PSP0201 Week 3 Writeup

Group Name: Hacktocrats

Members

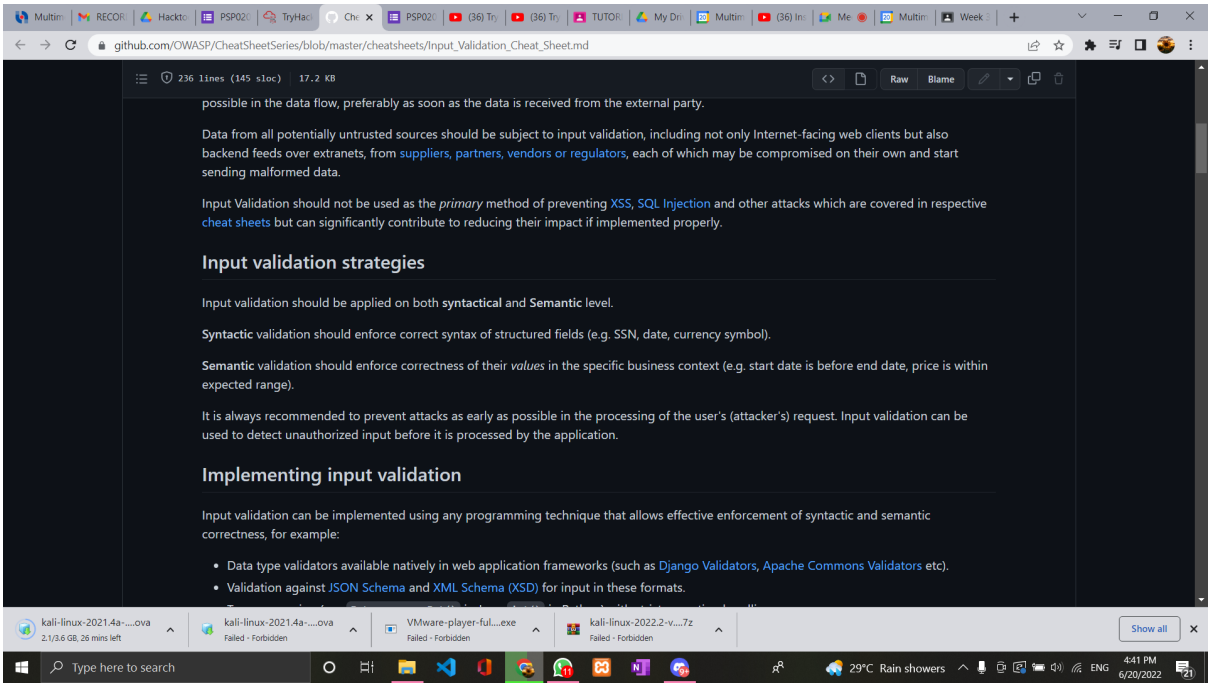
ID	Name	Role
1211103194	NUR FARAHIYA AIDA BINTI ABD RAZAK	Leader
1211103602	NUR ALIA AMELISA SYAZREEN BINTI MOHD SULEI	Member
1211103430	AINA SOFEA BINTI AMIER HAMZAH	Member
1211103237	NURUL AIN BINTI KAMARUDIN	Member

DAY 6 : Web Exploitation - Be Careful With What You Wish On A Christmas Night

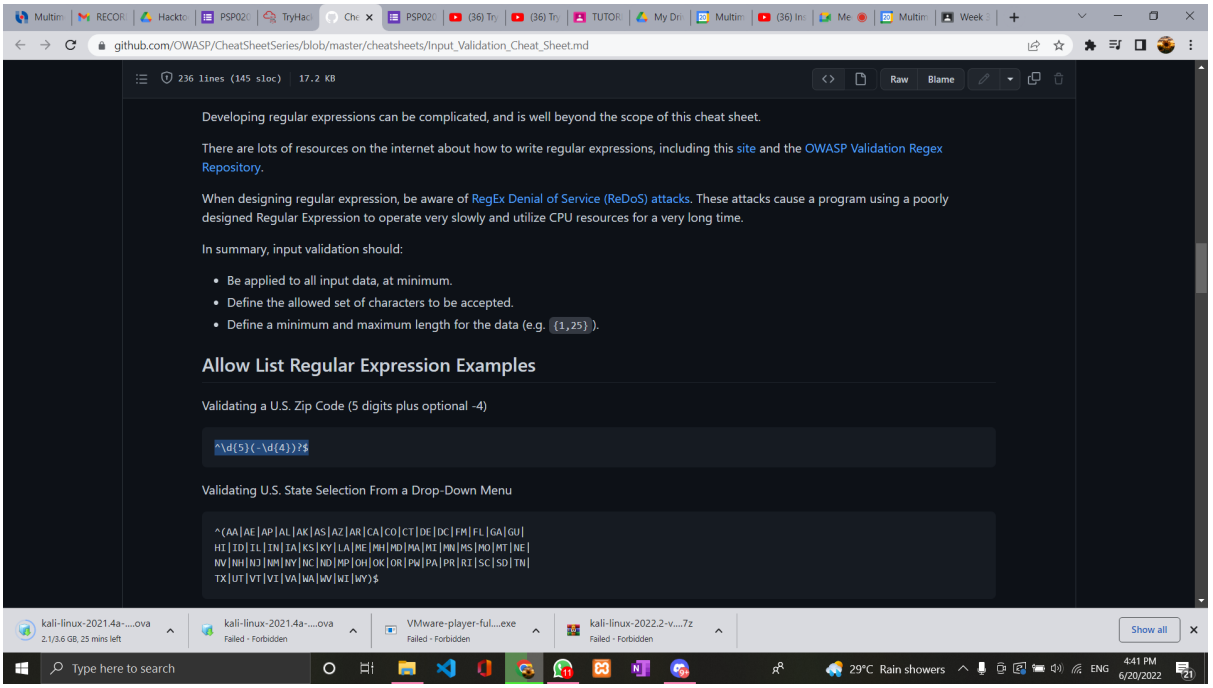
Tools used: Kali Linux, Firefox, Google Chrome

Solution/Walkthrough:

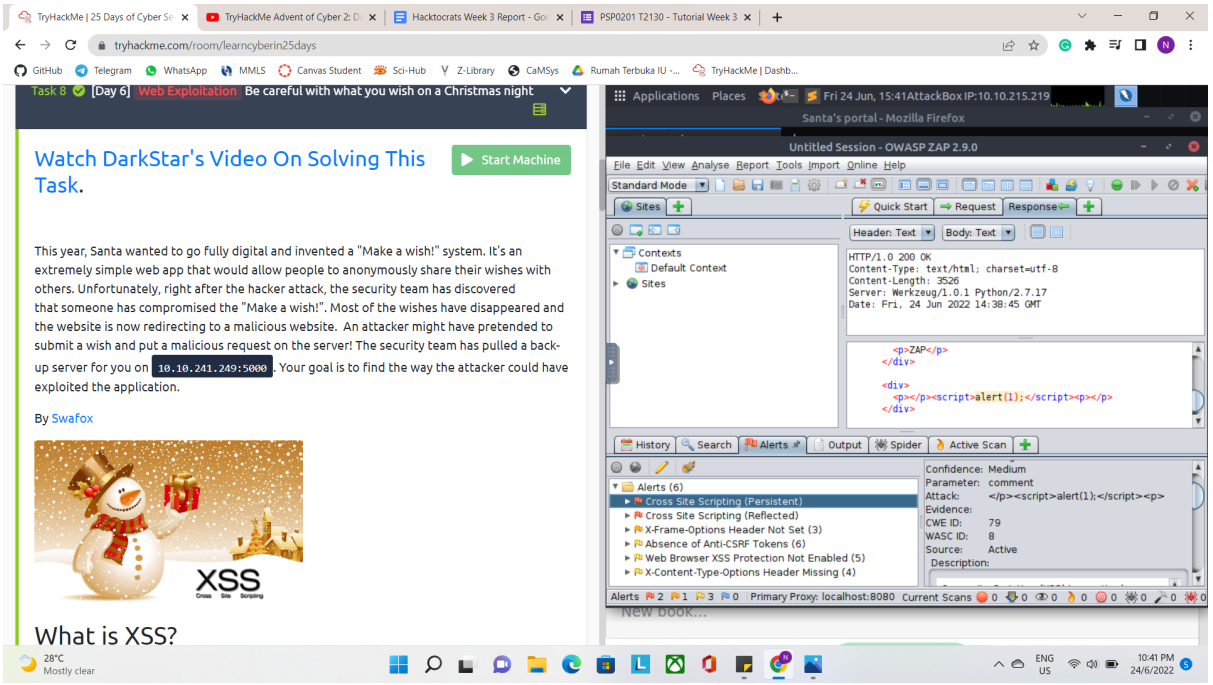
Question 1: Open OWASP Cheat Sheet on google chrome to read and match the correct description with its input validation level



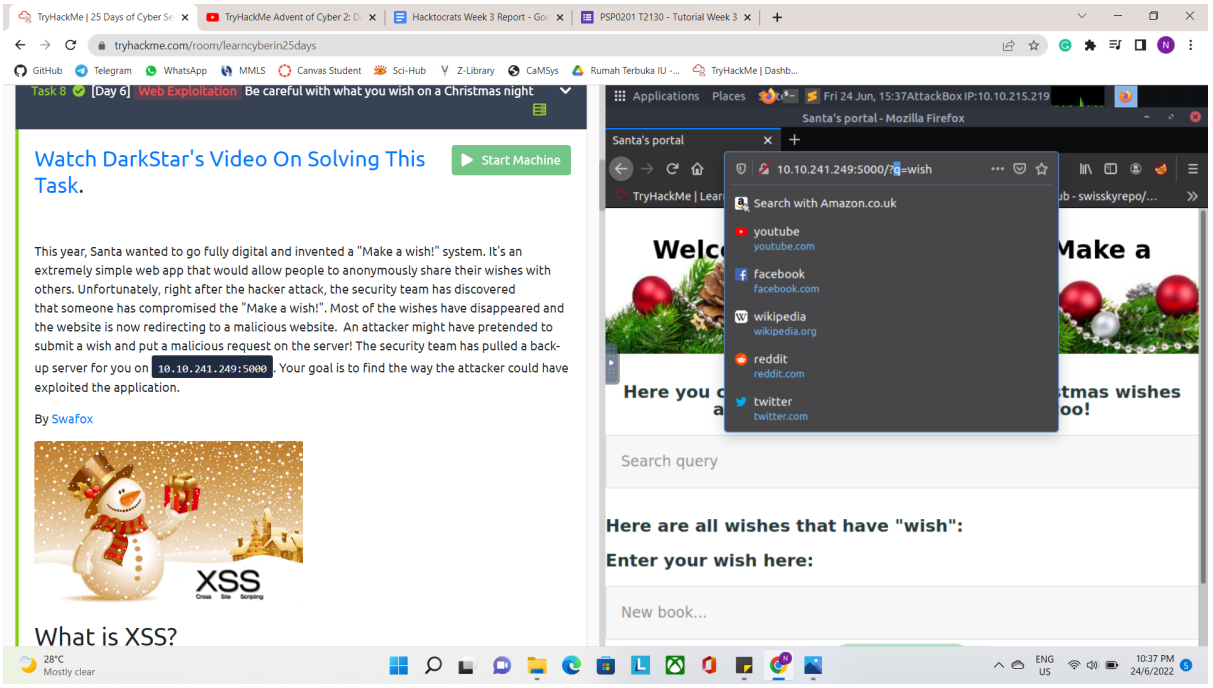
Question 2: Browse through OWASP Cheat Sheet to find the regular expression used to validate a US Zip code



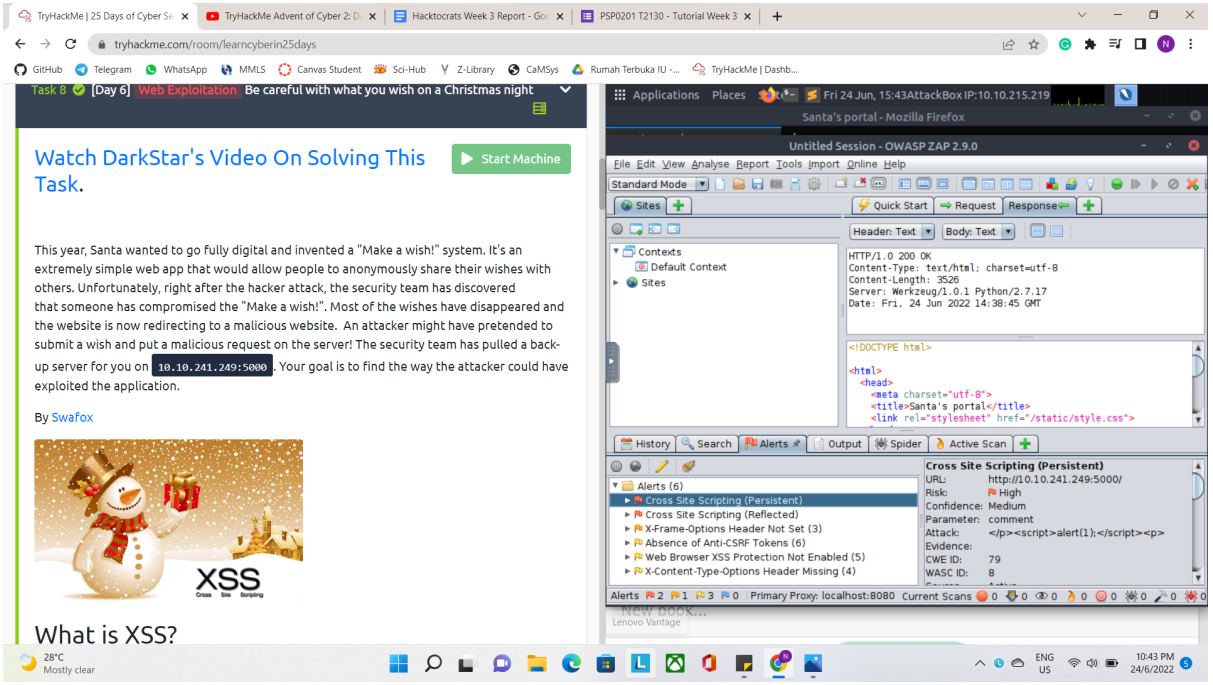
Question 3: Finding vulnerability type used to exploit the application using OWASP ZAP and found stored XSS inside <p> tag and <script> tag

