PSP0201
Week 5
Writeup

Group Name: Undecided

Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha binti Muhd Firdaus	Member

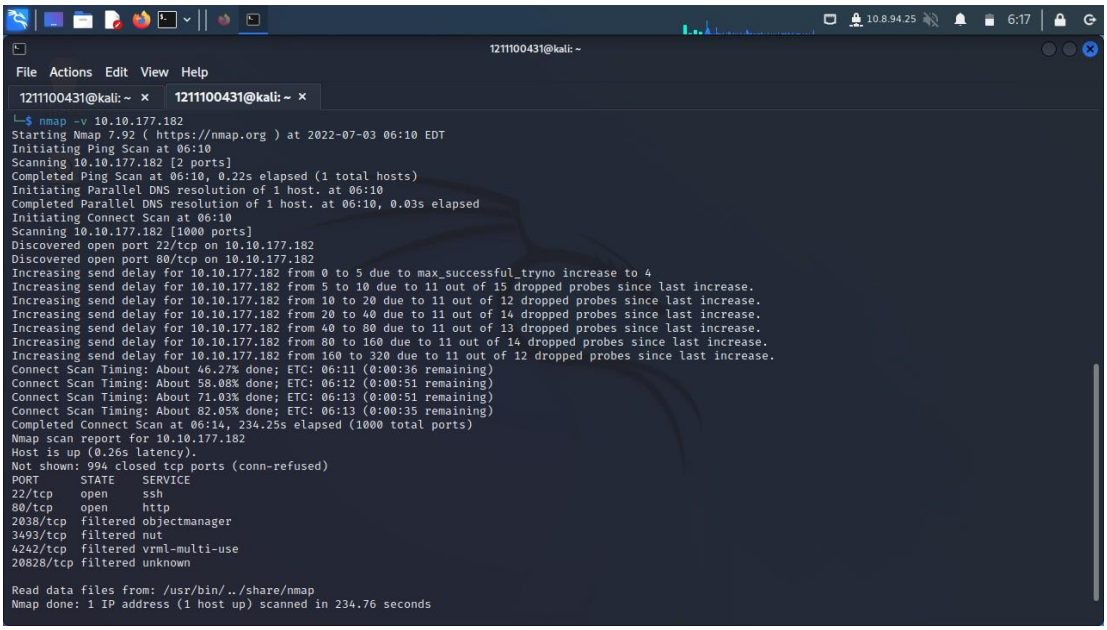
Day 16 : Scripting – Help! Where is Santa?

Tools used: Attackbox, Firefox

Solution/walkthrough:

