PSP0201

Week 3

Writeup

Group Name: Blessing Software

Members

ID	Name	Role
1211103213	Uwais	Leader
1211103149	Dzakry Hariz	Member
1211103184	Muzaffar	Member

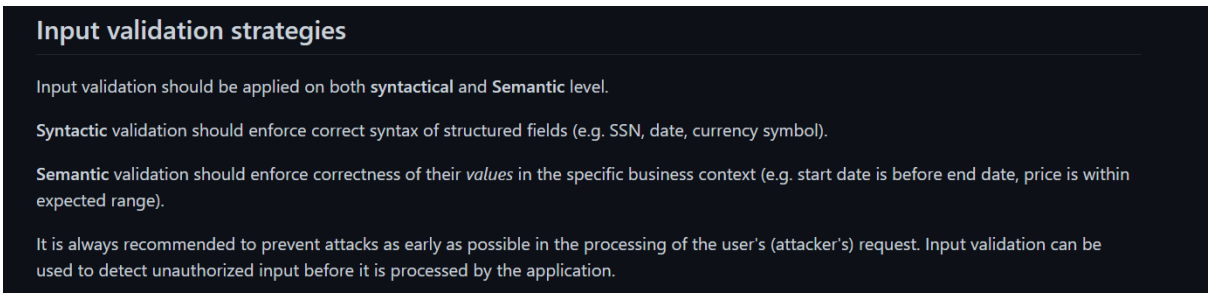
Day 6: Web Exploitation – Be careful with what you wish on a Christmas night

Tools used: Kali Linux, Firefox

Solution/walkthrough:

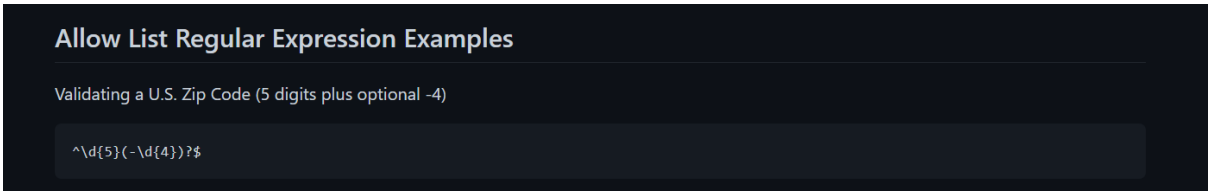
Question 1

Went to the Owasp Cheat Sheet site. Search for the input validation strategies.



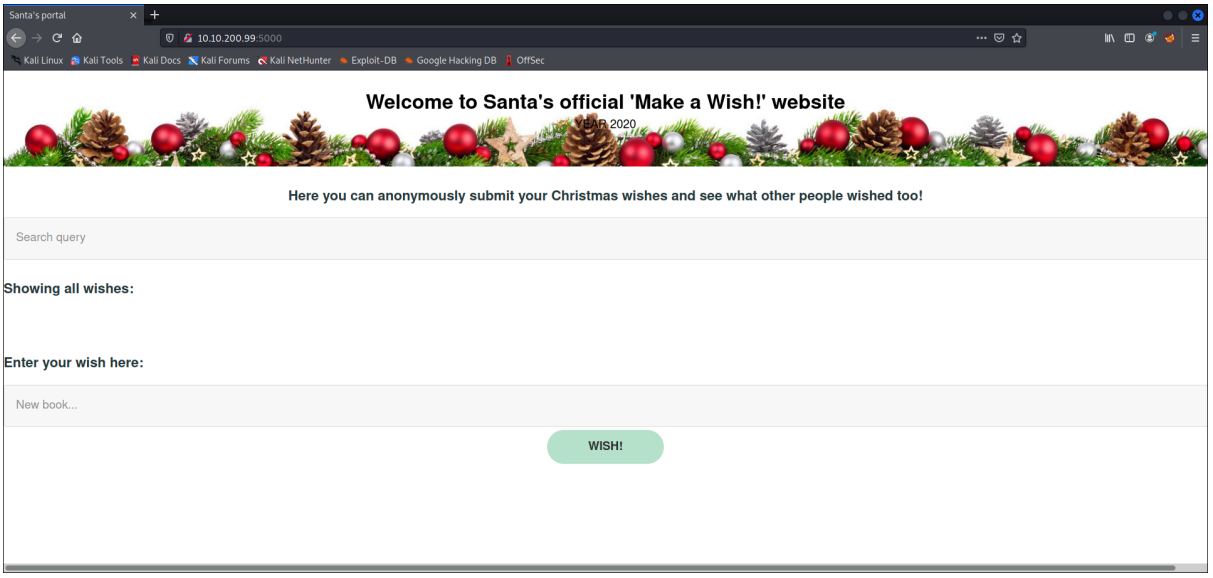
Question 2

Search for the Allow List Regular Expression Examples



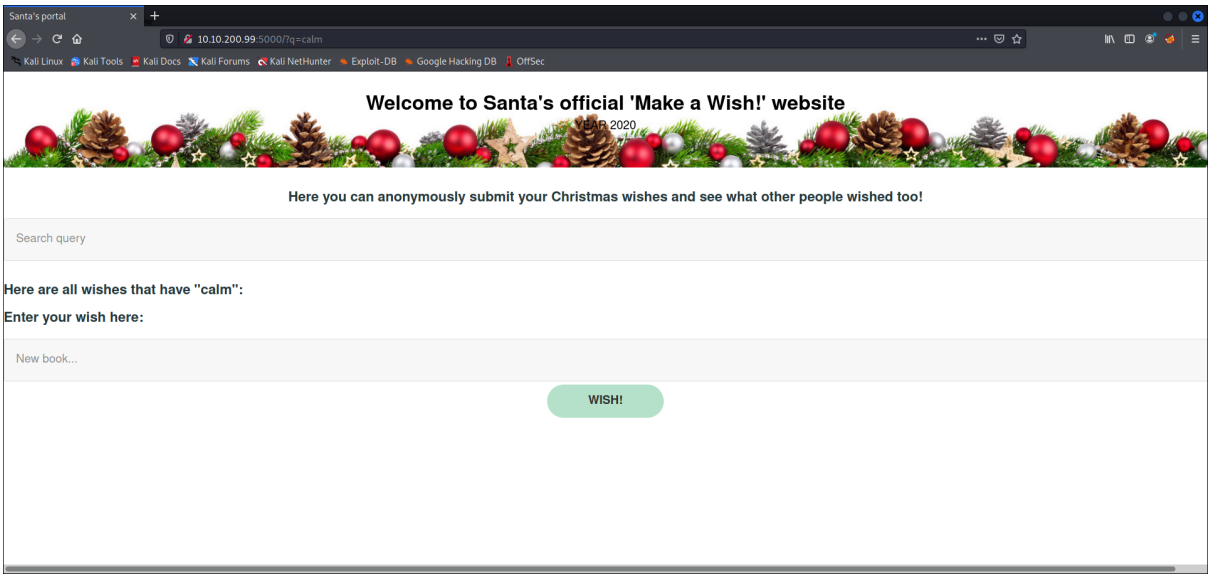
Question 3

In the site, there is a search query and submission box.



Question 4

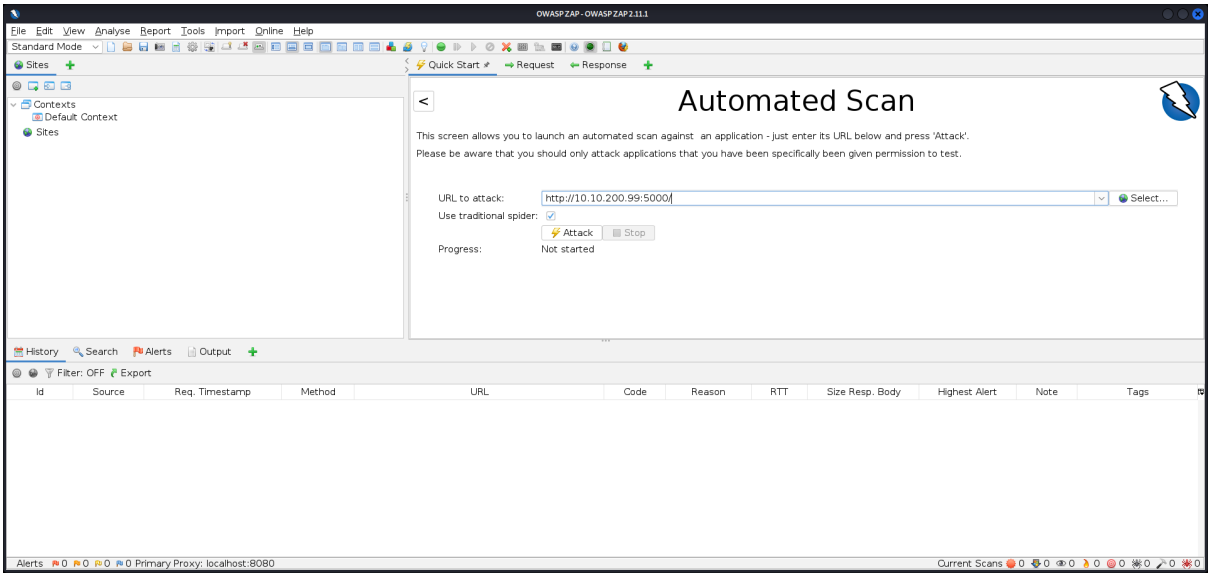
Tried searching using the website search function.

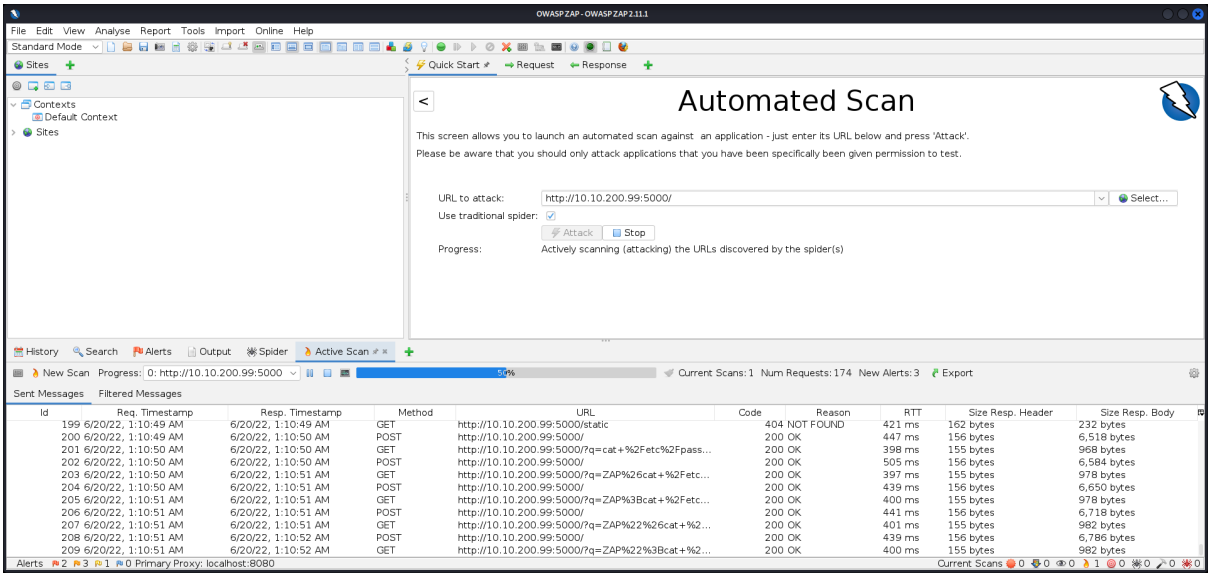


The search query showed the keyword parameter.

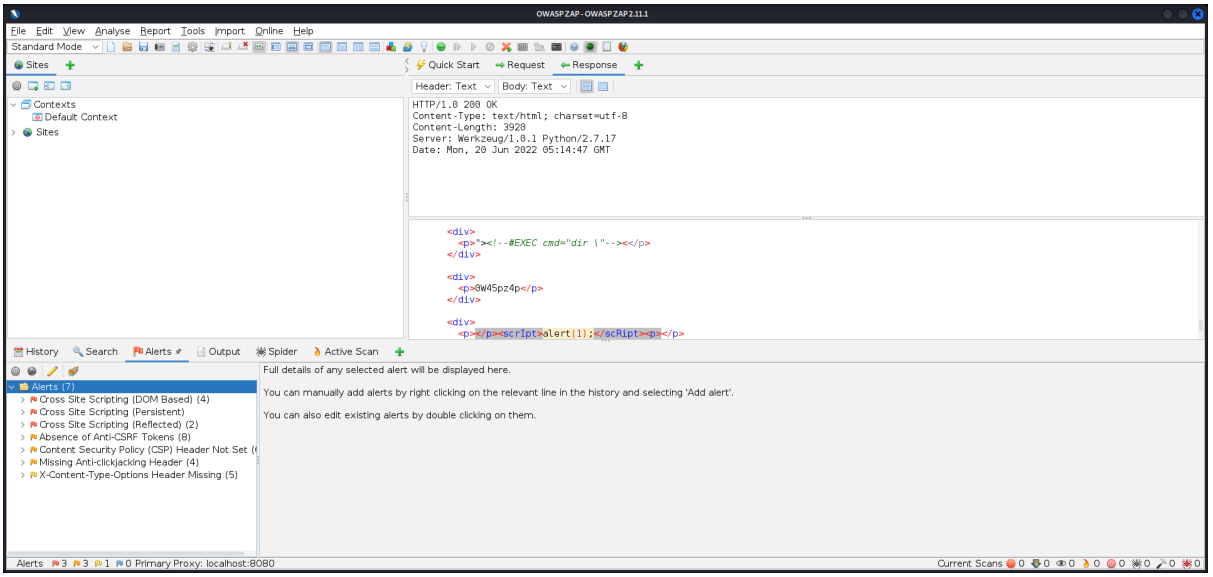
Question 5

Using OwaspZap, ran an Automated Scan on the website.





