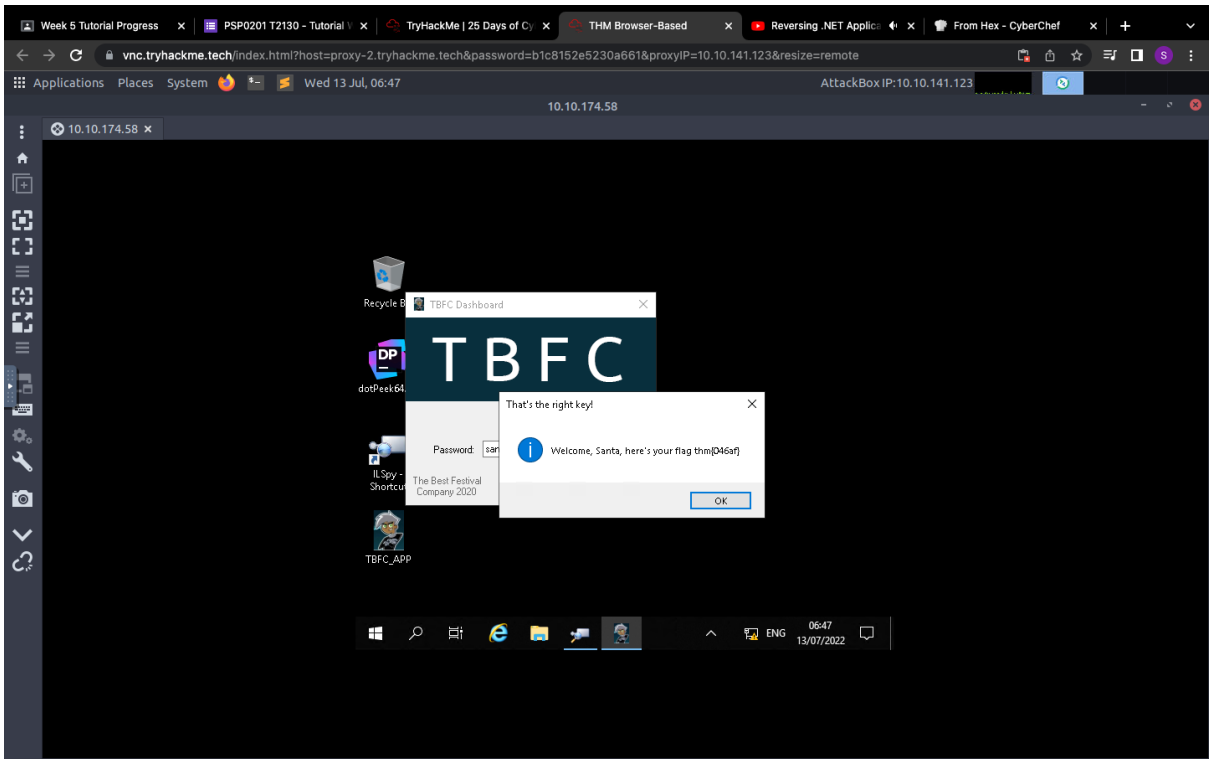
Question 6:

After getting the password that we want from “buttonActivate_Click” , we should copy and paste it in cyberchef, and then get santa’s password.



Question 7:

Since we retrieved the password, we can re-login again in TBFC and get the flag.



Thought Process/Methodology:

After starting the machine, we should open the remmina and run the ip address given. Then we should open the TBFC application. Since we don't know the password of santa, we should open IL spy and open the Tbfc application file. After decompiling the application, we should open the module called, “Crack me”. Within the module, we should open main form and gain the information we need. After getting the password that we want from “buttonActivate_Click” , we should copy and paste it in cyberchef, and then get santa’s password. Since we retrieved the password, we can re-login again in TBFC and get the flag.

Day 19 - The Naughty or Nice List

Tool used: google and try hackme

Solution/walkthrough:

Question 1:

Enter your IP address to run the browser then scroll to the bottom and enter any names in the Name Box and search about it. You will get a display on whether the name is a nice or naughty list.

Note that while the example of SSRF used in this task is effectively a Remote File Inclusion (RFI) vulnerability as well, not every SSRF is. Some SSRF vulnerabilities only trigger a DNS lookup, while others may not return any kind of response to the web app, but can still be used to "port scan" internal systems by measuring the time each request takes to complete. In other cases, SSRF may be used as a form of Denial of Service (DoS) since the attacker can continually request that the server download large files simultaneously (taking up memory, disk space, and network bandwidth).

