PSP0201
Week 3
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 6: Be careful with what you wish on a Christmas night

Tools used: google, attack box, Firefox, ZAP

Solution/walkthrough:

Question 1:

We searched in google to get the correct answer.

Input validation strategies

Input validation should be applied on both **syntactical** and **Semantic** level.

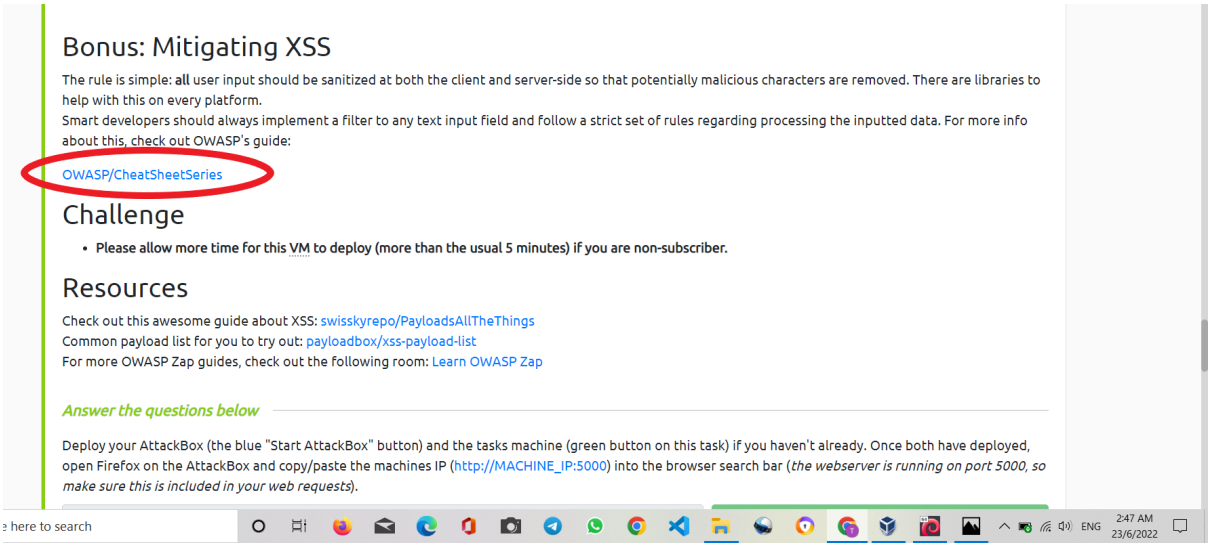
Syntactic validation should enforce correct syntax of structured fields (e.g. SSN, date, currency symbol).

Semantic validation should enforce correctness of their *values* in the specific business context (e.g. start date is before end date, price is within expected range).

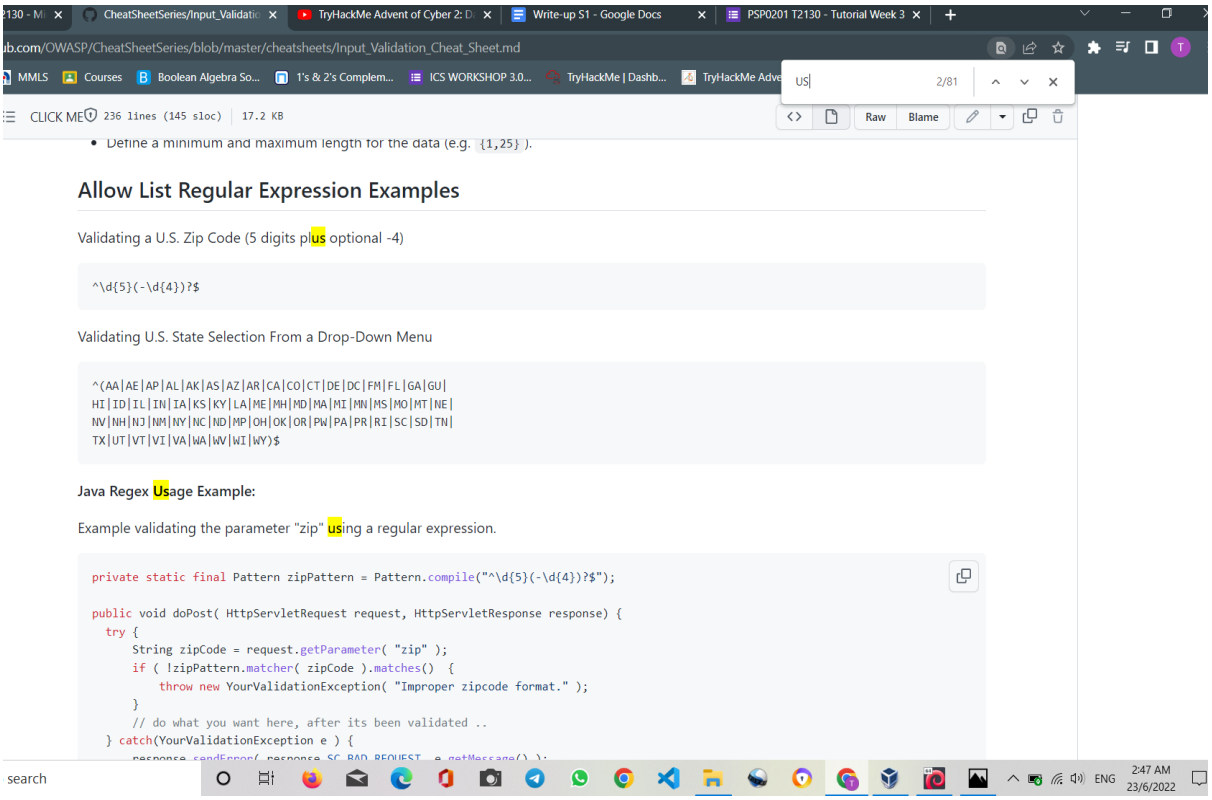
It is always recommended to prevent attacks as early as possible in the processing of the user's (attacker's) request. Input validation can be used to detect unauthorized input before it is processed by the application.

Question 2:

We open the link given to go to OWASP cheat sheet to find US zip code

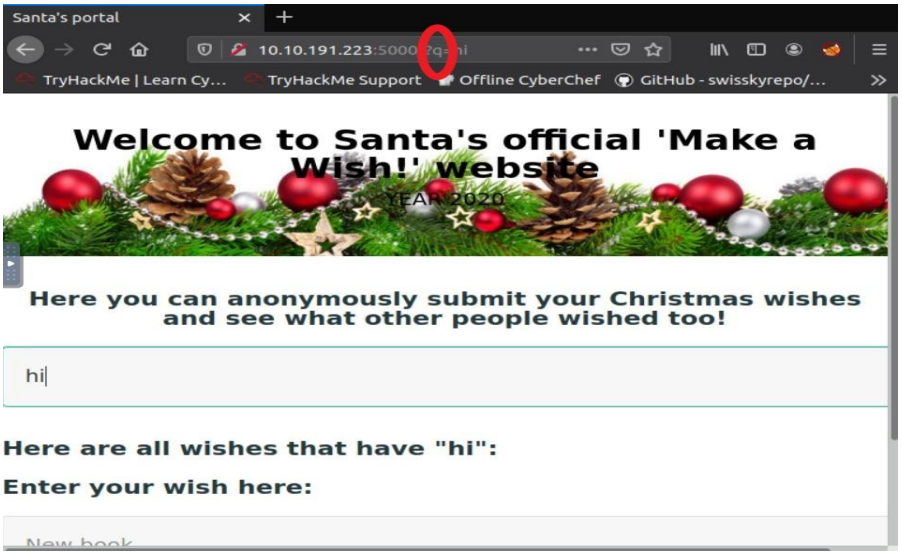


Press ctrl F then searsh for US. Then scroll down to get the answer.



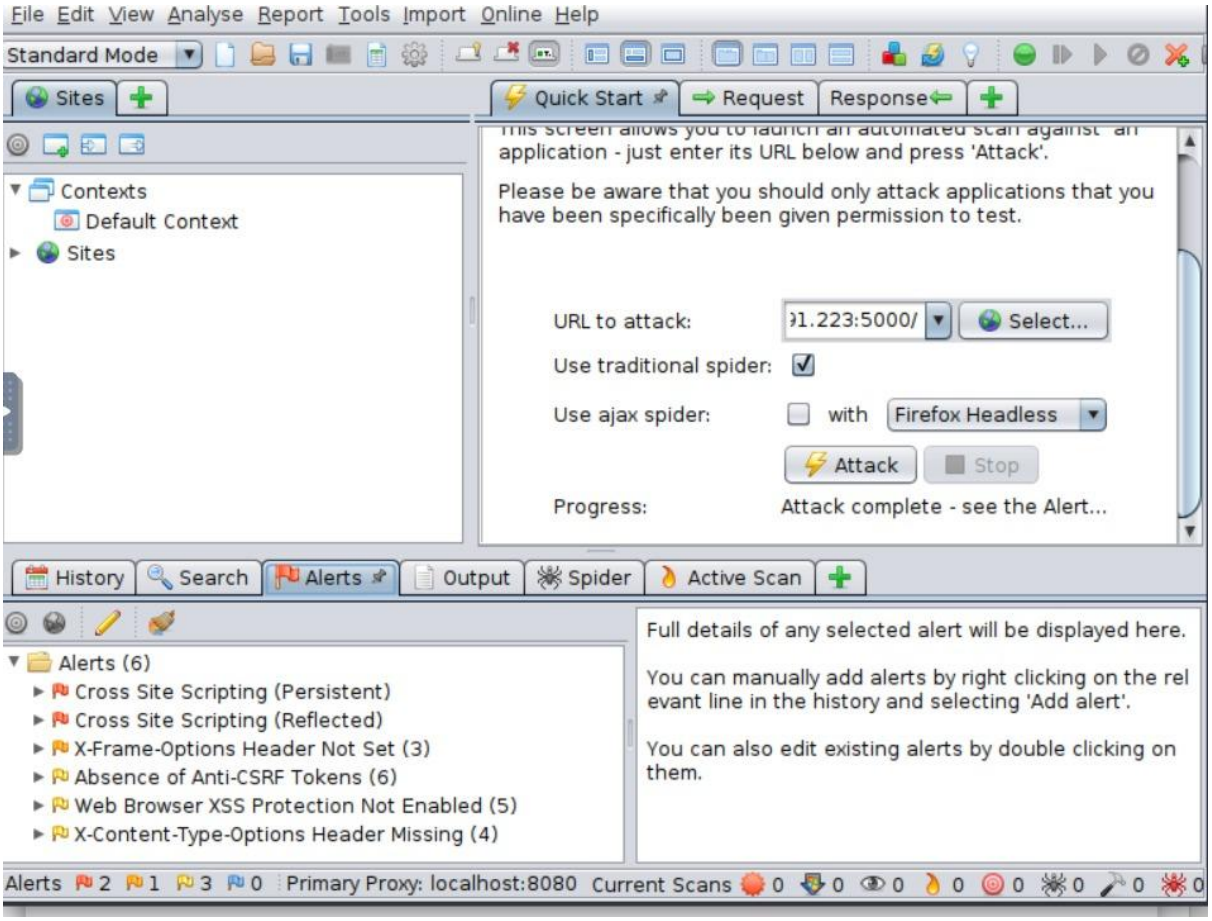
Question 4:

This is the query string can be abused to craft a reflected XSS. We will get this when type hi in query.



