PSP0201

Week 3

Writeup

Group Name: Modus Potent

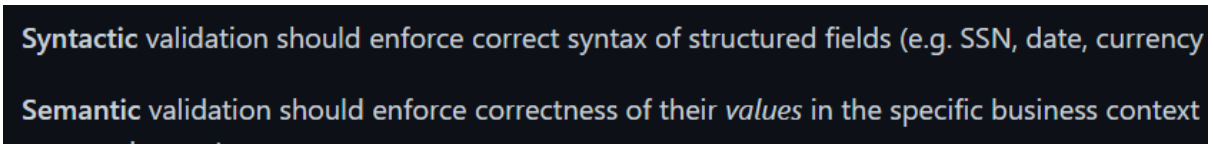
Members

ID	Name	Role
1211200107	Afiezar Ilyaz bin Alfie Iskandar	Leader
1211202025	Abdullah bin Kamaruddin	Member
1211103649	Nur Qistina binti Roslan	Member

Day 6: Web Exploitation - Be careful with what you wish on a Christmas night

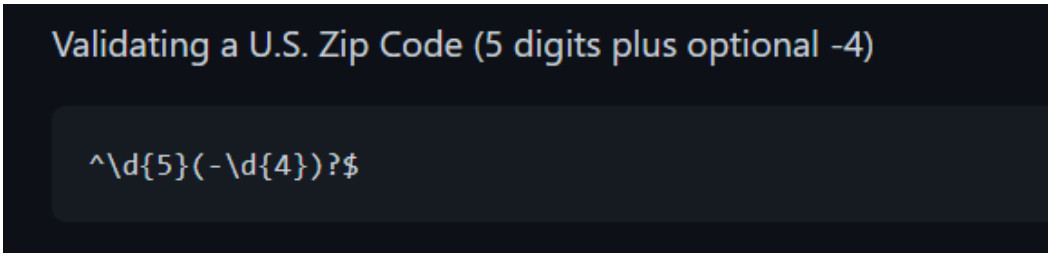
Tools Used: AttackBox, Kali linux, Firefox, OWASP ZAP

Question 1



Question 2

The regular expression used to validate a US Zip code is ^\d{5}(-\d{4})?$

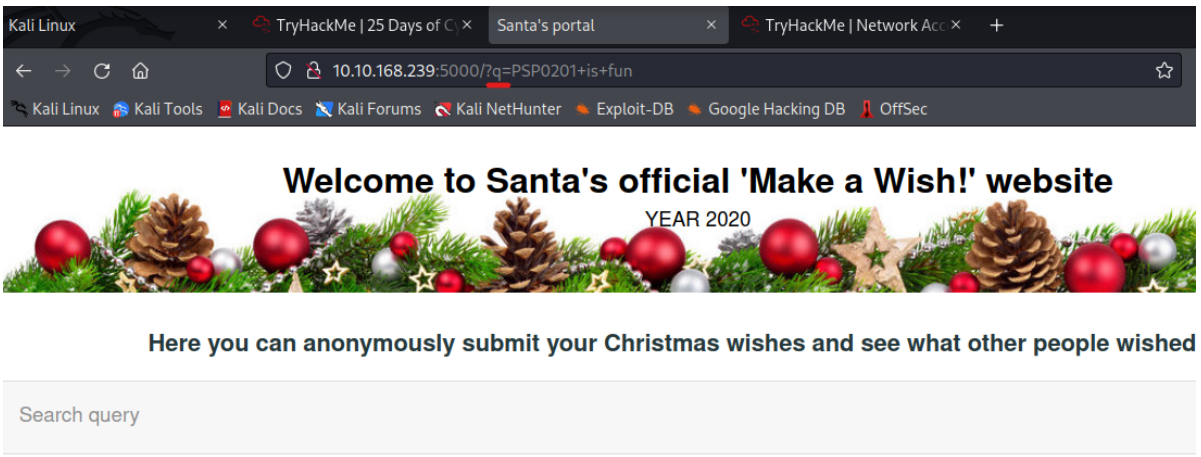


Question 3

The question was what type of vulnerability was used to exploit the application so since the page takes in a wish and stores it for later use, this is an example of stored cross-site scripting.

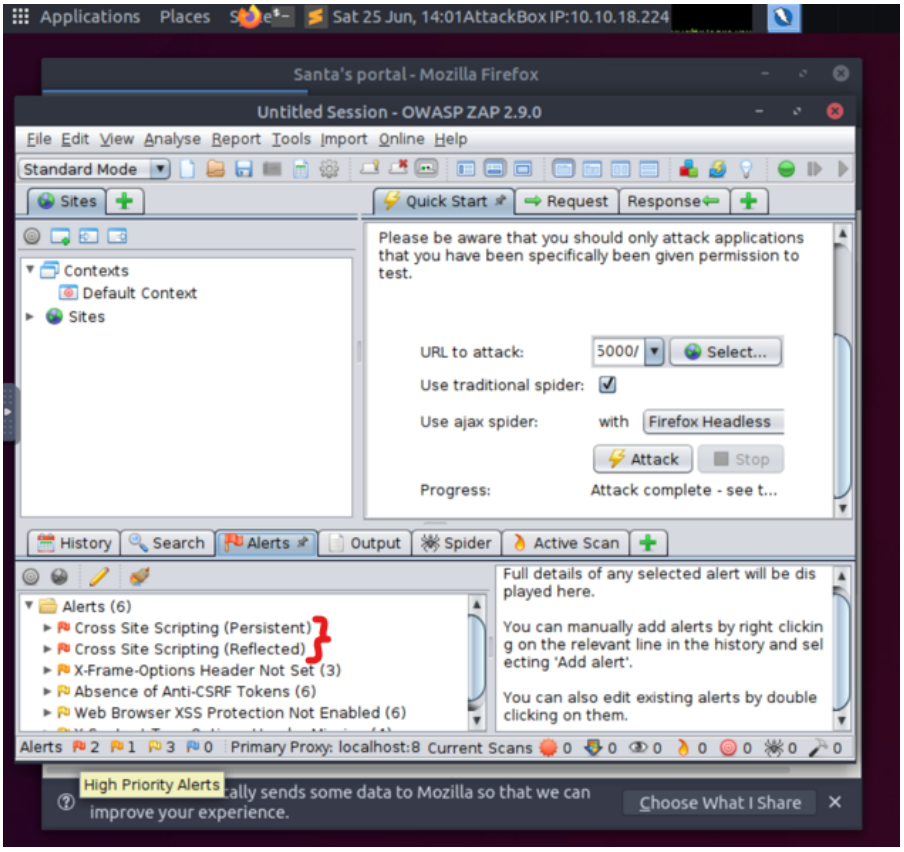
Question 4

We were able to find the query parameter used in the URL, which is q.



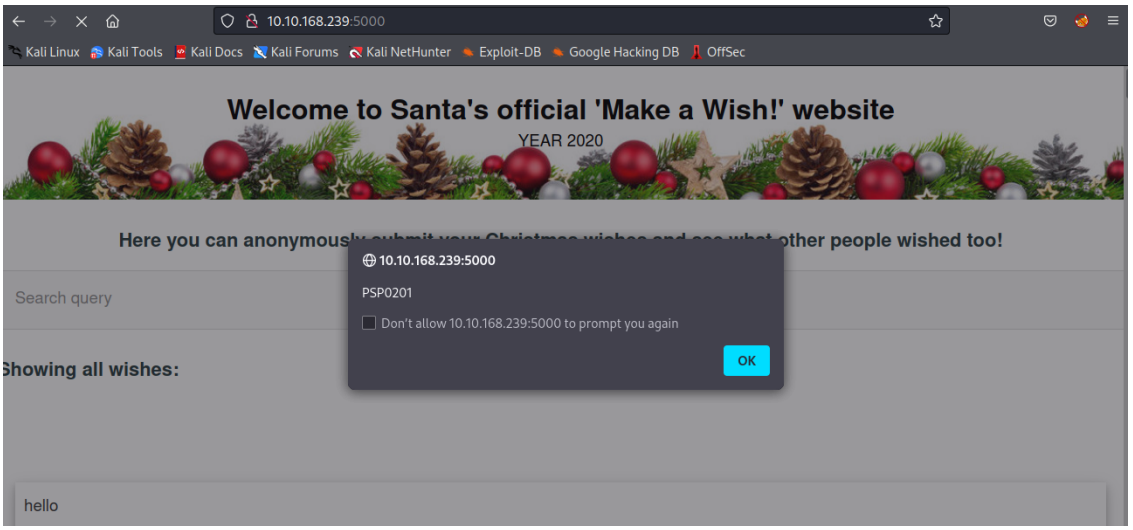
Question 5

After attacking the IP of the machine given into the “URL to attack” in OWASP ZAP, 2 XSS alerts of high priority are found in the scan.



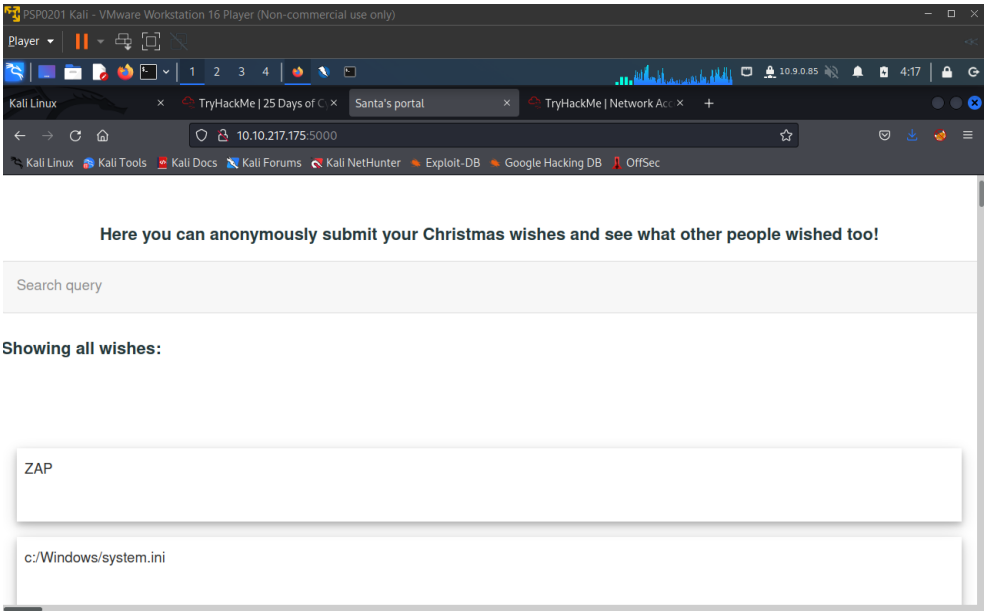
Question 6

By using the Javascript code <script>alert('PSP0201')</script> we were able to show an alert saying PSP0201.