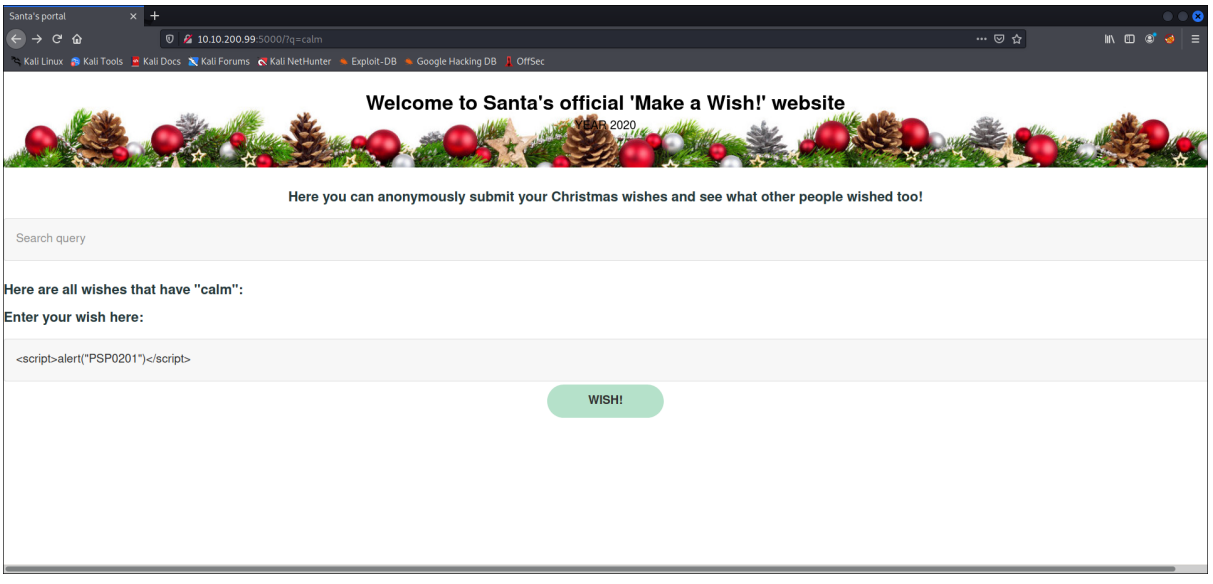
After the scan was completed, looked to the Alerts tab.

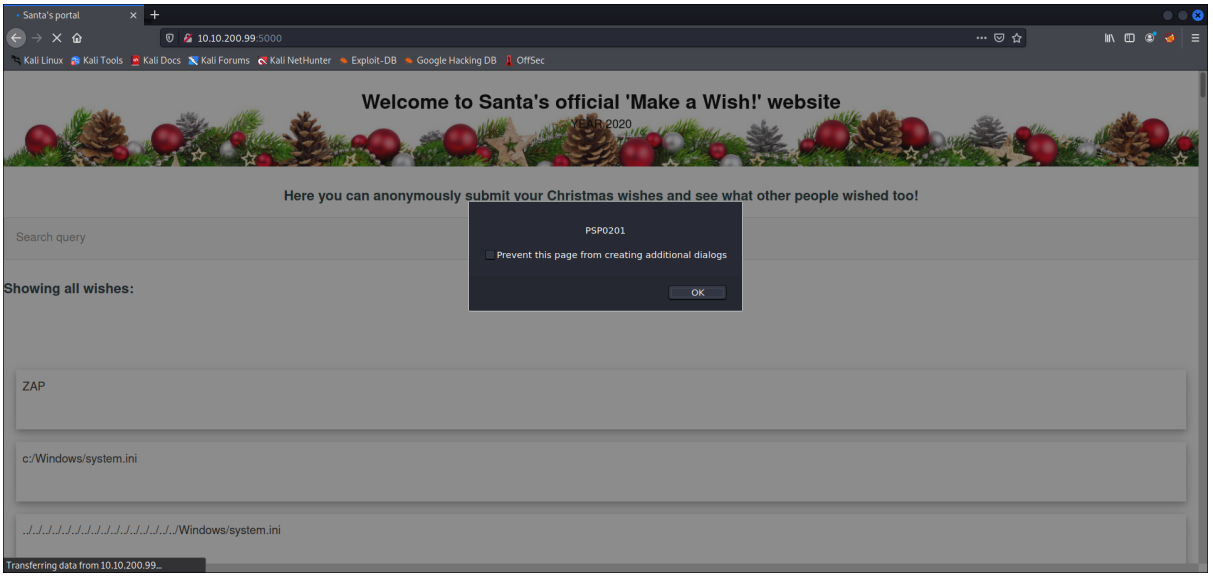


At the bottom shows the amount of high priority alerts.

Question 6

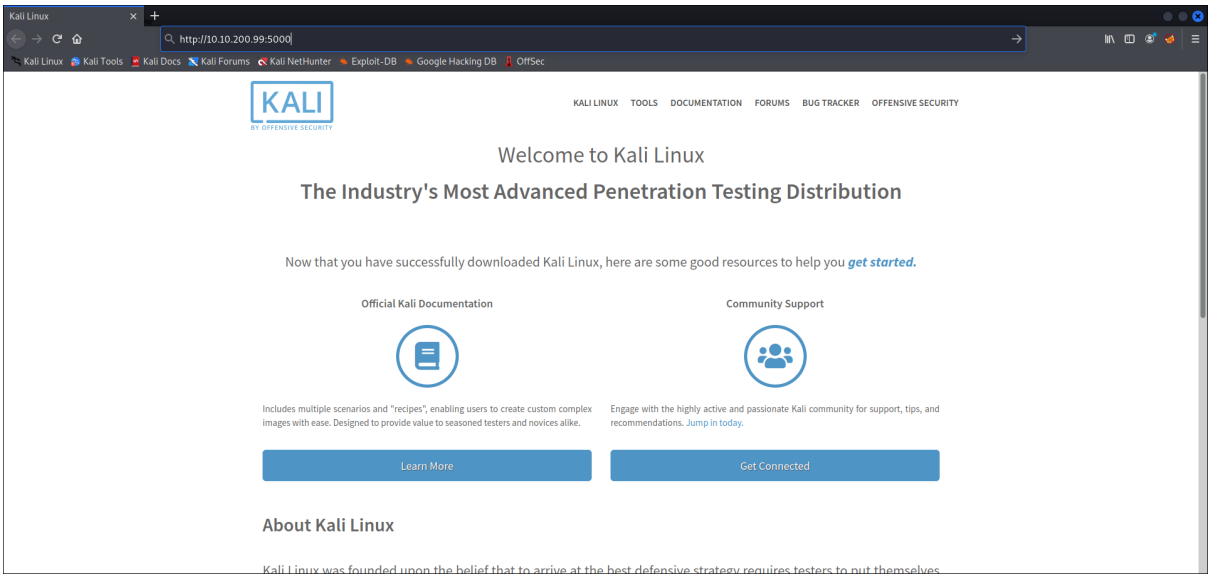
Entered the script into the wish text box.

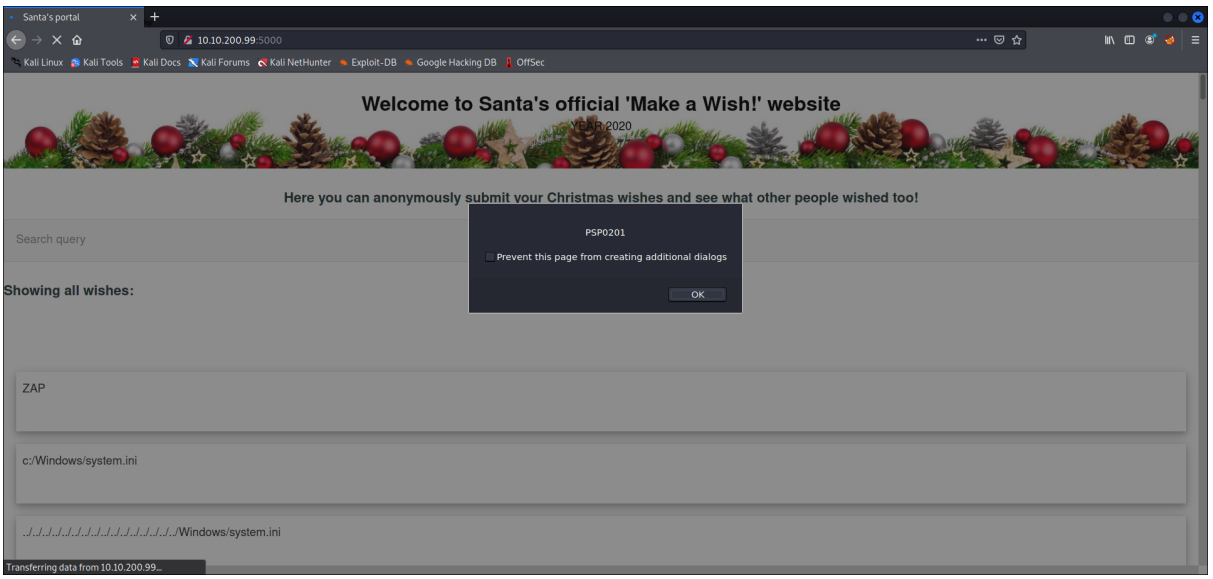




Question 7

Closed the browser, and reentered the site.





Thought Process/Methodology:

Using the reference given, which was the Owasp Cheat Sheet, we could see the explanation for input validation level and regular expression for a US Zip code. When going to the site, we say search inputs and comments that can be entered in by user. This shows the vulnerability type to exploit using XSS. Then, we used the search query to search for something. This gives us the query string that can be abused. After that, using OwaspZap application we ran an automated scan through the website. Once done, it gave us the amount of alert results and type of priorities, that included XSS, for us to exploit. After running XSS exploits, we closed the browser and revisited the site to see whether the XSS attacks persisted.

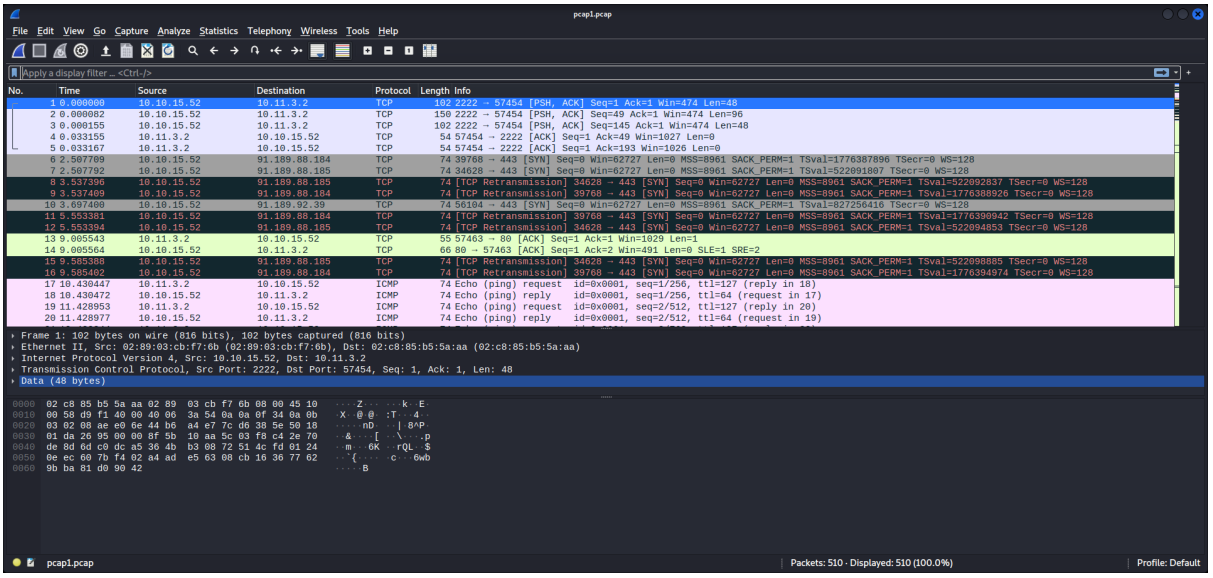
Day 7: Networking – The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox

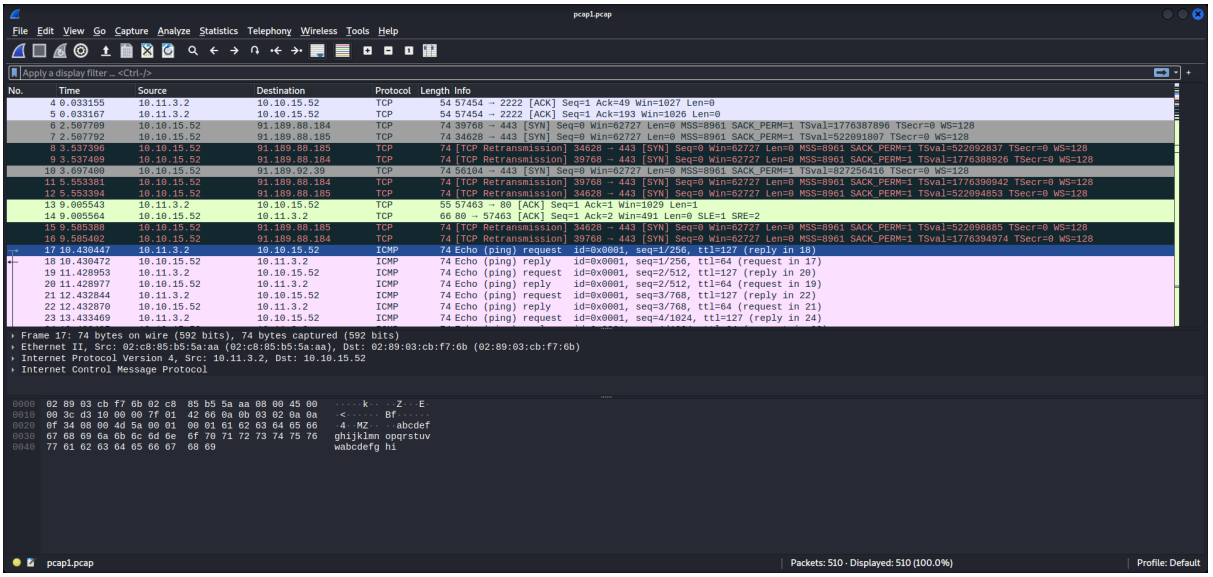
Solution/walkthrough:

Question 1

Opened Wireshark, and opened pcap1.pcap.

