PSP0201 WEEKLY REPORT

Group name: Apocalypse

Members

ID	NAME	ROLE
1211103698	UMMI SYAHIRAH BINTI MUHAMMAD ROZAIDEE	LEADER
1211103293	FARAH KAMILA BINTI YAHYA	MEMBER
1211102031	NOR ALIAH SYUHAIDAH BINTI SHARUDDIN	MEMBER
1211101673	NURUL MANJA MURNIRA NAJWA BINTI MALIKI	MEMBER

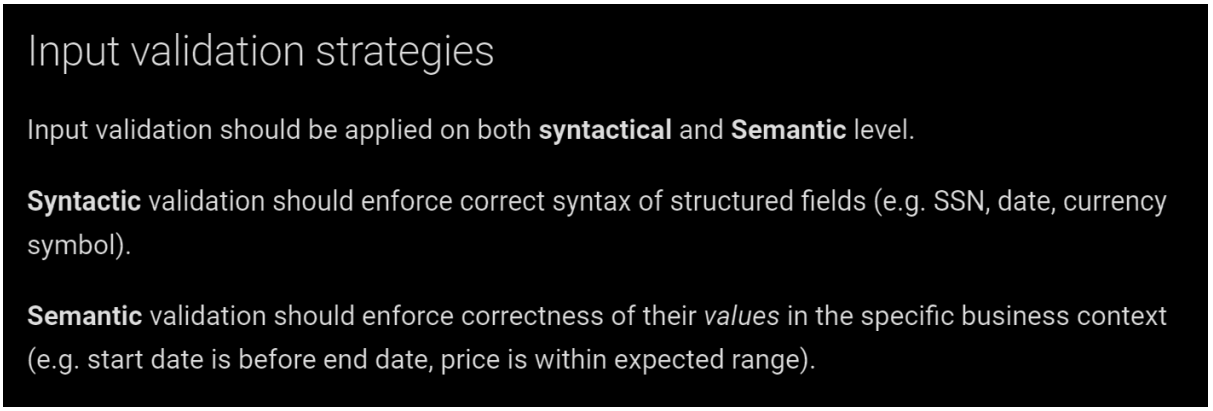
DAY 6 : [Web Exploitation] Be careful with what you wish on a Christmas night

Tools used : Kali Linux, Firefox, OWASP ZAP

Solution / Walkthrough :

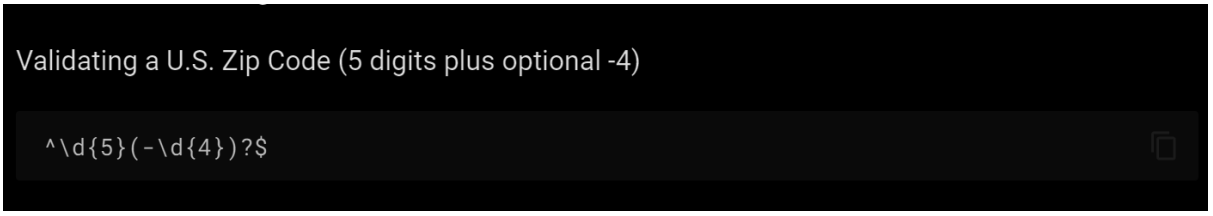
Question 1

The answer can be found on Google.



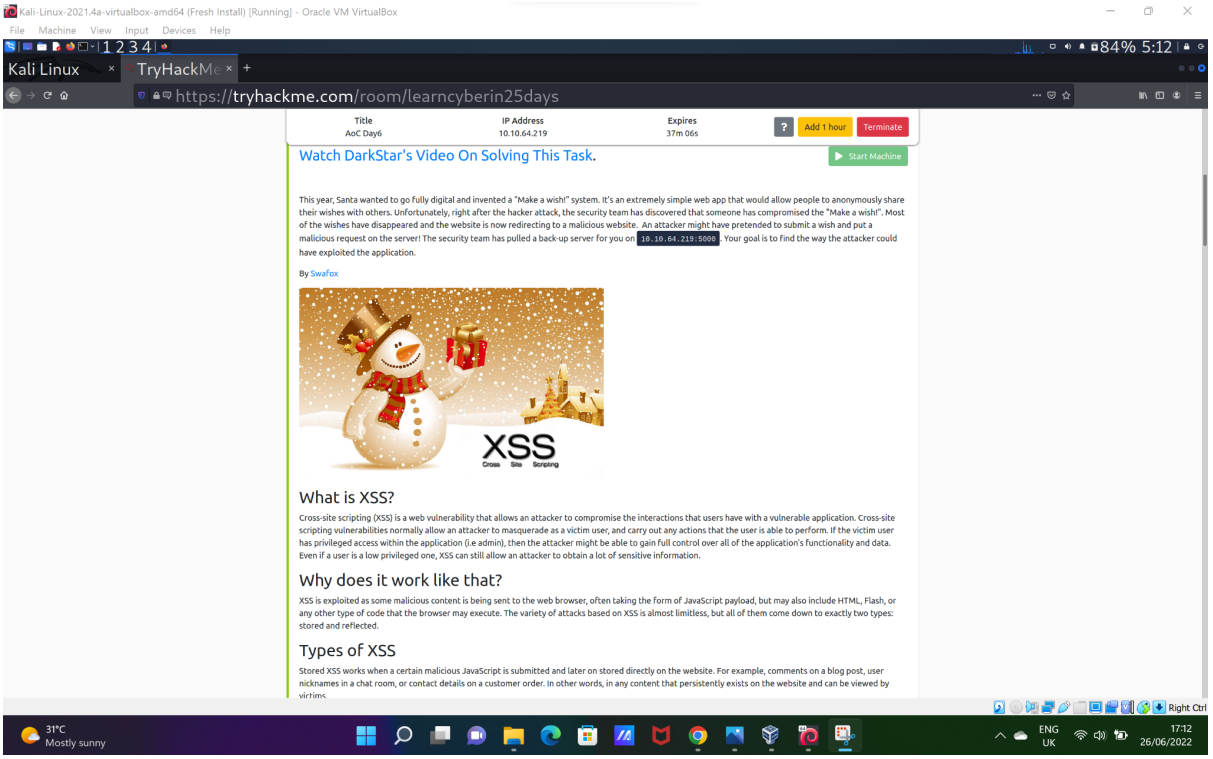
Question 2

The answer can be found on Google.



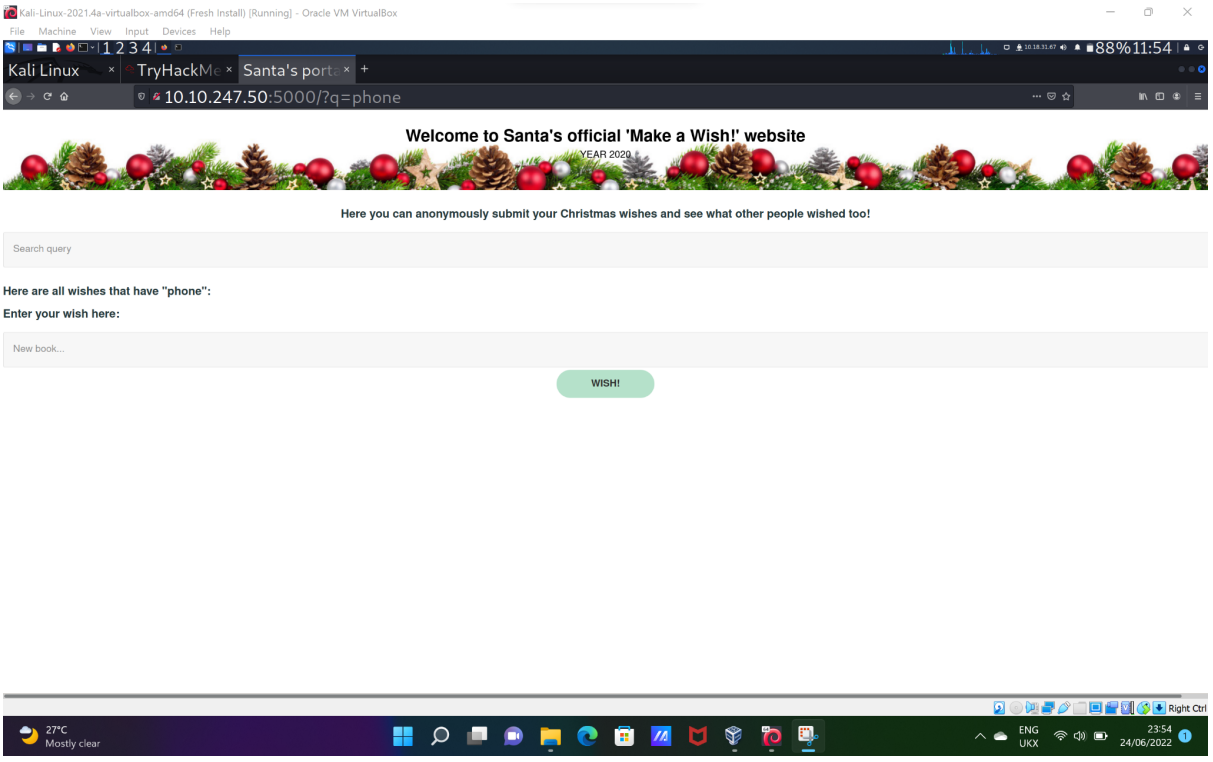
Question 3

The answer can be found at TryHackMe



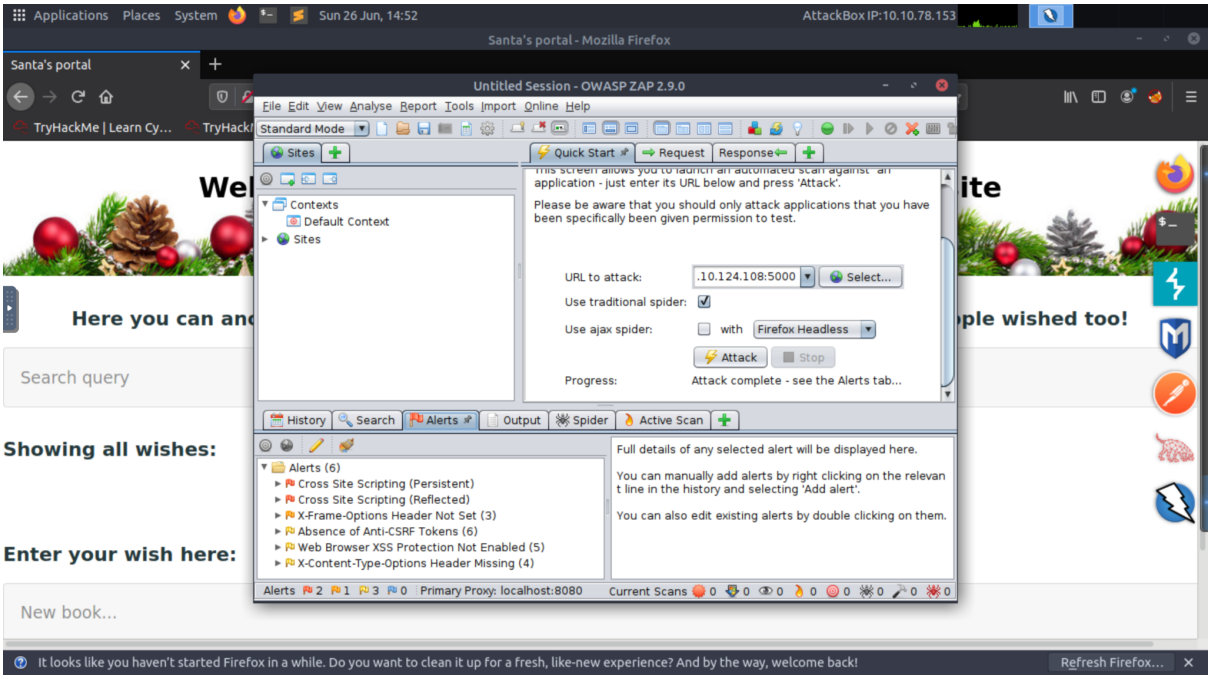
Question 4

The query string is:q



Question 5

2 XXS alerts in the scan



Question 6

Q6: What Javascript code should you put in the wish text box if you want to show an alert saying "PSP0201"? * 2 points

Answer hint: <script>xxxxxx</script> <--insert your answer TOGETHER with the script tags.