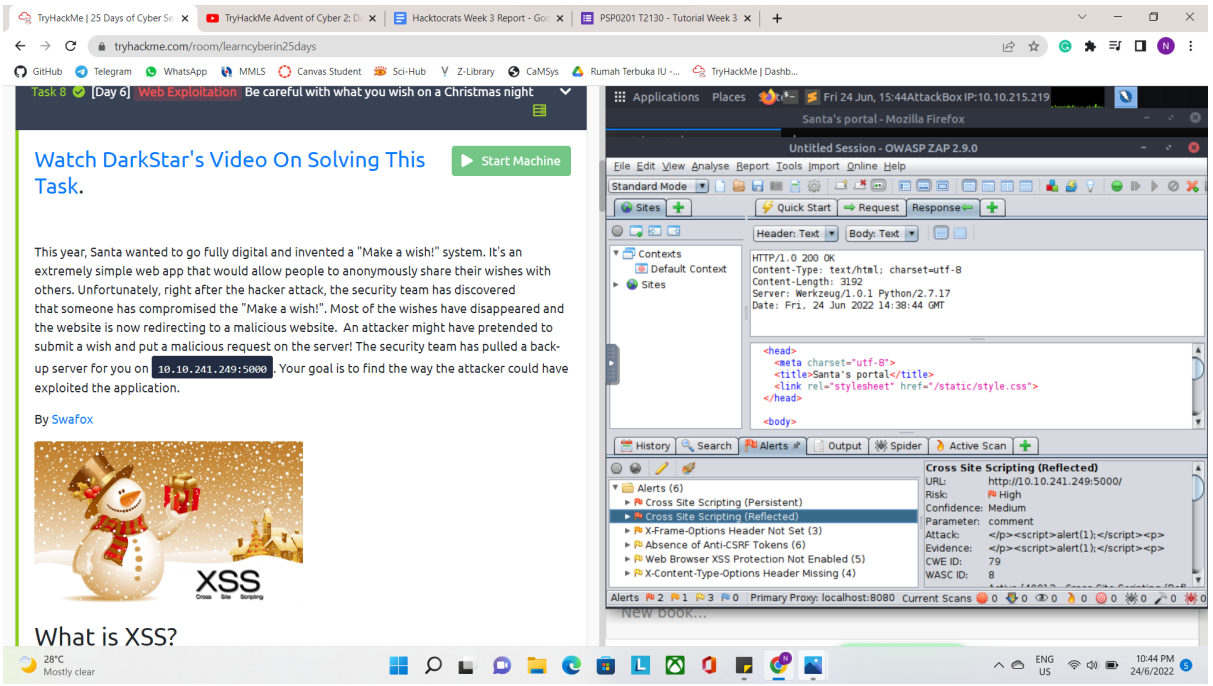


Question 4: Insert random words in christmas wish input and found the query string that can be abused to craft reflected XSS in the webpage

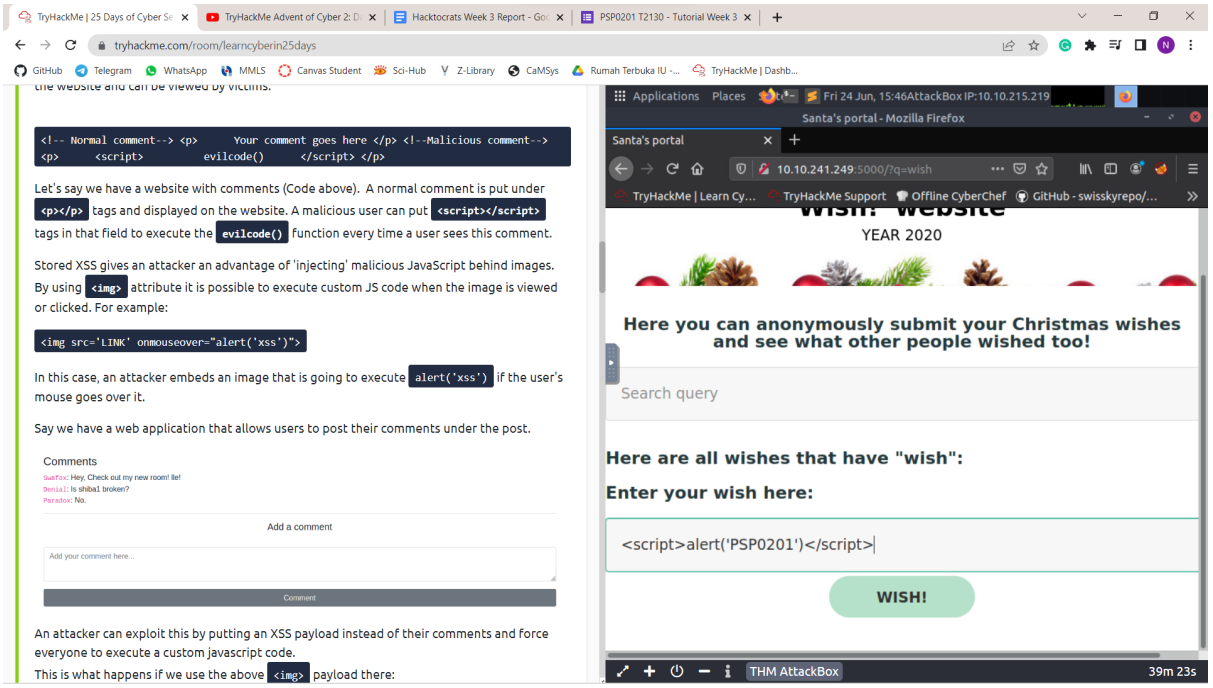


Question 5: After running automated scan on Zaproxy, two types of XSS alerts were found which is Persistent Cross Site Scripting (Stored XSS) and Reflected Cross Site Scripting

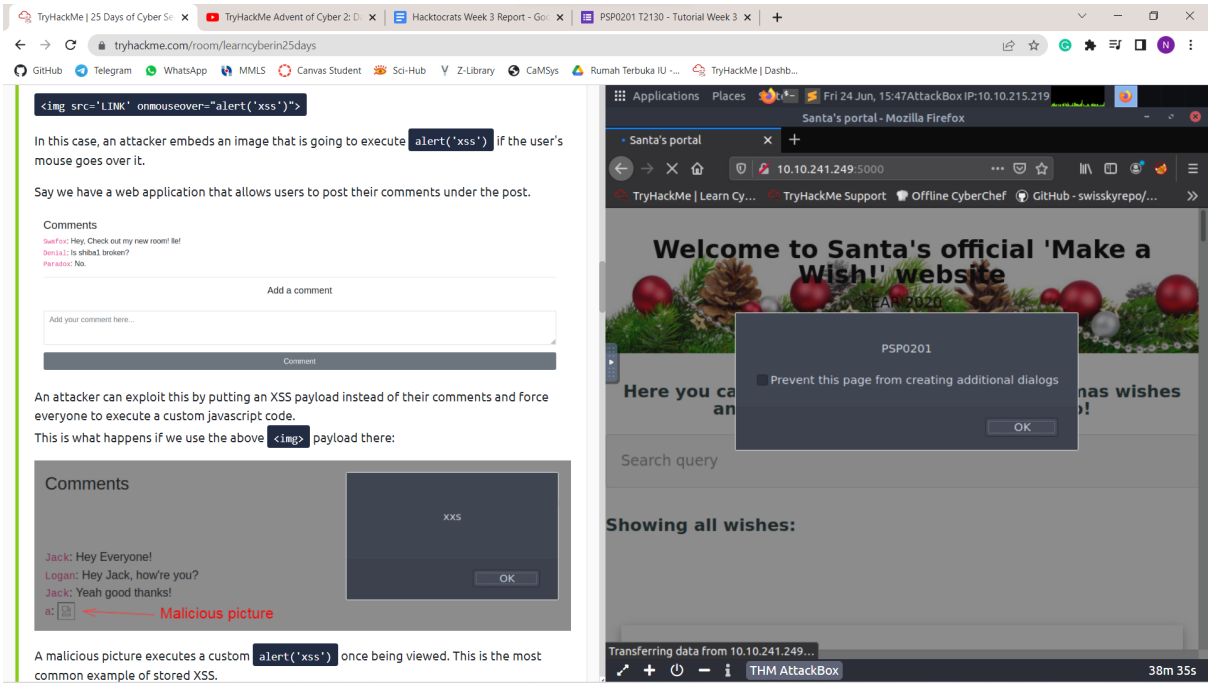




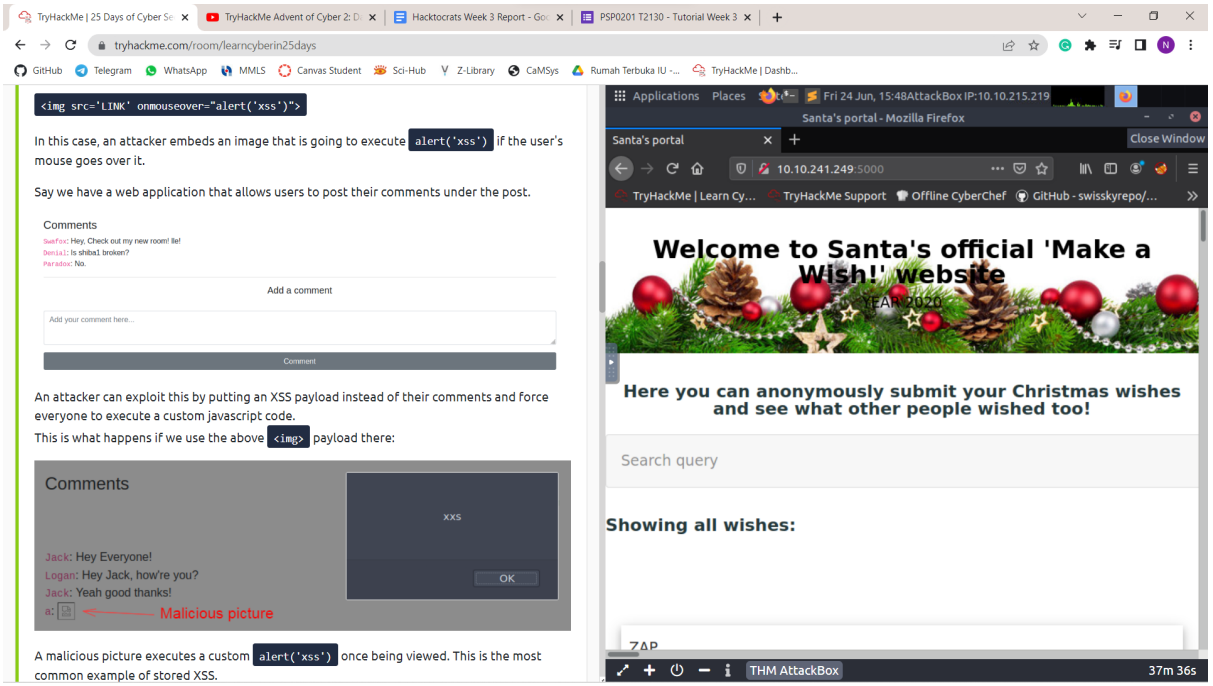
Question 6: Implementing stored XSS by inserting malicious Javascript code into Wish text box