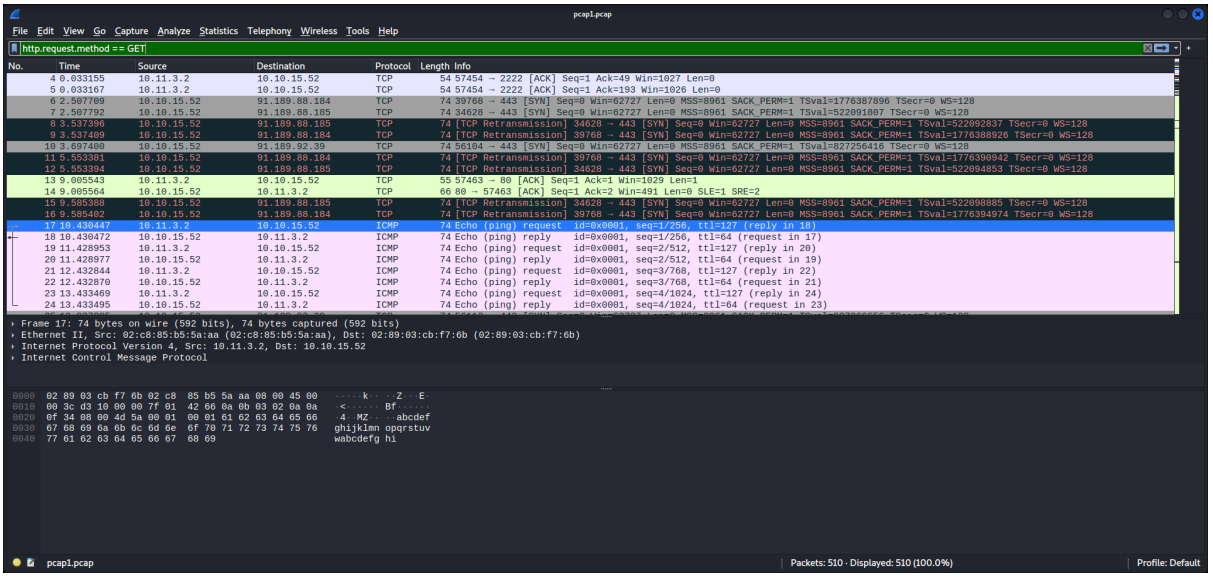


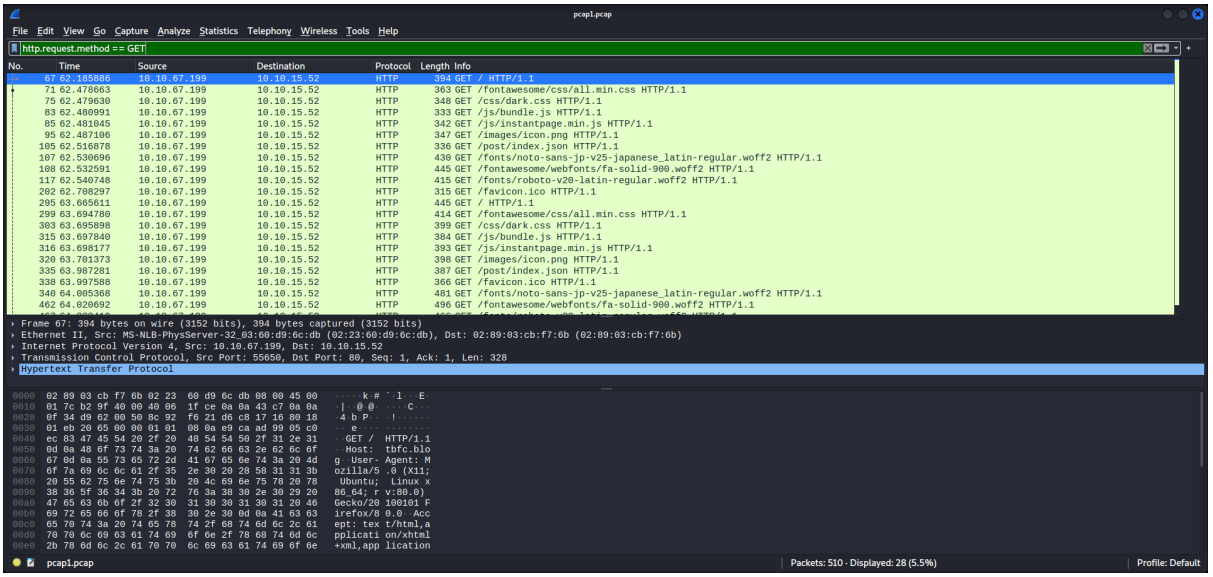
Search for the first IP address that has ICMP protocol.



Question 2

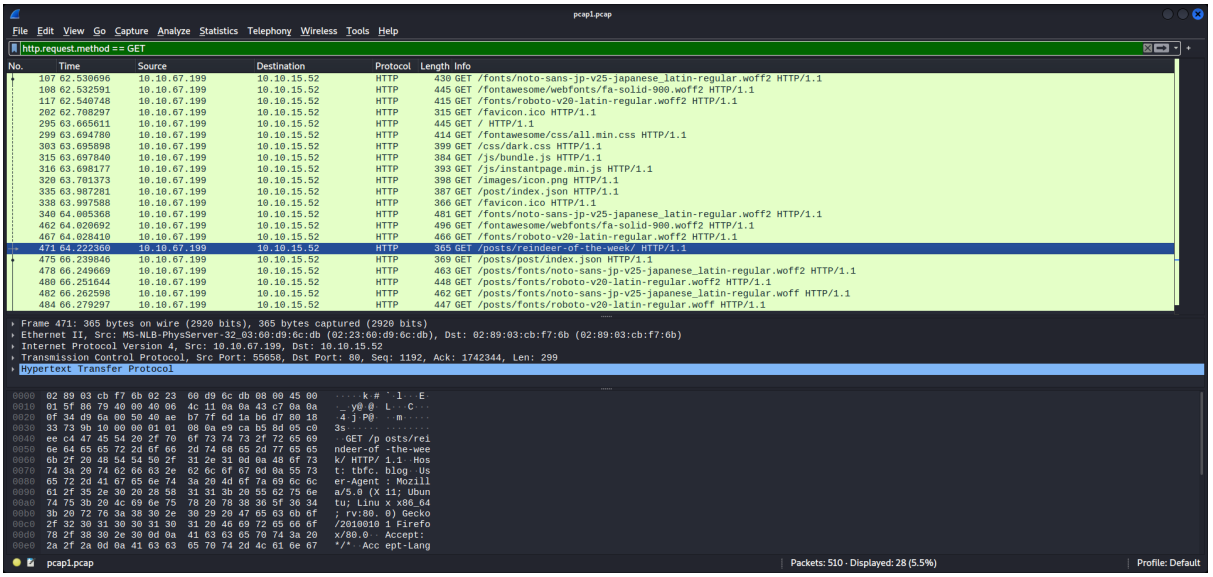
Use the search filter to specify for HTTP GET requests using command.





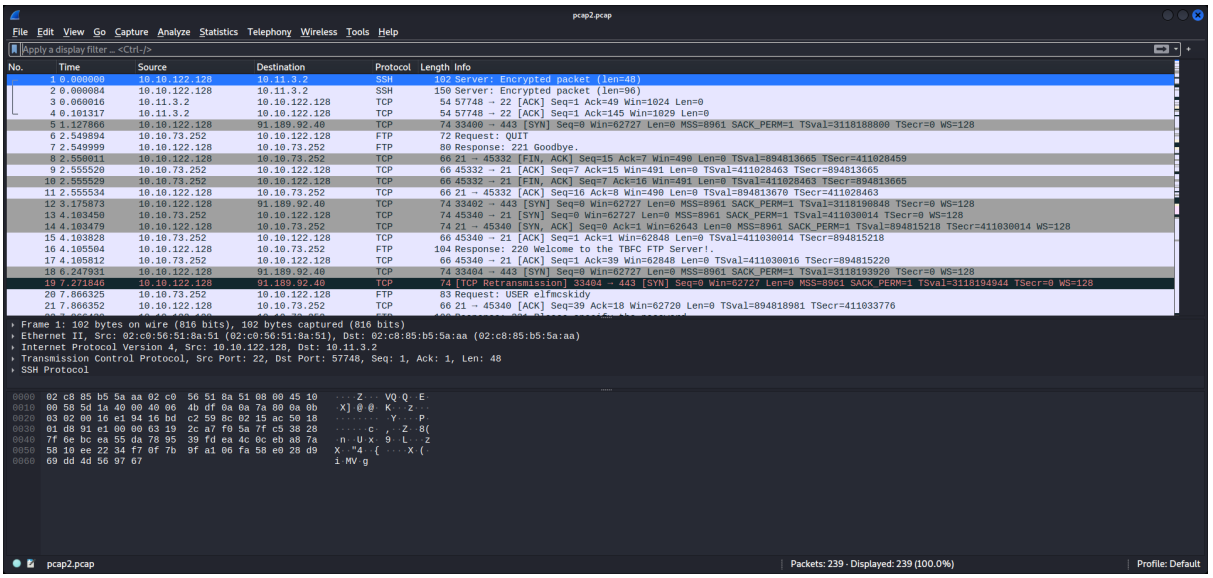
Question 3

Look for posts that could be an article.

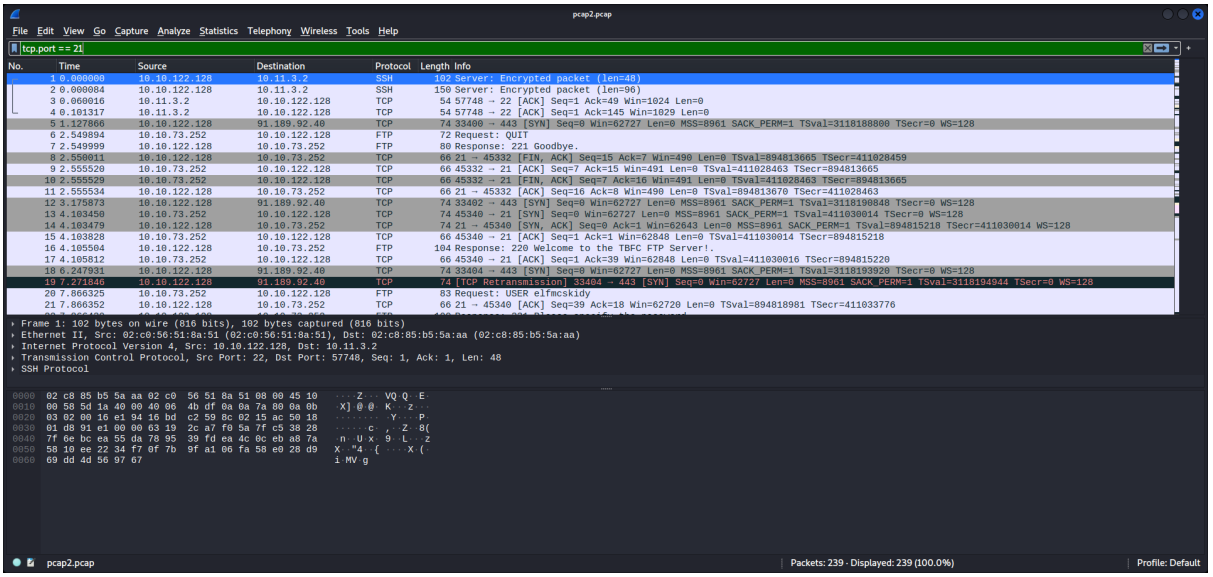


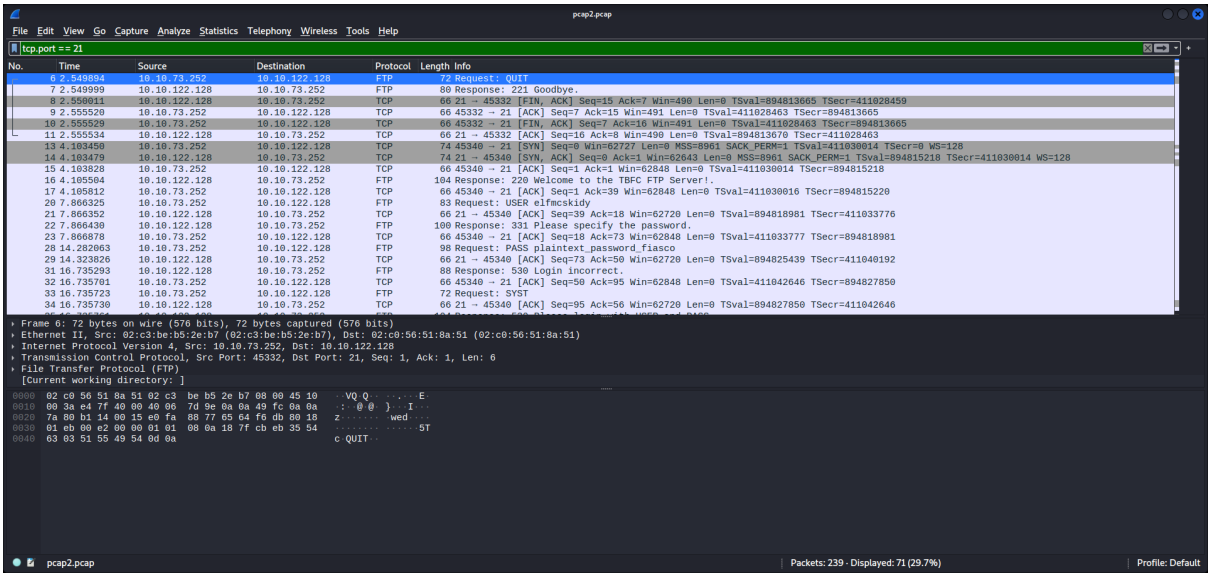
Question 4

Open pcap2.pcap on Wireshark.