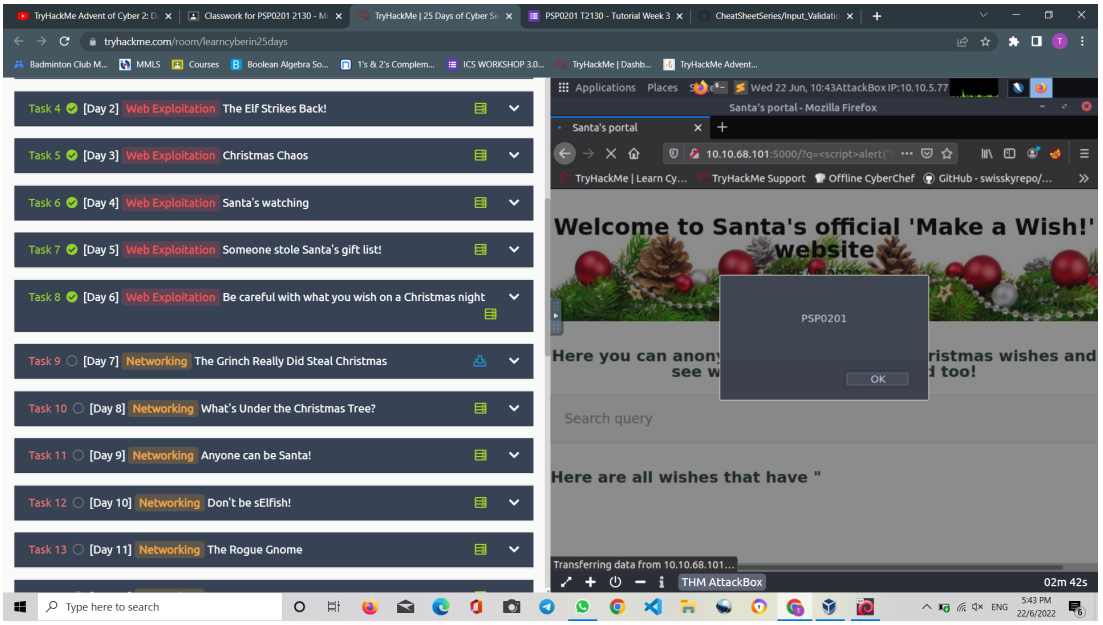
Question 5:

There are 2 XSS alerts of high priority are in the scan.



Question 6:

(<script>alert("PSP0201")</script>)put in the wish text box if we want to show an alert saying "PSP0201"



Question 7 :

After close my browser and revisit the site MACHINE-IP:5000 again it does persist XSS attack. We tried the question 6 after off and revisit the site.

Thought Process/Methodology:

Firstly, we start the machine and also the attack box. After get the IP address we type it in firefox in attackbox. Then we need to add :5000 behind our IP address. “Make a wish” website will appear. There is search query too in that page. So can type anything to get the query string. Our team typed hi then we get the string(q). Then go to application to open the OWASP ZAP. Choose automated scan and paste our make a wish website url at there and click attack. Then the alerts will show up. From that we can know that there are 2 types of XSS are there in the scan.(persistent and reflected). Then we went to the make a wish site and (<script>alert("PSP0201")</script>) put this in search query and also at the wish. Lastly, we manage to get to show an alert saying "PSP0201".

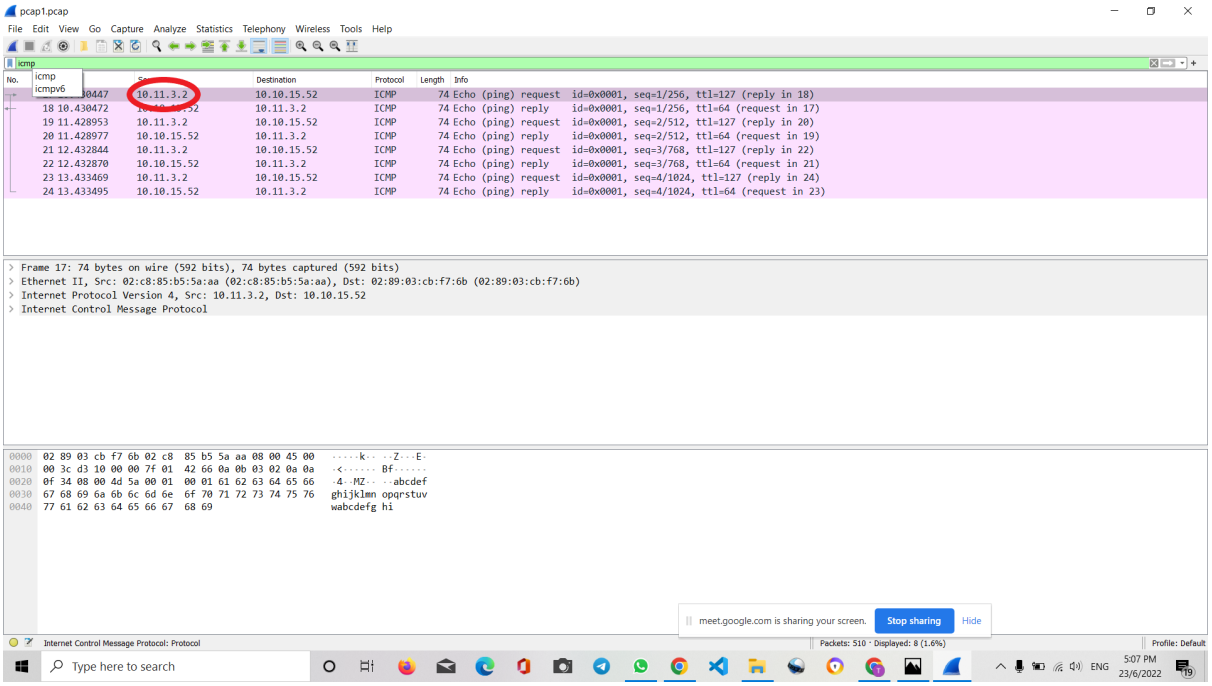
Day 7: The Grinch Really Did Steal Christmas

Tools used: google,wireshark

Solution/walkthrough:

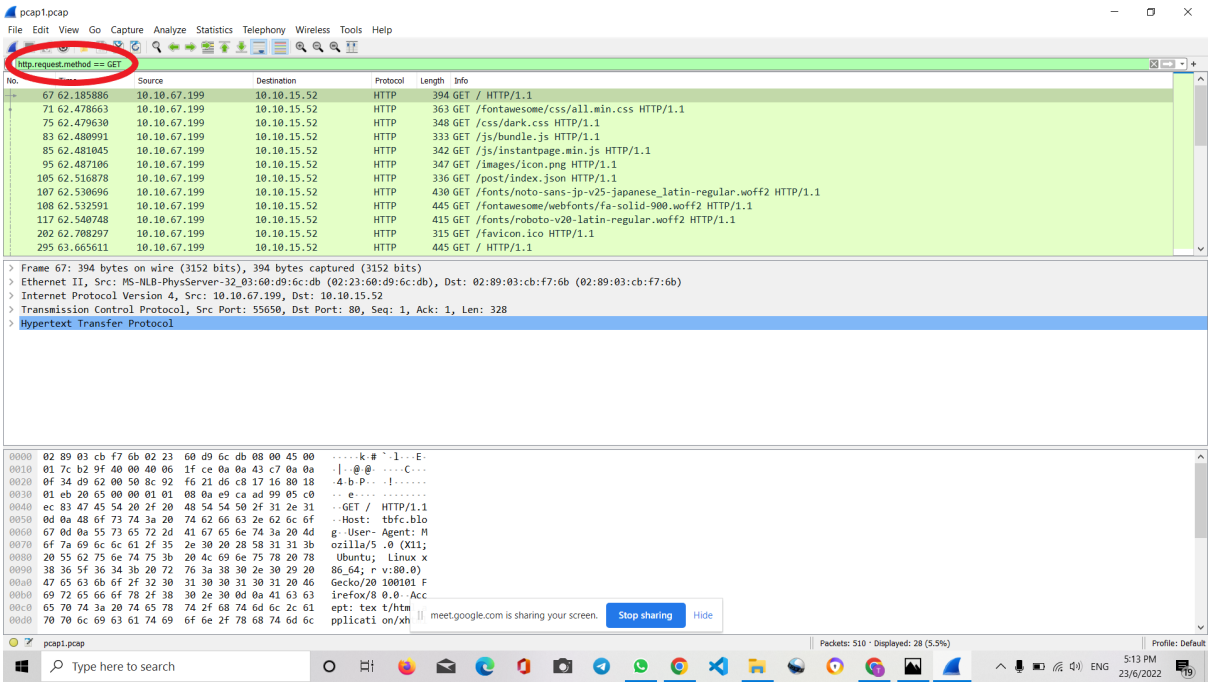
Question 1:

Open "pcap1.pcap" in Wireshark and type icmp to get the IP address. The first line is the answer (get IP address from source).