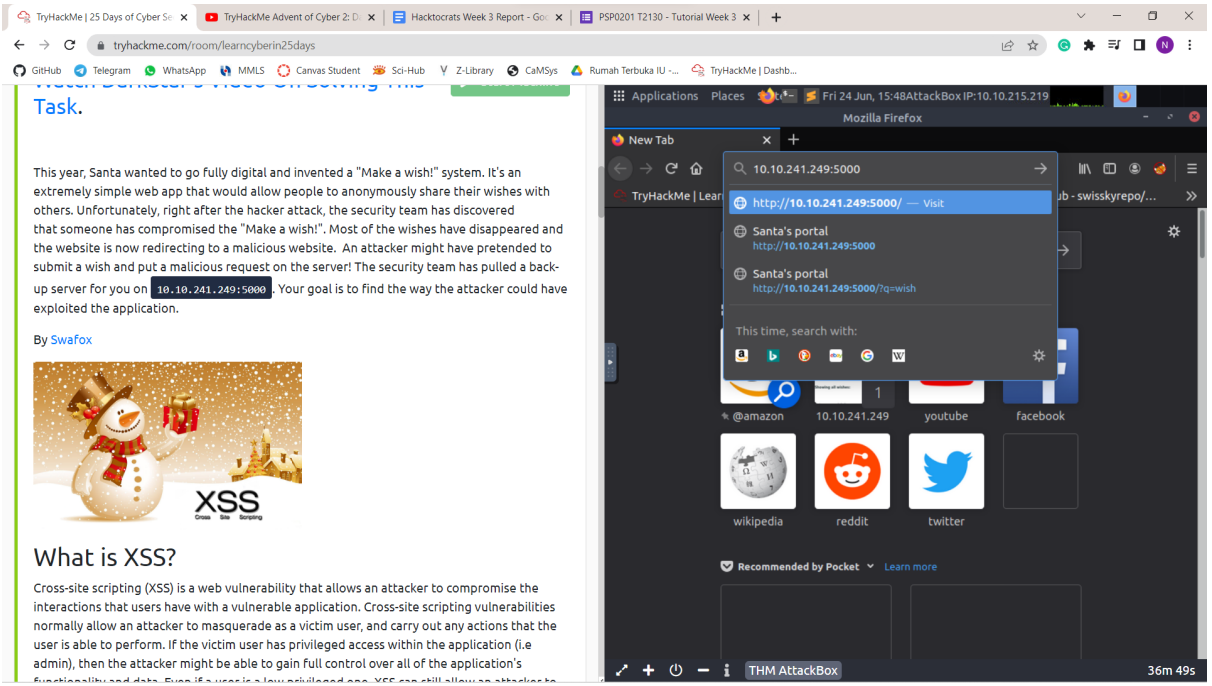


Once code entered, command was executed and alert box appeared on the screen

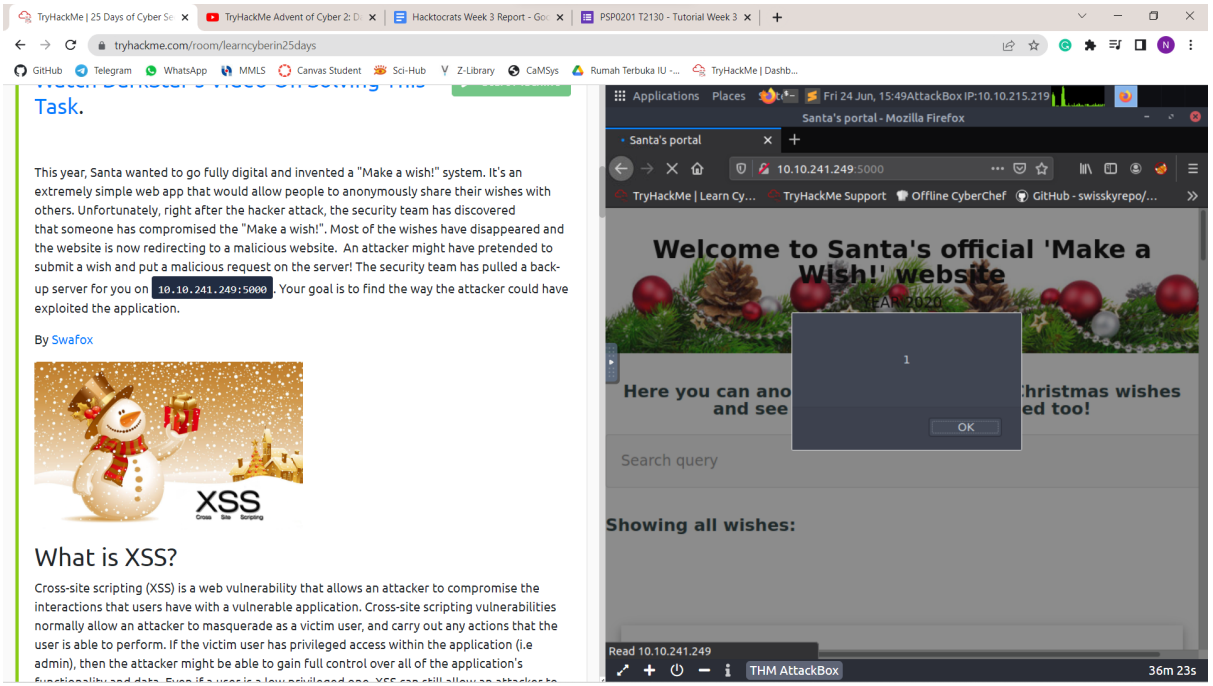


Question 7: Closing the browser and revisit the website





XSS attack persist by displaying alert box as soon as we revisit the webpage



Thought Process/Methodology:

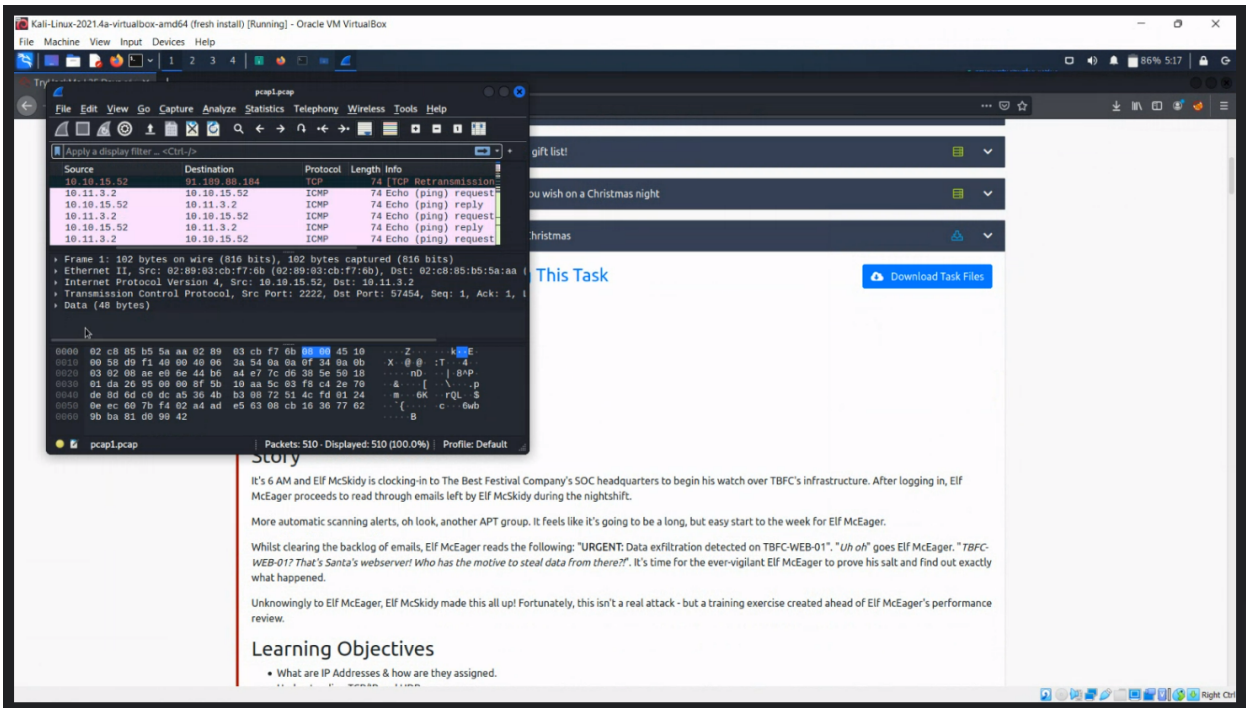
After gaining access to the backup server, we performed an automated scan in OWASP Zaproxy to find vulnerabilities in the web application. The scan showed a few vulnerabilities inside the web application including Stored Cross-Site Scripting and Reflected Cross-Site Scripting. Both were classified as high risk vulnerabilities. By using OWASP Zaproxy, we also found XSS payload written inside the comment parameter of the Javascript code. We wrote our own XSS payload in the wish text box and caused an alert box displaying ‘PSP0201’ to appear. This proved that a malicious code has been stored in the web application. After that, we close the web browser and revisit the webpage to see if the attack persists. An alert box popped up as soon as the web page load, signalling us that the XSS attack will continue even if we re-open the web application.

DAY 7 : Networking- The Grinch Really Did Steal Christmas

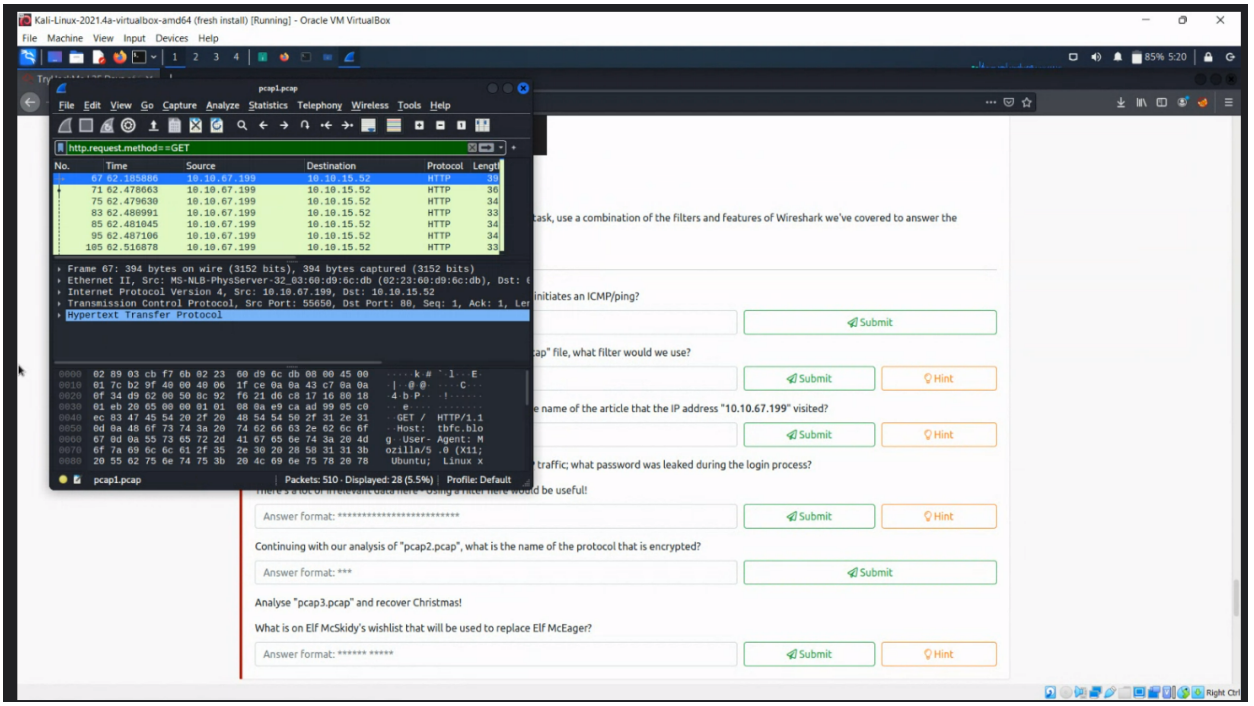
Tools used: Kali Linux, Wireshark

Solution/Walkthrough:

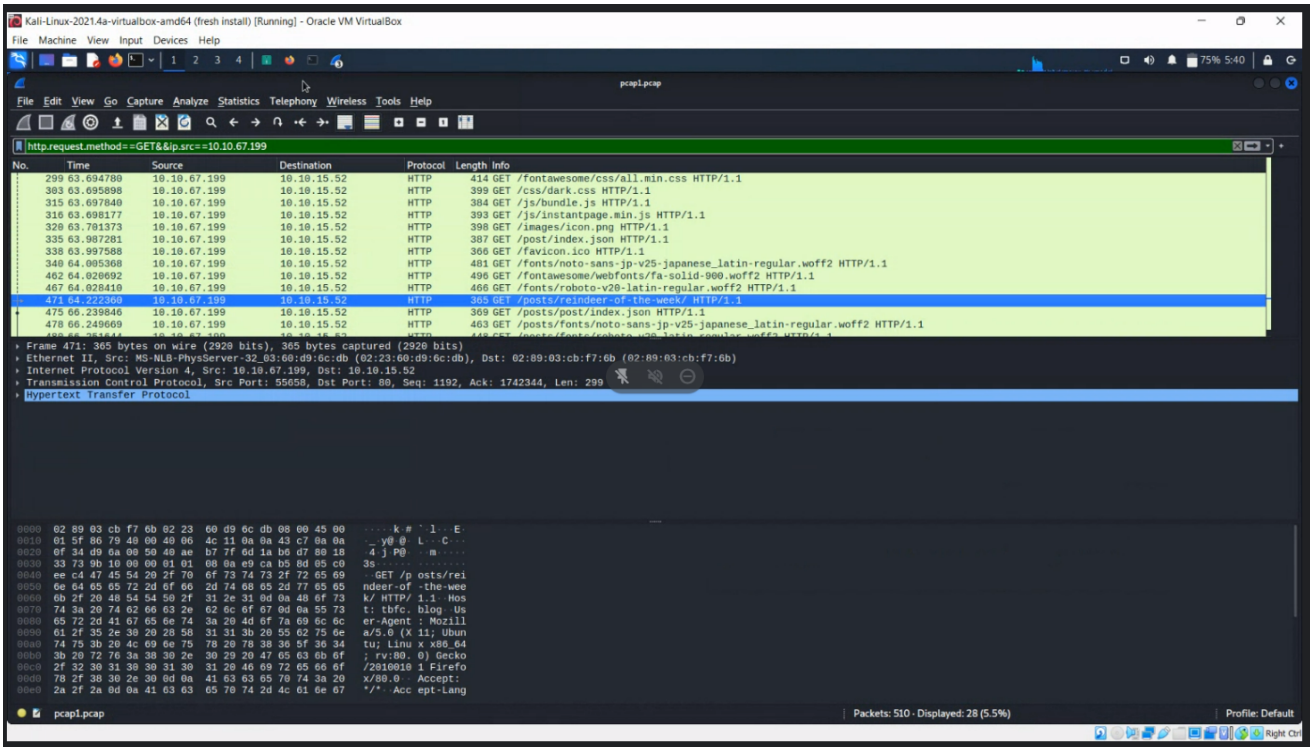
Question 1: Open “pcap1.pcap” in Wireshark and analyse through the protocol to find the first file of ICMP/ping