Use the search filter for TCP protocols under port 21.





Look for the password entered.

```
15 4.103828     10.10.73.252     10.10.122.128    TCP      66 45340 → 21 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=411030014 TSecr=894815218
16 4.105504     10.10.122.128    10.10.73.252     FTP     104 Response: 220 Welcome to the TBFC FTP Server!.
17 4.105812     10.10.73.252     10.10.122.128    TCP      66 45340 → 21 [ACK] Seq=1 Ack=39 Win=62848 Len=0 TSval=411030016 TSecr=894815220
20 7.866325     10.10.73.252     10.10.122.128    FTP      83 Request: USER elfmcskidy
21 7.866352     10.10.122.128    10.10.73.252     TCP      66 21 → 45340 [ACK] Seq=39 Ack=18 Win=62720 Len=0 TSval=894818981 TSecr=411033776
22 7.866430     10.10.122.128    10.10.73.252     FTP     100 Response: 331 Please specify the password.
23 7.866878     10.10.73.252     10.10.122.128    TCP      66 45340 → 21 [ACK] Seq=18 Ack=73 Win=62848 Len=0 TSval=411033777 TSecr=894818981
28 14.282063    10.10.73.252     10.10.122.128    FTP      98 Request: PASS plaintext_password_fiasco
```

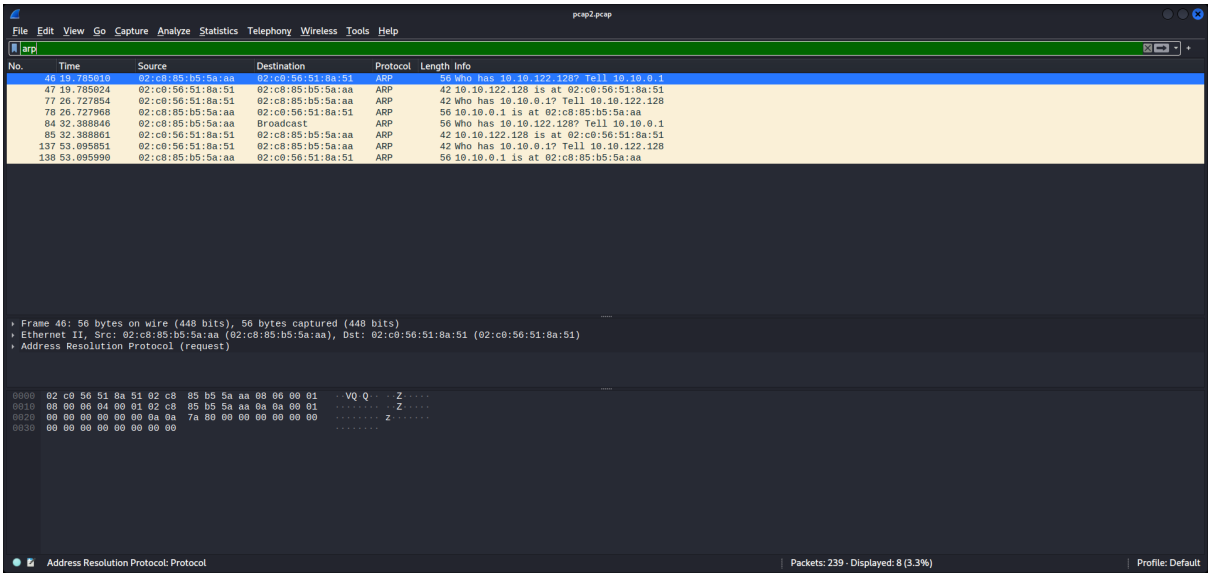
Question 5

Without any filters, search for the protocols with encrypted packets.

```
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 6

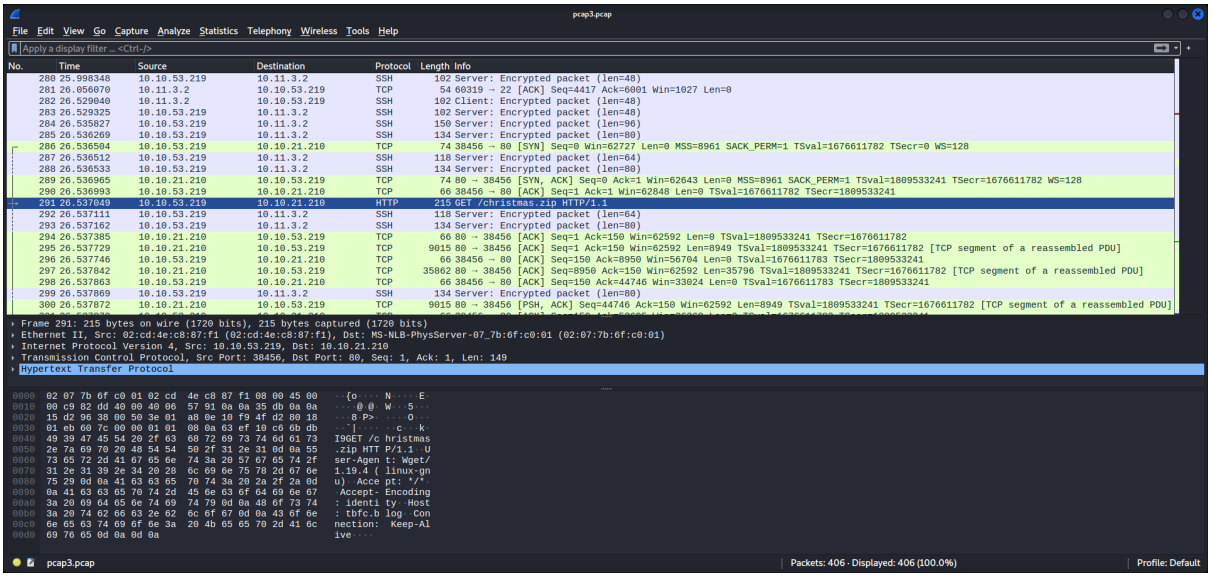
Search filter for ARP communications.



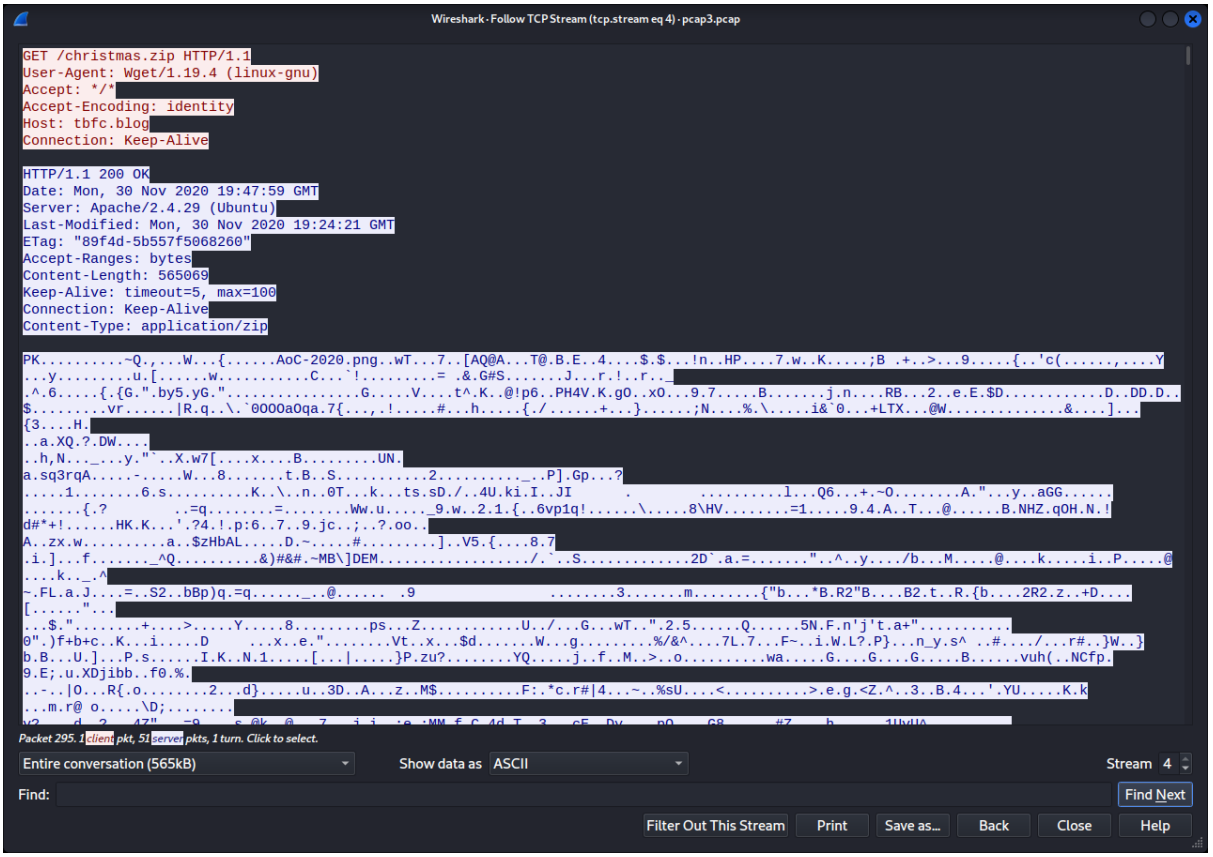

