# Week 3

# Writeup

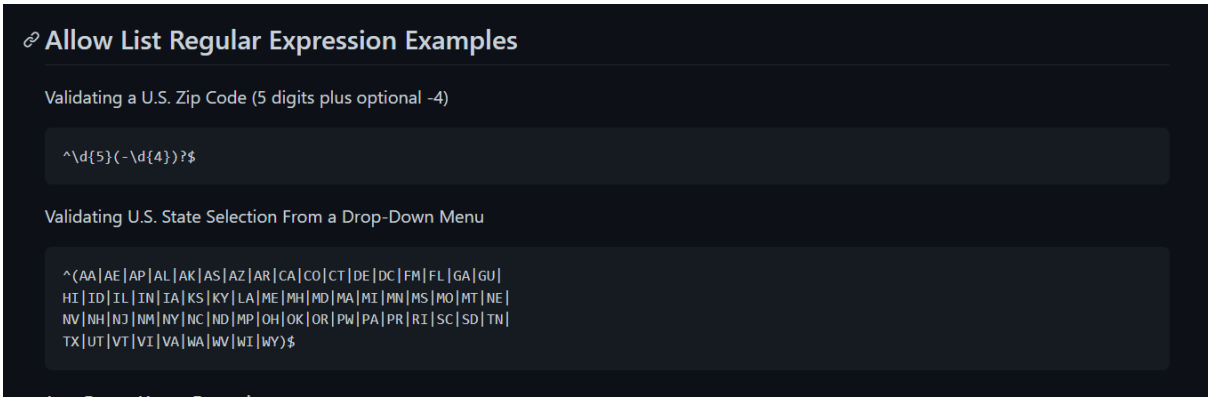
## Group Name:HUSTLERS

## Members

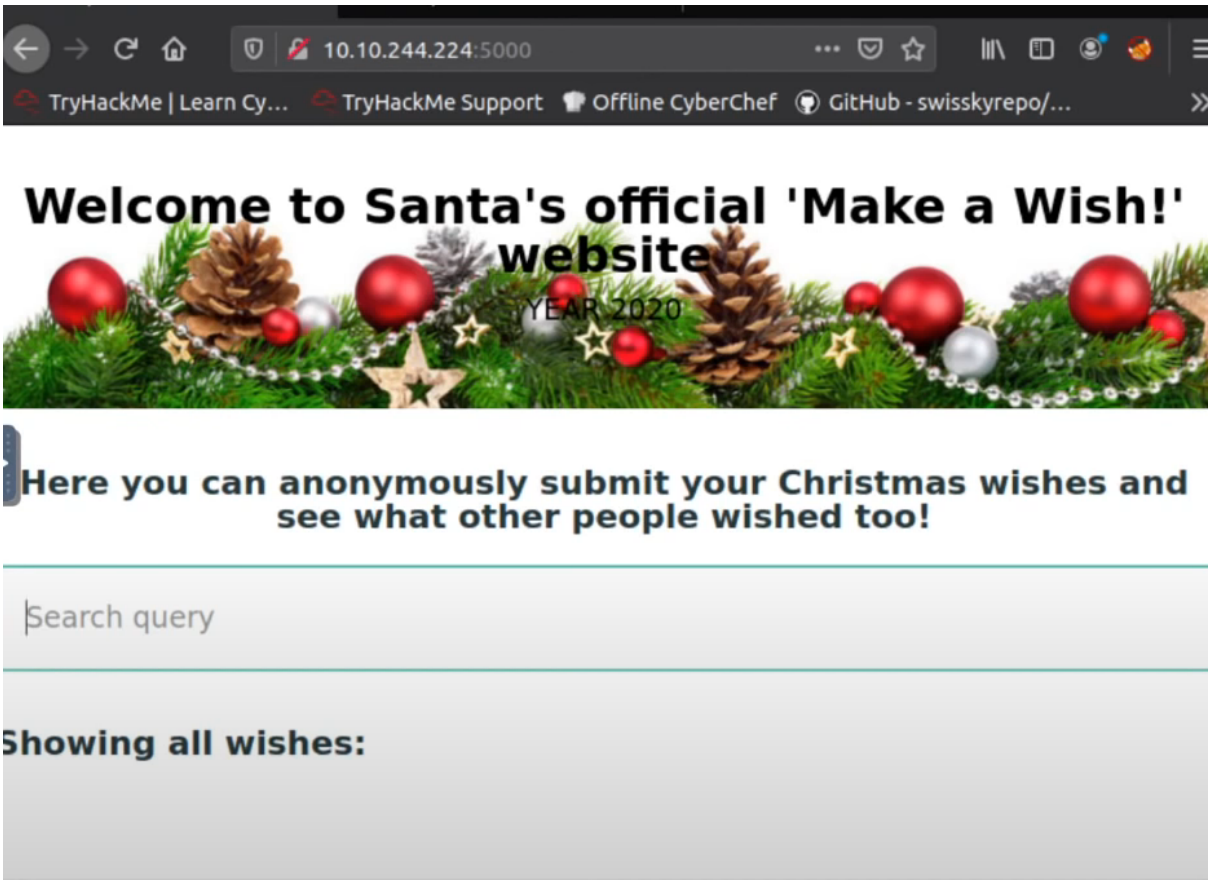
| ID | Name | Role |
|---|---|---|
| 1211100708 | Muhammad Faiz BIn Mohd Fauzi | leader |
| 1211101962 | Barath A L Saravanan | member |
| 1211101804 | AKHILESHNAIDU A/L JAYA KUMAR | member |