Walkthrough

1. Once the VM is deployed, connect to the web app: http://10.10.14.72

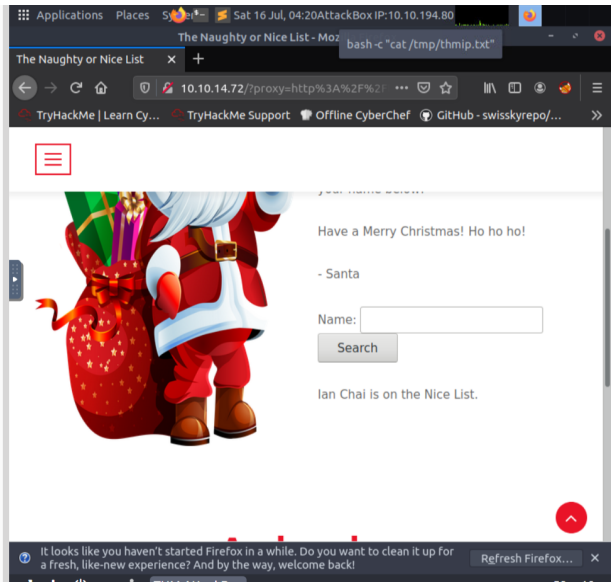
2. Enter a name in the form and click the "Search" button. When the page loads, it should tell you whether that name is on the Naughty List or the Nice List. Notice that the URL for the page looks something like this: http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2Fsearch.php%3Fname%3DTib3rius

   If we use a URL decoder on the value of the "proxy" parameter, we get: http://list.hohoho:8080/search.php?name=Tib3rius

   Since "list.hohoho" is not a valid hostname on the Internet (.hohoho is not a top-level domain), this hostname likely refers to some back-end machine. It seems that the web app works by taking this URL, making a request at the back-end, and then returning the result to the front-end web app. If the developer has not been careful, we may be able to exploit this functionality using Server-Side Request Forgery (SSRF).

3. The most obvious thing we can try to do first is to fetch the root of the same site. Browse to: http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F

   This seems to have potential, as in place of the original "Tib3rius is on the Nice List."



Question 2:

Browse in the website "http://MACHINE_IP/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F" to get a display at the bottom saying "Not Found. The requested URL was not found on this server."

If we use a URL decoder on the value of the "proxy" parameter, we get: http://list.hohoho:8080/search.php?name=Tib3rius

Since "list.hohoho" is not a valid hostname on the Internet (.hohoho is not a top-level domain), this hostname likely refers to some back-end machine. It seems that the web app works by taking this URL, making a request at the back-end, and then returning the result to the front-end web app. If the developer has not been careful, we may be able to exploit this functionality using Server-Side Request Forgery (SSRF).

3. The most obvious thing we can try to do first is to fetch the root of the same site. Browse to: http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F

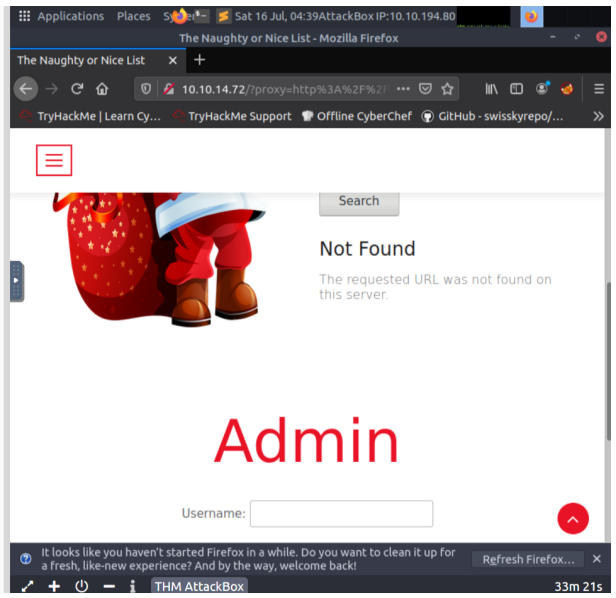
   This seems to have potential, as in place of the original "Tib3rius is on the Nice List." message, we instead see "Not Found. The requested URL was not found on this server." This seems like a generic 404 message, indicating that we were able to make the server request the modified URL and return the response.

   There are many things we could do now, such as trying to find valid URLs for the "list.hohoho" site. We could also try changing the port number from 8080 to something else, to see if we can connect to any other services running on the host, even if these services are not web servers.

4. Try changing the port number from 8080 to just 80 (the default HTTP port): http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A80

   The message now changes to "Failed to connect to list.hohoho port 80: Connection refused" which suggests that port 80 is not open on list.hohoho.

5. Try changing the port number to 22 (the default SSH port): http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A22



Question 3:

Change the port number from 8080 to just 80 in the default http port and you will get a display at the bottom saying "Failed to connect to list.hohoho port 80: Connection refused".

3. The most obvious thing we can try to do first is to fetch the root of the same site. Browse to: http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F

   This seems to have potential, as in place of the original "Tib3rius is on the Nice List." message, we instead see "Not Found. The requested URL was not found on this server." This seems like a generic 404 message, indicating that we were able to make the server request the modified URL and return the response.

   There are many things we could do now, such as trying to find valid URLs for the "list.hohoho" site. We could also try changing the port number from 8080 to something else, to see if we can connect to any other services running on the host, even if these services are not web servers.