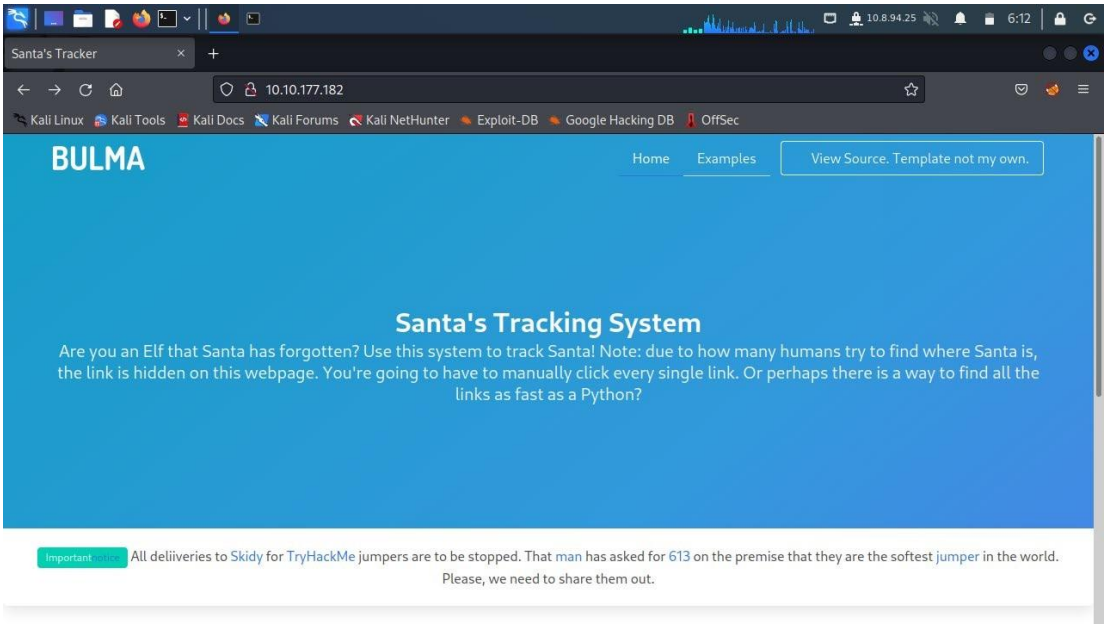
Question 1

By using the nmap command in the terminal we found the open port which is 22 and 80 as shown in the picture from the list of port, state, and service.



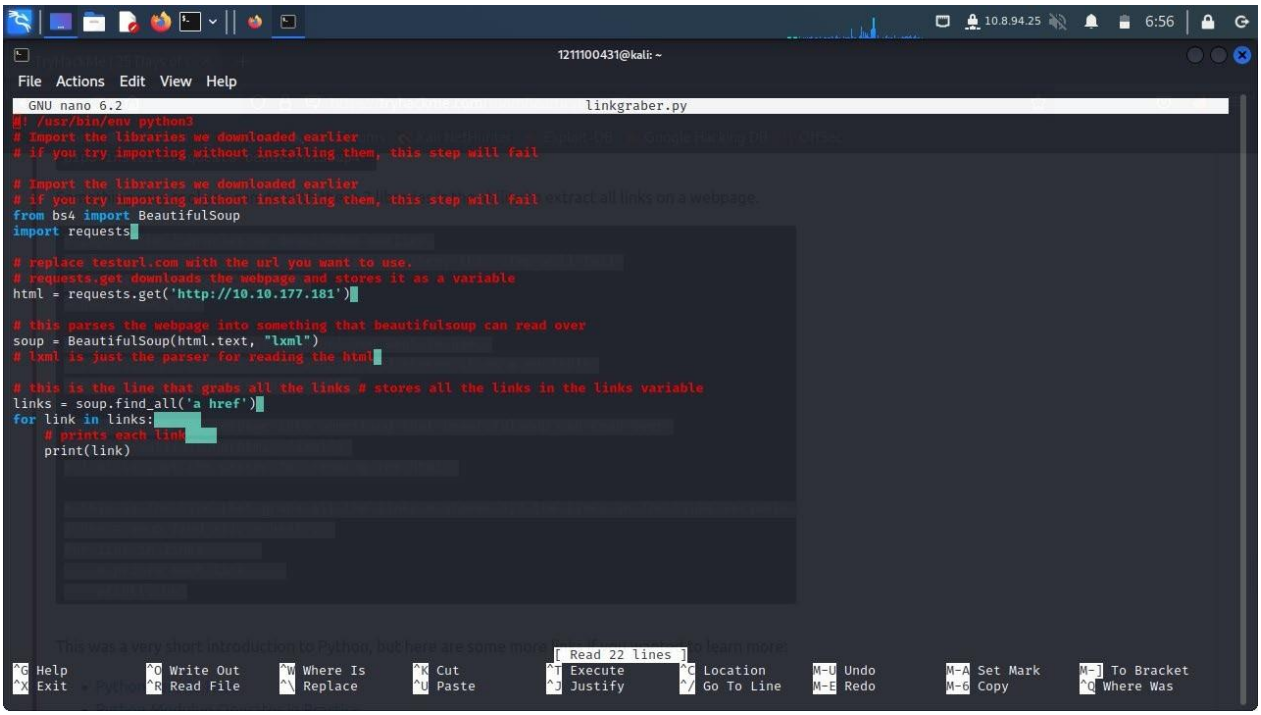
Question 2

We browse the IP address from the machine and was led to this website. Here, we found the templates that is being used.

