PSP0201
WEEKLY WRITE UP
WEEK 3
GROUP 7

Group Name : Sang Haekeo (The Hackers)

Sang
- Taken from a Malay word , sang , meaning ‘the’

Haekeo
- Taken from a Korean word , 해커 , meaning ‘hacker’
-

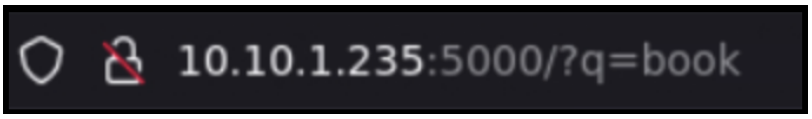
ID	NAME	ROLE	TASK
1211102162	AMILIA NADZEERA BINTI BAHARUDIN	Leader	- Day 6 & 7 write up
1211100930	KU NAJWA SYAUQINA BINTI KU AZRIN	Member	
1211101693	SAVITHA MURUGUMUNISEGARAN	Member	- Day 8 & 9 write up

Day 6 ; Web Exploitation : Be careful with what you wish on Christmas Night

Question 2 : What vulnerability type was used to exploit the application?

The 'Make a Wish' website mechanics works by storing the values entered in the form and writing them into memory, just like a comment on social media. Based on what we have found, the type of the vulnerability is 'Stored Cross Site Scripting'.

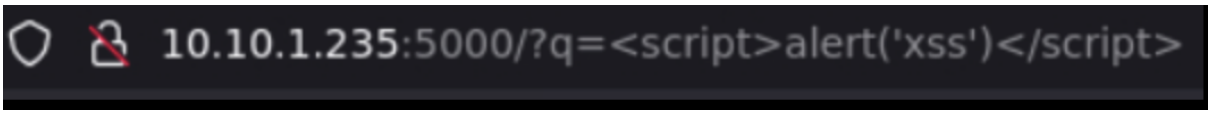
Question 3 : What query string can be abused to craft a reflected XSS?



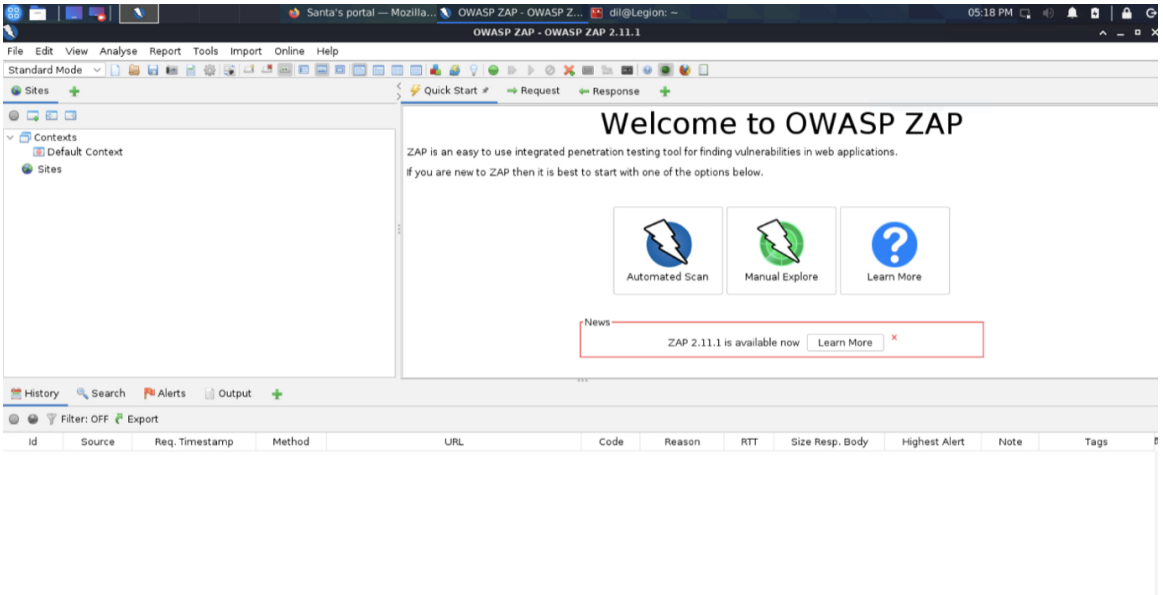
When we look for 'book' the url changes to

```
http://<ip>/?q=<value>
```

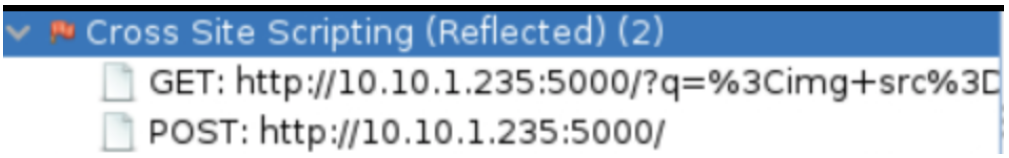
The '?' symbol represents that the GET method is being used , 'q' is the parameter and '=' is the value of the parameter.
The reflected XSS query string in URL is shown below



Question 4 : Launch the OWASP ZAP application



Question 5 : Run a ZAP (zaproxy) automated scan on the target. How many XSS alerts are in the scan?



