# PSP 0201
# Week 3 Report

**Group Name:DHM**

**Members:**

| Student ID | Name |
|---|---|
| 1211101844 | TAN EASON |
| 1211103690 | JERELL SU MING JIE |
| 1211103145 | AZRYL SHAMIN BIN AZRIZAL |

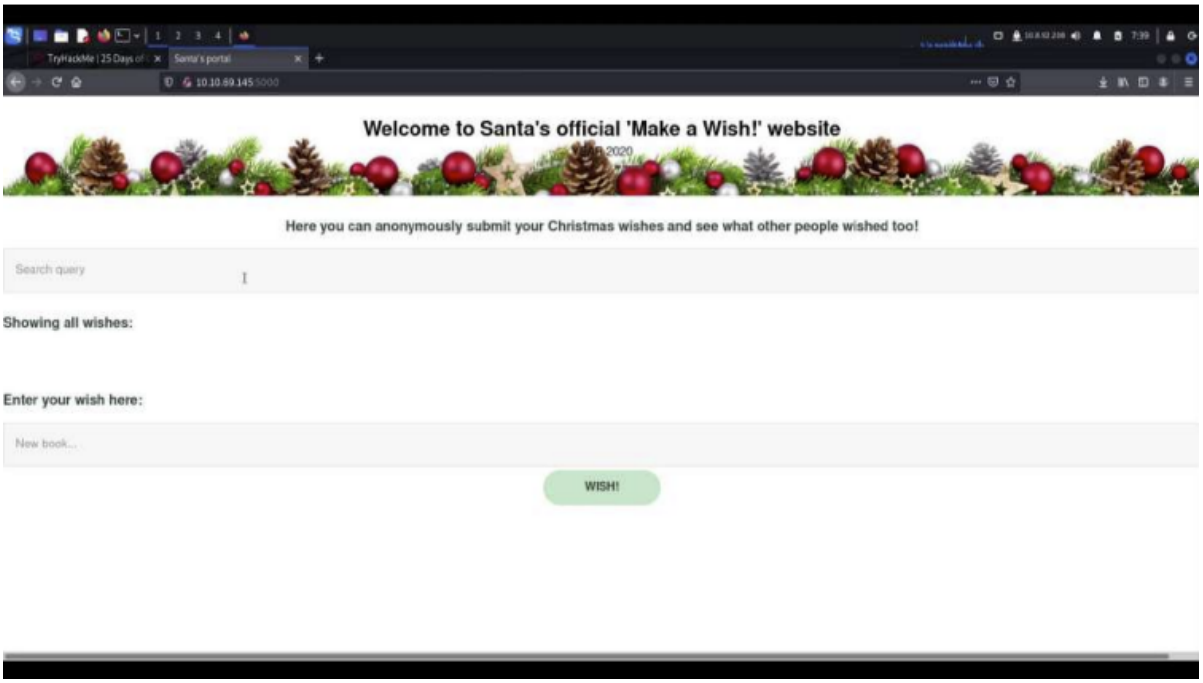
## Day 6: Web Exploitation – Be careful with what you wish on a Christmas night

**Tools Used:**Kali Linux, Firefox,Zaproxy

### Solution:

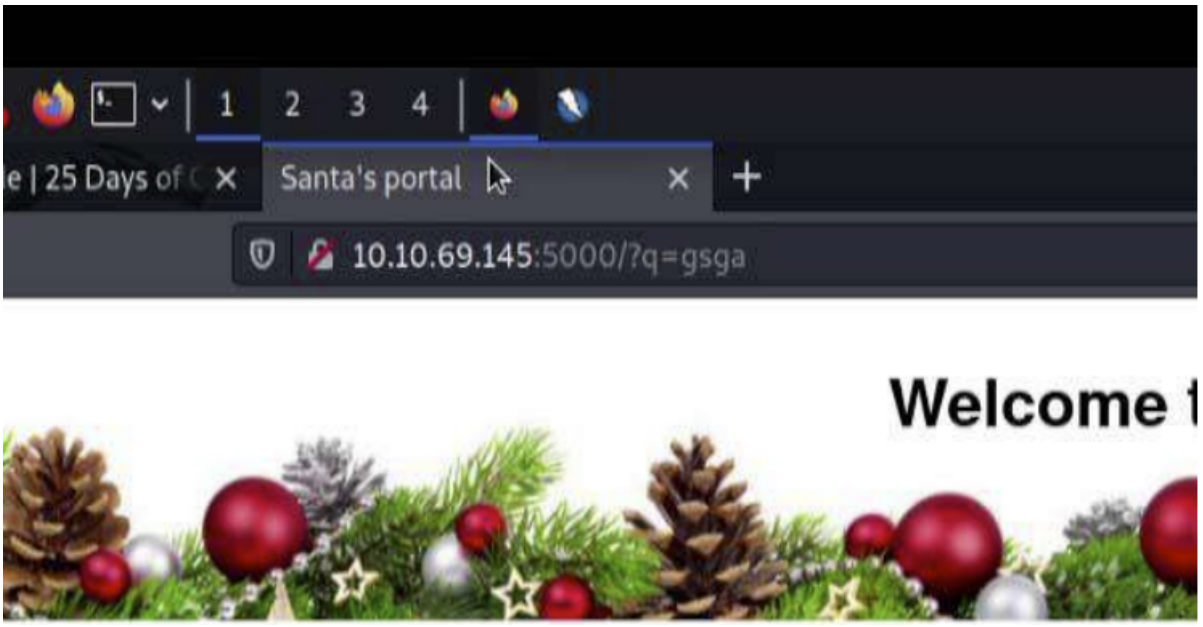
**Q1:**

Copy and paste the IP from try hack me



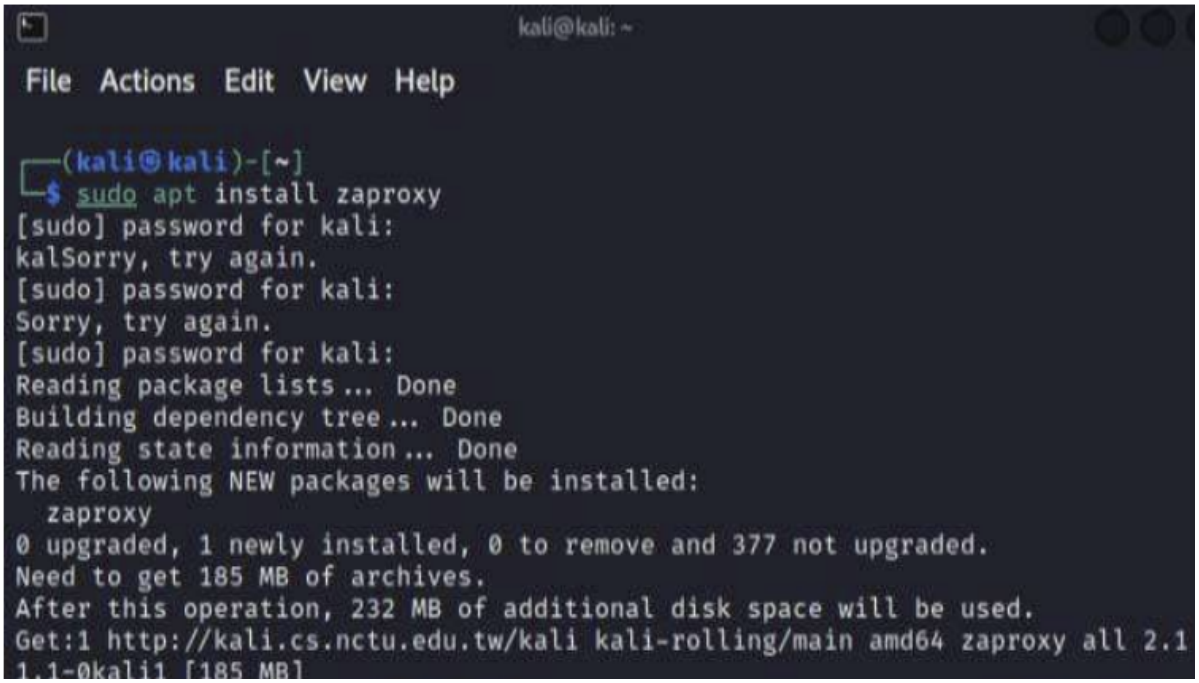

**Q2:**

Search anything and take a look at the link address.

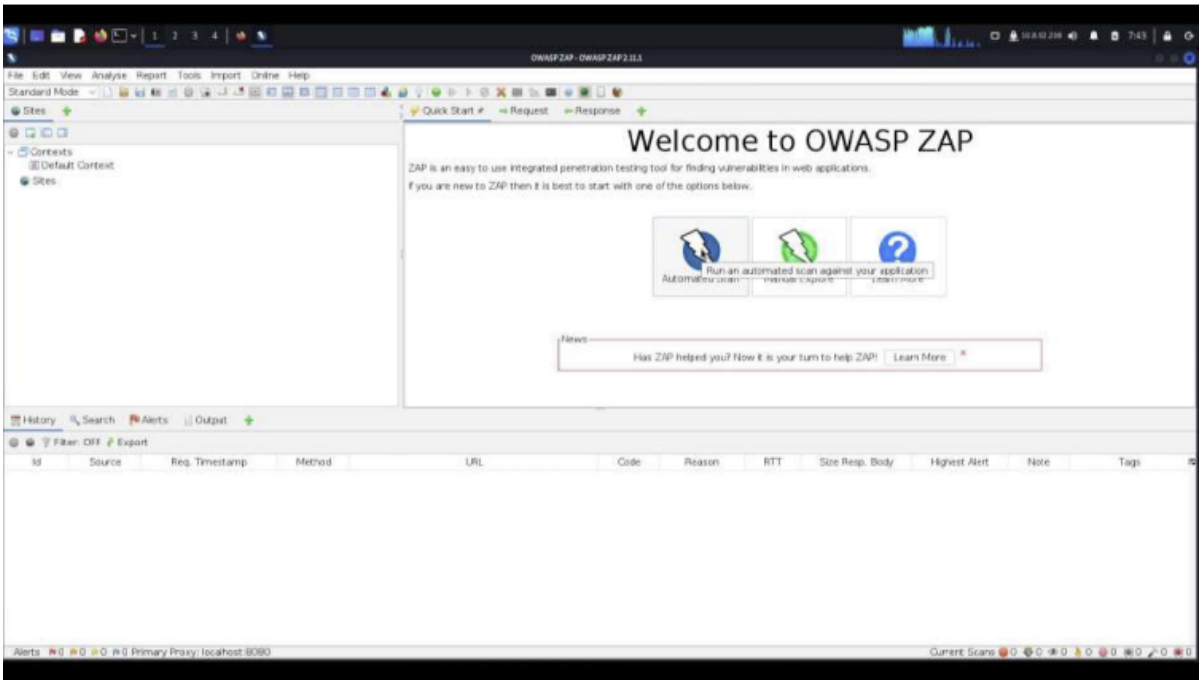



**S3:**

Open terminal and install Zaproxy using the following command:
sudo apt install zaproxy