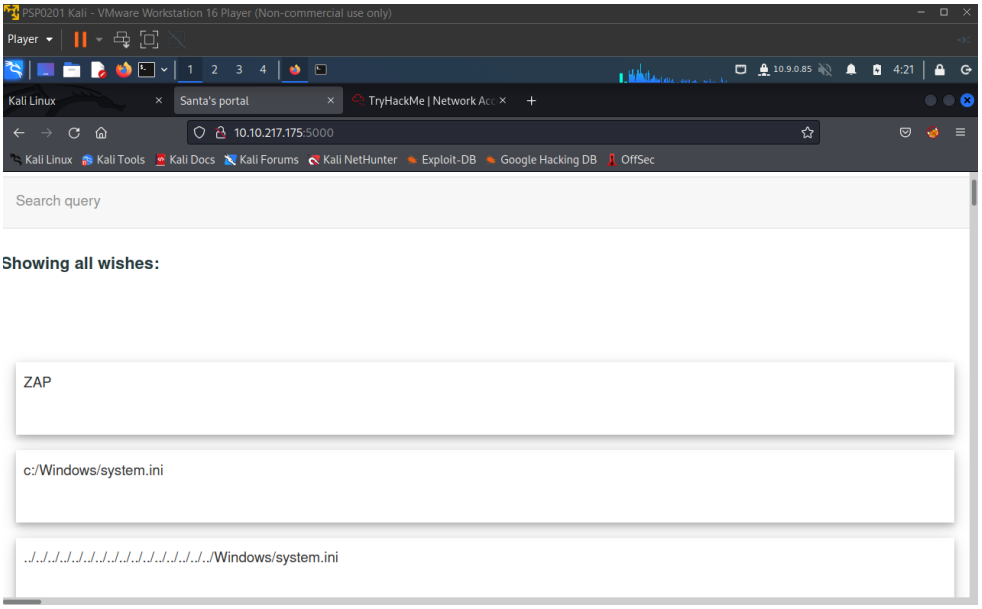


Question 7

Before



After



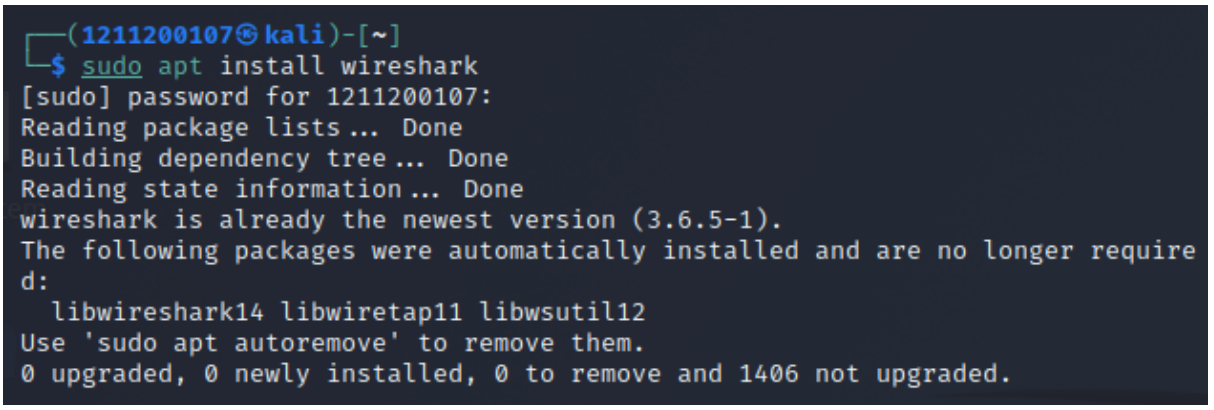
Thought Process/Methodology:

Having access to the machine, we went to the machine's IP together with the port IP given :5000 and was sent to a Santa's official 'Make a Wish!' website. Before doing the actual THM question, we skimmed through the OWASP Cheat Sheet and found the answers for question 1 and 2. After that for question 3, we know that it was stored cross-site scripting since the website takes a wish and stores it for its use later on. For question 4, we were able to know the query string used is q by putting in a test in the query box, in this case we put in PSP0201 is fun to make us more motivated. Thus, the q parameter was found in the URL. For question 5, we used a tool called OWASP ZAP to detect the XSS. We copied the URL altogether of the website, excluding the PSP0201 just now, put it in the automatic scan in ZAP and attacked it. That way, 2 XSS alerts of high priority are located. For question 6, we used the code <script>alert('PSP0201')</script> and entered it in the wish text box and an alert showing PSP0201 popped up, meaning that it worked. For the last question, we found that our XSS attack still persists since the website still shows all wishes and indeed all the stuff still exists. We experimented with it one last time by putting into the wish text box the same code we used to show the alert PSP0201 but this time with random stuff like sunway and etc. As expected, we could see the alert and that verified that our attack worked and it persists.

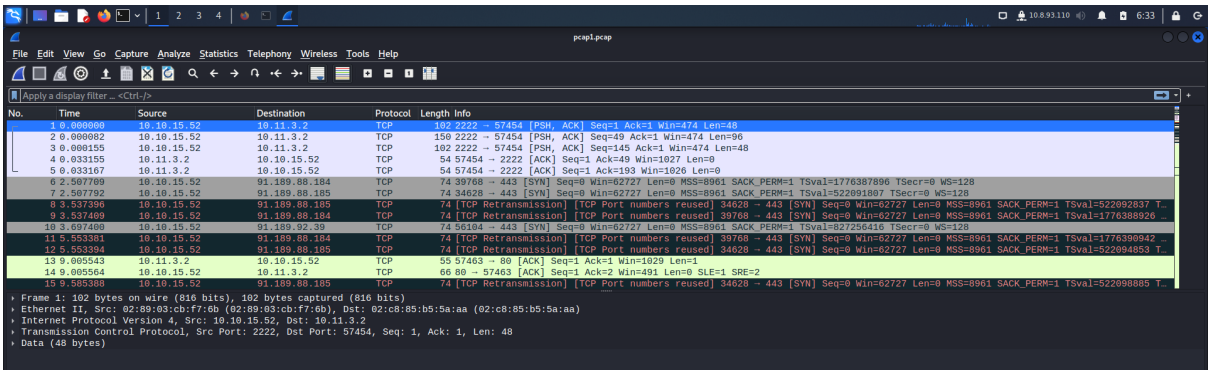
Day 7: Networking - The Grinch Really Did Steal Christmas

Tools Used: Kali Linux, Terminal, Wireshark

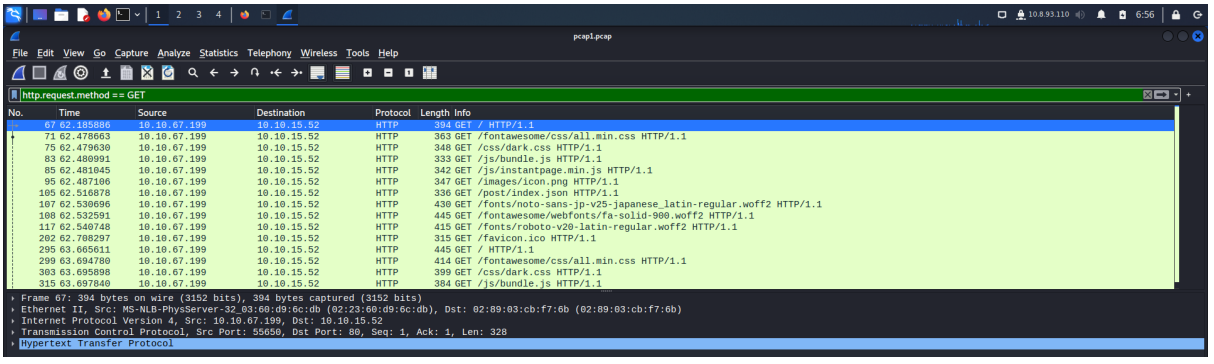
1. Install Wireshark on the terminal using the command *sudo apt install wireshark.*



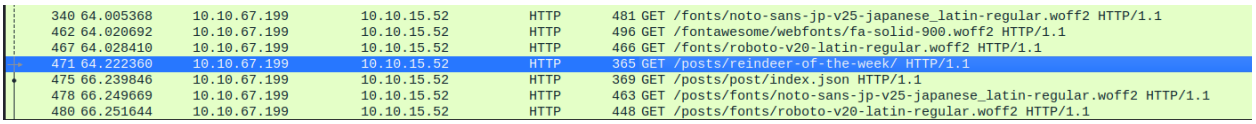
2. Download the zip files from TryHackMe and open *pcap1.pcap* on Wireshark. Find the IP address that initiates an ICMP/ping, which is 10.11.3.2



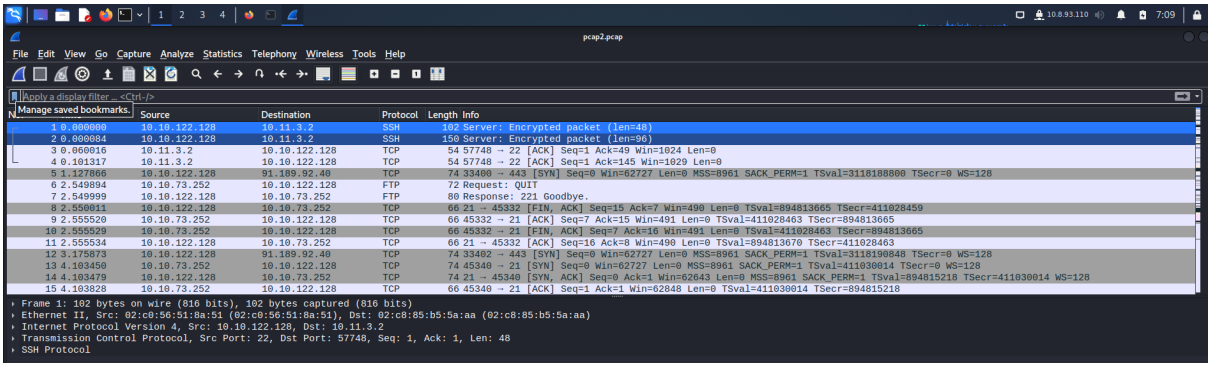
3. If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, we would have to type *http.request.method == GET* in the filter section. Apply the filter



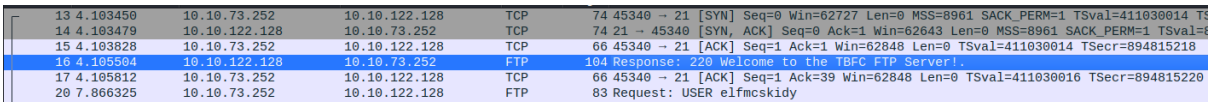
4. Look for a forward slash with *posts*. The answer to the third question is reindeer-of-the-week