Day 6 - [Web Exploitation] Be careful with what you wish on a Christmas night
Tools used = Kali linux, Firefox

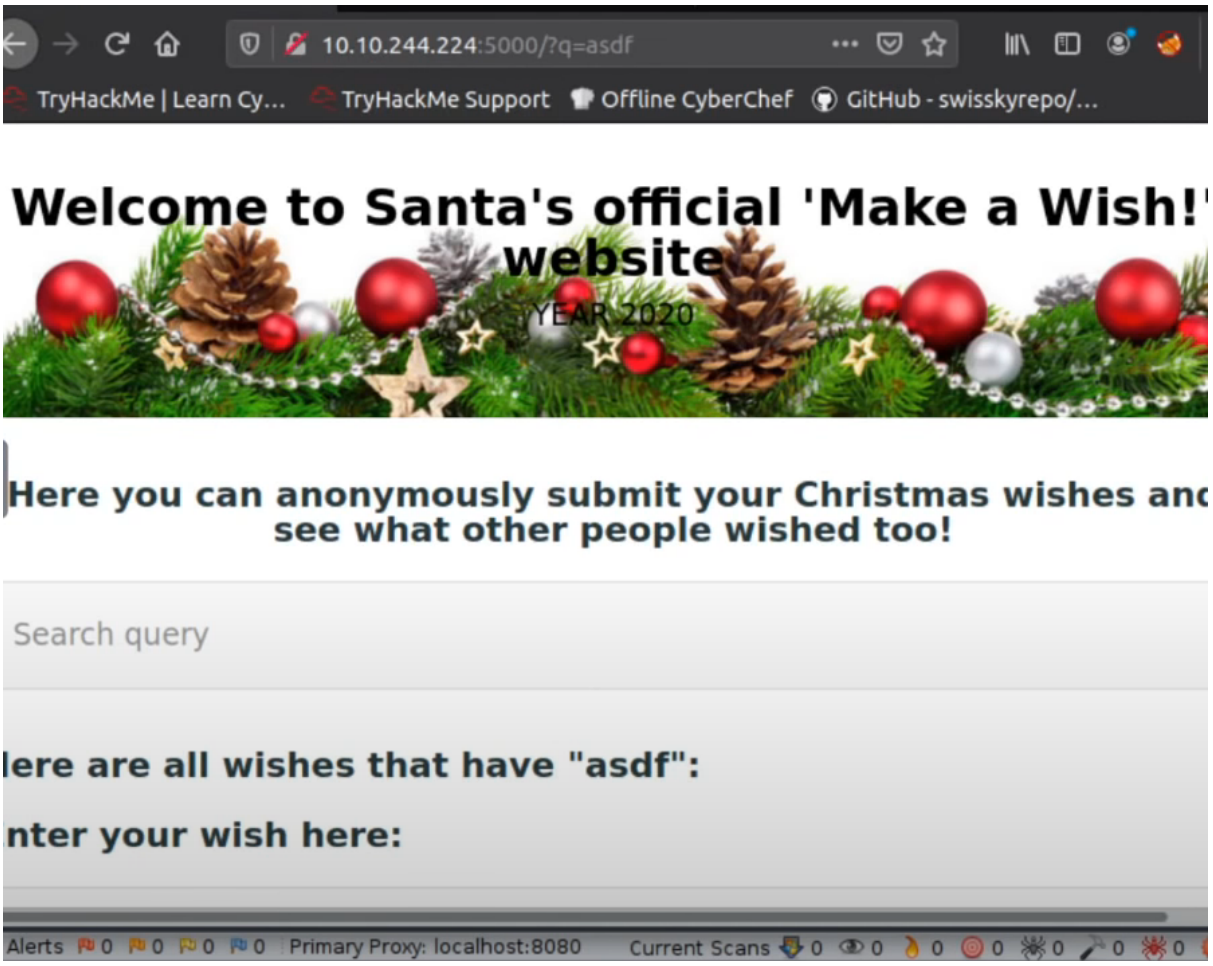
Question 1&2



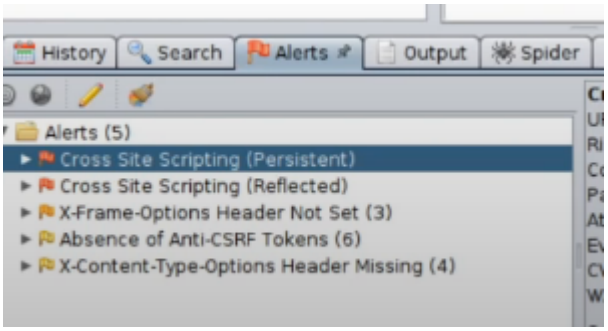

Question 3



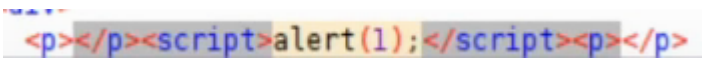
Question 4




Question 5&7
5 Alerts and 2 Cross site scripting




Question 6
Coding in Javascript



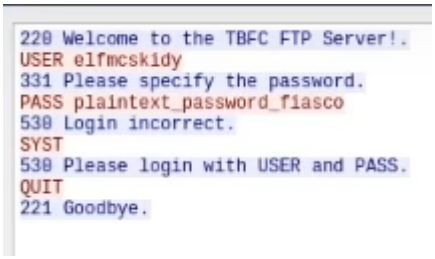
Day 7 [Networking] The Grinch Really Did Steal Christmas
Tools used: Wireshark,Kali linux, Firefox

