Report PSP0201 T2130 Tutorial – Week 5

Group name: **Marceline**

|  |  |  |
| --- | --- | --- |
| ID | Name | Role |
| 1211100899 | Muhammad Shahril Aiman | Leader |
| 1211101533 | Muhammad Aniq Fahmi | Member |
| 1211101303 | Aiman Faris | Member |
| 1211102759 | Muhammad Zaquan | Member |

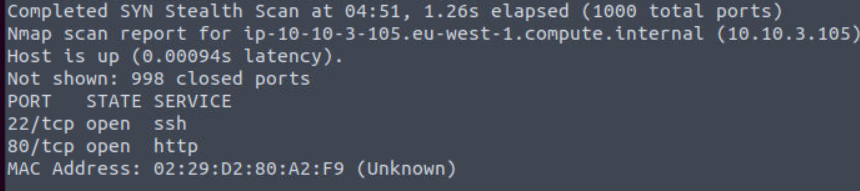
**Day 16 - Help! Where is Santa?**

**Tools used: AttackBox, Firefox, Python3**

Solution/Walkthrough:

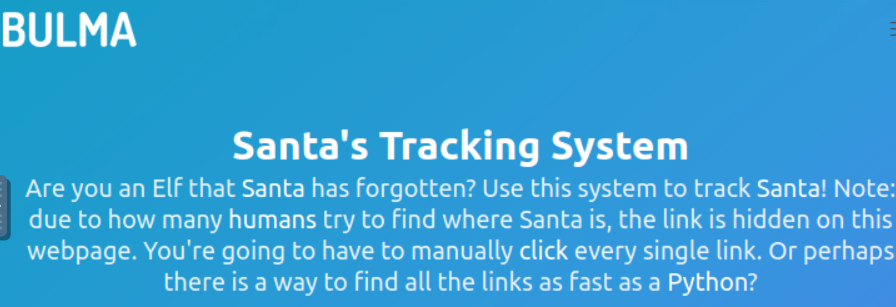
Question 1: What is the port number for the web server?

= 80



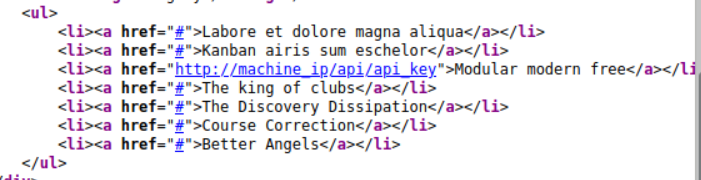
Question 2: What templates are being used?

= BULMA



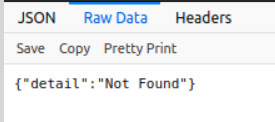
Question 3: Without using enumerations tools such as Dirbuster, what is the directory for the API?

= /api/



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

= {"detail":"Not Found"}

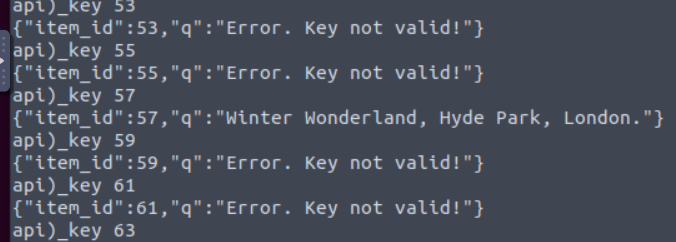


Question 5: Where is Santa right now?

= Winter Wonderland, Hyde Park, London.

Question 6: Find out the correct API key. Remember, this is an odd number between 0-100. After too many attempts, Santa's Sled will block you. To unblock yourself, simply terminate and re-deploy the target instance (10.10.94.92)

= 57



**METHODOLOGY:**

We launch the AttackBox to gain the Ip address. First of all, we scan the Ip address using nmap with setting of (-v) to obtain the port number of the web server. After that, we use Firefox and open website by searching the Ip address with the port number. It brings us to BULMA website. We view the page source to survey and find the directory API. Next, we change the endpoint API by entered no parameters in it to solve question 4. Lastly, we use python3 in the AttackBox to figure out the correct API key and Santa current location.