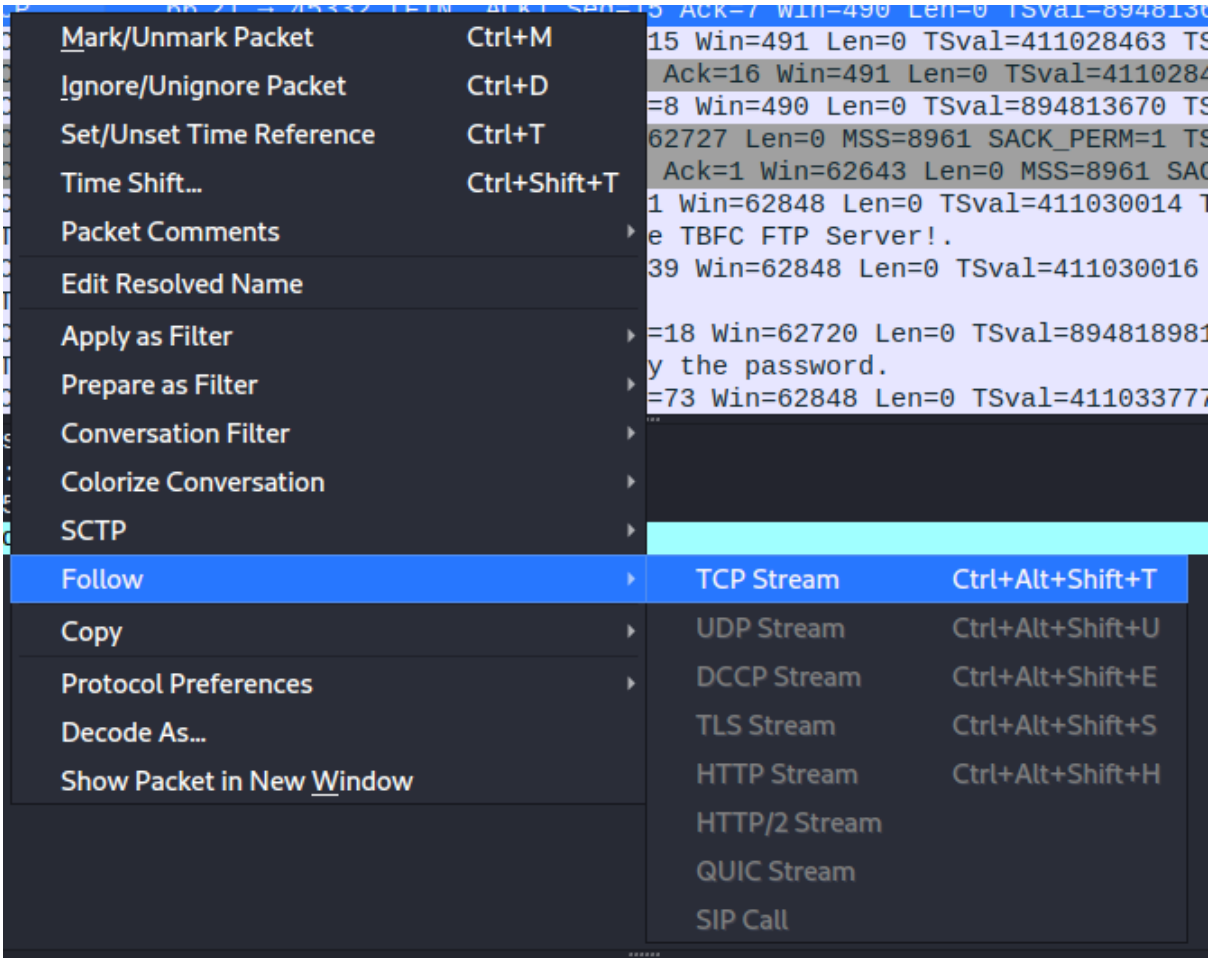


5. Open up *pcap2.pcap* in the Wireshark and filter it out by typing *tcp.port == 21*

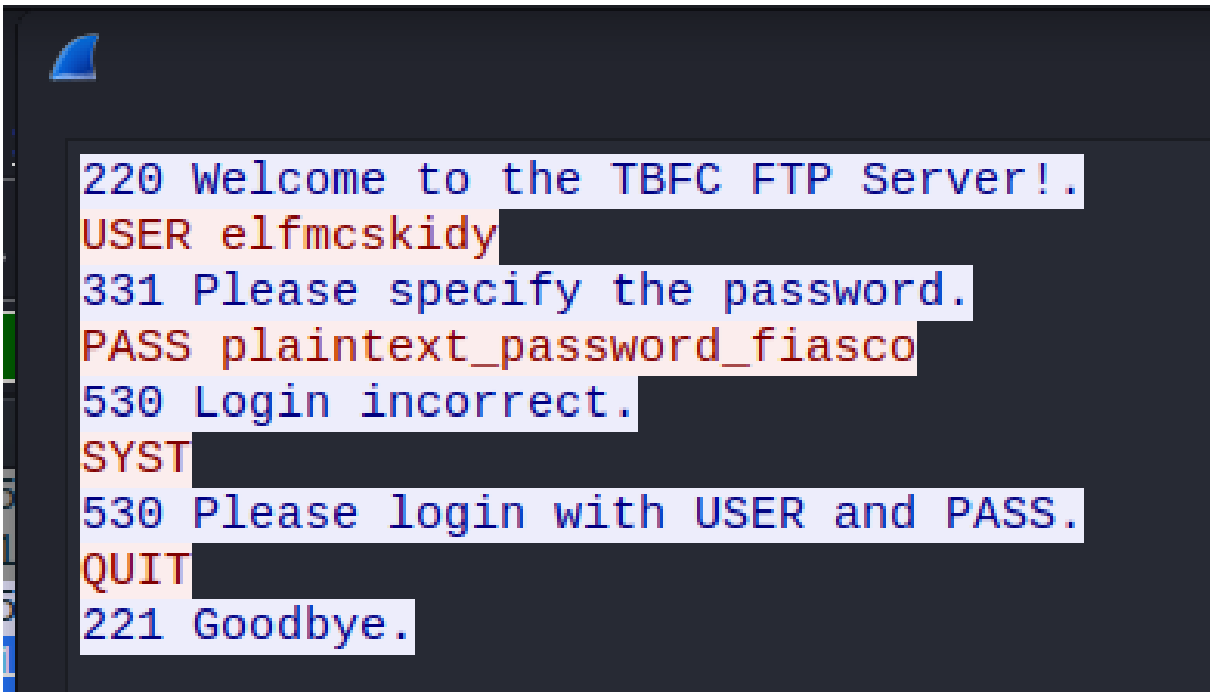


6. Right click on the one that says "*Response:220 Welcome to the TBFC FTP Server!"* and go to *Follow -> TCP Stream.*

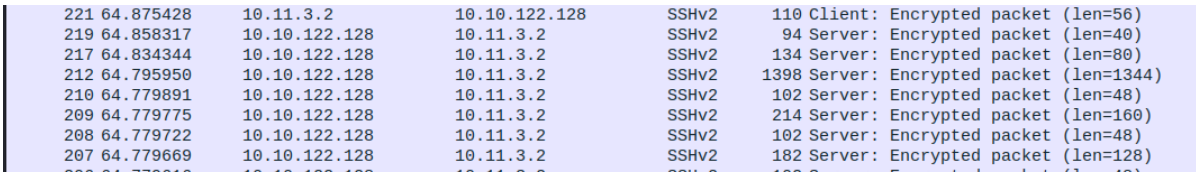




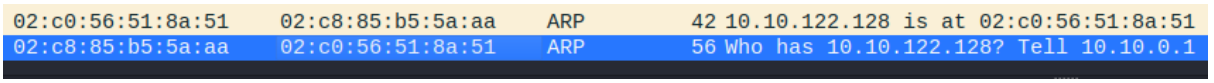
7. This should lead you to the leaked password, giving the answer to the fourth question



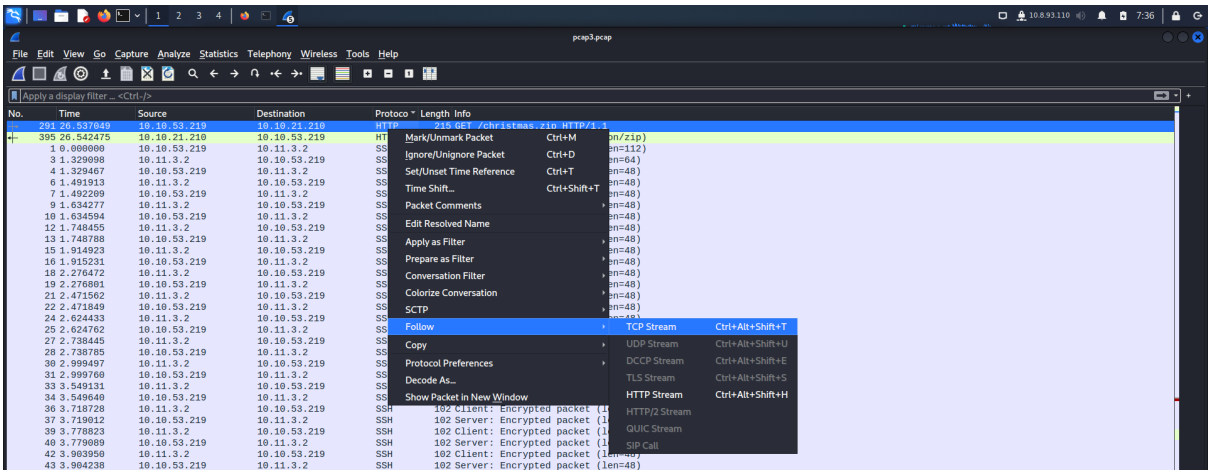
8. ARP, TCP, and FTP are not secured, meaning it is not encrypted. This leaves out the only other protocol which is SSH being encrypted, which is the answer for question 5

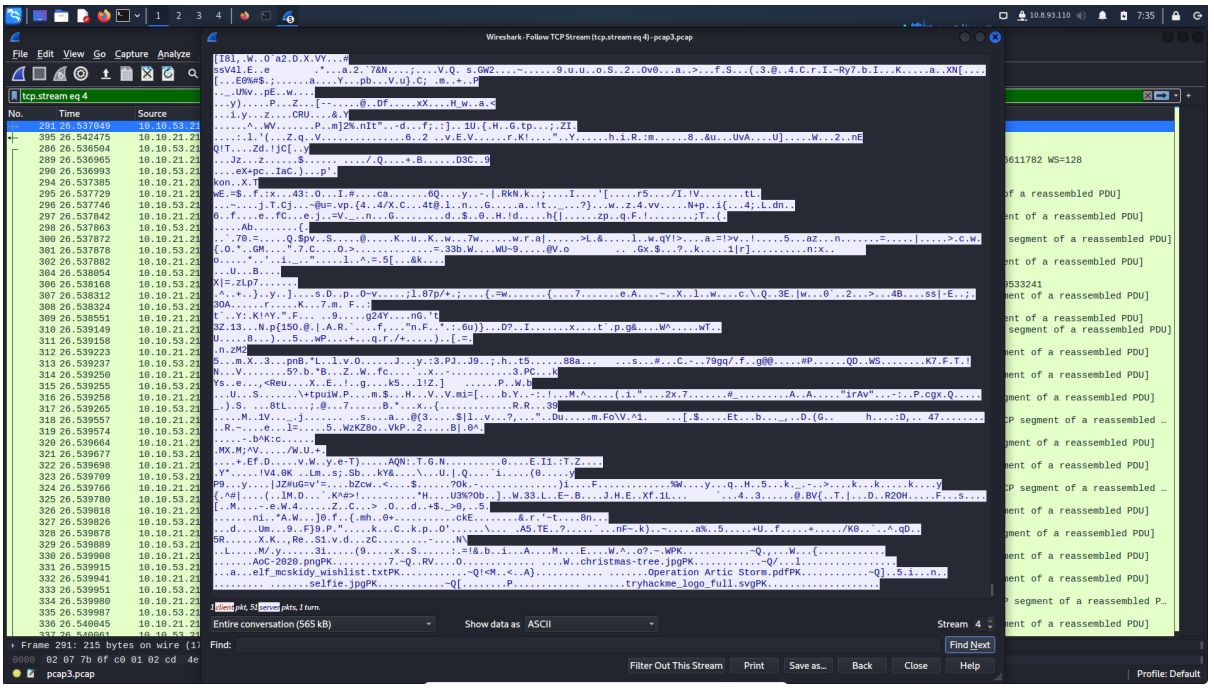


9. After examining ARP, we look out for the one with the info *"Who has 10.10.122.128? Tell 10.10.0.1".* Look for the destination to get the answer for question 6