On the OWASP ZAP interface we click on the “Automated Scan”. We pasted the URL of the targeted website and clicked on ‘Attack’

6. Explore the XSS alerts that ZAP has identified, are you able to make an alert appear on the “Make a wish” website?

To make the alert appear , we have used an alert function

```
<script> alert(‘xss’)</script>
```

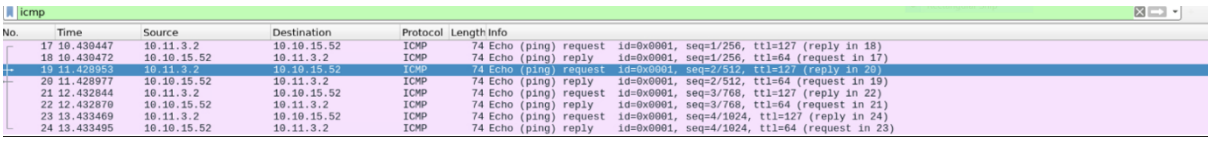
This code could be inserted in the ‘New Wish’ field.

Day 7 ; Networking : The grinch really did steal Christmas

Question 1 : Open “pcap1.pcap” in Wireshark. What is the IP address that initiates an ICMP/ping?

```
┌──(dil㉿Legion)-[~/course/tryhackme/rooms/25-Days-of-Cyber-Security/day7]
└─$ unzip aoc-pcaps.zip
Archive:  aoc-pcaps.zip
  inflating: pcap1.pcap
  inflating: pcap2.pcap
  inflating: pcap3.pcap
┌──(dil㉿Legion)-[~/course/tryhackme/rooms/25-Days-of-Cyber-Security/day7]
└─$ ls -lah
total 8.5M
drwxr-xr-x 2 dil dil 4.0K Jan  7 22:17 .
drwxr-xr-x 5 dil dil 4.0K Jan  7 22:16 ..
-rwxrwxrwx 1 dil dil 4.2M Jan  7 22:15 aoc-pcaps.zip
-rw-r--r-- 1 dil dil 3.7M Nov 30  2020 pcap1.pcap
-rw-r--r-- 1 dil dil  35K Nov 30  2020 pcap2.pcap
-rw-r--r-- 1 dil dil 598K Nov 30  2020 pcap3.pcap
```

There are three files inside , pcap1.pcap, pcap2.pcap, and pcap3.pcap



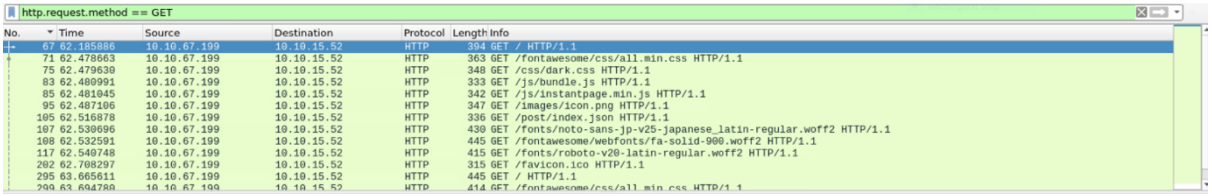
Open up wireshark , and apply a filter. Type in ICMP/PING protocol.

Packet number 17 is the first packet that uses ICMP/PING protocol. We can search the IP that initiates the connection by looking at the ‘Source’ column, that is ‘10.11.3.2’.

Question 2: If we only wanted to see HTTP GET requests in our “pcap1.pcap” file,

what filter would we use?

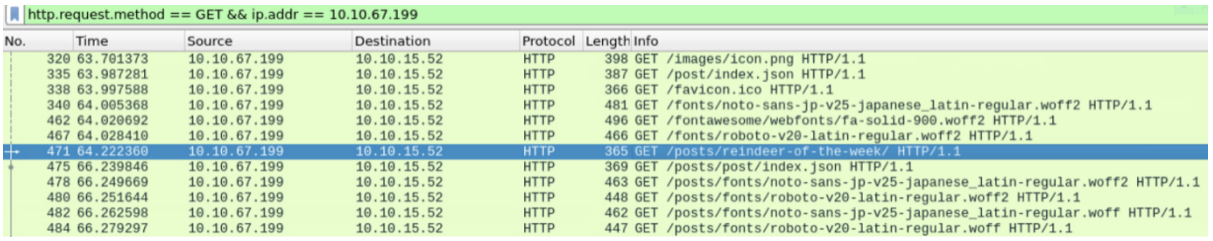
```
http.request.method == GET
```



Question 3 : Now apply this filter to “pcap1.pcap” in Wireshark, what is the name of the article that the IP address “10.10.67.199” visited? [Hint: /posts/]

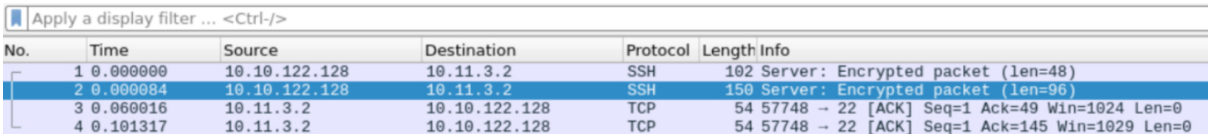
Using hint on question 3,On wireshark, the filter that we would apply are

```
http.request.method == GET && ip.addr == 10.10.67.199
```