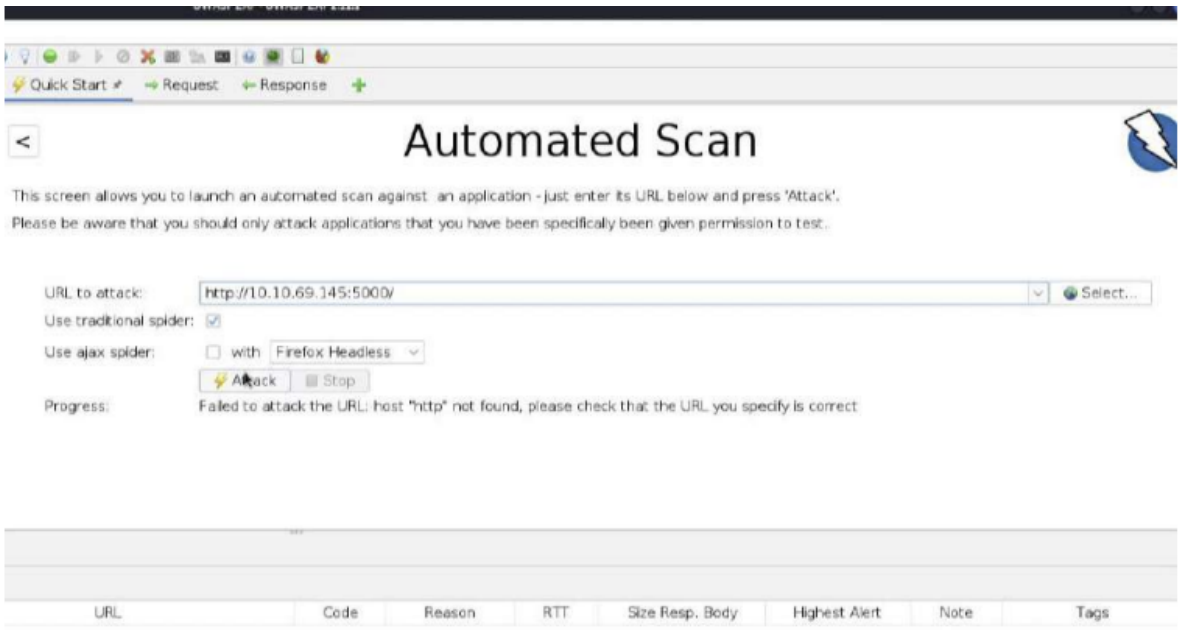



After installing, open Zaproxy and it will show the menu as below:

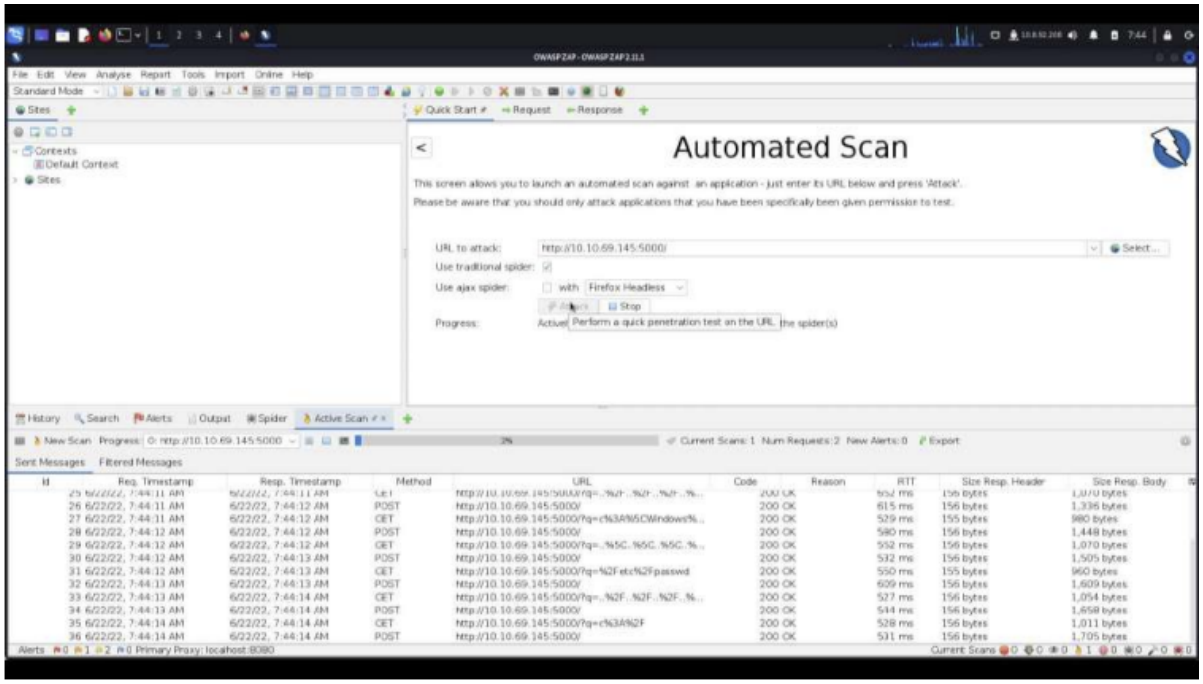



## S4:

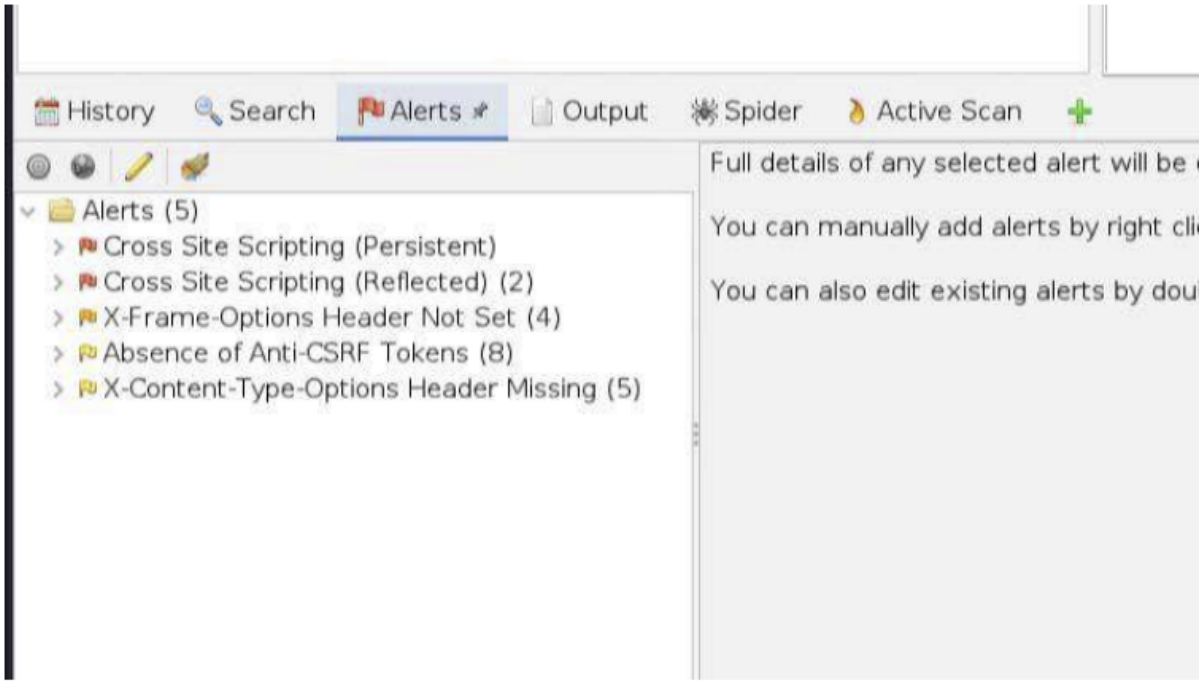
Now go to the automated scan and paste the machine ip.



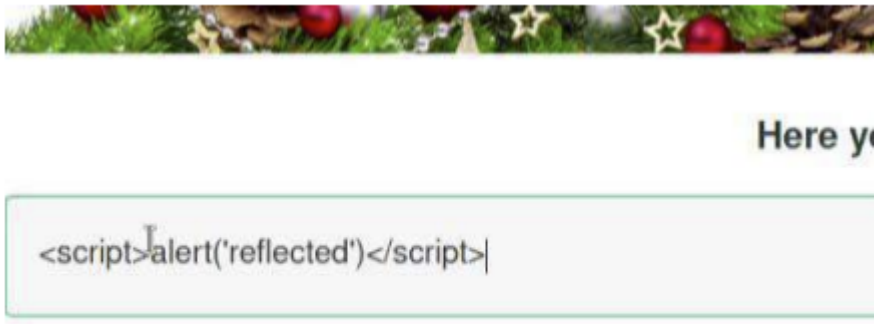

Press the Attack button.

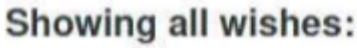



Go to the Alerts tab and count all the alerts.

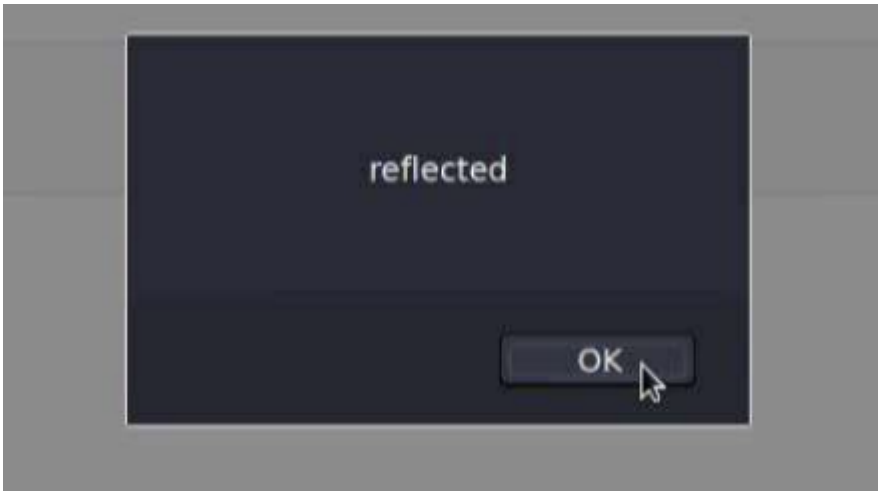



Q5:
Go to Wish a Wish website, type <script>alert(‘reflected’)</script> into the first search box.

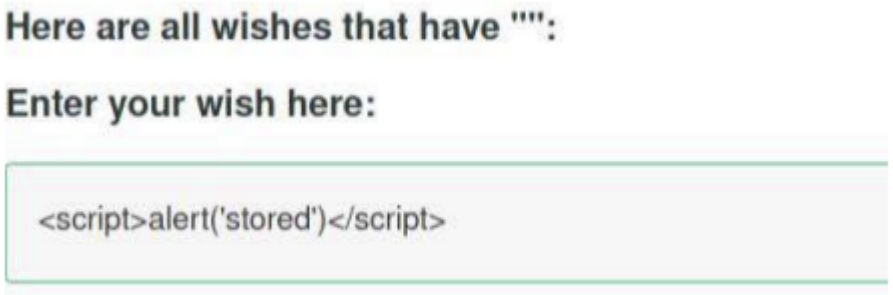



It will be reflected




For the second search box, type <script>alert('stored')</script>




It will be stored


**Thought Process/Methodology:**

After entering the machine ip, the website shows something about making a wish and having 2 search boxes. I tried to search for anything and it will show ?q= at the link address of the website. After that, I need to install Zaproxy using the command sudo apt

install zaproxy and attack the website. When attacking the website, the alerts will pop out inside the alerts tabs of Zaproxy. Here's how I am able to make an alert appear on the website: type on the first search box and first alert which saying reflected will pop out; type on the second search box and few alerts will pop out.