Question 1
IP address that initiates an ICMP/ping


Question 2
filter would we use to see HTTP GET requests in our "pcap1.pcap" file


Question 3
name of the article that the IP address "10.10.67.199" visited

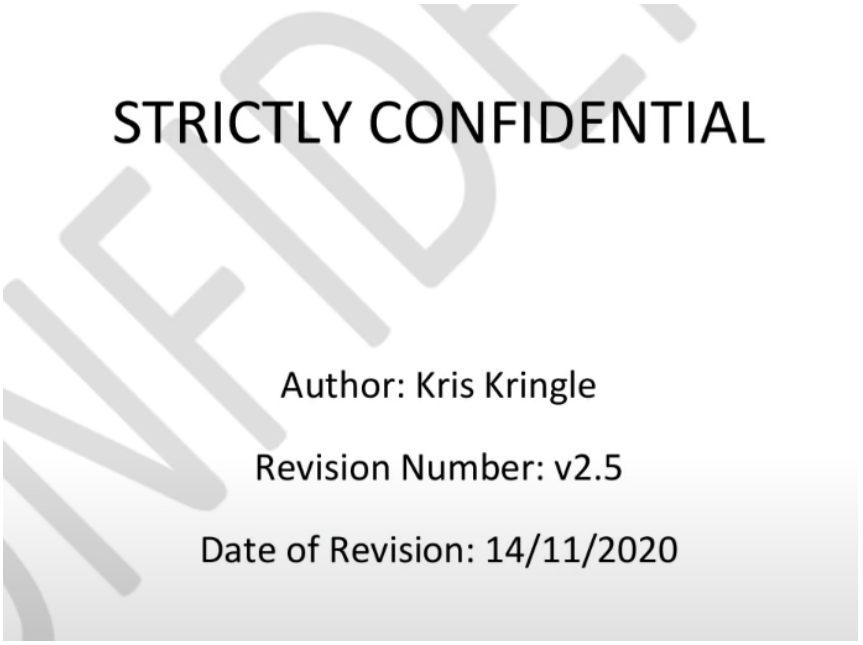

Question 4
password was leaked during the login process




Question 5
the name of the protocol that is encrypted

Question 8&9

Elf McSkidy's wishlist that will be used to replace Elf McEager and the author of Operation Artic Storm


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

Tools used: Kali Linux, nmap,Firefox

Solution/walkthrough:

Question 1

Open browser to search about snort

# 1998

**Snort** is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) **created** by Martin Roesch in 1998.

Question 2,3,4,5 and 6

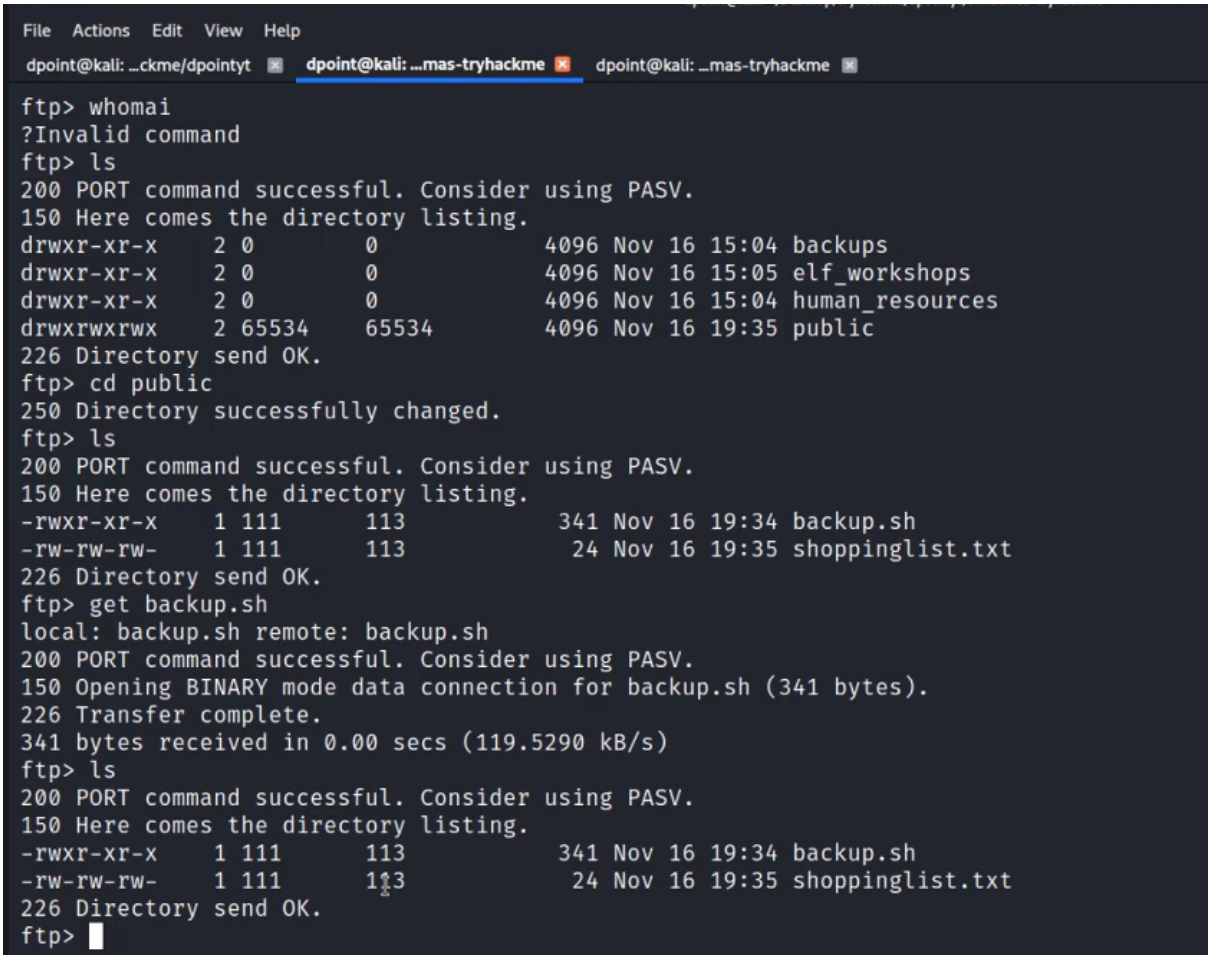
Using Nmap ip address to get the number of ports, the name of the Linux distribution that is running,the version of apache and what this website for.