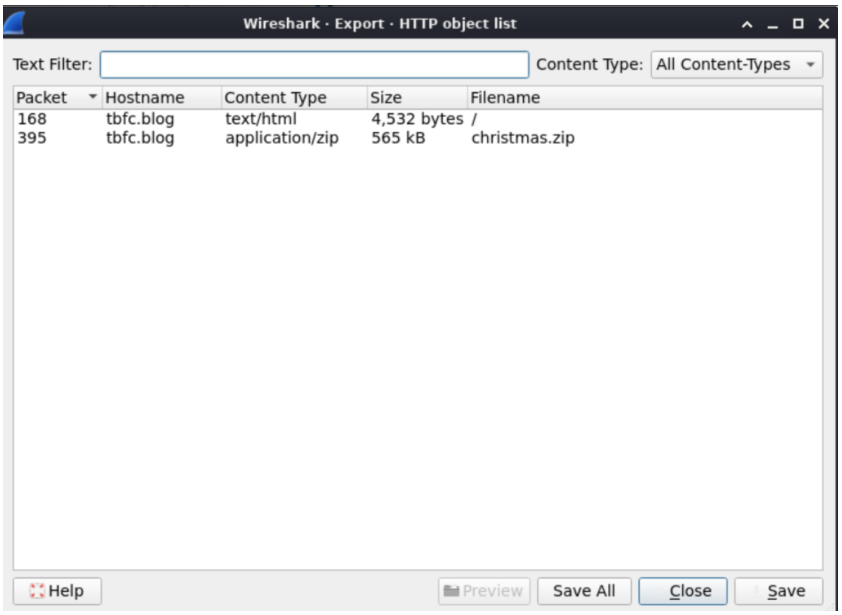
Based on the filter result, packet number 471 seems suspicious because the info column tells us it has ‘/posts/’ in it and the string ‘reindeer-of-the-week’ kind of an article title.

5. Continuing with our analysis of “pcap2.pcap”, what is the name of the protocol that is encrypted?



6. What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

Open wireshark and go to the export project. We Open terminal/file manager, there is a new file '%2f 'and 'christmas.zip'. After we unzip the file, there is a file named 'elf_mcskidy_wishlist.txt'. Inside the file, there is a list of wishes. One of them is 'x1 Rubber ducky (to replace Elf McEager)'