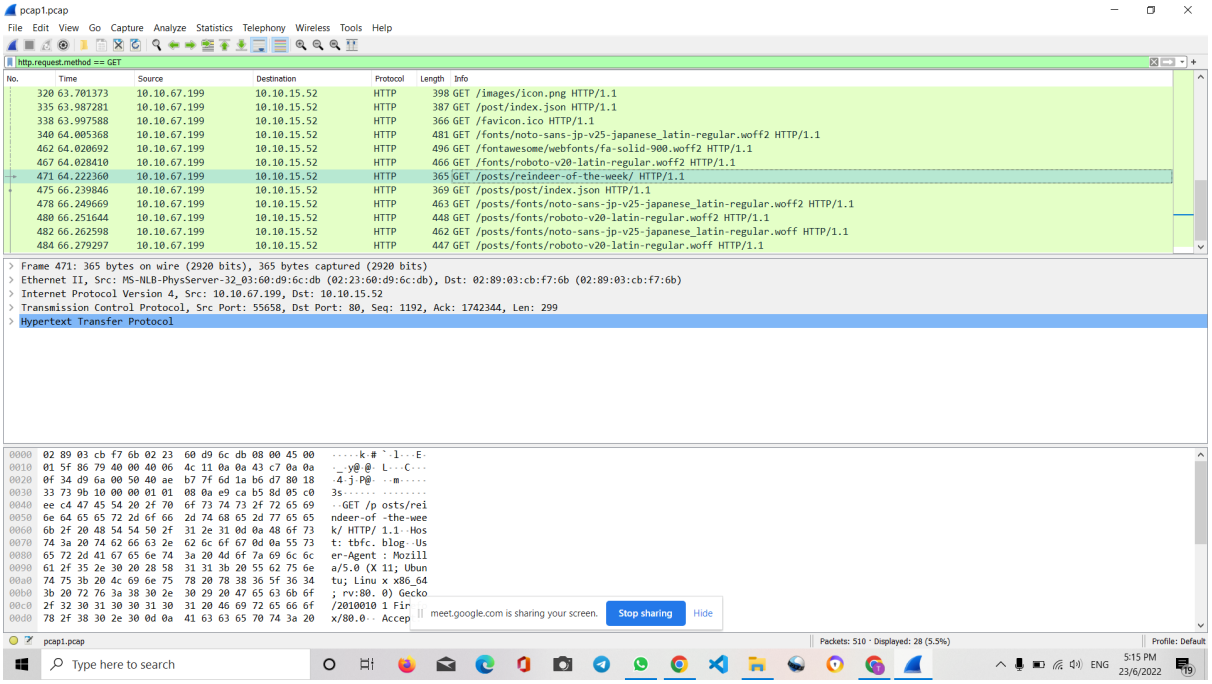
Question 2:

This is the filter we used to see HTTP GET requests.



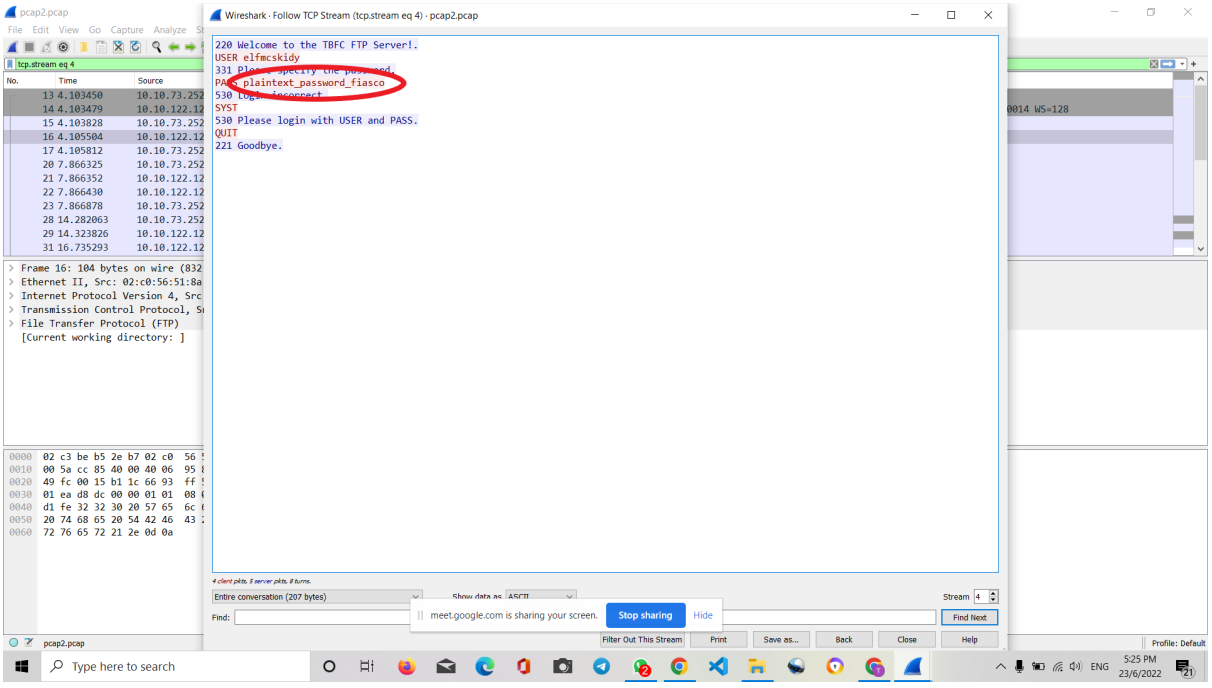
Question 3:

The name of the article that the IP address "10.10.67.199" visited is shown at the blue line which we clicked for the answer.



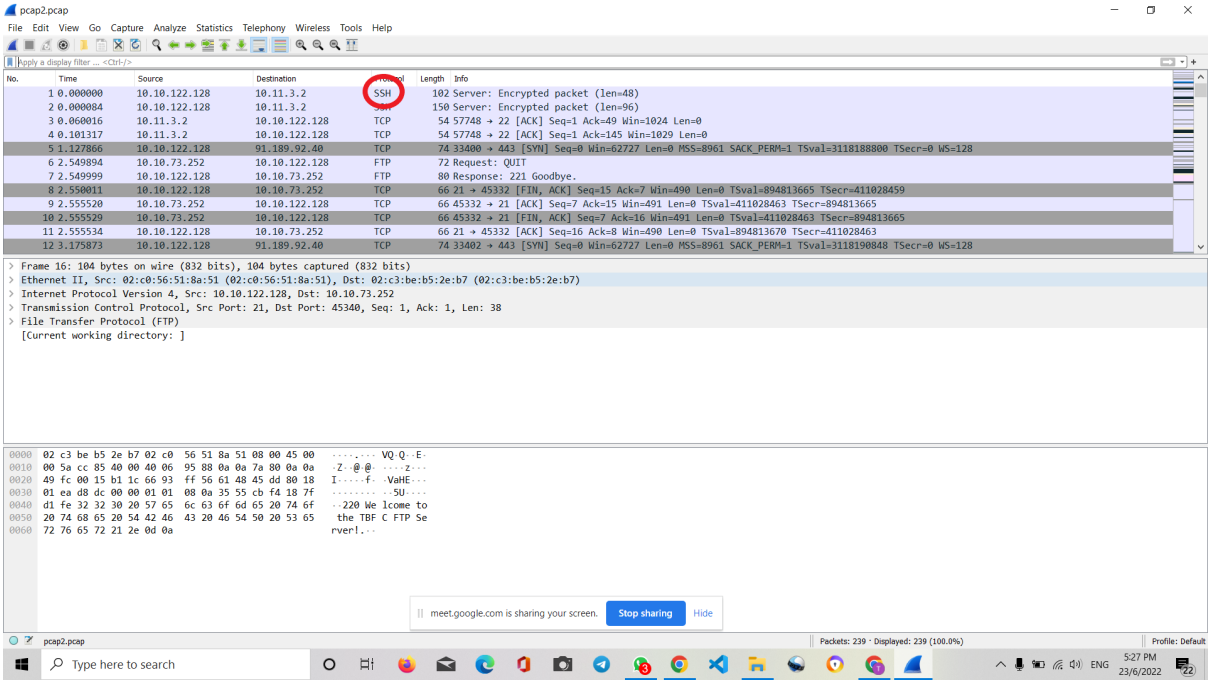
Question 4:

Password was leaked during the login process.



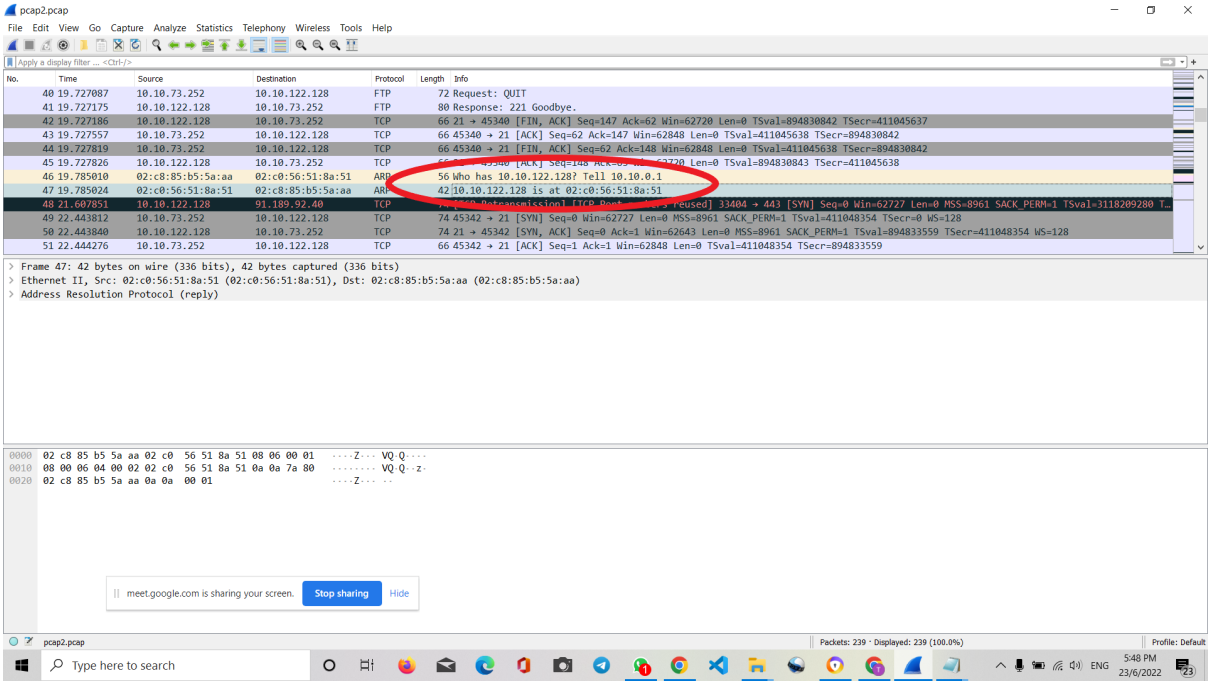
Question 5:

The name of the protocol that is encrypted is shown there. (circled in red)



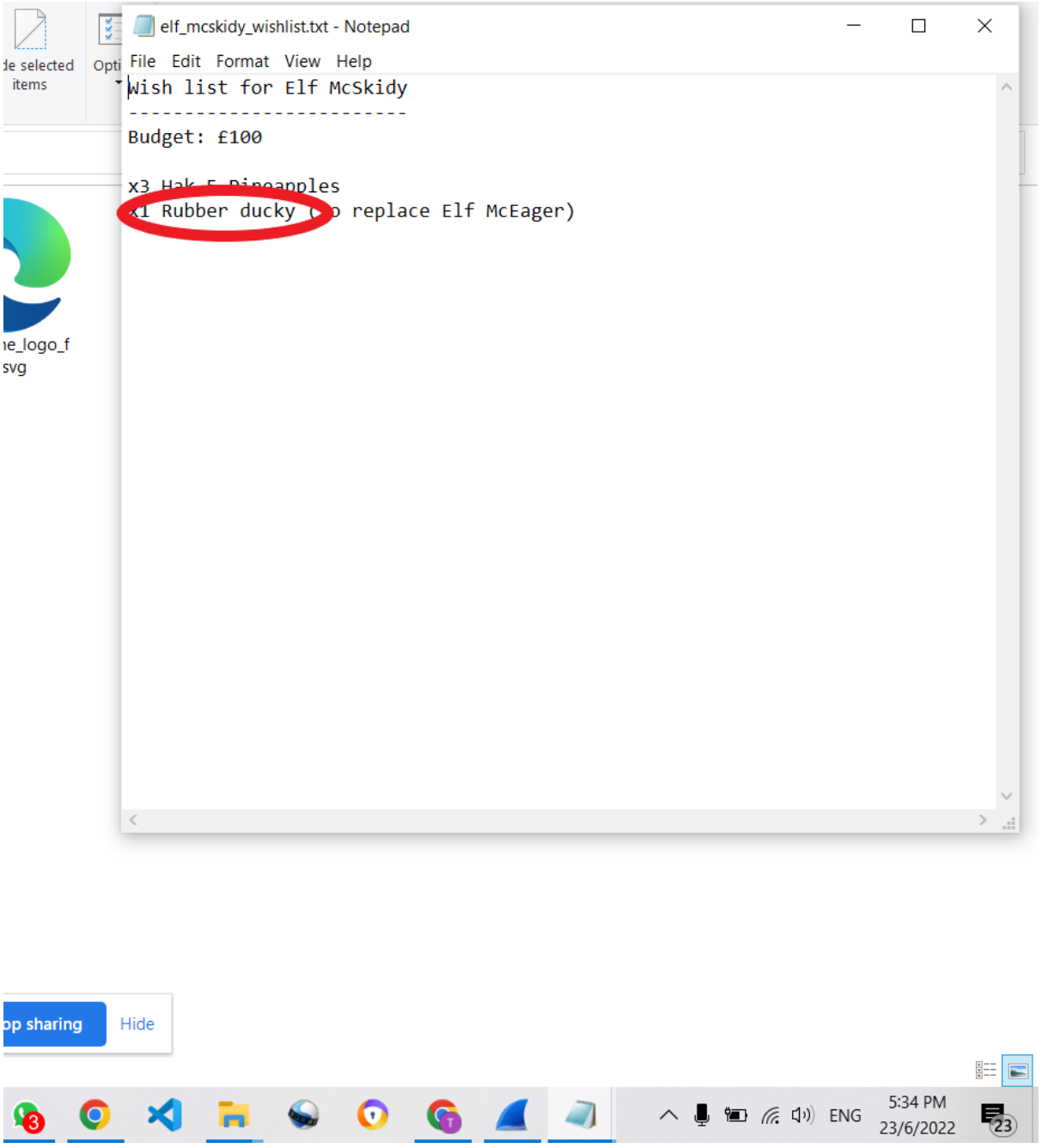
Question 6:

We get answer when scroll in "pcap2.pcap"



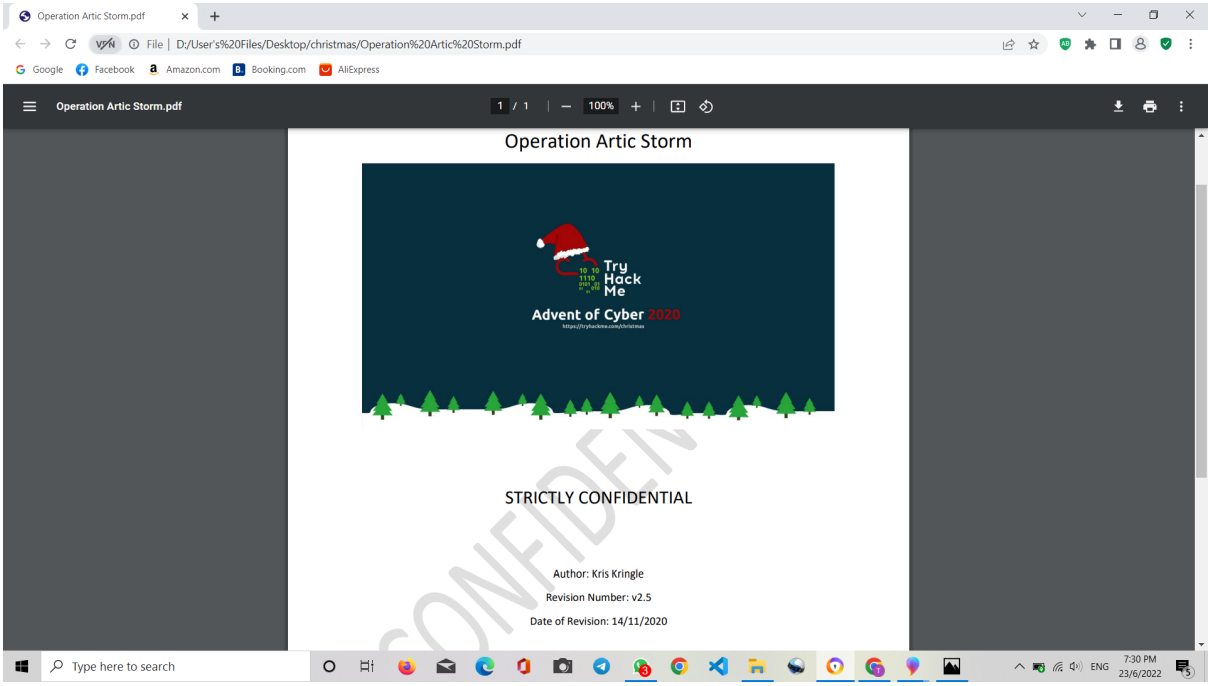
Question 7:

We have to download the christmas.zip to get the answer for question 7 and 8.



Question 8:

Get this pdf from the extracted christmas file. We will be able to identify the author.



Thought Process/Methodology:

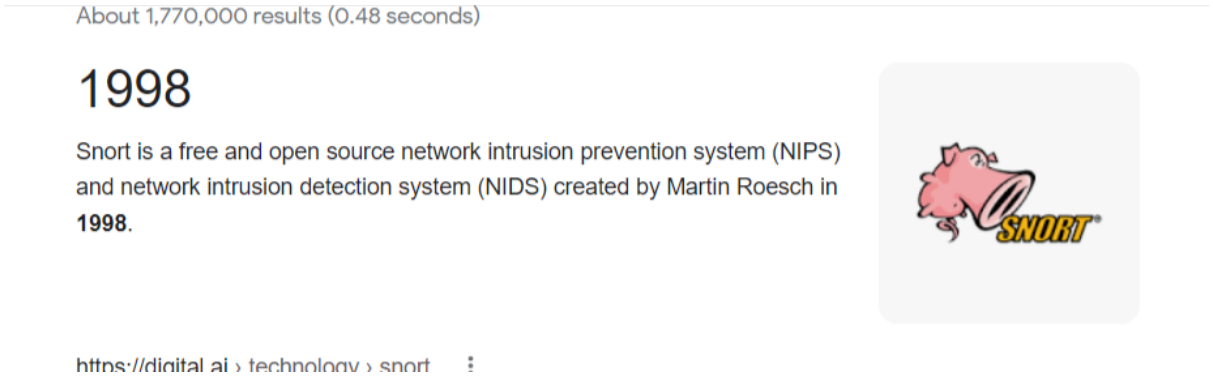
Firstly, we are supposed to download the files that's given and then install Wireshark. Once, it's downloaded we must extract the files.Open the extracted file in the Wireshark. After opening the files we started to find the IP address that initiates an ICMP/ping.We eventually guessed the filter because that's the format to get any type of request.To find out the visited pages we used the IP address that's given and add an extra part to it to filter so i can get a better view at pcap files.Later, we search specifically for ftp traffic by using the actual port that is involved and we have one out of four filters for that which we can do with the tcp dot port.We followed the tcp stream and then got the answer.In this pcap2.pcap there are lot of packets use differences type of protocol to transfer data over network the only encrypted protocol in here is SSH so answer is SSH.The next question we just scrolled to the list to find the matching details that were given. In pcap file when elf are transferring file they must use the http method so type http.request.method. There were two packets and we have to find the packet with matching details and extract the files.once we get the wishlist we could find the wishlist that will be used to replace Elf McEage.Lastly, for the author we just need to open the pdf from extracted files .