```
46 19.785010    02:c8:85:b5:5a:aa    02:c0:56:51:8a:51    ARP          56 Who has 10.10.122.128? Tell 10.10.0.1
47 19.785024    02:c0:56:51:8a:51    02:c8:85:b5:5a:aa    ARP          42 10.10.122.128 is at 02:c0:56:51:8a:51
```

Question 7

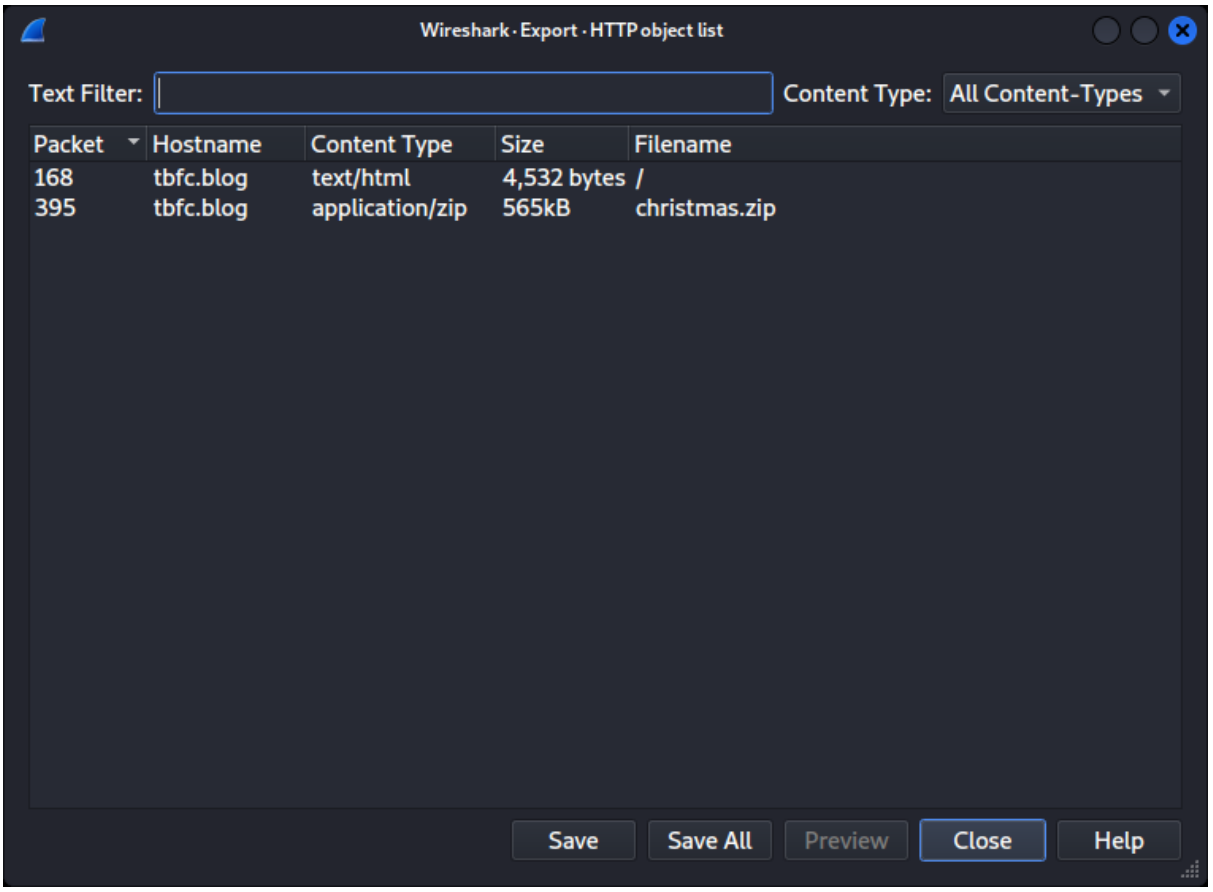
Look through pcap3.pcap for any informations.



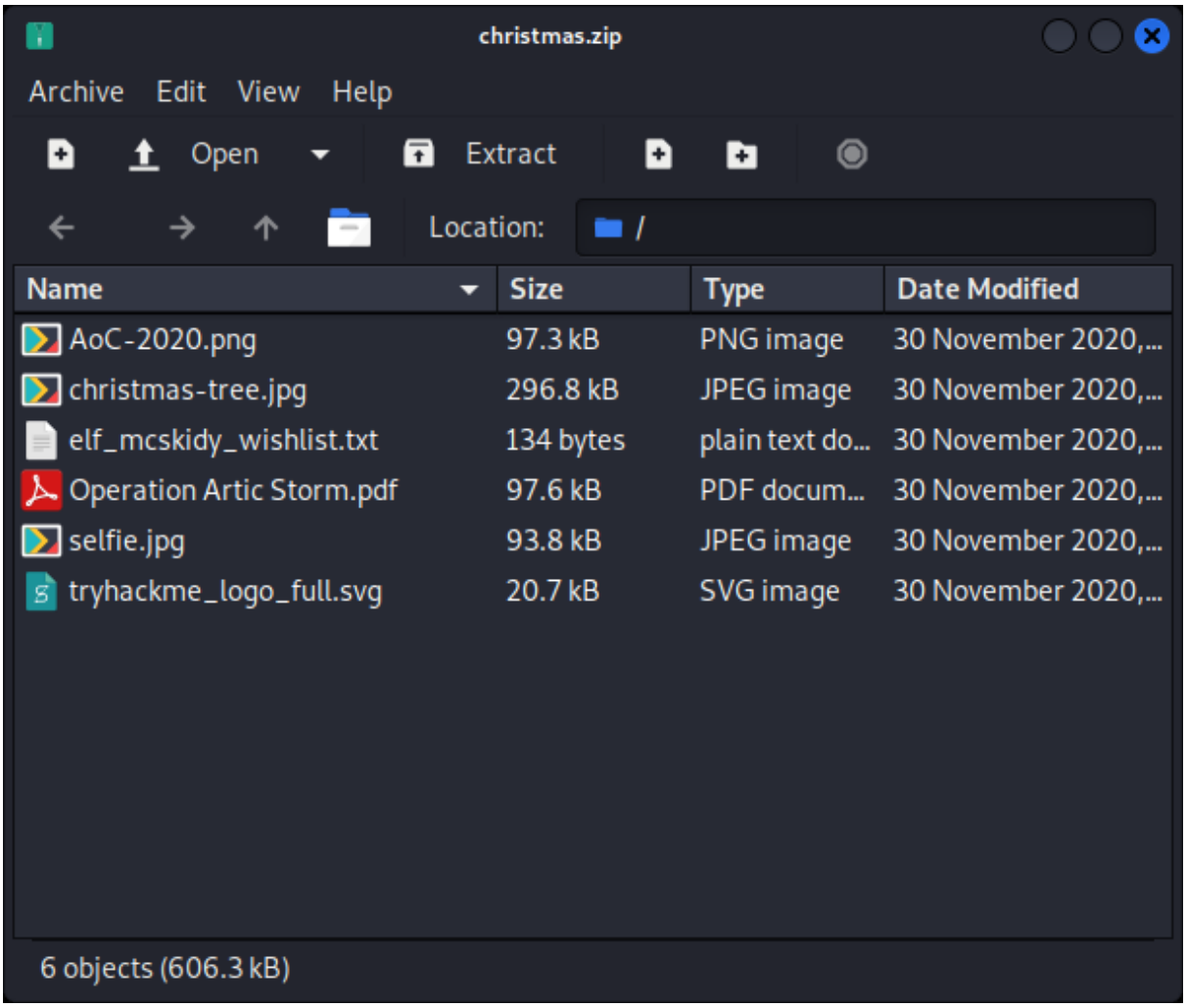
Follow the TCP stream.



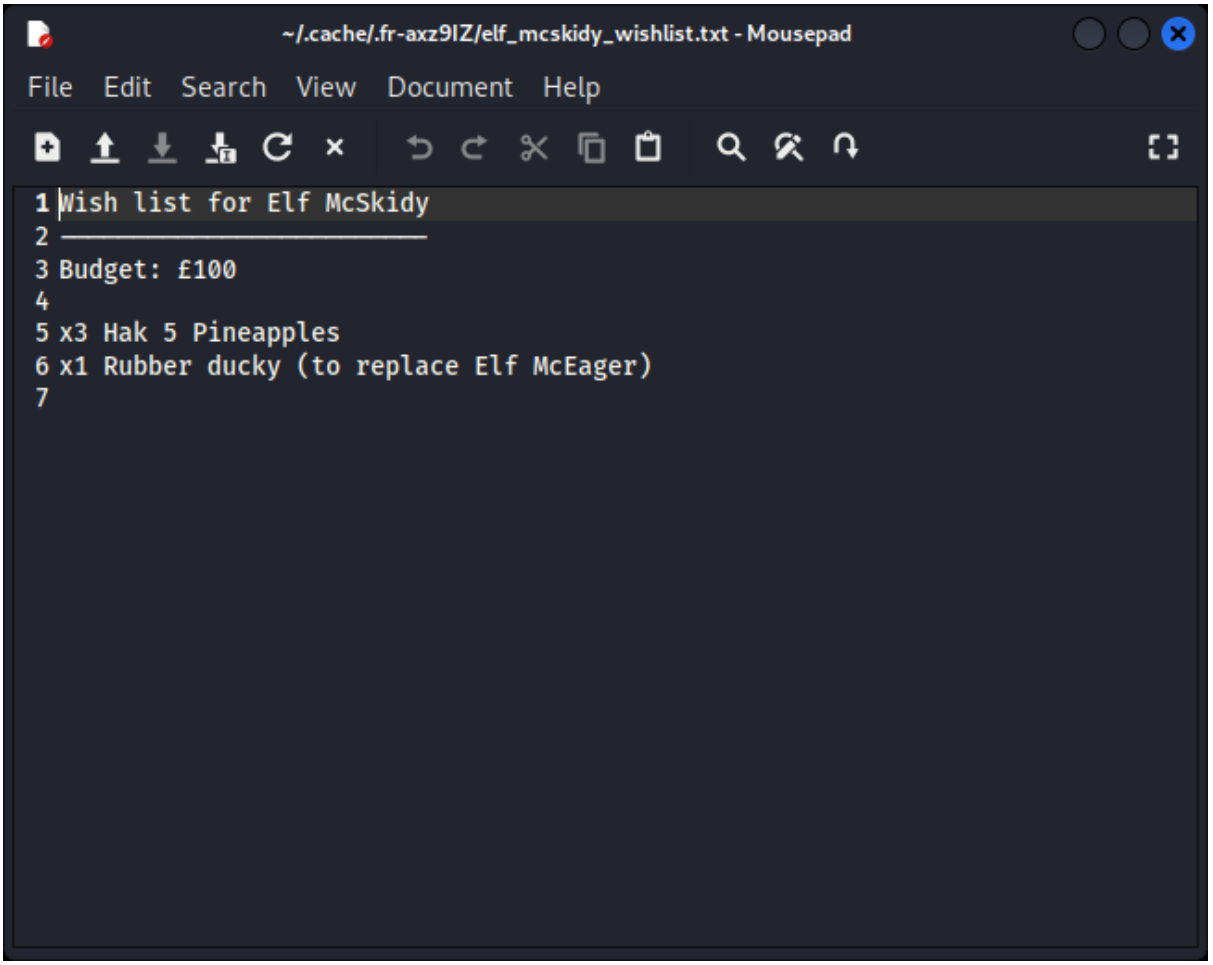
Export Objects HTTP.



Save the Christmas.zip file and open it.

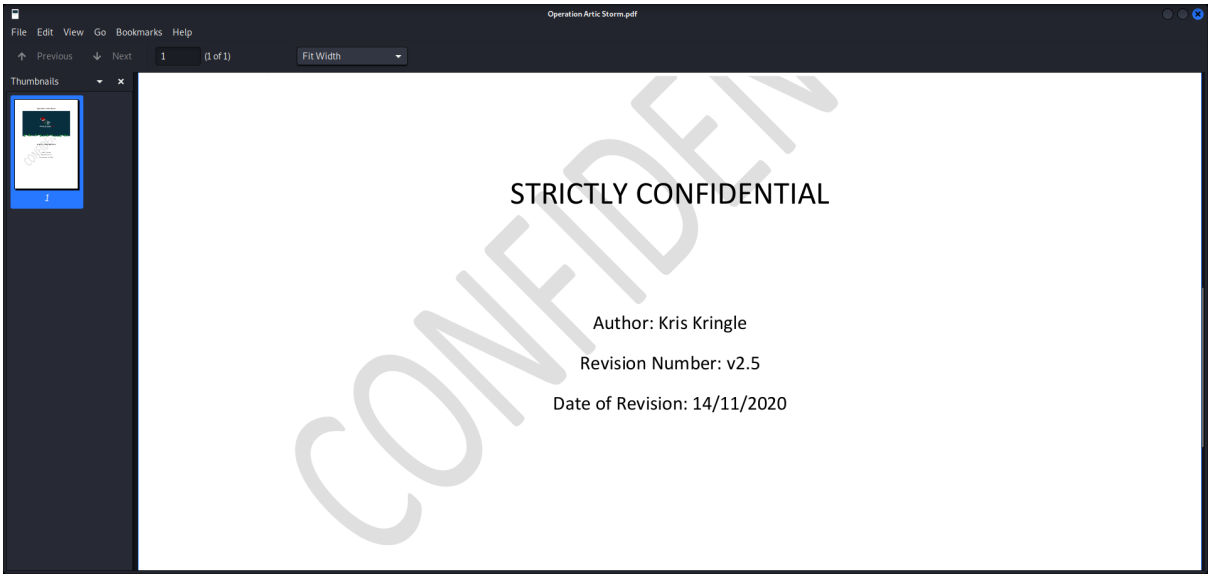


Look into wishlist.txt file.



Question 8

Open Operation Artic Storm.pdf and search for the author.



Thought Process/Methodology:

Using Wireshark, we analysed pcap1.pcap file first. We looked for an IP address that had a ping request using ICMP protocol. Then, we used a filter for HTTP GET methods to look for articles visited. Next was to look through pcap2.pcap. Since we are looking for an FTP traffic, we filtered for TCP protocols with port 21 and found the password. Without any search filters, we saw encrypted packets with SSH protocols. Search filtering for arp gives us the communications for the MAC address needed. Lastly, we analysed through pcap3.pcap. Looking through the output, we thought there was a file downloaded from the TCP stream. Following it shows an application/zip Content-Type. Thus we went to export Objects in HTTP and found the Christmas.zip file. From there, we discovered the wishlist.txt and Operation Artic Storm.pdf.

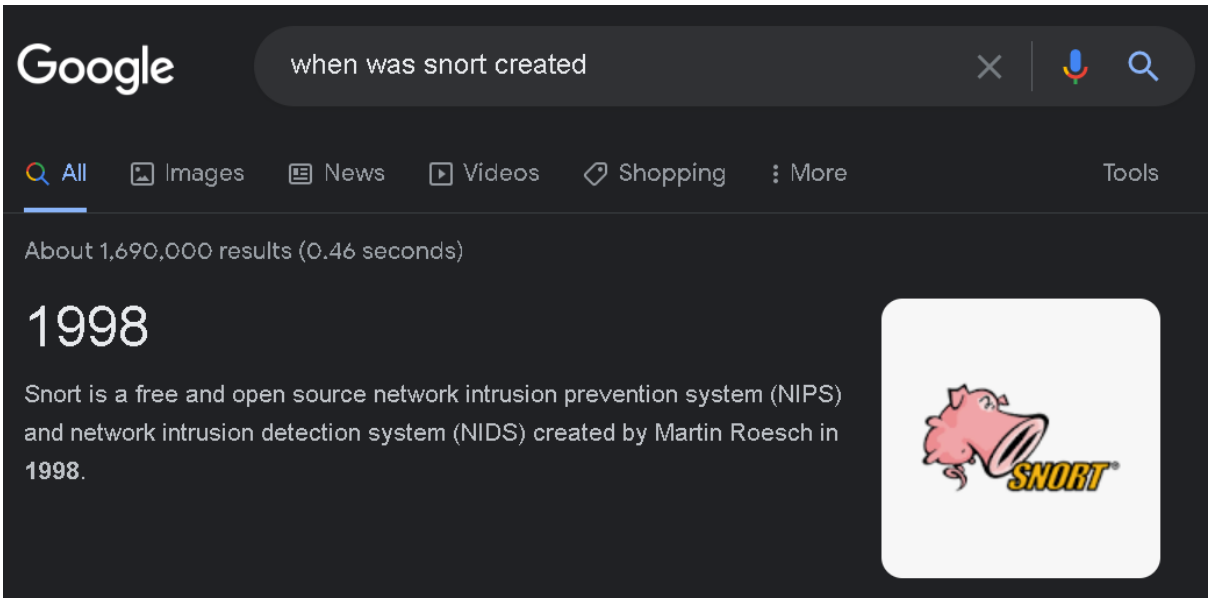
Day 8 : Networking- What's under the Christmas Tree?

Tool used: Kali Linux,Firefox,Nmap,Google

Solution/Walkthrough:

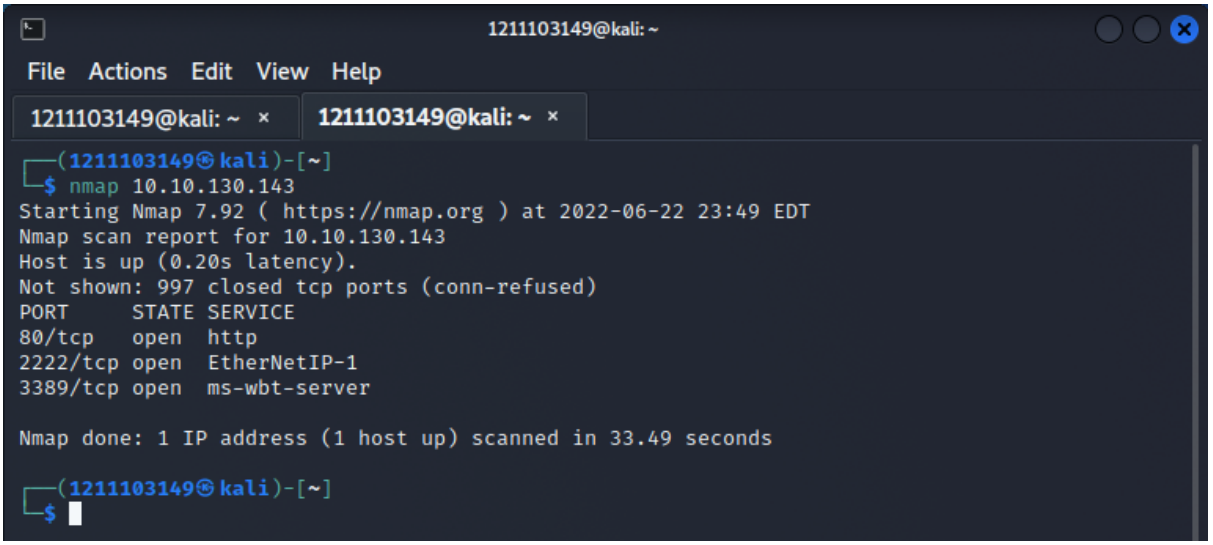
Question 1

Make a quick google search



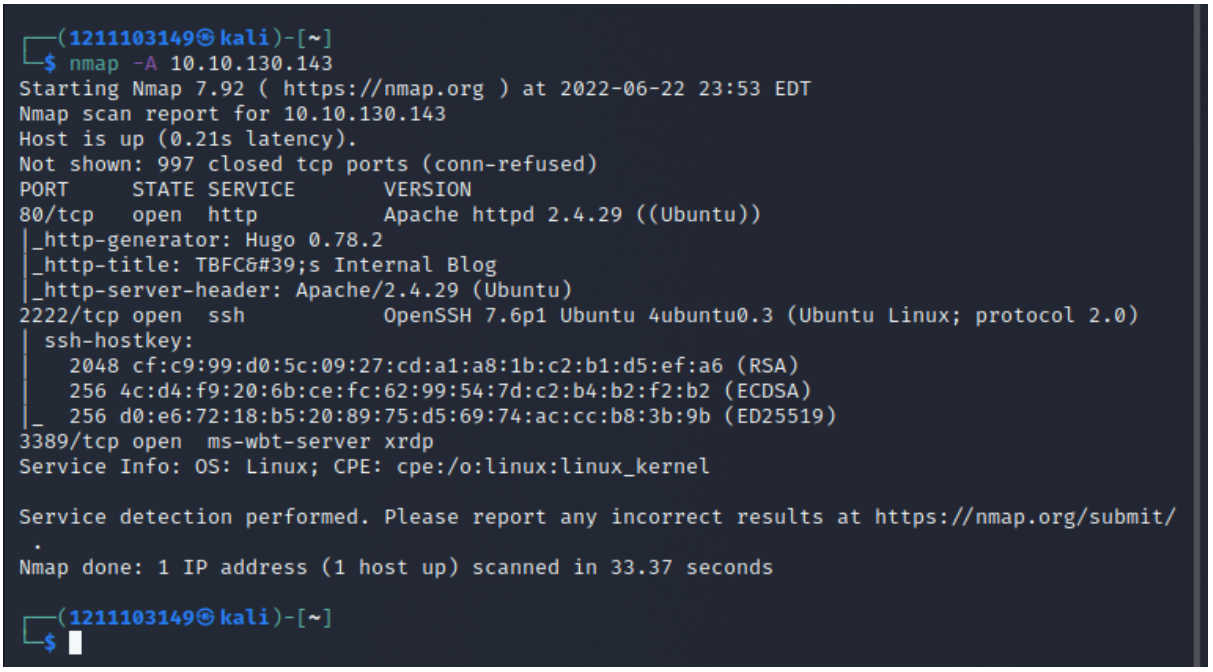
Question 2

Use Nmap on the on the machine IP



Question 3,4,5 and 6

Use the -A flag on the machine ip



Thought Process/Methodology:

Using Nmap on the ip will let us discover the host and services running on it so we'll be able to get the ports it's running. Then because we aren't afraid of getting detected, we used the -A(aggressive) flag to display even more information about the ip. With that, we can get all the information we needed, which were what distribution of Linux it was running, what version of apache it was using, what was running on the port 2222 and finally what the ip was most likely used for.

Day 9 : Networking - Anyone can be Santa!

Tool used: Kali Linux, Firefox

Solution/Walkthrough:

Question 1

Log in to the victim machine's FTP servers with anonymous mode.