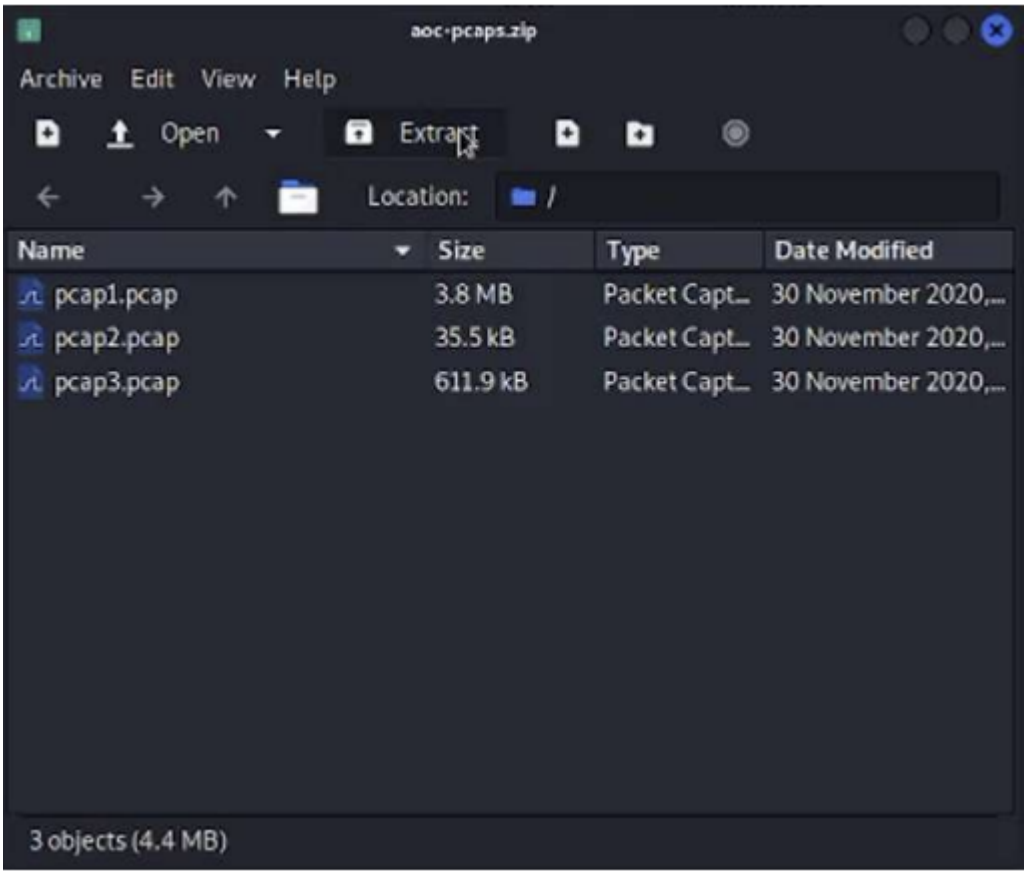
## Day 7: Networking - The Grinch Really Did Steal Christmas

**Tool used:Kali Linux,Wireshark**

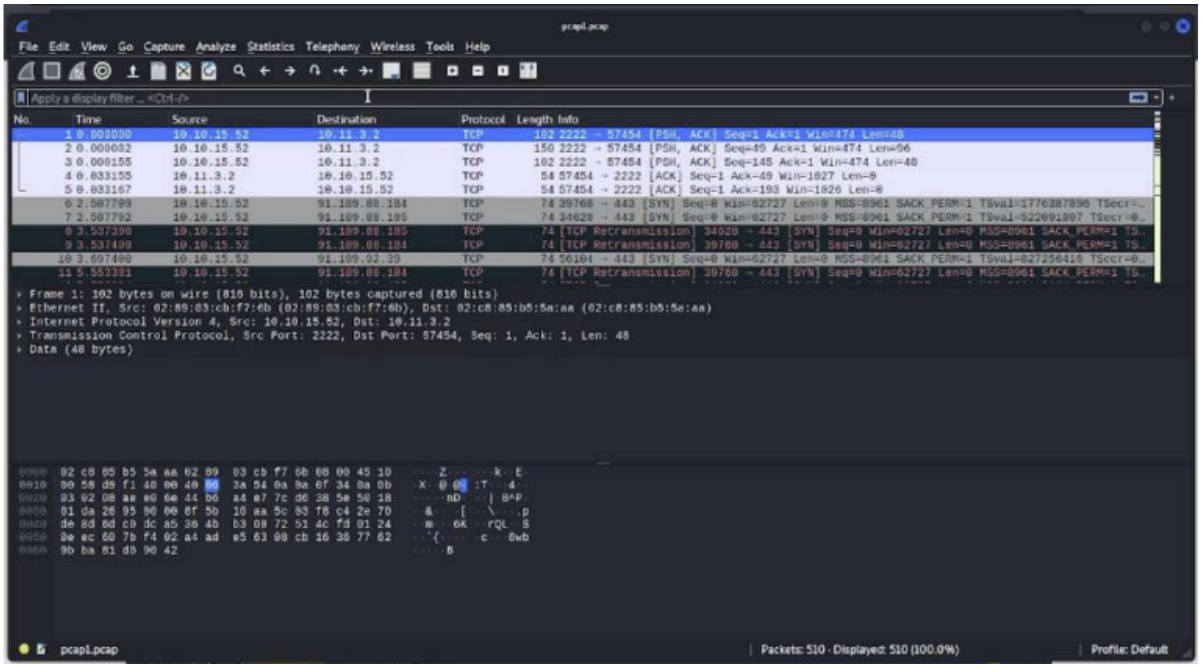
**Solution:**

Q1:

Download the file from THM and extract the zip file.

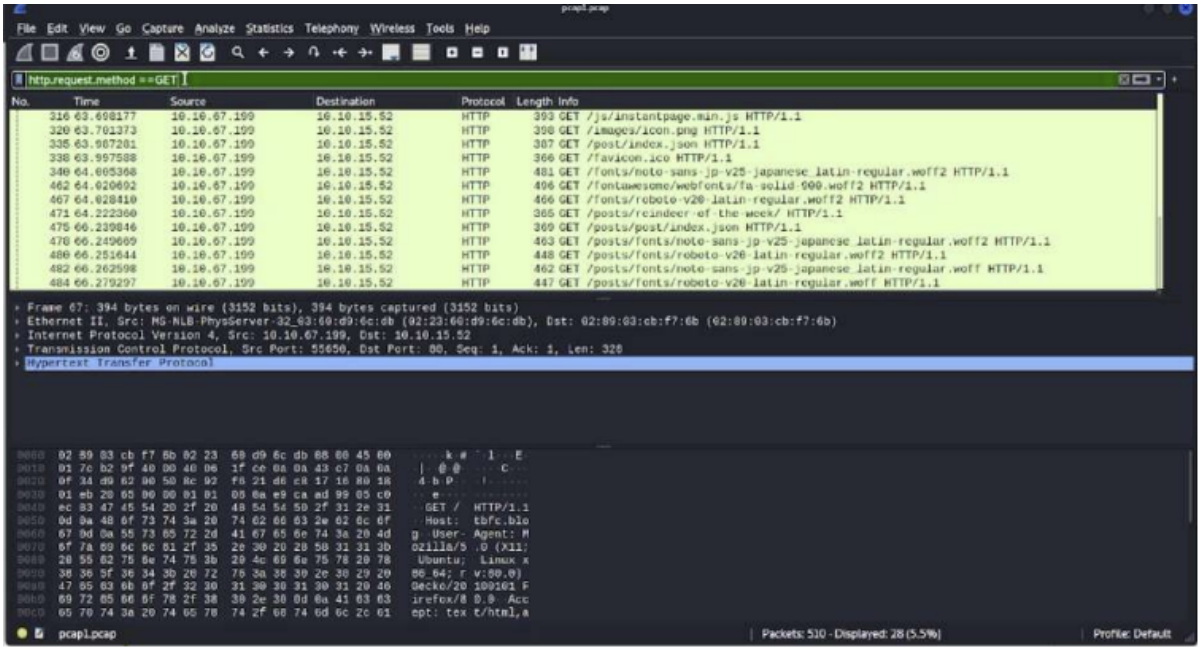



Find the IP address by searching ICMP from pcap1.pcap file.



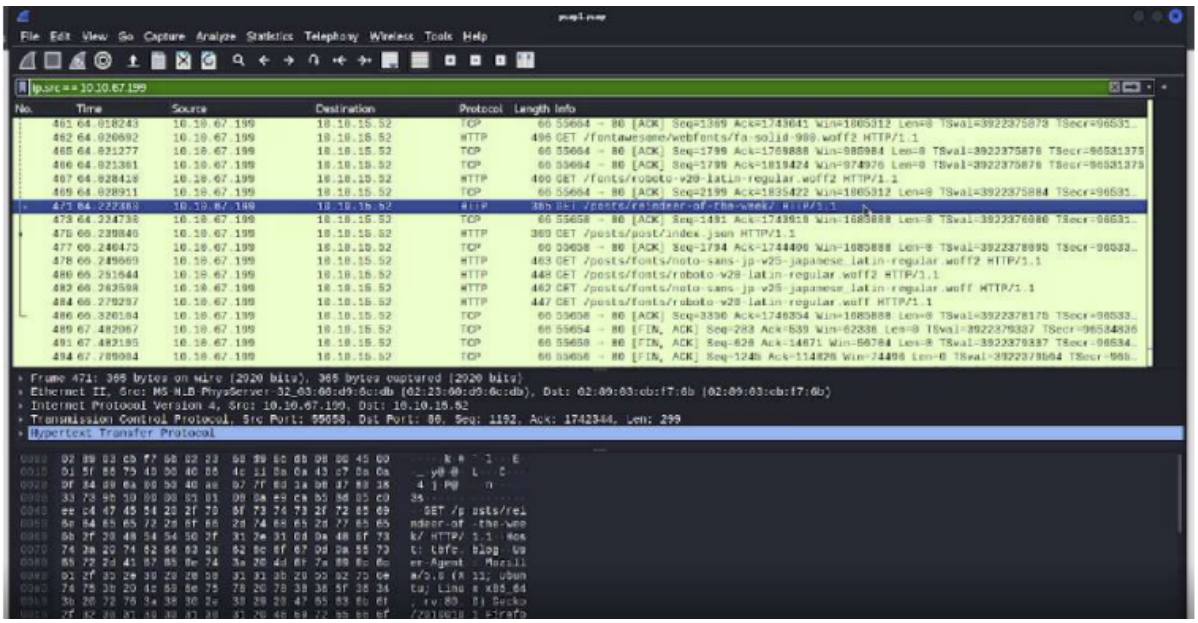

Q2:

We used the “http.request.method == GET " filter to GET request HTTP in the pcap1.pcap file.



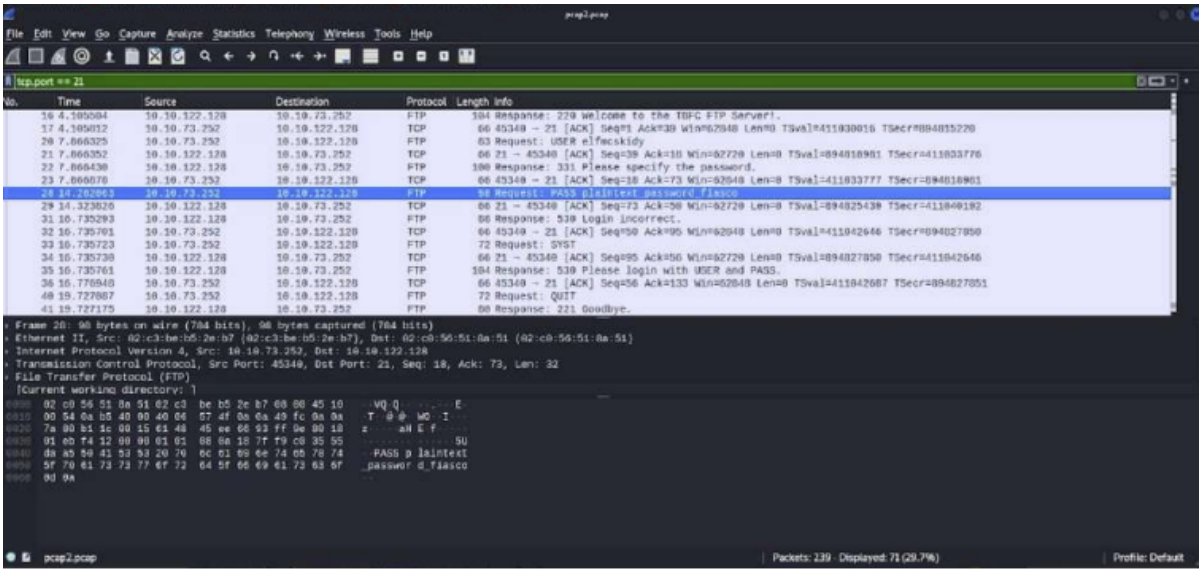

Q3:

To find the article of IP address 10.10.67.199, we need to apply a filter in pcap1.pcap. Key in “ip.src == 10.10.67.199” to find the article name from the info column.