<script>alert("PSP0201")</script>

Question 7

Yes, XSS attack persist.

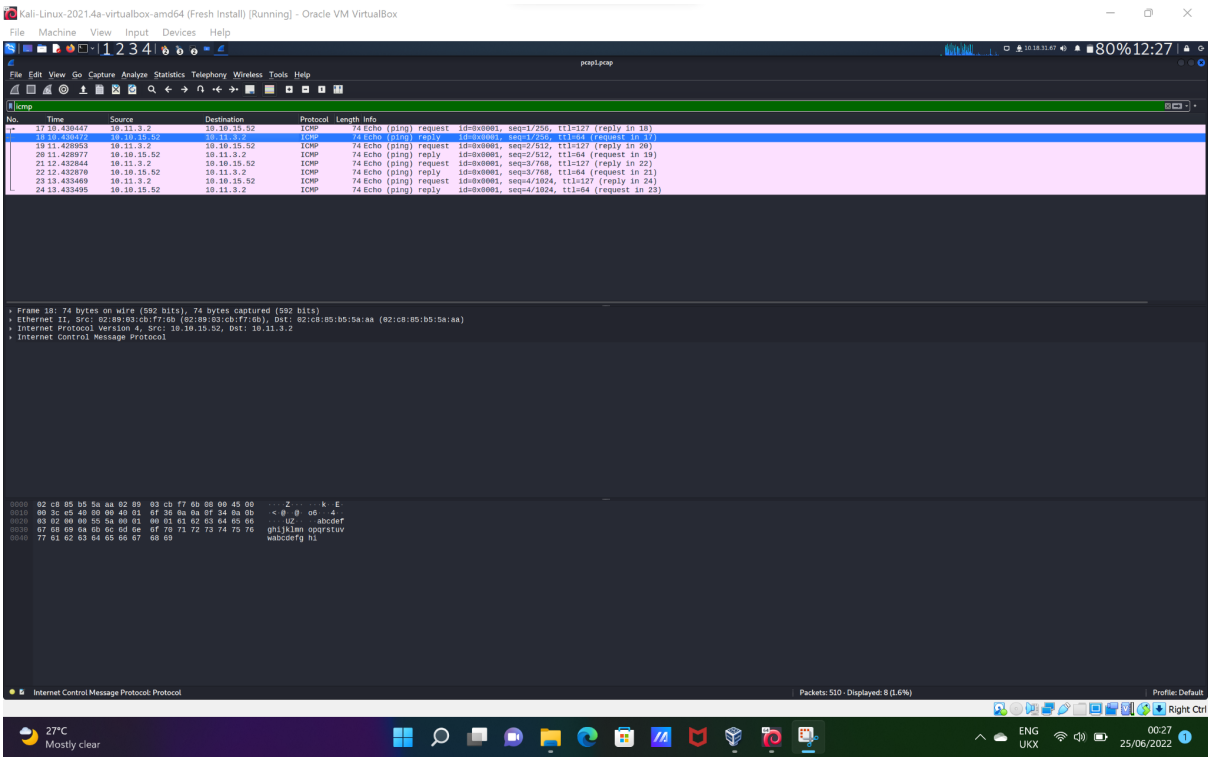
DAY 7 : [Networking] The Grinch Really Did Steal Christmas

Tools used : Kali Linux, Firefox, Wireshark

Solution / Walkthrough :

Question 1

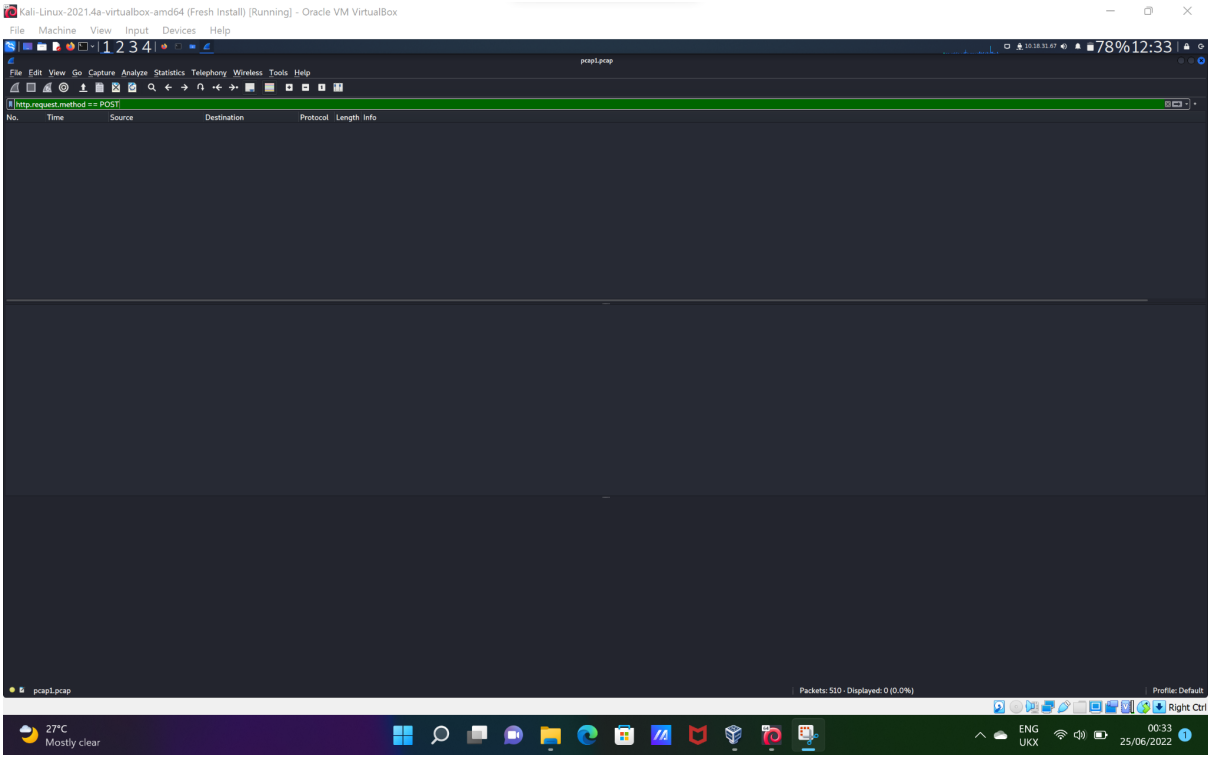
1. Open wireshark
2. Choose pcap1.pcap
3. Type “icmp” at filter section



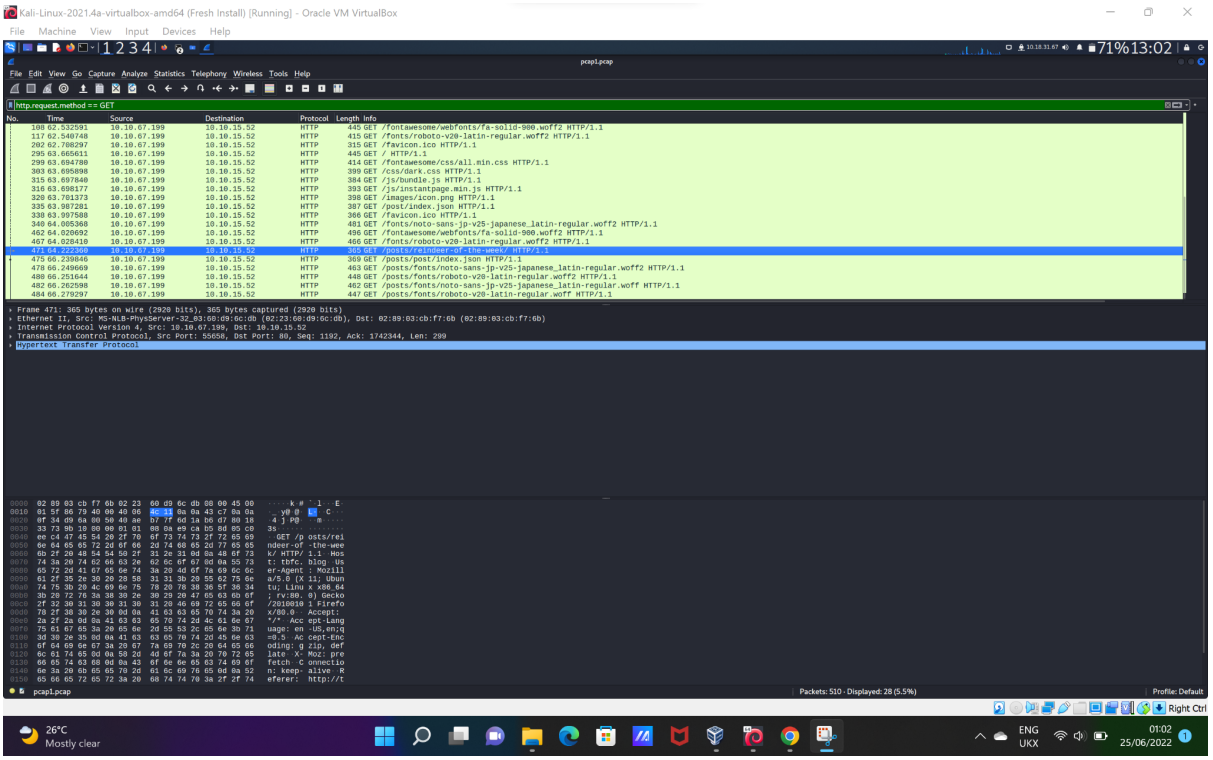
Question 2

1. Open Wireshark
2. Choose pcap1.pcap
3. Type **http.request.method == POST** at filter section.
4. Type **http.request.method == GET** at filter section.

If we use **http.request.method == POST** , we will not get the answer.

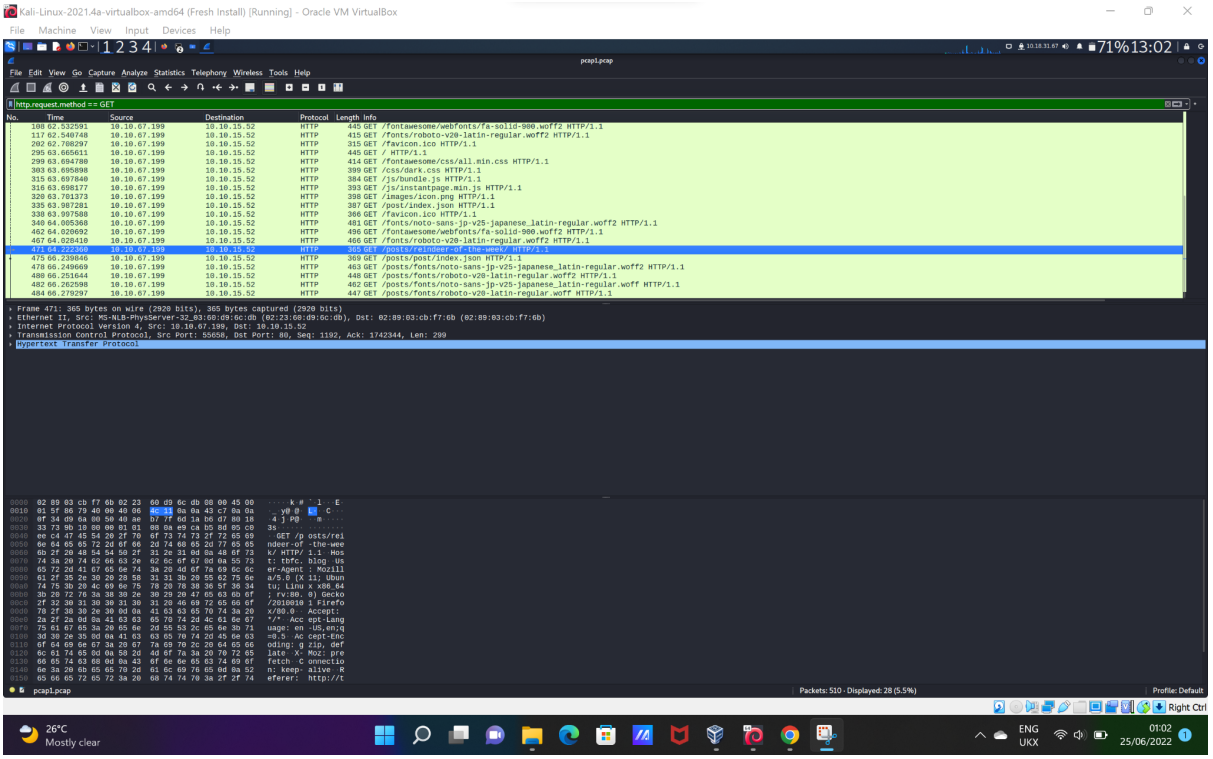


If we use **http.request.method == GET,** we will get the answer.