```
┌──(1211103213㉿kali)-[~]
└─$ ftp 10.10.46.122
Connected to 10.10.46.122.
220 Welcome to the TBFC FTP Server!.
Name (10.10.46.122:1211103213): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

List out the files found using ls command.

```
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.
```

Question 2

Look for directory that has data to be viewed.

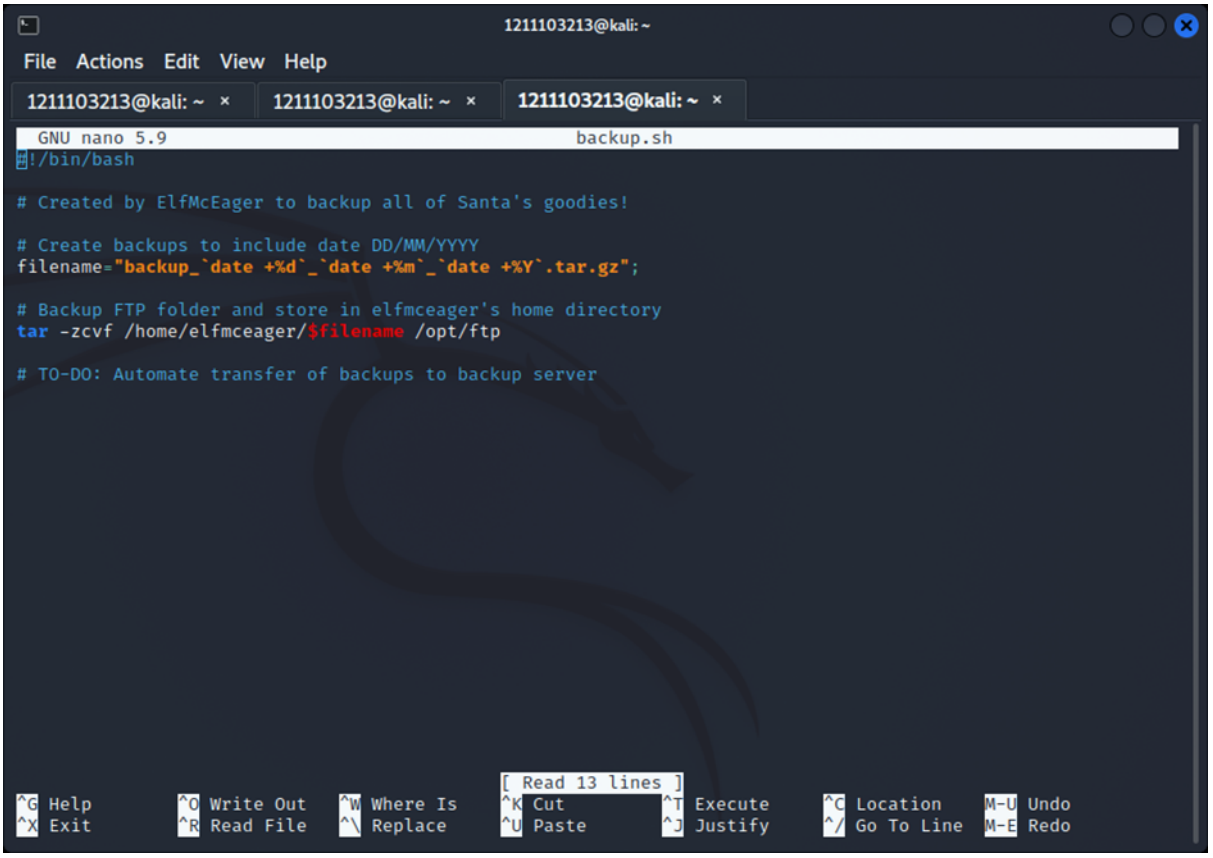
```
ftp> cd elf_workshops
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
ftp> cd human_resources
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> cd ..
250 Directory successfully changed.
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.
```

Question 3

Download the files in the public directory.

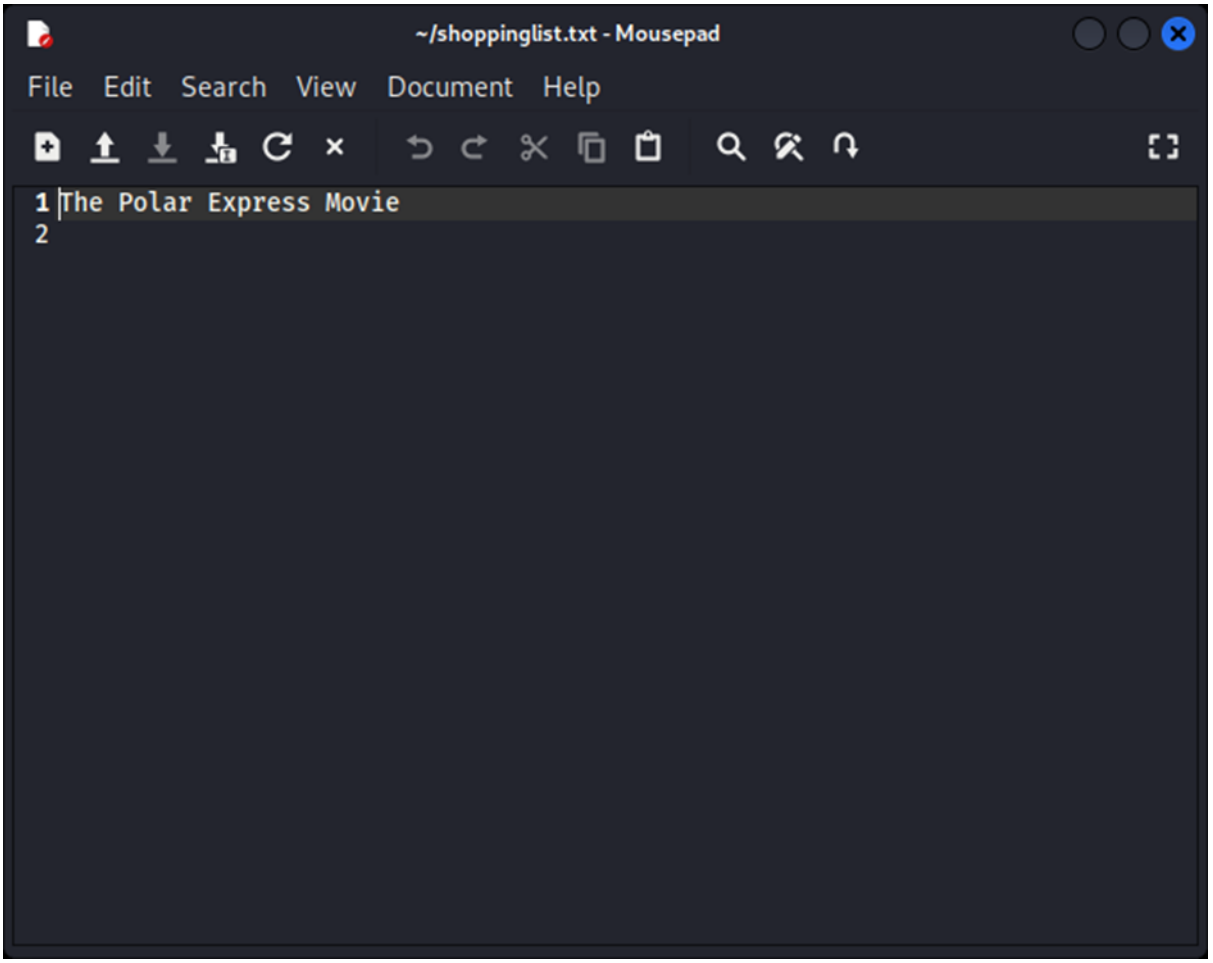
```
ftp> get backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup.sh (341 bytes).
226 Transfer complete.
341 bytes received in 0.00 secs (73.8377 kB/s)
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: 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 (756.0484 kB/s)
```

Open the shell using a text editor.