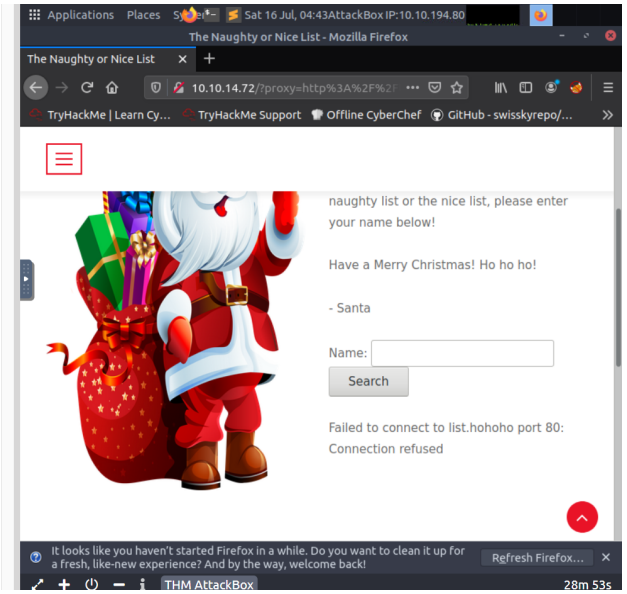
4. Try changing the port number from 8080 to just 80 (the default HTTP port): http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A80

   The message now changes to "Failed to connect to list.hohoho port 80: Connection refused" which suggests that port 80 is not open on list.hohoho.

5. Try changing the port number to 22 (the default SSH port): http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A22

   The message now changes to "Recv failure: Connection reset by peer" which suggests that port 22 is open but did not understand what was sent (this makes sense, as sending an HTTP request to an SSH server will not get you anywhere!)

   Enumerating open ports via SSRF can be performed in this manner, by iterating over common ports and measuring the differences between responses. Even in cases where error messages aren't returned, it is often possible to detect which ports are open vs closed by measuring the time each request takes to complete.



Question 4:

Change the port number again from 80 to 22 in the default http port and you will get a display at the bottom saying "Recv failure: Connection reset by peer".

The message now changes to "Failed to connect to list.hohoho port 80: Connection refused" which suggests that port 80 is not open on list.hohoho.

5. Try changing the port number to 22 (the default SSH port): http://10.10.14.72/?proxy=http%3A%2F%2Flist.hohoho%3A22

   The message now changes to "Recv failure: Connection reset by peer" which suggests that port 22 is open but did not understand what was sent (this makes sense, as sending an HTTP request to an SSH server will not get you anywhere!)

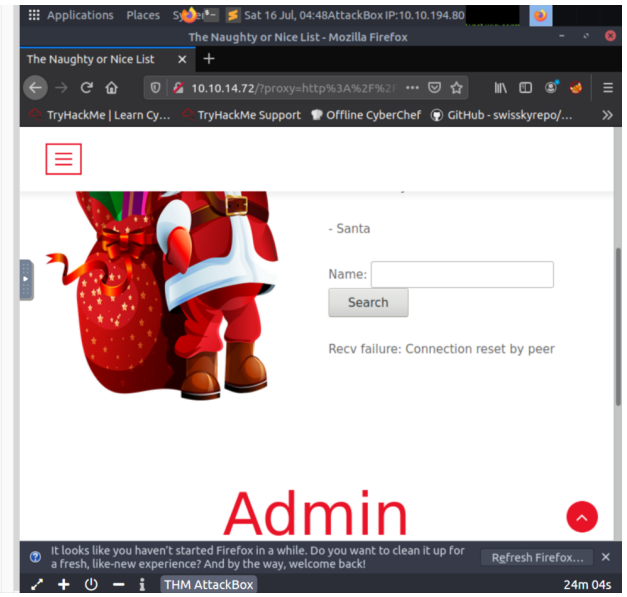
   Enumerating open ports via SSRF can be performed in this manner, by iterating over common ports and measuring the differences between responses. Even in cases where error messages aren't returned, it is often possible to detect which ports are open vs closed by measuring the time each request takes to complete.

6. Another thing we can try to do with SSRF is access services running locally on the server. We can do this by replacing the list.hohoho hostname with "localhost" or "127.0.0.1" (among others). Try this now: http://10.10.14.72/?proxy=http%3A%2F%2Flocalhost

   Oops! It looks like the developer has a check in place for this, as the message returned says "Your search has been blocked by our security team."