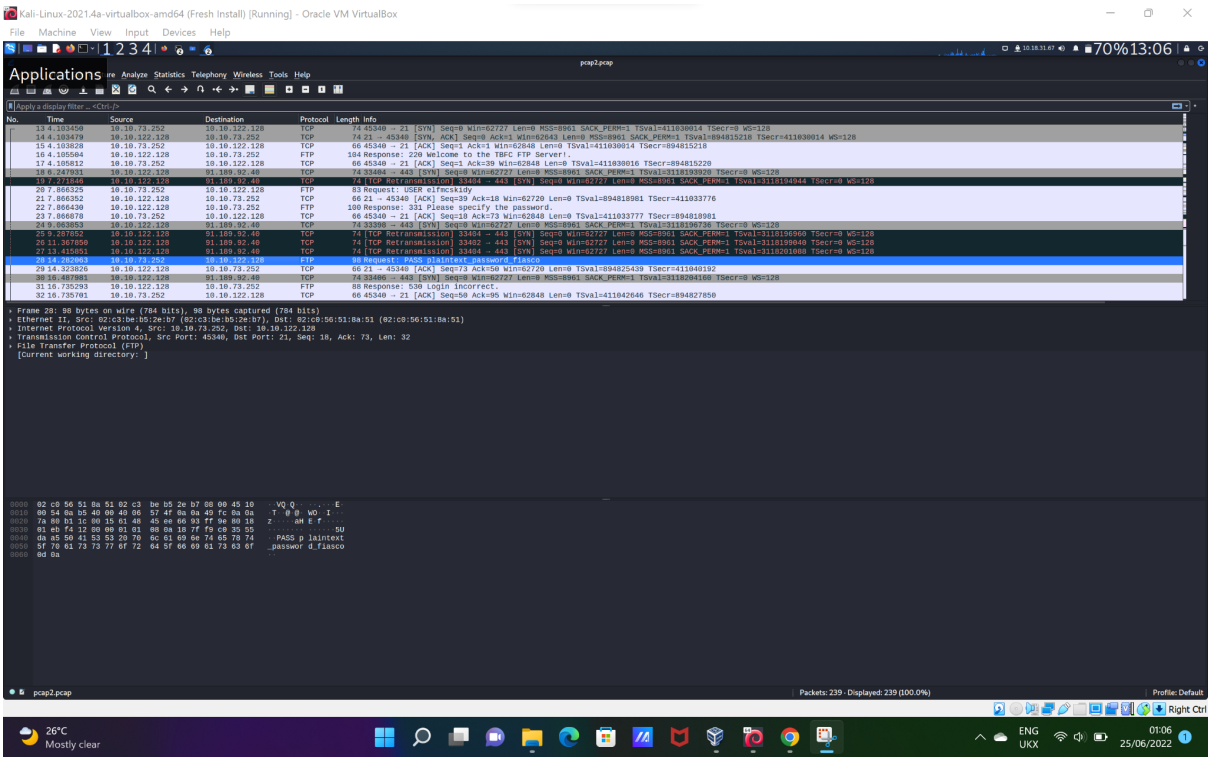
Question 3

1. Type **http.request.method == GET at** filter section.
2. Search **IP address "10.10.67.199"** to know what is the name of the article.



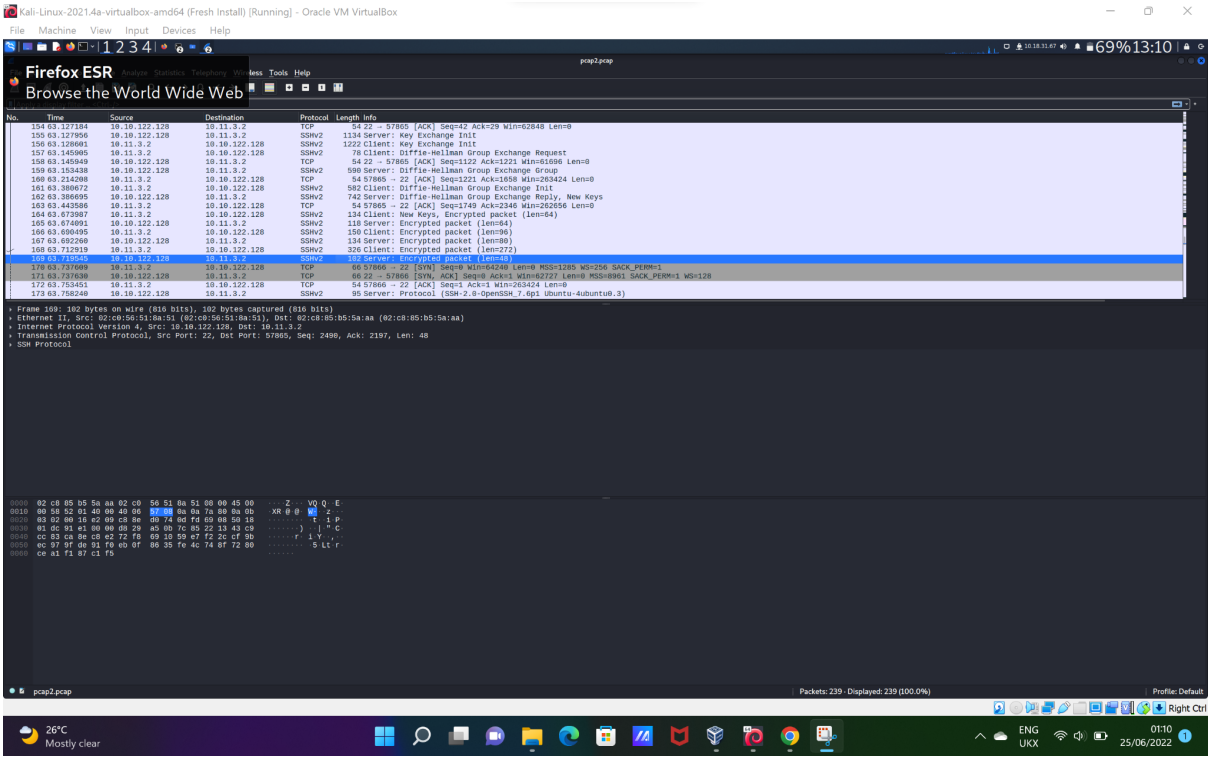
Question 4

1. Open Wireshark
2. Choose pcap2.pcap
3. Look at the captured FTP traffic
4. Choose the one that the password was leaked during the login process.