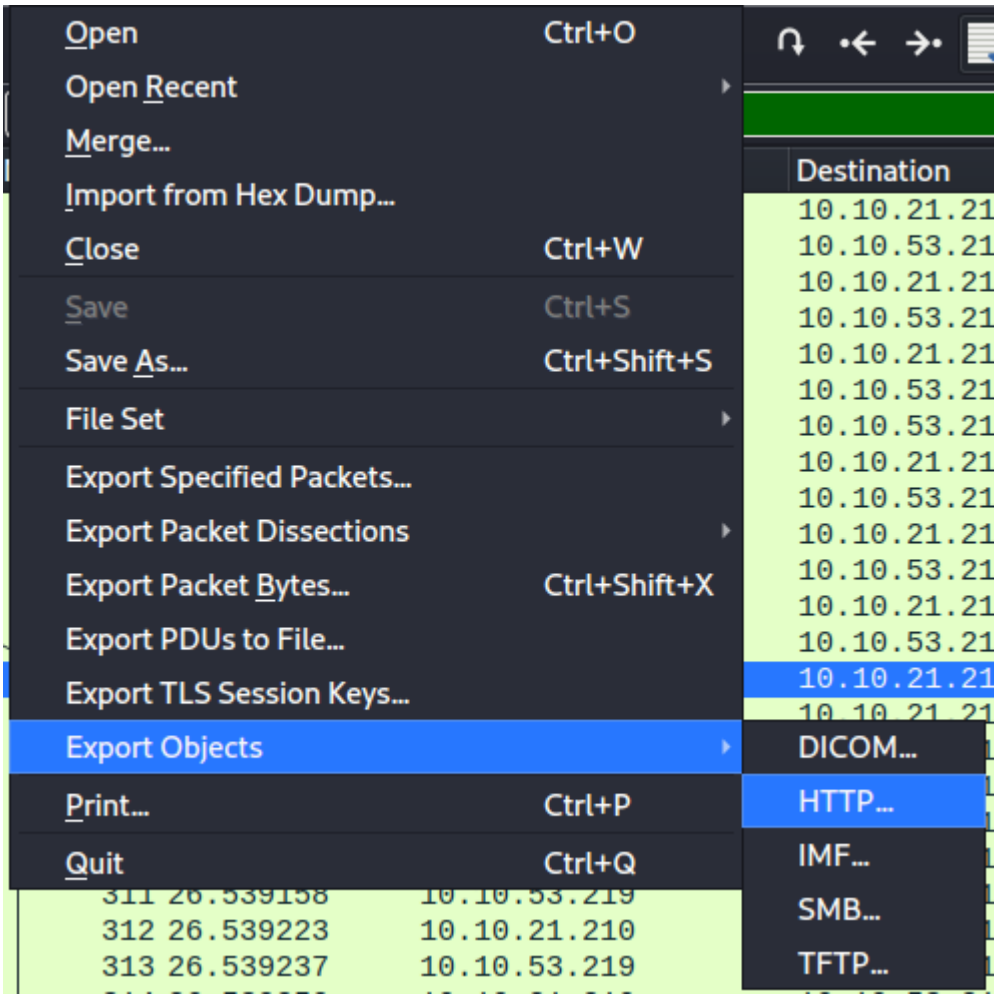
10. Open up *pcap3.pcap* and follow the HTTP traffic

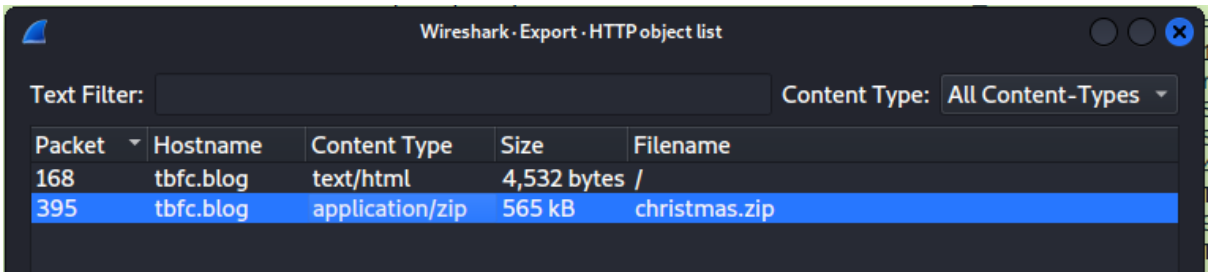




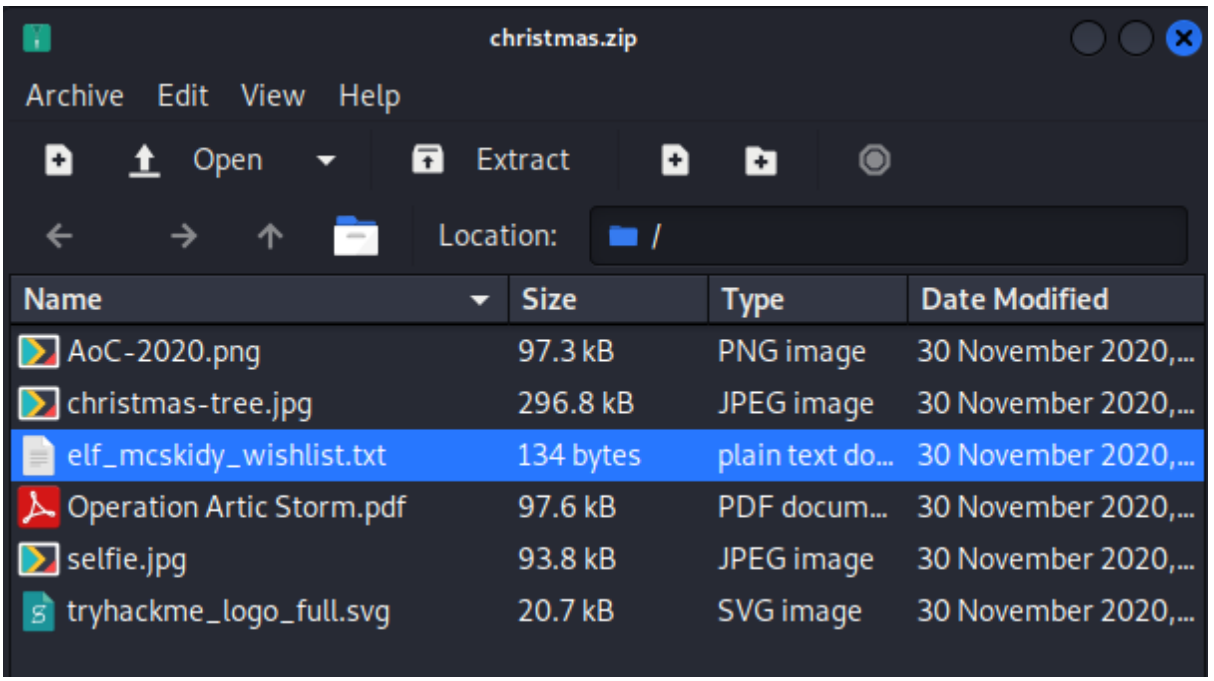

```
GET /christmas.zip HTTP/1.1
User-Agent: Wget/1.19.4 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: tbfc.blog
Connection: Keep-Alive
```

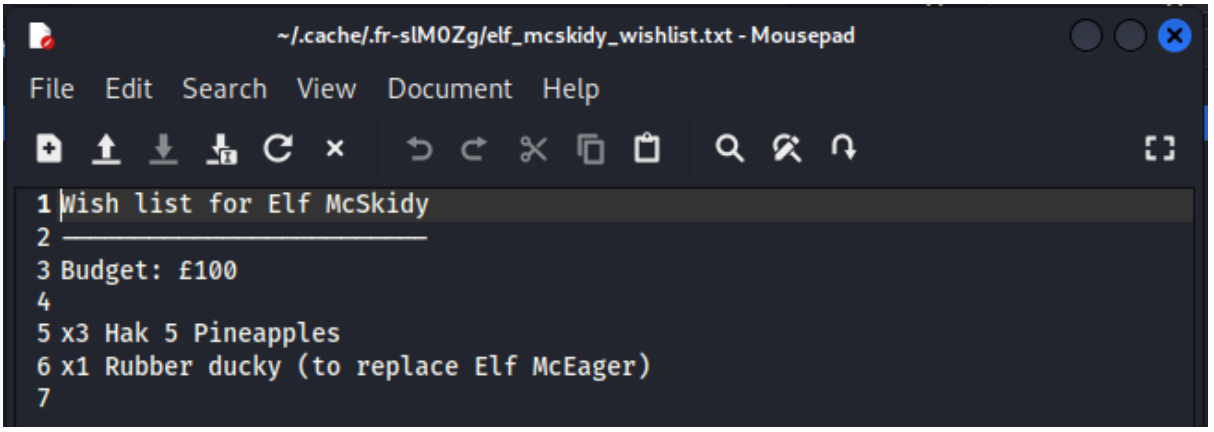
11. We find out that there is *GET /christmas/zip.* We will go to *Export Objects -> HTTP.* Save the file *christmas.zip*



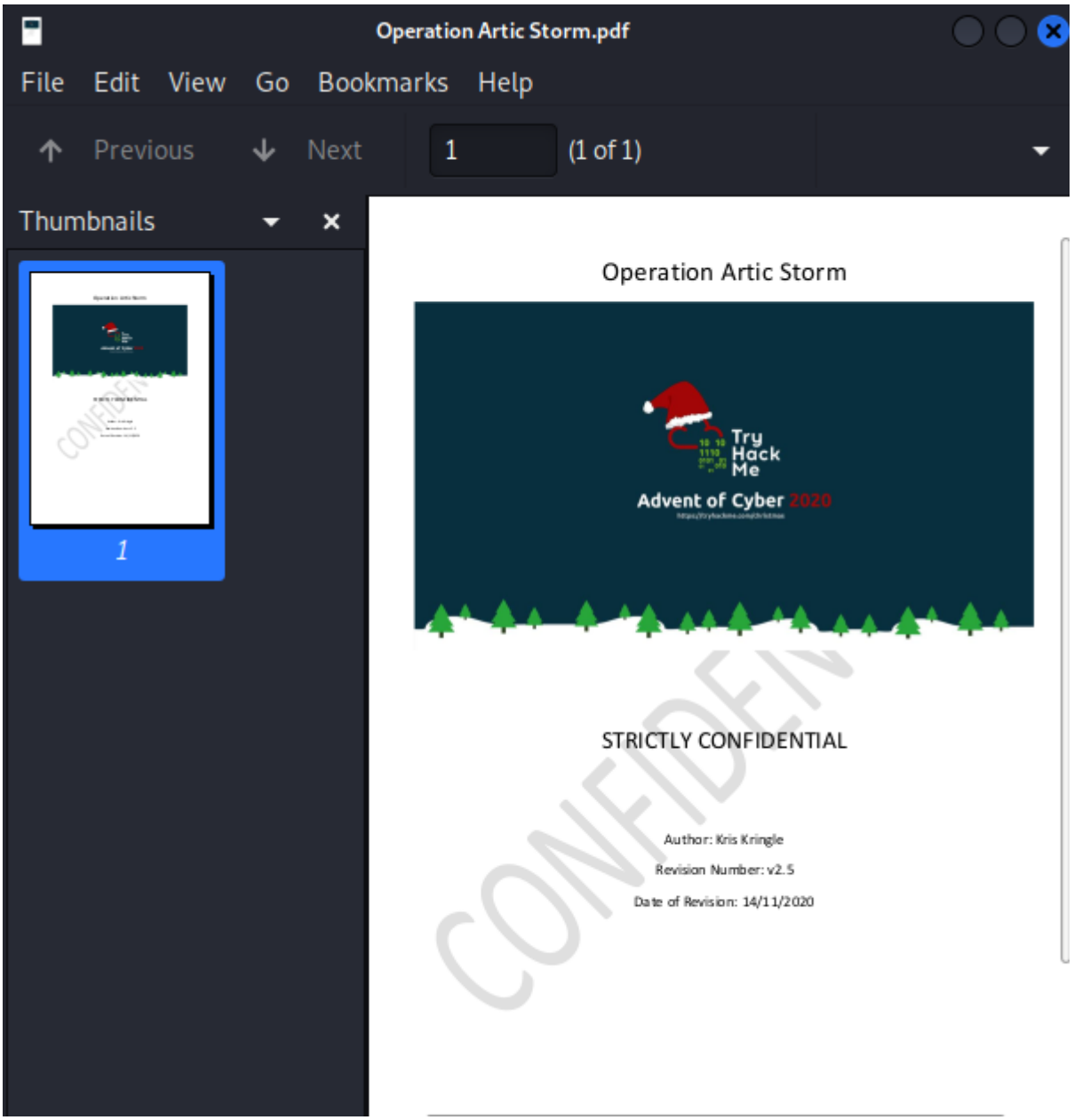


12. We then extract the zip file and check out what is in the zip file. There is a list of things in the zip file but we will check the *elf_mcskiddy_wishlist.txt* file. This will be the answer to question 7.