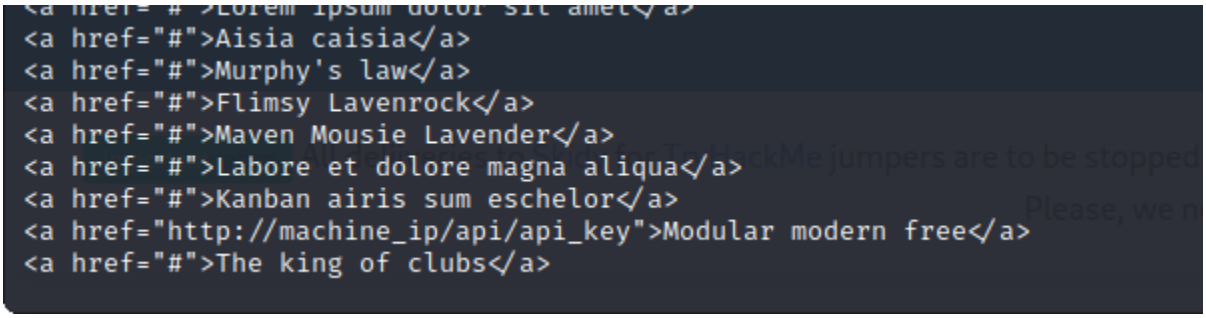


Question 3

Next, we were ordered to find the api directory. We repurpose the python code that we had used before in day 15 to find the api directory.

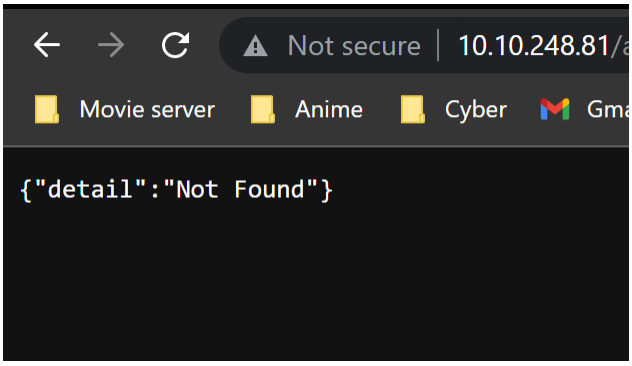


After running this python code, we receive the following output where we found the api directory.



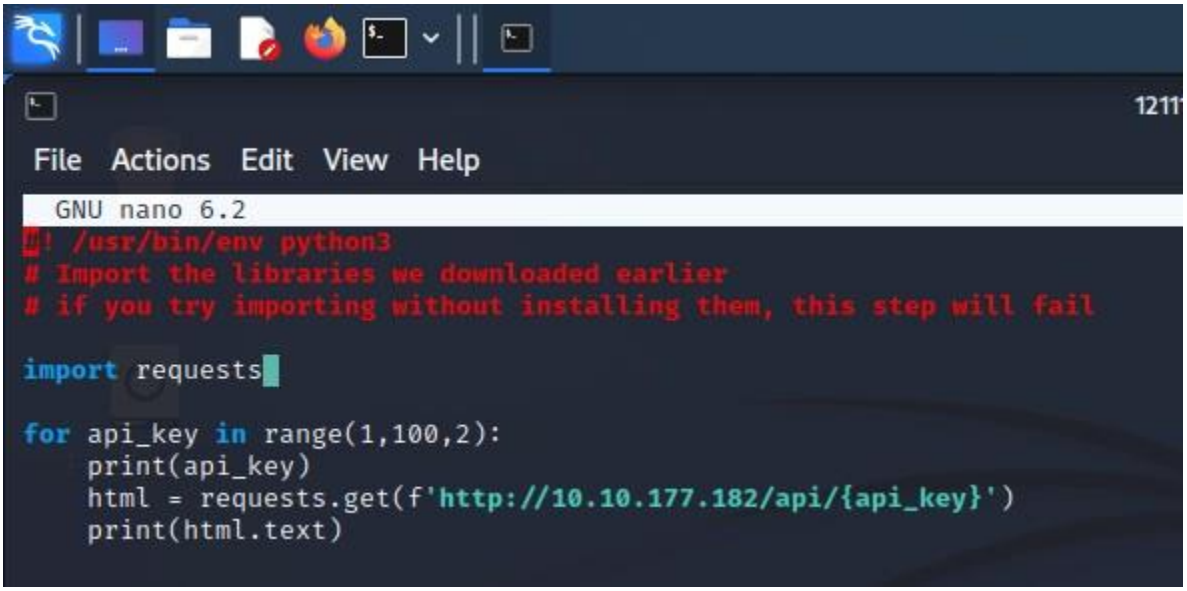
Question 4

We are asked to check what do we get if we don't add any parameters after api.