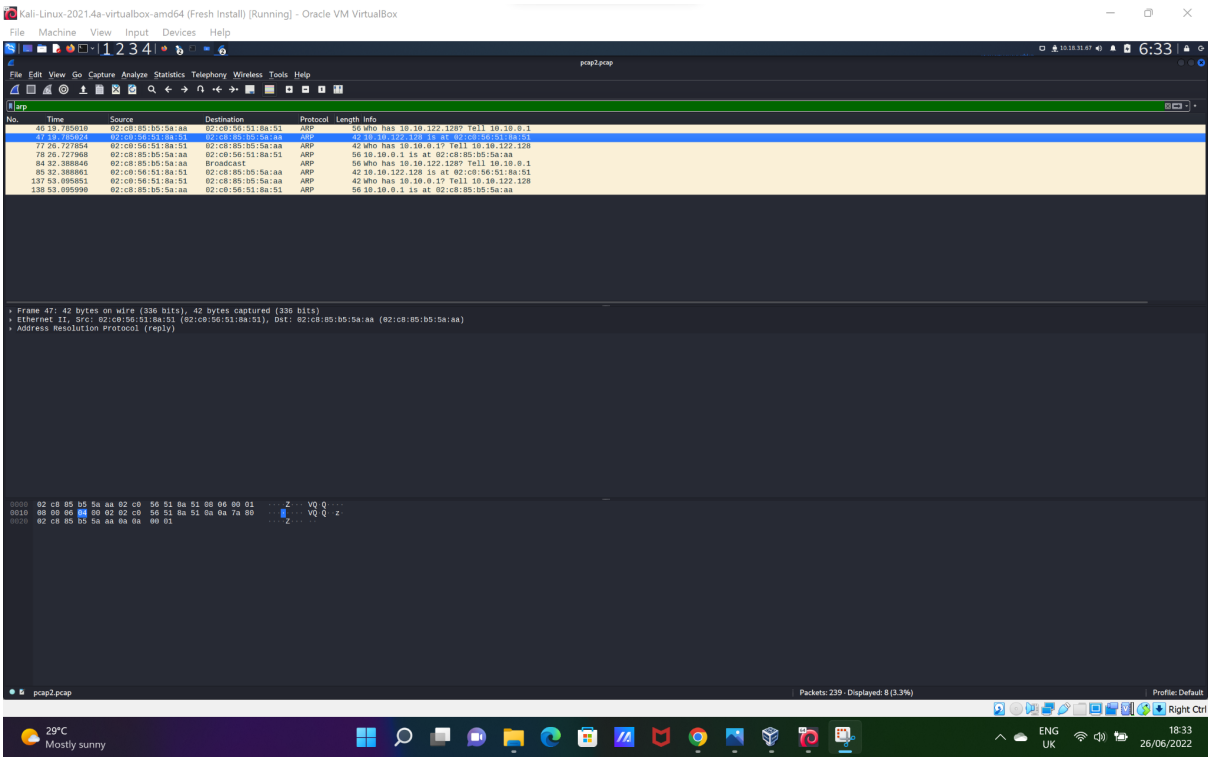
Question 5

1. Choose pcap2.pcap
2. Search what is the name of the protocol that is encrypted



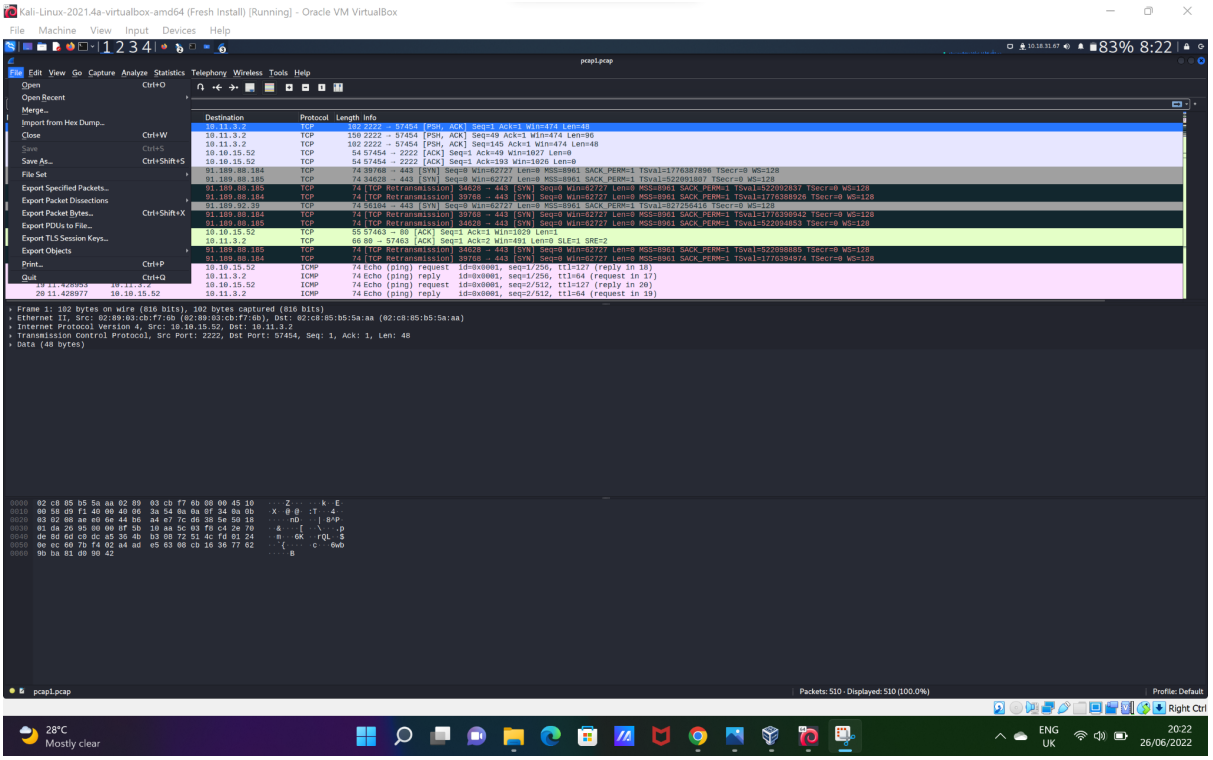
Question 6

1. Choose pcap2.pcap
2. Type ARP at the filter section
3. Search 10.10.122.128 where is at.

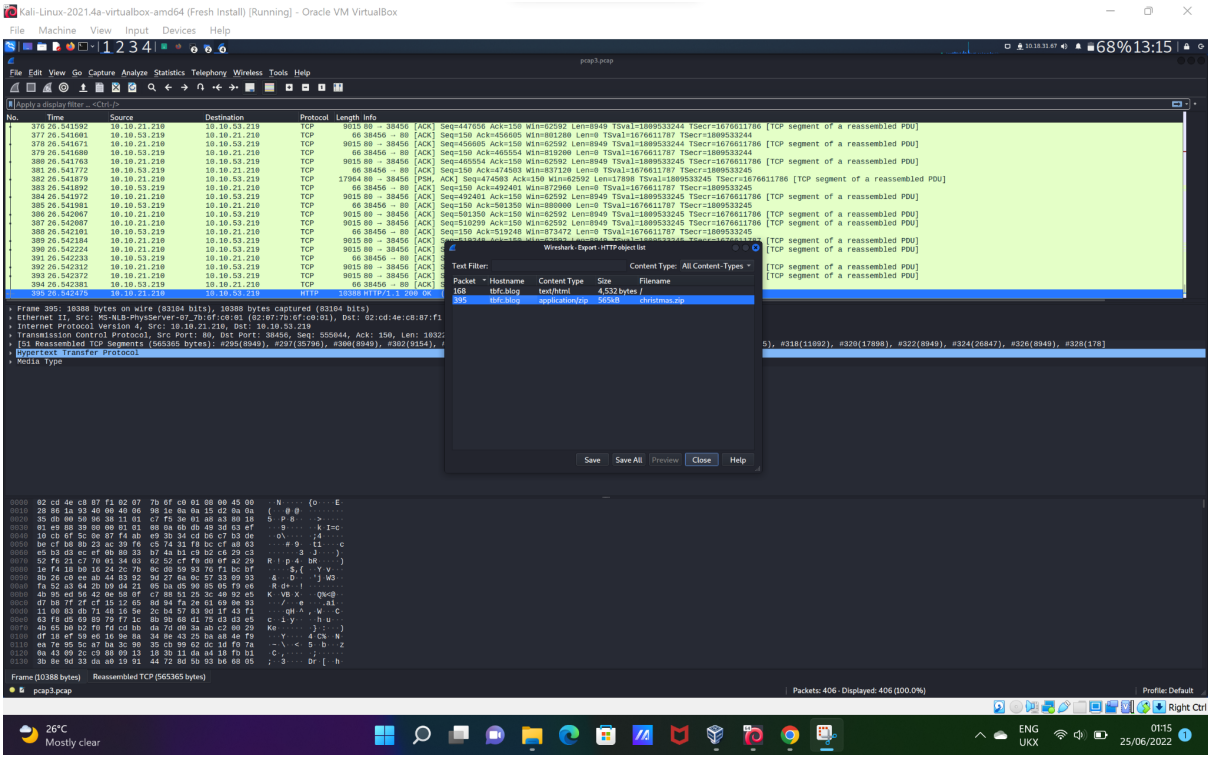


Question 7

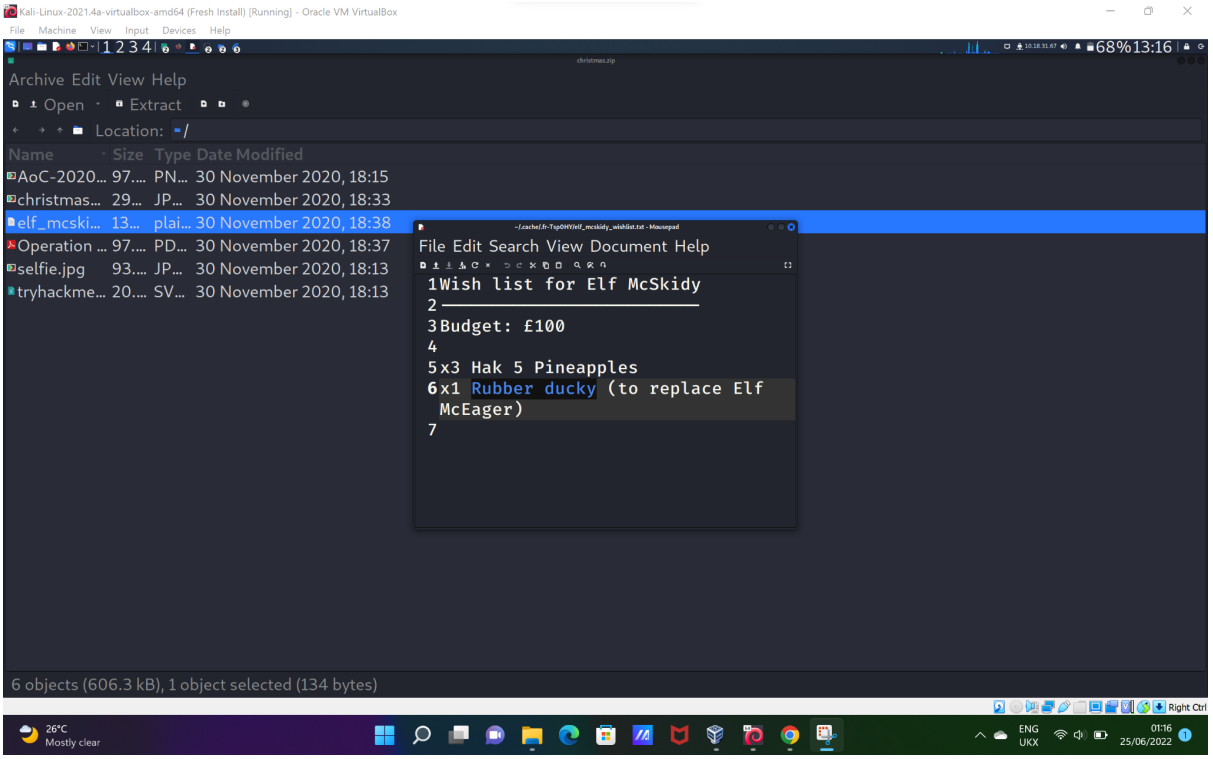
1. Choose pcap3.pcap
2. Open file



3. Choose export object ; **HTTP**



4. Save the file.
5. Open folder, go to download and choose christmas.zip file
6. Select elf_mcskidy
7. The answer : Rubber ducky



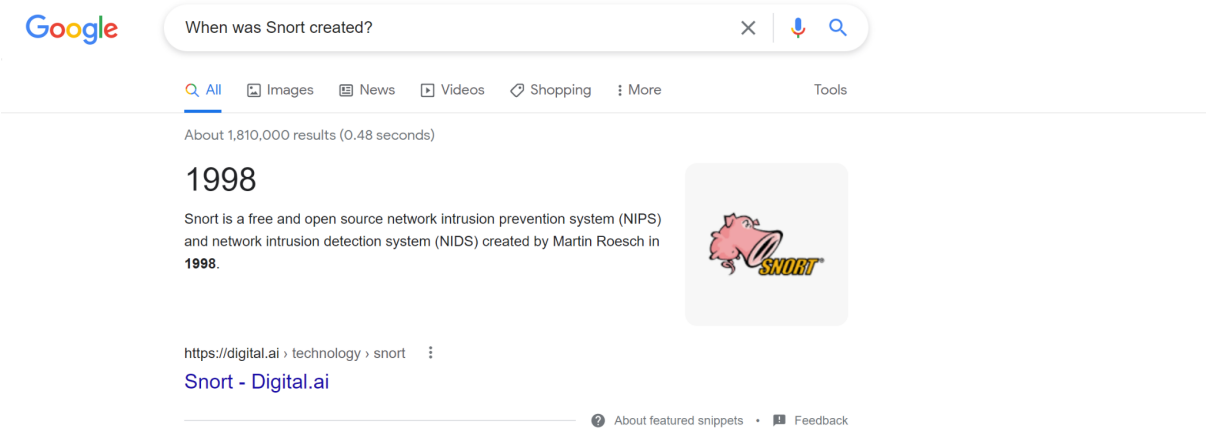
Day 8: [Networking] What's Under the Christmas Tree?

Tools used: Kali Linux, Google Chrome

Solution/walkthrough:

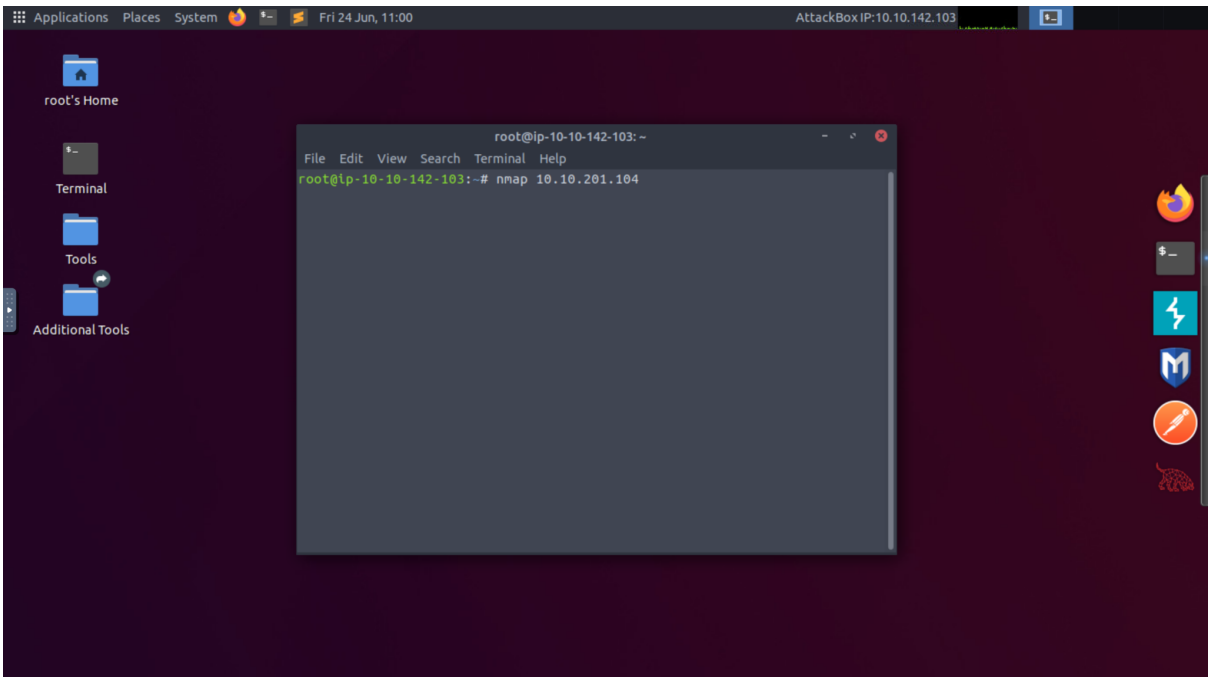
Question 1

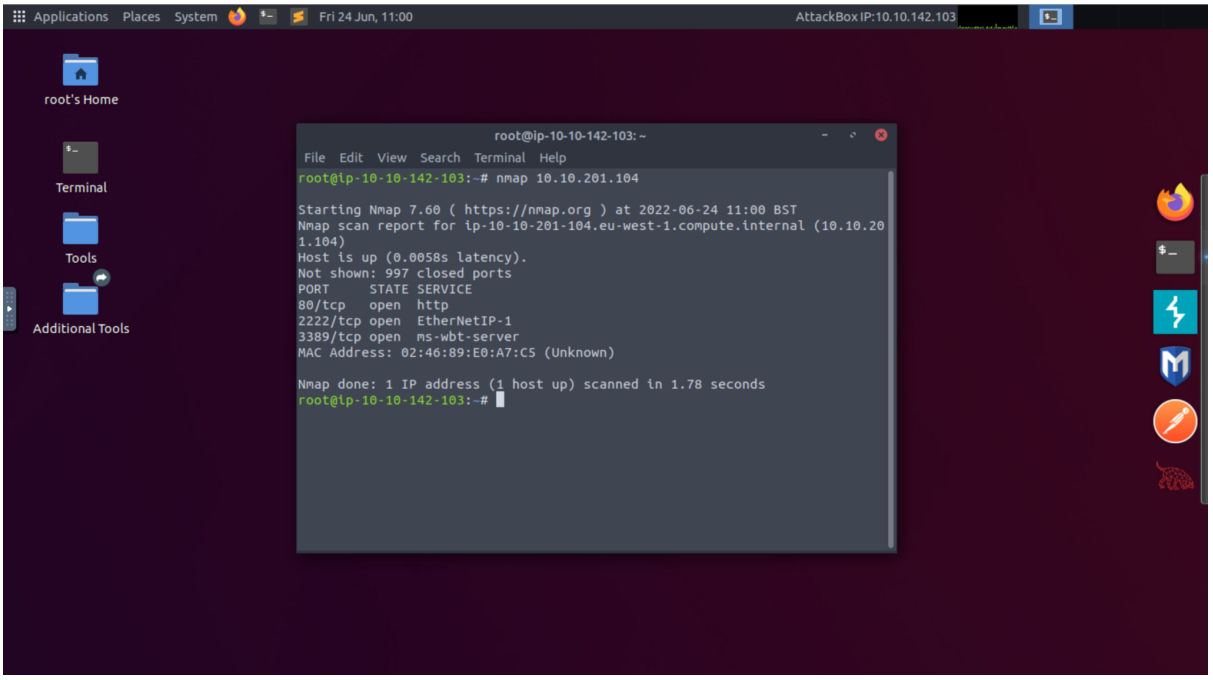
Self research. The answer can be found via Google search.



Question 2

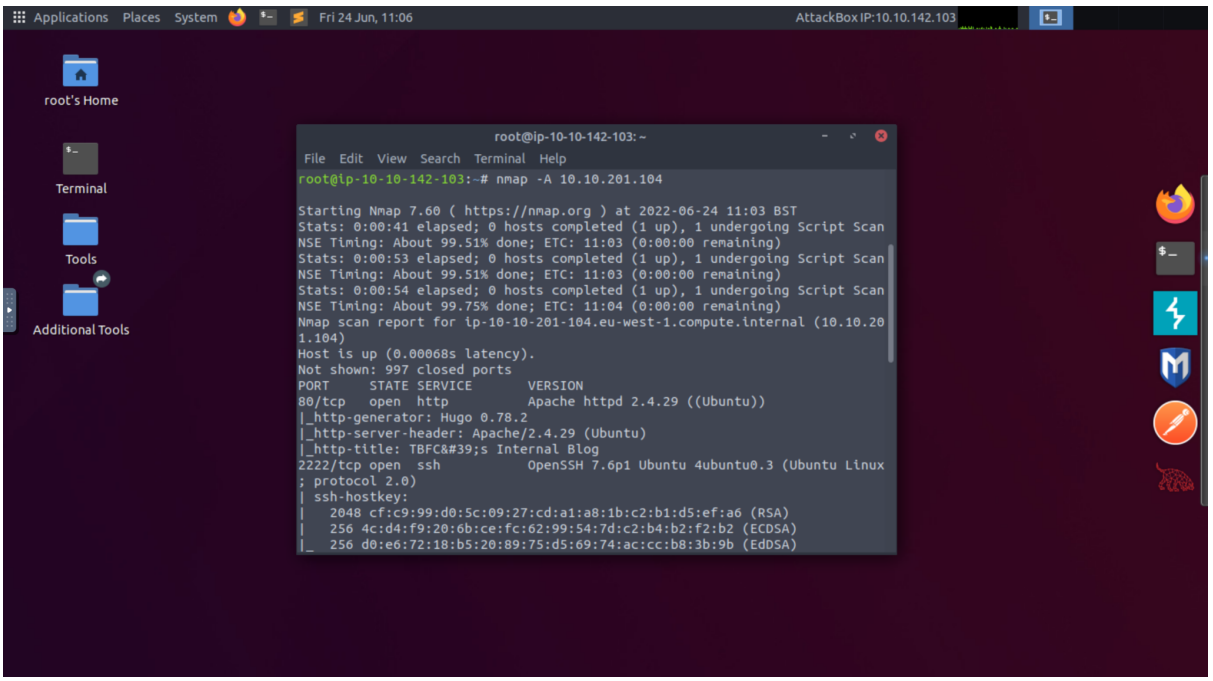
Open terminal. Scan **nmap [THM IP address]** and find the port numbers displayed.





Question 3

Scan **nmap -A [THM IP address]**. Find the name of Linux distribution running.

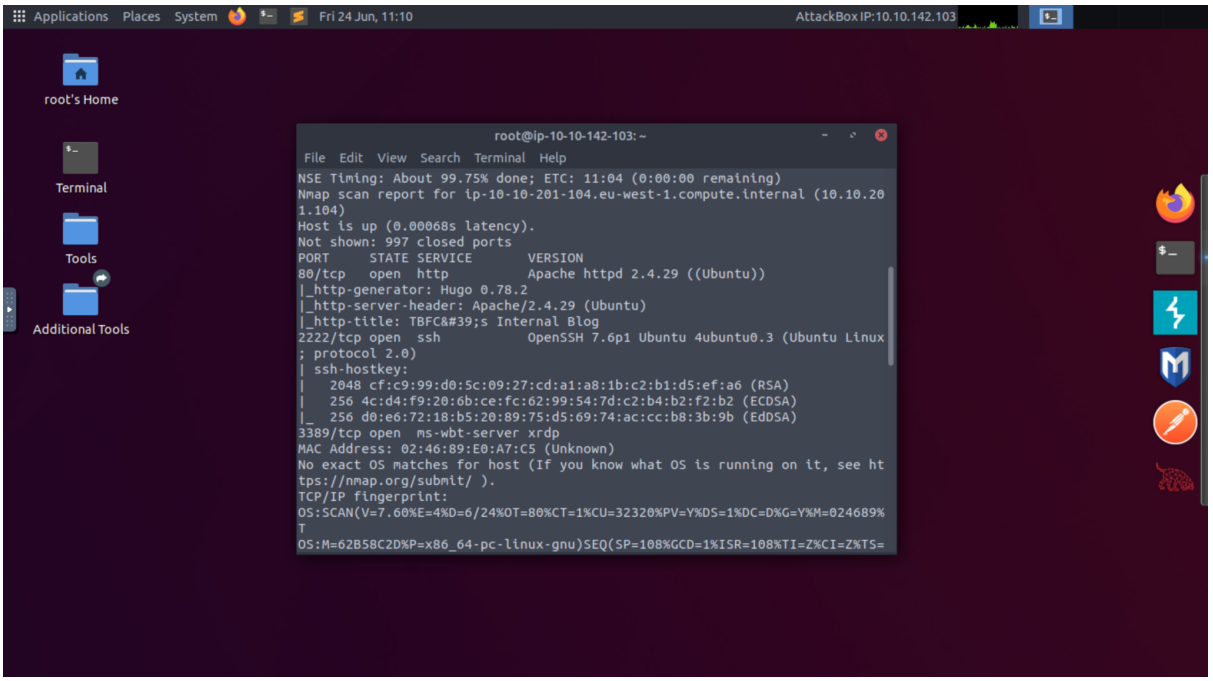


Question 4

On the same scan, find the version of the Apache.

Question 5

Scroll lower through the same scan and find port 2222.



Question 6

In the same scan, look for http-title, which explains the use of the website.

Thought process/methodology:

After opening the terminal on our device, we scan Nmap and the target IP address given by TryHackMe. By doing so we are able to use its functions such as NSE. The Nmap scan report will then be shown and from there information such as the ports running, state, and service will be shown. We then scan nmap -A flag with the target IP address to identify the services running by matching against Nmap's database with OS selection. From there, we can find all the necessary information like the name of the Linux distribution, the Apache version, what is being run on port 2222 and the http-title. The -A flag can function thanks to the Nmap Scripting Engine which uses scripts for exploitation, fuzzing and brute-forcing. Thus, we are able to find the answers to all the questions given.

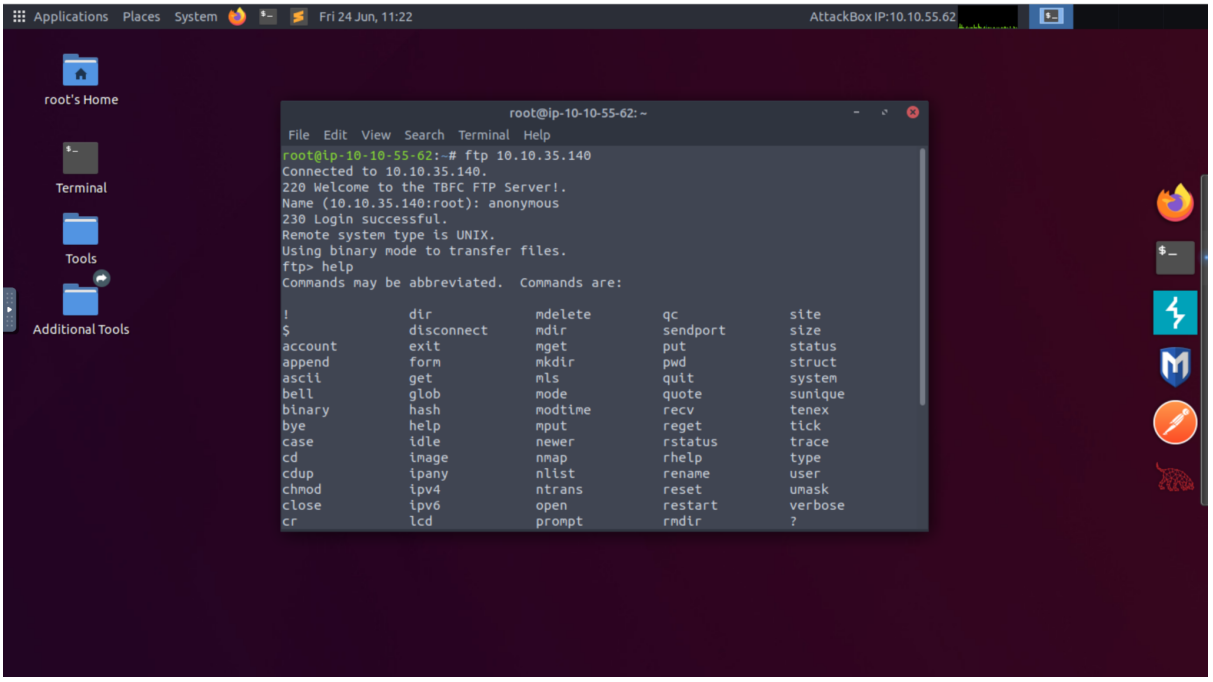
Day 9: [Networking] Anyone can be Santa

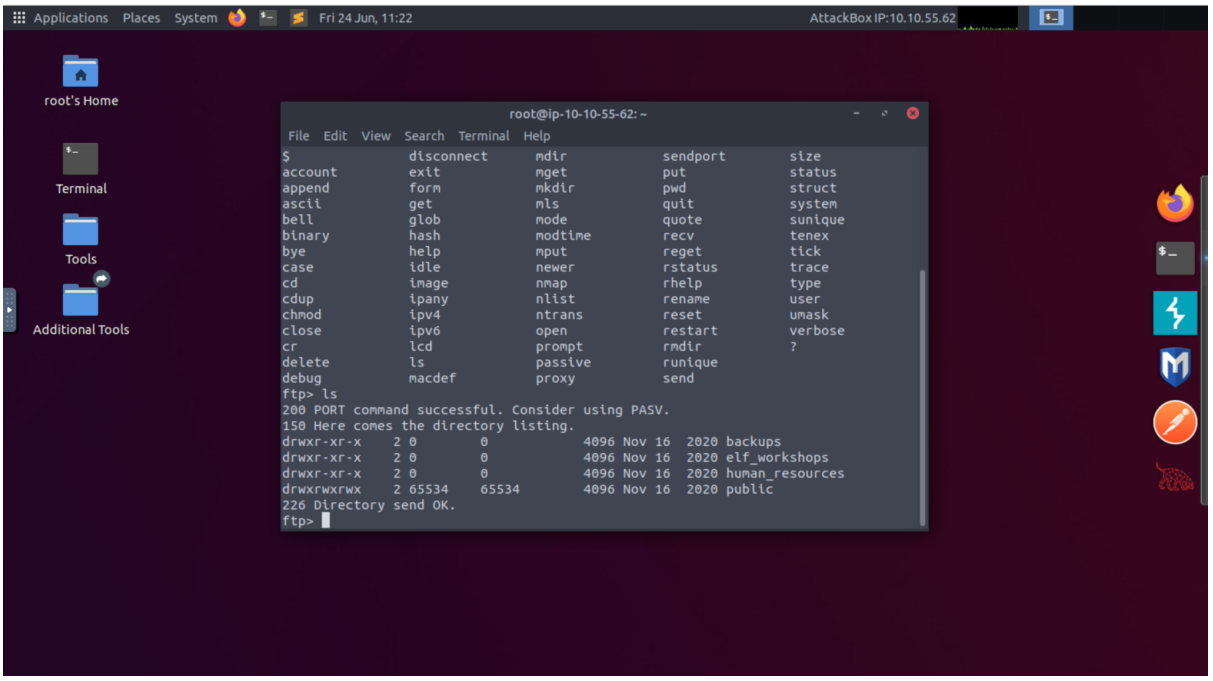
Tools used: Kali Linux

Solution/walkthrough:

Question 1

Open terminal. Scan **ftp [THM IP address]**. Login to the server using anonymous and put in the help command to see the command list. Use the **ls** command to open the directory listing.



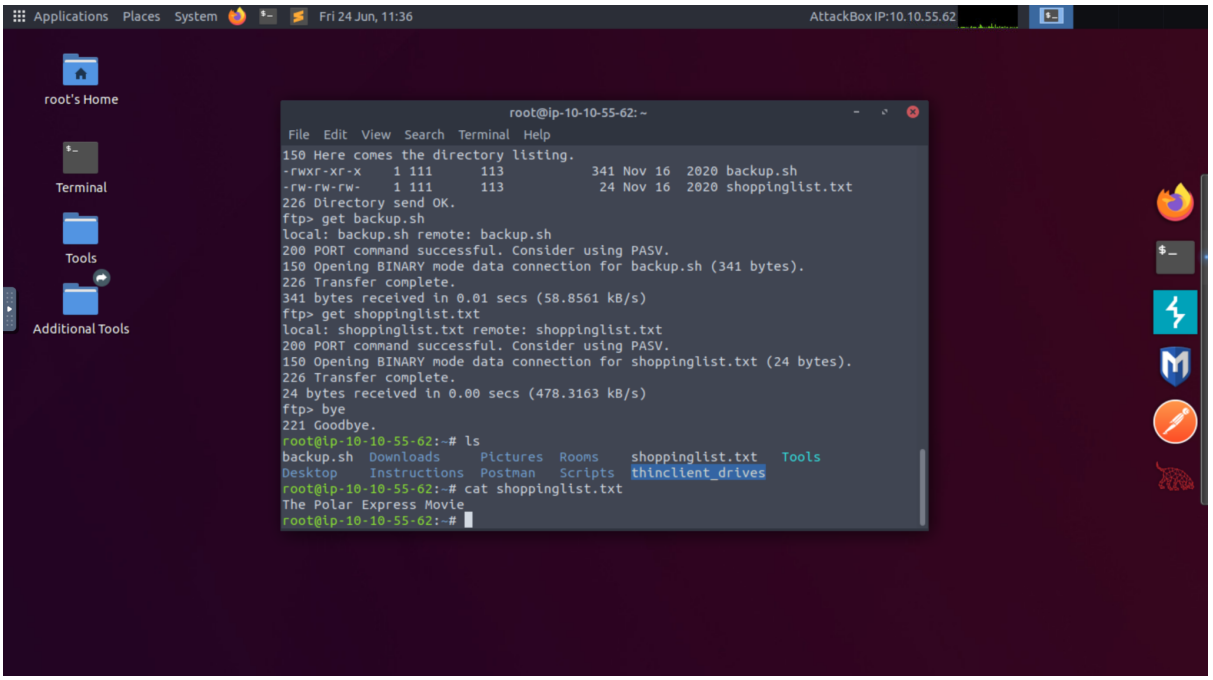


Question 2

On the directory listing, find the directory that has accessible data for the user.

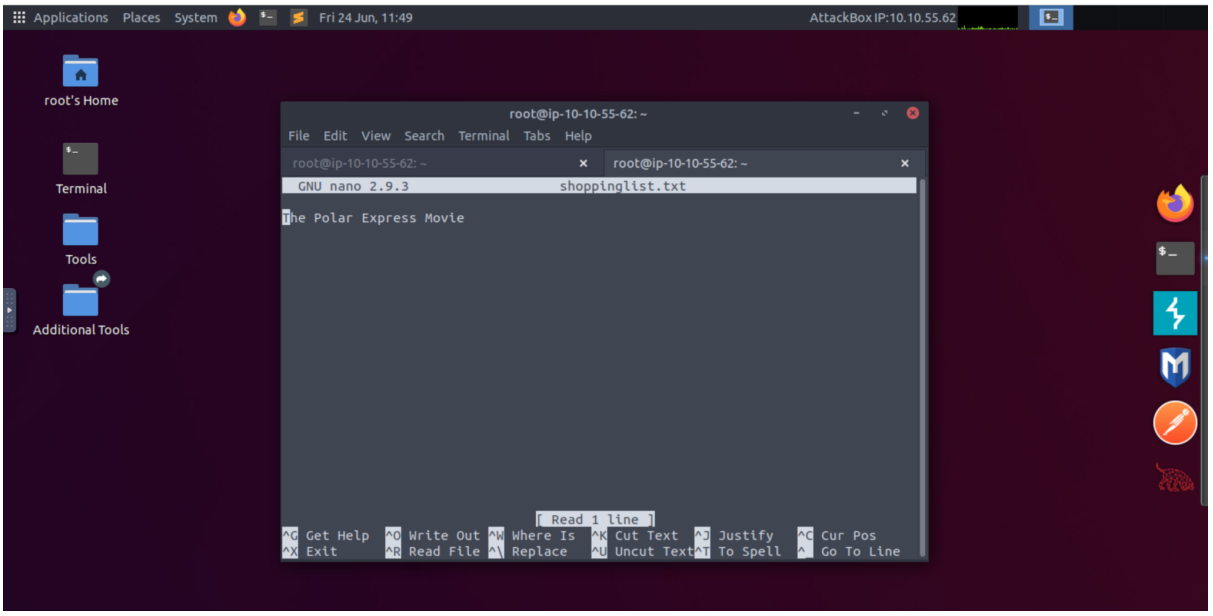
Question 3

Change the directory to public using **cd** command and open the new directory listing using **ls** to see the script being executed.



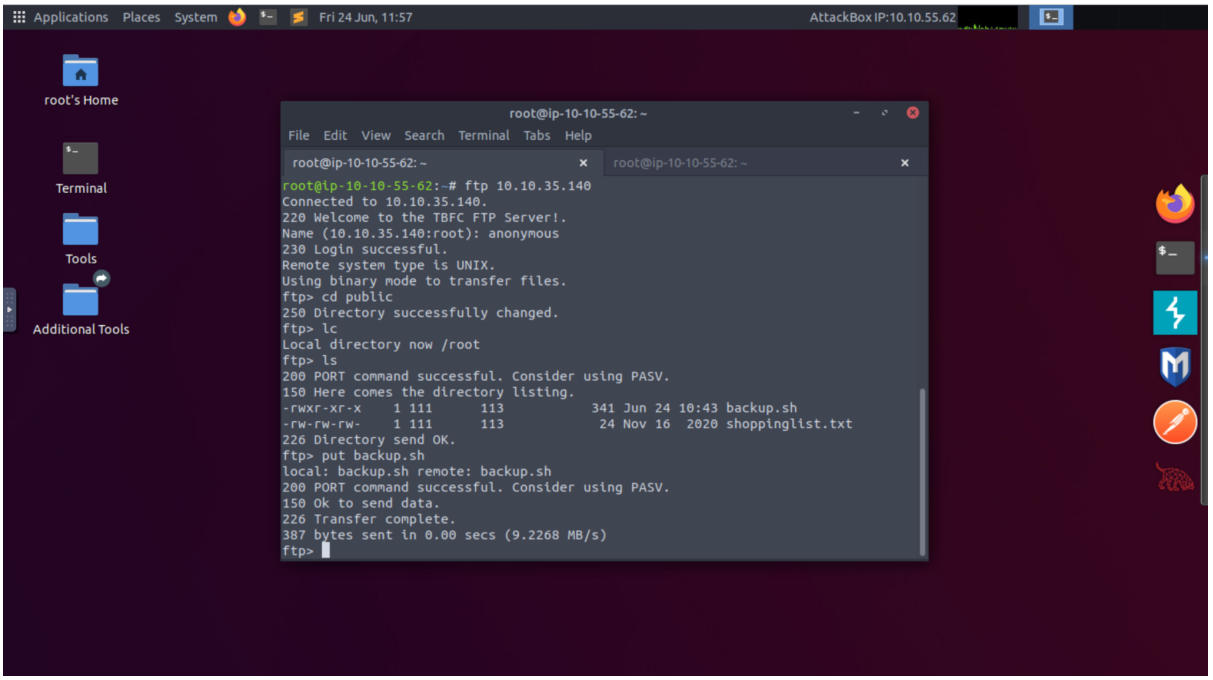
Question 4

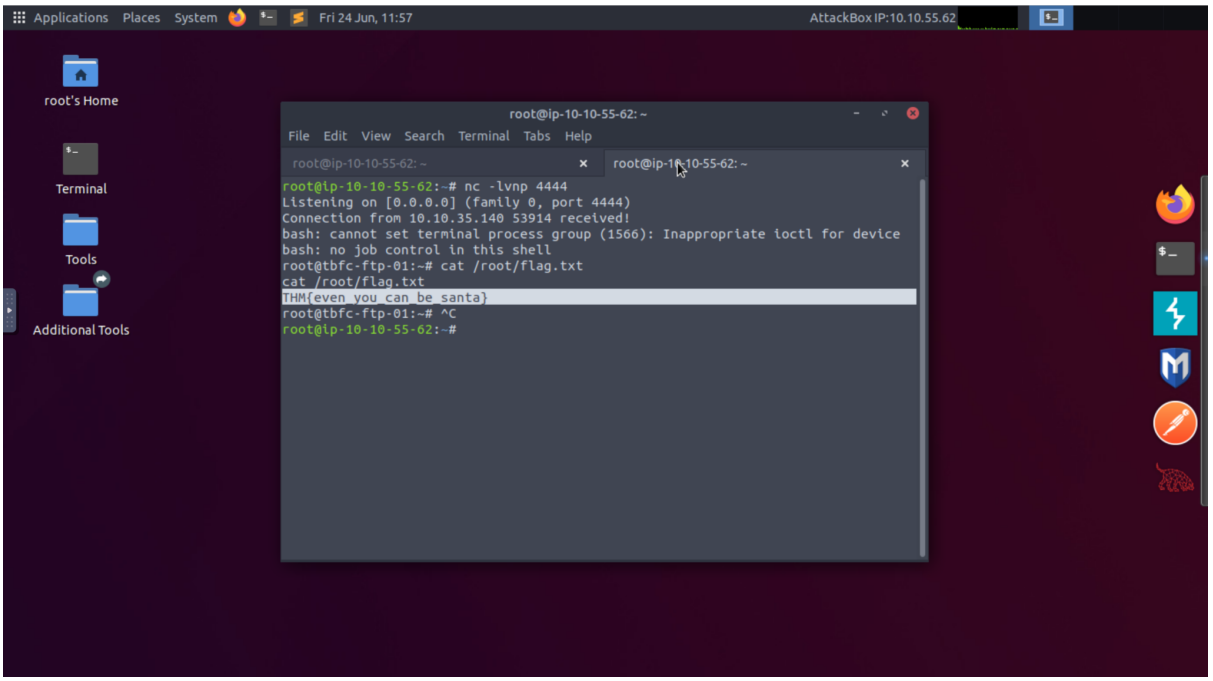
Use the **get** command to download the shoppinglist.txt file onto our device. Once downloaded, open the file on **nano**.