13. We will also check the *OperationArticStorm.pdf* file and check for the author's name, giving us the answer to question 8.



Thought Process/Methodology:

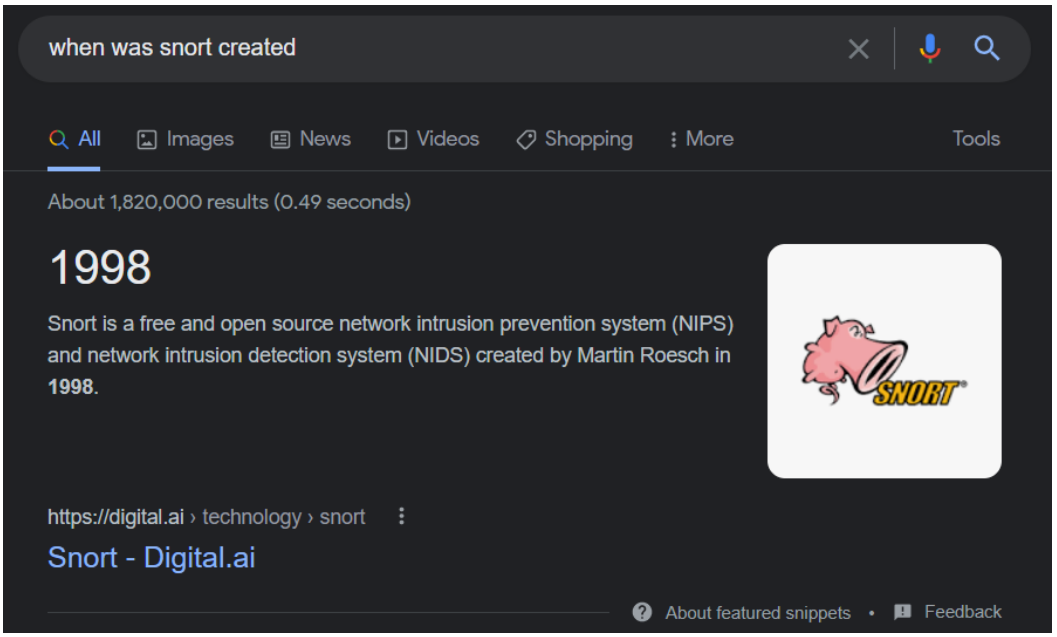
First and foremost, we must install the WireShark on the terminal and download the required zip files from TryHackMe. Then, we open up the file *pcap1.pcap* on the WireShark app and find the address that initiates a ping, which is 10.11.3.2. Moving on to the second question, we will use *http.request.method == GET* in the filter section if we only want to see the HTTP GET requests. To answer the third question, we must look for anything that has a source of 10.10.67.199, and realistically we must look for anything that is paged or article based. In this case, /posts/. This gives the answer to the third question which is reindeer-of-the-week. Now, open up the *pcap2.pcap* file and we will start analyzing the second file. Firstly we will type *tcp.port==21* in the filter and right-click on the one that says "*Response:220 Welcome to the TBFC FTP Server!"* and go to *Follow -> TCP Stream.* The answer to the fourth question should be next to the text "PASS", which is plaintext_password_fiasco. Moving on to the next question, we will be looking at which of the four traffics are secured. ARP, TCP, and FTP are all vulnerable and not secure, leaving only SSH being encrypted, giving us the answer to question 5. For question 6, all we have to do is filter out everything and only keep ARP protocols and look for the destination with the info of *"Who has 10.10.122.128? Tell 10.10.0.1".* This should give the answer as 02:c8:85:b5:5a:aa. Moving on to the last .pcap file, we will open it on the WireShark and follow the HTTP traffic, which we should see that there is a *GET /christmas/zip* command in the red highlighted text. We can go to *Export Objects -> HTTP* and save the *christmas.zip* file. We then extract the zip file and check out what is in the zip file. There is a list of things in the zip file but we will check the *elf_mcskiddy_wishlist.txt* file. We find that Elf McSkidy plans to replace Elf McEager with a rubber ducky. We will also be looking at the pdf file of OperationArticStorm and checking for the author's name to secure the answer to the last question.

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

Tools Used: Kali linux, Terminal/Command line

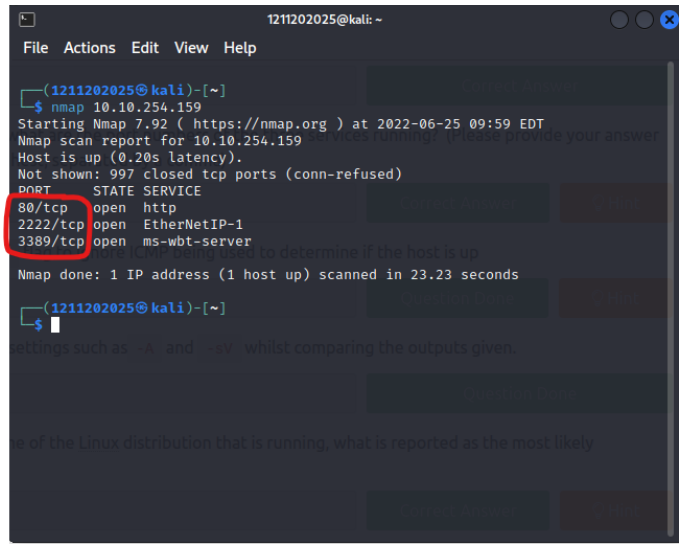
Question 1

Using the all-knowing Google, we were able to know when snort was created.



Question 2

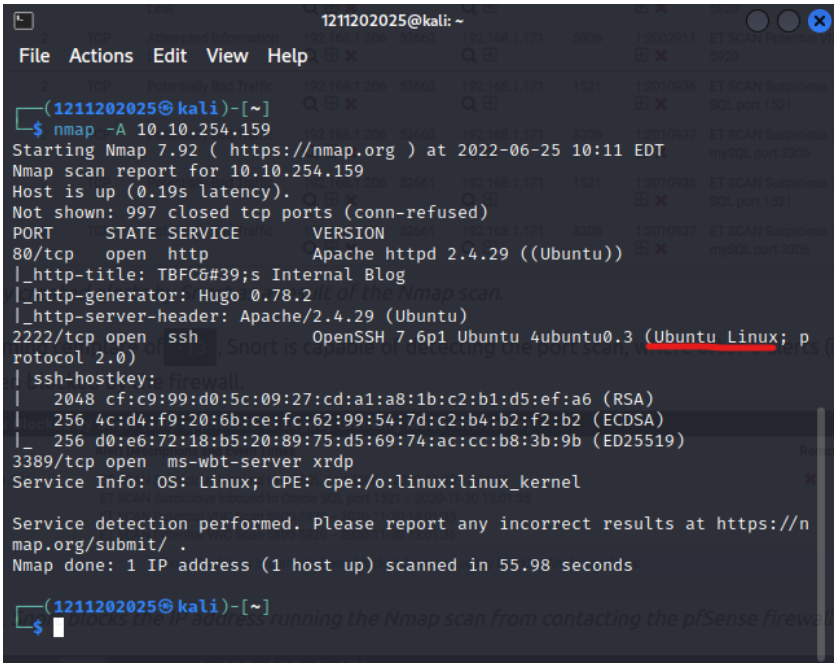
Using the command **nmap 10.10.254.159**, the port numbers of the three services running were shown and located.



Using the command **nmap -A 10.10.254.159**, we were able to find all the answers for the remaining questions.

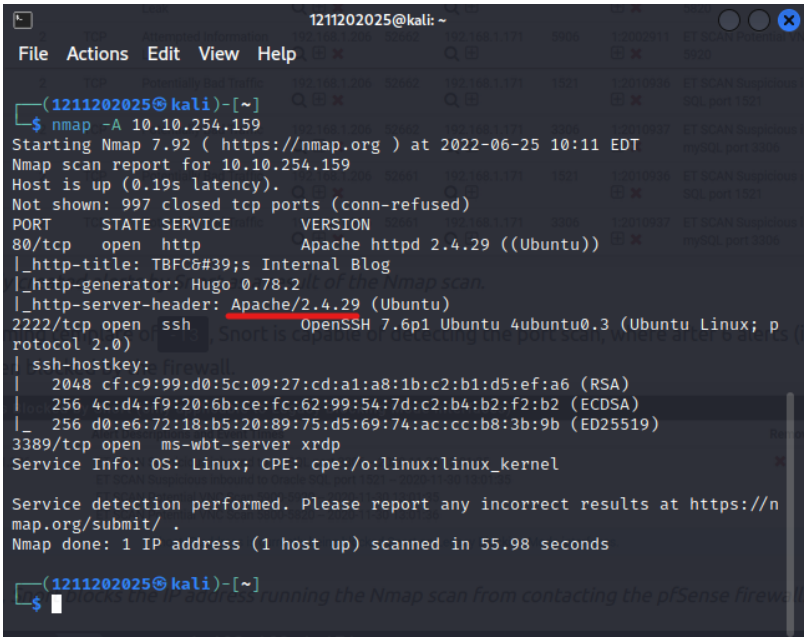
Question 3

Ubuntu as the name of the Linux distribution that is running.