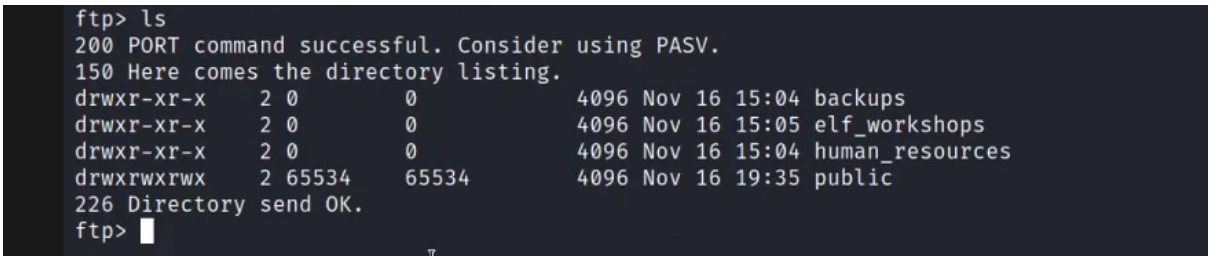
```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; prot
ocol 2.0)
| ssh-hostkey:
|   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 (EdDSA)
3389/tcp open  ms-wbt-server xrdp
MAC Address: 02:FA:6A:FB:3C:BB (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.60%E=4%D=12/8%OT=80%CT=1%CU=30072%PV=Y%DS=1%DC=D%G=Y%M=02FA6A%T