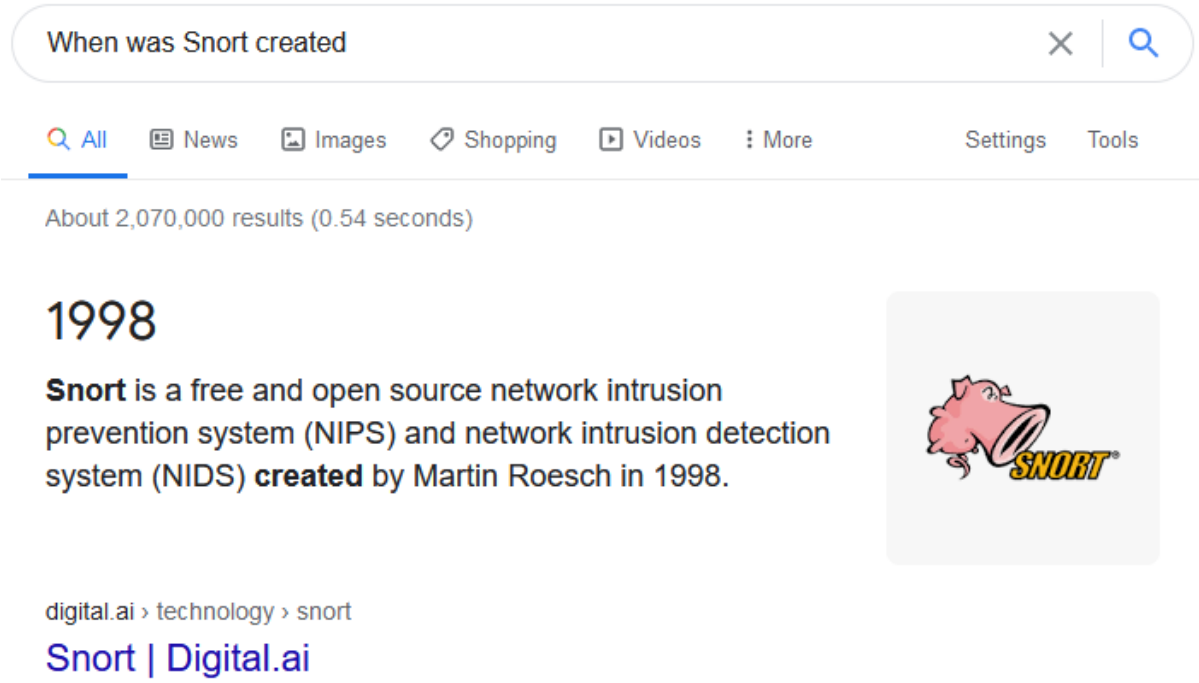

```
┌──(dil㉿Legion)-[~/course/tryhackme/rooms/25-Days-of-Cyber-Security/day7]
└─$ file christmas.zip
christmas.zip: Zip archive data, at least v2.0 to extract, compression method=deflate
┌──(dil㉿Legion)-[~/course/tryhackme/rooms/25-Days-of-Cyber-Security/day7]
└─$ unzip christmas.zip
Archive:  christmas.zip
  inflating: AoC-2020.png
  inflating: christmas-tree.jpg
  inflating: elf_mcskidy_wishlist.txt
  inflating: Operation Artic Storm.pdf
  inflating: selfie.jpg
  inflating: tryhackme_logo_full.svg
┌──(dil㉿Legion)-[~/course/tryhackme/rooms/25-Days-of-Cyber-Security/day7]
└─$ ls -la
total 9796
drwxr-xr-x 2 dil dil    4096 Jan  8 13:29  .
drwxr-xr-x 5 dil dil    4096 Jan  7 22:16  ..
-rw-r--r-- 1 dil dil    4532 Jan  8 13:28  %2f
-rw-r--r-- 1 dil dil   97267 Nov 30  2020  AoC-2020.png
-rwxrwxrwx 1 dil dil 4375867 Jan  7 22:15  aoc-pcaps.zip
-rw-r--r-- 1 dil dil  296783 Nov 30  2020  christmas-tree.jpg
-rw-r--r-- 1 dil dil  565069 Jan  8 13:28  christmas.zip
-rw-r--r-- 1 dil dil     134 Nov 30  2020  elf_mcskidy_wishlist.txt
-rw-r--r-- 1 dil dil   97601 Nov 30  2020 'Operation Artic Storm.pdf'
-rw-r--r-- 1 dil dil 3800495 Nov 30  2020  pcap1.pcap
-rw-r--r-- 1 dil dil   35490 Nov 30  2020  pcap2.pcap
-rw-r--r-- 1 dil dil  611893 Nov 30  2020  pcap3.pcap
-rw-r--r-- 1 dil dil   93831 Nov 30  2020  selfie.jpg
-rw-r--r-- 1 dil dil   20707 Nov 30  2020  tryhackme_logo_full.svg
┌──(dil㉿Legion)-[~/course/tryhackme/rooms/25-Days-of-Cyber-Security/day7]
└─$ cat elf_mcskidy_wishlist.txt
Wish list for Elf McSkidy
-------------------------
Budget: £100

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

Day 8: What's Under The Christmas Tree!

Question 1

When was Snort created?

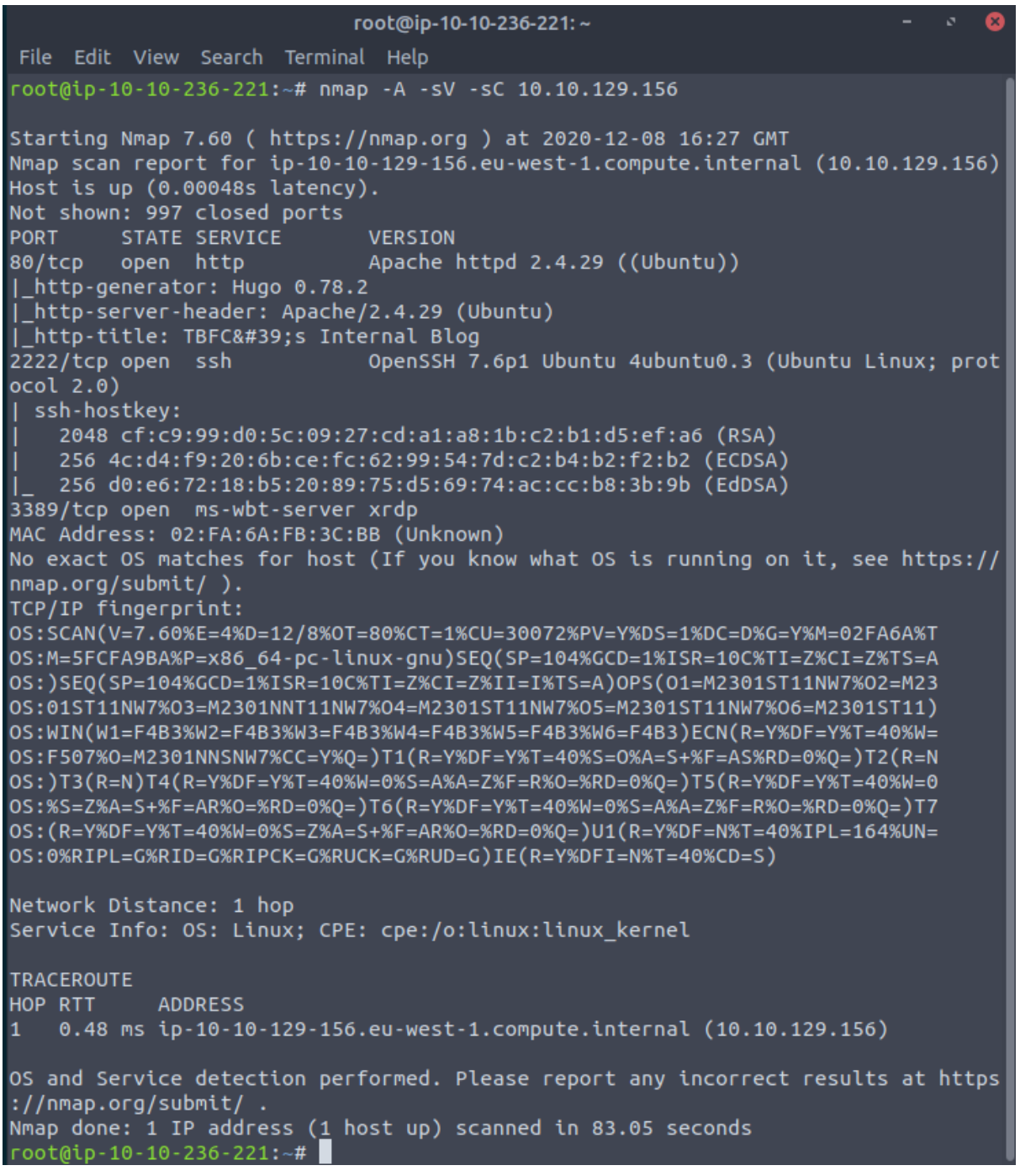
For this one, a short Google search revealed that Snort was developed in 1998:



Question 2

Using Nmap on 10.10.129.156, what are the port numbers of the three services running? (Please provide your answer in ascending order/lowest -> highest, separated by a comma)

We first ran a nmap scan against that IP address:



A HTTP server on port 80, SSH on port 2222, and a remote desktop connection on port 3389 are the three open ports that are displayed here.

Question 5

Use Nmap to determine the name of the Linux distribution that is running, what is reported as the most likely distribution to be running?

There are multiple references to Ubuntu while looking at the scan results up above.

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-12-08 16:35 GMT
Nmap scan report for ip-10-10-129-156.eu-west-1.compute.internal (10.10.129.156)
Host is up (0.00050s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; prot
ocol 2.0)
```

Question 6

Use Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver. Based on the value returned, what do we think this website might be used for?