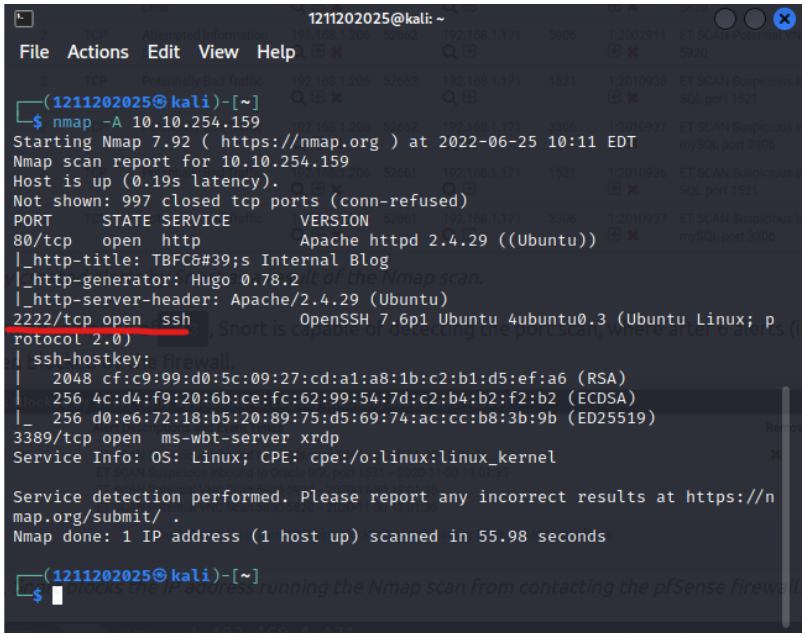
Question 4

The version of Apache is 2.4.29.



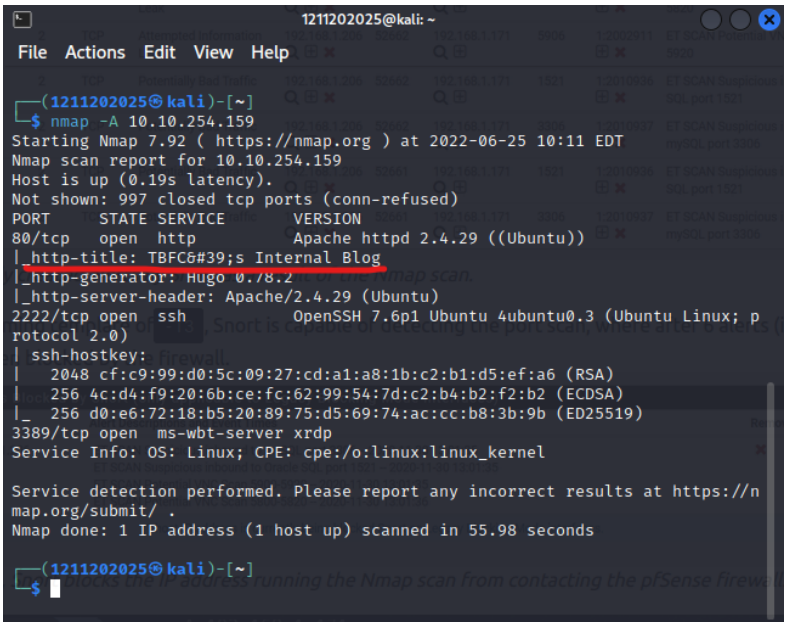
Question 5

SSH is running on port 2222.



Question 6

This website most probably might be used for blog.



Thought Process/Methodology:

After having access to the machine, we use the given IP to do everything via terminal. For question 2 that asks what port numbers of the three services running, we were able to achieve it by using a command that shows the port numbers 80, 2222 and 3389. As for the following remaining questions, we got the answers just by using a single command, where we found Ubuntu as the Linux distribution, 2.4.29 as the version of the Apache, SSH for what is running on port 2222 and lastly blog for what the website might be used for.

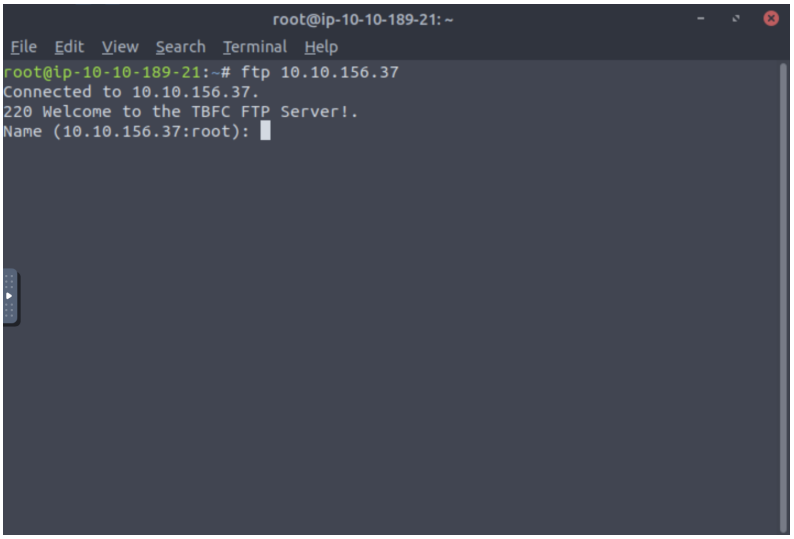
Day 9: Networking - Anyone can be Santa!

Tools Used: Terminal/Command Line, Attackbox, Firefox

Question 1

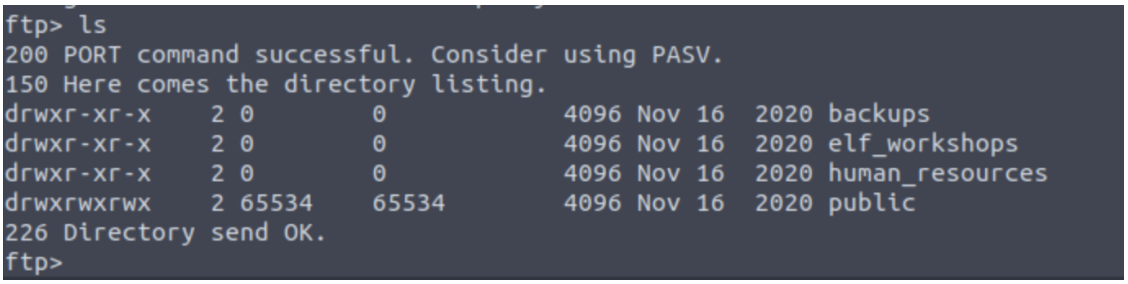
To retrace the steps of the attacker we must have to use the protocol Elf Mcskidy and their team have used which is the FTP protocol

The THM attackbox already has the protocol installed but if not you could just write out atp install ftp. Then writing out the IP address, the server has anonymous mode enabled therefore we are able to login



Question 2

To take a look at the directories available we can use the **ls** command which will show a folder containing data that "anonymous" has permission to have access to. To answer **question #1** , naming the directory on the FTP server that has data accessible by the " anonymous" user is public as it is the only directory that is showing data.



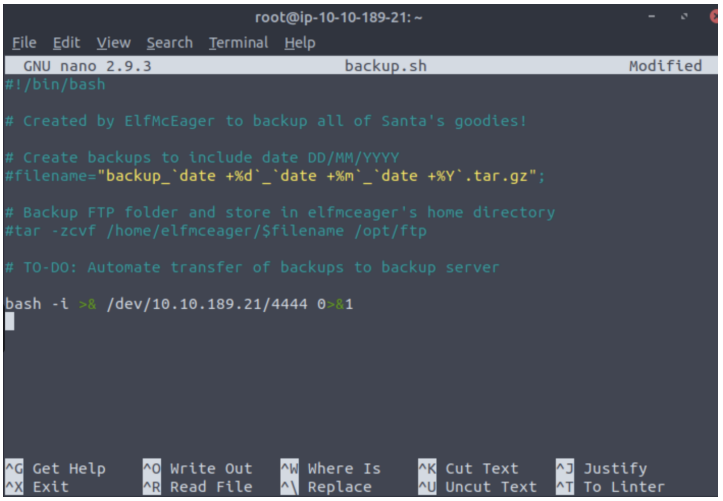
With public being the only one available for us we can change the directory using command cd public. To list the contents we can use command ls, **question #2** asks What script gets executed within this directory? There is a file named backup.sh where **.sh** indicates that when executed, can run. We can use the command get in order to to get the file from the server onto the device. After the file is downloaded, we can open it on our device using the terminal with the command nano

```
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp> get backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup.sh (341 bytes).
226 Transfer complete.
341 bytes received in 0.00 secs (214.1529 kB/s)
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
226 Transfer complete.
24 bytes received in 0.00 secs (468.7500 kB/s)
ftp> exit
221 Goodbye.
root@ip-10-10-189-21:~# ls
backup.sh  Downloads     Pictures  Rooms    shoppinglist.txt   Tools
Desktop    Instructions  Postman   Scripts  thinclient_drives
root@ip-10-10-189-21:~# nano backup.sh
root@ip-10-10-189-21:~#
```

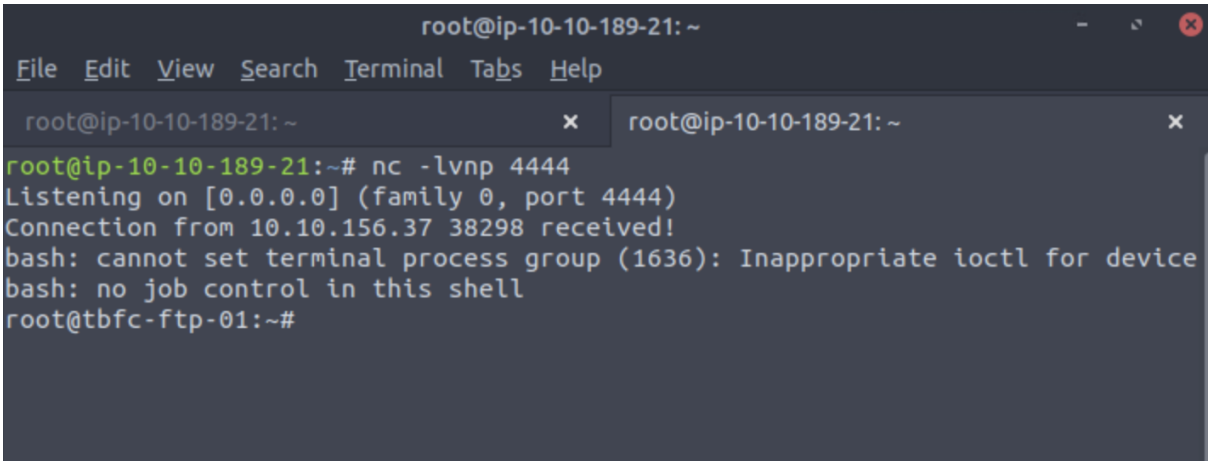
After running the command we are presented with the shell script

```
root@ip-10-10-189-21: ~
File  Edit  View  Search  Terminal  Help
  GNU nano 2.9.3                    backup.sh

#!/bin/bash

# Created by ElfMcEager to backup all of Santa's goodies!

# Create backups to include date DD/MM/YYYY
filename="backup_`date +%d`_`date +%m`_`date +%Y`.tar.gz";

# Backup FTP folder and store in elfmceager's home directory
tar -zcvf /home/elfmceager/$filename /opt/ftp

# TO-DO: Automate transfer of backups to backup server

                [ Read 13 lines ]
^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Linter
```

We can replace the original commands with our own malicious commands as well as upload files that supposedly should not be granted to the “anonymous” user although the permission in this case is prone to carelessness. With that, we can generate a shell through our attackbox by replacing the original IP address with the THM IP.



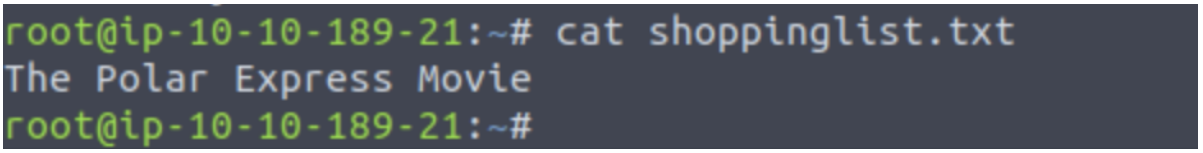
Setting up a net cat listener and uploading the malicious script we have access to by using put command for backup.sh, then we will be presented with the image below



Question 3

What movie did santa have on his christmas shopping list?