Day 8: What's Under the Christmas Tree?

Tools used: Attackbox, google and kali terminal

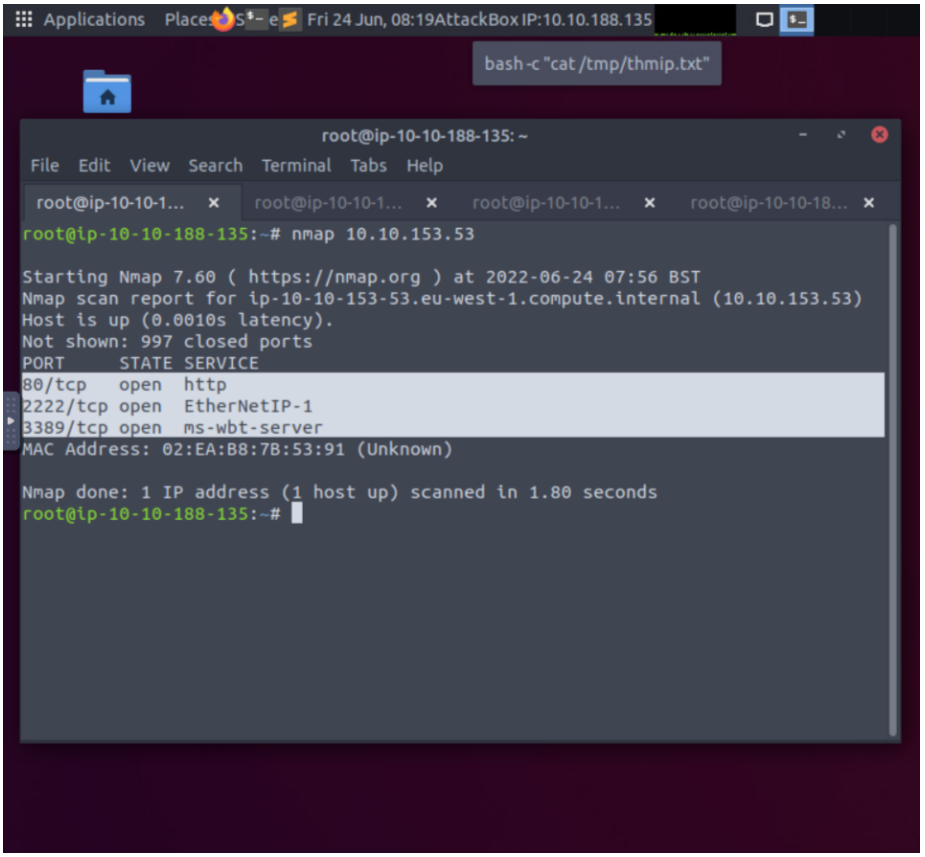
Question 1

We google searched on the year of when Snort was created.



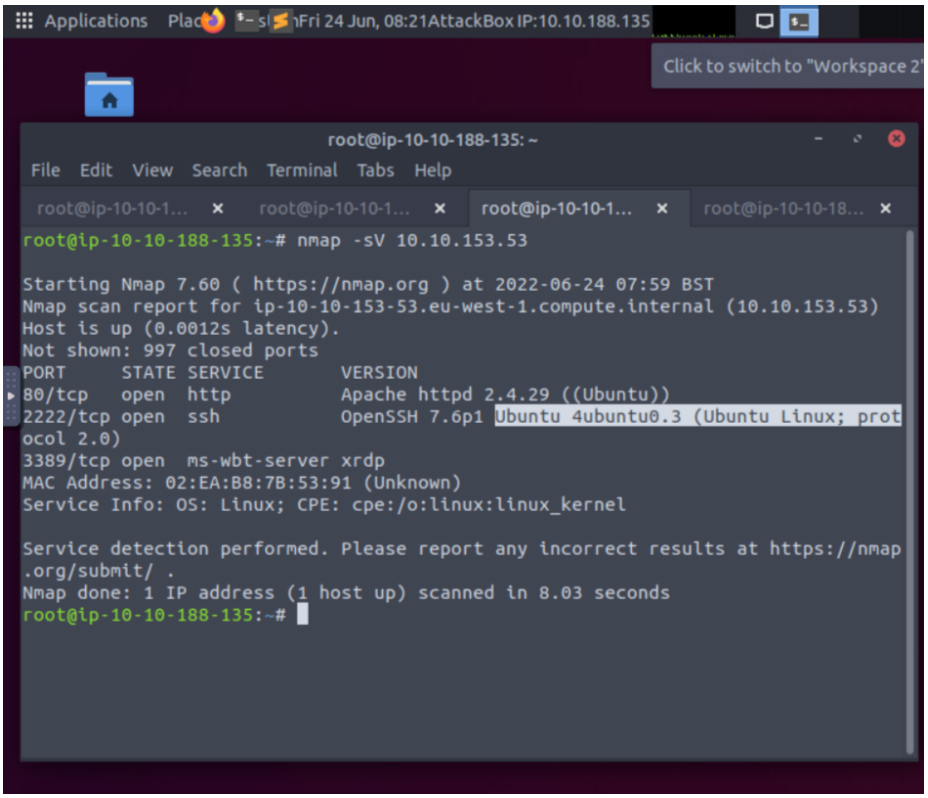
Question 2

We used Nmap on MACHINE_IP and found the port numbers of the three services running which are 80, 2222 and 3389.



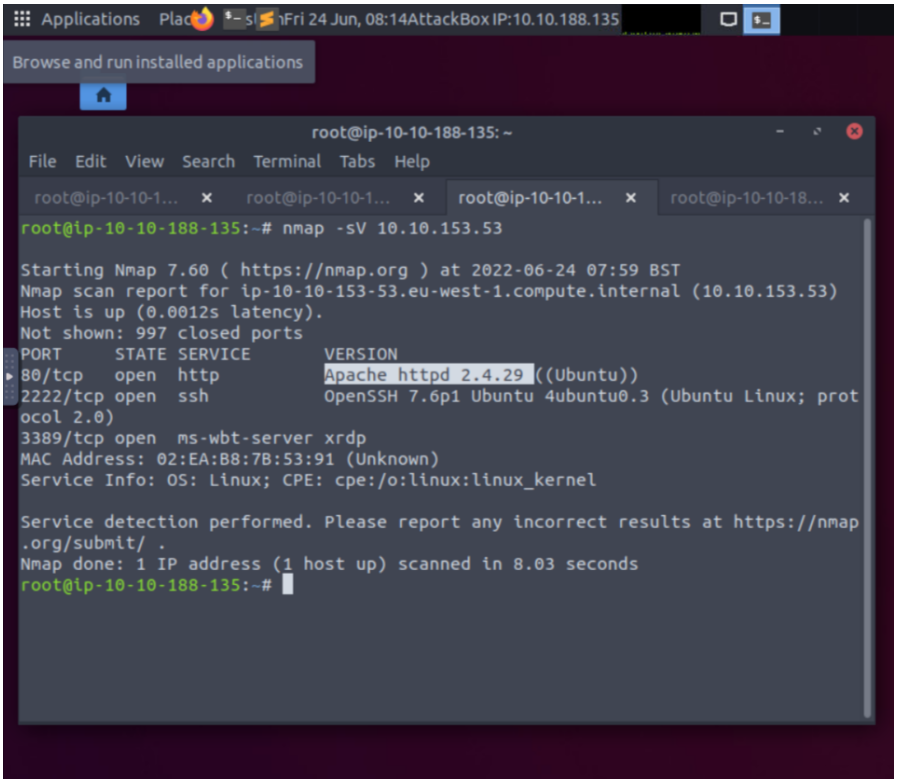
Question 3

We used Nmap -sV on MACHINE_IP and we got to determine the name of the Linux distribution that is running which is “Ubuntu”.



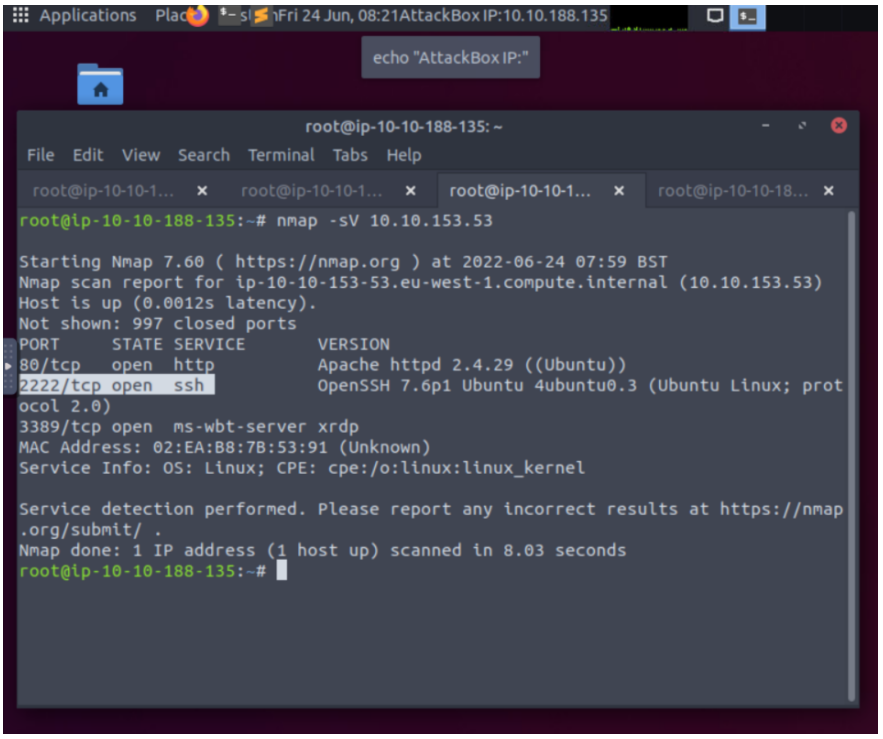
Question 4

We used Nmap -sV on MACHINE_IP again to get the version number of Apache which is 2.4.29.