**Day 17 - Reverse Engineering: ReverseELFneering**

**Tools used: Kali Linux, Firefox.**

Solution/Walkthrough

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

**Answer**:

Byte 1

Word 2

Double Word 4

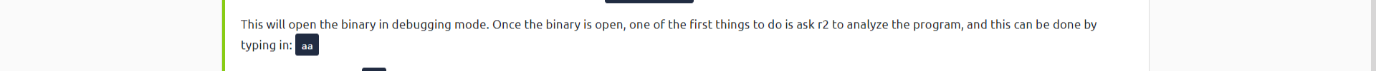
Quad 8

Single Precision 4

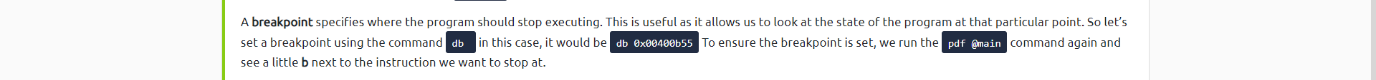
Double Precision 8

**Question 2**: What is the command to analyse the program in radare2?

**Answer**: aa

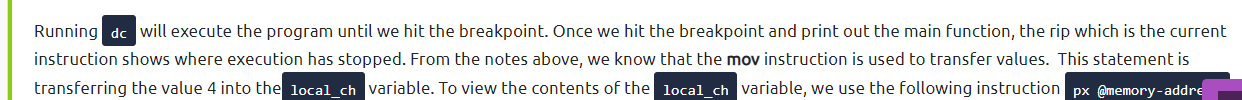


**Question 3**: What is the command to set a breakpoint in radare2?

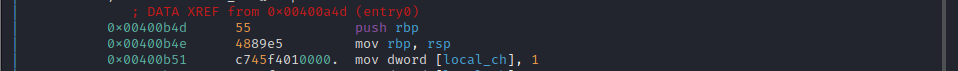
**Answer**: db

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

**Answer:** dc



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

**Answer**: 1

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

**Answer**: 6Graphical user interface

Description automatically generated

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

**Answer**:6

Graphical user interface, text

Description automatically generated

**METHODOLOGY**

We deploy the Virtual Machine and the Kali Linux and directly open Firefox to access the website. I use the Ip address that given to me. I put the code at CMD at put the Ip address at the CMD. After that, it shows that the Ip address have two file which is ./file1 and ./challenge1. I type the code to open the file ./challenge1. After that it appear the security to login the file. We’ll be using radare2 to do this - radare2 is a framework for reverse engineering and analysing binaries. We use the debugging mode for this task, so we have put the code and type “aa” So we type pdf @main and got into the data of file ./challenge1. Then, we can answer the question 5,6 and 7 using the data given to us at google form.

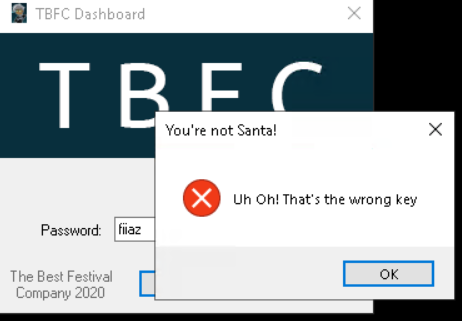
**Day 18 - The Bits of Christmas**

**Tools used: AttackBox, Remina, ILSpy, CyberChef**

Solution/Walkthrough:

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

= Uh oh! That's the wrong key



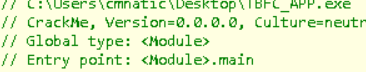
Question 2: What does TBFC stand for?

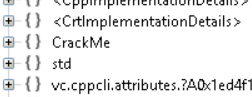
= The Best Festival Company



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

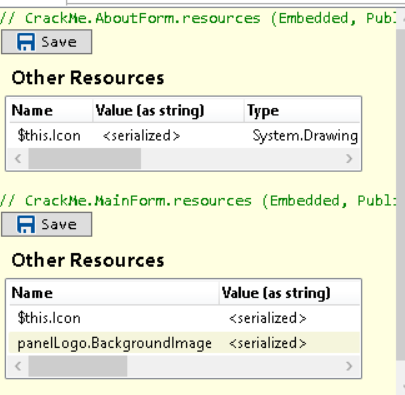
= CrackMe





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

= MainForm



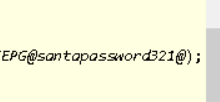
Question 5: Which method within the form from Q4 will contain the information we are seeking?

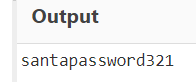
= buttonActivate\_Click



Question 6: What is Santa's password?