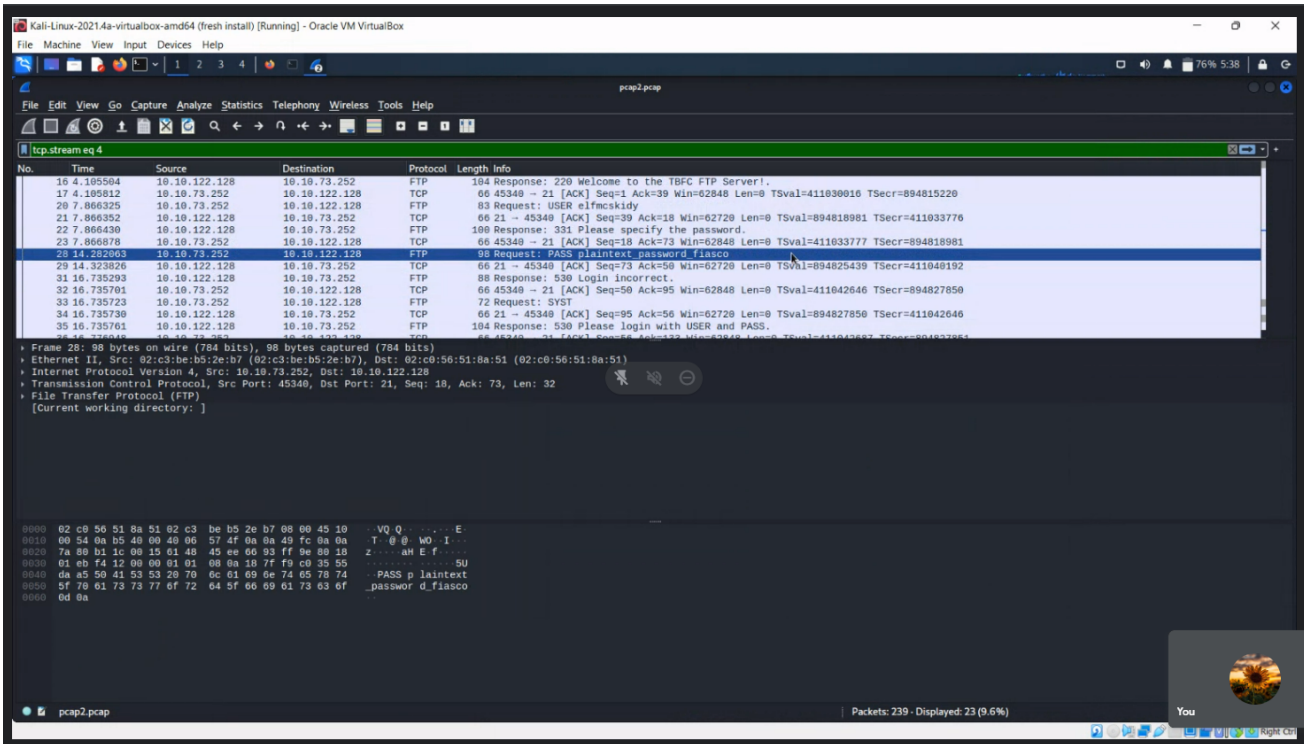
Question 2: Apply “http.request.method == GET” in the filter box to see files with HTTP GET requests only



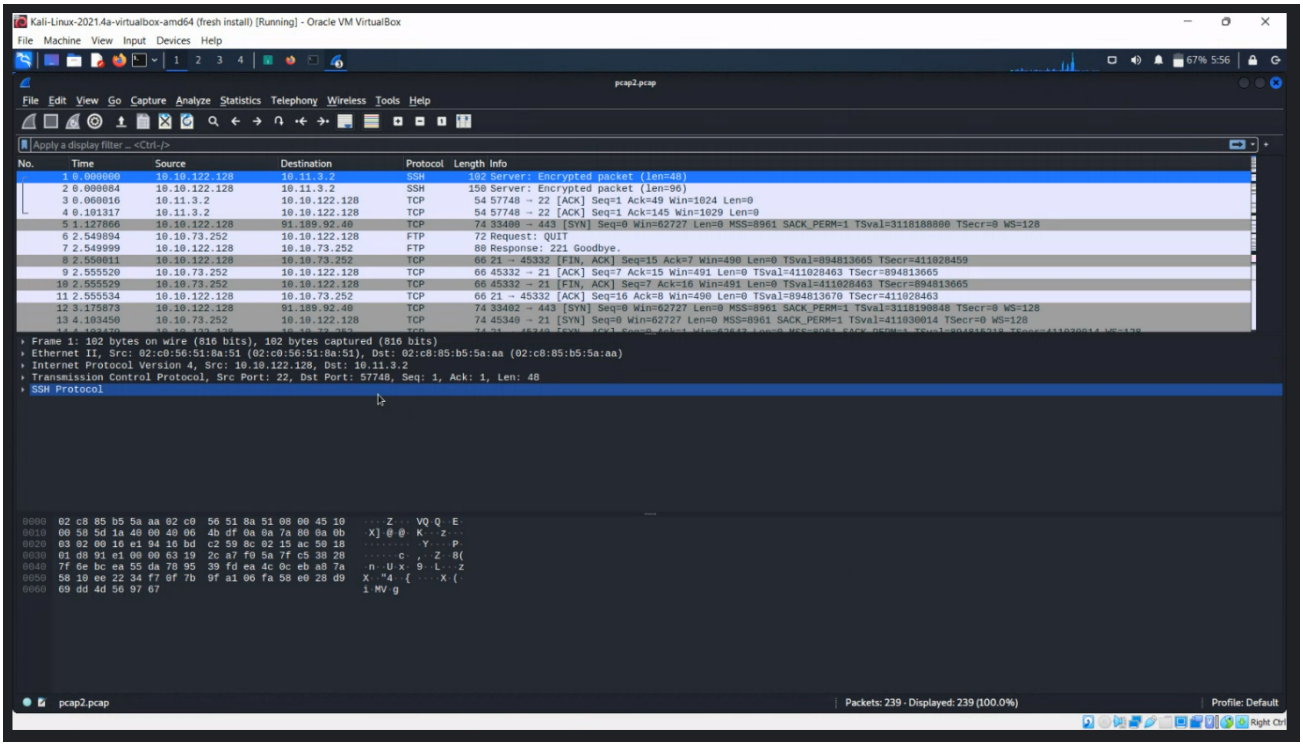
Question 3: Add “ip.src” filter alongside the ip address we are searching for to get the name of the article that IP address "10.10.67.199" visited



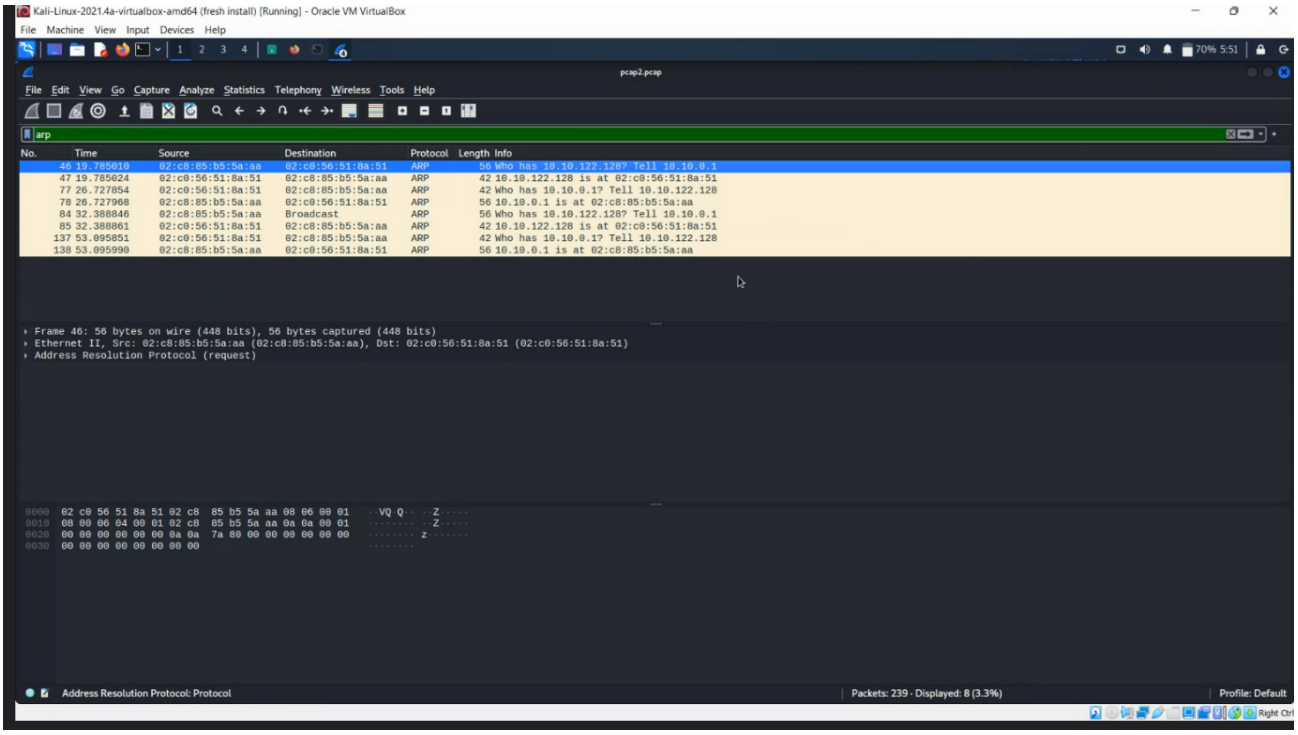
Question 4: We use filter “tcp.port == 21” to find the files with FTP protocol and analyse through the files to get the leaked password during login process



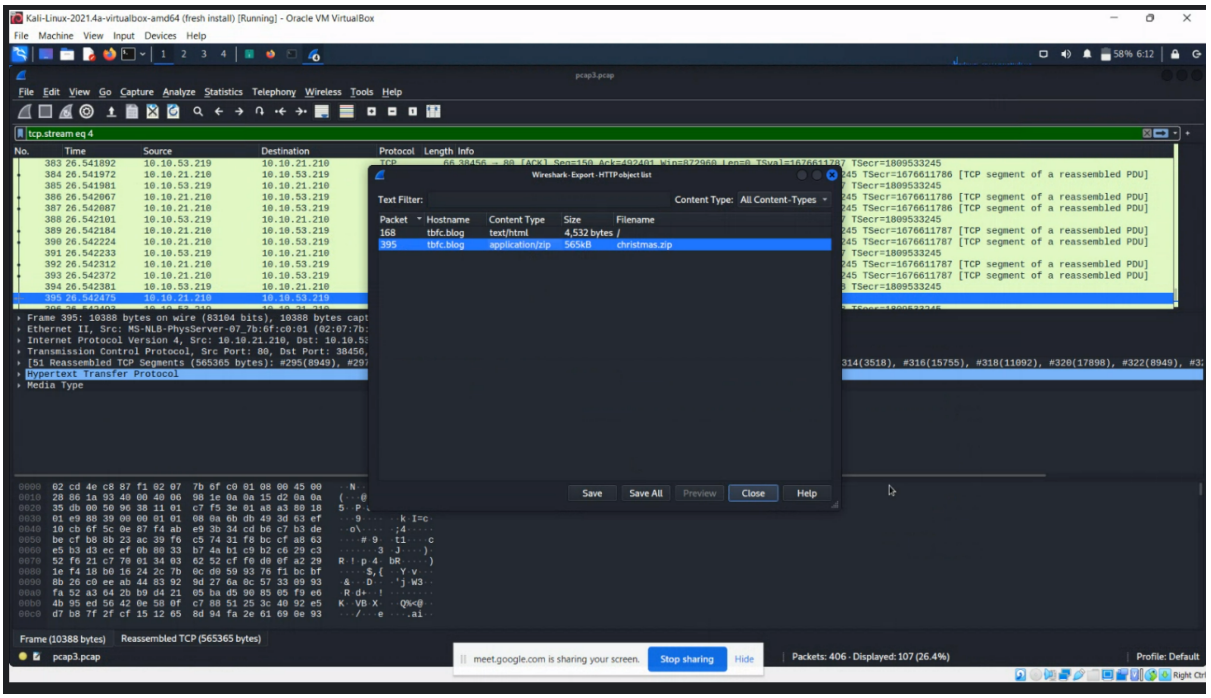
Question 5: Browse through the info section to find files that is encrypted and the name of the protocol