OS:M=5FCFA9BA%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10C%TI=Z%CI=Z%TS=A
OS:)SEQ(SP=104%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M2301ST11NW7%O2=M23
OS:01ST11NW7%O3=M2301NNT11NW7%O4=M2301ST11NW7%O5=M2301ST11NW7%O6=M2301ST11)
OS:WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=
OS:F507%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N
OS:)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0
OS:%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7
OS:(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=
OS:0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

Day 9 - [Networking] Anyone can be Santa!

Tools used = KALI LINUX,FIREFOX

Question 1

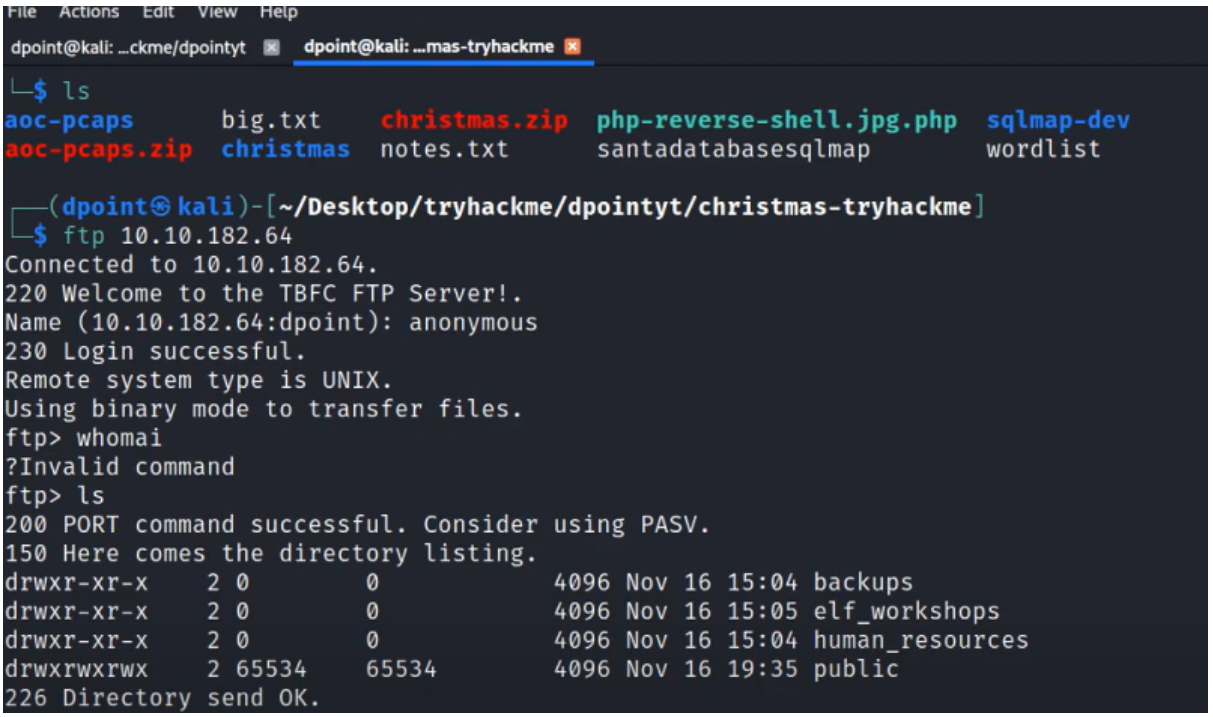



Backups,elf_workshops,human_resources and public found on FTP site.

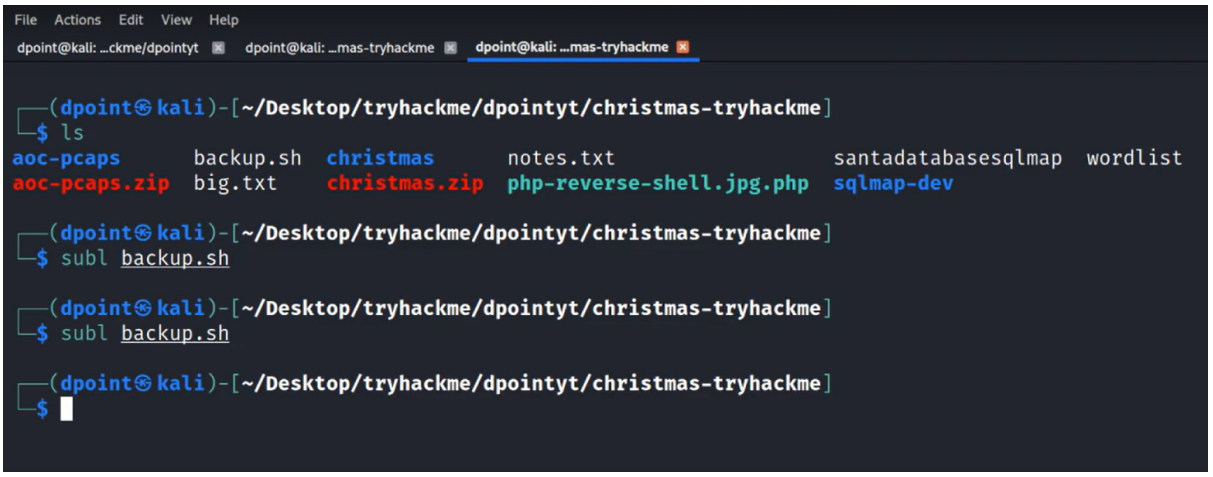