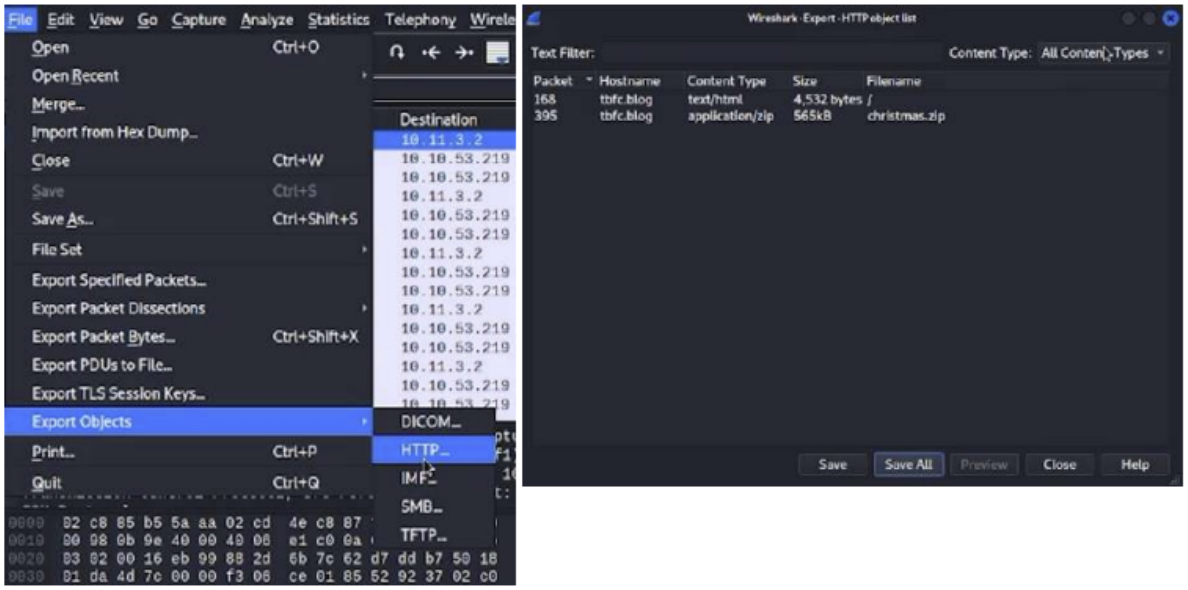
Q4:

As FTP uses the TCP protocol, we apply the "tcp.port == 21" filter in pcap2.pcap file order to look for the leaked password.

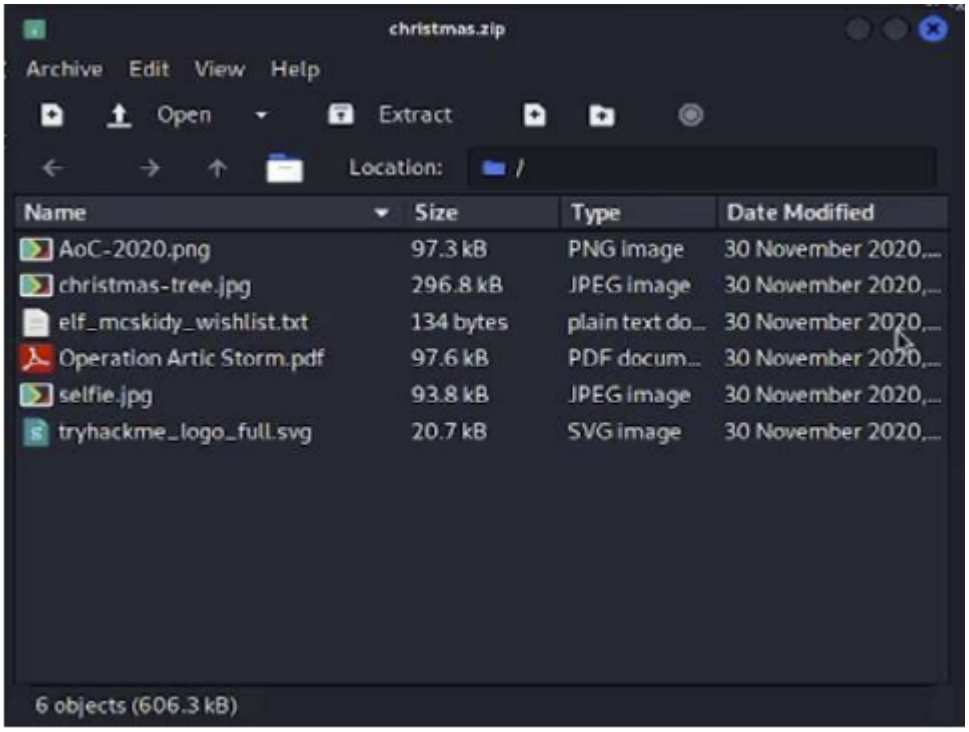


Q5:

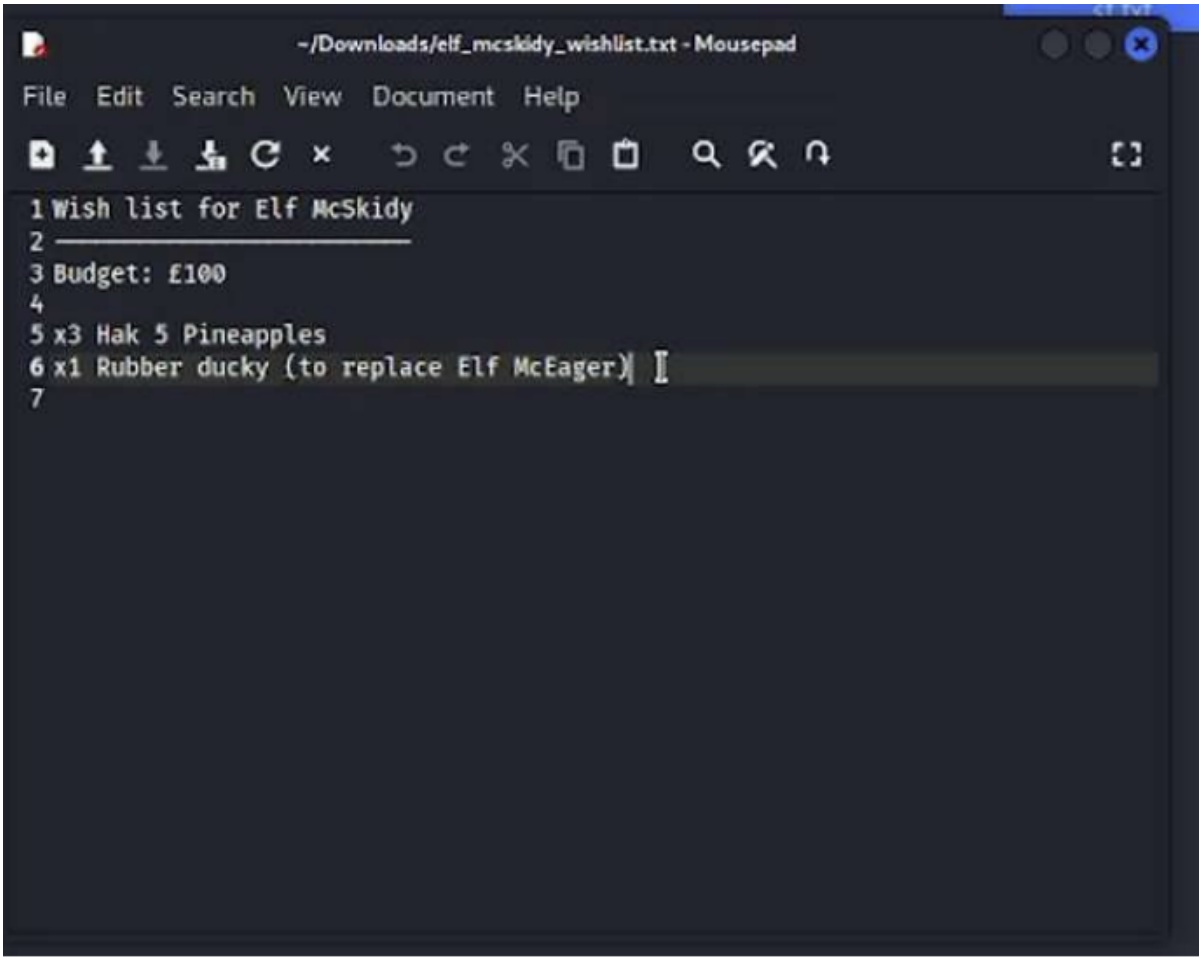
We need to use pcap3.pcap file to recover the “Christmas” zip file. Then, navigate File > Export Objects > HTTP and save into a folder.




Extract the zip file.




Open the elf_mcskidy_wishlist.txt file to get the info we want




**Thought Process/Methodology:**
This task will guide us about Wireshark. First and foremost, we need to download and extract the zip files from TryHackMe first. Then, in order to find the IP address of the request and reply, we search ICMP from pcap1.pcap file. After that in the pcap1.pcap file, we use the “http.request.method == GET " filter to make an HTTP GET request. Next, we know that we need to use “ip.src” to filter out the packets. Hence, to find the article of IP address 10.10.67.199, we apply the filter “ip.src == 10.10.67.199” in the pcap1.pcap file to find the article name from the info column. Then, in pcap2.pcap file order, we use the "tcp.port == 21" filter to look for all FTP traffic and follow the TCP stream we find the leaked password which is "plaintext_password_fiasco". Following that, we use pcap3.pcap file to recover the “Christmas” zip file. Then, navigate File > Export Objects > HTTP and save it, and extract the zip file and open the

elf_mcskidy_wishlist.txt file to get the information we need, which is Rubber Ducky.

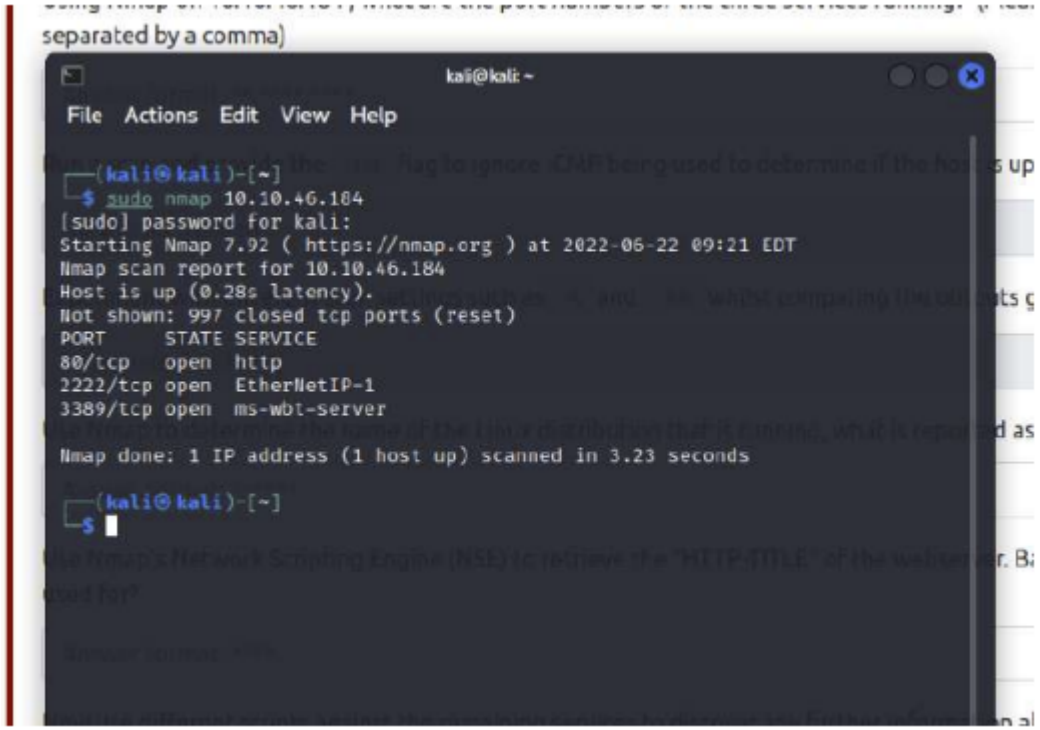
## Day 8: Networking What's Under the Christmas Tree?