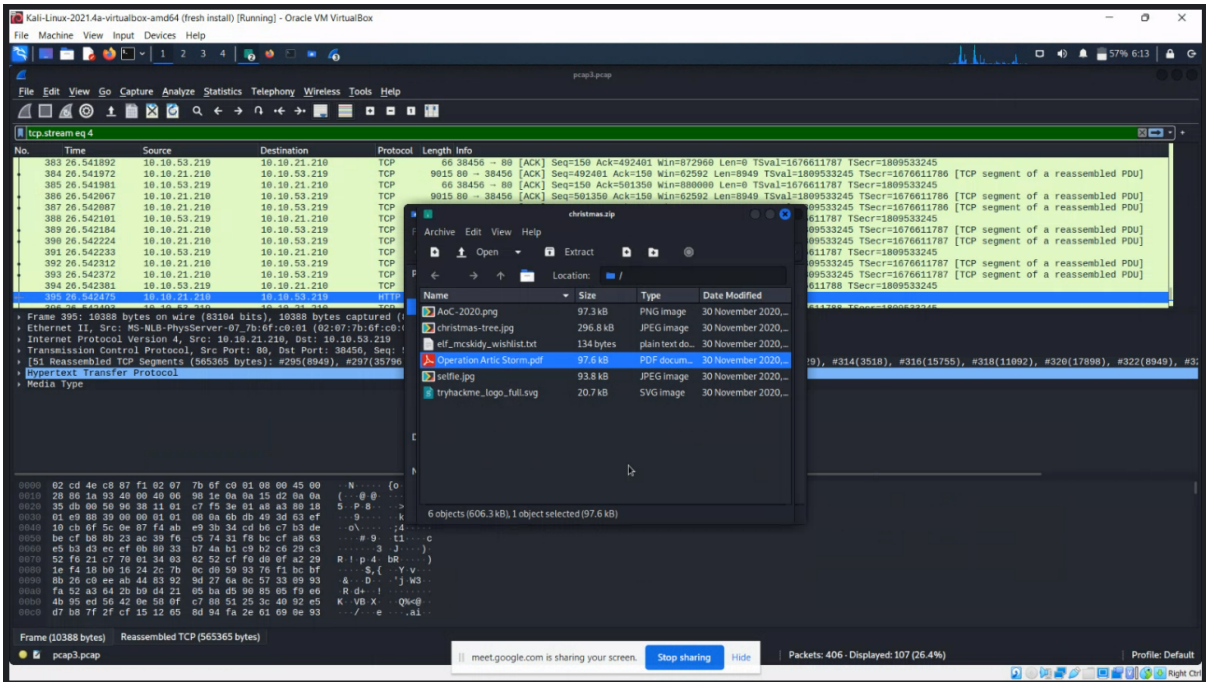
Question 6: Insert “arp” keyword into the filter box to see files with ARP protocol only and search for the destination of IP address 10.10.122.128



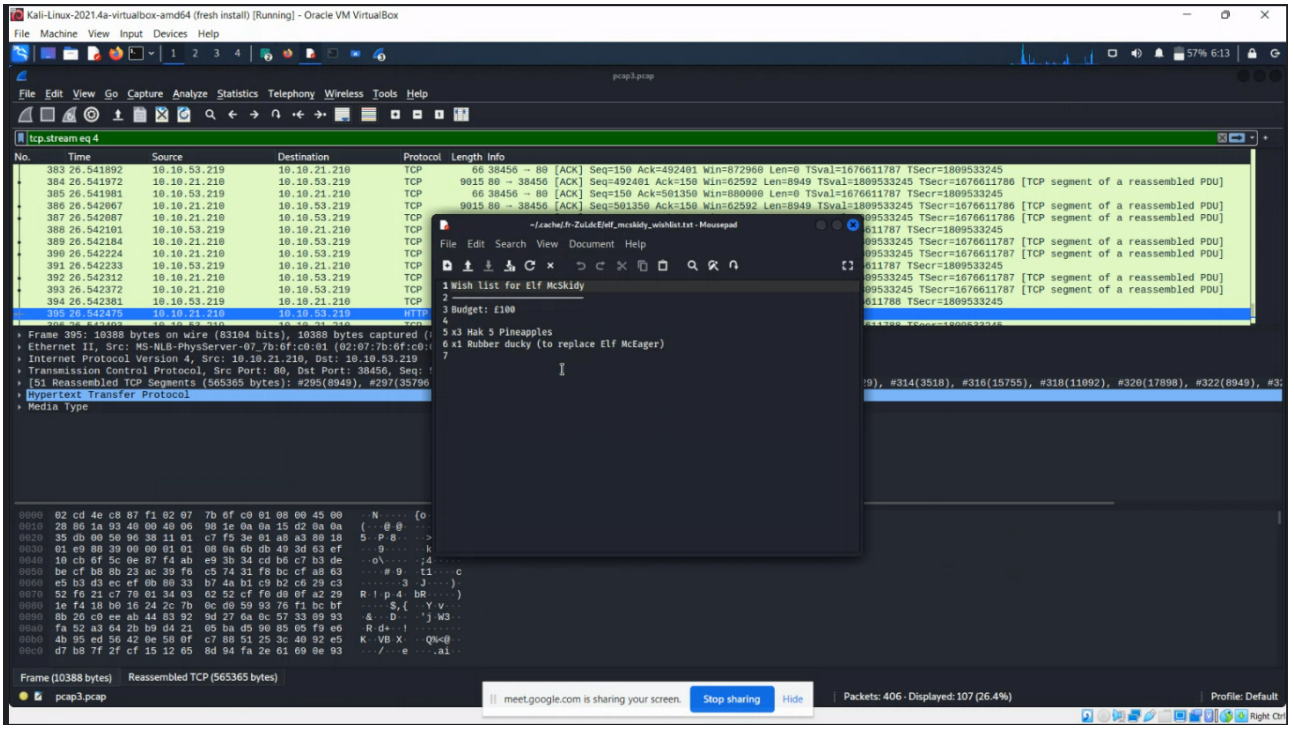
Question 7: Analyse through the info section and found a zip file with HTTP protocol. Continue to export the zip file into our local machine



Open the zip file and view elf_mcskidy_wishlist.txt



Successfully obtain object that will be used to replace Elf McEager



Question 8: Open “Operation Arctic Storm.pdf” in the zip file to find the author of the pdf

Thought methodology / process:

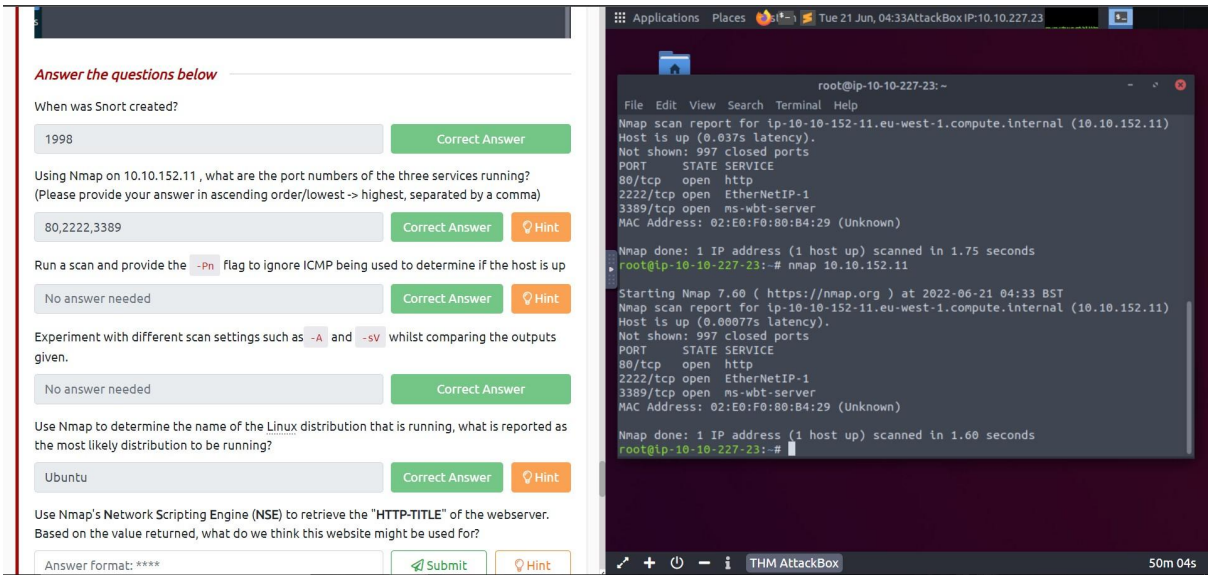
Day 7 tasks were done solely on Wireshark. First of all, we need to extract zip files containing recorded logs of all packets received and sent on a computer’s network. After that, we opened the files in Wireshark to view all recorded logs including their protocols, source ip address and destination ip address. We used a filter box provided to facilitate the search process. “ip.src”, “http.request.method == GET'', and “tcp.port == 21” were some of the filters and operators that we used to filter irrelevant data. “http.request.method == GET '' allows us to view data with HTTP protocol only. By using HTTP GET request and “ip.src” filter, we were able to find the name of the article that targeted the ip address visited. Other than that, we used “tcp.port == 21” filter to find all data with FTP protocol and proceed to find the leaked password. We also use single words as keywords such as “arp '' to see data with ARP protocol only. Last but not least, we utilise the info section to find the zip file containing Elf McSkidy wishlist and successfully view the content of the zip file.

DAY 8: What's Under the Christmas Tree?

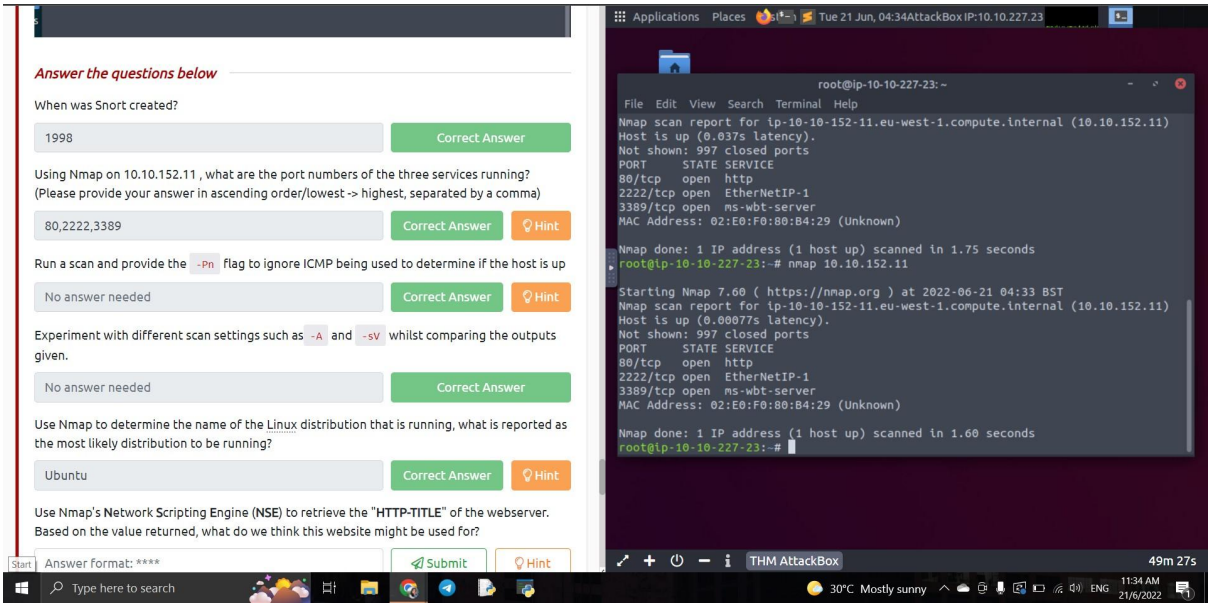
Tools used: Terminal, pf sense

Solution/Walkthrough:

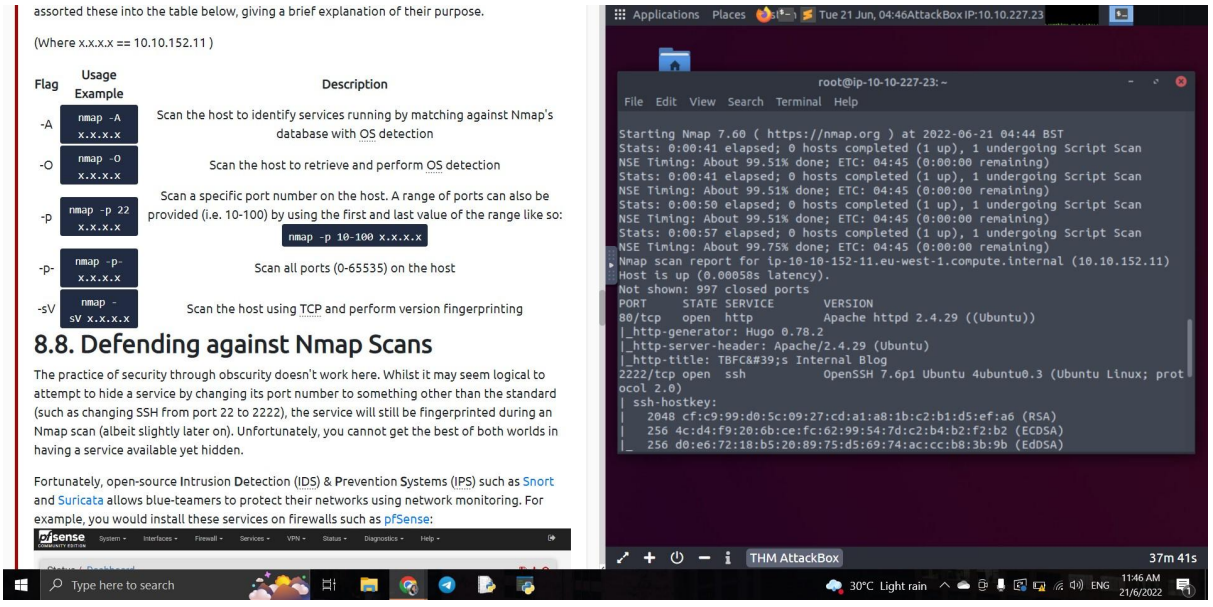
Question 1: we have used a searching machine called google in order to find when snort was created. The searching has been successful and answer has been obtained.