Question 2

Directory on the FTP server that has data accessible by the "anonymous" user is public

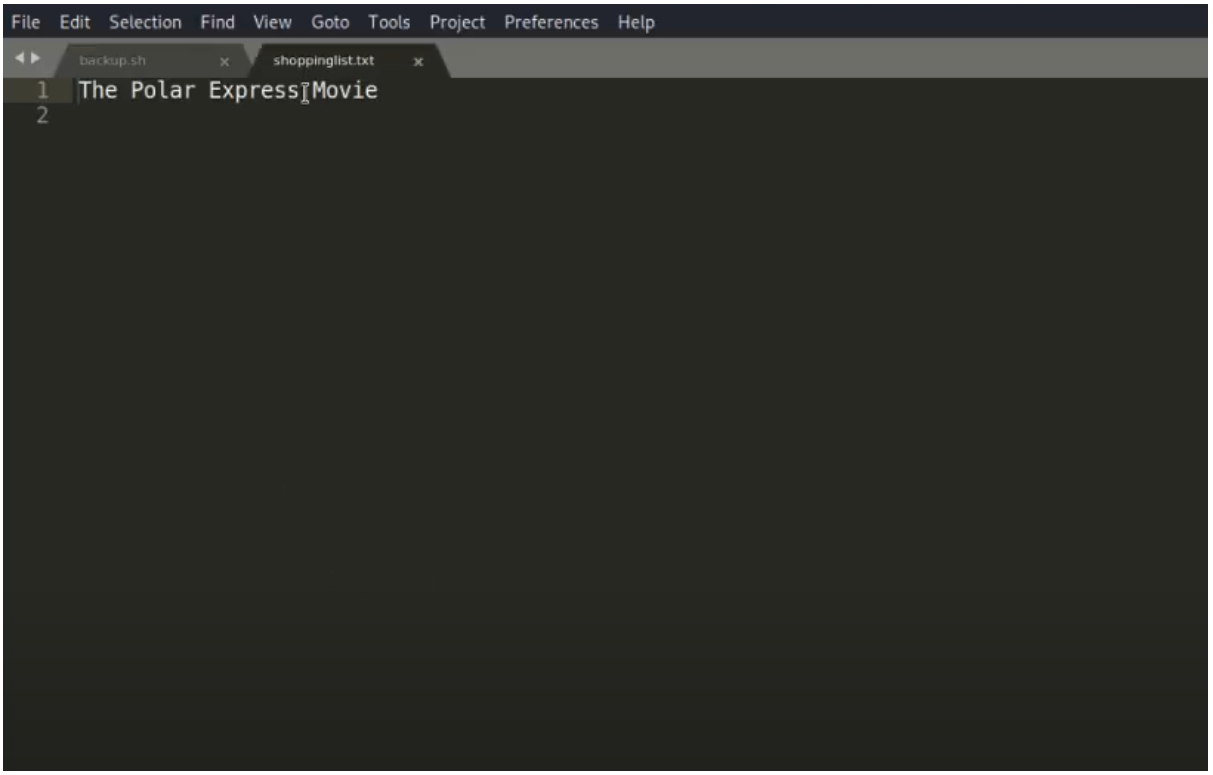


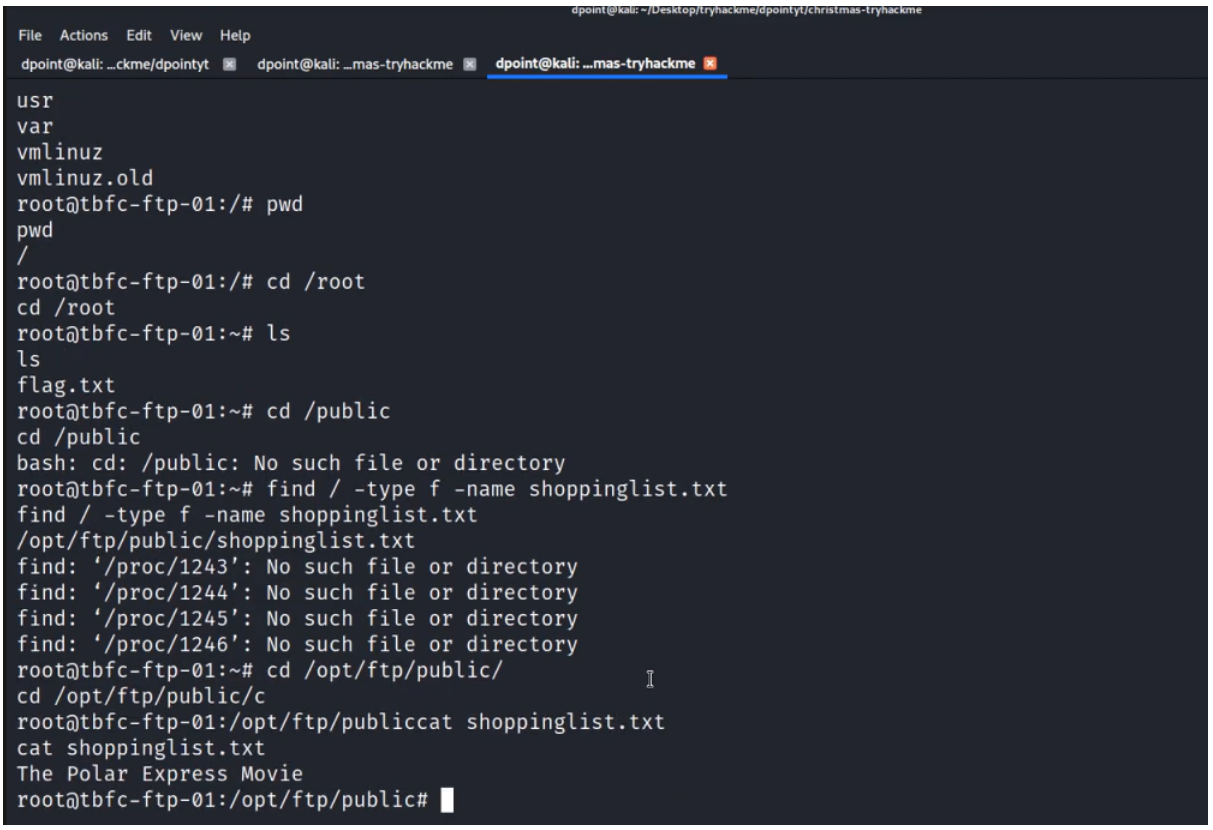

Question 3

Backup.sh script gets executed within this directory?



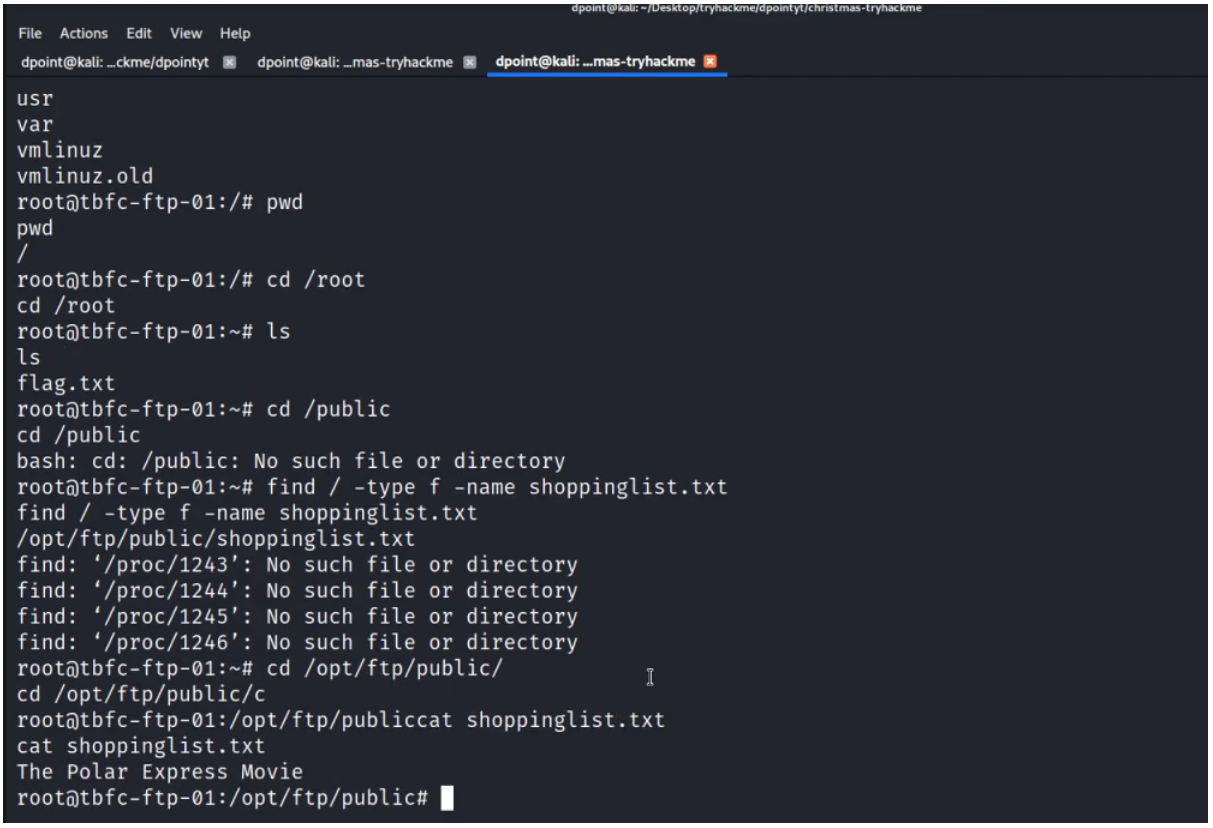

Question 4



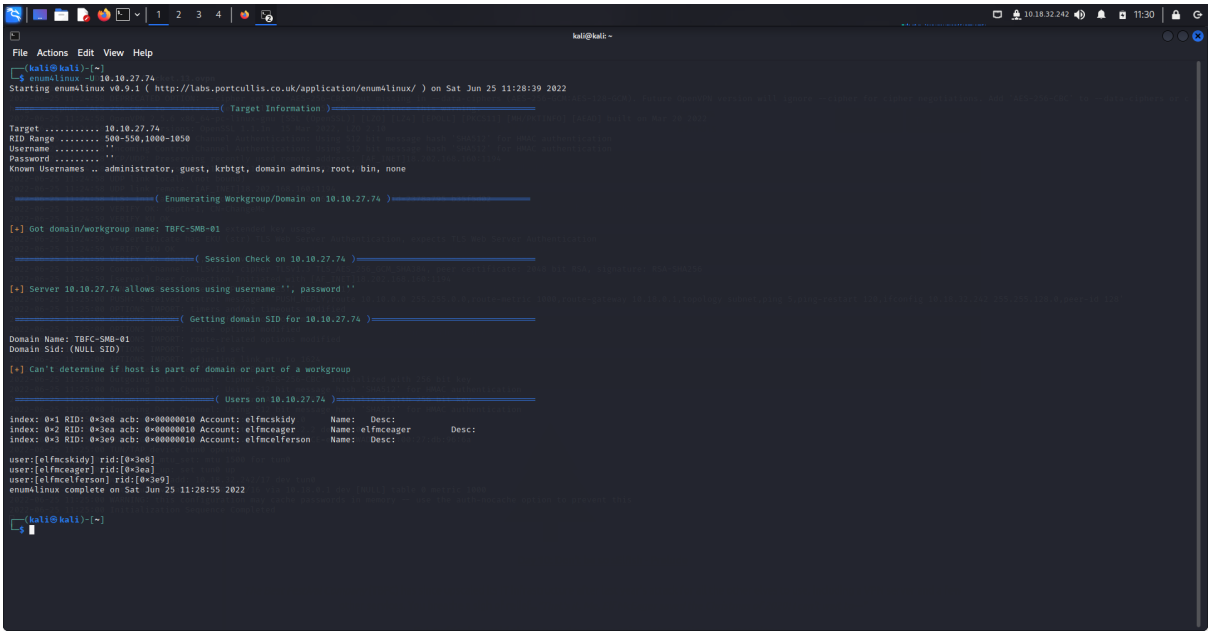



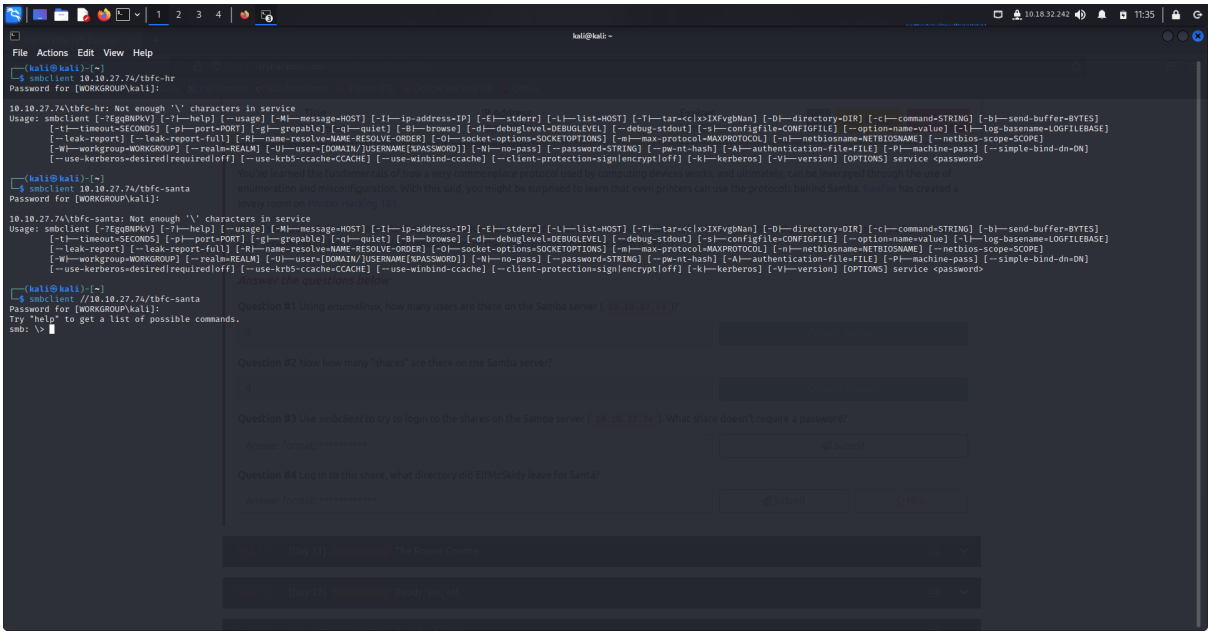