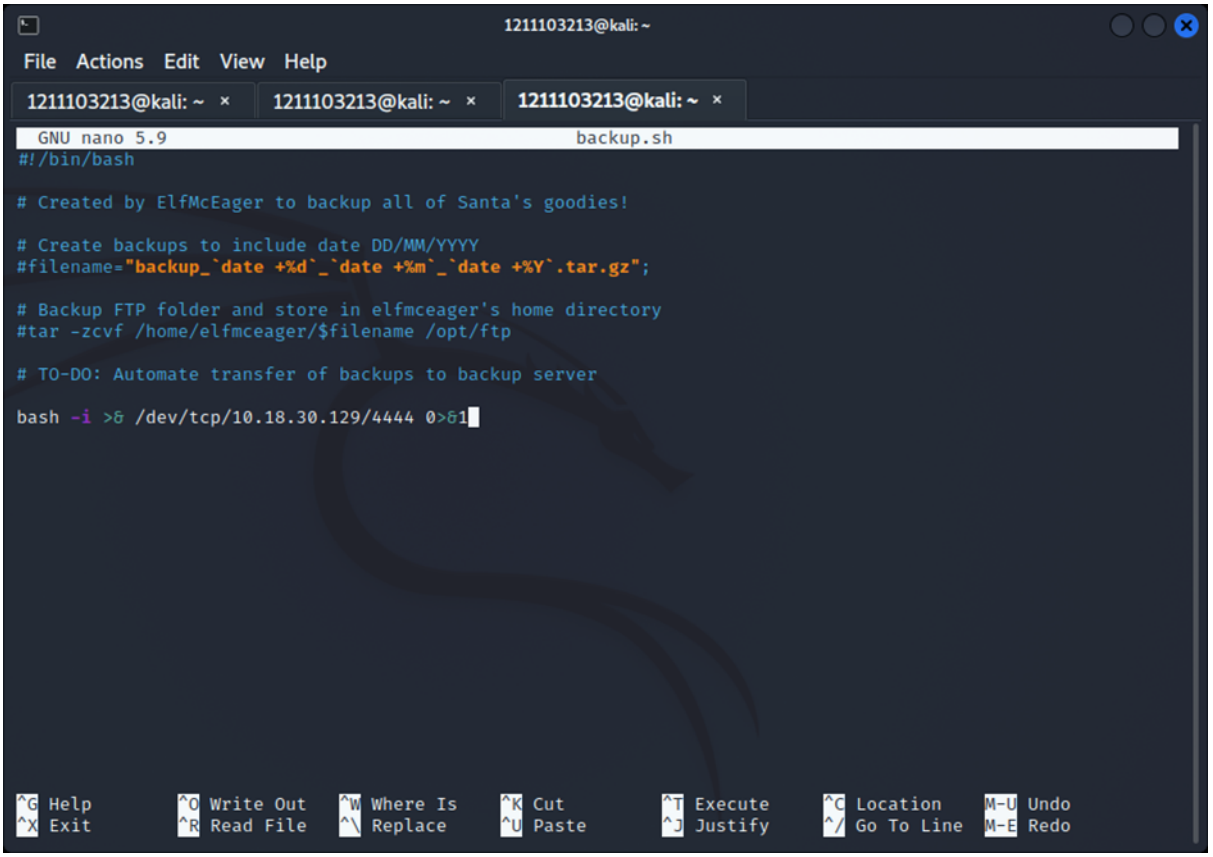
Question 4

Open the shoppinglist.txt file.

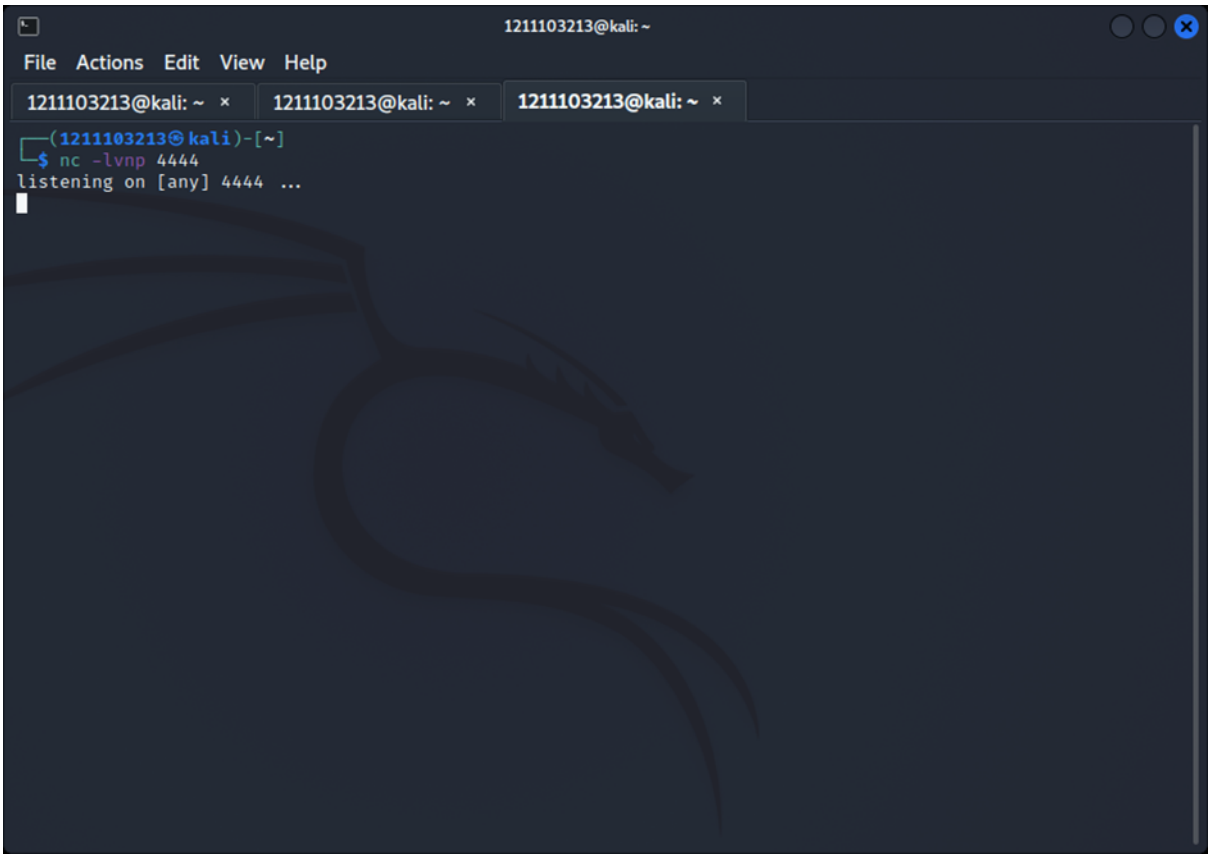


Question 5

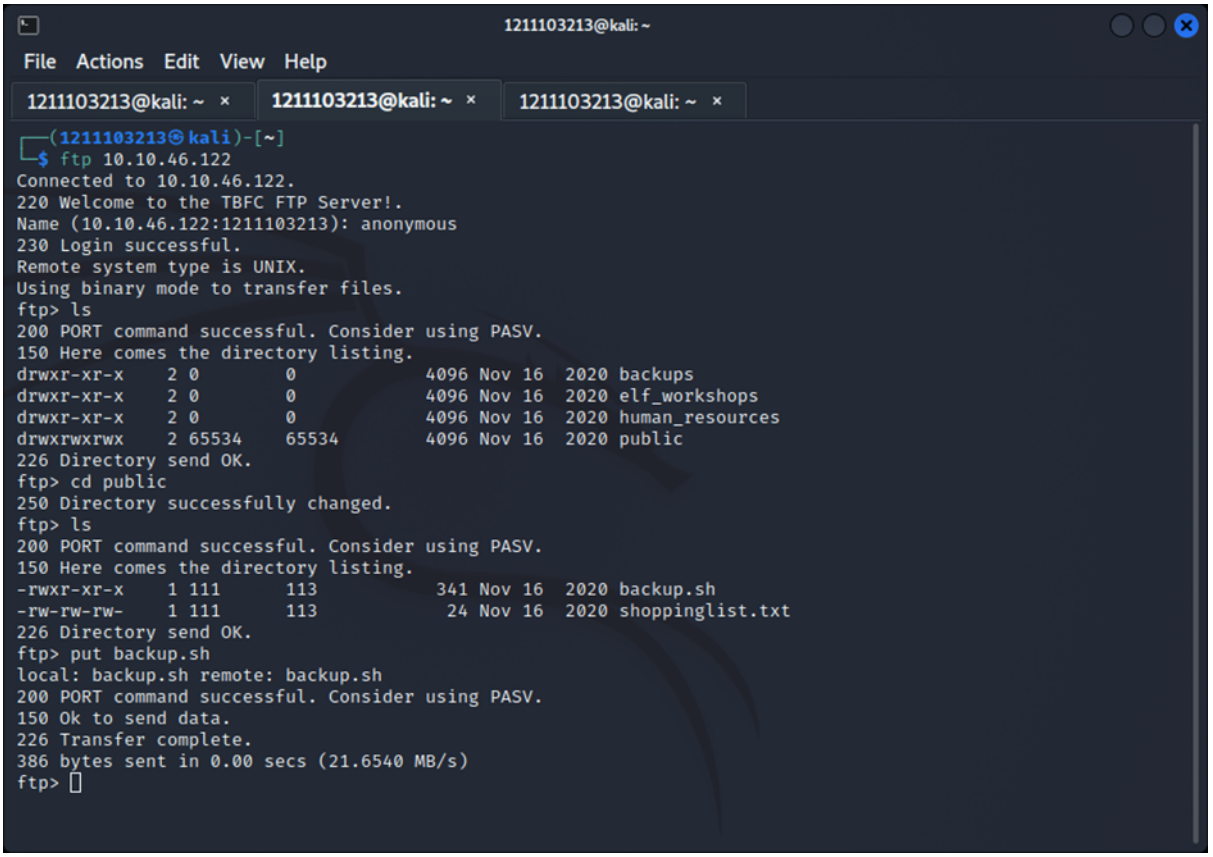
With the pentesters sheet, add command to generate a shell in the backup.sh file and save it.



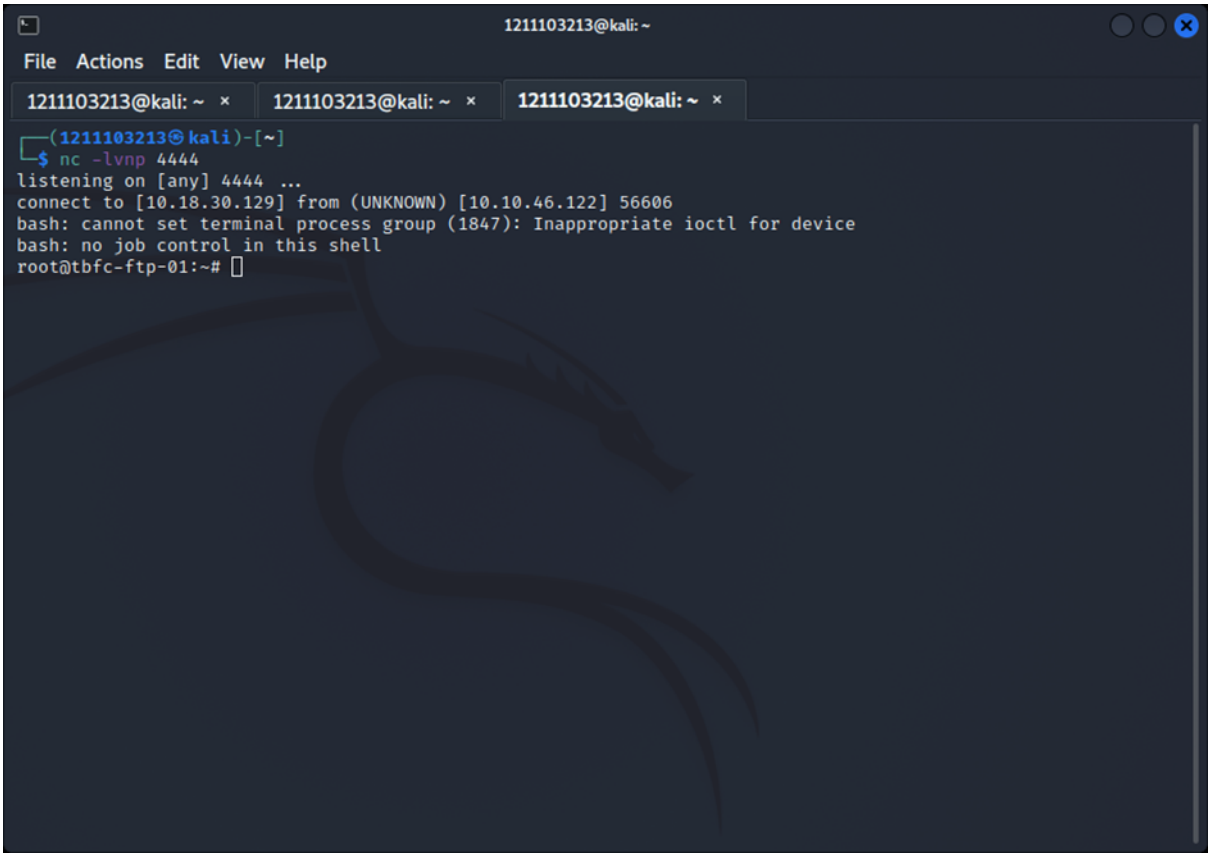
Setup a listener using netcat.