**Tools used:**Kali Linux,Firefox

**Solution:**

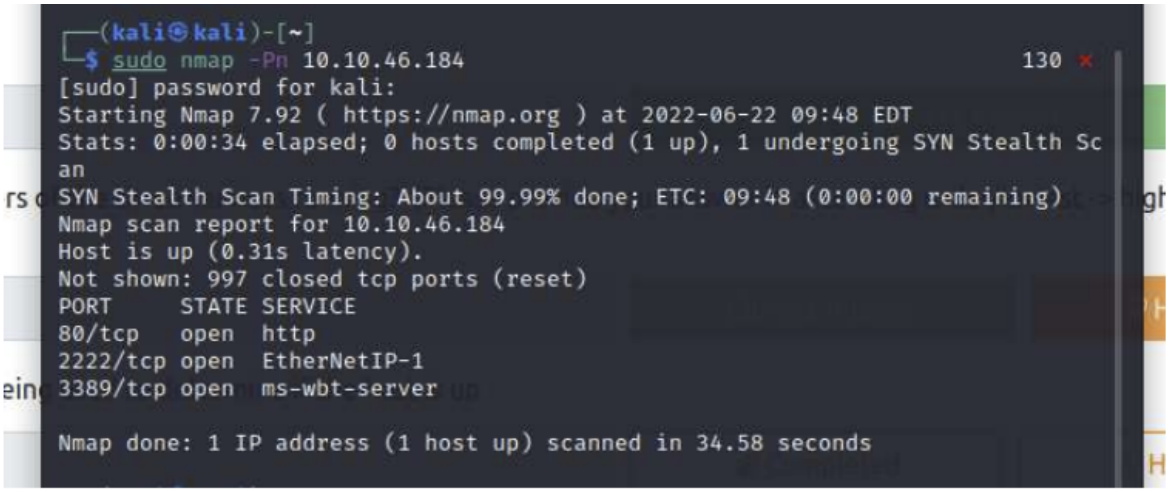
Q1:

Open the terminal and scan the IP given.




Q2:

Run a scan and provide the -Pn flag to ignore ICMP being used to determine if the host is up.




Q3:
Experiment with different scan settings such as -A and -sV while comparing the outputs.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 10.10.46.184
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 09:54 EDT
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Traceroute
Traceroute Timing: About 32.26% done; ETC: 09:55 (0:00:00 remaining)
Nmap scan report for 10.10.46.184
Host is up (0.30s latency).
Not shown: 997 closed tcp ports (reset)
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; p
rotocol 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
No exact OS matches for host (If you know what OS is running on it, see https
://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=6/22%OT=80%CT=1%CU=44404%PV=Y%DS=2%DC=T%G=Y%TM=62B31F5
OS:3%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=105%TI=Z%CI=Z%II=I%TS=A)OPS
OS:(O1=M506ST11NW6%O2=M506ST11NW6%O3=M506NNT11NW6%O4=M506ST11NW6%O5=M506ST1
OS:1NW6%O6=M506ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN
OS:(R=Y%DF=Y%T=40%W=F507%O=M506NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=A
OS:S%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R
OS:=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F
OS:=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%
OS:T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD
OS:=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 23/tcp)
HOP RTT       ADDRESS
1   277.41 ms 10.18.0.1
2   278.42 ms 10.10.46.184

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.20 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV 10.10.46.184
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 09:59 EDT
Nmap scan report for 10.10.46.184
Host is up (0.32s latency).
Not shown: 997 closed tcp ports (reset)
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; p
rotocol 2.0)
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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 56.49 seconds
```

Q4:
Use Nmap to determine the name of the Linux distribution that is running which is Ubuntu Linux.

```
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; p
rotocol 2.0)
```

Q5:
Use Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver which led us to the blog.

