PSP0201
Week 3
Writeup

Group Name : Fsociety
Members :

ID	Name	Role
1211102908	Wan Muhammad Ilhan Bin Wan Zil Azhar	Leader
1211101583	Luqman Hakim Bin Noorazmi	Member
1211203101	Jazlan Zuhair Bin Mohamed Zafrualam	Member
1211102054	Mithesh Kumar	Member

Day 6

(Be careful with what you wish on a Christmas night)

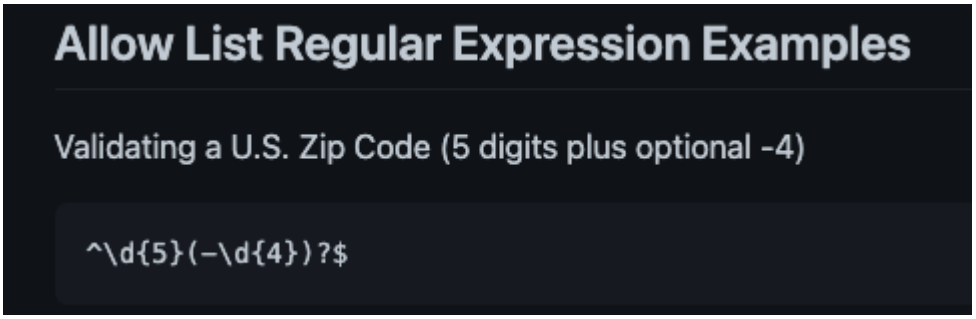
Tools Used: Kali, FireFox, ZAP

Question 1:

Based on the OWASP Cheat Sheet (under *Email Address Validation*), the Semantic Validation enforces correctness of their values in the specific business context while Syntactic Validation enforces correct syntax of structured fields.

Question 2:

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



(via the OWASP Cheat Sheet)

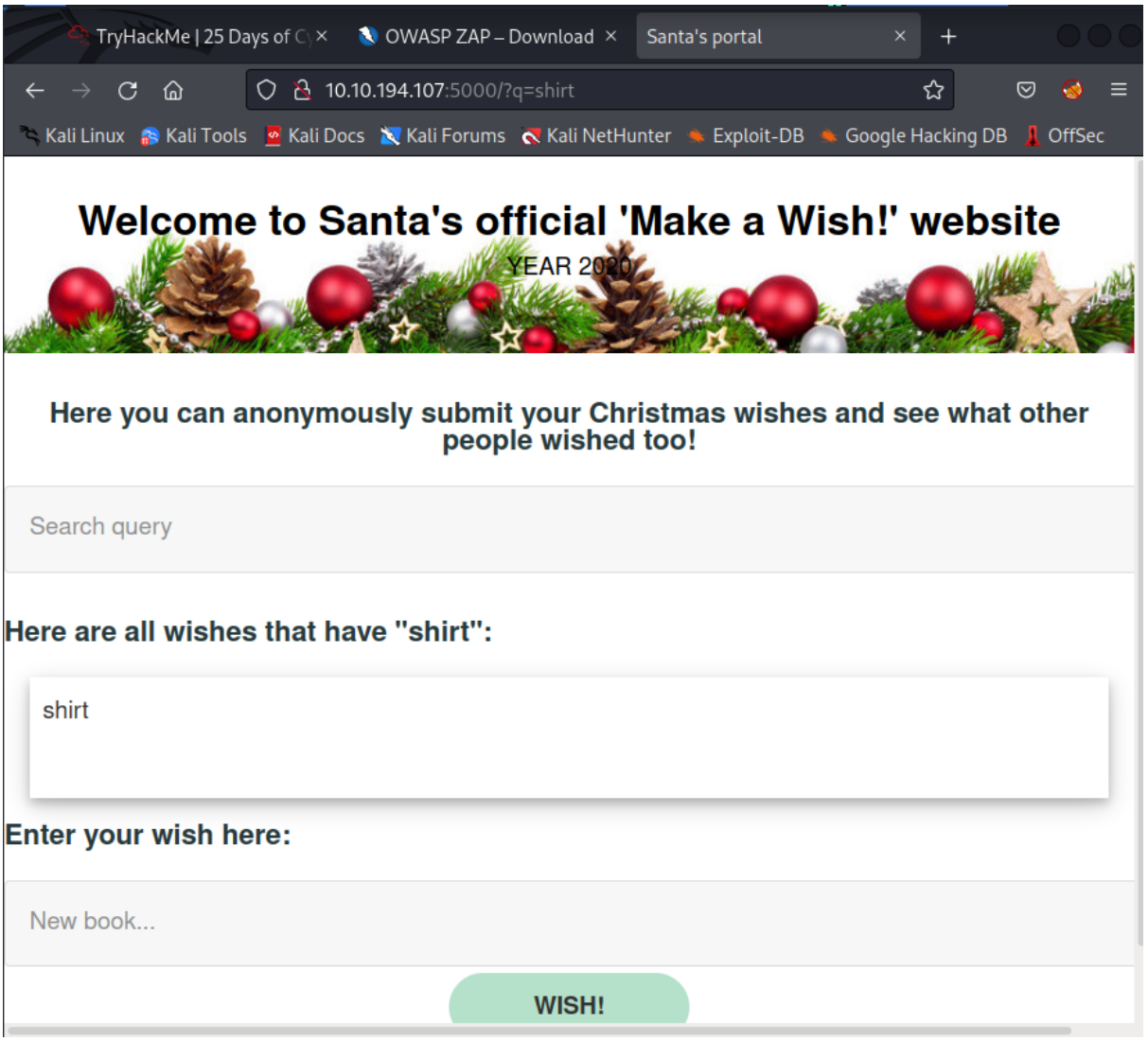
Question 3:

The vulnerability type used is the stored cross-site scripting because the form submitted is stored directly on the website.

Question 4:

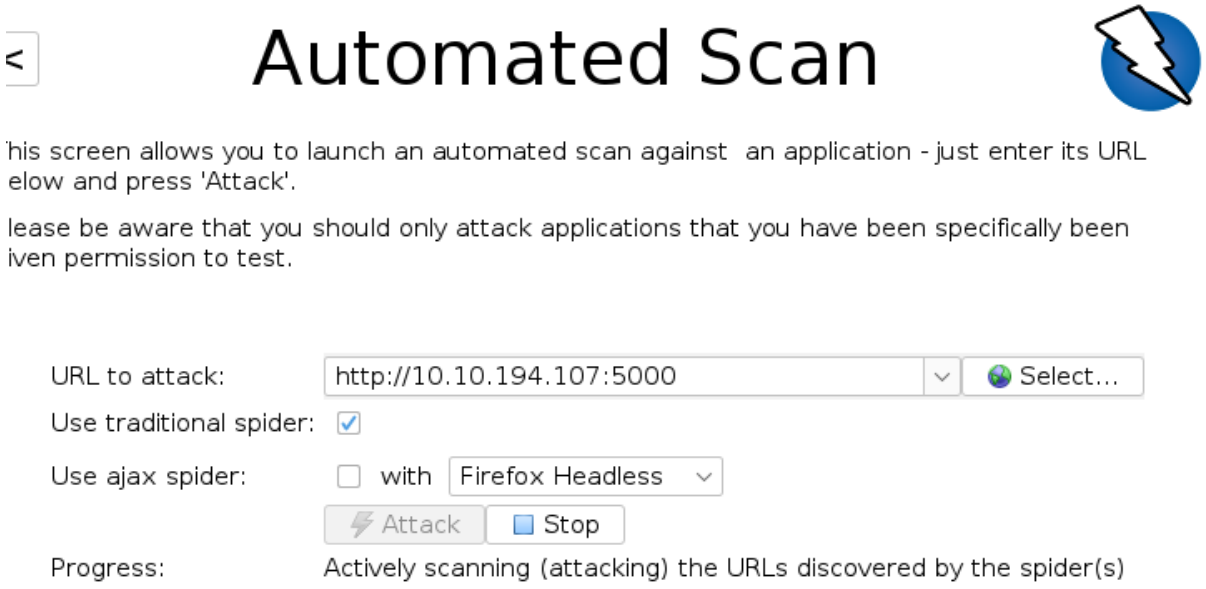
The query string is *q* because after using the search function, the keyword is used as the value for the GET parameter.

Example below: (typed in *shirt*, and it shows *q=shirt*)

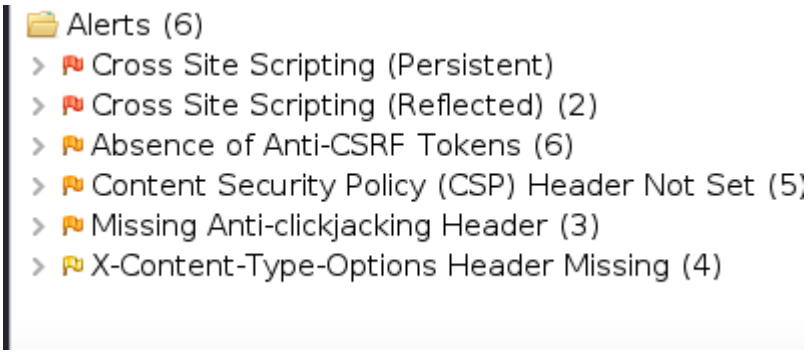


Question 5:

After launching the OWASP ZAP Application, in the URL to attack section, type in the URL:Port and then press attack.



Now, under the alerts tab, there are two XSS alerts that can be seen.