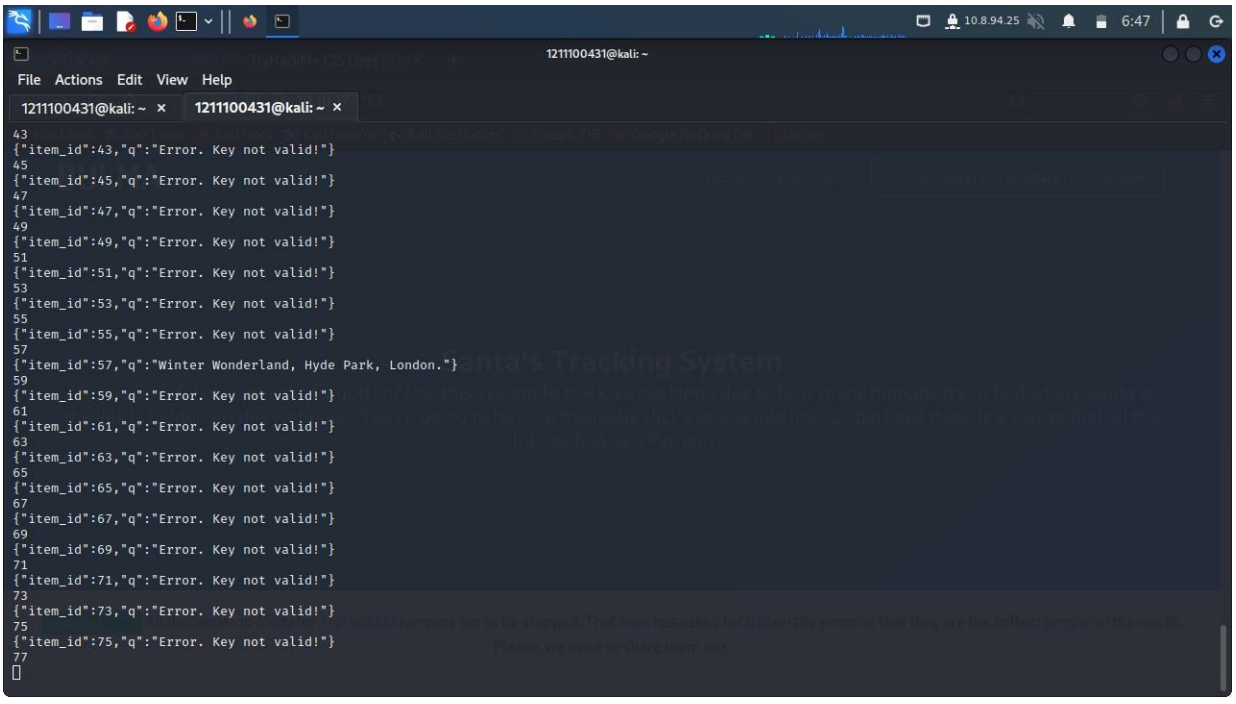


Question 5 & 6

Here we do know the api directory but not the api key, so now we need to find the api codes to find Santa's location. However, we are told that api key is between 0-100 and it's an odd number. So, we can use the codes again to automate the process.



When we run this, we got the result as shown, you can see code 57 is the key and Santa is currently in Winter Wonderland, Hyde Park, London.



Thought Process/Methodology:

At the beginning we used nmap to find information about the IP, where we were able to find that ports 22 and 80 is open. When we added this in the URL with the IP address, we were redirected to a website called Santa's tracking system. On the website, we found the templates that is being used. Next, we were ordered to find the api directory. We repurpose the python code that we had used before in day 15 to find the api directory. Next, we checked for the output when we do not add any parameters after api in raw data. Afterward, to find Santa's position, we utilize the python code that we had earlier to find his location, and which is the api key to find Santa. Although there was a chance that the system would block us if there were too many wrong inputs, we were told that the api key is in between 0-100 and that it is an odd number so it narrows down our search significantly. After running the python code, we found that Santa was in Winter wonder, Hyde Park, London and the api number was 57.