```
|_http-title: TBFC&#39;s Internal Blog
```

**Thought Process/Methodology:**
This task only requires a terminal. First of all, we scan the ip given by TryHackMe by using nmap. Then the terminal will display three port numbers which are 80, 2222, 3389. After that to determine if the host is up, we can run the -Pn flag to ignore ICMP being used. As we all know, -A can be used in nmap to scan the host to identify services running by matching against the nmap database, and -sV can scan the host using TCP and perform version fingerprinting. Hence, we used -A and -sV to get the report.And both of the reports lead to the Linux distribution that is running in Ubuntu Linux. Lastly, we use nmap to get the "HTTP-TITLE" of the web server is a blog.

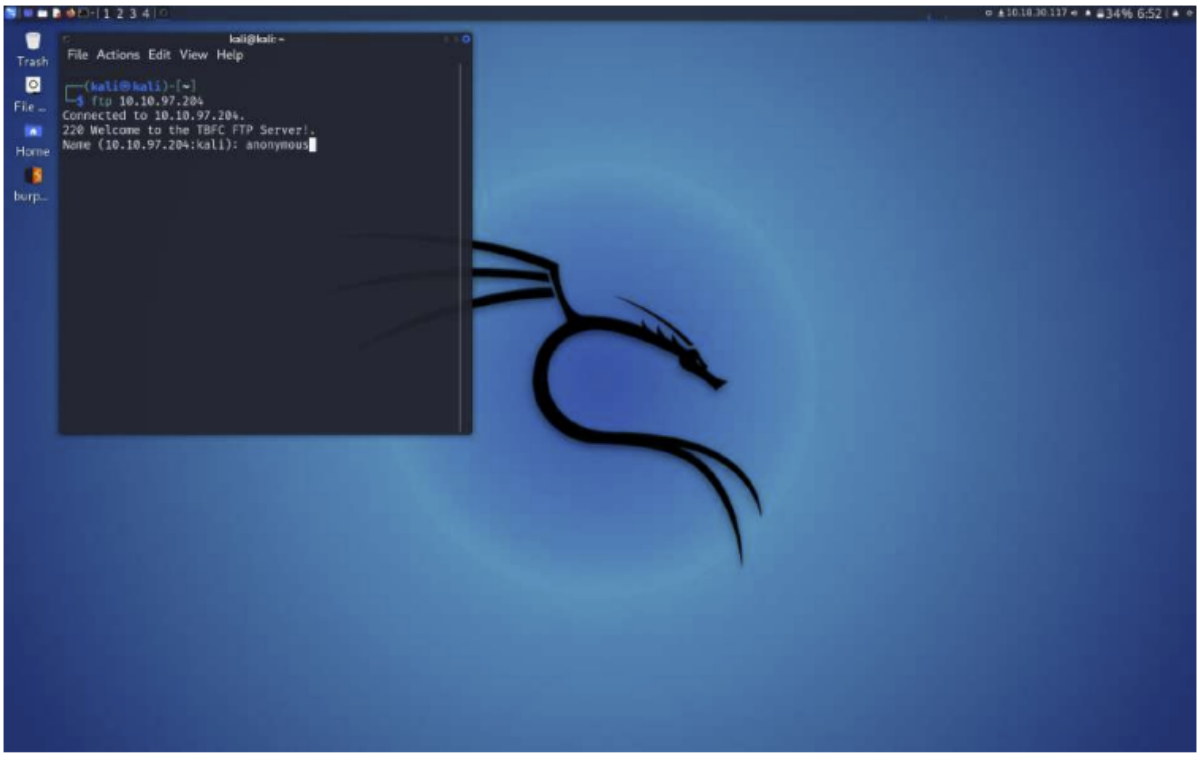
**Day 9: Anyone can be Santa!**

**Tools used:** Kali Linux, Mozilla Firefox

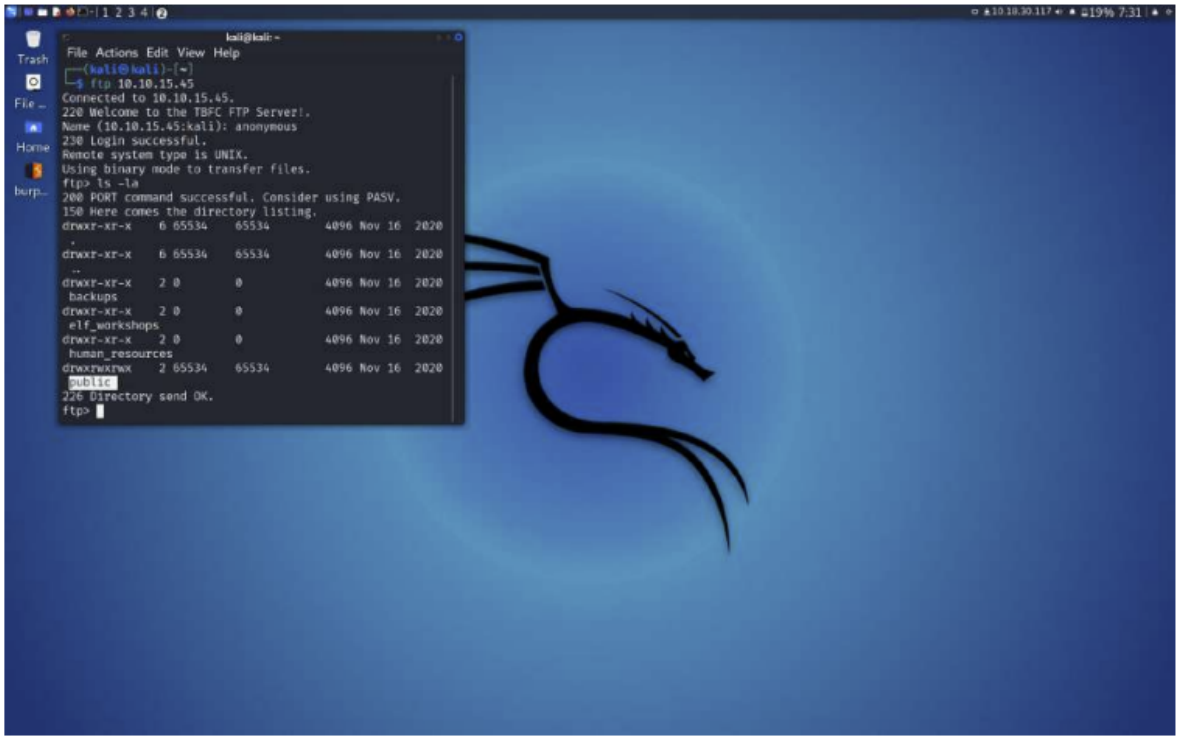
**Solution:**

Q1:

Ftp the IP address from TryHackMe and then name as anonymous.

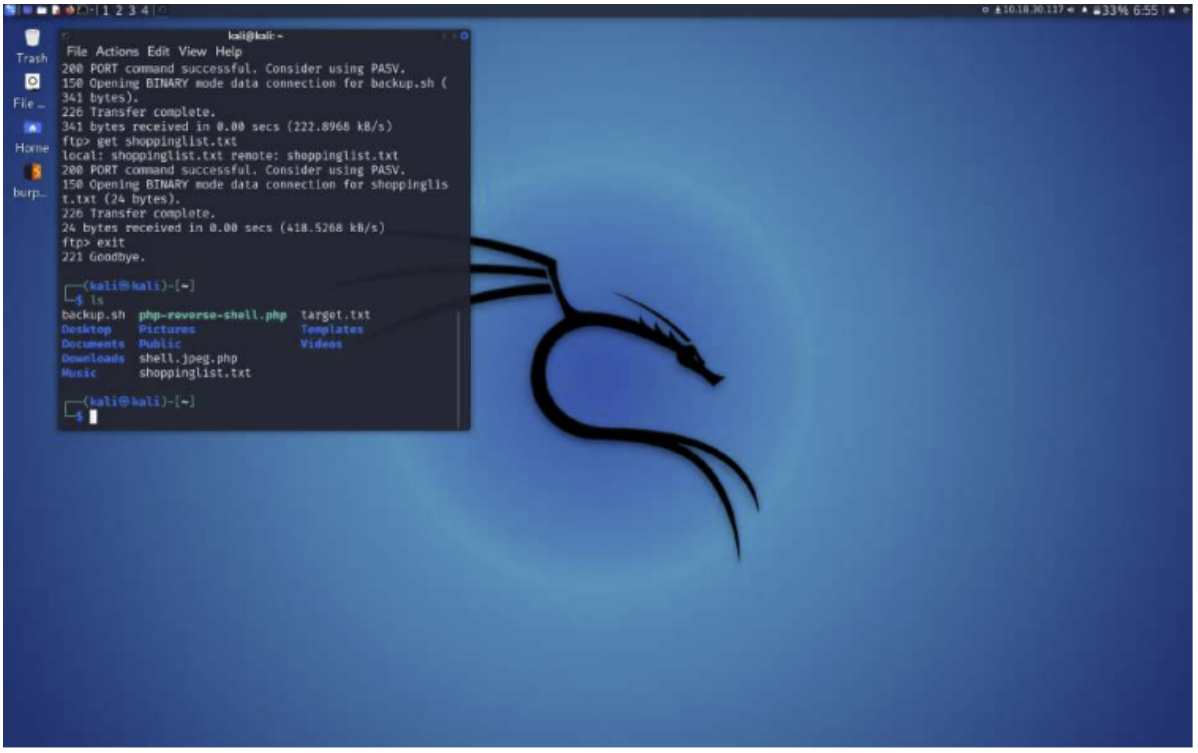



Type ls -la and it will show you the public.

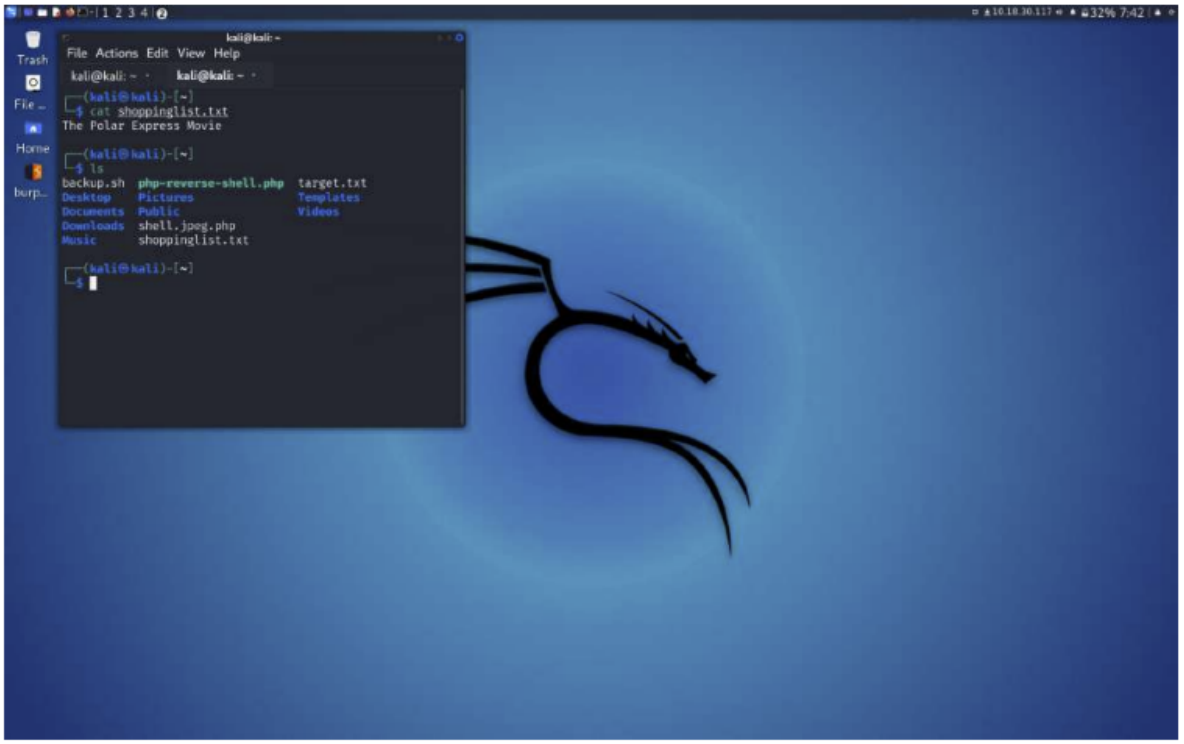



Q2:

List will be shown below after entering the backup.sh and shoppinglist.txt.

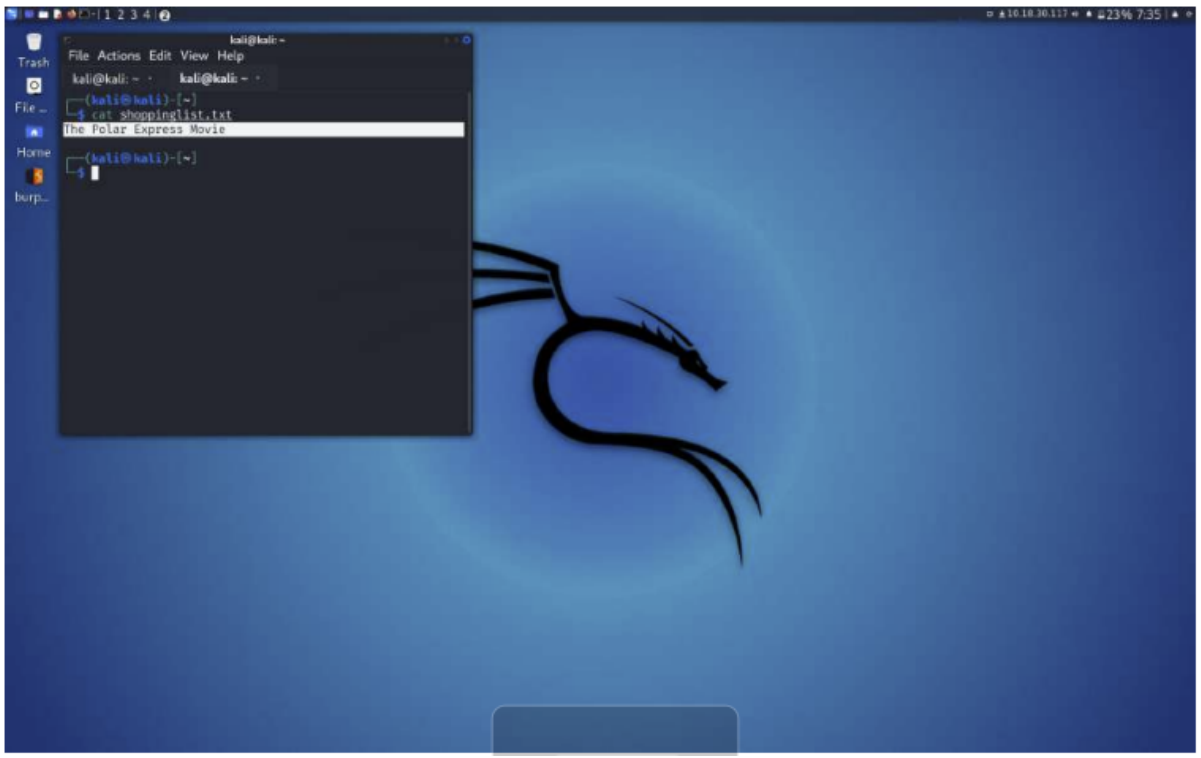



Type ls for the list, and it will show you backup.sh.



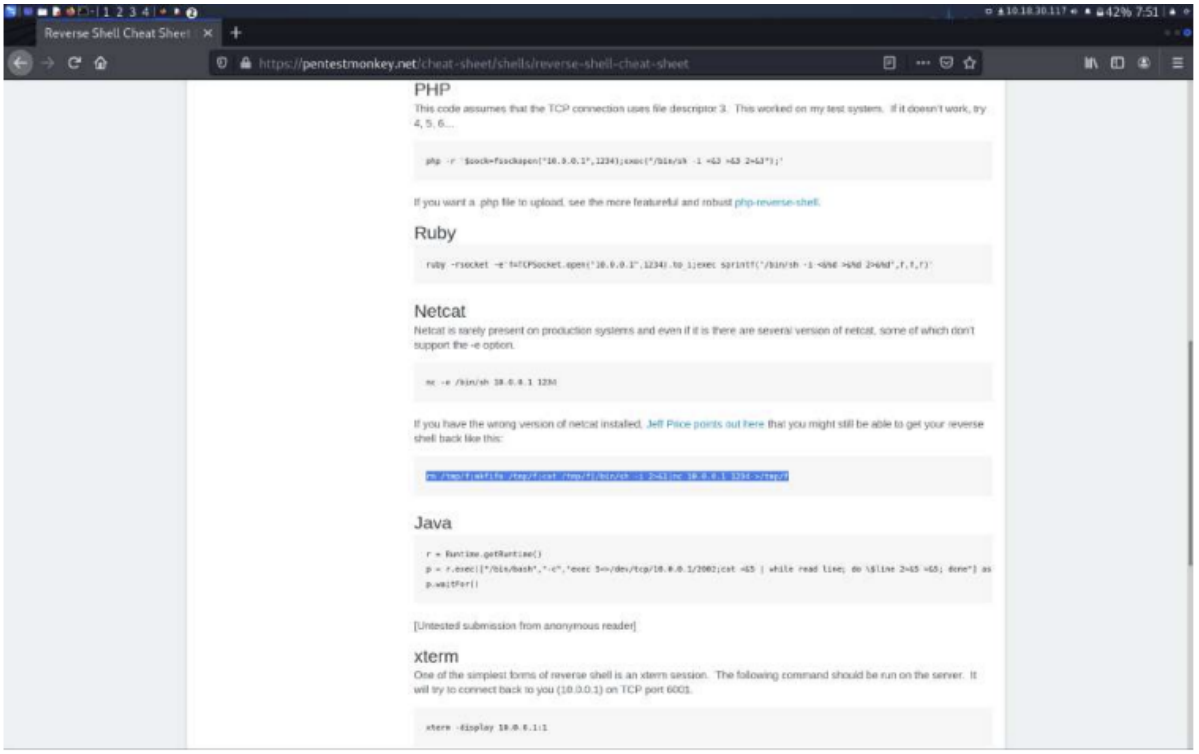

Q3:

On the other new tab, type cat shoppinglist.txt and you will be able to see what movie did Santa have on his Christmas shopping list.