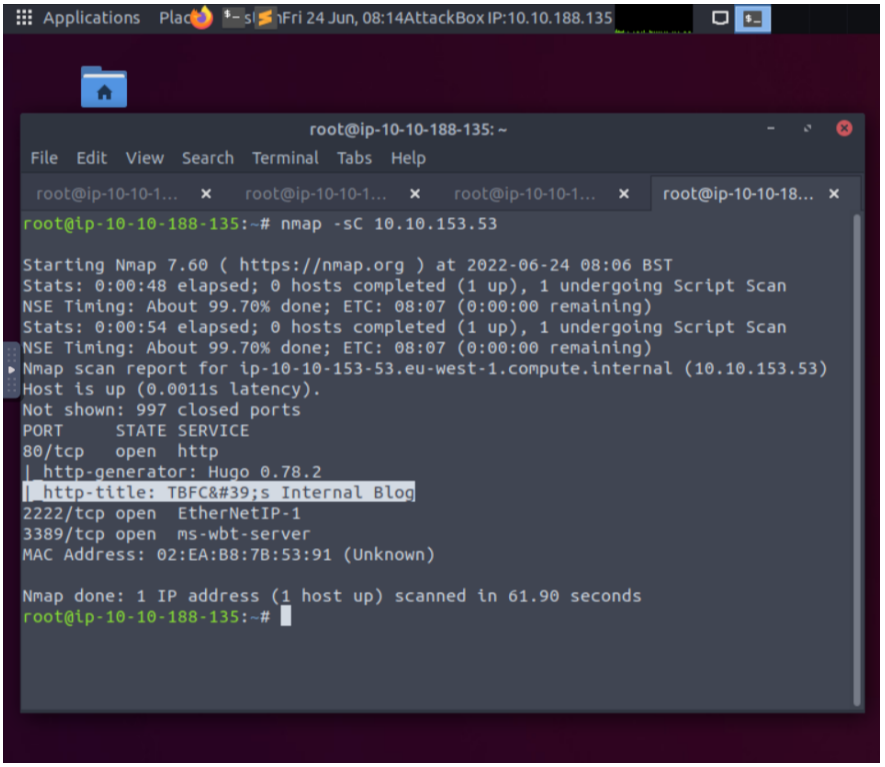
Question 5

We used Nmap -sV on MACHINE_IP again to search for the service running on port 2222 which is SSH.



Question 6:

We used Nmap -sC on MACHINE_IP and we found out that “http-title” is used for Internet Blog.



Thought Process/Methodology:

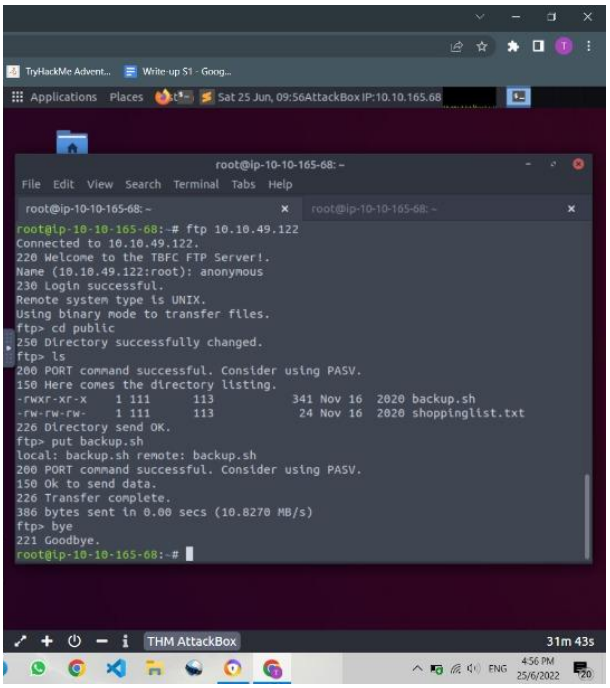
Firstly, we went to the tryhackme website and we started our machine and attack box. Then, we did research on the year when Snort was created on google which was in 1998. After that, we used the terminal and we typed in Nmap on MACHINE_IP and Nmap -Pn on MACHINE_IP and we were able to receive our port numbers which are 80, 2222 and 3389. Next, we made a new tab and we typed in Nmap -sV on MACHINE_IP and we were able to get the name of the Linux distribution that is running which is "Ubuntu", we are able to get the version of Apache which is version 2.4.29 and we are also able to get the service that is opened on port 2222 which is SSH. Last but not least, we typed in Nmap -sC on MACHINE_IP and we were able to get the http title which is used for Internet Blog.

Day 9: Anyone can be santa

Tools used: Attackbox, google

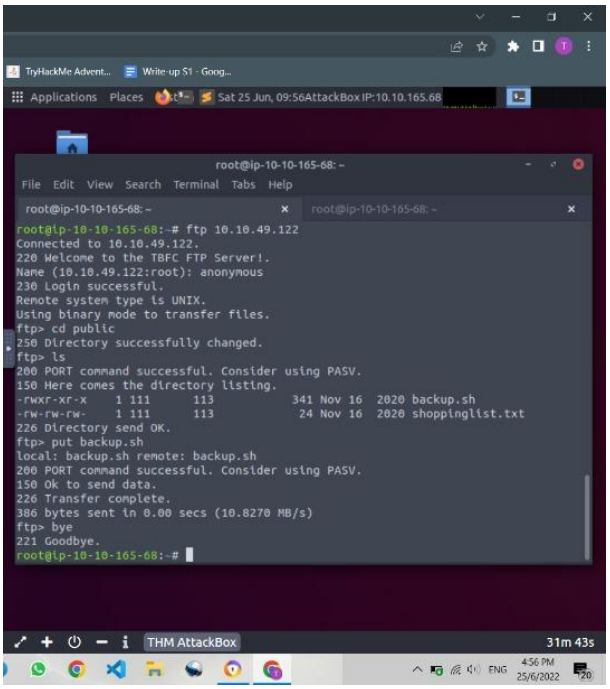
Question 1

We used terminal in Attack box and ran ftp in the terminal in order to get the directories that can be found.



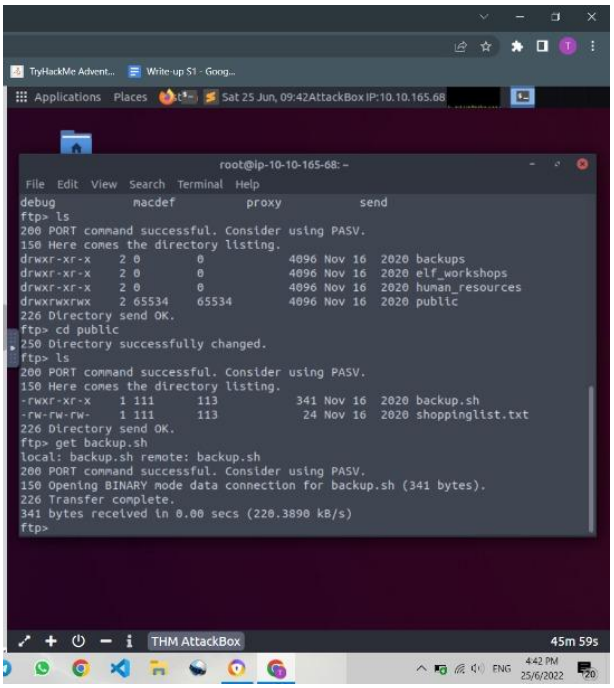
Question 2

We login ftp server as an anonymous user and found out where the data is accessible for anonymous users.



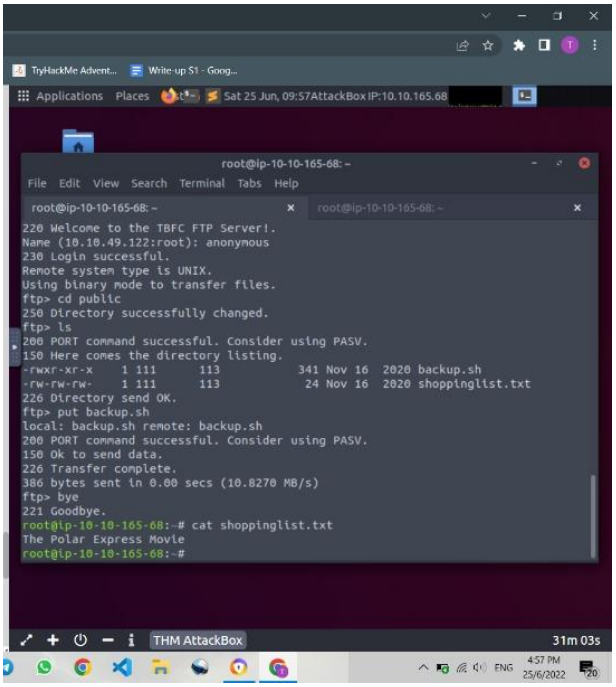
Question 3

We used “backup.sh” script in order to execute within this directory.



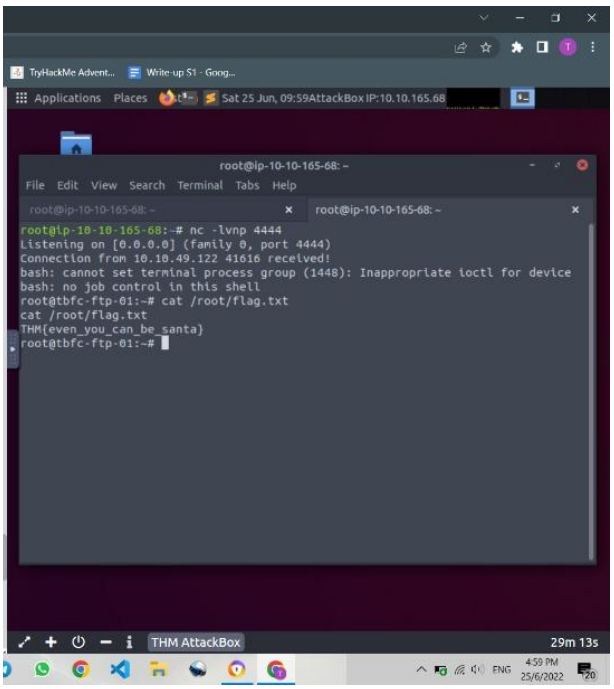
Question 4

We typed “cat shoppinglist.txt” in the directory and executed it in order to know which was Santa’s shopping list.



Question 5

We typed “ Cat/root/flag.txt” in another directory tab in order to get the flag.