Christmas shopping list movie - The Polar Express

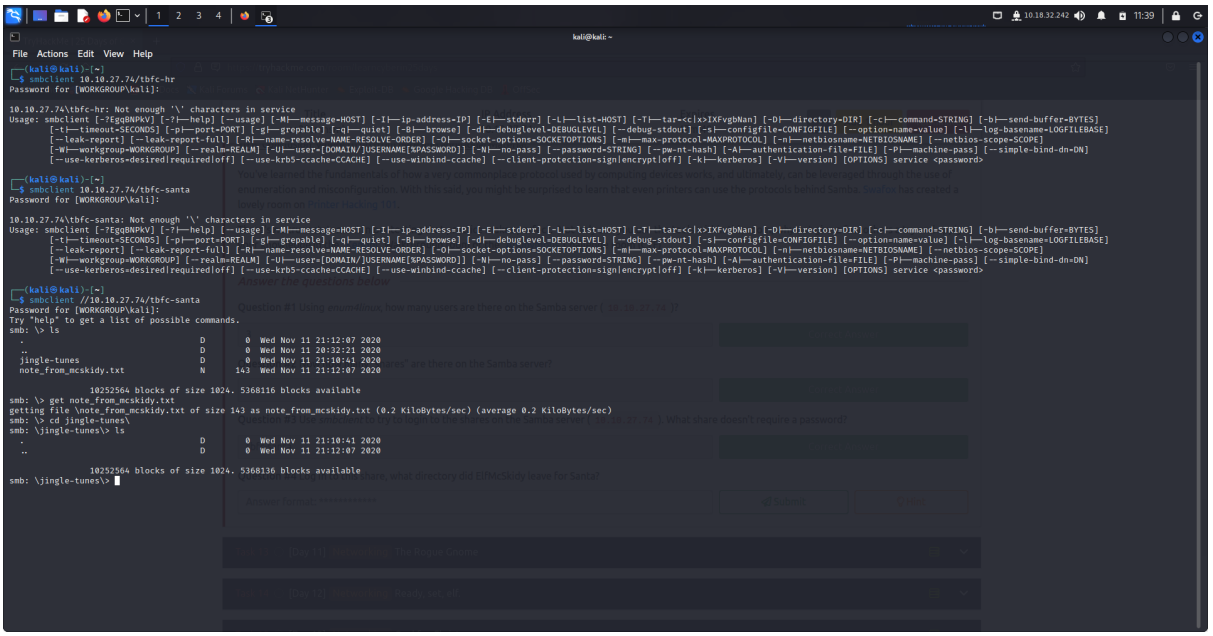
Question 5




Day 10 -[Networking] Don't be sElfish!
Tools used = KALI LINUX,FIREFOX






All answers for questions 1,2,3,4,5 are displayed in these screenshots.

It basically shows the amount of users.
And share that does not require password.
directory did ElfMcSkidy leave for Santa- (jingle-tunes)