Question 5

Set up a netcat listener using the **nc -lvnp 4444** command in a new tab. Return to our ftp server and use the **put** command to put the file in that directory. After one minute, return to the netcat listener and execute the **cat** command to output the content of /root/flag.txt.





Thought process/methodology:

Open terminal and run the FTP server by scanning ftp [THM IP address]. In order to share data, we are required to login. By using the “anonymous” mode,

it allows a default username to be used with any password by a client. Once we've successfully logged in, use the help command to open the list commands that can be run on the FTP server. The directories available can be opened using the ls command. Analyse the directory to find the folder that has data we can access (the ones that aren't zero). After that, change the accessible folder to the working directory using the cd command. Then, use the ls command again to see the files within that directory. The file with the .sh extension is a shell file, therefore when executed it will run the commands programmed. Use the get command to download the files from the server onto our device. The files can be opened using a text terminal such as nano to see the contents of the file. Then, on a new tab on the terminal, set up a netcat listener to catch the connection on our machine using the command given by TryHackMe. On our FTP server, use the put command to upload the malicious file back onto the directory to see an output on the netcat listener. This way, we have a reverse system shell on the FTP server as the most powerful user. Any commands used will be executed on the FTP server's system. After the output is shown on the netcat listener, run the cat command on /root/flag.txt to display the content on the file and obtain the flag.

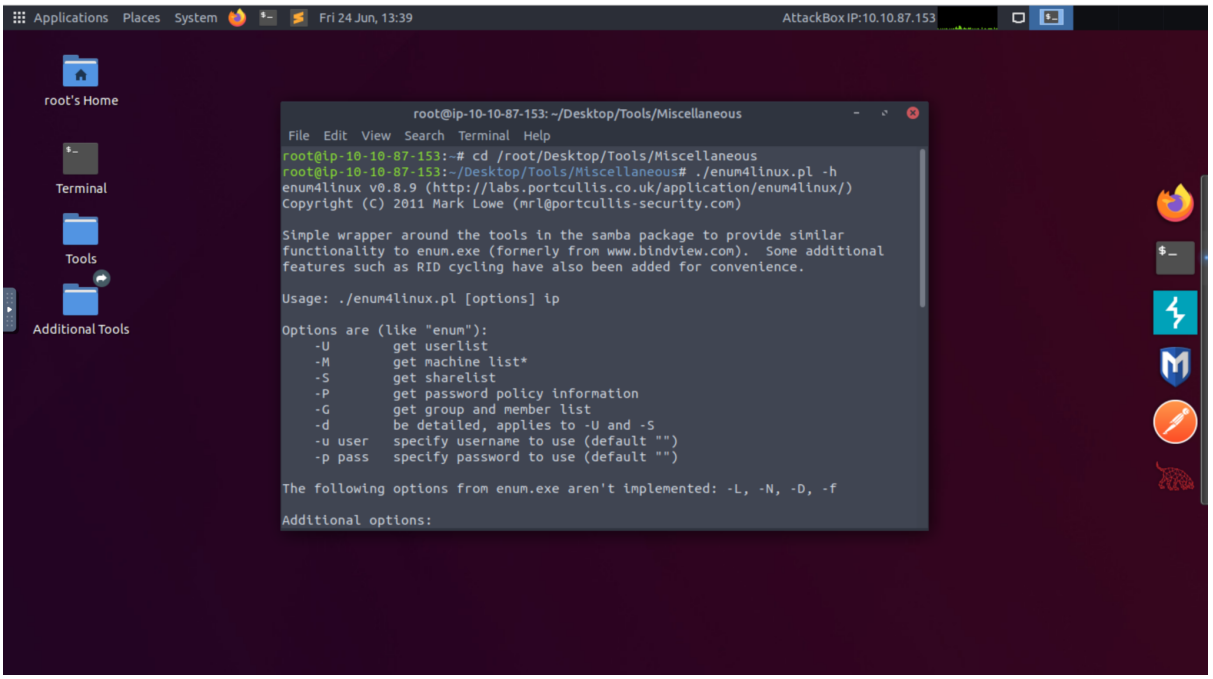
Day 10: [Networking] Don’t be so sElfish

Tools used: Kali linux

Solution/walkthrough:

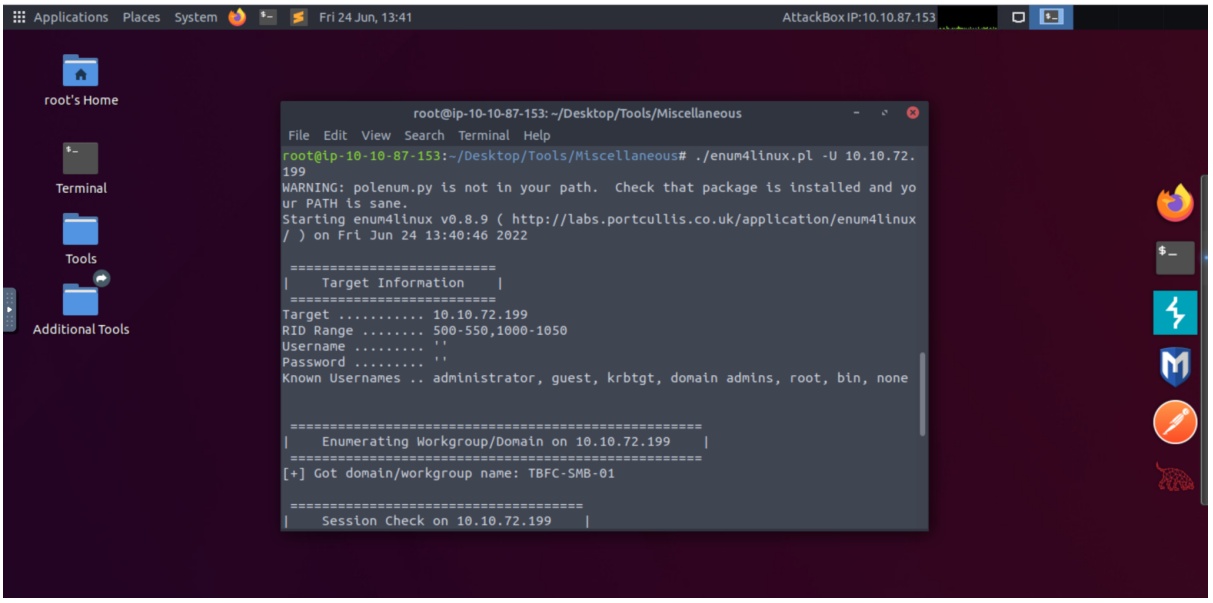
Question 1

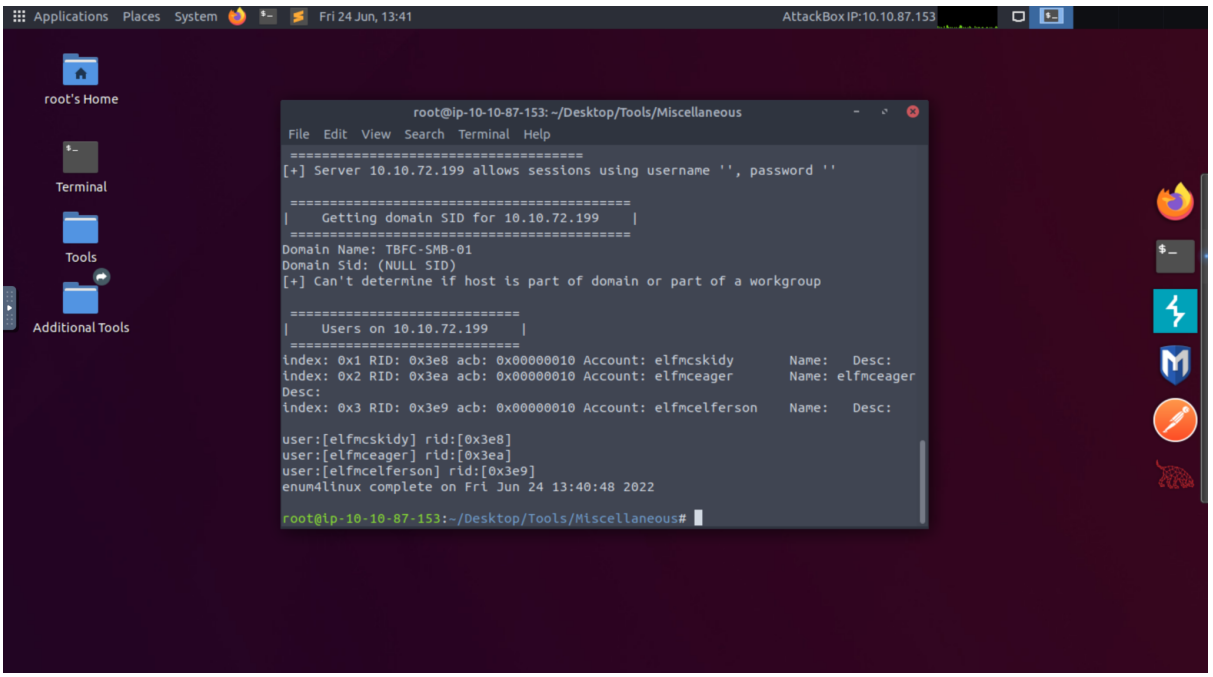
Open terminal and navigate to enum4linux using **cd /root/Desktop/Tools/Miscellaneous**. Examine the options available.



Question 2

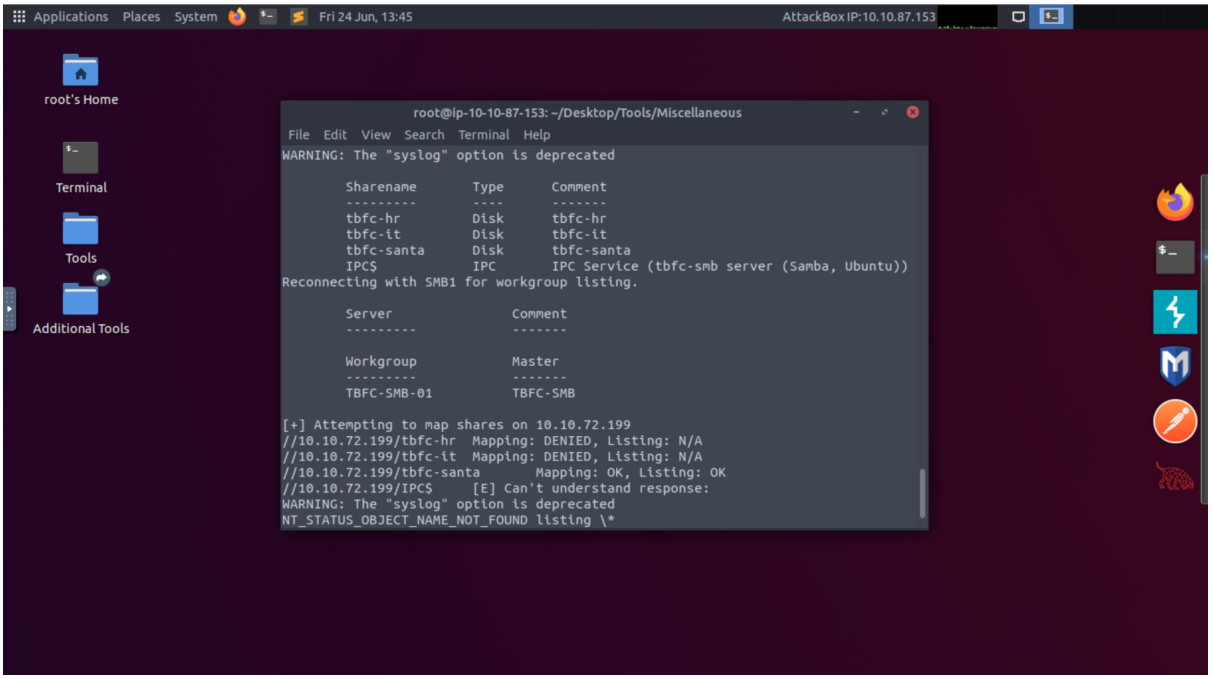
Use the **-U** flag to get userlist. Count the number of users that are listed.