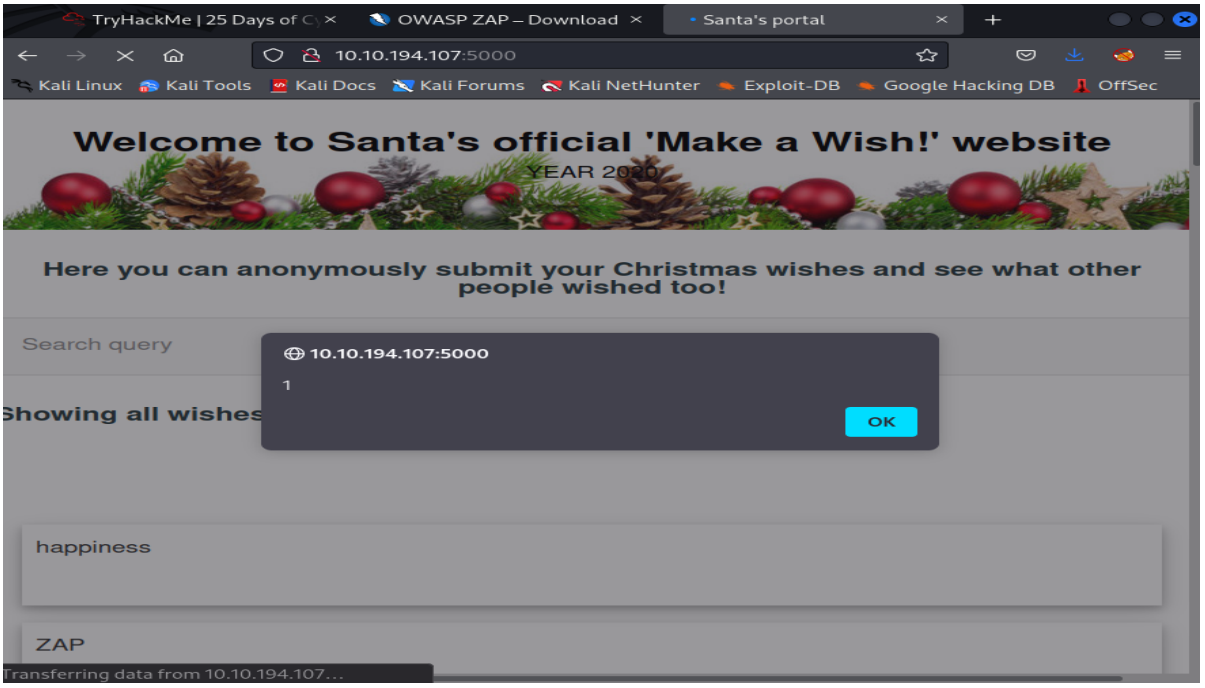
Question 6:

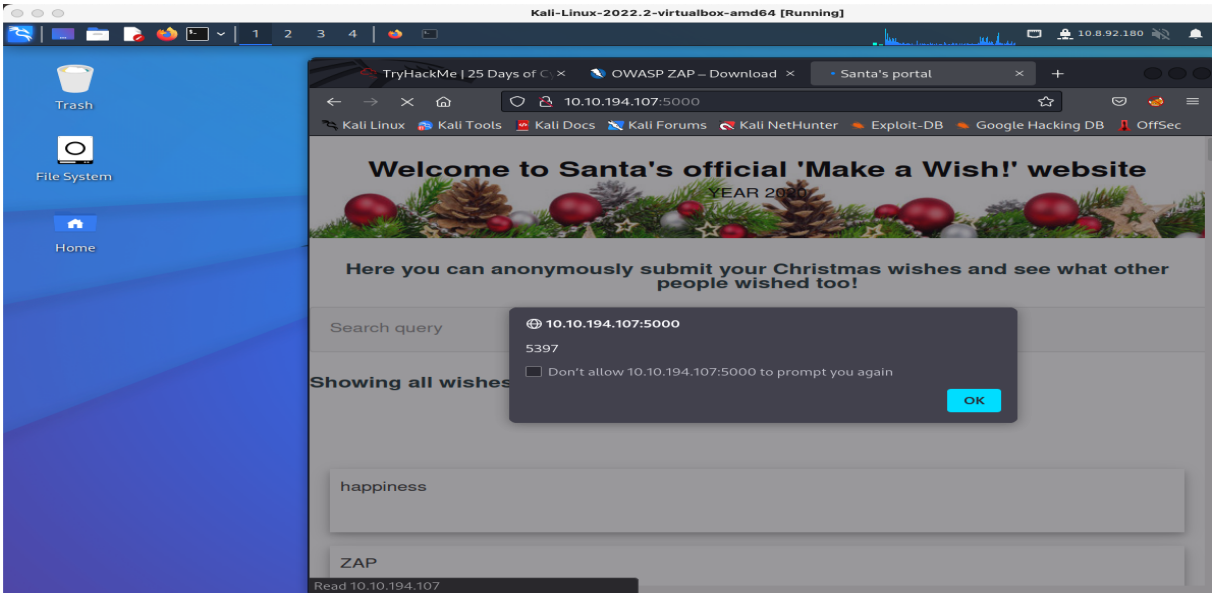
To show “PSP0201” as the alert, the javascript code will be:

<script>alert(‘PSP0201’)</script>

Question 7:

After looking through the XSS alerts and typing in the url, these alert boxes were shown.





Thought Process/Methodology : By referring to the OWASP Cheat Sheet, we were able to validate the US Zip Code and the validation type. After figuring out the vulnerability type used on the website, we used OWASP Zap to run an automated scan on the site. By confirming that the site is now popping up alert boxes, we can customize the text shown by using a script.

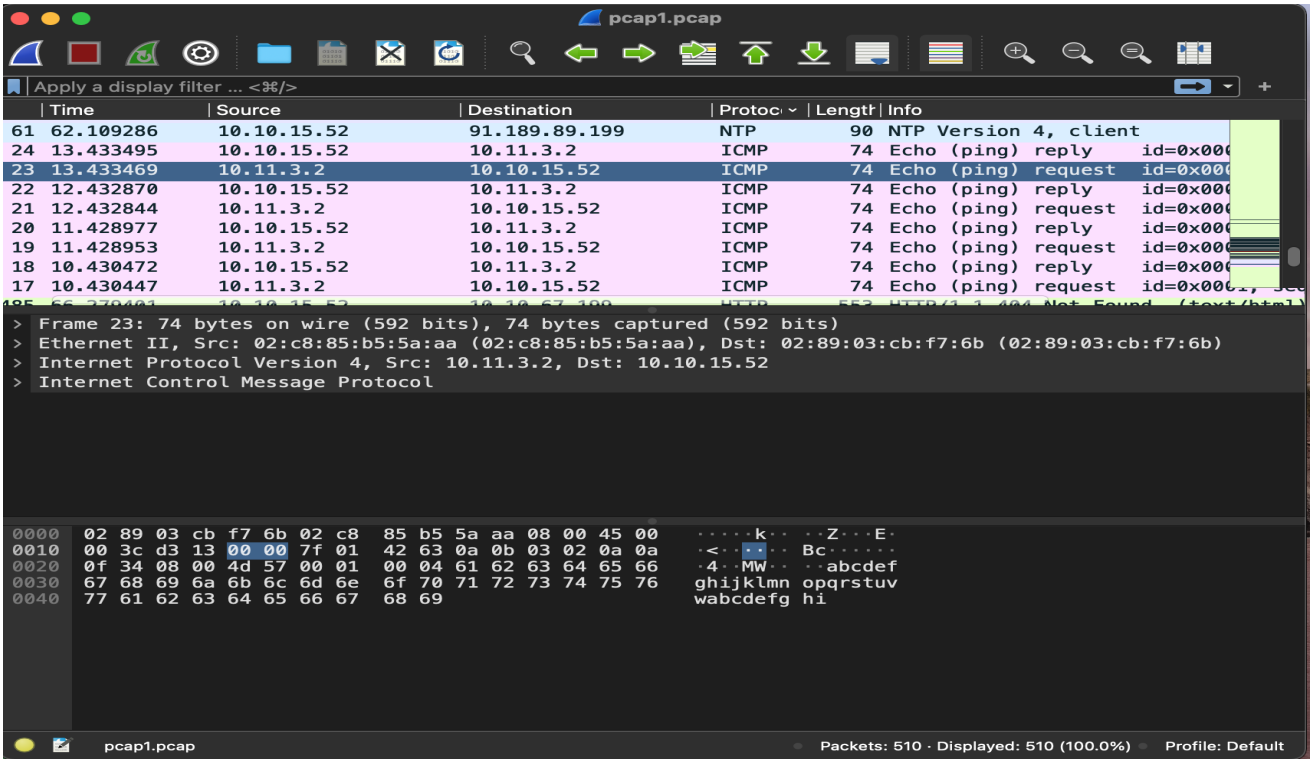
Day 7

(The Grinch Really Did Steal Christmas)

Tools used : Wireshark, Notepad, Google Chrome

Question 1 :

Open pcap1.pcap on WireShark and filter through the protocol to find ICMP data with a ping reply info. The IP address that initiates an ICMP/ping is 10.11.3.2