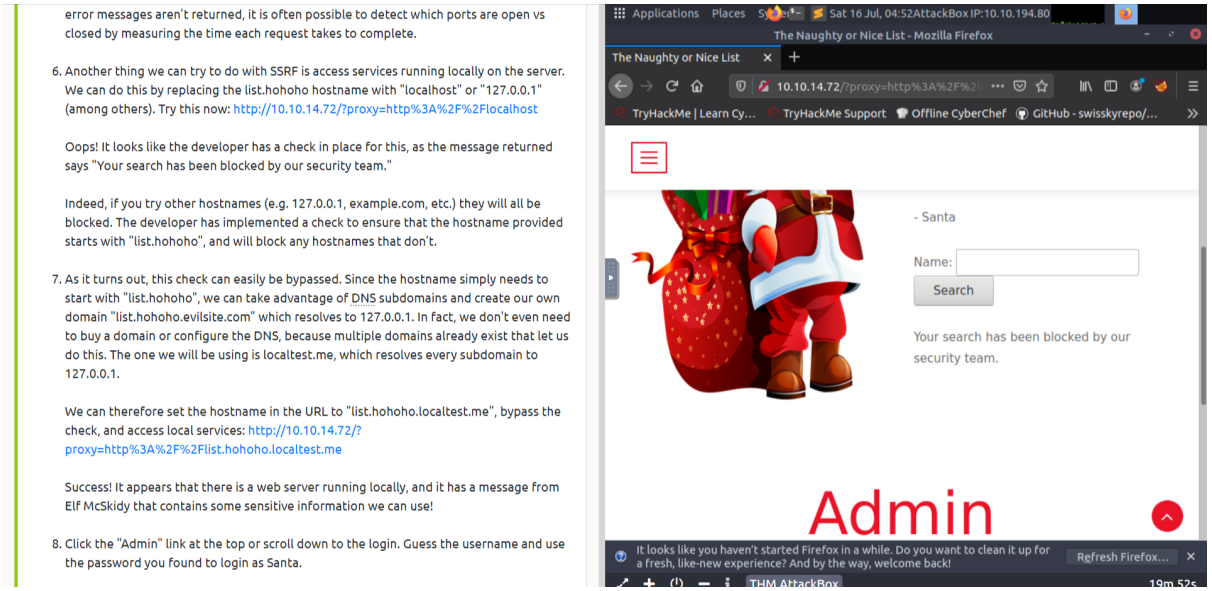
   Indeed, if you try other hostnames (e.g. 127.0.0.1, example.com, etc.) they will all be blocked. The developer has implemented a check to ensure that the hostname provided starts with "list.hohoho", and will block any hostnames that don't.

7. As it turns out, this check can easily be bypassed. Since the hostname simply needs to start with "list.hohoho", we can take advantage of DNS subdomains and create our own domain "list.hohoho.evilsite.com" which resolves to 127.0.0.1. In fact, we don't even need to buy a domain or configure the DNS, because multiple domains already exist that let us do this. The one we will be using is localtest.me, which resolves every subdomain to



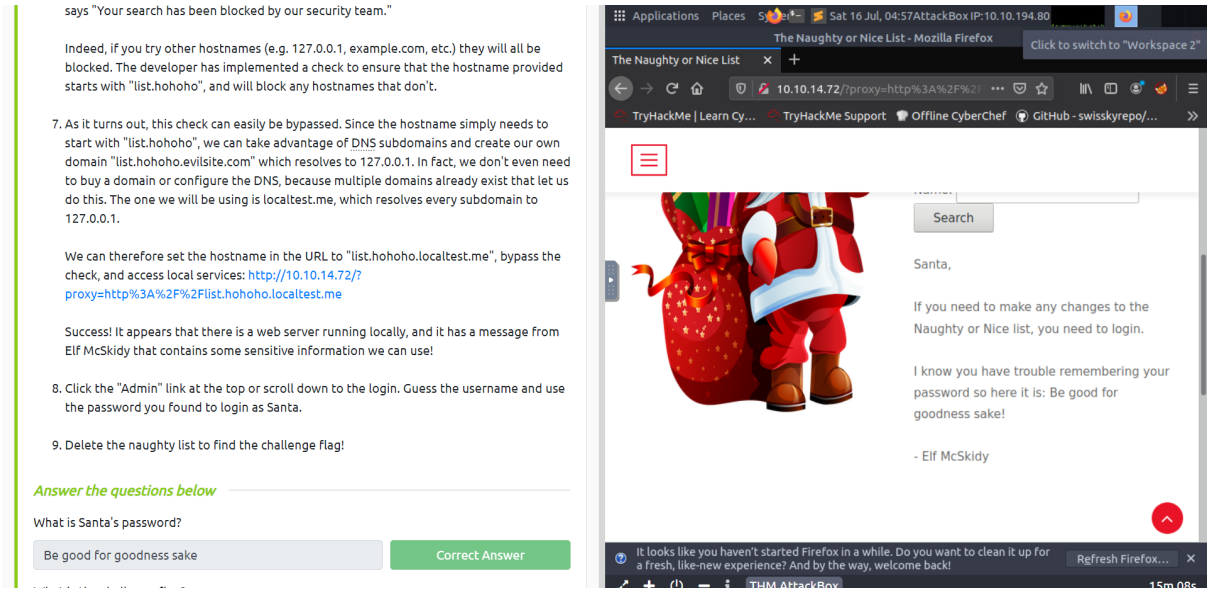
Question 5:

Replace the “list.hohoho hostname” with "localhost" or "127.0.0.1" and you will get a display at the bottom saying "Your search has been blocked by our security team."