Examine the HTTP-title section carefully, paying great attention to the web server (port 80), using the initial scan as a reference once more. This indicates that it serves as a blog.

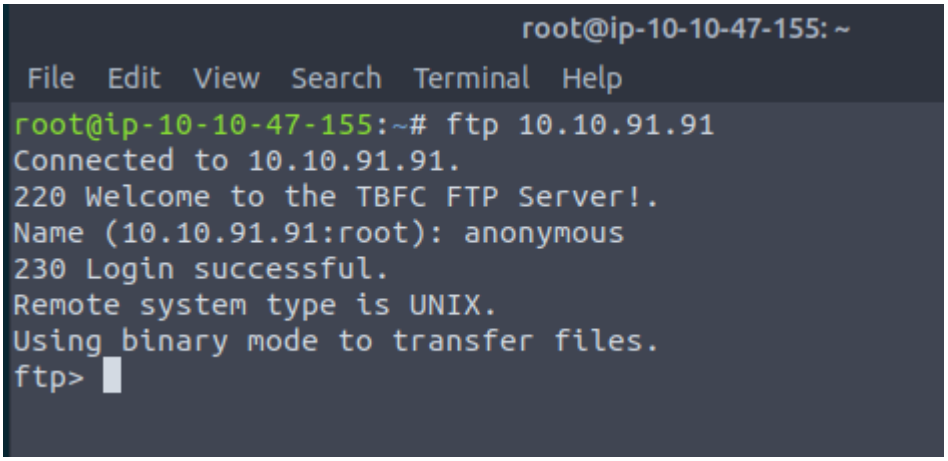
```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-12-08 16:35 GMT
Nmap scan report for ip-10-10-129-156.eu-west-1.compute.internal (10.10.129.156)
Host is up (0.00050s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; prot
ocol 2.0)
| ssh-hostkey:
```

Day 9: Anyone Can Be Santa!

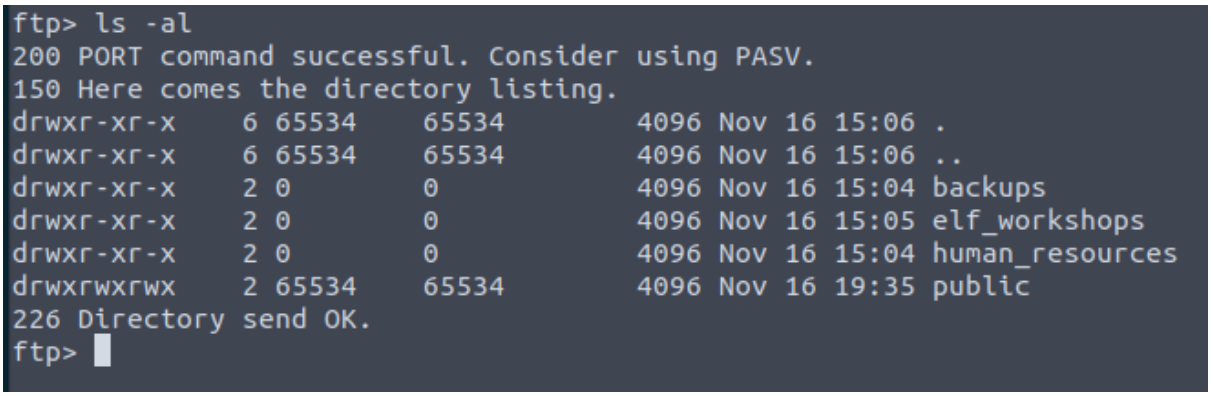
Question 1

Name the directory on the FTP server that has data accessible by the “anonymous” user

We first signed in as "anonymous" to the FTP server:



After examining the directories, we can see that there is one that the anonymous user may access and is open to the public:



Question 2

What script gets executed within this directory?

We moved directories into "public" and then searched through the contents to discover the answer to this. Within is a script with the name of backup.sh.

```
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 19:35 .
drwxr-xr-x    6 65534    65534        4096 Nov 16 15:06 ..
-rwxr-xr-x    1 111      113           341 Nov 16 19:34 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16 19:35 shoppinglist.txt
226 Directory send OK.
ftp>
```

Question 3

What movie did Santa have on his Christmas shopping list?

We used the "get" command to acquire the shopping list. We can see it right now since it is on my computer.

```
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 (18.5130 kB/s)
ftp>
```

```
root@ip-10-10-47-155: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-47-155:~# ls
Desktop    Instructions  Postman  shoppinglist.txt
Downloads  Pictures      Scripts  thinclient_drives
root@ip-10-10-47-155:~# cat shoppinglist.txt
The Polar Express Movie
root@ip-10-10-47-155:~#
```

Question 4

Re-upload this script to contain malicious data (just like we did in section 9.6. Output the contents of /root/flag.txt!