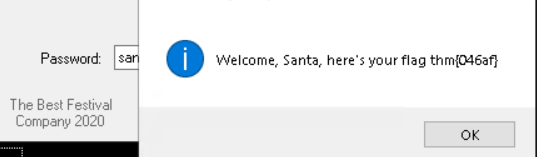
= santapassword321





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

= thm{046af}



**METHODOLOGY:**

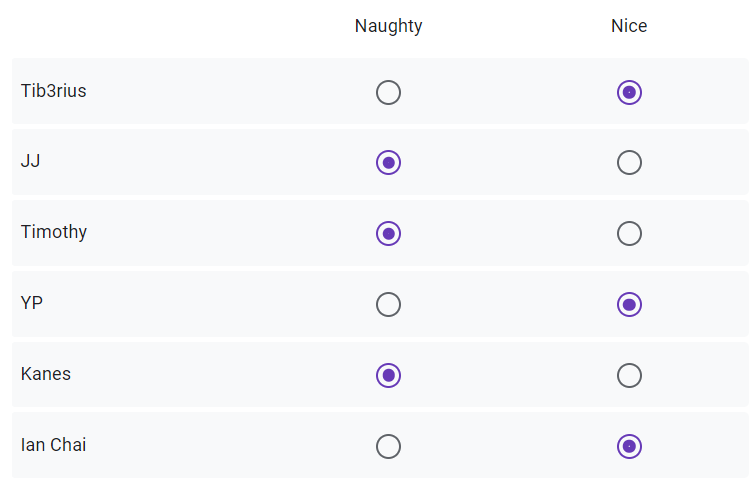
We deploy the AttackBox and VM to gain the Ip address. Then, we navigate to the "Applications" tab on the AttackBox where "Remmina" is located in the "Internet" sub-menu. Reminna will ask for a password to save sessions, we safely press "Cancel". After that, we filled out the IP address, input the Username (cmnatic) and password (Adventofcyber!) provided. Next, we open the TBFC\_APP and purposedly enter the wrong password to see what message show up. We decompile the TBFC\_APP with ILSpy and looking through resources in the ILSpy to answer the q3 until q7. We click the CrackMe file, went into MainForm file and reach to the buttonActivate\_Click source code. We finally obtain Santa’s password and the flag. To make sure the Santa’s password is real, we go to the CyberChef website and put the bytes in the input, insert Hex recipe to get its output. So in the end, we try login the TBFC\_APP by using the Santa’s password (santapassword321) and receive the flag.

**Day 19 - The Naughty or Nice List**

**Tools used: AttackBox, Firefox**

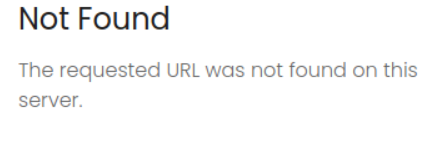
Solution/Walkthrough:

Question 1: Which list is this person on?



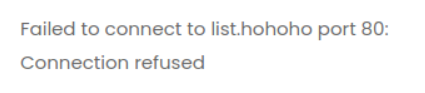
Question 2: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F"?

= Not Found. The requested URL was not found on this server.



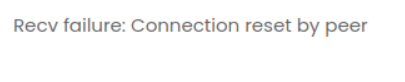
Question 3: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A80"?

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



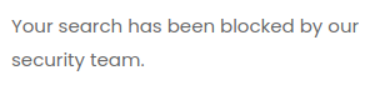
Question 4: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flist.hohoho%3A22"?

= Recv failure: Connection reset by peer



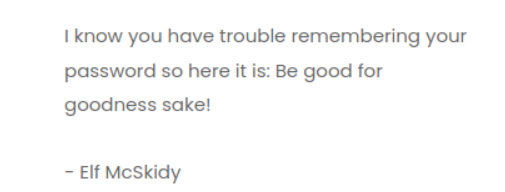
Question 5: What is displayed on the page when you use "/?proxy=http%3A%2F%2Flocalhost"?

= Your search has been blocked by our security team.



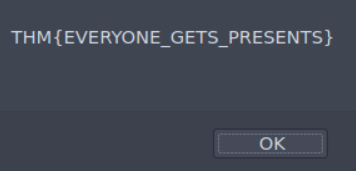
Question 6: What is Santa's password?

= Be good for goodness sake!



Question 7: What is the challenge flag?

= THM{EVERYONE\_GETS\_PRESENTS}



**METHODOLOGY:**

We deploy the Virtual Machine and the AttackBox and directly open Firefox to access the website The Naughty or Nice List by using the Ip address given by the VM. Next, we observe the website, enter a name in the form which is Santa and click the "Search" button then the page loads, and it tells us whether that name is on the Naughty List or the Nice List. We alternately test the name given in the google form to know which list is in the naughty or nice list. After that we tried to fetch the root of the same site by browsing to:(<http://MACHINE_IP/?proxy=http%3A%2F%2Flist.hohoho%3A8080%2F>) and the message shown was "Not Found. The requested URL was not found on this server." Beside that, we changed the port number from 8080 to just 80 and the message now changes to "Failed to connect to list.hohoho port 80: Connection refused". As well, we changed again the port number to 22 and now it displays "Recv failure: Connection reset by peer". Last but not least, we replaced the list.hohoho hostname with "localhost" the message returned says "Your search has been blocked by our security team." Finally, we access the local services by set the hostname in the URL to "list.hohoho.localtest.me" and quicken to finish the task by log in the admin use the Santa as the username and the password given by Elf McSkidy.