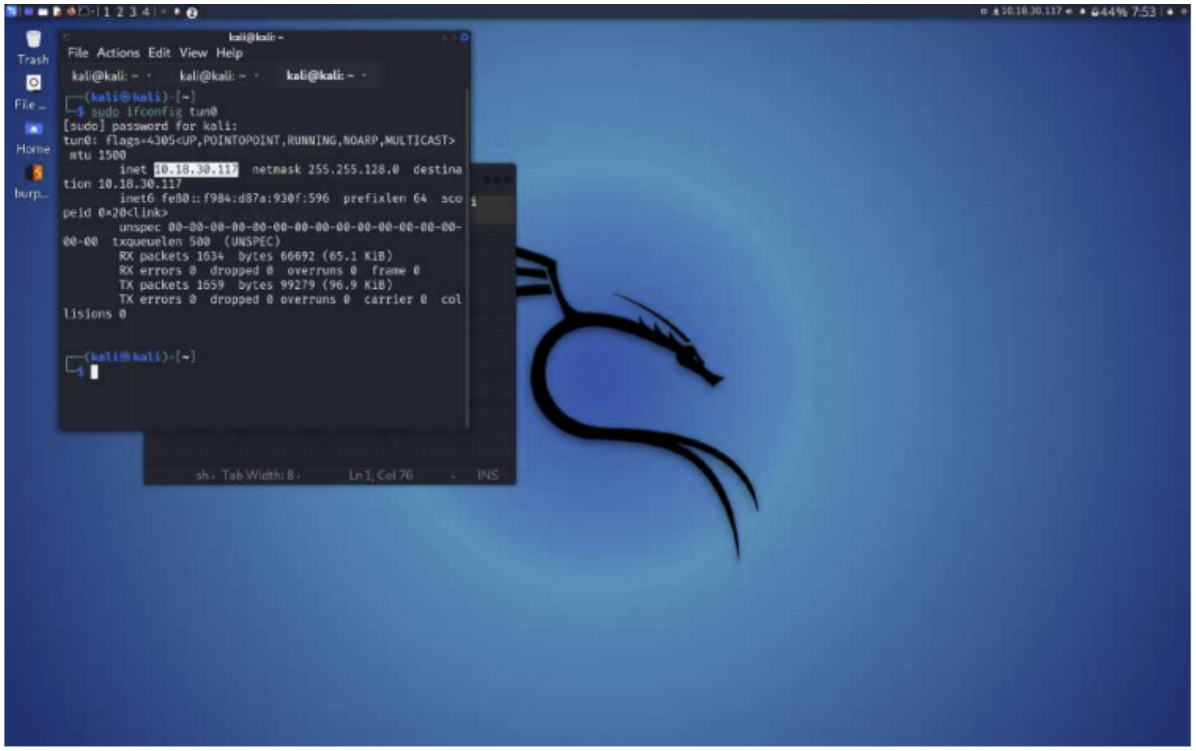



Q4:

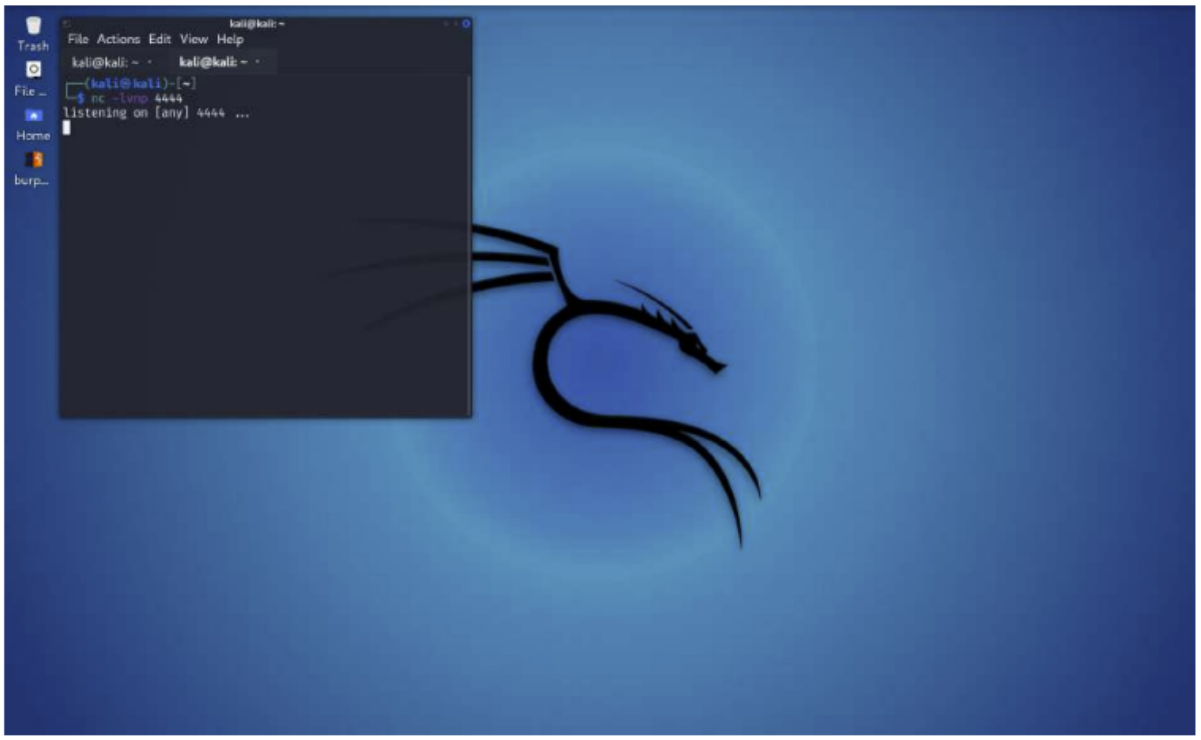
Browse reverse shell pentestmonkey and look for the Netcat.




Type sudo ifconfig tun0 . Thus enter the password to copy down the IP address.




Open a new terminal tab. Hence, type nc -lvnp 4444




View the file using cat flag.txt command


**Thought Process/Methodology:**

This task doesn't really use the web browser, any browser can do it. First of all, copy and paste the IP address into the terminal and add ftp in front of it. FTP is also known as file transfer protocol. Later on, type ls -la to show you the directory listing and public. After type get shoppinglist.txt and backup.sh, enter exit and type ls to show the list. At the tool bar, click file and add a new tab to proceed. type cat shoppinglist.txt and you will be able to see what movie Santa has on his Christmas shopping list. On the other hand, browse reverse

shell pentestmonkey on any browser and look for the Netcat. After setting up, type sudo ifconfig tun0, enter the password to copy down the IP address. Wait a while for the Netcat listener on the device. Last but not least, type cat flag.txt and it will show the answer.

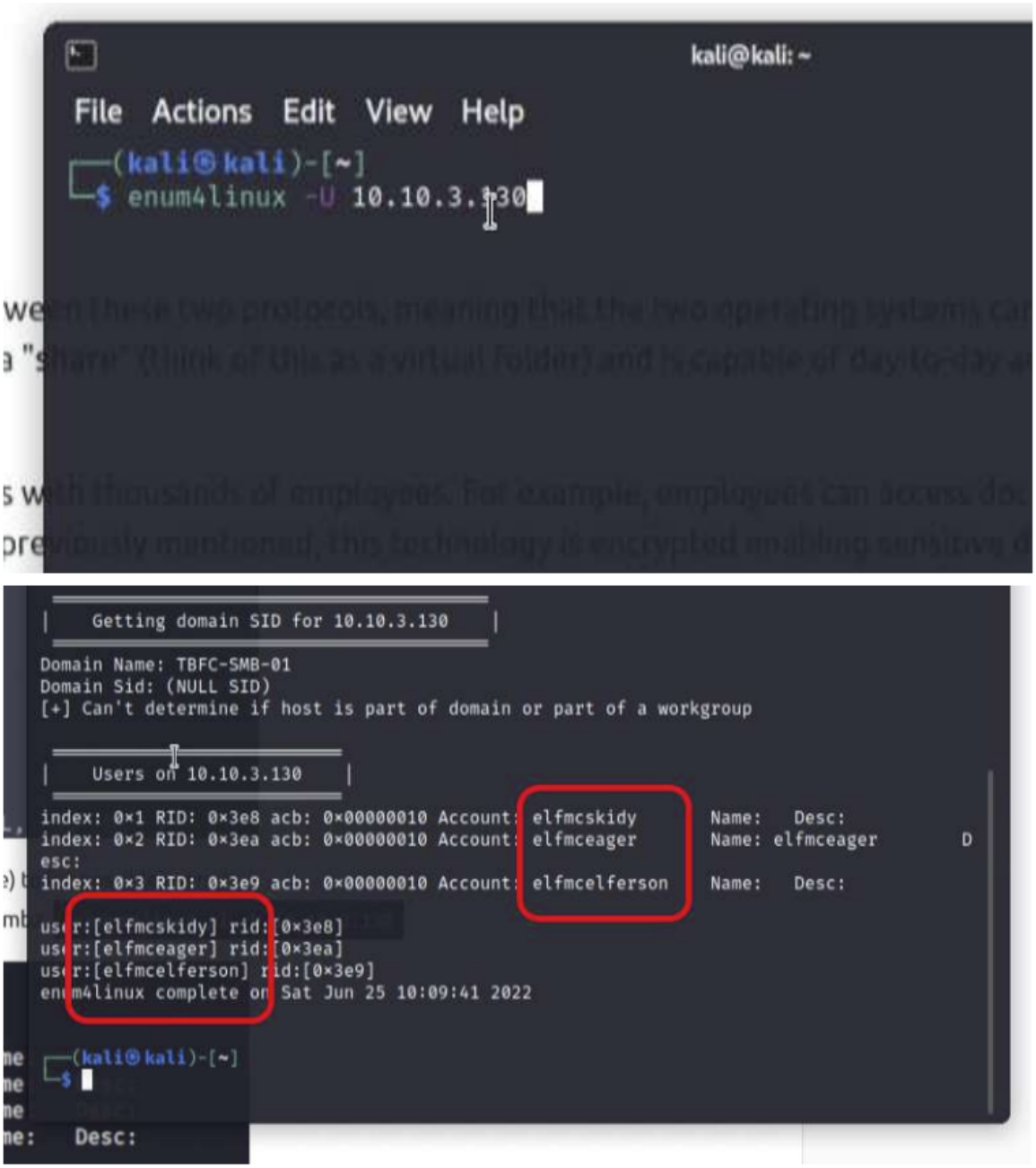
**Day 10: Don’t be sElfish!**

**Tool Used:**Kali Linux

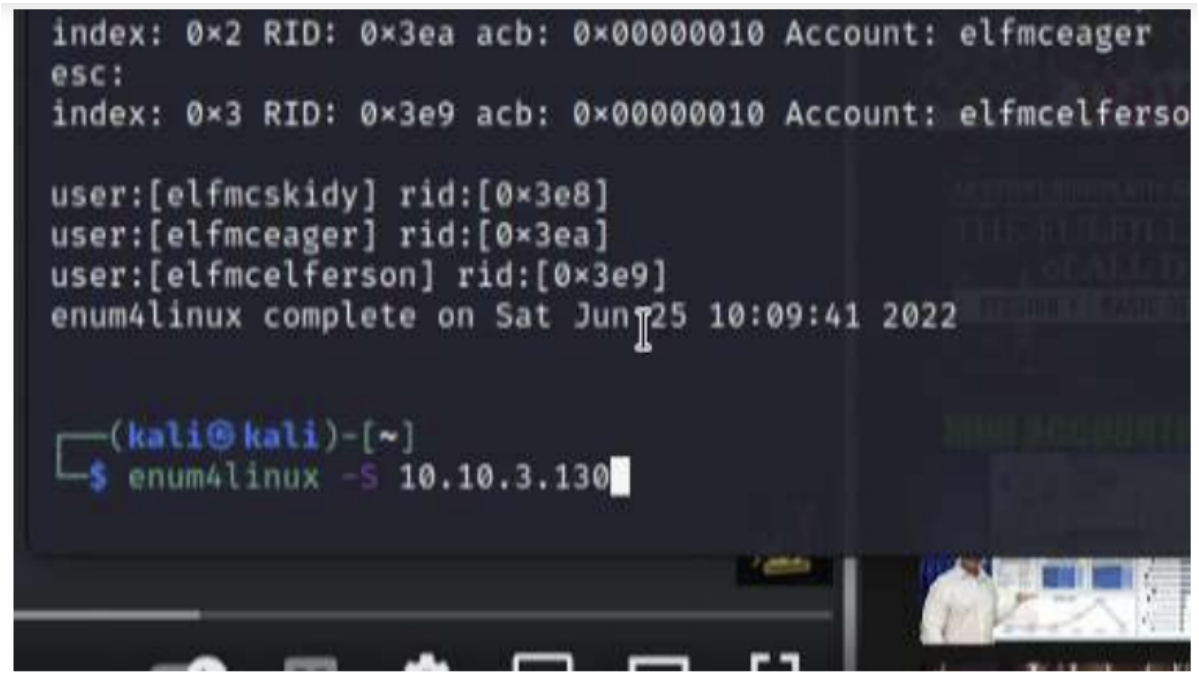
**Solution:**

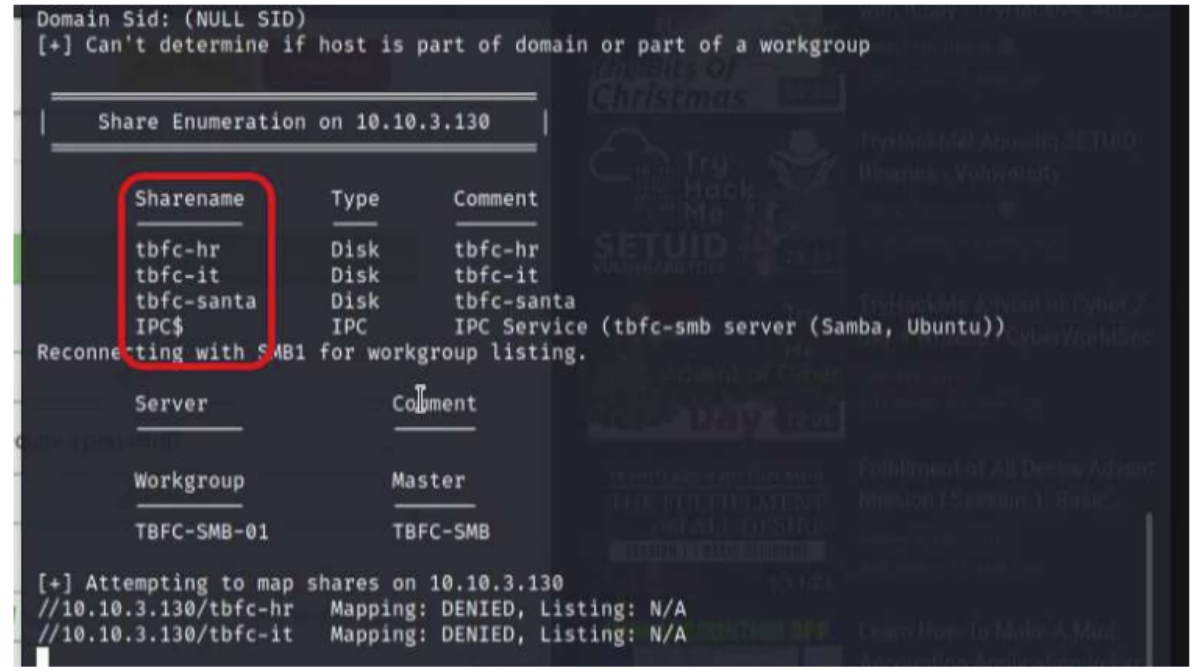
Q1:

After connecting to the machine ip, open the terminal and type enum4linux -U 10.10.3.130.



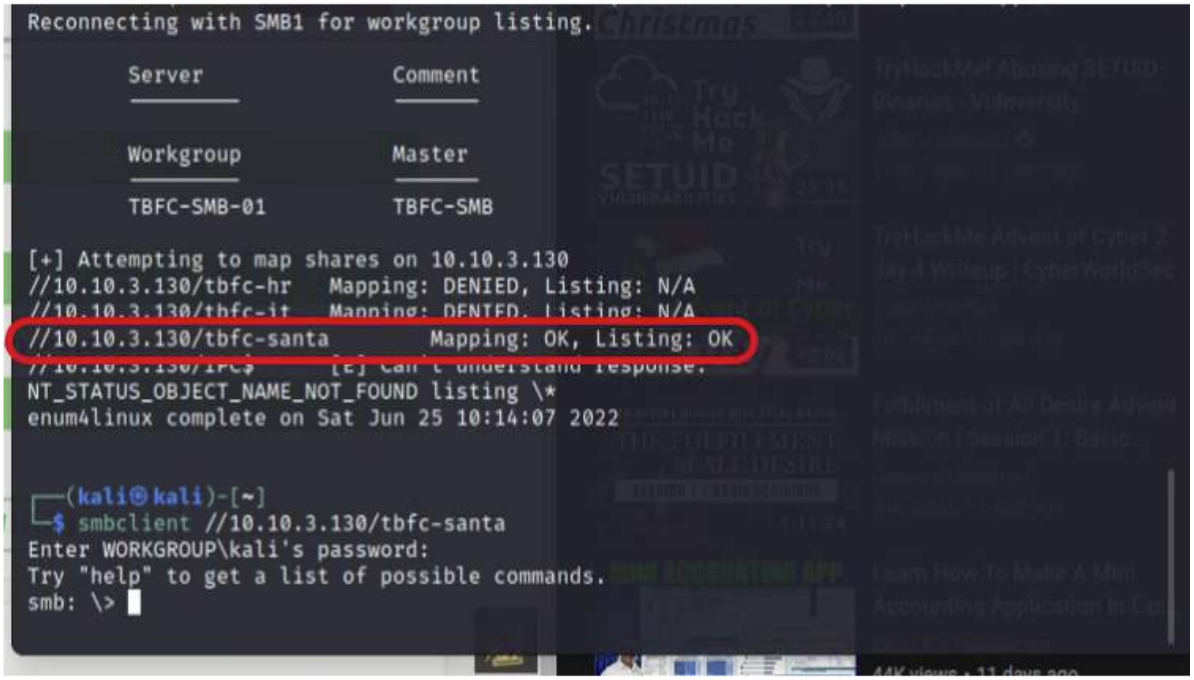