In the same manner, We first downloaded the file from the ftp site.

```
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 (6.2539 MB/s)
ftp>
```

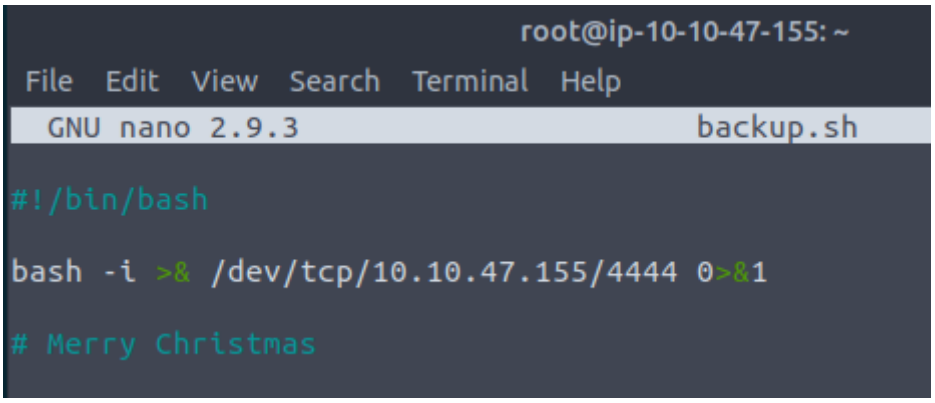
We could then see what was within.

```
root@ip-10-10-47-155: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-47-155:~# ls
backup.sh  Downloads     Pictures  Scripts          thinclient_drives
Desktop    Instructions  Postman   shoppinglist.txt
root@ip-10-10-47-155:~# cat 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


root@ip-10-10-47-155:~#
```

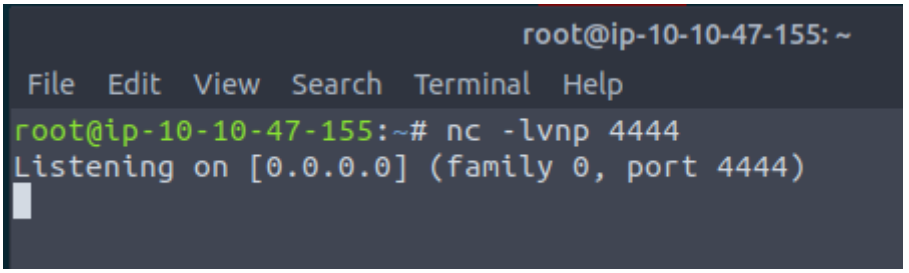
To begin editing, We opened the file in Nano.

```
root@ip-10-10-47-155:~# nano backup.sh
root@ip-10-10-47-155:~#
```

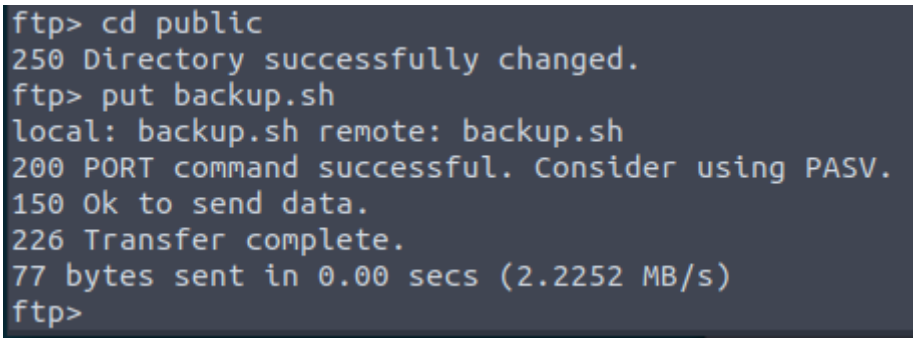
Then removed everything else and replaced it with something that would give me a reverse shell using a Reverse Shell Cheat Sheet.



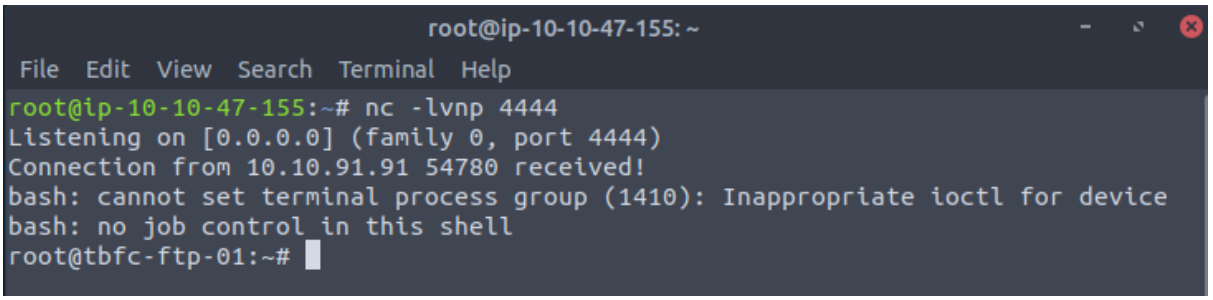
However, before We send it over. We're going to use netcat to create a listener. Use the same port that the script supplied.



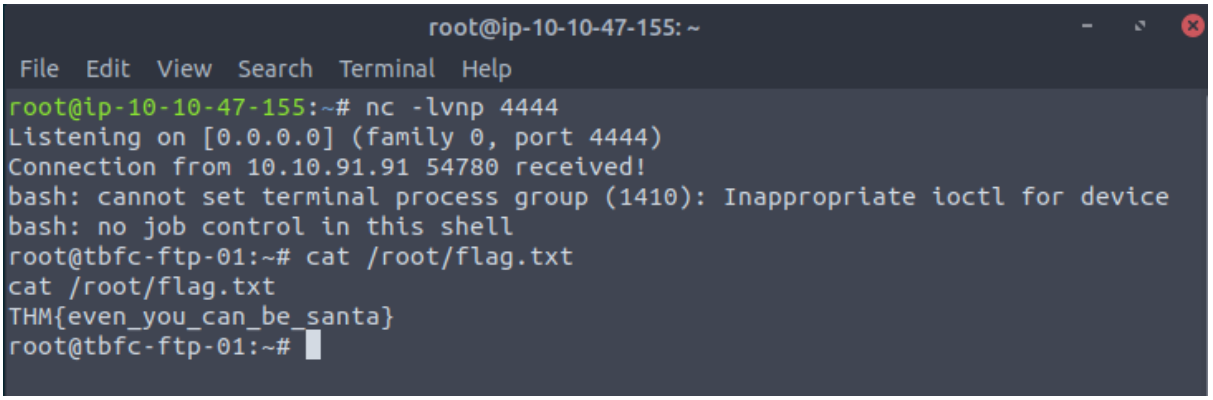
Close and save the document using Ctrl + X, then use the "put" command to submit it to the ftp server. It will be added to the same open file that we have access to.