**Day 20 - PowershELlF to the rescue**

**Tools used: AttackBox**

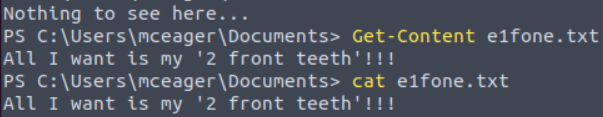
Solution/Walkthrough:

Question 1: Check the ssh manual. What does the parameter -l do?

= local host

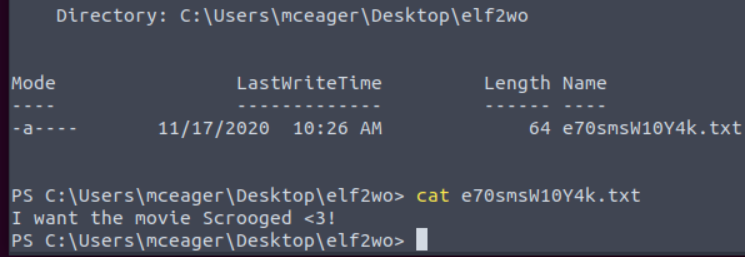
Question 2: Search for the first hidden elf file within the Documents folder. Read the contents of this file. What does Elf 1 want?

= 2 front teeth



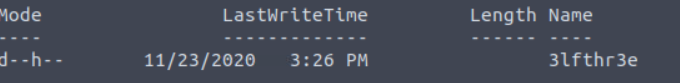
Question 3: Search on the desktop for a hidden folder that contains the file for Elf 2. Read the contents of this file. What is the name of that movie that Elf 2 wants?

= Scrooged



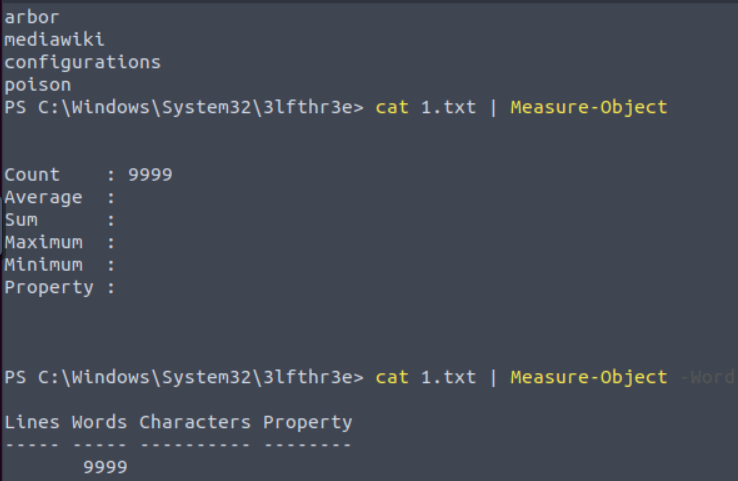
Question 4: Search the Windows directory for a hidden folder that contains files for Elf 3. What is the name of the hidden folder?

= 3lfthr3e



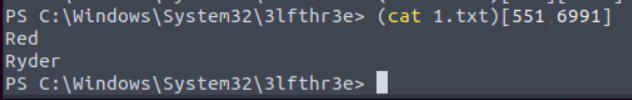
Question 5: How many words does the first file contain?

= 9999



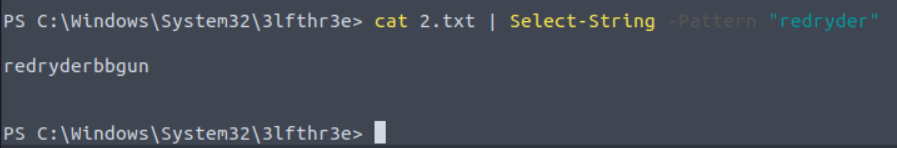
Question 6: What 2 words are at index 551 and 6991 in the first file?

= Red Ryder



Question 7: 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



**METHODOLOGY:**

We deploy the AttackBox as usual to receive the Ip address. We have been tasked to use SSH to connect to the remote machine by using command (ssh -l mceager MACHINE\_IP) and then we enter the password given (r0ckStar!). We proceed to launch the PowerShell and navigate the documents folder. Furthermore, we use Get-ChildItem cmdlet to enhance its capabilities and list the contents of the current directory that we are in. Other than that, we also make use of another useful cmdlet which is Get-Content or cat to read the contents of a file and Set-Loaction cmdlet to change directories. In the end, we directly solved the task.