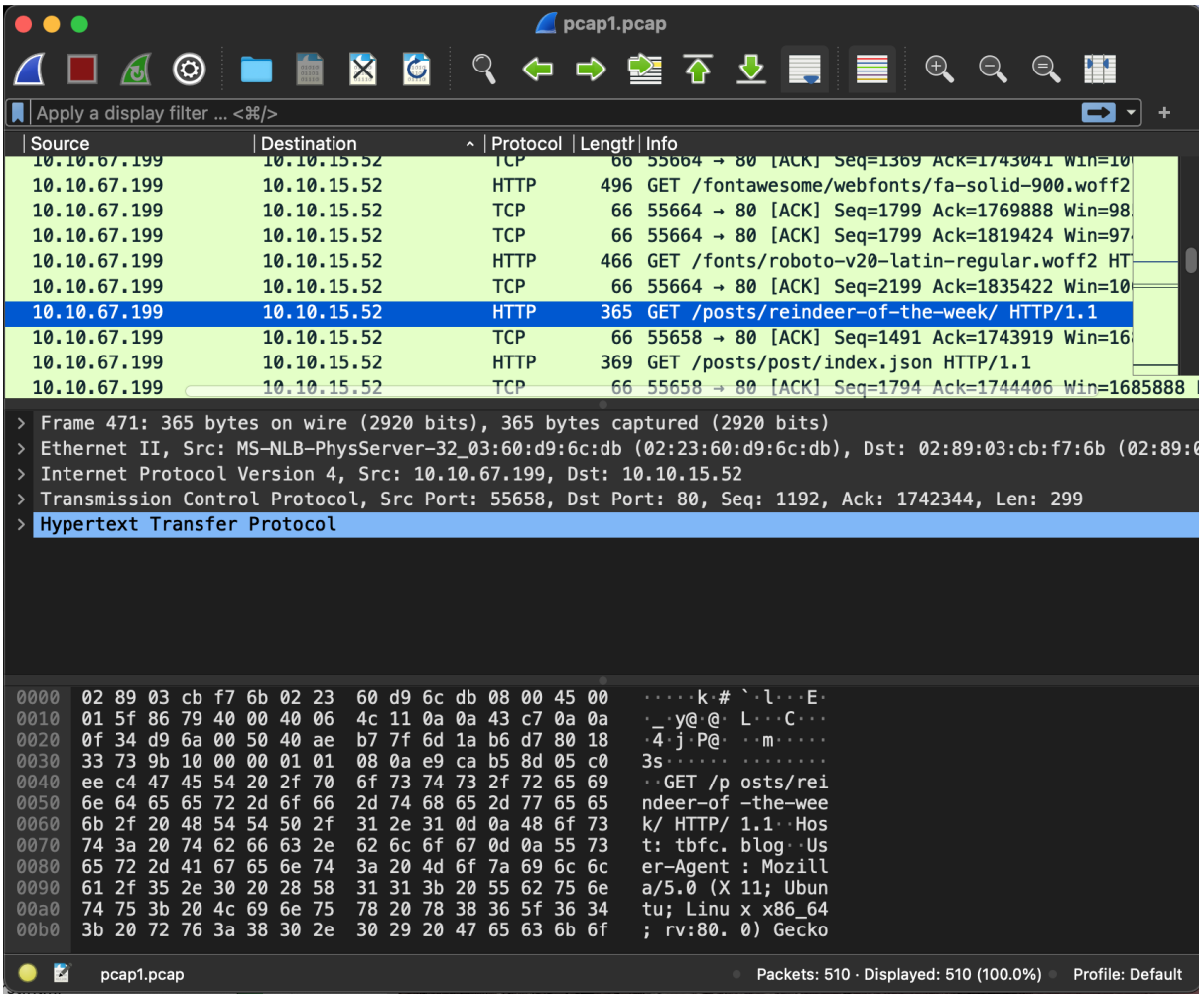
Question 2 :

To get the HTTP GET request, we need to use:

HTTP.REQUEST.METHOD == GET

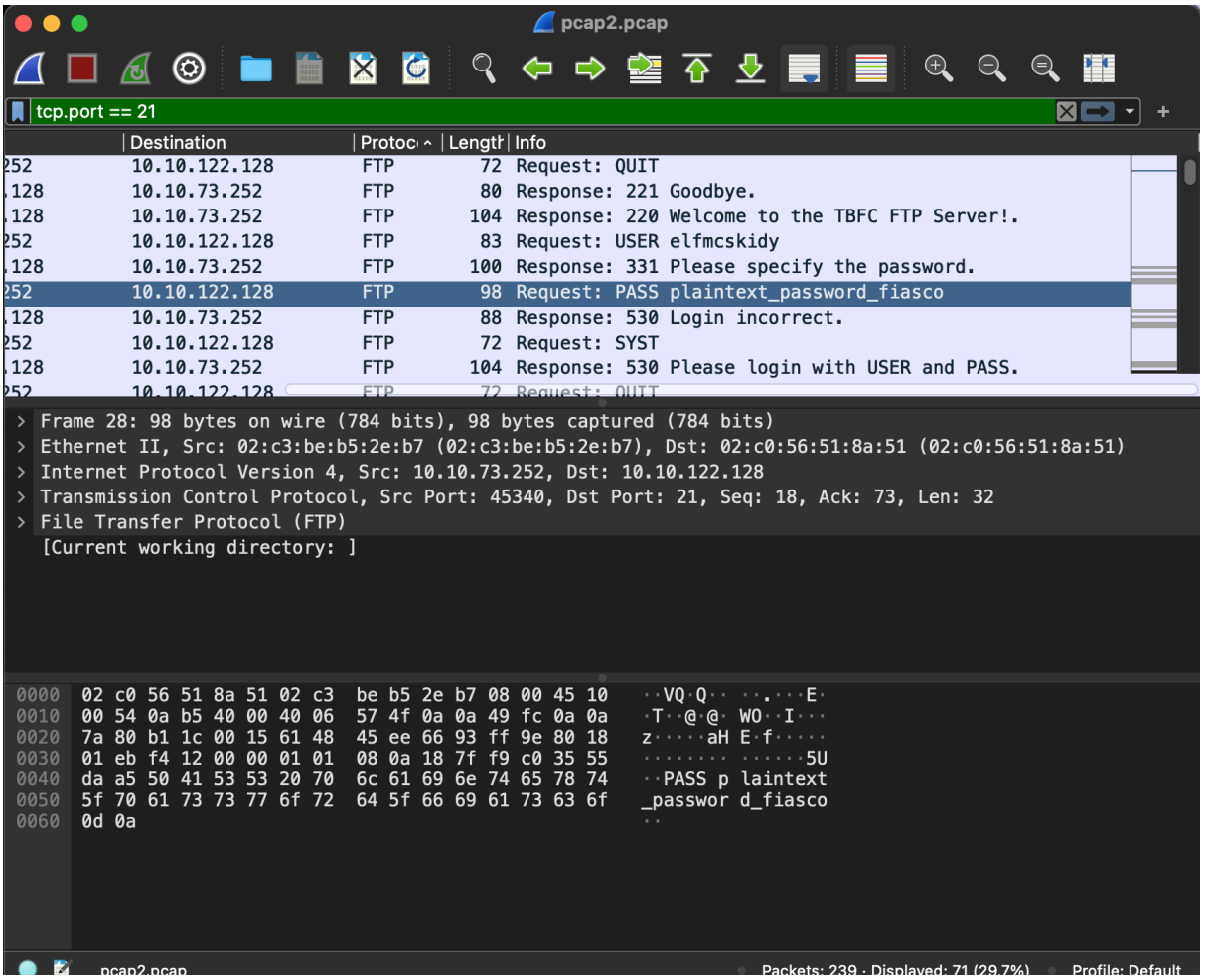
Question 3:

After applying the filter from question 2 on wireshark, the name of the article that the IP address "10.10.67.199" visited is *reindeer-of-the-week*



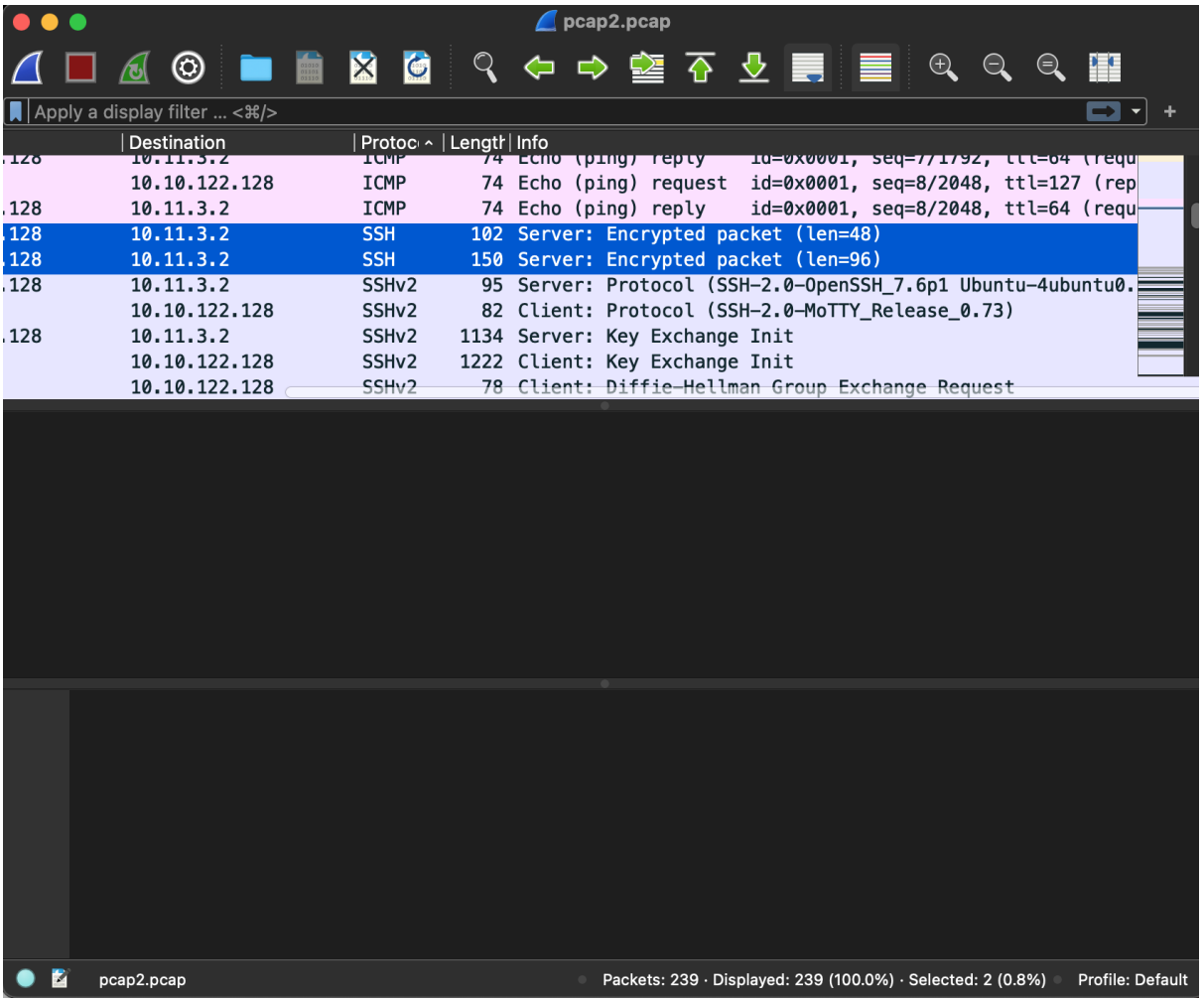
Question 4:

Moving on to pcap2.pcap, in the captured FTP traffic, the password leaked was *plaintext_password_fiasco*



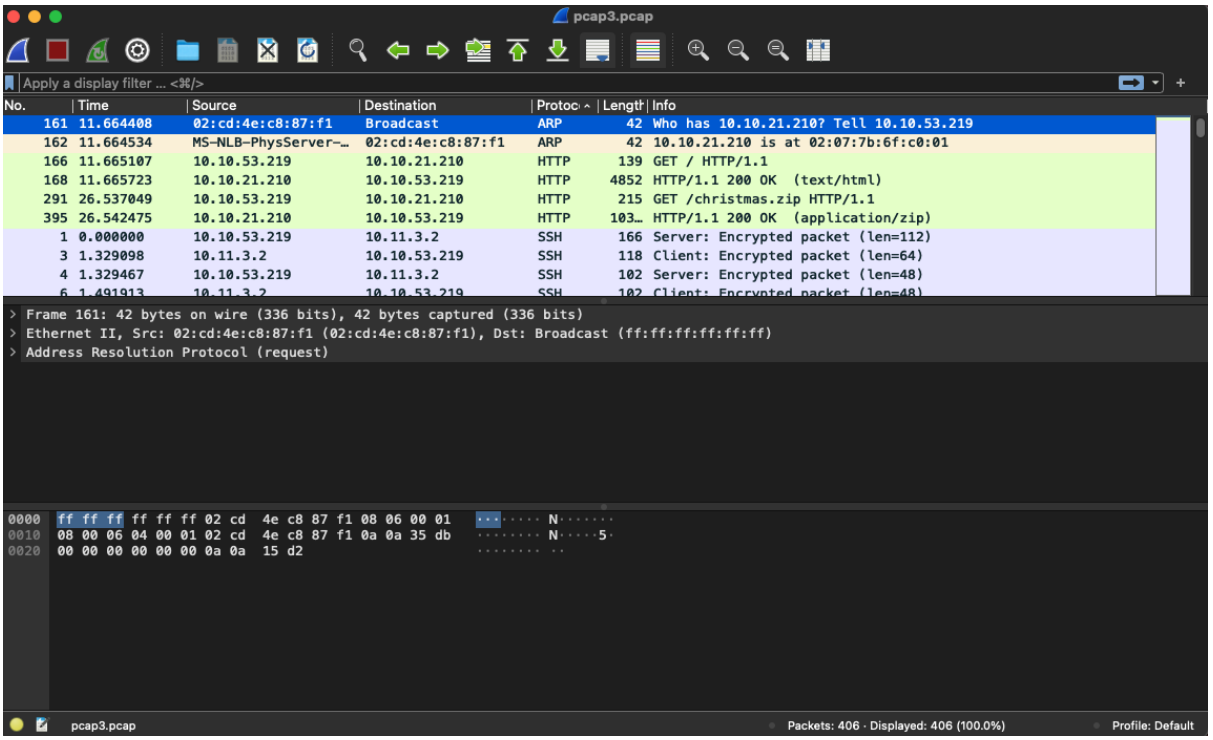
Question 5:

The name of the encrypted protocol is SSH



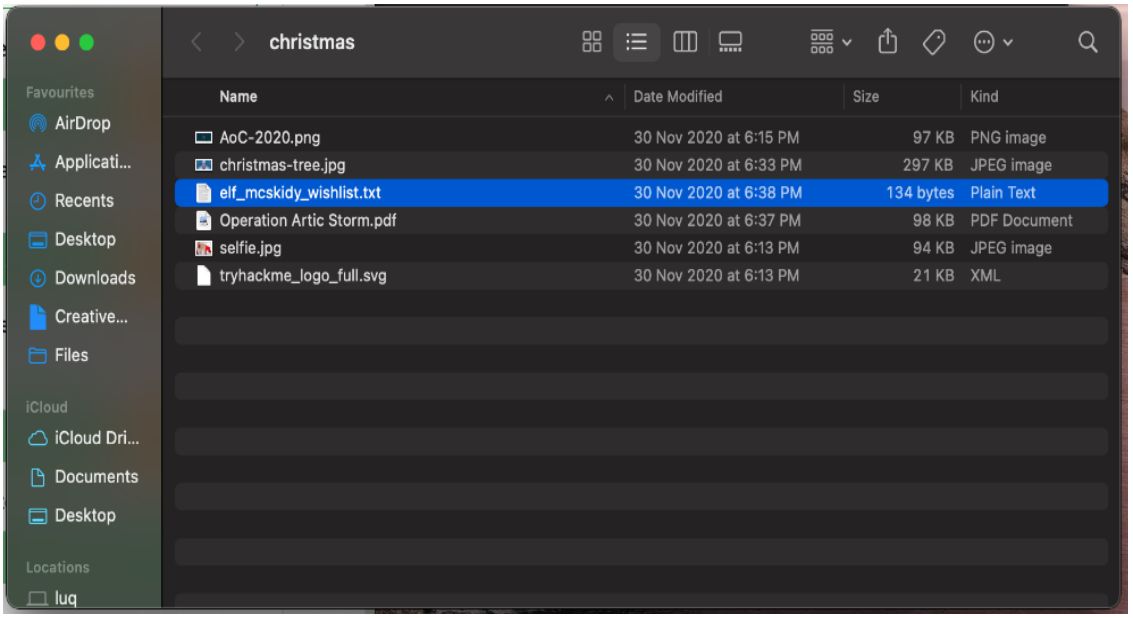
Question 6:

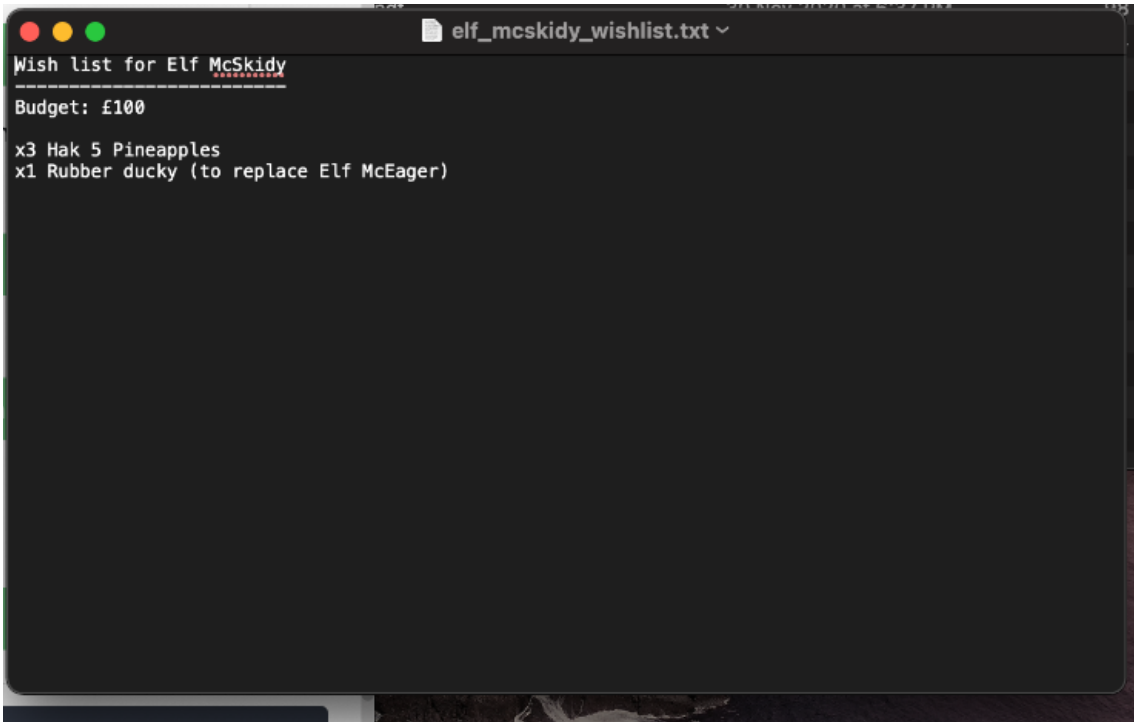
The ARP communication shows that 10.10.21.210 is at *02:07:7b:6f:c0:01*



Question 7:

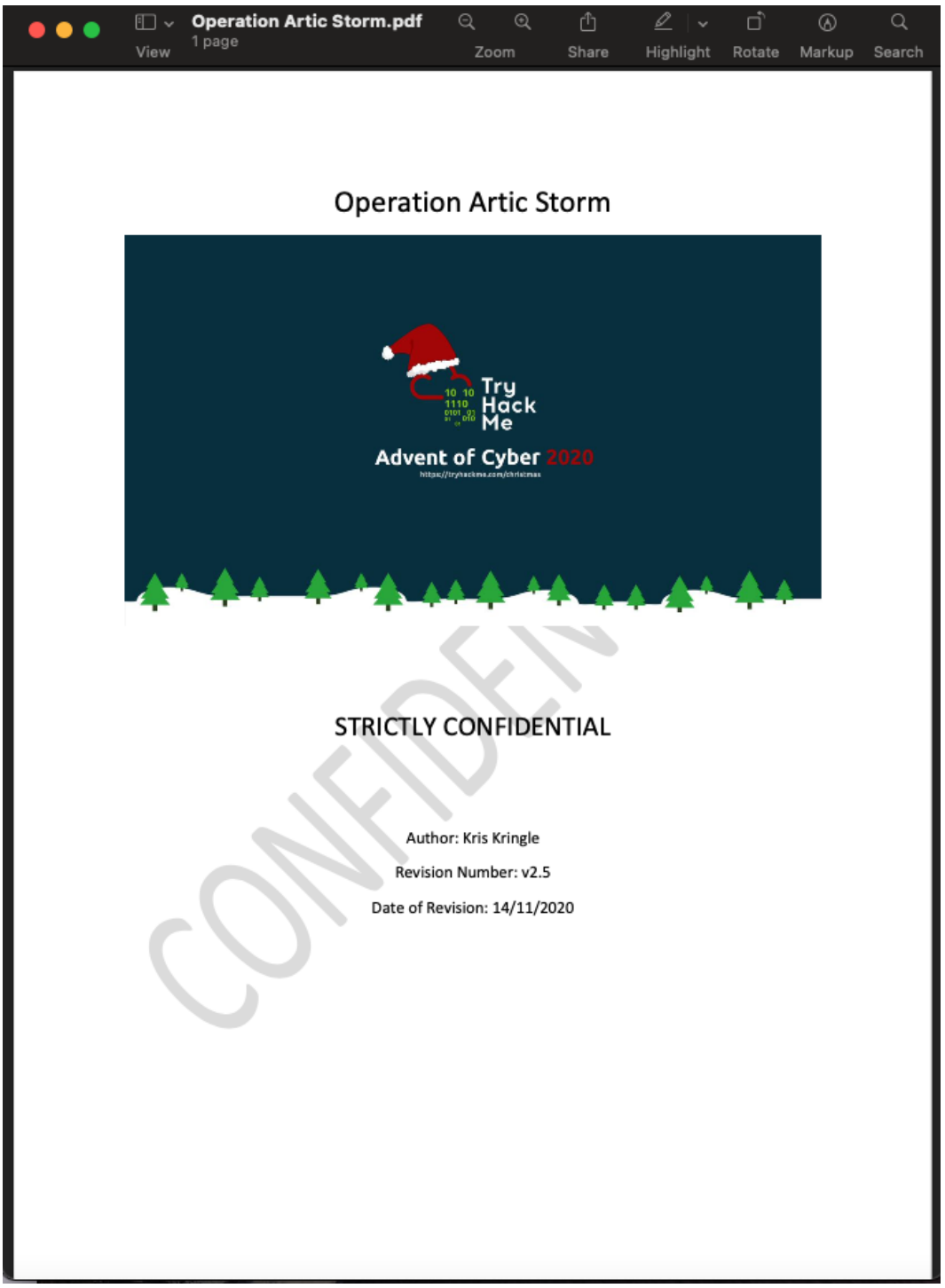
On pcap3.pcap, export the data by going to File > Export Objects > SMB. Now, search for the christmas file in the local device. Open the *elf_mcskidy_wishlist.txt* file. It seems that rubber ducky will be replacing Elf McEager.





Question 8:

From the same file that the *elf_mcskidy_wishlist.txt* located, open the Operation Artic Storm. From there we can see the author is Kris Kringle



Thought Process/Methodology : After downloading WireShark, we started by going through the pcap1 file and finding information based on the IP, Protocol and Info. To find the password in pcap2 we went through the FTP protocol files and found the information on the user's password. Then, we exported the files in pcap3 which contains a file and a txt file. Upon opening the txt file, we can find the wishlist for Elf McSkidy and the pdf for Operation Artic Storm.

Day 8

(What's Under The Christmas Tree)

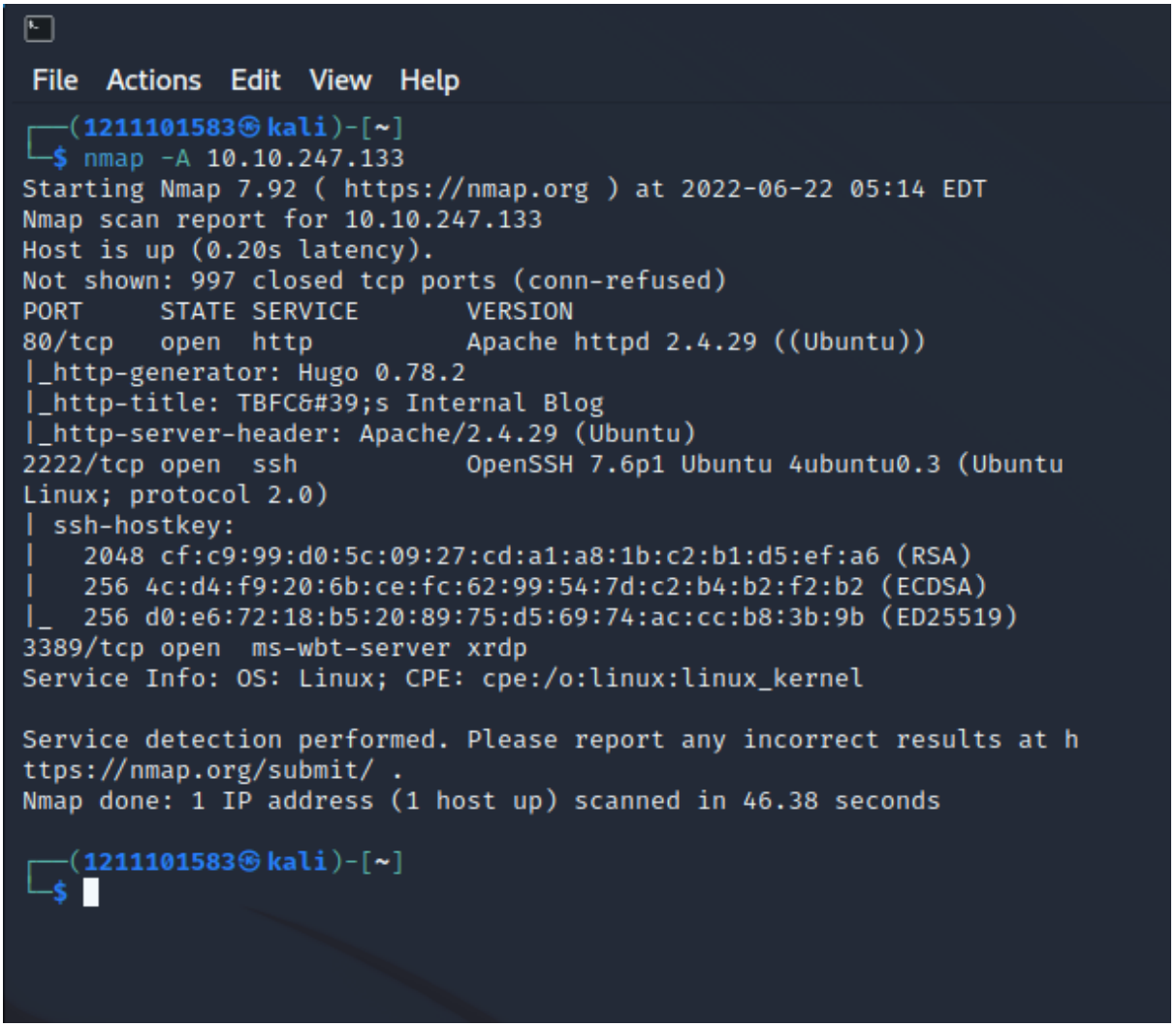
Tools used : FireFox, Terminal, Kali

Question 1:

A quick Google search indicates that Snort was created way back in 1998

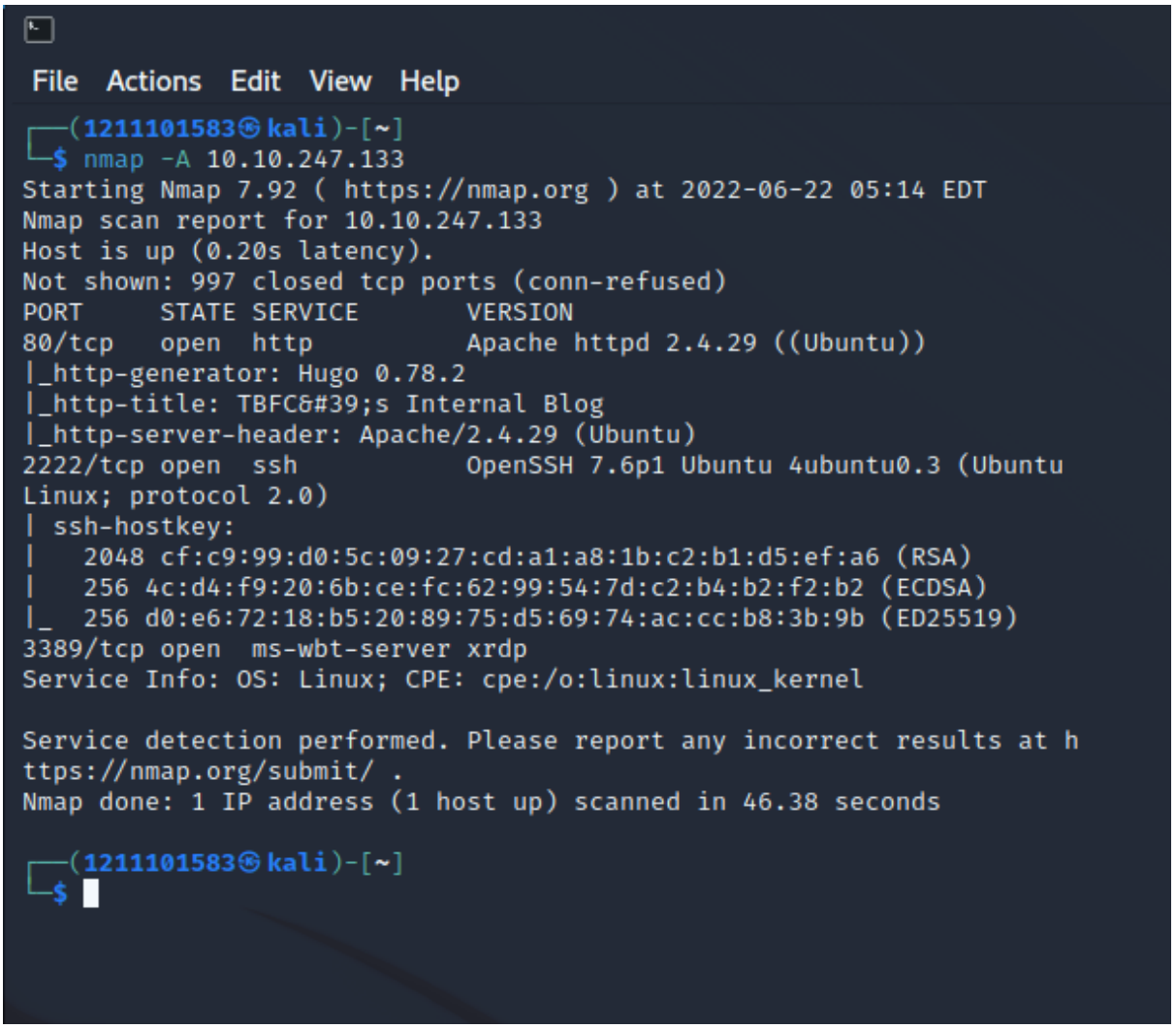
Question 2:

Using *nmap -A <MACHINE IP ADDRESS>* on terminal, the three ports number of the three services running are 80, 2222, 3389



Question 3:

By using the nmap, it was later discovered that the Linux Distribution that most likely is running is Ubuntu.



Question 4:

Run *nmap -sV <MACHINE IP ADDRESS>* and the Apache version can be seen there.

```
┌──(1211101583㉿kali)-[~]
└─$ nmap -sV 10.10.247.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 05:24 EDT
Nmap scan report for 10.10.247.133
Host is up (0.20s latency).
Not shown: 997 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
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 35.20 seconds
```

Question 5:

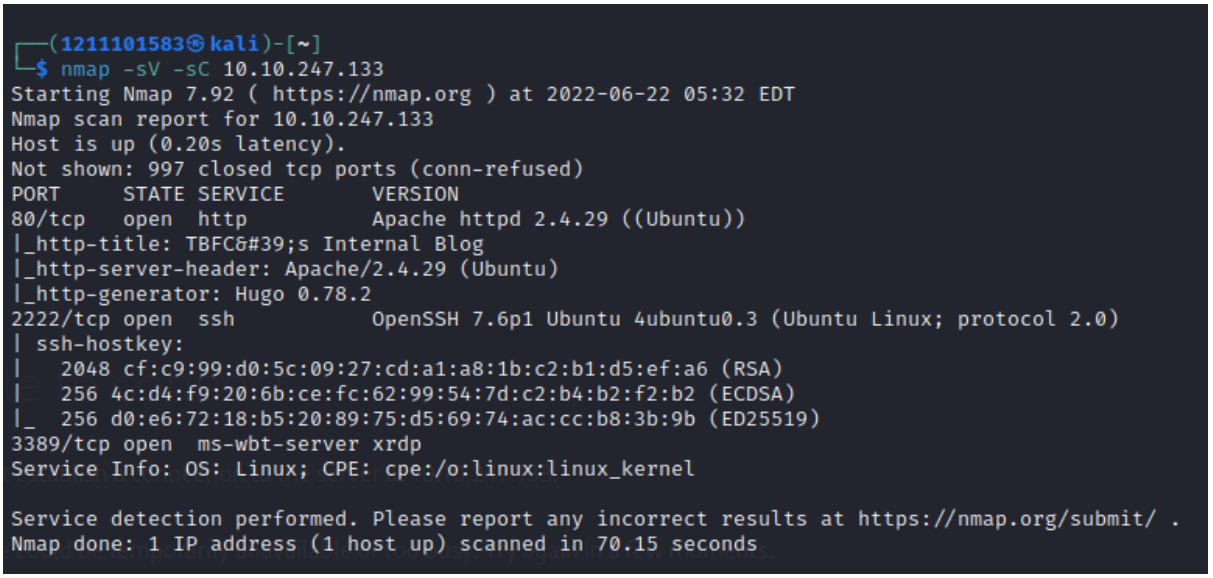
Again, from *nmap -sV <MACHINE IP ADDRESS>,* port 2222 is running SSH

```
┌──(1211101583㉿kali)-[~]
└─$ nmap -sV 10.10.247.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 05:24 EDT
Nmap scan report for 10.10.247.133
Host is up (0.20s latency).
Not shown: 997 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
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 35.20 seconds
```

Question 6:

After running *nmap -sV -sC <MACHINE IP ADDRESS>*, the HTTP-TITLE of the website is Internal Blog, so the website is being used as a blog.



Thought Process/Methodology : Using terminal, we navigated through the commands and helplines of nmap, then using the command nmap -A <IP ADDRESS> we can figure out the running services port on the ip and the version of Apache including the used linux distribution which is Ubuntu. We then used the command nmap -sV -sC <MACHINE IP ADDRESS> to figure out the title of the website and what the website might be used for. The website is being used as a blog.

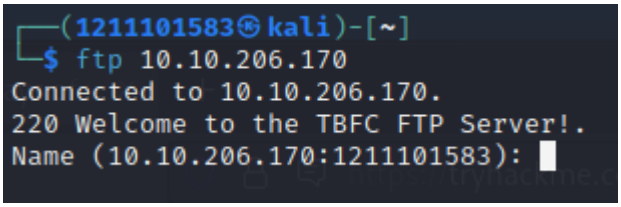
Day 9

(Anyone can be Santa!)

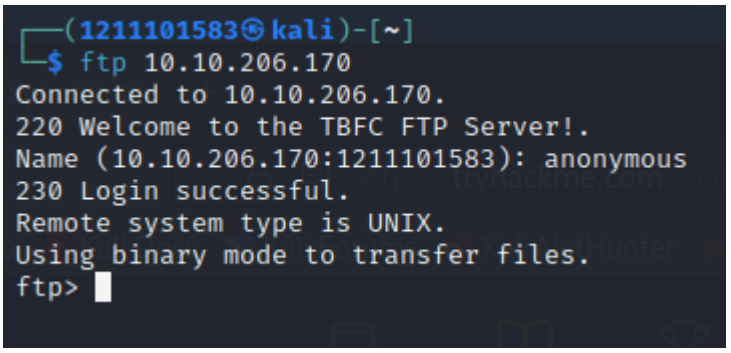
Tools used : Kali, Terminal, FireFox, AttackBox

Question 1:

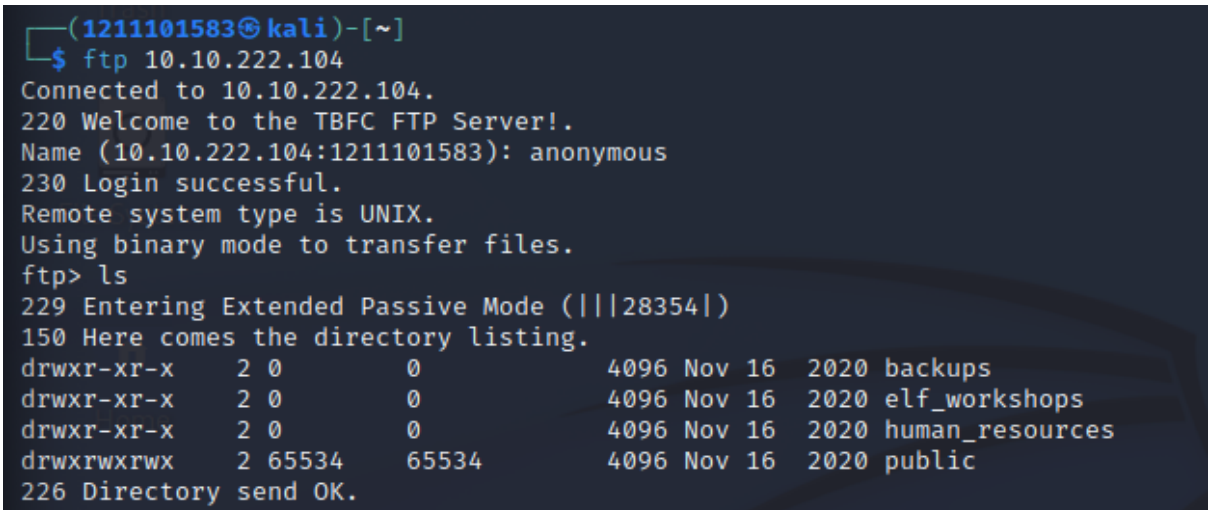
Start by opening the terminal and type in *ftp <MACHINE IP ADDRESS>*. Press enter.



When prompted for a name, type in *anonymous*. Press enter.



Type in *ls* to look for the directories.