We need to use the **cat** command to print out the content from the file in this case would be the shoppinglist.txt



Question 4

Re-upload this script to contain malicious data (just like we did in section 9.6. Output the contents of /root/flag.txt!, by running it we will get the THM{even_you _can_be_santa} flag.

```
root@tbfc-ftp-01:~# cat /root/flag.txt
cat /root/flag.txt
THM{even_you_can_be_santa}
root@tbfc-ftp-01:~#
```

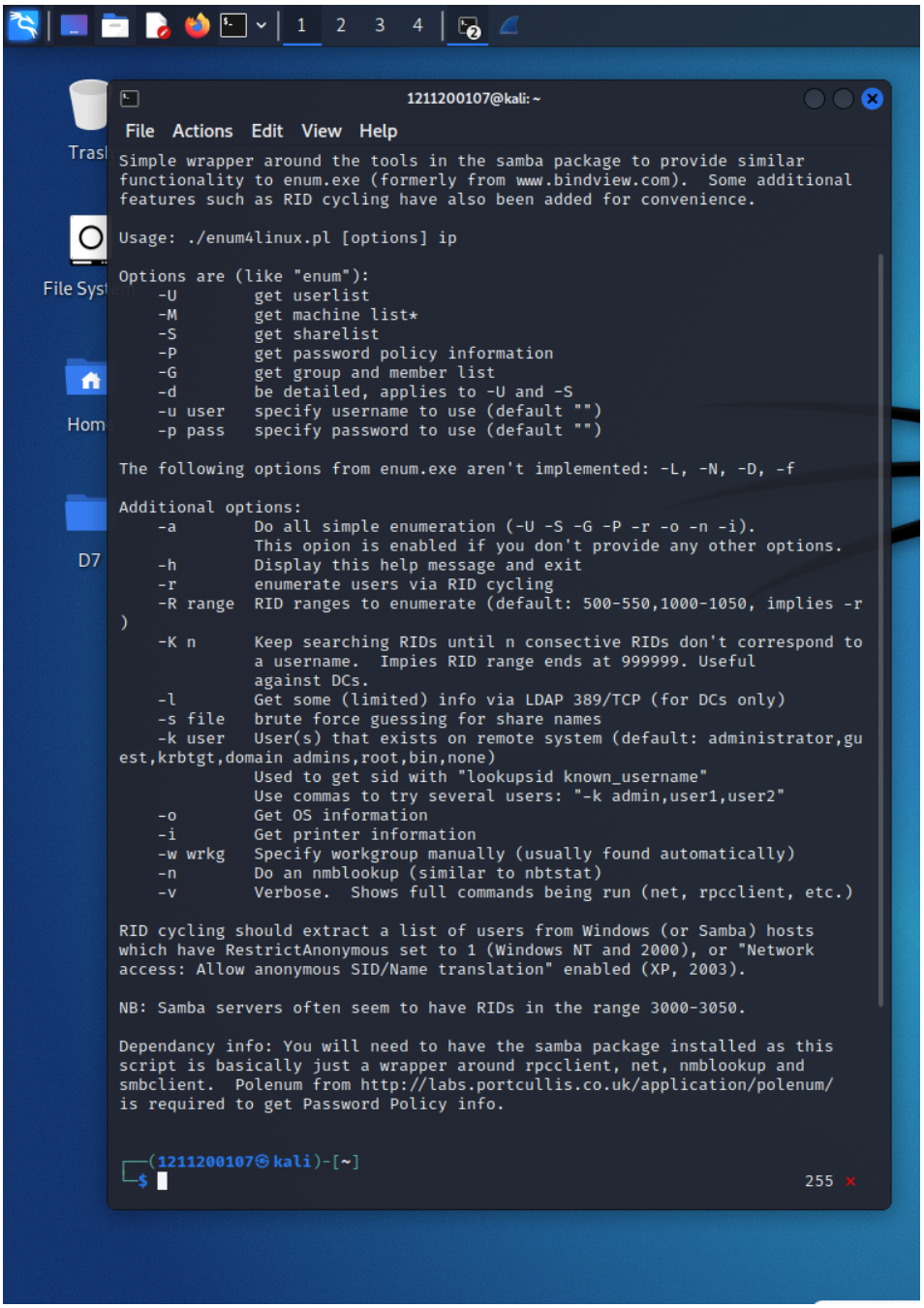
Thought Process/Methodology:

To explain why the FTP server was exploited, the server had anonymous mode enabled giving us to authenticate ourselves easily. It also explains why it is so easy to gain permission to upload and download files wherein should not be normalized for “anonymous” users. Other than that, we had taken the details from the backup script and created a reverse shell that will ultimately take advantage of the target system’s vulnerabilities. Furthermore, the script has taken the role of the “root” user also known as the admin where all of the information can be manipulated easily by the hacker. If the script were to execute on a different user, then we will only be able to have access to the system as the user.

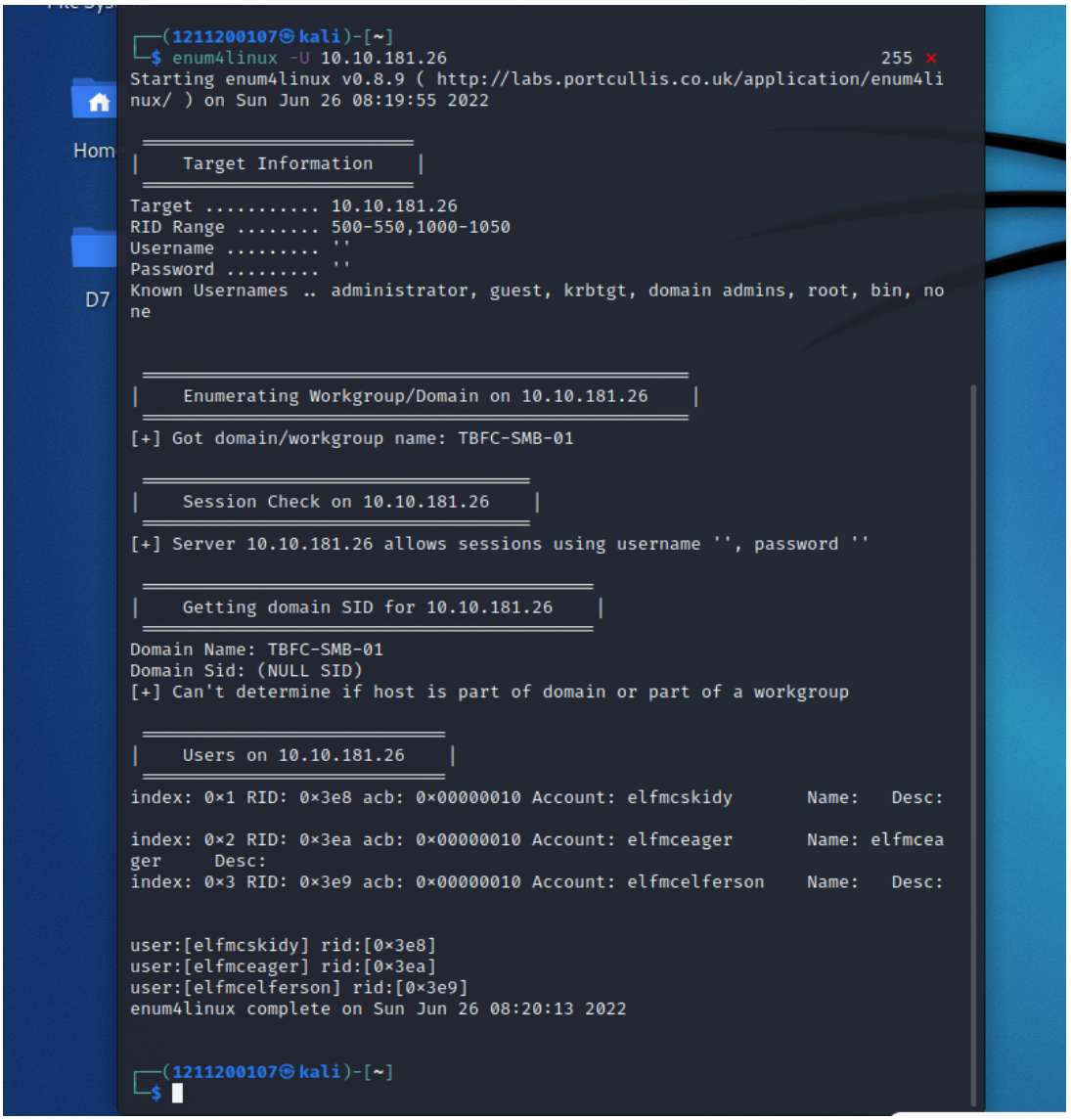
Day 10: Networking - Don't be sElfish!

Tools Used: Kali Linux, Terminal

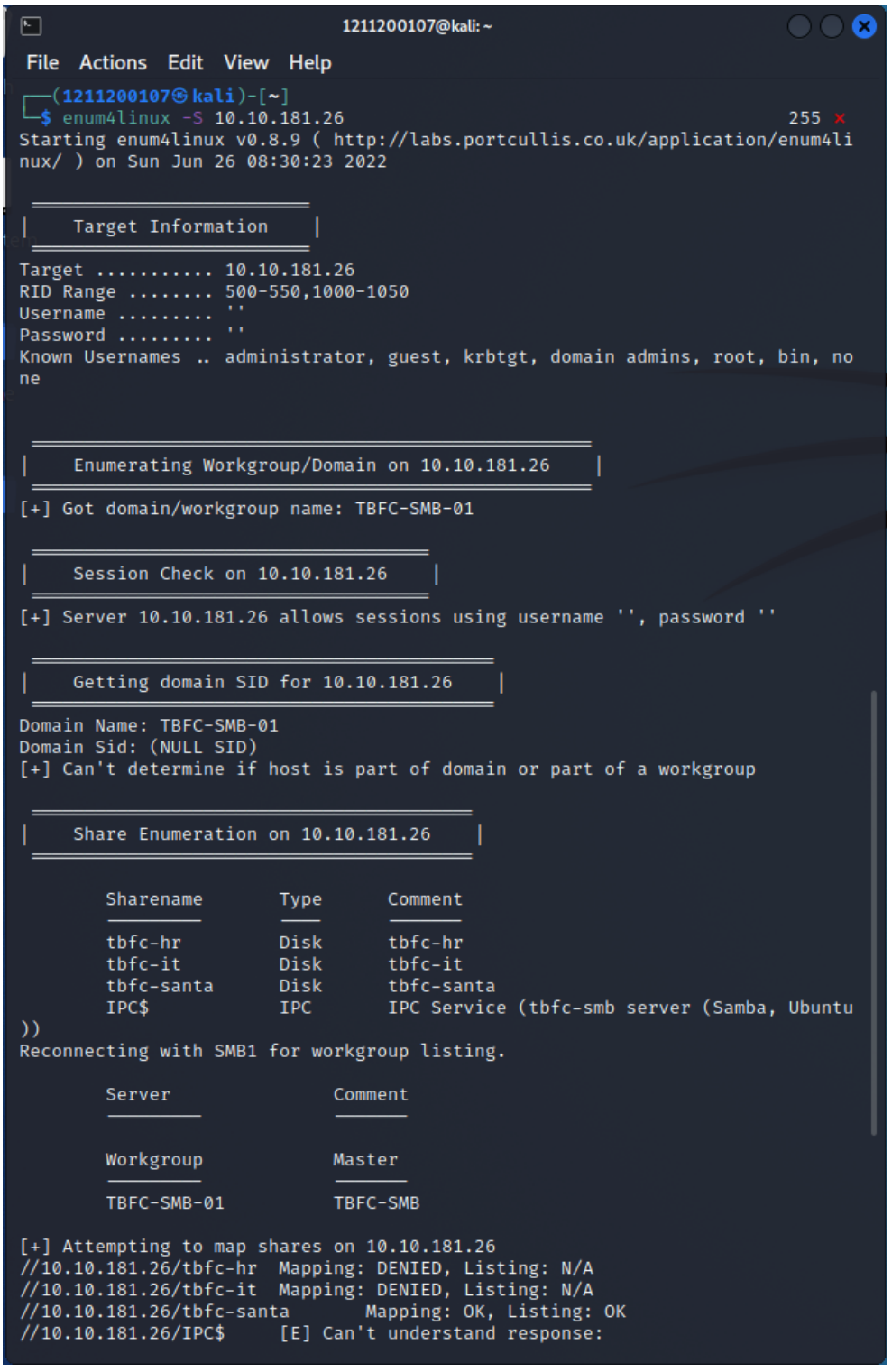
1. We will go on terminal for the first question and type in *enum4linux.* We will look for the answers on the list on terminal