Q2:
Type the command enum4linux -S 10.10.3.130

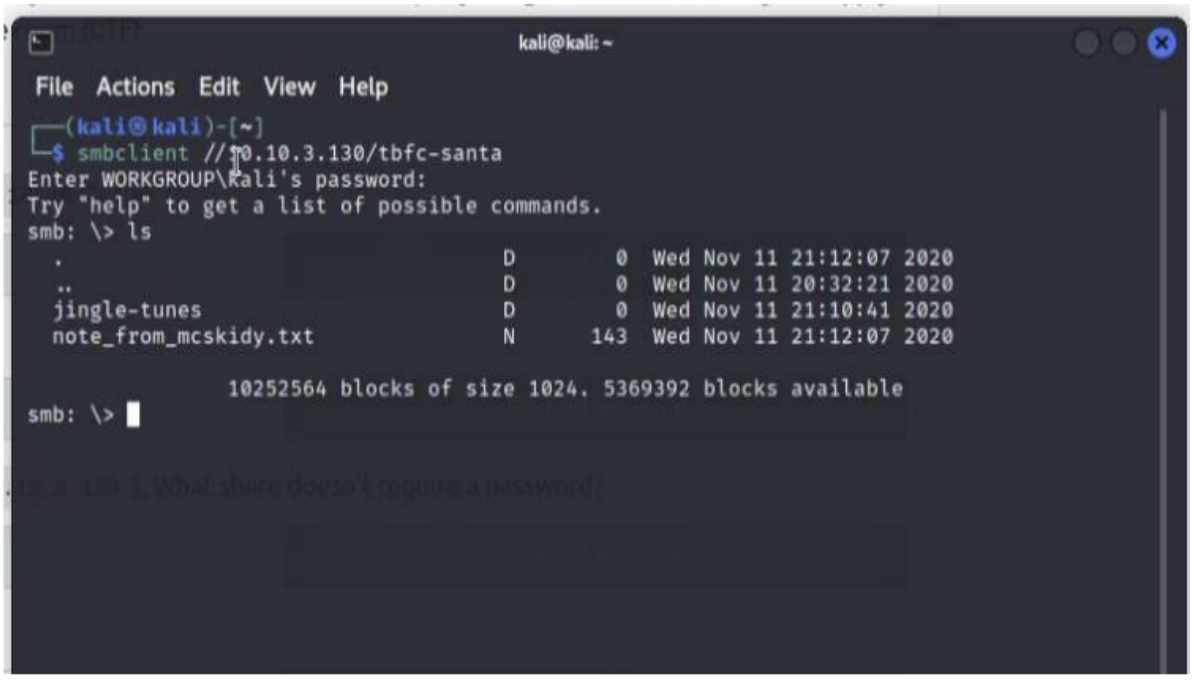


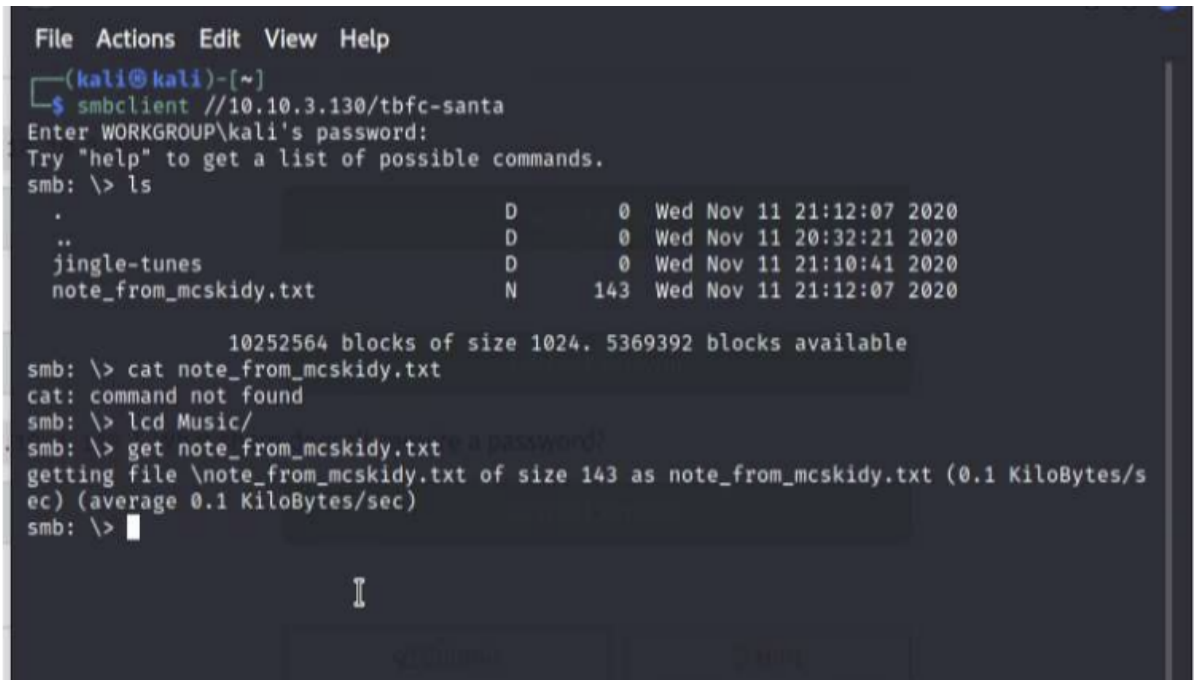

Q3:

Type smbclient //10.10.3.130/tbfc-santa




Q4:
After logging in using tbfc-santa, change the local working directory to Music/ and type get note_from_mcskidy.txt.




Open a new terminal, change the directory to Music/ and view the note_from_mcskidy.txt.


**Thought Process/Methodology:**

After starting the machine on TryHackMe, we can directly search for enum4linux or type enum4linux in the terminal. In enum4linux, -U is used to get a userlist which we can type the following command: enum4linux -U 10.10.3.130 to get all the user list. Other than that, -S in enum4linux is used to get a sharelist which we can type this

command: enum4linux -S 10.10.3.130 to know the shares. After that, it shows 4 shares and one of them has “Mapping: OK, Listing: OK” which is //10.10.3.130/tbfc-santa. We can log in using the login command: smbclient //10.10.3.130/tbfc-santa and the password is no password. When we are logged in, we can type ls for listing all the files contained inside and files consist of jingle-tunes and note_from_mcskidy.txt. Then, we need to look inside the .txt file where we can type lcd Music/ to change the local working directory and get note_from_mcskidy.txt to move the file to Music/. Lastly, we open a new terminal and change the directory using cd Music/ to view the .txt file using command cat note_from_mcskidy.txt.