Question 2:

The only directory that is accessible by *anonymous* is *public*. It was discovered by running *cd public*.

```
ftp> cd public
250 Directory successfully changed.
```

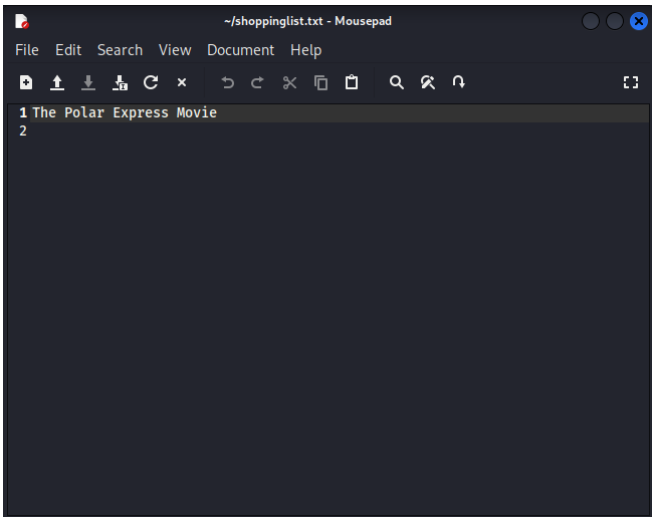
Question 3:

In the public directory (run *cd public*), we can see that the script that gets executed within this directory is backup.sh.

```
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||25766|)
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>
```

Question 4:

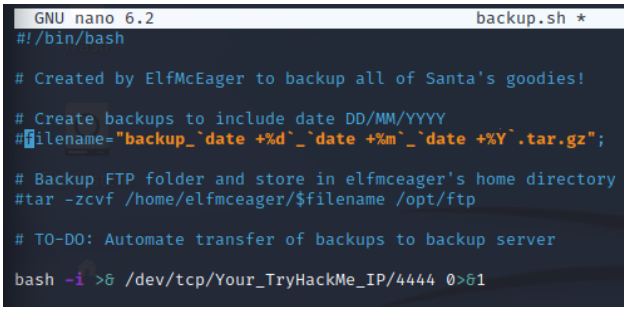
To know what movie did Santa have on his Christmas shopping list, we first need to run *get shoppinglist.txt* to save the file on the local device. Then, open the file and the name of the movie is stated there in the file (The Polar Express).



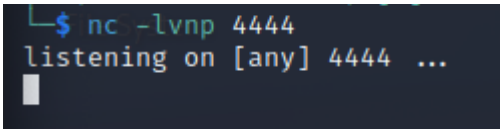
Question 5:

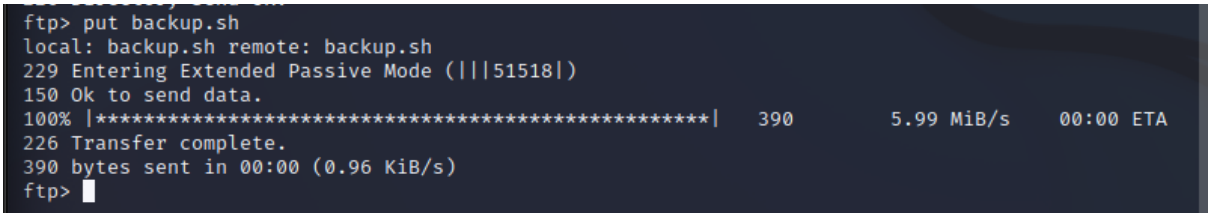
Now, let's upload the reverse shell to the backup.sh file.

First, use *get backup.sh* and run *nano backup.sh.* Then, paste the bash command into the file. Change <Your_TryHackMe_IP> with the device's IP Address.

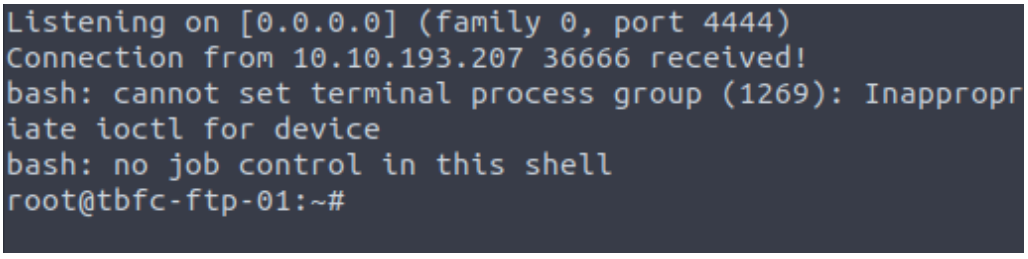


Save and use *put backup.sh* to replace the current backup.sh file with the one with the reverse shell. But before executing *put backup.sh*, let's set up a netcat listener.

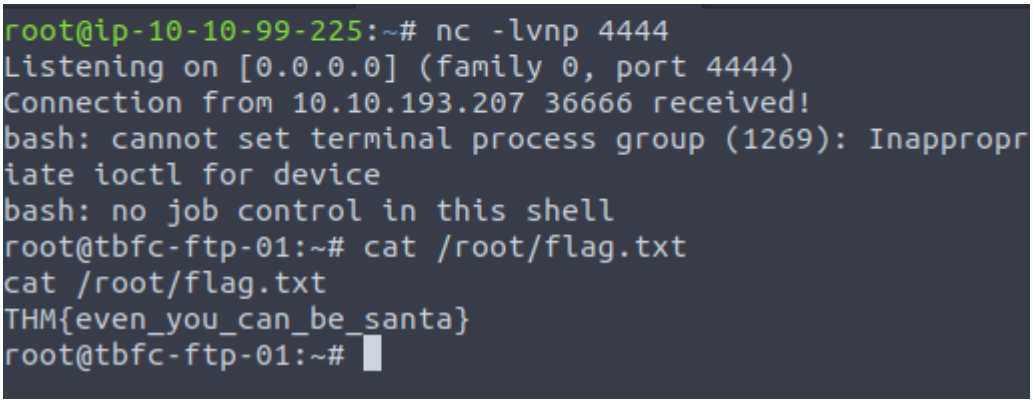




After the file has been uploaded, the netcat will show something like this:
(We have to change from Kali to Attackbox for some reasons but it doesn't change anything)



With that all done, run cat /root/flag.txt to see the flag.



Thought Process/Methodology : We begin by using terminal and using the command ftp <MACHINE ADDRESS> to connect to the TBFC FTP Server. We used the name ‘anonymous’ to access public servers. By using the command cd public, two files are revealed (backup.sh & shoppinglist.txt). We open shopppinglist.txt to see if Santa’s movie is stated in the file. Next, by using nano backup.sh, we’re able to edit the file and input a bash command to upload a reverse shell. We then tried to run a netcat listener and execute the reverse shell. We can then use the cat /root/flag.txt command to get the flag.

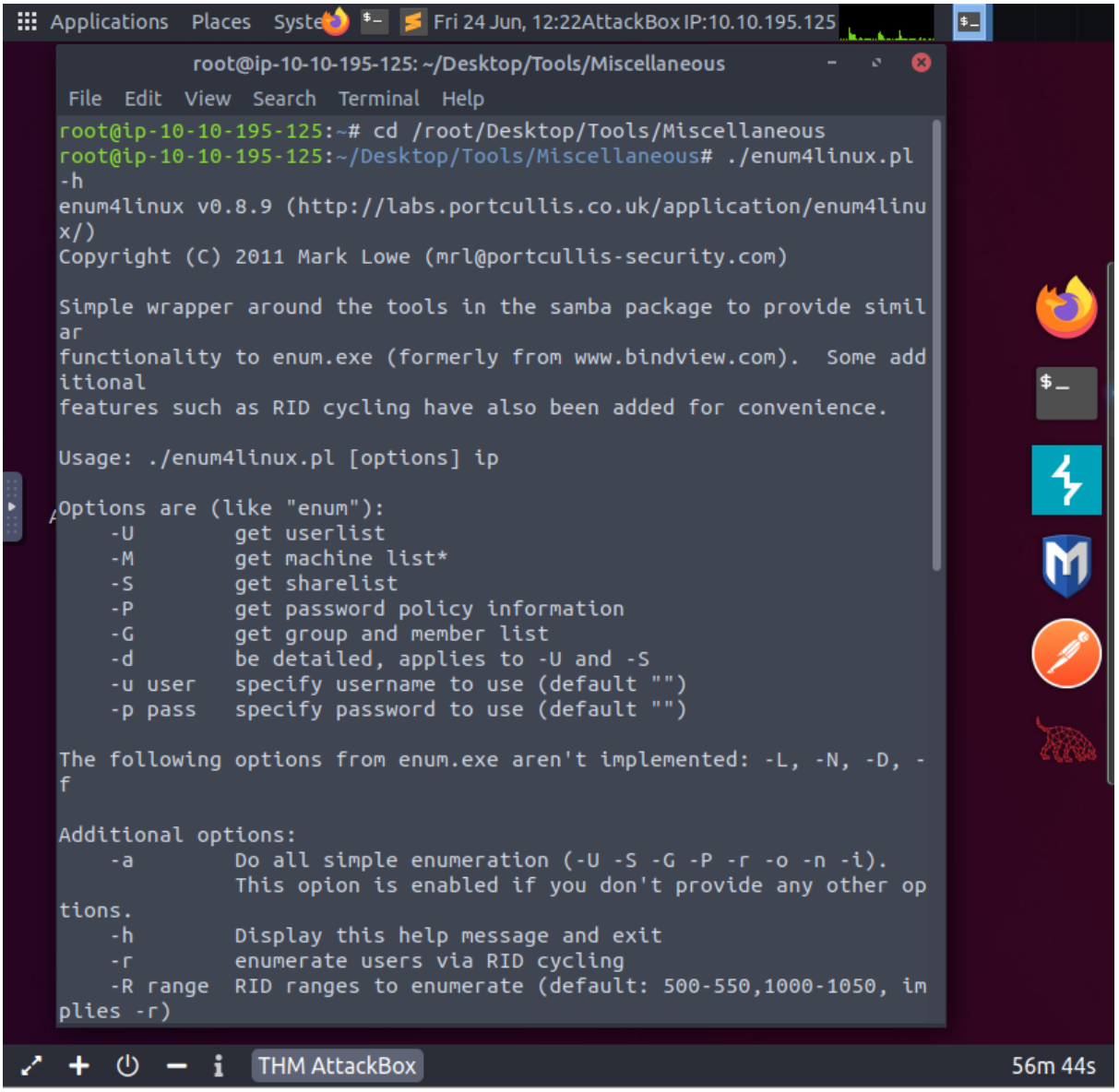
Day 10

(Don't be sElfish!)