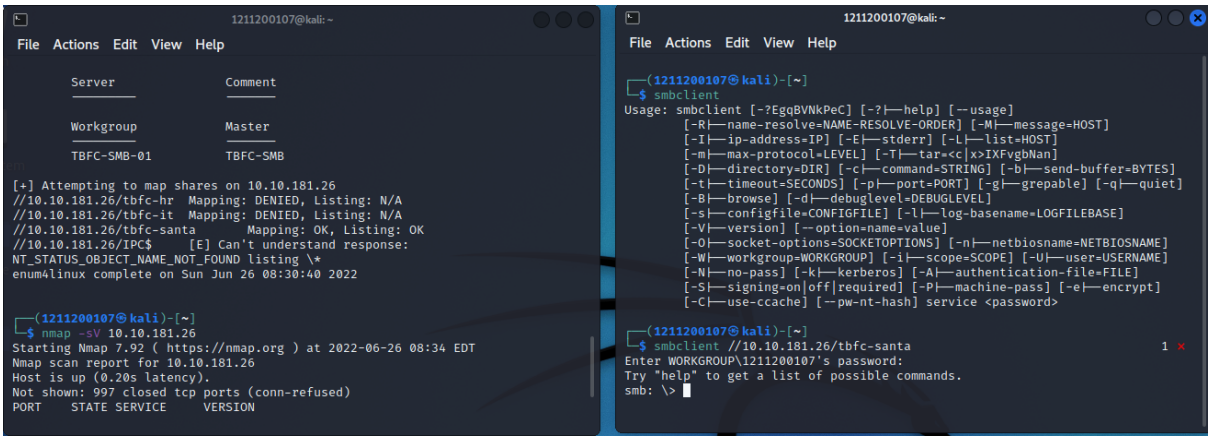
2. To check users on a server, we will go on terminal and type *enum4linux -U 10.10.181.26*, answering question 2



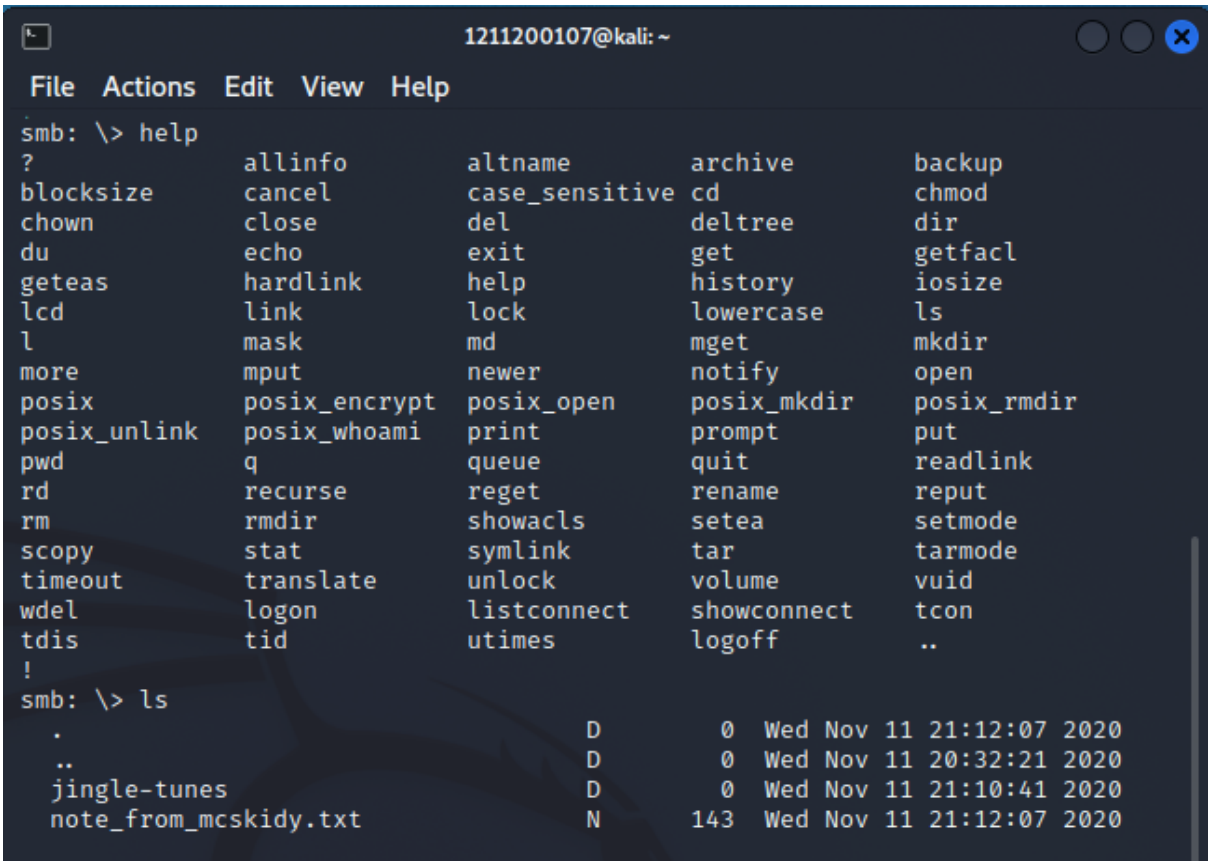
3. For the third question, we must use *enum4linux -S 10.10.181.26* to see the sharelist. This gives the answer to the third question, which is a total of 4.



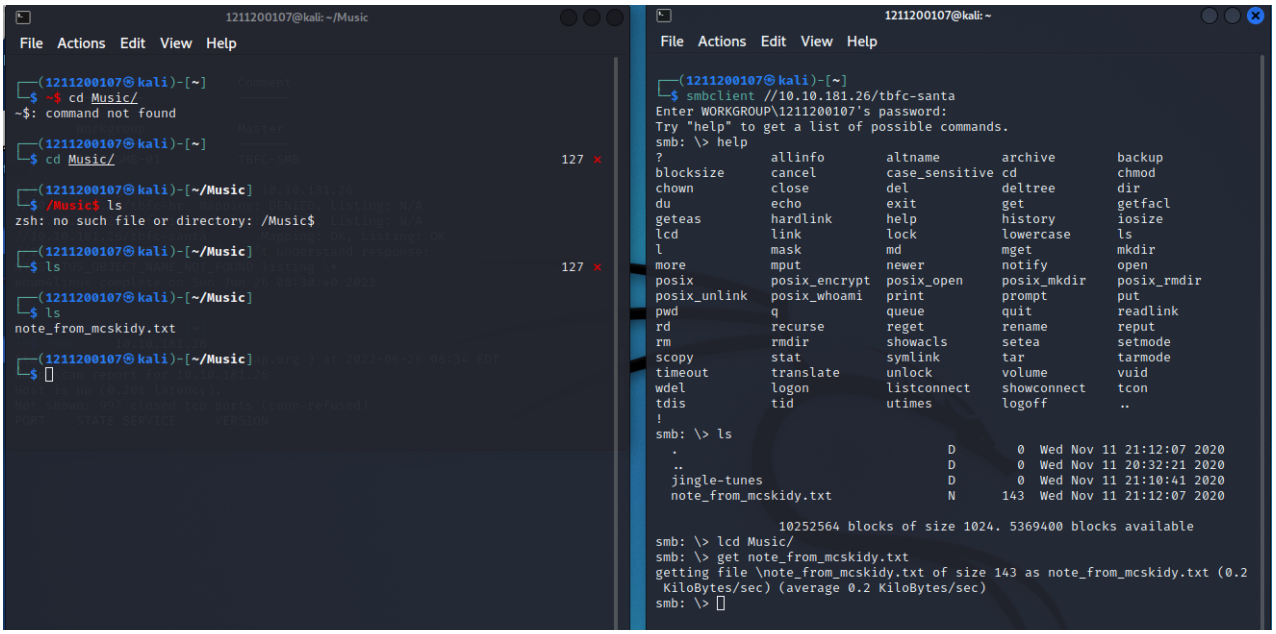
4. For the fourth question, we will be using *smbclient* in the terminal. Type in *smbclient //10.10.181.26/tbfc-santa*.



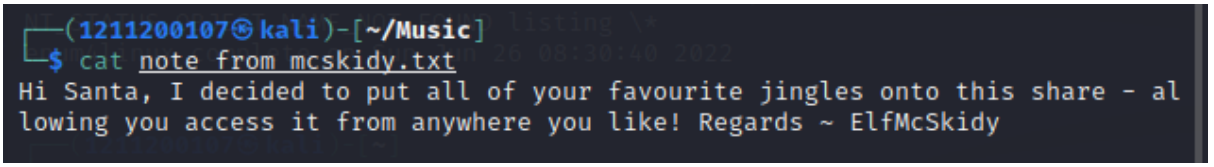
5. To check what directory ElfMcSkiddy left for Santa, we will use the *ls* command. we find that there is a note from McSkidy.



6. We use command *lcd Music/* (local current directory) and as well as *get note_from_mcskidy.*



7. Next, we use the *cat* command to find out what is said in the .txt file, leaving us with the answer to the last question.



Thought Process/Methodology:

Starting off, we will be using the terminal to type in *enum4linux*. The answers to question 1 are listed on the terminal. Next, we are going to check the users on the servers by typing *enu4linux -U 10.10.181.26* on the terminal and counting the number of users listed. After that, we will be using the *-S* command on the terminal for the sharelist, giving us a total of 4 listed on the sharelist. Later, on the terminal, we will then be using the *smbclient* and typing in *//10.10.181.26/tbfc-santa*. We will use the *ls* command which is used to list files or directories. After using the ls command, we find that there is a .txt file from Elf McSkidy. We then use the command *lcd Music/* along with the *get note_from_mcskidy.txt* command. We use the cat command to find out what the note is about and giving us the answer to last question. The directory left by Elf McSkidy for Santa is the jingle-tunes directory.