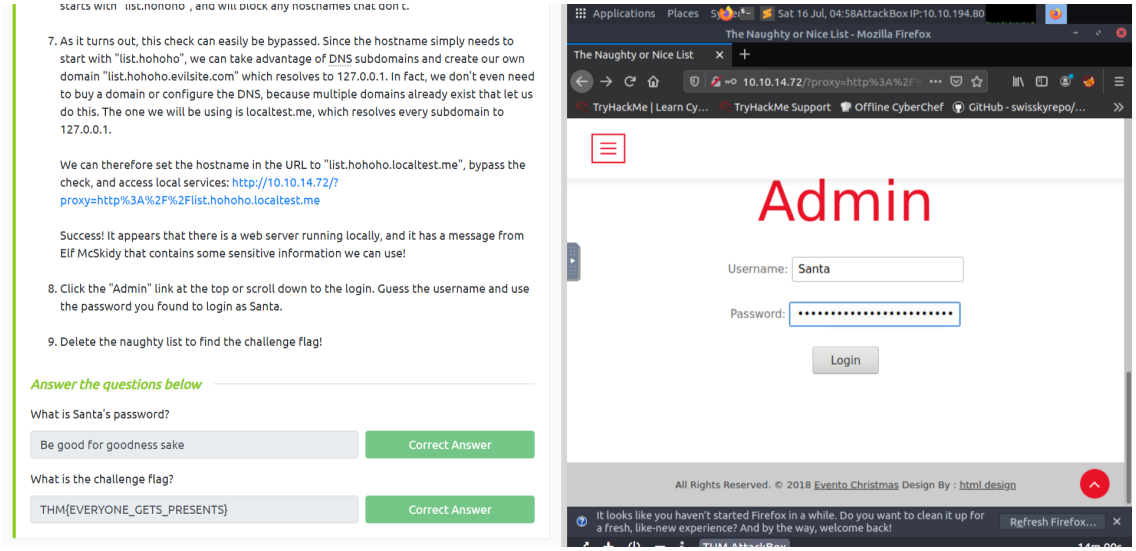
Question 6:

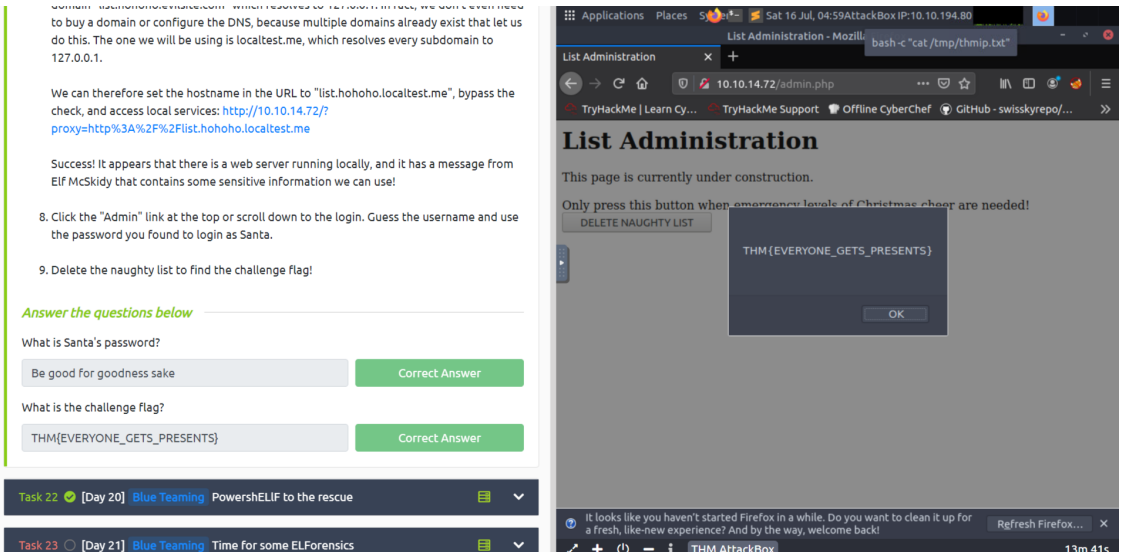
Replace the “localhost” with "list.hohoho.localtest.me" to get the password of Santa “Be good for goodness sake!”



Question 7:

Login as Santa and enter the password in the administration and click on “DELETE NAUGHTY LIST” to get the flag “THM{EVERYONE_GETS_PRESENTS}.





Thought Process/Methodology:

Firstly, we start our machine and attack box to start our process. Then, we should Enter your IP address to run the browser then scroll to the bottom and enter any names in the Name Box and search for it. You will get a display on whether the name is a nice or naughty list. Browse in the website "http://MACHINE_IP/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F" to get a display at the bottom saying "Not Found. The requested URL was not found on this server. Later on, Change the port number from 8080 to just 80 in the default http port and you will get a display at the bottom saying "Failed to connect to list.hohoho port 80: Connection refused". Then, we should Change the port number again from 80 to 22 in the default http port and you will get a display at the bottom saying "Recv failure: Connection reset by peer" and Replace the "list.hohoho hostname" with "localhost" or "127.0.0.1". Lastly, we should Replace the "localhost" with "list.hohoho.localtest.me" to get the password of Santa and then DELETE NAUGHTY LIST" to get the flag "THM{EVERYONE_GETS_PRESENTS}.