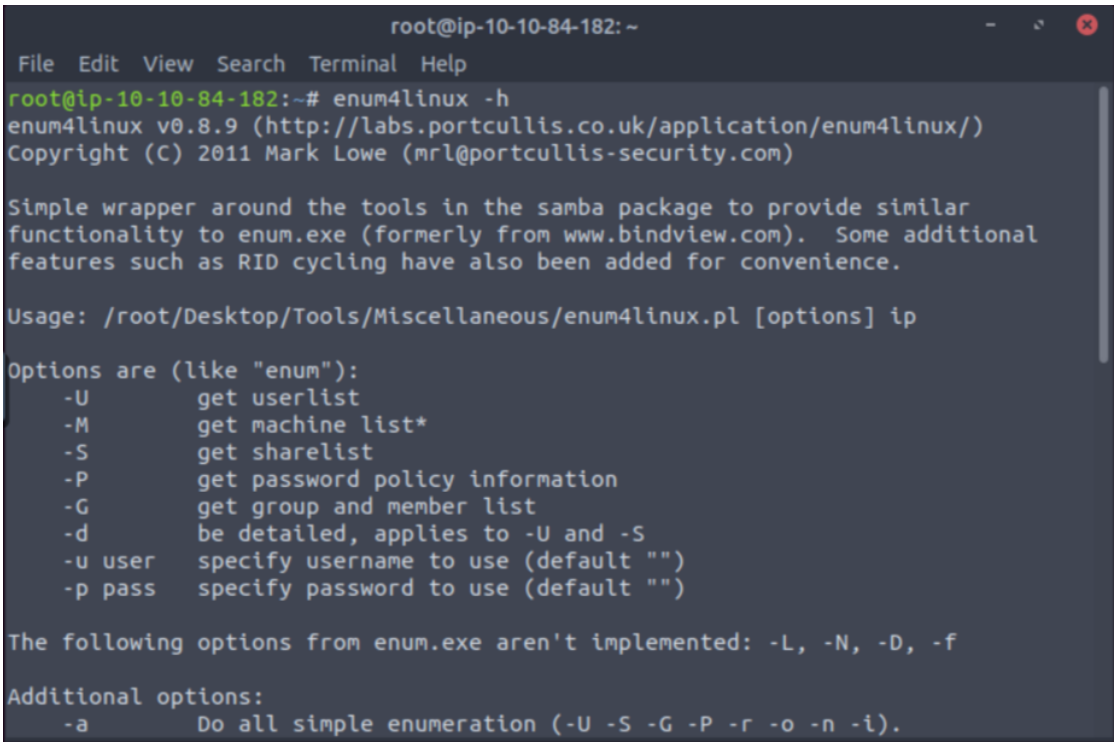
Thought Process/Methodology:

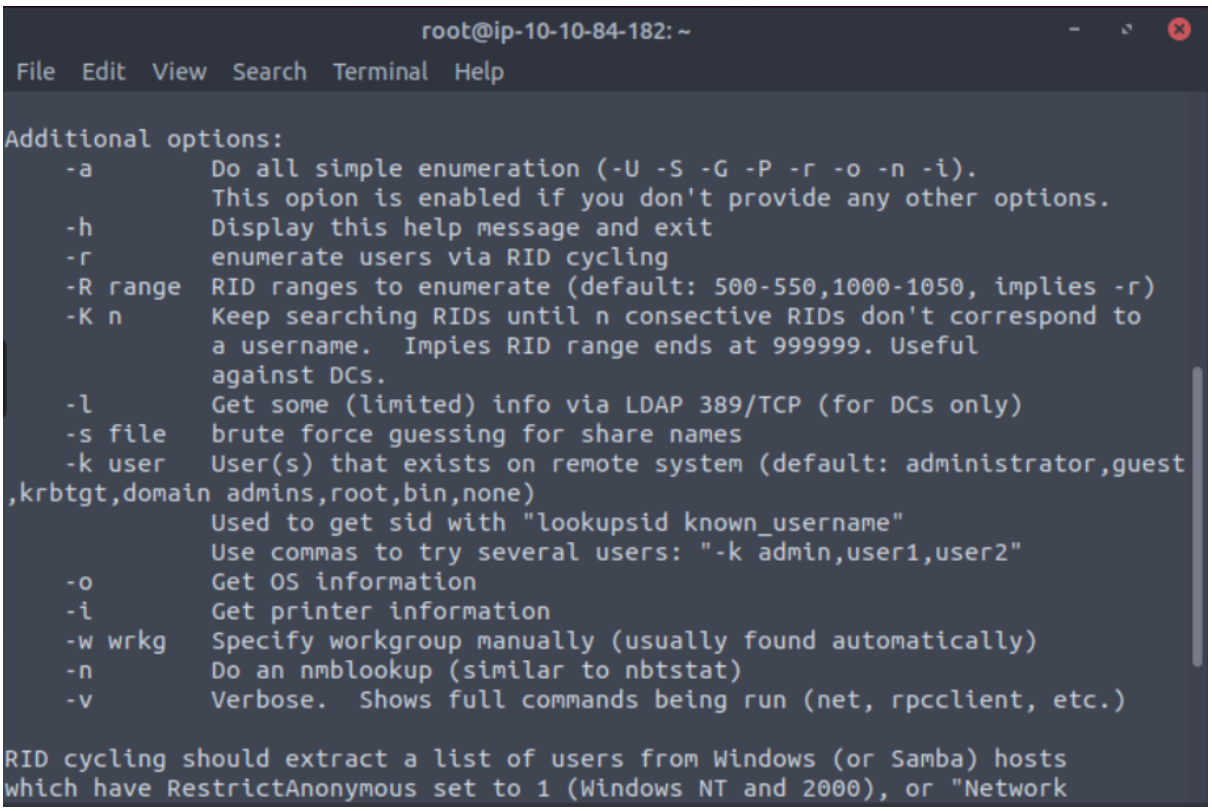
Firstly, we went to tryhackme and started our machine and attackbox for day 9. Then, we copied our ip address that was given and paste it in the terminal of the attack box. Then we ran FTP, and include the ip address that was given in the terminal as anonymous user. Nextly, we ran backup.sh in the directory. We also found four different directories on the FTP site such as, backup, elf workshop, human resources and public. Then , we typed “cat shoppinglist.txt” in the directory and executed it in order to know which was Santa’s shopping list. Lastly , We typed “ Cat/root/flag.txt” in another directory tab in order to get the flag.

Day 10: Don’t be sElfish!

Question 1

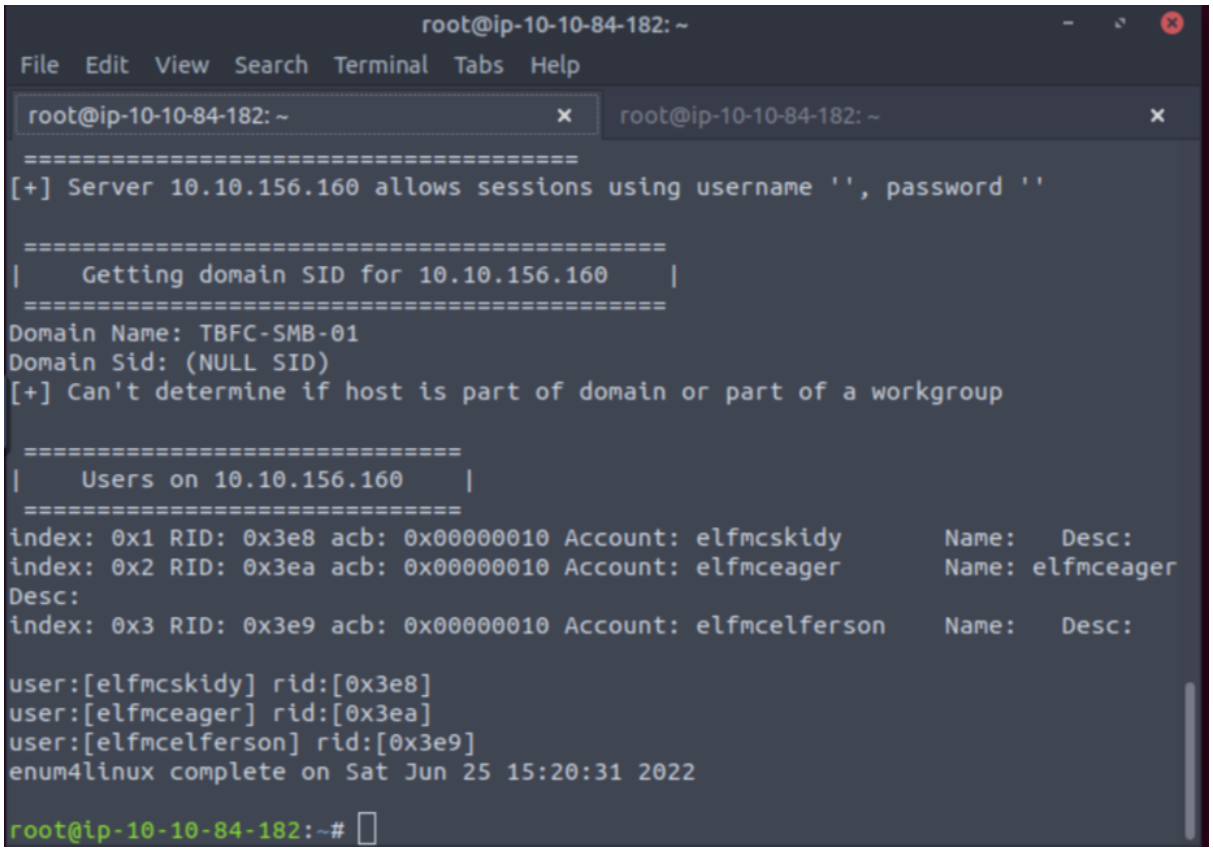
We went into the terminal and we typed in “enum4linux -h” to get help command. And we we were able to get the options and the functions of these options.