We will obtain a connection at our listener after a little while:



We just need to go to the flag.txt file from here.



DAY 10 : Networking – Don’t be selfish

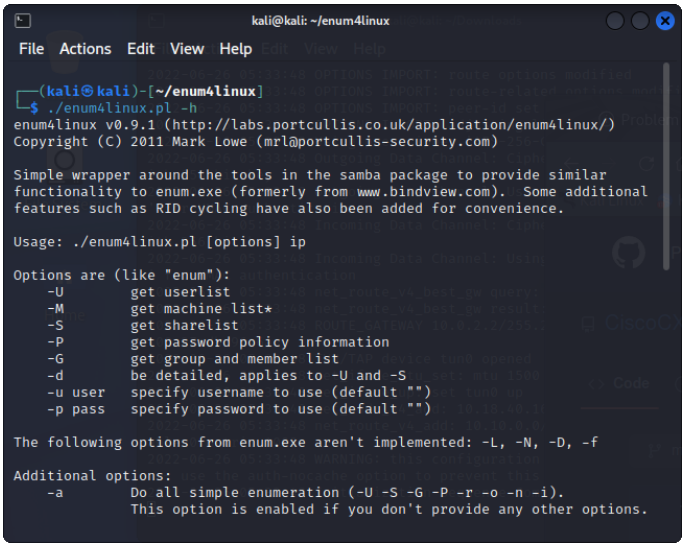
Question 1 : Examine the help options for enum4linux. Match the following flags with the descriptions.

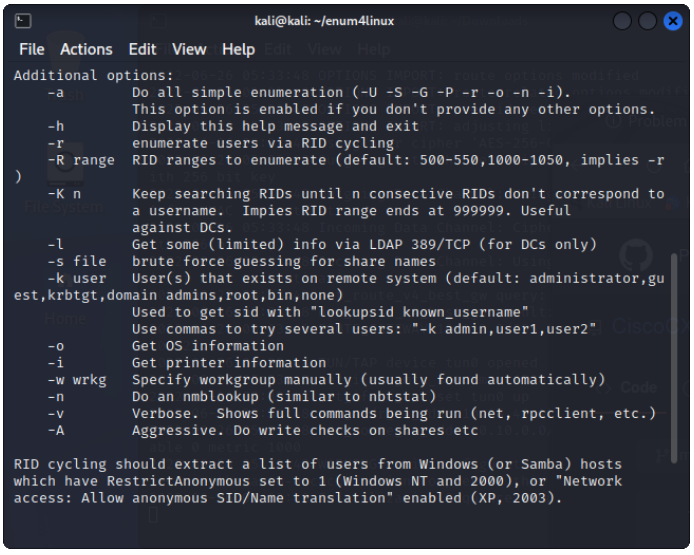
Using command ./enum4linux.pl -h to get help.