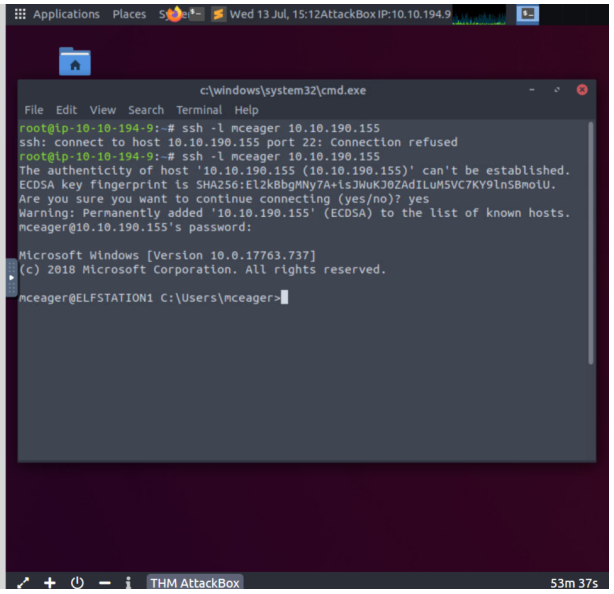
Day 20 - PowershELlF to the rescue

Tool used: google and try hackme

Solution/walkthrough:

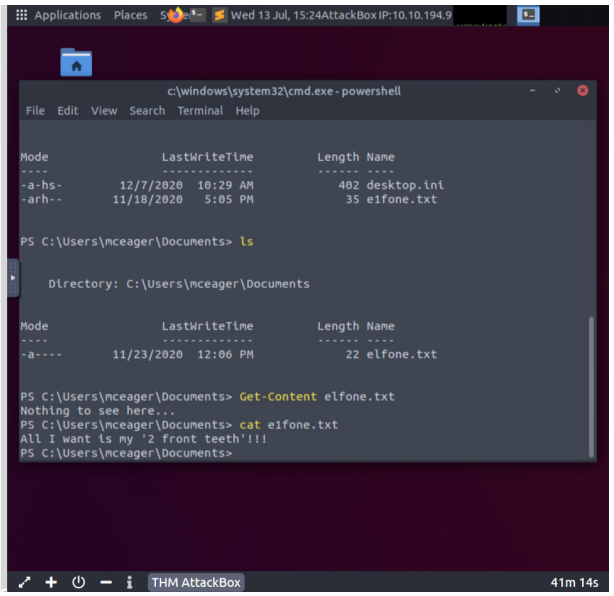
Question 1:

Parameter -l helps to connect with the local host using “ssh -l mceager MACHINE_IP” and its password “r0ckStar!”.



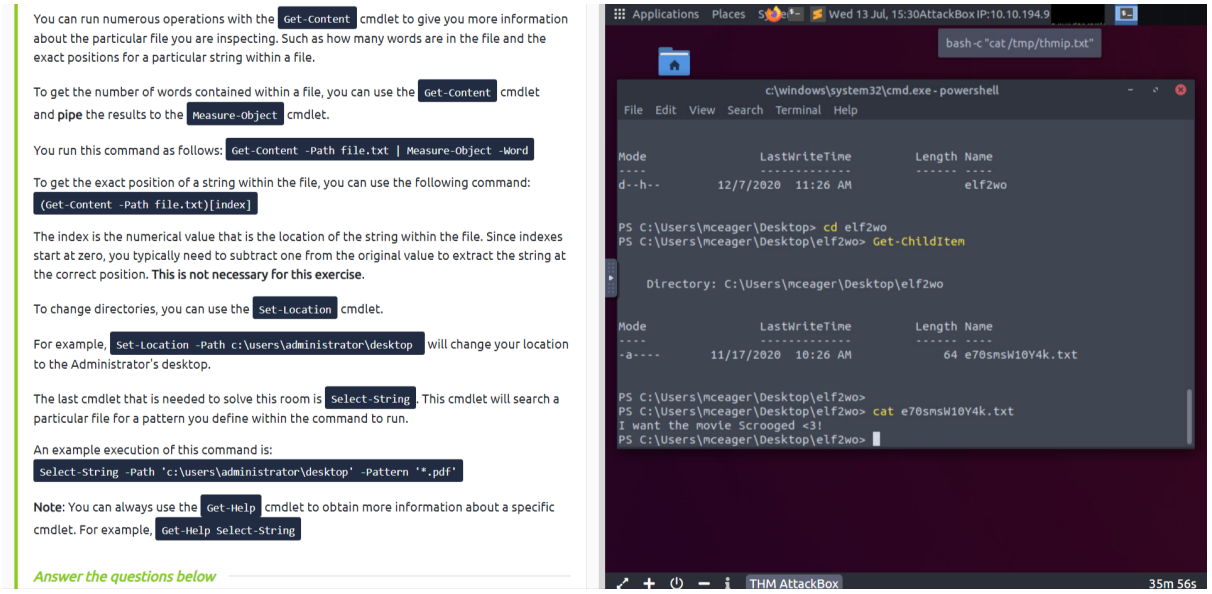
Question 2:

Cat out “e1fone.txt” to get what Elf 1 wants as it wants its 2 front teeth.