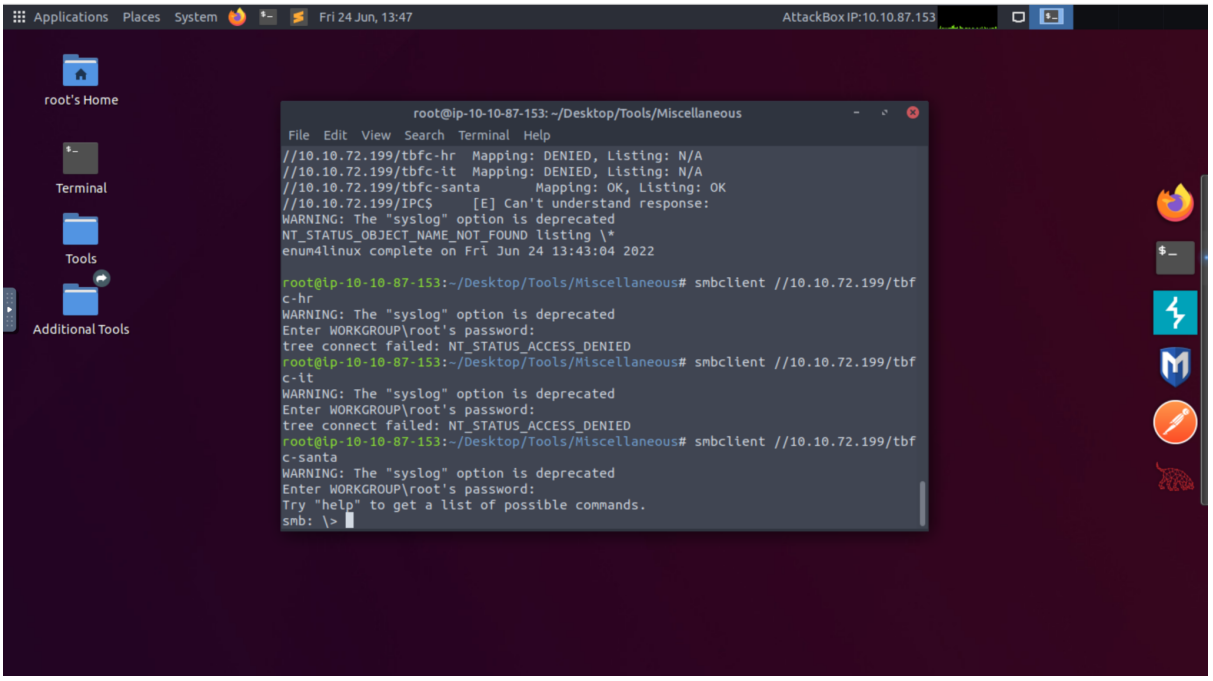
Question 3

Use the **-S** flag to get sharelist. The command is **./enum4linux.pl -S [THM IP address]**. Find the shares on the server.



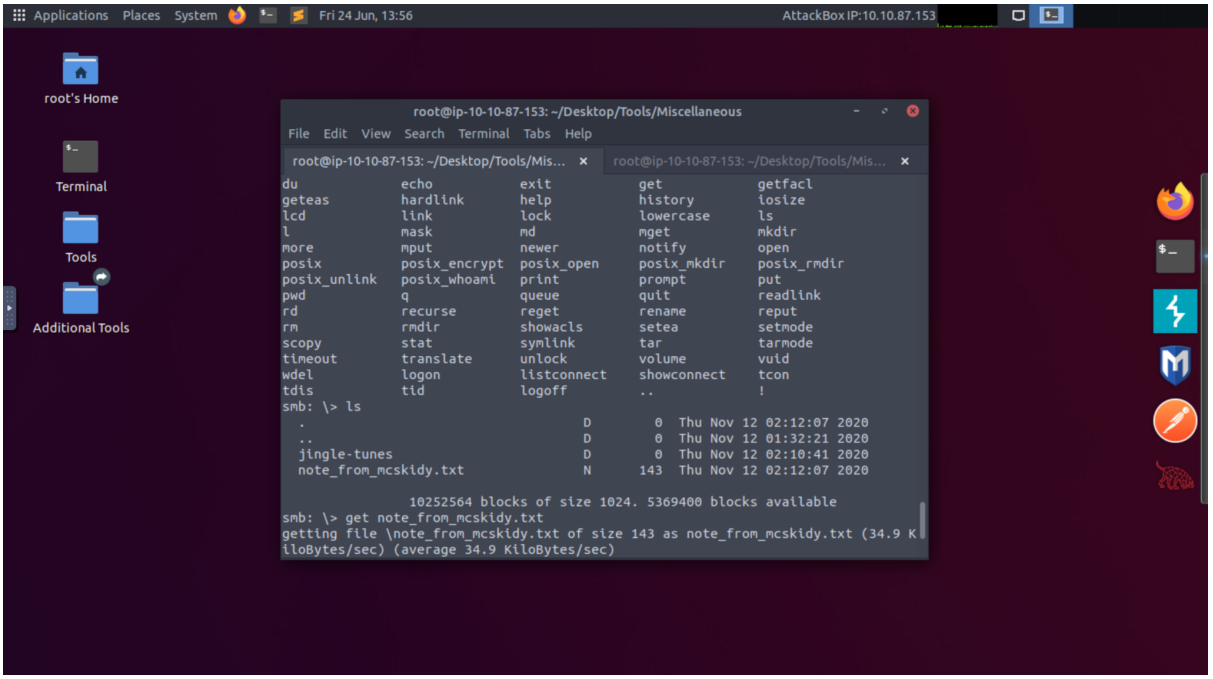
Question 4:

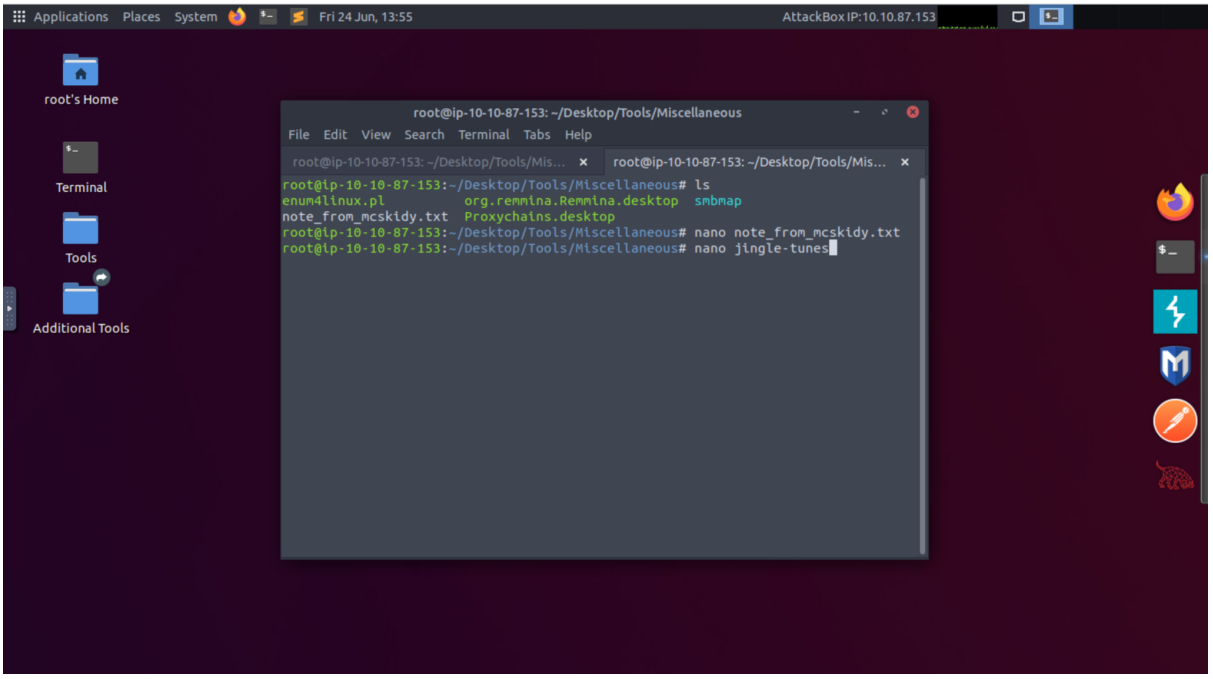
Use the smbclient command (**smbclient //**THM IP address****/****sharename****) to access the shares on the Samba server. Try each sharename and press enter until we find one we can log into without a password.

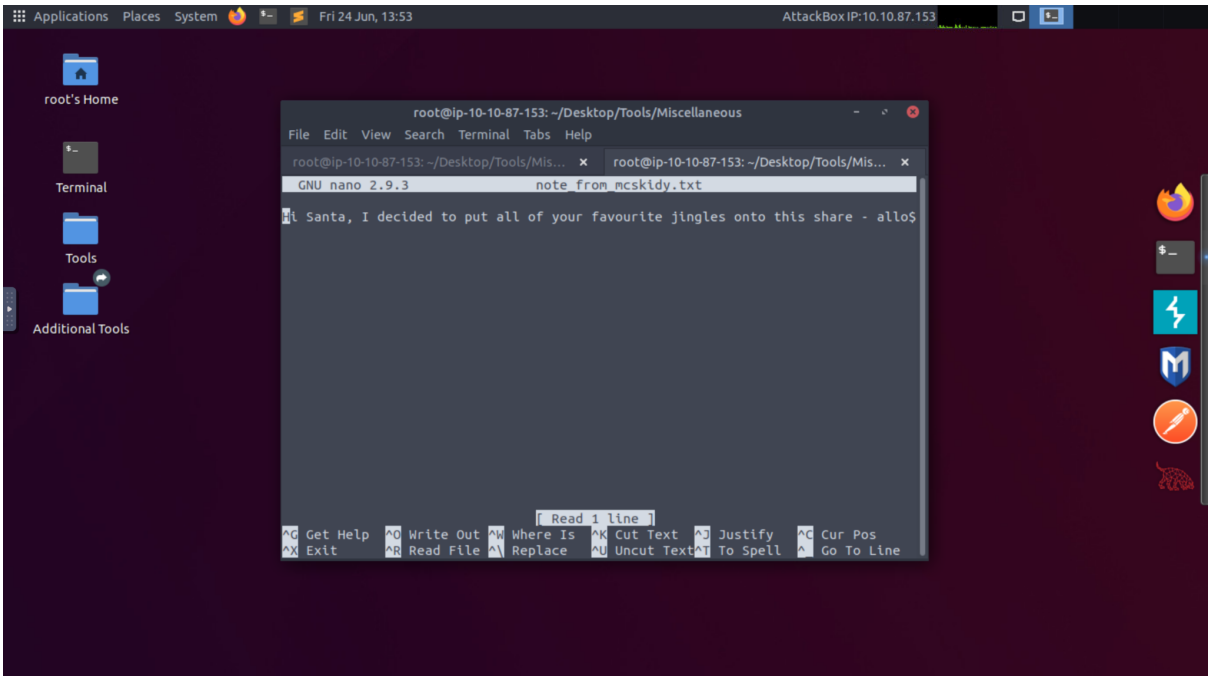


Question 5:

The **help** command will open a list of commands that can be run. Run the **ls** command to list the files in the share. Download the files using the **get** command and open the note_from_mcskidy file on **nano** to see its content.







Thought process/methodology:

Open a terminal prompt and run enum4linux. All the possible options will then be listed and the function of each flag will be given. The -U flag will show the userlist of the server where we can see the number of users and the usernames. The -S flag will show the sharelist and we will see the shares that are on the server. The smbclient tool can be used to access the Samba server and its shares. By using this tool, we can log in to each sharename manually until we find the one that doesn't require a password to log in. Once we've

logged into the share, open the directory on it using ls command and download the files in the directory onto our device using get command. This way, we will be able to open the files to see its contents. The files can be opened on a text terminal using the nano command. The note_from_mcskidy.txt file says that everything is in that share, meaning the only other file that is in the directory of the share is the directory Elf McSkidy left for Santa.