-S = get sharelist

-a = do all simple enumeration

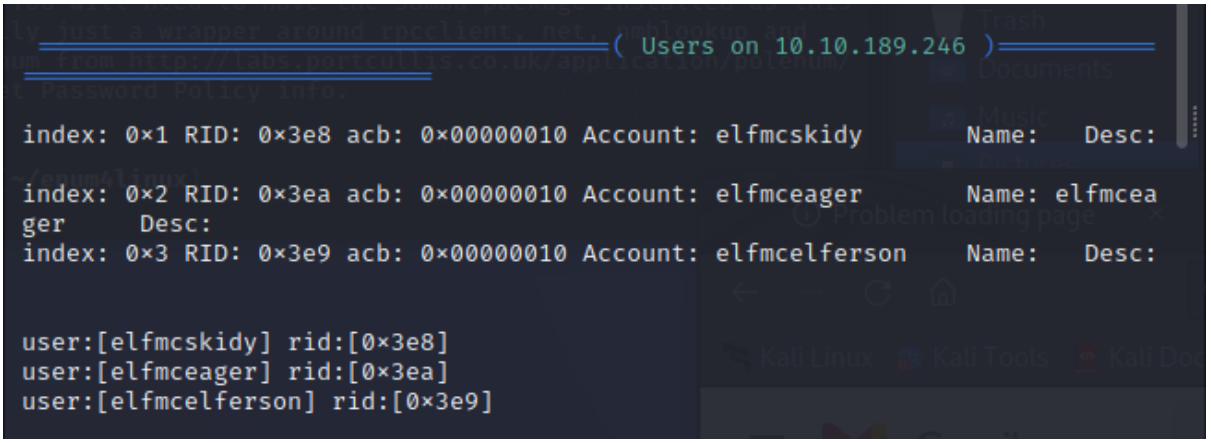
-o = get os information





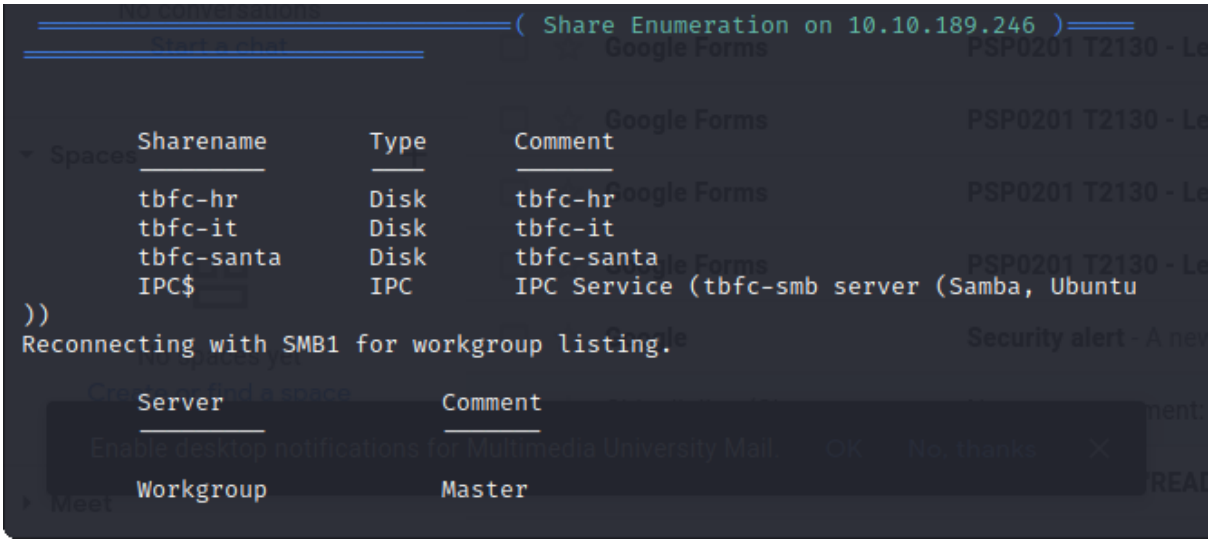
Question 2 : Using enum4linux, how many users are there on the Samba server? 3

Get userlist by using command ./enum4linux.pl -U 10.10.189.246



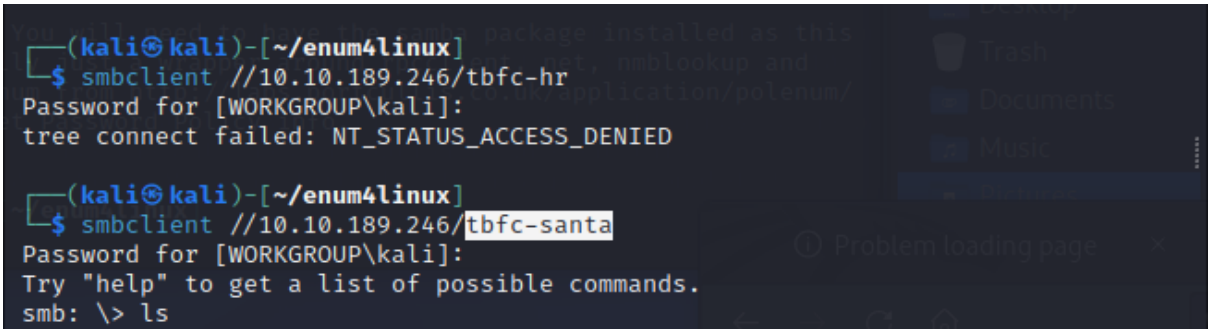
Question 3 : Now how many "shares" are there on the Samba server? 4

Get sharelist by using command ./enum4linux.pl -S 10.10.189.246



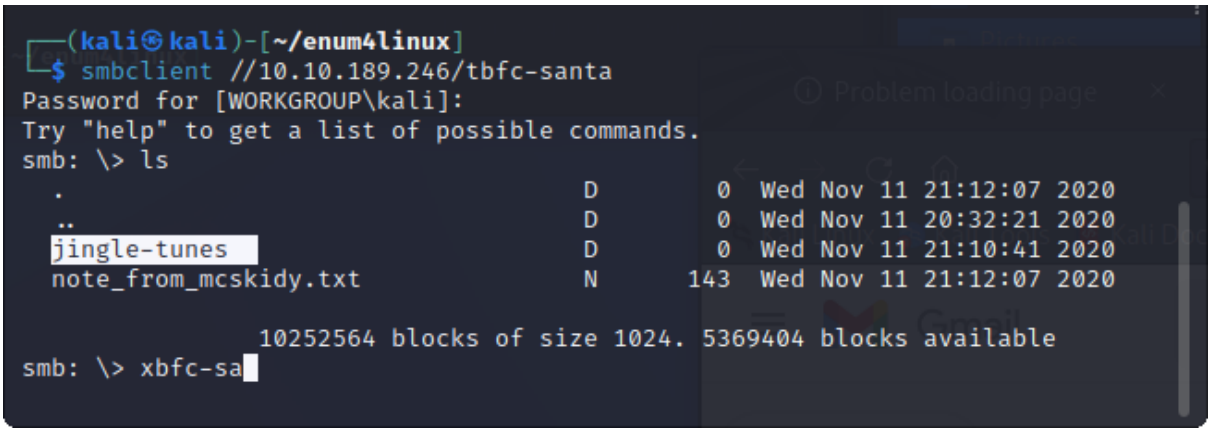
Question 4 : Use smbclient to try to login to the shares on the Samba server. What share doesn't require a password?

tbfc-santa



Question 5 : Log in to this share, what directory did ElfMcSkidy leave for Santa?

jingles-tunes



Thought/Process Mythology

To start off, We need to download enum4linux. Once downloaded, use terminal and command to get help. From that we can get the userlist by using command -u. We get the sharelist by using command -s. We get a sharename that doesn't require a password by logging in one by one using smbclient command. Once login we need to find the directory by using command ls.