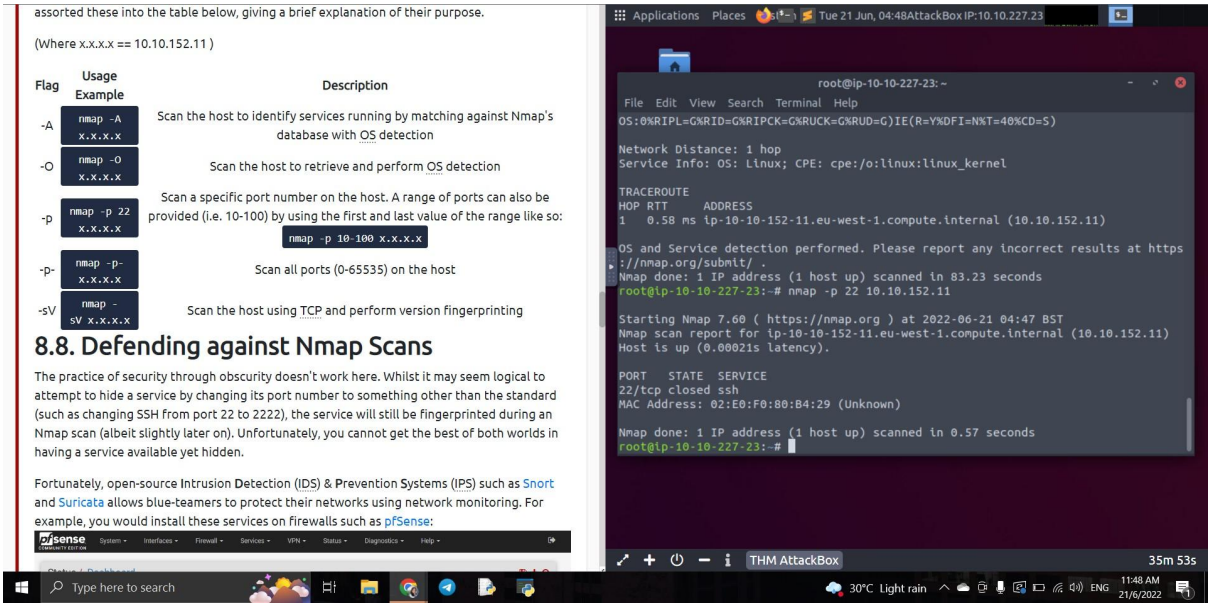
Question 2: Then, we obtained the port numbers of the three services running by using Nmap on MACHINE_IP. Answer has been provided in ascending order/lowest -> highest separated by comma.



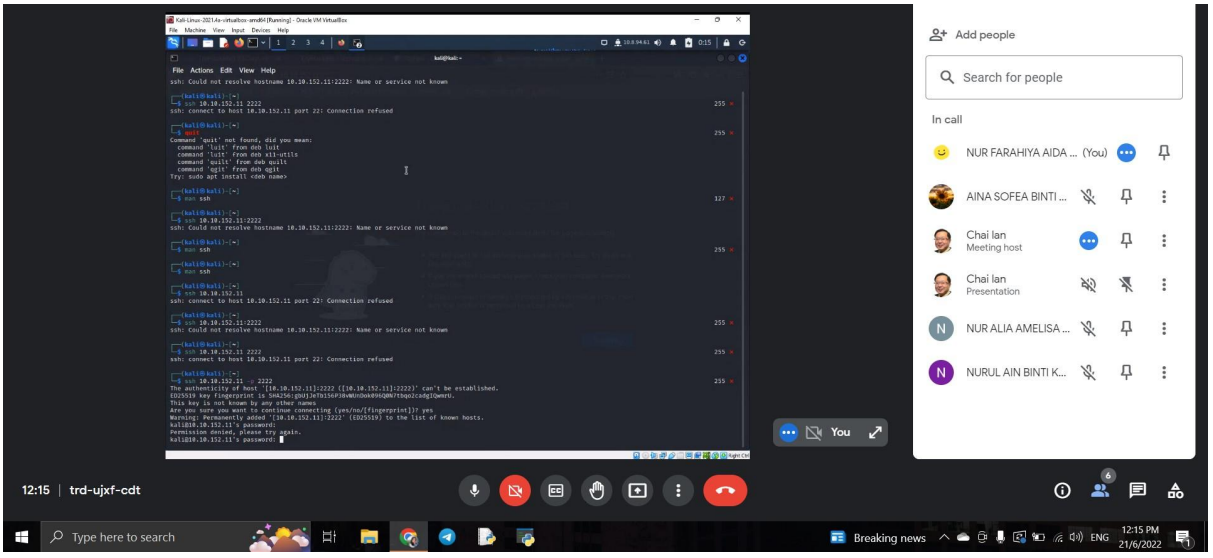
Question 3: After that, we used Nmap in order to determine the name of the Linux distribution that was running. The name of the linux is provided beside Apache/2.4/29. This was obtained by using nmap-A at the command prompt/terminal.



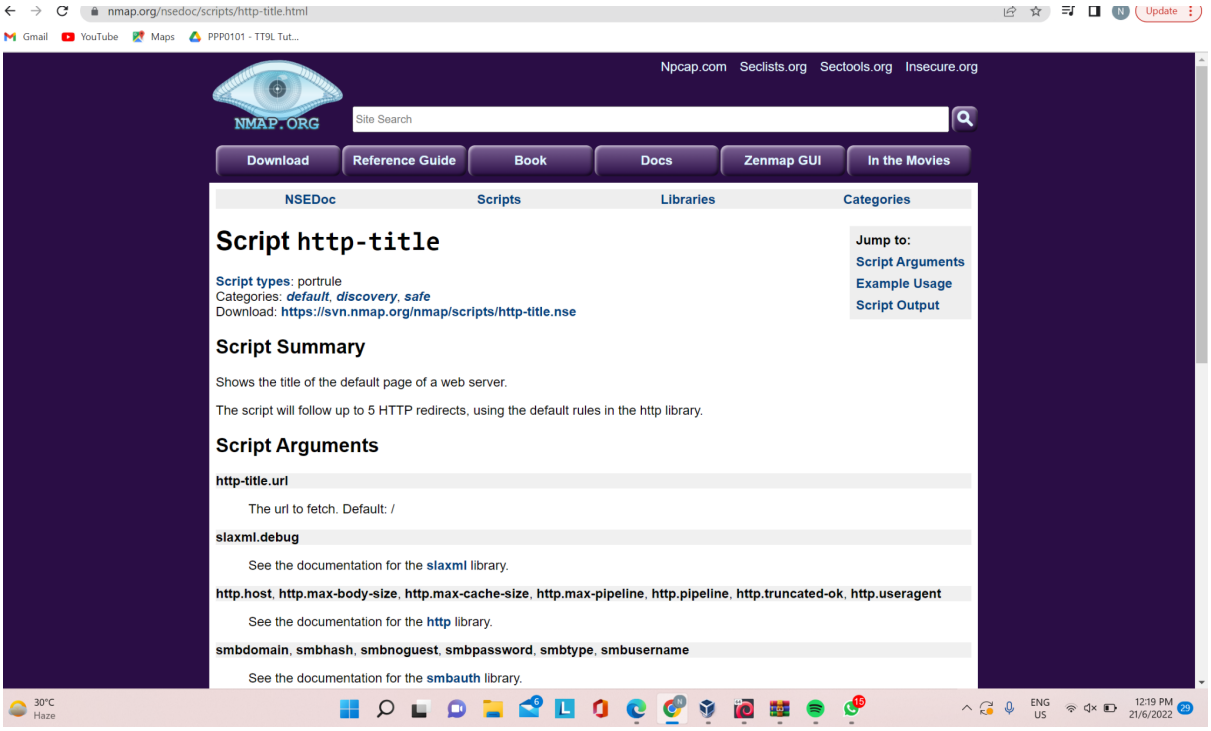
Question 4: Then, by using Nmap's Network Scripting Engine (NSE) in order to retrieve the "HTTP-TITLE" of the webserver, based on the value returned, we have successfully secured the thought of what this website might be used for.



Question 5 (google form): with the help of Dr Ian Chai, we have successfully acquired the port used by IP Address 10.10.152.11:2222 is SSH using kali linux.



Question 6: The "HTTP-TITLE" of the webserver turns out to be a blog.



Thoughts and Methodology:

First of all, we began by scanning that IP address using nmap. The three open ports shown above are for an HTTP server on port 80, SSH on port 2222, and a remote desktop connection on port 3389. After that, to proceed with the second question, there are multiple mentions of Ubuntu in the aforementioned scan findings using the code -A. After a while of trying, we used the initial scan as a reference to examine the HTTP-title section attentively, focusing on the web server (port 80). This demonstrates that it is utilised as a blog. And last but not least, that's how we complete our day 8 challenge.

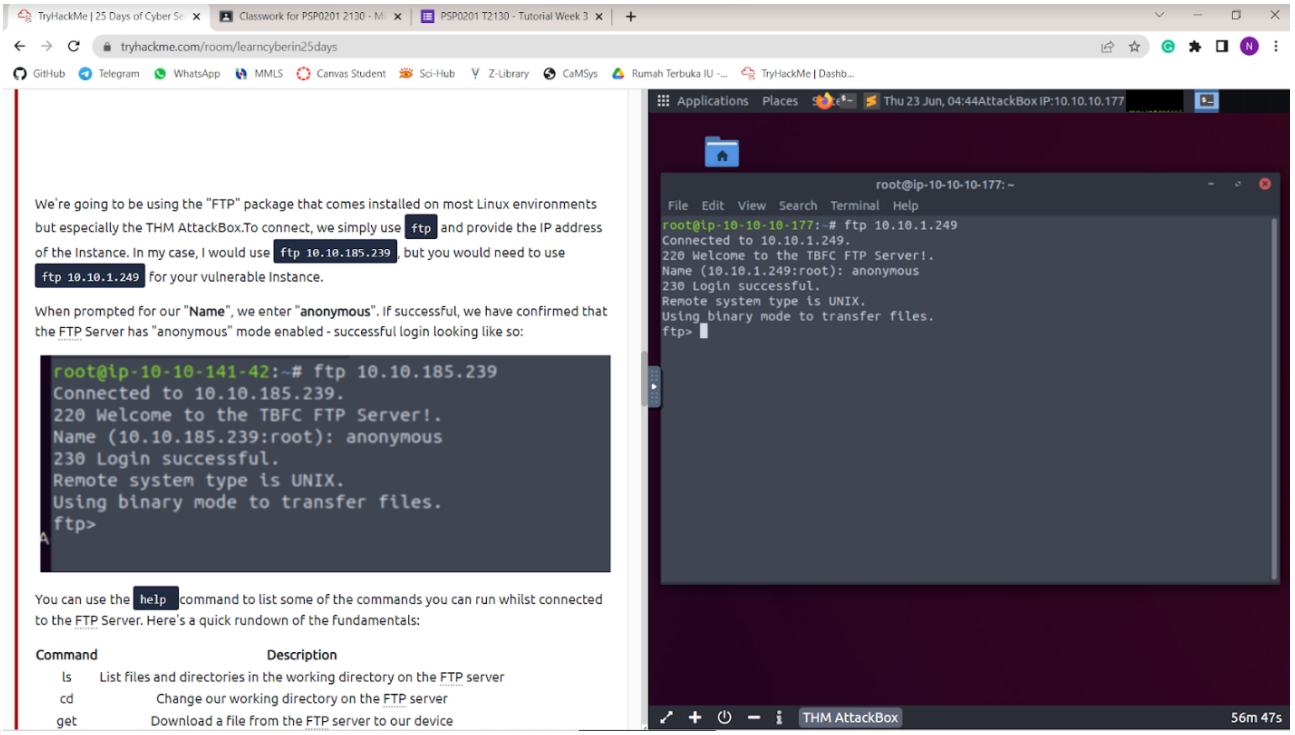
DAY 9: Anyone can be santa!