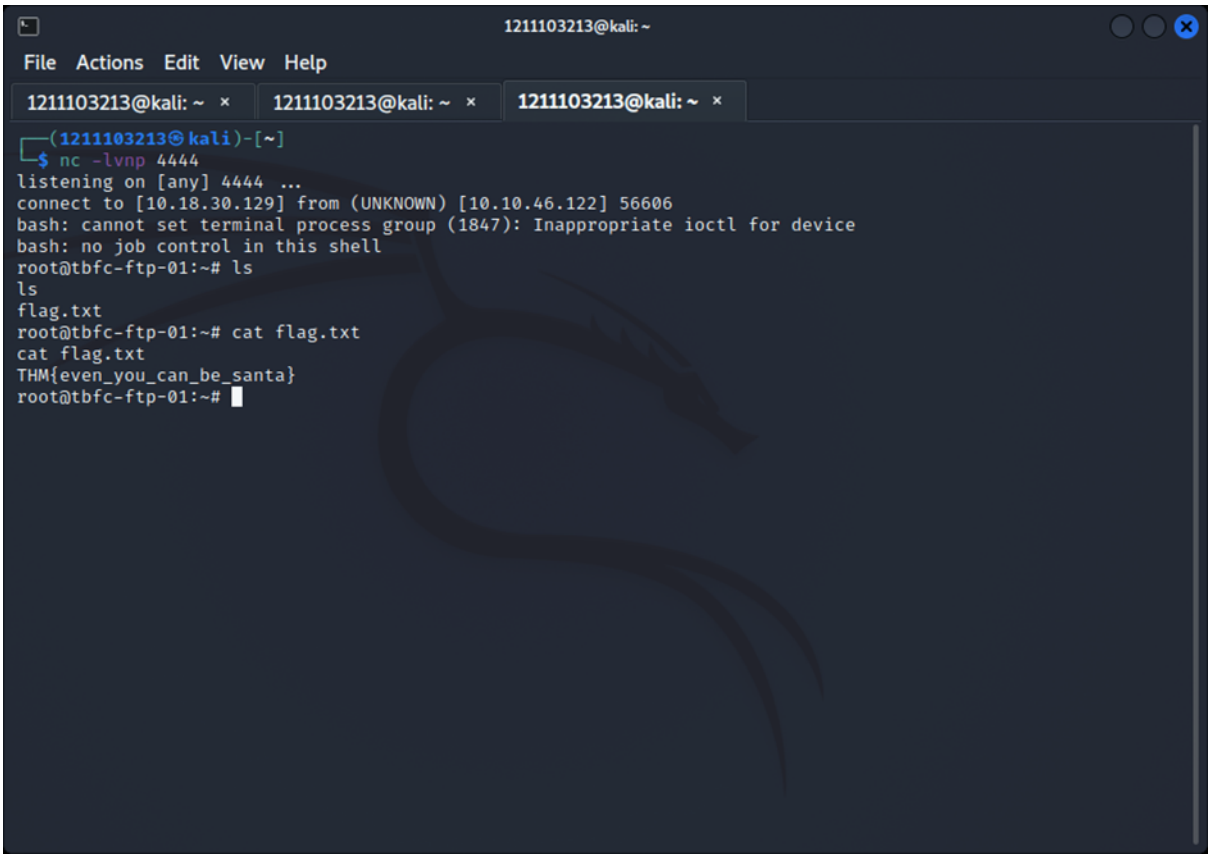
Go back to the victim machine's FTP server and upload the shell with malicious command.



Look back at the netcat listener.



Search for the flag.



Thought Process/Methodology:

After accessing the victim's FTP server using anonymous mode, we looked for the directories available. Only the public directory could be accessed. In there, there was a shell file and text file. Using the get command, we downloaded both files to our device. Opening the text file reveals Santa's movie to be bought. Then, opening the shell file allows us to insert a malicious code that runs a shell for us. Next, we prepared a shell listener using netcat. Going back to the victim's FTP server, we can upload the shell with our malicious code into the same public directory. Back to our netcat listener, we were able to gain root access on our victim's machine with the reverse shell. Thus, we searched and obtained the flag.

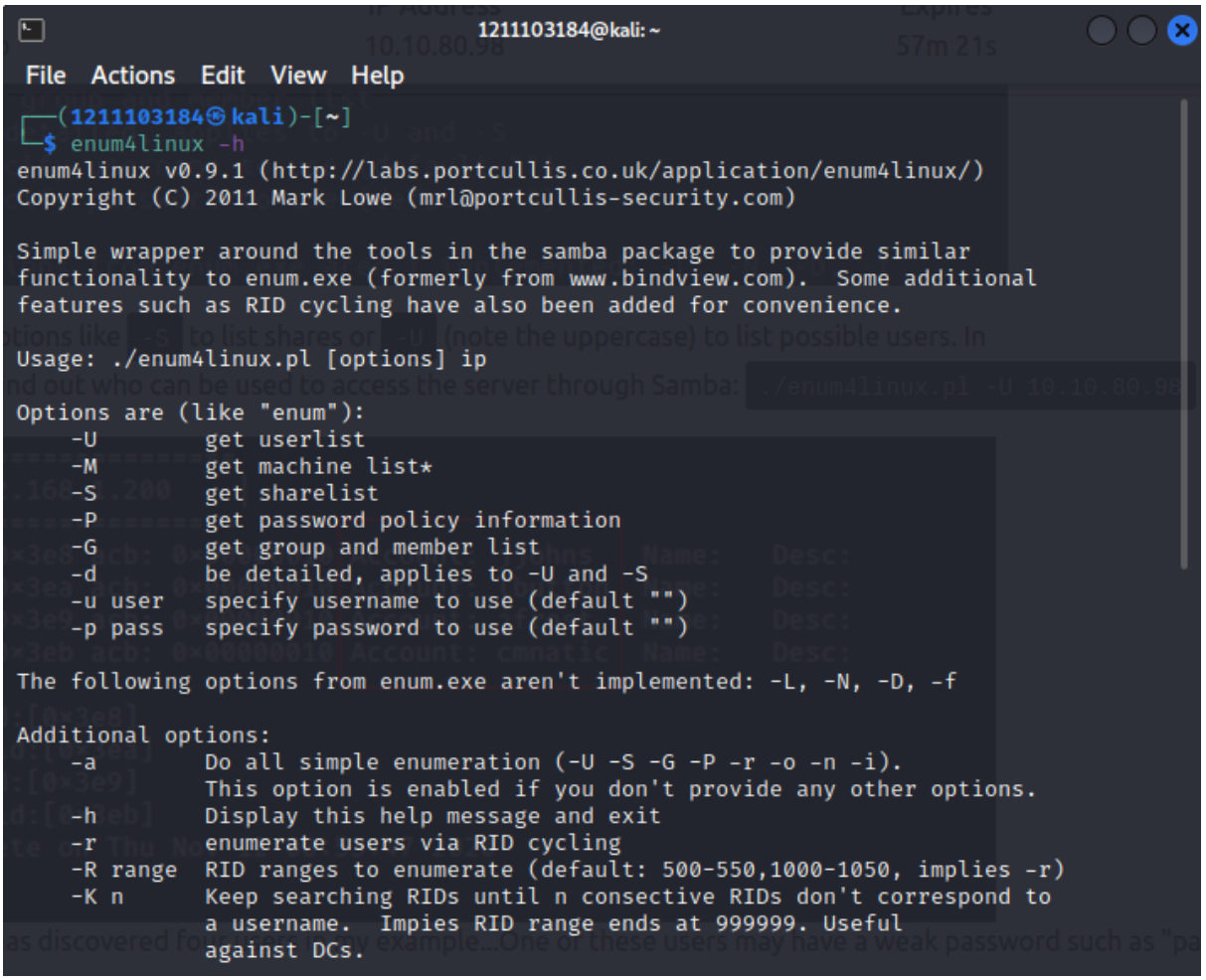
Day 10 : Networking - Don't Be sElfish!

Tools used: Kali Linux, Firefox

Solution/walkthrough:

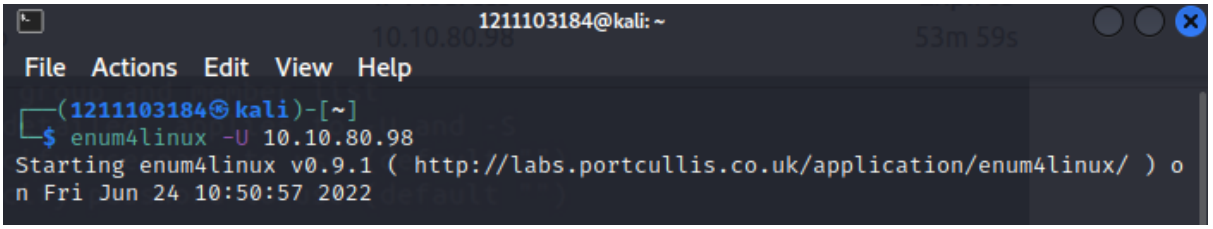
Question 1

open terminal and use enum4linux help command. Search for the options list.



Question 2

Use enum4linux userlist command followed by the IP address given.



```
( Users on 10.10.80.98 )

index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy      Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager      Name: elfmceager    D
esc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson   Name:   Desc:

user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
enum4linux complete on Fri Jun 24 10:51:10 2022
```

Question 3

Use enum4linux sharelist command with the IP address given.

```
1211103184@kali: ~
File  Actions  Edit  View  Help
┌──(1211103184㉿kali)-[~]
└─$ enum4linux -S 10.10.80.98
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ )
on Fri Jun 24 10:53:01 2022
```

```
( Share Enumeration on 10.10.80.98 )

        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.
```

Question 4

Use smbclient tool and do trial and error method for every sharelist.

```
┌──(1211103184㉿kali)-[~]
└─$ smbclient //10.10.80.98/tbfc-hr
Enter WORKGROUP\1211103184's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
```

```
┌──(1211103184㉿kali)-[~]
└─$ smbclient //10.10.80.98/tbfc-santa
Enter WORKGROUP\1211103184's password:
Try "help" to get a list of possible commands.
smb: \>
```

Question 5

Use the help command and search through the command lists.

```
┌──(1211103184㉿kali)-[~]
└─$ smbclient //10.10.80.98/tbfc-santa
Enter WORKGROUP\1211103184'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            utimes         logoff         ..
!
smb: \>
```

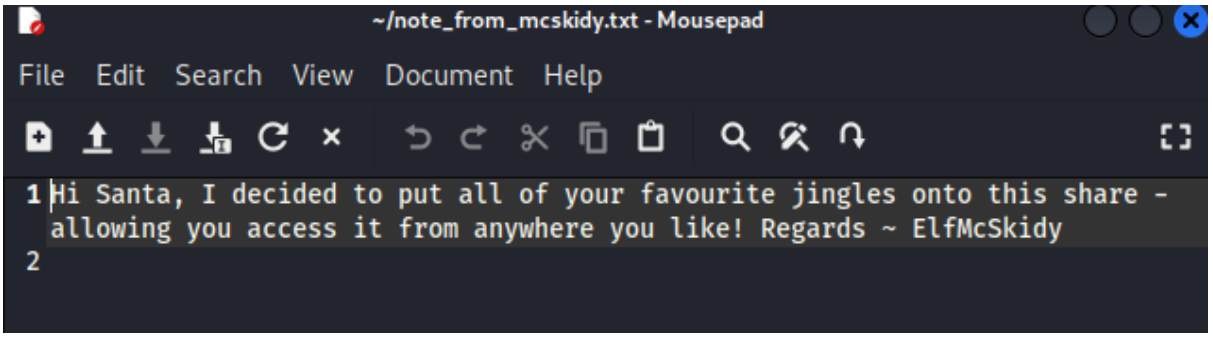
Type **dir** in the terminal to search for directory.

```
smb: \> dir
  .                                   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

                10252564 blocks of size 1024. 5368140 blocks available
smb: \>
```

Get the note from McSkidy and read it.

```
smb: \> get note_from_mcskidy.txt
getting file \note_from_mcskidy.txt of size 143 as note_from_mcskidy.txt (0.2 KiloBy
tes/sec) (average 0.2 KiloBytes/sec)
smb: \>
```



Thought Process/Methodology:

After you get the IP address, use enum4linux help command and look for every command list given. Then, use the -U command to get the user lists. Likewise, use the -S command to acquire the share lists and use the smbclient tool for every sharelist until you get the one without password. Look through every Samba command and use the dir command. Subsequently, you will get the jingle tunes and a note from McSkidy.