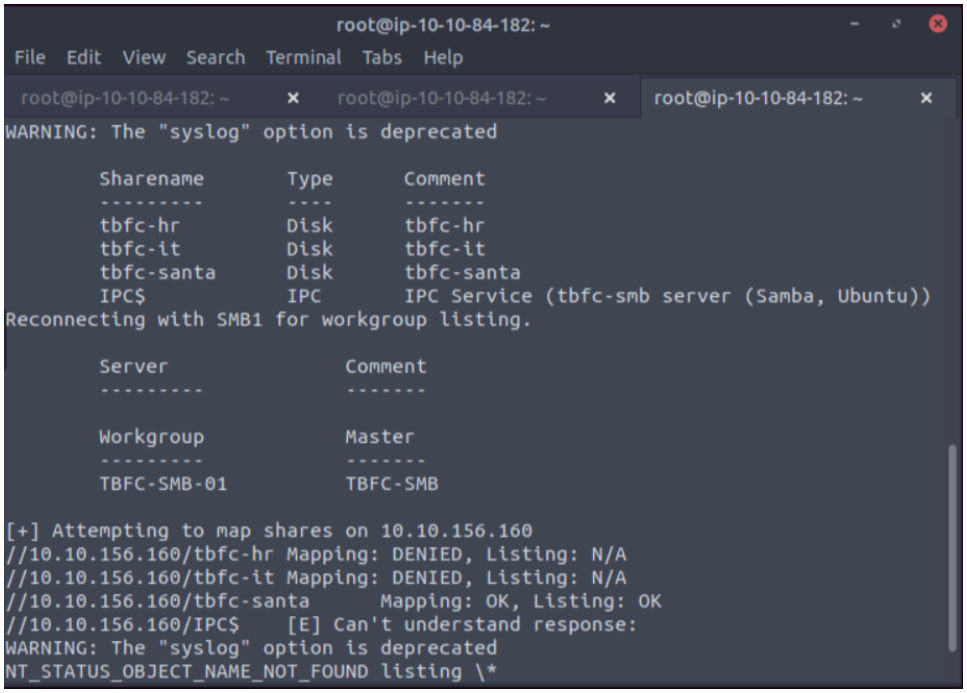
Question 2

We opened on a new tab in the terminal and there we typed in nmap -sV MACHINE_IP and we go back to the tab where we got our -h command and we scrolled down and we found 3 users on the Samba server.



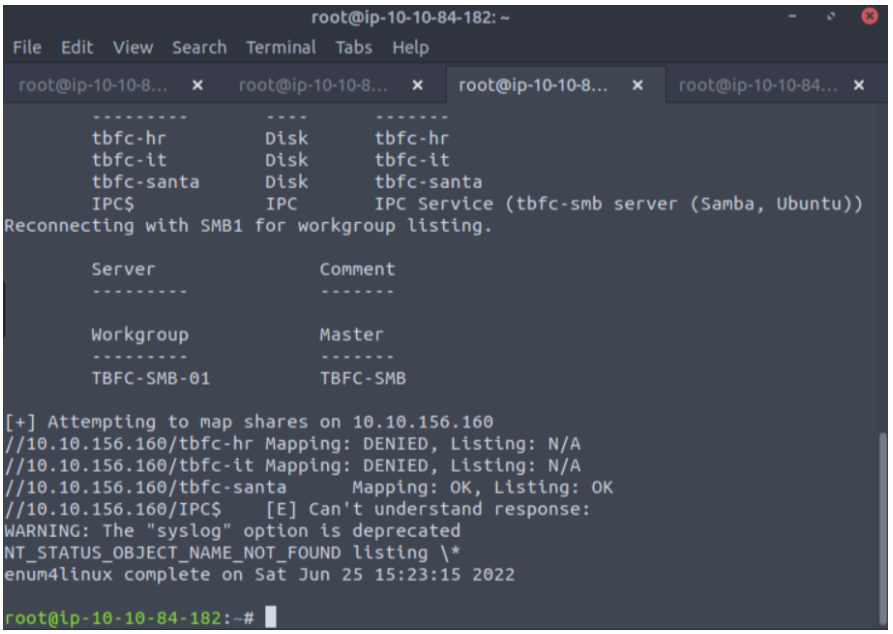
Question 3

We typed in enum4linux -S (sharelist) MACHINE_IP and we were able to find 4 names that share the same Samba server in sharelist.



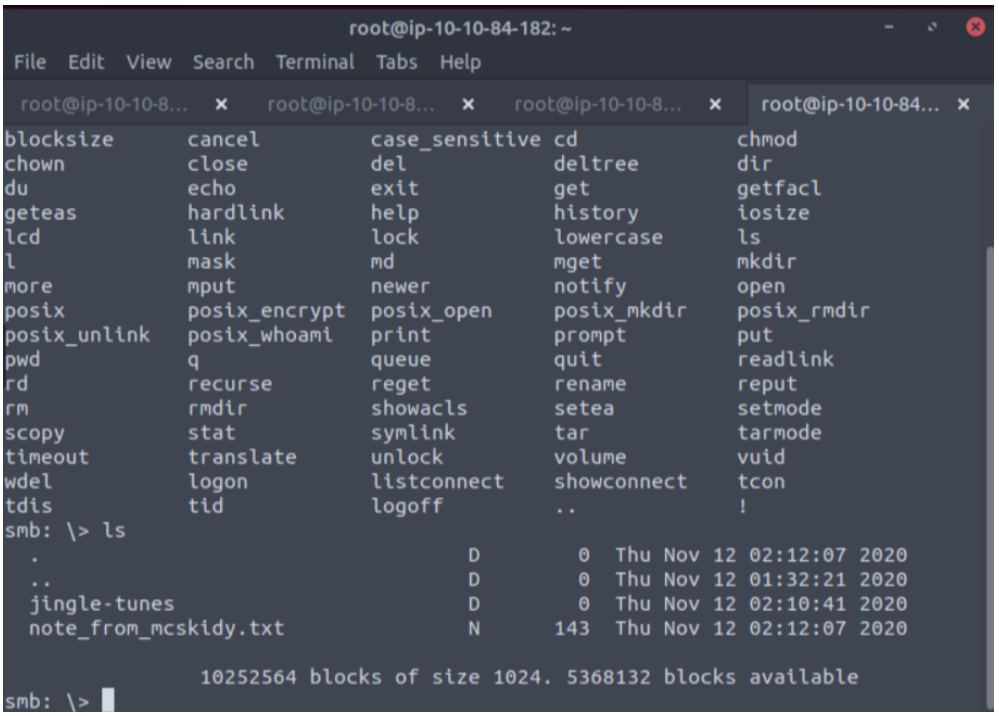
Question 4

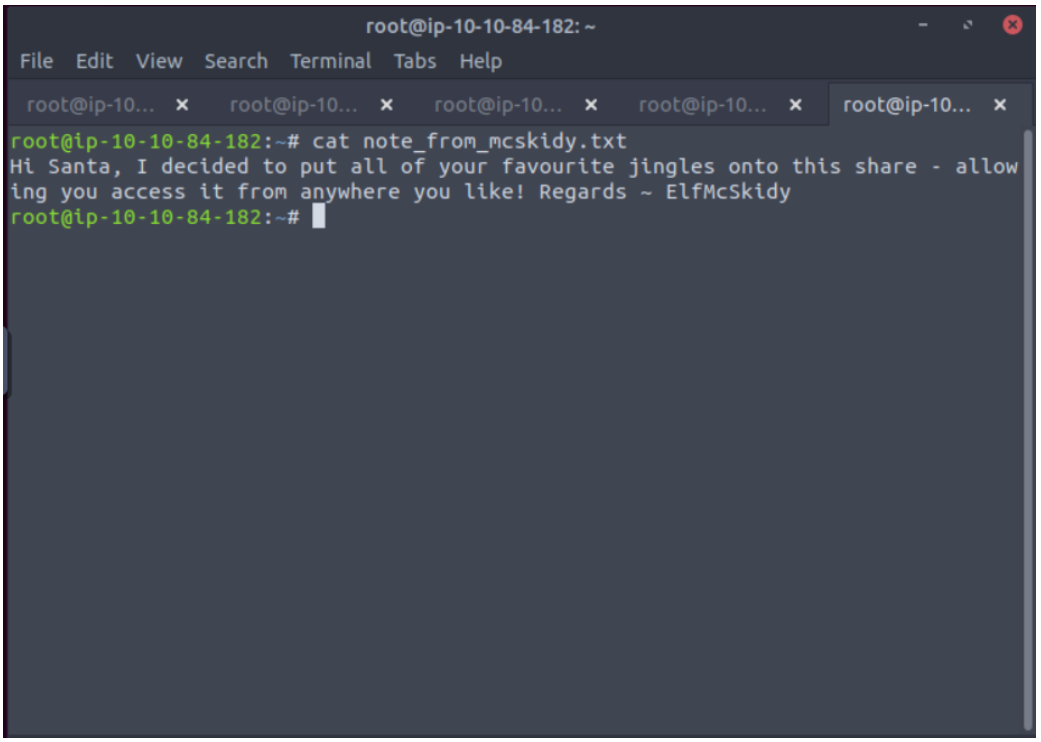
We opened another new tab and typed in “smbclient //IP address/tbfc-santa” because only tbfc-santa is opened. So tbfc-santa was our answer for Question 4.



Question 5

Continuing with how we did for Question 4 “smbclient //IP address/tbfc-santa”, we then typed in help command under SMB and we got the list here. Then we received a file “note_from_mcskidy.txt” and we cat it on the new tab and we got the message saying that ElfMcSkidy had left the jingle-tunes for santa.





Thought Process/Methodology:

Firstly, we started the machine and the attackbox. Then, We went into the terminal and we typed in “enum4linux -h” to get help command. And we were able to get the options and the functions of these options. Next, We opened on a new tab in the terminal and there we typed in nmap -sV MACHINE_IP and we went back to the tab where we got our -h command and we scrolled down in order to found 3 users on the Samba server. Next, in order to answer question 3, We typed in enum4linux -S (sharelist) MACHINE_IP and we were able to find 4 names that share the same Samba server in sharelist. Later on, We opened another new tab and typed in “smbclient //IP address/tbfc-santa” because only tbfc-santa was opened. Which means tbfc-santa is the answer for question 4. Lastly, we typed in the help command under SMB and we got the list here. Then we received a file “note_from_mcskidy.txt” and we cat it on the new tab and we got the message saying that ElfMcSkidy had left the jingle-tunes for santa for question 5.