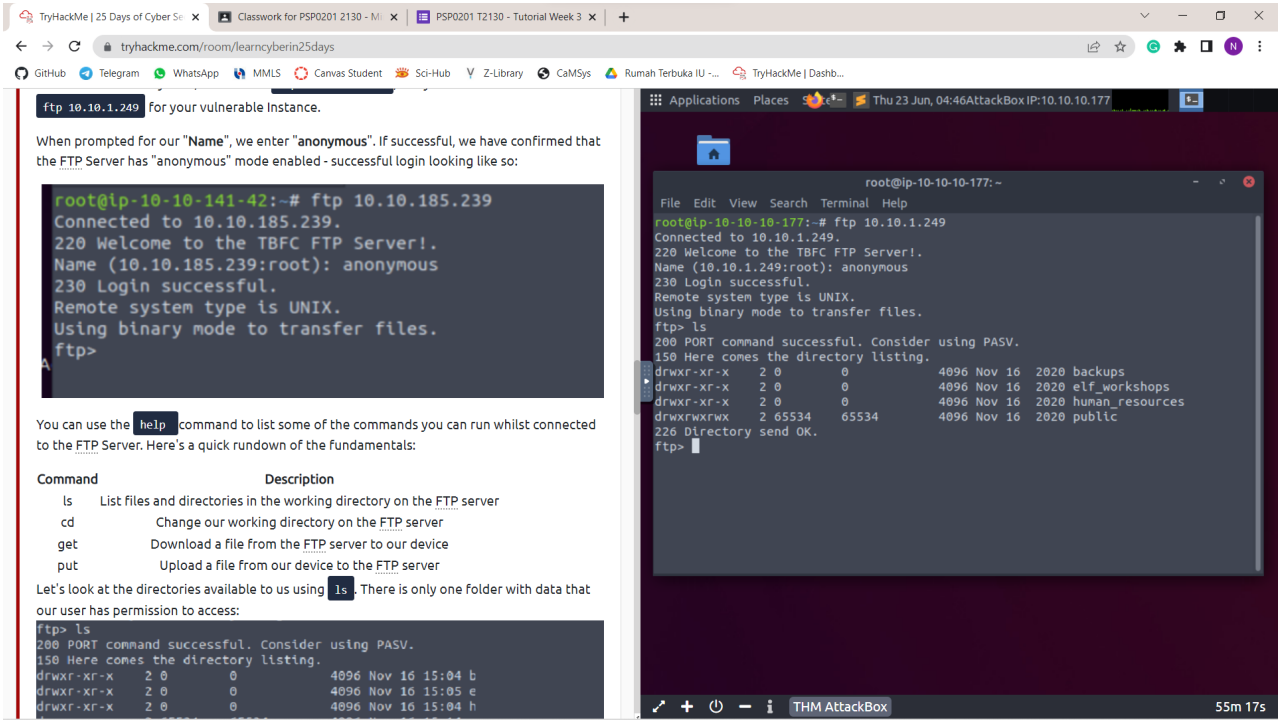
Tools used: Terminal

Solution/Walkthrough:

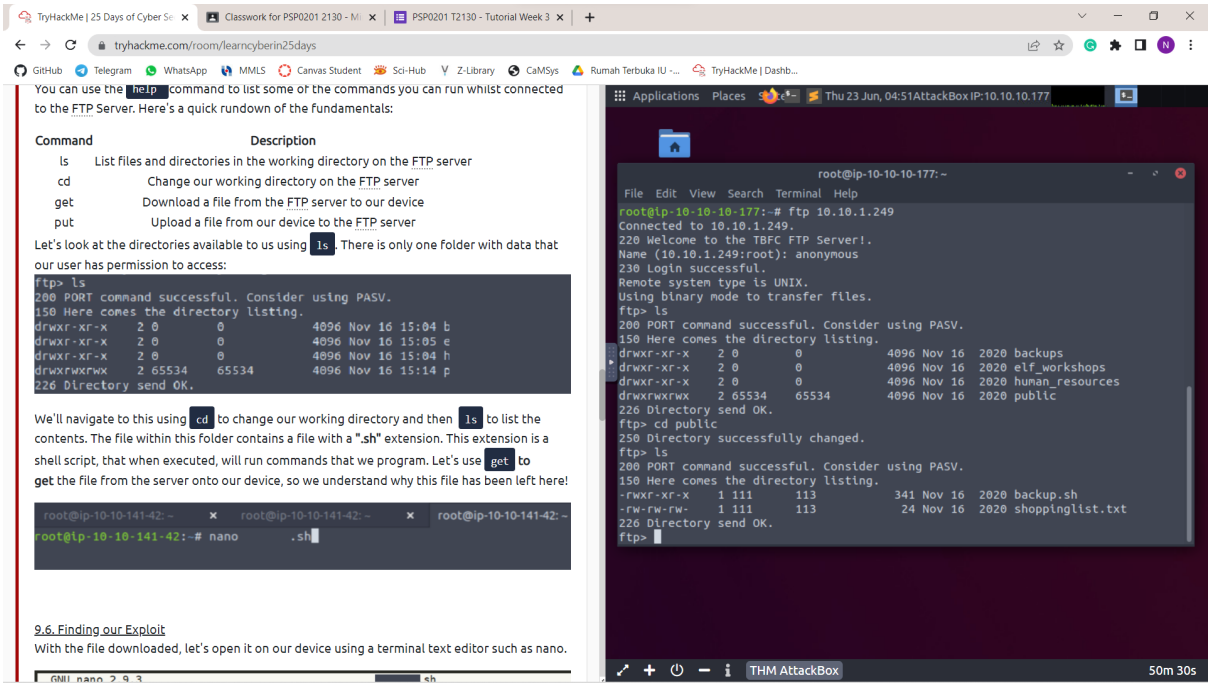
Question 1:

Get into the ftp server in the terminal and find the files using ‘ls’ command

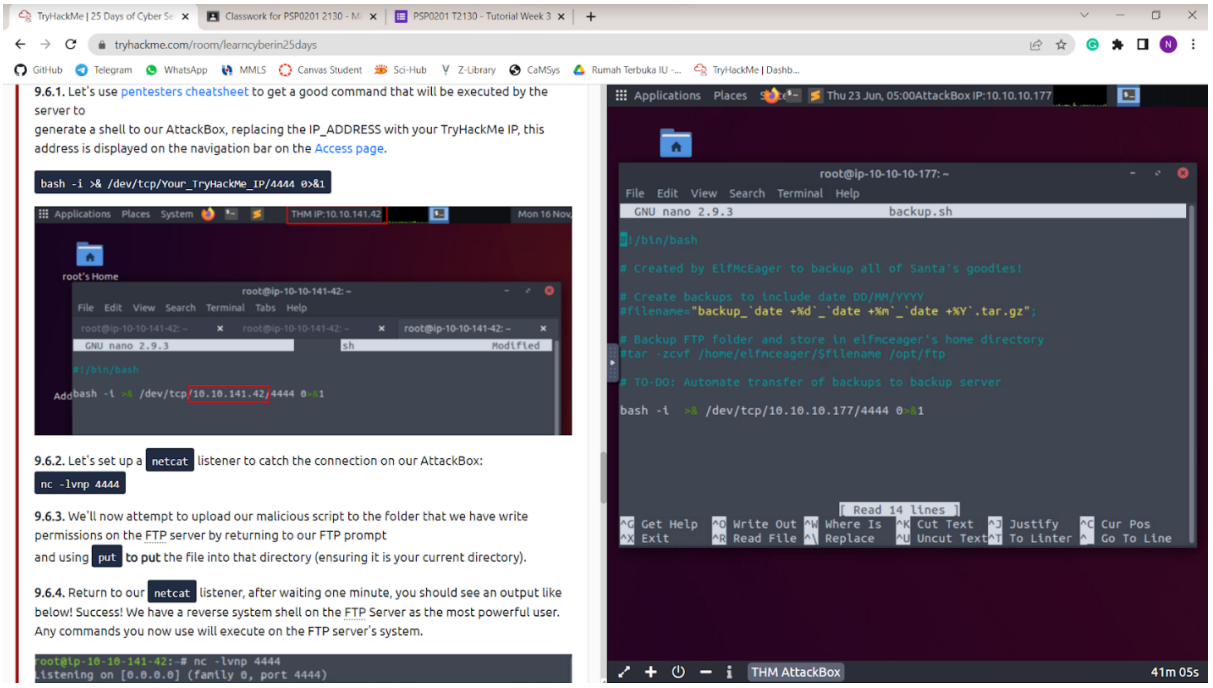




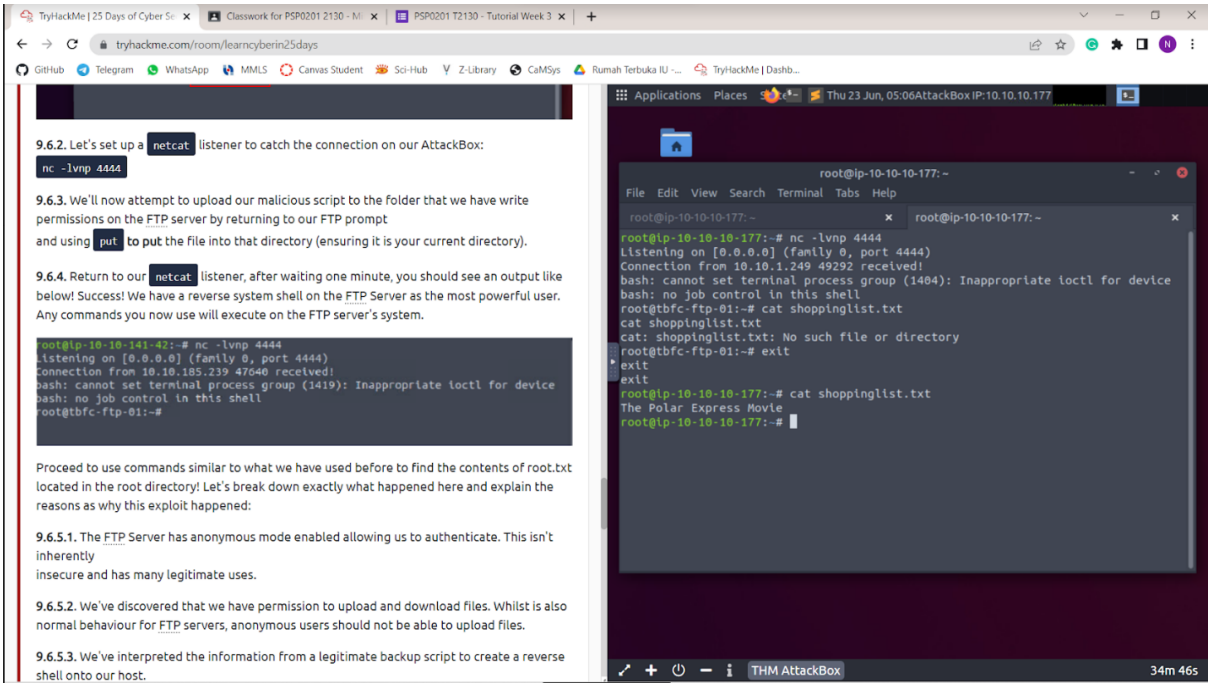
Question 2: We used the Try and Error method to find the files that are accessible by the “anonymous” user. Use the cd command to change the directory to the public, and “ls” command to get the list files and directories in the working directory.



Question 3: In the public directory, there are backup.sh and shoppinglist.txt files. To know which script can be executed within this directory, we use ‘get’ command to save the file into our local machine. The script that gets executed within this directory is backup.sh. Open the backup.sh using nano text editor.

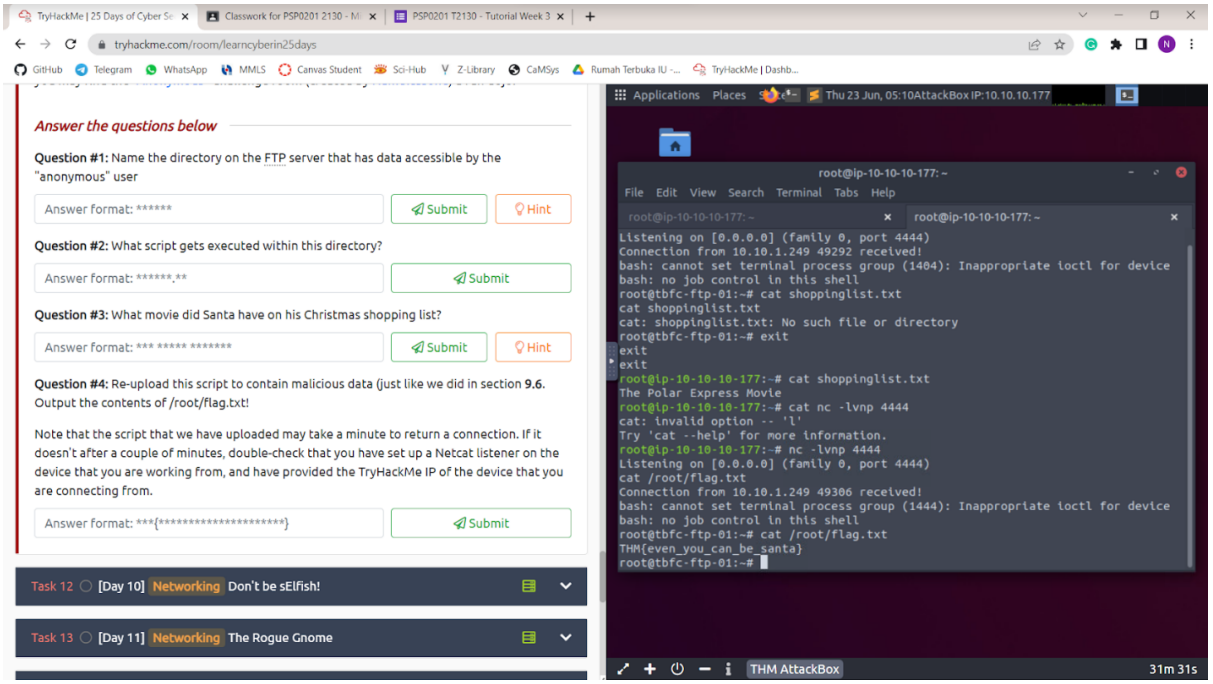


Question 4: To know the movie name in the shoppinglist.txt file, we use the ‘cat’ command followed by the file name



Question 5:

Using cat command and the contents of /root/flag.txt, we get the secret flag!!



Thought Process/Methodology:

First and foremost, deploy the machine as usual and open the terminal. We get into the ftp server with our ip addresses and it's asking for our name, so we will enter the anonymous. Then, login successfully using anonymous access. After that, using ls command we can see that many files and the public files have the data access. We can change to the public directory using cd command. So we can download the data inside the file. After get into the public directory, we use ls command again to find the data inside the public directory. There are backup.sh and shoppinglist.txt in the public directory. So we get the file to download using the get command. Then, we go finding our exploit with the file downloaded using a terminal text editor which is nano. So we will exit the ftp server first and open the exploit data which is nano backup.sh. After we get the data from the backup.sh, we will no the nc lvnp 4444. Next, to get to know the movie in the shopping list, we will use cat command. Then, for the last question, we use the cat command too to get the secret flag.