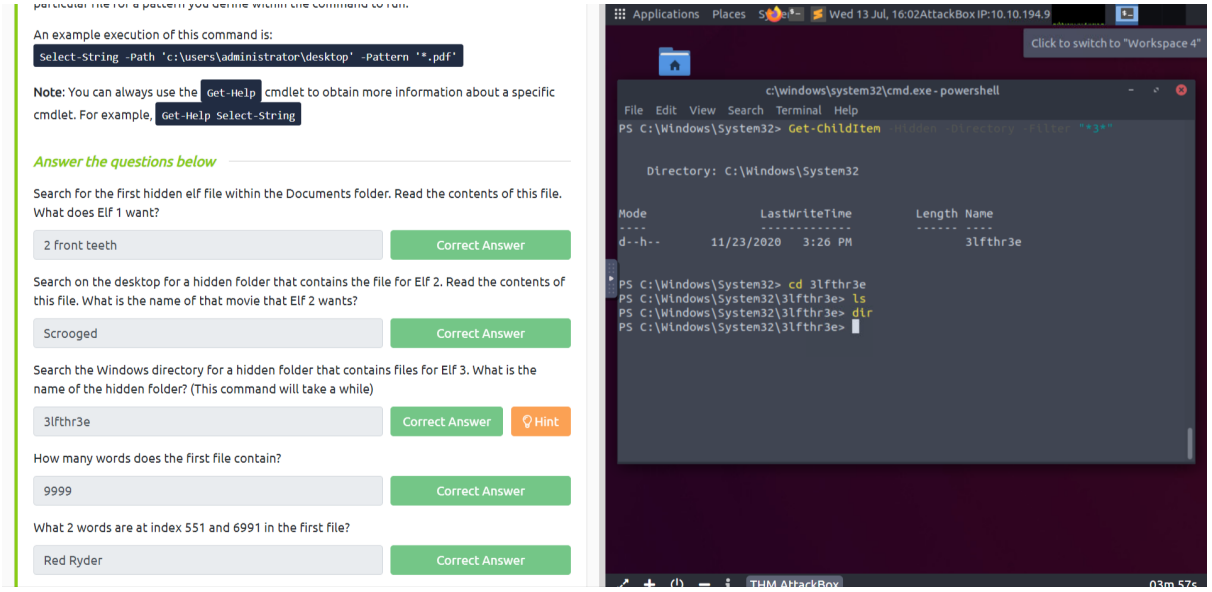
Question 3

Set-Location Desktop to the folder and find the hidden folder that contains the file for Elf 2. Cd the directory and “Get-ChildItem” and cat out “e70smsW10Y4k.txt” to get the movie Elf 2 wanted.



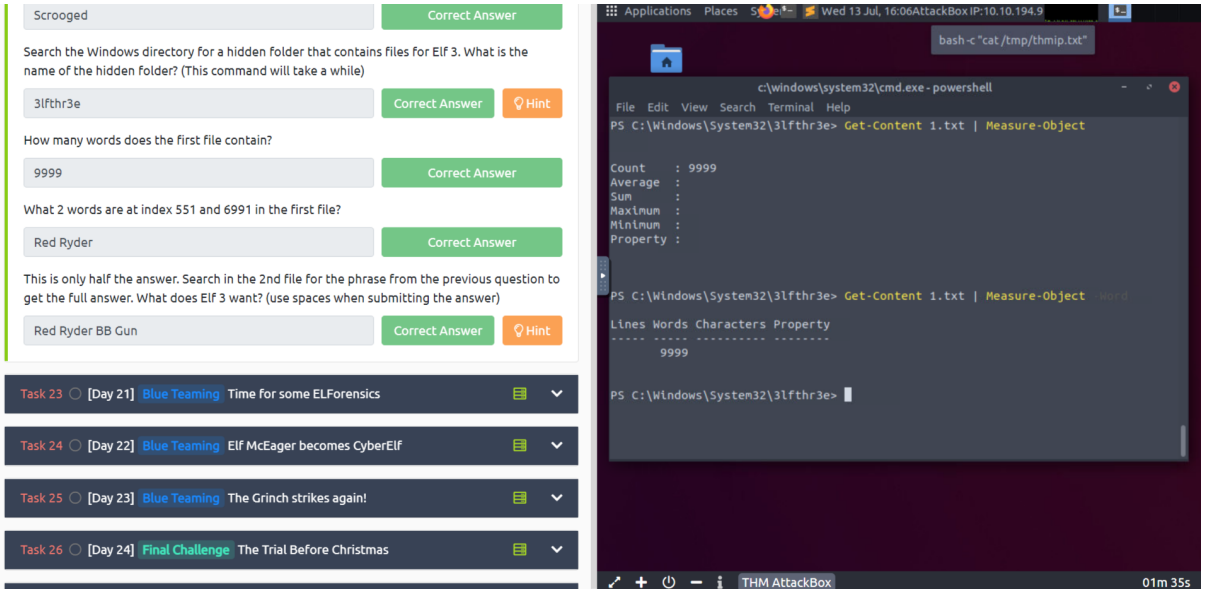
Question 4:

Set up the windows with cd C:/Windows and cd System32 to “Get-ChildItem” to find the hidden folder in the directory by filter “*3*” to get the length name “3lfthr3e” .