Tools used : FireFox, Terminal, Attackbox

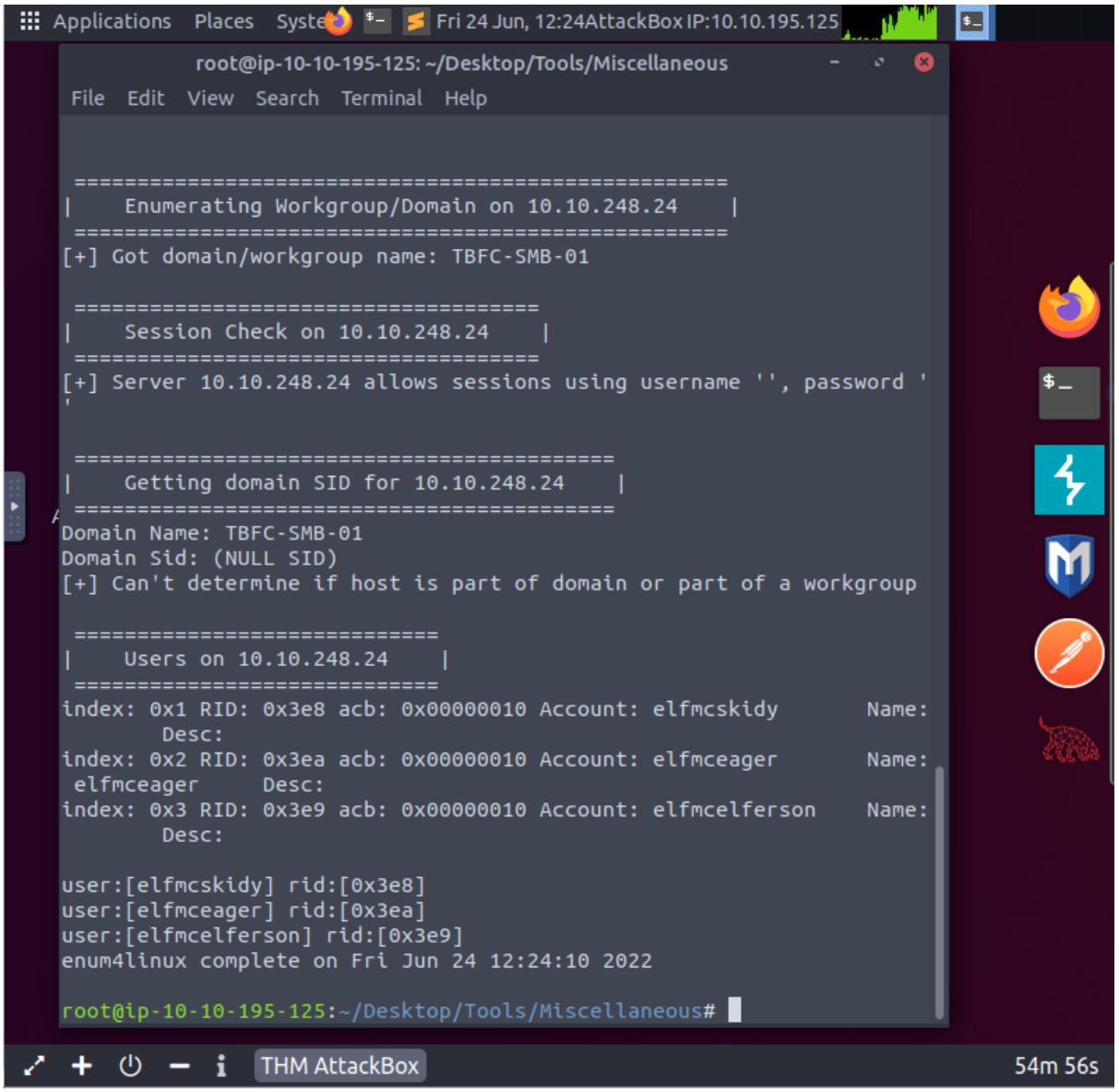
Question 1:

In the terminal, run *cd /root/Desktop/Tools/Miscellaneous*. Then, run *./enum4linux.pl -h* to see the help message.



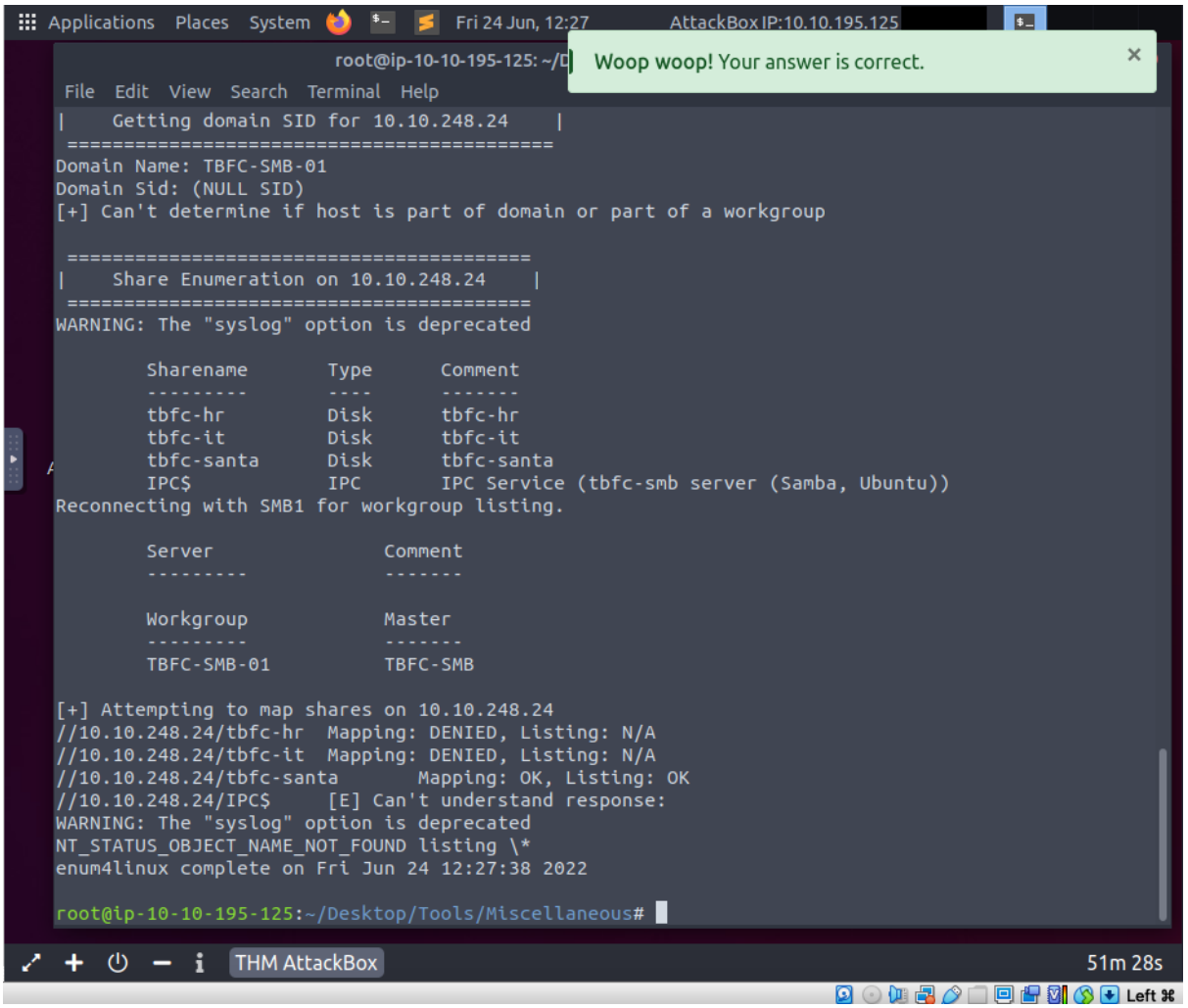
Question 2:

To see all users on the Samba server, run ./enum4linux.ph -U <MACHINE IP ADDRESS>. There are 3 accounts on the samba server.



Question 3:

To see the ‘shares’ on the Samba server, run ./enum4linux.ph -S <MACHINE IP ADDRESS>. There are 4 shares on the server.



Question 4:

To see which share does not require a password, we have to run *smbclient //REPLACE_INSTANCE_IP_ADDRESS/**sharename*** on each share (replace ***sharename*** with the name of the share) and then pressing enter when prompted for password. If no error is shown, that means the share does not require a password to be accessed.

The share that does not require a password is *tbfc-santa*.

```
root@ip-10-10-195-125:~/Desktop/Tools/Miscellaneous# smbclient //10.10.248.24/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \>
```

Question 5:

After successfully logging in to *tbfc-santa*, run *ls* to see all the directories. McSkidy left the *jingle-tunes* directory for santa.

```
root@ip-10-10-195-125:~/Desktop/Tools/Miscellaneous# smbclient //10.10.248.24/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Nov 12 02:12:07 2020
  ..                                  D        0  Thu Nov 12 01:32:21 2020
  jingle-tunes                        D        0  Thu Nov 12 02:10:41 2020
  note_from_mcskidy.txt               N      143  Thu Nov 12 02:12:07 2020

                10252564 blocks of size 1024. 5369396 blocks available
```

Thought Process/Methodology : We use terminal to run cd /Desktop/Tools/Miscellaneous and use .enum4linux.pl -h to see all available commands. After figuring out which commands we had to use, we then tried to get the user list by inputting .enum4linux.pl -U <MACHINE IP> and -S to get the sharelist. For us to find the share that doesn't require a password, we had to try every share and see which share can let us use a help command. Once we found out that tbfc-santa does not require a password, we proceeded to run ls and find the directory inside.