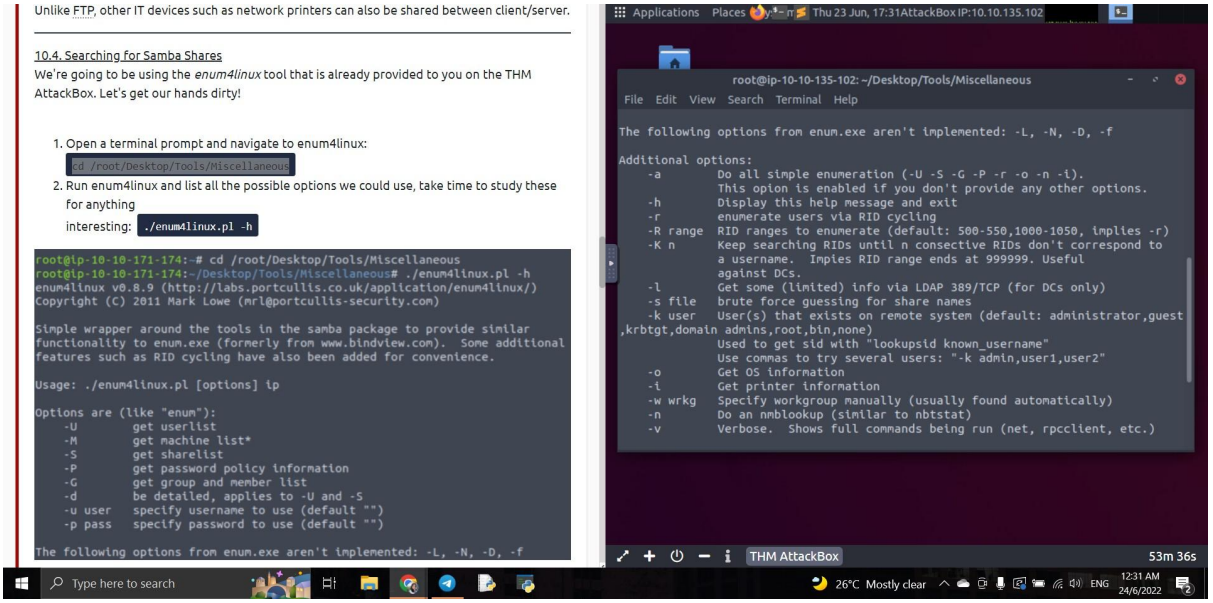
DAY 10 : Networking- Don't Be SElfish

Tools used: Kali Linux, Firefox, Google Chrome

Solution/Walkthrough:

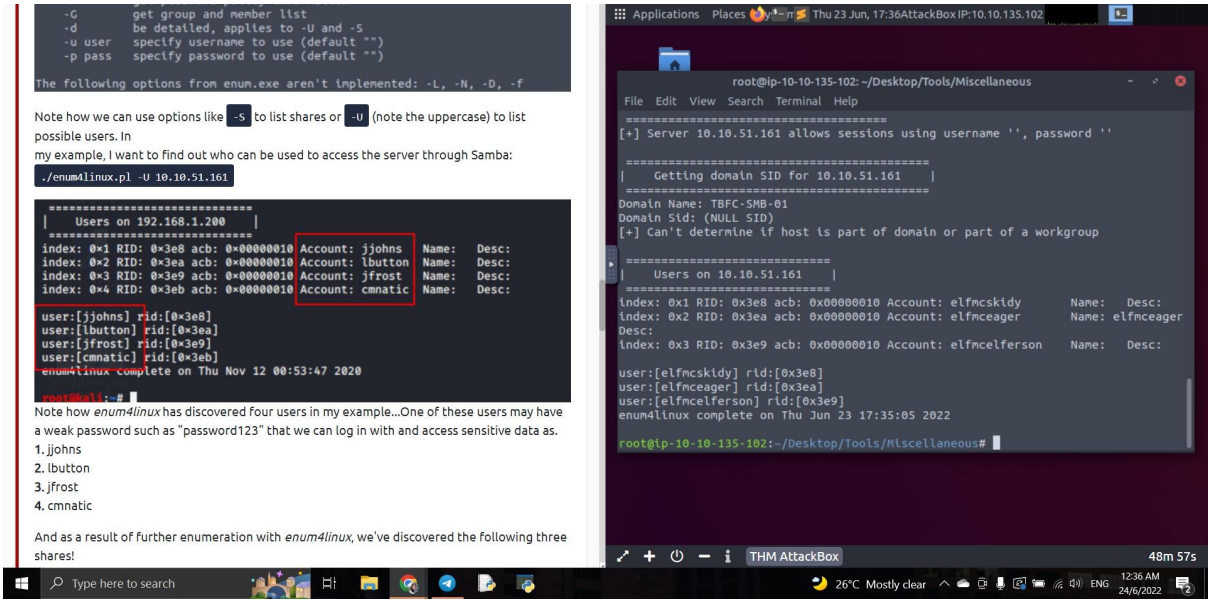
Question 1:

Open the terminal and navigate to enum4linux. A list of options will be shown in the terminal.



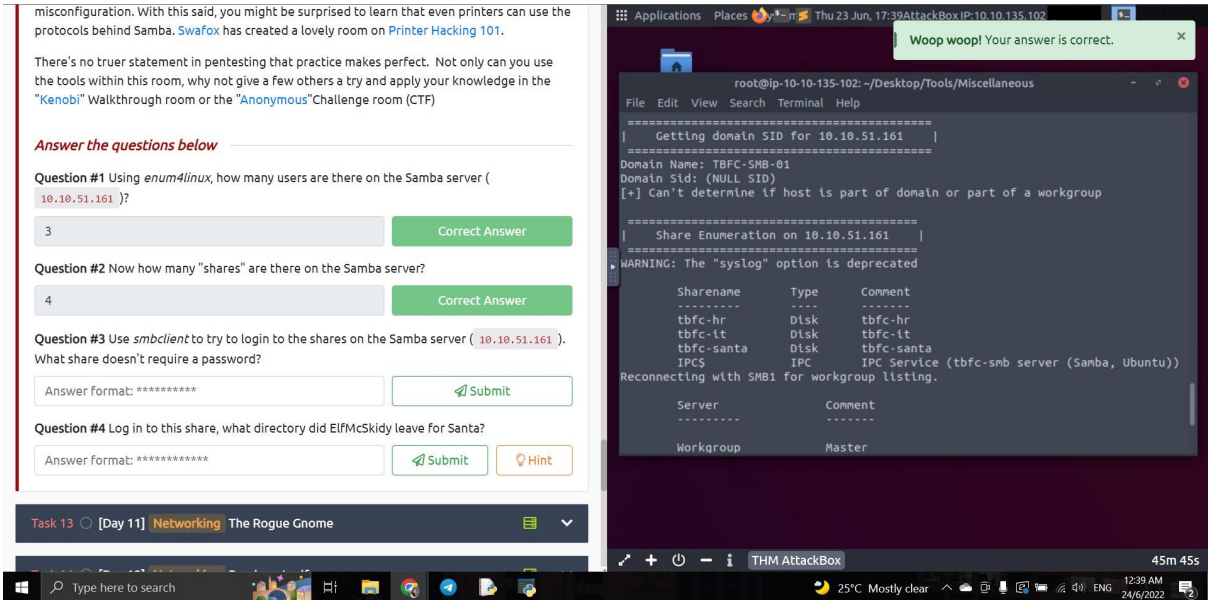
Question 2:

As we want to look for the number of users on Samba server, we use option -s to get the list. (./enumlinux.pl -s 10.10.51.161). We can see that there are 3 users on the list.



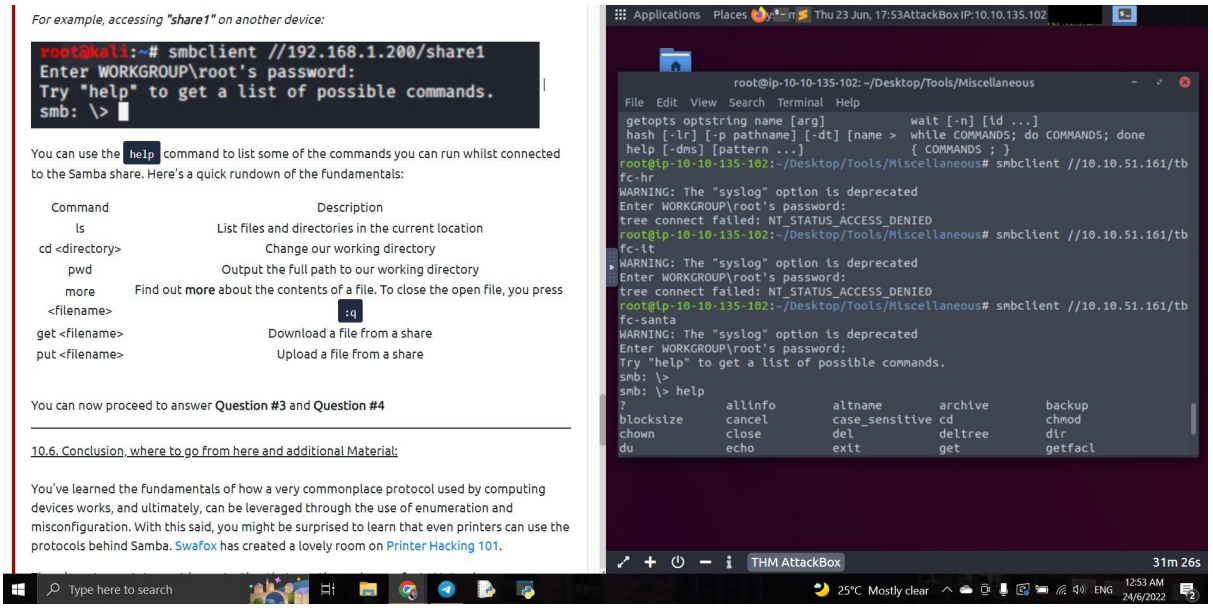
Question 3:

By further numeration, we can get the number of shares on the Samba server.



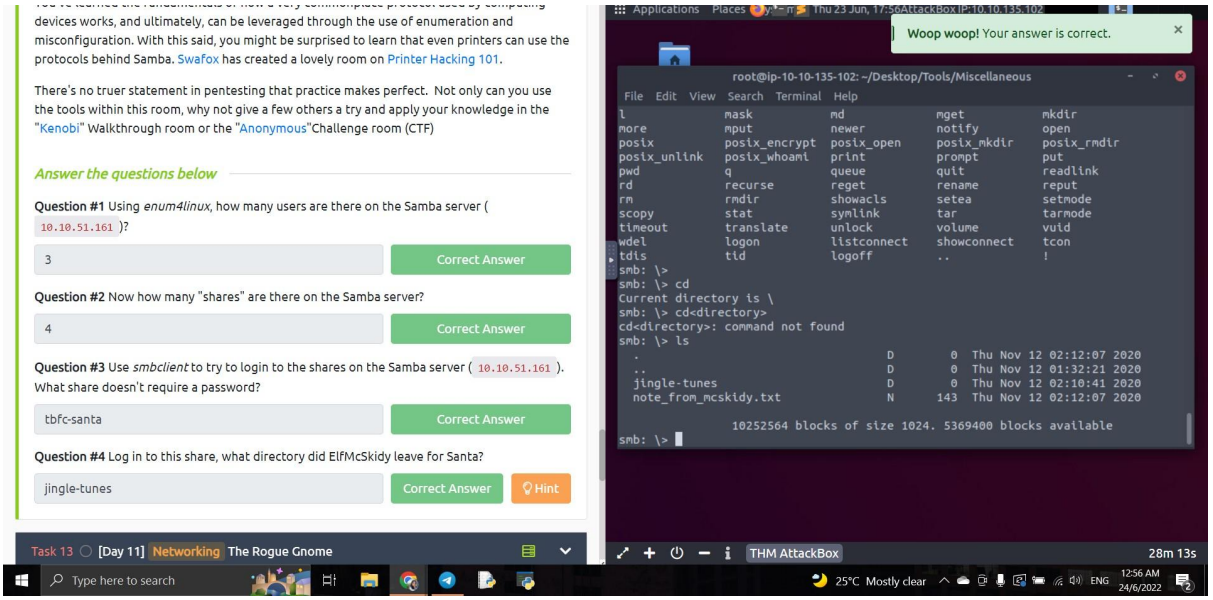
Question 4:

Use smbclient to access Samba server and insert the sharename we want to access in format (smbclient //10.10.51.161/*sharename*). We will be required to enter a password. As we want to look for a share that doesn't require any password, click enter to figure out which sharename fits the purpose.



Question 5:

As we found the intended sharename, we are now logged in the share. Scroll down to see the directory that ElfMcSkidy left for Santa.



Thought process/Methodology:

For this task, we will be using Samba which will make 2 operating systems can share resources including files amongst themselves. Our aim is to search for Samba Share and connect to the Share later on. After deploying the machine and starting AttackBox, we will use the enum4linux tool. In terminal, we navigate to the tool by inserting a certain command as mentioned in question 1. We have to use options like “-s” to list shares or “-U” to list possible users. When we do further enumeration, we shall find the shares under the sharename. To further look into the one that requires no password to access, we can try all the possible shares using command (smbclient //10.10.51.161/*sharename*). The one that works without needing a password is the one we are looking for. We are now logged in the share and can see all the resources in the particular share.