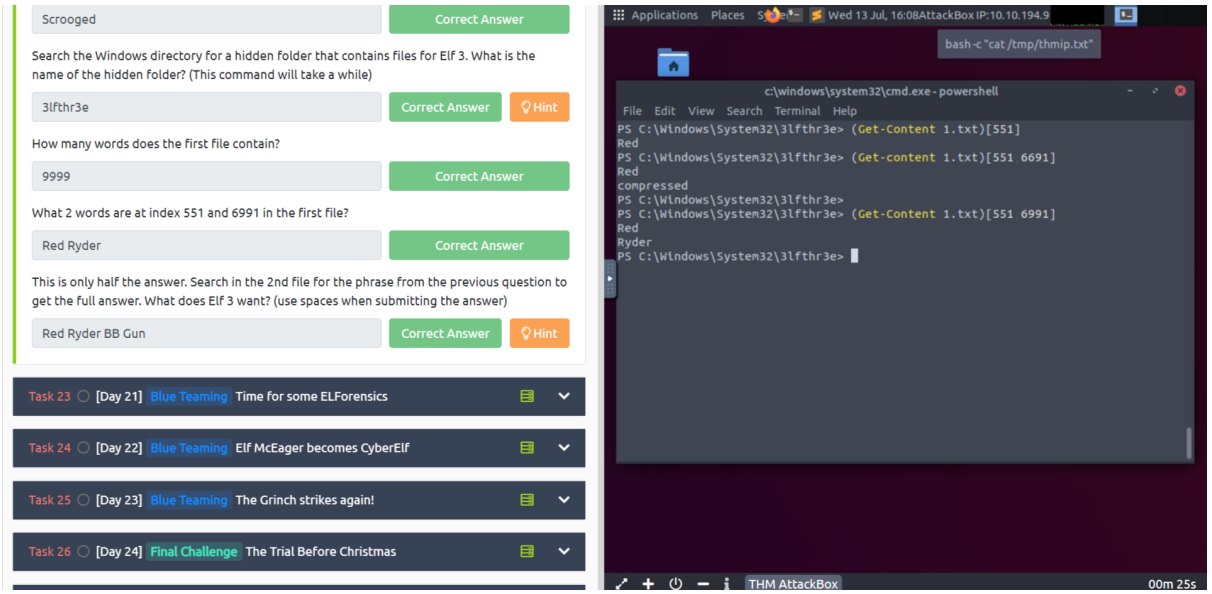
Question 5:

Get content for 1.txt by “Measure object” to get the number of words contained in the first file which is 9999 words count.



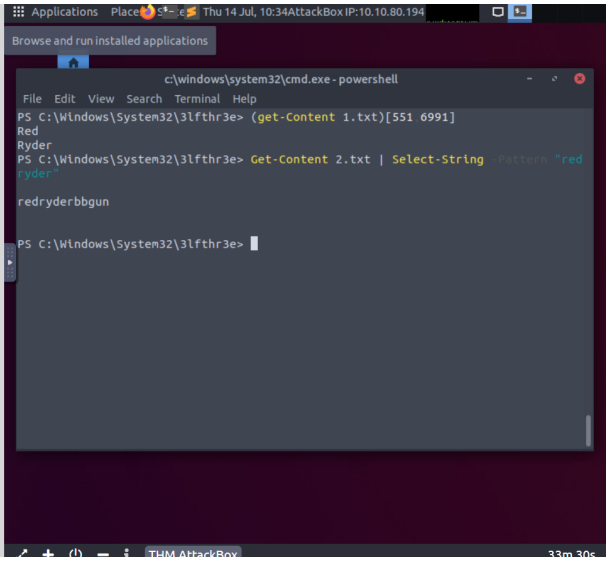
Question 6:

Wrap the command “Get-Content 1.txt” with brackets/parentheses and wrap the number 551,6991 with square brackets to get the 2 words which is red ryder.



Question 7:

Use the command “Get-Content 2.txt” with “Select-String” command on “redryder” with a specific pattern to get the full answer “redryderbbgun”.



Thought Process/Methodology:

Firstly, we start our machine and attack box to start our process. We then opened our terminal and key in “ssh -l mceager MACHINE_IP” and password “r0ckStar!” to connect to the host. We then set up Powershell and set-location for our documents. After that, we Get-ChildItem for the hidden file and got the file in the documents. We then ls the Hidden file to get another user name and we cat out “e1fone.txt” to get what Elf 1 wants which was its 2 front teeth. Secondly, we set the location for the desktop and ls the hidden folder and cat out “e70smsW10Y4k.txt” to get Scrooged as the name of the movie that Elf 2 wants. We set cd for Windows and System32 and get the hidden folder through directory by filter with “*3*” to get the length name “3lfthr3e”. We then used the command “Get content for 1.txt" by “Measure object” to get the number of words contained in the first file which is 9999 words count. We wrapped the command “Get-Content 1.txt” with brackets/parentheses and wrap the number [551,6991] with square brackets to get the 2 words which is red ryder. Last but not least, we finally used the command “Get-Content 2.txt” with “Select-String” command on “redryder” with a specific pattern to get the full answer “redryderbbgun”.